CyberHubs

Ανάλυση Αναγκών των Δεξιοτή-των Κυβερνοασφάλειας

Ελλάδα

Co-funded by
the European Union

Δίκτυο Ευρωπαϊκών Κόμβων Δεξιοτήτων Κυβερνοασφάλειας

Ανάλυση Αναγκών των Δεξιοτήτων Κυβερνοασφάλειας (ΕΛΛΑΔΑ)

Σχετικά με τα CyberHubs

Το ευρωπαϊκό δίκτυο κόμβων δεξιοτήτων κυβερνοασφάλειας (CyberHubs) είναι ένα τριετές έργο που αποσκοπεί στην ενίσχυση του οικοσυστήματος δεξιοτήτων κυβερνοασφάλειας στην Ευρώπη. Θα δημιουργήσει ένα δίκτυο επτά κόμβων δεξιοτήτων κυβερνοασφάλειας στο Βέλγιο, την Εσθονία, την Ελλάδα, την Ουγγαρία, τη Λιθουανία, τη Σλοβενία και την Ισπανία, το οποίο θα προωθήσει την ανάπτυξη ψηφιακών δεξιοτήτων στον τομέα της κυβερνοασφάλειας και θα υποστηρίξει την ανάπτυξη ενός εξειδικευμένου εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας.

Τα αναμενόμενα αποτελέσματα του έργου περιλαμβάνουν τη δημιουργία ενός βιώσιμου ευρωπαϊκού δικτύου κόμβων δεξιοτήτων κυβερνοασφάλειας, την ανάπτυξη εθνικών στρατηγικών δεξιοτήτων κυβερνοασφάλειας, τη δημιουργία καινοτόμων λύσεων κυβερνοασφάλειας μέσω του Hackathon και τη δημιουργία μακροχρόνιων εταιρικών σχέσεων και συνεργασίας με το ευρύτερο οικοσύστημα κυβερνοασφάλειας.

Κοινοπραξία Έργου

Η κοινοπραξία CyberHubs συγκεντρώνει **21** εταίρους – που καλύπτουν 11 ευρωπαϊκά κράτη μέλη – και **3** συνεργάτες.

Εταίροι

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | **Athens University of Economics and Business** | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | **SEPE** | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Συνεργάτες

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Χρηματοδοτείται από την Ευρωπαϊκή Ένωση. Οι απόψεις και οι γνώμες που εκφράζονται είναι αποκλειστικά του/των συγγραφέα/ων και δεν αντανακλούν κατ' ανάγκη εκείνες της Ευρωπαϊκής Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Ούτε η Ευρωπαϊκή Ένωση ούτε ο EACEA μπορούν να θεωρηθούν υπεύθυνοι γι' αυτές

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής

Ένωσης ή του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Δεδομένα ταυτοποίησης εγγράφου

Συγγραφείς	Δημήτρης **Γκρίτζαλης** (ΟΠΑ), Άννα **Ματσούκα** (ΣΕΠΕ), Γιώργος **Ιακωβάκης** (ΟΠΑ), Δέσποινα **Κοντοπούλου** (ΣΕΠΕ)
Συνδρομή	Γιώτα **Παπαρίδου** (ΣΕΠΕ), Δάφνη **Μπινιώρη** (ΣΕΠΕ)
Πρόγραμμα	ERASMUS+
Αναγνωριστικό Έργου	101140030
Κύρια Δράση	Partnerships for cooperation and exchanges of practices
Τύπος Δράσης	Alliances for Education and Enterprises
Πακέτο Εργασίας	WP2 - Cybersecurity skills intelligence, forecast, and strategy
Κύριος Δικαιούχος Πακέτου Εργασίας	Πανεπιστήμιο Τεχνολογίας του Κάουνας (LT)
Παραδοτέο	D2.1 - Cybersecurity skills mismatches analysis
Κύριος Δικαιούχος Παραδοτέου	DIGITALEUROPE (DE)
Δικαιούχοι Φορείς	(1) Σύνδεσμος Ελληνικών Επιχειρήσεων Πληροφορικής & Επικοινωνιών (ΣΕΠΕ) (GR) (2) Οικονομικό Πανεπιστήμιο Αθηνών (ΟΠΑ) (GR)

Κωδικός εγγράφου EU/CyberHubs/WP2/D2.1/GR/SEPE&AUEB/v3.5/06062024

Πίνακας περιεχομένων

Πίνακας Γραφημάτων

Πίνακας Πινάκων

Συνοπτική περιγραφή

Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας στο νέο ψηφιακό περιβάλλον, το οποίο εξελίσσεται με πρωτοφανείς ρυθμούς σε παγκόσμιο επίπεδο. Η προστασία από κυβερνοεπιθέσεις αποτελεί έναν νέο τομέα, στον οποίο η Ελλάδα σημειώνει ραγδαία ανάπτυξη και εξέλιξη ανταποκρινόμενη στις ανάγκες οργανισμών, επιχειρήσεων και πολιτών. Μέσω σύγχρονων και εξειδικευμένων προϊόντων, η χώρα παρέχει συνεχώς αναβαθμιζόμενη προστασία από κυβερνοεπιθέσεις και άλλους ψηφιακούς κινδύνους.

Για να αποτυπωθούν συστηματικά οι ανάγκες σε ρόλους και δεξιότητες στον τομέα της Κυβερνοασφάλειας στην Ελλάδα, ο Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών (ΣΕΠΕ) συνεργάστηκε με μια ομάδα ειδικών υπό την καθοδήγηση του καθηγητή Κυβερνοασφάλειας κ. Δημήτρη Γκρίτζαλη από το Οικονομικό Πανεπιστήμιο Αθηνών (ΟΠΑ). Η συνεργασία αυτή εντάσσεται στο έργο CyberHubs, το οποίο χρηματοδοτείται από το Erasmus+. Η έκθεση ανάλυσης αναγκών σε δεξιότητες κυβερνοασφάλειας αποτελεί το πρώτο παραδοτέο του ελληνικού CyberHub.

Στόχος

Στόχος της παρούσας έκθεσης είναι να εντοπίσει την αναντιστοιχία μεταξύ προσφοράς (κεφάλαιο 3) και ζήτησης (κεφάλαιο 4) σε δεξιότητες κυβερνοασφάλειας στην Ελλάδα. Παρέχει επίσης μια ολοκληρωμένη εικόνα της ωριμότητας, των ευκαιριών και των ιδιαιτεροτήτων του οικοσυστήματος δεξιοτήτων κυβερνοασφάλειας στην Ελλάδα. Στο Κεφάλαιο 2, γίνεται μια συνολική επισκόπηση του ελληνικού οικοσυστήματος κυβερνοασφάλειας.

Μεθοδολογία

Ακολουθήθηκε μια προσέγγιση πολλαπλών μεθόδων (ποσοτική και ποιοτική), η οποία περιλάμβανε: (α) έρευνα γραφείου, (β) έρευνα στα ελληνικά, (γ) αναζήτηση κενών θέσεων εργασίας με τη βοήθεια της πλατφόρμας SAP (Digital Skills Academy Platform) του EIT και (δ) ομάδες εστίασης εμπειρογνωμόνων. Όσον αφορά τις ομάδες εμπειρογνωμόνων, συγκροτήθηκαν δύο από αυτές. Η μία στελεχώθηκε από έμπειρους επαγγελματίες της κυβερνοασφάλειας τόσο από τον ιδιωτικό όσο και από τον δημόσιο τομέα και η δεύτερη από ακαδημαϊκούς που ειδικεύονται στην κυβερνοασφάλεια ή σε στενά συναφή τομέα.

Η χαρτογράφηση των δεξιοτήτων και των ρόλων ακολούθησε το Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (ECSF) του ENISA. Οι αρμοδιότητες κατηγοριοποιήθηκαν επίσης με βάση την αντίστοιχη ταξινομία υψηλής κρισιμότητας σύμφωνα με την Οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση(NIS2).

Αποκαλύφθηκαν έτσι οι κρίσιμες ανάγκες της αγοράς όσον αφορά στις δεξιότητες κυβερνοασφάλειας και τη ζήτηση επαγγελματικών ρόλων, καθώς και τα κενά σε προγράμματα κατάρτισης και εκπαίδευσης.

Αποτελέσματα

Η παρούσα έκθεση αποτελείται από τέσσερα κεφάλαια. Το κεφάλαιο 1 εξηγεί το γενικό πλαίσιο της μελέτης. Το Κεφάλαιο 2 αποτυπώνει το ελληνικό τοπίο παρέχοντας πληροφορίες σχετικά με τα δημογραφικά στοιχεία, την εκπαίδευση, την απασχόληση, την ψηφιακή οικονομία, τις επιχειρήσεις κυβερνοασφάλειας και τα ιδρύματα

κυβερνοασφάλειας. Το Κεφάλαιο 3 αναλύει την πλευρά της προσφοράς, δηλαδή τα προγράμματα εκπαίδευσης και κατάρτισης στον τομέα της κυβερνοασφάλειας. Η έρευνα γραφείου και οι έρευνες που διεξήχθησαν με ακαδημαϊκά ιδρύματα αποκάλυψαν εξειδικευμένα προγράμματα που προσφέρονται από συστήματα τυπικής και μη τυπικής εκπαίδευσης. Το Κεφάλαιο 4 εμβαθύνει στην πλευρά της ζήτησης, αναλύοντας τις ανάγκες σε εργατικό δυναμικό και με βάση τις απαντήσεις της έρευνας από τοπικούς (Έλληνες) εμπειρογνώμονες, παρουσιάζεται ένα τυπικό προφίλ ενός ειδικού στην κυβερνοασφάλεια.

Συμπεράσματα

Αξιολόγηση της ζήτησης

Στη χώρα μας δεν υπάρχουν συστηματικά και αξιόπιστα μέσα για την αντιμετώπιση και αξιολόγηση της ζήτησης δεξιοτήτων κυβερνοασφάλειας, είτε σε βραχυπρόθεσμη είτε σε μακροπρόθεσμη βάση. Ως εκ τούτου, η παρούσα έκθεση είναι μοναδική και τα συμπεράσματά της αντλούνται σε μεγάλο βαθμό από την έρευνα Επαληθεύονται επίσης από τις ομάδες εμπειρογνωμόνων και συμπληρώνονται από τις κενές θέσεις εργασίας που παρέχει το EIT Digital.

Πηγές εφοδιασμού

Στη χώρα μας δεν υπάρχει προπτυχιακό ακαδημαϊκό πρόγραμμα για τις δεξιότητες της κυβερνοασφάλειας, ωστόσο ορισμένα κολέγια προσφέρουν προπτυχιακά προγράμματα σπουδών στην κυβερνοασφάλεια σε συνεργασία με ξένα πανεπιστήμια.

Ενώ υπάρχει ένας καλός αριθμός μεταπτυχιακών προγραμμάτων στον κυβερνοχώρο (τόσο στα ελληνικά δημόσια πανεπιστήμια όσο και σε ορισμένα κολέγια), αρκετές θέσεις φοιτητών παραμένουνκενές.

Επιπλέον, (α) τα ελληνικά πανεπιστήμια μπορούν να χορηγούν διδακτορικά διπλώματα σε φοιτητές με θέμα διατριβής σχετικό με την ασφάλεια στον κυβερνοχώρο ενώ (β) οι σχετικές επαγγελματικές πιστοποιήσεις που παρέχονται από διεθνείς επαγγελματικές ενώσεις, (όπως, ICS2 και ISACA) φαίνεται να παίζουν εμφανώς υποστηρικτικό ρόλο.

Ρόλοι και δεξιότητες δημοφιλείς και περιζήτητες - τώρα και στο μέλλον

- Στον τομέα της Έρευνας και των Ακαδημαϊκών Ιδρυμάτων, η μεγαλύτερη ανάγκη είναι για ερευνητές κυβερνοασφάλειας, ενώ η μεγαλύτερη αύξηση είναι για ελεγκτές (600%).
- Στον τομέα των ψηφιακών υποδομών, η μεγαλύτερη ανάγκη είναι για Υλοποιητές Κυβερνοασφάλειας, ενώ η μεγαλύτερη αύξηση είναι για Ελεγκτές Διείσδυσης (68%).
- Στον τομέα της διαχείρισης υπηρεσιών ΤΠΕ, η μεγαλύτερη ανάγκη είναι για Cyber Incident Responders και Cybersecurity Implementers, ενώ η μεγαλύτερη αύξηση είναι για Cybersecurity Researchers (220%).
- Στον τομέα της διαχείρισης υπηρεσιών ΤΠΕ παρατηρείται αύξηση σε όλους τους ρόλους του ENISA, κάτι που δεν συμβαίνει στον τομέα των ψηφιακών υποδομών.

Οι πιο αναγκαίες δεξιότητες κυβερνοασφάλειας για άτομα σε ρόλους κυβερνοασφάλειας φαίνεται να είναι οι εξής: (α) ασφάλεια στο νέφος, (β) προστασία της ιδιωτικής ζωής των δεδομένων, (γ) ασφάλεια πληροφοριακών συστημάτων και δικτύων / ανθεκτικότητα στον κυβερνοχώρο και (δ) διαχείριση περιστατικών. Επιπλέον, αρκετοί ερωτηθέντες δήλωσαν ότι δεν υπάρχει ανάγκη για δεξιότητες ασφάλειας της εφοδιαστικής αλυσίδας.

Οι ρόλοι (με βάση το ECSF) με τη μεγαλύτερη μελλοντική ζήτηση φαίνεται να είναι οι εξής: (α) Cyber Security Implementer και (β) Cyber Incident Responder. Επιπλέον, ο εμπειρογνώμονας κυβερνοασφάλειας του μέλλοντος θα πρέπει να διαθέτει τις ακόλουθες δεξιότητες που σχετίζονται με την ΤΠ, οργανωτικές και κοινωνικές δεξιότητες: (i) λειτουργικά συστήματα, (ii) διαχείριση δικτύων, (iii) διαχείριση κινδύνων, (iv) εκπαίδευση και κατάρτιση, (v) αναλυτική και (vi) δημιουργική σκέψη.

Πρόσθετες εκπαιδευτικές δεξιότητες

Φαίνεται ότι υπάρχει σημαντική ζήτηση για δεξιότητες προσωπικότητας (soft/transversal) μεταξύ των ατόμων που κατέχουν θέσεις στην κυβερνοασφάλεια.

Σύμφωνα με τις ομάδες εμπειρογνωμόνων, η έλλειψη δεξιοτήτων προσωπικότητας μπορεί να οδηγήσει σε απερίσκεπτη επιχειρηματική συμπεριφορά, η οποία θεωρείται απαράδεκτη σε ρόλους κυβερνοασφάλειας.

ΚΕΦΑΛΑΙΟ 1 - Γενικό πλαίσιο μελέτης

1.1 Στόχοι μελέτης

Στόχος της παρούσας μελέτης είναι να συνδράμει στη βελτίωση της **ποιότητας και της συνάφειας των προγραμμάτων εκπαίδευσης και κατάρτισης στον Κυβερνοχώρο** μέσω του εντοπισμού σχετικών **αναντιστοιχιών** δεξιοτήτων για συγκεκριμένες χώρες, καθώς και της προσφοράς **καινοτόμων δεξιοτήτων,** οι οποίες χρειάζονται **μεθοδολογία πρόβλεψης** (αγορά/εκπαιδευτική προσφορά).

Οι χώρες που θα μελετηθούν, στο πλαίσιο αυτό, είναι οι εξής εφτά (αλφαβητικά): **Βέλγιο**, **Ελλάδα**, **Εσθονία**, **Ισπανία**, **Λιθουανία**, **Ουγγαρία** και **Σλοβενία**. Στην παρούσα μελέτη αναφερόμαστε αποκλειστικά στην **Ελλάδα**. Οι επιμέρους στόχοι για τις χώρες αυτές περιλαμβάνουν:

Σ1 Εκπόνηση **ολοκληρωμένης ανάλυσης αναντιστοιχιών δεξιοτήτων Κυβερνοασφάλειας** για κάθε χώρα, εντοπίζοντας τα κρίσιμα κενά μεταξύ των αναγκών της αγοράς και της προσφοράς εκπαίδευσης και κατάρτισης. Η ανάλυση θα γίνει με χρήση **κοινού πλαισίου δεξιοτήτων** και αντίστοιχης μεθοδολογίας έρευνας, προκειμένου να διασφαλιστεί η επεκτασιμότητα, ποιότητα και συγκρισιμότητα των αποτελεσμάτων στην Ευρωπαϊκή Ένωση (ΕΕ).

Σ2 Ανάπτυξη ενός καινοτόμου **μοντέλου πρόβλεψης δεξιοτήτων Κυβερνοασφάλειας** που υποστηρίζει τους παράγοντες της αγοράς εργασίας και της εκπαίδευσης και κατάρτισης, έτσι ώστε να λαμβάνουν τεκμηριωμένες αποφάσεις και να μειώνουν τον κίνδυνο μελλοντικών αναντιστοιχιών και επαγγελματικών ελλείψεων στον τομέα της Κυβερνοασφάλειας.

Σ3 Εκπόνηση **στρατηγικών δεξιοτήτων Κυβερνοασφάλειας** για συγκεκριμένες χώρες που αποβλέπουν στη μείωση των αναντιστοιχιών των δεξιοτήτων στον Κυβερνοχώρο, βραχυπρόθεσμα, μεσοπρόθεσμα και μακροπρόθεσμα.

Για την κάλυψη των παραπάνω στόχων η μελέτη θα εκπονήσει τις εξής επιμέρους εργασίες:

Ε1 **Ειδικές εκθέσεις για κάθε χώρα** σχετικά με την **αναντιστοιχία προσφοράς και ζήτησης** σε δεξιότητες Κυβερνοασφάλειας. Τα CyberHubs θα ακολουθήσουν **κοινή μεθοδολογία έρευνας**, με βάση μια προσέγγιση πολλαπλών μεθόδων (ποσοτικών και ποιοτικών), περιλαμβανομένης έρευνας πεδίου, καταγραφής κενών θέσεων εργασίας που τροφοδοτείται από το πρόγραμμα δεξιοτήτων του EIT Digital Skills Academy Platform (SAP), καθώς και διαβούλευση με ομάδες εμπειρογνωμόνων. Η χαρτογράφηση δεξιοτήτων και ρόλων θα ακολουθήσει το **Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (ECSF)** του ENISA. Η ανάλυση των χωρών θα αποκαλύψει τις κρίσιμες ανάγκες της Αγοράς σε δεξιότητες Κυβερνοασφάλειας, την ζήτηση επαγγελματικών ρόλων, καθώς και τα κενά εκπαίδευσης και κατάρτισης. Οι εκθέσεις θα δώσουν ακριβή εικόνα των δεξιοτήτων Κυβερνοασφάλειας, την ωριμότητα του σχετικού οικοσυστήματος, τις ευκαιρίες και τις ιδιαιτερότητες κάθε χώρας.

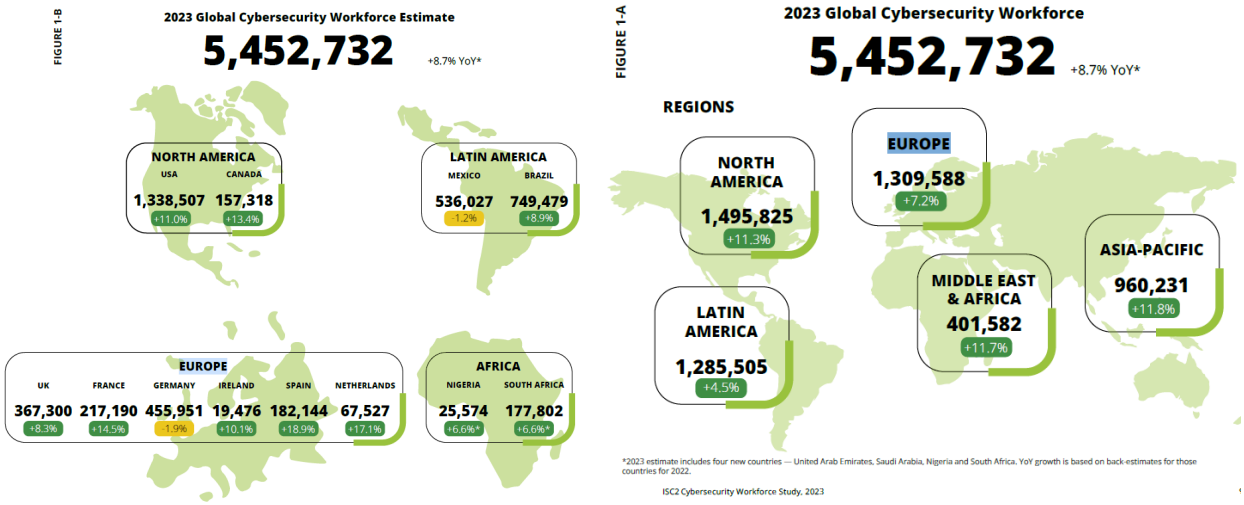
Ε2 **Καταγραφή δεξιοτήτων και ρόλων** Κυβερνοασφάλειας για **μακροπρόθεσμη πρόβλεψη**. Θα αξιοποιηθεί για πρόβλεψη των μελλοντικών επαγγελματιών Κυβερνοασφάλειας, καθώς και των δεξιοτήτων και ρόλων που απαιτούνται για μετριασμό της απόκλισης μεταξύ ζήτησης και προσφοράς στην αγορά εργασίας. Επίσης, θα υποστηρίξει τους παρόχους εκπαίδευσης και κατάρτισης, καθώς και τους φορείς της αγοράς εργασίας στη λήψη τεκμηριωμένων αποφάσεων. Τα δεδομένα για την πρόβλεψη της ζήτησης και προσφοράς δεξιοτήτων

Κυβερνοασφάλειας θα προέρχονται από διάφορες πηγές, όπως τάσεις στις θέσεις εργασίας, ανάλυση κενών θέσεων εργασίας, επαγγελματική ανάλυση του CEDEFOP και εκτιμήσεις ομάδων εμπειρογνωμόνων. Η υιοθέτηση του ECSF, στο πλαίσιο της μοντέλου προβλέψεων, θα ωφελήσει την πληρότητα των αποτελεσμάτων και τις ενέργειες που θα αναληφθούν. Τα στοιχεία του μοντέλου πρόβλεψης θα **ελεγχθούν και θα αξιολογηθούν** κατά τη διάρκεια του έργου. Μακροπρόθεσμα, το μοντέλο πρόβλεψης θα μπορεί να χρησιμοποιηθεί από την ΕΕ, κάτι που προβλέπεται ως μέρος του **σχεδίου βιωσιμότητας** του έργου.

Ε3 **Ειδικές στρατηγικές διαχείρισης δεξιοτήτων Κυβερνοασφάλειας ανά χώρα** για τη μείωση των απο-κλίσεων μεταξύ αγοράς και ζήτησης δεξιοτήτων Κυβερνοασφάλειας, βραχυπρόθεσμα, μεσοπρόθεσμα και μακροπρόθεσμα. Οι στρατηγικές θα βασιστούν στα αποτελέσματα των προηγούμενων εργασιών, καθώς και σε ήδη υπάρχουσες μελέτες (π.χ. ευρωπαϊκή στρατηγική για τις δεξιότητες Κυβερνοασφάλειας σχεδίου REWIRE). Θα αναζητηθούν προσεγγίσεις που είναι **συναφείς και βιώσιμες για κάθε χώρα**, μέσω της εμπλοκής των βασικών φορέων του εθνικού οικοσυστήματος Κυβερνοασφάλειας, έτσι ώστε να προκύψουν **αποτελεσματικές, καινοτόμες και συστημικές προσαρμογές στην εκπαίδευση και κατάρτιση** στην Κυβερνοασφάλεια σε κάθε χώρα. Θα ακολουθήσει **συγκριτική αξιολόγηση** των μελετών, ανά χώρα, με στόχο τον συντονισμό της ανάπτυξης δεξιοτήτων Κυβερνοασφάλειας στο επίπεδο της ΕΕ. Για το σκοπό αυτό θα προταθούν **δράσεις ευθυγράμμισης** με ευρωπαϊκά πλαίσια και εργαλεία, όπως το **Ευρωπαϊκό Πρόγραμμα Δεξιοτήτων Κυβερνοασφάλειας** του ENISA (ECSF), το **ESCO** και το **Europass**.

1.2 Παγκόσμιες τάσεις και προοπτικές απασχόλησης στην Κυβερνοασφάλεια

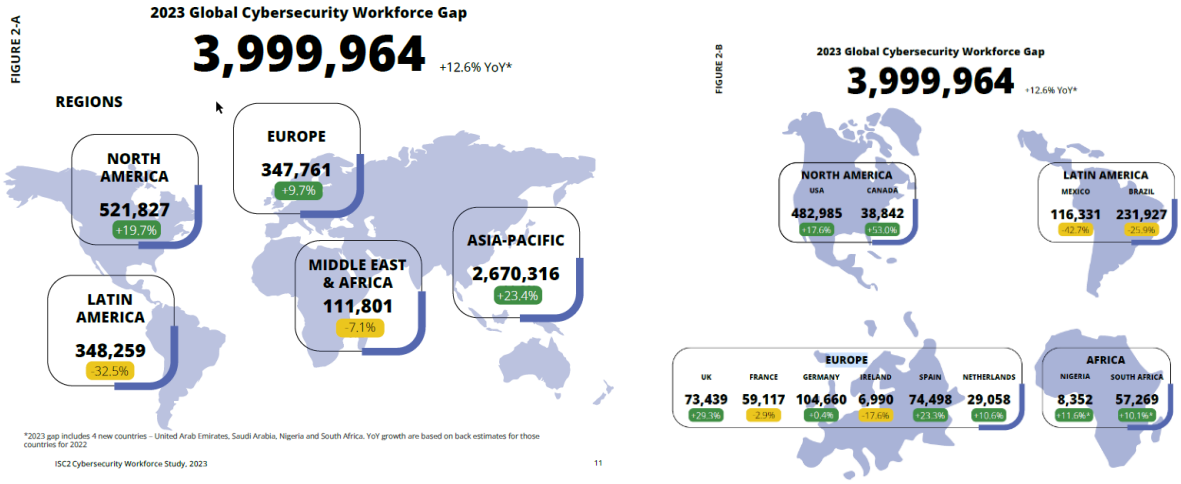
Η μελέτη **Cybersecurity Workforce Study** (ISC^2) [1] βασίστηκε σε δεδομένα διαδικτυακής έρευνας που συλλέχθηκαν σε συνεργασία με την Forrester Research (Απρίλιος-Μάιος 2023) από 14.865 άτομα, υπεύθυνα για την ασφάλεια στον Κυβερνοχώρο σε χώρους εργασίας στη Βόρεια Αμερική, Λατινική Αμερική (LATAM), Ασία-Ειρηνικό (APAC), Ευρώπη, Αφρική και Μέση Ανατολή (EMEA) (βλ. Γραφήματα 1-Α/Β) [1]



Γραφήματα 1Α-1Β: Παγκόσμιο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας (2023)(ISC2,2023)

Η μελέτη εκτιμά ότι το παγκόσμιο εργατικό δυναμικό στον τομέα της Κυβερνοασφάλειας ανέρχεται σε **5.5M**, γεγονός που αντιπροσωπεύει μια αύξηση **8.7%** σε ετήσια βάση και σχεδόν **440K** νέες θέσεις εργασίας. Σε όλες τις περιφέρειες σημειώθηκε αύξηση, αλλά οι αυξήσεις αυτές είναι ιδιαίτερα υψηλές στις δύο νέες χώρες της Μέσης Ανατολής, στην Ασία-Ειρηνικό και στη Βόρεια Αμερική. Ειδικά η Ιαπωνία αναπτύσσεται με ταχείς ρυθμούς (+24% σε ετήσια βάση). Η Λατινική Αμερική αρχίζει να εξισορροπεί, μετά από αρκετά χρόνια αξιόλογης ανάπτυξης.

Παρά τη συνεχή αύξηση του στελεχιακού δυναμικού, η μελέτη επιβεβαίωσε ότι η ζήτηση εξακολουθεί να ξεπερνάει την προσφορά. Η απόκλιση αυτή αυξήθηκε περαιτέρω κατά 12.6%, με τη μεγαλύτερη αύξηση στην περιοχή Ασίας-Ειρηνικού (ιδίως σε Ιαπωνία και Ινδία) και τη Βόρεια Αμερική. Περιοχές με ιδιαίτερα ταχεία αύξηση της προσφοράς, όπως η Μέση Ανατολή και η Λατινική Αμερική, διαπιστώνουν ότι η προσφορά ήδη περιορίζει το κενό του στελεχιακού δυναμικού (βλ. Γραφήματα 2-Α/Β) [1]



Γραφήματα 2Α-2Β: Παγκόσμια έλλειψη στελεχιακού δυναμικού στην Κυβερνοασφάλεια (2023) [1]

Η **έλλειψη εργαζομένων/δεξιοτήτων** (45%) ήταν η σημαντικότερη πρόκληση που αντιμετώπισαν οι επαγγελματίες της Κυβερνοασφάλειας (βλ. Γράφημα 3). Η γεωγραφική κατανομή της έλλειψης είναι βασικός διαφοροποιητικός παράγοντας, καθώς οι ερωτηθέντες στη Βόρεια Αμερική (55%) αισθάνθηκαν σημαντικότερο αντίκτυπο από αυτές τις ελλείψεις από ό,τι εκείνοι σε άλλα μέρη του κόσμου, όπως η Ευρώπη (42%), η Μέση Ανατολή (42%, Αφρική (42%), η Λατινική Αμερική (32%) και η Ασία-Ειρηνικός (31%). Αυτό εντείνει την αύξηση του ελλείμματος εργατικού δυναμικού στη Βόρεια Αμερική (~20% [1]

Γράφημα 3: Συρρίκνωση έλλειψης δεξιοτήτων Κυβερνοασφάλειας [1]

Σε ότι αφορά στην Ελλάδα, σύμφωνα με μελέτη του **ManpowerGroup**[1] η ζήτηση για επαγγελματίες Κυβερνοασφάλειας αναμένεται να αυξηθεί κατά **25%** τα επόμενα τρία χρόνια (2023-25). Η μελέτη αναφέρει ότι η Ελλάδα πάσχει από έλλειψη **10Κ** επαγγελματιών Κυβερνοασφάλειας. Αναφέρει, επίσης, ότι οι επαγγελματίες της Κυβερνοασφάλειας στη χώρα προσδοκάται να διαθέτουν ισχυρές δεξιότητες σε τεχνολογίες όπως η **Νεφοϋπολογιστική (Cloud Computing)**, η **Ανάλυση Δεδομένων** και η **Μηχανική Μάθηση**.

Τέλος, εκτιμάται ότι οι εταιρείες που αναζητούν επαγγελματίες Κυβερνοασφάλειας θα πρέπει να προσφέρουν **ανταγωνιστικές απολαβές** και **ευκαιρίες επαγγελματικής ανάπτυξης**, προκειμένου να καλύψουν τις κενές θέσεις (ManpowerGroup, 2022).

1.3 Τάσεις και προοπτικές: Ορίζοντας 2030

Σε ό,τι αφορά στις μεσοπρόθεσμες προβλέψεις της ζήτησης, ο ENISA[2] επικαιροποίησε (2024) την πρόβλεψή του για την ασφάλεια στον Κυβερνοχώρο. Η ανάλυση των αναδυόμενων απειλών που προβλέπονται για το 2030 (βλ. Πίνακα 1) περιλαμβάνει 2 σοβαρές απειλές (2η και 3η στον κατάλογο με τις 10 πρώτες) που αφορούν στην **έλλειψη καταρτισμένου στελεχιακού δυναμικού** στην Κυβερνοασφάλεια.

Ειδικότερα, στη **2η θέση** του πίνακα αναφέρεται η **έλλειψη δεξιοτήτων** (skills shortage) στην Κυβερνο-ασφάλεια. Η μελέτη σημειώνει ότι πρόθεση των οργανισμών είναι να εντάξουν στο δυναμικό τους προσωπικό με κατάλληλες γνώσεις και δεξιότητες και να γεφυρώσουν το εκπαιδευτικό χάσμα που εξακολουθεί να αποτελεί σοβαρό πρόβλημα στην ασφάλεια στον Κυβερνοχώρο. Αυτό συνδέεται με την **3η απειλή** που αφορά στα **ανεπίκαιρα συστήματα** (exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector tech ecosystem). Η σύνδεση των δύο αυτών μείζονων απειλών αναδεικνύει ότι η έλλειψη δεξιοτήτων παρεμποδίζει την **εξοικείωση του προσωπικού με τα διαθέσιμα εργαλεία** που χρησιμοποιούνται για την ενημέρωση των ανεπίκαιρων πληροφοριακών συστημάτων, με αποτέλεσμα τα συστήματα αυτά να καθίστανται, προοδευτικά, όλο και πιο ευάλωτα σε κυβερνοεπιθέσεις. [3]

#	Threat	Impact * Likelihood	Impact	Likelihood
1	Supply Chain Compromise of Software Dependencies	17,71	4,21	4,21
2	**Skill Shortage**	**17,20**	**4,10**	**4,20**
3	**Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems**	**16,69**	**3,96**	**4,22**
4	Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional]	16,21	4,05	4,00
5	Rise of Digital Surveillance Authoritarianism/Loss of Privacy	15,34	3,96	3,88
6	Cross-border ICT Service Providers as Single Point of Failure	15,12	4,14	3,65
7	Advanced Disinformation/Influence Operations (IO) Campaigns	14,38	3,42	4,21
8	Rise of Advanced Hybrid Threats	14,03	3,68	3,81
9	Abuse of AI	13,22	3,43	3,86

[1] ManpowerGroup, *The State of Cybersecurity Talent*, Greece 2022.

[2] ENISA, *Foresight Cybersecurity Threats for 2030* (update), March 2024, https://www.enisa.europa.eu/ news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

#	Threat	Impact * Likelihood	Impact	Likelihood
10	Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [Optional]	12,99	3,68	3,53

Πίνακας 1: Ιεράρχηση προβλεπόμενων νέων απειλών (2030)

Σύμφωνα με τον ENISA, η ευρωπαϊκή αγορά εργασίας πρέπει **να διασφαλίσει επαρκή αριθμό** εξειδικευμένων επαγγελματιών σε όλους τους τομείς της Κυβερνοασφάλειας, που πρέπει να εκπαιδευτούν κατάλληλα προκειμένου να είναι σε θέση να υποστηρίξουν και να ηγηθούν λύσεων στις επερχόμενες βιομηχανικές, επιστημονικές, κοινωνικές και πολιτικές προκλήσεις στον τομέα της Κυβερνοασφάλειας.

ΚΕΦΑΛΑΙΟ 2 - ΕΛΛΑΔΑ (Δημογραφία, Εκπαίδευση, Απασχόληση, Ψηφιακή Οικονομία, Επιχειρήσεις Κυβερνοασφάλειας, Θεσμοί Κυβερνοασφάλειας)

2.1 Επισκόπηση του εθνικού πλαισίου

2.1.1 ΕΛΛΑΔΑ – Βασική δημογραφία

Η Ελλάδα είναι Κράτος-μέλος της Ευρωπαϊκής Ένωσης, βρίσκεται στα νοτιοανατολικά σύνορα της Ευρωπαϊκής Ένωσης με την Ασία, διαθέτει πολύ εκτενή ακτογραμμή (Μεσόγειος Θάλασσα), το έδαφός της είναι κυρίως ηπειρωτικό και περιβάλλεται από πολλές δεκάδες κατοικούμενων νησιών. Ο πληθυσμός της ανέρχεται σε **10.6M** κατοίκους (2022) και βαίνει **σταθεροποιούμενος και γηράσκων**.

Οι βασικές πηγές πλούτου της χώρας είναι ο **Τουρισμός** και η **Ναυτιλία**. Δευτερευόντως, οι **Υπηρεσίες**, οι **ΜΜΕ** και η **Γεωργία**. Το **πνευματικό της κεφάλαιο** θεωρείται ιδιαίτερα αξιόλογο και το ποσοστό των απόφοιτων της πανεπιστημιακής εκπαίδευσης (ειδικά σε μεταπτυχιακό επίπεδο) αυξάνεται ταχύτατα. Η Οικονομία της χώρας περιγράφεται, σε αδρές γραμμές, στο Γράφημα 4. Κατά την τρέχουσα περίοδο η χώρα βαίνει εξερχόμεναπό μια σοβαρή **οικονομική κρίση** (2008-18) (βλ. Γράφημα 5).

Θεωρείται **τεχνολογικά αναπτυγμένη** χώρα, με σχετικά **αναποτελεσματικό Δημόσιο Τομέα** και κατά περίπτωση **δραστήριο Ιδιωτικό Τομέα**. Ο αριθμός των μεταναστών δεν είναι υψηλός και οι μεταναστευτικές ροές είναι ισορροπημένες (2023).

Γράφημα 4: ΕΛΛΑΔΑ – Ελληνική Οικονομία (2022)[3] [4]

[3] https://www.creativefabrica.com/product/greece-economy-infographic-presentation/

Γράφημα 5: ΕΛΛΑΔΑ – Οικονομική κρίση (2008-18) [4] [5]

Τα Γραφήματα 6-7[5] καταγράφουν με ποσοτικούς όρους ορισμένα από τα παραπάνω στοιχεία.

[4] https://www.thebalancemoney.com/what-is-the-greece-debt-crisis-3305525

[5] https://www.statistics.gr/en/elstat-infographics

Γράφημα 6: ΕΛΛΑΔΑ – Γενικά χαρακτηριστικά χώρας [6]

Γράφημα 7: ΕΛΛΑΔΑ – Χαρακτηριστκά πληθυσμού [6]

2.1.2 ΕΛΛΑΔΑ – Εκπαίδευση

Η δημόσια εκπαίδευση στην Ελλάδα **παρέχεται δωρεάν**, σε όλα τα επίπεδα και σε όλους τους πολίτες. Το εκπαιδευτικό σύστημα είναι συγκεντρωτικό. Η λειτουργία του ρυθμίζεται με νόμους, προεδρικά διατάγματα και υπουργικές αποφάσεις του **Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού**.

Η Ελλάδα έχει υιοθετήσει ένα **εκπαιδευτικό σύστημα τριών επιπέδων** (Α-βάθμια: Δημοτικό Σχολείο, Β-βάθμια: Γυμνάσιο και Λύκειο, Γ-βάθμια: Πανεπιστήμιο (βλ. Γράφημα 8). Συμπληρωματικά/επικουρικά του συστήματος αυτού λειτουργούν ορισμένες επιπλέον εκπαιδευτικές δομές, κυρίως σε θέματα κατάρτισης, επιμόρφωσης και πιστοποίησης, με ορατή αλλά περιορισμένη παρουσία.

Σε ό,τι αφορά στα εκπαιδευτικά επιτεύγματα του πληθυσμού την 20ετία **2000-20**, τα βασικά χαρακτηριστικά του είναι τα εξής (βλ. Πίνακα 2[6]). Το τμήμα του πληθυσμού που **δεν ολοκλήρωσε Α-βάθμια** εκπαίδευση είναι **πολύ περιορισμένο (3%)** και βαίνει μειούμενο γρήγορα (8.8-3.2%).

α) Το τμήμα του πληθυσμού που ολοκλήρωσε μόνο **Α-βάθμια** εκπαίδευση είναι **αρκετό (20.6%)** , αλλά μειώνεται γρήγορα (33.7-20.6%).

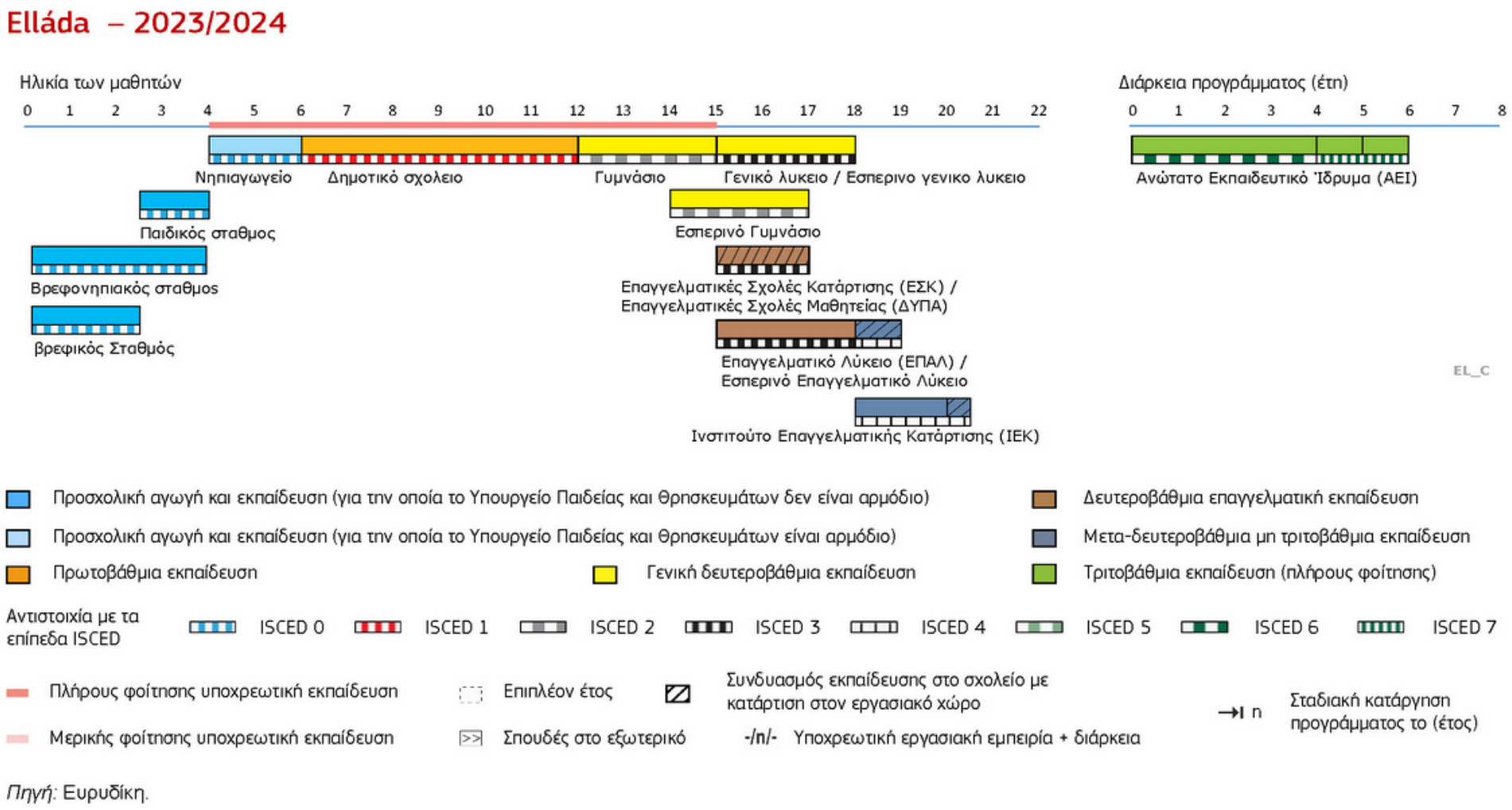
β) Το τμήμα του πληθυσμού που ολοκλήρωσε τουλάχιστον το **πρώτο τμήμα Β-βάθμιας** εκπαίδευσης είναι το σχετικά **μεγαλύτερο (44.2%)** και **διατηρείται σταθερό** (40-44%).

γ) Το τμήμα του πληθυσμού που διαθέτει **μεταδευτεροβάθμια** επαγγελματική κατάρτιση είναι **μικρό (7.7%)**, αλλά **αυξάνεται σχετικά γρήγορα** (4.9-7.7%).

δ) Το τμήμα του πληθυσμού που διαθέτει **πανεπιστημιακό τίτλο** (πτυχιακό ή μεταπτυχιακό) σπουδών είναι **σχετικά περιορισμένο** (24.3%), αλλά έχει **διπλασιαστεί σε 20 χρόνια** (12.6-24.3%, 2000-20).

ε) Το τμήμα του πληθυσμού που διαθέτει **μεταπτυχιακό** τίτλο είναι **σχετικά αξιόλογο (3.7%)**, αλλά έχει **αυξηθεί κατά 12 φορές** (από 28-334Κ) μέσα σε 20 χρόνια (0.3-3.7%, 2000-20). Σε ό,τι αφορά στις συνολικές δαπάνες της Γενικής Κυβέρνησης για εκπαίδευση, ως ποσοστό του ΑΕΠ (2016 -20), η Ελλάδα – παρά την σταδιακή αύξηση (4-4.5%) - **υστερεί κατά 10%** του μέσου όρου των (27) Κρατών-μελών της ΕΕ (4.5% έναντι 5%) (βλ. Πίνακα 3) [7].

[6] Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ), *Έρευνα Εργατικού Δυναμικού, Πληθυσμός, Εκπαίδευση, Κατάσταση Απασχόλησης 1981-2020*, Αθήνα 2023.



Πηγή: Ευρυδίκη.

Γράφημα 8: ΕΛΛΑΔΑ: Τυπικό Εκπαιδευτικό Σύστημα [8]

Πίνακας 2: ΕΛΛΑΔΑ – Εκπαίδευση πληθυσμού [7]

ΕΛΛΑΔΑ - Εκπαιδευτικά επιτεύγματα πληθυσμού	2000	2005	2015	2020
Πληθυσμός άνω των 15 ετών	**8.839.847**	**9.332.424**	**9.246.546**	**9.078.975**
Δεν πήγε σχολείο/λίγες τάξεις δημοτικού	777.061	646.564	392.641	286.580
Πρωτοβάθμια εκπαίδευση	2.982.153	2.757.790	2.183.999	1.871.320
Απολυτήριο Γυμνασίου	1.155.659	1.194.293	1.127.793	1.065.012
Απολυτήριο Λυκείου	2.373.080	2.728.414	2.950.137	2.952.851
Μεταδευτεροβάθμια επαγγελματική κατάρτιση	436.656	548.827	595.370	695.034
Πτυχίο ΑΕΙ/ΤΕΙ	1.087.180	1.381.804	1.820.087	1.873.951
Μεταπτυχιακός τίτλος (M.Sc., Ph.D.)	28.056	74.730	176.516	334.224

Πίνακας 3: ΕΛΛΑΔΑ – Δαπάνες εκπαίδευσης του πληθυσμού [7]

8. ΕΕ: Συνολικές δαπάνες της Γενικής Κυβέρνησης για την εκπαίδευση ως ποσοστό (%) του ΑΕΠ, 2018 - 2022					
	2018	2019	2020	2021	2022
ΕΕ 27	4,7	4,7	5,0	4,8	4,7
Ευρωζώνη					
Αυστρία (AT)	4,8	4,8	5,1	4,9	4,8
Βέλγιο (BE)	6,2	6,1	6,6	6,2	*6,3
Γαλλία (FR)	5,3	5,2	5,4	*5,3	*5,2
Γερμανία (DE)	4,3	4,4	*4,6	*4,5	*4,5
Ελλάς (EL)	4,1	4,0	4,5	4,1	3,8
Εσθονία (EE)	6,2	6,1	6,4	5,9	5,8
Ιρλανδία (IE)	3,2	3,2	3,2	2,9	2,7
Ισπανία (ES)	4,0	4,0	4,6	4,6	*4,4
Ιταλία (IT)	3,9	3,9	4,3	4,0	4,1
Κροατία (HR)	4,6	4,9	5,5	5,2	4,8
Κύπρος (CY)	5,0	5,1	5,7	5,3	5,1
Λετονία (LV)	5,8	5,7	5,8	5,7	5,3
Λιθουανία (LT)	4,5	4,6	5,2	4,7	4,9
Λουξεμβούργο (LU)	4,6	4,8	5,0	4,7	4,7
Μάλτα (MT)	4,9	5,0	5,6	5,4	5,0
Ολλανδία (NE)	5,1	5,0	5,2	5,1	5,1
Πορτογαλία (PT)	4,4	4,5	4,7	4,7	*4,3
Σλοβακία (SK)	3,9	4,2	4,4	4,3	4,5
Σλοβενία (SI)	5,4	5,4	5,6	5,8	5,6
Φινλανδία (FI)	5,5	5,6	5,9	5,7	5,5

Σε ό,τι αφορά στην απασχόληση στον Κλάδο των ΤΠΕ, πρόσφατες αναφορές της Eurostat και σχετικά δημοσιεύματα αναφέρουν ότι «η Ελλάδα εξακολουθεί να μην απασχολεί πολλούς εργαζομένους στον συγκεκριμένο κλάδο. Καταγράφει μάλιστα αρνητική πρωτιά σε σύγκριση με άλλες χώρες της ΕΕ, καθώς οι απαιτήσεις για τον ψηφιακό μετασχηματισμό τόσο του Δημοσίου όσο και του ιδιωτικού τομέα αυξάνονται ~~δραματικά~~ ραγδαία. Στο μεταξύ, οι επιχειρήσεις αναμένεται να επιδοθούν το επόμενο διάστημα σε ένα ακόμη μεγαλύτερο κυνήγι ταλέντων, δεδομένης και της ραγδαίας εξάπλωσης της «Τεχνητής Νοημοσύνης». Σύμφωνα με στοιχεία της Eurostat, το 2023 στην ΕΕ απασχολούνταν 9,8Μ ειδικοί στον Κλάδο

των ΤΠΕ, δηλαδή 4,8% του συνόλου των εργαζομένων (2023), ποσοστό αυξημένο κατά 1,5% από το 2013. Το ποσοστό της Ελλάδας ισούται με το μισό του μέσου όρου της ΕΕ (4,8%) (βλ. Γράφημα 9).

Γράφημα 9: ΕΛΛΑΔΑ – Απασχόληση στον Κλάδο ΤΠΕ[7]

Δημοσιεύματα που αναφέρονται σε σχετικό πόρισμα των ελληνικών ΑΕΙ και του Συνδέσμου Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας (ΣΕΠΕ) (2023) αναφέρουν ότι η αγορά ΤΠΕ χρειάζεται, για να καλύψει τις ανάγκες σε προσωπικό, 7.500 περισσότερους πτυχιούχους το χρόνο από όσους αποφοιτούν σήμερα. Ειδικότερα, ο ρυθμός αποφοίτησης από τα 37 πανεπιστημιακά τμήματα ΤΠΕ είναι στο 62% (το 2022 αποφοίτησαν 5.231), και περίπου 15% των φοιτητών ΤΠΕ δεν αποφοιτούν, διόλου ή έγκαιρα, ενώ πολλοί εργάζονται στον Κλάδο των ΤΠΕ πριν αποφοιτήσουν (βλ. Γράφημα 10).

Γράφημα 10: ΕΛΛΑΔΑ – Ρυθμός αποφοίτησης φοιτητών ΤΠΕ [8]

Παράλληλα, μελέτη του Ευρωβαρόμετρου δείχνει ότι όχι μόνο αυξάνεται η έλλειψη δεξιοτήτων στην Κυβερνοασφάλεια, αλλά χρειάζεται να υπάρχουν περισσότεροι ειδικοί καθώς και να αυξηθεί το προσωπικό με υψηλή επίγνωση (awareness) Κυβερνοασφάλειας σε κάθε εταιρεία σε ολόκληρη την ΕΕ. Τα

[7] https://www.kathimerini.gr/economy/563046397/ekpaideysi-agora-echoyme-toys-misoys-pliroforikarioys-se-schesi-me-tin-e-e/

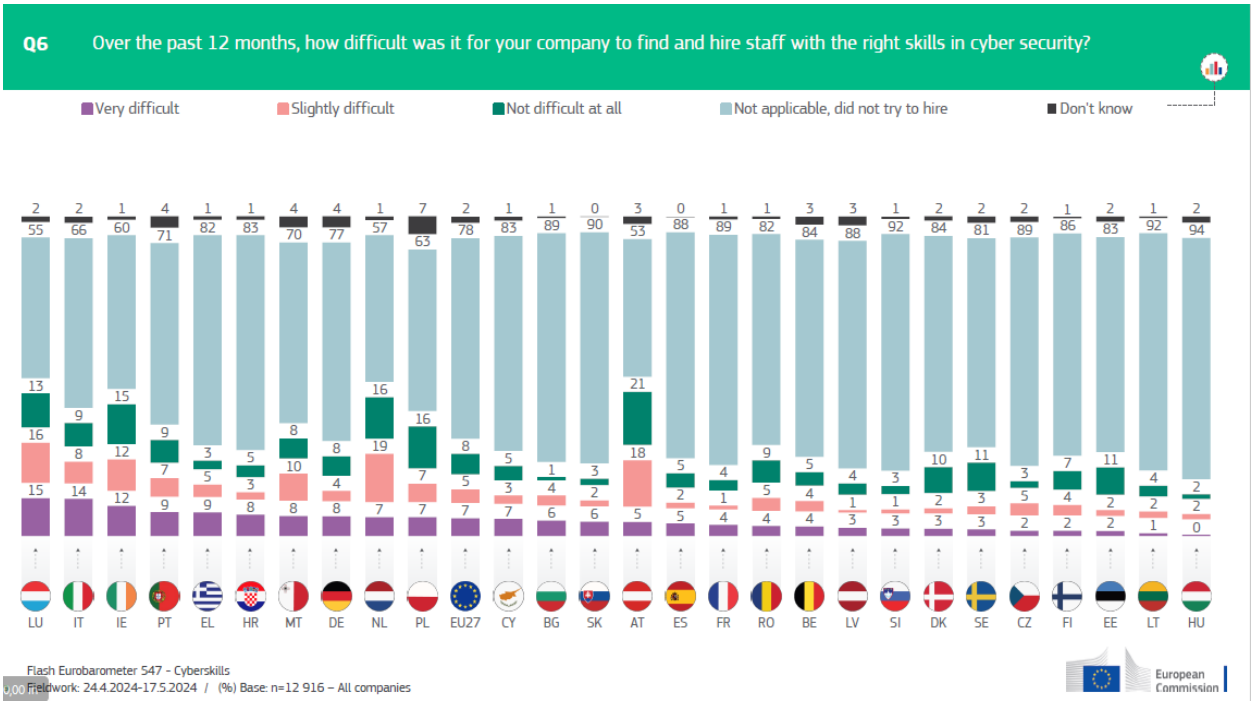
[8] https://www.kathimerini.gr/society/562702606/zitoyntai-ptychioychoi-pliroforikis/

αποτελέσματα της έρευνας περιέχουν ευρήματα σχετικά με την ευαισθητοποίηση στην Κυβερνοασφάλεια, τις δυσκολίες πρόσληψης, την απουσία προσόντων και πιστοποιήσεων, καθώς και το χάσμα μεταξύ των φύλων. Ειδικά για την Ελλάδα, προέκυψαν οι εξής βασικές διαπιστώσεις:

α) **Έλλειψη επίγνωσης** (awareness): Ενώ υπάρχει γενική παραδοχή ότι η Κυβερνοασφάλεια αποτελεί υψηλή προτεραιότητα (74% των εταιρειών), η ανάληψη δράσης παραμένει η κύρια πρόκληση, διότι το 78% των εταιρειών δεν έχουν παράσχει καμία εκπαίδευση, ούτε ε~~υαισθητοποιούν~~ κινητοποιούν τους υπαλλήλους τους. Επιπλέον, το 55% των εταιρειών δήλωσε ότι δεν απαιτείται εκπαίδευση ή ευαισθητοποίηση σχετικά με την Κυβερνοασφάλεια (25% δεν γνωρίζει ποιες ευκαιρίες κατάρτισης είναι οι κατάλληλες και το 20% αναφέρει περιορισμένους προϋπολογισμούς ως λόγο).

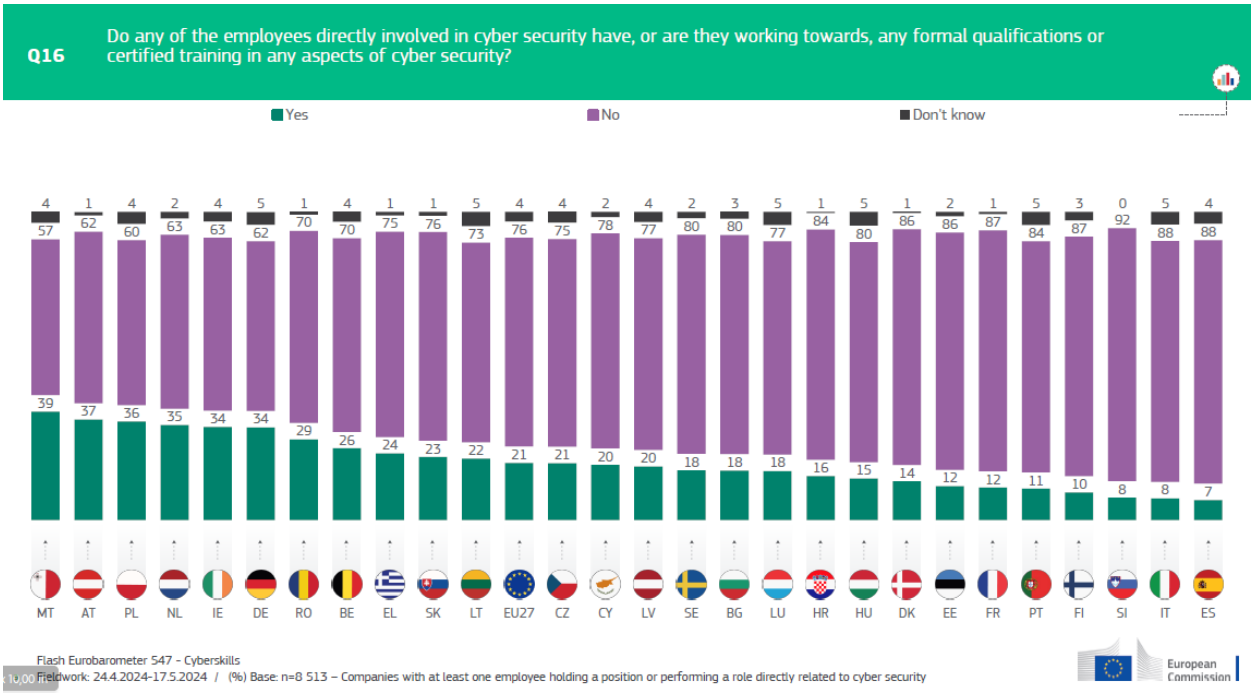
β) **Δυσκολίες πρόσληψης**: Οι περισσότερες εταιρίες (82%) που αναζήτησαν κατάλληλους υποψηφίους αντιμετώπισαν δυσκολίες, όπως η ύπαρξη κατάλληλων προσόντων των υποψηφίων (62%), η έλλειψη υποψηφίων (48%), η έλλειψη ενημέρωσης (16%) και περιορισμοί στον προϋπολογισμό τους (22%) (βλ. Γράφημα 11).

Γράφημα 11: ΕΛΛΑΔΑ – Δυσκολίες πρόσληψης επαγγελματιών Κυβερνοασφάλειας



γ) **Προσόντα και πιστοποιήσεις**: Το 75% των εργαζομένων σε ρόλους που σχετίζονται με την Κυβερνοασφάλεια δεν διαθέτουν τυπικά προσόντα ή πιστοποιημένες εκπαιδεύσεις. Το 35% προέρχεται από ρόλους που δεν σχετίζονται με την Κυβερνοασφάλεια, στο 32% ενσωματώθηκαν οι νέες ευθύνες στον υπάρχοντα ρόλο και το 21% ήταν πρόσληψη νέων αποφοίτων.

Γράφημα 12: ΕΛΛΑΔΑ – Έλλειψη προσόντων και πιστοποιήσεων επαγγελματιών Κυβερνοασφάλειας

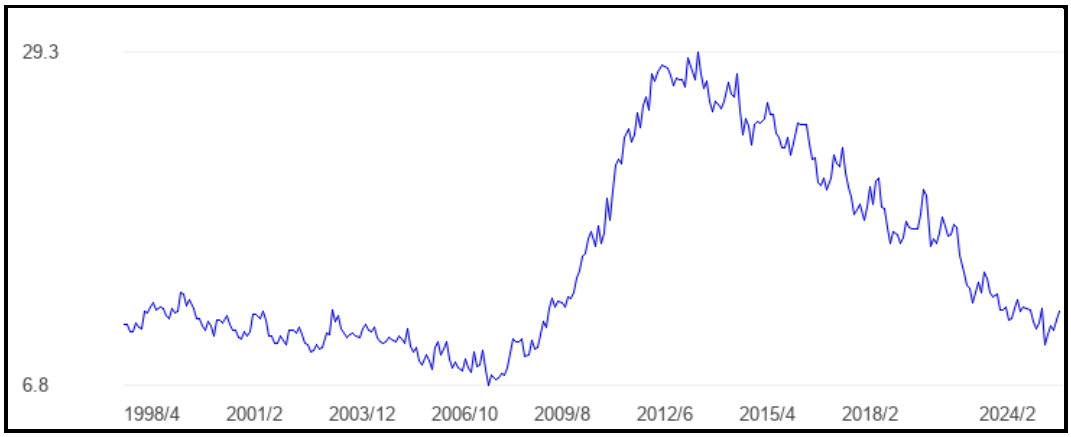


δ) **Διαφορετικότητα και συμπερίληψη**: Οι περισσότεροι από τους ερωτηθέντες (82%) στην έρευνα συμφωνούν ότι η διαφορετικότητα και η συμπερίληψη στον τομέα της Κυβερνοασφάλειας είναι σημαντικές στις αντίστοιχες εταιρείες τους. Παράλληλα, ενώ οι περισσότεροι συμφωνούν (82%) ότι οι γυναίκες ενθαρρύνονται να αναλαμβάνουν ρόλους και καθήκοντα στον τομέα της Κυβερνοασφάλειας, το 54% των εταιρειών δεν έχουν αναθέσει σε καμία γυναίκα κάποιον από αυτούς τους ρόλους.

2.1.3 ΕΛΛΑΔΑ – Απασχόληση

Στην Ελλάδα, το ποσοστό απασχόλησης κατά την περίοδο 2017-21 -κατά την οποία η χώρα διερχόταν σοβαρή οικονομική κρίση και οι κάτοικοι διαβιούσαν εν μέσω πανδημίας- ήταν **σταθερό** (40.9-43.3%). Η **ανεργία** κινήθηκε μεταξύ **21.5-14.7%**, παρουσιάζοντας **σταθερή βελτίωση** (βλ. Γραφήματα 13-14).

Γράφημα 13: ΕΛΛΑΔΑ – Ποσοστό ανεργίας (1998-2024)[9] [9]



[9] https://www.theglobaleconomy.com/Greece/unemployment_rate_monthly/

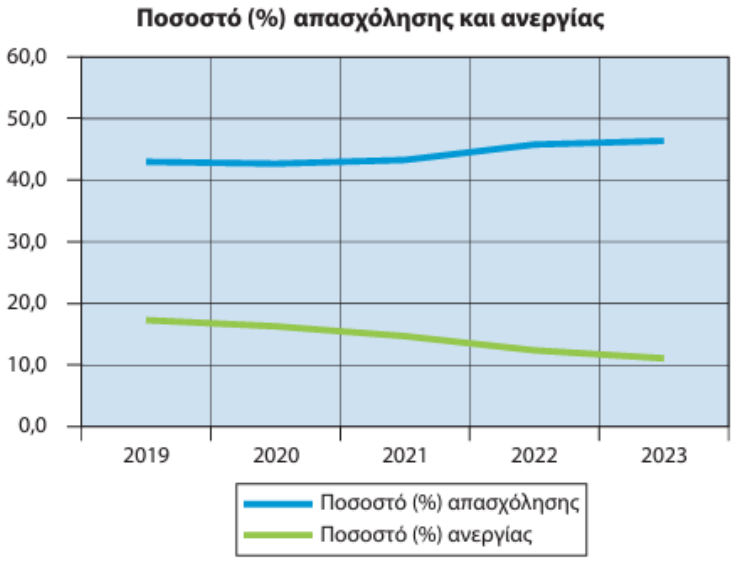
Γράφημα 14: ΕΛΛΑΔΑ – Απασχόληση και ανεργία (2019-23) [10] [7]

1. Πληθυσμός ηλικίας 15 ετών και άνω, κατά κατάσταση απασχόλησης, 2019 - 2023

Χιλιάδες

	2019	2020	2021	2022	2023
Απασχολούμενοι(1)	3.911,0	3.875,5	3.928,0	4.140,6	4.193,5
Άνεργοι(2)	818,9	755,0	677,7	588,2	521,8
Άτομα εκτός του εργατικού δυναμικού	4.373,6	4.448,5	4.459,7	4.321,3	4.321,7
Ποσοστό (%) απασχόλησης(3)	43,0	42,7	43,3	45,8	46,4
Ποσοστό (%) ανεργίας	17,3	16,3	14,7	12,4	11,1

(1) Από το έτος 2021 και εξής, αφορά σε άτομα 15 - 89 ετών.
(2) Αφορά σε άτομα 15 - 74 ετών.
(3) Το ποσοστό απασχόλησης είναι το ποσοστό των απασχολουμένων επί του συνολικού πληθυσμού.



2.1.4 ΕΛΛΑΔΑ – Ψηφιακή Οικονομία

Η βιομηχανία ψηφιακής τεχνολογίας είναι ένας στρατηγικός κλάδος για την ελληνική οικονομία. Στην παγκόσμια οικονομία της γνώσης, η ψηφιακή τεχνολογία αναμορφώνει την οικονομία, προωθεί την καινοτομία και τις διαρθρωτικές αλλαγές σε κάθε πτυχή της οικονομικής δραστηριότητας.

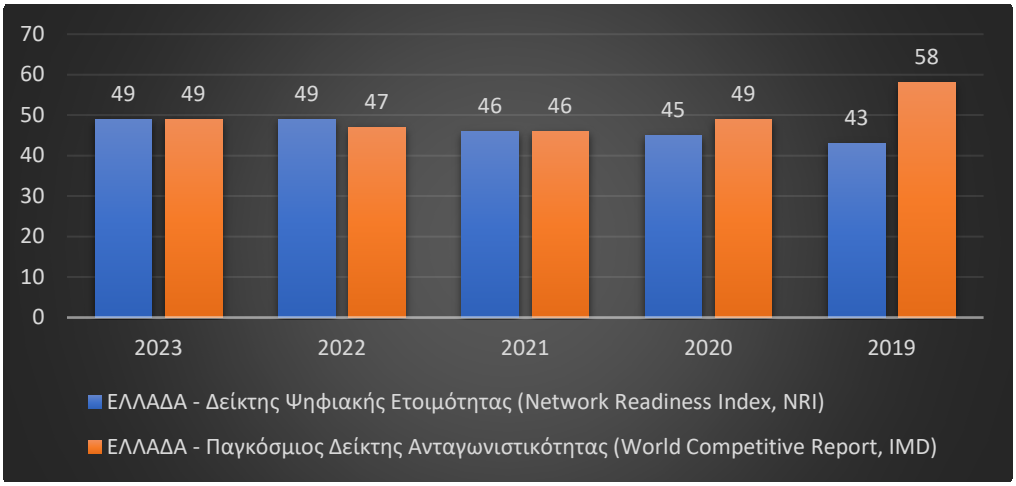
Οι πρόσφατες ψηφιακές επιδόσεις της Ελλάδας έχουν τάση αργής υποχώρησης, τόσο ως προς την ψηφιακή της ετοιμότητα, όσο και ως προς την παγκόσμια ανταγωνιστικότητα, όπως αποτυπώνεται σε σχετικούς δείκτες[11] [12] (βλ. Γράφημα 15).

[10] Ελληνική Στατιστική Αρχή, *ΕΛΛΑΣ ΜΕ ΑΡΙΘΜΟΥΣ Ιανουάριος – Μάρτιος 2024*.

[11] Portulans Institute, *Network Readiness Index*, https://networkreadinessindex.org/

[12] Συμβούλιο Ανταγωνιστικότητας της Ελλάδας, https://competegr.org/

Γράφημα 15: ΕΛΛΑΔΑ - Ψηφιακή ετοιμότητα & ανταγωνιστικότητα [10] [11]



Οι ελληνικές επιχειρήσεις Ψηφιακής Τεχνολογίας διαδραματίζουν σημαντικό ρόλο, υλοποιούν έργα και προσφέρουν προϊόντα και υπηρεσίες σε μεγάλες και μικρές επιχειρήσεις, στο δημόσιο και στον ιδιωτικό τομέα, στον καταναλωτή, τόσο στην Ελλάδα όσο και στο εξωτερικό. Σύμφωνα με στοιχεία της ICAP, ο κλάδος των ΤΠΕ στην Ελλάδα αριθμεί περισσότερες από 5.300 επιχειρήσεις και απασχολεί 260.000 εργαζόμενους, με κύκλο εργασιών την τελευταία τριετία €13.5Β€/έτος, που αντιστοιχεί σε ~8% του ΑΕΠ.

Η ψηφιακή οικονομία στην Ελλάδα αναπτύσσεται σταθερά και βρίσκεται σε μια δυναμική διαδικασία μετασχηματισμού. Αν και υπήρξε καθυστέρηση σε σύγκριση με άλλες ευρωπαϊκές χώρες, η ψηφιακή ανάπτυξη και η εφαρμογή νέων τεχνολογιών έχουν αρχίσει να κερδίζουν δυναμικό έδαφος. Συγκεκριμένα:

Υποδομές και Συνδεσιμότητα: Η Ελλάδα έχει επενδύσει σημαντικά στην ανάπτυξη ψηφιακών υποδομών και στη βελτίωση της συνδεσιμότητας. Τα δίκτυα πολύ υψηλής χωρητικότητας (VHCN) επεκτείνονται συνεχώς. Στην κινητή τηλεφωνία, με την έναρξη εμπορικής διάθεσης υπηρεσιών 5G ήδη από το τέλος του 2020, η Ελλάδα βρέθηκε ανάμεσα στις 10 πρώτες χώρες της Ευρωπαϊκής Ένωσης σε πληθυσμιακή κάλυψη και παραμένει και σήμερα άνω του ευρωπαϊκού μέσου όρου. Παράλληλα συνεχίζει να βρίσκεται πολύ ψηλά σε δείκτες ποιότητας, όπως η ταχύτητα ανοδικής και καθοδικής ζεύξης. Η συνδεσιμότητα είναι απαραίτητη για την πιο αποτελεσματική πρόσβαση στο Διαδίκτυο και τις ψηφιακές υπηρεσίες.

Ψηφιακός Μετασχηματισμός: Ο ψηφιακός μετασχηματισμός, τόσο του δημόσιου τομέα, όσο και των επιχειρήσεων, έχει σημειώσει αξιοσημείωτη πρόοδο, περιλαμβάνοντας την ψηφιοποίηση υπηρεσιών και διαδικασιών, καθώς και την επέκταση των διαδικτυακών υπηρεσιών για τους πολίτες και τις επιχειρήσεις. Ωστόσο, κρίνεται αναγκαία ~~σημαντική~~ η ένταξη όσο το δυνατόν περισσότερων επιχειρήσεων στις δράσεις ψηφιακού μετασχηματισμού, καθώς η διαφορά στο δείκτη DESI με το μέσο όρο της ΕΕ, σχετικά με την ενσωμάτωση της Ψηφιακής Τεχνολογίας στις επιχειρήσεις, είναι σημαντική.

Δεξιότητες: Κρίσιμη είναι η επένδυση στο Ανθρώπινο Κεφάλαιο και ειδικότερα στις Ψηφιακές δεξιότητες (digital skills), ως απαραίτητου καταλύτη για την ανάπτυξη όλων των κλάδων της οικονομίας. Η ανάπτυξη ενός εξειδικευμένου, υψηλών Ψηφιακών δεξιοτήτων Ανθρώπινου Δυναμικού αποτελεί τη βάση για τη δημιουργία νέων θέσεων εργασίας, με έμφαση στη συμμετοχή των γυναικών και τη μείωση των ανισοτήτων στην πρόσβαση στην αγορά εργασίας.

Η μελέτη[13] [12] του Συνδέσμου Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας (ΣΕΠΕ) για την αποτίμηση επάρκειας ειδικών ΤΠΕ στην Ελλάδα επιβεβαίωσε ότι η συντριπτική πλειονότητα των

[13] Μελέτη ΣΕΠΕ - Deloitte, *Αποτίμηση Επάρκειας Ειδικών ΤΠΕ στην Ελλάδα*, https://www.sepe.gr/research-studies/21142064

επιχειρήσεων στη χώρα έχουν κενές θέσεις ειδικών ΤΠΕ και στο άμεσο μέλλον αναμένεται σημαντική αύξηση των αναγκών τους στις ειδικότητες αυτές. Εκτιμήθηκε ότι η απόκλιση ζήτησης-προσφοράς για την περίοδο 2023-30 είναι 7.000-7.500 άτομα/έτος. Ο ΣΕΠΕ, σε συνεργασία με την Εθνική Αρχή Ανώτατης Εκπαίδευσης (ΕΘΑΑΕ) και τους Προέδρους των 37 Τμημάτων Πληροφορικής των ελληνικών πανεπιστημίων, έχει προτείνει σημαντικές, ουσιαστικές και καινοτόμες προτάσεις για την αντιμετώπιση της έλλειψης εξειδικευμένου ανθρώπινου δυναμικού στις ΤΠΕ, κρίσιμης παραμέτρου για την υλοποίηση του εθνικού στόχου του Ψηφιακού Μετασχηματισμού της χώρας.

Καινοτομία και Επιχειρηματικότητα: Ο ψηφιακός μετασχηματισμός έχει τη δυνατότητα να αυξήσει την καινοτομία και την παραγωγικότητα της οικονομίας της Ελλάδας, προσφέροντας νέες ευκαιρίες για τους πολίτες και τις επιχειρήσεις. Υπάρχει αυξανόμενη υποστήριξη για την καινοτομία και την επιχειρηματικότητα στον τομέα της τεχνολογίας και της ψηφιακής οικονομίας. Σύμφωνα με το European Innovation Scoreboard (EIS)[14] [13] η Ελλάδα είναι μεταξύ των τεσσάρων χωρών της ΕΕ με τη μεγαλύτερη βελτίωση (βελτίωση 22.2% για την Ελλάδα). Οι δείκτες, οι οποίοι υποστήριξαν τη βελτίωση είναι: (α) η κυβερνητική υποστήριξη για την Ε&Α επιχειρήσεων, (β) οι δημόσιες δαπάνες Ε&Α, (γ) η κινητικότητα από εργασία σε εργασία του ανθρώπινου δυναμικού στην επιστήμη και τεχνολογία και (δ) η παραγωγικότητα των πόρων.

Παράλληλα, όπως απεικονίζεται στα Γραφήματα 16 και 17[15], έχουν γίνει σημαντικά βήματα αναφορικά με τη χρήση των ΤΠΕ από τα νοικοκυριά και τους πολίτες αλλά και από τις επιχειρήσεις.

Από τα στοιχεία διαπιστώνουμε ότι το 2023:

- 86.9% των νοικοκυριών έχουν πρόσβαση στο διαδίκτυο από την κατοικία τους (56.3% το 2013).
- Στον πληθυσμό ηλικίας 16-74 ετών που χρησιμοποίησε το διαδίκτυο από Απρίλιο 2022 - Μάρτιο 2023, το 77.8% έκαναν χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης για προσωπικούς λόγους.
- 98.6% των επιχειρήσεων με απασχόληση 10 ατόμων και άνω είχαν πρόσβαση στο διαδίκτυο για επαγγελματικούς σκοπούς.

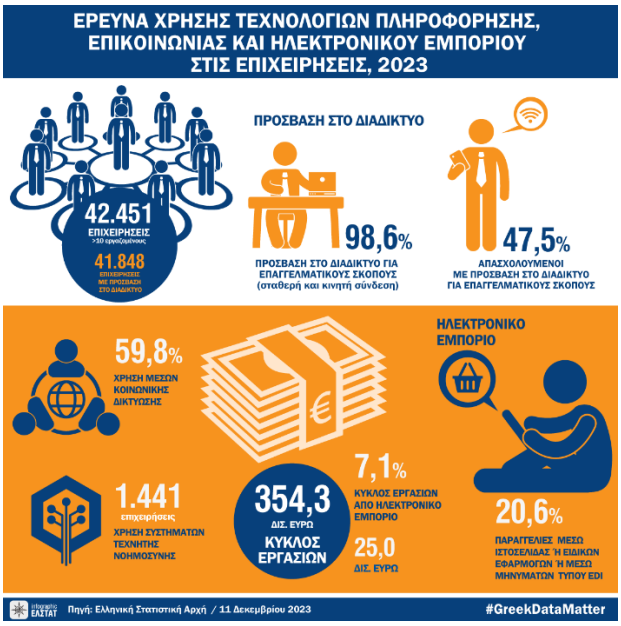
/m3eleti-sepe-deloitte-apotimisis-eparkeias-eidikon-tpe-stin-ellada/

14 European Innovation Scoreboard (EIS), https://op.europa.eu/en/home

15 https://www.statistics.gr/en/elstat-infographics

Γράφημα 16: ΕΛΛΑΔΑ: Χρήση Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ)

Γράφημα 17: ΕΛΛΑΔΑ: Χρήση Τεχνολογιών Πληροφορικής, Επικοινωνίας και Ηλεκτρονικού Εμπορίου



Το μέλλον της Ψηφιακής Οικονομίας είναι γεμάτο με νέες προκλήσεις και σημαντικά οφέλη για όσους μπορούν να αντεπεξέλθουν στις συνεχώς αυξανόμενες απαιτήσεις του διεθνοποιημένου ανταγωνισμού. Αν και έχουν γίνει σημαντικά βήματα για να αξιοποιηθούν πλήρως τα οφέλη της ψηφιοποίησης, απαιτείται πρόοδος σε αρκετούς τομείς. Ο ρόλος της Πολιτείας στην προσπάθεια αυτή είναι σημαντικός.

2.1.5 ΕΛΛΑΔΑ – Θεσμοί Κυβερνοασφάλειας

Η Ελλάδα, αναγνωρίζοντας τη θεμελιώδη σημασία της κυβερνοασφάλειας, ανέλαβε σημαντικές πρωτοβουλίες, με γνώμονα την ανταπόκριση στις διεθνείς και ενωσιακές απαιτήσεις, τη διαμόρφωση ασφα-

λούς περιβάλλοντος για τις ψηφιακές τεχνολογίες και την αύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων σε ψηφιακές εφαρμογές και υπηρεσίες προς όφελος της οικονομίας και της κοινωνίας.

Στο πλαίσιο αυτό, οι αρχικές πρωτοβουλίες της Ελλάδας περιλάμβαναν:

(α) Νόμος 4577/2018[16] για την «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις».

(β) Υπουργική Απόφαση 1027/2019[17] με βάση την οποία καθορίστηκε το πλαίσιο υποχρεώσεων για τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και για τους Παρόχους Ψηφιακών Υπηρεσιών (ΠΨΥ), περιλαμβανομένων των απαιτήσεων ασφαλείας που οφείλουν αυτοί να τηρούν κλπ.

2.1.6 Εθνική Αρχή Κυβερνοασφάλειας

Η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)[18] της Ελλάδας μετασχηματίστηκε, αναβαθμιζόμενη σε ανεξάρτητο Νομικό Πρόσωπο Δημοσίου Δικαίου (2024). Οι διαφοροποιήσεις, σε σχέση με την προϋπάρχουσα δομή και λειτουργία, καθώς και τα βασικά θεσμικά και λειτουργικά χαρακτηριστικά της νέας ΕΑΚ είναι:

- Ενίσχυση και αποσαφήνιση των δυνατοτήτων και αρμοδιοτήτων της, σύμφωνα με τις διεθνείς και ευρωπαϊκές καλές πρακτικές (βλ. Γράφημα 18).
- Θεσμικός μετασχηματισμός της σε αυτοτελές Νομικό Πρόσωπο Δημοσίου Δικαίου (ΝΠΔΔ), υπό την ευθύνη του Υπουργείου Ψηφιακής Διακυβέρνησης.
- Αύξηση πόρων, οργανωτική ενίσχυση και τριπλασιασμός των θέσεων του προσωπικού της.
- Οργανωτικός ανασχηματισμός της, με δύο νέους οργανωτικούς και λειτουργικούς πυλώνες: (α) Γενική Διεύθυνση Επιτελικού Σχεδιασμού και (β) Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού.

Γράφημα 18: Εθνική Αρχή Κυβερνοασφάλειας (2024) [16]

2.1.7 Εθνική Στρατηγική Κυβερνοασφάλειας

Στη συνέχεια, η Ελλάδα εκπόνησε Εθνική Στρατηγική Κυβερνοασφάλειας (ΕΣΚ), την οποία αναθεώρησε κατά περιόδους. Επίσης, μετασχημάτισε την Εθνική Αρχή Κυβερνοασφάλειας από Γενική Διεύθυνση του

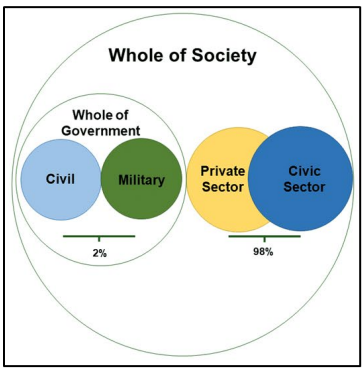
16 https://mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf

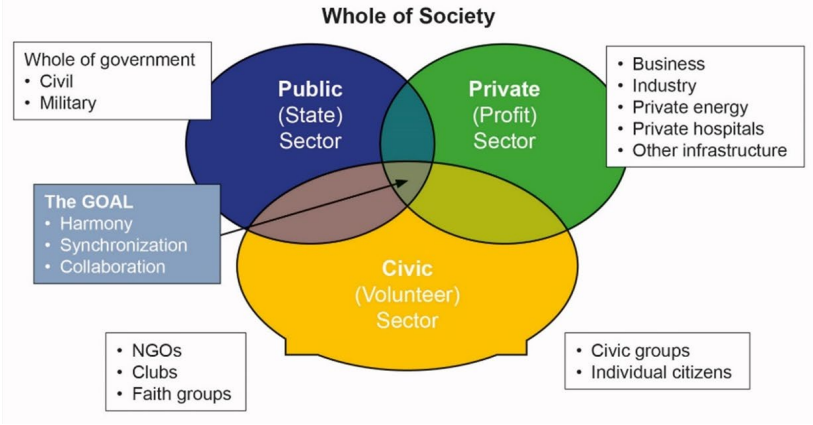
17 https://mindigital.gr/wp-content/uploads/2020/01/3739B-19-1.pdf

18 Εθνική Αρχή Κυβερνοασφάλειας (Ν. 5086/2024, ΦΕΚ 23/Α/14.02.2024, https://www.et.gr/).

Υπουργείου Ψηφιακής Διακυβέρνησης σε αυτοτελές Νομικό Πρόσωπο Δημοσίου Δικαίου (ΝΠΔΔ). Ο απώτερος στρατηγικός στόχος των πρωτοβουλιών και μεταρρυθμίσεων αυτών είναι ο μετασχηματισμός της προσέγγισης "whole-of-government" στη διακυβέρνηση "whole-of-society" (βλ. Γράφημα 19).

Γράφημα 19: Στρατηγική μετάβαση από "whole-of-government" σε "whole-of-society"





Η τρέχουσα ΕΣΚ[19] της Ελλάδας τέθηκε σε ισχύ το 2020 και αφορά στη χρονική περίοδο 2020-25 [17][18]. Η ισχύουσα ΕΣΚ (βλ. Γράφημα 20):

- Διαδέχεται λειτουργικά, εξειδικεύει, εκσυγχρονίζει, αναθεωρεί και συμπληρώνει την προηγούμενη ΕΣΚ (2016-21).
- Περιλαμβάνει λεπτομερές Σχέδιο Δράσης (Action Plan), επιτρέποντας την εφαρμογή διοίκησης μέσω στόχων (Management by Objectives, MBO).
- Πλαισιώνεται από σαφή καθορισμό ρόλων και αρμοδιοτήτων των εμπλεκόμενων φυσικών οντοτήτων, μέσω του ορισμού Συντονιστών και Χειριστών.
- Ακολουθεί το πλαίσιο καλών πρακτικών του ENISA και υιοθετεί τα συστήματα αξιολόγησης του εν λόγω οργανισμού
- Αποτελεί βάση για την αξιολόγηση του έργου της ΕΑΚ, αξιοποιώντας πρότυπα ποιότητας (TQM) και επιχειρηματικής αριστείας (Business Excellence).

Οι βασικοί θεσμικοί συμμέτοχοι-δρώντες (actors/stakeholders), στο πλαίσιο της νέας ΕΣΚ, είναι:

(α) Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) (National Cybersecurity Authority).

(β) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) (Data Protection Authority).

(γ) Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ) (National Authority for the Protection of Telecommunications).

(δ) Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) (National Committee for Telecommunications and Posts).

(ε) Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΔΗΕ) (Greek Police Cybercrime Unit).

(στ) Εθνικό CERT (National CERT) και Στρατιωτικό CSIRT (Military CSIRT).

[19] Οργανισμός Υπουργείου Ψηφιακής Διακυβέρνησης (Π.Δ. 40/2020, ΦΕΚ 85/Α/15.04.2020, https://www.kodiko.gr/nomothesia/document/616684/p.d.-40-2020) και Εθνική Στρατηγική Κυβερνοασφάλειας 2020-25 (Υ.Α. 34368, 07/12/2020, https://mindigital.gr/wp-content/uploads/2020/12/national-cybersecurity-strategy-2020-2025.pdf).

Γράφημα 20: Εθνική Στρατηγική Κυβερνοασφάλειας (2020-25): Στρατηγικοί και ειδικοί στόχοι [18]

				
1. Ένα λειτουργικό σύστημα διακυβέρνησης 1.Α. Βελτιστοποίηση του πλαισίου οργάνωσης και λειτουργίας δομών και διαδικασιών 1.Β. Αποτελεσματικός σχεδιασμός αποτίμησης επικινδυνότητας και διαχείρισης έκτακτης ανάγκης. 1.Γ. Ενδυνάμωση συνεργασιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο	**2. Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες** 2.Α. Κατανόηση των τεχνολογικών εξελίξεων και του τρόπου που επηρεάζουν την ψηφιακή διακυβέρνηση. 2.Β.Αναβάθμιση της προστασίας κρίσιμων υποδομών 2.Γ.Θωράκιση συστημάτων και εφαρμογών μέσω ενισχυμένων απαιτήσεων ασφαλείας	**3. Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας** 3.Α. Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων 3.Β. Ενδυνάμωση μηχανισμών αποτροπής και βελτιστοποίηση της επιχειρησιακής συνεργασίας 3.Γ. Κυβερνοασφάλεια και προστασία της ιδιωτικότητας	**4. Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης** 4.Α. Προαγωγή της Έρευνας και Ανάπτυξης 4.Β. Παροχή επενδυτικών κινήτρων 4.Γ. Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)	**5. Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης** 5.Α. Βελτίωση ικανοτήτων μέσω οργάνωσης κατάλληλων ασκήσεων 5.Β. Αξιοποίηση σύγχρονων μεθόδων και εργαλείων κατάρτισης και εκπαίδευσης 5.Γ. Διαρκής ενημέρωση Φορέων και πολιτών αναφορικά με θέματα κυβερνοασφάλειας

2.1.8 ΕΛΛΑΔΑ - Αγορά Κυβερνοασφάλειας

Κατά το Q1/2024 παρατηρήθηκε εξέλιξη και συνέχιση των προκλήσεων στον τομέα της Κυβερνοασφάλειας, οι οποίες είχαν εμφανιστεί το 2023, με αξιοσημείωτη αύξηση των κυβερνοεπιθέσεων σε διάφορους τομείς και περιοχές. Ειδικότερα, σημειώθηκε αύξηση 28% των επιθέσεων στον κυβερνοχώρο παγκοσμίως, σε σύγκριση με το τελευταίο τρίμηνο του 2023, με αύξηση 5% από το 2022. Αυτό δείχνει μια ανησυχητική τάση ταχείας κλιμάκωσης των απειλών στον κυβερνοχώρο.

Ο τομέας της Εκπαίδευσης/Έρευνας κατέχει την πρώτη θέση στη στοχοποίηση με 2.454 επιθέσεις/οργανισμό, σε εβδομαδιαία βάση, ακολουθούμενος από τον τομέα της Κυβέρνησης, των Ενόπλων Δυνάμεων και της Υγείας. Στον κλάδο των προμηθευτών Υλικού παρατηρήθηκε ετήσια αύξηση των επιθέσεων κατά 37%, γεγονός που αναδεικνύει μια ανησυχητική στρατηγική μετατόπιση στόχων (NetFaX, 11.04.2024).

Όσο αυξάνονται οι κίνδυνοι από το κυβερνοέγκλημα, αντίστοιχα πολλαπλασιάζονται και οι επενδύσεις στην Κυβερνοασφάλεια, σε ένα ιδιότυπο «αγώνα δρόμου» ο οποίος εξελίσσεται τα τελευταία χρόνια. Σύμφωνα με μελέτη της Marketsandmarkets[20] [19] η παγκόσμια αγορά Κυβερνοασφάλειας αναμένεται να αυξηθεί από 190.4B$ (2023) σε 298.5B$ (2028), αν περιληφθούν όλοι οι επιμέρους τομείς της. Σύμφωνα με την WatchGuard Technologies «το 2024, οι αναδυόμενες απειλές που στοχεύουν εταιρείες και άτομα θα είναι ακόμη πιο έντονες, περίπλοκες και δύσκολες ως προς τη διαχείριση".

Με τη συνεχιζόμενη έλλειψη δεξιοτήτων στον κυβερνοχώρο, η ανάγκη για Πάροχους Διαχειριζόμενων Υπηρεσιών (Managed Service Providers, MSP), ενοποιημένη ασφάλεια, ~~και~~ αυτοματοποιημένες πλατφόρμες ενίσχυσης της Κυβερνοασφάλειας και προστασία των επιχειρήσεων από το συνεχώς εξελισσόμενο τοπίο απειλών δεν ήταν ποτέ μεγαλύτερη. Η μελέτη [12] που εκπόνησε ο ΣΕΠΕ, σε συνεργασία με την Deloitte, για την αξιολόγηση της επάρκειας ειδικών ΤΠΕ στην Ελλάδα, συμπέρανε ότι η Κυβερνοασφάλεια είναι ανάμεσα στις τρεις ειδικότητες με την μεγαλύτερη ζήτηση στον κλάδο ΤΠΕ, τόσο στον ιδιωτικό τομέα, όσο και τον δημόσιο. Σε μια αγορά που παγκοσμίως εκτιμάται σε εκατοντάδες Β€, οι Έλληνες επιχειρηματίες του τεχνολογικού κλάδου διεκδικούν το μεγαλύτερο δυνατόν μερίδιο, συχνά συνεργαζόμενοι με ισχυρούς επενδυτές. Η ελληνική αγορά συνεχίζει τις επενδύσεις στην Κυβερνοασφάλεια. Οι ελληνικοί τεχνολογικοί όμιλοι που δραστηριοποιούνται στον κλάδο αναπτύσσονται με ποσοτικούς και ποιοτικούς όρους. Το ίδιο και οι επενδυτές οι οποίοι στηρίζουν τα σχετικά εγχειρήματα.

Σημαντικές είναι και οι δράσεις του κράτους. Το Q4/2023 η Ελλάδα υπέγραψε Συμφωνία Χρηματοδότησης (Grant Agreement) με το Ευρωπαϊκό Κέντρο Δεξιοτήτων Κυβερνοασφάλειας (ECCC), από την οποία θα χρηματοδοτηθεί η ανάπτυξη και η λειτουργία του Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας (Security Operations Center, SOC). Το SOC στοχεύει στην ανάπτυξη, υποστήριξη και ενδυνάμωση των ικανοτήτων σε εθνικό επίπεδο για την έγκαιρη ανίχνευση και αντιμετώπιση κυβερνοαπειλών, ιδίως μέσω της ενίσχυσης των δυνατοτήτων έγκαιρης προειδοποίησης, ανίχνευσης και αντιμετώπισης κυβερνοεπιθέσεων και με χρήση σύγχρονων εργαλείων Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης. Δημιουργείται Εθνικό Δίκτυο SOC, που αποτελείται από τομεακά SOC, για την υποστήριξη των Οργανισμών που θα μετέχουν σε αυτό, με στόχο την αναγνώριση, διαχείριση, αντιμετώπιση και ανάκαμψη από κυβερνοεπιθέσεις.

Τέλος, συνεχίζεται με εντατικό ρυθμό η «ψηφιοποίηση» του συνόλου της Οικονομίας και της Δημόσιας Διοίκησης, με στόχο την επαρκή θωράκιση πολιτών, επιχειρήσεων και Δημόσιας Διοίκησης απέναντι στις κυβερνοαπειλές κάθε είδους.

[20] Marketsandmarkets Cybersecurity Market, Global Forecast to2028, https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

ΚΕΦΑΛΑΙΟ 3 - Προσφορά εκπαίδευσης και κατάρτισης στην Κυβερνοασφάλεια

3.1 ΕΛΛΑΔΑ - Τυπικό εκπαιδευτικό σύστημα

Το τυπικό εκπαιδευτικό σύστημα της Ελλάδας [8] απαρτίζεται από τα εξής επίπεδα[21]: (α) **Πρωτοβάθμια εκπαίδευση** (Νηπιαγωγείο, Δημοτικό σχολείο), (β) **Δευτεροβάθμια εκπαίδευση** (Γυμνάσιο, Λύκειο), (γ) **Σχολεία Δεύτερης Ευκαιρίας**, (δ) **Μεταγυμνασιακή επαγγελματική εκπαίδευση και κατάρτιση** [Επαγγελματικές Σχολές Κατάρτισης, Επαγγελματικές Σχολές Μαθητείας (ΔΥΠΑ)], (ε) **Μεταδευτεροβάθμια επαγγελματική κατάρτιση** (Ινστιτούτα Επαγγελματικής Κατάρτισης, Μεταλυκειακό έτος - Τάξη Μαθητείας) και (στ) **Ανώτατη εκπαίδευση** (Πανεπιστήμια, Πολυτεχνεία, Ανώτατη Σχολή Καλών Τεχνών, Ανώτατη Σχολή Παιδαγωγικής & Τεχνολογικής Εκπαίδευσης).

Τα επίπεδα αντιστοίχισης του Ελληνικού με το **Ευρωπαϊκό Πλαίσιο Προσόντων [20]** (European Qualification Framework (**EQF**)) (βλ. Γράφημα 21) που θα μελετηθούν στο πλαίσιο του παραδοτέου είναι:

EQF 4: Απολυτήριο Γενικού Λυκείου, Απολυτήριο Επαγγελματικού Λυκείου-Επαγγελματικής Σχολής

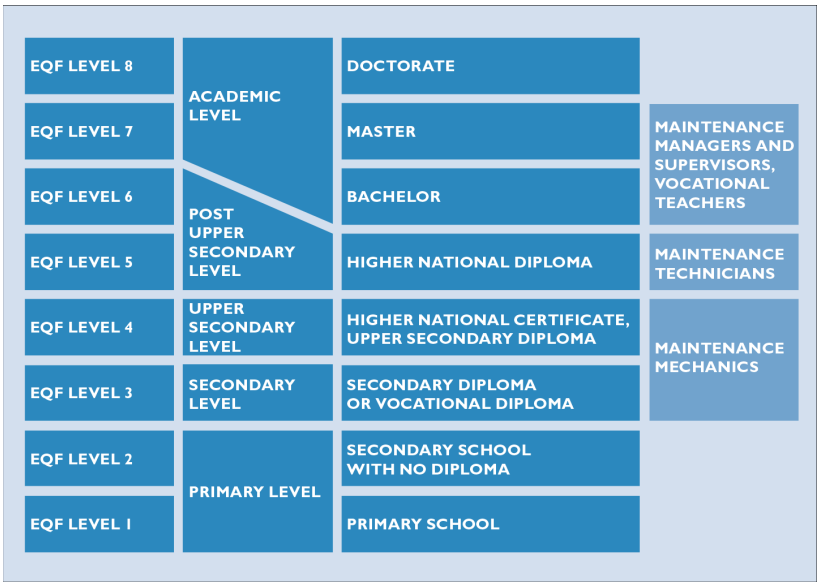
EQF 5: Απολυτήριο Τεχνικού-Επαγγελματικού Λυκείου, Τίτλος Ινστιτούτου Επαγγελματικής Κατάρτισης

EQF 6: Πανεπιστημιακός Τίτλος - Τίτλος Τεχνολογικού Εκπαιδευτικού Ιδρύματος

EQF 7: Μεταπτυχιακό Δίπλωμα Εξειδίκευσης

EQF 8: Διδακτορικό Δίπλωμα

Γράφημα 21: ΕΕ - Ευρωπαϊκό Πλαίσιο Προσόντων (EQF) [20]



Στα επίπεδα **EQF 4** και **EQF 5** δεν παρέχονται πιστοποιούμενες γνώσεις στην Κυβερνοασφάλεια. Ειδικότερα, στη **Δευτεροβάθμια εκπαίδευση** (Γυμνάσιο, Λύκειο) εκπαίδευση δεν υπάρχουν κατευθύνσεις που εξειδικεύουν σε Κυβερνοασφάλεια. Ομοίως, δεν παρέχεται τέτοια εξειδίκευση ούτε σε **Επαγγελματικές Σχολές Κατάρτισης ή Επαγγελματικές Σχολές Μαθητείας** (ΟΑΕΔ), ούτε σε **Ινστιτούτα Επαγγελματικής Κατάρτισης** (δημόσια και Ιδιωτικά).

[21] https://eurydice.eacea.ec.europa.eu/national-education-systems/greece/overview%20

Κατ' εξαίρεση, στην παρούσα μελέτη θα περιληφθούν οι απόφοιτοι **Κέντρων Δια Βίου Μάθησης και Επιμόρφωσης (**ΚΕΔΙΒΙΜ), καθώς και οι πιστοποιούμενοι από τοπικά παραρτήματα έγκυρων διεθνών επαγγελματικών συλλογικότητων (**ISC², ISACA**), δεδομένου ότι η παρουσία τους στο τοπικό επίπεδο είναι ορατή και εκτιμάται ως αξιόλογη. Το **ad hoc** επίπεδο των εκπαιδεύσεων/καταρτίσεων που παρέχονται από τους οργανισμούς αυτούς θα μπορούσε να θεωρηθεί ως **EQF4+** ή **EQF5**.

Περαιτέρω, στην Ελλάδα **δεν υπάρχουν** πανεπιστημιακά ιδρύματα που παρέχουν βασικό τίτλο σπουδών (επίπεδο **EQF 6**, «*Πτυχίο*» (**B.Sc.**)) στον τομέα «*Κυβερνοασφάλεια - Προστασία Ψηφιακών Υποδομών – Ασφάλεια Πληροφοριακών /Επικοινωνιακών/Ψηφιακών Συστημάτων*» (στο εξής και για λόγους συντομίας «*Κυβερνοασφάλεια*» ή «*Κυβερνοασφάλεια και συναφή γνωστικά πεδία*»).

Αναφορικά με τα επίπεδα **EQF 7** και **EQF 8**, τα ελληνικά πανεπιστήμια διαθέτουν προγράμματα σπουδών και στα δύο επίπεδα. Ειδικότερα, προφέρουν Προγράμματα Μεταπτυχιακών Σπουδών (**EQF 7**, «*Μεταπτυχιακό Δίπλωμα Εξειδίκευσης*» (**M.Sc.**) ή «*Δίπλωμα*» (**Dipl.Eng.**)), καθώς και Προγράμματα Διδακτορικών Σπουδών (**EQF 8**, «*Διδακτορικό Δίπλωμα*» (**Ph.D.**)).

3.2 ΕΛΛΑΔΑ – Μεταπτυχιακές σπουδές

3.2.1 Προγράμματα Μεταπτυχιακών Σπουδών

Μεταξύ των Προγραμμάτων Μεταπτυχιακών Σπουδών (ΠΜΣ) που προσφέρονται από ελληνικά πανεπιστήμια, περιλαμβάνονται προγράμματα που παρέχουν εκπαίδευση επιπέδου **EQF 7** (Μεταπτυχιακό Δίπλωμα Εξειδίκευσης, **M.Sc.**) με εξειδίκευση (και) στην «*Κυβερνοασφάλεια*». Ειδικότερα, τα ΠΜΣ με αυτή τη γνωστική εξειδίκευση (πλήρους ή/και μερικής φοίτησης) λειτουργούν σήμερα (02/2024) στα εξής **πέντε (5) Πανεπιστήμια** και **έξι (6) Πανεπιστημιακά Τμήματα**:

1. **Οικονομικό Πανεπιστήμιο Αθηνών** (Τμήμα Πληροφορικής)
2. **Πανεπιστήμιο Πειραιώς** (Τμήμα Πληροφορικής & Τμήμα Ψηφιακών Συστημάτων)
3. **Πανεπιστήμιο Αιγαίου** (Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων)
4. **Πανεπιστήμιο Δυτικής Αττικής** (Τμήμα Μηχανικών Πληροφορικής & Υπολογιστών)
5. **Διεθνές Πανεπιστήμιο της Ελλάδος** (Σχολή Επιστήμης & Τεχνολογίας)

Το σύνολο των θέσεων που προσφέρονται από τα ΠΜΣ αυτά ανέρχεται σε **360** ανά έτος. Η ολοκλήρωση των σπουδών σε κάθε ένα απαιτεί συμπλήρωση ενενήντα (**90) Πιστωτικών Μονάδων (ECTS)**. Ο Πίνακας 4 αποτυπώνει τα γενικά ακαδημαϊκά και λειτουργικά χαρακτηριστικά των ΠΜΣ αυτών.

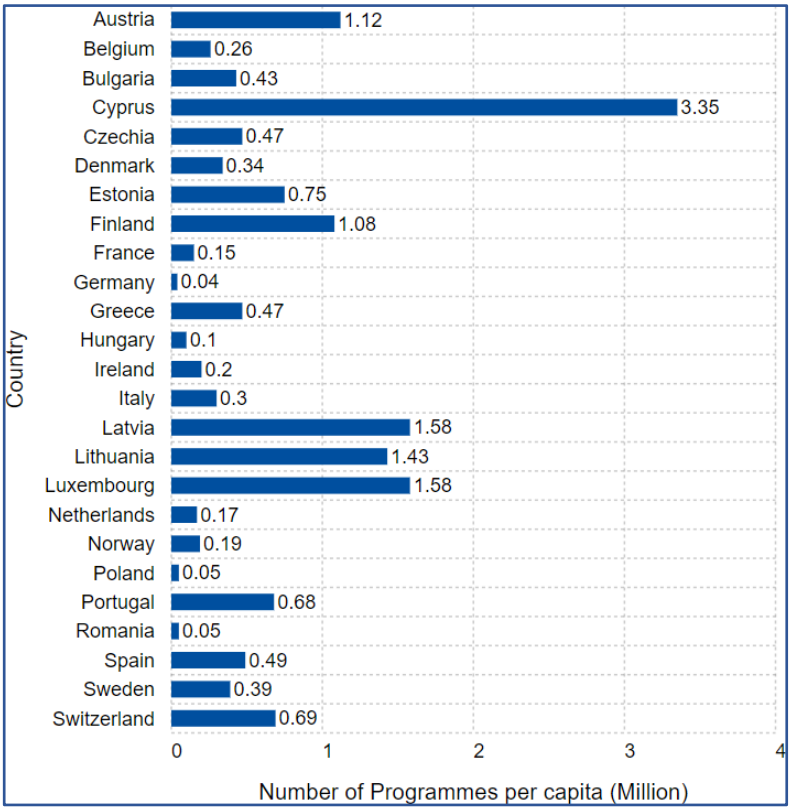
Πίνακας 4: ΕΛΛΑΔΑ - ΠΜΣ Πανεπιστημίων στην Κυβερνοασφάλεια

Πρόγραμμα Μεταπτυχιακών Σπουδών (εξειδίκευση, δίδακτρα, max αριθμός φοιτητών/έτος)	**Πλήρης/ Μερική Φοίτηση** (ΠΦ/ΜΦ)	**Διπλωματική Εργασία** (ΔΕ) **/Πρακτική Άσκηση** (ΠΑ)	**Πανεπιστήμιο** (ΑΕΙ)	**Τμήμα/Σχολή**	**Διάρκεια** (6-μηνα)
Ασφάλεια & Ανάπτυξη Πληροφοριακών Συστημάτων (4K€ ή 5.6K€) (**70**)	ΠΦ/ΜΦ	ΔΕ/ΠΑ (ΠΦ) ή ΔΕ (ΜΦ)	Οικονομικό Πανεπιστήμιο Αθηνών	Πληροφορικής	3-4
Κυβερνοασφάλεια & Επιστήμη Δεδομένων (4.5K€) (**60**)	ΠΦ	ΔΕ	Πανεπιστήμιο Πειραιώς	Πληροφορικής	3

Πρόγραμμα Μεταπτυχιακών Σπουδών (εξειδίκευση, δίδακτρα, max αριθμός φοιτητών/έτος)	**Πλήρης/ Μερική Φοίτηση** (ΠΦ/ΜΦ)	**Διπλωματική Εργασία** (ΔΕ) **/Πρακτική Άσκηση** (ΠΑ)	**Πανεπιστήμιο** (ΑΕΙ)	**Τμήμα/Σχολή**	**Διάρκεια** (6-μηνα)
Ασφάλεια Ψηφιακών Συστημάτων[22] (4.5Κ€) (**40**)	ΠΦ	ΔΕ		Ψηφιακών Συστημάτων	3
Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων (3Κ€) (**30**)	ΠΦ/ΜΦ	ΔΕ	Πανεπιστήμιο Αιγαίου	Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων	3-6
Κυβερνοασφάλεια (2.9Κ€) (**40**)	ΠΦ	ΔΕ	Πανεπιστήμιο Δυτικής Αττικής	Μηχανικών Πληροφορικής & Υπολογιστών	3
Κυβερνοασφάλεια (2.9Κ€) (**120**)	ΠΦ/ΜΦ	ΔΕ	Διεθνές Πανεπιστήμιο Ελλάδος	Σχολή Επιστήμης & Τεχνολογίας	3-5

Αναφορικά με το πλήθος των σχετικών ΠΜΣ/Capita και σε σχέση με τα λοιπά Κράτη-Μέλη της ΕΕ, η Ελλάδα κατέχει την **10η** θέση (βλ. Γράφημα 22).

Γράφημα 22: ΕΕ – Προγράμματα Πανεπιστημιακών Σπουδών σε Κυβερνοασφάλεια [21]



Οι πρόσφατες (2021-23) ετήσιες εκροές αποφοίτων των ΠΜΣ αυτών παρατίθενται στον Πίνακα 5.

[22] Από το ακαδημαϊκό έτος 2024-25 το συγκεκριμένο ΜΠΣ μετονομάζεται σε «Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης» (M.Sc. in Cybersecurity and AI Technologies). Το ύψος των διδάκτρων ανά φοιτητή καθορίζεται σε 4.9Κ€.

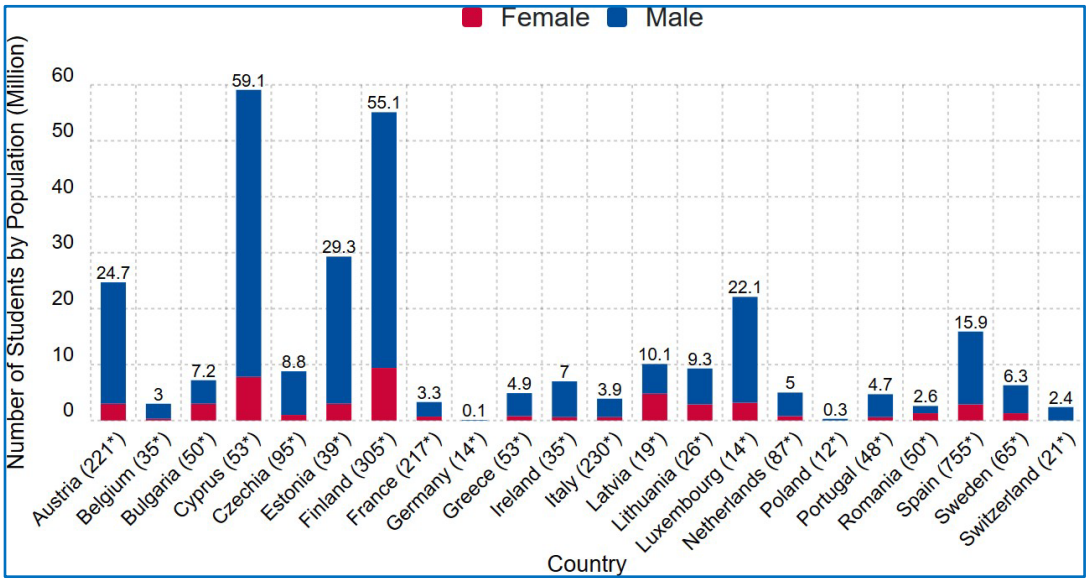
Πίνακας 5: ΕΛΛΑΔΑ - Απόφοιτοι ΠΜΣ Πανεπιστημίων σε Κυβερνοασφάλεια (ανά έτος & φύλο)

Πανεπιστήμιο & Πρόγραμμα Μεταπτυχιακών Σπουδών	2021		2022		2023		Σύνολο		
	Α	Γ	Α	Γ	Α	Γ	Α	Γ	Α+Γ
Οικονομικό Πανεπιστήμιο Αθηνών Ασφάλεια & Ανάπτυξη Πληροφοριακών Συστημάτων	28	10	39	18	34	11	**101**	**39**	**140**
Πανεπιστήμιο Πειραιώς Κυβερνοασφάλεια & Επιστήμη Δεδομένων	38	10	35	10	36	11	**109**	**31**	**140**
Πανεπιστήμιο Πειραιώς Ασφάλεια Ψηφιακών Συστημάτων	34	6	25	3	22	3	**81**	**12**	**93**
Πανεπιστήμιο Αιγαίου Ασφάλεια Πληροφοριακών & Επικοινωνιακών Συστημάτων	19	6	13	5	12	3	**44**	**14**	**58**
Πανεπιστήμιο Δυτικής Αττικής Κυβερνοασφάλεια	23	5	21	4	31	11	**75**	**20**	**95**
Διεθνές Πανεπιστήμιο της Ελλάδος Κυβερνοασφάλεια	7	1	5	2	10	2	**22**	**5**	**27**
Σύνολο	**149**	**38**	**138**	**42**	**145**	**41**	**432**	**121**	**553**

Τα επιμέρους χαρακτηριστικά των ΠΜΣ (πχ. ονομασία και φύση μαθημάτων, διάρκεια σπουδών, μεταπτυχιακή εργασία, πρακτική άσκηση κλπ.) παρατίθενται στο **Παράρτημα Ι**.

Στην Ελλάδα, οι απόφοιτοι των ΠΠΣ και ΜΠΣ με αυτή την εξειδίκευση (2020) ανέρχονται σε **4.9/1Μ** κατοίκους, γεγονός που κατατάσσει τη χώρα στην **13η** θέση ανάμεσα στα Κράτη-Μέλη της ΕΕ.

Γράφημα 23: ΕΕ – Απόφοιτοι Πανεπιστημιακών Προγραμμάτων σε Κυβερνοασφάλεια (ανά φύλο) [21]

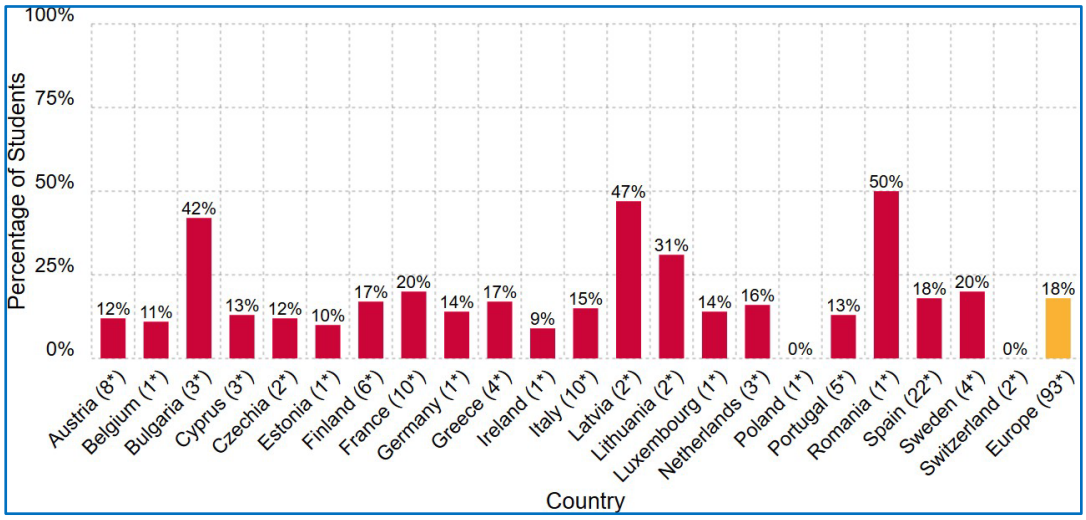


Το ποσοστό των **γυναικών** απόφοιτων στην Ελλάδα (2020) ισούται με τον αντίστοιχο μέσο όρο των Κρατών-Μελών της ΕΕ (**17%** έναντι **18%**) και κατατάσσει τη χώρα στην **15η** θέση. Επιπλέον, στην Ελλάδα το ποσοστό των γυναικών που φοιτούν σε σχετικό ΠΜΣ, σε σχέση με όσες αποφοίτησαν την προηγούμενη

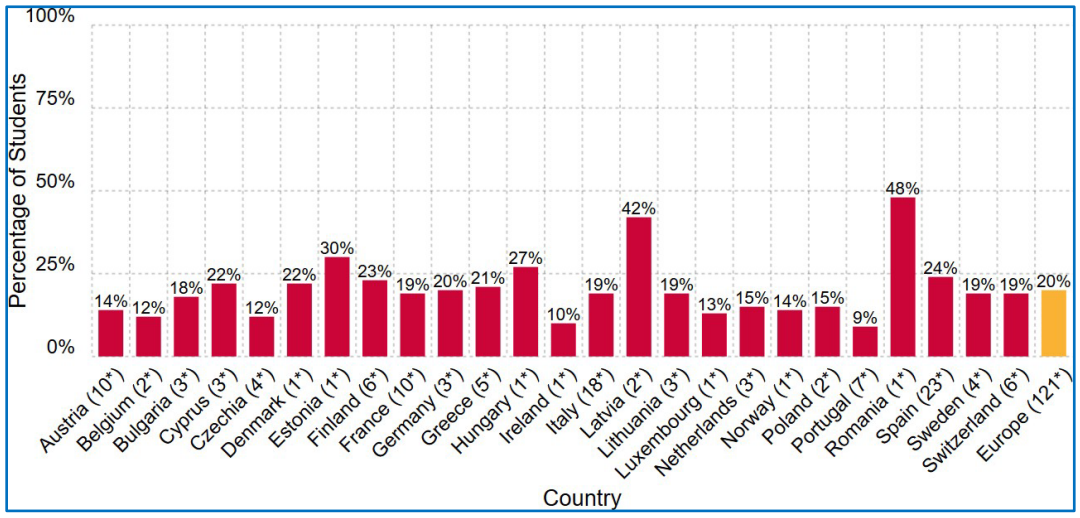
χρονιά, αυξήθηκε από **17%** σε **21%**. Η υπο-εκπροσώπηση των γυναικών παραμένει, διαχρονικά σε χαμηλό ποσοστό στη χώρα μας.

Γράφημα 24: ΕΕ – Απόφοιτες & φοιτήτριες Πανεπιστημιακών Σπουδών σε Κυβερνοασφάλεια (2020) [21]

Γυναίκες απόφοιτοι (ποσοστό ανά χώρα)



Γυναίκες φοιτήτριες (ποσοστό ανά χώρα)



3.2.2 Προγράμματα Διδακτορικών Σπουδών

"Όλα τα ελληνικά πανεπιστήμια έχουν τη δυνατότητα απονομής Διδακτορικών Διπλωμάτων. Τα Διπλώματα επιβεβαιώνουν την ολοκλήρωση εκπαίδευσης επιπέδου **EQF8** (Διδακτορικό Δίπλωμα, **Ph.D.).**

Ο Πίνακας 6 αναφέρει τα Διδακτορικά Διπλώματα (Ph.D.) που απονεμήθηκαν από τα ελληνικά πανεπιστήμια κατά το διάστημα 2021-23, ανά έτος και φύλο. Επιπλέον, στο **Παράρτημα ΙΙ** παρατίθενται τα θέματα των διδακτορικών διατριβών που εκπονήθηκαν, στα ελληνικά και αγγλικά [22].

Πίνακας 6: ΕΛΛΑΔΑ – Ph.D. σε Κυβερνοασφάλεια (έτος & φύλο)

2021		2022		2023		Σύνολο	
Α	Γ	Α	Γ	Α	Γ	Α	Γ

8	**3**	**5**	**1**	**11**	**3**	**24** (77 %)	**7** (23%)
11		**6**		**14**		**31**	

3.3 ΕΛΛΑΔΑ – Μη τυπική εκπαίδευση και κατάρτιση

Στην Ελλάδα, η γενική μη τυπική εκπαίδευση ενηλίκων παρέχεται μεν σε οργανωμένο εκπαιδευτικό πλαίσιο, αλλά εκτός του τυπικού εκπαιδευτικού συστήματος, σε: (α) **Κολλέγια** και (β) **Κέντρα Δια Βίου Μάθησης** (ΚΕΔΙΒΙΜ). Επίσης, σχετικές επαγγελματικές πιστοποιήσεις παρέχονται από τις διεθνείς ενώσεις επαγγελματιών **ICS²** και **ISACA**.

Διευκρινίζεται ότι, αν και τα Κολλέγια στην Ελλάδα παρέχουν στους απόφοιτους τίτλους σπουδών αντίστοιχους των Δημόσιων πανεπιστημίων, εν τούτοις δεν παρέχουν επαγγελματικά δικαιώματα. Δεδομένου δε ότι η παρούσα μελέτη εστιάζεται σε πρόσωπα που διαθέτουν επαγγελματικά δικαιώματα στο γνωστικό πεδίο της Κυβερνοασφάλειας και τα συναφή με αυτήν, επιλέξαμε να εντάξουμε τους απόφοιτους των Κολλεγίων σε όσους διαθέτουν (επαγγελματικούς) τίτλους μη τυπικής εκπαίδευσης.

3.3.1 Κολλέγια – Προγράμματα Σπουδών

Ορισμένα κολλέγια παρέχουν Προγράμματα Προπτυχιακών Σπουδών (ΠΠΣ) ή/και Προγράμματα Μεταπτυχιακών Σπουδών (ΠΜΣ) στην Κυβερνοασφάλεια. Οι Πίνακες 7-8 αποτυπώνουν τα γενικά ακαδημαϊκά και λειτουργικά χαρακτηριστικά των ΠΠΣ και ΠΜΣ, αντίστοιχα. Ο Πίνακας 9 απεικονίζει το πλήθος των απόφοιτων των Προγραμμάτων αυτών, ανά έτος (2021-23) και φύλο.

Τα επιμέρους χαρακτηριστικά αυτών των ΠΜΣ (πχ. ονομασία και φύση μαθημάτων, διάρκεια σπουδών, μεταπτυχιακή εργασία, πρακτική άσκηση κλπ.) παρατίθενται στο **Παράρτημα ΙΙΙ**.

Πίνακας 7: ΕΛΛΑΔΑ - ΠΠΣ Κολεγίων σε Κυβερνοασφάλεια

Πρόγραμμα Προπτυχιακών Σπουδών (ΠΠΣ) (εξειδίκευση)	**Πλήρης/ Μερική Φοίτηση** (ΠΦ/ΜΦ)	**Πτυχιακή Εργασία** (ΠΕ) **/ Πρακτική Άσκηση** (ΠΑ)	**Κολλέγιο**	**Σε συνεργασία με**	**Διάρκεια** (έτη)
B.Sc. Cyber Security & Networks	ΠΦ	ΠΕ	Metropolitan College	University of East London (UK)	3
B.Sc. Cybersecurity	ΠΦ	ΠΕ	New York College	University of Bolton (UK)	3-4
B.Sc. Web Development & Cyber Security	ΠΦ	ΠΕ	Epsilon College	University of Northampton (UK)	3
B.Sc. Cybersecurity & Networks	ΠΦ	--	The American College of Greece	Open University (UK)	3

Πίνακας 8: ΕΛΛΑΔΑ - ΠΜΣ Κολεγίων σε Κυβερνοασφάλεια

Πρόγραμμα Μεταπτυχιακών Σπουδών (εξειδίκευση)	**Πλήρης/ Μερική Φοίτηση** (ΠΦ/ΜΦ)	**Διπλωματική Εργασία** (ΔΕ) **/ Πρακτική Άσκηση** (ΠΑ)	**Κολλέγιο**	**Σχολή/Τμήμα**	**Διάρκεια** (έτη)
M.Sc. Maritime Cybersecurity	ΠΦ/ΜΦ	ΔΕ	BCA College	University of West London (UK)	1-2
M.Sc. Applied Cyber Security	ΠΦ/ΜΦ	ΔΕ	BCA College	University of West London (UK)	1-2
M.Sc. Cyber Security	ΜΦ	ΔΕ/ΠΑ	Aegean College	University of Essex (UK)	2
M.Sc. Information Security & Digital Forensics	ΠΦ	ΔΕ	Metropolitan College	University of East London (UK)	1

Πίνακας 9: ΕΛΛΑΔΑ - Απόφοιτοι ΠΠΣ & ΠΜΣ Κολλεγίων σε Κυβερνοασφάλεια (ανά έτος & φύλο)

Κολλέγιο & Πρόγραμμα (Προπτυχιακών ή Μεταπτυχιακών) **Σπουδών**[23]	**2021**		**2022**		**2023**		**Σύνολο**		
	Α	**Γ**	**Α**	**Γ**	**Α**	**Γ**	**Α**	**Γ**	**Α+Γ**
Προπτυχιακά Προγράμματα Σπουδών									
Metropolitan College B.Sc. Cyber Security & Networks	6	0	6	2	14	1	**26**	**3**	**29**
New York College B.Sc. Computing (Cybersecurity)			3	0	7	0	**10**	**0**	**10**
Epsilon College B.Sc. Web Development & Cyber Security					-	-	**0**	**0**	**0**
The American College of Greece B.Sc. Cybersecurity & Networks					3	0	**3**	**0**	**3**
Μεταπτυχιακά Προγράμματα Σπουδών									
BCA College M.Sc. Maritime Cybersecurity									
BCA College M.Sc. Applied Cyber Security									
Aegean College M.Sc. Cyber Security									
Metropolitan College M.Sc. Information Security & Digital Forensics	13	6	18	7	19	5	**50**	**18**	**68**
Σύνολο	**19**	**6**	**27**	**9**	**40**	**6**	**89**	**21**	**110**

3.3.2 ΕΛΛΑΔΑ - Κέντρα Δια Βίου Μάθησης

Στην Ελλάδα λειτουργούν **Κέντρα Δια Βίου Μάθησης (ΚΕΔΙΒΙΜ)**, κυρίως υπό την ευθύνη πανεπιστημιακών ιδρυμάτων. Παρέχουν ποικίλα προγράμματα επιμόρφωσης στην Κυβερνοασφάλεια και σε συναφή γνωστικά πεδία (βλ. Πίνακα 10). Τα χαρακτηριστικά των ΚΕΔΙΒΙΜ παρατίθενται στο **Παράρτημα IV**.

[23] Τα προγράμματα δεν προσφέρθηκαν κατά τα έτη που σημειώνονται με γραμμοσκίαση.

Πίνακας 10: ΕΛΛΑΔΑ - ΚΕΔΙΒΙΜ με προγράμματα επιμόρφωσης σε Κυβερνοασφάλεια (ανά διάρκεια)

ΚΕΔΙΒΙΜ - Αντικείμενο προγράμματος επιμόρφωσης	**Πανεπιστήμιο/Ιδιωτικός Φορέας**	**Διάρκεια** (ώρες)
Cisco Certified Network Associate v7 & CyberOps Associate [23] (https://kedivim.uom.gr/member/mavridis_ioannis/)	Πανεπιστήμιο Μακεδονίας	312
Ασφάλεια Δεδομένων – Κυβερνοασφάλεια [24]	Πανεπιστήμιο Πατρών	200
Cisco Certified CyberOps Associate – Κυβερνοασφάλεια [25] (https://learning.uth.gr/cybersecurity/)	Πανεπιστήμιο Θεσσαλίας	176
Ειδικός Πληροφορικής Προστασίας Δεδομένων - Κυβερνοασφάλεια [26] (https://kedivim.uowm.gr/course/eidikos-pliroforikis-se-themata-prostasias-dedomenon-gdpr-kyvernoasfaleia/)	Πανεπιστήμιο Δυτικής Μακεδονίας	80
Συστήματα Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια [27] (https://elearningekpa.gr/courses/sustimata-texnitis-noimosunis-stin-kubernoasfaleia)	Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών	60
Κυβερνοέγκλημα & Κυβερνοασφάλεια [29] (https://kedivim.auth.gr/programs/kyvernoeglima/)	Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	45

Ο Πίνακας 11 απεικονίζει το πλήθος των απόφοιτων των Προγραμμάτων Επιμόρφωσης των ΚΕΔΙΒΙΜ, ανά έτος (2021-23) και φύλο.

Πίνακας 11: ΕΛΛΑΔΑ - Απόφοιτοι Προγραμμάτων Επιμόρφωσης ΚΕΔΙΒΙΜ (ανά έτος & φύλο)

ΚΕΔΙΒΙΜ - Πρόγραμμα Επιμόρφωσης[24]	**2021**		**2022**		**2023**		**Σύνολο**		
	Α	**Γ**	**Α**	**Γ**	**Α**	**Γ**	**Α**	**Γ**	**Α+Γ**
Πανεπιστήμιο Πατρών Ασφάλεια Δεδομένων – Κυβερνοασφάλεια					35	20	**35**	**20**	**55**
Πανεπιστήμιο Μακεδονίας Cisco Certified Network Associate v7 & CyberOps Associate					8	0	**8**	**0**	**8**
Πανεπιστήμιο Θεσσαλίας Cisco Certified CyberOps Associate – Κυβερνοασφάλεια	10	2	14	2	5	2	**29**	**6**	**35**
Πανεπιστήμιο Δυτικής Μακεδονίας Ειδικός Πληροφορικής Προστασίας Δεδομένων – Κυβερνοασφάλεια	Δεν ανταποκρίθηκε						-	-	-
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης Κυβερνοέγκλημα & Κυβερνοασφάλεια	6	15	11	20	4	8	**21**	**43**	**64**
Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών - Συστήματα Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια							**0**	**0**	**0**
Σύνολο	**16**	**17**	**25**	**22**	**52**	**30**	**93**	**69**	**162**

[24] Τα προγράμματα δεν προσφέρθηκαν κατά τα έτη τα οποία σημειώνονται με γραμμοσκίαση.

3.4 ΕΛΛΑΔΑ - Επαγγελματικές Πιστοποιήσεις Κυβερνοασφάλειας

3.4.1 ISC2

Το **ISC² (International Information System Security Certification Consortium)** [30] ιδρύθηκε το 1989 και είναι ο μεγαλύτερος μη κερδοσκοπικός οργανισμός μελών πιστοποιημένων επαγγελματιών Ασφάλειας Πληροφοριακών Συστημάτων, παγκοσμίως (>110.000 μέλη σε >160 χώρες). Στην Ελλάδα, το Hellenic Chapter του ISC² (https://isc2-chapter.gr/) παρέχει στα μέλη του ένα forum που διευκολύνει την ανταλλαγή γνώσεων και ιδεών, την ανάπτυξη ηγετικών και επαγγελματικών δεξιοτήτων και την προώθηση της Ασφάλειας Πληροφοριακών Συστημάτων. Επίσης, παρέχει στα μέλη του πρόσβαση σε μια σειρά από βιομηχανικούς πόρους και εκπαιδευτικά προγράμματα, ώστε να ενημερώνονται για τις τελευταίες εξελίξεις στη γνωστική περιοχή.

Το Hellenic Chapter επικεντρώνεται στην ανταλλαγή γνώσεων και ιδεών μεταξύ των επαγγελματιών της Ασφάλειας Πληροφοριακών Συστημάτων στην Ελλάδα. Σκοπός του είναι να προωθήσει τον τομέα αυτόν, εκπαιδεύοντας τους επαγγελματίες, αλλά και το ευρύ κοινό, σχετικά με τον τρόπο προστασίας και άμυνας απέναντι σε κάθε απειλή κυβερνοασφάλειας.

3.4.2 ISACA

Ως παγκοσμίως αναγνωρισμένος ηγέτης στον τομέα Πληροφοριακά Συστήματα/Συστήματα Πληροφορικής (IS/IT), για περισσότερα από 50 χρόνια, ο **ISACA (Information Systems Audit and Control Association)** [31] είναι ένας επαγγελματικός οργανισμός μελών που σκοπό έχει την προώθηση της ψηφιακής εμπιστοσύνης, δίνοντας τη δυνατότητα στους επαγγελματίες IS/IT να αναπτύξουν δεξιότητες και γνώσεις στον έλεγχο, την ασφάλεια και τις αναδυόμενες τεχνολογίες. Το ISACA Athens Chapter ιδρύθηκε το 1994, ως σωματείο, από στελέχη του χώρου του Ελέγχου Συστημάτων Πληροφορικής, με την επωνυμία "**Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής**" (https://engage.isaca.org/athenschapter/home). Βασικός σκοπός του Ινστιτούτου είναι η προώθηση της εκπαίδευσης των μελών του για τη βελτίωση και ανάπτυξη των ικανοτήτων τους σχετικά με τον έλεγχο συστημάτων πληροφορικής ή με σχετιζόμενα.

Οι επιμέρους στόχοι του ISACA είναι: (α) η προώθηση της εκπαίδευσης και η προαγωγή της διάδοσης των γνώσεων και ικανοτήτων των μελών στην επιθεώρηση, ασφάλεια και έλεγχο συστημάτων πληροφορικής, (β) η προώθηση της ελεύθερης ανταλλαγής μεταξύ των μελών τεχνικών, μεθόδων και προσεγγίσεων για επίλυση προβλημάτων ελέγχου και ασφάλειας συστημάτων πληροφορικής, (γ) η προώθηση συνεχούς επιμόρφωσης των μελών, μέσω συνεχιζόμενης εκπαίδευσης (Continuing Professional Education, CPE) για τις τρέχουσες εξελίξεις στον έλεγχο και την ασφάλεια συστημάτων πληροφορικής, (δ) η μεταφορά στη Δημόσια Διοίκηση, στους ελεγκτές, στα πανεπιστήμια και σε επαγγελματίες συστημάτων πληροφορικής της σημασίας της καθιέρωσης του ελέγχου, ώστε να διασφαλίζεται η αποτελεσματική οργάνωση και αξιοποίηση των ΤΠΕ και (ε) ο προσδιορισμός, αποδοχή, προώθηση και υιοθέτηση προτύπων στα θέματα ελέγχου και ασφάλειας συστημάτων πληροφορικής.

3.4.3 Σύνολο επαγγελματικών πιστοποιήσεων

Οι ISC² και ISACA παρέχουν στα μέλη τους και σε ενδιαφερόμενους τη δυνατότητα να πιστοποιηθούν σε σειρά εξειδικεύσεων που έχουν σχέση με Κυβερνοασφάλεια και Ασφάλεια Πληροφοριών/Πληροφοριακών/Επικοινωνιακών Συστημάτων. Στον Πίνακα 12 παρουσιάζονται στατιστικά στοιχεία για τους πιστοποιημένους επαγγελματίες σε επιμέρους πεδία της Κυβερνοασφάλειας και της Ασφάλειας Πληροφοριών /Πληροφοριακών/Επικοινωνιακών Συστημάτων στην Ελλάδα (02/2024).

Πίνακας 12: ΕΛΛΑΔΑ - ISC2 & ISACA: Πιστοποιημένοι (ανά πιστοποίηση)

ΕΛΛΑΔΑ: Πιστοποιήσεις σε (Κυβερνο)Ασφάλεια (02/2024)			
ISC²	**Σύνολο**	**Α**	**Γ**
Certified in Cybersecurity (**CC**)	146	Δεν τηρούνται στοιχεία φύλου	
Certified Information Systems Security Professional (**CISSP**)	71		
Certified Cloud Security Professional (**CCSP**)	42		
Systems Security Certified Practitioner (**SSCP**)	13		
Governance, Risk and Compliance Certification (**CGRC**)	11		
Certified Secure Software Lifecycle Professional (**CSSLP**)	7		
Σύνολο ISC²	**290**		
ISACA	**Σύνολο**		
Certified Information Security Manager (**CISM**)	**190**		
Σύνολο ISACA	**190**		
Σύνολο πιστοποιήσεων	**480**		

3.5 ΕΛΛΑΔΑ – Προσφορά στελεχών σε Κυβερνοασφάλεια

Στο τυπικό εκπαιδευτικό σύστημα της Ελλάδας, εκπαίδευση στην Κυβερνοασφάλεια ή σε συναφείς γνωστικές περιοχές παρέχεται από **Προγράμματα Μεταπτυχιακών Σπουδών** (EQF 7) που παρέχουν Μεταπτυχιακά Διπλώματα Εξειδίκευσης (**M.Sc.**), καθώς και από **Προγράμματα Διδακτορικών Σπουδών** (EQF 8), που παρέχουν Διδακτορικά Διπλώματα (**Ph.D.**). Δεν παρέχεται τέτοια εξειδίκευση από **Προγράμματα Πτυχιακών Σπουδών** (EQF 6), συνεπώς δεν απονέμεται αντίστοιχος τίτλος σπουδών (**B.Sc.**).

Στην μη τυπική εκπαίδευση, τέτοιες εξειδικεύσεις παρέχονται από **Κολλέγια**, τόσο σε **προπτυχιακό** επίπεδο (**B.Sc.**), όσο και σε **μεταπτυχιακό** επίπεδο (**M.Sc.**). Επίσης, σχετικές βεβαιώσεις κατάρτισης παρέχουν τα **Κέντρα Δια Βίου Μάθησης** (ΚΕΔΙΒΙΜ) που λειτουργούν, κυρίως αλλά όχι αποκλειστικά, στο πλαίσιο Πανεπιστημίων.

Τέλος, σειρά σχετικών **επαγγελματικών πιστοποιήσεων**, με αξιόλογη αποδοχή από την εγχώρια Αγορά, αλλά όχι από τη ελληνική Δημόσια Διοίκηση, παρέχεται από συλλογικούς επαγγελματικούς φορείς/ενώσεις, με ευρεία διεθνή παρουσία (ISC2, ISACA).

Στον **Πίνακα 13** αναφέρονται τα συνολικά ποσοτικά στοιχεία του στελεχιακού δυναμικού της Ελλάδας που απέκτησε ακαδημαϊκές περγαμηνές και επαγγελματικές πιστοποιήσεις στην Κυβερνοασφάλεια (επίπεδα **EQF 4 έως 8** του Ευρωπαϊκού Πλαισίου Προσόντων), κατά την τριετία **2021-23.**

Πίνακας 13: ΕΛΛΑΔΑ – Κυβερνοασφάλεια: Νέο στελεχιακό δυναμικό (σύνολα, 2021-23)

ΕΛΛΑΔΑ	2021-23		
	Α	**Γ**	**Α+Γ**
ΤΥΠΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΣΥΣΤΗΜΑ			
ΠΑΝΕΠΙΣΤΗΜΙΑ	**456** (78%)	**128** (22%)	**584** (44%)
Προπτυχιακά Προγράμματα (**EQF 6**)	**0** (0%)	**0** (0%)	**0** (0%)
Μεταπτυχιακά Προγράμματα (**EQF 7**)	**432** (78%)	**121** (22%)	**553** (95%)
Διδακτορικά Διπλώματα (**EQF 8**)	**24** (77%)	**7** (23%)	**31** (5%)
ΜΗ ΤΥΠΙΚΗ ΕΚΠΑΙΔΕΥΣΗ & ΚΑΤΑΡΤΙΣΗ			
ΚΟΛΛΕΓΙΑ[25]	**89** (80%)	**21** (20%)	**110** (8%)
Προπτυχιακά Προγράμματα (**EQF 6**)	**39** (93%)	**3** (7%)	**42** (38%)
Μεταπτυχιακά Προγράμματα (**EQF 7**)	**50** (74%)	**18** (26%)	**68** (62%)
ΚΕΔΙΒΙΜ	**93** (57%)	**69** (43%)	**162** (12%)
ΣΥΝΟΛΟ (Εκπαίδευση, Κατάρτιση)	**638** (74%)	**218** (26%)	**856** (64%)
ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΠΙΣΤΟΠΟΙΗΣΕΙΣ	*Δεν τηρούνται στοιχεία φύλου*		**480** (36%)
ΣΥΝΟΛΟ (Εκπαίδευση, Κατάρτιση, Πιστοποίηση)			**1.336**

Στον **Πίνακα 14** παρατίθενται τα αντίστοιχα αναλυτικά ποσοτικά στοιχεία. Από τον πίνακα αυτόν προκύπτουν τα εξής βασικά συμπεράσματα:

1. Στα επίπεδα **EQF 4** και **EQF 5** στην Ελλάδα (Γυμνάσιο, Λύκειο, Επαγγελματικές Σχολές Κατάρτισης, Επαγγελματικές Σχολές Μαθητείας, Ινστιτούτα Επαγγελματικής Κατάρτισης) **δεν παρέχονται πιστοποιημένες γνώσεις** στην Κυβερνοασφάλεια ή σε συναφές γνωστικό πεδίο.
2. **Δεν υπάρχει Πανεπιστήμιο** στην Ελλάδα το οποίο παρέχει **βασικό τίτλο σπουδών** (επίπεδο: **EQF 6**, τίτλος: «Πτυχίο», **B.Sc**). Υπάρχουν, όμως, **Κολλέγια** (4) που παρείχαν τέτοιο τίτλο σπουδών (**42**, **B.Sc.**).
3. **Η πλειονότητα** (**553, 65%**) των εκπαιδευμένων/καταρτιζόμενων σε Κυβερνοασφάλεια στην Ελλάδα προέρχεται από **Προγράμματα Μεταπτυχιακών Σπουδών** (M.Sc.) Πανεπιστημίων (επίπεδο: **EQF 7**, τίτλος: «Μεταπτυχιακό Δίπλωμα Εξειδίκευσης», **M.Sc**.) (5 Πανεπιστήμια, 6 Προγράμματα).
4. Τα Κολλέγια στην Ελλάδα τα οποία παρέχουν εξειδίκευση, σε **πτυχιακό και μεταπτυχιακό** επίπεδο, σε Κυβερνοασφάλεια ή σε συναφές γνωστικό πεδίο είναι **αρκετά (14)** (6 Κολλέγια, 8 Προγράμματα), αλλά το πλήθος των αποφοίτων τους είναι **πολύ περιορισμένο** (**107, 13%**).
5. Τα **ΚΕΔΙΒΙΜ** που παρέχουν **κατάρτιση** σε Κυβερνοασφάλεια ή σε συναφή γνωστικά πεδία στην Ελλάδα είναι ολιγάριθμα (7), λειτουργούν κυρίως στο πλαίσιο Πανεπιστημιακών ιδρυμάτων, δεν διαθέτουν σαφή ένταξη στο EQF και έχουν καταρτίσει **περιορισμένο** αριθμό εκπαιδευόμενων (**162, 19%**).

[25] Στην Ελλάδα, οι απόφοιτοι των Κολλεγίων διαθέτουν πτυχίο που αναγνωρίζεται από το Κράτος ως ισότιμο των Πανεπιστημίων, αλλά δεν διαθέτουν αντίστοιχα επαγγελματικά δικαιώματα.

Πίνακας 14: ΕΛΛΑΔΑ – Κυβερνοασφάλεια: Νέο στελεχιακό δυναμικό (ανά έτος και προέλευση, 2021-23)

ΕΛΛΑΔΑ	2021			2022			2023			2021-23		
	Α	**Γ**	**Α+Γ**	**Α**	**Γ**	**Α+Γ**	**Α**	**Γ**	**Α+Γ**	**Α**	**Γ**	**Α+Γ**
ΤΥΠΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΣΥΣΤΗΜΑ												
ΠΑΝΕΠΙΣΤΗΜΙΑ	**157**	**41**	**198**	**143**	**43**	**186**	**156**	**44**	**200**	**456**	**128**	**584**
Προπτυχιακά Προγράμματα (**EQF 6**)	-	-	-	-	-	-	-	-	-	**0**	**0**	**0**
Μεταπτυχιακά Προγράμματα (**EQF 7**)	149	38	187	138	42	180	145	41	186	**432**	**121**	**553**
Διδακτορικά Διπλώματα (**EQF 8**)	8	3	11	5	1	6	11	3	14	**24**	**7**	**31**
ΜΗ ΤΥΠΙΚΗ ΕΚΠΑΙΔΕΥΣΗ & ΚΑΤΑΡΤΙΣΗ												
ΚΟΛΛΕΓΙΑ[26]	**19**	**6**	**25**	**27**	**9**	**36**	**43**	**6**	**49**	**89**	**21**	**110**
Προπτυχιακά Προγράμματα (**EQF 6**)	6	0	6	9	2	11	24	1	25	**39**	**3**	**42**
Μεταπτυχιακά Προγράμματα (**EQF 7**)	13	6	19	18	7	25	19	5	24	**50**	**18**	**68**
ΚΕΔΙΒΙΜ	**16**	**17**	**33**	**25**	**22**	**47**	**52**	**30**	**82**	**93**	**69**	**162**
ΣΥΝΟΛΟ (Εκπαίδευση, Κατάρτιση)	**173**	**58**	**231**	**171**	**65**	**236**	**218**	**74**	**292**	**638**	**218**	**856**
ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΠΙΣΤΟΠΟΙΗΣΕΙΣ	**ISC²**: 290 και **ISACA**: 190 (02/2024)									Δεν τηρούνται στοιχεία φύλου		**480**
ΣΥΝΟΛΟ (Εκπαίδευση, Κατάρτιση, Πιστοποίηση)												**1.336**

[26] Οι απόφοιτοι διαθέτουν πτυχίο (B.Sc.) ή μεταπτυχιακό (M.Sc.) τίτλο σπουδών, οι οποίοι αναγνωρίζονται από το Ελληνικό Κράτος ως αντίστοιχοι των Πανεπιστημίων, αλλά δεν παρέχονται στους κατόχους τους αντίστοιχα επαγγελματικά δικαιώματα.

6. Ορισμένες διεθνείς και αξιόπιστες **συλλογικότητες επαγγελματιών** (ISC2, ISACA) παρέχουν στην Ελλάδα, μετά από εξέταση, σχετικά **αξιόλογο** αριθμό **πιστοποιήσεων** (480) σε σειρά επιμέρους πεδίων της Κυβερνοασφάλειας και των συναφών της γνωστικών πεδίων.
7. Οι απόφοιτοι προγραμμάτων/σεμιναρίων σε Κυβερνοασφάλεια ή σε συναφή γνωστικά πεδία στην Ελλάδα είναι στη **μεγάλη πλειονότητά** τους **άνδρες, χωρίς να υπάρχει αξιοσημείωτη τάση εξισορρόπησης ή αντιστροφής** κατά την τριετία 2021-23.
8. Στην Ελλάδα, **η ποσόστωση σε βάρος των** γυναικών (**24-28%**) στην Κυβερνοασφάλεια ή σε συναφή γνωστικά πεδία, ισχύει ανεξαρτήτως προγραμμάτων ακαδημαϊκών σπουδών. Στα σεμινάρια των **ΚΕΔΙΒΙΜ** υπήρξε **συγκυριακά υψηλή** (**43%**), λόγω ενός σεμιναρίου κατάρτισης (ΚΕΔΙΒΙΜ) που είχε κυρίως **νομικό** χαρακτήρα. Κατά την τριετία **2021-23** παρατηρείται, εξελικτικά:

   (α) **σταθερός αριθμός απόφοιτων** Προγραμμάτων Μεταπτυχιακών Σπουδών ανά έτος (**205-210**),

   (β) **σημαντική μείωση γυναικών** απόφοιτων προγραμμάτων **ΚΕΔΙΒΙΜ** (από **51.5**% σε **36.5**%) (πιθανόν συγκυριακό εύρημα),

   (γ) **περιορισμένο ποσοστό** (**23%**) **διδακτόρων γυναικών**,

   (δ) **σταθερά περιορισμένο** ποσοστό **(21-24%) γυναικών** απόφοιτων Προγραμμάτων Μεταπτυχιακών Σπουδών και

   (ε) **ελάχιστο** ποσοστό **(7%) γυναικών** απόφοιτων Προγραμμάτων Προπτυχιακών Σπουδών.

ΚΕΦΑΛΑΙΟ 4 - Ζήτηση στελεχιακού δυναμικού στην Κυβερνοασφάλεια

4.1 ΕΛΛΑΔΑ – Εισαγωγή

Στον σημερινό ολοένα και πιο ψηφιακό κόσμο, η ζήτηση για επαγγελματίες της κυβερνοασφάλειας είναι μεγαλύτερη από ποτέ {στην Ελλάδα}. Οι απειλές στον κυβερνοχώρο πολλαπλασιάζονται ραγδαία με αποτέλεσμα οι οργανισμοί σε διάφορους τομείς να καταβάλλουν συνεχείς προσπάθειες για να ενισχύσουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας για την προστασία των δεδομένων και τη διατήρηση της ακεραιότητας των λειτουργιών τους.

Η EIT Digital και ο προμηθευτής της, Abodoo, συνεργάστηκαν για την ~~απόξεσης~~ αναζήτηση κενών θέσεων εργασίας στον τομέα της κυβερνοασφάλειας σε Βέλγιο, Εσθονία, Σλοβενία, Ουγγαρία, Ελλάδα, Λιθουανία και Ισπανία. Η διαδικασία αυτή περιλαμβάνει τη χρήση προηγμένων τεχνικών για τη συλλογή ολοκληρωμένων και ακριβών πληροφοριών σχετικά με τις διαθέσιμες θέσεις εργασίας στον τομέα της κυβερνοασφάλειας σε διάφορους κλάδους και περιοχές. Σκοπός ήταν η ανίχνευση των κενών θέσεων εργασίας και ο εντοπισμός τάσεων, προτύπων και κρίσιμων αναγκών της αγοράς αναφορικά με τις απαιτούμενες δεξιότητες και τους επαγγελματικούς ρόλους στον τομέα αυτό. Τα δεδομένα αυτά θα συμβάλλουν καθοριστικά στην ανάπτυξη στοχευμένων προγραμμάτων κατάρτισης και πρωτοβουλιών για την εξάλειψη του χάσματος δεξιοτήτων κυβερνοασφάλειας στην Ευρώπη.

Με βάση την ανάλυση των κενών θέσεων εργασίας που πραγματοποιήθηκε τον Ιούνιο του 2024, η έρευνα αναδεικνύει τους 5 πιο περιζήτητους ECSF τίτλους εργασίας στον τομέα της κυβερνοασφάλειας στην Ελλάδα, οι οποίοι απεικονίζονται στον παρακάτω πίνακα. Σύμφωνα με τα ευρήματα , οι εταιρείες στην Ελλάδα αναζητούν προσωπικό με δεξιότητες σε 3 βασικές κατηγορίες: Κυβερνοασφάλεια, κοινωνικές/μεταβατικές και οργανωτικές δεξιότητες.

Top 5 απαιτούμενοι ρόλοι κυβερνοασφάλειας (ECSF)	Top 5 απαιτούμενες δεξιότητες κυβερνοασφάλειας
Cybersecurity Implementer	Ανάλυση δεδομένων
Cyber incident Responder	Διαχείριση περιστατικών
Penetration Tester	Επικοινωνία
Cybersecurity Architect	Επίλυση προβλημάτων
Chief Information Security Officer (CISO)	Διαχείριση Έργου

4.2 ΕΛΛΑΔΑ – Δείγμα Έρευνας

Για την ανάπτυξη ειδικών εκθέσεων ανά χώρα σχετικά με τις ανάγκες σε δεξιότητες κυβερνοασφάλειας στο Βέλγιο, την Εσθονία, τη Σλοβενία, την Ουγγαρία, την Ελλάδα, τη Λιθουανία και την Ισπανία, τα CyberHubs εφάρμοσαν μια κοινή μεθοδολογία έρευνας. Αυτή η μεθοδολογία, που εκπονήθηκε από την Breyer Publico, χρησιμοποίησε μια προσέγγιση πολλαπλών μεθόδων που συνδυάζει ποσοτικές και ποιοτικές τεχνικές συλλογής δεδομένων. Η προσέγγιση περιλάμβανε έρευνες, σάρωση κενών θέσεων εργασίας [με τη χρήσητης πλατφόρμας Skills Academy Platform (SAP) του EIT Digital], έρευνα γραφείου και

ομάδες εστίασης εμπειρογνωμόνων. Η χαρτογράφηση των δεξιοτήτων και των ρόλων από τις κενές θέσεις εργασίας και τα προγράμματα εκπαίδευσης και κατάρτισης πραγματοποιήθηκε βάσειτου Ευρωπαϊκού Πλαισίου Δεξιοτήτων Κυβερνοασφάλειας (ECSF) του ENISA.

Χρησιμοποιήθηκε μια προσέγγιση πολλαπλών μεθόδων για τον προσδιορισμό τόσο των υφιστάμενων όσο και των αναδυόμενων αναγκών σε δεξιότητες για διάφορους επαγγελματικούςρόλους, με βάση υπάρχουσες πηγές και πρωτοβουλίες και με συλλογή πρωτογενών δεδομένων μέσω ερωτηματολογίων και ομάδων εμπειρογνωμόνων. Η έρευνα εξέτασε τόσο τις τρέχουσες όσο και τις μελλοντικές απαιτήσεις με τη χρήση ερωτηματολογίου που διανεμήθηκε σε οργανισμούς με ανάγκες σε δεξιότητες κυβερνοασφάλειας, ενώ η μελλοντική ζήτηση διερευνήθηκε περαιτέρω μέσω γνωμοδοτήσεων εμπειρογνωμόνων για την πρόβλεψη τάσεων και απαιτήσεων δεξιοτήτων.

Η έρευνα διεξήχθη σε διάστημα 3 εβδομάδων, από τις 15 Μαΐου έως τις 6 Ιουνίου 2024, με τη χρήση του EUSurvey, ένα εργαλείο για τη δημιουργία, διαχείριση και ανάλυση διαδικτυακών ερευνών και δημόσιων διαβουλεύσεων, και διανεμήθηκε μέσω: (α) του Συνδέσμου Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδος-ΣΕΠΕ (λίστα 40Κ, μέλη, τρεις επιτροπές του ΣΕΠΕ, επαφές του δημόσιου τομέα και κοινωνικά μέσα ενημέρωσης), (β) του Οικονομικού Πανεπιστημίου Αθηνών-ΟΠΑ, (γ) ομάδων εμπειρογνωμόνων, (δ) μελών του ISACA Athens Chapter, (ε) μελών του ISC2, και (στ) του Εθνικού Κέντρου Τεκμηρίωσης (άρθρο στον ιστότοπο, μέσα κοινωνικής δικτύωσης και ενημερωτικά δελτία με αποδέκτες 5Κ).

Η έρευνα συγκέντρωσε 139 απαντήσεις από οργανισμούς διαφόρων κατηγοριών και τομέων. Οι οργανισμοί αυτοί περιλάμβαναν παρόχους κυβερνοασφάλειας, εταιρείες ΤΠΕ, ιδιωτικούς και δημόσιους φορείς με εσωτερικές ανάγκες κυβερνοασφάλειας, ακαδημαϊκά ιδρύματα και άλλους. Τα συμπεράσματα της έρευνας τονίζουν τη δυναμική και εελισσόμενη φύση της ζήτησης εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας.

Οι περισσότερες απαντήσεις ελήφθησαν από ιδιωτικούς οργανισμούς (εκτός ΤΠΕ) με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας (20%) και από ακαδημαϊκούς φορείς (18%). Το 48% των ερωτηθέντων ανήκουν σε οργανισμούς, ιδιωτικούς ή δημόσιους, με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας. 16 ερωτηθέντες (12%) ανήκουν σε οργανισμούς χωρίς ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας.

	ΕΛΛΑΔΑ
Α.4. Σε ποια κατηγορία ανήκει ο φορέας σας;	
Επιχείρηση/πάροχος κυβερνοασφάλειας.	**21**
Επιχείρηση ΤΠΕ που χρειάζεται επαγγελματίες Κυβερνοασφάλειας ανάμεσα στα «εσωτερικά» στελέχη της.	**21**
Ιδιωτική επιχείρηση κλάδου πλην ΤΠΕ που χρειάζεται επαγγελματίες Κυβερνοασφάλειας	**28**
Δημόσιος οργανισμός που χρειάζεται επαγγελματίες Κυβερνοασφάλειας ανάμεσα στα «εσωτερικά» στελέχη του	**18**
Επιχείρηση που δεν χρειάζεται επαγγελματίες Κυβερνοασφάλειας	**16**
Πανεπιστημιακά ή Ερευνητικά Ιδρύματα	**25**
Άλλο.	**10**
Σύνολο	**139**

Πίνακας 15 (ερώτηση Α.4): Κατηγορία του οργανισμού

Στην επόμενη ερώτηση απάντησαν μόνο οι οργανισμοί ΤΠΕ με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας. Οι περισσότεροι ανέφεραν ότι ο τύπος της ψηφιακής υπηρεσίας του οργανισμού δεν κατατάσσεται στις διαθέσιμες επιλογές και δήλωσαν ότι παρέχουν προϊόντα και υπηρεσίες ΤΠΕ ή συμβουλευτικές υπηρεσίες (Πίνακας 16).

	ΕΛΛΑΔΑ
Α.4.1. Ποια είναι η κύρια ψηφιακή υπηρεσία που παρέχει ο φορέας σας;	
Διαδικτυακές αγορές	1
Επιγραμμική μηχανή αναζήτησης (online search engine)	0
Πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης	0
Άλλες ψηφιακές υπηρεσίες/δραστηριότητες ΤΠΕ	20
Καμία απάντηση	118
Σύνολο	**139**

Πίνακας 16 (ερώτηση Α.4.1): Τύπος ψηφιακής υπηρεσίας του οργανισμού

Οι 3 κορυφαίοι τομείς της NIS2, στους οποίους αντιστοιχεί το 45% των απαντήσεων, είναι η έρευνα και η ακαδημαϊκή κοινότητα, οι ψηφιακές υποδομές και η διαχείριση υπηρεσιών ΤΠΕ (B2B). Το 14% των ερωτηθέντων προέρχονταν από τομείς που δεν κατατάσσονται στους τομείς NIS2. Το 36% των ερωτηθέντων προέρχονταν από τομείς ΤΠΕ, συμπεριλαμβανομένων των ψηφιακών υποδομών, της διαχείρισης υπηρεσιών ΤΠΕ (business-to-business), του διαστήματος ή των ψηφιακών παρόχων. Οι τομείς της μεταποίησης, των ταχυδρομικών και ταχυμεταφορικών υπηρεσιών και του διαστήματος υποεκπροσωπούνταν σημαντικά (0%) στο δείγμα. Η κατηγορία «Άλλο» επιλέχθηκε από 10 στους 139 ερωτηθέντες (7%). Οι ομάδες εμπειρογνωμόνων σημείωσαν ότι, σε τοπικό επίπεδο, δεν ταιριάζουν όλοι οι τομείς με την ταξινομία της NIS2.

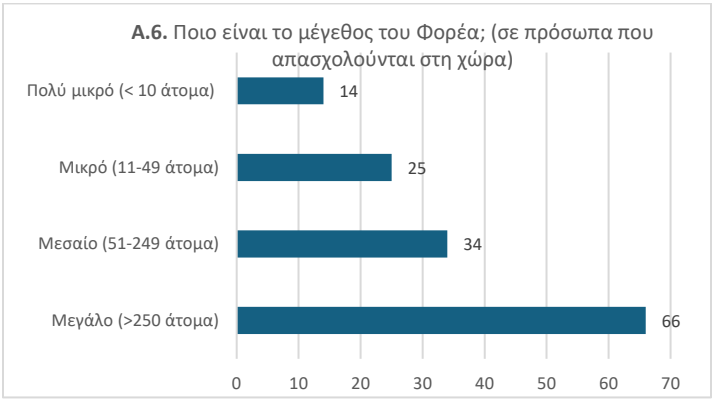
	ΕΛΛΑΔΑ	**Α.5:** Σε ποιον τομέα δραστηριοποιείται ο φορέας σας;	
Τομέας (ταξινόμηση NIS2)	**#**	**Τομέας** (ταξινόμηση NIS2)	**#**
1 Ενέργεια	8	**10** Υγρά απόβλητα	14
2 Υποδομές χρηματοπιστωτικών αγορών	13	**11** Ψηφιακές υποδομές	2
3 Υγεία	7	**12** Διαχείριση υπηρεσιών ΤΠΕ (B2B)	4
4 Μεταποίηση	19	**13** Διάστημα	17
5 Δημόσια διοίκηση	6	**14** Ταχυδρομικές και ταχυμεταφορικές υπηρεσίες	18
6 Μεταφορές	10	**15** Κατασκευή, παραγωγή & διανομή χημικών προϊόντων	15
7 Διαχείριση αποβλήτων	16	**16** Παραγωγή, μεταποίηση & διανομή τροφίμων	9
8 Τραπεζικές υπηρεσίες	11	**17** Ψηφιακοί πάροχοι	5
9 Πόσιμο νερό	12	**18** Έρευνα	1

		19 Άλλο	3

Πίνακας 17 (ερώτηση Α.5): Τομέας του φορέα

Όσον αφορά στο μέγεθος των οργανισμών, η πλειονότητα των ερωτηθέντων (47,5%) προέρχονταν από οργανισμούς με εργατικό δυναμικό άνω των 250 εργαζομένων (Πίνακας 18).

	ΕΛΛΑΔΑ
Α.6: Ποιο είναι το μέγεθος του Φορέα; (σε πρόσωπα που απασχολούνται στη χώρα)	
Μεγάλο (>250 άτομα)	66
Μεσαίο (51-249 άτομα)	34
Μικρό (11-49 άτομα)	25
Πολύ μικρό (< 10 άτομα)	14
Total	**139**



Πίνακας 18 (ερώτηση Α.6): Μέγεθος του οργανισμού

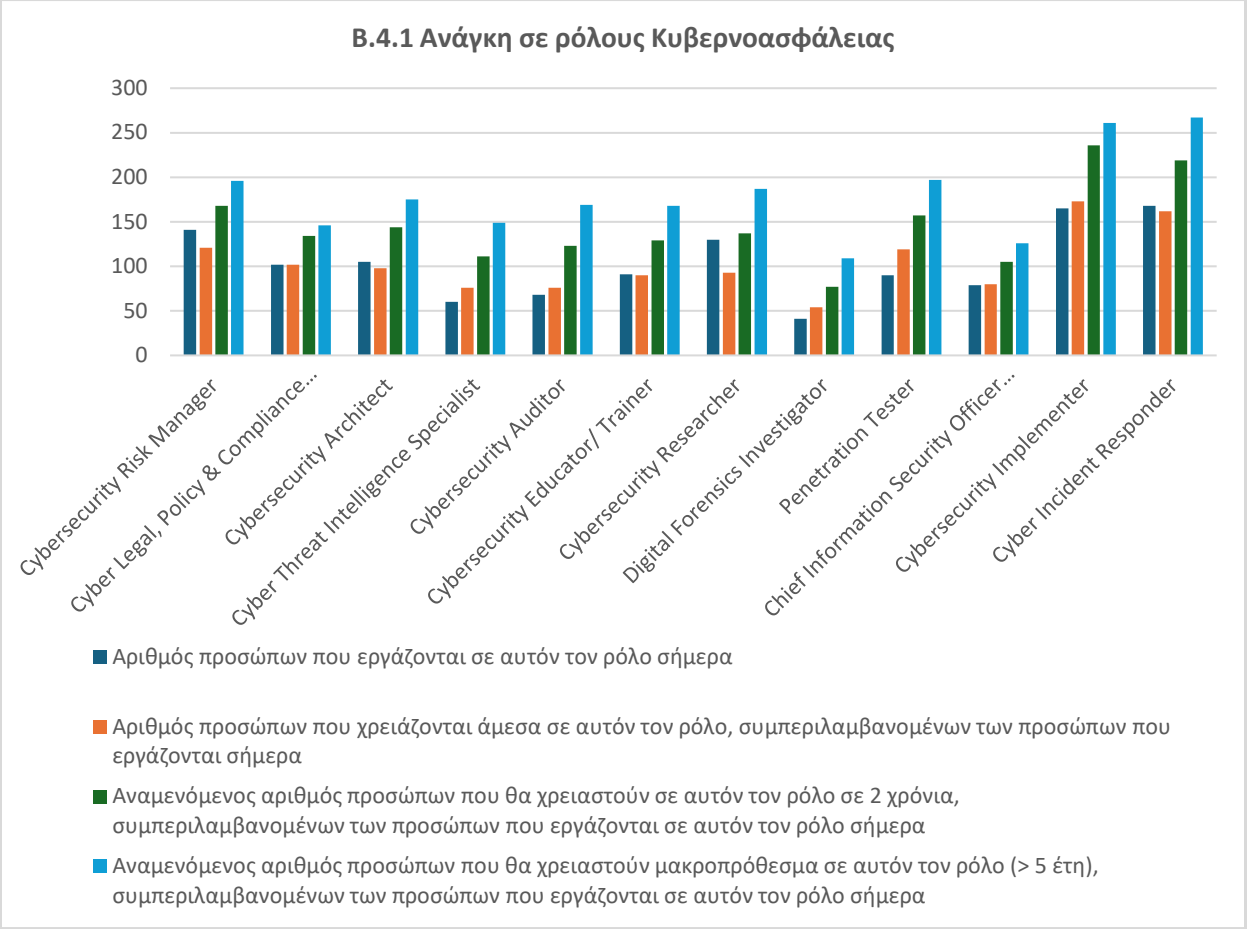
4.3 ΕΛΛΑΔΑ – Αποτελέσματα Έρευνας

Ρόλοι κυβερνοασφάλειας

Η ζήτηση για συγκεκριμένους ρόλους κυβερνοασφάλειας, σύμφωνα με το πλαίσιο ENISA, εμφανίζεται στον πίνακα 19. Οι γραμμές του πίνακα αντιπροσωπεύουν τους ρόλους ενώοι στήλες τους εργαζόμενους για τέσσερις περιπτώσεις (εργάζονται τώρα, χρειάζονται τώρα, χρειάζονται σε 2 χρόνια, χρειάζονται μετά από 5 χρόνια).

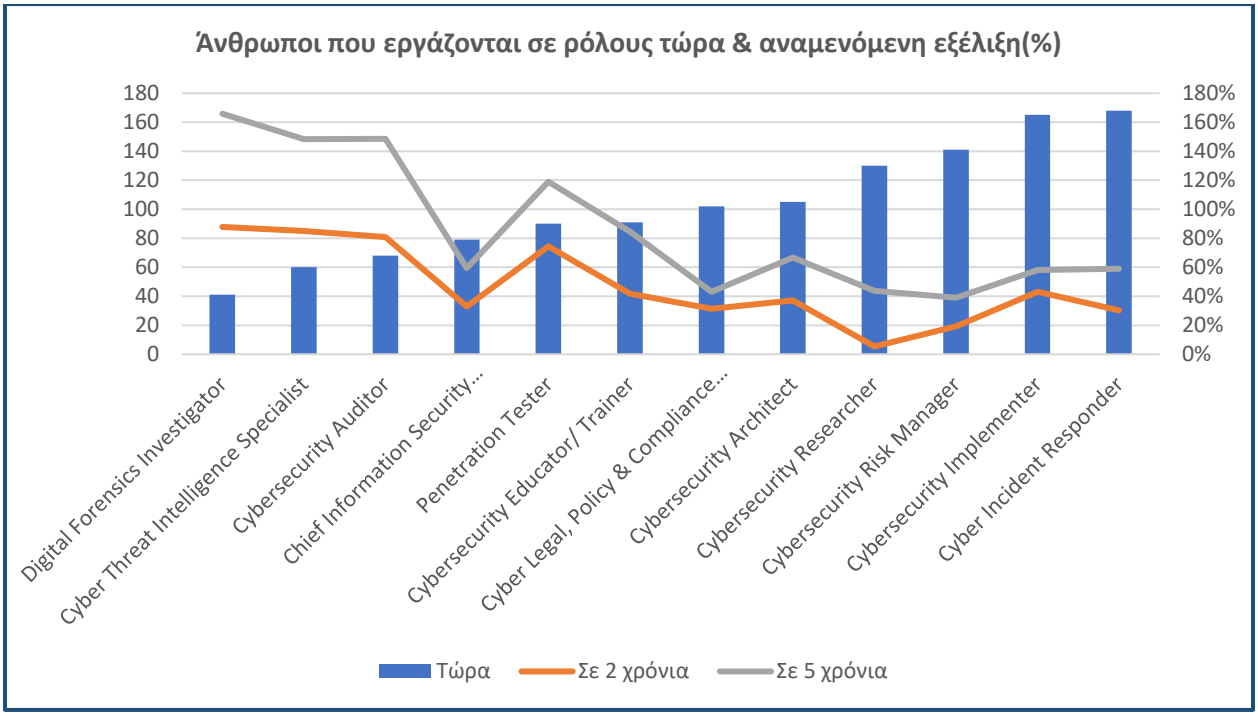
	ΕΛΛΑΔΑ	**Β.4.1**: Ανάγκες για ρόλους κυβερνοασφάλειας [27]			
Ρόλοι κυβερνοασφάλειας		Αριθμός προσώπων που εργάζονται σε αυτόν τον ρόλο σήμερα	Αριθμός προσώπων που χρειάζονται άμεσα σε αυτόν τον ρόλο, συμπεριλαμβανομένων των προσώπων που εργάζονται σήμερα	Αναμενόμενος αριθμός προσώπων που θα χρειαστούν σε αυτόν τον ρόλο σε 2 χρόνια, συμπεριλαμβανομένων των προσώπων που εργάζονται σε αυτόν τον ρόλο σήμερα	Αναμενόμενος αριθμός προσώπων που θα χρειαστούν μακροπρόθεσμα σε αυτόν τον ρόλο (> 5 έτη), συμπεριλαμβανομένων των προσώπων που εργάζονται σε αυτόν τον ρόλο σήμερα
Cybersecurity Risk Manager		141	121	168	196
Cyber Legal, Policy & Compliance Officer		102	102	134	146
Cybersecurity Architect		105	98	144	175
Cyber Threat Intelligence Specialist		60	76	111	149
Cybersecurity Auditor		68	76	123	169
Cybersecurity Educator/ Trainer		91	90	129	168
Cybersecurity Researcher		130	93	137	187
Digital Forensics Investigator		41	54	77	109
Penetration Tester		90	119	157	197
Chief Information Security Officer (CISO)		79	80	105	126
Cybersecurity Implementer		165	173	236	261
Cyber Incident Responder		168	162	219	267

[27] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



Οι κορυφαίοι ρόλοι κυβερνοασφάλειας, σύμφωνα με το πλαίσιο ENISA και τις τρέχουσες ανάγκες των οργανισμών, όπως προσδιορίστηκαν από τους ερωτηθέντες, εμφανίζονται στον πίνακα 20.

ΕΛΛΑΔΑ - Άνθρωποι που εργάζονται σήμερα σε ρόλους κυβερνοασφάλειας του ENISA (ECSF)		
Λιγότεροι από ό,τι χρειάζεται	**Όσοι χρειάζονται**	**Περισσότεροι από όσο χρειάζεται**
Penetration Tester	Cybersecurity Educator/Trainer	Cybersecurity Researcher
Cyber Threat Intelligence Specialist	Cyber Legal, Policy & Compliance Officer	Cybersecurity Risk Manager
Digital Forensics Investigator	Chief Information Security Officer (CISO)	Cybersecurity Architect
Cybersecurity Implementer		Cyber Incident Responder
Cybersecurity Auditor		



ΠΙΝΑΚΑ20: ΕΛΛΑΔΑ - Άτομα που εργάζονται σήμερα σε Ρόλους Κυβερνοασφάλειας στην ENISA (ECSF)

Σήμερα, οι περισσότεροι άνθρωποι εργάζονται ως Cyber Incident Responders και η τάση αυτή αναμένεται να συνεχιστεί τα επόμενα 5 χρόνια (Πίνακας 19). Στο εγγύς μέλλον (2-5 χρόνια), η μεγαλύτερη ανάγκη θα είναι για τους Cyber Incident Responders και τους Cyber Security Implementers. Επιπλέον, οι ρόλοι που αναμένεται να παρουσιάσουν τη μεγαλύτερη αύξηση των εμπειρογνωμόνων στον τομέα της κυβερνοασφάλειας είναι οι εξής: Digital Fo-rensics Investigator, Cybersecurity Auditor και Cyber Threat Intelligence Specialist.

Κατά τις συζητήσεις των ομάδων εμπειρογνωμόνων, ο ρόλος του Cyber Legal, Policy & Compliance Officer θεωρήθηκε ισοδύναμος/ομοειδής με αυτόν του Data Protection Officer (DPO), σύμφωνα με το Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (ECSF) του ENISA. Ωστόσο, παραδόξως, αρκετοί από τους ερωτηθέντες ανέφεραν ότι κανένας υπεύθυνος για την ασφάλεια στον κυβερνοχώρο, τη νομική πολιτική και τη συμμόρφωση δεν εργάζεται επί του παρόντος σε αυτόν τον ρόλο ή ότι δεν υπάρχει ανάγκη για τέτοιους υπευθύνους επί του παρόντος.

Κατηγορία φορέα	**No Cyber Legal, Policy & Compliance Officers** are working in this role now	**No Cyber Legal Policy & Compliance Officers** are needed in this role now
Επιχείρηση/Πάροχος υπηρεσιών Κυβερνοασφάλειας	0	0
Επιχείρηση ΤΠΕ που χρειάζεται επαγγελματίες Κυβερνοασφάλειας ανάμεσα στα «εσωτερικά» στελέχη της	2	1
Ιδιωτική επιχείρηση κλάδου πλην ΤΠΕ που χρειάζεται επαγγελματίες Κυβερνοασφάλειας	6	4

Δημόσιος οργανισμός που χρειάζεται επαγγελματίες Κυβερνοασφάλειας ανάμεσα στα «εσωτερικά» στελέχη του	6	2
Επιχείρηση που δεν χρειάζεται επαγγελματίες Κυβερνοασφάλειας	2	2
Πανεπιστημιακά ή Ερευνητικά Ιδρύματα	4	0
Άλλα	1	0
TOTAL	**21**	**9**

ΕΛΛΑΔΑ	Εργασία σε ρόλους κυβερνοασφάλειας σε σχέση με το μέγεθος του φορέα[28]							
Μέγεθος φορέα (αρ. προσωπικού)	Μεγάλο (>250)		Μεσαίο (51-249)		Μικρό (11-49)		Πολύ μικρό (< 10)	
Ρόλος	**Now working**	**Working in 5y**	**Now working**	**Working in 5y**	**Now working**	**Working in 5y**	**Now working**	**Working in 5y**
Cybersecurity Risk Manager	107	126	18	35	11	27	5	8
Cyber Legal, Policy & Compliance Officer	57	61	24	54	17	23	4	8
Cybersecurity Architect	79	105	17	35	7	31	2	4
Cyber Threat Intelligence Specialist	46	90	6	27	6	24	2	8
Cybersecurity Auditor	37	81	15	50	11	30	5	8
Cybersecurity Educator/ Trainer	59	96	16	36	13	27	3	9
Cybersecurity Researcher	111	136	6	20	11	27	2	4
Digital Forensics Investigator	32	63	5	20	2	20	2	6
Penetration Tester	72	126	8	33	6	25	4	13
Chief Information Security Officer (CISO)	55	79	13	24	8	19	3	4
Cybersecurity Implementer	124	176	28	48	9	29	4	8
Cyber Incident Responder	129	188	27	51	7	21	5	7

Πίνακας 21: ΕΛΛΑΔΑ - Άτομα που εργάζονται σε ρόλους Κυβερνοασφάλειας στην ENISA σε σχέση με το μέγεθος οργανισμού

Παρόλο που στον πίνακα 19 συμπεράναμε ότι οι περισσότεροι άνθρωποι εργάζονται ως ανταποκριτές περιστατικών στον κυβερνοχώρο και ότι σε 5 χρόνια η μεγαλύτερη ανάγκη θα είναι για ανταποκριτές περιστατικών στον κυβερνοχώρο και υλοποιητές κυβερνοασφάλειας, αυτό ισχύει μόνο για μεγάλους και μεσαίους οργανισμούς.

Σε οργανισμούς μικρού μεγέθους οι περισσότεροι άνθρωποι εργάζονται ως Cyber Legal, Policy & Compliance Officer και σε 5 χρόνια η μεγαλύτερη ανάγκη θα είναι για Αρχιτέκτονες και Ελεγκτές. Όσον αφορά

[28] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές

στην αύξηση, οι οργανισμοί μικρού μεγέθους θα αντιμετωπίσουν τη μεγαλύτερη αύξηση προσωπικού (252% κατά μέσο όρο), ενώ οι μεγάλοι τη μικρότερη (55% κατά μέσο όρο).

Σε 5 χρόνια, στους μικρούς οργανισμούς η ανάγκη για ερευνητές ψηφιακής εγκληματολογίας αυξάνεται κατά 900%. Στους οργανισμούς πολύ μικρού μεγέθους, η μεγαλύτερη αύξηση (300%) αφορά στους Cyber Threat Intelligence Specialist. Στους μεσαίους οργανισμούς η μεγαλύτερη αύξηση (350%) είναι για τον Cyber Threat Intelligence Specialist και για τους Auditors (119%) στους μεγάλους οργανισμούς.

Στον πίνακα 22, απεικονίζεται η ανάγκη για ρόλους κυβερνοασφάλειας του ENISA στους 3 κορυφαίους τομείς της NIS2.

- Στον τομέα της Έρευνας και της Ακαδημαϊκής κοινότητας, η μεγαλύτερη ανάγκη είναι για Ερευνητές Κυβερνοασφάλειας, ενώ η μεγαλύτερη αύξηση είναι για Ελεγκτές (600%).

- Στον τομέα των ψηφιακών υποδομών, η μεγαλύτερη ανάγκη είναι για Υλοποιητές Κυβερνοασφάλειας, ενώ η μεγαλύτερη αύξηση είναι για Ελεγκτές Διείσδυσης (68%).

- Στον τομέα της Διαχείρισης Υπηρεσιών ΤΠΕ, η μεγαλύτερη ανάγκη είναι για Cyber Incident Responders και Cybersecurity Implementers, ενώ η μεγαλύτερη αύξηση είναι για Cybersecurity Researchers (220%).

Αξίζει να σημειωθεί ότι στον τομέα της διαχείρισης υπηρεσιών ΤΠΕ παρατηρείται αύξηση σε όλους τους ρόλους του ENISA, κάτι που δεν συμβαίνει στον τομέα των ψηφιακών υποδομών. Αξίζει να σημειωθεί ότι στον τομέα της Διαχείρισης Υπηρεσιών ΤΠΕ παρατηρείται αύξηση σε όλους τους ρόλους του ENISA, κάτι που δεν συμβαίνει στον τομέα των Ψηφιακών Υποδομών.

 **ΕΛΛΑΔΑ**	Εργασία σε ρόλους κυβερνοασφάλειας σε σχέση με τον τομέα του φορέα[29]					
Τομείς φορέων / **Ρόλοι**	**Έρευνα**		**Ψηφιακές υποδομές**		**Διαχείριση υπηρεσιών ΤΠΕ**	
	Now working	Working in 5y	Now working	Working in 5y	Now working	Working in 5y
Cybersecurity Risk Manager	30	25	22	31	47	55
Cyber Legal, Policy & Compliance Officer	19	27	23	20	32	41
Cybersecurity Architect	9	20	43	33	42	54
Cyber Threat Intelligence Specialist	14	22	16	12	30	63
Cybersecurity Auditor	4	28	17	24	28	58
Cybersecurity Educator/ Trainer	29	47	12	16	21	43
Cybersecurity Researcher	102	116	38	16	10	32
Digital Forensics Investigator	16	19	19	21	23	33
Penetration Tester	12	43	22	37	45	94
Chief Information Security Officer (CISO)	13	23	12	14	26	46
Cybersecurity Implementer	36	45	62	46	74	102

[29] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές

Cyber Incident Responder	24	27	37	32	81	101

Table 22: GREECE - Άτομα που εργάζονται σε ρόλους κυβερνοασφάλειας του ENISA στους 3 σημαντικότερους τομείς της NIS2

Όσον αφορά τυχόν πρόσθετο ρόλο στην κυβερνοασφάλεια, οι περισσότεροι (91,66%) ερωτηθέντες θεώρησαν ότι δεν υπάρχει ανάγκη να περιγραφεί ένας πρόσθετος ρόλος στον οργανισμό τους εκτός από τα 12 προφίλ που προτείνει το ECSF του ENISA. Από την άλλη πλευρά, ορισμένοι ερωτηθέντες πρότειναν πρόσθετους ρόλους.

	Ε Λ Λ Α Δ Α
B.5: Υπάρχει κάποιος άλλος ρόλος στον Φορέα σας, ο οποίος απαιτεί μεν δεξιότητες Κυβερνοασφάλειας αλλά δεν μπορεί να ενταχθεί σε κάποιον από τους 12 παραπάνω ρόλους;	
Ναι	11
Όχι	121
Total	**132**

Επιπλέον Ρόλοι	Προτάσεις
IT Manager/Head	4
Cyber Security Liaison	1
AI Security Specialist	1
Product Manager	1
System Engineer	1
I&CT Security Officer	1

Table 23 (Question B.5): Other roles requiring cybersecurity skills

Οι ερωτηθέντες εξέτασαν επίσης πρόσθετα σχόλια σχετικά με τους ρόλους κυβερνοασφάλειας και τη ζήτησή τους σε έναν οργανισμό. Συγκεκριμένα, υπάρχει ανάγκη στην αγορά για α) Identity & Access Administrators και β) Cloud Security Administrators.

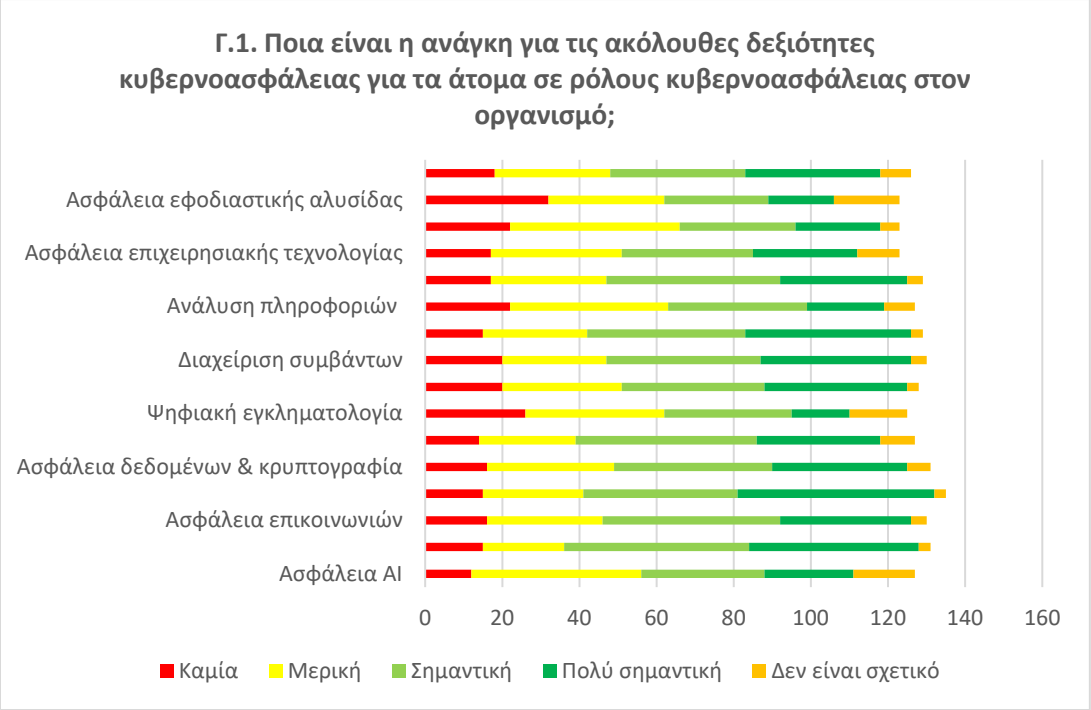
Επίσης, υπάρχει αυξανόμενη ζήτηση για δεξιότητες πληροφορικής γενικά, με έμφαση σε (α) τεχνικούς και μηχανικούς δικτύων, (β) ανάπτυξη/διαχείριση εφαρμογών και (γ) ανάπτυξη/διαχείριση υπηρεσιών δικτύου.

Cybersecurity skills

ΕΛΛΑΔΑ	**Γ.1**: Υπάρχει ανάγκη στο Φορέα για πρόσωπα με τις ακόλουθες **δεξιότητες Κυβερνοασφάλειας**; [30]				
Δεξιότητες κυβερνοασφάλειας	**Καμία**	**Μικρή**	**Σημαντική**	**Μεγάλη**	**Μη εφαρμόσιμο**
Ασφάλεια στην Τεχνητή Νοημοσύνη (AI Security)	12	44	32	23	16
Ασφάλεια Υπολογιστικού Νέφους (Cloud Security)	15	21	48	44	3
Ασφάλεια Επικοινωνιών (Communications Security*)*	16	30	46	34	4
Προστασία Δεδομένων (Data Privacy)	15	26	40	51	3
Κρυπτογράφηση και ασφάλεια δεδομένων (Data Security & Cryptography)	16	33	41	35	6
Συνδυασμός Πρακτικών Ανάπτυξης Ασφάλειας και Λειτουργιών (DevSecOps)	14	25	47	32	9
Ψηφιακά Πειστήρια (Digital Forensics)	26	36	33	15	15
Έλεγχος Πρόσβασης/Διαχείριση Ταυτότητας (Access Controls/ Identity Management)	20	31	37	37	3
Διαχείριση περιστατικών (Incident Management)	20	27	40	39	4
Information Systems & Network Security/ Cyber Resiliency *(Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων/ Ανθεκτικότητα στον Κυβερνοχώρο)*	15	27	41	43	3
Intelligence Analysis *(Ανάλυση Πληροφοριών)*	22	41	36	20	8
Ασφάλεια Λειτουργικών Συστημάτων (Operating Systems (OS) Security)	17	30	45	33	4
Ασφάλεια Επιχειρησιακής τεχνολογίας (Operational Technology Security)	17	34	34	27	11
Ασφάλεια Φυσικών Συσκευών (Physical Device Security)	22	44	30	22	5
Ασφάλεια Εφοδιαστικής Αλυσίδας (Supply Chain Security)	32	30	27	17	17
Ανάλυση απειλών (Threat Analysis)	18	30	35	35	8

Πίνακας 23 (ερώτηση Γ.1): Ανάγκη για δεξιότητες κυβερνοασφάλειας στον φορέα

[30] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



Οι κορυφαίες δεξιότητες κυβερνοασφάλειας που απαιτούνται τώρα, σύμφωνα με τους ερωτηθέντες, εμφανίζονται στον πίνακα 25.

ΕΛΛΑΔΑ – Οι δεξιότητες σε IT security που απαιτούνται στον οργανισμό (από πάνω προς τα κάτω)		
Καμία ανάγκη	**Σημαντική ανάγκη**	**Μεγάλη ανάγκη**
Ασφάλεια Εφοδιαστικής Αλυσίδας	Ασφάλεια Υπολογιστικού Νέφους	Προστασία Δεδομένων
	Συνδυασμός Πρακτικών Ανάπτυξης Ασφάλειας και Λειτουργιών	Information Systems & Network Security / Cyber Resiliency
Μικρή ανάγκη	Ασφάλεια Επικοινωνιών	Έλεγχος Πρόσβασης/Διαχείριση Ταυτότητας
Ασφάλεια στην Τεχνητή Νοημοσύνη	Ασφάλεια Λειτουργικών Συστημάτων	Ανάλυση απειλών
Ασφάλεια Φυσικών Συσκευών	Κρυπτογράφηση και ασφάλεια δεδομένων	
Intelligence Analysis	Διαχείριση περιστατικών	
Ψηφιακά Πειστήρια	Έλεγχος Πρόσβασης/ Διαχείριση Ταυτότητας	
Ασφάλεια Επιχειρησιακής τεχνολογίας	Ανάλυση απειλών	
	Ασφάλεια Λειτουργικών Συστημάτων	

Πίνακας 25: ΕΛΛΑΔΑ - Οι δεξιότητες σε IT security που απαιτούνται στον οργανισμό (από πάνω προς τα κάτω)

Το γεγονός ότι αρκετοί ερωτηθέντες δήλωσαν ότι δεν υπάρχει ανάγκη για δεξιότητες ασφάλειας της εφοδιαστικής αλυσίδας συζητήθηκε στις συνεδριάσεις της ομάδας εμπειρογνωμόνων. Οι επιτροπές κατέληξαν στο συμπέρασμα ότι η αντίληψη αυτή πιθανόν να οφείλεται στην πρακτική της ανάθεσης των προμηθειών σε εξωτερικούς συνεργάτες, η οποία αναθέτει την ευθύνη για την ασφάλεια της αλυσίδας εφοδιασμού στον προμηθευτή.

Οι ομάδες εμπειρογνωμόνων συζήτησαν επίσης την περιορισμένη ανάγκη που εξέφρασαν οι ερωτηθέντες για δεξιότητες ασφάλειας και ανάλυσης της ΤΝ. Το απέδωσαν στο γεγονός ότι οι περισσότεροι τοπικοί οργανισμοί αγοράζουν προϊόντα και λύσεις που έχουν αναπτυχθεί σε άλλες χώρες. Επιπλέον, οι ομάδες εμπειρογνωμόνων σημείωσαν ότι, ενώ η τεχνητή νοημοσύνη μπορεί να αποτελέσει ένα ιδιαίτερα επωφελές εργαλείο στην ασφάλεια στον κυβερνοχώρο, οι περισσότεροι τοπικοί οργανισμοί δεν έχουν ακόμη αναγνωρίσει πλήρως την επαρκή ωριμότητα αυτής της νέας τεχνολογίας.

Οι ομάδες εμπειρογνωμόνων δήλωσαν ότι είναι επιτακτική ανάγκη η θωράκιση των κρίσιμων υποδομών για την άμεση και αποτελεσματική αντιμετώπιση των παραβιάσεων ασφαλείας. Σημειώθηκε επίσης ότι η δεξιότητα της προστασίας των προσωπικών δεδομένων συγκεντρώνει πολύ υψηλή βαθμολογία λόγω των απαιτήσεων του ΓΚΠΔ.

	ΕΛΛΑΔΑ
Γ.2: Υπάρχουν **άλλες δεξιότητες Κυβερνοασφάλειας**, οι οποίες απαιτούνται ή αξιοποιούνται ήδη στον Φορέα σας και δεν περιλαμβάνονται στον παραπάνω κατάλογο;	
Ναι	6
Όχι	124
Σύνολο	**130**

Πίνακας 26 (ερώτηση Γ.2): Πρόσθετες δεξιότητες κυβερνοασφάλειας

	ΕΛΛΑΔΑ
Γ.2.1: Ποιες είναι ά**λλες δεξιότητες Κυβερνοασφάλειας** για τα πρόσωπα με ρόλους στην Κυβερνοασφάλεια;	
Ανάλυση κακόβουλου λογισμικού	1
Σχεδιασμός ασφαλούς διαδικασίας	1
Αναλυτές SOC	1
Έλεγχος ασφάλειας πληροφορικής ή πληροφοριών	1
Total	**4**

Πίνακας 27 (ερώτηση Γ.2.1): Πρόσθετες δεξιότητες κυβερνοασφάλειας για άτομα σε ρόλους κυβερνοασφάλειας

Δεξιότητες σχετικές με την πληροφορική

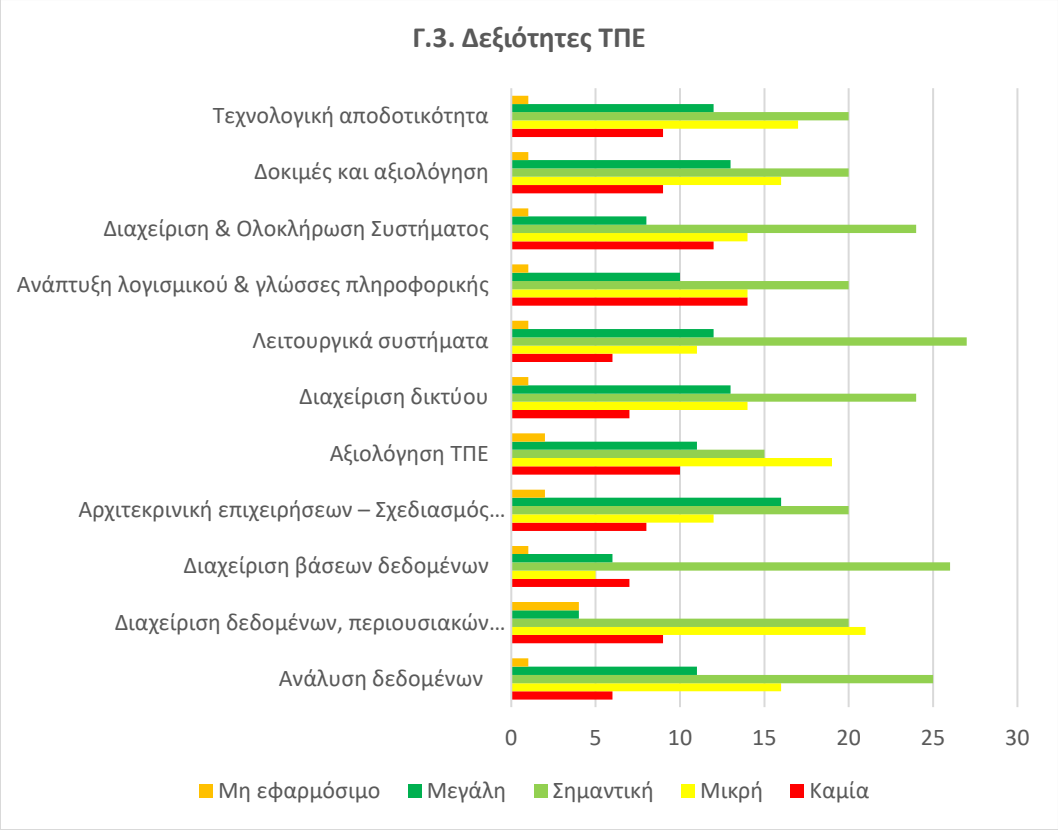
Όσον αφορά στην ανάγκη για δεξιότητες που σχετίζονται με την ΤΠ στους οργανισμούς, οι ερωτηθέντες εντόπισαν σημαντική ανάγκη για τις περισσότερες δεξιότητες κυβερνοασφάλειας, συμπεριλαμβανομένων της ανάλυσης δεδομένων, της διαχείρισης βάσεων δεδομένων, της αρχιτεκτονικής επιχειρήσεων και του σχεδιασμού υποδομών, της διαχείρισης δικτύων, των λειτουργικών συστημάτων, της ανάπτυξης λογισμικού και των γλωσσών υπολογιστών, της διαχείρισης και ολοκλήρωσης συστημάτων, της δοκιμής και αξιολόγησης και της τεχνολογικής ευχέρειας (Πίνακας 28). Αντίθετα, υπάρχει μόνο κάποια ανάγκη για δεξιότητες στη διαχείριση δεδομένων, περιουσιακών στοιχείων και αποθεμάτων, καθώς και στην αξιολόγηση της πληροφορικής.

Οι 3 πιο αναγκαίες δεξιότητες που σχετίζονται με την πληροφορική είναι: (α) διαχείριση βάσεων δεδομένων, (β) λειτουργικά συστήματα και (γ) επιχειρησιακή αρχιτεκτονική και σχεδιασμός υποδομών. Οι 3 λιγότερο αναγκαίες (ή καθόλου αναγκαίες) δεξιότητες που σχετίζονται με την ΤΠ είναι: (α) Διαχείριση δεδομένων, περιουσιακών στοιχείων και αποθεμάτων, (β) Αξιολόγηση ΤΠ και (γ) Ανάπτυξη λογισμικού και γλώσσες υπολογιστών.

	ΕΛΛΑΔΑ	**Γ.3:** Υπάρχει ανάγκη στον Φορέα τα πρόσωπα με ρόλους Κυβερνοασφάλειας να πρέπει να διαθέτουν και κάποιες από τις παρακάτω **δεξιότητες ΤΠΕ**;[31]			
Δεξιότητες ΤΠΕ		**Καμία**	**Μικρή**	**Σημαντική**	**Μεγάλη**	**Μη εφαρμόσιμο**
Ανάλυση δεδομένων		6	16	25	11	1
Διαχείριση δεδομένων, περιουσιακών στοιχείων και απογραφών		9	21	20	4	4
Διαχείριση βάσεων δεδομένων		7	5	26	6	1
Αρχιτεκρινική επιχειρήσεων – Σχεδιασμός Υποδομής		8	12	20	16	2
Αξιολόγηση ΤΠΕ		10	19	15	11	2
Διαχείριση δικτύου		7	14	24	13	1
Λειτουργικά συστήματα		6	11	27	12	1
Ανάπτυξη λογισμικού & γλώσσες πληροφορικής		14	14	20	10	1
Διαχείριση & Ολοκλήρωση Συστήματος		12	14	24	8	1
Δοκιμές και αξιολόγηση		9	16	20	13	1
Τεχνολογική αποδοτικότητα		9	17	20	12	1

Πίνακας 28 (ερώτηση Γ.3): Ανάγκη για δεξιότητες σχετικές με την πληροφορική στον οργανισμό

[31] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



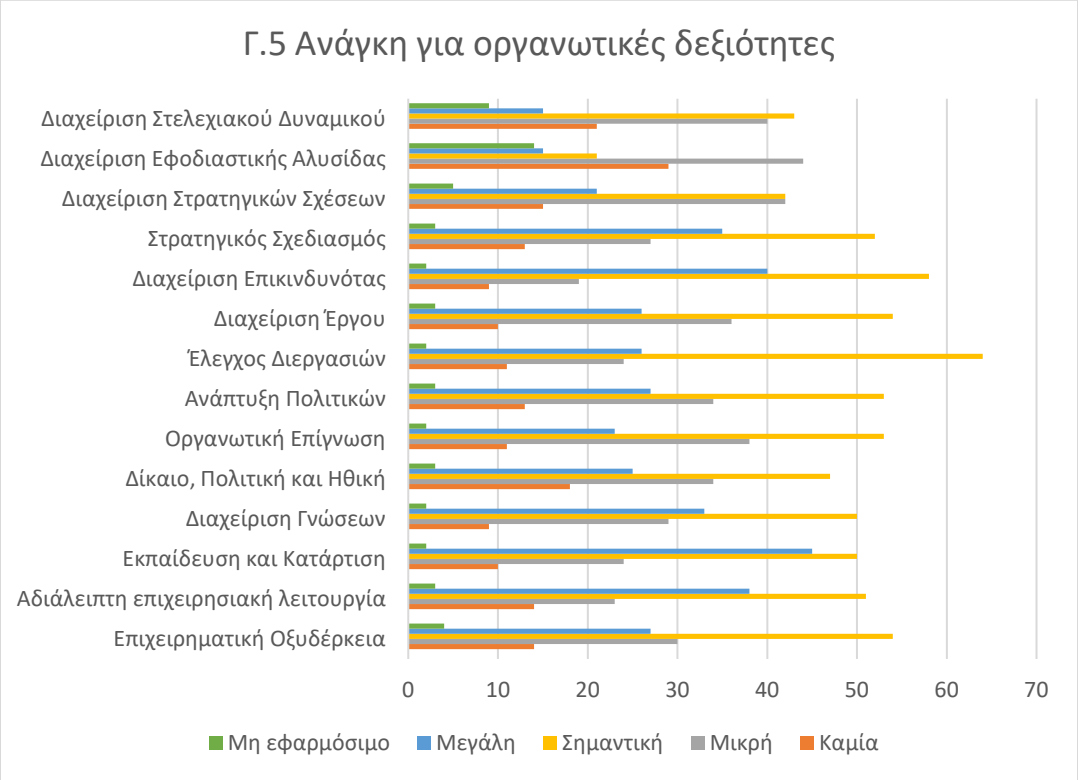
Οργανωτικές δεξιότητες

Οι 4 κορυφαίες οργανωτικές δεξιότητες που προτείνονται από τους ερωτηθέντες ως ουσιαστική ανάγκη στον οργανισμό τους είναι: (α) έλεγχος διαδικασιών, (β) διαχείριση κινδύνων, (γ) διαχείριση έργων και (δ) επιχειρηματικό δαιμόνιο. Αξίζει να σημειωθεί ότι οι ερωτηθέντες θεωρούν ότι υπάρχει μόνο περιορισμένη ανάγκη για (α) τη διαχείριση της αλυσίδας εφοδιασμού και (β) τη διαχείριση στρατηγικών σχέσεων (Πίνακας 29).

	ΕΛΛΑΔΑ	**Γ.5:** Υπάρχει ανάγκη στον Φορέα, τα πρόσωπα που κατέχουν ρόλους Κυβερνοασφάλειας να διαθέτουν και κάποιες από τις ακόλουθες **οργανωτικές δεξιότητες**;[32]				
Οργανωτικές δεξιότητες		**Καμία**	**Μικρή**	**Σημα-ντική**	**Μεγάλη**	**Μη εφαρμό-σιμο**
Επιχειρηματική Οξυδέρκεια		14	30	54	27	4
Αδιάλειπτη επιχειρησιακή λειτουργία		14	23	51	38	3
Εκπαίδευση και Κατάρτιση		10	24	50	45	2
Διαχείριση Γνώσεων		9	29	50	33	2
Δίκαιο, Πολιτική και Ηθική		18	34	47	25	3
Οργανωτική Επίγνωση		11	38	53	23	2
Ανάπτυξη Πολιτικών		13	34	53	27	3

[32] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.

Έλεγχος Διεργασιών	11	24	64	26	2
Διαχείριση Έργου	10	36	54	26	3
Διαχείριση Επικινδυνότας	9	19	58	40	2
Στρατηγικός Σχεδιασμός	13	27	52	35	3
Διαχείριση Στρατηγικών Σχέσεων	15	42	42	21	5
Διαχείριση Εφοδιαστικής Αλυσίδας	29	44	21	15	14
Διαχείριση Στελεχιακού Δυναμικού	21	40	43	15	9



Πίνακας 29 (ερώτηση Γ.5): Ανάγκη για οργανωτικές δεξιότητες στον φορέα

	ΕΛΛΑΔΑ
Γ.6: Υπάρχει ανάγκη τα πρόσωπα σε ρόλους Κυβερνοασφάλειας στον Φορέα να να διαθέτουν και κάποιες άλλες **οργανωτικές δεξιότητες** που δεν περιλαμβάνονται στον παραπάνω κατάλογο;	
Ναι	1
Όχι	129
Σύνολο	**130**

Πίνακας 30 (ερώτηση Γ.6): Πρόσθετες οργανωτικές δεξιότητες

Προσωπικότητα (ήπιες/μεταβατικές) δεξιότητες

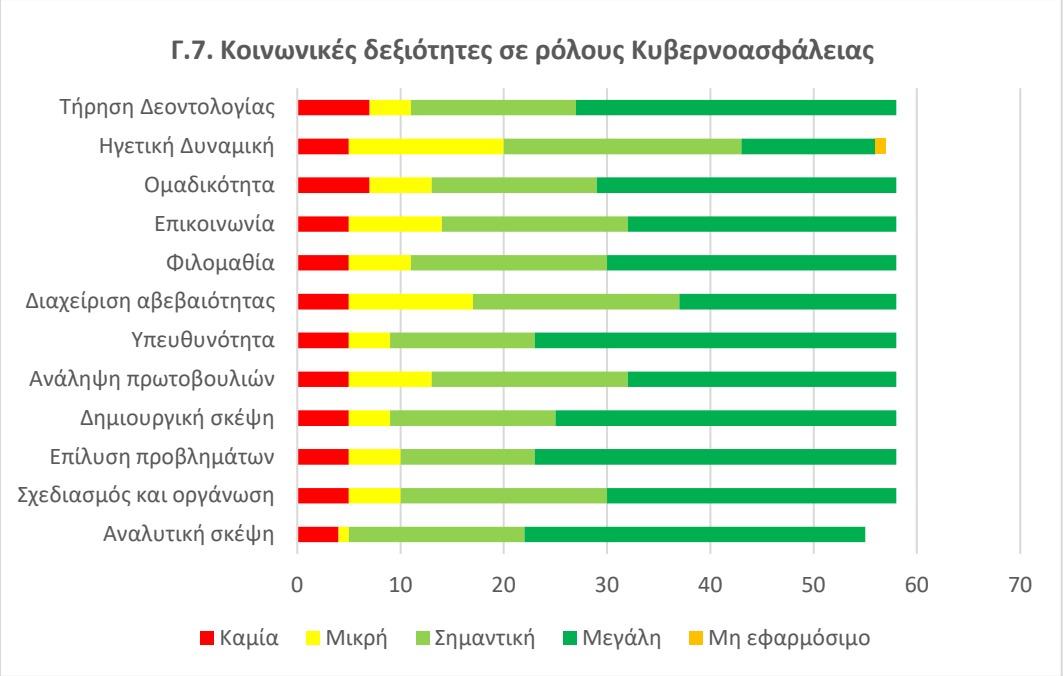
Οι ερωτηθέντες θεώρησαν ότι υπάρχει μεγάλη ανάγκη για τις περισσότερες κοινωνικές δεξιότητες για τα άτομα σε ρόλους κυβερνοασφάλειας (Πίνακας 31). Οι 4 πιο αναγκαίες δεξιότητες στους οργανισμούς των ερωτηθέντων είναι οι εξής: (α) επίλυση προβλημάτων, (β) υπεύθυνη δράση, (γ) δημιουργική σκέψη, (δ) αναλυτική σκέψη. Αξίζει να σημειωθεί ότι η Ηγεσία θεωρείται η συγκριτικά λιγότερο αναγκαία δεξιότητα.

Οι ομάδες εμπειρογνωμόνων θεωρούν ότι η έλλειψη κοινωνικών δεξιοτήτων οδηγεί σε απερίσκεπτη επιχειρηματική συμπεριφορά, η οποία είναι απαράδεκτη σε ρόλους κυβερνοασφάλειας. Τέθηκε επίσης το ερώτημα αν υπάρχει ηθική στην κυβερνοασφάλεια έχει σημασία ή αν ορισμένες αποφάσεις λαμβάνονται μόνο βάσει των εντολών που δίνει η ανώτατη διοίκηση.

	ΕΛΛΑΔΑ	**Γ.7:** Υπάρχει ανάγκη τα πρόσωπα σε ρόλους Κυβερνοασφάλειας στον Φορέα σας να πρέπει να διαθέτουν και κάποια από τις ακόλουθες **κοινωνικές δεξιότητες (soft skills)**;[33]			
Κοινωνικές Δεξιότητες	**Καμία**	**Μικρή**	**Σημαντική**	**Μεγάλη**	**Μη εφαρμόσιμο**
Αναλυτική σκέψη	4	1	17	33	0
Σχεδιασμός και οργάνωση	5	5	20	28	0
Επίλυση προβλημάτων	5	5	13	35	0
Δημιουργική σκέψη	5	4	16	33	0
Ανάληψη πρωτοβουλιών	5	8	19	26	0
Υπευθυνότητα	5	4	14	35	0
Διαχείριση αβεβαιότητας	5	12	20	21	0
Φιλομαθία	5	6	19	28	0
Επικοινωνία	5	9	18	26	0
Ομαδικότητα	7	6	16	29	0
Ηγετική Δυναμική	5	15	23	13	1
Τήρηση Δεοντολογίας	7	4	16	31	0

Πίνακας 31 (ερώτηση Γ.7):Ανάγκες για κοινωνικές δεξιότηρ

[33] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



Λίγοι ερωτηθέντες πρότειναν μια σειρά από πρόσθετες κοινωνικές δεξιότητες, π.χ. ικανότητα εργασίας υπό πίεση/διαχείριση του άγχους, διαχείριση χρόνου, διαχείριση ομάδων, ικανότητα παρουσίασης/εξήγησης πολύπλοκων θεμάτων με απλούς όρους, ενσυναίσθηση, προσαρμοστικότητα και προσοχή στη λεπτομέρεια (Πίνακας 32).

	ΕΛΛΑΔΑ
Γ.8: Γενικά, υπάρχει ανάγκη τα πρόσωπα που κατέχουν ρόλους στον τομέα της Κυβερνοασφάλειας να διαθέτουν επιπλέον **κοινωνικές δεξιότητες** που δεν περιλαμβάνονται στον παραπάνω κατάλογο;	
Ναι	3
Όχι	54
Σύνολο	**57**

Πίνακας 32 (ερώτηση Γ.8): Πρόσθετες κοινωνικές δεξιότητες

Επαγγελματική κατάρτιση σε θέματα κυβερνοασφάλειας

Οι περισσότεροι ερωτηθέντες (81,3%) πιστεύουν ότι υπάρχει ανάγκη για εκπαίδευση του προσωπικού σε ρόλους κυβερνοασφάλειας (Πίνακας 33). Ο κύριος λόγος για την ανάγκη αυτή είναι ότι οι νέες (τεχνολογικές) εξελίξεις απαιτούν νέες δεξιότητες.

	ΕΛΛΑΔΑ
Δ.1: Υπάρχει ανάγκη εκπαίδευσης ή κατάρτισης του προσωπικού του Φορέα σας σε ρόλους Κυβερνοασφάλειας;	
Ναι	113

Όχι	26
Σύνολο	**139**

Πίνακας 33 (ερώτηση Δ.1): Ανάγκη για κατάρτιση προσωπικού

ΕΛΛΑΔΑ	
Δ.2: Υπάρχει καθυστέρηση στην κατάρτιση προσωπικού σε ρόλους κυβερνοασφάλειας;	
Ναι	34
Όχι	105
Σύνολο	**139**

Πίνακας 34 (ερώτηση Δ.2): Εκπαιδευτικό προσωπικό

Οι περισσότεροι ερωτηθέντες (75,5%) θεωρούν ότι δεν υπάρχει καθυστέρηση στην εκπαίδευση του προσωπικού σε ρόλους κυβερνοασφάλειας (Πίνακας 34). Ο κύριο λόγος είναι ότι τα άτομα σε ρόλους κυβερνοασφάλειας δεν έχουν χρόνο για εκπαίδευση και ότι η εκπαίδευση είναι πολύ ακριβή.

Οι ομάδες εμπειρογνωμόνων αναγνωρίζουν την ανάγκη κατάρτισης του προσωπικού, αλλά επί του παρόντος δεν υπάρχει καθυστέρηση (πίνακες 32-34). Οι ανάγκες κατάρτισης εμφανίστηκαν πρόσφατα, πιθανώς με αφορμή το Covid. Αναφέρθηκε επίσης ότι η κατάρτιση είναι μια πολύπλοκη άσκηση για τις εταιρείες, καθώς πρέπει να ληφθούν υπόψη παράμετροι όπως ο χρόνος, το κόστος και η διαθεσιμότητα προσωπικού για την κατάρτιση στο χώρο εργασίας.

Οι 3 κορυφαίες στρατηγικές κατάρτισης που θεωρούνται από τους ερωτηθέντες ως πολύ σημαντικές στον οργανισμό τους είναι η αναβάθμιση των δεξιοτήτων του δικού τους προσωπικού ΤΠΕ, η πρόσληψη ατόμων με τις ήδη κατάλληλες δεξιότητες και η καθοδήγηση και κατάρτιση στην εργασία (πίνακας 35).

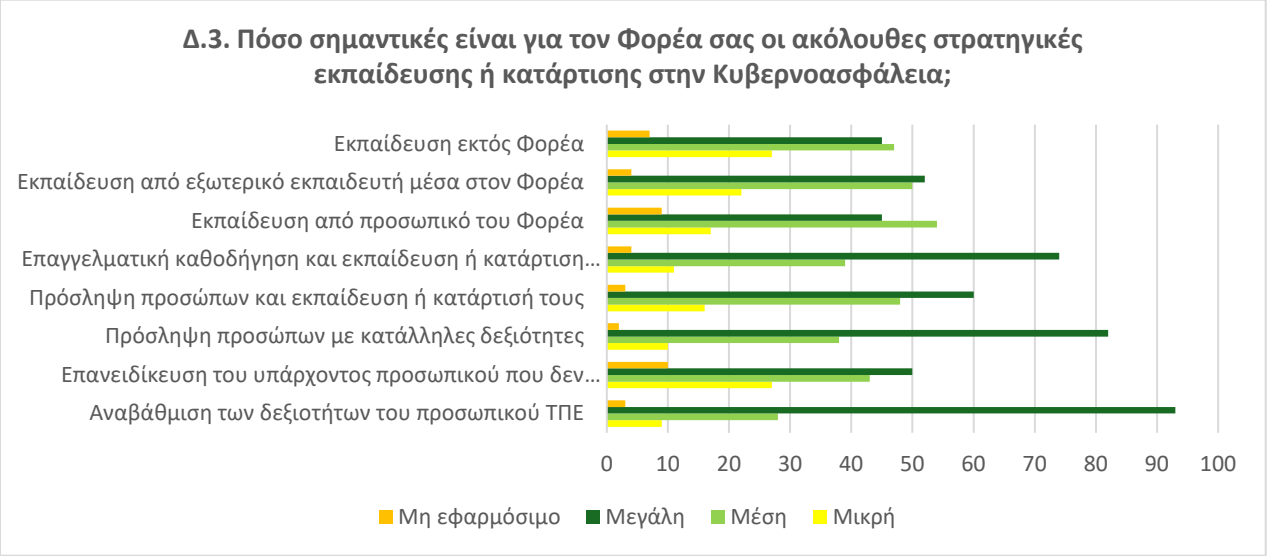
Οι ομάδες εμπειρογνωμόνων θεωρούν ότι οι περισσότεροι οργανισμοί προτιμούν να αναβαθμίσουν το προσωπικό τους στις ΤΠΕ παρά να προσλάβουν άτομα με τις κατάλληλες δεξιότητες, καθώς πιστεύουν ότι αυτό είναι εξαιρετικά δύσκολο.

ΕΛΛΑΔΑ	**Δ.3:** Πόσο σημαντικές είναι για τον Φορέα σας οι ακόλουθες **στρατηγικές εκπαίδευσης ή κατάρτισης** στην Κυβερνοασφάλεια;[34]			
Στρατηγικές κατάρτισης	**Μικρή**	**Μέση**	**Μεγάλη**	**Μη εφαρμόσιμο**
Αναβάθμιση των δεξιοτήτων του προσωπικού ΤΠΕ	9	28	93	3
Επανειδίκευση του υπάρχοντος προσωπικού που δεν ειναι ΤΠΕ	27	43	50	10

[34] Green color indicates high values and yellow low ones.

Πρόσληψη προσώπων με κατάλληλες δεξιότητες	10	38	82	2
Πρόσληψη προσώπων και εκπαίδευση ή κατάρτισή τους	16	48	60	3
Επαγγελματική καθοδήγηση και εκπαίδευση ή κατάρτιση κατά στην εργασία (on-the-job)	11	39	74	4
Εκπαίδευση από προσωπικό του Φορέα	17	54	45	9
Εκπαίδευση από εξωτερικό εκπαιδευτή μέσα στον Φορέα	22	50	52	4
Εκπαίδευση εκτός Φορέα	27	47	45	7

Πίνακας 35 (Ερώτηση Δ.3) Σημασία των στρατηγικών κατάρτισης



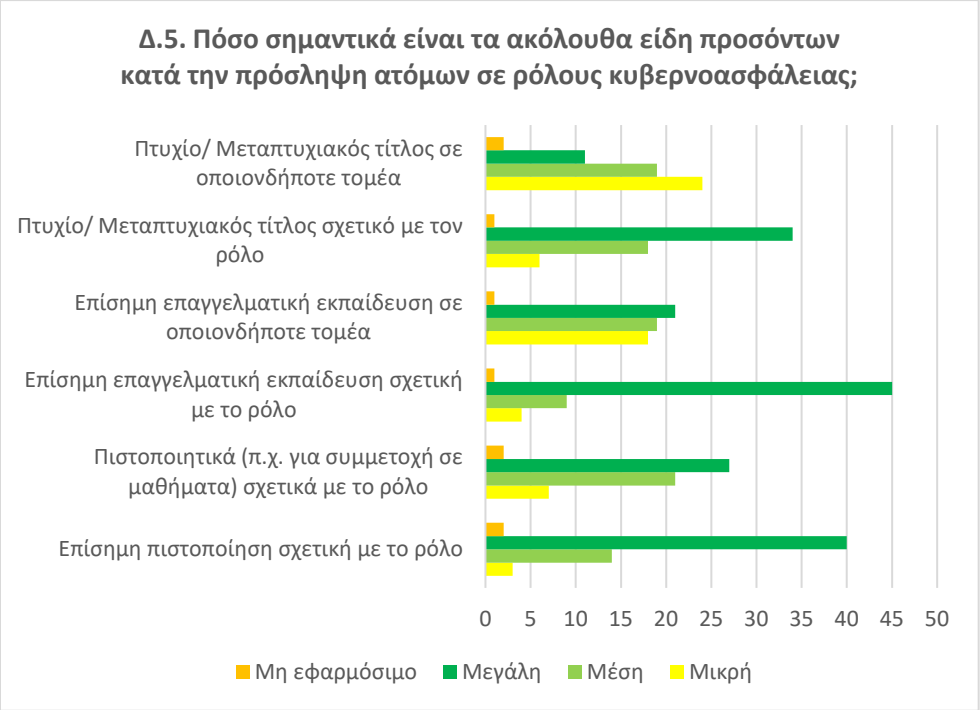
Πρόσθετα προσόντα

Τα 3 πιο επιθυμητά είδη προσόντων που προτείνονται κατά την πρόσληψη ατόμων σε ρόλους κυβερνοασφάλειας είναι: τυπική επαγγελματική εκπαίδευση σχετική με το ρόλο, τυπική πιστοποίηση σχετική με το ρόλο και πτυχίο Bachelor/Master σχετικό με το ρόλο (Πίνακας 36). Αξίζει να αναφερθεί ότι σχεδόν οι μισοί από τους ερωτηθέντες θεωρούν ότι το πτυχίο Bachelor/Master σε οποιοδήποτε τομέα είναι το λιγότερο σημαντικό προσόν.

Οι ερωτηθέντες θεώρησαν επίσης σημαντική τη σημασία της συνεχούς κατάρτισης του προσωπικού σε ρόλους κυβερνοασφάλειας για την προσαρμογή στην αυξανόμενη ζήτηση για τέτοια κατάρτιση εντός των οργανισμών. Τονίστηκε ότι (α) τα προσόντα θα πρέπει να συνοδεύονται από επιβεβαιωμένη επαγγελματική εμπειρία, (β) η προϋπηρεσία σε παρόμοια θέση παίζει μεγάλο ρόλο στην εκπαίδευση και (γ) το προσωπικό θα πρέπει να εκπαιδεύεται μέσω σεμιναρίων για να αποκτήσει τις γνώσεις που θα το βοηθήσουν να αντιμετωπίσει τους σημερινούς κινδύνους.

	Κυβερνοασφάλειας;[35]			
Προσόντα πρόσληψης	**Μικρή**	**Μέση**	**Μεγάλη**	**Μη εφαρμόσιμο**
Επίσημη πιστοποίηση σχετική με το ρόλο	3	14	40	2
Πιστοποιητικά (π.χ. για συμμετοχή σε μαθήματα) σχετικά με το ρόλο	7	21	27	2
Επίσημη επαγγελματική εκπαίδευση σχετική με το ρόλο	4	9	45	1
Επίσημη επαγγελματική εκπαίδευση σε οποιονδήποτε τομέα	18	19	21	1
Πτυχίο/ Μεταπτυχιακός τίτλος σχετικό με τον ρόλο	6	18	34	1
Πτυχίο/ Μεταπτυχιακός τίτλος σε οποιονδήποτε τομέα	24	19	11	2

Πίνακας 36 (ερώτηση Δ.5): Σημασία των προσόντων πρόσληψης



Τι πρότειναν/σημείωσαν οι ομάδες εμπειρογνωμόνων

Η ανάλυση των δεδομένων υποστηρίχθηκε επίσης από δύο ομάδες εμπειρογνωμόνων (ΟΕ). Στην πρώτη από αυτές συμμετείχαν έμπειροι επαγγελματίες της κυβερνοασφάλειας που προέρχονταν από τον ιδιωτικό και τον δημόσιο τομέα, ενώ στη δεύτερη συμμετείχαν μόνο ακαδημαϊκοί με ειδικότητα στην κυβερνοασφάλεια ή σε συναφές πεδίο.

[35] Green color indicates high values and yellow low ones.

Οι κύριες παρατηρήσεις και προτάσεις των μελών των ομάδων εμπειρογνωμόνων αναφέρονται συνοπτικά στη συνέχεια.

1. **Τομείς οργανισμών** (ερώτηση Α.5)

- Τα μέλη των ΟΕ σημείωσαν ότι δεν ταιριάζουν επαρκώς όλοι οι τομείς οργανισμών με την αντίστοιχη ταξινομία της NIS2.

2. **Ρόλοι κυβερνοασφάλειας** (ερώτηση Β.4.1)

- Η θέση του Υπεύθυνου Νομικής, Πολιτικής και Συμμόρφωσης στον Κυβερνοχώρο θεωρήθηκε ισοδύναμη ή συγκρίσιμη με αυτή του Υπεύθυνου Προστασίας Δεδομένων (DPO) σύμφωνα με το Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (ECSF) του ENISA.

- Τα μέλη των ΟΕ ανέφεραν ότι επί του παρόντος δεν υπάρχουν πολλοί αξιωματούχοι νομικής, πολιτικής και συμμόρφωσης στον κυβερνοχώρο που εργάζονται σε αυτόν τον ρόλο ή ότι δεν υπάρχει ανάγκη για τέτοιους αξιωματούχους αυτή τη στιγμή.

3. **Δεξιότητες κυβερνοασφάλειας** (ερώτηση Γ.1)

- Τα μέλη των ΟΕ θεώρησαν ότι η περιορισμένη ανάγκη για δεξιότητες ασφάλειας της εφοδιαστικής αλυσίδας είναι πιθανότατα αποτέλεσμα της πρακτικής της ανάθεσης των προμηθειών σε εξωτερικούς συνεργάτες, η οποία αναθέτει την ευθύνη για την ασφάλεια της εφοδιαστικής αλυσίδας στον προμηθευτή.

- Τα μέλη των ΟΕ θεωρούν επίσης ότι η περιορισμένη ζήτηση που εξέφρασαν οι ερωτηθέντες για ικανότητες ασφάλειας ΤΝ και ανάλυσης πληροφοριών οφείλεται στο γεγονός ότι οι περισσότεροι τοπικοί οργανισμοί αγοράζουν προϊόντα και λύσεις που έχουν αναπτυχθεί σε άλλες χώρες.

- Τα μέλη των ΟΕ σημείωσαν επίσης ότι, ενώ η τεχνητή νοημοσύνη μπορεί να αποτελέσει ένα ιδιαίτερα επωφελές εργαλείο στην ασφάλεια στον κυβερνοχώρο, οι περισσότεροι τοπικοί οργανισμοί δεν έχουν ακόμη εκτιμήσει πλήρως την ωριμότητα αυτής της νέας τεχνολογίας.

- Τα μέλη των ΟΕ θεώρησαν επιτακτική ανάγκη τη διασφάλιση των κρίσιμων υποδομών, ώστε να αντιμετωπίζονται άμεσα και αποτελεσματικά οι παραβιάσεις της ασφάλειας.

- Τα μέλη των ΟΕ ανέφεραν ότι οι δεξιότητες για την προστασία της ιδιωτικής ζωής των δεδομένων ήταν υψηλές κυρίως λόγω των απαιτητικών απαιτήσεων του ΓΚΠΔ.

4. **Δεξιότητες προσωπικότητας (Ήπιες/μεταβατικές)** (ερώτηση Γ.7)

- Τα μέλη της ομάδας εμπειρογνωμόνων θεωρούν ότι η έλλειψη δεξιοτήτων προσωπικότητας οδηγεί σε απερίσκεπτη επιχειρηματική συμπεριφορά, η οποία είναι απαράδεκτη σε ρόλους κυβερνοασφάλειας.

- Τέθηκε επίσης ένα ερώτημα σχετικά με το αν, στην πράξη, η ηθική στην ασφάλεια στον κυβερνοχώρο έχει σημασία ή αν οι περισσότερες αποφάσεις βασίζονται μόνο στις επιθυμίες της ανώτατης διοίκησης.

5. **Εκπαίδευση στον τομέα της ασφάλειας στον κυβερνοχώρο** (ερωτήσεις Δ.1-Δ.3):

- Οι ομάδες εμπειρογνωμόνων αναγνώρισαν την αναγκαιότητα της κατάρτισης του προσωπικού. Ωστόσο, υπογράμμισαν το γεγονός ότι επί του παρόντος δεν υπάρχει τέτοια ανεπάρκεια.

- Τα μέλη των ΟΕ σημείωσαν ότι οι σημαντικές ανάγκες κατάρτισης που εμφανίστηκαν πρόσφατα πιθανόν να προκλήθηκαν από την πανδημία Covid.

- Τα μέλη των ΟΕ σημείωσαν ότι η κατάρτιση είναι ένα πολύπλοκο εγχείρημα για τις εταιρείες, καθώς πρέπει να ληφθούν υπόψη διάφοροι παράγοντες, όπως ο χρόνος, το κόστος και η διαθεσιμότητα του προσωπικού.

4.4 ΕΛΛΑΔΑ – Τα αποτελέσματα με τα βλέμματα στραμμένα στο μέλον

Τα προφίλ των επαγγελματιών της ασφάλειας στον κυβερνοχώρο ανταποκρίνονται στη ζήτηση

Ένα τυπικό προφίλ ενός εμπειρογνώμονα κυβερνοασφάλειας που ανταποκρίνεται στη ζήτηση της εποχής εμφανίζεται στον Πίνακα 37. Τα χαρακτηριστικά του προφίλ βασίζονται στις απαντήσεις που δόθηκαν στο ερωτηματολόγιό μας από τοπικούς (Έλληνες) επαγγελματίες. Τα χαρακτηριστικά αναφέρονται εκ νέου στον πίνακα αφού προηγουμένως έχουν ιεραρχηθεί σύμφωνα με τους ερωτηθέντες του ερωτηματολογίου.

CyberHub Greece		ΕΛΛΑΔΑ: Ζήτηση για επαγγελματίες κυβερνοασφάλειας στο μέλλον - Ποιοτικά χαρακτηριστικά	
1. Ρόλοι Κυβερνοασφάλειας στο Μέλλο	**Ρόλοι σε 2 χρόνια** (κατά δημοτικότητα)	**2. Ζήτηση για δεξιότητες Κυβερνοασφάλειας**	**Μεγάλη ή ουσιαστική ζήτηση (κατά δημοτικότηταα)**
	Cybersecurity Implementer		**Προστασία Δεδομένων**
	Cyber Incident Responder		**Information Systems & Network Security / Cyber Resiliency**
	Cybersecurity Risk Manager		Διαχείρηση περιστατικών
	Penetration Tester		Έλεγχος Πρόσβασης/Διαχείριση Ταυτότητας
	Cybersecurity Architect		Ανάλυση Απειλών
	Ρόλοι μετά από 5+ χρόνια (κατά δημοτικότητα)		**Καμία ή περιοσμένη ζήτηση** (τα χαμηλότερα πρώτα)
	Cyber Incident Responder		**Supply Chain Security**
	Cybersecurity Implementer		**Operational Technology Security**
	Penetration Tester		Digital Forensics
	Cybersecurity Risk Manager		Intelligence Analysis
	Cybersecurity Researcher		AI Security

3. Ζήτηση για άλλες δεξιότητες (μεγάλη η ουσιαστική ανάγκη) (κατά δημοτικότητα)

Δεξιότητες ΤΠΕ	**Οργανωτικές δεξιότητες**	**Κοινωνικές δεξιότητες**	**Προτιμώμενα Προσόντα**
Λειτουργικά Συστήματα	**Διαχείρηση Επικινδυνότητας**	**Αναλυτική Σκέψη**	**Επίσημη πιστοποίηση σχετική με το ρόλο**
Διαχείρηση Δικτύου	**Εκπαίδευση και Κατάρτιση**	**Δημιουργική Σκέψη**	**Επίσημη επαγγελματική εκπαίδευση σχετική με το ρόλο**
Ανάλυση Δεδομένων	Έλεγχος Διεργασιών	Υπευθυνότητα	Πτυχίο/ Μεταπτυχιακός τίτλος σχετικό με τον ρόλο
Αρχιτεκρινική επιχειρήσεων – Σχεδιασμός Υποδομής	Αδιάλειπτη επιχειρησιακή λειτουργία	**Επίλυση Προβλημάτων**	Πιστοποιητικά (π.χ. για συμμετοχή σε μαθήματα) σχετικά με το ρόλο
Διαχείριση & Ολοκλήρωση Συστήματος	Στρατηγικός Σχεδιασμός	Σχεδιασμός και Οργάνωση	Επίσημη επαγγελματική εκπαίδευση σε οποιονδήποτε τομέα

Κεφάλαιο 5 - Συμπεράσματα

Στόχος της παρούσας έκθεσης είναι να εντοπίσει την αναντιστοιχία μεταξύ προσφοράς και ζήτησης σε δεξιότητες κυβερνοασφάλειας στην Ελλάδα και να παράσχει μια ακριβή εικόνα της ωριμότητας, των ευκαιριών και των ιδιαιτεροτήτων του οικοσυστήματος δεξιοτήτων κυβερνοασφάλειας στην Ελλάδα. Επιπλέον, παρουσιάζεται μια επισκόπηση 360 του ελληνικού οικοσυστήματος.

Από την πλευρά της προσφοράς, δεν υπάρχει κανένα προπτυχιακό ακαδημαϊκό πρόγραμμα για τις δεξιότητες κυβερνοασφάλειας στη χώρα, ωστόσο ορισμένα κολέγια προσφέρουν προπτυχιακά προγράμματα σπουδών στην κυβερνοασφάλεια σε συνεργασία με ξένα πανεπιστήμια.

Ενώ υπάρχει ένας καλός αριθμός διαθέσιμων μεταπτυχιακών προγραμμάτων στον κυβερνοχώρο (τόσο στα ελληνικά δημόσια πανεπιστήμια όσο και σε ορισμένα κολέγια), αρκετές θέσεις φοιτητών παραμένουν αδιάθετες.

Επιπλέον, (α) τα ελληνικά πανεπιστήμια μπορούν να χορηγούν διδακτορικά διπλώματα σε φοιτητές με θέμα διατριβής σχετικό με την κυβερνοασφάλεια (β) οι σχετικές επαγγελματικές πιστοποιήσεις που παρέχονται από διεθνείς επαγγελματικές ενώσεις, (όπως, ICS2 και ISACA) φαίνεται να παίζουν εμφανώς υποστηρικτικό ρόλο.

Από την πλευρά της ζήτησης, δεν υπάρχει καμία συστηματική και αξιόπιστη μελέτη που να εξετάζει και να αξιολογεί τη ζήτηση δεξιοτήτων κυβερνοασφάλειας, βραχυπρόθεσμα ή μακροπρόθεσμα. Ως εκ τούτου, η παρούσα έκθεση είναι μοναδική και τα συμπεράσματα, που παρουσιάζονται κατωτέρω, αντλούνται σε μεγάλο βαθμό από την έρευνα, επαληθεύονται από τις ομάδες εμπειρογνωμόνων και συμπληρώνονται από τις κενές θέσεις εργασίας που παρέχονται από το EIT Digital.

Ρόλοι κυβερνοασφάλειας

Όλη η παραπάνω ανάλυση μπορεί να συνοψιστεί στα ακόλουθα συμπεράσματα σχετικά με τους ρόλους του ENISA στον τομέα της κυβερνοασφάλειας:

Cyber Incident Responders: σήμερα οι περισσότεροι άνθρωποι εργάζονται σε αυτόν τον ρόλο και η τάση αυτή αναμένεται να συνεχιστεί τα επόμενα 5 χρόνια, κυρίως σε οργανισμούς μεσαίου και μεγάλου μεγέθους.

Cybersecurity Implementers: μεγάλη ανάγκη στο εγγύς μέλλον (2-5 χρόνια), κυρίως σε οργανισμούς μεσαίου και μεγάλου μεγέθους.

Digital Forensics Investigator, Cybersecurity Auditor και Cyber Threat Intelligence Specialist: αναμένεται να παρουσιάσουν τη μεγαλύτερη αύξηση. Συγκεκριμένα, τα επόμενα 5 χρόνια:

Cyber Threat Intelligence Specialist: μεγάλη αύξηση σε οργανισμούς πολύ μικρού μεγέθους (300%) και μεσαίου μεγέθους (350%).

Digital Forensics Investigators: μεγάλη αύξηση, σε μικρούς οργανισμούς (900%).

Cybersecurity Auditors: σημαντική αύξηση σε μεγάλους οργανισμούς (119%).

Παραδόξως, αρκετοί ερωτηθέντες ανέφεραν ότι δεν εργάζονται σήμερα αξιωματούχοι νομικής, πολιτικής και συμμόρφωσης στον κυβερνοχώρο ή ότι δεν υπάρχει ανάγκη για τέτοιους αξιωματούχους επί του παρόντος.

Επιπλέον, στους 3 κορυφαίους τομείς της NIS2, η ανάγκη για ρόλους κυβερνοασφάλειας του ENISA είναι:

Στον τομέα της **Έρευνας,** η μεγαλύτερη ανάγκη αφορά τους Cybersecurity Researchers, ενώ η μεγαλύτερη αύξηση αφορά τους Auditors (600%).

Στον τομέα των **Ψηφιακών Υποδομών**, η μεγαλύτερη ανάγκη είναι για Cybersecurity Implementer, ενώ η μεγαλύτερη αύξηση είναι για Penetration Tester (68%).

Στον τομέα της **Διαχείρισης Υπηρεσιών ΤΠΕ**, η μεγαλύτερη ανάγκη είναι για Cyber Incident Responders και Cybersecurity Implementers, ενώ η μεγαλύτερη αύξηση είναι για Cybersecurity Researchers (220%).

Αξίζει να σημειωθεί ότι στον τομέα της Διαχείρισης Υπηρεσιών ΤΠΕ παρατηρείται αύξηση σε όλους τους ρόλους του ENISA, κάτι που δεν συμβαίνει στον τομέα των Ψηφιακών Υποδομών.

Δεξιότητες για επαγγελματίες κυβερνοασφάλειας

Οι δεξιότητες για τους επαγγελματίες της ασφάλειας στον κυβερνοχώρο, χωρισμένες σε 4 κατηγορίες (ασφάλεια στον κυβερνοχώρο, σχετικές με την πληροφορική, οργανωτικές, κοινωνικές δεξιότητες), οι οποίες απαιτούνται κυρίως (μεγάλη ή σημαντική ανάγκη) παρουσιάζονται στον παρακάτω πίνακα:

Δεξιότητες Κυβερνοασφάλειας	Δεξιότητες σε ΤΠΕ	Οργανωτικές Δεξιότητες	Κοινωνικές Δεξιότητες
Προστασία Δεδομένων	**Λειτουργικά Συστήματα**	**Διαχείριση Επικινδυνότητας**	**Αναλυτική Σκέψη**
Information Systems & Network Security / Cyber Resiliency	**Διαχείριση Δικτύου**	**Εκπαίδευση και Κατάρτιση**	**Δημιουργική Σκέψη**
Διαχείριση Περιστατικών	**Ανάλυση Δεδομένων**	Έλεγχος Διεργασιών	Υπευθυνότητα
Έλεγχος Πρόσβασης/Διαχείριση Ταυτότητας	Αρχιτεκρινική επιχειρήσεων – Σχεδιασμός Υποδομής	Αδιάλειπτη επιχειρησιακή λειτουργία	**Επίλυση Προβλημάτων**
Ανάλυση Απειλών	Διαχείριση & Ολοκλήρωση Συστήματος	Στρατηγικός Σχεδιασμός	Σχεδιασμός και Οργάνωση

Η **ανάλυση των κενών θέσεων εργασίας** (Ιούνιος 2024) έδειξε ότι οι εταιρείες στην Ελλάδα αναζητούν προσωπικό για την ασφάλεια στον κυβερνοχώρο με δεξιότητες σε όλες τις κατηγορίες. Σύμφωνα με την ίδια ανάλυση, οι δεξιότητες που σημειώνονται με κόκκινο χρώμα παραπάνω, είναι μεταξύ των **πιο περιζήτητων** δεξιοτήτων.

Αρκετοί από τους ερωτηθέντες δήλωσαν ότι δεν υπάρχει ανάγκη για δεξιότητες Ασφάλειας Εφοδιαστικής Αλυσίδας., η ηγεσία θεωρείται η συγκριτικά λιγότερο αναγκαία δεξιότητα, ενώ οι ομάδες εμπειρογνωμόνων θεωρούν ότι η έλλειψη δεξιοτήτων προσωπικότητας οδηγεί σε απερίσκεπτη επιχειρηματική συμπεριφορά, η οποία είναι απαράδεκτη σε ρόλους κυβερνοασφάλειας.

Εκπαίδευση και κατάρτιση επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο

Έχει αποδειχθεί ότι το προσωπικό πρέπει να εκπαιδεύεται, καθώς οι νέες (τεχνολογικές) εξελίξεις απαιτούν νέες δεξιότητες. Ωστόσο, το γεγονός ότι οι εμπειρογνώμονες της κυβερνοασφάλειας δεν έχουν χρόνο για εκπαίδευση και ότι η εκπαίδευση είναι πολύ δαπανηρή, οδηγεί στο να μην υπάρχει καθυστέρηση στην εκπαίδευση του προσωπικού.

Οι εταιρείες, προκειμένου να διαθέτουν εμπειρογνώμονες κυβερνοασφάλειας με τις κατάλληλες δεξιότητες, προτιμούν να αναβαθμίζουν το δικό τους προσωπικό ΤΠΕ, να προσλαμβάνουν άτομα με ήδη τις κατάλληλες δεξιότητες ή να τους εκπαιδεύουν στην εργασία τους. Η πρόσληψη ατόμων με τις σωστές δεξιότητες θεωρείται πολύ δύσκολη και, ως εκ τούτου, προτιμάται η αναβάθμιση των δεξιοτήτων. Ωστόσο, όταν προσλαμβάνονται άτομα σε ρόλους κυβερνοασφάλειας, η επίσημη επαγγελματική εκπαίδευση σχετική με τον ρόλο και η επίσημη πιστοποίηση σχετική με τον ρόλο είναι τα πλέον προτιμώμενα προσόντα.

Προτιμώμενα Προσόντα
Επίσημη πιστοποίηση σχετική με το ρόλο
Επίσημη επαγγελματική εκπαίδευση σχετική με το ρόλο
Πτυχίο/ Μεταπτυχιακός τίτλος σχετικό με τον ρόλο
Πιστοποιητικά (π.χ. για συμμετοχή σε μαθήματα) σχετικά με το ρόλο
Επίσημη επαγγελματική εκπαίδευση σε οποιονδήποτε τομέα

Ευχαριστίες

Το CyberHub Greece θα ήθελε να εκφράσει την ειλικρινή εκτίμησή του στους επαγγελματίες της κυβερνοασφάλειας, τους φορείς, τις επαγγελματικές ενώσεις και τις επιχειρήσεις που απάντησαν στις έρευνες και συμμετείχαν στις ομάδες εμπειρογνωμόνων. Η υποστήριξή τους, η συμβολή τους και η εποικοδομητική ανατροφοδότησή τους συνέβαλαν καθοριστικά στην ολοκλήρωση της παρούσας έκθεσης.

Θερμές ευχαριστίες στους διευθυντές των μεταπτυχιακών προγραμμάτων των ελληνικών δημόσιων πανεπιστημίων, κολεγίων, κέντρων κατάρτισης και δια βίου μάθησης, τα οποία διαθέτουν προγράμματα στην κυβερνοασφάλεια ή σχετίζονται με αυτήν.

Αναφορές

[1] ISC^2 Cybersecurity Workforce Study, *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*, 2023, https://www.isc2.org/research

[2] ManpowerGroup, *The State of Cybersecurity Talent*, Greece 2022.

[3] ENISA, *Foresight Cybersecurity Threats for 2030* (update), March 2024, https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats

[4] Greece Economy Infographic Presentation, https://www.creativefabrica.com/product/greece-economy-infographic-presentation/

[5] Greek Debt Crisis Explained, https://www.thebalancemoney.com/what-is-the-greece-debt-crisis-3305525

[6] Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ), https://www.statistics.gr/en/elstat-infographics

[7] Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ), «ΕΛΛΑΣ ΜΕ ΑΡΙΘΜΟΥΣ» Ιανουάριος – Μάρτιος 2024, https://www.statistics.gr/el/greece-in-figures

[8] Eurydice - National Education Systems, https://eurydice.eacea.ec.europa.eu/national-education-systems/greece/overview

[9] Greece: Unemployment rate, https://www.theglobaleconomy.com/Greece/unemployment_rate_monthly/

[10] Portulans Institute, Network Readiness Index, https://networkreadinessindex.org/

[11] Συμβούλιο Ανταγωνιστικότητας της Ελλάδας, https://competegr.org/

[12] Μελέτη ΣΕΠΕ - Deloitte Αποτίμησης Επάρκειας Ειδικών ΤΠΕ στην Ελλάδα, https://www.sepe.gr/research-studies/21142064/meleti-sepe-deloitte-apotimisis-eparkeias-eidikon-tpe-stin-ellada/

[13] European Innovation Scoreboard (EIS), https://op.europa.eu/en/home

[14] ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4577/2018, https://mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf

[15] Υπουργική Απόφαση 1027/2019, https://mindigital.gr/wp-content/uploads/2020/01/3739B-19-1.pdf

[16] Εθνική Αρχή Κυβερνοασφάλειας (Ν. 5086/2024, ΦΕΚ 23/Α/14.02.2024, www.et.gr)

[17] Οργανισμός Υπουργείου Ψηφιακής Διακυβέρνησης (Π.Δ. 40/2020, ΦΕΚ 85/Α/15.04.2020, www.et.gr)

[18] Εθνική Στρατηγική Κυβερνοασφάλειας 2020-25 (Υ.Α. 34368, 07/12/2020, https://mindigital.gr/wp-content/uploads/2020/12/national-cybersecurity-strategy-2020-2025.pdf).

[19] Marketsandmarkets Cybersecurity Market to 2028, https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

[20] European Qualifications Framework, https://europa.eu/europass/en/europass-digital-tools/european-qualifications-framework

[21] European Union Agency for Cybersecurity (ENISA), *Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education* (Report), November 2021, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[22] Εθνικό Αρχείο Διδακτορικών Διατριβών, Ελλάδα, Μάρτιος 2024 https://www.didaktorika.gr/eadd/

[23] Cisco Certified Network Associate v7 & CyberOps Associate, https://kedivim.uom.gr/member/mavridis_ioannis/

[24] Ασφάλεια Δεδομένων – Κυβερνοασφάλεια, https://kedivim.upatras.gr/cooperatedcourse/asfaleia-dedomenon-kyvernoasfaleia/

[25] Cisco Certified CyberOps Associate – Κυβερνοασφάλεια, https://learning.uth.gr/cybersecurity/

[26] Ειδικός Πληροφορικής Προστασίας Δεδομένων – Κυβερνοασφάλεια, https://kedivim.uowm.gr/course/eidikos-pliroforikis-se-themata-prostasias-dedomenon-gdpr-kyvernoasfaleia/

[27] Συστήματα Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια, https://elearningekpa.gr/courses/sustimata-texnitis-noimosunis-stin-kubernoasfaleia

[28] Check Point Certified Security Administrator (CCSA), https://www.haec.gr/el/check-point-certified-security-administrator-ccsa

[29] Κυβερνοέγκλημα & Κυβερνοασφάλεια, https://kedivim.auth.gr/programs/kyvernoeglima/

[30] ISC^2 (International Information System Security Certification Consortium) Hellenic Chapter, https://isc2-chapter.gr/

[31] ISACA (Information Systems Audit and Control Association) Athens Chapter, https://engage.isaca.org/athenschapter/home

[32] Οικονομικό Πανεπιστήμιο Αθηνών, ΠΜΣ σε Ασφάλεια & Ανάπτυξη Πληροφοριακών Συστημάτων, Ελλάδα, 2024 http://mscis.cs.aueb.gr/

[33] Πανεπιστήμιο Πειραιώς, ΠΜΣ σε Κυβερνοασφάλεια και Επιστήμη Δεδομένων, Ελλάδα, 2024 https://cybersecdatasci.cs.unipi.gr

[34] Πανεπιστήμιο Πειραιώς, ΠΜΣ σε Ασφάλεια Ψηφιακών Συστημάτων, Ελλάδα, 2024 https://www.ds.unipi.gr/security/

[35] Πανεπιστήμιο Αιγαίου, ΠΜΣ σε Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων, Ελλάδα, 2024 https://msc.icsd.aegean.gr/masters/security/

[36] Πανεπιστήμιο Δυτικής Αττικής, ΠΜΣ σε Κυβερνοασφάλεια, Ελλάδα, 2024 http://www.ice.uniwa.gr/education/postgraduate/cybersecurity/

[37] Διεθνές Πανεπιστήμιο της Ελλάδος, ΠΜΣ σε Κυβερνοασφάλεια, Ελλάδα 2024, https://www.eduguide.gr/grad/prokiryksi/diethnes-panepistimio-msc-communications-cybersecurity,569

[38] Metropolitan College, B.Sc. Cyber Security & Networks, Ελλάδα 2024 https://www.mitropolitiko.edu.gr/ programmata-spoydon/scholi-pliroforikis/bsc-hons-cyber-security-and-networks/

[39] New York College, B.Sc. Cybersecurity, Ελλάδα 2024 https://www.nyc.gr/tmimata-spoudon-nyc/spoudes-kyvernoasfaleias/bsc-hons-computing-application-development#undefined1

[40] The American College of Greece, B.Sc. Cybersecurity & Networks, Ελλάδα 2024 https://www.acg.edu/undergraduate/undergraduate-programs/school-of-liberal-arts-sciences/liberal-arts-sciences-majors/cybersecurity-and-networks/

[41] Epsilon College, B.Sc. Web Development & Cyber Security, Ελλάδα 2024 https://epsiloncollege.gr/spoudes/bachelors/bsc-hons-in-web-development-cyber-security/

[42] BCA College, M.Sc. Maritime Cybersecurity, Ελλάδα 2024 https://www.bca.edu.gr/master-degrees/shipping-transport-logistics-department/msc-maritime-cybersecurity/

[43] BCA College, MSc Applied Cyber Security, Ελλάδα 2024 https://www.bca.edu.gr/master-degrees/business-department/ msc-applied-cybersecurity/

[44] Aegean College, M.Sc. Cyber Security, Ελλάδα 2024 https://aegeancollege.gr/programma/msc-cybersecurity/

[45] Μητροπολιτικό Κολλέγιο, M.Sc. Information Security & Digital Forensics, Ελλάδα 2024 https://www.mitropolitiko.edu.gr/ programmata-spoydon/scholi-pliroforikis/msc-information-security-and-digital-forensics/

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Ι: ΕΛΛΑΔΑ - Χαρακτηριστικά ΠΜΣ

Οικονομικό Πανεπιστήμιο Αθηνών

Τμήμα Πληροφορικής | ΠΜΣ σε Ασφάλεια & Ανάπτυξη Πληροφοριακών Συστημάτων [32]

Διάρκεια: 3-4 εξάμηνα (ΠΦ/ΜΦ[36])

Κατεύθυνση: *Κυβερνοασφάλεια & Προστασία Ψηφιακών Υποδομών*

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά & υποχρεωτικά κατεύθυνσης	Συστήματα Ανάλυσης & Διαχείρισης Μεγάλων Δεδομένων	Διοίκηση & Τεχνολογίες Κυβερνοασφάλειας
	Τεχνολογίες Ψηφιακών Υποδομών	Τεχνολογίες & Υπηρεσίες Διαδικτύου
	Ασφάλεια Λογισμικού & Δικτύων	Εφαρμοσμένη Κρυπτογραφία
	Προηγμένες Μέθοδοι Ανάπτυξης Λογισμικού	
Κατ' επιλογήν	Ψηφιακά Πειστήρια	Έλεγχος Ασφάλειας
	Δίκαιο Πληροφορίας	Ελεγκτική Πληροφοριακών Συστημάτων
	Αλυσίδες Καταχωρίσεων & Ευφυείς Συμβάσεις	Έλεγχος, Αξιοπιστία & Διασφάλιση Ποιότητας Λογισμικού
	Διοίκηση & Διαχείριση Έργων Πληροφορικής	Σεμινάρια: (α) Ψηφιακή Καινοτομία & Επιχειρηματικότητα, (β) Επικοινωνία & Επιχειρησιακό Περιβάλλον
Πρακτική Άσκηση	Ναι (μόνο το τμήμα ΠΦ)	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: http://mscis.cs.aueb.gr/

Πανεπιστήμιο Πειραιώς

Τμήμα Πληροφορικής | ΠΜΣ σε Κυβερνοασφάλεια και Επιστήμη Δεδομένων [33]

Διάρκεια: Τρία (3) εξάμηνα

Κατεύθυνση: *Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων* και *Ασφάλεια και Αξιοπιστία Υποδομών και Συστημάτων*

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά & υποχρεωτικά κατεύθυνσης	Ασφάλεια Δικτύων & Επικοινωνιών	Σχεδίαση Αρχιτεκτονικών Ασφάλειας
	Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων	Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων
	Αξιοπιστία Ενσωματωμένων Συστημάτων	Σχεδίαση Αξιόπιστων Συστημάτων & Κρίσιμων Υποδομών
	Ενσωματωμένα Συστήματα	Έλεγχος Εισβολών Δικτύων & Συστημάτων
	Ανάλυση Ψηφιακών Πειστηρίων	Ανάλυση Κακόβουλου Λογισμικού

[36] ΠΦ: Πλήρους Φοίτησης, ΜΦ: Μερικής Φοίτησης.

Κατηγορία μαθήματος	Ονομασία μαθήματος	
	Ασφάλεια Λογισμικού	Ασφάλεια Υλικού
Κατ' επιλογήν	Εφαρμοσμένη Κρυπτογραφία	Αναλυτική Γράφων & Δικτύων
	Ειδικά Θέματα Ασφάλειας & Ιδιωτικότητας	Προηγμένες Τεχνολογίες Κρυπτογραφίας & Ασφάλειας
	Ανάλυση Χρονοσειρών & Πρόβλεψη	
Πρακτική Άσκηση	Όχι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: https://cybersecdatasci.cs.unipi.gr

Τμήμα Ψηφιακών Συστημάτων | ΠΜΣ σε Ασφάλεια Ψηφιακών Συστημάτων [34]

Διάρκεια: Τρία (3) εξάμηνα

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά	Ασφάλεια Δικτύων	Εφαρμοσμένη Κρυπτογραφία
	Ασφάλεια Πληροφοριακών Συστημάτων & Προστασία Ιδιωτικότητας	Αποτίμηση Ασφάλειας & Εκμετάλλευση Αδυναμιών
	Ψηφιακή Εγκληματολογία & Ασφάλεια στον Παγκόσμιο Ιστό	Θεσμικό & Κανονιστικό Πλαίσιο Ασφάλειας
	Ασφάλεια στο Κινητό Διαδίκτυο	Ερευνητική Μεθοδολογία
Πρακτική Άσκηση	Όχι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: https://www.ds.unipi.gr/security/

Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων | ΠΜΣ σε Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων [35]

Διάρκεια: 3-6 εξάμηνα (ΠΦ/ΜΦ)

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά	Κρυπτογραφία	Ασφάλεια Συστημάτων Βάσεων Δεδομένων
	Θέματα Δικαίου Πληροφορίας	Ψηφιακή Εγκληματολογία
	Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο του Μέλλοντος	Ασφάλεια Δικτύων Υπολογιστών & Επικοινωνιών
	Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων	Ασφάλεια Ασύρματων & Κινητών Δικτύων Επικοινωνιών
Πρακτική Άσκηση	Όχι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: https://msc.icsd.aegean.gr/masters/security/

Πανεπιστήμιο Δυτικής Αττικής

Τμήμα Μηχανικών Πληροφορικής & Υπολογιστών | ΠΜΣ σε Κυβερνοασφάλεια [36]

Διάρκεια: Τρία (3) εξάμηνα

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά	Εφαρμοσμένη Κρυπτογραφία	Ασφάλεια Υλικού
	Ασφάλεια Πληροφοριακών Συστημάτων	Ασφάλεια Πληροφορίας και Τεχνολογίες Αλυσίδας Συστοιχιών
	Ασφάλεια Δικτύων	Ψηφιακή Εγκληματολογία
	Κανόνες & Πρωτόκολλα Κυβερνοασφάλειας	Ασφάλεια Λογισμικού & Βάσεων Δεδομένων
Πρακτική Άσκηση	Όχι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: http://www.ice.uniwa.gr/education/postgraduate/cybersecurity/

Παρέχει: *Μεταπτυχιακό Δίπλωμα Εξειδίκευσης σε Κυβερνοασφάλεια*

Διεθνές Πανεπιστήμιο της Ελλάδος

Σχολή Επιστήμης & Τεχνολογίας | ΠΜΣ σε Κυβερνοασφάλεια [37]

Διάρκεια: 3-5 εξάμηνα (ΠΦ/ΜΦ)

Κατηγορία μαθήματος	Ονομασία μαθήματος	
Υποχρεωτικά	Προστασία Δεδομένων & Κρυπτογραφία	Νομικές & Ηθικές Θεμελιώσεις Ιδιωτικότητας & Ασφάλειας
	Ασφάλεια Πληροφοριακών Συστημάτων	Κυβερνοέγκλημα & Διαχείριση Περιστατικών
	Δίκτυα Υπολογιστών	Ψηφιακά Πειστήρια
	Ασύρματες Επικοινωνίες & Δίκτυα	Ανίχνευση & Διαχείριση Γεγονότων
Κατ' επιλογήν	Έλεγχος Ασφάλειας & Ανάλυση Ιομορφικού Λογισμικού	Διαχείριση Γνώσης στον Παγκόσμιο Ιστό
	Διαδίκτυο των Πραγμάτων	Ανάπτυξη Λογισμικού
Πρακτική Άσκηση	Όχι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: https://www.eduguide.gr/grad/prokiryksi/diethnes-panepistimio-msc-communications-cybersecurity,569

Παρέχει: *Μεταπτυχιακό Δίπλωμα Εξειδίκευσης σε Κυβερνοασφάλεια*

Παράρτημα ΙΙ: ΕΛΛΑΔΑ – Διδακτορικά Διπλώματα (2021-23)

#	Θέμα διατριβής (GR) [22]	Θέμα διατριβής (EN)	Πανεπιστήμιο	Έτος
1	Πλαίσιο κουλτούρας κυβερνοασφάλειας με πρακτική εφαρμογή σε κρίσιμες υποδομές	Cyber security culture framework applied to critical infrastructures	Εθνικό Μετσόβιο Πολυτεχνείο	2023
2	Ασφάλεια και ανθεκτικότητα κυβερνοφυσικών διαδικασιών σε κρίσιμες ψηφιακές υποδομές	Increasing security and resilience in cyber-physical processes of critical infrastructures	Οικονομικό Πανεπιστήμιο Αθηνών	
3	Ασφάλεια και προστασία της ιδιωτικότητας κατά τον κοινωνικό σχεδιασμό πληροφοριακών συστημάτων με έμφαση σε ψηφιακή ταυτότητα και σε γεωεντοπισμό	Security and privacy in social software engineering, focusing on digital identity and geolocation	Πανεπιστήμιο Αιγαίου	
4	Ασφάλεια και προστασία υπεράκτιων εγκαταστάσεων πετρελαίου και φυσικού αερίου	Security for offshore oil and gas assets		
5	Ζητήματα προστασίας της ανωνυμίας τελικού χρήστη σε υπηρεσίες VoIP	Protecting user anonymity in VoIP services		
6	Συμπεριφορικές βιομετρικές μέθοδοι για συνεχή αυθεντικοποίηση: ζητήματα ασφάλειας και ιδιωτικότητας	Behavioral biometrics for continuous authentication: security and privacy issues		
7	Ψηφιακή εγκληματολογία στο υπολογιστικό νέφος	Cloud computing forensics		
8	Ασφαλής διαχείριση πόρων σε δίκτυα νέας γενιάς	Secure resource management in next generation networks (NGNs)	Πανεπιστήμιο Δυτικής Αττικής	
9	Ασφάλεια και ιδιωτικότητα στο διαδίκτυο των πραγμάτων	Security and privacy in the internet of things	Πανεπιστήμιο Δυτικής Μακεδονίας	
10	Μετριασμός των επιθέσεων στον κυβερνοχώρο σε φορητές συσκευές	Mitigation of cyberattacks in wearable devices	Πανεπιστήμιο Κρήτης	
11	Αναγνώριση επιθέσεων κοινωνικής μηχανικής βασισμένων σε συνομιλίες με χρήση τεχνικών βαθιάς μάθησης και επεξεργασίας φυσικής γλώσσας προς επίγνωση της κατάστασης κυβερνοασφάλειας	Utilizing deep learning and natural language processing to recognize chat-based social engineering attacks for cyber security situational awareness	Πανεπιστήμιο Μακεδονίας	
12	Ασφάλεια υπηρεσιών ευφυών μεταφορών: μοντελοποίηση και αξιολόγηση	Security of intelligent transportation services: modelling and assessment	Πανεπιστήμιο Πειραιώς	

#	Θέμα διατριβής (GR) [22]	Θέμα διατριβής (EN)	Πανεπιστήμιο	Έτος
13	Σχεδιασμός και υλοποίηση μεθοδολογιών τεχνητής νοημοσύνης για την ανίχνευση κυβερνοεπιθέσεων	Implementing ai-driven methodologies for cyberattack detection	Πανεπιστήμιο Πειραιώς	2023
14	Ψηφιακή εγκληματολογία στο διαδίκτυο των πραγμάτων	Iot forensics		
15	Ασφάλεια ενεργειακών υποδομών	Energy infrastructure security	Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	2022
16	Ασφαλής επικοινωνία πολλαπλών χρηστών με χρήση μεθόδων της θεωρίας πληροφορίας και κωδικοποίησης	Secure multi-user communications: an information-theoretic and coding approach	Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών	
17	Κινητά αδόμητα δίκτυα (MANET): διαχείριση εμπιστοσύνης - μηχανισμοί ασφαλείας	Mobile ad-hoc networks (MANET): trust management - security mechanisms		
18	Συστηματικός σχεδιασμός, ανάπτυξη και αξιολόγηση παιχνιδοποιημένων περιβαλλόντων εκμάθησης στην κυβερνοασφάλεια	Systematic design, deployment and evaluation of gamified cybersecurity learning environments	Ιόνιο Πανεπιστήμιο	
19	Νέοι αλγόριθμοι, μοντέλα και αρχιτεκτονικές για βελτιωμένη ασφάλεια στον κυβερνοχώρο και ενεργειακή απόδοση σε περιβάλλοντα διαδικτύου των πραγμάτων	Novel algorithms, models and architectures for enhanced cyber security and energy efficiency in Internet of Things environments	Πανεπιστήμιο Μακεδονίας	
20	Μεθοδολογίες ελέγχου ιδιωτικότητας και ασφάλειας σε ηλεκτρονικά παρεχόμενες υπηρεσίες	Privacy and security audit methodologies in electronically provided services	Πανεπιστήμιο Πειραιώς	
21	Παρακολούθηση ανοιχτού χώρου με ασύρματο δίκτυο αισθητηρίων σε εφαρμογές ασφαλείας	Wireless sensor network monitoring for intruder detection in open areas	Δημοκρίτειο Πανεπιστήμιο Θράκης	2021
22	Ανάπτυξη ανθεκτικότητας και κυβερνοφυσικών δυνατοτήτων προστασίας κρίσιμων ψηφιακών υποδομών αεροπλοΐας	Developing resilience and cyber physical protection capabilities for critical aviation infrastructures	Οικονομικό Πανεπιστήμιο Αθηνών	
23	Διαφύλαξη ιδιωτικότητας κατά την εξόρυξη δεδομένων	Privacy preserving data mining	Πανεπιστήμιο Αιγαίου	
24	Ψηφιακά κυκλώματα και συστήματα για ενίσχυση της ασφάλειας σε έξυπνες συσκευές διασυνδεδεμένες στο διαδίκτυο	Digital circuits and systems to enhance security in smart devices connected to the internet	Πανεπιστήμιο Θεσσαλίας.	
25	Αποτελεσματικοί και ασφαλείς αλγόριθμοι για χειρισμό, επεξεργασία και μεταφορά Big Data στο Cloud Computing για δίκτυα του Διαδικτύου των Πραγμάτων	Efficient and secure algorithms for big data handling, processing, and delivery in cloud computing for Internet of Things networks	Πανεπιστήμιο Μακεδονίας	

#	Θέμα διατριβής (GR) [22]	Θέμα διατριβής (EN)	Πανεπιστήμιο	Έτος
26	Δικτυακός έλεγχος και ασφάλεια νέας γενιάς για το διαδίκτυο των πραγμάτων	Next-generation network control and security for the internet of things	Πανεπιστήμιο Μακεδονίας	2021
27	Εκπαίδευση στην κυβερνοασφάλεια βασισμένη σε ψηφιακά παιχνίδια	Cyber security game-based training		
28	Ασφάλεια και απόρρητο χρηστών και υποδομών με γνώμονα την συμμόρφωση	User and infrastructure security and privacy with regard to compliance	Πανεπιστήμιο Πειραιώς	
29	Εφαρμογές της κρυπτογραφίας βάσει ταυτότητας στην ηλεκτρονική διακυβέρνηση και στη ναυσιπλοΐα	Applications of identity-based cryptography (ibc) in maritime and e-governance sectors		
30	Κυβερνο-ασφάλεια ανθρώπινος παράγοντας ναυτιλία	Cyber security Human Factor Maritime		
31	Μηχανισμοί ενίσχυσης της ασφάλειας και της ιδιωτικότητας στο λειτουργικό σύστημα android	Security and privacy enhancing mechanisms for the android operating system		

Παράρτημα ΙΙΙ: Κολλέγια - Χαρακτηριστικά ΠΠΣ και ΠΜΣ

Metropolitan College

B.Sc. Cyber Security & Networks [38]

Διάρκεια: 3 έτη (ΠΦ)

Ονομασία μαθήματος		
Ανάπτυξη Λογισμικού	Υπολογιστικά Συστήματα και Δίκτυα	Τεχνολογίες Διαδικτύου
Μαθηματικά Πληροφορικής	Σχεδίαση και Μοντελοποίηση Υπολογιστικών Συστημάτων	Επικοινωνίες Δεδομένων & Δίκτυα Υπολογιστών
Βάσεις Δεδομένων	Διαχείριση Συστημάτων	Διαχείριση Έργου
Κυβερνοασφάλεια	Στρατηγική και Διοίκηση Πληροφοριακών Συστημάτων	Πρακτικά Θέματα Πληροφορικής
Σχεδιασμός Αδιάλειπτης Επιχειρηματικής Λειτουργίας	Επιχειρησιακή Αρχιτεκτονική & Προγραμματισμός Υπολογιστικού Νέφους	Προηγμένα Θέματα Κυβερνοασφάλειας και Δικτύων Υπολογιστών
Πτυχιακή Εργασία	Ναι	
Πρακτική Άσκηση	Ναι	

Ιστότοπος: https://www.mitropolitiko.edu.gr/programmata-spoydon/scholi-pliroforikis/bsc-hons-cyber-security-and-networks/

New York College

B.Sc. Cybersecurity [39]

Διάρκεια: 3-4 έτη (ΠΦ)

Κατηγορία μαθήματος	**Ονομασία μαθήματος**	
Κορμού	Ακαδημαϊκές Γλωσσικές Δεξιότητες 1	Ακαδημαϊκές Γλωσσικές Δεξιότητες 2
	Βασικές Αρχές Συστημάτων Linux	Εισαγωγή στην Ανάπτυξη Λογισμικού
	Εισαγωγή στην Δικτύωση Υπολογιστών	Δομές Δεδομένων και Αλγόριθμοι
	Βασικές Αρχές Ασφάλειας	Θεμελιώδεις Αρχές Προγραμματισμού
	Αντικειμενοστρεφής Προγραμματισμός	Λογική Ανάλυση & Επίλυση Προβλημάτων
	Σχεδιασμός Βάσεων Δεδομένων	Δίκτυα και Υλικό Η/Υ
	Ανάπτυξη Συστημάτων με Ευέλικτες (Agile) Μεθόδους	Εισαγωγή στις Τεχνολογίες Ψηφιακής Διασκέδασης
Κατεύθυνσης	Ασφάλεια Πληροφορικής	Ανάλυση Σύγχρονων Προβλημάτων
	Εταιρική Υποδομή	Ηθικό Χάκινγκ και Κυβερνοεγκλήματα
	Προηγμένα Συστήματα Linux	Ασφάλεια Cloud και Τοπικών Δικτύων
	Ανάπτυξη Ασφαλών Εφαρμογών	Διαμόρφωση & Διαχείριση Εφαρμογών Διακομιστή
Πρακτική Άσκηση	Ναι	
Πτυχιακή Εργασία	Ναι	

Ιστότοπος: https://www.nyc.gr/tmimata-spoudon-nyc/spoudes-kyvernoasfaleias/bsc-hons-computing-application-development#undefined1

The American College of Greece

B.Sc. Cybersecurity & Networks [40]

Διάρκεια: 3 έτη (ΠΦ)

Κατηγορία μαθήματος	**Ονομασία μαθήματος**	
Υποχρεωτικά κατεύθυνσης	Business Information Systems	Mathematics for Computing
	Computer Networks & Cybersecurity Fundamentals	Cybersecurity & Networks Capstone Project
	Introduction to Programming	Fundamentals of RDBMS
	Principles of Wireless, IoT & Mobile Networks	Computer Networks, Modeling & Analysis
	Computer System Architecture	Network Administration
	Operating Systems Concepts	Cryptography & Network Security
	Object Oriented Programming Techniques	Security of Wireless, IoT & Mobile Networks
	Methods in ICT Project Research & Management	Intrusion Detection & Incident Response
	Internet Programming	Secure Software Development
	Digital Forensics	Ethical Hacking & Penetration Testing
	Distributed Systems	Privacy, Policy, Law & Technology
Επιλογές κατεύθυνσης	Information Systems Security & Control	Web Science & Social Media Platform Analytics
	Data Mining & Big Data	Edge Computing
Πτυχιακή Εργασία	Ναι	
Πρακτική Άσκηση	Ναι	

Ιστότοπος: https://www.acg.edu/undergraduate/undergraduate-programs/school-of-liberal-arts-sciences/liberal-arts-sciences-majors/cybersecurity-and-networks/

Epsilon College

B.Sc. Web Development & Cyber Security [41]

Διάρκεια: 3 έτη (ΠΦ)

Ονομασία μαθήματος		
Επίλυση Προβλημάτων & Προγραμματισμός	Θεμελιώδεις έννοιες Μηχανικής Λογισμικού	Αντικειμενοστραφείς Σχεσιακές Βάσεις Δεδομένων
Σχεδίαση και Ανάπτυξη Βάσεων Δεδομένων	Ηθικό Hacking και Δοκιμές Παρείσδυσης	Διαχείριση Κυβερνοασφάλειας
Υπολογιστικά Συστήματα	Διαχείριση Εξυπηρετητών και Ασφάλεια	Σύγχρονες Βάσεις Δεδομένων
Επικοινωνίες Υπολογιστών	Προγραμματισμός Διαδικτύου	Πληροφορική Κινητών Συσκευών

Ονομασία μαθήματος		
Ανάπτυξη Λογισμικού Διαδικτύου	Ανάπτυξη Εφαρμογών Κινητών Συσκευών	Κυβερνοασφάλεια και Εφαρμοσμένη Κρυπτογραφία
Πτυχιακή Εργασία	Ναι	
Πρακτική Άσκηση	Ναι	

Ιστότοπος: https://epsiloncollege.gr/spoudes/bachelors/bsc-hons-in-web-development-cyber-security/

BCA College

M.Sc. Maritime Cybersecurity [42]

Διάρκεια: 1-2 έτη (ΠΦ/ΜΦ)

Ονομασία μαθήματος	
Introduction to Cybersecurity Principles & Concepts	Maritime Cybersecurity Management Systems
Maritime Cybersecurity Regulations & Best Practices	Maritime Cybersecurity Reviews, Assessments, Audits
Digitalisation of Shipping	Advanced Topics in Applied Cybersecurity
Διπλωματική Εργασία	Ναι

Ιστότοπος: https://www.bca.edu.gr/master-degrees/shipping-transport-logistics-department/msc-maritime-cybersecurity/

BCA College

MSc Applied Cyber Security [43]

Διάρκεια: 1-2 έτη (ΠΦ/ΜΦ)

Ονομασία μαθήματος	
Systems Security & Defence	Principles of IT Law & Legislation
Network Security & Defence	Applied Digital Forensics
Security Management & Standards	Advanced Topics in Applied Cybersecurity
Διπλωματική Εργασία	Ναι

Ιστότοπος: https://www.bca.edu.gr/master-degrees/business-department/msc-applied-cybersecurity/

Aegean College

M.Sc. Cyber Security [44]

Διάρκεια: 2 έτη (ΜΦ)

Κατηγορία μαθήματος	**Ονομασία μαθήματος**	
Υποχρεωτικά	Ασφάλεια Υπολογιστών & Ασύρματων Δικτύων	Νομοθεσία της Πληροφορίας
	Διακυβέρνηση Ασφάλειας	Κρυπτογραφία
	Ασφάλεια Βάσεων Δεδομένων και Διαχείριση Μεγάλων Δεδομένων	Δοκιμή Διείσδυσης σε Πληροφοριακά Συστήματα & Ηθικό Hacking

Κατηγορία μαθήματος	**Ονομασία μαθήματος**	
Υποχρεωτικά κατεύθυνσης	Ψηφιακή Εγκληματολογία	Εφαρμοσμένη Κρυπτογραφία
	Ανάλυση Κακόβουλου Λογισμικού	Τεχνολογία Blockchain & εφαρμογές
Πρακτική Άσκηση	Ναι	
Διπλωματική Εργασία	Ναι	

Ιστότοπος: https://aegeancollege.gr/programma/msc-cybersecurity/

Metropolitan College

M.Sc. Information Security & Digital Forensics [45]

Διάρκεια: 1 έτος (ΠΦ) ή 1-2 έτη (ΠΦ/ΜΦ)

Ονομασία μαθήματος	
Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων	Νομοθεσία Τεχνολογίας Πληροφοριών & Διαδικτύου
Ασφάλεια Υπολογιστών	Ψηφιακή Εγκληματολογία
Διπλωματική Εργασία	Ναι
Πρακτική Άσκηση	Ναι

Ιστότοπος: https://www.mitropolitiko.edu.gr/programmata-spoydon/scholi-pliroforikis/msc-information-security-and-digital-forensics/

Παράρτημα IV: Κέντρα Δια Βίου Μάθησης - Χαρακτηριστικά

Πανεπιστήμιο Μακεδονίας

Cisco Certified Network Associate v7 & CyberOps Associate [23]

Διάρκεια (ώρες): 312

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Introduction to Networks // 80 ώρες	Enterprise Networking, Security, and Automation // 80 ώρες
Switching, Routing, and Wireless Essentials // 80 ώρες	Cyber Operations Associate // 72 ώρες

Ιστότοπος: https://kedivim.uom.gr/member/mavridis_ioannis/

Πανεπιστήμιο Πατρών

Ασφάλεια Δεδομένων – Κυβερνοασφάλεια [24]

Διάρκεια (ώρες): 200

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Θ.Ε. 1: Εισαγωγικές Έννοιες Ασφάλειας	Θ.Ε. 5: Ασφαλής Χρήση του Ιστού
Θ.Ε. 2: Λογισμικό Κακόβουλης Χρήσης	Θ.Ε. 6: Επικοινωνίες
Θ.Ε. 3: Ασφάλεια Δικτύου	Θ.Ε. 7: Ασφαλής Διαχείριση Δεδομένων
Θ.Ε. 4: Έλεγχος Πρόσβασης	Θ.Ε. 8: Νομικό Πλαίσιο Κυβερνοασφάλειας

Ιστότοπος: https://kedivim.upatras.gr/cooperatedcourse/asfaleia-dedomenon-kyvernoasfaleia/

Πανεπιστήμιο Θεσσαλίας

Cisco Certified CyberOps Associate – Κυβερνοασφάλεια [25]

Διάρκεια (ώρες): 176

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Threat Actors and Defenders	Threats and Attacks
Operating System Overview	Network Defense
Network Fundamentals	Cryptography and Endpoint Protection
Network Infrastructure Security	Protocols and Log Files
Analyzing Security Data	

Ιστότοπος: https://learning.uth.gr/cybersecurity/

Πανεπιστήμιο Δυτικής Μακεδονίας

Ειδικός Πληροφορικής Προστασίας Δεδομένων – Κυβερνοασφάλεια [26]

Διάρκεια (ώρες): 80

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Προστασία Δεδομένων Προσωπικού Χαρακτήρα – Κυβερνοασφάλεια // Ώρες Διδασκαλίας: 60	Προστασία Δεδομένων Προσωπικού Χαρακτήρα Και της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών // Ώρες Διδασκαλίας: 20

Ιστότοπος: https://kedivim.uowm.gr/course/eidikos-pliroforikis-se-themata-prostasias-dedomenon-gdpr-kyvernoasfaleia/

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Κυβερνοέγκλημα & Κυβερνοασφάλεια [29]

Διάρκεια (ώρες): 45

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Ενότητα 1: Εισαγωγή και τεχνική περιγραφή	Ενότητα 6: Δικονομικό Ποινικό Δίκαιο
Ενότητα 2: Γνήσια Κυβερνοεγκλήματα	Ενότητα 7: Ειδικές ανακριτικές πράξεις και Κυβερνοασφάλεια
Ενότητα 3: Εγκλήματα κατά της σεξουαλικής ελευθερίας και ανηλικότητας, τελούμενα μέσω Διαδικτύου	Ενότητα 8: Πολιτικές Κυβερνοασφάλειας
Ενότητα 4: Εγκλήματα σχετικά με τα προσωπικά δεδομένα και το Διαδίκτυο	Ενότητα 9: Απόρρητο και Κυβερνοασφάλεια
Ενότητα 5: Δικαστική και Αστυνομική Συνεργασία και Συνδρομή	

Ιστότοπος: https://kedivim.auth.gr/programs/kyvernoeglima/

Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών

Συστήματα Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια [27]

Διάρκεια (ώρες): 60

Θεματικές Ενότητες Εκπαιδευτικού Προγράμματος	
Εισαγωγή στην Κυβερνοασφάλεια και σε Συστήματα Τεχνητής Νοημοσύνης	Συστήματα Τεχνητής Νοημοσύνης στην Ανίχνευση και Πρόληψη Εισβολών
Ευφυείς Τεχνικές στην Κυβερνοασφάλεια και Ανάλυση - Επεξεργασία Κυβερνογνώσης	Προηγμένα Θέματα Τεχνητής Νοημοσύνης και Πρακτική Εφαρμογή

Ιστότοπος: https://elearningekpa.gr/courses/sustimata-texnitis-noimosunis-stin-kubernoasfaleia

Παράρτημα V: ΕΛΛΑΔΑ - Αποτελέσματα έρευνας για τη ζήτηση δεξιοτήτων κυβερνοασφάλειας

Μέρος 1: Χαρακτηριστικά δείγματος της έρευνας

	ΕΛΛΑΔΑ
Α.4. Σε ποια κατηγορία ανήκει ο οργανισμός σας;	
Οργανισμός/πάροχος κυβερνοασφάλειας.	**21**
Οργανισμός ΤΠΕ με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας.	**21**
Ιδιωτικός οργανισμός με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας σε άλλο τομέα.	**28**
Δημόσιος οργανισμός με ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας.	**18**
Οργανισμός χωρίς ανάγκη για εσωτερικούς επαγγελματίες κυβερνοασφάλειας.	**16**
Ακαδημαϊκή κοινότητα.	**25**
Άλλο.	**10**
Σύνολο	**139**

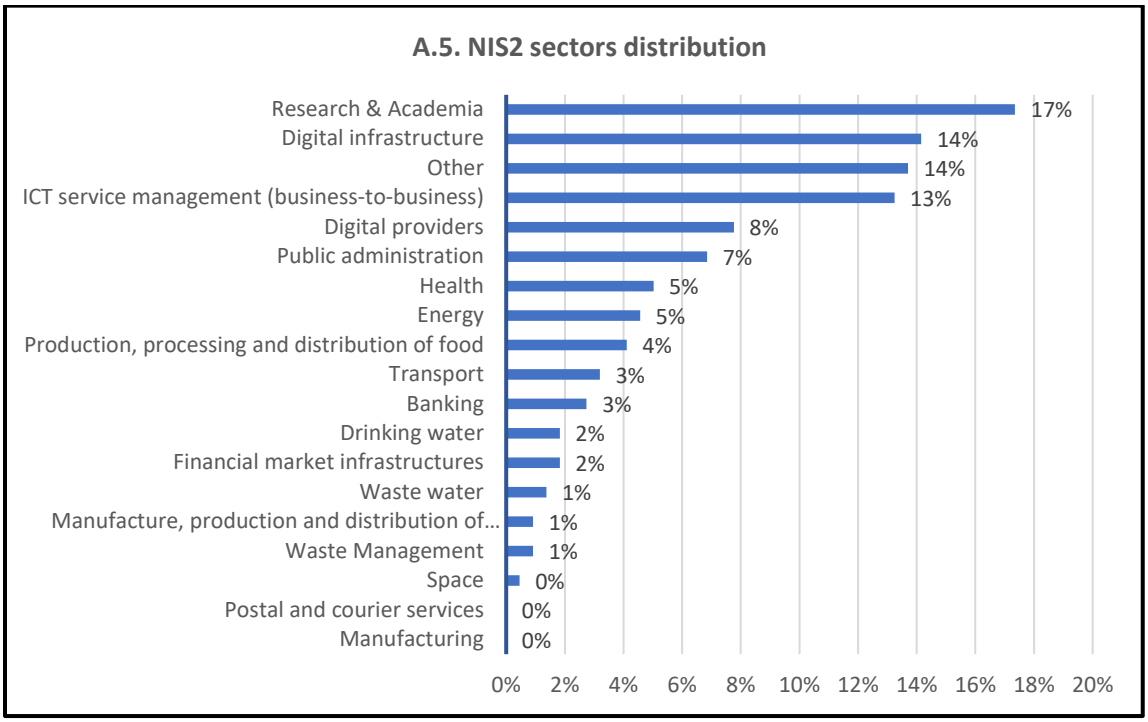
Πίνακας 15 (ερώτηση Α.4): Κατηγορία του οργανισμού

	ΕΛΛΑΔΑ
Α.4.1. Ποια είναι η κύρια ψηφιακή υπηρεσία που παρέχει ο οργανισμός σας;	
Διαδικτυακές αγορές	1
Ηλεκτρονική μηχανή αναζήτησης	0
Πλατφόρμα υπηρεσιών κοινωνικής δικτύωσης	0
Άλλες δραστηριότητες ψηφιακών υπηρεσιών/ΤΠΕ	20
Καμία απάντηση	118
Σύνολο	**139**

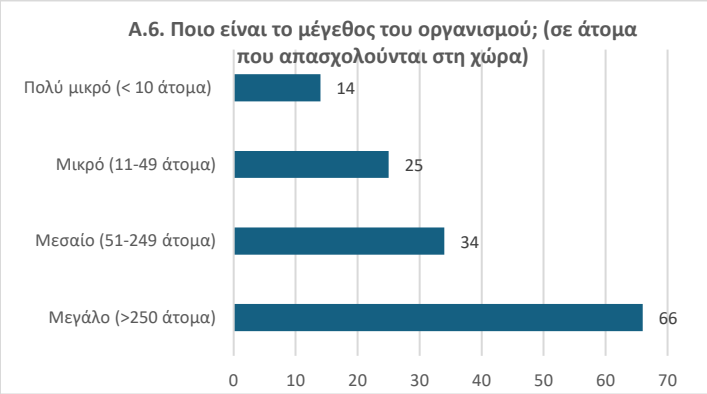
Πίνακας 16 (ερώτηση Α.4.1): Τύπος ψηφιακής υπηρεσίας του οργανισμού

ΕΛΛΑΔΑ		**Α.5:** Σε ποιον τομέα δραστηριοποιείται η οργάνωσή σας;	
Τομέας (ταξινόμηση NIS2)	**#**	**Τομέας** (ταξινόμηση NIS2)	**#**
1 Ενέργεια	8	**10** Υγρά απόβλητα	14
2 Υποδομές χρηματοπιστωτικών αγορών	13	**11** Ψηφιακές υποδομές	2
3 Υγεία	7	**12** Διαχείριση υπηρεσιών ΤΠΕ (B2B)	4
4 Μεταποίηση	19	**13** Διάστημα	17
5 Δημόσια διοίκηση	6	**14** Ταχυδρομικές και ταχυμεταφορικές υπηρεσίες	18
6 Μεταφορές	10	**15** Κατασκευή, παραγωγή & διανομή χημικών προϊόντων	15
7 Διαχείριση αποβλήτων	16	**16** Παραγωγή, μεταποίηση & διανομή τροφίμων	9
8 Τραπεζικές υπηρεσίες	11	**17** Ψηφιακοί πάροχοι	5
9 Πόσιμο νερό	12	**18** Έρευνα & ακαδημαϊκή κοινότητα	1
		19 Άλλο	3

Πίνακας 17 (ερώτηση Α.5): Τομέας του οργανισμού



	ΕΛΛΑΔΑ
Α.6: Ποιο είναι το μέγεθος του οργανισμού; (σε άτομα που απασχολούνται στη χώρα)	
Μεγάλο (>250 άτομα)	66
Μεσαίο (51-249 άτομα)	34
Μικρό (11-49 άτομα)	25
Πολύ μικρό (< 10 άτομα)	14
Total	**139**

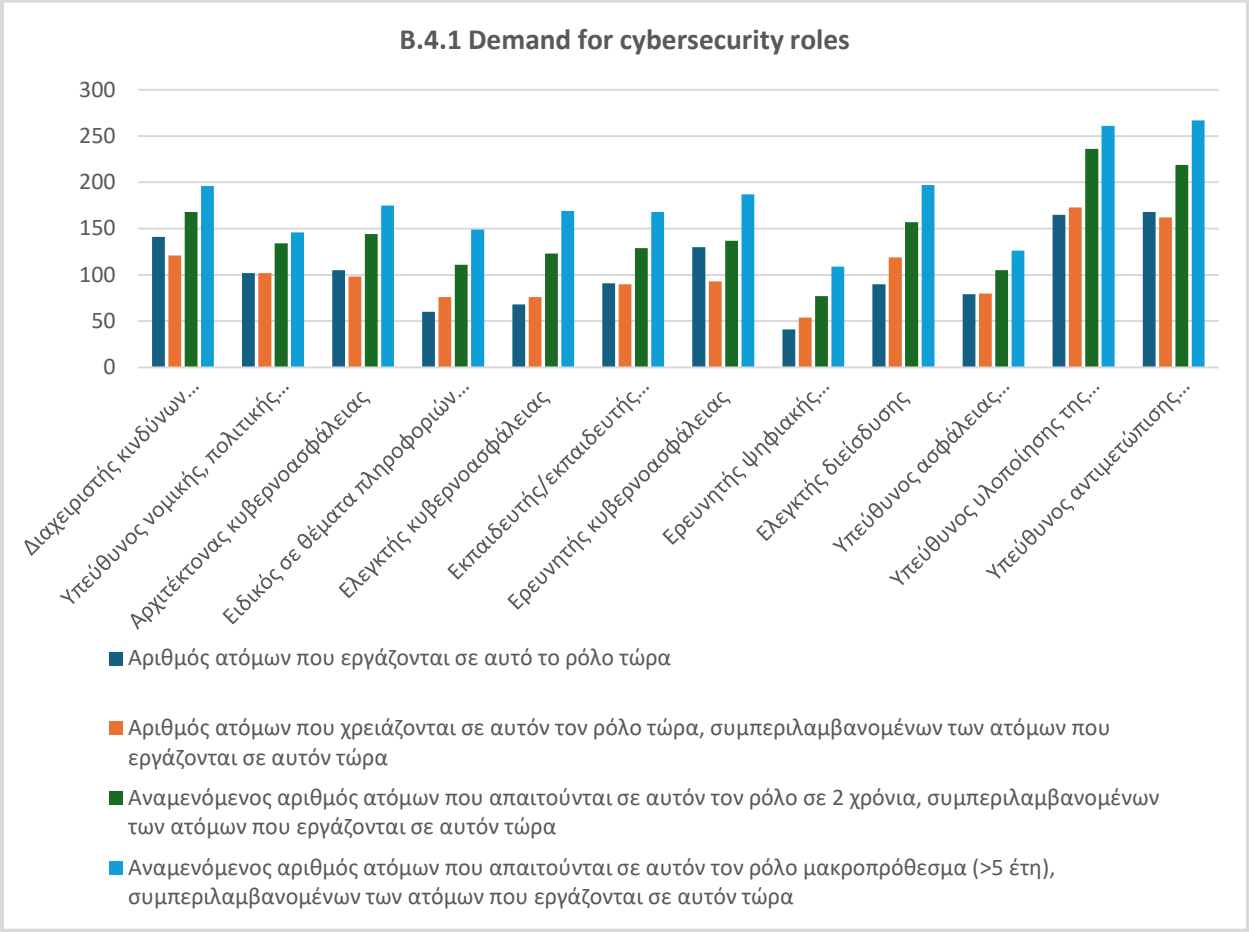


Πίνακας 18 (ερώτηση Α.6): Μέγεθος του οργανισμού

Μέρος 2: Αποτελέσματα της έρευνας

	ΕΛΛΑΔΑ	**Β.4.1**: Ζήτηση για ρόλους κυβερνοασφάλειας [37]			
Ρόλοι κυβερνοασφάλειας	Αριθμός ατόμων που εργάζονται σε αυτό το ρόλο τώρα	Αριθμός ατόμων που χρειάζονται σε αυτόν τον ρόλο τώρα, συμπεριλαμβανομένων των ατόμων που εργάζονται σε αυτόν τώρα	Αναμενόμενος αριθμός ατόμων που απαιτούνται σε αυτόν τον ρόλο σε 2 χρόνια, συμπεριλαμβανομένων των ατόμων που εργάζονται σε αυτόν τώρα	Αναμενόμενος αριθμός ατόμων που απαιτούνται σε αυτόν τον ρόλο μακροπρόθεσμα (>5 έτη), συμπεριλαμβανομένων των ατόμων που εργάζονται σε αυτόν τώρα
Cybersecurity Risk Manager	141	121	168	196
Cyber Legal, Policy & Compliance Officer	102	102	134	146
Cybersecurity Architect	105	98	144	175
Cyber Threat Intelligence Specialist	60	76	111	149
Cybersecurity Auditor	68	76	123	169
Cybersecurity Educator/ Trainer	91	90	129	168
Cybersecurity Researcher	130	93	137	187
Digital Forensics Investigator	41	54	77	109
Penetration Tester	90	119	157	197
Chief Information Security Officer (CISO)	79	80	105	126
Cybersecurity Implementer	165	173	236	261
Cyber Incident Responder	168	162	219	267

[37] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



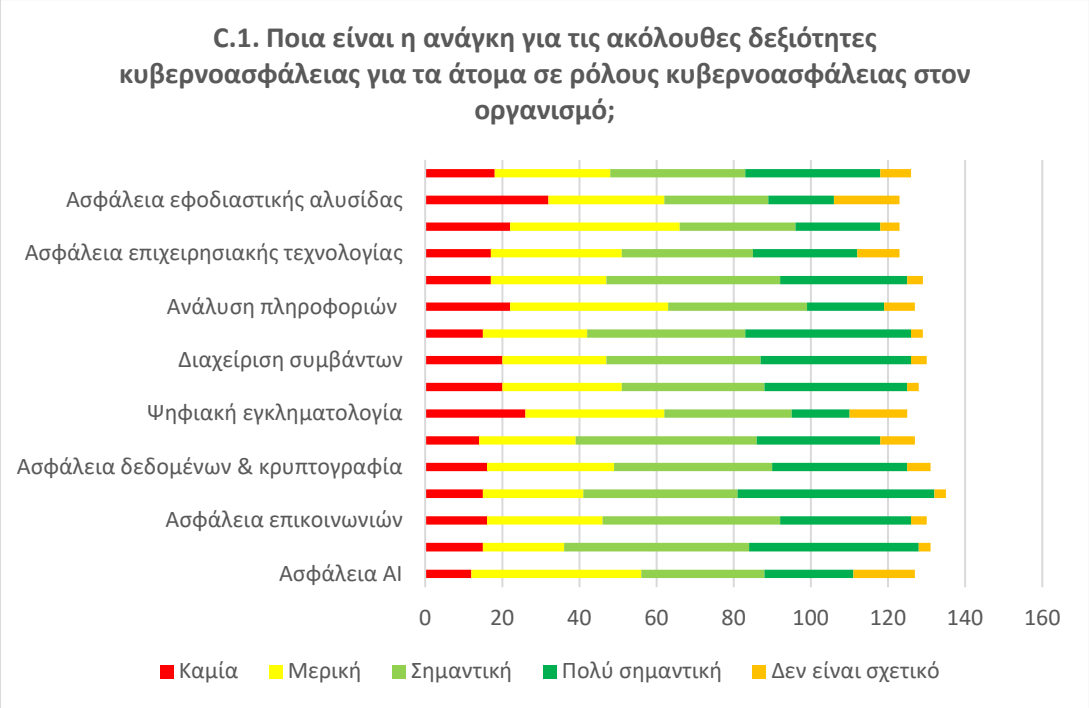
	ΕΛΛΑΔΑ
B.5: Έχετε κάποιον άλλο ρόλο στον οργανισμό σας που απαιτεί δεξιότητες κυβερνοασφάλειας, αλλά δεν μπορεί να κατηγοριοποιηθεί στους 12 παραπάνω ρόλους;	
Ναι	11
Όχι	121
Σύνολο	**132**

Πίνακας 21 (ερώτηση B.5): Άλλοι ρόλοι που απαιτούν δεξιότητες κυβερνοασφάλειας

ΕΛΛΑΔΑ	**C.1**: Ποια είναι η ανάγκη για τις ακόλουθες δεξιότητες κυβερνοασφάλειας για τα άτομα σε ρόλους κυβερνοασφάλειας στον οργανισμό;[38]				
Δεξιότητες κυβερνοασφάλειας	**Καμία**	**Μερική**	**Σημαντική**	**Πολύ σημαντική**	**Δεν είναι σχετικό**
Ασφάλεια στην Τεχνητή Νοημοσύνη (AI Security)	12	44	32	23	16
Ασφάλεια Υπολογιστικού Νέφους (Cloud Security)	15	21	48	44	3
Ασφάλεια Επικοινωνιών (Communications Security)	16	30	46	34	4
Προστασία Δεδομένων (Data Privacy)	15	26	40	51	3
Κρυπτογράφηση και ασφάλεια δεδομένων (Data Security & Cryptography)	16	33	41	35	6
Συνδυασμός Πρακτικών Ανάπτυξης Ασφάλειας και Λειτουργιών (DevSecOps)	14	25	47	32	9
Ψηφιακά Πειστήρια (Digital Forensics)	26	36	33	15	15
Έλεγχος Πρόσβασης/Διαχείριση Ταυτότητας (Access Controls/ Identity Management)	20	31	37	37	3
Διαχείριση περιστατικών (Incident Management)	20	27	40	39	4
Information Systems & Network Security/ Cyber Resiliency *(Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων/ Ανθεκτικότητα στον Κυβερνοχώρο)*	15	27	41	43	3
Intelligence Analysis *(Ανάλυση Πληροφοριών)*	22	41	36	20	8
Ασφάλεια Λειτουργικών Συστημάτων (Operating Systems (OS) Security)	17	30	45	33	4
Ασφάλεια Επιχειρησιακής τεχνολογίας (Operational Technology Security)	17	34	34	27	11
Ασφάλεια Φυσικών Συσκευών (Physical Device Security)	22	44	30	22	5
Ασφάλεια Εφοδιαστικής Αλυσίδας (Supply Chain Security)	32	30	27	17	17
Ανάλυση απειλών (Threat Analysis)	18	30	35	35	8

Πίνακας 23 (ερώτηση C.1): Ανάγκη για δεξιότητες κυβερνοασφάλειας στον οργανισμό

[38] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



	ΕΛΛΑΔΑ
C.2: Υπάρχουν άλλες τυπικές δεξιότητες κυβερνοασφάλειας που απαιτούνται ή χρησιμοποιούνται ήδη στον οργανισμό σας και δεν περιλαμβάνονται στον παραπάνω κατάλογο;	
Ναι	6
Όχι	124
Σύνολο	**130**

Πίνακας 26 (ερώτηση C.2): Πρόσθετες δεξιότητες κυβερνοασφάλειας

	ΕΛΛΑΔΑ

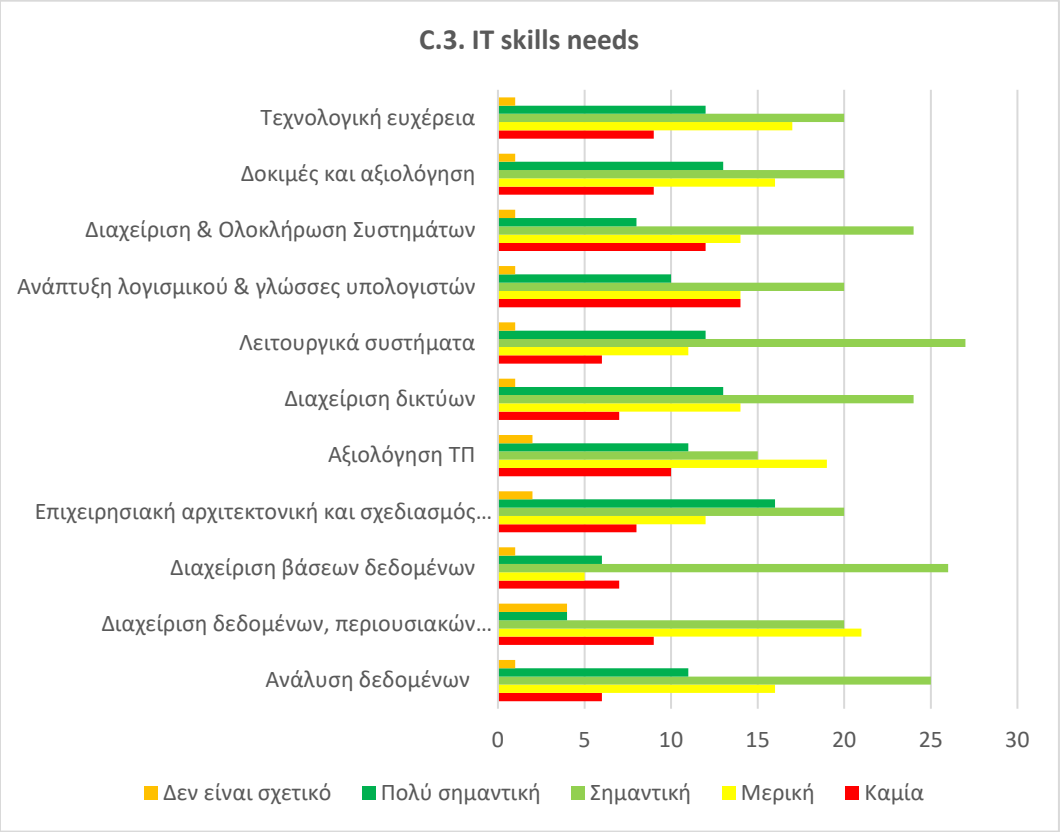
C.2.1: Ποιες είναι άλλες δεξιότητες κυβερνοασφάλειας για άτομα σε ρόλους κυβερνοασφάλειας; Και πόσο μεγάλη είναι η ανάγκη;	
Ανάλυση κακόβουλου λογισμικού	1
Σχεδιασμός ασφαλούς διαδικασίας	1
Αναλυτές SOC	1
Έλεγχος ασφάλειας πληροφορικής ή πληροφοριών	1
Total	**4**

Πίνακας 27 (ερώτηση C.2.1): Πρόσθετες δεξιότητες κυβερνοασφάλειας για άτομα σε ρόλους κυβερνοασφάλειας

ΕΛΛΑΔΑ	**C.3:** Ποια είναι η ανάγκη για τις ακόλουθες δεξιότητες που σχετίζονται με την πληροφορική για τα άτομα σε ρόλους κυβερνοασφάλειας στον οργανισμό;[39]				
IT-related Skills	**Καμία**	**Μερική**	**Σημαντική**	**Πολύ σημαντική**	**Δεν είναι σχετικό**
Ανάλυση δεδομένων	6	16	25	11	1
Διαχείριση δεδομένων, περιουσιακών στοιχείων και απογραφών	9	21	20	4	4
Διαχείριση βάσεων δεδομένων	7	5	26	6	1
Αρχιτεκρινική επιχειρήσεων – Σχεδιασμός Υποδομής	8	12	20	16	2
Αξιολόγηση ΤΠΕ	10	19	15	11	2
Διαχείριση δικτύου	7	14	24	13	1
Λειτουργικά συστήματα	6	11	27	12	1
Ανάπτυξη λογισμικού & γλώσσες πληροφορικής	14	14	20	10	1
Διαχείριση & Ολοκλήρωση Συστήματος	12	14	24	8	1
Δοκιμές και αξιολόγηση	9	16	20	13	1
Τεχνολογική αποδοτικότητα	9	17	20	12	1

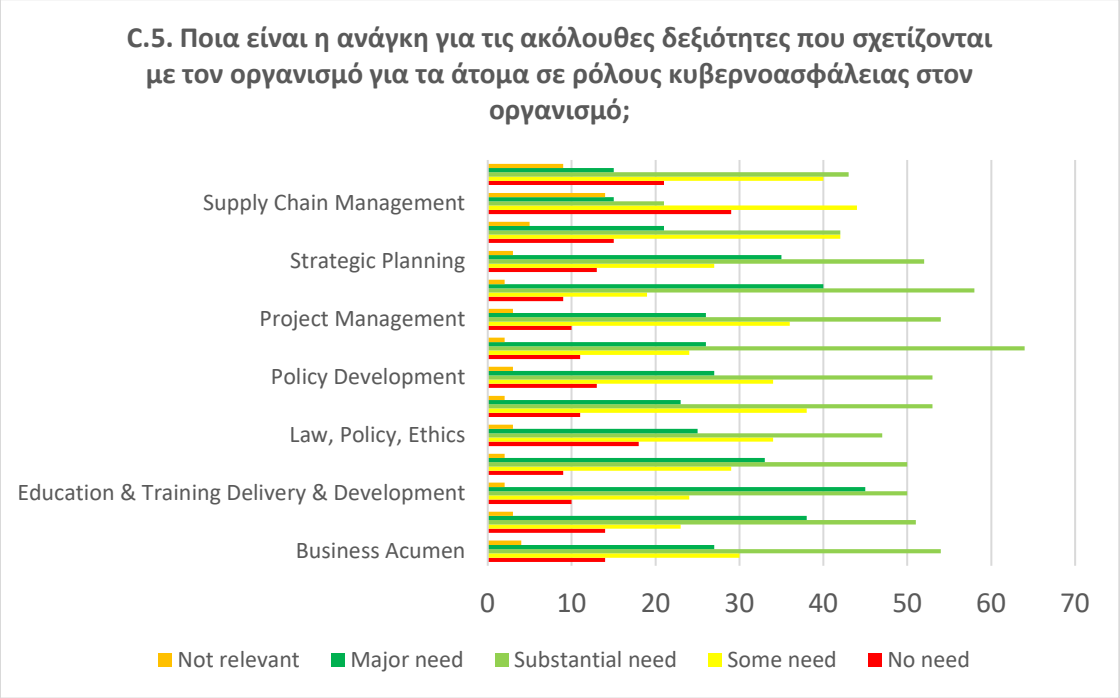
Πίνακας 28 (ερώτηση C.3): Ανάγκη για δεξιότητες σχετικές με την πληροφορική στον οργανισμό

[39] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



ΕΛΛΑΔΑ	**C.5:** Ποια είναι η ανάγκη για τις ακόλουθες δεξιότητες που σχετίζονται με τον οργανισμό για τα άτομα σε ρόλους κυβερνοασφάλειας στον οργανισμό?[40]				
Οργανωτικές δεξιότητες	**Καμία**	**Μερική**	**Σημαντική**	**Πολύ σημαντική**	**Δεν είναι σχετικό**
Επιχειρηματική Οξυδέρκεια	14	30	54	27	4
Αδιάλειπτη επιχειρησιακή λειτουργία	14	23	51	38	3
Εκπαίδευση και Κατάρτιση	10	24	50	45	2
Διαχείριση Γνώσεων	9	29	50	33	2
Δίκαιο, Πολιτική και Ηθική	18	34	47	25	3
Οργανωτική Επίγνωση	11	38	53	23	2
Ανάπτυξη Πολιτικών	13	34	53	27	3
Έλεγχος Διεργασιών	11	24	64	26	2
Διαχείριση Έργου	10	36	54	26	3
Διαχείριση Επικινδυνότας	9	19	58	40	2
Στρατηγικός Σχεδιασμός	13	27	52	35	3
Διαχείριση Στρατηγικών Σχέσεων	15	42	42	21	5
Διαχείριση Εφοδιαστικής Αλυσίδας	29	44	21	15	14
Διαχείριση Στελεχιακού Δυναμικού	21	40	43	15	9

[40] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.



Πίνακας 29 (ερώτηση C.5): Ανάγκη για συναφείς δεξιότητες στον οργανισμό

	ΕΛΛΔΑ
C.6: Υπάρχει ανάγκη για άλλες δεξιότητες που σχετίζονται με τον οργανισμό για τα άτομα σε ρόλους κυβερνοασφάλειας στον οργανισμό;	
Ναι	1
Όχι	129
Σύνολο	**130**

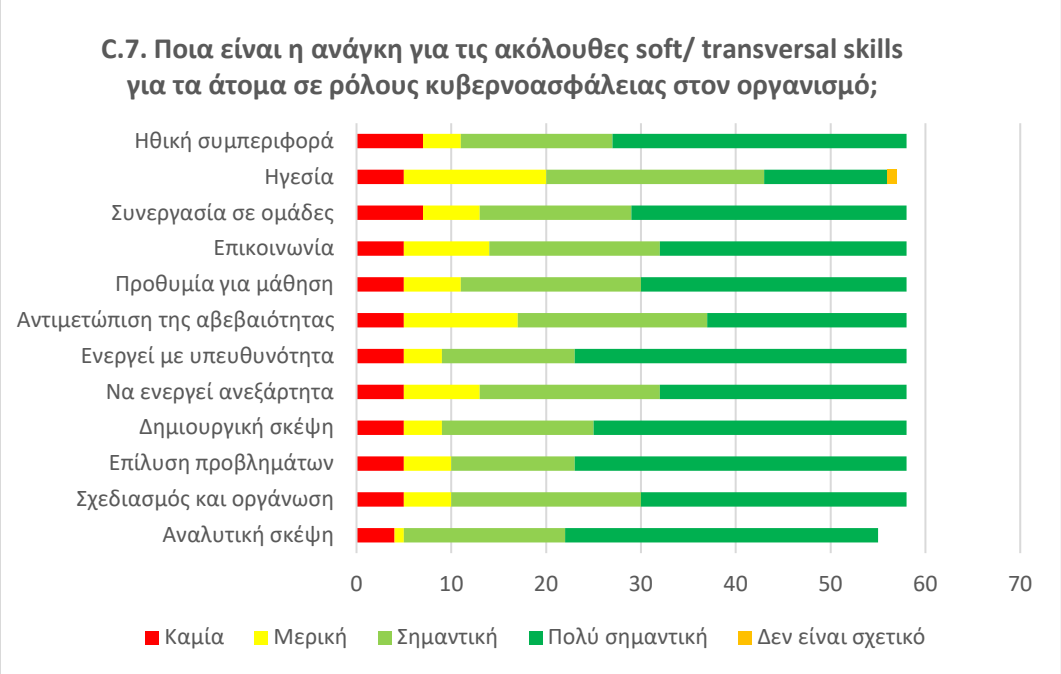
Πίνακας 30 (ερώτηση C.6): Πρόσθετες οργανωτικές δεξιότητες

	ΕΛΛΑΔΑ	**C.7:** Ποια είναι η ανάγκη για τις ακόλουθες ή-πιες/μεταβατικές δεξιότητες για τα άτομα σε ρό-λους κυβερνοασφάλειας στον οργανισμό?[41]			
Soft/Transversal Skills	**Καμία**	**Μερική**	**Σημαντική**	**Πολύση-μαντική**	**Δεν είναι σχετικό**
Αναλυτική σκέψη	4	1	17	33	0
Σχεδιασμός και οργάνωση	5	5	20	28	0

[41] Το πράσινο χρώμα υποδεικνύει υψηλές τιμές και το κίτρινο χαμηλές.

Επίλυση προβλημάτων	5	5	13	35	0
Δημιουργική σκέψη	5	4	16	33	0
Ανάληψη πρωτοβουλιών	5	8	19	26	0
Υπευθυνότητα	5	4	14	35	0
Διαχείριση αβεβαιότητας	5	12	20	21	0
Φιλομαθία	5	6	19	28	0
Επικοινωνία	5	9	18	26	0
Ομαδικότητα	7	6	16	29	0
Ηγετική Δυναμική	5	15	23	13	1
Τήρηση Δεοντολογίας	7	4	16	31	0

Πίνακας 31 (ερώτηση C.7):Ανάγκες για soft/transversal skills



	ΕΛΛΑΔΑ
C.8: Υπάρχει η ανάγκη για άλλα soft/ transversal skills για τα άτομα σε ρόλους κυβερνοασφάλειας στον οργανισμό;	
Ναι	3
Όχι	54
Σύνολο	**57**

Πίνακας 32 (ερώτηση C.8): Πρόσθετες κοινωνικές δεξιότητες

	ΕΛΛΑΔΑ
D.1: Υπάρχει ανάγκη για εκπαίδευση προσωπικού σε ρόλους κυβερνοασφάλειας;	
Ναι	113
Όχι	26
Σύνολο	**139**

Πίνακας 33 (ερώτηση D.1): Ανάγκη για κατάρτιση προσωπικού

	ΕΛΛΑΔΑ
D.2:Υπάρχει καθυστέρηση στην κατάρτιση προσωπικού σε ρόλους κυβερνοασφάλειας;	
Ναι	34
Όχι	105
Σύνολο	**139**

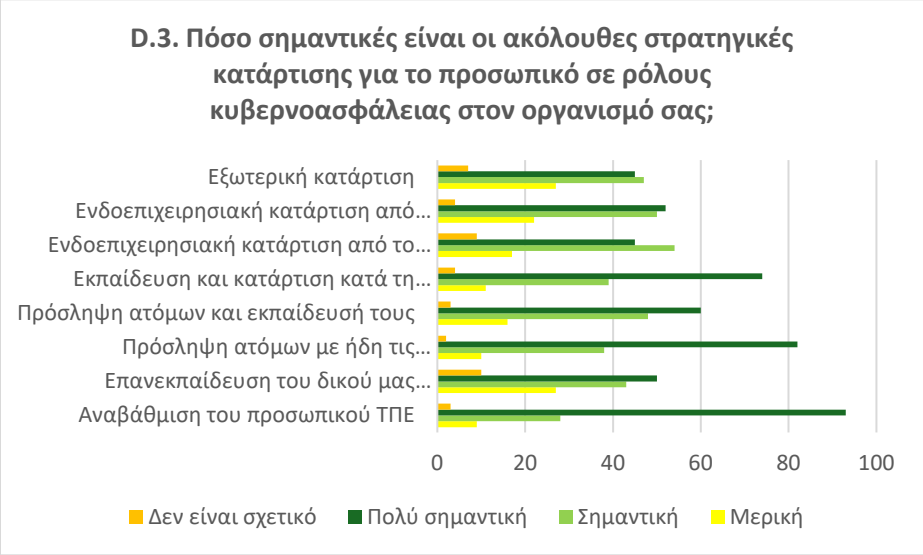
Πίνακας 34 (ερώτηση D.2): Εκπαιδευτικό προσωπικό

ΕΛΛΑΔΑ	**D.3:** Πόσο σημαντικές είναι οι ακόλουθες στρατηγικές κατάρτισης για το προσωπικό σε ρόλους κυβερνοασφάλειας στον οργανισμό σας;[42]

[42] Green color indicates high values and yellow low ones.

Στρατηγικές κατάρτισης	Μερική	Σημαντική	Πολύ σημαντική	Δεν είναι σχετικό
Αναβάθμιση του προσωπικού ΤΠΕ	9	28	93	3
Επανεκπαίδευση του δικού μας προσωπικού εκτός ΤΠΕ	27	43	50	10
Πρόσληψη ατόμων με ήδη τις κατάλληλες δεξιότητες	10	38	82	2
Πρόσληψη ατόμων και εκπαίδευσή τους	16	48	60	3
Εκπαίδευση και κατάρτιση κατά τη διάρκεια της εργασίας	11	39	74	4
Ενδοεπιχειρησιακή κατάρτιση από το δικό τους προσωπικό	17	54	45	9
Ενδοεπιχειρησιακή κατάρτιση από εξωτερικό πάροχο	22	50	52	4
Εξωτερική κατάρτιση	27	47	45	7

Πίνακας 35 (Ερώτηση D.3) Σημασία των στρατηγικών κατάρτισης

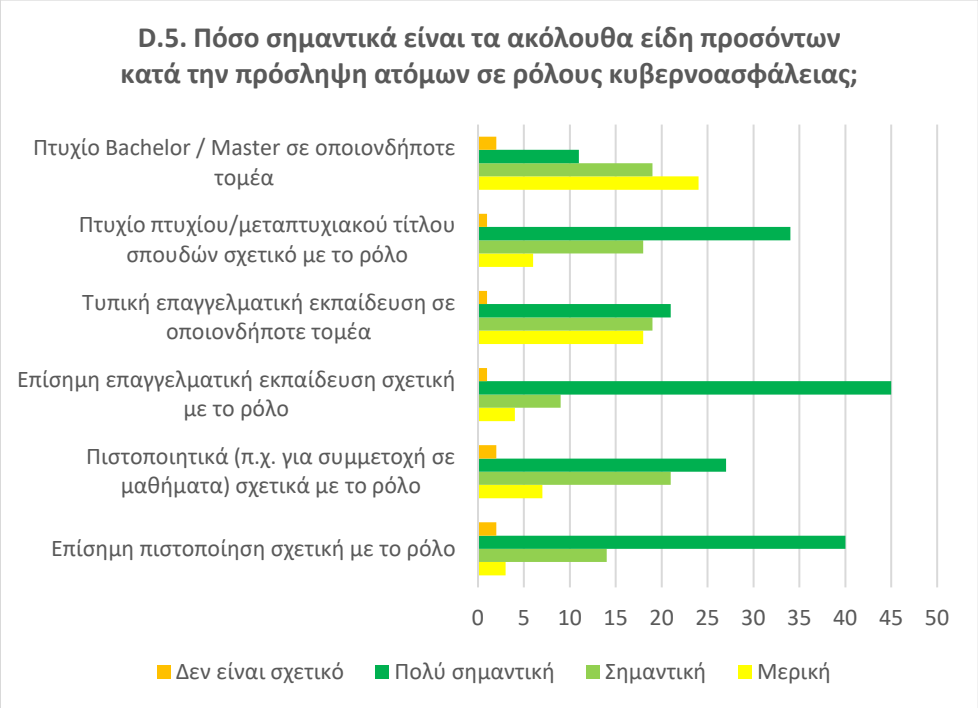


ΕΛΛΑΔΑ	**D.5:** Πόσο σημαντικά είναι τα ακόλουθα είδη προσόντων κατά την πρόσληψη ατόμων σε ρόλους κυβερνοασφάλειας;[43]			
Προσόντα πρόσληψης	**Μερική**	**Σημαντική**	**Πολύ σημαντική**	**Δεν είναι σχετικό**
Επίσημη πιστοποίηση σχετική με το ρόλο	3	14	40	2
Πιστοποιητικά (π.χ. για συμμετοχή σε μαθήματα) σχετικά με το ρόλο	7	21	27	2

[43] Green color indicates high values and yellow low ones.

Επίσημη επαγγελματική εκπαίδευση σχετική με το ρόλο	4	9	45	1
Τυπική επαγγελματική εκπαίδευση σε οποιονδήποτε τομέα	18	19	21	1
Πτυχίο πτυχίου/μεταπτυχιακού τίτλου σπουδών σχετικό με το ρόλο	6	18	34	1
Πτυχίο Bachelor / Master σε οποιονδήποτε τομέα	24	19	11	2

Πίνακας 36 (ερώτηση D.5): Σημασία των προσόντων πρόσληψης



<u>Παράρτημα VI:</u> ΕΛΛΑΔΑ - CyberHubsΈρευνα για τους ρόλους και τις δεξιότητες κυβερνοασφάλειας 2024

Η έρευνα CyberHubs για τους ρόλους και τις δεξιότητες στον κυβερνοχώρο 2024 απευθυνόταν σε οργανισμούς διαφόρων κατηγοριών και τομέων. Σε αυτούς περιλαμβάνονταν πάροχοι υπηρεσιών κυβερνοασφάλειας, εταιρείες ΤΠΕ, ιδιωτικοί και δημόσιοι φορείς με εσωτερικές ανάγκες κυβερνοασφάλειας, ακαδημαϊκά ιδρύματα και άλλοι. Τα αποτελέσματα της έρευνας θα αποτελέσουν κρίσιμη πηγή πληροφοριών για την ανάπτυξη στρατηγικών και εκπαιδευτικών προγραμμάτων, καθώς και για την προστασία της Ελλάδας από τις κυβερνοεπιθέσεις.

Το ερωτηματολόγιο αποτελούνταν από τέσσερα μέρη:

A. Γενικές ερωτήσεις σχετικά με τον οργανισμό

Σκοπός αυτού του μέρους ήταν να συγκεντρωθούν πληροφορίες σχετικά με τις απαιτήσεις του οργανισμού για τις δεξιότητες κυβερνοασφάλειας και να εξασφαλιστούν μοναδικές απαντήσεις. Οι ερωτήσεις περιλάμβαναν το αναγνωριστικό του οργανισμού, πληροφορίες για την κατηγορία, τις κύριες ψηφιακές υπηρεσίες, τη δραστηριότητα στον τομέα και το μέγεθος.

B. Ερωτήσεις σχετικά με τους ρόλους

Το μέρος αυτό αφορούσε στους διάφορους ρόλους σε έναν οργανισμό που απαιτούν ουσιαστικές δεξιότητες κυβερνοασφάλειας. Η έμφαση δόθηκε σε 12 βασικά προφίλ ρόλων, όπως ορίζονται από το Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (ECSF). Για τους ρόλους αυτούς, το ερωτηματολόγιο επεδίωξε να προσδιορίσει τον τρέχοντα αριθμό απασχολουμένων, την τρέχουσα ανάγκη για εργαζόμενους στους ρόλους αυτούς, την αναμενόμενη ανάγκη και τη μακροπρόθεσμη αναμενόμενη ανάγκη. Η παρούσα ενότητα είχε ως στόχο να παράσχει μια ολοκληρωμένη επισκόπηση της τρέχουσας και μελλοντικής ζήτησης για διάφορους ρόλους κυβερνοασφάλειας εντός των οργανισμών, ώστε να κατανοηθούν καλύτερα και να αντιμετωπιστούν οι ανάγκες σε δεξιότητες σε αυτόν τον κρίσιμο τομέα.

C: Δεξιότητες για ρόλους κυβερνοασφάλειας στον οργανισμό

Αυτή η ενότητα αφορούσε στις βασικές δεξιότητες που απαιτούνται για τα άτομα σε ρόλους κυβερνοασφάλειας εντός ενός οργανισμού. Περιλάμβανε ειδικές δεξιότητες για την ασφάλεια στον κυβερνοχώρο, γενικές δεξιότητες πληροφορικής, οργανωτικές και κοινωνικές δεξιότητες, αξιολογώντας την τρέχουσα και μελλοντική ανάγκη για αυτές τις δεξιότητες μεταξύ των επαγγελματιών της ασφάλειας στον κυβερνοχώρο, ώστε να αντιμετωπιστούν αυτά τα κενά και να ενισχυθούν οι ικανότητές τους στον κυβερνοχώρο.

D: Ερωτήσεις σχετικά με την κατάρτιση και την εκπαίδευση

Το τελευταίο μέρος κάλυψε τις βασικές πτυχές των απαιτήσεων κατάρτισης και εκπαίδευσης, των καθυστερήσεων, των στρατηγικών, των λόγων και των προσόντων που σχετίζονται με τους ρόλους κυβερνοασφάλειας σε έναν οργανισμό.

Παρακαλούμε ανατρέξτε σε αυτό το link για μια μεταφρασμένη έκδοση της πρωτότυπης ελληνικής έκδοσης του **πλήρους ερωτηματολογίου**.