ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Στρασβούργο, 18.4.2023
COM(2023) 207 final

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ

Κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ («Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας»)

Κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ(«Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας»)

1. Επείγουσα ανάγκη μείωσης των κινδύνων με την αντιμετώπιση της έλλειψης και των κενών κυβερνοδεξιοτήτων

Η κυβερνοασφάλεια δεν αποτελεί μόνο μέρος της ασφάλειας των πολιτών, των επιχειρήσεων και των κρατών μελών. Είναι επίσης αναγκαία για να διασφαλιστεί η πολιτική σταθερότητα της ΕΕ, η σταθερότητα των δημοκρατιών της και η ευημερία της κοινωνίας και των επιχειρήσεών μας. Το **τοπίο των απειλών** κατά της κυβερνοασφάλειας έχει εξελιχθεί σημαντικά τα τελευταία έτη και έχει εκδηλωθεί η ανησυχητική τάση όλο και περισσότερες κυβερνοεπιθέσεις να στοχεύουν σε στρατιωτικές και μη στρατιωτικές κρίσιμες υποδομές στην ΕΕ. Οι παράγοντες απειλής αυξάνουν τις ικανότητές τους και εμφανίζονται νέες, υβριδικές και αναδυόμενες απειλές, όπως η χρήση υπολογιστών ζόμπι (bot) και τεχνικών που βασίζονται στην τεχνητή νοημοσύνη[1]. Συγκεκριμένα, οι παράγοντες απειλής μέσω λυτρισμικού προκαλούν συστηματικά σημαντική ζημία σε οντότητες, τόσο οικονομική όσο και στη φήμη τους[2].

Μεγάλος αριθμός περιστατικών κυβερνοασφάλειας στόχευαν επίσης τη δημόσια διοίκηση και τις κυβερνήσεις των κρατών μελών, καθώς και τα ευρωπαϊκά θεσμικά και λοιπά όργανα και οργανισμούς[3]. Ο χρηματοοικονομικός τομέας[4] και ο τομέας της υγείας[5], οι οποίοι αποτελούν τη ραχοκοκαλιά της κοινωνίας και της οικονομίας, αποτελούν επίσης σταθερά στόχους[6]. Οι γεωπολιτικές εντάσεις που συνδέονται με τον επιθετικό πόλεμο της Ρωσίας κατά της Ουκρανίας έχουν αυξήσει την απειλή για την κυβερνοασφάλεια[7] και έχουν τη δυνατότητα να αποσταθεροποιήσουν την κοινωνία μας. Η **ασφάλεια** της ΕΕ δεν μπορεί να κατοχυρωθεί χωρίς το **πιο πολύτιμο στοιχείο της ΕΕ: τους ανθρώπους της.** Η ΕΕ χρειάζεται επειγόντως επαγγελματίες με δεξιότητες και ικανότητες για την πρόληψη, τον εντοπισμό, την αποτροπή και την υπεράσπιση της ΕΕ, συμπεριλαμβανομένων των

[1] ENISA, Threat Landscape 2022 (Τοπίο απειλών 2022) — ENISA (europa.eu).

[2] Ευρωπόλ, Internet Organised Crime Threat Assessment (Αξιολόγηση των απειλών όσον αφορά το οργανωμένο έγκλημα στο διαδίκτυο) (IOCTA), 2021. Οι εν λόγω παράγοντες βασίζονται στο μοντέλο του λυτρισμικού ως υπηρεσία. Το ετήσιο κόστος για τις επιχειρήσεις υπερέβη τα 18,4 δισ. EUR το 2022 (Έκθεση της Cybereason 2022 σχετικά με το πραγματικό κόστος του λυτρισμικού).

[3] Βλ., για παράδειγμα, την κοινή δημοσίευση του ENISA και της CERT-EE, JP-23-01 — Sustained activity by specific threat actors (Διαρκής δραστηριότητα συγκεκριμένων παραγόντων απειλής), TLP: CLEAR, 15 Φεβρουαρίου 2023.

[4] Βλ., για παράδειγμα, στη Γερμανία, το 90 % των περιστατικών απάτης μέσω ηλεκτρονικού ταχυδρομείου που δηλώθηκαν από την 1η Ιουνίου 2021 έως τις 31 Μαΐου 2022 αφορούσαν ηλεκτρονικό ψάρεμα στον χρηματοοικονομικό τομέα ή επίθεση κατά εταιρείας στον χρηματοοικονομικό τομέα, με την εμπλοκή περισσότερων από 20 000 προσβεβλημένων συσκευών από 125 χώρες, The State of IT Security in Germany in 2022 (Η κατάσταση της ασφάλειας ΤΠ στη Γερμανία το 2022), Bundesamt für Sicherheit in der Informationstechnik (BSI), 1η Ιανουαρίου 2023.

[5] Βλ., για παράδειγμα, στη Γαλλία επιθέσεις λυτρισμικού κατά δημόσιων εγκαταστάσεων υγειονομικής περίθαλψης, όπως του Centre Hospitalier Sud Francilien, κατά τη διάρκεια των οποίων εκλάπησαν και δημοσιεύθηκαν από τον παράγοντα απειλής 11 GB δεδομένων προσωπικού χαρακτήρα και ιατρικών δεδομένων, καθώς και δεδομένων που σχετίζονται με το προσωπικό, Panorama de la cybermenace 2022 (Πανόραμα κυβερνοαπειλών 2022), Agence nationale de la sécurité des produèmes d'information (ANSSI), Ιανουάριος 2023.

[6] Βλ. ENISA Threat Landscape 2022.

[7] Βλ. επίσης: CERT-EE – πόλεμος της Ρωσίας κατά της Ουκρανίας: ένα έτος κυβερνοεπιχειρήσεων (europa.eu)· Ρωσικές κυβερνοεπιχειρήσεις κατά της Ουκρανίας: Δήλωση του Ύπατου Εκπροσώπου εξ ονόματος της Ευρωπαϊκής Ένωσης, 10 Μαΐου 2022· Δήλωση του Ύπατου Εκπροσώπου, εξ ονόματος της Ευρωπαϊκής Ένωσης, σχετικά με κακόβουλες δραστηριότητες στον κυβερνοχώρο από χάκερ και ομάδες χάκερ στο πλαίσιο της επίθεσης της Ρωσίας κατά της Ουκρανίας, 19 Ιουλίου 2022.

κρισιμότερων υποδομών της, από κυβερνοεπιθέσεις και τη διασφάλιση της **ανθεκτικότητάς** της.

Η έλλειψη ταλέντων στον τομέα της κυβερνοασφάλειας παρεμποδίζει περαιτέρω την **ανταγωνιστικότητα** και την **ανάπτυξη** της Ευρώπης, οι οποίες εξαρτώνται σε μεγάλο βαθμό από την ανάπτυξη και την αξιοποίηση στρατηγικών ψηφιακών τεχνολογιών (π.χ. τεχνητής νοημοσύνης, 5G και υπολογιστικού νέφους). Απαιτείται ειδικευμένο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας προκειμένου η ΕΕ να συνεχίσει να μπορεί να παρέχει βασικές προηγμένες τεχνολογίες σε παγκόσμιο επίπεδο.

Για να προετοιμαστεί γι' αυτό το εξελισσόμενο τοπίο απειλών, για να το αντιμετωπίσει και να ενισχύσει την ανταγωνιστικότητα της ΕΕ, η πολιτική της ΕΕ για την κυβερνοασφάλεια έχει σημειώσει σημαντική πρόοδο τα τελευταία χρόνια, με αποτέλεσμα την έγκριση σειράς πρωτοβουλιών, όπως της στρατηγικής κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[8], της αναθεωρημένης οδηγίας για την ασφάλεια δικτύων και πληροφοριών (οδηγία NIS2)[9], της τομεακής νομοθεσίας της ΕΕ για την κυβερνοασφάλεια[10], της πολιτικής της ΕΕ για την κυβερνοάμυνα[11], της πράξης για την κυβερνοανθεκτικότητα[12] και της πράξης για την αλληλεγγύη στον κυβερνοχώρο, η οποία προτείνεται από την Επιτροπή μαζί με την παρούσα ανακοίνωση. Ωστόσο, χωρίς τα απαραίτητα ειδικευμένα άτομα για την εφαρμογή τους, οι εν λόγω νομοθετικές πράξεις δεν θα επιτύχουν τους στόχους τους. Ενώ οι βασικές γνώσεις κυβερνοασφάλειας του γενικού πληθυσμού εξετάζονται στο πλαίσιο πρωτοβουλιών οι οποίες στηρίζουν την ανάπτυξη των γενικών δεξιοτήτων που απαιτούνται για τη συμμετοχή στην κοινωνία[13], ένα ικανό εργατικό δυναμικό είναι απαραίτητο τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, σε εθνικό και ενωσιακό επίπεδο, μεταξύ άλλων σε οργανισμούς τυποποίησης, **για την εκπλήρωση των εν λόγω απαιτήσεων νομοθεσίας και πολιτικής για την κυβερνοασφάλεια.**

Ως εκ τούτου, η ασφάλεια και η ανταγωνιστικότητα της ΕΕ εξαρτώνται από την ύπαρξη ειδικευμένου εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας. Ωστόσο, η ΕΕ αντιμετωπίζει πολύ σημαντική έλλειψη ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας, γεγονός που θέτει την ΕΕ, τα κράτη μέλη της, τις επιχειρήσεις και τους πολίτες της σε κίνδυνο περιστατικών κυβερνοασφάλειας. Η έλλειψη επαγγελματιών στον

[8] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο — Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία [JOIN(2020) 18 final].

[9] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2).

[10] Όπως, για τον χρηματοοικονομικό τομέα, ο κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (πράξη για την ψηφιακή επιχειρησιακή ανθεκτικότητα).

[11] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο — Πολιτική της ΕΕ για την κυβερνοάμυνα [JOIN(2022) 49 final].

[12] Πρόταση για κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020 [COM(2022) 454 final].

[13] Οι σχετικές πρωτοβουλίες που αφορούν τις γενικές ψηφιακές δεξιότητες του πληθυσμού περιλαμβάνουν τα εξής: απόκτηση βασικών ψηφιακών δεξιοτήτων από το 80 % του πληθυσμού έως το 2030, ως στόχος του σχεδίου δράσης για τον ευρωπαϊκό πυλώνα κοινωνικών δικαιωμάτων και της ψηφιακής πυξίδας, το σχέδιο δράσης για την ψηφιακή εκπαίδευση 2021-2027, το εργαλείο του πλαισίου ψηφιακών ικανοτήτων ή την πρόταση για σύσταση του Συμβουλίου σχετικά με τη βελτίωση της παροχής ψηφιακών δεξιοτήτων στην εκπαίδευση και την κατάρτιση.

τομέα της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση κυμάνθηκε το 2022 **μεταξύ 260 000**[14] **και 500 000**[15], ενώ οι ανάγκες της ΕΕ σε εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας εκτιμήθηκαν σε 883 000 επαγγελματίες[16], γεγονός που υποδηλώνει αναντιστοιχία μεταξύ των διαθέσιμων ικανοτήτων και εκείνων που απαιτούνται από την αγορά εργασίας. Το εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας πάσχει περαιτέρω από την εσφαλμένη αντίληψη που συνδέεται με την τεχνική εικόνα του και ο τομέας εξακολουθεί να αδυνατεί να προσελκύσει **γυναίκες**, οι οποίες ανέρχονται στο 20 % των αποφοίτων στον τομέα της κυβερνοασφάλειας[17] και στο 19 % των ειδικών στον τομέα της τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ)[18]. Για να αντιμετωπιστεί αυτό, το ευρωπαϊκό **πρόγραμμα πολιτικής 2030 «Ψηφιακή Δεκαετία»**[19] έχει θέσει ως στόχο την αύξηση του αριθμού των επαγγελματιών στον τομέα των ΤΠΕ κατά 20 εκατομμύρια έως το 2030, επιτυγχάνοντας παράλληλα τη σύγκλιση των φύλων. Επίσης, για την εφαρμογή της αναδυόμενης πολιτικής της ΕΕ απαιτείται κατάλληλα καταρτισμένο και επαρκές εργατικό δυναμικό. Για παράδειγμα, πάνω από το 42 % των ανώτερων διευθυντικών στελεχών σε θέματα τεχνολογίας πληροφοριών (ΤΠ) στον κλάδο των χρηματοοικονομικών υπηρεσιών τόνισαν την έλλειψη δεξιοτήτων και εμπειρογνωσίας σε θέματα κυβερνοασφάλειας ως βασική πρόκληση που αντιμετωπίζουν οι επιχειρήσεις τους όσον αφορά την κυβερνοάμυνα και τη διαχείριση περιστατικών[20], σε μια χρονική στιγμή κατά την οποία θα χρειαστεί να εφαρμόσουν τομεακή νομοθεσία κυβερνοασφάλειας, όπως την πράξη για την ψηφιακή επιχειρησιακή ανθεκτικότητα (DORA).

Η επιφυλακτικότητα των εργοδοτών να επενδύσουν σε ανθρώπινο κεφάλαιο, αναζητώντας ήδη καταρτισμένο και πεπειραμένο εργατικό δυναμικό, συμβάλλει περαιτέρω στον περιορισμό της αγοράς εργασίας[21]. Η έλλειψη αυτή πλήττει όλα τα είδη εταιρειών, συμπεριλαμβανομένων των μικρομεσαίων επιχειρήσεων (**ΜΜΕ**), οι οποίες αντιπροσωπεύουν το 99 % του συνόλου των επιχειρήσεων στην ΕΕ[22]. Η πρόκληση είναι επίσης μεγάλη για τις **δημόσιες διοικήσεις** που πλήττονται σε μεγάλο βαθμό και επηρεάζονται περισσότερο από περιστατικά κυβερνοασφάλειας[23].

Ως εκ τούτου, η κάλυψη της έλλειψης επαγγελματικών ταλέντων που αντιμετωπίζει η ΕΕ στον τομέα της κυβερνοασφάλειας αποτελεί επείγον ζήτημα, δεδομένου ότι διακυβεύονται η ασφάλεια και η ανταγωνιστικότητα της ΕΕ.

---

[14] (ISC)² στο Assessing Cyber Skills on the basis of the ECSF (Αξιολόγηση των κυβερνοδεξιοτήτων με βάση το ευρωπαϊκό πλαίσιο κυβερνοδεξιοτήτων), διαδικτυακό σεμινάριο του ENISA, 16 Φεβρουαρίου 2023.

[15] Σύμφωνα με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο (ECSO), όπως αναφέρεται στην κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο — Πολιτική της ΕΕ για την κυβερνοάμυνα [JOIN(2022) 49 final].

[16] (ISC)² στο Assessing Cyber Skills on the basis of the ECSF, διαδικτυακό σεμινάριο του ENISA, 16 Φεβρουαρίου 2023.

[17] Βάση δεδομένων για την τριτοβάθμια εκπαίδευση στον τομέα της κυβερνοασφάλειας (CyberHEAD).

[18] Μόνο το 19 % των ειδικών στις ΤΠΕ στην ΕΕ είναι γυναίκες. Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας (DESI) 2022 | Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης (europa.eu). Δεν υπάρχουν διαθέσιμα αριθμητικά στοιχεία όσον αφορά το γυναικείο εργατικό δυναμικό της Ένωσης στον τομέα της κυβερνοασφάλειας.

[19] Απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία», με την οποία θεσπίζεται μηχανισμός παρακολούθησης και συνεργασίας για την επίτευξη των κοινών σκοπών και επιδιώξεων για τον ψηφιακό μετασχηματισμό της Ευρώπης που καθορίζεται στην Ψηφιακή Πυξίδα 2030, συμπεριλαμβανομένου του τομέα των δεξιοτήτων.

[20] S-RM Cyber Security Insights Report 2022.

[21] Cybersecurity Skills Development in the EU (Ανάπτυξη κυβερνοδεξιοτήτων στην ΕΕ), ENISA, Δεκέμβριος 2019.

[22] Ορισμός των ΜΜΕ (europa.eu).

[23] ENISA, Threat Landscape 2022 — ENISA (europa.eu).

2. Έλλειψη συνεργειών και συντονισμένης δράσης για την κάλυψη των ελλείψεων κυβερνοδεξιοτήτων

Αναλαμβάνονται όλο και περισσότερες πρωτοβουλίες σε ευρωπαϊκό και εθνικό επίπεδο από δημόσιους και ιδιωτικούς φορείς για την αντιμετώπιση των ελλείψεων της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας. Ωστόσο, είναι διάσπαρτες και, μέχρι στιγμής, δεν έχουν επιτύχει κρίσιμη μάζα για να κάνουν πραγματικά τη διαφορά.

Καταρχάς, επί του παρόντος υπάρχει περιορισμένη κοινή αντίληψη όσον αφορά τη σύνθεση του εργατικού δυναμικού της ΕΕ και των συναφών δεξιοτήτων στον τομέα της κυβερνοασφάλειας, ενώ παρόμοια προφίλ εργασίας στον τομέα της κυβερνοασφάλειας θα πρέπει να περιλαμβάνουν το ίδιο σύνολο δεξιοτήτων. Ο περιορισμένος βαθμός αξιοποίησης, από τους σχετικούς παράγοντες, ενός κοινού **ευρωπαϊκού πλαισίου αναφοράς για τους επαγγελματίες στον τομέα της κυβερνοασφάλειας** έχει ως αποτέλεσμα την έλλειψη ενός εργαλείου επικοινωνίας μεταξύ εργοδοτών, εκπαιδευτών και υπευθύνων χάραξης πολιτικής, καθώς και την αδυναμία διενέργειας μετρήσεων και αξιολόγησης των ελλείψεων στην αγορά εργασίας στον τομέα της κυβερνοασφάλειας. Επιπρόσθετα, αποτρέπει τον σχεδιασμό προγραμμάτων εκπαίδευσης και κατάρτισης και τη δημιουργία οδών σταδιοδρομίας που να ανταποκρίνονται στις ανάγκες της πολιτικής και της αγοράς για όσες και όσους επιθυμούν να εισέλθουν στο επάγγελμα. **Η αναβάθμιση των δεξιοτήτων και η επανειδίκευση** του εργατικού δυναμικού βασίζονται σε μεγάλο βαθμό σε προγράμματα κατάρτισης και πιστοποιητικά κυβερνοασφάλειας, τα οποία συνήθως προσφέρονται από ιδιωτικούς παρόχους. Ωστόσο, το εργατικό δυναμικό αντιμετωπίζει δυσκολίες να διαμορφώσει μια συνολική εικόνα για την ποιότητα των προσφερόμενων προγραμμάτων κατάρτισης στον τομέα της κυβερνοασφάλειας και των σχετικών εκδιδόμενων πιστοποιητικών.

Μολονότι η εκπαίδευση και κατάρτιση και η ανάπτυξη οδών σταδιοδρομίας είναι απαραίτητες για την ενίσχυση της πλευράς της προσφοράς στην αγορά εργασίας, ο ρόλος της **πλευράς της ζήτησης** στην κατάρτιση του οικείου εργατικού δυναμικού και στην προσαρμογή στην εξέλιξή της υποτιμάται επί του παρόντος. Η βιομηχανία και οι εργοδότες του δημόσιου τομέα δεν διαθέτουν κοινά φόρουμ και κοινούς χώρους για τη συγκέντρωση ιδεών σχετικά με το πώς μπορεί να καταρτιστεί καλύτερα το εργατικό δυναμικό και για να μελετηθεί το πώς μπορούν **να αξιολογούνται καλύτερα οι δεξιότητες**, ειδικότερα κατά τη διάρκεια της διαδικασίας πρόσληψης. Οι **τεχνικές δεξιότητες** με τη μεγαλύτερη ζήτηση μπορεί να σχετίζονται με την κυβερνοασφάλεια[24], όπως η ανάπτυξη λογισμικού ή η νεφοϋπολογιστική[25], αλλά οι **εγκάρσιες δεξιότητες** εξακολουθούν να αγνοούνται αδικαιολόγητα. Η κριτική σκέψη και ανάλυση, η επίλυση προβλημάτων και η αυτοδιαχείριση αποτελούν ομάδες δεξιοτήτων που απαιτούν περισσότερο οι εργοδότες[26] και που αποκτούν όλο και μεγαλύτερο ρόλο στην πορεία προς το 2025[27].

Υπάρχουν ήδη πολλές δημόσιες και ιδιωτικές επενδυτικές πρωτοβουλίες για τις κυβερνοδεξιότητες και η ΕΕ **χρηματοδοτεί** ευρέως έργα στο πλαίσιο διαφόρων μέσων[28]. Ωστόσο, η συνεχιζόμενη έλλειψη δεξιοτήτων στην ΕΕ εγείρει ερωτήματα όσον αφορά την προβολή και τον αντίκτυπό τους και υποδηλώνει ότι οι δεξιότητες ενδέχεται να μην

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most.

[25] ISACA, Ενημερωτικό γράφημα για την κατάσταση της κυβερνοασφάλειας το 2022.

[26] Όπως το εργαλείο του CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[27] The Future of Jobs Report, Οκτώβριος 2020, Παγκόσμιο Οικονομικό Φόρουμ.

[28] Για παράδειγμα: Συμμαχία για τις κυβερνοδεξιότητες — Νέο όραμα για την Ευρώπη — έργο REWIRE (χρηματοδοτούμενο από το πρόγραμμα Erasmus+)· έργα για την υποστήριξη του Κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας [ECHO, CONCORDIA, CyberSec4Europe, SPARTA (χρηματοδοτούμενο από το πρόγραμμα «Ορίζων 2020»), έργο Cybersecpro (χρηματοδοτούμενο από το πρόγραμμα «Ψηφιακή Ευρώπη»)].

ανταποκρίνονται συστηματικά στις ανάγκες της αγοράς, οι οποίες πρέπει να χαρτογραφηθούν επειγόντως σε επίπεδο ΕΕ. Επίσης, οι διάφορες πηγές χρηματοδότησης επιφέρουν αλληλεπικαλύψεις, με αποτέλεσμα να χάνεται η ευκαιρία κλιμάκωσης και επίτευξης πραγματικού αντικτύπου. Επιπρόσθετα, όσοι χρειάζονται την επένδυση δεν μπορούν πάντα να προσδιορίσουν τις καταλληλότερες πηγές για τις ανάγκες τους.

Τα **ενδιαφερόμενα μέρη** προσπαθούν να αντιμετωπίσουν το σύνθετο και πολύπλευρο ζήτημα της έλλειψης κυβερνοδεξιοτήτων. Ο Οργανισμός της ΕΕ για την Κυβερνοασφάλεια (ENISA) αναπτύσσει μέσα σχετικά με τα προφίλ ρόλων ή την τριτοβάθμια εκπαίδευση[29], το Ευρωπαϊκό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας (ECCC)[30] ασχολείται με τις κυβερνοδεξιότητες σε μια ειδική ομάδα εργασίας, η Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας (ΕΑΑΑ) ασχολείται με τις κυβερνοδεξιότητες του πολιτικού και στρατιωτικού εργατικού δυναμικού στο πλαίσιο της Κοινής Πολιτικής Ασφάλειας και Άμυνας[31], ιδιωτικοί οργανισμοί προσπαθούν να αντιμετωπίσουν το ζήτημα[32], ο κλάδος πιστοποίησης της κυβερνοασφάλειας αναπτύσσει χάρτη πορείας και προγράμματα κατάρτισης για την αντιμετώπιση της έλλειψης δεξιοτήτων[33]. Τα κράτη μέλη προσπαθούν επίσης να αντιμετωπίσουν το ζήτημα μέσω διαφόρων πρωτοβουλιών, οι οποίες κυμαίνονται από ρυθμιστικές διατάξεις[34] έως τη δημιουργία ακαδημιών κυβερνοδεξιοτήτων[35] ή πανεπιστημιουπόλεων για την κυβερνοασφάλεια[36], κέντρων αριστείας για το κυβερνοέγκλημα[37], ή μέσω συμπράξεων δημόσιου και ιδιωτικού τομέα[38]. Ωστόσο, το έργο όλων αυτών των ενδιαφερόμενων μερών συχνά στερείται συντονισμού και συνεργειών και δεν έχει αξιοποιήσει τις δυνατότητές του να κάνει ουσιαστική διαφορά στην αγορά εργασίας, όπως καταδεικνύεται από την αυξανόμενη έλλειψη εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας στην ΕΕ. Η αύξηση των συνεργειών μεταξύ των κυβερνοκοινοτήτων είναι επίσης αναγκαία, καθώς τα απαραίτητα σύνολα δεξιοτήτων για τη διατήρηση της κυβερνοασφάλειας, την καταπολέμηση του **κυβερνοεγκλήματος** ή την ανάπτυξη δυνατοτήτων αντίδρασης στον τομέα της **κυβερνοάμυνας** είναι συχνά παρόμοιας φύσης.

Τέλος, σήμερα, η ΕΕ διαθέτει περιορισμένα μέσα αξιολόγησης της **κατάστασης και της εξέλιξης της αγοράς εργασίας για την κυβερνοασφάλεια** και των δεξιοτήτων του εργατικού δυναμικού της. Τα κράτη μέλη και τα ευρωπαϊκά θεσμικά και λοιπά όργανα και οργανισμοί βασίζονται είτε σε δεδομένα που συλλέγονται από ιδιωτικούς φορείς είτε σε ένα ευρύτερο σύνολο δεδομένων που συλλέγονται από την ΕΕ, κυρίως από την Eurostat[39] και το

[29] Κυρίως: το ευρωπαϊκό πλαίσιο κυβερνοδεξιοτήτων (ECSF)· η βάση δεδομένων για την τριτοβάθμια εκπαίδευση στον τομέα της κυβερνοασφάλειας – CYBERHEAD· η πλατφόρμα κυβερνοασκήσεων (CEP)· η Ευρωπαϊκή Πρόκληση για την Κυβερνοασφάλεια· ο ευρωπαϊκός μήνας κυβερνοασφάλειας.

[30] Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού.

[31] Κυρίως η πλατφόρμα εκπαίδευσης, κατάρτισης, ασκήσεων και αξιολόγησης (EKAA) για τον κυβερνοχώρο.

[32] Για παράδειγμα, η ομάδα εργασίας 5 του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο (ECSO) με θέμα «Εκπαίδευση, κατάρτιση, ευαισθητοποίηση, κυβερνοπεδία, ανθρώπινοι παράγοντες»· ο οργανισμός DIGITALEUROPE·

[33] Για παράδειγμα, το SANS Institute, (ISC)², ISACA.

[34] Για παράδειγμα, στις εθνικές στρατηγικές για την εκπαίδευση ή την κυβερνοασφάλεια.

[35] Για παράδειγμα, το C-Academy στην Πορτογαλία.

[36] Για παράδειγμα, οι πανεπιστημιουπόλεις για την κυβερνοασφάλεια (Cyber Campus) στη Γαλλία.

[37] Για παράδειγμα, το λιθουανικό Κέντρο Αριστείας σε θέματα κυβερνοεγκλήματος για κατάρτιση, έρευνα και εκπαίδευση στη Λιθουανία (L3CE).

[38] Για παράδειγμα, η πρωτοβουλία της Microsoft για τη δημιουργία κυβερνοδεξιοτήτων.

[39] Ειδικοί σε θέματα ΤΠΕ στην αγορά εργασίας — Επεξήγηση στατιστικών (europa.eu).

Ευρωπαϊκό Κέντρο για την Ανάπτυξη της Επαγγελματικής Κατάρτισης (CEDEFOP)[40] σχετικά με τους επαγγελματίες των ΤΠΕ. Με άλλα λόγια, η ΕΕ διαθέτει μερική και κατακερματισμένη εικόνα των αναγκών της, γεγονός που την εμποδίζει να εδραιώσει ένα συνολικό όραμα για την κατάσταση της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας.

3. Συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ: η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας

3.1.Ο στόχος

Για να αντιμετωπιστεί η πρόκληση που θέτει το ζήτημα των κυβερνοδεξιοτήτων και της κάλυψης των ελλείψεων στην αγορά εργασίας, η Επιτροπή προτείνει μια **Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας**, όπως ανακοίνωσε η πρόεδρος της Ευρωπαϊκής Επιτροπής στην επιστολή προθέσεων για την κατάσταση της Ένωσης το 2022[41, 42]και στο πλαίσιο του Ευρωπαϊκού Έτους Δεξιοτήτων.

Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας (στο εξής: Ακαδημία) αποσκοπεί στη δημιουργία ενός **ενιαίου σημείου εισόδου και συνεργειών** για την παροχή εκπαίδευσης και κατάρτισης στον τομέα της κυβερνοασφάλειας, καθώς και για ευκαιρίες χρηματοδότησης και συγκεκριμένες δράσεις για τη στήριξη της ανάπτυξης κυβερνοδεξιοτήτων. Θα επεκτείνει τις πρωτοβουλίες των ενδιαφερόμενων μερών για την επίτευξη κρίσιμης μάζας που θα κάνει τη διαφορά στην αγορά εργασίας, μεταξύ άλλων σε θέματα άμυνας. Οι εν λόγω δραστηριότητες θα ευθυγραμμιστούν με κοινούς στόχους και βασικούς δείκτες επιδόσεων, ώστε να επιδιωχθεί μεγαλύτερος αντίκτυπος.

Επίκεντρο της Ακαδημίας θα είναι η ανάπτυξη των δεξιοτήτων των **επαγγελματιών στον τομέα της κυβερνοασφάλειας**. Η δραστηριότητα της Ακαδημίας θα αξιοποιηθεί στις πολιτικές της ΕΕ για την κυβερνοασφάλεια, αλλά και στην εκπαίδευση και τη διά βίου μάθηση. Συμπληρώνει τις δύο συστάσεις του Συμβουλίου σχετικά με την ψηφιακή εκπαίδευση και τις ψηφιακές δεξιότητες που προτείνει η Επιτροπή ταυτόχρονα με την παρούσα ανακοίνωση[43].

Η Ακαδημία θα βασίζεται σε τέσσερις πυλώνες: 1) προώθηση της **παραγωγής γνώσης μέσω της εκπαίδευσης και της κατάρτισης**, με την επεξεργασία ενός κοινού πλαισίου για τα προφίλ ρόλων και τις συναφείς δεξιότητες στον τομέα της κυβερνοασφάλειας, ενίσχυση της ευρωπαϊκής προσφοράς εκπαίδευσης και κατάρτισης για την κάλυψη των αναγκών, ανάπτυξη οδών σταδιοδρομίας και προβολή και παροχή σαφήνειας όσον αφορά την κατάρτιση και τις πιστοποιήσεις στον τομέα της κυβερνοασφάλειας, ώστε να ενισχυθεί η πλευρά της προσφοράς εργασίας· 2) διασφάλιση καλύτερης διοχέτευσης και προβολής των διαθέσιμων **ευκαιριών χρηματοδότησης** για δραστηριότητες που σχετίζονται με τις δεξιότητες, προκειμένου να μεγιστοποιηθεί ο αντίκτυπός τους· 3) κάλεσμα προς τα ενδιαφερόμενα μέρη **για ανάληψη δράσης**· και 4) καθορισμός δεικτών για να **παρακολουθείται η εξέλιξη της αγοράς** και να μπορεί να αξιολογηθεί η αποτελεσματικότητα των δράσεών τους.

---

[40] Όπως το εργαλείο του CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[41] Επιστολή προθέσεων για την κατάσταση της Ευρωπαϊκής Ένωσης του 2022 προς την πρόεδρο Roberta Metsola και τον πρωθυπουργό Petr Fiala.

[42] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο — Πολιτική της ΕΕ για την κυβερνοάμυνα [JOIN(2022) 49 final].

[43] Προτάσεις για συστάσεις του Συμβουλίου σχετικά με τους καθοριστικούς παράγοντες για επιτυχή ψηφιακή εκπαίδευση και κατάρτιση, καθώς και σχετικά με τη βελτίωση της παροχής ψηφιακών δεξιοτήτων στην εκπαίδευση και την κατάρτιση.

Η υλοποίηση της Ακαδημίας θα υποστηριχθεί με χρηματοδότηση ύψους 10 εκατ. EUR από το πρόγραμμα «Ψηφιακή Ευρώπη» (DEP)[44].

3.2.Η διακυβέρνηση της Ακαδημίας

Τελικά, για την παροχή μιας υποδομής που θα λειτουργεί ως **ενιαίο σημείο εισόδου** για την προώθηση της συνεργασίας μεταξύ της ακαδημαϊκής κοινότητας, των παρόχων κατάρτισης και της βιομηχανίας, στην οποία οι πλευρές της προσφοράς και της ζήτησης του οικοσυστήματος κυβερνοασφάλειας της ΕΕ θα μπορούν να συναντιούνται και να εκπαιδεύονται, η Ακαδημία θα μπορούσε να λάβει τη μορφή **κοινοπραξίας ευρωπαϊκής ψηφιακής υποδομής (EDIC)**[45]. Το μέσο αυτό θα δώσει στα κράτη μέλη τη δυνατότητα να εργαστούν από κοινού για την κάλυψη της έλλειψης κυβερνοδεξιοτήτων, καθώς και να συνεργαστούν στενά με την Επιτροπή, τον ENISA και το ECCC, σύμφωνα με τις εντολές και τις αρμοδιότητές τους, και να διασφαλίσουν τη συμμετοχή όλων των σχετικών ενδιαφερόμενων μερών, αλλά και να κατευθύνουν τις ευρωπαϊκές, εθνικές και ιδιωτικές επενδύσεις προς έναν κοινό στόχο. Για τον σκοπό αυτό, τα ενδιαφερόμενα κράτη μέλη ενθαρρύνονται να υποβάλουν στην Επιτροπή προκαταρκτική κοινοποίηση, έως τις 30 Μαΐου 2023, της μελλοντικής τους αίτησης για μια τέτοια EDIC. Αυτή η εθελοντική εκ των προτέρων κοινοποίηση θα δώσει στην Επιτροπή τη δυνατότητα να διατυπώσει εγκαίρως παρατηρήσεις σχετικά με το σχέδιο αίτησης για EDIC, καθιστώντας έτσι δυνατή την περαιτέρω ανάπτυξή του και την επίσημη υποβολή του με ταχύτερο τρόπο. Καθ' όλη τη διάρκεια της διαδικασίας και στον βαθμό που ζητείται από τα κράτη μέλη, η Επιτροπή, ενεργώντας ως επιταχυντής πολυκρατικών έργων, θα διευκολύνει την προετοιμασία της αίτησης για EDIC. Στη συνέχεια, μετά από θετική αξιολόγηση της αίτησης από την Επιτροπή και έγκριση από την επιτροπή του προγράμματος «Ψηφιακή Δεκαετία», η Επιτροπή θα εκδώσει απόφαση για τη σύσταση της EDIC και, έπειτα, θα συμβάλει στον συντονισμό της υλοποίησης της EDIC[46].

Εν τω μεταξύ, και κατά τη διάρκεια της επίσημης σύστασης της EDIC, η Επιτροπή θα δημιουργήσει εικονικό ενιαίο σημείο εισόδου, ενισχύοντας την **πλατφόρμα της Επιτροπής για τις ψηφιακές δεξιότητες και θέσεις εργασίας**[47] με την υποστήριξη του έργου στήριξης της ευρωπαϊκής κοινότητας κυβερνοασφάλειας (ECCO)[48].

Ο **ENISA** θα συμβάλει στην υλοποίηση της Ακαδημίας σύμφωνα με τους στόχους του Οργανισμού[49], κυρίως όσον αφορά τη συνδρομή στην εκπαίδευση και την κατάρτιση στον τομέα της κυβερνοασφάλειας, και λαμβάνοντας υπόψη τις υποχρεώσεις υποβολής εκθέσεων

---

[44] Κανονισμός (ΕΕ) 2021/694 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη και την κατάργηση της απόφασης (ΕΕ) 2015/2240.

[45] Οι EDIC θεσπίστηκαν με την απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία», άρθρο 13 κ.ε.

[46] Ό.π., άρθρο 12.

[47] Αρχική σελίδα | Πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας (europa.eu).

[48] Βλ. Ευρωπαϊκό κέντρο και δίκτυο ικανοτήτων στον τομέα της κυβερνοασφάλειας: νέο έργο χρηματοδοτούμενο από την ΕΕ για τη στήριξη της κοινότητας κυβερνοασφάλειας (europa.eu). Τον Δεκέμβριο του 2022 η Ευρωπαϊκή Επιτροπή υπέγραψε σύμβαση ύψους 3 εκατ. EUR για τη στήριξη της κοινότητας κυβερνοασφάλειας της ΕΕ στο πλαίσιο του ευρωπαϊκού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας. Το έργο αυτό θα συμβάλει στην επίτευξη των στόχων της ΕΕ για την ανάπτυξη κοινοτήτων και ικανοτήτων όσον αφορά την έρευνα, την καινοτομία, την αξιοποίηση και τη βιομηχανική βάση στον τομέα της κυβερνοασφάλειας.

[49] «Ο ENISA στηρίζει την ανάπτυξη ικανοτήτων και την ετοιμότητα στην Ένωση, επικουρώντας τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, καθώς και τα κράτη μέλη και τους ιδιωτικούς και δημόσιους συμφεροντούχους, (…) την ανάπτυξη δεξιοτήτων και ικανοτήτων στο πεδίο της κυβερνοασφάλειας.». Άρθρο 4 παράγραφος 3 της πράξης για την κυβερνοασφάλεια.

που υπέχει δυνάμει της οδηγίας NIS2[50]. Το **ECCC** θα εργαστεί σύμφωνα με το στρατηγικό του θεματολόγιο για να στηρίξει την υλοποίηση της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας. Ειδικότερα, το ECCC θα υλοποιήσει τον στρατηγικό στόχο 3 (Κυβερνοασφάλεια) του προγράμματος «Ψηφιακή Ευρώπη». Θα επωφεληθεί από τη στήριξη της Επιτροπής και των κρατών μελών, μέσω των **εθνικών κέντρων συντονισμού (ΕΚΣ)**. Η **ομάδα συνεργασίας** που συστάθηκε βάσει της οδηγίας NIS2[51] θα καλείται να συμβάλει, κατά περίπτωση. Τέλος, η συνένωση δυνάμεων με τη **βιομηχανία** και την **ακαδημαϊκή κοινότητα** θα είναι απαραίτητη για την επίτευξη του στόχου της Ακαδημίας για την κάλυψη της έλλειψης κυβερνοδεξιοτήτων.

4. Παραγωγή γνώσης και κατάρτιση: θέσπιση κοινής προσέγγισης της ΕΕ όσον αφορά την κατάρτιση στον τομέα της κυβερνοασφάλειας

Στο πλαίσιο του πυλώνα παραγωγής γνώσης και κατάρτισης της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας, θα αναπτυχθεί μια δομημένη προσέγγιση με σαφή στόχο την αύξηση του **αριθμού** των ατόμων που διαθέτουν κυβερνοδεξιότητες στην ΕΕ, την καλύτερη στόχευση της κατάρτισης στις **ανάγκες της αγοράς** και την προβολή των **οδών σταδιοδρομίας**.

4.1.Μιλώντας την ίδια γλώσσα: κοινή προσέγγιση για τα προφίλ ρόλων και τις συναφείς δεξιότητες στον τομέα της κυβερνοασφάλειας

Ο ENISA έχει ήδη εργαστεί προς την κατεύθυνση του καθορισμού προφίλ ρόλων για τους επαγγελματίες στον τομέα της κυβερνοασφάλειας, στο πλαίσιο του ευρωπαϊκού πλαισίου κυβερνοδεξιοτήτων (**ECSF**)[52]. Αυτό αναμένεται να αποτελέσει τη βάση ώστε η Ακαδημία να καθορίζει και να αξιολογεί τις σχετικές δεξιότητες, να παρακολουθεί την εξέλιξη της έλλειψης δεξιοτήτων και να παρέχει ενδείξεις σχετικά με τις νέες ανάγκες. Για κάθε ρόλο κυβερνοασφάλειας του ECSF, ενσωματώνεται, ως στοιχείο της περιγραφής του προφίλ[53], ένα σύνολο εφαρμοστέων απαιτήσεων του ευρωπαϊκού πλαισίου ηλεκτρονικών δεξιοτήτων[54].

Ως εκ τούτου, ο ENISA θα επανεξετάσει το ECSF και **θα προσδιορίσει τις εξελισσόμενες ανάγκες για δεξιότητες και ελλείψεις δεξιοτήτων** στο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων μέσω προηγμένων εργαλείων (π.χ. τεχνητής νοημοσύνης, μαζικών δεδομένων[55], εξόρυξης δεδομένων). Για τον σκοπό αυτό, ο ENISA θα εργαστεί υπό την καθοδήγηση της EDIC, όταν συσταθεί, του ECCC, από κοινού με τα ΕΚΣ, την Επιτροπή, το έργο ECCO και παράγοντες της αγοράς[56]. Για το εργατικό δυναμικό στον τομέα της

---

[50] Άρθρο 18 της οδηγίας NIS 2.

[51] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2).

[52] Ευρωπαϊκό πλαίσιο κυβερνοδεξιοτήτων (ECSF) — ENISA (europa.eu). Το ECSF υποστηρίζει τον προσδιορισμό και τη διάρθρωση των καθηκόντων, των ικανοτήτων, των δεξιοτήτων και των γνώσεων που συνδέονται με τους ρόλους των Ευρωπαίων επαγγελματιών στον τομέα της κυβερνοασφάλειας. Συνοψίζει όλους τους ρόλους που σχετίζονται με την κυβερνοασφάλεια σε προφίλ, τα οποία αναλύονται μεμονωμένα στις λεπτομέρειες των αντίστοιχων αρμοδιοτήτων, δεξιοτήτων, συνεργειών και αλληλεξαρτήσεών τους.

[53] Ευρωπαϊκό πλαίσιο ηλεκτρονικών δεξιοτήτων (e-CF) | Esco (europa.eu). Το e-CF παρέχει σταθερούς δεσμούς στο πλαίσιο των δεξιοτήτων ΤΠΕ και άλλων πλαισίων συναφών με τον τομέα, συμπεριλαμβανομένου του πλαισίου ψηφιακών δεξιοτήτων DigComp.

[54] Βλ. σχετικά User Manual - European Cybersecurity Skills Framework (ECSF) (Εγχειρίδιο χρήστη – Ευρωπαϊκό πλαίσιο κυβερνοδεξιοτήτων) – Σεπτέμβριος 2022.

[55] Βλ., για παράδειγμα, το εργαλείο Skills-OVATE που αναπτύχθηκε από το Cedefop.

[56] Ο Οργανισμός θα αξιοποιήσει περαιτέρω τα αποτελέσματα άλλων χρηματοδοτούμενων από την ΕΕ έργων [π.χ. REWIRE, Χώρος δεδομένων δεξιοτήτων (DS4S), CyberSecPro, Concordia] και μεθοδολογίες που προκύπτουν από παρόμοιες πρωτοβουλίες (π.χ. «Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada,

κυβερνοάμυνας, ο ENISA θα λάβει δεόντως υπόψη το έργο της ΕΑΑΑ. Ομοίως, στον τομέα της καταπολέμησης του κυβερνοεγκλήματος, ο ENISA θα λάβει υπόψη τις δραστηριότητες του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου (CEPOL) και της Ευρωπόλ για τη θέσπιση επιχειρησιακής ανάλυσης των αναγκών κατάρτισης[57] σχετικά με κυβερνοεπιθέσεις.

Το ECSF θα συμπληρώνεται και θα επανεξετάζεται τακτικά στο πλαίσιο της Ακαδημίας καθ' όλη τη διάρκεια ενός διετούς κύκλου. Επίσης, η Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης θα συμβάλουν στον καθορισμό ειδικών προφίλ και συναφών δεξιοτήτων για τους τομείς, ανάλογα με τις ανάγκες, με την υποστήριξη οργανισμών και οργάνων της ΕΕ, όπως η ΕΑΑΑ[58], η Ευρωπόλ και ο CEPOL[59].

Θα δημιουργηθούν επίσης δεσμοί μεταξύ του ECSF και των σχετικών μέσων της πολιτικής της ΕΕ για την απασχόληση[60]. Ειδικότερα, τα προφίλ εργασίας του ECSF καθώς και οι συναφείς δεξιότητες θα ενσωματωθούν στην **ευρωπαϊκή ταξινόμηση δεξιοτήτων, ικανοτήτων και επαγγελμάτων**. Αυτό θα βελτιώσει την ταξινόμηση και τους δεσμούς μεταξύ επαγγελμάτων και δεξιοτήτων στον τομέα της κυβερνοασφάλειας, διευκολύνοντας την αναβάθμιση των δεξιοτήτων και επανειδίκευση των ατόμων και στηρίζοντας την αντιστοίχιση των θέσεων εργασίας με βάση τις δεξιότητες και τη διασυνοριακή κινητικότητα.

4.2.Προώθηση της συνεργασίας για τον σχεδιασμό προγραμμάτων εκπαίδευσης και κατάρτισης στον τομέα της κυβερνοασφάλειας

Μόλις συσταθεί η EDIC, η Ακαδημία θα πρέπει να λάβει στήριξη από τα κράτη μέλη ώστε να καταστεί **σημείο αναφοράς στην Ευρώπη για τον σχεδιασμό και την παροχή κατάρτισης στον τομέα της κυβερνοασφάλειας**, καλύπτοντας τις δεξιότητες που έχουν τη μεγαλύτερη ζήτηση, και να παρέχει ευκαιρίες κατάρτισης και πρακτικής άσκησης στον χώρο εργασίας για νεοφυείς επιχειρήσεις και ΜΜΕ, καθώς και για δημόσιες διοικήσεις σε καινοτόμες εταιρείες στον τομέα της κυβερνοασφάλειας και σε κέντρα κυβερνοδεξιοτήτων. Η EDIC θα πρέπει να συνεργαστεί με όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένης της βιομηχανίας, για τον σχεδιασμό των εν λόγω προγραμμάτων κατάρτισης και να αξιοποιήσει έργα όπως το **CyberSecPro**[61] που χρηματοδοτείται από το πρόγραμμα «Ψηφιακή Ευρώπη», στο οποίο συμμετέχουν 17 ιδρύματα τριτοβάθμιας

New Zealand, United Kingdom and United States» (Δημιουργία ειδικευμένου εργατικού δυναμικού για την κυβερνοασφάλεια σε πέντε χώρες: Πληροφορίες από την Αυστραλία, τον Καναδά, τη Νέα Ζηλανδία, το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες), έκθεση του ΟΟΣΑ, η οποία δημοσιεύθηκε στις 21 Μαρτίου 2023) για να διασφαλιστεί στο μέλλον ένα επικαιροποιημένο όραμα των αναγκών σε ένα περιβάλλον στο οποίο η ζήτηση εξελίσσεται συνεχώς.

[57] CEPOL, Αξιολόγηση επιχειρησιακών αναγκών κατάρτισης (OTNA).

[58] Βλ., συναφώς, κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο — Πολιτική της ΕΕ για την κυβερνοάμυνα [JOIN(2022) 49 final].

[59] Στο πλαίσιο αυτό, θα δοθεί προσοχή στις εργασίες σχετικά με το πλαίσιο ικανοτήτων για την κατάρτιση στον τομέα του κυβερνοεγκλήματος (TCF), το οποίο εκπονείται επί του παρόντος.

[60] Όπως η ευρωπαϊκή ταξινόμηση δεξιοτήτων, ικανοτήτων και επαγγελμάτων (ESCO), το Europass, το ευρωπαϊκό δίκτυο συνεργασίας των υπηρεσιών απασχόλησης (EURES).

[61] CyberSecPro. Θα διενεργήσει, για παράδειγμα, ανάλυση των προγραμμάτων, των μαθημάτων και των θερινών σχολείων στον τομέα της κυβερνοασφάλειας που προσφέρονται στα πανεπιστήμια και των χρησιμοποιούμενων πινάκων κατάταξης του ευρωπαϊκού συστήματος μεταφοράς και συσσώρευσης ακαδημαϊκών μονάδων (ECTS), θα διασφαλίσει τη συμμετοχή του στοχευόμενου αριθμού εκπαιδευομένων, ήτοι πάνω από 530, κατά τη διάρκεια της τριετούς περιόδου, θα εκπαιδεύσει εξωτερικούς εκπαιδευόμενους από διάφορους κλάδους και τομείς.

εκπαίδευσης και 13 εταιρείες ασφάλειας από 16 κράτη μέλη, προκειμένου να αποτελέσει τη βέλτιστη πρακτική για όλα τα προγράμματα κατάρτισης στον τομέα της κυβερνοασφάλειας.

Η Ακαδημία θα συνεργαστεί με όλα τα σχετικά ενδιαφερόμενα μέρη για **να προσελκύσει τις νέες γενιές** ώστε να ακολουθήσουν σταδιοδρομία στον τομέα της κυβερνοασφάλειας. Σύμφωνα με την πρόταση για σύσταση του Συμβουλίου για τη βελτίωση της παροχής ψηφιακών δεξιοτήτων στην εκπαίδευση και την κατάρτιση, τα κράτη μέλη θα πρέπει να θεσπίσουν και να ενισχύσουν μέτρα για την πρόσληψη και την κατάρτιση ειδικευμένων εκπαιδευτικών και εκπαιδευτών και τη διευκόλυνση της απόκτησης κυβερνοδεξιοτήτων, μεταξύ άλλων μέσω τοποθετήσεων σε θέσεις μαθητείας. Θα πρέπει να ενθαρρυνθούν η ενσωμάτωση της κυβερνοασφάλειας στα προγράμματα εκπαίδευσης και κατάρτισης, παράλληλα με τη διασφάλιση της προσβασιμότητάς τους, η ανάπτυξη των προσφερόμενων θέσεων **μαθητείας** και πρακτικής άσκησης, η προώθηση καινοτόμων προσεγγίσεων, συμπεριλαμβανομένων, για παράδειγμα, σοβαρών παιχνιδιών και κοινών πλατφορμών προσομοίωσης, η διοργάνωση εβδομάδων εντατικής εκπαίδευσης σε θέσεις κυβερνοασφάλειας, η επεξήγηση των μη τεχνικών προφίλ ρόλων. Θα πρέπει επίσης να υποστηριχθεί η συμμετοχή, σε αυτές τις ευκαιρίες μάθησης για την κυβερνοασφάλεια, ομάδων που είναι δυσπρόσιτες, όπως νέων με αναπηρία, νέων που ζουν σε απομακρυσμένες ή αγροτικές περιοχές, καθώς και από άλλες μειονοτικές ομάδες.

Η Επιτροπή θα συνεχίσει να παρέχει στήριξη για την ανάπτυξη μικροδιαπιστευτηρίων και προγραμμάτων επαγγελματικής εκπαίδευσης και κατάρτισης. Ειδικότερα, στο πλαίσιο του Erasmus+ θα εξακολουθήσουν να χρηματοδοτούνται **κοινά προγράμματα προπτυχιακών και μεταπτυχιακών σπουδών, κοινά μαθήματα ή κοινές διδακτικές ενότητες που μπορούν να οδηγήσουν στη χορήγηση μικροδιαπιστευτηρίων** και **μεικτά εντατικά προγράμματα**[62] για όλα τα θέματα, συμπεριλαμβανομένης της **κυβερνοασφάλειας**. Η περαιτέρω ανάπτυξη της **πρωτοβουλίας σχετικά με τα δίκτυα ευρωπαϊκών πανεπιστημίων**[63] και των **κέντρων επαγγελματικής αριστείας**[64] θα υποστηριχθεί επίσης για να ενθαρρυνθεί η ενίσχυση της συνεργασίας μεταξύ ιδρυμάτων τριτοβάθμιας εκπαίδευσης και σχετικών ιδρυμάτων επαγγελματικής εκπαίδευσης και κατάρτισης σε ολόκληρη την Ευρώπη. Αυτόν τον στόχο της βαθύτερης συνεργασίας θα στηρίξουν τα χρηματοδοτικά προγράμματα της ΕΕ, συμπεριλαμβανομένων των προγραμμάτων Erasmus+ και «Ψηφιακή Ευρώπη», όπως και κονδύλια της ΕΕ για την ανάπτυξη **ατομικών λογαριασμών μάθησης**[65].

Για τη διευκόλυνση της συνεργασίας, σε εθνικό επίπεδο, της ακαδημαϊκής κοινότητας και των παρόχων κατάρτισης σε θέματα κυβερνοδεξιοτήτων με εργοδότες του ιδιωτικού και του δημόσιου τομέα και για την προώθηση συνεργειών μεταξύ του δημόσιου και του ιδιωτικού τομέα, τα ΕΚΣ καλούνται να διερευνήσουν το ενδεχόμενο δημιουργίας **πανεπιστημιουπόλεων για την κυβερνοασφάλεια** στα κράτη μέλη. Στόχος των πανεπιστημιουπόλεων για την κυβερνοασφάλεια θα είναι η παροχή πόλων αριστείας σε εθνικό επίπεδο για την κοινότητα της κυβερνοασφάλειας και η Ακαδημία θα συμβάλει στη δικτύωσή τους και στον περαιτέρω συντονισμό των δραστηριοτήτων τους.

[62] Τα μεικτά εντατικά προγράμματα συνδυάζουν επιγραμμική διδασκαλία με μια σύντομη περίοδο φυσικής κινητικότητας.

[63] Πρωτοβουλία σχετικά με τα δίκτυα ευρωπαϊκών πανεπιστημίων | Ευρωπαϊκός Χώρος Εκπαίδευσης (europa.eu).

[64] Κέντρα επαγγελματικής αριστείας | Erasmus+ (europa.eu).

[65] Σύμφωνα με τη σύσταση του Συμβουλίου, της 16ης Ιουνίου 2022, για τους ατομικούς λογαριασμούς μάθησης.

Ο ENISA θα ενισχύσει επίσης την κατάρτιση που προσφέρει στον τομέα της κυβερνοασφάλειας, ευθυγραμμίζοντας τον **κατάλογο εκπαιδευτικών προγραμμάτων**[66] του με τα προφίλ του ECSF και αναπτύσσοντας διδακτικές ενότητες κατάρτισης ανά προφίλ, γεγονός που μπορεί να ενισχύσει την προσφορά κατάρτισης από τα κράτη μέλη. Ο ENISA θα επεκτείνει επίσης το **πρόγραμμα κατάρτισης των εκπαιδευτών**[67], με στόχο την κάλυψη των επαγγελματικών αναγκών των ευρωπαϊκών θεσμικών και λοιπών οργάνων και οργανισμών, των δημόσιων αρχών των κρατών μελών και των **δημόσιων και ιδιωτικών κρίσιμων φορέων εκμετάλλευσης** που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS2.

Επίσης, άλλοι οργανισμοί και όργανα της ΕΕ θα ενισχύσουν την οικεία προσφορά κατάρτισης σε θέματα κυβερνοασφάλειας. Για παράδειγμα, εφαρμόζοντας την πολιτική της ΕΕ για την κυβερνοάμυνα, η **ΕΑΑΑ** θα αναπτύξει ένα νέο σύνολο μαθημάτων για την κυβερνοασφάλεια και θα ευθυγραμμίσει ορισμένα από τα τρέχοντα μαθήματα με το ECSF. Με την ολοκλήρωση των μαθημάτων θα παρέχεται πιστοποίηση των μαθησιακών αποτελεσμάτων[68]. Η ΕΑΑΑ, σε συνεργασία με την Επιτροπή, θα διερευνήσει τη δυνατότητα ενσωμάτωσης πιστοποιητικών στο ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας (EUeID). Η ΕΑΑΑ θα διερευνήσει περαιτέρω το ενδεχόμενο αξιολόγησης των μηχανισμών δεξιοτήτων, βάσει των οποίων θα εκδίδονται τα πιστοποιητικά. Ομοίως, στον τομέα της καταπολέμησης του κυβερνοεγκλήματος, θα επιδιωχθεί στενή σύνδεση με την **Ακαδημία Κυβερνοεγκλήματος του CEPOL**[69], ώστε να ενισχυθούν οι συνέργειες και η συμπληρωματικότητα στον σχεδιασμό και την εφαρμογή των προγραμμάτων κατάρτισης.

4.3.Δημιουργία συνεργειών και προβολή της κατάρτισης και της πιστοποίησης στον τομέα της κυβερνοασφάλειας σε όλα τα κράτη μέλη

Η Ακαδημία θα πρέπει να ασχοληθεί με το ζήτημα της προβολής και των συνεργειών της κατάρτισης και της πιστοποίησης. Αυτό θα ωφελήσει τις μη στρατιωτικές κοινότητες, τις κοινότητες άμυνας, τις κοινότητες επιβολής του νόμου και τις διπλωματικές κοινότητες στον κυβερνοχώρο, καθώς όλοι οι τομείς απαιτούν σε πολλές περιπτώσεις την ίδια εμπειρογνωσία, βάσει παρόμοιων προγραμμάτων σπουδών και μαθησιακών αποτελεσμάτων.

Η Ακαδημία θα παρέχει **ενιαίο σημείο εισόδου** για όσους ενδιαφέρονται να σταδιοδρομήσουν στον τομέα της κυβερνοασφάλειας. Βραχυπρόθεσμα, αυτό θα επιτευχθεί με την ενίσχυση της **πλατφόρμας της Επιτροπής για τις ψηφιακές δεξιότητες και θέσεις εργασίας**, με την υποστήριξη του έργου ECCO. Ένα ειδικό τμήμα για τις δυνατότητες σταδιοδρομίας στον τομέα της κυβερνοασφάλειας θα συνδεθεί με τα υφιστάμενα εργαλεία, από τα προγράμματα τριτοβάθμιας εκπαίδευσης έως τις ευκαιρίες κατάρτισης, συμπεριλαμβανομένων μαθημάτων για τη χορήγηση μικροδιαπιστευτηρίων και προγραμμάτων επαγγελματικής εκπαίδευσης και κατάρτισης, και τις προσφορές θέσεων εργασίας. Αυτό θα επιτευχθεί με αναφορά ή ενσωμάτωση στις εργασίες και πρωτοβουλίες που βρίσκονται σε εξέλιξη στην πλατφόρμα, όπως αυτές του ENISA, ο οποίος, σε συνεργασία με την ακαδημαϊκή κοινότητα, έχει προβεί σε **χαρτογράφηση των εκπαιδευτικών ιδρυμάτων** που παρέχουν προγράμματα κυβερνοασφάλειας. Αυτό θα

[66] Προγράμματα κατάρτισης – ENISA (europa.eu).

[67] Πρόγραμμα κατάρτισης των εκπαιδευτών – ENISA (europa.eu).

[68] Σύμφωνα με το άρθρο 20 παράγραφος 4 της απόφασης (ΚΕΠΠΑ) 2020/1515 του Συμβουλίου, της 19ης Οκτωβρίου 2020, για την ίδρυση Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας και την κατάργηση της απόφασης (ΚΕΠΠΑ) 2016/2382.

[69] Η Ακαδημία Κυβερνοεγκλήματος του CEPOL ιδρύθηκε το 2019 με σκοπό να παράσχει μια υπερσύγχρονη πλατφόρμα για τη βελτίωση των γνώσεων στον τομέα του κυβερνοεγκλήματος και των ικανοτήτων κυβερνοασφάλειας στην Ευρώπη.

ενισχυθεί περαιτέρω με τη στήριξη των ΕΚΣ. Επίσης, ο ENISA θα αναπτύξει και θα καθιερώσει δύο **αποθετήρια υφιστάμενων προγραμμάτων κατάρτισης στον δημόσιο και τον ιδιωτικό τομέα και πιστοποιήσεων κυβερνοασφάλειας**, με την υποστήριξη των ΕΚΣ, της Επιτροπής και του έργου ECCO, και σε συνεργασία με οντότητες που χορηγούν πιστοποιήσεις, αξιοποιώντας επίσης άλλες σχετικές πρωτοβουλίες[70]. Αυτά θα ενοποιηθούν επίσης με το ενιαίο σημείο εισόδου της πλατφόρμας για τις ψηφιακές δεξιότητες και θέσεις εργασίας. Το έργο αυτό θα ωφελήσει επίσης τα ΕΚΣ, έργο των οποίων είναι κυρίως η προώθηση και η διάδοση εκπαιδευτικών προγραμμάτων κυβερνοασφάλειας[71].

Είναι επίσης αναγκαίο να παρέχονται εγγυήσεις στους επαγγελματίες ότι τα προγράμματα κατάρτισης που παρακολουθούν έχουν την απαιτούμενη ποιότητα. Στο πλαίσιο αυτό, ο ENISA θα αναπτύξει **πιλοτικό έργο**, με το οποίο θα διερευνηθεί η δημιουργία ενός ευρωπαϊκού συστήματος πιστοποίησης των κυβερνοδεξιοτήτων.

Επίσης, είναι ουσιαστικής σημασίας να προσδιοριστούν οι δεξιότητες και η κατάρτιση και να συνδεθούν με ένα προφίλ εργασίας, αλλά είναι επίσης σημαντικό να διασφαλιστεί ότι οι υπηρεσίες κυβερνοασφάλειας παρέχονται με την απαιτούμενη ικανότητα, εμπειρογνωσία και πείρα. Αυτό ισχύει ιδίως για τους παρόχους υπηρεσιών διαχείρισης της ασφάλειας σε τομείς όπως η αντιμετώπιση περιστατικών, οι δοκιμές διείσδυσης, οι έλεγχοι ασφάλειας και η παροχή συμβουλών. Η οδηγία NIS2 και η πρόταση πράξης για την αλληλεγγύη στον κυβερνοχώρο ορίζουν συγκεκριμένα καθήκοντα για τους εν λόγω παρόχους υπηρεσιών διαχείρισης της ασφάλειας. Ως εκ τούτου, η Επιτροπή προτείνει επίσης **στοχευμένη τροποποίηση της πράξης για την κυβερνοασφάλεια**[72], ώστε να δοθεί δυνατότητα για συστήματα πιστοποίησης των υπηρεσιών διαχείρισης της ασφάλειας σε επίπεδο ΕΕ. Τα εν λόγω συστήματα πιστοποίησης θα πρέπει να αποσκοπούν, μεταξύ άλλων, στο να διασφαλίζεται ότι οι υπηρεσίες αυτές παρέχονται από προσωπικό με πολύ υψηλό επίπεδο τεχνικών γνώσεων και ικανοτήτων στους σχετικούς τομείς.

Οι **μηχανισμοί διασφάλισης της ποιότητας και αναγνώρισης για τη χορήγηση μικροδιαπιστευτηρίων**[73] διευκολύνουν τη διαφάνεια, τη συγκρισιμότητα και τη φορητότητα των μαθησιακών αποτελεσμάτων. Σύμφωνα με τη σύσταση του Συμβουλίου σχετικά με μια ευρωπαϊκή προσέγγιση για τα μικροδιαπιστευτήρια[74], τα κράτη μέλη ενθαρρύνονται να συμπεριλάβουν τα μικροδιαπιστευτήρια κυβερνοασφάλειας στα οικεία εθνικά πλαίσια επαγγελματικών προσόντων. Αυτό θα τους δώσει τη δυνατότητα να συνδέσουν τα μικροδιαπιστευτήρια κυβερνοασφάλειας με το ευρωπαϊκό πλαίσιο επαγγελματικών

[70] Για παράδειγμα, η Ακαδημία W4C – Women4Cyber ή το έργο παγκόσμιας πιστοποίησης στον τομέα του κυβερνοεγκλήματος για τις αρχές επιβολής του νόμου και τις δικαστικές αρχές.

[71] «1. Τα εθνικά κέντρα συντονισμού έχουν τα ακόλουθα καθήκοντα: (…) ζ) με την επιφύλαξη των αρμοδιοτήτων των κρατών μελών για την εκπαίδευση και λαμβανομένων υπόψη των σχετικών καθηκόντων του ENISA, συνεργάζονται με τις εθνικές αρχές σχετικά με πιθανή συμβολή στην προώθηση και τη διάδοση εκπαιδευτικών προγραμμάτων κυβερνοασφάλειας», άρθρο 7 παράγραφος 1 στοιχείο ζ) του κανονισμού για το ECCC. Βλ. επίσης τη σχετική αιτιολογική σκέψη 28.

[72] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια).

[73] Για παράδειγμα, αρχείο ή πιστοποιητικά μαθησιακών αποτελεσμάτων που αποκτώνται μετά από σύντομα προγράμματα κατάρτισης.

[74] Σύσταση του Συμβουλίου σχετικά με μια ευρωπαϊκή προσέγγιση για τα μικροδιαπιστευτήρια για τη δια βίου μάθηση και την απασχολησιμότητα.

προσόντων[75]. Η υποδομή ευρωπαϊκών ψηφιακών διαπιστευτηρίων για τη μάθηση είναι διαθέσιμη για την έκδοση ψηφιακά υπογεγραμμένων τίτλων προσόντων και μικροδιαπιστευτηρίων κυβερνοασφάλειας για φυσικά πρόσωπα. Αυτά περιέχουν πολλά δεδομένα, μεταξύ άλλων σχετικά με τα μαθησιακά αποτελέσματα στον τομέα της κυβερνοασφάλειας, και μπορούν να αποθηκευτούν στο μελλοντικό **ψηφιακό πορτοφόλι EUeID**[76].

Δράσεις στο πλαίσιο της Ακαδημίας

Κράτη μέλη και βιομηχανία

- Διασφάλιση της στήριξης για την ανάπτυξη και την αναγνώριση **μικροδιαπιστευτηρίων** μάθησης στον τομέα της κυβερνοασφάλειας, σύμφωνα με τη σύσταση του Συμβουλίου σχετικά με μια ευρωπαϊκή προσέγγιση για τα μικροδιαπιστευτήρια.
- Ένταξη των προσόντων στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των μικροδιαπιστευτηρίων, στα **εθνικά πλαίσια επαγγελματικών προσόντων**.
- Παροχή **ευκαιριών μάθησης στον χώρο εργασίας** μέσω προγραμμάτων μαθητείας για άτομα που συμμετέχουν σε πρωτοβουλίες ανάπτυξης κυβερνοδεξιοτήτων.

Επιτροπή

- Βραχυπρόθεσμα, δημιουργία **ενιαίου σημείου εισόδου** για προγράμματα κυβερνοασφάλειας, υφιστάμενα προγράμματα κατάρτισης και πιστοποιήσεις κυβερνοασφάλειας μέσω της **πλατφόρμας για τις ψηφιακές δεξιότητες και θέσεις εργασίας**, έως το τέλος του 2023.
- Πρόταση τροποποίησης της **πράξης για την κυβερνοασφάλεια**, ώστε να καταστεί δυνατή η πιστοποίηση των παρόχων υπηρεσιών διαχείρισης της ασφάλειας στις 18 Απριλίου 2023.

Όργανα και οργανισμοί της ΕΕ

- Καθιέρωση του **ECSF** ως κοινής προσέγγισης για τα προφίλ ρόλων και τις συναφείς δεξιότητες στον τομέα της κυβερνοασφάλειας έως το τέλος του 2023.
- Έναρξη, από τον ENISA, της υλοποίησης πιλοτικού έργου για τη δημιουργία **ευρωπαϊκού συστήματος πιστοποίησης** κυβερνοδεξιοτήτων το δεύτερο τρίμηνο του 2023.
- Επανεξέταση, από τον ENISA, του οικείου **καταλόγου εκπαιδευτικών προγραμμάτων** και άνοιγμα του οικείου **προγράμματος κατάρτισης των εκπαιδευτών** σε δημόσιους και ιδιωτικούς κρίσιμους φορείς εκμετάλλευσης έως το τέλος του 2023.
- Ολοκλήρωση της **ευθυγράμμισης των προγραμμάτων σπουδών της EAAA με το ECSF** έως τα μέσα του 2023.

5. Συμμετοχή των ενδιαφερόμενων μερών: δέσμευση για την κάλυψη της έλλειψης κυβερνοδεξιοτήτων

[75] Σύσταση του Συμβουλίου, της 22ας Μαΐου 2017, σχετικά με το ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων για τη διά βίου μάθηση και με την κατάργηση της σύστασης του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Απριλίου 2008, σχετικά με τη θέσπιση του ευρωπαϊκού πλαισίου επαγγελματικών προσόντων για τη διά βίου μάθηση.

[76] Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 όσον αφορά τη θέσπιση πλαισίου για την ευρωπαϊκή ψηφιακή ταυτότητα.

Στο πλαίσιο της Ακαδημίας, θα αναπτυχθεί μια συντονισμένη προσέγγιση όσον αφορά τη συμμετοχή των ενδιαφερόμενων μερών για την αντιμετώπιση της έλλειψης κυβερνοδεξιοτήτων. Στόχος θα είναι η μεγιστοποίηση της προβολής και του αντικτύπου των δεσμεύσεων που αναλαμβάνουν τα διάφορα ενδιαφερόμενα μέρη με στόχο τη μείωση της έλλειψης κυβερνοδεξιοτήτων.

Η Επιτροπή καλεί τα ενδιαφερόμενα μέρη να αναλάβουν συγκεκριμένες δεσμεύσεις για την αναβάθμιση των δεξιοτήτων και επανειδίκευση των εργαζομένων μέσω ειδικών δράσεων, βασιζόμενα όσο το δυνατόν περισσότερο στην έλλειψη κυβερνοδεξιοτήτων που έχει προσδιοριστεί. Οι εν λόγω **δεσμεύσεις των ενδιαφερόμενων μερών για την κυβερνοασφάλεια** θα πρέπει να αναφέρονται στην **πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας**, όπως και άλλες ψηφιακές δεσμεύσεις που είναι ήδη ορατές στην πλατφόρμα. Η Επιτροπή ενθαρρύνει επίσης τα ενδιαφερόμενα μέρη που αναλαμβάνουν δέσμευση για την κυβερνοασφάλεια στην πλατφόρμα να συμμετάσχουν στην **ψηφιακή σύμπραξη μεγάλης κλίμακας στο πλαίσιο του συμφώνου για τις δεξιότητες**[77]. Ενθαρρύνεται η υποβολή των δεσμεύσεων για την κυβερνοασφάλεια που αναλαμβάνονται βάσει της ψηφιακής σύμπραξης μεγάλης κλίμακας στην πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας. Ομοίως, ενθαρρύνεται η αναφορά των δεσμεύσεων που αναλαμβάνονται βάσει της πλατφόρμας για τις ψηφιακές δεξιότητες και θέσεις εργασίας στο πλαίσιο της ψηφιακής σύμπραξης μεγάλης κλίμακας του συμφώνου για τις δεξιότητες.

Η Επιτροπή καλεί επίσης τα κράτη μέλη να **συνεχίσουν τις προσπάθειες για την εφαρμογή της δήλωσης για τις γυναίκες στον ψηφιακό τομέα**[78], ώστε να ενθαρρυνθούν οι γυναίκες να διαδραματίσουν ενεργό και εξέχοντα ρόλο στον τομέα της ψηφιακής τεχνολογίας και να επιτευχθεί σύγκλιση των φύλων σε θέσεις κυβερνοασφάλειας. Η Επιτροπή ενθαρρύνει επίσης τα κράτη μέλη να αναπτύξουν συνέργειες με τα οικεία προγράμματα του **Ευρωπαϊκού Κοινωνικού Ταμείου+** (ΕΚΤ+) για την περαιτέρω στήριξη του στόχου της ισότητας των φύλων στη συμμετοχή στην εργασία[79], για παράδειγμα μέσω της θέσπισης **προγραμμάτων καθοδήγησης για κορίτσια και γυναίκες.** Αυτά μπορούν να διευκολύνουν την ανάπτυξη προτύπων ρόλων για την προσέλκυση κοριτσιών σε επαγγέλματα κυβερνοασφάλειας, καταπολεμώντας ταυτόχρονα στερεότυπα που σχετίζονται με το φύλο. Ενθαρρύνει επίσης την αναβάθμιση των δεξιοτήτων και επανειδίκευση των γυναικών και προωθεί την ανάπτυξη μιας κοινότητας, η οποία μπορεί να στηρίξει τις γυναίκες κατά την είσοδο ή την προαγωγή τους στην αγορά εργασίας στον τομέα της κυβερνοασφάλειας.

Τα κράτη μέλη θα πρέπει να θεσπίσουν, στο πλαίσιο **των οικείων εθνικών στρατηγικών για την κυβερνοασφάλεια, ειδικά μέτρα για τον μετριασμό της έλλειψης κυβερνοδεξιοτήτων**[80], τον προσδιορισμό και την καλύτερη διοχέτευση των προσπαθειών για την κάλυψη των ελλείψεων δεξιοτήτων και, τελικά, τη διασφάλιση της ορθής εφαρμογής των υποχρεώσεών τους βάσει της οδηγίας NIS2.

---

[77] Νέες ευρωπαϊκές συμπράξεις που δρομολογήθηκαν για την υλοποίηση των φιλοδοξιών της ΕΕ για την ψηφιακή δεκαετία | Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης (europa.eu), οι οποίες διαμορφώθηκαν βάσει του συμφώνου για τις δεξιότητες για την αντιμετώπιση της έλλειψης στις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ).

[78] Οι χώρες της ΕΕ δεσμεύονται να τονώσουν τη συμμετοχή γυναικών στον ψηφιακό τομέα | Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης (europa.eu).

[79] Άρθρο 4 παράγραφος 1 στοιχείο γ) του κανονισμού (ΕΕ) 2021/1057 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Ιουνίου 2021, περί ιδρύσεως του Ευρωπαϊκού Κοινωνικού Ταμείου+ (ΕΚΤ+) και καταργήσεως του κανονισμού (ΕΕ) αριθ. 1296/2013.

[80] Άρθρο 7 παράγραφος 2 στοιχείο στ) της οδηγίας NIS2.

Ορισμένα κράτη μέλη αξιοποιούν συνέργειες μεταξύ πρωτοβουλιών **στον μη στρατιωτικό τομέα, στον τομέα της άμυνας και στον τομέα επιβολής του νόμου**. Για παράδειγμα, η ανάπτυξη εργατικού δυναμικού με τη χρήση της οικείας εθνικής υποχρεωτικής στρατιωτικής θητείας ή η χρήση εφέδρων κυβερνοασφάλειας, οι οποίοι είναι πολίτες με στρατιωτική εκπαίδευση που καλύπτουν θέσεις κυβερνοασφάλειας στις ένοπλες δυνάμεις[81], επιτρέπει στον πληθυσμό, και ιδίως στους νέους ενήλικες, να αυξήσουν τις δεξιότητές τους στους τομείς της κυβερνοασφάλειας και της κυβερνοάμυνας. Το ίδιο ισχύει στον τομέα της **καταπολέμησης του κυβερνοεγκλήματος**, καθώς υπάρχουν πολλές ομοιότητες μεταξύ των γενικών προσπαθειών κυβερνοασφάλειας και των δραστηριοτήτων επιβολής του νόμου για την αντιμετώπιση περιστατικών κυβερνοασφάλειας. Η Επιτροπή ενθαρρύνει τις συζητήσεις μεταξύ των κρατών μελών σχετικά με τέτοιες πρωτοβουλίες και τα καλεί να αξιολογήσουν τον τρόπο με τον οποίο ένα ειδικευμένο εργατικό δυναμικό μπορεί να εξυπηρετήσει καλύτερα τόσο τις αμυντικές όσο και τις μη στρατιωτικές κοινότητες κυβερνοασφάλειας.

Η Επιτροπή θα εξετάσει προτάσεις σχετικά με τον τρόπο κάλυψης των υφιστάμενων και των αναμενόμενων ελλείψεων που προσδιορίζονται στην επανεξέταση των αναγκών των ευρωπαϊκών θεσμικών και λοιπών οργάνων και οργανισμών. Ειδικότερα, θα ενθαρρύνει το προσωπικό να επωφεληθεί από την επικείμενη **υποτροφία ΕΕ – Ηνωμένων Πολιτειών (ΗΠΑ) για την κυβερνοασφάλεια**, η οποία θα θεσπιστεί στο πλαίσιο του διαλόγου ΕΕ–ΗΠΑ.

Δράσεις στο πλαίσιο της Ακαδημίας

Η βιομηχανία

- Πρόταση ανάληψης συγκεκριμένων **δεσμεύσεων για την κυβερνοασφάλεια** στην πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας από τις 18 Απριλίου 2023.

Κράτη μέλη

- Συμπερίληψη στις **εθνικές στρατηγικές κυβερνοασφάλειας** ειδικών μέτρων για την αντιμετώπιση της έλλειψης κυβερνοδεξιοτήτων.

Κράτη μέλη και βιομηχανία

- Υλοποίηση της δήλωσης για τις γυναίκες στον ψηφιακό τομέα και επίτευξη **σύγκλισης των φύλων σε θέσεις κυβερνοασφάλειας** έως το 2030.

6. Χρηματοδότηση: δημιουργία συνεργειών με σκοπό τη μεγιστοποίηση του αντικτύπου των δαπανών για την ανάπτυξη κυβερνοδεξιοτήτων

Στο πλαίσιο της Ακαδημίας, ο αντίκτυπος των επενδύσεων σε κυβερνοδεξιότητες θα μεγιστοποιηθεί με την παροχή ενός κοινού σημείου εισόδου, τη διευκόλυνση της καλύτερης διοχέτευσης των κονδυλίων σύμφωνα με τις ανάγκες της αγοράς και τη συνεκτίμηση της χρήσης της χρηματοδότησης, τη διευκόλυνση των συνεργειών μεταξύ των διαφόρων μέσων και την αποφυγή της αλληλεπικάλυψης των προσπαθειών[82].

[81] Έκθεση – Cyber Conscription: Experience and Best Practice from Selected Countries, Martin Hurt και Tiia Sõmer, Διεθνές Κέντρο Άμυνας και Ασφάλειας, Φεβρουάριος 2021.

[82] Ευκαιρίες χρηματοδότησης (europa.eu). Οι υπηρεσίες υποστήριξης του συμφώνου για τις δεξιότητες παρέχουν ένα ενιαίο σημείο εισόδου για πληροφορίες σχετικά με τη χρηματοδότηση δεξιοτήτων, μεταξύ άλλων για το ψηφιακό οικοσύστημα. Οι υπηρεσίες υποστήριξης του συμφώνου παρέχουν γενικές πληροφορίες σχετικά με χρηματοδοτικά μέσα που δεν

6.1. Αντιστοίχιση των κονδυλίων με τις ανάγκες

Στο πλαίσιο της Ακαδημίας, το ECCC, με την υποστήριξη της Επιτροπής, του έργου ECCO και των ΕΚΣ, θα συγκεντρώσει **πληροφορίες σχετικά με τον τρόπο με τον οποίο χρησιμοποιούνται τα κονδύλια της ΕΕ για τη χρηματοδότηση κυβερνοδεξιοτήτων** και θα αξιολογήσει τον τρόπο με τον οποίο τα κονδύλια της ΕΕ στηρίζουν τη μείωση της έλλειψης κυβερνοδεξιοτήτων. Λαμβάνοντας υπόψη αυτές τις συγκεντρωτικές πληροφορίες, το ECCC θα επιδιώξει να διασφαλίζει την καλύτερη διοχέτευση των κονδυλίων της ΕΕ για την κάλυψη των αναγκών που εντοπίζονται. Θα χρηματοδοτεί δράσεις για την αντιμετώπιση των πιο πιεστικών ελλείψεων στο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων εκείνων που σχετίζονται με την κάλυψη των αναγκών της πολιτικής για την κυβερνοασφάλεια.

6.2. Προβολή των διαθέσιμων κονδυλίων και των πρωτοβουλιών σύμπραξης για κυβερνοδεξιότητες

Βραχυπρόθεσμα, η **πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας** θα αποτελέσει ενιαίο σημείο εισόδου για τα ενδιαφερόμενα μέρη, στο οποίο θα είναι διαθέσιμες όλες οι πληροφορίες σχετικά με τις ευκαιρίες χρηματοδότησης για κυβερνοδεξιότητες.

Η ΕΕ επενδύει στους ανθρώπους και στις δεξιότητές τους και χρησιμοποιεί συμπράξεις, κυρίως με τη βιομηχανία, για την κινητοποίηση δράσεων για την αναβάθμιση των δεξιοτήτων και την επανειδίκευση μέσω διαφόρων μέσων που προσδιορίζονται στο **ευρωπαϊκό θεματολόγιο δεξιοτήτων**[83], ειδικότερα το **σύμφωνο για τις δεξιότητες**[84] και το **σχέδιο δράσης για την ψηφιακή εκπαίδευση**[85]. Το **πρόγραμμα «Ψηφιακή Ευρώπη»** χρηματοδοτεί ευκαιρίες απόκτησης κυβερνοδεξιοτήτων, κυρίως μέσω πρωτοβουλιών για πολυκρατικά έργα, σε σαφή συμπληρωματικότητα με τη στήριξη που παρέχεται από το πρόγραμμα «Ορίζων Ευρώπη» για έρευνα και καινοτόμες τεχνολογικές λύσεις στον τομέα της κυβερνοασφάλειας. Το **Ευρωπαϊκό Ταμείο Άμυνας**[86] χρηματοδοτεί την έρευνα και την ανάπτυξη τεχνολογίας για τη διεξαγωγή αποδοτικών κυβερνοεπιχειρήσεων, συμπεριλαμβανομένων προγραμμάτων κατάρτισης και ασκήσεων[87]. Το **Erasmus+** θα συνεχίσει να στηρίζει τέτοιες πρωτοβουλίες, μεταξύ άλλων μέσω μεικτών εντατικών προγραμμάτων και έργων συνεργασίας.

Τα κράτη μέλη ενθαρρύνονται να κινητοποιήσουν τα κονδύλια της ΕΕ που διαχειρίζονται άμεσα για τη στήριξη δεξιοτήτων και θέσεων εργασίας στον τομέα της κυβερνοασφάλειας. Τα κονδύλια για την πολιτική συνοχής, όπως το **Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης (ΕΤΠΑ)** και το **ΕΚΤ+**, προσφέρουν σημαντικές δυνατότητες συνεργειών από την άποψη αυτή[88]. Το πεδίο δράσης στο πλαίσιο του **μηχανισμού ανάκαμψης και**

στοχεύουν ειδικά στην απόκτηση κυβερνοδεξιοτήτων, παρόλο που το έργο τους θα πρέπει να λαμβάνεται υπόψη από την Ακαδημία για την αποφυγή επικαλύψεων.

[83] Ευρωπαϊκό θεματολόγιο δεξιοτήτων – Απασχόληση, κοινωνικές υποθέσεις και κοινωνική ένταξη – Ευρωπαϊκή Επιτροπή (europa.eu).

[84] Χρηματοδοτικά μέσα της ΕΕ για την αναβάθμιση των δεξιοτήτων και την επανειδίκευση – Απασχόληση, κοινωνικές υποθέσεις και κοινωνική ένταξη – Ευρωπαϊκή Επιτροπή (europa.eu).

[85] Σχέδιο δράσης για την ψηφιακή εκπαίδευση 2021-2027.

[86] Κανονισμός (ΕΕ) 2021/697 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2021, για τη θέσπιση του Ευρωπαϊκού Ταμείου Άμυνας και την κατάργηση του κανονισμού (ΕΕ) 2018/1092.

[87] Τα κράτη μέλη έχουν δεσμευτεί για κοινά προγράμματα κατάρτισης και κοινές ασκήσεις, για παράδειγμα μέσω της δημιουργίας και της συμμετοχής σε προγράμματα κατάρτισης και ασκήσεις για την κυβερνοασφάλεια της μόνιμης διαρθρωμένης συνεργασίας (PESCO), όπως η Ακαδημία για τον κυβερνοχώρο και ο κόμβος καινοτομίας της ΕΕ (EU CAIH) και τα ομοσπονδοποιημένα εικονικά περιβάλλοντα κυβερνοτεχνολογίας.

[88] Κανονισμός (ΕΕ) 2021/1058, άρθρο 3 παράγραφος 1 και κανονισμός (ΕΕ) 2021/1057, άρθρο 4 παράγραφος 1 στοιχείο ζ).

ανθεκτικότητας (ΜΑΑ)[89] και του προγράμματος **InvestEU**[90] περιλαμβάνει περαιτέρω βασικές συμπληρωματικότητες για την υλοποίηση των στόχων της Ακαδημίας.

<u>Δράσεις στο πλαίσιο της Ακαδημίας</u>

Ευρωπαϊκό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας και ENISA

- **Χαρτογράφηση** της υφιστάμενης χρηματοδότησης της ΕΕ για κυβερνοδεξιότητες σε σύγκριση με τις ανάγκες της αγοράς, αξιολόγηση της **αποτελεσματικότητας** και προσδιορισμός των **προτεραιοτήτων** χρηματοδότησης έως το τέλος του 2024.

Επιτροπή

- Δημιουργία **ενιαίου σημείου εισόδου** για ευκαιρίες χρηματοδότησης για την απόκτηση κυβερνοδεξιοτήτων στην πλατφόρμα για τις ψηφιακές δεξιότητες και θέσεις εργασίας έως το τέλος του 2023.

7. Μέτρηση της προόδου: ενσωματωμένη λογοδοσία

Στο πλαίσιο της Ακαδημίας θα αναπτυχθεί **μεθοδολογία** που θα καθιστά δυνατή τη **μέτρηση της προόδου όσον αφορά την κάλυψη της έλλειψης κυβερνοδεξιοτήτων**.

7.1. Καθορισμός δεικτών κυβερνοασφάλειας για την παρακολούθηση της εξέλιξης της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας

Ο **δείκτης ψηφιακής οικονομίας και κοινωνίας** (DESI) συνοψίζει τους δείκτες των ψηφιακών επιδόσεων της Ευρώπης και παρακολουθεί την πρόοδο των κρατών μελών της ΕΕ. Στο πλαίσιο της Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας, ο ENISA, σε συνεργασία με την Επιτροπή και την ομάδα συνεργασίας NIS[91], θα αναπτύξει **δείκτες**, μεταξύ άλλων σε σχέση με το φύλο, για την παρακολούθηση της προόδου που σημειώνεται στα κράτη μέλη της ΕΕ για την αύξηση του αριθμού των επαγγελματιών στον τομέα της κυβερνοασφάλειας, ζητώντας επίσης τη γνώμη των σχετικών παραγόντων της αγοράς και των ΕΚΣ. Ο ENISA θα βασιστεί στη μεθοδολογία του DESI[92] και θα διασφαλίσει ότι οι δείκτες συνάδουν με τους ψηφιακούς στόχους της Ευρώπης για τους επαγγελματίες ΤΠΕ και για την επίτευξη σύγκλισης των φύλων στις ΤΠΕ. Στη συνέχεια, η Επιτροπή θα εργαστεί για την ενσωμάτωση

[89] Για παράδειγμα, το εσθονικό σχέδιο ανάκαμψης και ανθεκτικότητας προβλέπει επενδύσεις (10 εκατ. EUR) για τις ψηφιακές δεξιότητες, θα περιλαμβάνει την αναθεώρηση των προγραμμάτων κατάρτισης που διατίθενται σε εμπειρογνώμονες ΤΠΕ, θα χρηματοδοτήσει την αναβάθμιση των δεξιοτήτων και την επανεκπαίδευση ειδικών σε θέματα ΤΠΕ στον τομέα της κυβερνοασφάλειας και θα συμβάλει στην ανάπτυξη πιλοτικού προγράμματος για τον επανασχεδιασμό του πλαισίου προσόντων των ειδικών σε θέματα ΤΠΕ.

[90] Τα ενδιαφερόμενα μέρη (π.χ. πάροχοι κατάρτισης και εταιρείες που επιθυμούν να σχεδιάσουν ή να βελτιώσουν τις οικείες δραστηριότητες κατάρτισης στον τομέα της κυβερνοασφάλειας) μπορούν να προσεγγίσουν τον συμβουλευτικό κόμβο InvestEU, ο οποίος παρέχει τεχνική υποστήριξη και βοήθεια, συμπεριλαμβανομένης της ανάπτυξης ικανοτήτων, σε φορείς υλοποίησης έργων και οντότητες, και να συμβουλευτούν την πύλη InvestEU.

[91] Αξιοποιώντας τη μεθοδολογία που θα αναπτύξει ο ENISA για τους σκοπούς της διετούς έκθεσης του οργανισμού σχετικά με την κατάσταση της κυβερνοασφάλειας στην Ένωση σύμφωνα με το άρθρο 18 παράγραφος 3 της οδηγίας NIS2 και συμπληρωματικά προς αυτή.

[92] Βλ. μεθοδολογικό σημείωμα για τον Δείκτη Ψηφιακής Οικονομίας και Κοινωνίας 2022, το οποίο διατίθεται στην ιστοσελίδα Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας (DESI) | Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης (europa.eu).

των εν λόγω δεικτών στον DESI, ώστε να καταστεί δυνατή η ετήσια παρακολούθηση της κατάστασης των δεξιοτήτων κυβερνοασφάλειας και της σχετικής αγοράς εργασίας.

7.2.Συλλογή δεδομένων και υποβολή εκθέσεων

Ο ENISA θα συλλέγει τα δεδομένα σχετικά με τους δείκτες με την υποστήριξη του έργου ECCO και των ΕΚΣ. Με βάση τα δεδομένα που συλλέγονται, ο ENISA θα καταρτίζει **ετήσια έκθεση** που θα αξιοποιείται στην εκπόνηση της έκθεσης σχετικά με την κατάσταση της ψηφιακής δεκαετίας[93], η οποία, από κοινού με τον DESI, θα τροφοδοτεί περαιτέρω την ειδική ανά χώρα ανάλυση και τις ειδικές ανά χώρα συστάσεις του **Ευρωπαϊκού Εξαμήνου**[94]. Επίσης, οι δείκτες για τις κυβερνοδεξιότητες θα αξιοποιηθούν στη **διετή έκθεση** του ENISA σχετικά με την κατάσταση της κυβερνοασφάλειας στην ΕΕ που προβλέπεται στην οδηγία NIS2, η οποία καλύπτει τις ικανότητες, την ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας και την κυβερνοϋγιεινή σε ολόκληρη την ΕΕ.

7.3.Κατάρτιση βασικών δεικτών επιδόσεων για την κυβερνοασφάλεια

Με σκοπό την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας, ο ENISA, σε στενή συνεργασία με την Επιτροπή και τα ΕΚΣ, θα προτείνει βασικούς δείκτες επιδόσεων (ΒΔΕ) στην Επιτροπή, με βάση τη μεθοδολογία του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία», καθώς και την πείρα του κλάδου. Ο ENISA θα λάβει δεόντως υπόψη τους ΒΔΕ που χρησιμοποιούν τα κράτη μέλη για την αξιολόγηση των οικείων εθνικών στρατηγικών για την κυβερνοασφάλεια[95].

<u>Δράσεις στο πλαίσιο της Ακαδημίας</u>

ENISA

- Κατάρτιση **δεικτών και ΒΔΕ** για τις κυβερνοδεξιότητες έως το τέλος του 2023.
- **Συλλογή δεδομένων** σχετικά με τους δείκτες και υποβολή σχετικών εκθέσεων, με πρώτη συλλογή έως το 2025.

Επιτροπή

- Εργασίες για την ενσωμάτωση **δεικτών για την κυβερνοασφάλεια στον DESI** και στην **έκθεση για την κατάσταση της ψηφιακής δεκαετίας**.

8. Συμπέρασμα

Η παρούσα ανακοίνωση θέτει τα θεμέλια για την αναμόρφωση της προσέγγισης της ΕΕ για την ενίσχυση των κυβερνοδεξιοτήτων των επαγγελματιών στην ΕΕ. Στόχος είναι να μειωθεί η έλλειψη κυβερνοδεξιοτήτων και να αποκτήσει η ΕΕ το αναγκαίο εργατικό δυναμικό, ώστε να είναι σε θέση να ανταποκρίνεται στο συνεχώς εξελισσόμενο τοπίο των απειλών, να εφαρμόζει πολιτικές της ΕΕ που αποσκοπούν στην προστασία της ΕΕ από κυβερνοεπιθέσεις, αλλά και να ενισχύσει τις επιχειρηματικές ευκαιρίες και την επιχειρηματική ανταγωνιστικότητα. Ένα ειδικευμένο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας μπορεί να ωφελήσει τις **μη στρατιωτικές, αμυντικές, διπλωματικές κοινότητες και τις κοινότητες επιβολής του νόμου**, διευκολύνοντας τις συνέργειες μεταξύ τους.

[93] Απόφαση (ΕΕ) 2022/2481 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, για τη θέσπιση του προγράμματος πολιτικής 2030 «Ψηφιακή Δεκαετία».

[94] Ό.π., αιτιολογική σκέψη 25.

[95] Άρθρο 7 παράγραφος 4 της οδηγίας NIS2.

Η Επιτροπή καλεί τα κράτη μέλη και όλα τα ενδιαφερόμενα μέρη να συμβάλουν ώστε η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας να γίνει πραγματικότητα.