Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Πολιτική της ΕΕ για την κυβερνοάμυνα»

(γνωμοδότηση πρωτοβουλίας)

(2023/C 293/04)

Εισηγητής: ο κ. **Αναστάσης ΓΙΑΠΑΝΗΣ**

Συνεισηγητής: ο κ. **Alberto MAZZOLA**

Απόφαση της συνόδου ολομέλειας:	20.9.2022
Νομική βάση	Άρθρο 52 παράγραφος 2 του Εσωτερικού Κανονισμού
	Γνωμοδότηση πρωτοβουλίας
Αρμόδιο τμήμα	Συμβουλευτική Επιτροπή Βιομηχανικών Μεταλλαγών (CCMI)
Υιοθετήθηκε από το τμήμα	27.3.2023
Υιοθετήθηκε από την ολομέλεια	14.6.2023
Σύνοδος ολομέλειας αριθ.	579
Αποτέλεσμα της ψηφοφορίας	
(υπέρ/κατά/αποχές)	208/1/2

1. **Συμπεράσματα και συστάσεις**

1.1. Η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (ΕΟΚΕ) επιδοκιμάζει την προτεινόμενη πολιτική της ΕΕ για την κυβερνοάμυνα, θα ανέμενε ωστόσο να αποκτήσει η οργανωμένη κοινωνία των πολιτών σημαντικότερο ρόλο στη διαμόρφωση αυτών των προτάσεων. Η ΕΟΚΕ θεωρεί δύσκολο να αξιολογήσει σε αυτό το σημείο εάν οι μελλοντικές πρωτοβουλίες που περιγράφονται στην κοινή ανακοίνωση θα εφαρμοστούν και θα επιτύχουν τα επιδιωκόμενα αποτελέσματα. Καλεί τα θεσμικά όργανα της ΕΕ και τα κράτη μέλη να δώσουν προτεραιότητα και να προωθήσουν ταχέως τις εξαγγελθείσες πρωτοβουλίες.

1.2. Η ΕΟΚΕ τονίζει την ανάγκη λήψης πρόσθετων μέτρων για την ενίσχυση της ικανότητας της ΕΕ να εντοπίζει απειλές στον κυβερνοχώρο και ζητεί η χρηματοδότηση της έρευνας και ανάπτυξης (Ε & Α) να κατευθύνεται προς την ανάπτυξη ικανοτήτων αιχμής της ΕΕ. Η συνεργασία μεταξύ ιδιωτικού και δημόσιου τομέα είναι ουσιαστικής σημασίας και πρέπει να είναι αμφίδρομη. Η ΕΟΚΕ θεωρεί ότι ο συντονισμός σε επίπεδο ΕΕ είναι απαραίτητος για την αντιμετώπιση του κατακερματισμού και τη διασφάλιση της συνεργασίας και των κοινών επενδύσεων μεταξύ των κρατών μελών.

1.3. Η ΕΟΚΕ υποστηρίζει τη δημιουργία του Συντονιστικού Κέντρου Κυβερνοάμυνας της ΕΕ και συνιστά στα κράτη μέλη να δεσμευτούν για την ταχεία αντίδραση επί εικοσιτετραώρου βάσης, να αξιολογήσουν την ετοιμότητα και τις επιδόσεις των μηχανισμών της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο, με έμφαση τόσο στις στρατιωτικές ικανότητες όσο και σε κρίσιμους τομείς, όπως προσδιορίζονται στην οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [1] (οδηγία NIS 2). Η ΕΟΚΕ επικροτεί την επέκταση της εντολής του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Θέματα Κυβερνοασφάλειας (ECCC).με σκοπό τη στήριξη της δραστηριότητας του Συντονιστικού Κέντρου Κυβερνοάμυνας της ΕΕ.

1.4. Για την ενίσχυση της στρατηγικής αυτονομίας και κυριαρχίας της Ένωσης στον τομέα της κυβερνοασφάλειας, η ΕΟΚΕ πιστεύει ότι θα πρέπει να αναπτυχθεί ή να υιοθετηθεί από τον ιδιωτικό τομέα μια δυναμική πλατφόρμα δοκιμών και ανταλλαγής πληροφοριών σε πραγματικό χρόνο, προκειμένου να εντοπιστούν τα τρέχοντα κενά στις υφιστάμενες ικανότητες. Η πλατφόρμα θα μπορεί επίσης να χρησιμοποιηθεί για την ανταλλαγή βέλτιστων πρακτικών, την αναφορά συμβάντων στον κυβερνοχώρο και τη δημιουργία ενωσιακού καταλόγου όλων των εγκληματιών του κυβερνοχώρου.

---

[1] 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) (ΕΕ L 333 της 27.12.2022, σ. 80).

1.5. Η ΕΟΚΕ τονίζει την ανάγκη καλύτερης προετοιμασίας για την αντιμετώπιση κυβερνοεπιθέσεων, όπως οι ρωσικές στην Ουκρανία, με στόχο ιδίως υποδομές ζωτικής σημασίας. Η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών οικοσυστημάτων είναι ζωτικής σημασίας για την αποτελεσματική διαχείριση κρίσεων, τη διαλειτουργικότητα και την αποφυγή αλληλοεπικάλυψης προσπαθειών και επενδύσεων, μεταξύ άλλων μέσω δοκιμαστικών προσομοιώσεων κυβερνοεπιθέσεων.

1.6. Η ΕΟΚΕ πιστεύει ότι οι επενδύσεις στην κυβερνοάμυνα θα πρέπει να δίνουν προτεραιότητα στην προστασία των πολιτών της ΕΕ και των υποδομών ζωτικής σημασίας, μεταξύ άλλων με τη χρήση έμπιστων προμηθευτών υλικού και λογισμικού. Επιμένει ότι πρέπει να υπάρχουν έγκαιρες επικαιροποιήσεις των προτεραιοτήτων και των επενδύσεων, οι οποίες θα συμφωνούνται από την ΕΕ και τα κράτη μέλη, με τη συμμετοχή σχετικών ιδιωτικών φορέων.

1.7. Η ΕΕ πρέπει να διατηρήσει και να αναπτύξει τις αναγκαίες ικανότητες για τη διασφάλιση της ψηφιακής οικονομίας, της κοινωνίας, της δημοκρατίας και των κρίσιμων τεχνολογιών της, καθώς και για την παροχή βασικών υπηρεσιών κυβερνοασφάλειας. Για να διασφαλιστεί η στρατηγική αυτονομία της ΕΕ, η μείωση των εξαρτήσεων από τρίτες χώρες είναι ζωτικής σημασίας. Η ΕΟΚΕ θεωρεί απαραίτητο να υιοθετήσει η ΕΕ μια μεσοπρόθεσμη προσέγγιση όσον αφορά την αυτονομία σχετικά με τις βασικές τεχνολογίες και υποστηρίζει σθεναρά τη δημιουργία εγκαταστάσεων έρευνας και παραγωγής από εταιρείες με έδρα την ΕΕ, με κατάλληλη ευρωπαϊκή βιομηχανική πολιτική επικεντρωμένη σε ένα αυτόνομο οικοσύστημα στον κυβερνοχώρο.

1.8. Οι ΜΜΕ θα πρέπει να λαμβάνουν στοχευμένη στήριξη και να έχουν πρόσβαση σε προγράμματα χρηματοδότησης που αυξάνουν την ανθεκτικότητά τους σε επιθέσεις στον κυβερνοχώρο, καθώς και σε ευκαιρίες συνδρομής, κατάρτισης και εκπαίδευσης σχετικά με τους κινδύνους στον κυβερνοχώρο και τον τρόπο προστασίας από αυτούς. Η ΕΕ θα πρέπει να παράσχει έναν μηχανισμό παροχής κινήτρων που θα προωθεί τη σταδιακή εξοικείωση των ΜΜΕ και την ανάπτυξη καινοτόμων ΜΜΕ.

1.9. Η ΕΟΚΕ υποστηρίζει το σχέδιο για τη δημιουργία Ακαδημίας Κυβερνοδεξιοτήτων και ζητεί από την Ευρωπαϊκή Επιτροπή να συντονίσει και να χρηματοδοτήσει μεγάλης κλίμακας προγράμματα κατάρτισης και επαγγελματικής εκπαίδευσης στα οποία θα συμμετέχουν όλα τα κράτη μέλη και τα οποία θα αποσκοπούν στη δημιουργία ειδικευμένου εργατικού δυναμικού για το σύνολο των υπηρεσιών και των οργανισμών που ασχολούνται με την κυβερνοάμυνα, καθώς και για τα ιδιωτικά μη στρατιωτικά δίκτυα.

1.10. Η ΕΟΚΕ θεωρεί ότι η ευαισθητοποίηση των πολιτών σχετικά με την ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας για τη μείωση της έκθεσης σε κυβερνοεπιθέσεις και ζητεί εκπαιδευτικά προγράμματα για την κυβερνοασφάλεια, καθώς και προγράμματα διά βίου κατάρτισης που θα εστιάζουν στη βελτίωση των δεξιοτήτων και των γνώσεων στον κυβερνοχώρο. Η ΕΟΚΕ προκρίνει την ενσωμάτωση της κυβερνοασφάλειας σε όλες τις μελλοντικές δημόσιες πολιτικές της ΕΕ και την ενημέρωση του ευρέος κοινού σχετικά με τις κυβερνοαπειλές.

1.11. Η ΕΟΚΕ πιστεύει ότι η στενή συνεργασία με τους συμμάχους του ΝΑΤΟ σε στρατιωτικούς τομείς πρέπει να επικεντρωθεί στον πλήρη συντονισμό και την αμοιβαιότητα, στα κοινά έργα έρευνας, ανάπτυξης και καινοτομίας (Ε & Α&Κ), στην ανταλλαγή βέλτιστων πρακτικών, στα μεγάλης κλίμακας προγράμματα κατάρτισης και στις προσομοιώσεις κυβερνοεπιθέσεων, με κύριο στόχο την επέκταση της κοινής ικανότητας αντίδρασης.

1.12. Η ΕΟΚΕ καλεί τον Ύπατο Εκπρόσωπο να εξετάσει τους υφιστάμενους διμερείς διαλόγους για τον κυβερνοχώρο και να συμμετάσχει σε πρόσθετες συζητήσεις με άλλες χώρες και σχετικούς διεθνείς οργανισμούς με στόχο τη θέσπιση ενός παγκόσμιου πλαισίου για την τήρηση του διεθνούς δικαίου στον κυβερνοχώρο, με ιδιαίτερη έμφαση στην αμοιβαιότητα. Η ΕΟΚΕ θεωρεί ότι η ΕΕ είναι σε ιδανική θέση προκειμένου να αναλάβει ηγετικό ρόλο στις διεθνείς συζητήσεις για το μέλλον της κυβερνοασφάλειας, ιδίως στο πλαίσιο των Ηνωμένων Εθνών, δεδομένου ότι έχει ισχυρή βάση ως προς τις θεμελιώδεις δημοκρατικές ελευθερίες.

1.13. Η ΕΕ θα πρέπει αντιτάσσεται σθεναρά σε κάθε είδους σύστημα κοινωνικής βαθμολόγησης εις βάρος των πολιτών. Η ΕΟΚΕ καθιστά σαφές ότι δεν μπορεί να υπάρξει πραγματική δημοκρατία χωρίς αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα και πιστεύει ότι η υπεύθυνη και αποτελεσματική διαχείριση των δεδομένων είναι απαραίτητη για τη μετατροπή της υπερσυνδεσιμότητας σε ανταγωνιστικό πλεονέκτημα.

2. **Εισαγωγή και γενικές παρατηρήσεις**

2.1. Η ψηφιακή επέκταση των κοινωνιών συνοδεύεται από μεγάλο αριθμό απειλών για την κυβερνοασφάλεια που προκαλούν οι τεχνολογικές αναβαθμίσεις. Οι κυβερνοεπιθέσεις έχουν αυξηθεί σημαντικά σε αριθμό και πολυπλοκότητα τα τελευταία χρόνια, υπονομεύοντας την ασφάλεια τόσο των δημόσιων όσο και των ιδιωτικών φορέων. Είτε μιλάμε για λυτρισμικό, κακόβουλο λογισμικό, επιθέσεις ηλεκτρονικού ταχυδρομείου, παραβιάσεις δεδομένων, παραπληροφόρηση, κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) είτε για άλλες μορφές επιθέσεων, όλα αυτά συνιστούν μόνιμη και συνεχή απειλή για την ασφάλεια της ΕΕ στο σύνολό της.

2.2. Η ΕΟΚΕ επικροτεί την κοινή ανακοίνωση σχετικά με την *πολιτική της ΕΕ για την κυβερνοάμυνα* ([2]) και θεωρεί ότι είναι πλέον καιρός να αναληφθεί δράση επειγόντως και με συντονισμένο τρόπο σε επίπεδο ΕΕ, με τη συμμετοχή τόσο των μη στρατιωτικών όσο και των στρατιωτικών οικοσυστημάτων του κυβερνοχώρου και τη διασφάλιση του κατάλληλου επενδυτικού πλαισίου για τις ικανότητες κυβερνοάμυνας. Ωστόσο, η ΕΟΚΕ σημειώνει ότι η ανακοίνωση είναι απλώς μια δήλωση αποφασιστικότητας για δράση και ένας κατάλογος μελλοντικών πρωτοβουλιών της ΕΕ που πρέπει να υλοποιηθούν, και είναι αδύνατο για την ΕΟΚΕ να εκτιμήσει εάν αυτές οι μελλοντικές δεσμεύσεις θα τεθούν όντως σε εφαρμογή και εάν θα επιτύχουν όντως τα αναμενόμενα αποτελέσματα, δεδομένου ότι οι μελλοντικές διαπραγματεύσεις μεταξύ των συννομοθετών θα επηρεάσουν φυσικά το τελικό αποτέλεσμα του σχεδίου δράσης της ΕΕ για την κυβερνοασφάλεια.

2.3. Η ρωσική επίθεση στο δορυφορικό δίκτυο KA-SAT, η οποία διατάραξε την επικοινωνία μεταξύ των ουκρανικών στρατιωτικών δυνάμεων, και το πρόσφατο σκάνδαλο με τον Éric Léandri να έχει συνάψει σύμβαση με ορισμένες αμυντικές εταιρείες για κατασκοπεία στον κυβερνοχώρο για λογαριασμό τους, τοποθετούν την ασφάλεια στον κυβερνοχώρο στην κορυφή του καταλόγου απειλών κατά της ασφάλειας στην ΕΕ. Παρά το γεγονός ότι ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ) αποτελεί στέρεο νομοθέτημα της ΕΕ και ισχύει εδώ και αρκετά χρόνια, είναι σαφές ότι ο αυξανόμενος όγκος των διαθέσιμων δεδομένων είναι τρωτός και ο κίνδυνος τρίτα μέρη να υπερβούν τα όρια νομιμότητας αυξάνεται καθημερινά.

2.4. Δεδομένου του διακρατικού χαρακτήρα των κυβερνοεπιθέσεων, ο συντονισμός σε επίπεδο ΕΕ είναι απαραίτητος για να μειωθεί ο σημερινός κατακερματισμός και να διασφαλιστεί ότι τα κράτη μέλη είναι έτοιμα να συνεργαστούν και να επενδύσουν από κοινού. Αυτό είναι ιδιαίτερα σημαντικό για μελλοντικές υποθέσεις στις οποίες ένα κράτος μέλος θα μπορούσε να στοχοποιηθεί και όλα τα υπόλοιπα θα πρέπει να έχουν την ευκαιρία να παράσχουν άμεση στήριξη.

3. **Κοινή δράση για ισχυρότερη κυβερνοάμυνα**

3.1. Η ΕΟΚΕ λαμβάνει υπό σημείωση τις εξαγγελθείσες φιλόδοξες πρωτοβουλίες για τη δημιουργία ενός Συντονιστικού Κέντρου Κυβερνοάμυνας της ΕΕ, την ανάπτυξη του έργου CyDEf-X, τη δημιουργία ομάδων ταχείας αντίδρασης στον κυβερνοχώρο, την ανάπτυξη μιας πρωτοβουλίας αλληλεγγύης της ΕΕ για τον κυβερνοχώρο και τη διερεύνηση της ανάπτυξης συστημάτων πιστοποίησης της κυβερνοασφάλειας για προϊόντα, υπηρεσίες και διεργασίες ΤΠΕ. Η ΕΟΚΕ συνιστά όλα τα κράτη μέλη να δεσμευτούν ότι θα είναι έτοιμα να παράσχουν ταχεία αντίδραση επί εικοσιτετραώρου βάσης, με το Συντονιστικό Κέντρο της ΕΕ να συμμετέχει στην αξιολόγηση και την κατάρτιση τακτικών εκθέσεων σχετικά με την ετοιμότητα των κρατών μελών στον κυβερνοχώρο και την αποτελεσματικότητα του ευρωπαϊκού μηχανισμού αντιμετώπισης κρίσεων στον κυβερνοχώρο, εστιάζοντας τόσο στις στρατιωτικές ικανότητες όσο και στους κρίσιμους τομείς που προσδιορίζονται στην οδηγία NIS2. Κάθε κράτος μέλος θα πρέπει να διαθέτει ειδικευμένο προσωπικό, ειδικά καταρτισμένο προκειμένου να παρεμβαίνει σε περίπτωση συμβάντων στον κυβερνοχώρο, και να ελέγχει τακτικά την ικανότητα παρέμβασής τους σε άλλα κράτη μέλη.

3.2. Παρότι η ανακοίνωση παρέχει έναν μακρύ κατάλογο σταδιακών βελτιώσεων, η ΕΟΚΕ ανέμενε ότι θα καταρτιστεί ένας ρητός χάρτης πορείας για την εφαρμογή αυτών των πρωτοβουλιών, με σαφήνεια ως προς τη διακυβέρνηση και τις προθεσμίες υποβολής και έγκρισης. Επιπλέον, η ΕΟΚΕ θα ανέμενε να αποκτήσει η οργανωμένη κοινωνία των πολιτών σημαντικότερο ρόλο στη διαμόρφωση αυτών των προτάσεων.

3.3. Η ΕΟΚΕ θεωρεί ότι τα κράτη μέλη πρέπει να ενισχύσουν την εσωτερική τους ικανότητα αντιμετώπισης των κυβερνοαπειλών, συμμετέχοντας παράλληλα σε έργα συνεργασίας και ανταλλάσσοντας πληροφορίες και βέλτιστες πρακτικές με τους ομολόγους τους σε άλλα κράτη μέλη. Απαιτούνται άμεσες επενδύσεις σε ικανότητες κυβερνοάμυνας και ταχεία ανάπτυξη τεχνολογιών ([3]) σε όλα τα κράτη μέλη και σε κοινή ετοιμότητα για τον εντοπισμό, την ανάκαμψη και την άμυνα έναντι κυβερνοεπιθέσεων. Προκειμένου να υποστηριχθεί η αυτονομία της Ένωσης στον τομέα της κυβερνοασφάλειας, η ΕΟΚΕ θεωρεί ότι πρέπει να αναπτυχθεί ή να υιοθετηθεί από τον ιδιωτικό τομέα μια δυναμική πλατφόρμα δοκιμών και ανταλλαγής πληροφοριών σε πραγματικό χρόνο, η οποία θα επικεντρώνεται στον εντοπισμό των ικανοτήτων που λείπουν σήμερα.

3.4. Η ΕΟΚΕ συμμερίζεται την άποψη ότι, στο παρόν στάδιο, οι στρατιωτικές επιχειρήσεις στον κυβερνοχώρο θα πρέπει να παραμείνουν αυστηρά στην αρμοδιότητα των κρατών μελών· η ΕΟΚΕ υποστηρίζει την εξαγγελθείσα συνεργασία μεταξύ των στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (milCERTs), των ομάδων αντιμετώπισης συμβάντων που αφορούν την ασφάλεια των υπολογιστών (CSIRT) και της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική των EUIBA (CERT-EU).

3.5. Η πρόσφατα εγκριθείσα οδηγία NIS2 και η οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (CER) ([4]) έχουν ήδη θεσπίσει ειδικές εθνικές και τομεακές υποχρεώσεις όσον αφορά το πλαίσιο της ΕΕ για την κυβερνοάμυνα. Απαιτείται περαιτέρω δράση για τη βελτίωση της συλλογικής ικανότητας ανίχνευσης της ΕΕ και η ΕΟΚΕ ζητεί επενδύσεις στην έρευνα και ανάπτυξη για την ανάπτυξη ικανοτήτων αιχμής της ΕΕ.

([2]) Ανακοίνωση της Επιτροπής σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα.
([3]) Όπως ο επιταχυντής αμυντικής καινοτομίας για τον Βόρειο Ατλαντικό (DIANA) του ΝΑΤΟ.
([4]) Οδηγία CER.

4. **Προστασία του αμυντικού οικοσυστήματος της ΕΕ**

4.1. Η ΕΟΚΕ θεωρεί ότι η εγγενής πολυπλοκότητα και οι ταχέως εξελισσόμενες τεχνολογικές προκλήσεις έχουν μετασχηματίσει το αμυντικό οικοσύστημα και ότι η κυβερνοασφάλεια έχει καταστεί κοινό θέμα τόσο για τον στρατιωτικό όσο και για τον μη στρατιωτικό τομέα, καθώς και για τους πολίτες της ΕΕ. Η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών οικοσυστημάτων είναι πλέον πιο σημαντική από ποτέ και αναμένεται να αποφέρει οφέλη όσον αφορά την αποτελεσματικότερη διαχείριση κρίσεων, καθώς και τη συνεχή πρόοδο και διαλειτουργικότητα, αποφεύγοντας την επικάλυψη ή τον πολλαπλασιασμό των ίδιων προσπαθειών και επενδύσεων. Τα κράτη μέλη θα πρέπει να είναι έτοιμα να διενεργούν δοκιμές αντοχής των εθνικών υποδομών ζωτικής σημασίας, προκειμένου να αξιολογούν και να αυξάνουν την ανθεκτικότητα σε μελλοντικές κυβερνοεπιθέσεις.

4.2. Η ΕΟΚΕ θεωρεί ότι οι επενδύσεις στην κυβερνοάμυνα πρέπει, κατά προτεραιότητα, να στοχεύουν στην προστασία των πολιτών της ΕΕ και των υποδομών ζωτικής σημασίας. Δεδομένου του ταχέος ρυθμού του ψηφιακού μετασχηματισμού και της ταχείας εξέλιξης του τοπίου των απειλών, η ΕΟΚΕ ζητεί μετ' επιτάσεως να συμφωνηθούν εγκαίρως επικαιροποιήσεις των προτεραιοτήτων και των επενδύσεων μεταξύ της ΕΕ και των κρατών μελών, με ενδελεχή διαβούλευση με τα ενδιαφερόμενα μέρη του ιδιωτικού τομέα. Οι συσκευές του διαδικτύου των πραγμάτων (IoT) συχνά δεν προστατεύονται εξίσου με τις παραδοσιακές συσκευές, και η ΕΟΚΕ ζητεί να διασφαλιστεί ένα ελάχιστο επίπεδο ασφάλειας μέσω των πλατφορμών IDAM (διαχείριση ταυτότητας και πρόσβασης). Επίσης, δεδομένου ότι η πιστοποίηση αποτελεί βασική μέθοδο για την παροχή υψηλότερου επιπέδου ασφάλειας, η ΕΟΚΕ ζητεί η νέα προσέγγιση πιστοποίησης της ΕΕ να δώσει μεγαλύτερη έμφαση στην ασφάλεια του διαδικτύου των πραγμάτων.

4.3. Η ΕΕ πρέπει να ενισχύσει την ανθεκτικότητα έναντι των κυβερνοεπιθέσεων και να δημιουργήσει αποτελεσματική κυβερνοαποτροπή. Οι υποδομές ζωτικής σημασίας πρέπει να προστατεύονται από κάθε είδους κυβερνοεπιθέσεις, συμπεριλαμβανομένων των αμυντικών συστημάτων της ΕΕ. Η ΕΟΚΕ θεωρεί ότι είναι προς το στρατηγικό συμφέρον της ΕΕ να διασφαλιστεί ότι η Ένωση διατηρεί και αναπτύσσει τις βασικές ικανότητες για τη διασφάλιση της ψηφιακής οικονομίας, της κοινωνίας και της δημοκρατίας, για την επίτευξη πλήρους ψηφιακής κυριαρχίας ως μοναδικού τρόπου προστασίας των κρίσιμων τεχνολογιών, και την παροχή βασικών υπηρεσιών κυβερνοασφάλειας. Η μείωση των εξαρτήσεων από τρίτες χώρες είναι επίσης ζωτικής σημασίας για τη στρατηγική αυτονομία της ΕΕ. Η ΕΟΚΕ πιστεύει ότι οι τομεακοί οργανισμοί της ΕΕ (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA κ.λπ.) θα πρέπει να συμμετέχουν στη διαδικασία και να παρέχουν καθοδήγηση για την ανάπτυξη συστημάτων κυβερνοασφάλειας.

4.4. Η πανδημία COVID-19 επιτάχυνε την ψηφιακή μετάβαση και μετέτρεψε την παραδοσιακή εργασία σε υβριδική και/ή εξ αποστάσεως εργασία, δημιουργώντας νέες εργασιακές σχέσεις και προσδοκίες, καθώς και μια νέα τάξη ψηφιακών νομάδων, οι οποίοι αυξάνονται σε αριθμό. Η ΕΟΚΕ σημειώνει τις ταχείες αλλαγές στην αγορά εργασίας που οδήγησαν στην υιοθέτηση της αρχιτεκτονικής «μηδενικής εμπιστοσύνης» από τις εταιρείες, μέσω λύσεων IAM (Identity Access Management [διαχείριση ταυτότητας και πρόσβασης]) και PAM (Privileged Access Management [διαχείριση προνομιακής πρόσβασης]). Η ΕΟΚΕ θεωρεί ότι αυτό το είδος διαχείρισης των πόρων των εταιρειών προσφέρει νέες λύσεις που σχετίζονται με τις κυβερνοαπειλές και θεωρεί ότι ο ιδιωτικός τομέας πρέπει να υποστηριχθεί όσον αφορά την ενίσχυση του επιπέδου ασφάλειας των καινοτόμων ψηφιακών λύσεων.

4.5. Η ΕΟΚΕ είναι μάλλον απογοητευμένη από τη δήλωση της Επιτροπής ότι «σχέδιο εφαρμογής θα μπορούσε να καταρτιστεί σε συνεργασία με τα κράτη μέλη» και θεωρεί ότι ένα τέτοιο σχέδιο εφαρμογής είναι υποχρεωτικό. Πιστεύει ότι θα πρέπει να συνταχθεί από κοινού με τα κράτη μέλη και να εφαρμοστεί το συντομότερο δυνατόν. Η ΕΟΚΕ εκφράζει την ανησυχία της για την ήπια στάση της Επιτροπής και καλεί τα θεσμικά όργανα της ΕΕ και τα κράτη μέλη να διευκολύνουν την ταχεία πρόοδο όσον αφορά τις εξαγγελθείσες πρωτοβουλίες.

5. **Επενδύσεις σε ικανότητες κυβερνοάμυνας**

5.1. Καθώς η τεχνολογική ανάπτυξη εξελίσσεται ραγδαία, ο κυβερνοχώρος έχει καταστεί το νέο πεδίο πολέμου, μετά την ξηρά, τη θάλασσα, τον αέρα και το διάστημα. Έχει επίσης δημιουργήσει μεγάλες ευκαιρίες εγκληματικότητας για κακόβουλους φορείς του κυβερνοχώρου, που κυμαίνονται από ανεξάρτητους χάκερ έως επαγγελματίες εγκληματίες, ακόμη και κρατικούς παράγοντες.

5.2. Οι επενδύσεις στην έρευνα και την ανάπτυξη είναι ζωτικής σημασίας και η ΕΟΚΕ επικροτεί τα υφιστάμενα ειδικά κονδύλια στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», του Ευρωπαϊκού Ταμείου Άμυνας, του προγράμματος «Ορίζων Ευρώπη» και των εθνικών προγραμμάτων ανάκαμψης. Ωστόσο, η ΕΟΚΕ θα επιθυμούσε περισσότερα διακρατικά έργα που να επικεντρώνονται στη συνεργασία και τη διαλειτουργικότητα μεταξύ των συστημάτων κυβερνοάμυνας σε όλα τα κράτη μέλη, καθώς και περισσότερες συνέργειες μεταξύ των χρηματοδοτικών μέσων, ιδίως όσον αφορά τη στήριξη καινοτόμων ΜΜΕ.

5.3. Όπως ανακοινώθηκε στη στρατηγική της ΕΕ για την κυβερνοασφάλεια το 2020, η ΕΟΚΕ σημειώνει ότι η προθεσμία για τη δημιουργία της κοινής κυβερνομονάδας είναι το τρέχον έτος και αναμένει νέα σχετικά με την ολοκλήρωση της διαδικασίας και την ετοιμότητα της ΕΕ να αντιμετωπίζει συμβάντα μεγάλης κλίμακας στον κυβερνοχώρο. Η ΕΟΚΕ αναμένει ότι θα βελτιωθεί η αντίληψη της κατάστασης στην ΕΕ και η συνολική ικανότητα αντίδρασης και ανάκαμψης.

5.4. Η ΕΟΚΕ υποστηρίζει την επέκταση της εντολής του ECCC με σκοπό τη στήριξη της δραστηριότητας του Συντονιστικού Κέντρου Κυβερνοάμυνας της ΕΕ. Επιπλέον, το δίκτυο αυτό θα μπορούσε να στηρίξει την ευρωπαϊκή ψηφιακή κυριαρχία με την ανάπτυξη μιας ανταγωνιστικής ευρωπαϊκής βιομηχανικής βάσης για βασικές τεχνολογικές ικανότητες, η οποία θα στηρίζεται εν μέρει στο έργο που αναπτύσσεται από συμβατικές συμπράξεις δημόσιου και ιδιωτικού τομέα (ΣΔΙΤ). Οι ΣΔΙΤ έχουν αποδειχθεί η αποτελεσματικότερη προσέγγιση για τη βελτίωση της κυβερνοασφάλειας ολόκληρου του ψηφιακού οικοσυστήματος, αλλά πρέπει να λειτουργούν αμφίδρομα: οι δημόσιοι οργανισμοί πρέπει επίσης να ανταλλάσσουν τις πληροφορίες τους με τον ιδιωτικό τομέα.

5.5. Η ΕΟΚΕ σημειώνει ότι, προκειμένου να αντιμετωπιστούν μελλοντικές απόπειρες διαδικτυακής παραβίασης από κβαντικούς υπολογιστές, η ΕΕ πρέπει να επενδύσει άμεσα σε τεχνολογίες αιχμής, όπως η μετακβαντική κρυπτογραφία. Θεωρεί απαραίτητο η Ευρώπη να εστιάσει σε μια μεσοπρόθεσμη προοπτική για την επίτευξη αυτονομίας μέσω σθεναρής υποστήριξης ερευνητικών και παραγωγικών εγκαταστάσεων από εταιρείες με έδρα την ΕΕ. Η ΕΟΚΕ θεωρεί σημαντικό να αυξηθούν οι πόροι της ΕΕ για την ψηφιακή έρευνα και καινοτομία (Ε&Κ) και να υποστηριχθούν οι επενδύσεις των φορέων εκμετάλλευσης και των προμηθευτών σε νέες λειτουργίες τεχνικής ασφάλειας, μεταξύ άλλων όσον αφορά νέες τάσεις όπως η επαυξημένη πραγματικότητα και το μετασύμπαν. Ειδικότερα, είναι σημαντικό να δημιουργηθεί μια ευρωπαϊκή κατανεμημένη υποδομή υπολογιστικού νέφους που θα βασίζεται σε ευρωπαϊκούς κανόνες για θέματα όπως η αποθήκευση και η επεξεργασία δεδομένων ([5]).

5.6. Θα πρέπει να επιδειχθεί ιδιαίτερη προσοχή στις ΜΜΕ και να τους δοθεί πρόσβαση σε χρηματοδοτικά προγράμματα που ενισχύουν την ετοιμότητά τους απέναντι σε κυβερνοεπιθέσεις, καθώς και σε προγράμματα συνδρομής, κατάρτισης και εκπαίδευσης που θα τις βοηθήσουν να κατανοήσουν τους κινδύνους στον κυβερνοχώρο και τον τρόπο προστασίας από αυτούς. Η ΕΕ θα πρέπει να παράσχει έναν μηχανισμό παροχής κινήτρων που θα προωθεί τη σταδιακή εξοικείωση των ΜΜΕ.

5.7. Η Επιτροπή εκτιμά τη σημερινή έλλειψη δεξιοτήτων στον τομέα της κυβερνοασφάλειας σε μισό εκατομμύριο άτομα και η ΕΟΚΕ επικροτεί την πρόταση για την ίδρυση ακαδημίας κυβερνοδεξιοτήτων. Είναι σαφές ότι οι προσπάθειες σε επίπεδο κρατών μελών δεν επαρκούν για τη μείωση του χάσματος δεξιοτήτων και, ως εκ τούτου, η ΕΟΚΕ προτείνει στην Επιτροπή, μαζί με τη δρομολόγηση της ακαδημίας, να αξιοποιήσει την ώθηση που παρέχει το ευρωπαϊκό έτος Δεξιοτήτων και να συντονίσει και να χρηματοδοτήσει προγράμματα κατάρτισης μεγάλης κλίμακας και προγράμματα ΕΕΚ σε επίπεδο ΕΕ, στα οποία θα συμμετέχουν όλα τα κράτη μέλη και θα επικεντρώνονται στην παροχή ειδικευμένου εργατικού δυναμικού για όλους τους οργανισμούς και τους φορείς που εμπλέκονται στην κυβερνοάμυνα, καθώς και για ιδιωτικά μη στρατιωτικά δίκτυα. Ιδιαίτερη έμφαση πρέπει να δοθεί στην κατάρτιση του εργατικού δυναμικού, ιδίως στους τομείς των θετικών επιστημών, της τεχνολογίας, της μηχανικής και των μαθηματικών (STEM).

5.8. Επιπλέον, η ΕΟΚΕ θεωρεί ότι είναι ζωτικής σημασίας να αυξηθεί η ευαισθητοποίηση των πολιτών σχετικά με την κυβερνοασφάλεια, προκειμένου να μειωθεί η έκθεση σε κυβερνοεπιθέσεις, ιδίως όσον αφορά τα βασικά εγκλήματα στον κυβερνοχώρο που έχουν στόχο το ευρύ κοινό. Η ΕΟΚΕ ζητεί εκπαιδευτικά προγράμματα για την κυβερνοασφάλεια και προγράμματα διά βίου κατάρτισης στον τομέα της κυβερνοασφάλειας, τα οποία θα εστιάζουν στη βελτίωση των κυβερνοδεξιοτήτων και θα καθιστούν την κυβερνοασφάλεια πιο οικεία και ελκυστική στους πολίτες, ιδίως στη νεότερη γενιά. Η ΕΟΚΕ τάσσεται υπέρ της ενσωμάτωσης των προβληματισμών για την κυβερνοασφάλεια σε όλες τις μελλοντικές δημόσιες πολιτικές της ΕΕ και της ενημέρωσης του ευρύτερου κοινού σχετικά με τις κυβερνοαπειλές, μεταξύ άλλων μέσω δωρεάν προγραμμάτων κατάρτισης για τον γενικό πληθυσμό, δωρεάν ενημερωτικών εφαρμογών κινητής τηλεφωνίας, ή μέσω της επικοινωνίας κατά τη διάρκεια τηλεοπτικών ζωνών υψηλής τηλεθέασης. Παράλληλα με τις δράσεις αυτές, πρέπει να προωθηθεί η ευρεία πρόοδος σε όλα τα επίπεδα της κοινωνίας προς μια νοοτροπία «προσανατολισμένη στην κυβερνοασφάλεια».

5.9. Η ΕΟΚΕ θεωρεί ζωτικής σημασίας την αξιολόγηση του προφίλ κινδύνου των προμηθευτών και την εφαρμογή των σχετικών περιορισμών σε προμηθευτές που θεωρούνται υψηλού κινδύνου, συμπεριλαμβανομένων των αναγκαίων απαγορεύσεων σε βασικά στοιχεία ενεργητικού και εφαρμογές που ορίζονται ως ουσιώδη και ευαίσθητα στις συντονισμένες εκτιμήσεις κινδύνου της ΕΕ, καθώς και την πιστοποίηση των έμπιστων προμηθευτών υλικού και λογισμικού.

6. **Εταιρικές σχέσεις για την αντιμετώπιση κοινών προκλήσεων**

6.1. Το επίπεδο ετοιμότητας για μελλοντικές κυβερνοεπιθέσεις διαφέρει σημαντικά από το ένα κράτος μέλος στο άλλο. Η ΕΟΚΕ θεωρεί ότι το πρώτο βήμα είναι η δημιουργία μιας ενδοενωσιακής πλατφόρμας επικοινωνίας βέλτιστων πρακτικών, όπου τα πλέον προηγμένα στον κυβερνοχώρο κράτη μέλη θα μπορούν να ανταλλάσσουν τις γνώσεις τους με τις άλλες χώρες και να διευκολύνουν την άμεση αξιοποίησή τους από τις άλλες χώρες. Αυτό θα συμβάλει στη βελτίωση της αμοιβαίας εμπιστοσύνης μεταξύ των εθνικών φορέων. Δεύτερον, η ΕΟΚΕ πιστεύει ότι απαιτείται στενότερη συνεργασία μεταξύ κρατικών και μη κρατικών φορέων σε ολόκληρη την ΕΕ, προκειμένου να βελτιωθεί η κυβερνοασφάλεια των προϊόντων και των υπηρεσιών εντός της εσωτερικής αγοράς. Η ΕΟΚΕ προτείνει επίσης τη δημιουργία μιας κοινής πλατφόρμας της ΕΕ για την αναφορά συμβάντων στον κυβερνοχώρο, συμπεριλαμβανομένου ενός ενωσιακού μαύρου καταλόγου όλων των ακτιβιστών για εγκλήματα στον κυβερνοχώρο.

([5]) Όπως η γαλλογερμανική πρωτοβουλία Gaia-X.

6.2. Η ΕΟΚΕ είναι της γνώμης ότι η ισχυρή συνεργασία με τους συμμάχους μας στο ΝΑΤΟ στον στρατιωτικό τομέα πρέπει να επικεντρωθεί όχι μόνο στην ανάπτυξη ικανοτήτων και στον έγκαιρο εντοπισμό, αλλά και σε κοινά έργα έρευνας, ανάπτυξης και καινοτομίας (Ε & Α&Κ), ανταλλαγή βέλτιστων πρακτικών και ανταλλαγές απόψεων μεταξύ εμπειρογνωμόνων, μεγάλα προγράμματα κατάρτισης και προσομοιώσεις κυβερνοεπιθέσεων. Κύριος στόχος θα πρέπει να είναι η επέκταση της κοινής ικανότητας απόκρισης και η δημιουργία συνεργιών για την αντιμετώπιση μελλοντικών υβριδικών απειλών, σύμφωνα με τις κοινές δηλώσεις της Βαρσοβίας του 2016 και των Βρυξελλών του 2018. Η συνεργασία μεταξύ της ΕΕ και του ΝΑΤΟ εξακολουθεί να έχει ανεξερεύνητους διαύλους προς αξιοποίηση, και η άμεση πρόοδος μπορεί να συμβάλει ουσιαστικά στη διασφάλιση της ασφάλειας για τους πολίτες και τις κοινωνίες μας.

6.3. Η ΕΟΚΕ πιστεύει ότι οι συζητήσεις σε παγκόσμιο επίπεδο και με τους διεθνείς εταίρους μας θα πρέπει να θέσουν τις βάσεις για την προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου που θα προστατεύει τα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες και το κράτος δικαίου και θα επικεντρώνεται στην ανάπτυξη δεσμευτικών διεθνών προτύπων σε τομείς με ταχεία ψηφιακή ανάπτυξη. Η ΕΟΚΕ συνιστά στον Ύπατο Εκπρόσωπο να επανεξετάσει τους υφιστάμενους διμερείς διαλόγους για τον κυβερνοχώρο και να συμμετάσχει σε περαιτέρω διαπραγματεύσεις με άλλες χώρες και σχετικούς διεθνείς οργανισμούς, προκειμένου να προωθηθεί ένα παγκόσμιο πλαίσιο για την τήρηση του διεθνούς δικαίου στον κυβερνοχώρο, το οποίο θα βασίζεται σε αυστηρή προϋπόθεση αμοιβαιότητας.

6.4. Τέλος, η ΕΟΚΕ πιστεύει ότι η ΕΕ είναι η πλέον κατάλληλη να ηγηθεί των διεθνών συζητήσεων για το μέλλον της κυβερνοασφάλειας, ιδίως στο πλαίσιο των συζητήσεων του ΟΗΕ, λόγω των στέρεων θεμελίων της στις βασικές δημοκρατικές ελευθερίες. Η ΕΕ πρέπει επίσης να συμμετάσχει στην καταπολέμηση των ολοκληρωτικών καθεστώτων που παρακολουθούν τα δεδομένα των πολιτών και παραβιάζουν τα δικαιώματα και τις ελευθερίες τους, ενώ θα πρέπει να αντιτάσσεται σθεναρά σε κάθε είδους σύστημα κοινωνικής βαθμολόγησης εις βάρος των πολιτών. Η ΕΟΚΕ δηλώνει ξεκάθαρα πως δεν μπορεί να υπάρξει πραγματική δημοκρατία χωρίς αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα και θεωρεί ότι η υπεύθυνη και αποτελεσματική διαχείριση των δεδομένων είναι ζωτικής σημασίας για τη μετατροπή της υπερσυνδεσιμότητας σε πλεονέκτημα.

Βρυξέλλες, 14 Ιουνίου 2023.

Ο Πρόεδρος
της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής
Oliver RÖPKE