Ευρωπαϊκό Κοινοβούλιο
2019-2024

Επιτροπή Μεταφορών και Τουρισμού

2023/0109(COD)

25.10.2023

ΓΝΩΜΟΔΟΤΗΣΗ

της Επιτροπής Μεταφορών και Τουρισμού

προς την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Συντάκτης γνωμοδότησης: Gheorghe Falcă

PA_Legam

ΣΥΝΤΟΜΗ ΑΙΤΙΟΛΟΓΗΣΗ

Οι οργανισμοί που πλήττονται από κυβερνοεπιθέσεις, μεταξύ άλλων στον τομέα των μεταφορών, σπάνια τις αναφέρουν, ιδίως οι εταιρείες του ιδιωτικού τομέα, καθώς τείνουν να τις θεωρούν «επιβλαβή δημοσιότητα». Οι περισσότεροι οργανισμοί προτιμούν να τις αντιμετωπίζουν εσωτερικά και συχνά είναι οι ίδιοι οι δράστες που τις δημοσιοποιούν. Η καλή είδηση είναι ότι στην ΕΕ η έναρξη ισχύος της οδηγίας 2022/2555 για την ασφάλεια των δικτύων (γνωστή ως «οδηγία NIS2»), την οποία τα κράτη μέλη πρέπει να μεταφέρουν στο εθνικό τους δίκαιο έως τον Οκτώβριο του 2024, εναρμονίζει τις υποχρεώσεις αναφοράς περιστατικών σε όλα τα κράτη μέλη. Κατά συνέπεια, είναι πιθανό ότι τα επόμενα έτη θα μπορεί να γίνει καλύτερα κατανοητή η φύση και η κλίμακα του προβλήματος.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) δημοσίευσε πρόσφατη έκθεση1 που παρέχει πληροφορίες σχετικά με τις απειλές κατά της κυβερνοασφάλειας στον τομέα των μεταφορών, στην οποία τονίζεται ότι οι κυβερνοεγκληματίες ευθύνονται για περισσότερα από τα μισά περιστατικά που παρατηρήθηκαν κατά την περίοδο αναφοράς του 2022 (55 %) και ότι το κύριο κίνητρο για τις επιθέσεις αυτές ήταν το οικονομικό κέρδος. Σημειώνει, επίσης, ότι οι περισσότερες κυβερνοεπιθέσεις στον τομέα των μεταφορών θέτουν στο στόχαστρο τα συστήματα ΤΠ, προκαλώντας λειτουργικές διαταραχές.

Όσον αφορά την ετοιμότητα και την αντιμετώπιση περιστατικών κυβερνοασφάλειας, επί του παρόντος υπάρχει περιορισμένη στήριξη σε επίπεδο Ένωσης και αλληλεγγύη μεταξύ των κρατών μελών. Στα συμπεράσματα που ενέκρινε τον Μάιο του 2022, το Συμβούλιο τόνισε την ανάγκη να αντιμετωπιστούν αυτά τα κενά, καλώντας την Επιτροπή να υποβάλει πρόταση για ένα νέο **ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας**[2].

Ο παρών κανονισμός εφαρμόζει τη **στρατηγική κυβερνοασφάλειας της ΕΕ**, η οποία εγκρίθηκε τον Δεκέμβριο του 2020 και στο πλαίσιο της οποίας εξαγγέλθηκε η δημιουργία μιας **ευρωπαϊκής κυβερνοασπίδας** για την ενίσχυση των ικανοτήτων εντοπισμού απειλών στον κυβερνοχώρο και ανταλλαγής πληροφοριών στην Ευρωπαϊκή Ένωση μέσω μιας ομοσπονδίας εθνικών και διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (SOC). Οι δράσεις του παρόντος κανονισμού θα στηριχθούν με **χρηματοδότηση στο πλαίσιο του στρατηγικού στόχου «Κυβερνοασφάλεια» του προγράμματος «Ψηφιακή Ευρώπη» (DEP)**.

Ο συνολικός προϋπολογισμός περιλαμβάνει αύξηση κατά 100 εκατομμύρια EUR, η οποία προτείνεται στον παρόντα κανονισμό να κατανεμηθεί εκ νέου από άλλους στρατηγικούς στόχους του προγράμματος «Ψηφιακή Ευρώπη». Με τον τρόπο αυτό, το νέο συνολικό ποσό που διατίθεται για δράσεις κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» θα ανέλθει σε 842,8 εκατομμύρια EUR.

Μέρος των πρόσθετων 100 εκατομμυρίων EUR θα ενισχύσει τον προϋπολογισμό που διαχειρίζεται το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και

[1] «Understanding Cyber Threats in Transport» (Κατανόηση των κυβερνοαπειλών στον τομέα των μεταφορών), ENISA, που δημοσιεύτηκε στις 21 Μαρτίου 2023.

[2] Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, 23 Μαΐου 2022, (9364/22).

Ερευνητικά Θέματα Κυβερνοασφάλειας (ECCC) για την υλοποίηση δράσεων σχετικά με τα SOC και την ετοιμότητα στο πλαίσιο του προγράμματος ή των προγραμμάτων εργασίας τους. Επιπλέον, η πρόσθετη χρηματοδότηση θα αξιοποιηθεί για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Συμπληρώνει τον προϋπολογισμό που έχει ήδη προβλεφθεί για παρόμοιες δράσεις στο πλαίσιο του προγράμματος εργασίας του κύριου προγράμματος «Ψηφιακή Ευρώπη» και του προγράμματος εργασίας για την κυβερνοασφάλεια του προγράμματος «Ψηφιακή Ευρώπη» για την περίοδο 2023-2027, γεγονός που θα μπορούσε να αυξήσει το συνολικό ποσό σε 551 εκατομμύρια για την περίοδο 2023-2027, ενώ 115 εκατομμύρια διατέθηκαν ήδη με τη μορφή πιλοτικών έργων για την περίοδο 2021-2022. Συμπεριλαμβανομένων των συνεισφορών των κρατών μελών, ο συνολικός προϋπολογισμός μπορεί να ανέλθει σε 1 109 δισ. EUR.

Η θέση του συντάκτη γνωμοδότησης

Ο συντάκτης γνωμοδότησης χαιρετίζει τη νέα πρόταση και πιστεύει ότι θα προσφέρει σημαντικά οφέλη στα διάφορα ενδιαφερόμενα μέρη. Ο συντάκτης γνωμοδότησης υπογραμμίζει ότι είναι αναγκαία η βαθύτερη κατανόηση των αναγκών και των απαιτήσεων κυβερνοασφάλειας όσον αφορά τις μεταφορές, και ότι απαιτείται οι κρίσιμες οντότητες στον τομέα των μεταφορών να αποκτήσουν πρόσβαση σε επαρκή χρηματοδότηση με σκοπό την ετοιμότητα, την αντιμετώπιση και την επίλυση περιστατικών.

Ο συντάκτης γνωμοδότησης υποστηρίζει την «εργαλειοθήκη για την κυβερνοασφάλεια στον τομέα των μεταφορών», η οποία έχει ως στόχο να συμβάλει σε υψηλότερα επίπεδα ευαισθητοποίησης ως προς την κυβερνοασφάλεια και κυβερνοϋγιεινής, με ιδιαίτερη έμφαση στον τομέα των μεταφορών. Αφορά οργανισμούς στον τομέα των μεταφορών, ανεξάρτητα από το μέγεθος και τον τομέα δραστηριότητάς τους, λαμβανομένων επίσης υπόψη των κρίσιμων υποδομών για τις μεταφορές και της στρατιωτικής κινητικότητας, ιδίως όσον αφορά τον πόλεμο στην Ουκρανία, και ειδικότερα, ενδεικτικά:

- τους αερομεταφορείς, τους φορείς διαχείρισης αερολιμένων, τους κεντρικούς αερολιμένες, τα κέντρα διαχείρισης της εναέριας κυκλοφορίας και ελέγχου της εναέριας κυκλοφορίας, τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια της Αεροπορίας και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια της Αεροναυτιλίας (Eurocontrol)·
- τους διαχειριστές υποδομής, τις σιδηροδρομικές επιχειρήσεις και το Ευρωπαϊκό Σύστημα Διαχείρισης της Σιδηροδρομικής Κυκλοφορίας (ERTMS)·
- τις εταιρείες εσωτερικής πλωτής, θαλάσσιας και ακτοπλοϊκής μεταφοράς επιβατών και εμπορευμάτων, τους διαχειριστικούς φορείς των λιμένων, συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων, τους φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός λιμένων, τους φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων·
- τις αρμόδιες για τον έλεγχο της διαχείρισης της κυκλοφορίας οδικές αρχές, τους φορείς εκμετάλλευσης συστημάτων ευφυών μεταφορών·
- ταχυδρομεία και ταχυμεταφορές.

Ο συντάκτης γνωμοδότησης πιστεύει ότι το μέγεθος του προϋπολογισμού για τη λειτουργία του **ταμείου αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας** θα είναι καθοριστικό στοιχείο για την επιτυχία του· συνεπώς, ο προϋπολογισμός θα πρέπει να είναι επαρκής προκειμένου να στηριχθούν τα κράτη μέλη όσον αφορά την **προετοιμασία, την αντιμετώπιση και την ανάκαμψη** από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας· Η στήριξη για την αντιμετώπιση περιστατικών διατίθεται επίσης στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.

Η **ευρωπαϊκή κυβερνοασπίδα** θα βελτιώσει τις ικανότητες των κρατών μελών όσον αφορά την ανίχνευση κυβερνοαπειλών. Ο **μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο** θα συμπληρώσει τις δράσεις των κρατών μελών μέσω στήριξης έκτακτης ανάγκης για ετοιμότητα, αντιμετώπιση και άμεση ανάκαμψη/αποκατάσταση της λειτουργίας βασικών υπηρεσιών.

ΤΡΟΠΟΛΟΓΙΑ

Η Επιτροπή Μεταφορών και Τουρισμού καλεί την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας, που είναι αρμόδια επί της ουσίας, να λάβει υπόψη της τα ακόλουθα:

Τροπολογία 1

Πρόταση κανονισμού
Αιτιολογική σκέψη 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(2) Το μέγεθος, η συχνότητα και οι επιπτώσεις των περιστατικών κυβερνοασφάλειας αυξάνονται, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με στόχο την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών. Αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Ενόψει του ταχέως εξελισσόμενου τοπίου των απειλών, η απειλή πιθανών περιστατικών μεγάλης κλίμακας που προκαλούν σημαντική διαταραχή ή ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων και παραγόντων χακτιβισμού (ακτιβισμός στον κυβερνοχώρο) που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών και την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών, να προκαλέσουν σημαντική ζημία στην οικονομία της Ένωσης, και μπορούν ακόμη και να έχουν συνέπειες που απειλούν την υγεία ή τη ζωή.	(2) Το μέγεθος, η συχνότητα και οι επιπτώσεις των περιστατικών κυβερνοασφάλειας αυξάνονται, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με στόχο την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών. Αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών, ***καθώς και των κρίσιμων υποδομών ΤΠ και υλικών υποδομών.*** Ενόψει του ταχέως εξελισσόμενου τοπίου των απειλών, η απειλή πιθανών περιστατικών μεγάλης κλίμακας που προκαλούν σημαντική διαταραχή ή ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων και παραγόντων χακτιβισμού (ακτιβισμός στον κυβερνοχώρο) που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών***, δημόσιων και ιδιωτικών μεταφορών*** και την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών, να

Επιπλέον, τα περιστατικά κυβερνοασφάλειας είναι απρόβλεπτα, καθώς συχνά εμφανίζονται και εξελίσσονται σε πολύ σύντομο χρονικό διάστημα, δεν περιορίζονται σε κάποια συγκεκριμένη γεωγραφική περιοχή και συμβαίνουν ταυτόχρονα ή εξαπλώνονται αμέσως σε πολλές χώρες.	προκαλέσουν σημαντική ζημία στην οικονομία ***της Ένωσης, καθώς και στην κινητικότητα εντός*** της Ένωσης, και μπορούν ακόμη και να έχουν συνέπειες που απειλούν την υγεία ή τη ζωή. Επιπλέον, τα περιστατικά κυβερνοασφάλειας είναι απρόβλεπτα, καθώς συχνά εμφανίζονται και εξελίσσονται σε πολύ σύντομο χρονικό διάστημα, δεν περιορίζονται σε κάποια συγκεκριμένη γεωγραφική περιοχή και συμβαίνουν ταυτόχρονα ή εξαπλώνονται αμέσως σε πολλές χώρες.

Τροπολογία 2

Πρόταση κανονισμού
Αιτιολογική σκέψη 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(2α) Ο τομέας των μεταφορών αντιμετωπίζει ολοένα και πιο σοβαρές απειλές για την κυβερνοασφάλεια από κρατικά χρηματοδοτούμενους φορείς, κυβερνοεγκληματίες και χακτιβιστές που στοχεύουν αρχές, φορείς εκμετάλλευσης, κατασκευαστές, προμηθευτές και παρόχους υπηρεσιών στους τομείς των αεροπορικών, θαλάσσιων, σιδηροδρομικών και οδικών μεταφορών. Το 2022 ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) παρατήρησε αύξηση κατά 25 %, σε σύγκριση με τα επίπεδα του 2021, του μηνιαίου μέσου αριθμού των αναφερόμενων περιστατικών που επηρεάζουν τον τομέα των μεταφορών. Η πλειονότητα των επιθέσεων στον τομέα των μεταφορών θέτει στο στόχαστρο συστήματα τεχνολογίας πληροφοριών (ΤΠ), με αποτέλεσμα να προκύπτουν πιθανές διαταραχές στη λειτουργία τους[14α].
	[14α] ENISA (2023), ENISA Threat Landscape: Transport sector (Το τοπίο

των απειλών του ENISA: ο τομέας μεταφορών), σ. 7 και 17.

Τροπολογία 3

Πρόταση κανονισμού
Αιτιολογική σκέψη 2 β (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(2β) Η απρόκλητη εισβολή της Ρωσίας στην Ουκρανία ήταν καθοριστική για τη σημαντική αύξηση των περιστατικών κυβερνοασφάλειας, συμπεριλαμβανομένων των κυβερνοεπιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS), με στόχο τον τομέα των μεταφορών στην ΕΕ και σε περιοχές κοντά στην ΕΕ, κυρίως αερολιμένες, σιδηροδρόμους και αρχές του τομέα μεταφορών[14β]. Αυτή η αύξηση των επιθέσεων είναι πολύ πιθανό να συνεχιστεί.
	[14β] ENISA (2023), ENISA Threat Landscape: Transport sector (Το τοπίο των απειλών του ENISA: ο τομέας μεταφορών), σ. 9.

Τροπολογία 4

Πρόταση κανονισμού
Αιτιολογική σκέψη 2 γ (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(2γ) Οι κυβερνοεπιθέσεις θέτουν στο στόχαστρο αρχές και οργανισμούς από όλους τους υποτομείς των μεταφορών, ενώ επηρεάζονται σιδηροδρομικές επιχειρήσεις και διαχειριστές υποδομών, καθώς και φορείς εκμετάλλευσης λιμένων. Όσον αφορά τον τομέα των οδικών μεταφορών, στοχοποιήθηκαν κατασκευαστές πρωτότυπου εξοπλισμού (ΚΠΕ), προμηθευτές και πάροχοι

υπηρεσιών, καθώς και φορείς δημόσιων μεταφορών. Στον τομέα της αεροπορίας, κύριοι στόχοι υπήρξαν οι αεροπορικές εταιρείες και οι φορείς εκμετάλλευσης αερολιμένων, ενώ ακολουθούν οι πάροχοι υπηρεσιών, οι φορείς επίγειων μεταφορών και η αλυσίδα εφοδιασμού[14γ].

[14γ] ENISA (2023), ENISA Threat Landscape: Transport sector (Το τοπίο των απειλών του ENISA: ο τομέας μεταφορών), σ. 17.

Τροπολογία 5

Πρόταση κανονισμού
Αιτιολογική σκέψη 3

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(3) Είναι απαραίτητο να ενισχυθεί η ανταγωνιστική θέση των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιοποιημένη οικονομία και να στηριχθεί ο ψηφιακός μετασχηματισμός τους, διά της ενίσχυσης του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά. Όπως συνιστάται σε τρεις διαφορετικές προτάσεις της Διάσκεψης για το μέλλον της Ευρώπης[16], είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των πολιτών, των επιχειρήσεων και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορούν να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Ως εκ τούτου, απαιτούνται επενδύσεις σε υποδομές και υπηρεσίες που θα στηρίξουν την ταχύτερη ανίχνευση και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, και τα κράτη μέλη χρειάζονται βοήθεια για την καλύτερη προετοιμασία, καθώς και για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η Ένωση θα πρέπει	(3) Είναι απαραίτητο να ενισχυθεί η ανταγωνιστική θέση των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιοποιημένη οικονομία και να στηριχθεί ο ψηφιακός μετασχηματισμός τους, διά της ενίσχυσης του επιπέδου κυβερνοασφάλειας στην ψηφιακή ενιαία αγορά. Όπως συνιστάται σε τρεις διαφορετικές προτάσεις της Διάσκεψης για το μέλλον της Ευρώπης[16], είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των πολιτών, των επιχειρήσεων, των ***μεταφορέων*** και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορούν να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Ως εκ τούτου, απαιτούνται επενδύσεις σε υποδομές και υπηρεσίες που θα στηρίξουν την ταχύτερη ανίχνευση και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, και τα κράτη μέλη χρειάζονται βοήθεια για την καλύτερη προετοιμασία, καθώς και για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η Ένωση θα πρέπει

επίσης να αυξήσει τις ικανότητές της σε αυτούς τους τομείς, ιδίως όσον αφορά τη συλλογή και ανάλυση δεδομένων σχετικά με απειλές και περιστατικά κυβερνοασφάλειας.

επίσης να αυξήσει τις ικανότητές της σε αυτούς τους τομείς, ιδίως όσον αφορά τη συλλογή και ανάλυση δεδομένων σχετικά με απειλές και περιστατικά κυβερνοασφάλειας***, καθώς και σχετικά με την κατάσταση και την εξέλιξη της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας, δεδομένου ότι διαδραματίζει καθοριστικό ρόλο στην παροχή των απαραίτητων υπηρεσιών εντοπισμού και αντιμετώπισης***.

[16] https://futureu.europa.eu/el/

[16] https://futureu.europa.eu/el/

Τροπολογία 6

Πρόταση κανονισμού
Αιτιολογική σκέψη 4

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(4) Η Ένωση έχει ήδη λάβει σειρά μέτρων για τη μείωση των τρωτών σημείων και την αύξηση της ανθεκτικότητας των κρίσιμων υποδομών και οντοτήτων έναντι των κινδύνων κυβερνοασφάλειας, ιδίως με την οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17], τη σύσταση (ΕΕ) 2017/1584[18] της Επιτροπής, την οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[19] και τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20]. Επιπλέον, η σύσταση του Συμβουλίου σχετικά με μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών καλεί τα κράτη μέλη να λάβουν επείγοντα και αποτελεσματικά μέτρα και να συνεργαστούν καλόπιστα, αποδοτικά, με αλληλεγγύη και με συντονισμένο τρόπο μεταξύ τους, με την Επιτροπή και άλλες σχετικές δημόσιες αρχές, καθώς και με τις οικείες οντότητες, για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών που χρησιμοποιούνται	(4) Η Ένωση έχει ήδη λάβει σειρά μέτρων για τη μείωση των τρωτών σημείων και την αύξηση της ανθεκτικότητας των κρίσιμων υποδομών και οντοτήτων έναντι των κινδύνων κυβερνοασφάλειας, ιδίως με την οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17], τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής[18], την οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[19] και τον κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[20]***, καθώς και την πρόταση κανονισμού περί των προσανατολισμών για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών και την πρόταση κανονισμού σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (πράξη για την κυβερνοανθεκτικότητα)***. Επιπλέον, η σύσταση του Συμβουλίου σχετικά με μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών καλεί τα κράτη μέλη να λάβουν επείγοντα

για την παροχή βασικών υπηρεσιών στην εσωτερική αγορά.

και αποτελεσματικά μέτρα και να συνεργαστούν καλόπιστα, αποδοτικά, με αλληλεγγύη και με συντονισμένο τρόπο μεταξύ τους, με την Επιτροπή και άλλες σχετικές δημόσιες αρχές, καθώς και με τις οικείες οντότητες, για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών στην εσωτερική αγορά.

---

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

[18] Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

[19] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).

[20] 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) (ΕΕ L 151 της 7.6.2019, σ. 15).

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

[18] Σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ L 239 της 19.9.2017, σ. 36).

[19] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8).

[20] 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) (ΕΕ L 151 της 7.6.2019, σ. 15).

Τροπολογία 7

Πρόταση κανονισμού
Αιτιολογική σκέψη 4 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(4α) Μολονότι επικροτούμε την εργαλειοθήκη της Ευρωπαϊκής Επιτροπής για την κυβερνοασφάλεια στον τομέα των μεταφορών[2α], η οποία περιέχει βασικές πληροφορίες σχετικά με απειλές που ενδέχεται να επηρεάσουν τους οργανισμούς μεταφορών (διάδοση κακόβουλου λογισμικού, άρνηση υπηρεσίας, μη εξουσιοδοτημένη πρόσβαση και κλοπή, καθώς και παραποίηση λογισμικού) και παραθέτει ορθές πρακτικές μετριασμού, θα πρέπει να παρέχεται στους μεταφορείς κατάλληλη κατάρτιση σχετικά με την κυβερνοασφάλεια και κατάλληλα εργαλεία για την πρόληψη των κυβερνοαπειλών. Ο προϋπολογισμός της Ένωσης θα πρέπει επίσης να καλύπτει τη στήριξη, όπως η κατάρτιση, που παρέχεται από τον ENISA, ώστε να καταστεί δυνατή η αποτελεσματική εφαρμογή από τους μεταφορείς των βέλτιστων πρακτικών μετριασμού που περιλαμβάνονται στην εργαλειοθήκη.
	[1α] ENISA Threat Landscape: Transport sector (Το τοπίο των απειλών του ENISA: ο τομέας μεταφορών), ENISA, Μάρτιος 2023
	[2α] Ευρωπαϊκή Επιτροπή (2021). Εργαλειοθήκη για την κυβερνοασφάλεια στον τομέα των μεταφορών, διαθέσιμη στη διεύθυνση https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Τροπολογία 8

Πρόταση κανονισμού
Αιτιολογική σκέψη 4 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(4α) Η συντονισμένη προσέγγιση σε επίπεδο Ένωσης για την ενίσχυση της ετοιμότητας και της ανθεκτικότητας των κρίσιμων υποδομών, όπως οι υποδομές μεταφορών, βασίζεται στην ανάπτυξη ικανοτήτων των κρατών μελών. Όπως αναγνωρίζεται στην πρόσφατη ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ[19α], η ασφάλεια της ΕΕ δεν μπορεί να κατοχυρωθεί χωρίς το πιο πολύτιμο στοιχείο της ΕΕ: τους ανθρώπους της.
	[19α] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας για την ενίσχυση της ανταγωνιστικότητας, της ανάπτυξης και της ανθεκτικότητας της ΕΕ («Η Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας»), COM(2023) 207 final.

Τροπολογία 9

Πρόταση κανονισμού
Αιτιολογική σκέψη 12

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση και αντιμετώπιση κυβερνοαπειλών και περιστατικών, είναι αναγκαίο να αναπτυχθούν πληρέστερες γνώσεις σχετικά με τις απειλές κατά κρίσιμων πάγιων στοιχείων και υποδομών	(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση και αντιμετώπιση κυβερνοαπειλών και περιστατικών, είναι αναγκαίο να αναπτυχθούν πληρέστερες γνώσεις σχετικά με τις απειλές κατά κρίσιμων πάγιων στοιχείων και υποδομών

στο έδαφος της Ένωσης, συμπεριλαμβανομένης της γεωγραφικής κατανομής, της διασύνδεσης και των δυνητικών επιπτώσεών τους σε περίπτωση κυβερνοεπιθέσεων που επηρεάζουν τις εν λόγω υποδομές. Θα πρέπει να αναπτυχθεί μια μεγάλης κλίμακας ενωσιακή υποδομή SOC (στο εξής: ευρωπαϊκή κυβερνοασπίδα), η οποία θα αποτελείται από διάφορες διαλειτουργικές διασυνοριακές πλατφόρμες, καθεμία από τις οποίες θα συγκεντρώνει διάφορα εθνικά SOC. Οι εν λόγω υποδομές θα πρέπει να εξυπηρετούν εθνικά και ενωσιακά συμφέροντα και ανάγκες κυβερνοασφάλειας, αξιοποιώντας την τεχνολογία αιχμής για προηγμένα εργαλεία συλλογής και ανάλυσης δεδομένων, ενισχύοντας τις ικανότητες ανίχνευσης και διαχείρισης στον κυβερνοχώρο και παρέχοντας αντίληψη της κατάστασης σε πραγματικό χρόνο. Οι υποδομές αυτές θα πρέπει να χρησιμεύουν για την αύξηση της ανίχνευσης απειλών και περιστατικών κυβερνοασφάλειας και, ως εκ τούτου, να συμπληρώνουν και να στηρίζουν τις οντότητες και τα δίκτυα της Ένωσης που είναι αρμόδια για τη διαχείριση κρίσεων στην Ένωση, ιδίως το δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις της ΕΕ (στο εξής: EU-CyCLONe), όπως ορίζεται στην οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24].

[24] 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

στο έδαφος της Ένωσης, συμπεριλαμβανομένης της γεωγραφικής κατανομής, της διασύνδεσης και των δυνητικών επιπτώσεών τους σε περίπτωση κυβερνοεπιθέσεων που επηρεάζουν τις εν λόγω υποδομές***. Στα εν λόγω κρίσιμα πάγια στοιχεία και υποδομές περιλαμβάνονται τα συστήματα ευφυών μεταφορών, τα οποία, παρότι είναι απαραίτητα για την αυτοματοποιημένη και πολυτροπική κινητικότητα, λειτουργούν με βάση κρίσιμες ανταλλαγές ευαίσθητων δεδομένων.*** Θα πρέπει να αναπτυχθεί μια μεγάλης κλίμακας ενωσιακή υποδομή SOC (στο εξής: ευρωπαϊκή κυβερνοασπίδα), η οποία θα αποτελείται από διάφορες διαλειτουργικές διασυνοριακές πλατφόρμες, καθεμία από τις οποίες θα συγκεντρώνει διάφορα εθνικά SOC. Οι εν λόγω υποδομές θα πρέπει να εξυπηρετούν εθνικά και ενωσιακά συμφέροντα και ανάγκες κυβερνοασφάλειας, αξιοποιώντας την τεχνολογία αιχμής για προηγμένα εργαλεία συλλογής και ανάλυσης δεδομένων, ενισχύοντας τις ικανότητες ανίχνευσης και διαχείρισης στον κυβερνοχώρο και παρέχοντας αντίληψη της κατάστασης σε πραγματικό χρόνο. Οι υποδομές αυτές θα πρέπει να χρησιμεύουν για την αύξηση της ανίχνευσης απειλών και περιστατικών κυβερνοασφάλειας και, ως εκ τούτου, να συμπληρώνουν και να στηρίζουν τις οντότητες και τα δίκτυα της Ένωσης που είναι αρμόδια για τη διαχείριση κρίσεων στην Ένωση, ιδίως το δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις της ΕΕ (στο εξής: EU-CyCLONe), όπως ορίζεται στην οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[24].

[24] 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).

(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).

Τροπολογία 10

Πρόταση κανονισμού
Αιτιολογική σκέψη 14 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(14α) Ο τομέας των μεταφορών καθίσταται ολοένα και περισσότερο μία από τις πλέον επικερδείς επιχειρήσεις για τους κυβερνοεγκληματίες, καθώς τα δεδομένα των πελατών θεωρούνται εξαιρετικά πολύτιμο εμπόρευμα και η αλυσίδα εφοδιασμού στον τομέα των μεταφορών τίθεται όλο και συχνότερα στο στόχαστρο. Για τον λόγο αυτό, οι υποδομές μεταφορών που χαρακτηρίζονται από διασυνοριακό χαρακτήρα ή περιλαμβάνουν ανταλλαγή δεδομένων μέσω ασύρματων τεχνολογιών θα πρέπει να θεωρούνται κεντρικό αντικείμενο ανάλυσης και παρακολούθησης για τα εθνικά και, ιδίως, για τα διασυνοριακά SOC. Για παράδειγμα, η πρόσφατη πρόταση για την αναθεώρηση του κανονισμού ΔΕΔ-Μ απαιτεί μεγαλύτερη αλληλεγγύη και συνεργασία όσον αφορά την ανταλλαγή πληροφοριών σχετικά με διασυνοριακές κυβερνοαπειλές που ενδέχεται να αντιμετωπίσει αυτό το διακρατικό δίκτυο. Ομοίως, τα συστήματα ευφυών μεταφορών (ITS) είναι ζωτικής σημασίας για ασφαλέστερες, αποδοτικότερες και πιο βιώσιμες μεταφορές, εντούτοις καθιστούν τα συστήματα μεταφορών πιο ευάλωτα σε κυβερνοεπιθέσεις που μπορούν να προκαλέσουν ατυχήματα, κυκλοφοριακή συμφόρηση ή να επιφέρουν οικονομικές απώλειες τόσο σε ιδιωτικούς όσο και σε δημόσιους φορείς εκμετάλλευσης. Προκειμένου να διαφυλαχθεί η ασφάλεια των επιβατών, η

	προστασία των δεδομένων των χρηστών και των παρόχων και να αποφευχθούν οικονομικές ζημίες, είναι σημαντικό να συμπεριληφθούν στο πρόγραμμα εφαρμογής της αναθεωρημένης οδηγίας για τα συστήματα ευφυών μεταφορών διατάξεις και εργαλεία για την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών με σκοπό τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας.

Τροπολογία 11

Πρόταση κανονισμού
Αιτιολογική σκέψη 15

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών διασφαλίζεται συνήθως από τα SOC δημόσιων και ιδιωτικών οντοτήτων, σε συνδυασμό με τις CSIRT. Επιπλέον, οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Τα διασυνοριακά SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνωμόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης.	(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών διασφαλίζεται συνήθως από τα SOC δημόσιων και ιδιωτικών οντοτήτων, σε συνδυασμό με τις CSIRT. Επιπλέον, οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Τα διασυνοριακά SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνωμόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης. ***Στο πλαίσιο αυτό, προκειμένου να ενισχυθεί η αυτονομία της Ένωσης στον κυβερνοχώρο και με παραπομπή στο άρθρο 47 παράγραφος 4 της πρότασης κανονισμού περί των προσανατολισμών για την ανάπτυξη του διευρωπαϊκού δικτύου μεταφορών***

(COM(2021)0812), είναι επίσης αναγκαίο να αποτραπεί η πρόσβαση σε δεδομένα η οποία οδηγεί σε κυβερνοαπειλές, με την επιβολή ενός ισχυρού κανονιστικού πλαισίου που διέπει την ξένη ιδιοκτησία και τις ξένες επενδύσεις σε κρίσιμες υποδομές, όπως στις μεταφορές.

Τροπολογία 12

Πρόταση κανονισμού
Αιτιολογική σκέψη 21

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(21) Ενώ η ευρωπαϊκή κυβερνοασπίδα είναι ένα μη στρατιωτικό έργο, η κοινότητα κυβερνοάμυνας μπορεί να επωφεληθεί από ισχυρότερες μη στρατιωτικές ικανότητες ανίχνευσης και αντίληψης της κατάστασης που αναπτύχθηκαν για την προστασία κρίσιμων υποδομών. Τα διασυνοριακά SOC, με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC), και σε συνεργασία με τον/την ύπατο/-η εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: ύπατος/-η εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα και πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας. Η ανάπτυξη της ευρωπαϊκής κυβερνοασπίδας θα πρέπει να συνοδεύεται από προβληματισμό που θα επιτρέπει τη μελλοντική συνεργασία με δίκτυα και πλατφόρμες ανταλλαγής πληροφοριών στην κοινότητα κυβερνοάμυνας, σε στενή συνεργασία με τον/την ύπατο/-η εκπρόσωπο.	(21) Ενώ η ευρωπαϊκή κυβερνοασπίδα είναι ένα μη στρατιωτικό έργο, η κοινότητα κυβερνοάμυνας μπορεί να επωφεληθεί από ισχυρότερες μη στρατιωτικές ικανότητες ανίχνευσης και αντίληψης της κατάστασης που αναπτύχθηκαν για την προστασία κρίσιμων υποδομών. Τα διασυνοριακά SOC, με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC), και σε συνεργασία με τον/την ύπατο/-η εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: ύπατος/-η εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα και πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας. Η ανάπτυξη της ευρωπαϊκής κυβερνοασπίδας θα πρέπει να συνοδεύεται από προβληματισμό που θα επιτρέπει τη μελλοντική συνεργασία με δίκτυα και πλατφόρμες ανταλλαγής πληροφοριών στην κοινότητα κυβερνοάμυνας, σε στενή συνεργασία με τον/την ύπατο/-η εκπρόσωπο. ***Θα πρέπει επίσης να καθιστά δυνατές συνέργειες με το σχέδιο δράσης για τη στρατιωτική κινητικότητα 2.0. Ένα δίκτυο στρατιωτικής κινητικότητας με εύρυθμη***

	λειτουργία πρέπει να είναι ανθεκτικό, μεταξύ άλλων στο πλαίσιο κυβερνοαπειλών και άλλων υβριδικών απειλών που θα μπορούσαν να επηρεάσουν κρίσιμους κόμβους διπλής χρήσης του συστήματος μεταφορών. Για παράδειγμα, τυχόν κυβερνοεπίθεση σε συστήματα που χρησιμοποιούνται σε αερολιμένες, λιμένες ή σιδηροδρόμους ή κυβερνοεπίθεση σε στρατιωτικά πάγια στοιχεία θα μπορούσε να έχει σοβαρές συνέπειες. Επομένως, η ψηφιοποίηση διεργασιών και διαδικασιών, μεταξύ άλλων για την αναγκαία μη στρατιωτική και στρατιωτική συνεργασία, θα απαιτήσει την ενίσχυση των ηλεκτρονικών συστημάτων πληροφοριών (CIS) κατά των κυβερνοαπειλών.

Τροπολογία 13

Πρόταση κανονισμού
Αιτιολογική σκέψη 21 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(21α) Σε περίπτωση κρίσης κυβερνοασφάλειας, η αποτελεσματική ανταλλαγή πληροφοριών είναι καίριας σημασίας για να διασφαλιστεί η αντίληψη της κατάστασης μεταξύ του στρατιωτικού και του μη στρατιωτικού τομέα μεταφορών. Αυτή η ανταλλαγή πληροφοριών θα πρέπει επίσης να τονώσει τη συνεργασία μεταξύ των σχετικών τομεακών αρχών που είναι υπεύθυνες για τις μεταφορές, των αρμόδιων αρχών κυβερνοασφάλειας, των SOC και των CSIRT.

Τροπολογία 14

Πρόταση κανονισμού
Αιτιολογική σκέψη 29

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*

(29) Στο πλαίσιο των δράσεων ετοιμότητας, για την προώθηση συνεκτικής προσέγγισης και την ενίσχυση της ασφάλειας σε ολόκληρη την Ένωση και την εσωτερική αγορά της, θα πρέπει να παρέχεται στήριξη για τη δοκιμή και την αξιολόγηση της κυβερνοασφάλειας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας οι οποίοι προσδιορίζονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 με συντονισμένο τρόπο. Για τον σκοπό αυτό, η Επιτροπή, με την υποστήριξη του ENISA και σε συνεργασία με την ομάδα συνεργασίας NIS που συστάθηκε με την οδηγία (ΕΕ) 2022/2555, θα πρέπει να προσδιορίζει τακτικά σχετικούς τομείς ή υποτομείς, οι οποίοι θα πρέπει να είναι επιλέξιμοι για χρηματοδοτική στήριξη για συντονισμένες δοκιμές σε επίπεδο Ένωσης. Οι τομείς ή υποτομείς θα πρέπει να επιλέγονται από το παράρτημα I της οδηγίας (ΕΕ) 2022/2555 (στο εξής: τομείς υψηλής κρισιμότητας). Οι συντονισμένες δοκιμές θα πρέπει να βασίζονται σε κοινά σενάρια και μεθοδολογίες κινδύνου. Κατά την επιλογή των τομέων και την ανάπτυξη σεναρίων κινδύνου θα πρέπει να λαμβάνονται υπόψη οι σχετικές εκτιμήσεις κινδύνου και τα σενάρια κινδύνου σε επίπεδο Ένωσης, συμπεριλαμβανομένης της ανάγκης αποφυγής επικαλύψεων, όπως η εκτίμηση κινδύνου και τα σενάρια κινδύνου που απαιτούνται στα συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο που διενεργεί/εκπονεί η Επιτροπή, ο/η ύπατος/-η εκπρόσωπος και η ομάδα συνεργασίας NIS, σε συντονισμό με τους αρμόδιους μη στρατιωτικούς και στρατιωτικούς φορείς και οργανισμούς και τα δημιουργηθέντα δίκτυα, συμπεριλαμβανομένου του EU-CyCLONe, καθώς και η εκτίμηση κινδύνου των δικτύων και υποδομών επικοινωνιών που ζητείται από την κοινή υπουργική έκκληση της Nevers και διενεργείται από την ομάδα συνεργασίας NIS, με την υποστήριξη της Επιτροπής και του ENISA, και σε

(29) Στο πλαίσιο των δράσεων ετοιμότητας, για την προώθηση συνεκτικής προσέγγισης και την ενίσχυση της ασφάλειας σε ολόκληρη την Ένωση και την εσωτερική αγορά της, θα πρέπει να παρέχεται στήριξη για τη δοκιμή και την αξιολόγηση της κυβερνοασφάλειας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας οι οποίοι προσδιορίζονται σύμφωνα με την οδηγία (ΕΕ) 2022/2555 με συντονισμένο τρόπο. Για τον σκοπό αυτό, η Επιτροπή, με την υποστήριξη του ENISA και σε συνεργασία με την ομάδα συνεργασίας NIS που συστάθηκε με την οδηγία (ΕΕ) 2022/2555, θα πρέπει να προσδιορίζει τακτικά σχετικούς τομείς ή υποτομείς, οι οποίοι θα πρέπει να είναι επιλέξιμοι για χρηματοδοτική στήριξη για συντονισμένες δοκιμές σε επίπεδο Ένωσης. Οι τομείς ή υποτομείς θα πρέπει να επιλέγονται από το παράρτημα I της οδηγίας (ΕΕ) 2022/2555 (στο εξής: τομείς υψηλής κρισιμότητας)**.** ***Ιδιαίτερη προσοχή θα πρέπει να δοθεί στον τομέα των μεταφορών και στους υποτομείς του (εναέριες, σιδηροδρομικές, πλωτές, οδικές μεταφορές), καθώς ενσωματώνουν κρίσιμες υποδομές όπου περιστατικά στον κυβερνοχώρο και κυβερνοεπιθέσεις θα μπορούσαν να υπονομεύσουν σοβαρά την ασφάλεια των επιβατών και των φορέων εκμετάλλευσης.*** Οι συντονισμένες δοκιμές θα πρέπει να βασίζονται σε κοινά σενάρια και μεθοδολογίες κινδύνου. Κατά την επιλογή των τομέων και την ανάπτυξη σεναρίων κινδύνου θα πρέπει να λαμβάνονται υπόψη οι σχετικές εκτιμήσεις κινδύνου και τα σενάρια κινδύνου σε επίπεδο Ένωσης, συμπεριλαμβανομένης της ανάγκης αποφυγής επικαλύψεων, όπως η εκτίμηση κινδύνου και τα σενάρια κινδύνου που απαιτούνται στα συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο που διενεργεί/εκπονεί η Επιτροπή, ο/η ύπατος/-η εκπρόσωπος και η ομάδα συνεργασίας NIS, σε συντονισμό με τους

συνεργασία με τον Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), οι συντονισμένες εκτιμήσεις κινδύνου που πρέπει να διενεργούνται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555 και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[29]. Κατά την επιλογή των τομέων θα πρέπει επίσης να λαμβάνεται υπόψη η σύσταση του Συμβουλίου σχετικά με συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών.

[29] 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.

αρμόδιους μη στρατιωτικούς και στρατιωτικούς φορείς και οργανισμούς και τα δημιουργηθέντα δίκτυα, συμπεριλαμβανομένου του EU-CyCLONe, καθώς και η εκτίμηση κινδύνου των δικτύων και υποδομών επικοινωνιών που ζητείται από την κοινή υπουργική έκκληση της Nevers και διενεργείται από την ομάδα συνεργασίας NIS, με την υποστήριξη της Επιτροπής και του ENISA, και σε συνεργασία με τον Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), οι συντονισμένες εκτιμήσεις κινδύνου που πρέπει να διενεργούνται σύμφωνα με το άρθρο 22 της οδηγίας (ΕΕ) 2022/2555 και οι δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας, όπως προβλέπεται στον κανονισμό (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[29]. Κατά την επιλογή των τομέων θα πρέπει επίσης να λαμβάνεται υπόψη η σύσταση του Συμβουλίου σχετικά με συντονισμένη προσέγγιση σε επίπεδο Ένωσης με σκοπό την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών.

[29] 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.

Τροπολογία 15

Πρόταση κανονισμού
Αιτιολογική σκέψη 30 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(30α) Δεδομένης της κρισιμότητας του τομέα και των επιπτώσεων των κυβερνοαπειλών στην κινητικότητα και,

	κατά συνέπεια, στη ζωή των επιβατών και των πεζών, θα πρέπει να δοθεί προτεραιότητα στον τομέα των μεταφορών όσον αφορά τις συντονισμένες δοκιμές ετοιμότητας των οντοτήτων.

Τροπολογία 16

Πρόταση κανονισμού
Αιτιολογική σκέψη 35 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(35α) Δεδομένων των αυξημένων καθηκόντων και αρμοδιοτήτων που ανατίθενται στον ENISA με την παρούσα πρόταση, καθώς και με την πρόταση σχετικά με την πράξη για την κυβερνοανθεκτικότητα, είναι αναγκαία η έγκριση του διορθωτικού προϋπολογισμού 1/2022 του ENISA για την πιλοτική εφαρμογή δράσης στήριξης για την κυβερνοασφάλεια. Επιπλέον, λαμβανομένων υπόψη των συμφερόντων της Ένωσης που διακυβεύονται, θα πρέπει να διατεθούν στον ENISA πρόσθετοι χρηματοδοτικοί και ανθρώπινοι πόροι.

Τροπολογία 17

Πρόταση κανονισμού
Αιτιολογική σκέψη 38 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(38α) Ως εκ τούτου, η ανάπτυξη δεξιοτήτων και ικανοτήτων θα πρέπει να βρίσκεται στο επίκεντρο σε όλους τους τομείς, ιδίως για αυτούς που είναι ευάλωτοι σε απειλές κατά της κυβερνοασφάλειας, όπως το προσωπικό που εργάζεται σε μαζικές συγκοινωνίες ή σε κρίσιμες υποδομές, συμπεριλαμβανομένων των συστημάτων ελέγχου αμαξοστοιχιών και των

	ψηφιακών εργαλείων σχεδιασμού μεταφορών για όλα τα μέσα μεταφοράς. Επομένως, η εισαγωγή και η περαιτέρω ανάπτυξη της νοοτροπίας κυβερνοασφάλειας είναι υψίστης σημασίας για την επιτυχία της εφαρμογής του παρόντος κανονισμού τόσο για την ευαισθητοποίηση των πολιτών όσο και για τις γνώσεις των ειδικών σε όλους τους τομείς κρίσιμων υποδομών.

Τροπολογία 18

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 2 – στοιχείο α

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
α) την ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά απειλές και περιστατικά στον κυβερνοχώρο, ώστε να παρέχεται η δυνατότητα ενίσχυσης της ανταγωνιστικής θέσης των τομέων της βιομηχανίας και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία και συμβολής στην τεχνολογική κυριαρχία της Ένωσης στον τομέα της κυβερνοασφάλειας,	α) την ενίσχυση της κοινής ενωσιακής ανίχνευσης και αντίληψης της κατάστασης όσον αφορά απειλές και περιστατικά στον κυβερνοχώρο, ώστε να παρέχεται η δυνατότητα ενίσχυσης της ανταγωνιστικής θέσης των τομέων της βιομηχανίας, ***των υποδομών μεταφορών*** και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία και συμβολής στην τεχνολογική κυριαρχία της Ένωσης στον τομέα της κυβερνοασφάλειας,

Τροπολογία 19

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 2 – στοιχείο β

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
β) την αύξηση του βαθμού ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση και την ενίσχυση της αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την εξασφάλιση ενωσιακής	β) την αύξηση του βαθμού ετοιμότητας των οντοτήτων που δραστηριοποιούνται σε τομείς κρίσιμης και εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση και την ενίσχυση της αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, ***με ιδιαίτερη έμφαση σε κρίσιμες υποδομές ΤΠ και***

στήριξης για την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη»,	***υλικές υποδομές,*** μεταξύ άλλων με την εξασφάλιση ενωσιακής στήριξης για την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη»·

Τροπολογία 20

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 2 – στοιχείο γ α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	γ α) την ενίσχυση της ετοιμότητας, της συνεργασίας και της αποτελεσματικότητας της Ένωσης όσον αφορά την προστασία των υποδομών και των υπηρεσιών μεταφορών στα κράτη μέλη από περιστατικά κυβερνοασφάλειας, ώστε να διασφαλιστεί η συνεχής λειτουργία του τομέα των μεταφορών, η ακεραιότητα των αλυσίδων εφοδιασμού και η κινητικότητα σε ολόκληρη την Ένωση.

Τροπολογία 21

Πρόταση κανονισμού
Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο γ

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
γ) συμβάλλει στην καλύτερη προστασία και αντιμετώπιση των κυβερνοαπειλών,	γ) συμβάλλει στην καλύτερη προστασία και αντιμετώπιση των κυβερνοαπειλών***, μεταξύ άλλων για τις υποδομές μεταφορών που διακρίνονται για τον διασυνοριακό τους χαρακτήρα, όπως το ΔΕΔ-Μ, ή περιλαμβάνουν την ανταλλαγή δεδομένων μέσω ασύρματων τεχνολογιών, όπως τα συστήματα ευφυών μεταφορών.***

Τροπολογία 22

Πρόταση κανονισμού

Άρθρο 3 – παράγραφος 2 – εδάφιο 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
Αναπτύσσεται σε συνεργασία με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε δυνάμει του κανονισμού (ΕΕ) 2021/1173.	Αναπτύσσεται σε συνεργασία με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε δυνάμει του κανονισμού (ΕΕ) 2021/1173. ***Καθιστά δυνατή τη συνεργασία, μέσω ειδικών πρωτοκόλλων και προτύπων, με την κοινότητα κυβερνοάμυνας, προκειμένου να διασφαλιστεί η ανάπτυξη ισχυρότερων ικανοτήτων μη στρατιωτικής ανίχνευσης και αντίληψης της κατάστασης για την προστασία των κρίσιμων υποδομών. Στο πλαίσιο αυτό, αναπτύσσονται συνέργειες και με το σχέδιο δράσης για τη στρατιωτική κινητικότητα 2.0 και εξασφαλίζεται αποτελεσματική ανταλλαγή πληροφοριών προκειμένου να διασφαλιστεί η αντίληψη της κατάστασης μεταξύ του στρατιωτικού και του μη στρατιωτικού τομέα μεταφορών.***

Τροπολογία 23

Πρόταση κανονισμού
Άρθρο 8 – παράγραφος 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	2α. Η Επιτροπή εμπλέκει την ευρωπαϊκή κυβερνοασπίδα, ιδίως τα διασυνοριακά SOC, στη γνώμη που απευθύνει προς τα κράτη μέλη στο πλαίσιο της πρότασης κανονισμού σχετικά με το διευρωπαϊκό δίκτυο μεταφορών (COM(2021)0812), σε περίπτωση που η οποιουδήποτε είδους συμμετοχή ή συνεισφορά φυσικού προσώπου τρίτης χώρας ή επιχείρησης τρίτης χώρας είναι πιθανό να επηρεάσει την κυβερνοασφάλεια διασυνοριακών κρίσιμων υποδομών, όπως το ΔΕΔ-Μ.

Τροπολογία 24

Πρόταση κανονισμού
Άρθρο 10 – παράγραφος 1 – στοιχείο α

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
α) δράσεις ετοιμότητας, συμπεριλαμβανομένων των συντονισμένων δοκιμών ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση,	α) δράσεις ετοιμότητας, συμπεριλαμβανομένων των συντονισμένων δοκιμών ετοιμότητας οντοτήτων που δραστηριοποιούνται σε τομείς εξαιρετικά κρίσιμης σημασίας σε ολόκληρη την Ένωση***, με ιδιαίτερη προσοχή στις υποδομές μεταφορών και στους υποτομείς τους που περιλαμβάνονται στο παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555·***

Τροπολογία 25

Πρόταση κανονισμού
Άρθρο 18 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλεύεται άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.	2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας**,** ***συμπεριλαμβανομένων των μεταφορέων***. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλεύεται άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.

Τροπολογία 26

Πρόταση κανονισμού
Άρθρο 19 – παράγραφος 1 – σημείο 1 – στοιχείο β
Κανονισμός (ΕΕ) 2021/694
Άρθρο 6 – παράγραφος 2α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	2α. Λαμβανομένων υπόψη των συμφερόντων της Ένωσης που διακυβεύονται, σε σχέση με τις αρμοδιότητές του για την προετοιμασία των υποψήφιων συστημάτων πιστοποίησης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881, τις αρμοδιότητές του να εξετάζει και να αξιολογεί τις κυβερνοαπειλές, τα τρωτά σημεία και τον μετριασμό τους, να καταρτίζει έκθεση εξέτασης περιστατικού για τον μηχανισμό εξέτασης περιστατικών κυβερνοασφάλειας, καθώς και να παρέχει κατάρτιση κατά των κυβερνοεπιθέσεων και των περιστατικών στον κυβερνοχώρο σε φορείς εκμετάλλευσης κρίσιμων υποδομών και υπό το πρίσμα των νέων αρμοδιοτήτων του στο πλαίσιο της πρότασης για την πράξη για την κυβερνοανθεκτικότητα, ο ENISA λαμβάνει τους αναγκαίους πόρους στο πλαίσιο του προϋπολογισμού της Ένωσης σύμφωνα με την ισχύουσα νομοθεσία.

Τροπολογία 27

Πρόταση κανονισμού
Άρθρο 19 – παράγραφος 1 – σημείο 1α (νέο)
Κανονισμός (ΕΕ) 2021/694
Άρθρο 7 – παράγραφος 1 – στοιχείο γα (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	1α) το άρθρο 7 τροποποιείται ως εξής:
	α) η παράγραφος 1 τροποποιείται ως εξής:
	(1) παρεμβάλλεται το ακόλουθο στοιχείο γ α):
	γ α) στήριξη της κατάρτισης υψηλής ποιότητας για τους μεταφορείς, καθώς

και τους διαχειριστές και το εργατικό δυναμικό κρίσιμων υποδομών μεταφορών, με στόχο επίσης την αποτελεσματική ανταλλαγή και εφαρμογή πρακτικών μετριασμού κατά κυβερνοεπιθέσεων ή περιστατικών σε κρίσιμες υποδομές, όπως οι πρακτικές που παρέχονται από την εργαλειοθήκη για την κυβερνοασφάλεια στον τομέα των μεταφορών.

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΓΝΩΜΟΔΟΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ

Τίτλος	Καθορισμός μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας
Έγγραφα αναφοράς	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Επιτροπή αρμόδια επί της ουσίας Ημερομ. αναγγελίας στην ολομέλεια	ITRE 1.6.2023
Γνωμοδότηση της Ημερομ. αναγγελίας στην ολομέλεια	TRAN 1.6.2023
Συντάκτης γνωμοδότησης Ημερομηνία ορισμού	Gheorghe Falcă 7.7.2023
Ημερομηνία έγκρισης	25.10.2023
Αποτέλεσμα της τελικής ψηφοφορίας	+: 38 –: 0 0: 0
Βουλευτές παρόντες κατά την τελική ψηφοφορία	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Έλενα Κουντουρά, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Ελισσάβετ Βόζεμπεργκ-Βρυωνίδη, Lucia Vuolo
Αναπληρωτές παρόντες κατά την τελική ψηφοφορία	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

ΤΕΛΙΚΗ ΨΗΦΟΦΟΡΙΑ ΜΕ ΟΝΟΜΑΣΤΙΚΗ ΚΛΗΣΗ ΣΤΗ ΓΝΩΜΟΔΟΤΙΚΗ ΕΠΙΤΡΟΠΗ

38	**+**
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Έλενα Κουντουρά
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	**-**

0	**0**

Υπόμνημα των χρησιμοποιούμενων συμβόλων::
+ : υπέρ
- : κατά
0 : αποχή