Ευρωπαϊκό Κοινοβούλιο
2019-2024

Επιτροπή Εξωτερικών Υποθέσεων

2023/0109(COD)

27.10.2023

ΓΝΩΜΟΔΟΤΗΣΗ

της Επιτροπής Εξωτερικών Υποθέσεων

προς την Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας

σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με 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: Dragoş Tudorache

PA_Legam

Τροπολογία 1

Πρόταση κανονισμού
Αιτιολογική σκέψη 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής δραστηριότητας, καθώς οι δημόσιες διοικήσεις, οι εταιρείες μας και οι πολίτες είναι πιο διασυνδεδεμένοι και αλληλεξαρτώμενοι από ποτέ, πέρα από τομείς και σύνορα.	(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής ***και στρατιωτικής*** δραστηριότητας, καθώς οι δημόσιες διοικήσεις, οι εταιρείες μας και οι πολίτες***, όπως και οι στρατιωτικοί φορείς και οι φορείς στον τομέα της άμυνας*** είναι πιο διασυνδεδεμένοι και αλληλεξαρτώμενοι από ποτέ, πέρα από τομείς και σύνορα.

Τροπολογία 2

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	(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 σοβαρότητα αυτών των απειλών κατέστη ακόμη πιο σημαντική λόγω της επιστροφής του πολέμου στην ήπειρό μας. Οι απειλές αυτές υπερβαίνουν*** τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και ***είναι*** πιθανό να

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. 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.

συνεχίσουν να υφίστανται, 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 ***και την ασφάλεια*** της Ένωσης, και μπορούν ακόμη και να έχουν συνέπειες που απειλούν την υγεία ή τη ζωή, ***υπονομεύοντας ενδεχομένως εγκαταστάσεις που σχετίζονται με την τοπική ή εθνική ασφάλεια***. 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. ***Η κυβερνοασφάλεια είναι σημαντική για την προστασία των ευρωπαϊκών αξιών μας και διασφαλίζει τη λειτουργία των δημοκρατιών μας, θωρακίζοντας τις εκλογικές μας υποδομές και τις δημοκρατικές μας διαδικασίες από κάθε ξένη παρέμβαση.***

Τροπολογία 3

Πρόταση κανονισμού
Αιτιολογική σκέψη 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(2α) Η κυβερνοασφάλεια είναι ζωτικής σημασίας για την ασφάλεια της Ένωσης μας και την πρόληψη της υπονόμευσης της δημοκρατίας, της οικονομίας και της ασφάλειάς μας από κακόβουλους,

	κρατικούς και μη κρατικούς παράγοντες. Είναι σημαντικό να αποφευχθεί ο κατακερματισμός του τομέα, δεδομένου ότι μια τέτοια κατάσταση δεν θα αποτελούσε κατάλληλη προσέγγιση, ιδίως κατά την αντιμετώπιση προκλήσεων όπως μια πιθανή μελλοντική επίθεση μεγάλης κλίμακας στον κυβερνοχώρο που θα στοχεύει πολλά κράτη μέλη ταυτόχρονα ή διακρατικές κρίσιμες υποδομές· Ως εκ τούτου είναι σημαντικό να οριστεί ένας φορέας της Ένωσης που θα λειτουργεί ως πλατφόρμα συντονισμού για όλα τα υφιστάμενα και μελλοντικά μέσα, κονδύλια και μηχανισμούς κυβερνοασφάλειας.

Τροπολογία 4

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

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***, καθώς και την ικανότητά της να ενεργεί προορατικά και να αντιδρά αποφασιστικά σε τέτοιες απειλές και περιστατικά κυβερνοασφάλειας***.

[16] https://wayback.archive-it.org/12090/20230417171535/https://futureu.europa.eu/el/

[16] https://wayback.archive-it.org/12090/20230417171535/https://futureu.europa.eu/el/

Τροπολογία 5

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 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]. 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	(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]. 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 ***και προορατικά***, με αλληλεγγύη και με συντονισμένο τρόπο μεταξύ τους, με την Επιτροπή και άλλες

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.

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. ***Επιπλέον, η Ένωση ενέκρινε και παρουσίασε τον Μάρτιο του 2022 τη στρατηγική πυξίδα της για την ασφάλεια και την άμυνα, η οποία επικεντρώνεται, μεταξύ άλλων, στην ενίσχυση της κυβερνοασφάλειας και στην ενδυνάμωση της διεθνούς συνεργασίας με συμμάχους και δημοκρατικούς εταίρους που συμμερίζονται τις ίδιες απόψεις, ιδίως σε αυτό το θέμα. Επιπλέον, η κυβερνοασφάλεια αποτέλεσε το επίκεντρο της πρόσφατης τρίτης κοινής δήλωσης για τη συνεργασία ΕΕ-ΝΑΤΟ του Ιανουαρίου 2023. Ειδικότερα, η τελική έκθεση αξιολόγησης της ειδικής ομάδας ΕΕ-ΝΑΤΟ συνέστησε την πλήρη αξιοποίηση των συνεργειών μεταξύ της ΕΕ και του ΝΑΤΟ[1], συμπεριλαμβανομένης της ανταλλαγής βέλτιστων πρακτικών μεταξύ πολιτικών και στρατιωτικών παραγόντων όσον αφορά την εφαρμογή των σχετικών πολιτικών και νομοθεσίας σε σχέση με τον κυβερνοχώρο***.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[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

[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).

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 6

Πρόταση κανονισμού
Αιτιολογική σκέψη 6

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(6) Η κοινή ανακοίνωση σχετικά με την «Πολιτική της ΕΕ για την κυβερνοάμυνα»[22], που εκδόθηκε στις 10 Νοεμβρίου 2022, ανήγγειλε μια πρωτοβουλία αλληλεγγύης της ΕΕ στον κυβερνοχώρο με τους ακόλουθους στόχους: ενίσχυση των κοινών ικανοτήτων ανίχνευσης, αντίληψης της κατάστασης και αντίδρασης της ΕΕ μέσω της προώθησης της ανάπτυξης υποδομής κέντρων επιχειρήσεων ασφάλειας της ΕΕ (στο εξής: SOC), της στήριξης της σταδιακής δημιουργίας εφεδρείας στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και της δοκιμής κρίσιμων οντοτήτων για πιθανά τρωτά σημεία με	(6) Η κοινή ανακοίνωση σχετικά με την «Πολιτική της ΕΕ για την κυβερνοάμυνα»[22], που εκδόθηκε στις 10 Νοεμβρίου 2022, ανήγγειλε μια πρωτοβουλία αλληλεγγύης της ΕΕ στον κυβερνοχώρο με τους ακόλουθους στόχους: ενίσχυση των κοινών ικανοτήτων ανίχνευσης, αντίληψης της κατάστασης και αντίδρασης της ΕΕ μέσω της προώθησης της ανάπτυξης υποδομής κέντρων επιχειρήσεων ασφάλειας της ΕΕ (στο εξής: SOC), της στήριξης της σταδιακής δημιουργίας εφεδρείας στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ με υπηρεσίες από αξιόπιστους ιδιωτικούς παρόχους και της δοκιμής κρίσιμων οντοτήτων για πιθανά τρωτά σημεία με

βάση εκτιμήσεις κινδύνου της ΕΕ.	βάση εκτιμήσεις κινδύνου της ΕΕ. ***Επιπλέον, το ταχέως εξελισσόμενο τοπίο των κυβερνοαπειλών και ο ταχύς ρυθμός της τεχνολογικής ανάπτυξης καταδεικνύουν επίσης την ανάγκη για ενισχυμένο πολιτικοστρατιωτικό συντονισμό και συνεργασία, όπως τόνισε το Συμβούλιο στα συμπεράσματά του σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα[1].*** ***[1] Συμπεράσματα του Συμβουλίου σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα, τα οποία εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 22 Μαΐου 2023 (9618/23).***
[22] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].	[22] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].

Τροπολογία 7

Πρόταση κανονισμού
Αιτιολογική σκέψη 6 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(6α) Δεδομένου ότι δεν είναι σαφής ο διαχωρισμός των ζητημάτων που εμπίπτουν στον στρατιωτικό και στον μη στρατιωτικό τομέα και ότι τα εργαλεία και οι τεχνολογίες στον κυβερνοχώρο έχουν εκ φύσεως διπλή χρήση, υπάρχει ανάγκη για μια ολοκληρωμένη και ολιστική προσέγγιση στον ψηφιακό τομέα. Σε περίπτωση περιστατικού και κρίσης κυβερνοασφάλειας μεγάλης κλίμακας που αφορά περισσότερα του ενός κράτη μέλη, θα πρέπει να θεσπιστεί κατάλληλη διαχείριση και διακυβέρνηση κρίσεων. Οι δομές αυτές θα πρέπει να οργανώνουν την ανταλλαγή πληροφοριών, τον συντονισμό και τη συνεργασία με τις δομές εξωτερικής ασφάλειας και διαχείρισης στρατιωτικών κρίσεων της

Ένωσης, καθώς και με τους φορείς των κρατών μελών που είναι αρμόδιοι για την ασφάλεια και την άμυνα (την κοινότητα κυβερνοάμυνας). Αυτό θα πρέπει να ισχύει επίσης για τις επιχειρήσεις και αποστολές της Κοινής Πολιτικής Ασφάλειας και Άμυνας που διεξάγονται από την Ένωση για τη διασφάλιση της ειρήνης και της σταθερότητας στη γειτονία της και πέραν αυτής.

Τροπολογία 8

Πρόταση κανονισμού
Αιτιολογική σκέψη 7

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(7) Είναι αναγκαίο να ενισχυθούν η ανίχνευση και η αντίληψη της κατάστασης όσον αφορά τις απειλές και τα περιστατικά στον κυβερνοχώρο σε ολόκληρη την Ένωση και να ενισχυθεί η αλληλεγγύη με την ενίσχυση της ετοιμότητας και των ικανοτήτων των κρατών μελών και της Ένωσης για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, θα πρέπει να αναπτυχθεί πανευρωπαϊκή υποδομή SOC (ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης· θα πρέπει να δημιουργηθεί μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντίδραση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας· θα πρέπει να θεσπιστεί μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση συγκεκριμένων σημαντικών ή μεγάλης κλίμακας περιστατικών. Οι εν λόγω δράσεις δεν θίγουν τα άρθρα 107 και 108 της Συνθήκης για τη λειτουργία της	(7) Είναι αναγκαίο να ενισχυθούν η ανίχνευση και η αντίληψη της κατάστασης όσον αφορά τις απειλές και τα περιστατικά στον κυβερνοχώρο σε ολόκληρη την Ένωση και να ενισχυθεί η αλληλεγγύη με την ενίσχυση της ετοιμότητας και των ικανοτήτων των κρατών μελών και της Ένωσης για την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Ως εκ τούτου, θα πρέπει να αναπτυχθεί πανευρωπαϊκή υποδομή SOC (ευρωπαϊκή κυβερνοασπίδα) για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης· θα πρέπει να δημιουργηθεί μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια με σκοπό τη στήριξη των κρατών μελών όσον αφορά την προετοιμασία, την αντίδραση και την άμεση ανάκαμψη από σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας***, συμπεριλαμβανομένων των περιστατικών που αφορούν περισσότερα του ενός κράτη μέλη. Στις περιπτώσεις που είναι εφικτό και αναγκαίο, ένας μηχανισμός έκτακτης ανάγκης για την κυβερνοασφάλεια θα πρέπει να οργανώνει την ανταλλαγή πληροφοριών και τη συνεργασία με τις***

Ευρωπαϊκής Ένωσης (στο εξής: ΣΛΕΕ).	***αμυντικές αρχές των κρατών μελών που υποστηρίζονται από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ (κοινότητα κυβερνοάμυνας της ΕΕ)***· θα πρέπει να θεσπιστεί μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση συγκεκριμένων σημαντικών ή μεγάλης κλίμακας περιστατικών. Τέτοιου είδους νέες δομές θα πρέπει επίσης να στηρίζουν τις επιχειρήσεις και τις αποστολές της Κοινής Πολιτικής Ασφάλειας και Άμυνας της ΕΕ. Οι εν λόγω δράσεις δεν θίγουν τα άρθρα 107 και 108 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (στο εξής: ΣΛΕΕ).

Τροπολογία 9

Πρόταση κανονισμού
Αιτιολογική σκέψη 11

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(11) Για τους σκοπούς της χρηστής δημοσιονομικής διαχείρισης, θα πρέπει να θεσπιστούν ειδικοί κανόνες για τη μεταφορά αχρησιμοποίητων πιστώσεων ανάληψης υποχρεώσεων και πιστώσεων πληρωμών. Τηρουμένης της αρχής ότι ο προϋπολογισμός της Ένωσης καθορίζεται ετησίως, ο παρών κανονισμός θα πρέπει, λόγω του απρόβλεπτου, έκτακτου και ειδικού χαρακτήρα του τοπίου της κυβερνοασφάλειας, να προβλέπει δυνατότητες μεταφοράς αχρησιμοποίητων κονδυλίων πέραν εκείνων που ορίζονται στον δημοσιονομικό κανονισμό, μεγιστοποιώντας έτσι την ικανότητα του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια να στηρίζει τα κράτη μέλη όσον αφορά την αποτελεσματική αντιμετώπιση κυβερνοαπειλών.	(11) Για τους σκοπούς της χρηστής δημοσιονομικής διαχείρισης, θα πρέπει να θεσπιστούν ειδικοί κανόνες για τη μεταφορά αχρησιμοποίητων πιστώσεων ανάληψης υποχρεώσεων και πιστώσεων πληρωμών. Τηρουμένης της αρχής ότι ο προϋπολογισμός της Ένωσης καθορίζεται ετησίως, ο παρών κανονισμός θα πρέπει, λόγω του απρόβλεπτου, έκτακτου και ειδικού χαρακτήρα του τοπίου της κυβερνοασφάλειας, να προβλέπει δυνατότητες μεταφοράς αχρησιμοποίητων κονδυλίων πέραν εκείνων που ορίζονται στον δημοσιονομικό κανονισμό, μεγιστοποιώντας έτσι την ικανότητα του μηχανισμού έκτακτης ανάγκης για την κυβερνοασφάλεια να στηρίζει τα κράτη μέλη όσον αφορά την αποτελεσματική αντιμετώπιση κυβερνοαπειλών. ***Οι εν λόγω ειδικοί κανόνες θα καταστήσουν επίσης δυνατή μια πιο μακροπρόθεσμη χρηματοδοτική στήριξη για την από κοινού προμήθεια εξαιρετικά ασφαλών εργαλείων και υποδομών επόμενης γενιάς,***

	με σκοπό τη βελτίωση των συλλογικών ικανοτήτων ανίχνευσης με τη χρήση της πλέον πρόσφατης τεχνητής νοημοσύνης (ΤΝ) και ανάλυσης δεδομένων.

Τροπολογία 10

Πρόταση κανονισμού
Αιτιολογική σκέψη 13

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(13) Κάθε κράτος μέλος θα πρέπει να ορίσει έναν δημόσιο φορέα σε εθνικό επίπεδο επιφορτισμένο με τον συντονισμό των δραστηριοτήτων ανίχνευσης κυβερνοαπειλών στο εν λόγω κράτος μέλος. Τα εν λόγω εθνικά SOC θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή στην ευρωπαϊκή κυβερνοασπίδα και θα πρέπει να διασφαλίζουν ότι οι πληροφορίες σχετικά με τις κυβερνοαπειλές από δημόσιους και ιδιωτικούς φορείς ανταλλάσσονται και συλλέγονται σε εθνικό επίπεδο με αποτελεσματικό και εξορθολογισμένο τρόπο.	(13) Κάθε κράτος μέλος θα πρέπει να ορίσει έναν δημόσιο φορέα σε εθνικό επίπεδο επιφορτισμένο με τον συντονισμό των δραστηριοτήτων ανίχνευσης κυβερνοαπειλών στο εν λόγω κράτος μέλος. Τα εν λόγω εθνικά SOC θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή στην ευρωπαϊκή κυβερνοασπίδα και θα πρέπει να διασφαλίζουν ότι οι πληροφορίες σχετικά με τις κυβερνοαπειλές από δημόσιους και ιδιωτικούς φορείς ανταλλάσσονται και συλλέγονται σε εθνικό επίπεδο με αποτελεσματικό και εξορθολογισμένο τρόπο. ***Όταν είναι εφικτό και αναγκαίο, τα SOC θα πρέπει επίσης να επιτρέπουν τη συμμετοχή αμυντικών οντοτήτων, δημιουργώντας έναν «αμυντικό πυλώνα» όσον αφορά τη διακυβέρνηση και το είδος των πληροφοριών που ανταλλάσσονται, όπως ορίζεται στην κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα[1] και υποστηρίζεται από τον/την ύπατο/-η εκπρόσωπο.*** ***[1] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].***

Τροπολογία 11

Πρόταση κανονισμού
Αιτιολογική σκέψη 14

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(14) Στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας, θα πρέπει να συσταθούν ορισμένα διασυνοριακά κέντρα επιχειρήσεων κυβερνοασφάλειας (στο εξής: διασυνοριακά SOC). Σε αυτά θα πρέπει να συμμετέχουν εθνικά SOC από τουλάχιστον τρία κράτη μέλη, ώστε να μπορούν να επιτευχθούν πλήρως τα οφέλη της διασυνοριακής ανίχνευσης απειλών και της ανταλλαγής και διαχείρισης πληροφοριών. Γενικός στόχος των διασυνοριακών SOC θα πρέπει να είναι η ενίσχυση των ικανοτήτων ανάλυσης, πρόληψης και ανίχνευσης απειλών κυβερνοασφάλειας και η υποστήριξη της παραγωγής υψηλής ποιότητας πληροφοριών σχετικά με τις απειλές κυβερνοασφάλειας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες ή ιδιωτικές, καθώς και μέσω της ανταλλαγής και της κοινής χρήσης εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης σε ένα αξιόπιστο περιβάλλον. Θα πρέπει να παρέχουν νέα πρόσθετη ικανότητα, αξιοποιώντας και συμπληρώνοντας τα υφιστάμενα SOC και τις ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT) και άλλους σχετικούς παράγοντες.	(14) Στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας, θα πρέπει να συσταθούν ορισμένα διασυνοριακά κέντρα επιχειρήσεων κυβερνοασφάλειας (στο εξής: διασυνοριακά SOC). Σε αυτά θα πρέπει να συμμετέχουν εθνικά SOC από τουλάχιστον τρία κράτη μέλη, ***συμπεριλαμβανομένου ενός «πυλώνα άμυνας»,*** ώστε να μπορούν να επιτευχθούν πλήρως τα οφέλη της διασυνοριακής ανίχνευσης απειλών και της ανταλλαγής και διαχείρισης πληροφοριών. Γενικός στόχος των διασυνοριακών SOC θα πρέπει να είναι η ενίσχυση των ικανοτήτων ανάλυσης, πρόληψης και ανίχνευσης απειλών κυβερνοασφάλειας και η υποστήριξη της παραγωγής υψηλής ποιότητας πληροφοριών σχετικά με τις απειλές κυβερνοασφάλειας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες ή ιδιωτικές ***και, όταν είναι απαραίτητο και εφικτό, στρατιωτικές, με επαρκή καθοδήγηση για ανταλλαγή πληροφοριών,*** καθώς και μέσω της ανταλλαγής και της κοινής χρήσης εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης σε ένα αξιόπιστο περιβάλλον. Θα πρέπει να παρέχουν νέα πρόσθετη ικανότητα, αξιοποιώντας και συμπληρώνοντας τα υφιστάμενα SOC και τις ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT) και άλλους σχετικούς παράγοντες.

Τροπολογία 12

Πρόταση κανονισμού
Αιτιολογική σκέψη 15

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών	(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.

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 ***ανθεκτικότητας*** της Ένωσης.

Τροπολογία 13

Πρόταση κανονισμού
Αιτιολογική σκέψη 16

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(16) Τα διασυνοριακά SOC θα πρέπει να λειτουργούν ως κεντρικό σημείο που επιτρέπει την ευρεία συγκέντρωση σχετικών δεδομένων και πληροφοριών για κυβερνοαπειλές, να καθιστούν δυνατή τη διάδοση πληροφοριών σχετικά με απειλές σε ένα ευρύ και ποικίλο σύνολο παραγόντων [π.χ. ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης σε υπολογιστές (στο εξής: CERT), CSIRT, κέντρα ανταλλαγής και ανάλυσης πληροφοριών (στο εξής: ISAC), φορείς εκμετάλλευσης κρίσιμων υποδομών]. Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε ένα διασυνοριακό SOC μπορούν να περιλαμβάνουν δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, ενδείξεις της παραβίασης και εντός πλαισίου πληροφορίες σχετικά με περιστατικά, απειλές και τρωτά σημεία. Επιπλέον, τα	(16) Τα διασυνοριακά SOC θα πρέπει να λειτουργούν ως κεντρικό σημείο που καθιστά δυνατή την ευρεία συγκέντρωση σχετικών δεδομένων και πληροφοριών για κυβερνοαπειλές, να διευκολύνουν τη διάδοση πληροφοριών σχετικά με απειλές σε ένα ευρύ και ποικίλο σύνολο παραγόντων [π.χ. ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης σε υπολογιστές (στο εξής: CERT), CSIRT, κέντρα ανταλλαγής και ανάλυσης πληροφοριών (στο εξής: ISAC), φορείς εκμετάλλευσης κρίσιμων υποδομών, ***καθώς και στην κοινότητα κυβερνοάμυνας]***. Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε ένα διασυνοριακό SOC μπορούν να περιλαμβάνουν δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, ενδείξεις της παραβίασης και εντός πλαισίου

διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC.

πληροφορίες σχετικά με περιστατικά, απειλές και τρωτά σημεία. Επιπλέον, τα διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC και ένα ***επιχειρησιακό δίκτυο (MICNET) για στρατιωτικές ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (milCERT), όταν δημιουργούνται***.

Τροπολογία 14

Πρόταση κανονισμού
Αιτιολογική σκέψη 17

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(17) Η κοινή αντίληψη της κατάστασης μεταξύ των αρμόδιων αρχών αποτελεί απαραίτητη προϋπόθεση για την ετοιμότητα και τον συντονισμό σε επίπεδο Ένωσης όσον αφορά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Η οδηγία (ΕΕ) 2022/2555 συστήνει το EU-CyCLONe για να στηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και να διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Η σύσταση (ΕΕ) 2017/1584 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο πραγματεύεται τον ρόλο όλων των σχετικών φορέων. Η οδηγία (ΕΕ) 2022/2555 υπενθυμίζει επίσης τις αρμοδιότητες της Επιτροπής στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης (στο εξής: ΜΠΠΕ) που θεσπίστηκε με την απόφαση 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και όσον αφορά την υποβολή αναλυτικών εκθέσεων για τις ρυθμίσεις για τον μηχανισμό	(17) Η κοινή αντίληψη της κατάστασης μεταξύ των αρμόδιων αρχών αποτελεί απαραίτητη προϋπόθεση για την ετοιμότητα και τον συντονισμό σε επίπεδο Ένωσης όσον αφορά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Η οδηγία (ΕΕ) 2022/2555 συστήνει το EU-CyCLONe για να στηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων στον τομέα της κυβερνοασφάλειας σε επιχειρησιακό επίπεδο και να διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Η σύσταση (ΕΕ) 2017/1584 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο πραγματεύεται τον ρόλο όλων των σχετικών φορέων. Η οδηγία (ΕΕ) 2022/2555 υπενθυμίζει επίσης τις αρμοδιότητες της Επιτροπής στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης (στο εξής: ΜΠΠΕ) που θεσπίστηκε με την απόφαση 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, καθώς και όσον αφορά την υποβολή αναλυτικών εκθέσεων για τις ρυθμίσεις για τον μηχανισμό

ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων της ΕΕ (στο εξής: IPCR) βάσει της εκτελεστικής απόφασης (ΕΕ) 2018/1993. Ως εκ τούτου, σε περιπτώσεις όπου τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, θα πρέπει να παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή. Ειδικότερα, ανάλογα με την κατάσταση, οι πληροφορίες που πρέπει να ανταλλάσσονται θα μπορούσαν να περιλαμβάνουν τεχνικές πληροφορίες, πληροφορίες σχετικά με τη φύση και τα κίνητρα του δράστη της επίθεσης ή του δυνητικού δράστη της επίθεσης, καθώς και μη τεχνικές πληροφορίες υψηλότερου επιπέδου σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνεται δεόντως υπόψη η αρχή της ανάγκης για γνώση και ο δυνητικά ευαίσθητος χαρακτήρας των πληροφοριών που ανταλλάσσονται.

ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων της ΕΕ (στο εξής: IPCR) βάσει της εκτελεστικής απόφασης (ΕΕ) 2018/1993. Ως εκ τούτου, σε περιπτώσεις όπου τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, θα πρέπει να παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT, ***στην κοινότητα κυβερνοάμυνας*** και στην Επιτροπή. Ειδικότερα, ανάλογα με την κατάσταση, οι πληροφορίες που πρέπει να ανταλλάσσονται θα μπορούσαν να περιλαμβάνουν τεχνικές πληροφορίες, πληροφορίες σχετικά με τη φύση και τα κίνητρα του δράστη της επίθεσης ή του δυνητικού δράστη της επίθεσης, καθώς και μη τεχνικές πληροφορίες υψηλότερου επιπέδου σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο αυτό, θα πρέπει να λαμβάνεται δεόντως υπόψη η αρχή της ανάγκης για γνώση και ο δυνητικά ευαίσθητος χαρακτήρας των πληροφοριών που ανταλλάσσονται.

Τροπολογία 15

Πρόταση κανονισμού
Αιτιολογική σκέψη 19

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(19) Προκειμένου να καταστεί δυνατή η ανταλλαγή δεδομένων σχετικά με απειλές κυβερνοασφάλειας από διάφορες πηγές, σε ευρεία κλίμακα και σε ένα αξιόπιστο περιβάλλον, οι οντότητες που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει να είναι εφοδιασμένες με προηγμένα και υψηλής ασφάλειας εργαλεία, εξοπλισμό και υποδομές. Με τον τρόπο αυτό θα καταστεί δυνατή η βελτίωση των συλλογικών ικανοτήτων ανίχνευσης και των έγκαιρων προειδοποιήσεων προς τις	(19) Προκειμένου να καταστεί δυνατή η ανταλλαγή δεδομένων σχετικά με απειλές κυβερνοασφάλειας από διάφορες πηγές, σε ευρεία κλίμακα και σε ένα αξιόπιστο περιβάλλον, οι οντότητες που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει να είναι εφοδιασμένες με προηγμένα και υψηλής ασφάλειας εργαλεία, εξοπλισμό και υποδομές, ***κάτι το οποίο αποκλείει τους υψηλού κινδύνου προμηθευτές κρίσιμων προϊόντων με ψηφιακά στοιχεία***. Με τον τρόπο αυτό θα καταστεί

αρχές και τις σχετικές οντότητες, ιδίως με τη χρήση των πλέον πρόσφατων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων.	δυνατή η βελτίωση των συλλογικών ικανοτήτων ανίχνευσης και των έγκαιρων προειδοποιήσεων προς τις αρχές και τις σχετικές οντότητες, ιδίως με τη χρήση των πλέον πρόσφατων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. ***Θα πρέπει να υπάρχει ανθρώπινη εποπτεία κατά τη χρήση της ΤΝ και να διασφαλίζεται επαρκές επίπεδο γραμματισμού σε θέματα ΤΝ, καθώς και η αναγκαία υποστήριξη και εξουσία για την άσκηση των σχετικών καθηκόντων***.

Τροπολογία 16

Πρόταση κανονισμού
Αιτιολογική σκέψη 19 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	(19α) Σύμφωνα με τον κανονισμό [XX/XXXX (πράξη για την ανθεκτικότητα στον κυβερνοχώρο)], οι οντότητες που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα θα πρέπει επίσης να καλύπτουν τις απαιτήσεις που ορίζονται στον παρόντα κανονισμό για όλα τα προϊόντα με ψηφιακά στοιχεία. Δεδομένων των αυξανόμενων κινδύνων που απορρέουν από τις οικονομικές εξαρτήσεις, είναι αναγκαίο να ελαχιστοποιηθεί η έκθεση σε υψηλού κινδύνου προμηθευτές κρίσιμων προϊόντων, μέσω ενός κοινού στρατηγικού πλαισίου για την οικονομική ασφάλεια της ΕΕ. Οι εξαρτήσεις από υψηλού κινδύνου προμηθευτές κρίσιμων προϊόντων με ψηφιακά στοιχεία ενέχουν στρατηγικό κίνδυνο που θα πρέπει να αντιμετωπιστεί σε επίπεδο Ένωσης, ιδίως εάν μια χώρα επιδίδεται σε οικονομική κατασκοπεία ή οικονομικό εξαναγκασμό και η νομοθεσία της καθιστά υποχρεωτική την αυθαίρετη πρόσβαση σε οποιοδήποτε είδος εταιρικών δραστηριοτήτων ή δεδομένων, ιδίως όταν τα κρίσιμα προϊόντα προορίζονται για χρήση από βασικές οντότητες που

	αναφέρονται στην οδηγία (ΕΕ) 2022/2555.

Τροπολογία 17

Πρόταση κανονισμού
Αιτιολογική σκέψη 20

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(20) Με τη συλλογή, την κοινοποίηση και την ανταλλαγή δεδομένων, η ευρωπαϊκή κυβερνοασπίδα θα πρέπει να ενισχύσει την τεχνολογική κυριαρχία της Ένωσης. Η συγκέντρωση επιμελημένων δεδομένων υψηλής ποιότητας θα πρέπει επίσης να συμβάλει στην ανάπτυξη προηγμένων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. Η εν λόγω συγκέντρωση θα πρέπει να διευκολυνθεί μέσω της σύνδεσης της ευρωπαϊκής κυβερνοασπίδας με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/1173 του Συμβουλίου[25].	(20) Με τη συλλογή, την κοινοποίηση και την ανταλλαγή δεδομένων, η ευρωπαϊκή κυβερνοασπίδα θα πρέπει να ενισχύσει την τεχνολογική κυριαρχία της Ένωσης***, τη στρατηγική αυτονομία, την ανταγωνιστικότητα και την ανθεκτικότητά της.*** Η συγκέντρωση επιμελημένων δεδομένων υψηλής ποιότητας θα πρέπει επίσης να συμβάλει στην ανάπτυξη προηγμένων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων. Η εν λόγω συγκέντρωση θα πρέπει να διευκολυνθεί μέσω της σύνδεσης της ευρωπαϊκής κυβερνοασπίδας με την πανευρωπαϊκή υποδομή υπολογιστικής υψηλών επιδόσεων που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/1173 του Συμβουλίου[25].
[25] Κανονισμός (ΕΕ) 2021/1173 του Συμβουλίου, της 13ης Ιουλίου 2021, σχετικά με τη σύσταση της κοινής επιχείρησης για την ευρωπαϊκή υπολογιστική υψηλών επιδόσεων και σχετικά με την κατάργηση του κανονισμού (ΕΕ) 2018/1488 (ΕΕ L 256 της 19.7.2021, σ. 3).	[25] Κανονισμός (ΕΕ) 2021/1173 του Συμβουλίου, της 13ης Ιουλίου 2021, σχετικά με τη σύσταση της κοινής επιχείρησης για την ευρωπαϊκή υπολογιστική υψηλών επιδόσεων και σχετικά με την κατάργηση του κανονισμού (ΕΕ) 2018/1488 (ΕΕ L 256 της 19.7.2021, σ. 3).

Τροπολογία 18

Πρόταση κανονισμού
Αιτιολογική σκέψη 25

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(25) Ο μηχανισμός έκτακτης ανάγκης	(25) Ο μηχανισμός έκτακτης ανάγκης

στον κυβερνοχώρο θα πρέπει να παρέχει στήριξη στα κράτη μέλη συμπληρώνοντας τα μέτρα και τους πόρους τους, καθώς και άλλες υφιστάμενες επιλογές στήριξης σε περίπτωση αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και άμεσης ανάκαμψης από αυτά, όπως οι υπηρεσίες που παρέχονται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA) στο πλαίσιο των αρμοδιοτήτων του, η συντονισμένη αντίδραση και συνδρομή από το δίκτυο CSIRT, η στήριξη μετριασμού από το EU-CyCLONe, καθώς και η αμοιβαία συνδρομή μεταξύ των κρατών μελών, μεταξύ άλλων στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ, οι ομάδες ταχείας αντίδρασης στον κυβερνοχώρο***[26]*** και οι υβριδικές ομάδες ταχείας αντίδρασης της μόνιμης διαρθρωμένης συνεργασίας (PESCO). Θα πρέπει να αντιμετωπίσει την ανάγκη να διασφαλιστεί η διαθεσιμότητα εξειδικευμένων μέσων για τη στήριξη της ετοιμότητας και της αντιμετώπισης περιστατικών κυβερνοασφάλειας σε ολόκληρη την Ένωση και σε τρίτες χώρες.

στον κυβερνοχώρο θα πρέπει να παρέχει στήριξη στα κράτη μέλη συμπληρώνοντας τα μέτρα και τους πόρους τους, καθώς και άλλες υφιστάμενες επιλογές στήριξης σε περίπτωση αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και άμεσης ανάκαμψης από αυτά, όπως οι υπηρεσίες που παρέχονται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ENISA) στο πλαίσιο των αρμοδιοτήτων του, η συντονισμένη αντίδραση και συνδρομή από το δίκτυο CSIRT, η στήριξη μετριασμού από το EU-CyCLONe, καθώς και η αμοιβαία συνδρομή μεταξύ των κρατών μελών, μεταξύ άλλων στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ, οι ομάδες ταχείας αντίδρασης στον κυβερνοχώρο***[1], το νέο συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών (CIDCC) που αποτελεί έργο της PESCO και το κέντρο συντονισμού της ΕΕ για την κυβερνοάμυνα (EUCDCC) που αποτελεί τον προταθέντα διάδοχό του,*** και οι υβριδικές ομάδες ταχείας αντίδρασης της μόνιμης διαρθρωμένης συνεργασίας (PESCO). Θα πρέπει να καλύψει την ανάγκη να διασφαλιστεί η διαθεσιμότητα εξειδικευμένων μέσων για τη στήριξη της ετοιμότητας και της αντιμετώπισης περιστατικών κυβερνοασφάλειας σε ολόκληρη την Ένωση και σε τρίτες χώρες***, ιδίως στις υποψήφιες προς ένταξη στην ΕΕ χώρες που ευθυγραμμίζονται με την κοινή εξωτερική πολιτική και πολιτική ασφαλείας και την κοινή πολιτική ασφάλειας και άμυνας, παρέχοντάς τους στήριξη για την ανάπτυξη των ικανοτήτων τους στον κυβερνοχώρο και ενισχύοντας τη διασυνοριακή και περιφερειακή συνεργασία μεταξύ των εν λόγω υποψήφιων χωρών στον τομέα του κυβερνοχώρου.***

[1] Απόφαση (ΚΕΠΠΑ) 2017/2315 του Συμβουλίου, της 11ης Δεκεμβρίου 2017, για τη θεσμοθέτηση μόνιμης

	διαρθρωμένης συνεργασίας (PESCO) και την κατάρτιση του καταλόγου των συμμετεχόντων κρατών μελών.
[26] Απόφαση (ΚΕΠΠΑ) 2017/2315 του Συμβουλίου, της 11ης Δεκεμβρίου 2017, για τη θεσμοθέτηση μόνιμης διαρθρωμένης συνεργασίας (PESCO) και την κατάρτιση του καταλόγου των συμμετεχόντων κρατών μελών.	[26] Απόφαση (ΚΕΠΠΑ) 2017/2315 του Συμβουλίου, της 11ης Δεκεμβρίου 2017, για τη θεσμοθέτηση μόνιμης διαρθρωμένης συνεργασίας (PESCO) και την κατάρτιση του καταλόγου των συμμετεχόντων κρατών μελών.

Τροπολογία 19

Πρόταση κανονισμού
Αιτιολογική σκέψη 26

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(26) Το παρόν μέσο δεν θίγει τις διαδικασίες και τα πλαίσια για τον συντονισμό της αντιμετώπισης κρίσεων σε επίπεδο Ένωσης, ιδίως τον ΜΠΠΕ[27], τον IPCR[28], και την οδηγία (ΕΕ) 2022/2555. Μπορεί να συμβάλλει ή να συμπληρώνει δράσεις που υλοποιούνται στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ ή σε καταστάσεις που ορίζονται στο άρθρο 222 ΣΛΕΕ. Η χρήση του εν λόγω μέσου θα πρέπει επίσης να συντονίζεται με την εφαρμογή των μέτρων της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο, ***κατά περίπτωση***.	(26) Το παρόν μέσο δεν θίγει τις διαδικασίες και τα πλαίσια για τον συντονισμό της αντιμετώπισης κρίσεων σε επίπεδο Ένωσης, ιδίως τον ΜΠΠΕ[27], τον IPCR[28], και την οδηγία (ΕΕ) 2022/2555. Μπορεί να συμβάλλει ή να συμπληρώνει δράσεις που υλοποιούνται στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ ή σε καταστάσεις που ορίζονται στο άρθρο 222 ΣΛΕΕ. Η χρήση του εν λόγω μέσου θα πρέπει επίσης να συντονίζεται με την εφαρμογή των μέτρων της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο, ***ενισχύοντας τη συνεργασία σε στρατηγικό, επιχειρησιακό και τεχνικό επίπεδο μεταξύ της κυβερνοάμυνας και άλλων κοινοτήτων στον κυβερνοχώρο, ιδίως προκειμένου να ενισχυθούν οι ικανότητες κατά των απειλών της κυβερνοασφάλειας από χώρες εκτός της Ένωσης, συμπεριλαμβανομένων περιοριστικών μέτρων, που μπορούν να χρησιμοποιηθούν για την πρόληψη και την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο***.
[27] Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του	[27] Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του

Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

[28] Ρυθμίσεις ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων (IPCR) και σύμφωνα με τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση μεγάλης κλίμακας περιστατικών και κρίσεων στον κυβερνοχώρο.

Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης (ΕΕ L 347 της 20.12.2013, σ. 924).

[28] Ρυθμίσεις ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων (IPCR) και σύμφωνα με τη σύσταση (ΕΕ) 2017/1584 της Επιτροπής, της 13ης Σεπτεμβρίου 2017, για τη συντονισμένη αντιμετώπιση μεγάλης κλίμακας περιστατικών και κρίσεων στον κυβερνοχώρο.

Τροπολογία 20

Πρόταση κανονισμού
Αιτιολογική σκέψη 28

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(28) Η οδηγία (ΕΕ) 2022/2555 απαιτεί από τα κράτη μέλη να ορίσουν ή να συστήσουν μία ή περισσότερες αρχές διαχείρισης κυβερνοκρίσεων και να διασφαλίσουν ότι διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντά τους. Απαιτεί επίσης από τα κράτη μέλη να προσδιορίζουν τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν στην περίπτωση κρίσης καθώς και να θεσπίζουν εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας. Τα κράτη μέλη υποχρεούνται επίσης να συστήσουν μία ή περισσότερες CSIRT που είναι υπεύθυνες για τον χειρισμό περιστατικών σύμφωνα με σαφώς καθορισμένη διαδικασία και να καλύπτουν τουλάχιστον τους τομείς, υποτομείς και τύπους οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας, και να διασφαλίζουν ότι	(28) Η οδηγία (ΕΕ) 2022/2555 απαιτεί από τα κράτη μέλη να ορίσουν ή να συστήσουν μία ή περισσότερες αρχές διαχείρισης κυβερνοκρίσεων και να διασφαλίσουν ότι διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά και αποδοτικά τα καθήκοντά τους. Απαιτεί επίσης από τα κράτη μέλη να προσδιορίζουν τις ικανότητες, τα πάγια στοιχεία και τις διαδικασίες που μπορούν να χρησιμοποιηθούν στην περίπτωση κρίσης καθώς και να θεσπίζουν εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, στο οποίο καθορίζονται οι στόχοι και οι ρυθμίσεις για τη διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον τομέα της κυβερνοασφάλειας. Τα κράτη μέλη υποχρεούνται επίσης να συστήσουν μία ή περισσότερες CSIRT που είναι υπεύθυνες για τον χειρισμό περιστατικών σύμφωνα με σαφώς καθορισμένη διαδικασία και να καλύπτουν τουλάχιστον τους τομείς, υποτομείς και τύπους οντοτήτων που εμπίπτουν στο πεδίο εφαρμογής της εν λόγω οδηγίας, και να διασφαλίζουν ότι

διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά τα καθήκοντά τους. Ο παρών κανονισμός δεν θίγει τον ρόλο της Επιτροπής όσον αφορά τη διασφάλιση της συμμόρφωσης των κρατών μελών προς τις υποχρεώσεις που απορρέουν από την οδηγία (ΕΕ) 2022/2555. Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει βοήθεια για δράσεις που αποσκοπούν στην ενίσχυση της ετοιμότητας, καθώς και για δράσεις αντιμετώπισης περιστατικών με σκοπό τον μετριασμό των επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, τη στήριξη της άμεσης ανάκαμψης και/ή την αποκατάσταση της λειτουργίας βασικών υπηρεσιών.

διαθέτουν επαρκείς πόρους για να επιτελούν αποτελεσματικά τα καθήκοντά τους. Ο παρών κανονισμός δεν θίγει τον ρόλο της Επιτροπής όσον αφορά τη διασφάλιση της συμμόρφωσης των κρατών μελών προς τις υποχρεώσεις που απορρέουν από την οδηγία (ΕΕ) 2022/2555. Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να παρέχει βοήθεια για δράσεις που αποσκοπούν στην ενίσχυση της ετοιμότητας, καθώς και για δράσεις αντιμετώπισης περιστατικών με σκοπό τον μετριασμό των επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, τη στήριξη της άμεσης ανάκαμψης και/ή την αποκατάσταση της λειτουργίας βασικών υπηρεσιών***, κάνοντας κατάλληλη χρήση ολόκληρου του εύρους των αμυντικών επιλογών που διαθέτουν οι μη στρατιωτικές και στρατιωτικές κοινότητες***.

Τροπολογία 21

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	(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 Ι 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 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.

οποίοι θα πρέπει να είναι επιλέξιμοι για χρηματοδοτική στήριξη για συντονισμένες δοκιμές σε επίπεδο Ένωσης. ***Κατά περίπτωση, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ), ιδίως μέσω του Κέντρου Πληροφοριών της ΕΕ (INTCEN) και της Μονάδας Ανάλυσης Υβριδικών Απειλών, με την υποστήριξη της Διεύθυνσης Πληροφοριών του Στρατιωτικού Επιτελείου της Ευρωπαϊκής Ένωσης (EUMS) στο πλαίσιο της Ενιαίας Δυνατότητας Ανάλυσης Πληροφοριών (SIAC), θα πρέπει επίσης να συμμετέχει στην παροχή επικαιροποιημένων αξιολογήσεων και, ως εκ τούτου, να συμβάλλει στον προσδιορισμό των*** τομέων ή υποτομέων ***που*** θα πρέπει να επιλέγονται από το παράρτημα Ι της οδηγίας (ΕΕ) 2022/2555 (στο εξής: τομείς υψηλής κρισιμότητας). Οι συντονισμένες δοκιμές θα πρέπει να βασίζονται σε κοινά σενάρια και μεθοδολογίες κινδύνου. ***Οι ασκήσεις αυτές θα πρέπει επίσης να διαδραματίσουν σημαντικό ρόλο στη βελτίωση της συνεργασίας μεταξύ μη στρατιωτικών και στρατιωτικών οντοτήτων. Για τον λόγο αυτόν, κατά τη διοργάνωση των ασκήσεων, η Επιτροπή, η ΕΥΕΔ και ο ENISA θα πρέπει να εξετάζουν συστηματικά το ενδεχόμενο να συμπεριλαμβάνουν συμμετέχοντες από άλλες κοινότητες κυβερνοάμυνας, όπως ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ) και άλλες συναφείς οντότητες.*** 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 δικτύου 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***[1]***. 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.

[1] 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.

---

[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.

---

[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 22

Πρόταση κανονισμού
Αιτιολογική σκέψη 32

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(32) Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να στηρίζει τη βοήθεια που παρέχεται από τα κράτη μέλη σε κράτος μέλος που επηρεάζεται από σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων από το δίκτυο CSIRT που ορίζεται στο άρθρο 15 της οδηγίας (ΕΕ) 2022/2555. Τα κράτη μέλη που παρέχουν συνδρομή θα πρέπει να έχουν τη δυνατότητα να υποβάλλουν αιτήσεις για την κάλυψη των δαπανών που σχετίζονται με την αποστολή ομάδων εμπειρογνωμόνων στο πλαίσιο της αμοιβαίας συνδρομής. Οι επιλέξιμες δαπάνες μπορούν να περιλαμβάνουν έξοδα ταξιδίου, διαμονής και ημερήσιας αποζημίωσης των εμπειρογνωμόνων κυβερνοασφάλειας.	(32) Ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο θα πρέπει να στηρίζει τη βοήθεια που παρέχεται από τα κράτη μέλη σε κράτος μέλος που επηρεάζεται από σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων από το δίκτυο CSIRT που ορίζεται στο άρθρο 15 της οδηγίας (ΕΕ) 2022/2555. Τα κράτη μέλη που παρέχουν συνδρομή θα πρέπει να έχουν τη δυνατότητα να υποβάλλουν αιτήσεις για την κάλυψη των δαπανών που σχετίζονται με την αποστολή ομάδων εμπειρογνωμόνων στο πλαίσιο της αμοιβαίας συνδρομής***, διασφαλίζοντας τον αποτελεσματικό συντονισμό μεταξύ των σχετικών προγραμμάτων και μέσων της ΕΕ, συμπεριλαμβανομένων του Ευρωπαϊκού Μηχανισμού για την Ειρήνη (ΕΜΕ), της ΚΕΠΠΑ και του Μηχανισμού Γειτονίας, Ανάπτυξης και Διεθνούς Συνεργασίας, κατά την παροχή βοήθειας σε τρίτες χώρες, ιδίως στην Ουκρανία και τη Μολδαβία.*** Οι επιλέξιμες δαπάνες μπορούν να περιλαμβάνουν έξοδα ταξιδίου, διαμονής και ημερήσιας αποζημίωσης των εμπειρογνωμόνων κυβερνοασφάλειας.

Τροπολογία 23

Πρόταση κανονισμού
Αιτιολογική σκέψη 33

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(33) Θα πρέπει σταδιακά να δημιουργηθεί εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης, η οποία θα αποτελείται από υπηρεσίες από ιδιωτικούς παρόχους διαχειριζόμενων	(33) Θα πρέπει σταδιακά να δημιουργηθεί εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης, η οποία θα αποτελείται από υπηρεσίες από ιδιωτικούς παρόχους διαχειριζόμενων

υπηρεσιών ασφάλειας για την υποστήριξη δράσεων αντιμετώπισης και άμεσης ανάκαμψης σε περιπτώσεις σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να διασφαλίζει τη διαθεσιμότητα και την ετοιμότητα των υπηρεσιών. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται για τη στήριξη των εθνικών αρχών όσον αφορά την παροχή βοήθειας σε επηρεαζόμενες οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, συμπληρωματικά προς τις δικές τους δράσεις σε εθνικό επίπεδο. Όταν ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη θα πρέπει να προσδιορίζουν τη στήριξη που παρέχεται στην πληγείσα οντότητα σε εθνικό επίπεδο, η οποία θα πρέπει να λαμβάνεται υπόψη κατά την αξιολόγηση του αιτήματος του κράτους μέλους. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας μπορούν επίσης να χρησιμεύσουν για τη στήριξη των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, υπό παρόμοιες συνθήκες.	υπηρεσιών ασφάλειας για την υποστήριξη δράσεων αντιμετώπισης και άμεσης ανάκαμψης σε περιπτώσεις σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να διασφαλίζει τη διαθεσιμότητα και την ετοιμότητα των υπηρεσιών. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να χρησιμοποιούνται για τη στήριξη των εθνικών αρχών όσον αφορά την παροχή βοήθειας σε επηρεαζόμενες οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, συμπληρωματικά προς τις δικές τους δράσεις σε εθνικό επίπεδο. Όταν ζητούν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, τα κράτη μέλη θα πρέπει να προσδιορίζουν τη στήριξη που παρέχεται στην πληγείσα οντότητα σε εθνικό επίπεδο, η οποία θα πρέπει να λαμβάνεται υπόψη κατά την αξιολόγηση του αιτήματος του κράτους μέλους. Οι υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας μπορούν επίσης να χρησιμεύσουν για τη στήριξη των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, ***συμπεριλαμβανομένων των αποστολών ΚΠΑΑ***, υπό παρόμοιες συνθήκες.

Τροπολογία 24

Πρόταση κανονισμού
Αιτιολογική σκέψη 34

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(34) Για τους σκοπούς της επιλογής ιδιωτικών παρόχων υπηρεσιών για την παροχή υπηρεσιών στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, είναι αναγκαίο να θεσπιστεί ένα σύνολο ελάχιστων κριτηρίων που θα πρέπει να περιλαμβάνονται στην πρόσκληση υποβολής προσφορών για την επιλογή των εν λόγω παρόχων, ώστε να	(34) Για τους σκοπούς της επιλογής ιδιωτικών παρόχων υπηρεσιών για την παροχή υπηρεσιών στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, είναι αναγκαίο να θεσπιστεί ένα σύνολο ελάχιστων κριτηρίων που θα πρέπει να περιλαμβάνονται στην πρόσκληση υποβολής προσφορών για την επιλογή των εν λόγω παρόχων, ώστε να

διασφαλίζεται η κάλυψη των αναγκών των αρχών και των οντοτήτων των κρατών μελών που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας.

διασφαλίζεται η κάλυψη των αναγκών των αρχών και των οντοτήτων των κρατών μελών που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας***, λαμβανομένων επίσης υπόψη των κινδύνων που σχετίζονται με τη συμμετοχή των παρόχων από στρατηγικές ανταγωνιστικές χώρες, οι οποίοι ενδέχεται να συνεπάγονται κινδύνους οικονομικής ασφάλειας, καθώς και επιπτώσεις για τη στρατηγική ασφάλεια της Ένωσης***.

Τροπολογία 25

Πρόταση κανονισμού
Αιτιολογική σκέψη 36

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(36) Προκειμένου να υποστηριχθούν οι στόχοι του παρόντος κανονισμού για την προώθηση της κοινής αντίληψης της κατάστασης, την ενίσχυση της ανθεκτικότητας της Ένωσης και τη διευκόλυνση της αποτελεσματικής αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, το EU-CyCLONe, το δίκτυο CSIRT ή η Επιτροπή θα πρέπει να είναι σε θέση να ζητούν από τον ENISA να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA θα πρέπει να συντάσσει έκθεση εξέτασης περιστατικού, σε συνεργασία με τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων του ιδιωτικού τομέα, των κρατών μελών, της Επιτροπής και άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. Όσον αφορά τον ιδιωτικό τομέα, ο ENISA αναπτύσσει διαύλους ανταλλαγής πληροφοριών με εξειδικευμένους παρόχους, συμπεριλαμβανομένων	(36) Προκειμένου να υποστηριχθούν οι στόχοι του παρόντος κανονισμού για την προώθηση της κοινής αντίληψης της κατάστασης, την ενίσχυση της ανθεκτικότητας της Ένωσης και τη διευκόλυνση της αποτελεσματικής αντιμετώπισης σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, το EU-CyCLONe, το δίκτυο CSIRT ή η Επιτροπή θα πρέπει να είναι σε θέση να ζητούν από τον ENISA να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας. ***Ενόψει της ανάπτυξης ενός ασφαλούς συστήματος συνδεσιμότητας, με βάση την ευρωπαϊκή υποδομή κβαντικής επικοινωνίας (EuroQCI) και τις κυβερνητικές δορυφορικές επικοινωνίες της Ευρωπαϊκής Ένωσης (GOVSATCOM), ιδίως την υλοποίηση του συστήματος GNSS Galileo για χρήστες του αμυντικού τομέα, οποιαδήποτε μελλοντική πιθανή ανάπτυξη θα πρέπει να λαμβάνει υπόψη την έλευση του «υπερπολέμου» που συγχωνεύει την ταχύτητα και την***

παρόχων διαχειριζόμενων λύσεων ασφάλειας και εταιρειών, προκειμένου να συμβάλει στην αποστολή του ENISA για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση. Με βάση τη συνεργασία με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένου του ιδιωτικού τομέα, η έκθεση εξέτασης συγκεκριμένων περιστατικών θα πρέπει να αποσκοπεί στην αξιολόγηση των αιτίων, των επιπτώσεων και των μέτρων μετριασμού ενός περιστατικού, μετά την επέλευση του. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις πληροφορίες και τα διδάγματα που ανταλλάσσουν οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας που πληρούν τις προϋποθέσεις της ύψιστης επαγγελματικής ακεραιότητας, αμεροληψίας και της απαιτούμενης τεχνικής εμπειρογνωσίας, όπως απαιτείται από τον παρόντα κανονισμό. Η έκθεση θα πρέπει να υποβάλλεται και να αξιοποιείται στο πλαίσιο των εργασιών του EU-CyCLONe, του δικτύου CSIRT και της Επιτροπής. Όταν το περιστατικό αφορά τρίτη χώρα, θα πρέπει να κοινοποιείται από την Επιτροπή στον/στην ύπατο/-η εκπρόσωπο.

εξειδίκευση της κβαντικής υπολογιστικής με ιδιαίτερα αυτόνομα στρατιωτικά συστήματα. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA θα πρέπει να συντάσσει έκθεση εξέτασης περιστατικού, σε συνεργασία με τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων του ιδιωτικού τομέα, των κρατών μελών, της Επιτροπής και άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. Όσον αφορά τον ιδιωτικό τομέα, ο ENISA αναπτύσσει διαύλους ανταλλαγής πληροφοριών με εξειδικευμένους παρόχους, συμπεριλαμβανομένων παρόχων διαχειριζόμενων λύσεων ασφάλειας και εταιρειών, προκειμένου να συμβάλει στην αποστολή του ENISA για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση. Με βάση τη συνεργασία με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένου του ιδιωτικού τομέα, η έκθεση εξέτασης συγκεκριμένων περιστατικών θα πρέπει να αποσκοπεί στην αξιολόγηση των αιτίων, των επιπτώσεων και των μέτρων μετριασμού ενός περιστατικού, μετά την επέλευση του. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις πληροφορίες και τα διδάγματα που ανταλλάσσουν οι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας που πληρούν τις προϋποθέσεις της ύψιστης επαγγελματικής ακεραιότητας, αμεροληψίας και της απαιτούμενης τεχνικής εμπειρογνωσίας, όπως απαιτείται από τον παρόντα κανονισμό. Η έκθεση θα πρέπει να υποβάλλεται και να αξιοποιείται στο πλαίσιο των εργασιών του EU-CyCLONe, του δικτύου CSIRT και της Επιτροπής. Όταν το περιστατικό αφορά τρίτη χώρα, θα πρέπει να κοινοποιείται από την Επιτροπή στον/στην ύπατο/-η εκπρόσωπο***, την ΕΥΕΔ και οποιαδήποτε αποστολή ΚΠΑΑ στη χώρα που επηρεάζεται από το συμβάν μέσω των αρχηγείων τους***.

Τροπολογία 26

Πρόταση κανονισμού
Αιτιολογική σκέψη 37

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
(37) Λαμβάνοντας υπόψη την απρόβλεπτη φύση των κυβερνοεπιθέσεων και το γεγονός ότι συχνά δεν περιορίζονται σε συγκεκριμένη γεωγραφική περιοχή και ενέχουν υψηλό κίνδυνο δευτερογενών επιπτώσεων, η ενίσχυση της ανθεκτικότητας των γειτονικών χωρών και της ικανότητάς τους να αντιμετωπίζουν αποτελεσματικά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας συμβάλλει στην προστασία της Ένωσης στο σύνολό της. Ως εκ τούτου, οι τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη» ***μπορούν*** να λαμβάνουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας***, εφόσον αυτό προβλέπεται στην αντίστοιχη συμφωνία σύνδεσης με το πρόγραμμα «Ψηφιακή Ευρώπη»***. Η χρηματοδότηση συνδεδεμένων τρίτων χωρών θα πρέπει να στηρίζεται από την Ένωση στο πλαίσιο σχετικών εταιρικών σχέσεων και χρηματοδοτικών μέσων για τις εν λόγω χώρες. Η στήριξη θα πρέπει να καλύπτει υπηρεσίες στον τομέα της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Οι προϋποθέσεις που καθορίζονται στον παρόντα κανονισμό για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και για τους αξιόπιστους παρόχους θα πρέπει να εφαρμόζονται κατά την παροχή στήριξης στις τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη».	(37) Λαμβάνοντας υπόψη την απρόβλεπτη φύση των κυβερνοεπιθέσεων και το γεγονός ότι συχνά δεν περιορίζονται σε συγκεκριμένη γεωγραφική περιοχή και ενέχουν υψηλό κίνδυνο δευτερογενών επιπτώσεων, η ενίσχυση της ανθεκτικότητας των γειτονικών χωρών***, ιδίως της Ουκρανίας και της Μολδαβίας,*** και της ικανότητάς τους να αντιμετωπίζουν αποτελεσματικά σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας συμβάλλει στην προστασία της Ένωσης στο σύνολό της. Ως εκ τούτου, οι τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη» ***θα πρέπει*** να λάβουν στήριξη από την εφεδρεία κυβερνοασφάλειας της ΕΕ στον τομέα της κυβερνοασφάλειας***. Η στήριξη θα πρέπει επίσης να εφαρμόζεται στις τρίτες χώρες*** στις οποίες ***αναπτύσσεται αποστολή ΚΠΑΑ με ειδική εντολή για την ενίσχυση της ανθεκτικότητας σε υβριδικές απειλές, συμπεριλαμβανομένου του κυβερνοχώρου, ή στις οποίες έχει εγκριθεί μέτρο συνδρομής του ΕΜΕ για την ενίσχυση της κυβερνοανθεκτικότητας της χώρας***. Η χρηματοδότηση συνδεδεμένων τρίτων χωρών θα πρέπει να στηρίζεται από την Ένωση στο πλαίσιο σχετικών εταιρικών σχέσεων και χρηματοδοτικών μέσων για τις εν λόγω χώρες. Η στήριξη θα πρέπει να καλύπτει υπηρεσίες στον τομέα της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Οι προϋποθέσεις που καθορίζονται στον παρόντα κανονισμό για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας και για τους αξιόπιστους παρόχους θα πρέπει να εφαρμόζονται κατά την παροχή στήριξης

στις τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη».

Τροπολογία 27

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 1 – στοιχείο γ

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
γ) θέσπιση ενός ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών.	γ) θέσπιση ενός ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας για την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών ***ή απειλών***.

Τροπολογία 28

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 και των υπηρεσιών στην Ένωση σε ολόκληρη την ψηφιακή οικονομία και συμβολής στην τεχνολογική ***ανθεκτικότητα*** της Ένωσης στον τομέα της κυβερνοασφάλειας,

Τροπολογία 29

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	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 στήριξης για την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη»,	αλληλεγγύης με την ανάπτυξη κοινών ικανοτήτων αντιμετώπισης σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με την εξασφάλιση ενωσιακής στήριξης για την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε τρίτες χώρες που είναι συνδεδεμένες με το πρόγραμμα «Ψηφιακή Ευρώπη» ***ή στις τρίτες χώρες που είναι υποψήφιες για προσχώρηση στην Ένωση και δεν ενεργούν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως αυτά ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον Τίτλο V της ΣΕΕ· τα κράτη μέλη θα πρέπει να εξετάσουν το ενδεχόμενο να συμπεριλάβουν στην εθνική στρατηγική τους για την κυβερνοασφάλεια ένα ενεργό πρόγραμμα κυβερνοάμυνας, το οποίο θα περιλαμβάνει τακτικές κοινές εκπαιδευτικές ασκήσεις μεταξύ κρατών μελών και διεθνών οργανισμών. Ένα τέτοιο πρόγραμμα θα πρέπει να παρέχει συγχρονισμένη, σε πραγματικό χρόνο ικανότητα εντοπισμού, ανίχνευσης, ανάλυσης και μετριασμού των απειλών,***

Τροπολογία 30

Πρόταση κανονισμού
Άρθρο 1 – παράγραφος 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	2α. τη μείωση των συστημικών κινδύνων κυβερνοασφάλειας που ενέχουν οι εξαρτήσεις από κρίσιμο εξοπλισμό από χώρες που θα ενεργούσαν αντίθετα προς στα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον τίτλο V της ΣΕΕ,

Τροπολογία 31

Πρόταση κανονισμού
Άρθρο 2 – παράγραφος 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	«κοινότητα κυβερνοάμυνας»: οι αμυντικές αρχές των κρατών μελών που υποστηρίζονται από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ, όπως ορίζεται στην κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα[1]
	[1] Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Πολιτική της ΕΕ για την κυβερνοάμυνα» [JOIN(2022) 49 final].

Τροπολογία 32

Πρόταση κανονισμού
Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο β α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	β α) συμβάλλει στον εκσυγχρονισμό του συνόλου των συστημάτων κυβερνοάμυνας, αυξάνοντας την ποιότητα των ικανοτήτων κυβερνοάμυνας μέσω της ανάπτυξης συστημάτων ΤΝ, και στην επιτάχυνση της ανταλλαγής πληροφοριών μεταξύ των εθνικών SOC και των διασυνοριακών SOC,

Τροπολογία 33

Πρόταση κανονισμού
Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο δ α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	δ α) επανεξετάζει και αξιολογεί κρίσιμες τεχνολογίες και εξοπλισμό κυβερνοασφάλειας που χρησιμοποιούν τα

	SOC για την αντιμετώπιση περιστατικών κυβερνοασφάλειας για συστημικούς κινδύνους που απορρέουν από τον έλεγχο παρόχων υψηλού κινδύνου από χώρες που θα ενεργούσαν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον τίτλο V της ΣΕΕ,

Τροπολογία 34

Πρόταση κανονισμού
Άρθρο 4 – παράγραφος 1 – εδάφιο 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
Έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας και για τη συμβολή σε διασυνοριακό SOC. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.	Έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς ***και, όταν είναι απαραίτητο, στρατιωτικούς,*** οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας και για τη συμβολή σε διασυνοριακό SOC. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.

Τροπολογία 35

Πρόταση κανονισμού
Άρθρο 4 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, τα εθνικά SOC επιλέγονται από το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC) για να συμμετάσχουν σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί επιχορηγήσεις στα επιλεγμένα εθνικά SOC για τη	2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, τα εθνικά SOC επιλέγονται από το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC) για να συμμετάσχουν σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί επιχορηγήσεις στα επιλεγμένα εθνικά SOC για τη

χρηματοδότηση της λειτουργίας των εν λόγω εργαλείων και υποδομών. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 50 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από το κράτος μέλος. Πριν από την έναρξη της διαδικασίας για την αγορά των εργαλείων και των υποδομών, το ECCC και το εθνικό SOC συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των υποδομών.	χρηματοδότηση της λειτουργίας των εν λόγω εργαλείων και υποδομών***, αυστηρά υπό τον όρο ότι τα εν λόγω εργαλεία και υποδομές παρέχονται από αξιόπιστους παρόχους σύμφωνα με το άρθρο 16***. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 50 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από το κράτος μέλος. Πριν από την έναρξη της διαδικασίας για την αγορά των εργαλείων και των υποδομών, το ECCC και το εθνικό SOC συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των υποδομών.

Τροπολογία 36

Πρόταση κανονισμού
Άρθρο 5 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, η κοινοπραξία υποδοχής επιλέγεται από το ECCC για να συμμετάσχει σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί στην κοινοπραξία υποδοχής επιχορήγηση για τη χρηματοδότηση της λειτουργίας των εργαλείων και των υποδομών. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 75 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από την κοινοπραξία υποδοχής. Πριν από την έναρξη της διαδικασίας αγοράς των εργαλείων και των υποδομών, το ECCC και η κοινοπραξία υποδοχής συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των υποδομών.	2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, η κοινοπραξία υποδοχής επιλέγεται από το ECCC για να συμμετάσχει σε κοινή διαδικασία προμήθειας εργαλείων και υποδομών με το ECCC. Το ECCC μπορεί να χορηγεί στην κοινοπραξία υποδοχής επιχορήγηση για τη χρηματοδότηση της λειτουργίας των εργαλείων των και υποδομών***, αυστηρά υπό τον όρο ότι τα εν λόγω εργαλεία και υποδομές παρέχονται από αξιόπιστους παρόχους σύμφωνα με το άρθρο 16***. Η χρηματοδοτική συνεισφορά της Ένωσης καλύπτει έως και το 75 % του κόστους αγοράς των εργαλείων και των υποδομών και έως το 50 % του κόστους λειτουργίας, ενώ το υπόλοιπο κόστος καλύπτεται από την κοινοπραξία υποδοχής. Πριν από την έναρξη της διαδικασίας αγοράς των εργαλείων και των υποδομών, το ECCC και η κοινοπραξία υποδοχής συνάπτουν συμφωνία υποδοχής και χρήσης που ρυθμίζει τη χρήση των εργαλείων και των

υποδομών.

Τροπολογία 37

Πρόταση κανονισμού
Άρθρο 5 – παράγραφος 2 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	2α. Κάθε υποδομή ή πάροχος που προέρχεται από τρίτη χώρα υψηλού κινδύνου αποκλείεται αυτομάτως.

Τροπολογία 38

Πρόταση κανονισμού
Άρθρο 6 – παράγραφος 1 – στοιχείο β α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	β α) υποστηρίζει άμεσα την ενίσχυση των στρατιωτικών και αμυντικών ικανοτήτων των συμμετεχόντων μελών ή αποτρέπει τυχόν άμεση και επικείμενη απειλή για την ασφάλειά τους. Δεδομένου ότι η εκμετάλλευση των τρωτών σημείων στον τομέα της άμυνας μπορεί να προκαλέσει σημαντικές διαταραχές και ζημίες, η κυβερνοασφάλεια της αμυντικής βιομηχανίας απαιτεί ειδικά μέτρα για την κατοχύρωση της ασφάλειας των αλυσίδων εφοδιασμού, ιδίως για τις οντότητες που βρίσκονται χαμηλότερα στις αλυσίδες εφοδιασμού, οι οποίες δεν χρειάζονται πρόσβαση σε διαβαθμισμένες πληροφορίες, αλλά θα μπορούσαν να θέσουν σε σοβαρό κίνδυνο ολόκληρο τον τομέα. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις επιπτώσεις πιθανής παραβίασης και στον κίνδυνο που προκύπτει από οποιαδήποτε πιθανή παραποίηση δεδομένων δικτύου, η οποία θα μπορούσε να αχρηστεύσει κρίσιμους αμυντικούς μηχανισμούς ή ακόμη και να εξουδετερώσει τα λειτουργικά τους συστήματα, καθιστώντας τα ευάλωτα

στην πειρατεία.

Τροπολογία 39

Πρόταση κανονισμού
Άρθρο 6 – παράγραφος 1 – στοιχείο β β (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	β β) υποστηρίζει την ενίσχυση των αμυντικών ικανοτήτων των συμμετεχόντων μελών ή αποτρέπει τυχόν άμεση και επικείμενη απειλή για την ασφάλειά τους, κατοχυρώνοντας την ασφάλεια των αλυσίδων εφοδιασμού, ιδίως για τις οντότητες που βρίσκονται χαμηλότερα στις αλυσίδες εφοδιασμού, οι οποίες δεν χρειάζονται πρόσβαση σε διαβαθμισμένες πληροφορίες, αλλά θα μπορούσαν να θέσουν σε σοβαρό κίνδυνο ολόκληρο τον τομέα.

Τροπολογία 40

Πρόταση κανονισμού
Άρθρο 7 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
1. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.	1. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, ***συμπεριλαμβανομένου του/της ύπατου/-ης εκπροσώπου και της ΕΥΕΔ όταν αφορά τρίτη χώρα,*** λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

Τροπολογία 41

Πρόταση κανονισμού
Άρθρο 8 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
1. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν υψηλό επίπεδο ασφάλειας των δεδομένων και υλικής ασφάλειας της υποδομής της ευρωπαϊκής κυβερνοασπίδας και μεριμνούν για την κατάλληλη διαχείριση και έλεγχο της υποδομής ώστε να προστατεύεται από απειλές και να διασφαλίζεται η ασφάλειά της και η ασφάλεια των συστημάτων, συμπεριλαμβανομένης της ασφάλειας των δεδομένων που ανταλλάσσονται μέσω της υποδομής.	1. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν υψηλό επίπεδο ασφάλειας των δεδομένων και υλικής ασφάλειας της υποδομής της ευρωπαϊκής κυβερνοασπίδας και μεριμνούν για την κατάλληλη διαχείριση και έλεγχο της υποδομής ώστε να προστατεύεται από απειλές και να διασφαλίζεται η ασφάλειά της και η ασφάλεια των συστημάτων, ***να ελαχιστοποιούνται οι κίνδυνοι και να προωθείται η τεχνολογική υπεροχή της ΕΕ σε κρίσιμους τομείς,*** συμπεριλαμβανομένων ***μέτρων για τον περιορισμό ή τον αποκλεισμό των προμηθευτών υψηλού κινδύνου, καθώς και για την προστασία της ασφάλειας*** των δεδομένων που ανταλλάσσονται μέσω της υποδομής.

Τροπολογία 42

Πρόταση κανονισμού
Άρθρο 8 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν ότι η ανταλλαγή πληροφοριών στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας με οντότητες που δεν είναι δημόσιοι φορείς των κρατών μελών δεν επηρεάζει αρνητικά τα συμφέροντα ασφάλειας της Ένωσης.	2. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν ότι η ανταλλαγή πληροφοριών στο πλαίσιο της ευρωπαϊκής κυβερνοασπίδας με οντότητες που δεν είναι δημόσιοι φορείς των κρατών μελών δεν επηρεάζει αρνητικά τα συμφέροντα ασφάλειας της Ένωσης ***και ότι οποιαδήποτε ανταλλαγή πληροφοριών με παρόχους υψηλού κινδύνου είναι περιορισμένη όσον αφορά το πεδίο εφαρμογής και δεν θίγει την ασφάλεια και τα στρατηγικά συμφέροντα της Ένωσης***.

Τροπολογία 43

Πρόταση κανονισμού
Άρθρο 8 – παράγραφος 3

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
3. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις για τον καθορισμό τεχνικών απαιτήσεων ώστε τα κράτη μέλη να συμμορφώνονται προς την υποχρέωση που υπέχουν δυνάμει των παραγράφων 1 και 2. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού. Στο πλαίσιο αυτό, η Επιτροπή, υποστηριζόμενη από τον/την ύπατο/-η εκπρόσωπο, λαμβάνει υπόψη τα σχετικά πρότυπα ασφάλειας σε επίπεδο άμυνας, προκειμένου να διευκολύνει τη συνεργασία με στρατιωτικούς φορείς.	3. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις για τον καθορισμό τεχνικών απαιτήσεων ώστε τα κράτη μέλη να συμμορφώνονται προς την υποχρέωση που υπέχουν δυνάμει των παραγράφων 1 και 2. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού. Στο πλαίσιο αυτό, η Επιτροπή, υποστηριζόμενη από τον/την ύπατο/-η εκπρόσωπο, λαμβάνει υπόψη τα σχετικά πρότυπα ασφάλειας σε επίπεδο άμυνας, προκειμένου να διευκολύνει τη συνεργασία με στρατιωτικούς φορείς***, αξιοποιώντας κατάλληλα όλο το φάσμα των αμυντικών επιλογών που έχουν στη διάθεσή τους οι πολιτικές και στρατιωτικές κοινότητες για την ευρύτερη ασφάλεια και άμυνα της ΕΕ, και ενημερώνει το Ευρωπαϊκό Κοινοβούλιο***.

Τροπολογία 44

Πρόταση κανονισμού
Άρθρο 9 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Οι δράσεις που υλοποιούν τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο στηρίζονται από χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη» και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694 και ιδίως τον ειδικό στόχο 3.	2. Οι δράσεις που υλοποιούν τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο στηρίζονται από χρηματοδότηση από το πρόγραμμα «Ψηφιακή Ευρώπη» και υλοποιούνται σύμφωνα με τον κανονισμό (ΕΕ) 2021/694 και ιδίως τον ειδικό στόχο 3 ***και από τον Ευρωπαϊκό Μηχανισμό για την Ειρήνη (ΕΜΕ) κατά την παροχή μέτρων***

	συνδρομής σε τρίτες χώρες, ιδίως στην Ουκρανία και τη Μολδαβία.

Τροπολογία 45

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***, όπως οι δημόσιες υποδομές, οι εκλογικές υποδομές, οι μεταφορές, η υγειονομική περίθαλψη, ο χρηματοοικονομικός τομέας, οι τηλεπικοινωνίες, ο εφοδιασμός τροφίμων και η ασφάλεια,*** σε ολόκληρη την Ένωση,

Τροπολογία 46

Πρόταση κανονισμού
Άρθρο 10 – παράγραφος 1 – στοιχείο γ

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
γ) δράσεις αμοιβαίας συνδρομής που συνίστανται στην παροχή συνδρομής από τις εθνικές αρχές ενός κράτους μέλους σε άλλο κράτος μέλος, ιδίως όπως προβλέπεται στο άρθρο 11 παράγραφος 3 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555**.**	γ) δράσεις αμοιβαίας συνδρομής που συνίστανται στην παροχή συνδρομής από τις εθνικές αρχές ενός κράτους μέλους σε άλλο κράτος μέλος, ιδίως όπως προβλέπεται στο άρθρο 11 παράγραφος 3 στοιχείο στ) της οδηγίας (ΕΕ) 2022/2555 ***και στο πλαίσιο του άρθρου 42 παράγραφος 7 ΣΕΕ και του άρθρου 222 ΣΛΕΕ,***

Τροπολογία 47

Πρόταση κανονισμού
Άρθρο 10 – παράγραφος 1 – στοιχείο γ α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	γ α) αντικατάσταση και σταδιακή κατάργηση του κρίσιμου εξοπλισμού από προμηθευτές υψηλού κινδύνου που θα ενεργούσαν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον τίτλο V της ΣΕΕ.

Τροπολογία 48

Πρόταση κανονισμού
Άρθρο 11 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ENISA και τον/την ύπατο/-η εκπρόσωπο, αναπτύσσει κοινά σενάρια και μεθοδολογίες κινδύνου για τις συντονισμένες δοκιμές.	2. Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ENISA, τον/την ύπατο/-η εκπρόσωπο, ***την ΕΥΕΔ και, κατά περίπτωση, τον ΕΟΑ,*** αναπτύσσει κοινά σενάρια και μεθοδολογίες κινδύνου για τις συντονισμένες δοκιμές.

Τροπολογία 49

Πρόταση κανονισμού
Άρθρο 12 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 16. Η εφεδρεία περιλαμβάνει προδεσμευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη.	2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 16. Η εφεδρεία περιλαμβάνει προδεσμευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη ***και σε τρίτες χώρες που πληρούν τις εφαρμοστέες απαιτήσεις του παρόντος κανονισμού***.

Τροπολογία 50

Πρόταση κανονισμού
Άρθρο 12 – παράγραφος 3 – στοιχείο β

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
β) τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης.	β) τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης***, συμπεριλαμβανομένων των αποστολών ΚΠΑΑ***.

Τροπολογία 51

Πρόταση κανονισμού
Άρθρο 12 – παράγραφος 4

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
4. Οι χρήστες που αναφέρονται στην παράγραφο 3 στοιχείο α) χρησιμοποιούν τις υπηρεσίες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας για την αντιμετώπιση ή την υποστήριξη της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά που επηρεάζουν οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας.	4. Οι χρήστες που αναφέρονται στην παράγραφο 3 στοιχείο α) χρησιμοποιούν τις υπηρεσίες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας για την αντιμετώπιση ή την υποστήριξη της αντιμετώπισης και της άμεσης ανάκαμψης από σημαντικά ή μεγάλης κλίμακας περιστατικά που επηρεάζουν οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας***, όπως οι δημόσιες υποδομές, οι εκλογικές υποδομές, οι μεταφορές, η υγειονομική περίθαλψη, ο χρηματοοικονομικός τομέας, οι τηλεπικοινωνίες, ο εφοδιασμός τροφίμων και η ασφάλεια***.

Τροπολογία 52

Πρόταση κανονισμού
Άρθρο 12 – παράγραφος 5

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
5. Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η Επιτροπή καθορίζει τις προτεραιότητες	5. Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η Επιτροπή καθορίζει τις προτεραιότητες

και την εξέλιξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, σύμφωνα με τις απαιτήσεις των χρηστών που αναφέρονται στην παράγραφο 3, εποπτεύει την υλοποίησή της και διασφαλίζει τη συμπληρωματικότητα, τη συνοχή, τις συνέργειες και τους δεσμούς με άλλες δράσεις στήριξης στο πλαίσιο του παρόντος κανονισμού, καθώς και με άλλες δράσεις και προγράμματα της Ένωσης.

και την εξέλιξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, σύμφωνα με τις απαιτήσεις των χρηστών που αναφέρονται στην παράγραφο 3, εποπτεύει την υλοποίησή της και διασφαλίζει τη συμπληρωματικότητα, τη συνοχή, τις συνέργειες και τους δεσμούς με άλλες δράσεις στήριξης στο πλαίσιο του παρόντος κανονισμού, καθώς και με άλλες δράσεις και προγράμματα της Ένωσης ***και σκοπούς της Ένωσης, και ιδίως τον στρατηγικό στόχο της μείωσης των εξαρτήσεων από προμηθευτές υψηλού κινδύνου που θα ενεργούσαν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως αυτά ορίζονται στο πλαίσιο της ΚΕΠΠΑ, σύμφωνα με τον Τίτλο V της ΣΕΕ***.

Τροπολογία 53

Πρόταση κανονισμού
Άρθρο 12 – παράγραφος 7

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
7. Προκειμένου να στηρίξει την Επιτροπή στη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ο ENISA εκπονεί χαρτογράφηση των αναγκαίων υπηρεσιών, αφού ζητήσει τη γνώμη των κρατών μελών και της Επιτροπής. Ο ENISA εκπονεί παρόμοια χαρτογράφηση, αφού ζητήσει τη γνώμη της Επιτροπής, για τον προσδιορισμό των αναγκών των τρίτων χωρών που είναι επιλέξιμες για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 17. Η Επιτροπή, κατά περίπτωση, ζητά τη γνώμη του/της ύπατου/-ης εκπροσώπου.	7. Προκειμένου να στηρίξει την Επιτροπή στη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ο ENISA εκπονεί χαρτογράφηση των αναγκαίων υπηρεσιών, αφού ζητήσει τη γνώμη των κρατών μελών και της Επιτροπής. Ο ENISA εκπονεί παρόμοια χαρτογράφηση, αφού ζητήσει τη γνώμη της Επιτροπής, για τον προσδιορισμό των αναγκών των τρίτων χωρών που είναι επιλέξιμες για στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας σύμφωνα με το άρθρο 17***, με την υποστήριξη της ΕΥΕΔ***. Η Επιτροπή, κατά περίπτωση, ζητά τη γνώμη του/της ύπατου/-ης εκπροσώπου.

Τροπολογία 54

Πρόταση κανονισμού
Άρθρο 14 – παράγραφος 2 – στοιχείο α α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	α α) ο αντίκτυπος του συμβάντος στην ασφάλεια και την άμυνα της Ένωσης,

Τροπολογία 55

Πρόταση κανονισμού
Άρθρο 15 – παράγραφος 3

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
3. Σε διαβούλευση με τον/την ύπατο/-η εκπρόσωπο, η στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο μπορεί να συμπληρώνει τη βοήθεια που παρέχεται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας και της κοινής πολιτικής ασφάλειας και άμυνας, μεταξύ άλλων μέσω των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο. Μπορεί επίσης να συμπληρώνει ή να συμβάλλει στη συνδρομή που παρέχεται από ένα κράτος μέλος σε άλλο κράτος μέλος στο πλαίσιο του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση.	3. Σε διαβούλευση με τον/την ύπατο/-η εκπρόσωπο, η στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο μπορεί να συμπληρώνει τη βοήθεια που παρέχεται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας και της κοινής πολιτικής ασφάλειας και άμυνας, μεταξύ άλλων μέσω των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο ***(CRRT), προκειμένου να στηριχθούν καλύτερα τα κράτη μέλη της ΕΕ, οι αποστολές και επιχειρήσεις ΚΠΑΑ και οι τρίτες χώρες που ευθυγραμμίζονται με την κοινή εξωτερική πολιτική και πολιτική ασφαλείας και την κοινή πολιτική ασφάλειας και άμυνας στις προσπάθειές τους για ανάπτυξη ικανοτήτων κυβερνοάμυνας, ιδίως η Ουκρανία και η Μολδαβία***. Μπορεί επίσης να συμπληρώνει ή να συμβάλλει στη συνδρομή που παρέχεται από ένα κράτος μέλος σε άλλο κράτος μέλος στο πλαίσιο του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση.

Τροπολογία 56

Πρόταση κανονισμού
Άρθρο 16 – παράγραφος 2 – στοιχείο β α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	β α) ο πάροχος αποδεικνύει ότι οι δομές λήψης αποφάσεων και διαχείρισής του είναι απαλλαγμένες από οποιαδήποτε αθέμιτη επιρροή από κυβερνήσεις κρατών που θα ενεργούσαν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον τίτλο V της ΣΕΕ,

Τροπολογία 57

Πρόταση κανονισμού
Άρθρο 16 – παράγραφος 2 – στοιχείο στ

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
στ) ο πάροχος είναι εξοπλισμένος με τον τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας,	στ) ο πάροχος είναι εξοπλισμένος με τον τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας ***και πληροί τις απαιτήσεις που ορίζονται στο άρθρο Χ του κανονισμού XX/XXXX (πράξη για την κυβερνοανθεκτικότητα)***,

Τροπολογία 58

Πρόταση κανονισμού
Άρθρο 16 – παράγραφος 2 – στοιχείο ι α (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	ι α) κανένας πάροχος που προέρχεται από τρίτη χώρα υψηλού κινδύνου δεν μπορεί να γίνει δεκτός,

Τροπολογία 59

Πρόταση κανονισμού
Άρθρο 16 – παράγραφος 2 – στοιχείο ι β (νέο)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*

	ι β) ο πάροχος συνεργάζεται στενά με τις σχετικές ΜΜΕ, στο μέτρου του δυνατού,

Τροπολογία 60

Πρόταση κανονισμού
Άρθρο 17 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
1. Τρίτες χώρες μπορούν να ζητήσουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον αυτό προβλέπεται από συμφωνίες σύνδεσης που έχουν συναφθεί σχετικά με τη συμμετοχή τους στο πρόγραμμα «Ψηφιακή Ευρώπη».	1. Τρίτες χώρες μπορούν να ζητήσουν στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, εφόσον***:***
	α) αυτό προβλέπεται από συμφωνίες σύνδεσης που έχουν συναφθεί σχετικά με τη συμμετοχή τους στο πρόγραμμα «Ψηφιακή Ευρώπη»***,***
	β) αυτές οι τρίτες χώρες στις οποίες αναπτύσσεται αποστολή ΚΠΑΑ με ειδική εντολή για την ενίσχυση της ανθεκτικότητας σε υβριδικές απειλές, συμπεριλαμβανομένου του κυβερνοχώρου, ή στις οποίες έχει εγκριθεί μέτρο συνδρομής του ΕΜΕ για την ενίσχυση της κυβερνοανθεκτικότητας της χώρας.

Τροπολογία 61

Πρόταση κανονισμού
Άρθρο 17 – παράγραφος 2

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
2. Η στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι σύμφωνη προς τις διατάξεις του παρόντος κανονισμού και συμμορφώνεται με τυχόν ειδικούς όρους που καθορίζονται στις συμφωνίες σύνδεσης που αναφέρονται	2. Η στήριξη από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας είναι σύμφωνη προς τις διατάξεις του παρόντος κανονισμού και συμμορφώνεται με τυχόν ειδικούς όρους που καθορίζονται στις συμφωνίες σύνδεσης που αναφέρονται στην παράγραφο 1, ***εκτός των τρίτων***

στην παράγραφο 1.

χωρών που καλύπτονται από τις διατάξεις της παραγράφου 1 στοιχείο β).

Τροπολογία 62

Πρόταση κανονισμού
Άρθρο 18 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
1. Κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, ο ENISA θα πρέπει να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA υποβάλλει έκθεση εξέτασης περιστατικού στο δίκτυο CSIRT, στο EU-CyCLONe και στην Επιτροπή για να τους στηρίξει κατά την εκτέλεση των καθηκόντων τους, ιδίως όσον αφορά τα καθήκοντα που ορίζονται στα άρθρα 15 και 16 της οδηγίας (ΕΕ) 2022/2555. Κατά περίπτωση, η Επιτροπή κοινοποιεί την έκθεση στον/στην ύπατο/-η εκπρόσωπο.	1. Κατόπιν αιτήματος της Επιτροπής, του EU-CyCLONe ή του δικτύου CSIRT, ο ENISA θα πρέπει να εξετάζει και να αξιολογεί απειλές, τρωτά σημεία και δράσεις μετριασμού σε σχέση με συγκεκριμένο σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας. Μετά την ολοκλήρωση της εξέτασης και της αξιολόγησης ενός περιστατικού, ο ENISA υποβάλλει έκθεση εξέτασης περιστατικού στο δίκτυο CSIRT, στο EU-CyCLONe και στην Επιτροπή για να τους στηρίξει κατά την εκτέλεση των καθηκόντων τους, ιδίως όσον αφορά τα καθήκοντα που ορίζονται στα άρθρα 15 και 16 της οδηγίας (ΕΕ) 2022/2555. Κατά περίπτωση, ***ιδίως όταν το περιστατικό αφορά τρίτη χώρα,*** η Επιτροπή κοινοποιεί την έκθεση στον/στην ύπατο/-η εκπρόσωπο ***και στην ΕΥΕΔ***.

Τροπολογία 63

Πρόταση κανονισμού
Άρθρο 18 – παράγραφος 3 α (νέα)

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
	3α. Η έκθεση κοινοποιείται στο Ευρωπαϊκό Κοινοβούλιο σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο για την προστασία των ευαίσθητων διαβαθμισμένων πληροφοριών.

Τροπολογία 64

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

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
α α) στήριξη της ανάπτυξης ενωσιακής κυβερνοασπίδας, συμπεριλαμβανομένης της ανάπτυξης, της εγκατάστασης και της λειτουργίας εθνικών και διασυνοριακών πλατφορμών SOC που συμβάλλουν στην αντίληψη της κατάστασης στην Ένωση και στην ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά τη συλλογή πληροφοριών για τις κυβερνοαπειλές·	α α) στήριξη της ανάπτυξης ενωσιακής κυβερνοασπίδας, συμπεριλαμβανομένης της ανάπτυξης, της εγκατάστασης και της λειτουργίας εθνικών και διασυνοριακών πλατφορμών SOC που συμβάλλουν στην αντίληψη της κατάστασης στην Ένωση και στην ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά τη συλλογή πληροφοριών για τις κυβερνοαπειλές ***και στη μείωση της εξάρτησης της Ένωσης από τους υψηλού κινδύνου προμηθευτές κρίσιμου εξοπλισμού ή εξαρτημάτων κυβερνοασφάλειας, που θα ενεργούσαν αντίθετα προς τα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών της, όπως ορίζονται στο πλαίσιο της ΚΕΠΠΑ σύμφωνα με τον τίτλο V της ΣΕΕ***·

Τροπολογία 65

Πρόταση κανονισμού
Άρθρο 20 – παράγραφος 1

Κείμενο που προτείνει η Επιτροπή	*Τροπολογία*
Έως [***τέσσερα*** έτη μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού], η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εκθέσεις σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού.	Έως [***τρία*** έτη μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού ***και έπειτα κάθε δύο έτη***], η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο εκθέσεις σχετικά με την αξιολόγηση και την επανεξέταση του παρόντος κανονισμού.

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΓΝΩΜΟΔΟΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ

Τίτλος	Θέσπιση μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων στην Ένωση όσον αφορά τον εντοπισμό, την ετοιμότητα και την αντίδραση σε απειλές και περιστατικά 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	AFET 1.6.2023
Συντάκτης(τρια) γνωμοδότησης Ημερομηνία ορισμού	Dragoş Tudorache 16.6.2023
Εξέταση στην επιτροπή	18.9.2023
Ημερομηνία έγκρισης	24.10.2023
Αποτέλεσμα της τελικής ψηφοφορίας	+: 39 –: 4 0: 0
Βουλευτές παρόντες κατά την τελική ψηφοφορία	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Γιώργος Γεωργίου, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Βαγγέλης Μεϊμαράκης, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Δημήτρης Παπαδάκης, Κώστας Παπαδάκης, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Αναπληρωτές παρόντες κατά την τελική ψηφοφορία	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Γεώργιος Κύρτσος, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

ΤΕΛΙΚΗ ΨΗΦΟΦΟΡΙΑ ΜΕ ΟΝΟΜΑΣΤΙΚΗ ΚΛΗΣΗ ΣΤΗ ΓΝΩΜΟΔΟΤΙΚΗ ΕΠΙΤΡΟΠΗ

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Βαγγέλης Μεϊμαράκης, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Γεώργιος Κύρτσος, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Δημήτρης Παπαδάκης, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Κώστας Παπαδάκης
The Left	Γιώργος Γεωργίου, Mick Wallace

0	0

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