



2023/0109(COD)

22.9.2023

# ΤΡΟΠΟΛΟΓΙΕΣ 46 - 216

Σχέδιο έκθεσης  
**Lina Gálvez Muñoz**  
(PE752.795v01-00)

σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την αντίχρευση, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας

Πρόταση κανονισμού  
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))



**Τροπολογία 46**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Τίτλος 1**

*Κείμενο που προτείνει η Επιτροπή*

Πρόταση  
ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ  
ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ  
ΣΥΜΒΟΥΛΙΟΥ  
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

*Τροπολογία*

Πρόταση  
ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ  
ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ  
ΣΥΜΒΟΥΛΙΟΥ  
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 (*πράξη για την  
αλληλεγγύη στον κυβερνοχώρο*)

Or. en

**Τροπολογία 47**  
**Ville Niinistö**

εξ ονόματος της Ομάδας Verts/ALE

**Πρόταση κανονισμού**  
**Αιτιολογική σκέψη 1**

*Κείμενο που προτείνει η Επιτροπή*

(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.

*Τροπολογία*

(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές **και τρωτά σημεία** 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.

Or. en

## Αιτιολόγηση

*Η ανάγκη για το εν λόγω νομικό κείμενο προκύπτει από το γεγονός ότι οι θεμελιώδεις εξαρτήσεις γίνονται επίσης τρωτά σημεία.*

### Τροπολογία 48

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

#### Πρόταση κανονισμού

#### Αιτιολογική σκέψη 2

*Κείμενο που προτείνει η Επιτροπή*

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

*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 **σε ολόκληρη την Ένωση** απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων και παραγόντων χακτιβισμού (ακτιβισμός στον κυβερνοχώρο) που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών και την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, να προκαλέσουν σημαντικές οικονομικές ζημιές, να υπονομεύσουν την εμπιστοσύνη

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.

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. ***Συνεπώς, η στενή και συντονισμένη συνεργασία μεταξύ του δημόσιου τομέα, του ιδιωτικού τομέα, των κρατών μελών, θεσμικών οργάνων ή οργανισμών της Ένωσης και της ακαδημαϊκής κοινότητας είναι απαραίτητη για τη βελτίωση της κατάστασης της κυβερνοασφάλειας στην Ένωση. Η αντίδραση της Ένωσης θα πρέπει να πραγματοποιηθεί σε συνεργασία με έμπιστους και ομοφρονούντες διεθνείς εταίρους και διεθνείς οργανισμούς, και να είναι ευθυγραμμισμένη με διεθνή πλαίσια και συμφωνίες συνεργασίας.***

Or. en

## **Τροπολογία 49**

**Ville Niinistö**

εξ ονόματος της Ομάδας Verts/ALE

### **Πρόταση κανονισμού**

#### **Αιτιολογική σκέψη 2**

*Κείμενο που προτείνει η Επιτροπή*

(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

*Τροπολογία*

(2) Το μέγεθος, η συχνότητα και οι επιπτώσεις των περιστατικών κυβερνοασφάλειας αυξάνονται, συμπεριλαμβανομένων των επιθέσεων στην αλυσίδα εφοδιασμού με στόχο την κυβερνοκατασκοπεία, την εγκατάσταση λυτρισμικού ή την πρόκληση διαταραχών. Αποτελούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και

πληροφοριών. Ενόψει του ταχέως εξελισσόμενου τοπίου των απειλών, η απειλή πιθανών περιστατικών μεγάλης κλίμακας που προκαλούν σημαντική διαταραχή ή ζημία σε κρίσιμες υποδομές απαιτεί αυξημένη ετοιμότητα σε όλα τα επίπεδα του πλαισίου κυβερνοασφάλειας της Ένωσης. Η απειλή αυτή υπερβαίνει τη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας και είναι πιθανό να συνεχίσει να υφίσταται, δεδομένης της πληθώρας των συνασπιζόμενων με το κράτος εγκληματικών παραγόντων **και παραγόντων χακτιβισμού (ακτιβισμός στον κυβερνοχώρο)** που εμπλέκονται στις τρέχουσες γεωπολιτικές εντάσεις. Τέτοια περιστατικά μπορούν να παρεμποδίσουν την παροχή δημόσιων υπηρεσιών και την άσκηση οικονομικών δραστηριοτήτων, μεταξύ άλλων σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, να προκαλέσουν σημαντικές οικονομικές ζημιές, 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.

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 **και εγκληματικών παραγόντων 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 ζημιές, 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.

Or. en

#### Αιτιολόγηση

*Η γενική ένταξη του χακτιβισμού (ακτιβισμός στον κυβερνοχώρο) στις εγκληματικές δραστηριότητες δεν αντικατοπτρίζει το εύρος των εν λόγω δραστηριοτήτων, συμπεριλαμβανομένων νόμιμων διαμαρτυριών και καταγγελιών δυσλειτουργίας. Το κείμενο θα επωφελούνταν από την αποφυγή ασαφειών και την προστασία νόμιμων δραστηριοτήτων.*

#### Τροπολογία 50

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareș**

Πρόταση κανονισμού  
Αιτιολογική σκέψη 3

*Κείμενο που προτείνει η Επιτροπή*

(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*<sup>16</sup>, 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 στηρίζουν 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.

*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, είναι αναγκαίο να αυξηθεί η ανθεκτικότητα των πολιτών, των επιχειρήσεων, **συμπεριλαμβανομένων των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων (ΜΜΕ)**, και των οντοτήτων που διαχειρίζονται κρίσιμες υποδομές, **συμπεριλαμβανομένων των τοπικών ή περιφερειακών αρχών**, έναντι των αυξανόμενων απειλών κυβερνοασφάλειας, οι οποίες μπορούν να έχουν καταστροφικές κοινωνικές και οικονομικές επιπτώσεις. Ως εκ τούτου, απαιτούνται επενδύσεις σε υποδομές, υπηρεσίες **και προσωπικό υψηλής ειδίκευσης με τις αναγκαίες δεξιότητες** που θα στηρίζουν 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, **μέσω και της προορατικής συλλογής πληροφοριών**. 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. [1]  
<https://futureu.europa.eu/el/>

<sup>16</sup> <https://futureu.europa.eu/el/>

**Τροπολογία 51****Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan****Πρόταση κανονισμού  
Αιτιολογική σκέψη 5***Κείμενο που προτείνει η Επιτροπή*

(5) Οι αυξανόμενοι κίνδυνοι κυβερνοασφάλειας και ένα συνολικά σύνθετο τοπίο απειλών, με σαφή κίνδυνο ταχείας πρόκλησης δευτερογενών επιπτώσεων από τα περιστατικά στον κυβερνοχώρο από ένα κράτος μέλος σε άλλα και από τρίτη χώρα στην Ένωση, απαιτούν ενισχυμένη αλληλεγγύη σε επίπεδο Ένωσης για την καλύτερη ανίχνευση, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας. Τα κράτη μέλη κάλεσαν επίσης την Επιτροπή να υποβάλει πρόταση σχετικά με ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας στα συμπεράσματα του Συμβουλίου σχετικά με τη στάση της ΕΕ<sup>21</sup>.

---

<sup>21</sup> Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, τα οποία εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022 (9364/22).

*Τροπολογία*

(5) Οι αυξανόμενοι κίνδυνοι κυβερνοασφάλειας και ένα συνολικά σύνθετο τοπίο απειλών, με σαφή κίνδυνο ταχείας πρόκλησης δευτερογενών επιπτώσεων από τα περιστατικά στον κυβερνοχώρο από ένα κράτος μέλος σε άλλα και από τρίτη χώρα στην Ένωση, απαιτούν ενισχυμένη αλληλεγγύη σε επίπεδο Ένωσης για την καλύτερη ανίχνευση, προετοιμασία και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας, **καθώς και για την καλύτερη ανάκαμψη από αυτά**. Τα κράτη μέλη κάλεσαν επίσης την Επιτροπή να υποβάλει πρόταση σχετικά με ένα νέο ταμείο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της κυβερνοασφάλειας στα συμπεράσματα του Συμβουλίου σχετικά με τη στάση της ΕΕ<sup>21</sup>.

---

<sup>21</sup> Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, τα οποία εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022 (9364/22).

**Τροπολογία 52****Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**



**Πρόταση κανονισμού  
Αιτιολογική σκέψη 9 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*(9α) Υπό το φως των γεωπολιτικών εξελίξεων και του τοπίου των αυξανόμενων απειλών στον κυβερνοχώρο, η συνέχεια και η περαιτέρω εξέλιξη των μέτρων που ορίζονται στον παρόντα κανονισμό, ιδίως της ευρωπαϊκής κυβερνοασπίδας και του ευρωπαϊκού μηχανισμού έκτακτης ανάγκης, είναι σημαντική. Επομένως, είναι απαραίτητο να διασφαλιστεί συγκεκριμένη γραμμή του προϋπολογισμού στο πολυετές δημοσιονομικό πλαίσιο για την περίοδο 2028 έως 2034. Τα κράτη μέλη θα πρέπει επίσης να δεσμευτούν για τη στήριξη όλων των αναγκαίων μέτρων με σκοπό την ενίσχυση της αλληλεγγύης εντός της Ένωσης και τη μείωση των απειλών και των περιστατικών στον κυβερνοχώρο σε ολόκληρη την Ένωση.*

Or. en

**Τροπολογία 53**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 12**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση και αντιμετώπιση κυβερνοαπειλών και περιστατικών, είναι αναγκαίο να αναπτυχθούν πληρέστερες γνώσεις σχετικά με τις απειλές κατά κρίσιμων πάγιων στοιχείων και υποδομών στο έδαφος της Ένωσης, συμπεριλαμβανομένης της γεωγραφικής κατανομής, της διασύνδεσης και των δυνητικών επιπτώσεών τους σε περίπτωση

(12) Για την αποτελεσματικότερη πρόληψη, αξιολόγηση και αντιμετώπιση κυβερνοαπειλών και περιστατικών, **και ανάκαμψη από αυτά**, είναι αναγκαίο να αναπτυχθούν πληρέστερες γνώσεις σχετικά με τις απειλές κατά κρίσιμων πάγιων στοιχείων και υποδομών στο έδαφος της Ένωσης, συμπεριλαμβανομένης της γεωγραφικής κατανομής, της διασύνδεσης και των δυνητικών επιπτώσεών τους σε

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

---

<sup>24</sup> 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

περίπτωση κυβερνοεπιθέσεων που επηρεάζουν τις εν λόγω υποδομές, **μεταξύ άλλων, μέσω της προορατικής συλλογής πληροφοριών**. Θα πρέπει να αναπτυχθεί μια μεγάλη κλίμακας ενωσιακή υποδομή SOC (στο εξής: ευρωπαϊκή κυβερνοασπίδα), η οποία θα αποτελείται από διάφορες διαλειτουργικές διασυνοριακές πλατφόρμες, καθεμία από τις οποίες θα συγκεντρώνει διάφορα εθνικά SOC. **Ένα εθνικό SOC είναι μια κεντρική ικανότητα υπεύθυνη για τη συνεχή συλλογή πληροφοριών για απειλές και για τη βελτίωση της κατάστασης κυβερνοασφάλειας οντοτήτων υπό εθνική δικαιοδοσία μέσω της πρόληψης, της ανίχνευσης και της ανάλυσης απειλών κυβερνοασφάλειας**. Οι εν λόγω υποδομές θα πρέπει να εξυπηρετούν εθνικά και ενωσιακά συμφέροντα και ανάγκες κυβερνοασφάλειας, αξιοποιώντας την τεχνολογία αιχμής για προηγμένα εργαλεία συλλογής και ανάλυσης δεδομένων, ενισχύοντας τις ικανότητες ανίχνευσης και διαχείρισης στον κυβερνοχώρο και παρέχοντας αντίληψη της κατάστασης σε πραγματικό χρόνο. Οι υποδομές αυτές θα πρέπει να χρησιμεύουν για την αύξηση της ανίχνευσης απειλών και περιστατικών κυβερνοασφάλειας και, ως εκ τούτου, να συμπληρώνουν και να στηρίζουν τις οντότητες και τα δίκτυα της Ένωσης που είναι αρμόδια για τη διαχείριση κρίσεων στην Ένωση, ιδίως το δίκτυο οργανισμών διασύνδεσης για κυβερνοκρίσεις της ΕΕ (στο εξής: EU-CyCLONe), όπως ορίζεται στην οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>24</sup>.

---

<sup>24</sup> 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

## Τροπολογία 54

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan

### Πρόταση κανονισμού Αιτιολογική σκέψη 13

*Κείμενο που προτείνει η Επιτροπή*

(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.

*Τροπολογία*

(13) **Προκειμένου να συμμετάσχει στην ευρωπαϊκή κυβερνοασπίδα**, κάθε κράτος μέλος θα πρέπει να ορίσει έναν δημόσιο φορέα σε εθνικό επίπεδο επιφορτισμένο με τον συντονισμό των δραστηριοτήτων ανίχνευσης **και ανταλλαγής πληροφοριών** κυβερνοαπειλών στο εν λόγω κράτος μέλος. **Τα κράτη μέλη ενθαρρύνονται θερμά να ενσωματώσουν την ικανότητα των εθνικών SOC στην ήδη υπάρχουσα δομή και διακυβέρνησή τους για τον κυβερνοχώρο, ώστε να μη δημιουργηθούν πρόσθετα επίπεδα διακυβέρνησης και να ευθυγραμμιστεί η πράξη για την αλληλεγγύη στον κυβερνοχώρο με την ήδη υπάρχουσα νομοθεσία, συμπεριλαμβανομένης της οδηγίας 2022/2555.** Τα εν λόγω εθνικά SOC θα πρέπει να λειτουργούν ως σημείο αναφοράς και πύλη σε εθνικό επίπεδο για τη συμμετοχή **ιδιωτικών και δημόσιων οντοτήτων, ιδίως των SOC τους**, 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. **Τα εθνικά SOC θα πρέπει να ενισχύσουν τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ δημόσιων και ιδιωτικών οντοτήτων, ώστε να σπάσουν τα στεγανά που**

*υπάρχουν επί του παρόντος στην επικοινωνία. Με αυτόν τον τρόπο, μπορούν να στηρίζουν τη δημιουργία μοντέλων ανταλλαγής δεδομένων και θα πρέπει να διευκολύνουν και να ενθαρρύνουν την ανταλλαγή πληροφοριών σε ένα αξιόπιστο και ασφαλές περιβάλλον. Η στενή και συντονισμένη συνεργασία μεταξύ δημόσιων και ιδιωτικών οντοτήτων είναι πολύ σημαντική για την ενίσχυση της ανθεκτικότητας της Ένωσης στον τομέα της κυβερνοασφάλειας.*

Or. en

## Τροπολογία 55

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού Αιτιολογική σκέψη 14

*Κείμενο που προτείνει η Επιτροπή*

(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

*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 **και προορατικών** 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.**

κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης σε ένα αξιόπιστο περιβάλλον. **Τα διασυνοριακά SOC θα πρέπει να διευκολύνουν και να ενθαρρύνουν την ανταλλαγή πληροφοριών σε ένα αξιόπιστο και ασφαλές περιβάλλον. Ο ENISA θα πρέπει να στηρίζει τα διασυνοριακά SOC σε θέματα που σχετίζονται με την επιχειρησιακή συνεργασία.** Θα πρέπει να παρέχουν νέα πρόσθετη ικανότητα **και παράλληλα να είναι ενσωματωμένα στις ήδη υφιστάμενες υποδομές κυβερνοασφάλειας, συμπεριλαμβανομένων των SOC και των ομάδων** αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (στο εξής: CSIRT) και **άλλων σχετικών παραγόντων.**

Or. en

## Τροπολογία 56

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rares Bogdan

### Πρόταση κανονισμού Αιτιολογική σκέψη 15

*Κείμενο που προτείνει η Επιτροπή*

(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

*Τροπολογία*

(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών διασφαλίζεται συνήθως από τα SOC δημόσιων και ιδιωτικών οντοτήτων, σε συνδυασμό με τις CSIRT. Επιπλέον, οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Τα διασυνοριακά SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα **είναι ενσωματωμένη στην ήδη υφιστάμενη υποδομή κυβερνοασφάλειας, πιο συγκεκριμένα στο** δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κυβερνοασφάλειας από δημόσιες και

εμπειρογνομόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης.

ιδιωτικές οντότητες, **ιδίως από τα SOC τους**, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνομόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης, **ώστε να ενισχυθεί η ανθεκτικότητα της Ένωσης.**

Or. en

## Τροπολογία 57

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### Πρόταση κανονισμού

#### Αιτιολογική σκέψη 15

*Κείμενο που προτείνει η Επιτροπή*

(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 εμπειρογνομόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη **των ικανοτήτων και της τεχνολογικής κυριαρχίας της Ένωσης.**

*Τροπολογία*

(15) Σε εθνικό επίπεδο, η παρακολούθηση, η ανίχνευση και η ανάλυση των κυβερνοαπειλών διασφαλίζεται συνήθως από τα SOC δημόσιων και ιδιωτικών οντοτήτων, σε συνδυασμό με τις CSIRT. Επιπλέον, οι CSIRT ανταλλάσσουν πληροφορίες στο πλαίσιο του δικτύου CSIRT, σύμφωνα με την οδηγία (ΕΕ) 2022/2555. Τα διασυνοριακά SOC θα πρέπει να αποτελέσουν μια νέα ικανότητα που θα συμπληρώνει το δίκτυο CSIRT, συγκεντρώνοντας και ανταλλάσσοντας δεδομένα σχετικά με απειλές κυβερνοασφάλειας από δημόσιες και ιδιωτικές οντότητες, ενισχύοντας την αξία των εν λόγω δεδομένων μέσω αναλύσεων εμπειρογνομόνων και από κοινού αποκτηθεισών υποδομών και εργαλείων αιχμής και συμβάλλοντας στην ανάπτυξη **ενός σημαντικού οικοσυστήματος κυβερνοασφάλειας με ισχυρές ενωσιακές ικανότητες και συνεργασία με ομοφρονούντες εταίρους.**

Or. en

## Τροπολογία 58

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

### Πρόταση κανονισμού Αιτιολογική σκέψη 16

*Κείμενο που προτείνει η Επιτροπή*

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

*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], **ώστε να διευκολυνθεί η υπέρβαση των στεγανών που υπάρχουν επί του παρόντος στην επικοινωνία. Με τον τρόπο αυτόν, τα διασυνοριακά SOC θα μπορούσαν επίσης να στηρίζουν τη δημιουργία μοντέλων ανταλλαγής δεδομένων σε ολόκληρη την Ένωση.** Οι πληροφορίες που ανταλλάσσονται μεταξύ των συμμετεχόντων σε ένα διασυνοριακό SOC μπορούν να περιλαμβάνουν δεδομένα από δίκτυα και αισθητήρες, ροές πληροφοριών σχετικά με απειλές, **συμπεριλαμβανομένης της συλλογής προορατικών πληροφοριών**, ενδείξεις της παραβίασης και εντός πλαισίου πληροφορίες σχετικά με περιστατικά, απειλές και τρωτά σημεία. Επιπλέον, τα διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC.

Or. en

## Τροπολογία 59

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 16**

*Κείμενο που προτείνει η Επιτροπή*

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

*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 **αναλυμένα** δεδομένα από δίκτυα, αισθητήρες, **καταχωρίσεις, τηλεμετρία**, ροές πληροφοριών σχετικά με απειλές, ενδείξεις της παραβίασης και εντός πλαισίου πληροφορίες σχετικά με **τακτικές, τεχνικές και διαδικασίες**, περιστατικά, **δείγματα κακόβουλου λογισμικού**, απειλές και τρωτά σημεία. Επιπλέον, τα διασυνοριακά SOC θα πρέπει επίσης να συνάπτουν συμφωνίες συνεργασίας με άλλα διασυνοριακά SOC.

Or. en

**Τροπολογία 60**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 17**

*Κείμενο που προτείνει η Επιτροπή*

(17) Η κοινή αντίληψη της κατάστασης

*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 ολοκληρωμένης αντιμετώπισης πολιτικών κρίσεων της ΕΕ (στο εξής: ΙΡCΗ) βάσει της εκτελεστικής απόφασης (ΕΕ) 2018/1993. Ως εκ τούτου, σε περιπτώσεις όπου τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο μεγάλη 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

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: ΙΡCΗ) βάσει της εκτελεστικής απόφασης (ΕΕ) 2018/1993. Ως εκ τούτου, σε περιπτώσεις όπου τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με πιθανό ή εξελισσόμενο μεγάλη κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, θα πρέπει να παρέχουν σχετικές πληροφορίες στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, **σύμφωνα με τις ήδη υπάρχουσες διατάξεις στο πλαίσιο της οδηγίας (ΕΕ) 2022/2555**. 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

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.

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.

Or. en

### **Τροπολογία 61**

**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rares Bogdan**

#### **Πρόταση κανονισμού Αιτιολογική σκέψη 19**

*Κείμενο που προτείνει η Επιτροπή*

(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 αρχές και τις σχετικές οντότητες, ιδίως με τη χρήση των πλέον πρόσφατων τεχνολογιών τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

*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 **και υψηλής ειδικότητας προσωπικό**. Με τον τρόπο αυτό θα καταστεί 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.

Or. en

### **Τροπολογία 62**

**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rares Bogdan**

## Πρόταση κανονισμού Αιτιολογική σκέψη 20

*Κείμενο που προτείνει η Επιτροπή*

(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<sup>25</sup>.

---

<sup>25</sup> 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*

(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. ***Πρέπει να σημειωθεί, ωστόσο, ότι η τεχνητή νοημοσύνη είναι πιο αποτελεσματική όταν συνδυάζεται με ανθρώπινη ανάλυση. Επομένως, το υψηλής ειδίκευσης προσωπικό παραμένει ζωτικής σημασίας για τη συγκέντρωση δεδομένων υψηλής ποιότητας και τη συλλογή προορατικών πληροφοριών για απειλές.*** 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<sup>25</sup>.

---

<sup>25</sup> 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).

Or. en

**Τροπολογία 63**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**

## Αιτιολογική σκέψη 20

*Κείμενο που προτείνει η Επιτροπή*

(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<sup>25</sup>.

---

<sup>25</sup> 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*

(20) Με τη συλλογή, την κοινοποίηση και την ανταλλαγή δεδομένων, η ευρωπαϊκή κυβερνοασπίδα θα πρέπει να ενισχύσει **το σημαντικό οικοσύστημα κυβερνοασφάλειας** 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<sup>25</sup>.

---

<sup>25</sup> 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).

Or. en

## Τροπολογία 64

**Ville Niinistö**

εξ ονόματος της Ομάδας Verts/ALE

### Πρόταση κανονισμού

## Αιτιολογική σκέψη 21

*Κείμενο που προτείνει η Επιτροπή*

(21) Ενώ η ευρωπαϊκή κυβερνοασπίδα είναι ένα μη στρατιωτικό έργο, η κοινότητα κυβερνοάμυνας μπορεί να επωφεληθεί από ισχυρότερες μη

*Τροπολογία*

(21) Ενώ η ευρωπαϊκή κυβερνοασπίδα είναι ένα μη στρατιωτικό έργο, η κοινότητα κυβερνοάμυνας μπορεί να επωφεληθεί από ισχυρότερες μη

στρατιωτικές ικανότητες ανίχνευσης και αντίληψης της κατάστασης που αναπτύχθηκαν για την προστασία κρίσιμων υποδομών. Τα διασυνοριακά SOC, με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC), και σε συνεργασία με τον/την ύπατο/-η εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: ύπατος/-η εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα και πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας. Η ανάπτυξη της ευρωπαϊκής κυβερνοασπίδας θα πρέπει να συνοδεύεται από προβληματισμό που θα επιτρέπει τη μελλοντική συνεργασία με δίκτυα και πλατφόρμες ανταλλαγής πληροφοριών στην κοινότητα κυβερνοάμυνας, σε στενή συνεργασία με τον/την ύπατο/-η εκπρόσωπο.

στρατιωτικές ικανότητες ανίχνευσης και αντίληψης της κατάστασης που αναπτύχθηκαν για την προστασία κρίσιμων υποδομών. Τα διασυνοριακά SOC, με την υποστήριξη της Επιτροπής και του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (στο εξής: ECCC), και σε συνεργασία με τον/την ύπατο/-η εκπρόσωπο της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας (στο εξής: ύπατος/-η εκπρόσωπος), θα πρέπει σταδιακά να αναπτύξουν ειδικά πρωτόκολλα **όρων πρόσβασης και εγγυήσεων** και πρότυπα που θα επιτρέπουν τη συνεργασία με την κοινότητα κυβερνοάμυνας, συμπεριλαμβανομένων των όρων ελέγχου και ασφάλειας, **σεβόμενα τον μη στρατιωτικό χαρακτήρα των θεσμικών οργάνων και τον προορισμό της χρηματοδότησης με επακόλουθη χρήση των κονδυλίων που είναι διαθέσιμα στην κοινότητα άμυνας**. Η ανάπτυξη της ευρωπαϊκής κυβερνοασπίδας θα πρέπει να συνοδεύεται από προβληματισμό που θα επιτρέπει τη μελλοντική συνεργασία με δίκτυα και πλατφόρμες ανταλλαγής πληροφοριών στην κοινότητα κυβερνοάμυνας, σε στενή συνεργασία με τον/την ύπατο/-η εκπρόσωπο **και με πλήρη σεβασμό των δικαιωμάτων και των ελευθεριών**.

Or. en

#### *Αιτιολόγηση*

*Προκειμένου να αποφευχθεί η αλληλεπικάλυψη και να διασφαλιστούν τα δικαιώματα και οι ελευθερίες, η συνεργασία μεταξύ της μη στρατιωτικής και της αμυντικής πλευράς της κυβερνοασφάλειας πρέπει να βασίζεται σε εγγυήσεις, με αποφυγή της αλλαγής προορισμού της μη στρατιωτικής χρηματοδότησης.*

#### **Τροπολογία 65**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 24**

*Κείμενο που προτείνει η Επιτροπή*

(24) Λαμβανομένων υπόψη των αυξανόμενων κινδύνων και του αριθμού των περιστατικών στον κυβερνοχώρο που επηρεάζουν τα κράτη μέλη, είναι αναγκαίο να δημιουργηθεί ένα μέσο στήριξης κρίσεων για τη βελτίωση της ανθεκτικότητας της Ένωσης σε σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας και τη συμπλήρωση των δράσεων των κρατών μελών μέσω χρηματοδοτικής στήριξης έκτακτης ανάγκης της ετοιμότητας, της αντίδρασης και της άμεσης ανάκαμψης βασικών υπηρεσιών. Το μέσο αυτό θα πρέπει να επιτρέπει την ταχεία παροχή βοήθειας σε συγκεκριμένες περιστάσεις και υπό σαφείς προϋποθέσεις και να επιτρέπει την προσεκτική παρακολούθηση και αξιολόγηση του τρόπου με τον οποίο χρησιμοποιήθηκαν οι πόροι. Ενώ η πρόληψη, η ετοιμότητα και η αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας είναι πρωτίστως ευθύνη των κρατών μελών, ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο προωθεί την αλληλεγγύη μεταξύ των κρατών μελών σύμφωνα με το άρθρο 3 παράγραφος 3 της Συνθήκης για την Ευρωπαϊκή Ένωση (στο εξής: ΣΕΕ).

*Τροπολογία*

(24) Λαμβανομένων υπόψη των αυξανόμενων κινδύνων και του αριθμού των περιστατικών στον κυβερνοχώρο που επηρεάζουν τα κράτη μέλη, είναι αναγκαίο να δημιουργηθεί ένα μέσο στήριξης κρίσεων για τη βελτίωση της ανθεκτικότητας της Ένωσης σε σημαντικά και μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας και τη συμπλήρωση των δράσεων των κρατών μελών μέσω χρηματοδοτικής στήριξης έκτακτης ανάγκης της ετοιμότητας, της αντίδρασης και της άμεσης ανάκαμψης βασικών υπηρεσιών. Το μέσο αυτό θα πρέπει να επιτρέπει την ταχεία **και αποτελεσματική** παροχή βοήθειας σε συγκεκριμένες περιστάσεις και υπό σαφείς προϋποθέσεις και να επιτρέπει την προσεκτική παρακολούθηση και αξιολόγηση του τρόπου με τον οποίο χρησιμοποιήθηκαν οι πόροι. Ενώ η πρόληψη, η ετοιμότητα και η αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας είναι πρωτίστως ευθύνη των κρατών μελών, ο μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο προωθεί την αλληλεγγύη μεταξύ των κρατών μελών σύμφωνα με το άρθρο 3 παράγραφος 3 της Συνθήκης για την Ευρωπαϊκή Ένωση (στο εξής: ΣΕΕ).

Or. en

**Τροπολογία 66**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 27**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

(27) Η βοήθεια που παρέχεται δυνάμει του παρόντος κανονισμού θα πρέπει να στηρίζει και να συμπληρώνει τις δράσεις που αναλαμβάνουν τα κράτη μέλη σε εθνικό επίπεδο. Για τον σκοπό αυτό, θα πρέπει να εξασφαλίζεται στενή συνεργασία και διαβούλευση μεταξύ της Επιτροπής και του επηρεαζόμενου κράτους μέλους. Όταν ζητεί στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο, το κράτος μέλος θα πρέπει να παρέχει σχετικές πληροφορίες που αιτιολογούν την ανάγκη στήριξης.

(27) Η βοήθεια που παρέχεται δυνάμει του παρόντος κανονισμού θα πρέπει να στηρίζει και να συμπληρώνει τις δράσεις που αναλαμβάνουν τα κράτη μέλη σε εθνικό επίπεδο. Για τον σκοπό αυτό, θα πρέπει να εξασφαλίζεται στενή συνεργασία και διαβούλευση μεταξύ της Επιτροπής, **του ENISA** και του επηρεαζόμενου κράτους μέλους. Όταν ζητεί στήριξη στο πλαίσιο του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο, το κράτος μέλος θα πρέπει να παρέχει σχετικές πληροφορίες που αιτιολογούν την ανάγκη στήριξης.

Or. en

## Τροπολογία 67

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

### Πρόταση κανονισμού Αιτιολογική σκέψη 33

*Κείμενο που προτείνει η Επιτροπή*

(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

*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 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, **ενώ παράλληλα να ενισχύει την ανθεκτικότητα και την ανταγωνιστικότητα της Ένωσης, συμπεριλαμβανομένης της συμμετοχής ευρωπαϊκών παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας που είναι ΜΜΕ. Αξιόπιστοι πάροχοι, συμπεριλαμβανομένων ΜΜΕ, θα πρέπει να μπορούν να συνεργάζονται μεταξύ**

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.

*τους για την εκπλήρωση των ανωτέρω κριτηρίων.* 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. **Όπου είναι δυνατόν, οι υπηρεσίες θα πρέπει να βασίζονται σε τεχνολογίες αιχμής, συμπεριλαμβανομένων του υπολογιστικού νέφους και της τεχνητής νοημοσύνης. Επομένως, η εφεδρεία στον τομέα της κυβερνοασφάλειας θα πρέπει να παρέχει κίνητρα για την επένδυση στην έρευνα και καινοτομία, ώστε να ενισχυθεί η ανάπτυξη των τεχνολογιών αυτών. Κατά περίπτωση, θα μπορούσαν να λάβουν χώρα κοινές ασκήσεις με τους αξιόπιστους παρόχους και τους πιθανούς χρήστες της εφεδρείας στον τομέα της κυβερνοασφάλειας, προκειμένου να διασφαλιστεί η αποτελεσματική λειτουργία της εφεδρείας όταν υπάρξει η ανάγκη.** 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.

Or. en

## **Τροπολογία 68**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### **Πρόταση κανονισμού**



### Αιτιολογική σκέψη 33

*Κείμενο που προτείνει η Επιτροπή*

(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.

*Τροπολογία*

(33) Θα πρέπει σταδιακά να δημιουργηθεί εφεδρεία στον τομέα της κυβερνοασφάλειας σε επίπεδο Ένωσης, **με αρχική χρηματοδότηση 10 εκατ. EUR δυνάμει του παρόντος κανονισμού έως την αξιολόγηση.** 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. **Η Επιτροπή διασφαλίζει ότι παρόμοιες πρωτοβουλίες εντός του NATO δεν θα επικαλύπτονται μεταξύ τους.**

Or. en

## Αιτιολόγηση

*The Commission foresees a "gradual set up" of the Reserve but this is not reflected in the rest of the proposed Regulation. This amendment therefore proposes to reduce the initial budget for the Reserve from 36 million to 10 million euro until the evaluation of this Regulation. This would return 26 million euro to the Digital Europe Program - Special Objective 4 on Advanced Digital Skills (of the 35 million taken from it). Developing a EU Cybersecurity Reserve next to an existing NATO cyber reserve comes with a high risk of duplication and should not be at the expense of investing more in developing and attracting cybersecurity talent in Europe.*

### Τροπολογία 69

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rares Bogdan**

#### Πρόταση κανονισμού

#### Αιτιολογική σκέψη 35

*Κείμενο που προτείνει η Επιτροπή*

(35) Για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η Επιτροπή **μπορεί να εξετάσει το ενδεχόμενο** να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα πιστοποίησης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 για τις διαχειριζόμενες υπηρεσίες ασφάλειας στους τομείς που καλύπτονται από τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο.

*Τροπολογία*

(35) Για τη στήριξη της δημιουργίας της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η Επιτροπή **θα πρέπει** να ζητήσει από τον ENISA να καταρτίσει υποψήφιο σύστημα πιστοποίησης σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 για τις διαχειριζόμενες υπηρεσίες ασφάλειας στους τομείς που καλύπτονται από τον μηχανισμό έκτακτης ανάγκης στον κυβερνοχώρο.

Or. en

### Τροπολογία 70

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti**

#### Πρόταση κανονισμού

#### Αιτιολογική σκέψη 35 α (νέα)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(35α) Δεδομένων των πρόσθετων καθηκόντων που προβλέπονται στον παρόντα κανονισμό, καθώς και στην [πρόταση σχετικά με οριζόντιες**

*απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία], θα πρέπει να παρασχεθούν στον ENISA οι αναγκαίοι ανθρωπίνοι και δημοσιονομικοί πόροι στο πλαίσιο του προϋπολογισμού της Ένωσης.*

Or. en

### **Τροπολογία 71**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

#### **Πρόταση κανονισμού**

**Αιτιολογική σκέψη 37 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*(37α) Πάροχοι υπηρεσιών αντιμετώπισης περιστατικών από τρίτες χώρες, συμπεριλαμβανομένων χωρών που συνδέονται με τα μέλη του προγράμματος «Ψηφιακή Ευρώπη» ή του NATO ή άλλων ομοφρονουσών χωρών που αποτελούν διεθνείς εταίρους, μπορεί να χρειάζονται για την παροχή συγκεκριμένων υπηρεσιών στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Προκειμένου να ενισχυθούν η ανθεκτικότητα και η κυριαρχία της Ένωσης και να διασφαλιστούν οι στρατηγικοί πόροι, τα συμφέροντα ή η ασφάλεια της Ένωσης, μπορεί να είναι αναγκαίο να περιοριστεί ή να αποκλειστεί η συμμετοχή νομικών οντοτήτων εγκατεστημένων σε μη συνδεδεμένες χώρες ή που ελέγχονται από μη συνδεδεμένες χώρες.*

Or. en

### **Τροπολογία 72**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

**Πρόταση κανονισμού  
Αιτιολογική σκέψη 38 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*(38α) Χρειάζεται υψηλής ειδίκευσης προσωπικό, το οποίο μπορεί να παρέχει αξιόπιστα τις σχετικές υπηρεσίες κυβερνοασφάλειας σύμφωνα με τα υψηλότερα πρότυπα, για την αποτελεσματική υλοποίηση της ευρωπαϊκής κυβερνοασπίδας και του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο. Είναι, συνεπώς, ανησυχητικό ότι η Ένωση αντιμετωπίζει έλλειψη ταλέντων, η οποία χαρακτηρίζεται από έλλειψη εξειδικευμένων επαγγελματιών, ενώ αντιμετωπίζει ένα ραγδαία εξελισσόμενο τοπίο απειλών, όπως αναγνωρίζεται στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, για την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας. Είναι σημαντικό να καλυφθεί η εν λόγω έλλειψη ταλέντων μέσω της ενίσχυσης της συνεργασίας και του συντονισμού μεταξύ των διαφορετικών ενδιαφερόμενων μερών, συμπεριλαμβανομένων του ιδιωτικού τομέα, του ακαδημαϊκού τομέα, των κρατών μελών, της Επιτροπής και του ENISA, για την αναβάθμιση και τη δημιουργία συνεργειών για την επένδυση στην εκπαίδευση και στην κατάρτιση, για την ανάπτυξη εταιρικών σχέσεων μεταξύ δημόσιου και ιδιωτικού τομέα, τη στήριξη πρωτοβουλιών έρευνας και καινοτομίας, την ανάπτυξη και την από κοινού αναγνώριση κοινών προτύπων και πιστοποίησης δεξιοτήτων κυβερνοασφάλειας, μεταξύ άλλων μέσω του ευρωπαϊκού πλαισίου δεξιοτήτων κυβερνοασφάλειας. Αυτό αναμένεται επίσης να διευκολύνει την κινητικότητα των επαγγελματιών στον τομέα της κυβερνοασφάλειας εντός της Ένωσης. Ο παρών κανονισμός θα πρέπει να έχει ως στόχο την προώθηση ενός πιο ποικιλόμορφου εργατικού δυναμικού στον*

**Τροπολογία 73**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού**

**Αιτιολογική σκέψη 38 β (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*(38β) Η οικοδόμηση ικανοτήτων των κρατών μελών είναι σημαντική για μια συντονισμένη προσέγγιση σε επίπεδο Ένωσης, προκειμένου να ενισχυθεί η ανθεκτικότητα της κατάστασης κυβερνοασφάλειας της Ένωσης. Όπως τονίζεται στην ανακοίνωση της Επιτροπής, της 18ης Απριλίου 2023, για την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας, η ασφάλεια της Ένωσης δεν μπορεί να διασφαλιστεί χωρίς τον πιο πολύτιμο πόρο της Ένωσης: τους ανθρώπους της. Το ευρωπαϊκό πλαίσιο δεξιοτήτων κυβερνοασφάλειας μπορεί να βοηθήσει στην καλύτερη κατανόηση της σύνθεσης του εργατικού δυναμικού της Ένωσης, συμπεριλαμβανομένων των υφιστάμενων και των απαιτούμενων ικανοτήτων εντός των συμμετεχουσών οντοτήτων.*

**Τροπολογία 74**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού**

**Αιτιολογική σκέψη 39**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

(39) Ο στόχος του παρόντος κανονισμού μπορεί να επιτευχθεί καλύτερα σε επίπεδο Ένωσης απ' ό,τι από τα κράτη μέλη. Επομένως, η Ένωση μπορεί να θεσπίσει μέτρα σύμφωνα με την αρχή της επικουρικότητας και της αναλογικότητας που ορίζονται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου,

(39) Ο στόχος του παρόντος κανονισμού, **δηλαδή η υπέρβαση των στεγανών στην επικοινωνία και η ενίσχυση των ικανοτήτων πρόληψης, ανίχνευσης, αντιμετώπισης και ανάκαμψης της Ένωσης έναντι απειλών στον κυβερνοχώρο**, μπορεί να επιτευχθεί καλύτερα σε επίπεδο Ένωσης απ' ό,τι από τα κράτη μέλη. Επομένως, η Ένωση μπορεί να θεσπίσει μέτρα σύμφωνα με την αρχή της επικουρικότητας και της αναλογικότητας που ορίζονται στο άρθρο 5 της Συνθήκης για την Ευρωπαϊκή Ένωση. Ο παρών κανονισμός δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη του εν λόγω στόχου,

Or. en

## **Τροπολογία 75** **Nicola Danti**

### **Πρόταση κανονισμού** **Αιτιολογική σκέψη 39 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(39α) Δεδομένων των πρόσθετων καθηκόντων που προβλέπονται στον παρόντα κανονισμό, καθώς και στην [πρόταση σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία], θα πρέπει να παρασχεθούν στον ENISA οι αναγκαίοι ανθρώπινοι και δημοσιονομικοί πόροι στο πλαίσιο του προϋπολογισμού της Ένωσης.**

Or. en

## **Τροπολογία 76** **Johan Nissinen**

### **Πρόταση κανονισμού** **Άρθρο 1 – παράγραφος 1 – εισαγωγικό μέρος**

PE753.628v01-00

30/103

AM\1286499EL.docx

*Κείμενο που προτείνει η Επιτροπή*

1. Ο παρών κανονισμός θεσπίζει μέτρα για την ενίσχυση των ικανοτήτων της Ένωσης να ανιχνεύει, να προετοιμάζεται και να αντιμετωπίζει απειλές και περιστατικά κυβερνοασφάλειας, ιδίως μέσω των ακόλουθων δράσεων:

*Τροπολογία*

1. Ο παρών κανονισμός θεσπίζει μέτρα για την ενίσχυση των ικανοτήτων της Ένωσης να ανιχνεύει, να προετοιμάζεται και να αντιμετωπίζει απειλές και περιστατικά κυβερνοασφάλειας, **ενώ παράλληλα σέβεται το γεγονός ότι η εθνική ασφάλεια, μεταξύ άλλων, στον τομέα της κυβερνοασφάλειας, παραμένει αποκλειστική ευθύνη του κάθε κράτους μέλους, όπως αναφέρεται στο άρθρο 4 παράγραφος 2 της ΣΕΕ**, ιδίως μέσω των ακόλουθων δράσεων:

Or. en

**Τροπολογία 77**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 1 – παράγραφος 1 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

α) ανάπτυξη **πανευρωπαϊκής υποδομής** κέντρων επιχειρήσεων ασφάλειας **(στο εξής: ευρωπαϊκή κυβερνοασπίδα)** για την οικοδόμηση και ενίσχυση κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης,

*Τροπολογία*

α) **ενίσχυση των ομάδων αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές (CSIRT), που αναφέρονται στο άρθρο 10 της οδηγίας (ΕΕ) 2022/2555, και του δικτύου CSIRT, που αναφέρεται στο άρθρο 15 της οδηγίας (ΕΕ) 2022/2555, και ανάπτυξη κέντρων επιχειρήσεων ασφάλειας (SOC) για την οικοδόμηση και ενίσχυση εθνικών και κοινών ικανοτήτων ανίχνευσης και αντίληψης της κατάστασης (ευρωπαϊκή κυβερνοασπίδα),**

Or. en

**Τροπολογία 78**  
**Enĵen Tošenovský**

**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.**

**διαγράφεται**

Or. en

**Τροπολογία 79**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού**  
**Άρθρο 1 – παράγραφος 2 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

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

Or. en

**Τροπολογία 80**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 1 – παράγραφος 2 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

α) την ενίσχυση της κοινής ενωσιακής

α) την ενίσχυση της **εθελοντικής**



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,

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,

Or. en

## **Τροπολογία 81** **Johan Nissinen**

### **Πρόταση κανονισμού** **Άρθρο 1 – παράγραφος 2 – στοιχείο β**

*Κείμενο που προτείνει η Επιτροπή*

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»,

*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 **εθελοντικής συνεργασίας** 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»,

Or. en

## **Τροπολογία 82** **Enžen Tošenovský**

### **Πρόταση κανονισμού** **Άρθρο 1 – παράγραφος 2 – στοιχείο γ**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**γ) την ενίσχυση της ανθεκτικότητας της Ένωσης και τη συμβολή στην αποτελεσματική αντιμετώπιση με την εξέταση και την αξιολόγηση σημαντικών ή μεγάλης κλίμακας περιστατικών, συμπεριλαμβανομένης της άντλησης διδαγμάτων και, κατά περίπτωση, συστάσεων.**

**διαγράφεται**

Or. en

### **Τροπολογία 83**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

#### **Πρόταση κανονισμού**

**Άρθρο 1 – παράγραφος 2 – στοιχείο γ α (νέο)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**γα) την ανάπτυξη και τη βελτίωση δεξιοτήτων και ικανοτήτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας με συντονισμένο τρόπο, μέσω συνεργασίας με την Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας, για την παροχή κατάρτισης και ευκαιριών με στόχο την κάλυψη της έλλειψης ταλέντων στον τομέα της κυβερνοασφάλειας.**

Or. en

### **Τροπολογία 84**

**Johan Nissinen**

#### **Πρόταση κανονισμού**

**Άρθρο 1 - παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**3. Ο παρών κανονισμός δεν θίγει την πρωταρχική ευθύνη των κρατών μελών για**

**3. Ο παρών κανονισμός δεν θίγει την πρωταρχική ευθύνη των κρατών μελών για**

την εθνική ασφάλεια, τη δημόσια ασφάλεια και την πρόληψη, διερεύνηση, εντοπισμό και δίωξη ποινικών αδικημάτων.

την εθνική ασφάλεια, τη δημόσια ασφάλεια και την πρόληψη, διερεύνηση, εντοπισμό και δίωξη ποινικών αδικημάτων, **και αποτρέπει περιττές αλληλοεπικαλύψεις με υφιστάμενες πρωτοβουλίες.**

Or. en

**Τροπολογία 85**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 1 - παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

3. Ο παρών κανονισμός δεν θίγει την **πρωταρχική ευθύνη** των κρατών μελών **για την** εθνική ασφάλεια, τη δημόσια ασφάλεια και την πρόληψη, διερεύνηση, εντοπισμό και δίωξη ποινικών αδικημάτων.

*Τροπολογία*

3. Ο παρών κανονισμός δεν θίγει την **αποκλειστική αρμοδιότητα** των κρατών **στην** εθνική ασφάλεια, τη δημόσια ασφάλεια και την πρόληψη, διερεύνηση, εντοπισμό και δίωξη ποινικών αδικημάτων.

Or. en

**Τροπολογία 86**  
**Nicola Danti**

**Πρόταση κανονισμού**  
**Άρθρο 1 – παράγραφος 3 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**3a. Κάθε έτος, κατά την υποβολή του σχεδίου προϋπολογισμού για το επόμενο έτος, η Επιτροπή υποβάλλει λεπτομερή αξιολόγηση των καθηκόντων του ENISA δυνάμει του παρόντος κανονισμού, καθώς και [της πρότασης σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία] και άλλων νομοθετικών πράξεων της Ένωσης, και περιγράφει λεπτομερώς τους δημοσιονομικούς και ανθρωπίνους**

**Τροπολογία 87**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 1**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(1)** «διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής: διασυνοριακό SOC): πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την πρόληψη απειλών και περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον·

*διαγράφεται*

**Τροπολογία 88**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 1**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(1)** «διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής:

**(1)** «διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής:

διασυνοριακό SOC): πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την **πρόληψη** απειλών και περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον·

διασυνοριακό SOC): πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την **ανίχνευση και την ανάλυση** απειλών και **την πρόληψη** περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον·

Or. en

## Τροπολογία 89 Johan Nissinen

### Πρόταση κανονισμού Άρθρο 2 – παράγραφος 1 – σημείο 1

*Κείμενο που προτείνει η Επιτροπή*

(1) «διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής: διασυνοριακό SOC): πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την πρόληψη απειλών και περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο

*Τροπολογία*

(1) «διασυνοριακό κέντρο επιχειρήσεων ασφάλειας» (στο εξής: διασυνοριακό SOC): πολυεθνική πλατφόρμα που συγκεντρώνει σε μια συντονισμένη δομή δικτύου τα εθνικά SOC από τουλάχιστον τρία κράτη μέλη που συγκροτούν κοινοπραξία υποδοχής, και η οποία έχει σχεδιαστεί για την πρόληψη απειλών και περιστατικών στον κυβερνοχώρο και για την υποστήριξη της παραγωγής πληροφοριών υψηλής ποιότητας, ιδίως μέσω της **εθελοντικής** ανταλλαγής δεδομένων από διάφορες πηγές, δημόσιες και ιδιωτικές, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης, πρόληψης και προστασίας στον κυβερνοχώρο σε ένα

περιβάλλον·

αξιόπιστο περιβάλλον·

Or. en

### Τροπολογία 90

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

#### Πρόταση κανονισμού

Άρθρο 2 – παράγραφος 1 – σημείο 1 α (νέο)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*1α) «κέντρο επιχειρήσεων ασφάλειας» (στο εξής: SOC): κεντρική ικανότητα, η οποία μπορεί να είναι ενδοεπιχειρησιακή ή να έχει ανατεθεί εξωτερικά, η οποία είναι υπεύθυνη για τη συνεχή παρακολούθηση και βελτίωση της κατάστασης της κυβερνοασφάλειας μιας οντότητας, για την πρόληψη, την ανίχνευση, την ανάλυση, καθώς και την αντιμετώπιση απειλών στον κυβερνοχώρο.*

Or. en

### Τροπολογία 91

Enĵen Tošenovský

#### Πρόταση κανονισμού

Άρθρο 2 – παράγραφος 1 – σημείο 1 α (νέο)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*1α) «κέντρο επιχειρήσεων ασφάλειας» (στο εξής: SOC): κέντρο, το οποίο έχει ιδρυθεί από ιδιωτικές και δημόσιες οντότητες ή εθνικές αρχές, το οποίο συνεχώς παρακολουθεί και αναλύει τα δίκτυα επικοινωνίας και τα συστήματα πληροφορικής για την ανίχνευση παραβιάσεων και ανωμαλιών σε πραγματικό χρόνο.*

## Τροπολογία 92

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

Άρθρο 2 – παράγραφος 1 – σημείο 1 β (νέο)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**1β) «εθνικό κέντρο επιχειρήσεων ασφάλειας» (στο εξής: εθνικό SOC): κεντρική ικανότητα για τη συνεχή συλλογή πληροφοριών για απειλές και για τη βελτίωση της κατάστασης κυβερνοασφάλειας οντοτήτων υπό εθνική δικαιοδοσία μέσω της πρόληψης, της ανίχνευσης και της ανάλυσης απειλών κυβερνοασφάλειας, για την καλύτερη αντιμετώπιση απειλών κυβερνοασφάλειας. Η ικανότητα αυτή, κατά περίπτωση, ενσωματώνεται σε ήδη υφιστάμενες εθνικές δομές όπως οι CSIRT, όπως συστήνονται δυνάμει της οδηγίας 2022/2555.**

Or. en

## Τροπολογία 93

Enĵen Tošenovský

### Πρόταση κανονισμού

Άρθρο 2 – παράγραφος 1 – σημείο 2

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(2) «δημόσιος φορέας»: φορέας δημοσίου δικαίου, όπως ορίζεται στο άρθρο 2 παράγραφος 1 σημείο 4) της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>30</sup>.**

**(2) «οντότητα δημόσιας διοίκησης»: οντότητα δημόσιας διοίκησης, όπως ορίζεται στο άρθρο 6 σημείο 35) της οδηγίας (ΕΕ) 2022/2555.**

<sup>30</sup> Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της

26ης Φεβρουαρίου 2014, σχετικά με τις διαδικασίες σύναψης δημοσίων συμβάσεων και την κατάργηση της οδηγίας 2004/18/EK (EE L 94 της 28.3.2014, σ. 65).

Or. en

**Τροπολογία 94**  
Enĵen Tošenovský

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 3**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(3) «κοινοπραξία υποδοχής»:**  
**κοινοπραξία αποτελούμενη από συμμετέχοντα κράτη, εκπροσωπούμενα από εθνικά SOC, τα οποία έχουν συμφωνήσει να δημιουργήσουν και να συμβάλουν στην αγορά εργαλείων και υποδομών για ένα διασυνοριακό SOC και στη λειτουργία αυτού·**

*διαγράφεται*

Or. en

**Τροπολογία 95**  
Enĵen Tošenovský

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 5 α (νέο)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**5α) «χειρισμός περιστατικών»:** ο χειρισμός περιστατικών όπως ορίζεται στο άρθρο 6 σημείο 8) της οδηγίας (EE) 2022/2555·

Or. en

**Τροπολογία 96**



Enĵen Toĥenovský

Πρόταση κανονισμού  
Άρθρο 2 – παράγραφος 1 – σημείο 5 β (νέο)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**5β) «κίνδυνος»:** κίνδυνος όπως ορίζεται στο άρθρο 6 σημείο 9 της οδηγίας (ΕΕ) 2022/2555·

Or. en

Τροπολογία 97  
Enĵen Toĥenovský

Πρόταση κανονισμού  
Άρθρο 2 – παράγραφος 1 – σημείο 6 α (νέο)

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**6α) «σημαντική κυβερνοαπειλή»:** κυβερνοαπειλή όπως ορίζεται στο άρθρο 6 σημείο 11) της οδηγίας (ΕΕ) 2022/2555·

Or. en

Τροπολογία 98  
Enĵen Toĥenovský

Πρόταση κανονισμού  
Άρθρο 2 – παράγραφος 1 – σημείο 9

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**(9) «ετοιμότητα»:** κατάσταση ετοιμότητας και ικανότητας για τη διασφάλιση αποτελεσματικής ταχείας αντίδρασης σε σημαντικό ή μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, η οποία επιτυγχάνεται ως αποτέλεσμα των δράσεων εκτίμησης κινδύνων και παρακολούθησης που λαμβάνονται εκ των προτέρων·

**διαγράφεται**

**Τροπολογία 99**  
**EnĽen ToĽenovskŷ**

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 10**

*Κείμενο που προτείνει η Επιτροπή*

**(10) «αντιμετώπιση»: δράση σε περίπτωση σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, ή κατά τη διάρκεια ή μετά το περιστατικό αυτό, για την αντιμετώπιση των άμεσων και βραχυπρόθεσμων δυσμενών συνεπειών του·**

*Τροπολογία*

**διαγράφεται**

**Τροπολογία 100**  
**EnĽen ToĽenovskŷ**

**Πρόταση κανονισμού**  
**Άρθρο 2 – παράγραφος 1 – σημείο 11**

*Κείμενο που προτείνει η Επιτροπή*

**(11) «αξιόπιστοι πάροχοι»: πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας, όπως ορίζονται στο άρθρο 6 σημείο 40 της οδηγίας (ΕΕ) 2022/2555, οι οποίοι επιλέγονται σύμφωνα με το άρθρο 16 του παρόντος κανονισμού.**

*Τροπολογία*

**(11) «αξιόπιστοι πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας»: πάροχοι διαχειριζόμενων υπηρεσιών ασφάλειας, όπως ορίζονται στο άρθρο 6 σημείο 40 της οδηγίας (ΕΕ) 2022/2555, οι οποίοι επιλέγονται *ώστε να συμπεριληφθούν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας* σύμφωνα με το άρθρο 16 του παρόντος κανονισμού.**

**Τροπολογία 101**

## **Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### **Πρόταση κανονισμού**

#### **Άρθρο 3 – παράγραφος 1 – εδάφιο 1**

*Κείμενο που προτείνει η Επιτροπή*

Θεσπίζεται διασυνδεδεμένη πανευρωπαϊκή υποδομή κέντρων επιχειρήσεων ασφάλειας (στο εξής: ευρωπαϊκή κυβερνοασπίδα) με σκοπό την ανάπτυξη προηγμένων ικανοτήτων της Ένωσης για την ανίχνευση, την ανάλυση και την επεξεργασία δεδομένων σχετικά με απειλές και **περιστατικά** στον κυβερνοχώρο στην Ένωση. Η κυβερνοασπίδα αποτελείται από το σύνολο των εθνικών κέντρων επιχειρήσεων ασφάλειας (στο εξής: εθνικά SOC) και των διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (στο εξής: διασυνοριακά SOC).

*Τροπολογία*

Θεσπίζεται διασυνδεδεμένη πανευρωπαϊκή υποδομή κέντρων επιχειρήσεων ασφάλειας (στο εξής: ευρωπαϊκή κυβερνοασπίδα) με σκοπό την ανάπτυξη προηγμένων ικανοτήτων της Ένωσης για την ανίχνευση, την ανάλυση και την επεξεργασία δεδομένων σχετικά με απειλές και **την πρόληψη περιστατικών** στον κυβερνοχώρο στην Ένωση. Η κυβερνοασπίδα αποτελείται από το σύνολο των εθνικών κέντρων επιχειρήσεων ασφάλειας (στο εξής: εθνικά SOC) και των διασυνοριακών κέντρων επιχειρήσεων ασφάλειας (στο εξής: διασυνοριακά SOC).

Or. en

### **Τροπολογία 102**

**Johan Nissinen**

### **Πρόταση κανονισμού**

#### **Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

α) συγκεντρώνει και επιτρέπει την ανταλλαγή δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο από διάφορες πηγές μέσω **διασυνοριακών** SOC,

*Τροπολογία*

α) συγκεντρώνει και επιτρέπει την ανταλλαγή δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο από διάφορες πηγές μέσω **εθελοντικής ανταλλαγής πληροφοριών από διασυνοριακά** SOC,

Or. en

### **Τροπολογία 103**

**Enžen Tošenovský**

### **Πρόταση κανονισμού**

### Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο α

*Κείμενο που προτείνει η Επιτροπή*

α) συγκεντρώνει και επιτρέπει την ανταλλαγή δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο από διάφορες πηγές μέσω διασυνοριακών SOC,

*Τροπολογία*

α) συγκεντρώνει και επιτρέπει την ανταλλαγή δεδομένων σχετικά με απειλές και περιστατικά στον κυβερνοχώρο από διάφορες πηγές μέσω διασυνοριακών SOC **τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο,**

Or. en

### Τροπολογία 104

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

### Πρόταση κανονισμού

### Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο γ

*Κείμενο που προτείνει η Επιτροπή*

γ) συμβάλλει στην καλύτερη προστασία και αντιμετώπιση των κυβερνοαπειλών,

*Τροπολογία*

γ) συμβάλλει στην καλύτερη προστασία και αντιμετώπιση των κυβερνοαπειλών, **μεταξύ άλλων μέσω της παροχής συγκεκριμένων συστάσεων σε οντότητες,**

Or. en

### Τροπολογία 105

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

### Πρόταση κανονισμού

### Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο δ

*Κείμενο που προτείνει η Επιτροπή*

δ) συμβάλλει στην ταχύτερη ανίχνευση των κυβερνοαπειλών και στην αντίληψη της κατάστασης σε ολόκληρη την Ένωση,

*Τροπολογία*

δ) συμβάλλει στην ταχύτερη ανίχνευση των κυβερνοαπειλών και στην αντίληψη της κατάστασης σε ολόκληρη την Ένωση, **μεταξύ άλλων μέσω της συλλογής προορατικών πληροφοριών,**

**Τροπολογία 106**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 3 – παράγραφος 2 – εδάφιο 1 – στοιχείο ε**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

ε) παρέχει υπηρεσίες και δραστηριότητες για την κοινότητα κυβερνοασφάλειας στην Ένωση, μεταξύ άλλων συμβάλλοντας στην ανάπτυξη προηγμένων εργαλείων τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

*(Δεν αφορά το ελληνικό κείμενο.)*

**Τροπολογία 107**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 4 – τίτλος**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*Εθνικά κέντρα επιχειρήσεων ασφάλειας*

*Ενισχυμένη συνεργασία και ανταλλαγή πληροφοριών σε εθνικό επίπεδο*

**Τροπολογία 108**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 4 – παράγραφος 1 – εδάφιο 1**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

Για να *συμμετάσχει* στην ευρωπαϊκή κυβερνοασπίδα, κάθε κράτος μέλος ορίζει *τουλάχιστον ένα εθνικό SOC. Το εθνικό*

Για να *συμβάλει* στην ευρωπαϊκή κυβερνοασπίδα, κάθε κράτος μέλος ορίζει *μία από τις ομάδες αντιμετώπισης περιστατικών ασφάλειας σε υπολογιστές*

*SOC είναι δημόσιος φορέας.*

*(CSIRT), όπως αναφέρεται στο άρθρο 10 της οδηγίας (ΕΕ) 2022/2555, ως κέντρο ανταλλαγής και ανάλυσης πληροφοριών (ISAC).*

Or. en

**Τροπολογία 109**  
**Enžhen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 4 – παράγραφος 1 – εδάφιο 1 α (νέο)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*Ιδιωτικοί και δημόσιοι οργανισμοί ή εθνικές αρχές, ιδίως οντότητες που δραστηριοποιούνται σε τομείς κρίσιμης ή εξαιρετικά κρίσιμης σημασίας, ενθαρρύνονται να συστήσουν και να θέσουν σε λειτουργία οικεία αυτόνομα ή κοινά SOC.*

Or. en

**Τροπολογία 110**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές κυβερνοασφάλειας και για τη συμβολή σε διασυνοριακό SOC. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας. **Το εθνικό SOC ή η εθνική CSIRT μπορεί να ζητήσει από**

*αξιόπιστους παρόχους ή παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας δεδομένα τηλεμετρίας, αισθητήρων ή καταχωρίσεων τα οποία αφορούν τομείς εξαιρετικής κρισιμότητας, όπως ορίζονται στην 2022/2555. Τα εν λόγω δεδομένα μπορούν να κοινοποιηθούν μόνο για τη στήριξη των καθηκόντων και των ευθυνών του εθνικού SOC ή της εθνικής CSIRT στην ανίχνευση και πρόληψη περιστατικών κυβερνοασφάλειας.*

Or. en

**Τροπολογία 111**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 4 – παράγραφος 1 – εδάφιο 2**

*Κείμενο που προτείνει η Επιτροπή*

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 διασυννοριακό SOC**. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.

*Τροπολογία*

Έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη **κυρίως** προς **SOC που έχουν συσταθεί από ιδιωτικές και δημόσιες οντότητες ή εθνικές αρχές, άλλες CSIRT του ίδιου κράτους μέλους, ως συντονιστές για τη διαχείριση περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας, καθώς και προς** άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο για τη συλλογή και ανάλυση πληροφοριών σχετικά με απειλές και περιστατικά κυβερνοασφάλειας και, **κατά περίπτωση, για την ανταλλαγή των πληροφοριών αυτών με άλλα μέλη του δικτύου CSIRT**. Είναι εφοδιασμένο με προηγμένες τεχνολογίες ανίχνευσης, συγκέντρωσης και ανάλυσης δεδομένων σχετικών με απειλές και περιστατικά κυβερνοασφάλειας.

Or. en

## Τροπολογία 112

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rares Bogdan

### Πρόταση κανονισμού

#### Άρθρο 4 – παράγραφος 1 – εδάφιο 2

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

Έχει την ικανότητα να λειτουργεί ως σημείο αναφοράς και πύλη προς άλλους δημόσιους και ιδιωτικούς οργανισμούς σε εθνικό επίπεδο, **ιδίως προς τα SOC τους**, 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.

Or. en

## Τροπολογία 113

Enĵen Tošenovský

### Πρόταση κανονισμού

#### Άρθρο 4 – παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

**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**

*Τροπολογία*

**διαγράφεται**



*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.*

Or. en

## **Τροπολογία 114**

**Ville Niinistö**

εξ ονόματος της Ομάδας Verts/ALE

### **Πρόταση κανονισμού**

#### **Άρθρο 4 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, τα εθνικά SOC **μπορούν να** 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.

Or. en

## Αιτιολόγηση

Η απολυτότητα του «επιλέγονται» δεν συνάδει με την έννοια της πρόσκλησης εκδήλωσης ενδιαφέροντος και των διαδικασιών επιλογής. Εκ φύσεως τα SOC μπορούν να συμμετάσχουν και να επιλεγούν.

### Τροπολογία 115 EnĽen ToĽenovský

#### Πρόταση κανονισμού Άρθρο 4 – παράγραφος 3

*Κείμενο που προτείνει η Επιτροπή*

**3. Το εθνικό SOC που επιλέγεται σύμφωνα με την παράγραφο 2 δεσμεύεται να υποβάλει αίτηση συμμετοχής σε διασυνοριακό SOC εντός δύο ετών από την ημερομηνία αγοράς των εργαλείων και των υποδομών ή από την ημερομηνία κατά την οποία λαμβάνει επιχορήγηση, όποιο από τα δύο συμβεί νωρίτερα. Εάν ένα εθνικό SOC δεν συμμετέχει μέχρι τότε σε διασυνοριακό SOC, δεν είναι επιλέξιμο για πρόσθετη στήριξη της Ένωσης δυνάμει του παρόντος κανονισμού.**

*Τροπολογία*

**διαγράφεται**

Or. en

### Τροπολογία 116 EnĽen ToĽenovský

#### Πρόταση κανονισμού Άρθρο 5 – τίτλος

*Κείμενο που προτείνει η Επιτροπή*

**Διασυνοριακά κέντρα επιχειρήσεων ασφάλειας**

*Τροπολογία*

**Κοινή διαδικασία προμηθειών εργαλείων και υποδομών**

Or. en

### Τροπολογία 117 EnĽen ToĽenovský

**Πρόταση κανονισμού**  
**Άρθρο 5 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

**1. Κοινοπραξία υποδοχής**  
**αποτελούμενη από τουλάχιστον τρία**  
**κράτη μέλη, εκπροσωπούμενα από εθνικά**  
**SOC, που δεσμεύονται να συνεργαστούν**  
**για τον συντονισμό των δραστηριοτήτων**  
**τους με σκοπό την ανίχνευση και την**  
**παρακολούθηση απειλών στον**  
**κυβερνοχώρο, είναι επιλέξιμη για**  
**συμμετοχή σε δράσεις για τη δημιουργία**  
**διασυννοριακού SOC.**

*Τροπολογία*

**διαγράφεται**

Or. en

**Τροπολογία 118**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 5 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

**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**

*Τροπολογία*

**2. Κατόπιν πρόσκλησης εκδήλωσης**  
**ενδιαφέροντος, οι CSIRT-ISAC μπορούν**  
**να επιλέγονται από το ECCC για να**  
**συμμετάσχουν σε κοινή διαδικασία**  
**προμήθειας εργαλείων και υποδομών με το**  
**ECCC. Το ECCC μπορεί να χορηγεί στις**  
**CSIRT-ISAC 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**  
**τις CSIRT-ISAC. Πριν από την έναρξη της**  
**διαδικασίας αγοράς των εργαλείων και των**  
**υποδομών, το ECCC και οι CSIRT-ISAC**  
**που συμμετέχουν συνάπτουν συμφωνία**  
**υποδοχής και χρήσης που ρυθμίζει τη**  
**χρήση των εργαλείων και των υποδομών,**

υποδομών.

*συμπεριλαμβανομένης της χρήσης τους από άλλες CSIRT και άλλα SOC στο εν λόγω κράτος μέλος.*

Or. en

## Τροπολογία 119

Ville Niinistö

εξ ονόματος της Ομάδας Verts/ALE

### Πρόταση κανονισμού

#### Άρθρο 5 – παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

2. Κατόπιν πρόσκλησης εκδήλωσης ενδιαφέροντος, η κοινοπραξία υποδοχής **μπορεί να** 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.

Or. en

#### *Αιτιολόγηση*

*Ενώ ο παρών κανονισμός δεν περιλαμβάνει σαφή κριτήρια, άλλη ισχύουσα νομοθεσία μπορεί να μειώσει τη βεβαιότητα ότι ένας/κάθε αιτών είναι επιτυχών.*

## Τροπολογία 120

**Πρόταση κανονισμού  
Άρθρο 5 – παράγραφος 2 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**2α. Η προμήθεια από ιδιωτική οντότητα που είναι εγκατεστημένη σε ομοφρονούσα τρίτη χώρα και η συμμετοχή της θα πρέπει να επιτρέπονται, αν αυτό δεν αντιβαίνει στα συμφέροντα ασφάλειας και άμυνας της Ένωσης και των κρατών μελών, όπως ορίζεται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας δυνάμει του τίτλου V της ΣΕΕ, ή στους στόχους που ορίζονται στον παρόντα κανονισμό. Οι εν λόγω ιδιωτικές οντότητες δεν θα πρέπει να ελέγχονται από μη συνδεδεμένη τρίτη χώρα ή έχουν υποβληθεί σε έλεγχο υπό την έννοια του κανονισμού (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.**

Or. en

**Τροπολογία 121  
Enĵen Tošenovský**

**Πρόταση κανονισμού  
Άρθρο 5 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**3. Τα μέλη της κοινοπραξίας υποδοχής συνάπτουν γραπτή συμφωνία κοινοπραξίας στην οποία καθορίζονται οι εσωτερικές τους ρυθμίσεις όσον αφορά την εφαρμογή της συμφωνίας υποδοχής και χρήσης.**

**διαγράφεται**

Or. en

**Τροπολογία 122**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 5 – παράγραφος 4**

*Κείμενο που προτείνει η Επιτροπή*

**4. Ένα διασυνοριακό SOC εκπροσωπείται για νομικούς σκοπούς από ένα εθνικό SOC που ενεργεί ως SOC συντονισμού ή από την κοινοπραξία υποδοχής, εάν αποτελεί νομικό πρόσωπο. Το SOC συντονισμού είναι υπεύθυνο για τη συμμόρφωση προς τις απαιτήσεις της συμφωνίας υποδοχής και χρήσης και του παρόντος κανονισμού.**

*Τροπολογία*

*διαγράφεται*

Or. en

**Τροπολογία 123**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 6 – τίτλος**

*Κείμενο που προτείνει η Επιτροπή*

**Συνεργασία και ανταλλαγή πληροφοριών εντός και μεταξύ διασυνοριακών SOC**

*Τροπολογία*

**Ενισχυμένη** συνεργασία και ανταλλαγή πληροφοριών **σε ενωσιακό επίπεδο**

Or. en

**Τροπολογία 124**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 6 – παράγραφος 1 – εισαγωγικό μέρος**

*Κείμενο που προτείνει η Επιτροπή*

1. Τα μέλη μιας κοινοπραξίας υποδοχής ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες στο πλαίσιο της διασυνοριακής SOC,

*Τροπολογία*

1. Τα μέλη μιας κοινοπραξίας υποδοχής **μπορούν να** ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες στο πλαίσιο της διασυνοριακής SOC,

συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτά σημεία, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτά σημεία, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

Or. en

## **Τροπολογία 125** **Enĵen Tošenovský**

### **Πρόταση κανονισμού** **Άρθρο 6 – παράγραφος 1 – εισαγωγικό μέρος**

*Κείμενο που προτείνει η Επιτροπή*

1. **Τα μέλη μιας κοινοπραξίας υποδοχής** ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες στο πλαίσιο **της διασυννοριακής SOC**, συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτά σημεία, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

*Τροπολογία*

1. **Οι CSIRT-ISAC και άλλες CSIRT** ανταλλάσσουν μεταξύ τους σχετικές πληροφορίες στο πλαίσιο **του δικτύου CSIRT**, συμπεριλαμβανομένων πληροφοριών που αφορούν κυβερνοαπειλές, παρ' ολίγον περιστατικά, τρωτά σημεία, τεχνικές και διαδικασίες, ενδείξεις της παραβίασης, εχθρικές τακτικές, πληροφορίες που αφορούν συγκεκριμένους παράγοντες απειλής, προειδοποιήσεις για την κυβερνοασφάλεια και συστάσεις σχετικά με την παραμετροποίηση εργαλείων κυβερνοασφάλειας για τον εντοπισμό κυβερνοεπιθέσεων, στον βαθμό που η εν λόγω ανταλλαγή πληροφοριών:

Or. en

## **Τροπολογία 126** **Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 6 – παράγραφος 1 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

α) **αποσκοπεί στην** πρόληψη, τον εντοπισμό, **την αντιμετώπιση ή την ανάκαμψη από περιστατικά ή στον** μετριασμό **των επιπτώσεών τους,**

*Τροπολογία*

α) **βελτιώνει την ανταλλαγή πληροφοριών για απειλές στον κυβερνοχώρο μεταξύ SOC και ISAC της βιομηχανίας με στόχο την** πρόληψη, τον εντοπισμό ή **τον μετριασμό περιστατικών,**

Or. en

**Τροπολογία 127**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 6 – παράγραφος 2 – εισαγωγικό μέρος**

*Κείμενο που προτείνει η Επιτροπή*

2. **Στην γραπτή** συμφωνία **κοινοπραξίας που αναφέρεται στο άρθρο 5 παράγραφος 3** καθορίζονται τα ακόλουθα:

*Τροπολογία*

2. **Στη** συμφωνία **ανταλλαγής πληροφοριών και στοιχείων μεταξύ CSIRT-ISAC, ή κατά περίπτωση, άλλων CSIRT, μπορούν να** καθορίζονται τα ακόλουθα:

Or. en

**Τροπολογία 128**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 6 – παράγραφος 2 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

α) δέσμευση για ανταλλαγή **σημαντικού όγκου** δεδομένων που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται οι εν λόγω πληροφορίες,

*Τροπολογία*

α) δέσμευση για **εθελοντική** ανταλλαγή δεδομένων που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται οι εν λόγω πληροφορίες,

Or. en



## Τροπολογία 129

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

### Πρόταση κανονισμού

#### Άρθρο 6 – παράγραφος 2 – στοιχείο α

*Κείμενο που προτείνει η Επιτροπή*

α) δέσμευση για ανταλλαγή **σημαντικού όγκου** δεδομένων που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται οι εν λόγω πληροφορίες,

*Τροπολογία*

α) δέσμευση για ανταλλαγή **σημαντικών** δεδομένων που αναφέρονται στην παράγραφο 1 και οι προϋποθέσεις υπό τις οποίες πρέπει να ανταλλάσσονται οι εν λόγω πληροφορίες,

Or. en

## Τροπολογία 130

Enĵen Tošenovský

### Πρόταση κανονισμού

#### Άρθρο 6 – παράγραφος 3

*Κείμενο που προτείνει η Επιτροπή*

**3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους. Για τη διευκόλυνση της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC, η Επιτροπή μπορεί, με εκτελεστικές πράξεις, αφού ζητήσει τη γνώμη του ECCC, να καθορίζει τους όρους της εν λόγω διαλειτουργικότητας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.**

*Τροπολογία*

**διαγράφεται**

Or. en

## Τροπολογία 131

**Πρόταση κανονισμού  
Άρθρο 6 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους. Για τη διευκόλυνση της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC, **η Επιτροπή μπορεί, με εκτελεστικές πράξεις, αφού ζητήσει τη γνώμη του ECCC, να καθορίζει** τους όρους της εν λόγω διαλειτουργικότητας. Οι εν λόγω **εκτελεστικές** πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

*Τροπολογία*

3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC **και με ISAC της βιομηχανίας**, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας μεταξύ τους **και, όπου είναι δυνατόν, με βιομηχανικά ISAC**. Για τη διευκόλυνση της διαλειτουργικότητας μεταξύ των διασυνοριακών SOC **και με ISAC της βιομηχανίας, τα πρότυπα και πρωτόκολλα ανταλλαγής πληροφοριών θα πρέπει να εναρμονιστούν με τα διεθνή πρότυπα και τις βέλτιστες πρακτικές της βιομηχανίας. Το ECCC μπορεί να ζητήσει από την** Επιτροπή **να προτείνει με κατ' εξουσιοδότηση** πράξεις τους όρους της εν λόγω διαλειτουργικότητας **σε στενή συνεργασία με τα περιφερειακά SOC και με βάση τα διεθνή πρότυπα και τις βέλτιστες πρακτικές της βιομηχανίας**. Οι εν λόγω **κατ' εξουσιοδότηση** πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

Or. en

**Τροπολογία 132**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan**

**Πρόταση κανονισμού  
Άρθρο 6 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας

*Τροπολογία*

3. Για να ενθαρρυνθεί η ανταλλαγή πληροφοριών μεταξύ των διασυνοριακών SOC, τα διασυνοριακά SOC εξασφαλίζουν υψηλό επίπεδο διαλειτουργικότητας

μεταξύ τους. **Για τη διευκόλυνση της διαλειτουργικότητας** μεταξύ των διασυνοριακών SOC, η Επιτροπή μπορεί, με εκτελεστικές πράξεις, αφού ζητήσει τη γνώμη του ECCC, να καθορίζει τους όρους της εν λόγω διαλειτουργικότητας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

μεταξύ τους. **Η κοινή διαδικασία προμηθειών υποδομών, υπηρεσιών και εργαλείων στον τομέα του κυβερνοχώρου μπορεί να διευκολύνει τη διαλειτουργικότητα** μεταξύ των διασυνοριακών SOC. **Για τον καθορισμό των όρων διαλειτουργικότητας μεταξύ των διασυνοριακών SOC**, η Επιτροπή μπορεί, με εκτελεστικές πράξεις, αφού ζητήσει τη γνώμη του ECCC **και του ENISA**, να καθορίζει τους όρους της εν λόγω διαλειτουργικότητας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

Or. en

### Τροπολογία 133 Enĵen Tošepnovský

#### Πρόταση κανονισμού Άρθρο 6 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

**4. Τα διασυνοριακά SOC συνάπτουν μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών πλατφορμών.**

*Τροπολογία*

**διαγράφεται**

Or. en

### Τροπολογία 134 Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

#### Πρόταση κανονισμού Άρθρο 6 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

4. Τα διασυνοριακά SOC συνάπτουν

*Τροπολογία*

4. Τα διασυνοριακά SOC συνάπτουν

μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών πλατφορμών.

μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών πλατφορμών, λαμβάνοντας υπόψη τους ήδη υφιστάμενους σχετικούς μηχανισμούς ανταλλαγής πληροφοριών βάσει της οδηγίας (ΕΕ) 2022/2555. Στο πλαίσιο πιθανού ή εν εξελίξει μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας, οι μηχανισμοί ανταλλαγής πληροφοριών συμμορφώνονται με τις σχετικές διατάξεις της οδηγίας (ΕΕ) 2022/2555.

Or. en

### Τροπολογία 135

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

#### Πρόταση κανονισμού

#### Άρθρο 6 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

4. Τα διασυνοριακά SOC συνάπτουν μεταξύ τους συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών μεταξύ των διασυνοριακών πλατφορμών.

*Τροπολογία*

4. Τα διασυνοριακά SOC συνάπτουν μεταξύ τους **και με ISAC της βιομηχανίας** συμφωνίες συνεργασίας, στις οποίες καθορίζονται οι αρχές ανταλλαγής πληροφοριών **και διαλειτουργικότητας** μεταξύ των διασυνοριακών πλατφορμών.

Or. en

### Τροπολογία 136

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

#### Πρόταση κανονισμού

#### Άρθρο 7 – τίτλος

*Κείμενο που προτείνει η Επιτροπή*

Συνεργασία και ανταλλαγή πληροφοριών με **οντότητες της Ένωσης**

*Τροπολογία*

Συνεργασία και ανταλλαγή πληροφοριών με **το δίκτυο CSIRT**

Or. en

## Τροπολογία 137

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

### Πρόταση κανονισμού

#### Άρθρο 7 – παράγραφος 1

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

1. Όταν τα διασυνοριακά SOC λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας **για τον σκοπό της κοινής αντίληψης της κατάστασης, το SOC συντονισμού παρέχει** σχετικές πληροφορίες **στην CSIRT του ή στην αρμόδια αρχή, οι οποίες τις υποβάλλουν** στο EU-CyCLONe, στο δίκτυο CSIRT και στην Επιτροπή, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων **και τις διαδικασίες** σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

Or. en

*Αιτιολόγηση*

*Πρόταση να διατηρηθεί η διαδικασία της NIS2 για μεγάλης κλίμακας περιστατικά.*

## Τροπολογία 138

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan

### Πρόταση κανονισμού

#### Άρθρο 7 – παράγραφος 1

*Κείμενο που προτείνει η Επιτροπή*

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,

*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, στην Επιτροπή **και στον**

*λαμβανομένων υπόψη των αντίστοιχων ρόλων* τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

*ENISA, σύμφωνα με τους αντίστοιχους ρόλους* τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

Or. en

**Τροπολογία 139**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 7 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

1. Όταν *τα διασυννοριακά 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.

*Τροπολογία*

1. Όταν *οι CSIRT-ISAC* λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό στον τομέα της κυβερνοασφάλειας, παρέχουν σχετικές πληροφορίες στο EU-CyCLONe *και* στο δίκτυο CSIRT, λαμβανομένων υπόψη των αντίστοιχων ρόλων τους όσον αφορά τη διαχείριση κρίσεων σύμφωνα με την οδηγία (ΕΕ) 2022/2555, χωρίς αδικαιολόγητη καθυστέρηση.

Or. en

**Τροπολογία 140**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 7 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

2. *Η Επιτροπή δύναται να καθορίζει, με εκτελεστικές πράξεις, τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται*

*Τροπολογία*

*διαγράφεται*

*σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.*

Or. en

## **Τροπολογία 141**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### **Πρόταση κανονισμού**

#### **Άρθρο 7 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

2. Η Επιτροπή δύναται να καθορίζει, με εκτελεστικές πράξεις, τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

*Τροπολογία*

2. Η Επιτροπή δύναται, **αφού ζητήσει τη γνώμη των διασυνοριακών πλατφορμών και του δικτύου CSIRT**, να καθορίζει, με εκτελεστικές πράξεις, τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού **και σύμφωνα με την οδηγία (ΕΕ) 2022/2555**.

Or. en

### *Αιτιολόγηση*

*Πρόταση να διατηρηθεί η διαδικασία της NIS2 για μεγάλης κλίμακας περιστατικά και συνεπώς να ζητείται η γνώμη του δικτύου CSIRT πρώτα.*

## **Τροπολογία 142**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

### **Πρόταση κανονισμού**

#### **Άρθρο 7 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

2. Η Επιτροπή δύναται να καθορίζει, με εκτελεστικές πράξεις, τις διαδικαστικές

*Τροπολογία*

2. Η Επιτροπή δύναται, **αφού ζητήσει τη γνώμη του ENISA**, να καθορίζει, με

ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

εκτελεστικές πράξεις, τις διαδικαστικές ρυθμίσεις για την ανταλλαγή πληροφοριών που προβλέπεται στην παράγραφο 1. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2 του παρόντος κανονισμού.

Or. en

## **Τροπολογία 143** **Johan Nissinen**

### **Πρόταση κανονισμού** **Άρθρο 8 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

1. Τα κράτη μέλη που συμμετέχουν στην ευρωπαϊκή κυβερνοασπίδα διασφαλίζουν υψηλό επίπεδο **εμπιστευτικότητας**, 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.

Or. en

## **Τροπολογία 144** **Enžen Tošenovský**

### **Πρόταση κανονισμού** **Άρθρο 8 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

**3. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις για τον καθορισμό**

*Τροπολογία*

**διαγράφεται**



*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.*

Or. en

## **Τροπολογία 145**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### **Πρόταση κανονισμού Άρθρο 8 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

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.

*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 **και με τις οδηγίες (EE) 2022/2555 και (EE) 2022/2557**. 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.

Or. en

## **Τροπολογία 146**

**Πρόταση κανονισμού**  
**Άρθρο 8 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

3. Η Επιτροπή δύναται να εκδίδει εκτελεστικές πράξεις, **αφού ζητήσει τη γνώμη του ENISA**, 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.

Or. en

**Τροπολογία 147**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 9 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε μείζονες απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας (στο εξής: μηχανισμός).

*Τροπολογία*

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε μείζονες απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας (στο εξής: μηχανισμός), **κατόπιν ρητού αιτήματος του/των ενδιαφερόμενου/-ων κράτους/-ών μέλους/-ών.**

**Τροπολογία 148**  
**Enĵen Toĝenovský**

**Πρόταση κανονισμού**  
**Άρθρο 9 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε **μείζονες** απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας (στο εξής: μηχανισμός).

*Τροπολογία*

1. Θεσπίζεται μηχανισμός έκτακτης ανάγκης στον κυβερνοχώρο με σκοπό τη βελτίωση της ανθεκτικότητας της Ένωσης σε **σημαντικές** απειλές κυβερνοασφάλειας και την προετοιμασία και τον μετριασμό, σε πνεύμα αλληλεγγύης, των βραχυπρόθεσμων επιπτώσεων σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας (στο εξής: μηχανισμός).

Or. en

**Τροπολογία 149**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 10 – παράγραφος 1 – στοιχείο β**

*Κείμενο που προτείνει η Επιτροπή*

β) δράσεις αντιμετώπισης, οι οποίες στηρίζουν την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από αυτά, και οι οποίες πρέπει να παρέχονται από αξιόπιστους παρόχους που συμμετέχουν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται δυνάμει του άρθρου 12,

*Τροπολογία*

β) δράσεις αντιμετώπισης, οι οποίες στηρίζουν την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από αυτά, και οι οποίες πρέπει να παρέχονται από αξιόπιστους παρόχους που συμμετέχουν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται δυνάμει του άρθρου 12, **κατόπιν ρητού αιτήματος του/των ενδιαφερόμενου/-ων κράτους/-ών μέλους/-ών,**

Or. en

**Τροπολογία 150**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 10 – παράγραφος 1 – στοιχείο β**

*Κείμενο που προτείνει η Επιτροπή*

β) δράσεις αντιμετώπισης, οι οποίες στηρίζουν την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από αυτά, και οι οποίες πρέπει να παρέχονται από αξιόπιστους παρόχους που συμμετέχουν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται δυνάμει του άρθρου 12,

*Τροπολογία*

β) δράσεις αντιμετώπισης, οι οποίες στηρίζουν την αντιμετώπιση σημαντικών και μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από αυτά, και οι οποίες πρέπει να παρέχονται από αξιόπιστους παρόχους **διαχειριζόμενων υπηρεσιών ασφάλειας** που συμμετέχουν στην εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας που θεσπίζεται δυνάμει του άρθρου 12,

Or. en

**Τροπολογία 151**  
**Ville Niinistö**  
εξ ονόματος της Ομάδας Verts/ALE

**Πρόταση κανονισμού**  
**Άρθρο 10 – παράγραφος 1 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**1α. Μετά την ενεργοποίηση του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο, η Επιτροπή υποβάλλει κάθε χρόνο την αξιολόγηση τόσο του θετικού όσο και του αρνητικού έργου του μηχανισμού, μεταξύ άλλων, αν χρειάζονται περισσότερες απαιτήσεις συνεργασίας ή κατάρτισης.**

Or. en

**Τροπολογία 152**

Enžen Tošenovský

**Πρόταση κανονισμού**  
**Άρθρο 11 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

1. Για τους σκοπούς της στήριξης των συντονισμένων δοκιμών ετοιμότητας των οντοτήτων που αναφέρονται στο άρθρο 10 παράγραφος 1 στοιχείο α), σε ολόκληρη την Ένωση, η Επιτροπή, αφού ζητήσει τη γνώμη της ομάδας συνεργασίας NIS και του ENISA, προσδιορίζει τους σχετικούς τομείς, ή υποτομείς, από τους τομείς υψηλής κρισιμότητας που παρατίθενται στο παράρτημα I της οδηγίας (ΕΕ) 2022/2555, των οποίων οι οντότητες μπορούν να υποβληθούν σε συντονισμένες δοκιμές ετοιμότητας, λαμβάνοντας υπόψη τις υφιστάμενες και προγραμματισμένες συντονισμένες εκτιμήσεις κινδύνου και δοκιμές ανθεκτικότητας σε επίπεδο Ένωσης.

*Τροπολογία*

1. Για τους σκοπούς της στήριξης των συντονισμένων δοκιμών ετοιμότητας των οντοτήτων που αναφέρονται στο άρθρο 10 παράγραφος 1 στοιχείο α), σε ολόκληρη την Ένωση, η Επιτροπή, αφού ζητήσει τη γνώμη της ομάδας συνεργασίας NIS και του ENISA, προσδιορίζει τους σχετικούς τομείς, ή υποτομείς, από τους τομείς υψηλής κρισιμότητας που παρατίθενται στο παράρτημα I της οδηγίας (ΕΕ) 2022/2555, των οποίων οι οντότητες μπορούν να υποβληθούν σε **εθελοντικές** συντονισμένες δοκιμές ετοιμότητας, λαμβάνοντας υπόψη τις υφιστάμενες και προγραμματισμένες συντονισμένες εκτιμήσεις κινδύνου και δοκιμές ανθεκτικότητας σε επίπεδο Ένωσης.

Or. en

**Τροπολογία 153**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 11 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

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.

*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 **ετοιμότητας. Αυτό θα επηρεάσει τον προσδιορισμό των σχετικών τομέων ή υποτομέων, από τους οποίους οντότητες μπορεί να υποβληθούν στις συντονισμένες δοκιμές ετοιμότητας, όπως περιγράφεται στην παράγραφο 1.**

## Τροπολογία 154

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

#### Άρθρο 11 – παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

2. Η ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή, τον ENISA, τον/την ύπατο/-η εκπρόσωπο **και τις οντότητες που μπορούν να υποβληθούν σε δοκιμές ετοιμότητας**, αναπτύσσει κοινά σενάρια και μεθοδολογίες κινδύνου για τις συντονισμένες δοκιμές.

Or. en

## Τροπολογία 155

Johan Nissinen

### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 1

*Κείμενο που προτείνει η Επιτροπή*

1. Δημιουργείται εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, με σκοπό να βοηθήσει τους χρήστες που αναφέρονται στην παράγραφο 3 να αντιμετωπίζουν ή να παρέχουν στήριξη για την αντιμετώπιση σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από τέτοια περιστατικά.

*Τροπολογία*

1. Δημιουργείται εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, με σκοπό να βοηθήσει τους χρήστες που αναφέρονται στην παράγραφο 3 να αντιμετωπίζουν ή να παρέχουν στήριξη για την αντιμετώπιση σημαντικών ή μεγάλης κλίμακας περιστατικών στον τομέα της κυβερνοασφάλειας και την άμεση ανάκαμψη από τέτοια περιστατικά, **κατόπιν ρητού αιτήματος του/των ενδιαφερόμενου/-ων κράτους/-ών μέλους/-ών και με την επιφύλαξη του ειδικού χαρακτήρα της πολιτικής ασφαλείας και άμυνας ορισμένων κρατών μελών.**

## Τροπολογία 156

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

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 προοδευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη.

*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 προοδευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη, **ενισχύουν την ανθεκτικότητα και την κυριαρχία της Ένωσης, και βελτιώνουν την ανταγωνιστικότητά της. Τα ονόματα των επιλεγμένων αξιόπιστων παρόχων και οι υπηρεσίες τους θα παραμένουν απόρρητα.**

## Τροπολογία 157

Johan Nissinen

### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

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 προοδευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη.

*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 προοδευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη. **Η εφεδρεία της ΕΕ στον τομέα της**

*κυβερνοασφάλειας δεν περιορίζει την ανάγκη να επιτρέπεται στις χώρες να παρακολουθούν και να αξιολογούν τις δικές τους ανάγκες.*

Or. en

**Τροπολογία 158**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

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 προδεδουλευμένες υπηρεσίες. Οι υπηρεσίες μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη.

*Τροπολογία*

2. Η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας συνίσταται σε υπηρεσίες αντιμετώπισης περιστατικών από αξιόπιστους παρόχους **διαχειριζόμενων υπηρεσιών ασφάλειας** που επιλέγονται σύμφωνα με τα κριτήρια που ορίζονται στο άρθρο 16. Η εφεδρεία περιλαμβάνει προδεδουλευμένες υπηρεσίες. Οι υπηρεσίες μπορούν, **κατόπιν αιτήματος**, να αναπτυχθούν σε όλα τα κράτη μέλη.

Or. en

**Τροπολογία 159**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 3 – στοιχείο β**

*Κείμενο που προτείνει η Επιτροπή*

β) **τα θεσμικά και λοιπά όργανα και οργανισμοί της Ένωσης.**

*Τροπολογία*

β) **τις τρίτες χώρες που αναφέρονται στο άρθρο 17 του παρόντος κανονισμού.**

Or. en

**Τροπολογία 160**



Enžen Tošenovský

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 4**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

4. Οι χρήστες που αναφέρονται στην παράγραφο 3 στοιχείο α) **μπορούν, κατόπιν αιτήματος, να** 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.

Or. en

**Τροπολογία 161**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 5**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

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, **σε συντονισμό με την ομάδα συντονισμού NIS2 και** 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.

Or. en

**Τροπολογία 162**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 5**

*Κείμενο που προτείνει η Επιτροπή*

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.

*Τροπολογία*

5. Η Επιτροπή έχει τη συνολική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Η Επιτροπή, **σε συνεργασία με τον ENISA**, 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.

Or. en

**Τροπολογία 163**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 6**

*Κείμενο που προτείνει η Επιτροπή*

6. **Η Επιτροπή μπορεί να αναθέσει τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν όλω ή εν μέρει, στον ENISA, μέσω συμφωνιών συνεισφοράς.**

*Τροπολογία*

**διαγράφεται**

Or. en

## Τροπολογία 164

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 6

*Κείμενο που προτείνει η Επιτροπή*

6. Η Επιτροπή **μπορεί να αναθέσει** τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν όλω ή εν μέρει, στον ENISA, μέσω συμφωνιών συνεισφοράς.

*Τροπολογία*

6. Η Επιτροπή **αναθέτει** τη λειτουργία και τη διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν όλω ή εν μέρει, στον ENISA, μέσω συμφωνιών συνεισφοράς.

Or. en

## Τροπολογία 165

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 7

*Κείμενο που προτείνει η Επιτροπή*

7. Προκειμένου να στηρίζει 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.

*Τροπολογία*

7. Προκειμένου να στηρίζει την Επιτροπή στη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, ο ENISA εκπονεί χαρτογράφηση των αναγκαίων υπηρεσιών, **συμπεριλαμβανομένων των αναγκαίων δεξιοτήτων και ικανοτήτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας**, αφού ζητήσει τη γνώμη των κρατών μελών και της Επιτροπής. Ο ENISA εκπονεί παρόμοια χαρτογράφηση, αφού ζητήσει τη γνώμη της Επιτροπής **και σε συνεργασία με τον ιδιωτικό τομέα**, 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.

**Τροπολογία 166**  
**Enžen Tošovský**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

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.

*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 **και ενημερώνει το Συμβούλιο σχετικά με τις ανάγκες τρίτων χωρών.**

**Τροπολογία 167**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 12 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

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

*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, της Επιτροπής, **των παρόχων διαχειριζόμενων υπηρεσιών**

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.

**ασφάλειας και των εκπροσώπων της βιομηχανίας.** 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.

Or. en

### Τροπολογία 168

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

#### Πρόταση κανονισμού

#### Άρθρο 12 – παράγραφος 8

*Κείμενο που προτείνει η Επιτροπή*

8. Η Επιτροπή μπορεί, **με εκτελεστικές πράξεις**, να **προσδιορίζει τα είδη και τον αριθμό** των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.

*Τροπολογία*

8. Η Επιτροπή μπορεί να **εκδίδει κατ' εξουσιοδότηση πράξη, σύμφωνα με το άρθρο 20α του παρόντος κανονισμού, για τον προσδιορισμό των ειδών και του αριθμού** των υπηρεσιών αντιμετώπισης που απαιτούνται για την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.

Or. en

### Τροπολογία 169

Enĵen Tošenovský

#### Πρόταση κανονισμού

#### Άρθρο 13 – παράγραφος 5 – στοιχείο α

*Κείμενο που προτείνει η Επιτροπή*

α) **κατάλληλες πληροφορίες σχετικά με την πληγείσα οντότητα** και τις πιθανές

*Τροπολογία*

α) **το είδος της πληγείσας οντότητας** και τις πιθανές επιπτώσεις του

επιπτώσεις του περιστατικού και την προγραμματισμένη χρήση της αιτούμενης στήριξης, συμπεριλαμβανομένης αναφοράς των εκτιμώμενων αναγκών,

περιστατικού και την προγραμματισμένη χρήση της αιτούμενης στήριξης, συμπεριλαμβανομένης αναφοράς των εκτιμώμενων αναγκών,

Or. en

**Τροπολογία 170**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 13 – παράγραφος 5 – στοιχείο β**

*Κείμενο που προτείνει η Επιτροπή*

β) *πληροφορίες* σχετικά με τα μέτρα που λαμβάνονται για τον μετριασμό του περιστατικού για το οποίο ζητείται η στήριξη, όπως αναφέρεται στην παράγραφο 2,

*Τροπολογία*

β) *γενικά στοιχεία* σχετικά με τα μέτρα που λαμβάνονται για τον μετριασμό του περιστατικού για το οποίο ζητείται η στήριξη, όπως αναφέρεται στην παράγραφο 2,

Or. en

**Τροπολογία 171**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 13 – παράγραφος 5 – στοιχείο γ**

*Κείμενο που προτείνει η Επιτροπή*

γ) πληροφορίες σχετικά με άλλες μορφές στήριξης που έχει στη διάθεσή της η πληγείσα οντότητα,  
*συμπεριλαμβανομένων των συμβατικών ρυθμίσεων που ισχύουν για τις υπηρεσίες αντιμετώπισης περιστατικών και άμεσης ανάκαμψης, καθώς και ασφαλιστήριων συμβολαίων που ενδέχεται να καλύπτουν τέτοιου είδους περιστατικά.*

*Τροπολογία*

γ) πληροφορίες σχετικά με άλλες μορφές στήριξης που έχει στη διάθεσή της η πληγείσα οντότητα.

Or. en

**Τροπολογία 172**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 13 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

**7. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίζει περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.**

*Τροπολογία*

**διαγράφεται**

Or. en

**Τροπολογία 173**  
**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

**Πρόταση κανονισμού**  
**Άρθρο 13 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

**7. Η Επιτροπή μπορεί, με εκτελεστικές πράξεις, να προσδιορίζει περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.**

*Τροπολογία*

**7. Η Επιτροπή μπορεί να εκδίδει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 20α του παρόντος κανονισμού, για να προσδιορίσει περαιτέρω τις λεπτομερείς ρυθμίσεις για την κατανομή των υπηρεσιών στήριξης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω εκτελεστικές πράξεις εκδίδονται σύμφωνα με τη διαδικασία εξέτασης που αναφέρεται στο άρθρο 21 παράγραφος 2.**

Or. en

**Τροπολογία 174**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 14 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

1. Τα αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αξιολογούνται από την Επιτροπή, με την υποστήριξη του ENISA **ή όπως ορίζεται στις συμφωνίες συνεισφοράς δυνάμει του άρθρου 12 παράγραφος 6, και η απάντηση** διαβιβάζεται στους χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 χωρίς καθυστέρηση.

*Τροπολογία*

1. Τα αιτήματα στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας αξιολογούνται από την Επιτροπή, με την υποστήριξη του ENISA, **και η απόφασή της** διαβιβάζεται στους χρήστες που αναφέρονται στο άρθρο 12 παράγραφος 3 χωρίς **αδικοιολόγητη** καθυστέρηση **και, σε κάθε περίπτωση, εντός 24 ωρών.**

Or. en

**Τροπολογία 175**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**

**Άρθρο 14 – παράγραφος 2 – στοιχείο δ**

*Κείμενο που προτείνει η Επιτροπή*

δ) ο δυνητικός διασυνωριακός χαρακτήρας του περιστατικού και ο κίνδυνος πρόκλησης δευτερογενών επιπτώσεων σε άλλα κράτη μέλη ή χρήστες,

*Τροπολογία*

δ) **η κλίμακα και** ο δυνητικός διασυνωριακός χαρακτήρας του περιστατικού και ο κίνδυνος πρόκλησης δευτερογενών επιπτώσεων σε άλλα κράτη μέλη ή χρήστες,

Or. en

**Τροπολογία 176**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan**

**Πρόταση κανονισμού**

**Άρθρο 14 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

3. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας

*Τροπολογία*

3. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας



παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω συμφωνίες περιλαμβάνουν όρους ευθύνης.

παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω συμφωνίες περιλαμβάνουν όρους ευθύνης **και τυχόν άλλη διάταξη την οποία τα μέρη της συμφωνίας θεωρούν απαραίτητη για την παροχή της αντίστοιχης υπηρεσίας.**

Or. en

### Τροπολογία 177

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

#### Πρόταση κανονισμού

#### Άρθρο 14 – παράγραφος 3

*Κείμενο που προτείνει η Επιτροπή*

3. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας παρέχονται σύμφωνα με ειδικές συμφωνίες μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω συμφωνίες περιλαμβάνουν όρους ευθύνης.

*Τροπολογία*

3. Οι υπηρεσίες εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας παρέχονται **κατόπιν έγκρισης του χρήστη και** σύμφωνα με ειδικές συμφωνίες μεταξύ του παρόχου υπηρεσιών και του χρήστη στον οποίο παρέχεται η στήριξη στο πλαίσιο της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Οι εν λόγω συμφωνίες περιλαμβάνουν όρους ευθύνης.

Or. en

### Τροπολογία 178

**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

#### Πρόταση κανονισμού

#### Άρθρο 14 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

4. Οι συμφωνίες που αναφέρονται στην παράγραφο 3 **μπορούν να** βασίζονται σε υποδείγματα που καταρτίζει ο ENISA,

*Τροπολογία*

4. Οι συμφωνίες που αναφέρονται στην παράγραφο 3 βασίζονται σε υποδείγματα που καταρτίζει ο ENISA,

αφού ζητήσει τη γνώμη των κρατών μελών.

αφού ζητήσει τη γνώμη των κρατών μελών και άλλων χρηστών της εφεδρείας.

Or. en

**Τροπολογία 179**  
**Enžen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 14 – παράγραφος 5**

*Κείμενο που προτείνει η Επιτροπή*

**5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.**

*Τροπολογία*

**διαγράφεται**

Or. en

**Τροπολογία 180**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 14 – παράγραφος 5**

*Κείμενο που προτείνει η Επιτροπή*

5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

*Τροπολογία*

5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, **εξαιρουμένων περιπτώσεων αμέλειας στην αξιολόγηση της αίτησης του παρόχου υπηρεσίας ή περιπτώσεων στις οποίες η Επιτροπή ή ο ENISA είναι χρήστες και διαπιστώνεται πως φέρουν ευθύνη για ζημίες.**

Or. en

## Τροπολογία 181

Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

### Πρόταση κανονισμού

#### Άρθρο 14 – παράγραφος 5

*Κείμενο που προτείνει η Επιτροπή*

5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας.

*Τροπολογία*

5. Η Επιτροπή και ο ENISA δεν φέρουν συμβατική ευθύνη για ζημίες που προκαλούνται σε τρίτους από τις υπηρεσίες που παρέχονται στο πλαίσιο της υλοποίησης της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, **εξαιρουμένων περιπτώσεων στις οποίες η Επιτροπή ή ο ENISA είναι χρήστες της εφεδρείας σύμφωνα με το άρθρο 14 παράγραφος 3.**

Or. en

## Τροπολογία 182

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

### Πρόταση κανονισμού

#### Άρθρο 14 – παράγραφος 6

*Κείμενο που προτείνει η Επιτροπή*

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν. Όταν ο χρήστης προέρχεται από τρίτη χώρα, όπως ορίζεται στο άρθρο 17, η εν λόγω έκθεση κοινοποιείται στον/στην ύπατο/-η εκπρόσωπο.

*Τροπολογία*

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν. Όταν ο χρήστης προέρχεται από τρίτη χώρα, όπως ορίζεται στο άρθρο 17, η εν λόγω έκθεση κοινοποιείται στον/στην ύπατο/-η εκπρόσωπο. **Η έκθεση σέβεται το ενωσιακό ή εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.**

Or. en

**Τροπολογία 183**  
**Enĵen Toĥenovský**

**Πρόταση κανονισμού**  
**Άρθρο 14 – παράγραφος 6**

*Κείμενο που προτείνει η Επιτροπή*

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή **και** στον ENISA συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν. Όταν ο χρήστης προέρχεται από τρίτη χώρα, όπως ορίζεται στο άρθρο 17, η εν λόγω έκθεση κοινοποιείται στον/στην ύπατο/-η εκπρόσωπο.

*Τροπολογία*

6. Εντός ενός μηνός από το τέλος της δράσης στήριξης, οι χρήστες υποβάλλουν στην Επιτροπή, στον ENISA, **στο δίκτυο CSIRT και, κατά περίπτωση, στο EU-CyCLONe** συνοπτική έκθεση σχετικά με την παρασχεθείσα υπηρεσία, τα αποτελέσματα που επιτεύχθηκαν και τα διδάγματα που αντλήθηκαν. Όταν ο χρήστης προέρχεται από τρίτη χώρα, όπως ορίζεται στο άρθρο 17, η εν λόγω έκθεση κοινοποιείται στον/στην ύπατο/-η εκπρόσωπο.

Or. en

**Τροπολογία 184**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Πρόταση κανονισμού**  
**Άρθρο 14 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

7. Η Επιτροπή υποβάλλει τακτικά έκθεση στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.

*Τροπολογία*

7. Η Επιτροπή υποβάλλει τακτικά έκθεση στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης. **Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.**

Or. en

**Τροπολογία 185**

**Enĵen Toĥenovský**

**Πρόταση κανονισμού  
Άρθρο 14 – παράγραφος 7**

*Κείμενο που προτείνει η Επιτροπή*

7. Η Επιτροπή υποβάλλει **τακτικά** έκθεση στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.

*Τροπολογία*

7. Η Επιτροπή υποβάλλει έκθεση **τουλάχιστον δύο φορές τον χρόνο** στην ομάδα συνεργασίας NIS σχετικά με τη χρήση και τα αποτελέσματα της στήριξης.

Or. en

**Τροπολογία 186  
Enĵen Toĥenovský**

**Πρόταση κανονισμού  
Άρθρο 15 – τίτλος**

*Κείμενο που προτείνει η Επιτροπή*

Συντονισμός με τους μηχανισμούς διαχείρισης κρίσεων

*Τροπολογία*

Συντονισμός **του μηχανισμού έκτακτης ανάγκης στον κυβερνοχώρο** με τους μηχανισμούς διαχείρισης κρίσεων

Or. en

**Τροπολογία 187  
Enĵen Toĥenovský**

**Πρόταση κανονισμού  
Άρθρο 15 – παράγραφος 3**

*Κείμενο που προτείνει η Επιτροπή*

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**

*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.

*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.*

Or. en

**Τροπολογία 188**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Άρθρο 16 – τίτλος**

*Κείμενο που προτείνει η Επιτροπή*

Αξιόπιστοι πάροχοι

*Τροπολογία*

Αξιόπιστοι πάροχοι *διαχειριζόμενων υπηρεσιών ασφάλειας*

Or. en

**Τροπολογία 189**  
**Johan Nissinen**

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 1 – εισαγωγικό μέρος**

*Κείμενο που προτείνει η Επιτροπή*

1. Στις διαδικασίες προμηθειών με σκοπό τη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή ενεργεί σύμφωνα με τις αρχές που καθορίζονται στον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046 και σύμφωνα με τις ακόλουθες αρχές:

*Τροπολογία*

1. Στις διαδικασίες προμηθειών με σκοπό τη δημιουργία της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, η αναθέτουσα αρχή ενεργεί σύμφωνα με τις αρχές που καθορίζονται στον κανονισμό (ΕΕ, Ευρατόμ) 2018/1046, **με την επιφύλαξη της πρωταρχικής ευθύνης των κρατών μελών για εθνική ασφάλεια** και σύμφωνα με τις ακόλουθες αρχές:

Or. en

**Τροπολογία 190**

Enĵen Tošenovský

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 1 – στοιχείο α**

*Κείμενο που προτείνει η Επιτροπή*

α) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνει υπηρεσίες που μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη, λαμβάνοντας ιδίως υπόψη τις εθνικές απαιτήσεις για την παροχή των εν λόγω υπηρεσιών, συμπεριλαμβανομένης της πιστοποίησης ή της διαπίστευσης,

*Τροπολογία*

α) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας περιλαμβάνει υπηρεσίες που μπορούν να αναπτυχθούν σε όλα τα κράτη μέλη **και σε τρίτες χώρες σύμφωνα με το άρθρο 17 του παρόντος κανονισμού**, λαμβάνοντας ιδίως υπόψη τις εθνικές απαιτήσεις για την παροχή των εν λόγω υπηρεσιών, συμπεριλαμβανομένης της πιστοποίησης ή της διαπίστευσης,

Or. en

**Τροπολογία 191**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 1 – στοιχείο γ**

*Κείμενο που προτείνει η Επιτροπή*

γ) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας προσδίδει ενωσιακή προστιθέμενη αξία, συμβάλλοντας στην επίτευξη των στόχων που ορίζονται στο άρθρο 3 του κανονισμού (ΕΕ) 2021/694, συμπεριλαμβανομένης της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ.

*Τροπολογία*

γ) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας προσδίδει ενωσιακή προστιθέμενη αξία, συμβάλλοντας στην επίτευξη των στόχων που ορίζονται στο άρθρο 3 του κανονισμού (ΕΕ) 2021/694, συμπεριλαμβανομένης της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ, **της ενίσχυσης της ανθεκτικότητας και της κυριαρχίας της Ένωσης, καθώς και της βελτίωσης της ανταγωνιστικότητας της Ένωσης.**

Or. en

**Τροπολογία 192**

Enĵen Toĥenovský

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 1 – στοιχείο γ**

*Κείμενο που προτείνει η Επιτροπή*

γ) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας **προσδίδει ενωσιακή προστιθέμενη αξία, συμβάλλοντας** στην επίτευξη των στόχων που ορίζονται στο άρθρο 3 του κανονισμού (ΕΕ) 2021/694, συμπεριλαμβανομένης της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ.

*Τροπολογία*

γ) διασφαλίζει ότι η εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας **συμβάλλει** στην επίτευξη των στόχων που ορίζονται στο άρθρο 3 του κανονισμού (ΕΕ) 2021/694, συμπεριλαμβανομένης της προώθησης της ανάπτυξης δεξιοτήτων κυβερνοασφάλειας στην ΕΕ.

Or. en

**Τροπολογία 193**

**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 2 – στοιχείο στ**

*Κείμενο που προτείνει η Επιτροπή*

στ) ο πάροχος είναι εξοπλισμένος με τον τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας,

*Τροπολογία*

στ) ο πάροχος είναι εξοπλισμένος με τον **σύγχρονο** τεχνικό εξοπλισμό υλισμικού και λογισμικού που απαιτείται για την υποστήριξη της αιτούμενης υπηρεσίας **και εκπληρώνει, κατά περίπτωση, τις απαιτήσεις που ορίζονται στον κανονισμό XX/XXXX (πράξη για την κυβερνοανθεκτικότητα),**

Or. en

**Τροπολογία 194**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan**

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



*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**στ α) ο πάροχος αποδεικνύει ότι οι δομές λήψης αποφάσεων και διαχείρισής του είναι απαλλαγμένες από οποιαδήποτε αθέμιτη επιρροή από κυβερνήσεις κρατών που έχουν χαρακτηριστεί ως συστημικοί αντίπαλοι της Ένωσης·**

Or. en

**Τροπολογία 195**  
**Enĵen Toĝenovský**

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 2 – στοιχείο η**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

η) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία εντός σύντομου χρονικού διαστήματος στο κράτος μέλος/-η όπου μπορεί να παρέχει την υπηρεσία,

η) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία εντός σύντομου χρονικού διαστήματος στο κράτος μέλος/-η **ή σε τρίτες χώρες** όπου μπορεί να παρέχει την υπηρεσία,

Or. en

**Τροπολογία 196**  
**Enĵen Toĝenovský**

**Πρόταση κανονισμού**  
**Άρθρο 16 – παράγραφος 2 – στοιχείο θ**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

θ) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία στην τοπική γλώσσα του κράτους μέλους ή των κρατών μελών όπου μπορεί να παρέχει την υπηρεσία,

θ) ο πάροχος είναι σε θέση να παρέχει την υπηρεσία στην τοπική γλώσσα του κράτους μέλους ή των κρατών μελών **ή των τρίτων χωρών** όπου μπορεί να παρέχει την υπηρεσία **ή σε μία από τις γλώσσες εργασίας των θεσμικών οργάνων της ΕΕ,**

Or. en

## Τροπολογία 197

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rareș Bogdan

### Πρόταση κανονισμού

#### Άρθρο 16 – παράγραφος 2 – στοιχείο ι

*Κείμενο που προτείνει η Επιτροπή*

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης της ΕΕ για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα.

*Τροπολογία*

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης της ΕΕ για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα, **εντός διαστήματος δύο ετών μετά την έγκριση του συστήματος.**

Or. en

## Τροπολογία 198

Enžen Tošenovský

### Πρόταση κανονισμού

#### Άρθρο 16 – παράγραφος 2 – στοιχείο ι

*Κείμενο που προτείνει η Επιτροπή*

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης **της ΕΕ** για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα.

*Τροπολογία*

ι) μόλις τεθεί σε εφαρμογή **ευρωπαϊκό** σύστημα πιστοποίησης **της κυβερνοασφάλειας** για τις διαχειριζόμενες υπηρεσίες ασφάλειας **βάσει** του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα.

Or. en

## Τροπολογία 199

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

### Πρόταση κανονισμού

#### Άρθρο 16 – παράγραφος 2 – στοιχείο ι

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης της ΕΕ για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα.

ι) μόλις τεθεί σε εφαρμογή σύστημα πιστοποίησης της ΕΕ για τις διαχειριζόμενες υπηρεσίες ασφάλειας του κανονισμού (ΕΕ) 2019/881, ο πάροχος πιστοποιείται σύμφωνα με το εν λόγω σύστημα *εντός δύο ετών*.

Or. en

*Αιτιολόγηση*

*Η πρόταση της Επιτροπής είναι οι τεχνικές απαιτήσεις που αναφέρονται στον παρόντα κανονισμό να αντικατασταθούν από σύστημα πιστοποίησης. Η τροπολογία αυτή παρέχει σε εταιρείες, ιδίως ΜΜΕ, περισσότερο χρόνο για μετάβαση στο εν λόγω σύστημα, ενθαρρύνοντας πιο ισότιμους όρους ανταγωνισμού σε ολόκληρη την Ένωση. Έως τότε, θα πρέπει να συμμορφώνονται με τις τεχνικές απαιτήσεις του παρόντος κανονισμού.*

## **Τροπολογία 200**

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### **Πρόταση κανονισμού**

**Άρθρο 16 – παράγραφος 2 – στοιχείο ι α (νέο)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

*ια) ο πάροχος μπορεί να διαχωρίσει τις υπηρεσίες του από τη σύμβαση, ώστε ο χρήστης να μπορεί να αλλάξει πάροχο υπηρεσιών·*

Or. en

## **Τροπολογία 201**

**Enžen Tošenovský**

### **Πρόταση κανονισμού**

**Άρθρο 17 – παράγραφος 6**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

6. Η Επιτροπή συντονίζει με τον/την ύπατο/-η εκπρόσωπο τα αιτήματα που λαμβάνει και την υλοποίηση της στήριξης που παρέχεται σε τρίτες χώρες από την

6. Η Επιτροπή *χωρίς αδικαιολόγητη καθυστέρηση ενημερώνει το Συμβούλιο και* συντονίζει με τον/την ύπατο/-η εκπρόσωπο τα αιτήματα που λαμβάνει και

εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

την υλοποίηση της στήριξης που παρέχεται σε τρίτες χώρες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.

Or. en

**Τροπολογία 202**  
**Enĵen Toĝepovský**

**Πρόταση κανονισμού**  
**Άρθρο 18**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**Άρθρο 18**

**διαγράφεται**

**Μηχανισμός εξέτασης περιστατικών κυβερνοασφάλειας**

**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.**

**2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας**

*και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλευέται άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.*

*3. Η έκθεση καλύπτει εξέταση και ανάλυση του συγκεκριμένου σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των κύριων αιτίων, των τρωτών σημείων και των διδαγμάτων που αντλήθηκαν. Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.*

*4. Κατά περίπτωση, η έκθεση διατυπώνει συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.*

*5. Όπου είναι δυνατόν, μια έκδοση της έκθεσης δημοσιοποιείται. Η έκδοση αυτή περιλαμβάνει μόνο πληροφορίες που προορίζονται για το κοινό.*

Or. en

## **Τροπολογία 203**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

### **Πρόταση κανονισμού**

#### **Άρθρο 18 – παράγραφος 2**

*Κείμενο που προτείνει η Επιτροπή*

2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη,

*Τροπολογία*

2. Για την εκπόνηση της έκθεσης εξέτασης περιστατικού που αναφέρεται στην παράγραφο 1, ο ENISA συνεργάζεται με όλα τα σχετικά ενδιαφερόμενα μέρη **και**

συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλευτεί άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.

*συλλέγει σχόλια από αυτά,* συμπεριλαμβανομένων εκπροσώπων των κρατών μελών, της Επιτροπής, άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας και χρηστών υπηρεσιών κυβερνοασφάλειας. Κατά περίπτωση, ο ENISA συνεργάζεται επίσης με οντότητες που πλήττονται από σημαντικά ή μεγάλης κλίμακας περιστατικά στον τομέα της κυβερνοασφάλειας. Για την υποστήριξη της εξέτασης, ο ENISA μπορεί επίσης να συμβουλευτεί άλλα είδη ενδιαφερόμενων μερών. Οι εκπρόσωποι των οποίων ζητείται η γνώμη γνωστοποιούν κάθε πιθανή σύγκρουση συμφερόντων.

Or. en

## Τροπολογία 204

**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

### Πρόταση κανονισμού

#### Άρθρο 18 – παράγραφος 3

*Κείμενο που προτείνει η Επιτροπή*

3. Η έκθεση καλύπτει εξέταση και ανάλυση του συγκεκριμένου σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των κύριων αιτίων, των τρωτών σημείων και των διδαγμάτων που αντλήθηκαν. Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών.

*Τροπολογία*

3. Η έκθεση καλύπτει εξέταση και ανάλυση του συγκεκριμένου σημαντικού ή μεγάλης κλίμακας περιστατικού στον τομέα της κυβερνοασφάλειας, συμπεριλαμβανομένων των κύριων αιτίων, των τρωτών σημείων και των διδαγμάτων που αντλήθηκαν. Προστατεύει τις εμπιστευτικές πληροφορίες, σύμφωνα με το ενωσιακό ή το εθνικό δίκαιο σχετικά με την προστασία ευαίσθητων ή διαβαθμισμένων πληροφοριών. ***Δεν περιλαμβάνει λεπτομέρειες σχετικά με τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και δεν έχουν ακόμα διορθωθεί.***

Or. en

## Τροπολογία 205

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

### Πρόταση κανονισμού

#### Άρθρο 18 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

4. Κατά περίπτωση, η έκθεση διατυπώνει συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.

*Τροπολογία*

4. Κατά περίπτωση, η έκθεση διατυπώνει **συγκεκριμένες** συστάσεις, **μεταξύ άλλων για όλα τα σχετικά ενδιαφερόμενα μέρη**, για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο·

Or. en

## Τροπολογία 206

Johan Nissinen

### Πρόταση κανονισμού

#### Άρθρο 18 – παράγραφος 4

*Κείμενο που προτείνει η Επιτροπή*

4. Κατά περίπτωση, η έκθεση διατυπώνει συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.

*Τροπολογία*

4. Κατά περίπτωση, η έκθεση διατυπώνει **μη δεσμευτικές νομικά εθελοντικές** συστάσεις για τη βελτίωση της στάσης της Ένωσης στον κυβερνοχώρο.

Or. en

## Τροπολογία 207

Enĵen Tošenovský

### Πρόταση κανονισμού

#### Άρθρο 19 – παράγραφος 1 – σημείο 1 – στοιχείο α – σημείο 1

Κανονισμός (ΕΕ) 2021/694

Άρθρο 1 – παράγραφος 1 – στοιχείο αα

*Κείμενο που προτείνει η Επιτροπή*

αα) στήριξη της ανάπτυξης ενωσιακής κυβερνοασπίδας, συμπεριλαμβανομένης

*Τροπολογία*

αα) 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»

της ανάπτυξης, της εγκατάστασης και της λειτουργίας *CSIRT-ISAC και* SOC που συμβάλλουν στην αντίληψη της κατάστασης στην Ένωση και στην ενίσχυση των ικανοτήτων της Ένωσης όσον αφορά τη συλλογή πληροφοριών για τις κυβερνοαπειλές»

Or. en

### **Τροπολογία 208**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

#### **Πρόταση κανονισμού**

#### **Άρθρο 19 – παράγραφος 1 – σημείο 3**

Κανονισμός (ΕΕ) 2021/694

Άρθρο 14 παράγραφος 2

*Κείμενο που προτείνει η Επιτροπή*

Το πρόγραμμα μπορεί να παρέχει χρηματοδότηση με οποιαδήποτε από τις μορφές που καθορίζονται στον δημοσιονομικό κανονισμό, συμπεριλαμβανομένων κυρίως μέσω των δημοσίων συμβάσεων ως πρωταρχικής μορφής ή των επιχορηγήσεων και των βραβείων.

*Τροπολογία*

Το πρόγραμμα μπορεί να παρέχει χρηματοδότηση με οποιαδήποτε από τις μορφές που καθορίζονται στον δημοσιονομικό κανονισμό, συμπεριλαμβανομένων κυρίως μέσω των δημοσίων συμβάσεων ως πρωταρχικής μορφής ή των επιχορηγήσεων και των βραβείων. ***Ο ENISA λαμβάνει πρόσθετους πόρους για την εκτέλεση των πρόσθετων καθηκόντων του που ορίζονται στον κανονισμό XX/XXX (πράξη για την αλληλεγγύη στον κυβερνοχώρο). Η εν λόγω πρόσθετη χρηματοδότηση δεν θέτει σε κίνδυνο την επίτευξη των στόχων του προγράμματος.***

Or. en

### **Τροπολογία 209**

**Enĵen Tošenovský**

#### **Πρόταση κανονισμού**

#### **Άρθρο 19 – παράγραφος 1 – σημείο 5**

Κανονισμός (ΕΕ) 2021/694



## Άρθρο 19

*Κείμενο που προτείνει η Επιτροπή*

Στήριξη με τη μορφή επιχορηγήσεων μπορεί να χορηγείται απευθείας από το ECCC χωρίς πρόσκληση υποβολής προτάσεων προς τα **εθνικά SOC** που αναφέρονται στο άρθρο 4 του κανονισμού XXXX **και την κοινοπραξία υποδοχής** που αναφέρεται στο άρθρο 5 του κανονισμού XXXX, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του δημοσιονομικού κανονισμού.

*Τροπολογία*

Στήριξη με τη μορφή επιχορηγήσεων μπορεί να χορηγείται απευθείας από το ECCC χωρίς πρόσκληση υποβολής προτάσεων προς τα **CSIRT-ISAC** που αναφέρονται στο άρθρο 4 του κανονισμού XXXX που αναφέρεται στο άρθρο 5 του κανονισμού XXXX, σύμφωνα με το άρθρο 195 παράγραφος 1 στοιχείο δ) του δημοσιονομικού κανονισμού.

Or. en

## Τροπολογία 210

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan**

### Πρόταση κανονισμού

#### Άρθρο 20 – τίτλος

*Κείμενο που προτείνει η Επιτροπή*

Αξιολόγηση

*Τροπολογία*

Αξιολόγηση **και επανεξέταση**

Or. en

## Τροπολογία 211

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Bușoi, Ioan-Rares Bogdan**

### Πρόταση κανονισμού

#### Άρθρο 20 – παράγραφος 1

*Κείμενο που προτείνει η Επιτροπή*

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.**

*Τροπολογία*

Έως [δύο έτη μετά την ημερομηνία εφαρμογής του παρόντος κανονισμού **και ακολούθως ανά δύο έτη**], η Επιτροπή **πραγματοποιεί αξιολόγηση της λειτουργίας των μέτρων που ορίζονται στον παρόντα κανονισμό και υποβάλλει**

*έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο.*

*Πιο συγκεκριμένα, στο πλαίσιο της αξιολόγησης εκτιμώνται:*

*α) η συμμετοχή των κρατών μελών στην ευρωπαϊκή κυβερνοασπίδα, συμπεριλαμβανομένου του αριθμού εθνικών SOC και διασυννοριακών SOC που έχουν συσταθεί στο πλαίσιο του κανονισμού και της αποτελεσματικότητας της ανταλλαγής πληροφοριών·*

*β) η συμβολή του παρόντος κανονισμού στην ενίσχυση της ανθεκτικότητας και της κυριαρχίας της Ένωσης, στη βελτίωση της ανταγωνιστικότητας των σχετικών τομέων της βιομηχανίας, συμπεριλαμβανομένων των ΜΜΕ, και στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας στην ΕΕ·*

*γ) η χρήση της εφεδρείας στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων αν το πεδίο εφαρμογής της εφεδρείας θα πρέπει να διευρυνθεί ώστε να περιλαμβάνει υπηρεσίες ετοιμότητας για περιστατικά ή κοινές ασκήσεις με τους αξιόπιστους παρόχους και τους πιθανούς χρήστες της εφεδρείας στον τομέα της κυβερνοασφάλειας, ώστε να διασφαλιστεί η αποτελεσματική λειτουργία της εφεδρείας όταν είναι αναγκαία·*

*δ) η συμβολή του παρόντος κανονισμού στην ανάπτυξη και βελτίωση των δεξιοτήτων και ικανοτήτων του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας, η οποία είναι αναγκαία για την ενίσχυση της ικανότητας της Ένωσης στην ανίχνευση, πρόληψη και αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας και στην ανάκαμψη από αυτά·*

*ε) η συμβολή του παρόντος κανονισμού στην εφαρμογή και ανάπτυξη τεχνολογιών αιχμής στην Ένωση·*

*Βάσει της εν λόγω έκθεσης, η Επιτροπή υποβάλλει, κατά περίπτωση, νομοθετική*

*πρόταση στο Ευρωπαϊκό Κοινοβούλιο και  
το Συμβούλιο για την τροποποίηση του  
παρόντος κανονισμού.*

Or. en

**Τροπολογία 212**  
**Enĵen Toĝenovský**

**Πρόταση κανονισμού**  
**Άρθρο 20 – παράγραφος 1**

*Κείμενο που προτείνει η Επιτροπή*

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.

*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. ***Η έκθεση συνοδεύεται, εφόσον είναι αναγκαίο, από νομοθετική πρόταση.***

Or. en

**Τροπολογία 213**  
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti**

**Πρόταση κανονισμού**  
**Άρθρο 20 – παράγραφος 1 α (νέα)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

***Κάθε έτος, κατά την υποβολή του σχεδίου προϋπολογισμού για το επόμενο έτος, η Επιτροπή υποβάλλει λεπτομερή αξιολόγηση των καθηκόντων του ENISA δυνάμει του παρόντος κανονισμού, καθώς και [της πρότασης σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία] και άλλων νομοθετικών πράξεων της Ένωσης, και περιγράφει λεπτομερώς τους δημοσιονομικούς και ανθρώπινους πόρους που απαιτούνται για την***

**Τροπολογία 214**

**Angelika Niebler, Sara Skytvedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Πρόταση κανονισμού**

**Άρθρο 20 α (νέο)**

*Κείμενο που προτείνει η Επιτροπή*

*Τροπολογία*

**Άρθρο 20α**

**Άσκηση της εξουσιοδότησης**

**1. Ανατίθεται στην Επιτροπή η εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις υπό τους όρους του παρόντος άρθρου.**

**2. Η εξουσία έκδοσης κατ' εξουσιοδότηση πράξεων που αναφέρεται στο άρθρο 12 παράγραφος 8 και στο άρθρο 13 παράγραφος 7 ανατίθεται στην Επιτροπή για περίοδο 5 ετών από την ... [ημερομηνία έναρξης ισχύος της βασικής νομοθετικής πράξης ή οποιαδήποτε άλλη ημερομηνία ορίσουν οι συννομοθέτες]. Η Επιτροπή υποβάλλει έκθεση σχετικά με τις εξουσίες που της έχουν ανατεθεί το αργότερο εννέα μήνες πριν από τη λήξη της περιόδου των πέντε ετών. Η εξουσιοδότηση ανανεώνεται σιωπηρά για περιόδους ίδιας διάρκειας, εκτός αν το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο προβάλλουν αντιρρήσεις το αργότερο εντός τριών μηνών πριν από τη λήξη της κάθε περιόδου.**

**3. Η εξουσιοδότηση που αναφέρεται στο άρθρο 12 παράγραφος 8 και στο άρθρο 13 παράγραφος 7 μπορεί να ανακληθεί ανά πάσα στιγμή από το Ευρωπαϊκό Κοινοβούλιο ή από το Συμβούλιο. Η απόφαση ανάκλησης περατώνει την εξουσιοδότηση που προσδιορίζεται στην εν λόγω απόφαση. Αρχίζει να ισχύει την επομένη της δημοσίευσης της απόφασης**

*στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ή σε μεταγενέστερη ημερομηνία που ορίζεται σε αυτή. Δεν θίγει το κύρος των κατ' εξουσιοδότηση πράξεων που ισχύουν ήδη.*

*4. Πριν από την έκδοση μιας κατ' εξουσιοδότηση πράξης, η Επιτροπή διεξάγει διαβουλεύσεις με εμπειρογνώμονες που ορίζουν τα κράτη μέλη σύμφωνα με τις αρχές της διοργανικής συμφωνίας της 13ης Απριλίου 2016 για τη βελτίωση του νομοθετικού έργου.*

*5. Μόλις εκδώσει κατ' εξουσιοδότηση πράξη, η Επιτροπή την κοινοποιεί ταυτόχρονα στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.*

*6. Η κατ' εξουσιοδότηση πράξη που εκδίδεται δυνάμει του άρθρου 12 παράγραφος 8 ή του άρθρου 13 παράγραφος 7 αρχίζει να ισχύει μόνον εφόσον δεν έχει διατυπωθεί αντίρρηση από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο εντός δύο μηνών από την ημέρα που η πράξη κοινοποιείται στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο ή αν, πριν λήξει αυτή η περίοδος, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενημερώσουν αμφότερα την Επιτροπή ότι δεν θα προβάλουν αντιρρήσεις. Η προθεσμία αυτή παρατείνεται κατά [δύο μήνες] κατόπιν πρωτοβουλίας του Ευρωπαϊκού Κοινοβουλίου ή του Συμβουλίου.*

Or. en

**Τροπολογία 215**  
**Enĵen Tošenovský**

**Πρόταση κανονισμού**  
**Παράρτημα I – παράγραφος 1 – σημείο 1**  
Κανονισμός (ΕΕ) 2021/694  
Παράρτημα I – κεφάλαιο «Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη»

1. Συνεπένδυση με τα κράτη μέλη σε προηγμένο εξοπλισμό, υποδομές και τεχνογνωσία κυβερνοασφάλειας που είναι ουσιώδεις για την προστασία των υποδομών ζωτικής σημασίας και της ψηφιακής ενιαίας αγοράς γενικότερα. Η εν λόγω συνεπένδυση θα μπορούσε να περιλαμβάνει επενδύσεις σε κβαντικές εγκαταστάσεις και πόρους δεδομένων για την κυβερνοασφάλεια, την αντίληψη της κατάστασης στον κυβερνοχώρο συμπεριλαμβανομένων των εθνικών SOC και των διασυννοριακών SOC που απαρτίζουν την ευρωπαϊκή κυβερνοασπίδα, καθώς και άλλα εργαλεία που θα τίθενται στη διάθεση του δημόσιου και του ιδιωτικού τομέα σε ολόκληρη την Ευρώπη.

1. Συνεπένδυση με τα κράτη μέλη σε προηγμένο εξοπλισμό, υποδομές και τεχνογνωσία κυβερνοασφάλειας που είναι ουσιώδεις για την προστασία των υποδομών ζωτικής σημασίας και της ψηφιακής ενιαίας αγοράς γενικότερα. Η εν λόγω συνεπένδυση θα μπορούσε να περιλαμβάνει επενδύσεις σε κβαντικές εγκαταστάσεις και πόρους δεδομένων για την κυβερνοασφάλεια, την αντίληψη της κατάστασης στον κυβερνοχώρο συμπεριλαμβανομένων των εθνικών CSIRT και SOC που απαρτίζουν την ευρωπαϊκή κυβερνοασπίδα, καθώς και άλλα εργαλεία που θα τίθενται στη διάθεση του δημόσιου και του ιδιωτικού τομέα σε ολόκληρη την Ευρώπη.

Or. en

## Τροπολογία 216 Enĵen Tošenovský

### Πρόταση κανονισμού Παράρτημα I – παράγραφος 1 – σημείο 1

Κανονισμός (ΕΕ) 2021/694

Παράρτημα I – κεφάλαιο «Ειδικός στόχος 3 – Κυβερνοασφάλεια και εμπιστοσύνη»

5. Προώθηση της αλληλεγγύης μεταξύ των κρατών μελών όσον αφορά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών στον τομέα της κυβερνοασφάλειας μέσω της ανάπτυξης υπηρεσιών κυβερνοασφάλειας σε διασυννοριακό επίπεδο, συμπεριλαμβανομένης της στήριξης για αμοιβαία συνδρομή μεταξύ των δημόσιων αρχών και της δημιουργίας εφεδρείας αξιόπιστων παρόχων κυβερνοασφάλειας σε επίπεδο Ένωσης.»

5. Προώθηση της αλληλεγγύης μεταξύ των κρατών μελών όσον αφορά την προετοιμασία και την αντιμετώπιση σημαντικών περιστατικών στον τομέα της κυβερνοασφάλειας μέσω της ανάπτυξης υπηρεσιών κυβερνοασφάλειας σε διασυννοριακό επίπεδο, συμπεριλαμβανομένης της στήριξης για αμοιβαία συνδρομή μεταξύ των δημόσιων αρχών και της δημιουργίας εφεδρείας αξιόπιστων παρόχων διαχειριζόμενων υπηρεσιών ασφάλειας σε επίπεδο Ένωσης.»

Or. en