Συμβούλιο της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 6 Ιουνίου 2025
(OR. en)

9794/25

Διοργανικός φάκελος:
2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	6 Ιουνίου 2025
Αποδέκτης:	Αντιπροσωπίες
Θέμα:	Σύσταση του Συμβουλίου σχετικά με σχέδιο στρατηγικής της ΕΕ για τη διαχείριση κυβερνοκρίσεων — Σύσταση του Συμβουλίου που εγκρίθηκε από το Συμβούλιο κατά τη σύνοδό του στις 6 Ιουνίου 2025

Διαβιβάζεται συνημμένως στις αντιπροσωπίες η σύσταση του Συμβουλίου, όπως εγκρίθηκε από το Συμβούλιο κατά τη σύνοδό του στις 6 Ιουνίου 2025.

ΠΑΡΑΡΤΗΜΑ

ΣΥΣΤΑΣΗ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

σχετικά με σχέδιο στρατηγικής της ΕΕ για τη διαχείριση κυβερνοκρίσεων

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης και ιδίως το άρθρο 114 και το άρθρο 292,

Έχοντας υπόψη την πρόταση της Ευρωπαϊκής Επιτροπής,

Εκτιμώντας τα ακόλουθα:

(1) Η ψηφιακή τεχνολογία και η παγκόσμια συνδεσιμότητα αποτελούν τη ραχοκοκαλιά της οικονομικής ανάπτυξης, της ανταγωνιστικότητας και του μετασχηματισμού των κρίσιμων υποδομών της Ένωσης. Ωστόσο, η διασυνδεδεμένη και ολοένα και πιο ψηφιακή οικονομία αυξάνει επίσης τον κίνδυνο εμφάνισης περιστατικών κυβερνοασφάλειας και κυβερνοεπιθέσεων. Επιπλέον οι αυξανόμενες γεωπολιτικές εντάσεις, συγκρούσεις και στρατηγικές αντιπαλότητες αντικατοπτρίζονται στον αντίκτυπο, στον όγκο και στην πολυπλοκότητα των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. Τέτοιες δραστηριότητες μπορούν να αποτελούν μέρος υβριδικών εκστρατειών ή στρατιωτικών επιχειρήσεων. Μπορούν επίσης να πλήξουν άμεσα την ασφάλεια, την οικονομία και την κοινωνία της Ένωσης. Επιπλέον, έχουν πιθανές δευτερογενείς επιπτώσεις, ιδίως όταν ο στόχος αυτών των δραστηριοτήτων είναι διεθνείς στρατηγικές χώρες-εταίροι, όπως υποψήφιες ή γειτονικές χώρες.

(2) Ένα μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας μπορεί να προκαλέσει διατάραξη τέτοιου επιπέδου, που να υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτή ή να έχει σημαντικό αντίκτυπο σε περισσότερα από ένα κράτη μέλη. Ένα τέτοιο περιστατικό, ανάλογα με την αιτία και τις συνέπειές του, θα μπορούσε να κλιμακωθεί και να μετατραπεί σε πλήρους κλίμακας κρίση που θα πλήξει την ομαλή λειτουργία της εσωτερικής αγοράς ή θα εκθέσει σε σοβαρό κίνδυνο τη δημόσια ασφάλεια και προστασία οντοτήτων ή πολιτών σε πολλά κράτη μέλη ή στην Ένωση στο σύνολό της.
Η αποτελεσματική διαχείριση κρίσεων είναι απαραίτητη για τη διατήρηση της οικονομικής σταθερότητας και την προστασία των ευρωπαϊκών κυβερνήσεων, των κρίσιμων υποδομών, των επιχειρήσεων και των πολιτών, καθώς και για τη συμβολή στη διεθνή ασφάλεια και σταθερότητα στον κυβερνοχώρο. Ως εκ τούτου, η διαχείριση κυβερνοκρίσεων αποτελεί αναπόσπαστο μέρος του πρωταρχικού πλαισίου διαχείρισης κρίσεων της ΕΕ.

(3) Δεδομένων των αλληλεξαρτήσεων και των διασυνδέσεων μεταξύ των περιβαλλόντων ΤΠΕ που χρησιμοποιούν οι οντότητες της Ένωσης και τα κράτη μέλη, ένα περιστατικό σε οντότητα της Ένωσης μπορεί να θέσει σε κίνδυνο την κυβερνοασφάλεια των κρατών μελών και αντιστρόφως. Η ανταλλαγή πληροφοριών σε αυτόν τον τομέα και ο συντονισμός όσον αφορά τόσο τα μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας όσο και τα σοβαρά περιστατικά, όπως ορίζονται στο άρθρο 3 παράγραφος 8 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841[1], έχουν ζωτική σημασία στο πλαίσιο του σχεδίου στρατηγικής της ΕΕ για τη διαχείριση κυβερνοκρίσεων («σχέδιο στρατηγικής για τον κυβερνοχώρο»).

[1] Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, ΕΕ L, 2023/2841, 18.12.2023, σ. 1.

(4) Σε περίπτωση κρίσης για την οποία έχει ενεργοποιηθεί η ολοκληρωμένη πολιτική αντιμετώπιση κρίσεων («IPCR») της ΕΕ δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2018/1993 του Συμβουλίου[2] («ρυθμίσεις IPCR»), το σχέδιο στρατηγικής για τον κυβερνοχώρο θα πρέπει να σέβεται πλήρως τις ρυθμίσεις IPCR για τον συντονισμό και την αντιμετώπιση. Ο πολιτικός και στρατηγικός συντονισμός θα πραγματοποιείται στο πλαίσιο της IPCR. Οι ρυθμίσεις IPCR αποτελούν το εργαλείο για οριζόντιο συντονισμό και αντιμετώπιση σε ενωσιακό πολιτικό επίπεδο. Σύμφωνα με τις ρυθμίσεις IPCR, την απόφαση για την ενεργοποίηση ή την απενεργοποίηση της IPCR λαμβάνει η Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης. Το έργο της IPCR όσον αφορά τόσο τη λειτουργία ανταλλαγής πληροφοριών όσο και τη θέση της σε λειτουργία πλήρους ενεργοποίησης υποστηρίζεται με εκθέσεις για την ολοκληρωμένη επίγνωση και ανάλυση καταστάσεων («ISAA») που εκπονούν οι υπηρεσίες της Επιτροπής και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης («ΕΥΕΔ»).

(5) Τα κράτη μέλη έχουν την πρωταρχική ευθύνη για τη διαχείριση περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων. Ωστόσο, ο δυνητικά διασυνοριακός και διατομεακός χαρακτήρας των περιστατικών κυβερνοασφάλειας απαιτεί από τα κράτη μέλη και τις αρμόδιες οντότητες της Ένωσης να συνεργάζονται σε τεχνικό, επιχειρησιακό και πολιτικό επίπεδο, ώστε να συντονίζονται αποτελεσματικά ανά την Ένωση. Η διαχείριση των κυβερνοκρίσεων καθ' όλη τη διάρκεια του κύκλου ζωής τους απαιτεί ετοιμότητα και κοινή επίγνωση της κατάστασης, ώστε να εντοπίζονται από πριν πιθανά μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας, να υπάρχουν οι αναγκαίες ικανότητες ανίχνευσης, ώστε να εντοπίζονται τα εργαλεία που απαιτούνται για την αντιμετώπιση και την αποκατάσταση καθώς και για τον μετριασμό και τον περιορισμό μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας, καθώς και οι ικανότητες αντίδρασης για την αποτροπή και την πρόληψη νέων περιστατικών.

---

[2] Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ολοκληρωμένες ρυθμίσεις της ΕΕ για την πολιτική αντιμετώπιση κρίσεων, ΕΕ L 320 της 17.12.2018, σ. 28.

(6) Η σύσταση (ΕΕ) 2017/1584 της Επιτροπής[3] για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο καθορίζει τους στόχους και τους τρόπους συνεργασίας μεταξύ των κρατών μελών και των οντοτήτων της Ένωσης με σκοπό την αντιμετώπιση μεγάλης κλίμακας περιστατικών στον κυβερνοχώρο και κυβερνοκρίσεων. Χαρτογραφεί τους σχετικούς φορείς σε τεχνικό, επιχειρησιακό και πολιτικό επίπεδο και εξηγεί πώς ενσωματώθηκαν στους υπάρχοντες μηχανισμούς της Ένωσης για τη διαχείριση κρίσεων, όπως οι ρυθμίσεις IPCR. Οι βασικές αρχές που προβλέπονται στη σύσταση (ΕΕ) 2017/1584, δηλαδή η επικουρικότητα, η συμπληρωματικότητα και η εμπιστευτικότητα των πληροφοριών, καθώς και η προσέγγιση τριών επιπέδων (τεχνικό, επιχειρησιακό και πολιτικό), εξακολουθούν να ισχύουν. Η παρούσα σύσταση στηρίζεται σε αυτές τις βασικές αρχές και προορίζεται να αντικαταστήσει τη σύσταση (ΕΕ) 2017/1584, θεσπίζοντας ένα νέο ενωσιακό πλαίσιο για τη διαχείριση κρίσεων κυβερνοασφάλειας.

(7) Κάποιοι από τους ορισμούς που χρησιμοποιούνται στην παρούσα σύσταση βασίζονται σε ορισμούς και όρους που έχουν χρησιμοποιηθεί στην οδηγία (ΕΕ) 2022/2555.[4] Ωστόσο, το πεδίο εφαρμογής της είναι διαφορετικό από εκείνο της οδηγίας (ΕΕ) 2022/2555. Η παρούσα σύσταση καθορίζει το ενωσιακό πλαίσιο για τη διαχείριση κυβερνοκρίσεων στο πλαίσιο της συνολικής ετοιμότητας της ΕΕ για μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις που προκύπτουν από τέτοια περιστατικά — ασχέτως του τομέα ή της οντότητας που πλήττεται. Στο μέτρο του δυνατού, οι ορισμοί βασίζονται στους ορισμούς της οδηγίας (ΕΕ) 2022/2555.

---

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

[4] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80).

(8) Απαιτείται ένα επικαιροποιημένο σχέδιο στρατηγικής για τον κυβερνοχώρο, το οποίο θα προσφέρει σαφή και κατανοητή καθοδήγηση και θα εξηγεί τι είναι ένα μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή μια πανενωσιακή κυβερνοκρίση, πώς ενεργοποιείται το πλαίσιο διαχείρισης κρίσεων και ποιοι είναι οι ρόλοι των σχετικών δικτύων, παραγόντων και φορέων σε επίπεδο Ένωσης, καθώς και πώς αλληλεπιδρούν οι εν λόγω φορείς και μηχανισμοί καθ' όλη τη διάρκεια του κύκλου ζωής μιας κυβερνοκρίσης. Το σχέδιο στρατηγικής για τον κυβερνοχώρο θέτει σαν στόχο να στηρίξει το ευρύτερο πλαίσιο των πολιτικοστρατιωτικών σχέσεων της ΕΕ σε συνάρτηση με τη διαχείριση κυβερνοκρίσεων, μεταξύ άλλων κατά την εμβάθυνση των σχέσεων ΕΕ-ΝΑΤΟ, όπου είναι δυνατόν με τη χρήση συμπεριληπτικών, αμοιβαίων και χωρίς διακρίσεις ενισχυμένων μηχανισμών ανταλλαγής πληροφοριών, για τη διαχείριση κυβερνοκρίσεων.

(9) Η διατομεακή διαχείριση κρίσεων σε επίπεδο Ένωσης θα πρέπει να ενισχυθεί ώστε να μπορεί να υπάρχει ολοκληρωμένη αντιμετώπιση στις κρίσεις, ιδίως σε περιπτώσεις κατά τις οποίες μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κρίσεις προκαλούν υλικές συνέπειες. Η παρούσα σύσταση συμπληρώνει τις ρυθμίσεις IPCR και άλλους ενωσιακούς μηχανισμούς διαχείρισης κρίσεων, συμπεριλαμβανομένων του γενικού συστήματος ταχείας προειδοποίησης ARGUS της Επιτροπής, του μηχανισμού πολιτικής προστασίας της Ένωσης («ΜΠΠΕ») που υποστηρίζεται από το Κέντρο Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών («ΚΣΑΕΑ») που συστάθηκε στο πλαίσιο του ΜΠΠΕ με την απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί μηχανισμού πολιτικής προστασίας της Ένωσης[5] («απόφαση ΜΠΠΕ»), του μηχανισμού αντιμετώπισης κρίσεων της ΕΥΕΔ («CRM»), καθώς και άλλες διαδικασίες, όπως αυτές που περιγράφονται στην εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο[6], στην εργαλειοθήκη για τις υβριδικές απειλές[7] και στο αναθεωρημένο πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών.[8] Συμπληρώνει επίσης και θα πρέπει να συνάδει με τη σύσταση (ΕΕ) 2024/4371 του Συμβουλίου σχετικά με σχέδιο στρατηγικής για τον συντονισμό της αντιμετώπισης σε ενωσιακό επίπεδο διαταράξεων σε υποδομές ζωτικής σημασίας με σημαντικό διασυνοριακό ενδιαφέρον[9] («σχέδιο στρατηγικής της ΕΕ για τις κρίσιμες υποδομές»), το οποίο καλύπτει την υλική ανθεκτικότητα εκτός κυβερνοχώρου, και αποσκοπεί στη βελτίωση του συντονισμού της αντίδρασης σε επίπεδο Ένωσης σε αυτόν τον τομέα.

---

5 Απόφαση αριθ. 1313/2013/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2013, περί μηχανισμού πολιτικής προστασίας της Ένωσης, ΕΕ L 347 της 20.12.2013, σ. 924.

6 Συμπεράσματα του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο (9916/17)

7 Συμπεράσματα του Συμβουλίου σχετικά με πλαίσιο για τη συντονισμένη αντίδραση της ΕΕ σε υβριδικές εκστρατείες, 22 Ιουνίου 2022

8 Κοινό έγγραφο εργασίας των υπηρεσιών της Επιτροπής — Πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών (SWD (2023) 116 τελικό).

9 ΕΕ C, C/2024/4371, 5.7.2024.

(10) Το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο («EU-CyCLONe») είναι το δίκτυο για τον συντονισμό της διαχείρισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων σε επιχειρησιακό επίπεδο, όπως και σε περίπτωση διατομεακών μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων. Προκειμένου να μην περιπλακούν περαιτέρω τα υφιστάμενα πλαίσια, θα πρέπει να αποφευχθεί η δημιουργία τομεακών δομών που θα αλληλεπικαλύπτονται με τα καθήκοντα του EU-CyCLONe. Το EU-CyCLONe θα πρέπει να λαμβάνει και από τους τομείς επιχειρησιακές πληροφορίες σχετικές με την κυβερνοασφάλεια και να τις διαβιβάζει στο πολιτικό επίπεδο.

(11) Αναμένεται από τα κράτη μέλη να αξιοποιήσουν πλήρως τους χρηματοδοτικούς πόρους που διατίθενται για την κυβερνοασφάλεια, οι οποίοι παρέχονται από σχετικά προγράμματα της Ένωσης. Θα πρέπει να διασφαλίζεται ότι τα προγράμματα αυτά επιβάλλουν ελάχιστες διοικητικές επιβαρύνσεις στους αιτούντες χρηματοδότηση και ότι η συμμετοχή των κρατών μελών στα εν λόγω προγράμματα διευκολύνεται με την παροχή σχετικής καθοδήγησης για βιώσιμες επιλογές χρηματοδοτικής στήριξης.

(12) Η παρούσα σύσταση συμβάλλει σε ευρύτερες δράσεις ετοιμότητας που απαιτούνται, ώστε η Ένωση να αντιμετωπίζει διατομεακές κρίσεις σύμφωνα με τις αρχές που περιλαμβάνονται στη στρατηγική της ΕΕ για την Ένωση Ετοιμότητας: μια ολοκληρωμένη προσέγγιση για όλους τους κινδύνους, για το σύνολο της διοίκησης και για το σύνολο της κοινωνίας, ιδίως όσον αφορά τη βελτίωση της ευαισθητοποίησης σχετικά με τους κινδύνους και τις απειλές και τη διατομεακή αντιμετώπιση κρίσεων,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

Ι: Σκοπός, πεδίο εφαρμογής και κατευθυντήριες αρχές του ενωσιακού πλαισίου διαχείρισης κυβερνοκρίσεων

Σκοπός και πεδίο εφαρμογής

1) Η παρούσα σύσταση για σχέδιο στρατηγικής της ΕΕ για τη διαχείριση κυβερνοκρίσεων («σχέδιο στρατηγικής για τον κυβερνοχώρο») καθορίζει το ενωσιακό πλαίσιο για τη διαχείριση κυβερνοκρίσεων στο πλαίσιο της εν γένει ετοιμότητας της ΕΕ για μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις. Στο πλαίσιο αυτό απεικονίζονται οι ρόλοι τόσο των κρατών μελών όσο και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης («οντότητες της Ένωσης») εντός των οικείων τους αρμοδιοτήτων, με πλήρη σεβασμό των εθνικών νομοθεσιών και εσωτερικών κανόνων, με σκοπό να διασφαλίζεται η ολοκληρωμένη και συντονισμένη δράση σε επίπεδο Ένωσης.

2) Το σχέδιο στρατηγικής για τον κυβερνοχώρο θα πρέπει να εφαρμόζεται σύμφωνα με το σχέδιο στρατηγικής της ΕΕ για τις κρίσιμες υποδομές, ιδίως στην περίπτωση περιστατικών που επηρεάζουν τόσο την υλική ανθεκτικότητα όσο και την κυβερνοασφάλεια των κρίσιμων υποδομών[10].

3) Το σχέδιο στρατηγικής για τον κυβερνοχώρο παρέχει καθοδήγηση για την αντιμετώπιση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας ή κυβερνοκρίσεων και θα πρέπει να χρησιμοποιείται συμπληρωματικά με τους όποιους σχετικούς τομεακούς μηχανισμούς αντιμετώπισης, όπως εκείνοι που απαριθμούνται στο παράρτημα ΙΙ. Τα ενδιαφερόμενα μέρη στον τομέα της κυβερνοασφάλειας θα πρέπει να βοηθούν και να επικουρούν, προκειμένου να επιτυγχάνονται οι στόχοι των εν λόγω τομεακών μηχανισμών, τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο.

4) Σε περίπτωση πανενωσιακής και διατομεακής κρίσης που περιλαμβάνει και θέματα κυβερνοχώρου και για την οποία ενεργοποιείται η IPCR τον συντονισμό της αντίδρασης σε ενωσιακό πολιτικό επίπεδο θα πρέπει να αναλαμβάνει το Συμβούλιο, χρησιμοποιώντας τις ρυθμίσεις IPCR. Αφού ενεργοποιηθεί η IPCR, τα μέτρα βάσει του σχεδίου στρατηγικής για τον κυβερνοχώρο θα πρέπει να στηρίζουν την αντίδραση της ΕΕ σε πολιτικό επίπεδο, παρέχοντας συγκεκριμένη στήριξη για την κυβερνοασφάλεια.

---

10 Το σχέδιο στρατηγικής της ΕΕ για τις κρίσιμες υποδομές περιγράφει λεπτομερέστερα τον συντονισμό στις περιπτώσεις αυτές στο τμήμα 4 του μέρους Ι του παραρτήματός του.

Κατευθυντήριες αρχές

5) Για τη διαχείριση κυβερνοκρίσεων σε επίπεδο Ένωσης ισχύουν οι ακόλουθες κατευθυντήριες αρχές:

α) *Αναλογικότητα*: τα περισσότερα περιστατικά κυβερνοασφάλειας που πλήττουν κράτη μέλη δεν πληρούν τα απαραίτητα κριτήρια ώστε να θεωρηθούν εθνικό ή ενωσιακό μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση. Σε περίπτωση περιστατικών και απειλών στον τομέα της κυβερνοασφάλειας τα κράτη μέλη συνεργάζονται και ανταλλάσσουν πληροφορίες, οικειοθελώς και σε τακτική βάση, στο πλαίσιο του δικτύου ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστών («δίκτυο CSIRT») και του EU-CyCLONe, σύμφωνα με τις τυποποιημένες διαδικασίες λειτουργίας («SOP») των δικτύων.

β) *Επικουρικότητα*: σε περίπτωση που πληγούν από περιστατικό κυβερνοασφάλειας, μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση, τα κράτη μέλη έχουν την πρωταρχική ευθύνη για την αντιμετώπισή τους και την αποκατάσταση. Σε περίπτωση διασυνοριακών επιπτώσεων, το Συμβούλιο, η Επιτροπή, ο Ύπατος Εκπρόσωπος, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια («ENISA»), η Υπηρεσία Κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης («CERT-EE»), ο Ευρωπόλ και όλες οι άλλες συναρμόδιες οντότητες της Ένωσης θα πρέπει να συνεργάζονται καθ' όλη τη διάρκεια του κύκλου ζωής της κρίσης. Ο ρόλος αυτός απορρέει από το δίκαιο της Ένωσης και αντανακλά το γεγονός ότι τα μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και οι κυβερνοκρίσεις επηρεάζουν έναν ή περισσότερους τομείς της οικονομικής δραστηριότητας στην ενιαία αγορά, την ασφάλεια και τις διεθνείς σχέσεις της Ένωσης, καθώς και τις οντότητες της Ένωσης.

γ) *Συμπληρωματικότητα*: η σύσταση λαμβάνει πλήρως υπόψη τους υφιστάμενους μηχανισμούς διαχείρισης κρίσεων σε επίπεδο Ένωσης που απαριθμούνται στο παράρτημα ΙΙ, και ειδικότερα τις ρυθμίσεις IPCR, το ARGUS και τον CRM της ΕΥΕΔ. Η παρούσα σύσταση λαμβάνει υπόψη τις εντολές που έχουν ανατεθεί στο δίκτυο CSIRT και στο EU-CyCLONe, καθώς και τον κανονισμό (ΕΕ, Ευρατόμ) 2023/2841. Όταν ενεργοποιείται η IPCR, οι εργασίες των οικείων δικτύων, οντοτήτων και ενεργοποιημένων τομεακών μηχανισμών θα πρέπει να συνεχίζονται και να εντάσσονται στον πολιτικό και στρατηγικό συντονισμό που πραγματοποιεί η IPCR και να τον στηρίζουν.

δ) *Εμπιστευτικότητα των πληροφοριών*: όλες οι ανταλλαγές πληροφοριών στο πλαίσιο της παρούσας σύστασης πρέπει να συμμορφώνονται με τους ισχύοντες κανόνες για την ασφάλεια και την προστασία δεδομένων προσωπικού χαρακτήρα. Εφόσον συντρέχει περίπτωση, θα πρέπει να λαμβάνονται υπόψη οι άτυπες συμφωνίες περί μη γνωστοποίησης, όπως το πρωτόκολλο «traffic light» για την επισήμανση ευαίσθητων πληροφοριών. Για την ανταλλαγή διαβαθμισμένων πληροφοριών –και ανεξάρτητα από το εφαρμοζόμενο σύστημα διαβάθμισης– θα πρέπει, παράλληλα με τα διαθέσιμα διαπιστευμένα εργαλεία, να χρησιμοποιούνται οι υφιστάμενοι δεσμευτικοί κανόνες και συμφωνίες για την επεξεργασία διαβαθμισμένων πληροφοριών.

6) Σύμφωνα με τις προαναφερθείσες κατευθυντήριες αρχές, τα κράτη μέλη και οι οντότητες της Ένωσης θα πρέπει να εμβαθύνουν τη συνεργασία τους για τη διαχείριση κυβερνοκρίσεων ενισχύοντας την αμοιβαία εμπιστοσύνη και αξιοποιώντας τα υφιστάμενα δίκτυα και τους υφιστάμενους μηχανισμούς. Η συνεργασία αυτή, στο πλαίσιο του σχεδίου στρατηγικής για τον κυβερνοχώρο, διευκολύνεται από την εφαρμογή των άρθρων 22 και 23 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841. Πιο συγκεκριμένα, το σχέδιο διαχείρισης κυβερνοκρίσεων που καταρτίστηκε βάσει του άρθρου 23 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841, μεταξύ άλλων συμβάλλει στην τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των οντοτήτων της Ένωσης και με τα κράτη μέλη και καθορίζει ρυθμίσεις σχετικές με τον συντονισμό και τη ροή πληροφοριών μεταξύ οντοτήτων της Ένωσης.

ΙΙ: Ορισμοί

7) Για τον σκοπό του σχεδίου στρατηγικής για τον κυβερνοχώρο ισχύουν οι ακόλουθοι ορισμοί:

α) «περιστατικό»: συμβάν που θέτει σε κίνδυνο τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω συστημάτων δικτύων και πληροφοριών·

β) «σημαντικό περιστατικό»: περιστατικό το οποίο:

α. έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διατάραξη των υπηρεσιών ή οικονομική ζημία για την οικεία οντότητα·

β. έχει επηρεάσει ή είναι ικανό να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία·

γ) «μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας»: περιστατικό το οποίο προκαλεί διατάραξη που υπερβαίνει την ικανότητα ενός κράτους μέλους να ανταποκριθεί σε αυτήν, ή το οποίο έχει σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη·

δ) «κυβερνοκρίση»: μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας το οποίο έχει κλιμακωθεί σε πλήρους κλίμακας κρίση που παρεμποδίζει την ομαλή λειτουργία της εσωτερικής αγοράς ή εκθέτει σε σοβαρό κίνδυνο τη δημόσια ασφάλεια και προστασία οντοτήτων ή πολιτών σε πολλά κράτη μέλη ή στην Ένωση στο σύνολό της.

ΙΙΙ: Οι εθνικές δομές διαχείρισης κυβερνοκρίσεων και οι ευθύνες τους

8) Σε περίπτωση που πληγούν από μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας ή κυβερνοκρίσεις, τα κράτη μέλη έχουν την πρωταρχική ευθύνη για την αντιμετώπισή τους. Σύμφωνα με την οδηγία (ΕΕ) 2022/2555, κάθε κράτος μέλος διαθέτει μία ή περισσότερες αρχές διαχείρισης κυβερνοκρίσεων, καθώς και μία ή περισσότερες CSIRT.

9) Με την έκδοση της οδηγίας (ΕΕ) 2022/2555 και άλλων νομοθετικών και μη νομοθετικών πράξεων για την κυβερνοασφάλεια, τα κράτη μέλη έχουν αναλάβει να ευθυγραμμίσουν τα οικεία πλαίσια κυβερνοασφάλειας, θεσπίζοντας ελάχιστους κανόνες για τη λειτουργία του συντονισμένου κανονιστικού πλαισίου, καθορίζοντας μηχανισμούς για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος και παρέχοντας αποτελεσματικά μέσα έννομης προστασίας και μέτρα επιβολής τα οποία έχουν καθοριστική σημασία για την αποτελεσματική επιβολή των εν λόγω υποχρεώσεων.

10) Σύμφωνα με το άρθρο 9 παράγραφος 4 της οδηγίας (ΕΕ) 2022/2555, τα κράτη μέλη θεσπίζουν εθνικά σχέδια αντιμετώπισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων. Τα σχέδια αυτά περιλαμβάνουν, μεταξύ άλλων, εθνικά μέτρα ετοιμότητας, διαδικασίες διαχείρισης κυβερνοκρίσεων και εθνικές διαδικασίες καθώς και ρυθμίσεις μεταξύ εθνικών αρχών και φορέων που θα διασφαλίζουν την αποτελεσματική τους συμμετοχή και στήριξη της συντονισμένης διαχείρισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων σε επίπεδο Ένωσης. Οι διαδικασίες διαχείρισης κυβερνοκρίσεων περιλαμβάνουν επίσης διατάξεις για την ενσωμάτωσή τους στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων και στους διαύλους ανταλλαγής πληροφοριών.

11) Σύμφωνα με το άρθρο 9 παράγραφος 1 της οδηγίας (ΕΕ) 2022/2555, τα κράτη μέλη θα πρέπει να διασφαλίζουν τη συνοχή με τα υφιστάμενα πλαίσια για τη γενική εθνική διαχείριση κρίσεων. Σε περίπτωση που ενεργοποιηθεί η IPCR, οι εθνικές αρχές διαχείρισης κρίσεων θα πρέπει να συλλέγουν στοιχεία από τις αρχές διαχείρισης κυβερνοκρίσεων και τους εθνικούς τομεακούς μηχανισμούς αντιμετώπισης κρίσεων για να ενημερώνουν την IPCR.

12) Σύμφωνα με το άρθρο 9 παράγραφος 5 της οδηγίας (ΕΕ) 2022/2555, το EU-CyCLONe, κατόπιν αιτήματος ενδιαφερόμενου κράτους μέλους, θα πρέπει να ανταλλάσσει πληροφορίες σχετικά με τα μέρη των εθνικών σχεδίων αντιμετώπισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων, ιδίως όσον αφορά τις διατάξεις για τη διασφάλιση της αποτελεσματικής συμμετοχής και στήριξης της συντονισμένης διαχείρισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων σε επίπεδο Ένωσης, προκειμένου να ανταλλάσσονται βέλτιστες πρακτικές και να εξετάζεται αν το συνολικό πλαίσιο θα λειτουργεί στην πράξη.

13) Το EU-CyCLONe και το διοργανικό συμβούλιο κυβερνοασφάλειας («IICB») καλούνται να ανταλλάσσουν, εφόσον συντρέχει περίπτωση, στοιχεία σχετικά με τη συνοχή του σχεδίου διαχείρισης κρίσεων που καταρτίζει το IICB σύμφωνα με το άρθρο 23 του κανονισμού (ΕΕ, Ευρατόμ) 2023/2841 με τα εθνικά σχέδια αντιμετώπισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων.

14) Το EU-CyCLONe, υποστηριζόμενο από τον ENISA ως γραμματεία του, τηρεί επικαιροποιημένο κατάλογο των εθνικών αρχών διαχείρισης κυβερνοκρίσεων με τα στοιχεία επικοινωνίας των υπαλλήλων και των στελεχών του EU-CyCLONe και τον θέτει στη διάθεση των μελών του EU-CyCLONe.

IV: Κύρια δίκτυα και φορείς στο οικοσύστημα της ΕΕ για τη διαχείριση κυβερνοκρίσεων

15) Το δίκτυο CSIRT είναι το κύριο τεχνικό δίκτυο για την ανταλλαγή πληροφοριών σχετικά με περιστατικά, ιδίως δε περιστατικά σχετικά με το πεδίο εφαρμογής της παρούσας σύστασης, σύμφωνα με τα καθήκοντα που περιγράφονται στο άρθρο 15 παράγραφος 3 της οδηγίας (ΕΕ) 2022/2555. Συμβάλλει στην ανάπτυξη εμπιστοσύνης και στην προώθηση ταχείας και αποτελεσματικής επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών. Ο πρόεδρος του δικτύου CSIRT μπορεί να συμμετέχει ως παρατηρητής στο IICB.

16) Η CERT-ΕΕ είναι η υπηρεσία κυβερνοασφάλειας για όλες τις οντότητες της Ένωσης. Η CERT-ΕΕ λειτουργεί ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας για τις οντότητες της Ένωσης, σύμφωνα με το άρθρο 13 του κανονισμού (ΕΕ) 2023/2841. Η CERT-ΕΕ είναι μέλος του δικτύου CSIRT και υποστηρίζει την Επιτροπή στο EU-CyCLONe. Η CERT-ΕΕ λειτουργεί σε τεχνικό επίπεδο και είναι υπεύθυνη για τον συντονισμό της διαχείρισης σοβαρών περιστατικών που πλήττουν οντότητες της Ένωσης.

17) Το EU-CyCLONe λειτουργεί ως διαμεσολαβητής μεταξύ του τεχνικού και του πολιτικού επιπέδου, ιδίως κατά τη διάρκεια μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων. Υποστηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων σε επιχειρησιακό επίπεδο και διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης σύμφωνα με το άρθρο 16 της οδηγίας (ΕΕ) 2022/2555. Ο πρόεδρος του EU-CyCLONe μπορεί να συμμετέχει ως παρατηρητής στο IICB.

18) Ο ENISA είναι οργανισμός της Ένωσης ο οποίος εκτελεί τα καθήκοντα που του ανατίθενται δυνάμει του κανονισμού (ΕΕ) 2019/881[11], με σκοπό να επιτύχει ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, μεταξύ άλλων υποστηρίζοντας ενεργά τα κράτη μέλη, τα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης.
Ο ENISA παρέχει, μεταξύ άλλων, γραμματειακή υποστήριξη στο δίκτυο CSIRT και στο EU-CyCLONe, υπηρεσίες επίγνωσης της κατάστασης και βοηθά τα κράτη μέλη διοργανώνοντας τακτικά ασκήσεις κυβερνοασφάλειας σε ενωσιακό επίπεδο. Σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και τον κανονισμό (ΕΕ) 2024/2847[12], ο ENISA λαμβάνει πληροφορίες σχετικά με σημαντικά διασυνοριακά περιστατικά και τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και με περιστατικά που πλήττουν ψηφιακά προϊόντα.

19) Το Συμβούλιο της Ευρωπαϊκής Ένωσης («Συμβούλιο») είναι το θεσμικό όργανο στο οποίο έχουν ανατεθεί καθήκοντα χάραξης πολιτικής και συντονισμού σύμφωνα με το άρθρο 16 της Συνθήκης για την Ευρωπαϊκή Ένωση («ΣΕΕ») και είναι επιφορτισμένο με την IPCR που αφορά τον συντονισμό και την αντιμετώπιση σε ενωσιακό πολιτικό επίπεδο. Το Συμβούλιο λειτουργεί μέσω των συνθέσεων του Συμβουλίου, της Επιτροπής των Μόνιμων Αντιπροσώπων και των σχετικών προπαρασκευαστικών οργάνων του Συμβουλίου, ιδίως της Οριζόντιας Ομάδας «Θέματα κυβερνοχώρου» («HWPCI»), καθώς και, κατά περίπτωση, των ρυθμίσεων IPCR.

---

11 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), ΕΕ L 151 της 7.6.2019, σ. 15.

12 Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα), ΕΕ L, 2024/2847, 20.11.2024, σ. 1.

20) Η Επιτροπή, ως το θεσμικό όργανο που προωθεί το γενικό συμφέρον της Ένωσης και αναλαμβάνει τις ενδεδειγμένες πρωτοβουλίες για τον σκοπό αυτόν, ενώ παράλληλα διασφαλίζει την εφαρμογή των Συνθηκών και των μέτρων που θεσπίζουν τα θεσμικά όργανα δυνάμει του άρθρου 17 της ΣΕΕ, είναι υπεύθυνη για ορισμένες δράσεις γενικής ετοιμότητας σε επίπεδο Ένωσης και ορισμένες δράσεις επίγνωσης της κατάστασης, συμπεριλαμβανομένης της διαχείρισης του ΚΣΑΕΑ και του κοινού συστήματος επικοινωνίας και πληροφόρησης έκτακτης ανάγκης («CECIS»), σύμφωνα με την απόφαση για τον ΜΠΠΕ. Διευκολύνει τη συνοχή και τον συντονισμό μεταξύ συναφών πανενωσιακών δράσεων αντιμετώπισης κρίσεων σε επιχειρησιακό επίπεδο. Ζητείται η γνώμη της σχετικά με αποφάσεις ενεργοποίησης ή απενεργοποίησης της IPCR. Οι υπηρεσίες της Επιτροπής καταρτίζουν, μαζί με την ΕΥΕΔ, τις εκθέσεις ISAA. Είναι μέλος του EU-CyCLONe σε περιπτώσεις όπου δυνητικό ή υπό εξέλιξη μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας έχει ή είναι πιθανό να έχει σημαντικό αντίκτυπο σε υπηρεσίες και δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2022/2555 και σε άλλες περιπτώσεις είναι παρατηρητής. Είναι επίσης το σημείο επαφής του IICB με το EU-CyCLONe. και παρατηρητής στο δίκτυο CSIRT.

21) Ο Ύπατος Εκπρόσωπος για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας (Ύπατος Εκπρόσωπος), επικουρούμενος από την ΕΥΕΔ, ασκεί την Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας της Ένωσης («ΚΕΠΠΑ») και συμβάλλει με τις προτάσεις του στην ανάπτυξη της πολιτικής αυτής καθώς και της Κοινής Πολιτικής Ασφάλειας και Άμυνας («ΚΠΑΑ»). Για την υλοποίηση των ανωτέρω υπάρχουν διπλωματικές και στρατιωτικές δομές και μηχανισμοί καθώς και δομές και μηχανισμοί πληροφοριών, ιδίως η ενιαία ικανότητα ανάλυσης πληροφοριών (SIAC) –το ενιαίο σημείο εισόδου πληροφοριών από τα κράτη μέλη– το Στρατιωτικό Επιτελείο της ΕΕ (EUMS) – πηγή στρατιωτικής εμπειρογνωσίας– η εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο, καθώς και το δίκτυο των αντιπροσωπιών της ΕΕ, που μπορούν να συμβάλουν στη διαχείριση κρίσεων από εξωτερική διάσταση. Η ΕΥΕΔ καταρτίζει επίσης, μαζί με την Επιτροπή, τις εκθέσεις ISAA.

22) Στο παράρτημα ΙΙ περιγράφονται οι ρόλοι και οι αρμοδιότητες των φορέων σε επίπεδο Ένωσης για θέματα που αφορούν τη διαχείριση κυβερνοκρίσεων, συμπεριλαμβανομένων των κύριων δικτύων και φορέων.

V: Προετοιμασία για μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις

Τοπίο των απειλών

23) Τα κράτη μέλη και οι αρμόδιες οντότητες της Ένωσης θα πρέπει να λαμβάνουν τα αναγκαία μέτρα προκειμένου να αποκτούν καλύτερη επίγνωση της κατάστασης, αναγνωρίζοντας ότι το τοπίο των απειλών και η επίγνωση της κατάστασης ανά περιστατικό απαιτούν διαφορετικούς τρόπους λειτουργίας. Τα κράτη μέλη και οι αρμόδιες οντότητες της Ένωσης θα πρέπει να συνεργάζονται βάσει επαληθευμένων και αξιόπιστων δεδομένων, συμπεριλαμβανομένων των τάσεων που παρουσιάζουν τα περιστατικά, οι τακτικές, οι τεχνικές και οι διαδικασίες, καθώς και των τρωτών σημείων που αποτελούν αντικείμενο ενεργού εκμετάλλευσης.

24) Κατά την ανταλλαγή πληροφοριών σε ενωσιακό επίπεδο, τα κράτη μέλη θα πρέπει να αξιοποιούν πλήρως τις υφιστάμενες πλατφόρμες τεχνικής και επιχειρησιακής συνεργασίας, όπως αυτές που χρησιμοποιούν το δίκτυο CSIRT και το EU-CyCLONe.

25) Προκειμένου να ενισχύεται κοινή επίγνωση της κατάστασης και να διευκολύνεται η αξιολόγηση του αντικτύπου της ΕΕ, το EU-CyCLONe και το δίκτυο CSIRT, με την υποστήριξη του ENISA, θα πρέπει να χρησιμοποιούν εσωτερικά συμφωνημένο μηχανισμό υποβολής εκθέσεων για την επισκόπηση των τεχνικών και επιχειρησιακών δραστηριοτήτων σε επίπεδο ΕΕ με βάση τις πληροφορίες που συλλέγονται σε εθνικό επίπεδο.

26) Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει:

α) να συνεργάζονται για τη βελτίωση της ανταλλαγής πληροφοριών μεταξύ του τεχνικού και επιχειρησιακού επιπέδου και της επίγνωσης της κατάστασης στο σύνολό της·

β) να συνεχίσουν να οικοδομούν κλίμα εμπιστοσύνης μεταξύ των μελών τους και μεταξύ των δικτύων·

γ) να αξιοποιούν πλήρως τα διαθέσιμα εργαλεία για την ανταλλαγή πληροφοριών, με την υποστήριξη του ENISA, να εξετάζουν τρόπους βελτίωσης των εργαλείων αυτών και να διασφαλίζουν τη διαλειτουργικότητα μεταξύ των δικτύων.

27) Το EU-CyCLONe, το δίκτυο CSIRT και το IICB θα πρέπει να συνεργάζονται, ώστε να διασφαλίζουν την αποτελεσματική ανταλλαγή των σχετικών πληροφοριών.

28) Ο ENISA, ως γραμματεία του δικτύου CSIRT και του EU-CyCLONe, διαδραματίζει κεντρικό ρόλο στη στήριξη των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, προκειμένου να καταλήγουν σε κοινή ανά την Ένωση επίγνωση της κατάστασης σε τεχνικό και επιχειρησιακό επίπεδο, με σκοπό την υποστήριξη στην προετοιμασία για μεγάλης κλίμακας περιστατικά και κυβερνοκρίσεις.

29) Σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και τον κανονισμό (ΕΕ) 2019/881, τα κράτη μέλη και οι αρμόδιες οντότητες της Ένωσης θα πρέπει να συντονίζονται με τον ιδιωτικό τομέα, συμπεριλαμβανομένων των κοινοτήτων ανοικτού κώδικα και των κατασκευαστών, για να βελτιώνουν την ανταλλαγή πληροφοριών. Ειδικότερα, ο ENISA θα πρέπει να κάνει χρήση του προγράμματος εταιρικών του σχέσεων στο πλαίσιο αυτό. Επιπλέον, τα κράτη μέλη και οι σχετικές οντότητες της Ένωσης θα μπορούσαν επίσης να αξιοποιήσουν τα υφιστάμενα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών («ISAC») σε ενωσιακό και εθνικό επίπεδο, προκειμένου να ενισχύουν την ικανότητα στον τομέα της κυβερνοασφάλειας και της αντιμετώπισης περιστατικών κυβερνοασφάλειας, μεταξύ άλλων μέσω κοινών συνεδριάσεων του ιδιωτικού τομέα με το EU-CyCLONe ή το δίκτυο CSIRT.

30) Για να ενισχυθεί η ανταλλαγή πληροφοριών εντός και μεταξύ των δικτύων και για να αποσαφηνιστούν οι εκατέρωθεν προσδοκίες από μια τέτοια ανταλλαγή, το EU-CyCLONe θα πρέπει, με την υποστήριξη του ENISA ως γραμματείας, και έπειτα από διαβούλευση με το δίκτυο CSIRT και την ομάδα συνεργασίας NIS, να συμφωνήσει εντός 24μήνου από την έκδοση της παρούσας σύστασης σχετικά με μια κοινή ευθυγραμμισμένη ταξινομία των επιπέδων σοβαρότητας των περιστατικών. Με την ταξινομία αυτή θα πρέπει να μπορεί να συγκρίνεται η σοβαρότητα περιστατικών στα κράτη μέλη, λαμβάνοντας υπόψη τον αντίκτυπο στην παροχή υπηρεσιών, τον αριθμό των επηρεαζόμενων οντοτήτων και την αντίστοιχη συνάφειά τους, τον αντίκτυπο σε άλλες υπηρεσίες και υποδομές, καθώς και τη χρηματική ζημία, τη ζημία στη φήμη και την πολιτική ζημία που προκλήθηκε. Θα πρέπει να βασίζεται σε παρεμφερείς ήδη υπάρχουσες κλίμακες ή ταξινομίες, όπως η ταξινομία ταξινόμησης περιστατικών αναφοράς.

Τεχνικό επίπεδο

31) Το δίκτυο CSIRT είναι η πλατφόρμα για την τεχνική συνεργασία και την ανταλλαγή πληροφοριών μεταξύ όλων των κρατών μελών και μέσω της CERT-ΕΕ με τις οντότητες της Ένωσης.

32) Σύμφωνα με την οδηγία (ΕΕ) 2022/2555, κάθε CSIRT έχει καθήκον να παρακολουθεί και να αναλύει κυβερνοαπειλές, τρωτά σημεία και περιστατικά σε εθνικό επίπεδο. Οι CSIRT θα πρέπει να ανταλλάσσουν, τόσο εντός του δικτύου CSIRT όσο και διμερώς, πληροφορίες σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και τρωτά σημεία, ώστε να αποκτούν κοινή επίγνωση της κατάστασης.

33) Για να ενισχυθεί η επιχειρησιακή συνεργασία σε επίπεδο Ένωσης, το δίκτυο CSIRT θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλεί όργανα και οργανισμούς της Ένωσης που εμπλέκονται στην πολιτική για την κυβερνοασφάλεια, όπως ο Ευρωπόλ, να συμμετέχουν στις εργασίες του.

34) Σύμφωνα με τον κανονισμό 2023/2841, η CERT-ΕΕ θα πρέπει να συλλέγει, να διαχειρίζεται, να αναλύει και να ανταλλάσσει πληροφορίες με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης σχετικά με κυβερνοαπειλές, τρωτά σημεία και περιστατικά σε μη διαβαθμισμένες υποδομές ΤΠΕ και, όταν απαιτείται, να απευθύνει συγκεκριμένες προτάσεις στο ΙΙCB για κατευθυντήριες γραμμές και συστάσεις προς τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης. Η CERT-ΕΕ θα πρέπει να συνεργάζεται και να ανταλλάσσει πληροφορίες με τους ομολόγους της στα κράτη μέλη, μεταξύ άλλων μέσω του δικτύου CSIRT.

Επιχειρησιακό επίπεδο

35) Σύμφωνα με την οδηγία (ΕΕ) 2022/2555, το EU-CyCLONe θα πρέπει να λειτουργεί ως πλατφόρμα συνεργασίας μεταξύ των αρχών διαχείρισης κυβερνοκρίσεων των κρατών μελών και, μέσω της Επιτροπής, με τις αρμόδιες οντότητες της Ένωσης, με στόχο την αύξηση του επιπέδου ετοιμότητας για τη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων και την ανάπτυξη κοινής επίγνωσης της κατάστασης για μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις.

36) Σύμφωνα με την οδηγία (ΕΕ) 2022/2555 και τον κανονισμό (ΕΕ) 2024/2847, ο ENISA λαμβάνει πληροφορίες σχετικά με σημαντικά διασυνοριακά περιστατικά και τρωτά σημεία που αποτελούν αντικείμενο ενεργού εκμετάλλευσης και με περιστατικά που πλήττουν ψηφιακά προϊόντα. Ο ENISA, ως γραμματεία, θα πρέπει να συμβουλεύει το δίκτυο CSIRT και το EU-CyCLONe, με στόχο να υποστηρίζει τα δίκτυα, όταν προσδιορίζουν κατά πόσον θα πρέπει να αναληφθούν περαιτέρω δράσεις και να συμβάλλει στην κοινή επίγνωση της κατάστασης.

Πολιτικό επίπεδο

37) Τα κράτη μέλη και οι αρμόδιες οντότητες της Ένωσης θα πρέπει να παρακολουθούν τις διεθνείς εξελίξεις που επηρεάζουν την κυβερνοασφάλεια (συμπεριλαμβανομένων των κυβερνοαπειλών, των υβριδικών απειλών και της χειραγώγησης πληροφοριών και παρεμβάσεων από το εξωτερικό («FIMI»), συμπεριλαμβανομένης της παραπληροφόρησης, κατά περίπτωση). Πρωτοβουλίες όπως οι κοινές εκθέσεις για την κατάσταση της κυβερνοασφάλειας («JCAR»), οι αναλύσεις που παρέχει η SIAC και άλλα συναφή προϊόντα που παρέχουν εξειδικευμένες πληροφορίες θα πρέπει να λαμβάνονται υπόψη.

38) Ο Ύπατος Εκπρόσωπος θα πρέπει να συνεχίσει να ενημερώνει και να προωθεί τη συμμετοχή των κρατών μελών στις διπλωματικές προσπάθειες της Ένωσης που σχετίζονται με κυβερνοαπειλές, ιδίως εκείνες στις οποίες συμμετέχουν κρατικοί φορείς, στη συνεργασία με τρίτες χώρες και διεθνείς οργανισμούς, συμπεριλαμβανομένου του ΝΑΤΟ, και στην εφαρμογή διπλωματικών μέτρων, συμπεριλαμβανομένων των περιοριστικών μέτρων.

39) Η Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης μπορεί να δημιουργήσει σελίδα παρακολούθησης στη διαδικτυακή πλατφόρμα της IPCR, όπου τα κράτη μέλη και τα θεσμικά όργανα και οι οργανισμοί της ΕΕ μπορούν να ανταλλάσσουν πληροφορίες σχετικά με πιθανώς εξελισσόμενες κρίσεις.

Κοινές ασκήσεις

40) Η Επιτροπή, σε συντονισμό με τον Ύπατο Εκπρόσωπο, με την υποστήριξη του ENISA και έπειτα από διαβούλευση με το EU-CyCLONe και το δίκτυο CSIRT, θα πρέπει να καταρτίζει αποτελεσματικό ετήσιο κυλιόμενο πρόγραμμα κυβερνοασκήσεων, με σκοπό την προετοιμασία για κυβερνοκρίσεις και την ενίσχυση της οργανωτικής αποτελεσματικότητας. Το κυλιόμενο πρόγραμμα κυβερνοασκήσεων θα πρέπει να λαμβάνει υπόψη τις ασκήσεις του ΜΠΠΕ και άλλων μηχανισμών αντιμετώπισης κρίσεων σε επίπεδο Ένωσης, συμπεριλαμβανομένης της άσκησης που περιγράφεται στο σχέδιο στρατηγικής της ΕΕ για τις υποδομές ζωτικής σημασίας. Το πρώτο κυλιόμενο πρόγραμμα θα πρέπει να σχεδιαστεί εντός 12 μηνών από την έγκριση του σχεδίου στρατηγικής για τον κυβερνοχώρο, ενώ τα επόμενα προγράμματα θα πρέπει να ολοκληρώνονται έως τις 31 Μαρτίου κάθε έτους. Το κυλιόμενο πρόγραμμα θα πρέπει να υποβάλλεται στο Συμβούλιο προς ενημέρωση.

41) Το κυλιόμενο πρόγραμμα θα πρέπει επίσης να καλύπτει τις ασκήσεις που σχεδιάζονται με τη χρήση των σεναρίων εκτιμήσεων κινδύνων τα οποία συντονίζει η ΕΕ. Θα πρέπει να καλύπτει ασκήσεις στις οποίες συμμετέχουν όλοι οι σχετικοί παράγοντες, ιδίως δε ο ιδιωτικός τομέας και το ΝΑΤΟ.

42) Ο ENISA, στο πλαίσιο του ρόλου του ως γραμματεία του δικτύου CSIRT και του EU-CyCLONe, θα πρέπει να διασφαλίζει τη συστηματική συλλογή των διδαγμάτων που αντλούνται από τις ασκήσεις και θα πρέπει να καθορίζει και να προτείνει τρόπους για την υλοποίηση των προκυπτουσών δράσεων, ώστε να διασφαλίζονται η αποτελεσματική εκτέλεσή τους και ο θετικός αντίκτυπός τους στην από κοινού ανθεκτικότητα της ΕΕ, συμπεριλαμβανομένων των αντίστοιχων SOP.

43) Όλοι οι παράγοντες και τα δίκτυα θα πρέπει να βελτιώνουν τον συντονισμό σε περίπτωση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης με βάση τα διδάγματα που έχουν αντληθεί από τις ασκήσεις. Ειδικότερα, το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να βρίσκουν λύσεις στις προκλήσεις που εντοπίζονται κατά τη διάρκεια των ασκήσεων, ώστε να βελτιώνεται ο συντονισμός, ιδίως δε τις προκλήσεις που αφορούν τη συνεργασία μεταξύ των δικτύων και, εάν χρειάζεται, να προσαρμόζουν γρήγορα τις SOP.

44) Η ομάδα συνεργασίας NIS θα πρέπει να προσκαλέσει το δίκτυο CSIRT, το EU-CyCLONe και τον ENISA για να παρουσιάσουν τα διδάγματα που αντλήθηκαν από τις ασκήσεις, καθώς και τον καθορισμό και τον προτεινόμενο τρόπο υλοποίησης των δράσεων που προέκυψαν από αυτά.

45) Το Συμβούλιο μπορεί να καλέσει τους προέδρους του δικτύου CSIRT, του EU-CyCLONe, της ομάδας συνεργασίας NIS και του ENISA να παρουσιάσουν πώς χρησίμευσαν τα διδάγματα που αντλήθηκαν από τις ασκήσεις.

46) Ο ENISA καλείται να διοργανώσει, σε συνεργασία με την Επιτροπή και τον Ύπατο Εκπρόσωπο, άσκηση στην οποία θα τεθεί σε δοκιμή το σχέδιο στρατηγικής για τον κυβερνοχώρο στο πλαίσιο της προσεχούς άσκησης Cyber Europe. Στην άσκηση θα πρέπει να συμμετάσχουν όλοι οι εμπλεκόμενοι παράγοντες, συμπεριλαμβανομένου του πολιτικού επιπέδου. Ο ENISA, σε συνεργασία με την Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης, καλείται να συντονίσει τη συμμετοχή του πολιτικού επιπέδου. Η άσκηση μπορεί επίσης να περιλαμβάνει τον ιδιωτικό τομέα και το ΝΑΤΟ.

VI: Εντοπισμός περιστατικού που θα μπορούσε να κλιμακωθεί σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση

47) Σύμφωνα με τις αντίστοιχες εντολές τους και με βάση την προσέγγιση για όλους τους κινδύνους, όλοι οι παράγοντες θα πρέπει να συνεισφέρουν, παρέχοντας πληροφορίες που να υποδεικνύουν πιθανό μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση στα σχετικά δίκτυα.

48) Σύμφωνα με τον κανονισμό (ΕΕ) 2025/38[13], όταν οι διασυνοριακοί κυβερνοκόμβοι λαμβάνουν πληροφορίες σχετικά με δυνητικό ή εξελισσόμενο μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας, θα πρέπει να διασφαλίζουν, για τους σκοπούς της κοινής αντίληψης της κατάστασης, ότι παρέχονται σχετικές πληροφορίες στις αρχές των κρατών μελών και στην Επιτροπή μέσω του EU-CyCLONe και του δικτύου CSIRT, χωρίς αδικαιολόγητη καθυστέρηση.

[13] Κανονισμός (ΕΕ) 2025/38 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Δεκεμβρίου 2024, σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας και για την τροποποίηση του κανονισμού (ΕΕ) 2021/694 (κανονισμός για την αλληλεγγύη στον κυβερνοχώρο), ΕΕ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) Όταν παρατηρείται σημαντικό περιστατικό, ιδίως μάλιστα περιστατικό με άμεσες συνέπειες, μπορεί να κοινοποιείται σε CSIRT ή να εντοπίζεται από αυτήν καθώς και σε, ή από, αρχές διαχείρισης κυβερνοκρίσεων των κρατών μελών ή άλλες τομεακές αρχές. Τα κράτη μέλη ενθαρρύνονται να ανταλλάσσουν πληροφορίες σχετικά με ένα τέτοιο περιστατικό διαμέσου των δικτύων, τα οποία θα πρέπει να μελετούν τη λήψη ενδεδειγμένων μέτρων. Η ενεργοποίηση του δικτύου CSIRT και του EU-CyCLONe μπορεί να είναι ανεξάρτητη η μία από την άλλη και να συναρτάται με τη φύση του περιστατικού και την απαιτούμενη αντίδραση. Ωστόσο, τα δύο δίκτυα παροτρύνονται να συνεχίσουν τη μεταξύ τους συνεργασία βάσει συμφωνημένων διαδικαστικών ρυθμίσεων. Η απόφαση για ενεργοποίηση εναπόκειται αποκλειστικά και ανεξάρτητα σε κάθε αντίστοιχο δίκτυο.

50) Το δίκτυο CSIRT θα πρέπει να συμβουλεύει το EU-CyCLONe σχετικά με το αν ένα περιστατικό κυβερνοασφάλειας που έχει παρατηρηθεί μπορεί να θεωρηθεί δυνητικό ή υπό εξέλιξη μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας.

51) Όπως αναφέρεται στην οδηγία (ΕΕ) 2022/2555, σε περίπτωση δυνητικού ή υπό εξέλιξη μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας, το δίκτυο CSIRT και το EU-CyCLONe θα πρέπει να συμφωνούν πάραυτα τις διαδικαστικές ρυθμίσεις, προκειμένου να διασφαλίζεται ο τεχνικός και ο επιχειρησιακός συντονισμός και η παροχή έγκαιρων και χρήσιμων πληροφοριών στο πολιτικό επίπεδο.

VII: Αντίδραση σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση σε επίπεδο Ένωσης

Αντίδραση σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση για τα οποία η IPCR δεν τίθεται σε λειτουργία πλήρους ενεργοποίησης

52) Η αποτελεσματική αντίδραση σε μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας ή κυβερνοκρίσεων σε επίπεδο ΕΕ εξαρτάται από την αποτελεσματική τεχνική, επιχειρησιακή και πολιτική συνεργασία στο πλαίσιο μιας προσέγγισης που αφορά το σύνολο της διοίκησης, στην οποία θα περιλαμβάνεται, όπου είναι δυνατόν, και η επιβολή του νόμου.

53) Σε κάθε επίπεδο, οι εμπλεκόμενοι φορείς θα πρέπει να εκτελούν συγκεκριμένες δραστηριότητες για την επίτευξη κοινής επίγνωσης της κατάστασης και για συντονισμένη αντίδραση. Με μέτρα αυτού του είδους θα εξασφαλίζεται η ομαλή και αποτελεσματική διάδοση των πληροφοριών.

54) Η αντίδραση θα πρέπει να είναι η ενδεδειγμένη, αναλόγως των συνεπειών του μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης. Σύμφωνα με την οδηγία (ΕΕ) 2022/2555, οι αρχές διαχείρισης κυβερνοκρίσεων των κρατών μελών θα πρέπει να διασφαλίζουν την εθνική συνοχή και τον συντονισμό μεταξύ των τομεακών αντιδράσεων στην κυβερνοκρίση.

55) Σε περίπτωση μεγάλης κλίμακας περιστατικού στον κυβερνοχώρο ή κυβερνοκρίσης, όλοι οι φορείς και τα δίκτυα θα πρέπει να αντιδρούν σε στενό συντονισμό, ως εξής:

α) σε τεχνικό επίπεδο:

i. Τα επηρεαζόμενα κράτη μέλη και οι CSIRT τους θα πρέπει να συνεργάζονται με τις επηρεαζόμενες οντότητες για την αντιμετώπιση περιστατικών και την παροχή βοήθειας, εφόσον απαιτείται·

ii. Οι CSIRT θα πρέπει να συνεργάζονται μέσω του δικτύου CSIRT για την ανταλλαγή τεχνικών πληροφοριών σχετικών με το περιστατικό· κατά τις προσπάθειές τους να αναλύσουν τα τεχνικά κατασκευάσματα και άλλες τεχνικές πληροφορίες που διαθέτουν και σχετίζονται με το περιστατικό, οι CSIRT συνεργάζονται, προκειμένου να αναζητήσουν τα αίτια και να εξεύρουν πιθανά τεχνικά μέτρα μετριασμού·

iii. Όταν μια CSIRT ή μια αρχή διαχείρισης κυβερνοκρίσεων ενός κράτους μέλους ενημερωθεί για σοβαρό περιστατικό, ενθαρρύνεται να ανταλλάξει πληροφορίες στο δίκτυο CSIRT ή στο EU-CyCLONe.

iv. Το δίκτυο CSIRT, υποστηριζόμενο από τον ENISA, θα πρέπει να συγκεντρώνει τις εθνικές εκθέσεις που παρέχουν οι CSIRT και να τις υποβάλλει στο EU-CyCLONe·

v. Όταν ένα περιστατικό κυβερνοασφάλειας θα μπορούσε να κλιμακωθεί σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή σε κυβερνοκρίση, το δίκτυο CSIRT θα πρέπει να ανταλλάσσει τις σχετικές πληροφορίες με το EU-CyCLONe. Το EU-CyCLONe θα πρέπει να χρησιμοποιεί τις πληροφορίες αυτές για να ενημερώνει το Συμβούλιο·

vi. Το δίκτυο CSIRT θα πρέπει να βρίσκεται σε στενή επαφή με τον Ευρωπόλ για να διασφαλίζεται η ανταλλαγή των σχετικών τεχνικών πληροφοριών. Το δίκτυο CSIRT και ο Ευρωπόλ θα πρέπει να καθορίσουν σημεία επαφής για να βελτιώσουν την ανταλλαγή πληροφοριών, όπου απαιτείται, σε περίπτωση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας·

β) σε επιχειρησιακό επίπεδο:

i. Τα κράτη μέλη θα πρέπει να μετριάζουν τον αντίκτυπο του περιστατικού σε εθνικό επίπεδο, χρησιμοποιώντας κατάλληλα μέτρα·

ii. Το δίκτυο CSIRT θα πρέπει να παρέχει στο EU-CyCLONe τεχνικές αξιολογήσεις των περιστατικών που βρίσκονται σε εξέλιξη, τις οποίες το EU-CyCLONe θα μπορεί να χρησιμοποιεί·

iii. Το EU-CyCLONe θα πρέπει να αξιολογεί τις συνέπειες και τον αντίκτυπο των μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων και να προτείνει πιθανά μέτρα μετριασμού, να στηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων καθώς και να στηρίζει τη λήψη αποφάσεων σε πολιτικό επίπεδο·

iv. Σε περίπτωση που σε μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας με διατομεακό αντίκτυπο απαιτείται η ενεργοποίηση δράσεων αντιμετώπισης σε επίπεδο Ένωσης, κυρίως δε των σχετικών οριζόντιων και τομεακών μηχανισμών διαχείρισης κρίσεων σε επίπεδο Ένωσης που απαριθμούνται στο παράρτημα ΙΙ,

α) οι αρμόδιοι φορείς μπορούν, ανάλογα με το είδος των τομεακών μηχανισμών διαχείρισης κρίσεων σε επίπεδο Ένωσης, να ζητήσουν την ενεργοποίηση τέτοιων μηχανισμών·

β) σε περίπτωση ενεργοποίησης τέτοιων τομεακών μηχανισμών, οι οικείες οντότητες στηρίζουν τις τομεακές οντότητες, προκειμένου να μετριασθούν οι επιπτώσεις του περιστατικού·

γ) η Επιτροπή θα πρέπει να διευκολύνει τη ροή των αναγκαίων πληροφοριών μεταξύ των σημείων επαφής για τους σχετικούς οριζόντιους και τομεακούς μηχανισμούς αντιμετώπισης κρίσεων σε επίπεδο Ένωσης που απαριθμούνται στο παράρτημα ΙΙ και του EU-CyCLONe, να επιδιώξει μια ολοκληρωμένη διατομεακή ανάλυση και να προτείνει επιλογές για ενδεδειγμένο ολοκληρωμένο σχέδιο αντιμετώπισης·

δ) η Επιτροπή, μέσω του EU-CyCLONe, εφόσον συντρέχει περίπτωση, σε συνεργασία με τον Ύπατο Εκπρόσωπο, θα πρέπει να διασφαλίζει τη συνοχή και τον συντονισμό των επιχειρησιακών μέτρων σε επίπεδο ΕΕ στον κυβερνοχώρο με δράσεις αντιμετώπισης σε επίπεδο Ένωσης, ιδίως σε σχέση με αιτήματα συνδρομής μέσω του ΜΠΠΕ·

ε) εάν έχει ξεκινήσει ανάρτηση πληροφοριών σχετικά με το περιστατικό σε σελίδα παρακολούθησης της IPCR, θα πρέπει επίσης μέσω της διαδικτυακής πλατφόρμας της IPCR να κοινοποιούνται μεταξύ των κρατών μελών και των οντοτήτων της Ένωσης πληροφορίες για τις επιπτώσεις του και τα μέτρα που έχουν ληφθεί·

v. τα κράτη μέλη μπορούν να ζητούν υπηρεσίες από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας, σύμφωνα με το άρθρο 15 του κανονισμού (ΕΕ) αριθ. 2025/38. Με την επιφύλαξη τυχόν μελλοντικών εκτελεστικών πράξεων δυνάμει του εν λόγω κανονισμού, οι υπηρεσίες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας θα πρέπει να ξεκινούν εντός 24 ωρών από την υποβολή του αιτήματος.

γ) σε πολιτικό επίπεδο:

i. Το Συμβούλιο μπορεί να ζητεί να ενημερώνεται από τα κύρια ενδιαφερόμενα μέρη, ιδίως την Επιτροπή, τον Ύπατο Εκπρόσωπο και το EU-CyCLONe, προκειμένου να δίνει ορθές πολιτικές και στρατηγικές κατευθύνσεις·

ii. Το Συμβούλιο, με την υποστήριξη της Επιτροπής και του Ύπατου Εκπροσώπου, θα μπορούσε να αποφασίζει σχετικά με τα κατάλληλα μέτρα για την αντιμετώπιση του μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας, συμπεριλαμβανομένων των πιθανών διπλωματικών αντιδράσεων σύμφωνα με το κεφάλαιο IX·

iii. Τα κράτη μέλη μπορούν να ενεργοποιούν πρόσθετους μηχανισμούς ή μέσα διαχείρισης κυβερνοκρίσεων, ανάλογα με τη φύση και τον αντίκτυπο του περιστατικού·

iv. Όταν η IPCR τίθεται σε λειτουργία ανταλλαγής πληροφοριών, πυροδοτείται και η ικανότητα υποστήριξης της ISAA με αποτέλεσμα να αυξάνονται οι ανταλλαγές πληροφοριών μέσω της διαδικτυακής πλατφόρμας της IPCR και να διασφαλίζεται μια κοινή αντίληψη της κατάστασης. Οι εκθέσεις του EU-CyCLONe και του δικτύου CSIRT για την κατάσταση θα πρέπει να παραμείνουν τα κύρια μέσα που παρουσιάζουν την κοινή επίγνωση της κατάστασης σε επιχειρησιακό και τεχνικό επίπεδο αντίστοιχα. Οι εκθέσεις αυτές μπορούν να τροφοδοτούν τις εκθέσεις της ISAA·

v. Σε περίπτωση περιστατικού που απαιτεί την ενεργοποίηση δράσεων αντιμετώπισης σε επίπεδο Ένωσης, ιδίως των οριζόντιων και τομεακών μηχανισμών διαχείρισης κρίσεων σε επίπεδο Ένωσης που απαριθμούνται στο παράρτημα ΙΙ, το Συμβούλιο, σε συνεργασία με την Επιτροπή και τον Ύπατο Εκπρόσωπο, θα πρέπει να διασφαλίζει τη συνοχή και τον συντονισμό μεταξύ των αντιδράσεων στην κυβερνοκρίση και των δράσεων αντιμετώπισης σε επίπεδο Ένωσης·

vi. Όταν ζητούνται τέτοιοι μηχανισμοί, ιδίως οι υπηρεσίες της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, οι υπηρεσίες της Επιτροπής και, κατά περίπτωση, η ΕΥΕΔ, καθώς και τα αρμόδια όργανα του Συμβουλίου, ιδίως η HWPCI και η Οριζόντια Ομάδα «ενίσχυση της ανθεκτικότητας και αντιμετώπιση των υβριδικών απειλών» («HWP-ERCHT»), κατά περίπτωση, θα πρέπει να συντονίζονται όσον αφορά τον σχεδιασμό και την υλοποίηση των μέτρων και την κατάλληλη διαδικασία λήψης αποφάσεων για πρόσθετα μέτρα, σύμφωνα με την εργαλειοθήκη για την αντιμετώπιση υβριδικών απειλών[14] στην περίπτωση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο που αποτελούν μέρος ευρύτερης υβριδικής εκστρατείας.

Αντίδραση σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση για τα οποία η IPCR τίθεται σε λειτουργία πλήρους ενεργοποίησης

56) Θα πρέπει να εφαρμόζονται τα στάδια που αναφέρονται στο τμήμα «*Αντίδραση σε μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση για τα οποία η IPCR δεν τίθεται σε λειτουργία πλήρους ενεργοποίησης*» πιο πάνω.

57) Όταν η IPCR τίθεται σε λειτουργία πλήρους ενεργοποίησης, οι εκθέσεις ISAA χρησιμοποιούνται για να διασφαλίζουν κοινή επίγνωση της κατάστασης σε πολιτικό επίπεδο. Οι εκθέσεις του EU-CyCLONe και του δικτύου CSIRT για την κατάσταση θα πρέπει να παραμείνουν τα κύρια μέσα που παρουσιάζουν την κοινή επίγνωση της κατάστασης σε επιχειρησιακό και τεχνικό επίπεδο αντίστοιχα. Οι εκθέσεις αυτές μπορούν να τροφοδοτούν τις εκθέσεις της ISAA.

58) Σε περίπτωση που, λόγω μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης, η IPCR τίθεται σε λειτουργία πλήρους ενεργοποίησης, θα πρέπει να ανταποκρίνονται όλοι οι φορείς, σε στενό συντονισμό, στο πλαίσιο μιας προσέγγισης που θα αφορά το σύνολο της διοίκησης ως εξής:

α) ο συντονισμός της αντίδρασης στο πολιτικό επίπεδο της Ένωσης πραγματοποιείται από το Συμβούλιο, με χρήση των ρυθμίσεων IPCR·

[14] Η εργαλειοθήκη για την αντιμετώπιση υβριδικών απειλών είναι ένα πλαίσιο για συντονισμένη αντίδραση σε υβριδικές εκστρατείες που πλήττουν την ΕΕ και τα κράτη μέλη της και περιλαμβάνει, για παράδειγμα, μέτρα πρόληψης, συνεργασίας, σταθερότητας, περιορισμού και ανάκαμψης και τη στήριξη της αλληλεγγύης και της αμοιβαίας συνδρομής.

β) το EU-CyCLONe, σε συνεργασία με το δίκτυο CSIRT, θα πρέπει να παρέχει σαφείς πληροφορίες στο πολιτικό επίπεδο σχετικά με τον αντίκτυπο, τις πιθανές συνέπειες και τα μέτρα για την αντιμετώπιση και την επανόρθωση του περιστατικού, μεταξύ άλλων συνεισφέροντας στις εκθέσεις της ISAA·

γ) εκτός από την ικανότητα ISAA, η Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης θα διοργανώνει συζητήσεις στρογγυλής τραπέζης IPCR για να μπορεί να συντονίζεται η πολιτική και η στρατηγική διάσταση της αντίδρασης της ΕΕ, με δράσεις βάσει του σχεδίου στρατηγικής για τον κυβερνοχώρο και των εργασιών των σχετικών τομεακών μηχανισμών που εντάσσονται στις εργασίες της IPCR. Επιπλέον, στις συζητήσεις στρογγυλής τραπέζης είναι δυνατό να εντοπίζονται κενά στην αντιμετώπιση και να καλούνται συγκεκριμένοι φορείς της ΕΕ να δώσουν λύσεις και να υποβάλουν έκθεση σε μελλοντικές συζητήσεις στρογγυλής τραπέζης, με σκοπό την ενίσχυση του πολιτικού και στρατηγικού συντονισμού της IPCR·

δ) η Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης θα πρέπει να εξετάσει το ενδεχόμενο να προσκαλεί το EU-CyCLONe σε σχετικές συνεδριάσεις, συμπεριλαμβανομένων των συζητήσεων στρογγυλής τραπέζης στο πλαίσιο των ρυθμίσεων IPCR, καθώς και σε άλλες συνόδους του Συμβουλίου·

ε) οι αρχές διαχείρισης κρίσεων των κρατών μελών θα πρέπει να διασφαλίζουν τη συνοχή και τον συντονισμό μεταξύ των τομεακών αντιδράσεων στην κυβερνοκρίση που υποστηρίζονται από αρχές διαχείρισης κυβερνοκρίσεων·

στ) οι όποιες διπλωματικές αντιμετωπίσεις θα πρέπει να εξετάζονται και να υλοποιούνται σύμφωνα με το κεφάλαιο IX.

VIII: Προσπάθειες επικοινωνίας με το κοινό

59) Ενώ η ενημέρωση του πληθυσμού ενός μεμονωμένου κράτους μέλους σχετικά με εν εξελίξει μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας ή κυβερνοκρίση, μεταξύ άλλων στο πλαίσιο της ευαισθητοποίησης, αποτελεί εθνική αρμοδιότητα, τα κράτη μέλη, η Επιτροπή και ο Ύπατος Εκπρόσωπος θα πρέπει να έχουν ως στόχο τον συντονισμό της ενημέρωσης του κοινού στο μέτρο του δυνατού. Το άτυπο δίκτυο επικοινωνίας της IPCR για την αντιμετώπιση κρίσεων μπορεί να συμμετέχει, κατά περίπτωση.

60) Για τους σκοπούς της προετοιμασίας για μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις, τα κράτη μέλη και, κατά περίπτωση, η Επιτροπή και η CERT-ΕΕ καλούνται να ανταλλάσσουν πληροφορίες σχετικά με τις επικοινωνιακές τους προσπάθειες στο πλαίσιο του EU-CyCLONe και του δικτύου CSIRT, συμπεριλαμβανομένων βέλτιστων πρακτικών, όπως συμβουλές ή εκστρατείες ευαισθητοποίησης. Ο ENISA θα πρέπει να παρέχει εργαλεία που να υποστηρίζουν την εν λόγω ανταλλαγή και να διασφαλίζουν εύκολη πρόσβαση.

61) Σε περίπτωση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης, τα κράτη μέλη καλούνται να ανταλλάσσουν στο πλαίσιο του EU-CyCLONe πληροφορίες σχετικά με τις προσπάθειές τους για επικοινωνία με το κοινό, με σκοπό την οικοδόμηση κοινής ευαισθητοποίησης και τον συντονισμό των δράσεων. Το EU-CyCLONe με δική του πρωτοβουλία ή κατόπιν αιτήματος του Συμβουλίου μπορεί να κοινοποιεί στο Συμβούλιο επισκόπηση των εν λόγω προσεγγίσεων.

IX: Διπλωματική αντιμετώπιση και συνεργασία με στρατηγικούς εταίρους

62) Ο Ύπατος Εκπρόσωπος, σε στενή συνεργασία με την Επιτροπή και άλλες αρμόδιες οντότητες της Ένωσης, θα πρέπει:

α) να στηρίζει τη διαδικασία λήψης αποφάσεων στο Συμβούλιο, μεταξύ άλλων μέσω αναλύσεων, εκθέσεων και προτάσεων, σχετικά με τη χρήση πιθανών μέτρων στο πλαίσιο της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο. Με αυτόν τον τρόπο, θα καταστεί δυνατή η χρήση του πλήρους φάσματος των διαθέσιμων εργαλείων της Ένωσης για την πρόληψη, την αποτροπή και την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, ενισχύοντας την οικεία κατάσταση κυβερνοασφάλειας και προωθώντας τη διεθνή ειρήνη, ασφάλεια και σταθερότητα στον κυβερνοχώρο·

β) όταν εντοπίζεται σχετικό περιστατικό, να διευκολύνει τη ροή των αναγκαίων πληροφοριών με στρατηγικούς εταίρους, μεταξύ άλλων με το ΝΑΤΟ, κατά περίπτωση·

γ) να ενισχύει τον συντονισμό με στρατηγικούς εταίρους, μεταξύ άλλων με το ΝΑΤΟ, κατά περίπτωση, για την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο από επίμονους παράγοντες απειλής, ιδίως κατά τη χρήση της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο, σύμφωνα με τις κατευθυντήριες γραμμές εφαρμογής.

63) Τα κράτη μέλη, ο Ύπατος Εκπρόσωπος, η Επιτροπή και άλλες αρμόδιες οντότητες της Ένωσης θα πρέπει να συνεργάζονται με στρατηγικούς εταίρους και διεθνείς οργανισμούς, με σκοπό την προώθηση ορθών πρακτικών και υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο και τη διασφάλιση της ταχείας και συντονισμένης αντιμετώπισης δυνητικών ή μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας.

64) Η συνεργασία της Ευρωπαϊκής Ένωσης και του ΝΑΤΟ θα πρέπει να διεξάγεται σύμφωνα με τις συμφωνημένες κατευθυντήριες αρχές της συμπερίληψης, της αμοιβαιότητας και της διαφάνειας, και με πλήρη σεβασμό της αυτόνομης λήψης αποφάσεων της Ένωσης.

65) Η Επιτροπή και ο Ύπατος Εκπρόσωπος, λαμβάνοντας υπόψη τις υφιστάμενες συμφωνίες, όπως την τεχνική συμφωνία CERT-ΕΕ/ΝΑΤΟ του 2016, θα πρέπει να δημιουργήσουν σημεία επαφής για τον συντονισμό με το ΝΑΤΟ σε περίπτωση κυβερνοκρίσης, με σκοπό την ανταλλαγή των αναγκαίων πληροφοριών σχετικά με την κατάσταση και τη χρήση μηχανισμών αντιμετώπισης κρίσεων, προκειμένου να ενισχυθούν η συνεργασία για την αντιμετώπιση και η αποτελεσματικότητα της αντιμετώπισης. Για τον σκοπό αυτό, η Ένωση θα πρέπει να διερευνήσει τρόπους για τη βελτίωση της ανταλλαγής πληροφοριών με το ΝΑΤΟ, χωρίς αποκλεισμούς και διακρίσεις και με αμοιβαίο τρόπο, ιδίως μέσω της κατοχύρωσης εργαλείων ασφαλούς επικοινωνίας, λαμβάνοντας παράλληλα υπόψη τα πρότυπα ανταλλαγής πληροφοριών των διαφόρων κρατών μελών.

66) Στο πλαίσιο του ενωσιακού προγράμματος περιοδικών ασκήσεων στον κυβερνοχώρο που αναφέρεται στο κεφάλαιο V ανωτέρω, οι υπηρεσίες της Επιτροπής και η ΕΥΕΔ θα πρέπει να εξετάσουν πώς θα διοργανώσουν άσκηση σε επίπεδο προσωπικού με το ΝΑΤΟ, προκειμένου να δοκιμαστεί η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών οντοτήτων σε περίπτωση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης, όταν τα κράτη μέλη ή οι σύμμαχοι του ΝΑΤΟ αναζητούν τρόπους αντιμετώπισης κυβερνοεπίθεσης που επηρεάζει την ασφάλειά τους. Η άσκηση θα πρέπει να διεξαχθεί χωρίς αποκλεισμούς και διακρίσεις και με πλήρη σεβασμό των συμφωνημένων αρχών των παραμέτρων της συνεργασίας ΕΕ-ΝΑΤΟ. Η άσκηση θα πρέπει να διεξαχθεί στο πλαίσιο της άσκησης EU Integrated Resolve (παράλληλη και συντονισμένη άσκηση, «PACE»). Θα πρέπει να ληφθούν όλα τα αναγκαία μέτρα για να διασφαλιστεί η συμμετοχή όλων των φορέων που αναφέρονται στο σχέδιο στρατηγικής για τον κυβερνοχώρο.

67) Θα πρέπει επίσης να εξεταστεί το ενδεχόμενο διοργάνωσης κοινών ασκήσεων στον κυβερνοχώρο σε επίπεδο Ένωσης με τις χώρες των Δυτικών Βαλκανίων, τη Δημοκρατία της Μολδαβίας, την Ουκρανία, καθώς και άλλους στρατηγικούς εταίρους και ομόφρονες τρίτες χώρες, σε διαβούλευση με το Συμβούλιο, την Επιτροπή και τον Ύπατο Εκπρόσωπο.

Χ. Συντονισμός της διαχείρισης κυβερνοκρίσεων με στρατιωτικούς φορείς σε επίπεδο ΕΕ

68) Τα κράτη μέλη θα πρέπει να συνεχίσουν να ενισχύουν τη συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών φορέων του κυβερνοχώρου σε εθνικό επίπεδο.

69) Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να προσδιορίσουν πιθανούς τρόπους και διαδικασίες συνεργασίας με τους αρμόδιους στρατιωτικούς φορείς της ΕΕ, όπως η διάσκεψη των διοικητών κυβερνοχώρου της ΕΕ και το επιχειρησιακό δίκτυο της στρατιωτικής ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική («MICNET»), προκειμένου να επωφεληθούν από μια κοινή στρατιωτική και μη στρατιωτική προοπτική, ιδίως μέσω κοινών συνεδριάσεων. Το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να ενημερώνουν το Συμβούλιο σχετικά με την πρόοδο που σημειώνεται όσον αφορά την εν λόγω συνεργασία.

70) Το επηρεαζόμενο κράτος μέλος καλείται να ενημερώσει το EU-CyCLONe, καθώς και την ΕΥΕΔ, εάν χρησιμοποιούνται σχετικές εθνικές ή πολυεθνικές ικανότητες στρατιωτικής αντιμετώπισης στο πλαίσιο μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης, και η παροχή των πληροφοριών αυτών συμφωνείται αμοιβαία μεταξύ του χρήστη και του παρόχου της εν λόγω ικανότητας αντιμετώπισης.

71) Στο πλαίσιο του ενωσιακού προγράμματος περιοδικών κυβερνοασκήσεων που αναφέρεται στο κεφάλαιο V ανωτέρω, η Επιτροπή και ο Ύπατος Εκπρόσωπος θα πρέπει να εξετάσουν το ενδεχόμενο διοργάνωσης κοινής άσκησης, προκειμένου να δοκιμαστεί η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών φορέων του κυβερνοχώρου σε περίπτωση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας που επηρεάζει τα κράτη μέλη.

XI: Ανάκαμψη από κυβερνοκρίση και σχετικά διδάγματα

72) Τα κράτη μέλη, οι αρμόδιες οντότητες και τα δίκτυα της Ένωσης των κρατών μελών θα πρέπει να συνεργάζονται κατά τη φάση ανάκαμψης μετά από κυβερνοκρίση, ώστε να διασφαλίζεται η ταχεία αποκατάσταση των βασικών λειτουργιών. Οι κοινότητες επιβολής του νόμου θα πρέπει επίσης, κατά περίπτωση, να συμμετέχουν σε μια τέτοια συνεργασία. Σε αυτό το στάδιο, η συνεργασία με τον ιδιωτικό τομέα έχει ζωτική σημασία, ιδίως για τη διευκόλυνση της ανάκτησης δεδομένων και την αποκατάσταση των συστημάτων. Κατά τον αποτελεσματικό συντονισμό μεταξύ των ενδιαφερόμενων μερών θα πρέπει να δίνεται προτεραιότητα στην ελαχιστοποίηση των διαταραχών και στη διασφάλιση της επιχειρησιακής συνέχειας.

73) Τα κράτη μέλη, οι σχετικές οντότητες και τα δίκτυα της Ένωσης θα πρέπει να συνεργάζονται κατά το στάδιο της ανάκαμψης με βάση τα διδάγματα τα οποία αντλήθηκαν από κυβερνοκρίσεις ή περιστατικά κυβερνοασφάλειας υπό διαχείριση που συνέβησαν κατά το παρελθόν, καθώς και τις αναφορές περιστατικών, ιδίως στο πλαίσιο του ευρωπαϊκού μηχανισμού εξέτασης περιστατικών κυβερνοασφάλειας που θεσπίστηκε με τον κανονισμό (ΕΕ) 2025/38.

74) Το EU-CyCLONe θα πρέπει να παράσχει στο δίκτυο CSIRT, στην ομάδα συνεργασίας NIS και στο Συμβούλιο ολοκληρωμένο κατάλογο με διδάγματα τα οποία αντλήθηκαν από κυβερνοκρίσεις ή περιστατικά κυβερνοασφάλειας που αντιμετωπίστηκαν επιτυχώς κατά το παρελθόν, καθώς και βέλτιστες πρακτικές. Ο ENISA θα πρέπει να διασφαλίζει ότι τα διδάγματα αυτά αντικατοπτρίζονται δεόντως στις μελλοντικές δραστηριότητες ετοιμότητας και κατά την εξέταση του σχεδιασμού μελλοντικών ασκήσεων.

XII: Ασφαλής επικοινωνία

75) Με βάση τη χαρτογράφηση των υφιστάμενων εργαλείων ασφαλούς επικοινωνίας[15], η Επιτροπή θα πρέπει να προτείνει έως το τέλος του 2026 ένα διαλειτουργικό σύνολο λύσεων ασφαλούς επικοινωνίας. Το Συμβούλιο, η Επιτροπή, ο Ύπατος Εκπρόσωπος, το EU-CyCLONe και το δίκτυο CSIRT θα πρέπει να συμφωνήσουν επ' αυτού έως το τέλος του 2027. Οι λύσεις αυτές θα πρέπει να επωφελούνται από τις δράσεις στον τομέα των ασφαλών επικοινωνιών που θα μπορούσαν να αναλάβουν τα θεσμικά όργανα της ΕΕ στο πλαίσιο της στρατηγικής της ΕΕ για την Ένωση Ετοιμότητας και θα πρέπει να καλύπτουν το πλήρες φάσμα των απαιτούμενων τρόπων επικοινωνίας (φωνή, δεδομένα, βιντεοδιάσκεψη, ανταλλαγή μηνυμάτων, συνεργασία και ανταλλαγή και εξέταση εγγράφων). Οι λύσεις θα πρέπει να πληρούν από κοινού καθορισμένες απαιτήσεις για την προστασία ευαίσθητων μη διαβαθμισμένων πληροφοριών. Θα πρέπει να χρησιμοποιούνται λύσεις που βασίζονται σε ανοικτό πρωτόκολλο με εφαρμογές ανοικτής πηγής κατάλληλες για επικοινωνία σε πραγματικό χρόνο, τις οποίες θα διαχειρίζεται οντότητα εγκατεστημένη στην ΕΕ.

76) Το EU-CyCLONe και το δίκτυο CSIRT, για τους σκοπούς της ανταλλαγής πληροφοριών με διαβάθμιση RESTREINT UE/EU RESTRICTED, εφόσον απαιτείται, θα πρέπει να είναι σε θέση να χρησιμοποιούν ασφαλείς διαύλους επικοινωνίας που εξασφαλίζονται για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ για την ανταλλαγή διαβαθμισμένων πληροφοριών μεταξύ τους και με τα κράτη μέλη.

---

15 WK 862/2023.

77) Το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας («ECCC») που συστάθηκε με τον κανονισμό (ΕΕ) 2021/887[16], με την επιφύλαξη του μελλοντικού πολυετούς δημοσιονομικού πλαισίου, θα πρέπει να εξετάσει το ενδεχόμενο χρηματοδότησης μέσω του προγράμματος Ψηφιακή Ευρώπη, προκειμένου να βοηθήσει τα κράτη μέλη στη χρήση των εργαλείων ασφαλούς επικοινωνίας. Θα πρέπει να αποφεύγεται κάθε αλληλεπικάλυψη επενδύσεων στα διαλειτουργικά ασφαλή συστήματα.

78) Ειδικότερα, οι οντότητες της ΕΕ και τα κράτη μέλη θα πρέπει να καταρτίζουν σχέδια αντιμετώπισης έκτακτων καταστάσεων για σοβαρές κρίσεις, όταν οι καθιερωμένοι δίαυλοι επικοινωνίας που βασίζονται στο διαδίκτυο ή στα δίκτυα τηλεπικοινωνιών διαταράσσονται ή δεν είναι διαθέσιμοι.

79) Θα πρέπει να θεσπιστούν μηχανισμοί επικοινωνίας και ανταλλαγής πληροφοριών μεταξύ των δικτύων επιβολής του νόμου και των δικτύων κυβερνοασφάλειας, ιδίως σε τεχνικό επίπεδο, με σκοπό την αποτελεσματική αντιμετώπιση κυβερνοκρίσεων. Οι μηχανισμοί αυτοί θα πρέπει να σέβονται τον ρόλο κάθε μέρους, να μην παρεμβαίνουν στις δραστηριότητες που βρίσκονται σε εξέλιξη και να εγγυώνται πλεονάζοντες τρόπους επικοινωνίας. Το ευρωπαϊκό σύστημα κρίσιμων επικοινωνιών (EUCCS) μπορεί να ωφελήσει την κοινή αντίδραση με τις σχετικές κυβερνοκοινότητες.

XIII: Τελικές διατάξεις

80) Το EU-CyCLONe, σε συνεργασία με το δίκτυο CSIRT και άλλους βασικούς φορείς του οικοσυστήματος διαχείρισης κυβερνοκρίσεων της ΕΕ, με την υποστήριξη του ENISA, θα πρέπει να αναπτύξει, εντός ενός έτους από τη δημοσίευση της σύστασης, λεπτομερή διαγράμματα ροής διαδικασιών, στα οποία θα παρουσιάζονται οι ροές πληροφοριών μεταξύ των σχετικών φορέων, οι διαδικασίες λήψης αποφάσεων και οι εκθέσεις που καταρτίζονται κατά τη διαχείριση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης, όπως περιγράφονται στην παρούσα σύσταση. Τα διαγράμματα ροής θα πρέπει να καλύπτουν διαφορετικούς τρόπους και επίπεδα συνεργασίας. Θα πρέπει να επικαιροποιούνται, όταν απαιτείται.

---

16 Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού, ΕΕ L 202 της 8.6.2021, σ. 1.

81) Για τη στήριξη της αποτελεσματικής εφαρμογής του αναθεωρημένου σχεδίου στρατηγικής για τον κυβερνοχώρο και με βάση την πείρα από τις κοινές ασκήσεις για τον κυβερνοχώρο που θα διεξαχθούν στο πλαίσιο αυτού, το Συμβούλιο μπορεί να αναπτύξει, εάν χρειαστεί, δέσμη κατευθυντήριων γραμμών εφαρμογής. Οι εν λόγω κατευθυντήριες γραμμές θα μπορούσαν να αντιμετωπίσουν τις πρακτικές προκλήσεις που προσδιορίζονται κατά τη διάρκεια των ασκήσεων και να καλύψουν τα κενά που εντοπίζονται και τους ελλείποντες κρίκους όσον αφορά τον συντονισμό, την επικοινωνία και την επιχειρησιακή αλληλεπίδραση.

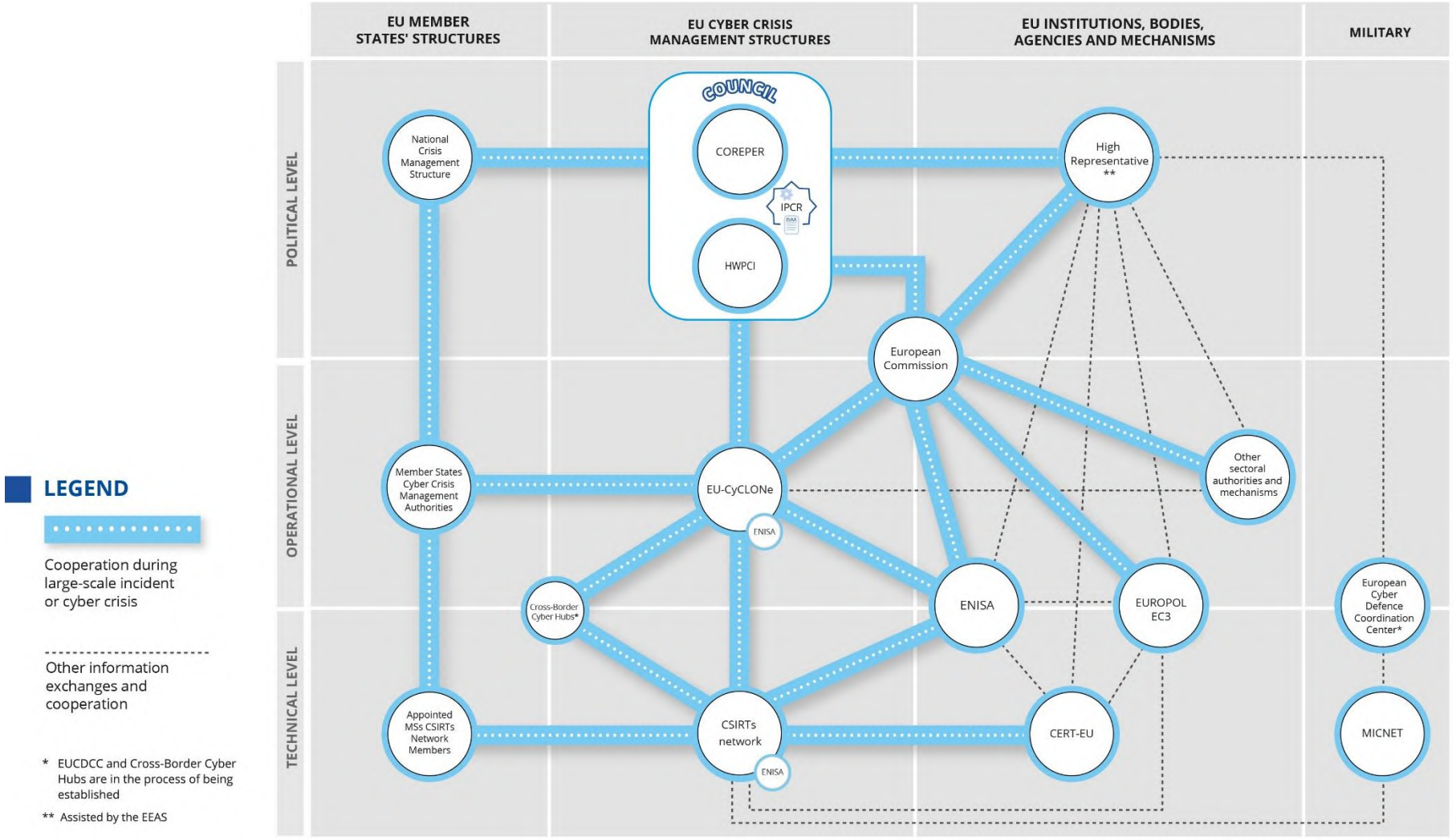
82) Η παρούσα σύσταση θα πρέπει να επανεξετάζεται από την Επιτροπή σε συνεργασία με τα κράτη μέλη, τουλάχιστον ανά τετραετία μετά τη δημοσίευσή της. Μετά από κάθε επανεξέταση, η Επιτροπή θα πρέπει να δημοσιεύει έκθεση και να την υποβάλλει στο Συμβούλιο. Η Επιτροπή και τα κράτη μέλη θα πρέπει να λαμβάνουν υπόψη, ιδίως, τον αντίκτυπο του μεταβαλλόμενου τοπίου απειλών, τα αποτελέσματα των κοινών ασκήσεων και τις νομοθετικές αλλαγές —ιδίως τυχόν αλλαγές που απορρέουν από την αναθεώρηση του κανονισμού (ΕΕ) 2019/881.

Βρυξέλλες,

Για το Συμβούλιο

Ο Πρόεδρος / Η Πρόεδρος

ΠΑΡΑΡΤΗΜΑ I — Το σχέδιο στρατηγικής της Ένωσης για την αντιμετώπιση κρίσεων κυβερνοασφάλειας



ΠΑΡΑΡΤΗΜΑ ΙΙ — ΑΡΜΟΔΙΟΙ ΦΟΡΕΙΣ (ΟΝΤΟΤΗΤΕΣ ΚΑΙ ΔΙΚΤΥΑ) ΣΕ ΕΠΙΠΕΔΟ ΕΝΩΣΗΣ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΚΡΙΣΕΩΝ

1) Συμμετοχή των κύριων φορέων σε ολόκληρο τον κύκλο ζωής της διαχείρισης κυβερνοκρίσεων (μεγάλης κλίμακας περιστατικά κυβερνοασφάλειας και κυβερνοκρίσεις)

	Ετοιμότητα	Εντοπισμός	Αντιμετώπιση μεγάλης κλίμακας περιστατικού κυβερνοασφάλειας ή κυβερνοκρίσης			Επικοινωνία με το κοινό	Ανάκαμψη και διδάγματα που αντλήθηκαν
			σε τεχνικό επίπεδο	σε επιχειρησιακό επίπεδο	σε πολιτικό επίπεδο		
Κράτη μέλη	X	X	X	X	X	X	X
Επιτροπή	X			X	X	X	
Ύπατος Εκπρόσωπος επικουρούμενος από την ΕΥΕΔ	X			X	X	X	
Συμβούλιο	X				X	X	X
ENISA	X		X	X			
CERT-EE	X	X	X	X		X	X
Δίκτυο CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

2) Ρόλοι και αρμοδιότητες των σχετικών φορέων και μηχανισμών σε επίπεδο Ένωσης (με αλφαβητική σειρά) σε σχέση με τη διαχείριση κυβερνοκρίσεων

Φορέας	**Επίπεδο**	**Ρόλος και αρμοδιότητες**	**Παραπομπή**
CERT-ΕΕ	Τεχνικό / Επιχειρησιακό	Συντονίζει την αντιμετώπιση κρίσεων σε τεχνικό επίπεδο και τη διαχείριση σοβαρών περιστατικών που επηρεάζουν οντότητες της Ένωσης. Τηρεί κατάλογο της διαθέσιμης τεχνικής εμπειρογνωσίας που απαιτείται για την αντιμετώπιση περιστατικών σε περίπτωση σοβαρών περιστατικών και επικουρεί το ΙΙCB στον συντονισμό των σχεδίων διαχείρισης κυβερνοκρίσεων των οντοτήτων της Ένωσης για σοβαρά περιστατικά. Μέλος του δικτύου CSIRT. Υποστηρίζει την Επιτροπή στο EU-CyCLONe όσον αφορά τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων. Ενεργεί ως κόμβος συντονισμού για την ανταλλαγή πληροφοριών και την αντιμετώπιση περιστατικών στον τομέα της κυβερνοασφάλειας, διευκολύνοντας την ανταλλαγή πληροφοριών σχετικά με περιστατικά, κυβερνοαπειλές, ευπάθειες και παρ’ ολίγον περιστατικά μεταξύ	Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841 Κανονισμός (ΕΕ) 2025/38

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		οντοτήτων της Ένωσης και ομολόγων της. Ζητεί την ανάπτυξη της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας εξ ονόματος οντοτήτων της Ένωσης. Συνεργάζεται με το Κέντρο Κυβερνοασφάλειας του ΝΑΤΟ βάσει της τεχνικής συμφωνίας τους.	
Συμβούλιο της Ευρωπαϊκής Ένωσης	Πολιτικό	Καθήκοντα χάραξης πολιτικής και συντονισμού. Είναι επιφορτισμένο με την IPCR που αφορά τον συντονισμό και την αντιμετώπιση σε ενωσιακό πολιτικό επίπεδο.	Άρθρο 16 της Συνθήκης για την Ευρωπαϊκή Ένωση
Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης	Πολιτικό	Αποφασίζει (εκτός από τις περιπτώσεις στις οποίες γίνεται επίκληση της ρήτρας αλληλεγγύης δυνάμει του άρθρου 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης) αν θα ενεργοποιήσει την IPCR, σε διαβούλευση με τα επηρεαζόμενα κράτη μέλη, κατά περίπτωση, καθώς και με την Επιτροπή και τον ΥΕ.	Άρθρο 16 της Συνθήκης για την Ευρωπαϊκή Ένωση Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου
Διασυνοριακοί κυβερνοκόμβοι	Τεχνικό	Ο διασυνοριακός κυβερνοκόμβος είναι πολυεθνική πλατφόρμα, συσταθείσα με γραπτή συμφωνία κοινοπραξίας, η οποία συγκεντρώνει σε συντονισμένη δομή δικτύου εθνικούς κυβερνοκόμβους από	Κανονισμός (ΕΕ) 2025/38

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		τουλάχιστον τρία κράτη μέλη, και η οποία έχει σχεδιαστεί για την ενίσχυση της παρακολούθησης, της ανίχνευσης και της ανάλυσης κυβερνοαπειλών, με σκοπό την πρόληψη περιστατικών και τη στήριξη της παραγωγής πληροφοριών σχετικά με κυβερνοαπειλές, ιδίως μέσω της ανταλλαγής σχετικών δεδομένων και πληροφοριών, ανωνυμοποιημένων κατά περίπτωση, καθώς και μέσω της ανταλλαγής εργαλείων αιχμής και της από κοινού ανάπτυξης ικανοτήτων ανίχνευσης, ανάλυσης και πρόληψης και προστασίας στον κυβερνοχώρο σε ένα αξιόπιστο περιβάλλον· Συνεργάζονται στενά με το δίκτυο CSIRT για την ανταλλαγή πληροφοριών. Παρέχουν πληροφορίες σχετικά με δυνητικό ή υπό εξέλιξη περιστατικό κυβερνοασφάλειας μεγάλης κλίμακας στις αρχές των κρατών μελών και στην Επιτροπή μέσω του EU-CyCLONe και του δικτύου CSIRT.	

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
Δίκτυο CSIRT	Τεχνικό	Συμβάλλει στην ανάπτυξη εμπιστοσύνης και στην προώθηση ταχείας επιχειρησιακής συνεργασίας μεταξύ των κρατών μελών. Είναι το κύριο δίκτυο για την ανταλλαγή πληροφοριών σχετικά με περιστατικά, παρ' ολίγον περιστατικά, κυβερνοαπειλές, κινδύνους και ευπάθειες. Κατόπιν αιτήματος μέλους που ενδεχομένως έχει επηρεαστεί από περιστατικό, το δίκτυο ανταλλάσσει και συζητά σχετικά με πληροφορίες που αφορούν το εν λόγω περιστατικό και σχετικές κυβερνοαπειλές. Το δίκτυο μπορεί επίσης να διευκολύνει τη συντονισμένη αντίδραση σε περιστατικό που έχει εντοπιστεί εντός της δικαιοδοσίας αιτούντος μέλους. Παρέχει συνδρομή στα κράτη μέλη για τη διαχείριση διασυνοριακών περιστατικών και διερευνά περαιτέρω μορφές συνεργασίας, συμπεριλαμβανομένης της αμοιβαίας συνδρομής. Λαμβάνει πληροφορίες από τα κράτη μέλη όσον αφορά τα αιτήματά τους προς την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας.	Οδηγία (ΕΕ) 2022/2555 Κανονισμός (ΕΕ) 2025/38

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
Διάσκεψη των διοικητών κυβερνοχώρου		Φόρουμ για τους διοικητές του κυβερνοχώρου σε εθνικό επίπεδο εντός των κρατών μελών με σκοπό τη συνεργασία και την ανταλλαγή πληροφοριών ζωτικής σημασίας σχετικά με υπό εξέλιξη επιχειρήσεις στον κυβερνοχώρο και στρατηγικές για τον μετριασμό κυβερνοπεριστατικών μεγάλης κλίμακας. Διοργανώνεται από την εκ περιτροπής Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης με την υποστήριξη του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ) και της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ), συμπεριλαμβανομένου του Στρατιωτικού Επιτελείου της ΕΕ (EUMS).	Κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα (2022)
Επιτροπή	Επιχειρησιακό / Πολιτικό	Εκτελεστικό όργανο της Ευρωπαϊκής Ένωσης. Διασφαλίζει την εύρυθμη λειτουργία της εσωτερικής αγοράς. Διευκολύνει τη συνοχή και τον συντονισμό μεταξύ συναφών πανενωσιακών δράσεων αντιμετώπισης κρίσεων. Ορισμένες γενικές δράσεις ετοιμότητας σε επίπεδο Ένωσης, βάσει της απόφασης για τον ΜΠΠΕ,	Άρθρο 17 της Συνθήκης για την Ευρωπαϊκή Ένωση Εκτελεστική απόφαση (ΕΕ) 2018/1993 Απόφαση αριθ. 1313/2013/ΕΕ Οδηγία (ΕΕ) 2022/2555 Κανονισμός (ΕΕ) 2025/38

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		συμπεριλαμβανομένης της διαχείρισης του Κέντρου Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών και του κοινού συστήματος επικοινωνίας και πληροφόρησης έκτακτης ανάγκης. Παρατηρητής στο EU-CyCLONe και μέλος σε περίπτωση όπου δυνητικό ή υπό εξέλιξη μεγάλης κλίμακας περιστατικό έχει ή είναι πιθανό να έχει σημαντικό αντίκτυπο σε υπηρεσίες και δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2022/2555. Παρατηρητής στο δίκτυο CSIRT. Γενική ευθύνη για την υλοποίηση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας. Σημείο επαφής του διοργανικού συμβουλίου κυβερνοασφάλειας για την ανταλλαγή σχετικών πληροφοριών με το EU-CyCLONe σε σχέση με σοβαρά περιστατικά. Παρέχει τη γνώμη της στην Προεδρία του Συμβουλίου σχετικά με αποφάσεις ενεργοποίησης ή απενεργοποίησης της IPCR (εκτός εάν γίνεται επίκληση της ρήτρας αλληλεγγύης δυνάμει του άρθρου 222 της ΣΛΕΕ).	Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		Οι υπηρεσίες της Επιτροπής καταρτίζουν, μαζί με την ΕΥΕΔ, τις εκθέσεις ISAA.	
Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)	Τεχνικό / Επιχειρησιακό	Εκτελεί καθήκοντα με σκοπό την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση, μεταξύ άλλων με ενεργό στήριξη στα κράτη μέλη και στα θεσμικά όργανα της Ένωσης. Παρέχει γραμματειακή υποστήριξη για το δίκτυο CSIRT και το EU-CyCLONe. Συντάσσει τακτικά τεχνικές εκθέσεις για την κατάσταση της κυβερνοασφάλειας στην ΕΕ σχετικά με περιστατικά και κυβερνοαπειλές (με το EC3 και τη CERT-ΕΕ και σε στενή συνεργασία με τα κράτη μέλη). Συμβάλλει στην ανάπτυξη από κοινού αντιμετώπισης διασυνοριακών περιστατικών ή κρίσεων μεγάλης κλίμακας με τους εξής κυρίως τρόπους: - συγκέντρωση και ανάλυση εκθέσεων από εθνικές πηγές· - διασφάλιση της ροής πληροφοριών μεταξύ τεχνικού, επιχειρησιακού και πολιτικού επιπέδου·	Οδηγία (ΕΕ) 2022/2555 Κανονισμός (ΕΕ) 2019/881 Κανονισμός (ΕΕ) 2025/38 Κανονισμός (ΕΕ) 2024/2847

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		- κατόπιν αιτήματος, διευκόλυνση για τον χειρισμό περιστατικών· - στήριξη των οντοτήτων της Ένωσης όσον αφορά την επικοινωνία με το κοινό· - στήριξη των κρατών μελών όσον αφορά την επικοινωνία με το κοινό, κατόπιν αιτήματος· - δοκιμή ικανοτήτων αντιμετώπισης περιστατικών και τακτική διοργάνωση ασκήσεων κυβερνοασφάλειας. Ενεργεί ως αναθέτουσα αρχή όταν του ανατίθεται η λειτουργία και η διαχείριση της εφεδρείας της ΕΕ στον τομέα της κυβερνοασφάλειας, εν μέρει ή πλήρως. Διοργανώνει ανά διετία ολοκληρωμένη άσκηση κυβερνοασφάλειας μεγάλης κλίμακας σε επίπεδο Ένωσης με τεχνικά, επιχειρησιακά ή στρατηγικά στοιχεία. Συντάσσει έκθεση εξέτασης περιστατικού σε συνεργασία με το ενδιαφερόμενο κράτος μέλος και άλλα αρμόδια ενδιαφερόμενα μέρη, όπου αξιολογούνται τα αίτια, οι επιπτώσεις και ο μετριασμός ενός περιστατικού (κατόπιν αιτήματος της Επιτροπής ή του EU-CyCLONe και	

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		με την έγκριση του ενδιαφερόμενου κράτους μέλους). Ενημερώνει το EU-CyCLONe αν οι πληροφορίες που παρέχονται στο πλαίσιο των υποχρεώσεων αναφοράς του κανονισμού για την κυβερνοανθεκτικότητα είναι σημαντικές για τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κυβερνοκρίσεων σε επιχειρησιακό επίπεδο.	
Ευρωπαϊκό δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe)	Επιχειρησιακό	Υποστηρίζει τη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων σε επιχειρησιακό επίπεδο. Διασφαλίζει την τακτική ανταλλαγή σχετικών πληροφοριών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης. Συντονίζει τη διαχείριση μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων και στηρίζει τη λήψη αποφάσεων σε πολιτικό επίπεδο σε σχέση με τέτοιου είδους περιστατικά και κρίσεις. Αξιολογεί τις συνέπειες και τον αντίκτυπο των σχετικών μεγάλης κλίμακας περιστατικών	Οδηγία (ΕΕ) 2022/2555 Κανονισμός (ΕΕ) 2025/38

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		κυβερνοασφάλειας και κυβερνοκρίσεων και υποβάλλει προτάσεις για πιθανά μέτρα μετριασμού. Συμβάλλει στα εθνικά σχέδια αντιμετώπισης μεγάλης κλίμακας περιστατικών κυβερνοασφάλειας και κυβερνοκρίσεων, κατόπιν αιτήματος ενδιαφερόμενου κράτους μέλους. Καταρτίζει, από κοινού με τον ENISA και την Επιτροπή, το υπόδειγμα για τη διευκόλυνση της υποβολής αιτημάτων στήριξης από την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Λαμβάνει πληροφορίες από τα κράτη μέλη όσον αφορά τα αιτήματά τους προς την εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας. Λαμβάνει πληροφορίες σχετικά με δυνητικό ή υπό εξέλιξη περιστατικό μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας από τους διασυνοριακούς κυβερνοκόμβους ή το δίκτυο CSIRT.	
Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας,	Πολιτικό	Κατευθύνει και συντονίζει τις προσπάθειες της Ένωσης για την αντιμετώπιση εξωτερικών απειλών κατά της ασφάλειας στους τομείς των υβριδικών μέσων και του κυβερνοχώρου	Απόφαση 2010/427/ΕΕ του Συμβουλίου

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
επικουρούμενος από την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης		Υπεύθυνος για τα μέσα κυβερνοδιπλωματίας και κυβερνοάμυνας της Ένωσης, με σκοπό την αποτροπή και την αντιμετώπιση εξωτερικών απειλών, μεταξύ άλλων, χρησιμοποιώντας τις εργαλειοθήκες της Ένωσης για την υβριδική διπλωματία και τη διπλωματία στον κυβερνοχώρο. Συνεργάζεται με εξωτερικούς εταίρους, μεταξύ άλλων μέσω της δραστηριοποίησης στο πλαίσιο της ΚΠΑΑ. Παρέχει ετοιμότητα στην Ένωση και στα κράτη μέλη όσον αφορά την επίγνωση της κατάστασης και την ικανότητα αντίδρασης σε υβριδικές απειλές και κυβερνοαπειλές, για παράδειγμα μέσω πρακτικών ασκήσεων, κατάρτισης και δικτύων. Χειρίζεται τις επιπτώσεις των διαστημικών πόρων της Ένωσης στην ασφάλεια και την άμυνα, ιδίως στο πλαίσιο της κοινής πολιτικής ασφάλειας και άμυνας (ΚΠΑΑ) της Ένωσης. Υποστηρίζει τη διάσκεψη των διοικητών κυβερνοχώρου της ΕΕ. Υποστηρίζει το επιχειρησιακό δίκτυο των στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών	

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
		στην πληροφορική («MICNET») της ΕΕ. Παρέχει τη γνώμη του στην Προεδρία του Συμβουλίου σχετικά με αποφάσεις ενεργοποίησης ή απενεργοποίησης της IPCR (εκτός εάν γίνεται επίκληση της ρήτρας αλληλεγγύης δυνάμει του άρθρου 222 της ΣΛΕΕ). Η ΕΥΕΔ καταρτίζει, μαζί με τις υπηρεσίες της Επιτροπής, τις εκθέσεις ISAA.	
Κέντρο συντονισμού της ΕΕ για την κυβερνοάμυνα	Οριζόντιος	Αρχικός στόχος του είναι να ενισχύσει πρωτίστως τις ικανότητες της Ένωσης και των κρατών μελών της για κοινή επίγνωση της κατάστασης όσον αφορά κακόβουλες δραστηριότητες στον κυβερνοχώρο, ιδίως όσον αφορά στρατιωτικές αποστολές και επιχειρήσεις της ΚΠΑΑ.	Κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα (2022)
Ευρωπόλ	Επιχειρησιακό	Παρέχει επιχειρησιακή και τεχνική υποστήριξη στις αρμόδιες αρχές των κρατών μελών για την πρόληψη και την αποτροπή του κυβερνοεγκλήματος. Επικουρεί τις αρμόδιες αρχές των κρατών μελών, κατόπιν αιτήματός τους, στην αντιμετώπιση κυβερνοεπιθέσεων με εικαζόμενη εγκληματική προέλευση.	Κανονισμός (ΕΕ) 2016/794, συμπεριλαμβανομένων όλων των τροποποιήσεων

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
Διοργανικό συμβούλιο κυβερνοασφάλειας		Καταρτίζει σχέδιο διαχείρισης κυβερνοκρίσεων με σκοπό τη στήριξη, σε επιχειρησιακό επίπεδο, της συντονισμένης διαχείρισης σοβαρών περιστατικών που επηρεάζουν οντότητες της Ένωσης, και τη συμβολή στην τακτική ανταλλαγή σχετικών πληροφοριών. Συντονίζει την έγκριση των σχεδίων διαχείρισης κυβερνοκρίσεων που καταρτίζουν οι επιμέρους οντότητες της Ένωσης. Εκδίδει, βάσει πρότασης της CERT-ΕΕ, κατευθυντήριες γραμμές ή συστάσεις σχετικά με τη συνεργασία στην αντιμετώπιση περιστατικών για σημαντικά περιστατικά που αφορούν οντότητες της Ένωσης.	Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841
Επιχειρησιακό δίκτυο των στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (MICNET)	Τεχνικό	Προωθεί μια πιο ισχυρή και συντονισμένη αντίδραση στις κυβερνοαπειλές που πλήττουν τα αμυντικά συστήματα στην Ένωση, συμπεριλαμβανομένων εκείνων που χρησιμοποιούνται σε στρατιωτικές αποστολές και επιχειρήσεις της ΚΠΑΑ· υποστηρίζεται από τον Ευρωπαϊκό Οργανισμό Άμυνας.	Κοινή ανακοίνωση για την κυβερνοάμυνα 2022

Φορέας	Επίπεδο	Ρόλος και αρμοδιότητες	Παραπομπή
Ενιαία Ικανότητα Ανάλυσης Πληροφοριών (SIAC)		Αποτελείται από 1) το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (EU INTCEN) και 2) τη Διεύθυνση Πληροφοριών του Στρατιωτικού Επιτελείου της ΕΕ (EUMS INT). Παρέχει στρατηγικές πληροφορίες σχετικά με την εξωτερική πολιτική, την τρομοκρατία και τις κυβερνοαπειλές και τις υβριδικές απειλές, και Χειρίζεται τις στρατιωτικές πληροφορίες για τις αποστολές ΚΠΑΑ και στηρίζει τις επιχειρήσεις άμυνας και διαχείρισης κρίσεων της Ένωσης. Τελεί υπό την εποπτεία του Ύπατου Εκπροσώπου.	Άρθρα 38 και 42 έως 46 της Συνθήκης για την Ευρωπαϊκή Ένωση.

3) Σχετικοί μηχανισμοί και πλατφόρμες διαχείρισης κρίσεων σε επίπεδο Ένωσης

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
ARGUS	Οριζόντιος	Η διαδικασία συντονισμού και το γενικό σύστημα προειδοποίησης της Επιτροπής για μια συνεκτική αντίδραση σε περίπτωση μείζονος διασυνοριακής κρίσης που απαιτεί δράση σε επίπεδο ΕΕ. Συγκεντρώνει όλες τις αρμόδιες υπηρεσίες και τα ιδιαίτερα γραφεία που θα αποφασίσουν και θα συντονίσουν τα μέτρα. Δίνει τη δυνατότητα στην Επιτροπή να ανταλλάσσει σχετικές πληροφορίες σχετικά με αναδυόμενες πολυτομεακές κρίσεις ή προβλέψιμες ή επικείμενες απειλές που απαιτούν δράση σε ενωσιακό επίπεδο.	Ανακοίνωση (2005) 662 της Επιτροπής
Κέντρο Αντιμετώπισης Κρίσεων της ΕΥΕΔ	Οριζόντιος	Το ενιαίο σημείο επαφής στην ΕΥΕΔ για όλα τα συνυφασμένα με κρίσεις θέματα στην και η ικανότητα συνεχούς αντιμετώπισης κρίσεων σε 24ωρη βάση 7 ημέρες την εβδομάδα για καταστάσεις έκτακτης ανάγκης που απειλούν την ασφάλεια του προσωπικού των αντιπροσωπιών της ΕΕ και/ή για την ανταπόκριση σε κρίσεις που επηρεάζουν πολίτες της Ένωσης στο εξωτερικό. Συγκεντρώνει ειδικούς σε θέματα ασφάλειας, προξενικών υπηρεσιών και επίγνωσης της κατάστασης, ενώ παράλληλα βασίζεται σε	Στρατηγική πυξίδα για την ασφάλεια και την άμυνα — Για μια Ευρωπαϊκή Ένωση που προστατεύει τους πολίτες, τις αξίες και τα συμφέροντά της και συμβάλλει στη διεθνή ειρήνη και ασφάλεια (21 Μαρτίου 2022)

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
		αφοσιωμένους επαγγελματίες στις αντιπροσωπίες της Ένωσης.	
Σχέδιο στρατηγικής για τις κρίσιμες υποδομές	Οριζόντιος	Συντονίζει σε ενωσιακό επίπεδο την αντιμετώπιση διαταράξεων σε κρίσιμες υποδομές με σημαντικό διασυνοριακό ενδιαφέρον.	Σύσταση του Συμβουλίου C/2024/4371
Σύστημα προειδοποίησης για την κυβερνοασφάλεια	Ειδικός για τον κυβερνοχώρο	Διασφαλίζει προηγμένες ικανότητες της Ένωσης για την ενίσχυση των ικανοτήτων εντοπισμού, ανάλυσης και επεξεργασίας δεδομένων σε σχέση με κυβερνοαπειλές και την πρόληψη περιστατικών στην Ένωση.	Κανονισμός (ΕΕ) 2025/38
Εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο (Πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο)	Ειδικός για τον κυβερνοχώρο	Καθιστά δυνατή μια κοινή διπλωματική αντίδραση της Ένωσης έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, η οποία συμβάλλει στην πρόληψη των συγκρούσεων, στον μετριασμό απειλών κατά της κυβερνοασφάλειας και στη βελτίωση της σταθερότητας στις διεθνείς σχέσεις.	Συμπεράσματα του Συμβουλίου της 19ης Ιουνίου 2017 Αναθεωρημένες κατευθυντήριες γραμμές εφαρμογής 10289/23, 8 Ιουνίου 2023
Εφεδρεία της ΕΕ στον τομέα της κυβερνοασφάλειας	Ειδικός για τον κυβερνοχώρο	Κινητοποιεί εμπειρογνώμονες και πόρους στον τομέα της κυβερνοασφάλειας κατά τη διάρκεια κρίσεων για τη στήριξη των προσπαθειών αντίδρασης στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης	Κανονισμός (ΕΕ) 2025/38

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
Κώδικας δικτύου σχετικά με ειδικούς τομεακούς κανόνες για τις πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας	Τομεακός	Θεσπίζει μια επαναλαμβανόμενη διαδικασία εκτιμήσεων κινδύνων για την κυβερνοασφάλεια στον τομέα της ηλεκτρικής ενέργειας, σε επίπεδο Ένωσης, κρατών μελών, περιφερειών και οντοτήτων. Περιλαμβάνει ειδικές διατάξεις για τη διαχείριση κρίσεων και τη συνεργασία με το δίκτυο CSIRT και το EU-CyCLONe σε περιπτώσεις όπου ένα μεγάλης κλίμακας περιστατικό κυβερνοασφάλειας έχει αντίκτυπο σε άλλους τομείς που εξαρτώνται από την ασφάλεια του εφοδιασμού με ηλεκτρική ενέργεια.	Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2024/1366 της Επιτροπής
Εργαλειοθήκη για την αντιμετώπιση υβριδικών απειλών	Οριζόντιος	Περιλαμβάνει δέσμη διατάξεων για τη διασφάλιση της επισκόπησης των εργαλείων που είναι διαθέσιμα σε επίπεδο ΕΕ για την αντιμετώπιση κάθε είδους υβριδικών απειλών, και τη συντονισμένη χρήση τους, διασφαλίζοντας τη συνοχή των δράσεών μας μεταξύ διαφορετικών τομέων. Η εργαλειοθήκη για την αντιμετώπιση υβριδικών απειλών συμβάλλει στο να διασφαλιστεί ότι οι αποφάσεις λαμβάνονται με βάση ολοκληρωμένη επίγνωση της κατάστασης και τα διδάγματα που αντλήθηκαν	Συμπεράσματα του Συμβουλίου σχετικά με πλαίσιο για τη συντονισμένη αντίδραση της ΕΕ σε υβριδικές εκστρατείες, 22 Ιουνίου 2022. Κατευθυντήριες γραμμές εφαρμογής όσον αφορά το πλαίσιο για τη συντονισμένη αντίδραση της ΕΕ σε υβριδικές εκστρατείες, 14 Δεκεμβρίου 2022

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
Ομάδες ταχείας αντίδρασης σε υβριδικές ενέργειες (HRRT)	Οριζόντιος	Στο πλαίσιο της εργαλειοθήκης της ΕΕ για την αντιμετώπιση υβριδικών απειλών, οι ενωσιακές ομάδες ταχείας αντίδρασης σε υβριδικές ενέργειες βασίζονται στη σχετική τομεακή στρατιωτική και μη στρατιωτική εμπειρογνωσία σε εθνικό και ενωσιακό επίπεδο, με στόχο την παροχή εξατομικευμένης και στοχευμένης βραχυπρόθεσμης βοήθειας στα κράτη μέλη, στις αποστολές και επιχειρήσεις της κοινής πολιτικής ασφάλειας και άμυνας, καθώς και στις χώρες-εταίρους για την αντιμετώπιση υβριδικών απειλών και εκστρατειών.	Πλαίσιο καθοδήγησης για τη σύσταση στην πράξη ενωσιακών ομάδων ταχείας αντίδρασης σε υβριδικές ενέργειες (21 Μαΐου 2024) Επιχειρησιακή καθοδήγηση για την ανάπτυξη ομάδων ταχείας αντίδρασης σε υβριδικές ενέργειες, που εγκρίθηκε από την ΕΜΑ στις 4 Δεκεμβρίου 2024
IPCR	Οριζόντιος	Υποστηρίζει την ταχεία και συντονισμένη λήψη αποφάσεων σε ενωσιακό πολιτικό επίπεδο για μείζονες και πολύπλοκες κρίσεις. Η απόφαση ενεργοποίησης και απενεργοποίησης λαμβάνεται από την Προεδρία του Συμβουλίου, κατόπιν διαβούλευσης (εκτός από τις περιπτώσεις κατά τις οποίες γίνεται επίκληση της ρήτρας αλληλεγγύης) με τα επηρεαζόμενα κράτη μέλη, την Επιτροπή και τον Ύπατο Εκπρόσωπο.	Εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
		Η Γενική Γραμματεία του Συμβουλίου (ΓΓΣ), οι υπηρεσίες της Επιτροπής και η ΕΥΕΔ μπορούν επίσης να συμφωνήσουν, σε διαβούλευση με την Προεδρία, να ενεργοποιήσουν την IPCR σε κατάσταση λειτουργίας ανταλλαγής πληροφοριών. Το έργο της IPCR αξιοποιεί τις εκθέσεις ISAA που καταρτίζουν οι υπηρεσίες της Επιτροπής και η ΕΥΕΔ. Οι εν λόγω εκθέσεις βασίζονται σε σχετικές πληροφορίες και αναλύσεις που παρέχουν τα κράτη μέλη (π.χ. από τα αρμόδια εθνικά κέντρα αντιμετώπισης κρίσεων) και οι αρμόδιοι οργανισμοί και όργανα της Ένωσης.	
Πρωτόκολλο της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου	Οριζόντιος	Εργαλείο που στηρίζει τις αρχές επιβολής του νόμου της Ένωσης στην παροχή άμεσης αντίδρασης σε μείζονες διασυνοριακές κυβερνοεπιθέσεις μέσω ταχείας αξιολόγησης, ασφαλούς και έγκαιρης ανταλλαγής κρίσιμων πληροφοριών και αποτελεσματικού συντονισμού των διεθνών πτυχών των ερευνών τους.	Συμπεράσματα του Συμβουλίου, της 26ης Ιουνίου 2018, για τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο.
Ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο στο	Ειδικός για τον κυβερνοχώρο	Οι CRRT της PESCO είναι μια από κοινού ανεπτυγμένη πολιτικοστρατιωτική ικανότητα	Άρθρο 42 παράγραφος 6, άρθρο 46 και πρωτόκολλο

Μηχανισμός	Οριζόντιος / τομεακός / ειδικός για τον κυβερνοχώρο	Περιγραφή	Παραπομπή
πλαίσιο της PESCO (CRRT)		κυβερνοάμυνας των κρατών μελών της ΕΕ για την ταχεία αντιμετώπιση σημαντικών κυβερνοπεριστατικών και κυβερνοκρίσεων, καθώς και για την εφαρμογή προληπτικών μέτρων, όπως αξιολογήσεις ευπαθειών και παρακολούθηση εκλογών. Αποστολή των CRRT της PESCO είναι η παροχή στήριξης σχετικά με τον κυβερνοχώρο, κατόπιν αιτήματος, στα κράτη μέλη της ΕΕ, στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ, στις στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ της ΕΕ, καθώς και στις χώρες εταίρους.	10 της Συνθήκης για την Ευρωπαϊκή Ένωση.

Αρχιτεκτονική απόκρισης σε διαστημικές απειλές (STRA)	Τομεακός (Διαστημικές απειλές, συμπεριλαμβανομένων των κυβερνοαπειλών)	Αρχιτεκτονική απόκρισης σε διαστημικές απειλές (STRA) σχετικά με τις αρμοδιότητες που πρέπει να ασκεί το Συμβούλιο και ο Ύπατος Εκπρόσωπος με σκοπό την αποτροπή απειλής που προκύπτει από την ανάπτυξη, τη λειτουργία ή τη χρήση των συστημάτων που δημιουργούνται και των υπηρεσιών που παρέχονται στο πλαίσιο του ενωσιακού διαστημικού προγράμματος	Απόφαση (ΚΕΠΠΑ) 2021/698 του Συμβουλίου
Πλαίσιο συντονισμού συστημικών κυβερνοπεριστατικών (EU-SCICF)	Τομεακός	Πλαίσιο που βρίσκεται σε στάδιο ανάπτυξης για την επικοινωνία και τον συντονισμό, και το οποίο αντιμετωπίζει και διαχειρίζεται πιθανά συστημικά κυβερνοπεριστατικά στον χρηματοοικονομικό τομέα. Θα βασιστεί σε έναν από τους προβλεπόμενους ρόλους των Ευρωπαϊκών Εποπτικών Αρχών (ΕΕΑ) δυνάμει του κανονισμού (ΕΕ) 2022/2554 για τη σταδιακή εξασφάλιση της δυνατότητας αποτελεσματικής συντονισμένης απόκρισης σε επίπεδο ΕΕ, σε περίπτωση μείζονος διασυνοριακού συμβάντος που σχετίζεται με τις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) ή σχετικής απειλής με συστημικές επιπτώσεις στον χρηματοοικονομικό τομέα της Ένωσης συνολικά.	Σύσταση του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου, της 2ας Δεκεμβρίου 2021, σχετικά με ένα πανευρωπαϊκό πλαίσιο συντονισμού συστημικών κυβερνοπεριστατικών για τις σχετικές αρχές (ΕΣΣΚ/2021/17)
Μηχανισμός πολιτικής προστασίας της Ένωσης (ΜΠΠΕ)	Οριζόντιος	Διασφαλίζει τη συνεργασία στον τομέα της πολιτικής προστασίας με σκοπό τη βελτίωση της πρόληψης, της ετοιμότητας και της αντιμετώπισης καταστροφών.	Απόφαση 1313/2013.

CISE — Κοινό περιβάλλον ανταλλαγής πληροφοριών	Αφορά ειδικά τη ναυτιλία και καλύπτει επτά τομείς.	Το CISE είναι ένα δίκτυο που συνδέει τα συστήματα των αρχών της ΕΕ / του ΕΟΧ οι οποίες είναι αρμόδιες για τη θαλάσσια επιτήρηση. Το CISE καθιστά δυνατή την ανταλλαγή σχετικών πληροφοριών σε διασυνοριακό επίπεδο και σε διάφορους τομείς με απρόσκοπτο και αυτοματοποιημένο τρόπο.	Στρατηγική πυξίδα για την ασφάλεια και την άμυνα — Για μια Ευρωπαϊκή Ένωση που προστατεύει τους πολίτες, τις αξίες και τα συμφέροντά της και συμβάλλει στη διεθνή ειρήνη και ασφάλεια (21 Μαρτίου 2022).

4) Τομείς υψηλής κρισιμότητας και άλλοι κρίσιμοι τομείς βάσει της οδηγίας (ΕΕ) 2022/2555 και τομεακοί μηχανισμοί διαχείρισης κρίσεων σε επίπεδο Ένωσης (κατά περίπτωση)		
Τομείς	**Υποτομέας**	**Εφαρμοστέοι τομεακοί μηχανισμοί αντιμετώπισης κρίσεων**
Ενέργεια	Ηλεκτρική ενέργεια	Συντονιστική ομάδα για την ηλεκτρική ενέργεια
	Τηλεθέρμανση και τηλεψύξη	ά.α.
	Πετρέλαιο	Συντονιστική ομάδα για το πετρέλαιο Ομάδα Αρχών Εποπτείας των Υπεράκτιων Εργασιών της Ευρωπαϊκής Ένωσης (EUOAG)
	Αέριο	Συντονιστική ομάδα για το αέριο
	Υδρογόνο	ά.α.
Μεταφορές	Εναέριες	Ευρωπαϊκή μονάδα συντονισμού αεροπορικών κρίσεων (EACCC)
	Σιδηροδρομικές	ά.α.
	Πλωτές	Ευρωπαϊκή Υπηρεσία Ελέγχου της Αλιείας (EFCA) SafeSeaNet (SSN) Ολοκληρωμένες θαλάσσιες υπηρεσίες (IMS) Κέντρο δεδομένων για την ταυτοποίηση και τον εντοπισμό σκαφών εξ αποστάσεως (LRIT) Υπηρεσίες θαλάσσιας υποστήριξης του EMSA

	Οδικές	ά.α.
	Οριζόντιος	Το δίκτυο εθνικών σημείων επαφής για τις μεταφορές, το οποίο συστάθηκε με το σχέδιο έκτακτης ανάγκης για τις μεταφορές [COM(2022) 211]
Τραπεζικός κλάδος		ΕΕ-SCICF
Υποδομές χρηματοπιστωτικών αγορών		ΕΕ-SCICF Ευρωπαϊκός Μηχανισμός Χρηματοοικονομικής Σταθεροποίησης

Υγεία		Σύστημα έγκαιρης προειδοποίησης και αντίδρασης (EWRS) Μηχανισμός επιχειρήσεων έκτακτης ανάγκης στον τομέα της υγείας (HEOF) Σύστημα έγκαιρης προειδοποίησης για ιστούς, κύτταρα και συστατικά του αίματος (RATC/RAB) Πλαίσιο για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της δημόσιας υγείας Σύστημα έγκαιρης ειδοποίησης για χημικά συμβάντα (RASCHEM) Η ευρωπαϊκή πύλη επιτήρησης για τις λοιμώδεις νόσους Αρχή Ετοιμότητας και Αντιμετώπισης Καταστάσεων Έκτακτης Υγειονομικής Ανάγκης (HERA) Σύστημα ιατρικών πληροφοριών για την υγεία (MediSys) Εκτελεστική ομάδα καθοδήγησης για τις ελλείψεις ιατροτεχνολογικών προϊόντων (MDSSG) Σύστημα ταχείας προειδοποίησης για τη φαρμακοεπαγρύπνηση Ειδική ομάδα της ΕΕ για την υγεία (EUHTF) Επιτροπή υγειονομικής ασφάλειας
Πόσιμο νερό		ά.α.

Λύματα		ά.α.
Ψηφιακές υποδομές		ά.α.
Διαχείριση υπηρεσιών ΤΠΕ		ά.α.
Δημόσια διοίκηση		ά.α.
Διάστημα		Αρχιτεκτονική απόκρισης σε διαστημικές απειλές (STRA)
Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών		ά.α.
Διαχείριση αποβλήτων		ά.α.
Παρασκευή, παραγωγή και διανομή χημικών προϊόντων		Σύστημα έγκαιρης ειδοποίησης για χημικά συμβάντα (RASCHEM)

Παραγωγή, επεξεργασία και διανομή τροφίμων		Ευρωπαϊκό σύστημα παρακολούθησης των καλλιεργειών Παγκόσμιο σύστημα ανίχνευσης ανωμαλιών στη γεωργική παραγωγή (ASAP) Ευρωπαϊκό δίκτυο πληροφοριακών συστημάτων για την υγεία των φυτών (EUROPHYT) Κτηνιατρική ομάδα έκτακτης ανάγκης της ΕΕ (EUVET) Σύστημα έγκαιρης ειδοποίησης για τα τρόφιμα και τις ζωοτροφές (RASFF) Ευρωπαϊκός μηχανισμός ετοιμότητας και αντιμετώπισης κρίσεων επισιτιστικής ασφάλειας (EFSCM) Μέσο αντιμετώπισης έκτακτων αναγκών στην ενιαία αγορά (IMERA)
Κατασκευαστικός τομέας	Ιατροτεχνολογικά προϊόντα	ά.α.
	Ηλεκτρονικοί υπολογιστές, ηλεκτρονικά και οπτικά προϊόντα	ά.α.
	Μηχανήματα και εξοπλισμός	ά.α.

	Κατασκευή μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων οχημάτων	ά.α.
	Κατασκευή λοιπού εξοπλισμού μεταφορών	ά.α.
Ψηφιακοί πάροχοι		ά.α.
Έρευνα		ά.α.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ – Πλαίσιο διαχείρισης κρίσεων κυβερνοασφάλειας και συναφή μέσα της ΕΕ

Από το 2017 η Ένωση έχει διαμορφώσει το οικείο πλαίσιο κυβερνοασφάλειας μέσω διαφόρων πράξεων που περιέχουν διατάξεις σχετικές με τη διαχείριση κρίσεων κυβερνοασφάλειας:

- Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[1],
- Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[2],
- Εκτελεστικός κανονισμός 2024/2690 της Επιτροπής [3], κανονισμός (ΕΕ, Ευρατόμ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[4],
- Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[5],
- Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[6], και
- Κανονισμός (ΕΕ) 2025/38 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («κανονισμός για την αλληλεγγύη στον κυβερνοχώρο»)[7].

Τα ειδικά τομεακά μέτρα για την αντιμετώπιση κρίσεων κυβερνοασφάλειας περιλαμβάνουν τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2024/1366 της Επιτροπής[8] και το επικείμενο πλαίσιο συντονισμού συστημικών κυβερνοπεριστατικών (EU-SCICF) στο πλαίσιο του κανονισμού (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[9].

Η οδηγία 2013/40[10] αποτελεί πηγή αναφοράς για τον ορισμό των εγκληματικών δραστηριοτήτων που σχετίζονται με κυβερνοεπιθέσεις, ενώ οι ενωσιακοί κανόνες σχετικά με τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία, ιδίως ο κανονισμός (ΕΕ) 2023/1543 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[11], μόλις εφαρμοστούν, θα διευκολύνουν σημαντικά τα μέτρα επιβολής του νόμου στον συγκεκριμένο τομέα.

Η πολιτική της ΕΕ για την κυβερνοάμυνα[12] περιγράφει τους ρόλους του επιχειρησιακού δικτύου στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (στο εξής: MICNET) και της διάσκεψης των διοικητών κυβερνοχώρου της ΕΕ, και προβλέπει τη δημιουργία κέντρου συντονισμού της ΕΕ για την κυβερνοάμυνα (EUCDCC).

Άλλοι μηχανισμοί επίγνωσης της κατάστασης και αντιμετώπισης κρίσεων που δεν σχετίζονται με τον κυβερνοχώρο υπάρχουν σε ορισμένους από τους κρίσιμους τομείς που απαριθμούνται στα παραρτήματα Ι και ΙΙ της οδηγίας (ΕΕ) 2022/2555.

Η «σύσταση του Συμβουλίου σχετικά με σχέδιο στρατηγικής για τον συντονισμό της αντιμετώπισης σε ενωσιακό επίπεδο διαταράξεων σε υποδομές ζωτικής σημασίας με σημαντικό διασυνοριακό ενδιαφέρον»[13] προβλέπει τη συνεργασία μεταξύ των σχετικών φορέων όταν ένα περιστατικό επηρεάζει τόσο φυσικές πτυχές όσο και την κυβερνοασφάλεια κρίσιμων υποδομών.

[1] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια) (ΕΕ L 151 της 7.6.2019, σ. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (ΕΕ L 333 της 27.12.2022, σ. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Εκτελεστικός κανονισμός (ΕΕ) 2024/2690 της Επιτροπής, της 17ης Οκτωβρίου 2024, για τη θέσπιση κανόνων εφαρμογής της οδηγίας (ΕΕ) 2022/2555 όσον αφορά τις τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας και τον περαιτέρω προσδιορισμό των περιπτώσεων στις οποίες ένα περιστατικό θεωρείται σημαντικό όσον αφορά τους παρόχους υπηρεσιών DNS, τα μητρώα ονομάτων TLD, τους παρόχους υπηρεσιών υπολογιστικού νέφους, τους παρόχους υπηρεσιών κέντρων δεδομένων, τους παρόχους δικτύων διανομής περιεχομένου, τους παρόχους διαχειριζόμενων υπηρεσιών, τους παρόχους διαχειριζόμενων υπηρεσιών ασφάλειας, τους παρόχους επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης και πλατφορμών υπηρεσιών κοινωνικής δικτύωσης και τους παρόχους υπηρεσιών εμπιστοσύνης (ΕΕ L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Κανονισμός (ΕΕ, Ευρατόμ) 2023/2841 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 2023, για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης (ΕΕ L, 2023/2841, 18.12.2023, ELI:http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Κανονισμός (ΕΕ) 2021/887 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Μαΐου 2021, για τη σύσταση του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού (ΕΕ L 202 της 8.6.2021, σ. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Κανονισμός (ΕΕ) 2025/38 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Δεκεμβρίου 2024, σχετικά με τον καθορισμό μέτρων για την ενίσχυση της αλληλεγγύης και των ικανοτήτων της Ένωσης για την ανίχνευση, την προετοιμασία και την αντιμετώπιση κυβερνοαπειλών και περιστατικών κυβερνοασφάλειας και για την τροποποίηση του

κανονισμού (ΕΕ) 2021/694 (κανονισμός για την αλληλεγγύη στον κυβερνοχώρο) (ΕΕ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2024/1366 της Επιτροπής, της 11ης Μαρτίου 2024, για τη συμπλήρωση του κανονισμού (ΕΕ) 2019/943 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τη θέσπιση κώδικα δικτύου σχετικά με ειδικούς τομεακούς κανόνες για τις πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας (ΕΕ L, 2024/1366, 24.5.2024, ELI:http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου (ΕΕ L 218 της 14.8.2013, σ. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Κανονισμός (ΕΕ) 2023/1543 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2023, σχετικά με τις ευρωπαϊκές εντολές υποβολής στοιχείων και τις ευρωπαϊκές εντολές διατήρησης στοιχείων για ηλεκτρονικά αποδεικτικά στοιχεία σε ποινικές διαδικασίες και για την εκτέλεση περιοριστικών της ελευθερίας ποινών κατόπιν ποινικών διαδικασιών και οδηγία (ΕΕ) 2023/1544 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2023, σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό ορισθεισών εγκαταστάσεων και νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών (ΕΕ L 191 της 28.7.2023, σ. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

[13] *ΕΕ C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371