II

(Μη νομοθετικές πράξεις)

ΣΥΣΤΑΣΕΙΣ

ΣΥΣΤΑΣΗ (ΕΕ) 2021/1086 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 23ης Ιουνίου 2021

σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

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

Εκτιμώντας τα ακόλουθα:

(1) Η κυβερνοασφάλεια είναι απαραίτητη για την επιτυχία του ψηφιακού μετασχηματισμού της οικονομίας και της κοινωνίας. Η ΕΕ έχει δεσμευτεί να διασφαλίσει την εμπιστοσύνη των πολιτών, των επιχειρήσεων και των δημόσιων αρχών στα ψηφιακά εργαλεία με πρωτοφανή επίπεδα επενδύσεων.

(2) Η πανδημία COVID-19 έχει αυξήσει τη σημασία της συνδεσιμότητας και της εξάρτησης της Ευρώπης από σταθερά συστήματα δικτύου και πληροφοριών και έχει καταδείξει την ανάγκη για προστασία ολόκληρης της αλυσίδας εφοδιασμού. Η εξασφάλιση αξιόπιστων και ασφαλών συστημάτων δικτύου και πληροφοριών είναι ιδιαίτερα σημαντική για τις οντότητες που βρίσκονται στην πρώτη γραμμή της καταπολέμησης της πανδημίας, όπως νοσοκομεία, ιατρικές υπηρεσίες και παρασκευαστές εμβολίων. Ο συντονισμός των προσπαθειών της ΕΕ για την πρόληψη, τον εντοπισμό, την αποθάρρυνση, τον μετριασμό και την αντιμετώπιση των πιο επιζήμιων κυβερνοεπιθέσεων έναντι των οντοτήτων αυτών θα μπορούσε να αποτρέψει απώλειες ανθρώπινων ζωών και απόπειρες υπονόμευσης της ικανότητας της ΕΕ να καταπολεμήσει την πανδημία με τον ταχύτερο δυνατό τρόπο. Επιπλέον, η ενίσχυση της ικανότητας της ΕΕ να αντιμετωπίζει αποτελεσματικά τις κυβερνοεπιθέσεις συμβάλλει στην προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου.

(3) Αντιμέτωποι με τον διασυνοριακό χαρακτήρα των κυβερνοαπειλών και τη συνεχή εμφάνιση ολοένα και πιο σύνθετων, εκτεταμένων και στοχευμένων επιθέσεων ([1]), οι σχετικοί θεσμοί και παράγοντες κυβερνοασφάλειας θα πρέπει να αυξήσουν την ικανότητά τους να αντιμετωπίζουν τέτοιες απειλές και επιθέσεις με την αξιοποίηση των υφιστάμενων πόρων και τον καλύτερο συντονισμό των προσπαθειών. Όλοι οι σχετικοί παράγοντες στην ΕΕ πρέπει να είναι προετοιμασμένοι να αντιδρούν συλλογικά και να ανταλλάσσουν πληροφορίες με βάση την «ανάγκη ανταλλαγής» και όχι την «ανάγκη γνώσης».

(4) Παρά τη σημαντική πρόοδο που έχει επιτευχθεί χάρη στη συνεργασία μεταξύ των κρατών μελών για την κυβερνοασφάλεια, ιδίως μέσω της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών («ομάδα συνεργασίας NIS») και του δικτύου ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT), που συστάθηκε δυνάμει της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]), εξακολουθεί να μην υπάρχει μια κοινή πλατφόρμα της ΕΕ για την αποτελεσματική και ασφαλή ανταλλαγή των πληροφοριών που συλλέγονται από διάφορες κοινότητες κυβερνοασφάλειας και για τον συντονισμό και την κινητοποίηση των επιχειρησιακών ικανοτήτων από τους σχετικούς φορείς. Ως εκ τούτου, υπάρχει ο κίνδυνος αποσπασματικής αντιμετώπισης των κυβερνοαπειλών και κυβερνοπεριστατικών, με περιορισμένη αποδοτικότητα και μεγαλύτερη τρωτότητα. Επιπλέον, δεν υπάρχει σε επίπεδο ΕΕ δίαυλος τεχνικής και επιχειρησιακής συνεργασίας με τον ιδιωτικό τομέα, για ανταλλαγή πληροφοριών και για υποστήριξη στην αντιμετώπιση συμβάντων.

([1]) ENISA, 2020 Threat Landscape; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020

([2]) Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

(5) Τα υφιστάμενα πλαίσια, οι δομές και οι πόροι, καθώς και η εμπειρογνωσία που διαθέτουν τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ παρέχουν μια ισχυρή βάση για τη συλλογική αντιμετώπιση απειλών, περιστατικών και κρίσεων κυβερνοασφάλειας ([3]). Η υφιστάμενη αρχιτεκτονική περιλαμβάνει, από επιχειρησιακή άποψη, το προσχέδιο συντονισμένης αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο («προσχέδιο») ([4]), το δίκτυο CSIRT και το δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο («EU CyCLONe») ([5]), καθώς και το ευρωπαϊκό κέντρο για τα εγκλήματα στον κυβερνοχώρο («EC3») και την κοινή ειδική ομάδα για την καταπολέμηση του κυβερνοεγκλήματος («J-CAT»), στο πλαίσιο του οργανισμού της Ευρωπαϊκής Ένωσης για τη συνεργασία στον τομέα της επιβολής του νόμου («Ευρωπόλ») και το πρωτόκολλο για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου («EU LE ERP»). Η ομάδα συνεργασίας NIS, το κέντρο ανάλυσης πληροφοριών της ΕΕ («EU INTCEN») και η εργαλειοθήκη για την κυβερνοδιπλωματία ([6]) και τα έργα που δρομολογήθηκαν στο πλαίσιο της μόνιμης διαρθρωμένης συνεργασίας (PESCO) ([7]) στον τομέα της κυβερνοάμυνας συμβάλλουν επίσης στην πολιτική και την επιχειρησιακή συνεργασία σε διάφορες κοινότητες κυβερνοασφάλειας. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια («ENISA»), δυνάμει της ενισχυμένης εντολής του, έχει επιφορτιστεί με την υποστήριξη της επιχειρησιακής συνεργασίας ([8]) όσον αφορά την κυβερνοασφάλεια των συστημάτων δικτύου και πληροφοριών, τους χρήστες των εν λόγω συστημάτων και άλλα πρόσωπα που πλήττονται από κυβερνοαπειλές και κυβερνοπεριστατικά. Μέσω των ολοκληρωμένων ρυθμίσεων για την πολιτική αντιμετώπιση κρίσεων («IPCR»), η ΕΕ είναι σε θέση να συντονίζει την πολιτική της αντίδραση σε μείζονες κρίσεις, μεταξύ άλλων σε περίπτωση κυβερνοεπιθέσεων μεγάλης κλίμακας.

(6) Ωστόσο, δεν υπάρχει ακόμη μηχανισμός για την αξιοποίηση των υφιστάμενων πόρων και την παροχή αμοιβαίας συνδρομής μεταξύ των κυβερνοκοινοτήτων που είναι υπεύθυνες για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, για την καταπολέμηση του κυβερνοεγκλήματος, για την άσκηση κυβερνοδιπλωματίας και, κατά περίπτωση, για την κυβερνοάμυνα σε περίπτωση κρίσης. Επίσης, δεν υπάρχει ολοκληρωμένος μηχανισμός σε επίπεδο ΕΕ για την τεχνική και επιχειρησιακή συνεργασία μεταξύ όλων των κοινοτήτων όσον αφορά την επίγνωση των καταστάσεων, την ετοιμότητα και την αντιμετώπιση. Επιπλέον, θα πρέπει να επιτευχθούν συνέργειες με τις αρχές επιβολής του νόμου και τις υπηρεσίες πληροφοριών μέσω της Ευρωπόλ και του INTCEN αντίστοιχα.

(7) Η Επιτροπή, ο ύπατος εκπρόσωπος της Ένωσης για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας (ύπατος εκπρόσωπος), τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ αναγνωρίζουν τη σημασία που έχει η ανάλυση των πλεονεκτημάτων, των αδυναμιών, των ελλείψεων και αλληλεπικαλύψεων της υφιστάμενης αρχιτεκτονικής κυβερνοασφάλειας της ΕΕ, η οποία δημιουργήθηκε τα τελευταία χρόνια. Σε διαβούλευση με τα κράτη μέλη, η Επιτροπή, με τη συμμετοχή του ύπατου εκπροσώπου, ανέπτυξε την ιδέα μιας Κοινής Κυβερνομονάδας ως απάντηση στην ανάλυση αυτή και ως μια σημαντική συνιστώσα της στρατηγικής για την Ένωση Ασφάλειας ([9]), της ψηφιακής στρατηγικής ([10]) και της στρατηγικής κυβερνοασφάλειας ([11]).

([3]) Το δίκτυο οργανισμών διασύνδεσης της ΕΕ για τις κρίσεις στον κυβερνοχώρο (EU CyCLONe) δημιουργήθηκε από τα κράτη μέλη ως απάντηση στη σύσταση για το προσχέδιο. Είναι ένα δίκτυο εθνικών εμπειρογνωμόνων σε θέματα επιχειρησιακής διαχείρισης και διαχείρισης κρίσεων το οποίο η Επιτροπή πρότεινε να κωδικοποιηθεί μέσω της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148, COM(2020) 823 final, 2020/0359 (COD) του Δεκεμβρίου 2020.

([4]) 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).

([5]) Η παρούσα σύσταση λαμβάνει υπόψη την έκθεση μετά τη δράση του 2020 στο πλαίσιο του σχεδίου άσκησης επί χάρτου σε επιχειρησιακό επίπεδο (Blue OLEx) και ιδίως τη συνοψη της προεδρίας όσον αφορά τη συζήτηση σε επίπεδο στρατηγικής πολιτικής σχετικά με την Κοινή Κυβερνομονάδα.

([6]) Συμπεράσματα του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο») της 19ης Ιουνίου 2017 (9916/17).

([7]) Ειδικότερα, τα έργα PESCO για «ομάδες ταχείας αντίδρασης στον κυβερνοχώρο και αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο», που συντονίζει η Λιθουανία, και για το «συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών», που συντονίζει η Γερμανία

([8]) Το άρθρο 7 του κανονισμού (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) απαιτεί από τον Οργανισμό να υποστηρίζει την επιχειρησιακή συνεργασία μεταξύ κρατών μελών, θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης και ενδιαφερόμενων μερών. Μεταξύ άλλων, στηρίζει τα κράτη μέλη όσον αφορά την επιχειρησιακή συνεργασία εντός του δικτύου CSIRT, εκπονεί τακτικά αναλυτική τεχνική έκθεση για την κατάσταση της κυβερνοασφάλειας στην ΕΕ όσον αφορά περιστατικά και κυβερνοαπειλές και συμβάλλει στην ανάπτυξη μιας κοινής αντιμετώπισης, σε επίπεδο Ένωσης και κρατών μελών, των διασυνοριακών περιστατικών και κρίσεων μεγάλης κλίμακας. Επιπλέον, ο ENISA συμβάλλει στις εκπαιδευτικές δραστηριότητες της Ευρωπαϊκής Σχολής Ασφάλειας και Άμυνας (ESDC).

([9]) Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας, COM/2020/605 final

([10]) Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, COM(2020) 67 final.

([11]) Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία, JOIN/2020/18 final

(8) Σε περιπτώσεις κρίσης, τα κράτη μέλη θα πρέπει να μπορούν να βασίζονται στην αλληλεγγύη της ΕΕ με τη μορφή συντονισμένης βοήθειας, μεταξύ άλλων και από τις τέσσερις κυβερνοκοινότητες, δηλαδή μη στρατιωτικές, διπλωματικές, αστυνομικές ([12]) και, όπου απαιτείται, αμυντικές. Ο βαθμός παρέμβασης των συμμετεχόντων από μία ή περισσότερες κοινότητες μπορεί να εξαρτάται από τη φύση ενός περιστατικού ή μιας κρίσης μεγάλης κλίμακας και, κατά συνέπεια, από το είδος αντιμέτρων που απαιτούνται για την αντιμετώπιση. Σε περίπτωση αντιμετώπισης απειλών, περιστατικών και κρίσεων στον κυβερνοχώρο, βασικά μέσα που μπορούν να συμβάλουν στην αποφυγή σοβαρών ζημιών και στην αποτελεσματική αποκατάσταση είναι οι καλά εκπαιδευμένοι εμπειρογνώμονες και ο τεχνικός εξοπλισμός. Ως εκ τούτου, στο επίκεντρο της Κοινής Κυβερνομονάδας θα βρίσκονται σαφώς προσδιορισμένες τεχνικές και επιχειρησιακές ικανότητες, κυρίως εμπειρογνώμονες και εξοπλισμός, έτοιμες να αποσταλούν στα κράτη μέλη σε περίπτωση ανάγκης. Σε αυτή την πλατφόρμα, οι συμμετέχοντες θα βρίσκονται σε μοναδική θέση για να προωθούν και να συντονίζουν τις εν λόγω ικανότητες μέσω των ομάδων ταχείας αντίδρασης της ΕΕ για την κυβερνοασφάλεια, εξασφαλίζοντας παράλληλα κατάλληλες συνέργειες με τα ήδη υφιστάμενα έργα PESCO που σχετίζονται με τον κυβερνοχώρο.

(9) Η Κοινή Κυβερνομονάδα παρέχει μια εικονική και φυσική πλατφόρμα και δεν απαιτεί τη δημιουργία πρόσθετου, αυτόνομου φορέα. Η σύστασή της δεν θα πρέπει να θίγει τις αρμοδιότητες και τις εξουσίες των εθνικών αρχών κυβερνοασφάλειας και των σχετικών φορέων της Ένωσης. Η Κοινή Κυβερνομονάδα θα πρέπει να βασίζεται σε μνημόνια συμφωνίας μεταξύ των συμμετεχόντων σε αυτήν. Θα πρέπει να αξιοποιεί και να προσθέτει αξία στις υφιστάμενες δομές, ικανότητες και στους διατιθέμενους πόρους, ως μια πλατφόρμα για ασφαλή και ταχεία επιχειρησιακή και τεχνική συνεργασία μεταξύ των φορέων της ΕΕ και των αρχών των κρατών μελών. Θα πρέπει επίσης να φέρνει σε επαφή όλες τις κοινότητες κυβερνοασφάλειας, δηλαδή μη στρατιωτικές, διπλωματικές, αστυνομικές και αμυντικές. Οι συμμετέχοντες στην πλατφόρμα θα πρέπει να έχουν είτε επιχειρησιακό είτε υποστηρικτικό ρόλο. Στους επιχειρησιακούς συμμετέχοντες θα πρέπει να περιλαμβάνονται ο ENISA, η Ευρωπόλ, η ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ («CERT-EU»), η Επιτροπή, η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (συμπεριλαμβανομένου του INTCEN), τα δίκτυα CSIRT και EU-CyCLONe. Στους συμμετέχοντες υποστήριξης θα πρέπει να περιλαμβάνονται ο Ευρωπαϊκός Οργανισμός Άμυνας («ΕΟΑ»), οι πρόεδροι της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS) και της οριζόντιας ομάδας εργασίας του Συμβουλίου για θέματα κυβερνοχώρου και εκπρόσωπος των σχετικών έργων PESCO ([13]). Δεδομένου ότι τα κράτη μέλη διαθέτουν επιχειρησιακές ικανότητες και αρμοδιότητες για την αντιμετώπιση απειλών, περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο, οι συμμετέχοντες στην πλατφόρμα θα πρέπει πρωτίστως να βασίζονται στις ικανότητές τους, με τη βοήθεια των σχετικών φορέων της Ένωσης, για την επίτευξη των στόχων τους.

(10) Η Κοινή Κυβερνομονάδα θα πρέπει να δώσει νέα ώθηση στη διαδικασία που ξεκίνησε με το προσχέδιο το 2017. Θα πρέπει να καταστήσει ακόμη πιο λειτουργική την αρχιτεκτονική του προσχεδίου και να σηματοδοτήσει ένα αποφασιστικό βήμα προς ένα ευρωπαϊκό πλαίσιο διαχείρισης κρίσεων κυβερνοασφάλειας, όπου οι απειλές και οι κίνδυνοι θα εντοπίζονται, θα μετριάζονται και θα αντιμετωπίζονται με συντονισμένο και έγκαιρο τρόπο. Με τη λήψη του εν λόγω μέτρου, η Κοινή Κυβερνομονάδα θα βοηθήσει την ΕΕ να ανταποκριθεί στις τρέχουσες και σε επικείμενες απειλές.

(11) Με τη συμμετοχή τους στην Κοινή Κυβερνομονάδα, τόσο οι επιχειρησιακοί συμμετέχοντες όσο και οι συμμετέχοντες υποστήριξης θα πρέπει να είναι σε θέση να συνεργάζονται με ευρύτερο φάσμα ενδιαφερομένων εντός του πλαισίου της ΕΕ για την αντιμετώπιση κρίσεων κυβερνοασφάλειας. Κατά την άσκηση των καθηκόντων τους μέσα στα όρια των εντολών τους, οι συμμετέχοντες θα πρέπει να επωφελούνται από ενισχυμένη ετοιμότητα και ευρύτερη αντίληψη της κατάστασης καλύπτοντας όλες τις πτυχές που σχετίζονται με κυβερνοαπειλές και κυβερνοπεριστατικά, και να αξιοποιούν πρόσθετη εμπειρογνωσία στον τομέα της κυβερνοασφάλειας. Για παράδειγμα, οι συμμετέχοντες θα πρέπει να συμμετέχουν τακτικά σε διακοινοτικές ασκήσεις, να αποκτούν σαφώς καθορισμένο ρόλο στο σχέδιο αντιμετώπισης κρίσεων της ΕΕ, να ενισχύουν την προβολή των δράσεών τους μέσω κοινής δημόσιας επικοινωνίας, και να συνάπτουν συμφωνίες επιχειρησιακής συνεργασίας με τον ιδιωτικό τομέα. Παράλληλα, με τη συμβολή τους στην Κοινή Κυβερνομονάδα οι συμμετέχοντες θα πρέπει να είναι σε θέση να ενισχύουν τα υφιστάμενα δίκτυα, όπως το CSIRT και το EU CyCLONe, να τους διαθέτουν ασφαλή εργαλεία ανταλλαγής πληροφοριών και μεγαλύτερες ικανότητες εντοπισμού (π.χ. κέντρα επιχειρήσεων ασφαλείας, «SOC») και να έχουν τη δυνατότητα να αξιοποιούν τις διαθέσιμες επιχειρησιακές ικανότητες της ΕΕ.

(12) Οι συμμετέχοντες στην Κοινή Κυβερνομονάδα θα πρέπει να επικεντρώνονται στην τεχνική και επιχειρησιακή συνεργασία, όπως σε κοινές επιχειρήσεις. Οι συμμετέχοντες θα πρέπει να συμβάλλουν στην εν λόγω συνεργασία στον βαθμό που το επιτρέπουν οι εντολές τους. Η συνεργασία θα πρέπει να βασίζεται στις προσπάθειες που ήδη καταβάλλονται και να τις συμπληρώνει. Ανάλογα με το είδος της συνεργασίας, μπορούν να προστίθενται και άλλοι συμμετέχοντες.

([12]) Αφορά και τη δικαστική συνεργασία.

([13]) Βλ. υποσημείωση (5). Η ΕΥΕΔ και ο ΕΟΑ, μέσω του ρόλου τους ως γραμματείας της PESCO, θα λειτουργούν ως σύνδεσμοι με τους συντονιστές των σχετικών έργων PESCO.

(13) Η πλατφόρμα θα πρέπει να συγκεντρώνει τεχνικούς και επιχειρησιακούς εμπειρογνώμονες διαχείρισης κρίσεων από τα κράτη μέλη και τις οντότητες της ΕΕ με σκοπό τον συντονισμό των αντιδράσεων σε απειλές, περιστατικά και κρίσεις στον κυβερνοχώρο, αξιοποιώντας τις υφιστάμενες ικανότητες και την υφιστάμενη εμπειρογνωμοσύνη. Οι εμπειρογνώμονες που συμμετέχουν στην Κοινή Κυβερνομονάδα θα είναι σε θέση να παρακολουθούν και να προστατεύουν μια πολύ ευρύτερη επιφάνεια έκθεσης σε πιθανές επιθέσεις χρησιμοποιώντας τόσο τη φυσική όσο και την εικονική πλατφόρμα. Για τον σκοπό αυτό, οι συμμετέχοντες θα πρέπει να συντονίζουν τις προσπάθειες σε περίπτωση διασυνοριακών περιστατικών και κρίσεων, καθώς και την παροχή βοήθειας στις πληγείσες χώρες μέσω της πλατφόρμας.

(14) Η δημιουργία της Κοινής Κυβερνομονάδας απαιτεί αφενός μεν σταδιακή διαδικασία αξιοποίησης και εδραίωσης των υφιστάμενων πλαισίων και δομών που αναφέρονται στην παρούσα σύσταση, όπως των μηχανισμών συνεργασίας που έχουν θεσπιστεί στο πλαίσιο φόρουμ υπό την καθοδήγηση των κρατών μελών (π.χ. τα δίκτυα CSIRT και EU CyCLONe, η οριζόντια ομάδα εργασίας του Συμβουλίου για θέματα κυβερνοχώρου, η J-CAT και τα σχετικά έργα PESCO), από την πλευρά των θεσμικών και λοιπών οργάνων και των οργανισμών της ΕΕ, στο πλαίσιο της διαρθρωμένης συνεργασίας ανάμεσα στον ENISA και στην CERT-ΕΕ, καθώς και στη διοργανική ομάδα ανταλλαγής πληροφοριών για την κυβερνοασφάλεια. Επιπλέον, θα πρέπει να συμμετέχουν επαρκώς τα πλαίσια υβριδικών απειλών, πολιτικής προστασίας ([14]) και τα τομεακά πλαίσια ([15]). Ομοίως, θα πρέπει να δημιουργηθεί διαρθρωμένη σύνδεση με τις IPCR ([16]). Αυτό θα καθιστά δυνατή, σε περίπτωση κρίσης, την ταχεία και αποτελεσματική διαβίβαση πληροφοριών στους φορείς λήψης αποφάσεων σε πολιτικό επίπεδο, που συγκεντρώνονται στο Συμβούλιο.

(15) Ως εκ τούτου, η δημιουργία της Κοινής Κυβερνομονάδας θα πρέπει να ακολουθήσει μια σταδιακή και διαφανή διαδικασία που θα ολοκληρωθεί κατά την επόμενη διετία. Για τον λόγο αυτόν, οι στόχοι που καθορίζονται στην παρούσα σύσταση θα πρέπει να επιτευχθούν μέσω μιας διαδικασίας τεσσάρων σταδίων, όπως περιγράφεται στο παράρτημα της παρούσας σύστασης. Μια προπαρασκευαστική διαδικασία, οργανωμένη και υποστηριζόμενη από τον ENISA, με επιχειρησιακούς συμμετέχοντες και συμμετέχοντες υποστήριξης σε επίπεδο ΕΕ και κρατών μελών, θα πρέπει να δρομολογηθεί στα δύο πρώτα στάδια και να πραγματοποιηθεί στο πλαίσιο ομάδας εργασίας που θα συσταθεί από την Επιτροπή. Οι προπαρασκευαστικές εργασίες θα πρέπει να διέπονται από τις αρχές της αμοιβαίας δέσμευσης, της συμπεριληπτικότητας και της επίτευξης συναίνεσης. Θα πρέπει να ενισχυθεί η εμπλοκή όλων των συμμετεχόντων ώστε να καθίσταται δυνατή η έκφραση διαφορετικών απόψεων και θέσεων, και να επιδιώκεται η εξεύρεση λύσεων που τυγχάνουν της ευρύτερης δυνατής στήριξης. Το χρονοδιάγραμμα για τα διάφορα στάδια που αναφέρονται στην παρούσα σύσταση μπορεί να προσαρμόζεται ανάλογα με τις ανάγκες και με βάση δεόντως αιτιολογημένες προϋποθέσεις.

(16) Στο πρώτο στάδιο, η προπαρασκευαστική διαδικασία θα πρέπει να ξεκινήσει με τον προσδιορισμό των σχετικών διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ και την έναρξη αξιολόγησης των ρόλων και των αρμοδιοτήτων των συμμετεχόντων στο πλαίσιο της πλατφόρμας. Το δεύτερο στάδιο θα πρέπει να περιλαμβάνει την ανάπτυξη του σχεδίου της ΕΕ για την αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας, που συνάδει με το προσχέδιο ([17]) και με το πρωτόκολλο της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου, την ανάπτυξη δραστηριοτήτων που σχετίζονται με την ετοιμότητα και την αντίληψη της κατάστασης, που συνάδει με την πράξη για την κυβερνοασφάλεια και με τον κανονισμό Ευρωπόλ ([18]), καθώς και την ολοκλήρωση της αξιολόγησης σχετικά με τους ρόλους και τις αρμοδιότητες των συμμετεχόντων εντός της πλατφόρμας. Η ομάδα εργασίας θα πρέπει να υποβάλει τα αποτελέσματα της εν λόγω αξιολόγησης στην Επιτροπή και στον ύπατο εκπρόσωπο, οι οποίοι στη συνέχεια θα κοινοποιήσουν τα αποτελέσματα αυτά στο Συμβούλιο. Η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει να συνεργαστούν, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, για την εκπόνηση κοινής έκθεσης με βάση την εν λόγω αξιολόγηση και να καλέσουν το Συμβούλιο να εγκρίνει την έκθεση αυτή μέσω συμπερασμάτων του Συμβουλίου.

(17) Μετά την έγκριση αυτή, η Κοινή Κυβερνομονάδα θα καταστεί επιχειρησιακή, με σκοπό την ολοκλήρωση των δύο υπόλοιπων σταδίων της διαδικασίας. Στο τρίτο στάδιο, οι συμμετέχοντες θα πρέπει να είναι σε θέση να αναπτύσσουν ομάδες ταχείας αντίδρασης της ΕΕ στο πλαίσιο της Κοινής Κυβερνομονάδας, σύμφωνα με τις διαδικασίες που ορίζονται στο σχέδιο της ΕΕ για την αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας, αξιοποιώντας τόσο τη φυσική όσο και την εικονική πλατφόρμα και συμβάλλοντας σε διάφορες πτυχές της αντιμετώπισης περιστατικών (από τη δημόσια επικοινωνία έως την εκ των υστέρων αποκατάσταση). Τέλος, στο τέταρτο στάδιο, ενδιαφερόμενοι φορείς του ιδιωτικού τομέα, τόσο χρήστες όσο και πάροχοι λύσεων και υπηρεσιών κυβερνοασφάλειας, θα κληθούν να συνεισφέρουν στην πλατφόρμα, δίνοντας στους συμμετέχοντες τη δυνατότητα να βελτιώσουν την ανταλλαγή πληροφοριών και να ενισχύσουν τη συντονισμένη αντίδραση της ΕΕ σε κυβερνοαπειλές και περιστατικά.

([14]) Στο πλαίσιο αυτό, η Κοινή Κυβερνομονάδα θα πρέπει να δημιουργήσει συνέργειες με τον μηχανισμό πολιτικής προστασίας της ΕΕ ώστε να ενισχυθεί η ευρωπαϊκή ετοιμότητα και αντίδραση σε περιπτώσεις πολλαπλών καταστροφών και καταστάσεων έκτακτης ανάγκης που περιλαμβάνουν ένα κυβερνοστοιχείο.

([15]) Όπως το σχετικό με τον χρηματοπιστωτικό τομέα, που προβλέπεται στον κανονισμό (ΕΕ) 2021/xx του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου* [DORA].

([16]) Βλ. αιτιολογική σκέψη 5.

([17]) Βλέπε υποσημείωση 3.

([18]) Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπόλ) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ (ΕΕ L 135 της 24.5.2016, σ. 53).

(18) Στο τέλος της διαδικασίας των τεσσάρων σταδίων, οι συμμετέχοντες θα πρέπει να συντάξουν έκθεση δραστηριοτήτων σχετικά με την πρόοδο που έχει σημειωθεί στην εφαρμογή των τεσσάρων σταδίων που προβλέπονται στη σύσταση, στην οποία θα περιγράφονται τα επιτεύγματα και οι προκλήσεις που αντιμετώπισαν, και η οποία θα πρέπει να υποβληθεί στην Επιτροπή και στον ύπατη εκπρόσωπο. Με βάση την έκθεση αυτή, η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει να προβούν σε αξιολόγηση των εν λόγω αποτελεσμάτων και σε εξαγωγή συμπερασμάτων για το μέλλον της Κοινής Κυβερνομονάδας.

(19) Η Επιτροπή, ο ENISA, ο Ευρωπόλ και η CERT-EU θα πρέπει να παρέχουν διοικητική, οικονομική και τεχνική υποστήριξη στην Κοινή Κυβερνομονάδα, όπως ορίζεται στο τμήμα IV της παρούσας σύστασης, με την επιφύλαξη της διαθεσιμότητας προϋπολογισμού και ανθρώπινων πόρων. Η ενίσχυση των επιχειρησιακών ικανοτήτων των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ στον τομέα της κυβερνοασφάλειας θα είναι καίριας σημασίας για την εξασφάλιση της αποτελεσματικής προετοιμασίας και βιωσιμότητας της Κοινής Κυβερνομονάδας. Η Επιτροπή προτίθεται να διασφαλίσει ότι ο επικείμενος κανονισμός σχετικά με κοινούς δεσμευτικούς κανόνες κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ (Οκτώβριος 2021) θα παράσχει τη νομική βάση για την εν λόγω συνεισφορά στην περίπτωση της CERT-EU.

(20) Λαμβανομένης υπόψη της ενισχυμένης εντολής του δυνάμει του κανονισμού (ΕΕ) 2019/881 («πράξη για την κυβερνοασφάλεια»), ο ENISA βρίσκεται σε μοναδική θέση για να οργανώσει και να στηρίξει την προετοιμασία της Κοινής Κυβερνομονάδας, καθώς και για να συμβάλει στην έναρξη λειτουργίας της. Σύμφωνα με τις διατάξεις της πράξης για την κυβερνοασφάλεια, ο ENISA ιδρύει επί του παρόντος γραφείο στις Βρυξέλλες για την υποστήριξη της διαρθρωμένης συνεργασίας του με την CERT-EU. Η εν λόγω διαρθρωμένη συνεργασία, συμπεριλαμβανομένων των παρακείμενων γραφείων, παρέχει χρήσιμο πλαίσιο που διευκολύνει τη δημιουργία της Κοινής Κυβερνομονάδας, όπως και τη δημιουργία του φυσικού χώρου ο οποίος θα πρέπει να διατίθεται στους συμμετέχοντες σε περίπτωση ανάγκης, καθώς και στο προσωπικό άλλων σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. Η φυσική πλατφόρμα θα πρέπει να συνδυάζεται με εικονική πλατφόρμα αποτελούμενη από εργαλεία συνεργασίας και ασφαλούς ανταλλαγής πληροφοριών. Τα εργαλεία αυτά θα αξιοποιούν την πληθώρα των πληροφοριών που συλλέγονται μέσω της ευρωπαϊκής κυβερνοασπίδας ([19]), όπως και μέσω των κέντρων επιχειρήσεων ασφάλειας («SOC») και των κέντρων ανταλλαγής και ανάλυσης πληροφοριών («ISAC»).

(21) Το πρωτόκολλο της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου για μείζονες διασυνοριακές κυβερνοεπιθέσεις, το οποίο εγκρίθηκε από το Συμβούλιο το 2018, αναθέτει κεντρικό ρόλο στο Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο («EC3») της Ευρωπόλ ([20]) που εντάσσεται στο πλαίσιο του «προσχεδίου». Το εν λόγω πρωτόκολλο επιτρέπει στις αρχές επιβολής του νόμου της ΕΕ να αντιδρούν, καθημερινά και καθ' όλο το εικοσιτετράωρο, σε μεγάλης κλίμακας διασυνοριακές επιθέσεις εικαζόμενης κακόβουλης φύσης μέσω ταχείας αντίδρασης και αξιολόγησης, καθώς και την ασφαλή και έγκαιρη ανταλλαγή κρίσιμων πληροφοριών για τον αποτελεσματικό συντονισμό των αντιδράσεων σε διασυνοριακά περιστατικά. Το πρωτόκολλο αναπτύσσει περαιτέρω τη συνεργασία με άλλα θεσμικά όργανα της ΕΕ και πρωτόκολλα κρίσης σε επίπεδο ΕΕ, καθώς και τη συνεργασία με τον ιδιωτικό τομέα σε καταστάσεις κρίσης. Η κοινότητα επιβολής του νόμου, με την υποστήριξη της Ευρωπόλ όποτε κρίνεται σκόπιμο, θα πρέπει να συμβάλλει στην Κοινή Κυβερνομονάδα λαμβάνοντας τα αναγκαία μέτρα στο πλαίσιο του πλήρους κύκλου έρευνας, σύμφωνα με τις απαιτήσεις του πλαισίου ποινικής δικαιοσύνης και με τις ισχύουσες διαδικασίες χειρισμού ηλεκτρονικών αποδεικτικών στοιχείων. Η Ευρωπόλ παρέχει επιχειρησιακή υποστήριξη και διευκολύνει την επιχειρησιακή συνεργασία κατά των κυβερνοαπειλών από την έναρξη λειτουργίας του EC3 το 2013. Η Ευρωπόλ θα πρέπει να στηρίζει την πλατφόρμα σύμφωνα με την εντολή της και με την προσέγγιση αστυνόμευσης βάσει εμπιστευτικών πληροφοριών, αξιοποιώντας παράλληλα κάθε είδους εσωτερική εμπειρογνωμοσύνη, προϊόντα, εργαλεία και υπηρεσίες που σχετίζονται με την αντιμετώπιση περιστατικών ή κρίσεων.

(22) Η οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών απαιτεί επίσης από τα κράτη μέλη να εξασφαλίζουν ότι διαθέτουν ένα επιχειρησιακό εθνικό σημείο επαφής διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας για τους σκοπούς της ανταλλαγής πληροφοριών σχετικά με τα αδικήματα που ορίζονται στην εν λόγω οδηγία. Το δίκτυο των επιχειρησιακών εθνικών σημείων επαφής θα πρέπει επίσης να συμβάλλει στην Κοινή Κυβερνομονάδα, διασφαλίζοντας τη συμμετοχή των αρχών επιβολής του νόμου των κρατών μελών, κατά περίπτωση.

(23) Η κοινότητα της κυβερνοδιπλωματίας της ΕΕ συμβάλλει στην προώθηση και την προστασία ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου και στην πρόληψη, την αποτροπή και την αντιμετώπιση κακόβουλων κυβερνοδραστηριοτήτων στο πλαίσιο αυτό. Το 2017, η ΕΕ θέσπισε πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη κυβερνοδιπλωματίας»). Το πλαίσιο αυτό εντάσσεται στην ευρύτερη πολιτική στον τομέα της κυβερνοδιπλωματίας της ΕΕ. Συμβάλλει στην πρόληψη των συγκρούσεων και στη μεγαλύτερη σταθερότητα των διεθνών σχέσεων. Δίνει τη δυνατότητα στην ΕΕ και στα κράτη μέλη, σε συνεργασία με διεθνείς εταίρους κατά περίπτωση, να χρησιμοποιούν όλα τα μέτρα της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας («ΚΕΠΠΑ»), σύμφωνα με τις αντίστοιχες διαδικασίες για την επίτευξή τους, για να ενθαρρύνουν τη συνεργασία, να μετριάζουν τις απειλές και να επηρεάζουν την τρέχουσα και ενδεχόμενη κακόβουλη συμπεριφορά στον κυβερνοχώρο. Η κοινότητα της κυβερνοδιπλωματίας θα πρέπει να συνεργάζεται στο πλαίσιο της Κοινής Κυβερνομονάδας χρησιμοποιώντας και παρέχοντας στήριξη για τη χρήση ολόκληρου του φάσματος των διπλωματικών μέτρων, ιδίως όσον αφορά την κοινή επικοινωνία, υποστηρίζοντας την κοινή αντίληψη της κατάστασης και τη συνεργασία με τρίτες χώρες σε περίπτωση κρίσης.

([19]) JOIN/2020/18 τελικό, τμήμα 1.2.

([20]) Θεσπίστηκε με τον κανονισμό (ΕΕ) 2016/794 .

(24) Σύμφωνα με το πλαίσιο του προσχεδίου, ο ύπατος εκπρόσωπος θα πρέπει να συμβάλει στη δράση της Κοινής Κυβερνομονάδας, μεταξύ άλλων μέσω του INTCEN, παρέχοντας συνεχή και κοινή επίγνωση της κατάστασης βάσει πληροφοριών σχετικά με υφιστάμενες και αναδυόμενες απειλές, συμπεριλαμβανομένης της απαραίτητης στρατηγικής επίγνωσης της κατάστασης για κάθε δεδομένο συμβάν.

(25) Στο πλαίσιο της κοινότητας κυβερνοάμυνας, η ΕΕ και τα κράτη μέλη επιδιώκουν να ενδυναμώσουν τις ικανότητες κυβερνοάμυνας και να ενισχύσουν περαιτέρω τις συνέργειες, τον συντονισμό και τη συνεργασία μεταξύ των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, καθώς και με τα κράτη μέλη και μεταξύ αυτών, μεταξύ άλλων όσον αφορά τις αποστολές και τις επιχειρήσεις της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ). Η κοινότητα λειτουργεί βάσει διακυβερνητικής διαχείρισης σε επίπεδο ΕΕ, εθνικών στρατιωτικών δομών διοίκησης και στρατιωτικών ικανοτήτων και μέσων ή ικανοτήτων και μέσων διπλής χρήσης. Δεδομένης της διαφορετικής φύσης της Κοινής Κυβερνομονάδας, θα πρέπει να δημιουργηθούν ειδικές διεπαφές με αυτήν, ώστε να καταστεί δυνατή η ανταλλαγή πληροφοριών με την κοινότητα κυβερνοάμυνας ([21]).

(26) Η μόνιμη διαρθρωμένη συνεργασία είναι ένα νομικό πλαίσιο το οποίο εισήχθηκε με τη Συνθήκη της Λισαβόνας ([22]) και θεσπίστηκε το 2017 στο πλαίσιο της Ένωσης. Η διαρθρωμένη συνεργασία οδήγησε στη θέσπιση μιας σειράς έργων PESCO στον κυβερνοχώρο, συμβάλλοντας στην εκπλήρωση της δέσμευσης 11 ([23]) περί «καταβολής αυξανόμενων προσπαθειών στον τομέα της συνεργασίας για την άμυνα στον κυβερνοχώρο, λ.χ. στην ανταλλαγή πληροφοριών, την κατάρτιση και την επιχειρησιακή στήριξη». Η ΕΥΕΔ, συμπεριλαμβανομένων του Στρατιωτικού Επιτελείου της ΕΕ και του ΕΟΑ, αποτελεί τη γραμματεία της PESCO, η οποία παρέχει ένα ενιαίο σημείο επαφής εντός του πλαισίου της Ένωσης για όλα τα ζητήματα που αφορούν την PESCO, συμπεριλαμβανομένων των υποστηρικτικών και συντονιστικών λειτουργιών που σχετίζονται με τα έργα PESCO (π.χ. αξιολόγηση νέων προτάσεων έργων, προετοιμασία των εκθέσεων προόδου των έργων κ.λπ.). Οι εκπρόσωποι των σχετικών έργων PESCO θα πρέπει να υποστηρίζουν την Κοινή Κυβερνομονάδα, ιδίως όσον αφορά την επίγνωση της κατάστασης και την ετοιμότητα.

(27) Μέσω της Κοινής Κυβερνομονάδας, οι συμμετέχοντες θα πρέπει να διασφαλίζουν την επαρκή ένταξη των ενδιαφερόμενων φορέων του ιδιωτικού τομέα, συμπεριλαμβανομένων τόσο των παρόχων όσο και των χρηστών λύσεων και υπηρεσιών κυβερνοασφάλειας, με σκοπό τη στήριξη του ευρωπαϊκού πλαισίου για τη διαχείριση κρίσεων κυβερνοασφάλειας, λαμβανομένου δεόντως υπόψη του νομικού πλαισίου για την ανταλλαγή δεδομένων και την ασφάλεια των πληροφοριών. Οι πάροχοι κυβερνοασφάλειας θα πρέπει να συνεισφέρουν στην πρωτοβουλία, κοινοποιώντας πληροφορίες σχετικά με απειλές και παρέχοντας προσωπικό αντιμετώπισης περιστατικών το οποίο θα διευρύνει ταχέως την ικανότητα της μονάδας να ανταποκρίνεται σε επιθέσεις και κρίσεις μεγάλης κλίμακας. Οι χρήστες προϊόντων και υπηρεσιών κυβερνοασφάλειας, κυρίως εκείνοι που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS, θα πρέπει να είναι σε θέση να αναζητούν βοήθεια και συμβουλές μέσω —ελλειπόντων επί του παρόντος— διαρθρωμένων διαύλων που συνδέονται με τα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) σε επίπεδο ΕΕ ([24]). Η πλατφόρμα θα μπορούσε επίσης να συμβάλει στην ενίσχυση της συνεργασίας με διεθνείς εταίρους.

(28) Η ανάπτυξη και η διατήρηση της επίγνωσης της κατάστασης απαιτούν πρωτοποριακές ικανότητες ανίχνευσης και πρόληψης εισβολών. Η Κοινή Κυβερνομονάδα θα πρέπει να βασίζεται σε ένα υπερσύγχρονο δίκτυο το οποίο θα είναι σε θέση να αναλύει κακόβουλες απειλές και περιστατικά που ενδέχεται να επηρεάσουν βασικά συστήματα επικοινωνίας και πληροφοριών της Ένωσης. Αυτό σημαίνει ότι οι γνώσεις σχετικά με απειλές, οι οποίες εξάγονται, μεταξύ άλλων πηγών, από δίκτυα επικοινωνιών που παρακολουθούνται από εθνικά, τομεακά και διασυνοριακά SOC, θα πρέπει να τροφοδοτούν την Κοινή Κυβερνομονάδα με σκοπό τη βελτίωση της αξιολόγησης του τοπίου των απειλών στην ΕΕ από τους συμμετέχοντες.

(29) Προκειμένου να υποστηριχθεί η ανταλλαγή επιχειρησιακών πληροφοριών, συμπεριλαμβανομένου ενδεχομένως εμπιστευτικού υλικού, η πλατφόρμα θα πρέπει να βασίζεται σε επαρκώς ασφαλείς διαύλους επικοινωνίας. Οι δίαυλοι αυτοί θα μπορούσαν επίσης να βασιστούν σε υφιστάμενες υποδομές, όπως η εφαρμογή δικτύου ασφαλούς ανταλλαγής πληροφοριών (SIENA) που χρησιμοποιείται από την Ευρωπόλ και την κοινότητα επιβολής του νόμου. Όπως ανακοινώθηκε στο πλαίσιο της στρατηγικής κυβερνοασφάλειας, τα εργαλεία που χρησιμοποιούνται από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ θα πρέπει να τηρούν τους κανόνες σχετικά με την ασφάλεια των πληροφοριών που θα προτείνει σύντομα η Επιτροπή.

([21]) Ιδίως μέσω εκπροσώπησης της ΕΥΕΔ, προκειμένου να καταστεί δυνατή η κατάλληλη συμμετοχή της κοινότητας κυβερνοάμυνας, η οποία βασίζεται στις εθελοντικές εθνικές συνεισφορές.

([22]) Άρθρο 42 παράγραφος 6, άρθρο 46 και πρωτόκολλο 10 της ΣΕΕ

([23]) Κάθε κράτος μέλος που συμμετέχει στην PESCO αναλαμβάνει 20 επιμέρους δεσμεύσεις, οι οποίες κατανέμονται στους πέντε βασικούς τομείς που ορίζονται στο άρθρο 2 του πρωτοκόλλου αριθ. 10 σχετικά με την PESCO, το οποίο προσαρτάται στη Συνθήκη για την Ευρωπαϊκή Ένωση.

([24]) Αξιοσημείωτα παραδείγματα υφιστάμενων ISAC που θα μπορούσαν να συμμετέχουν στην εν λόγω ανταλλαγή είναι το ISAC για την Ενέργεια (EE-ISAC) ή το ISAC για τα Ευρωπαϊκά Χρηματοπιστωτικά Ιδρύματα (FI-ISAC).

(30) Η Επιτροπή, κυρίως μέσω του προγράμματος «Ψηφιακή Ευρώπη», θα στηρίξει τις αναγκαίες επενδύσεις για τη δημιουργία της φυσικής και ψηφιακής πλατφόρμας και για τη δημιουργία και τη διατήρηση ασφαλών διαύλων επικοινωνίας και δυνατοτήτων κατάρτισης, καθώς και για την ανάπτυξη και τη χρησιμοποίηση ικανοτήτων ανίχνευσης. Επιπλέον, το Ευρωπαϊκό Ταμείο Άμυνας θα μπορούσε να συμβάλει στη χρηματοδότηση βασικών τεχνολογιών κυβερνοάμυνας και ικανοτήτων κυβερνοάμυνας που θα ενίσχυαν την εθνική ετοιμότητα στον τομέα της κυβερνοάμυνας,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

I. **ΣΚΟΠΟΣ ΤΗΣ ΣΥΣΤΑΣΗΣ**

1) Σκοπός της παρούσας σύστασης είναι να προσδιοριστούν οι δράσεις που απαιτούνται για τον συντονισμό των προσπαθειών της ΕΕ για την πρόληψη, τον εντοπισμό, την αποθάρρυνση, τον μετριασμό και την αντιμετώπιση κυβερνοπεριστατικών και κυβερνοκρίσεων μεγάλης κλίμακας μέσω μιας Κοινής Κυβερνομονάδας. Για τον σκοπό αυτό, η παρούσα σύσταση καθορίζει επίσης τη διαδικασία, τα ορόσημα και το χρονοδιάγραμμα που θα πρέπει να επιδιώξουν τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ σε σχέση με τη δημιουργία και την ανάπτυξη της εν λόγω πλατφόρμας.

2) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διασφαλίζουν ότι, σε περιπτώσεις κυβερνοσυμβάντων και κυβερνοκρίσεων μεγάλης κλίμακας, συντονίζουν τις προσπάθειές τους μέσω μιας Κοινής Κυβερνομονάδας, η οποία παρέχει τη δυνατότητα αμοιβαίας συνδρομής ([25]) με βάση την εμπειρογνωσία των αρχών των κρατών μελών και των σχετικών θεσμικών και λοιπών οργάνων και των οργανισμών της ΕΕ. Η Κοινή Κυβερνομονάδα θα πρέπει επίσης να επιτρέπει στους συμμετέχοντες να συνεργάζονται με τον ιδιωτικό τομέα.

II. **ΟΡΙΣΜΟΙ**

3) Για τους σκοπούς της παρούσας σύστασης:

α) «ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας»: σύνολο ρόλων, μέσων και διαδικασιών που οδηγούν στην ολοκλήρωση του ενωσιακού πλαισίου αντιμετώπισης κρίσεων κυβερνοασφάλειας το οποίο περιγράφεται στο σημείο 1) της σύστασης της Επιτροπής της 13ης Σεπτεμβρίου 2017 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο («προσχέδιο»).

β) «κοινότητες κυβερνοασφάλειας»: συνεργατικές μη στρατιωτικές ομάδες, ομάδες επιβολής του νόμου, διπλωματικές ομάδες και αμυντικές ομάδες οι οποίες εκπροσωπούν τόσο τα κράτη μέλη όσο και τα σχετικά θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ και ανταλλάσσουν πληροφορίες επιδιώκοντας κοινούς στόχους, συμφέροντα και αποστολές σε σχέση με την κυβερνοασφάλεια.

γ) «συμμετέχοντες του ιδιωτικού τομέα»: εκπρόσωποι οντοτήτων του ιδιωτικού τομέα που παρέχουν ή χρησιμοποιούν λύσεις ([26]) και υπηρεσίες ([27]) κυβερνοασφάλειας.

δ) «περιστατικό μεγάλης κλίμακας»: περιστατικό (συμβάν) όπως ορίζεται στο άρθρο 4 σημείο 7 της οδηγίας (ΕΕ) 2016/1148 με σημαντικό αντίκτυπο σε τουλάχιστον δύο κράτη μέλη.

ε) «ολοκληρωμένη έκθεση για την κατάσταση της κυβερνοασφάλειας στην ΕΕ»: έκθεση στην οποία συγκεντρώνονται στοιχεία από τους συμμετέχοντες στην Κοινή Κυβερνομονάδα και η οποία βασίζεται στην τεχνική έκθεση για την κατάσταση της κυβερνοασφάλειας στην ΕΕ που ορίζεται στο άρθρο 7 παράγραφος 6 του κανονισμού (ΕΕ) 2019/881.

στ) «ομάδα ταχείας αντίδρασης της ΕΕ για την κυβερνοασφάλεια»: ομάδα αποτελούμενη από αναγνωρισμένους εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας, προερχόμενους κυρίως από τις CSIRT των κρατών μελών, με τη στήριξη του ENISA, της CERT-EU και της Ευρωπόλ, η οποία είναι έτοιμη να συνδράμει εξ αποστάσεως τους συμμετέχοντες που πλήττονται από περιστατικά και κρίσεις μεγάλης κλίμακας.

ζ) «μνημόνια συμφωνίας»: συμφωνία μεταξύ των συμμετεχόντων στην οποία καθορίζονται οι αναγκαίες λεπτομέρειες συνεργασίας, συμπεριλαμβανομένου του ορισμού των μέσων και των διαδικασιών που απαιτούνται για τη σύσταση και την κινητοποίηση των ομάδων ταχείας αντίδρασης της ΕΕ για την κυβερνοασφάλεια, καθώς και για την παροχή αμοιβαίας συνδρομής.

([25]) Κατά τρόπο συνεκτικό με την προσέγγιση και τις αρχές που αναφέρονται στην οδηγία (ΕΕ) 2016/1148 και στο άρθρο 222 (ΣΛΕΕ). Με την επιφύλαξη του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση.

([26]) Συμπεριλαμβανομένων των πωλητών λογισμικού.

([27]) Συμπεριλαμβανομένων των πληροφοριών σχετικά με απειλές.

III. **ΣΤΟΧΟΣ ΤΗΣ ΚΟΙΝΗΣ ΚΥΒΕΡΝΟΜΟΝΑΔΑΣ**

4) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διασφαλίζουν μια **συντονισμένη ενωσιακή αντιμετώπιση** και ανάκαμψη μετά από κυβερνοπεριστατικά και κυβερνοκρίσεις μεγάλης κλίμακας. Ειδικότερα, η αντιμετώπιση αυτή θα πρέπει να διασφαλίζεται μεταξύ των επιχειρησιακών συμμετεχόντων, ιδίως του ENISA, της Ευρωπόλ, της CERT-EU, της Επιτροπής, της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (συμπεριλαμβανομένου του INTCEN), του δικτύου CSIRT, του EU-CyCLONe, και των συμμετεχόντων υποστήριξης, ιδίως του/της προέδρου της ομάδας συνεργασίας NIS, του/της προέδρου της οριζόντιας ομάδας εργασίας του Συμβουλίου για θέματα κυβερνοχώρου, του Ευρωπαϊκού Οργανισμού Άμυνας και ενός/μίας εκπροσώπου των σχετικών έργων PESCO ([28]). Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να είναι σε θέση να κινητοποιούν γρήγορα και αποτελεσματικά επιχειρησιακούς πόρους για την αμοιβαία συνδρομή στο πλαίσιο της Κοινής Κυβερνομονάδας. Για τον σκοπό αυτό, στο πλαίσιο της Κοινής Κυβερνομονάδας, οι μηχανισμοί αμοιβαίας συνδρομής θα πρέπει να συντονίζονται κατόπιν αιτήματος ενός ή περισσότερων κρατών μελών.

5) Προκειμένου να παρέχεται αποτελεσματική συντονισμένη αντιμετώπιση, οι επιχειρησιακοί συμμετέχοντες και οι συμμετέχοντες υποστήριξης που απαριθμούνται στο σημείο 4) θα πρέπει να είναι σε θέση να ανταλλάσσουν βέλτιστες πρακτικές, να αξιοποιούν τη συνεχή **κοινή επίγνωση της κατάστασης** και να διασφαλίζουν την αναγκαία **ετοιμότητα**, στον βαθμό που το επιτρέπουν οι εντολές τους. Οι εν λόγω συμμετέχοντες θα πρέπει να λαμβάνουν υπόψη τις υφιστάμενες διαδικασίες και την εμπειρογνωσία των διαφόρων κοινοτήτων κυβερνοασφάλειας.

IV. **ΚΑΘΟΡΙΣΜΟΣ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΚΟΙΝΗΣ ΚΥΒΕΡΝΟΜΟΝΑΔΑΣ**

6) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει, με βάση τη συνεισφορά του ENISA σύμφωνα με το άρθρο 7 παράγραφος 7 του κανονισμού (ΕΕ) 2019/881, να εξασφαλίζουν τη **συντονισμένη αντιμετώπιση** και την ανάκαμψη μετά από περιστατικά και κρίσεις μεγάλης κλίμακας μέσα από:

α) Τη σύσταση, την κατάρτιση, τις δοκιμές και τη συντονισμένη ανάπτυξη **ομάδων κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ**, αξιοποιώντας στο έπακρο το άρθρο 7 παράγραφος 4 του κανονισμού (ΕΕ) 2019/881 και τα άρθρα 3 και 4 του κανονισμού (ΕΕ) 2016/794·

β) Τη συντονισμένη χρήση μιας **εικονικής και φυσικής πλατφόρμας**, αξιοποιώντας στο έπακρο τη διαρθρωμένη συνεργασία μεταξύ ENISA και CERT-EU που κατοχυρώνεται στο άρθρο 7 παράγραφος 4 του κανονισμού 2019/881, η οποία θα πρέπει να χρησιμεύει ως υποστηρικτική υποδομή για την τεχνική και επιχειρησιακή συνεργασία μεταξύ των συμμετεχόντων και για τη συγκέντρωση του σχετικού προσωπικού και άλλων πόρων από τους συμμετέχοντες·

γ) Τη δημιουργία και την τήρηση καταλόγου των **επιχειρησιακών και τεχνικών ικανοτήτων που είναι διαθέσιμες στην ΕΕ**, σε όλες τις κοινότητες κυβερνοασφάλειας ([29]) της Ένωσης, οι οποίες είναι έτοιμες για ανάπτυξη σε περίπτωση περιστατικών ή κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας.

Δ) Την υποβολή εκθέσεων στην Επιτροπή και τον ύπατο εκπρόσωπο σχετικά με την πείρα που αποκτάται από τις **δραστηριότητες επιχειρησιακής συνεργασίας στον τομέα της κυβερνοασφάλειας** εντός και μεταξύ των κοινοτήτων κυβερνοασφάλειας.

7) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διασφαλίζουν ότι η Κοινή Κυβερνομονάδα παρέχει συνεχή κοινή **επίγνωση των καταστάσεων** και **ετοιμότητα** έναντι κρίσεων που διευκολύνονται από τον κυβερνοχώρο, σε όλες τις κοινότητες κυβερνοασφάλειας, καθώς και εντός των εν λόγω κοινοτήτων, επιδιώκοντας τους στόχους που ορίζονται στο άρθρο 7 του κανονισμού (ΕΕ) 2019/881 και στο άρθρο 3 του κανονισμού (ΕΕ) 2016/794. Για τον σκοπό αυτό, τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει, σύμφωνα με τον κανονισμό (ΕΕ) 2019/881 και τον κανονισμό (ΕΕ) 2016/794, να καθιστούν δυνατή την υλοποίηση των ακόλουθων **υποστηρικτικών** δράσεων:

α) Την εκπόνηση της **ολοκληρωμένης έκθεσης για την κατάσταση της κυβερνοασφάλειας στην ΕΕ** με τη συλλογή και την ανάλυση όλων των σχετικών πληροφοριών και των πληροφοριών για απειλές·

β) Τη χρήση κατάλληλων και ασφαλών **εργαλείων**, σύμφωνα με το άρθρο 7 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881, για την ταχεία ανταλλαγή πληροφοριών μεταξύ των συμμετεχόντων και με άλλες οντότητες·

γ) Την **ανταλλαγή πληροφοριών και εμπειρογνωσίας** που απαιτούνται για την προετοιμασία της Ένωσης για τη διαχείριση περιστατικών και κρίσεων μεγάλης κλίμακας που διευκολύνονται από τον κυβερνοχώρο, με την υποστήριξη του ENISA, όπως ορίζεται στο άρθρο 7 παράγραφος 2 του κανονισμού (ΕΕ) 2019/881·

δ) Την έγκριση και τις δοκιμές των εθνικών **σχεδίων αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας** ([30]) σύμφωνα με το άρθρο 7 παράγραφοι 2, 5 και 7 του κανονισμού (ΕΕ) 2019/881·

([28]) «Συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών» (CIDCC) και «Ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο και αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο» (CRRT)

([29]) Συμπεριλαμβανομένης, κατά περίπτωση, της κοινότητας κυβερνοάμυνας.

([30]) Προτείνεται βάσει του άρθρου 7 παράγραφος 3 της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

ε) Την ανάπτυξη, τη διαχείριση και τις δοκιμές, μεταξύ άλλων μέσω διακοινοτικών ασκήσεων και κατάρτισης, **του ενωσιακού σχεδίου αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας**, σύμφωνα με τη σύσταση «προσχέδιο» και με βάση το άρθρο 7 παράγραφος 3 της πρότασης της Επιτροπής σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την αναθεώρηση της οδηγίας (ΕΕ) 2016/1148 ([31])·

στ) Τη συνδρομή των συμμετεχόντων στη σύναψη συμφωνιών ανταλλαγής πληροφοριών, καθώς και συμφωνιών επιχειρησιακής συνεργασίας με **οντότητες του ιδιωτικού τομέα** που παρέχουν, μεταξύ άλλων, υπηρεσίες πληροφοριών για απειλές και υπηρεσίες αντιμετώπισης περιστατικών, με την υποστήριξη του ENISA, όπως ορίζεται στο άρθρο 7 παράγραφος 1 του κανονισμού (ΕΕ) 2019/881·

ζ) Τη δημιουργία διαρθρωμένων συνεργειών με εθνικές, τομεακές και διασυνοριακές **ικανότητες παρακολούθησης και ανίχνευσης**, ιδίως με τα κέντρα επιχειρήσεων ασφάλειας·

η) Τη συνδρομή των συμμετεχόντων στη **διαχείριση** περιστατικών και κρίσεων μεγάλης κλίμακας, σύμφωνα με τον υποστηρικτικό ρόλο του ENISA, όπως ορίζεται στο άρθρο 7 του κανονισμού (ΕΕ) 2019/881. Στη συνδρομή αυτή περιλαμβάνονται, μεταξύ άλλων, η συμβολή στην κοινή επίγνωση των καταστάσεων, η στήριξη της διπλωματικής δράσης, ο καταλογισμός σε πολιτικό επίπεδο καθώς και σε επίπεδο ποινικών ερευνών, μεταξύ άλλων μέσω της Ευρωπόλ ([32]), ο συντονισμός της δημόσιας επικοινωνίας και η διευκόλυνση της ανάκαμψης μετά από περιστατικά.

8) Για την εφαρμογή των σημείων 6) και 7), τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διασφαλίζουν:

α) Τον καθορισμό των οργανωτικών πτυχών της Κοινής Κυβερνομονάδας και των **ρόλων και αρμοδιοτήτων** των επιχειρησιακών συμμετεχόντων και των συμμετεχόντων υποστήριξης στην πλατφόρμα, επιτρέποντας την αποτελεσματική λειτουργία της πλατφόρμας σύμφωνα με τις πτυχές και τις αρχές που προσδιορίζονται στο παράρτημα της παρούσας σύστασης·

β) Τη σύναψη **μνημονίων συνεννόησης**, στα οποία καθορίζονται οι αναγκαίες λεπτομέρειες της συνεργασίας μεταξύ των συμμετεχόντων που αναφέρονται στο σημείο 4).

9) Σύμφωνα με το άρθρο 7 του κανονισμού (ΕΕ) 2019/881, ο ENISA θα πρέπει να διασφαλίζει τον συντονισμό και την υποστήριξη των κρατών μελών και των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης που συμμετέχουν στην Κοινή Κυβερνομονάδα, παρέχοντας, μεταξύ άλλων, γραμματειακή υποστήριξη, διοργανώνοντας συνεδριάσεις και συμβάλλοντας στην υλοποίηση των δράσεων τόσο σε επίπεδο κρατών μελών όσο και σε επίπεδο ΕΕ. Ο ENISA θα πρέπει να δημιουργήσει τόσο μια ασφαλή εικονική πλατφόρμα όσο και ένα φυσικό χώρο για τη διοργάνωση συνεδριάσεων και θα πρέπει να διευκολύνει τις εκτελεστικές δράσεις.

V. **ΟΙΚΟΔΟΜΗΣΗ ΤΗΣ ΚΟΙΝΗΣ ΚΥΒΕΡΝΟΜΟΝΑΔΑΣ**

10) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να διασφαλίσουν ότι η Κοινή Κυβερνομονάδα θα εισέλθει στην επιχειρησιακή φάση στις **30 Ιουνίου 2022**. Έως τότε, οι επιχειρησιακοί συμμετέχοντες θα πρέπει να καταστήσουν διαθέσιμες/-ους τις επιχειρησιακές ικανότητες και τους εμπειρογνώμονες που μπορούν να αποτελέσουν τη βάση των ομάδων κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ. Τα σχέδια για τη φυσική και εικονική πλατφόρμα θα πρέπει να έχουν προχωρήσει ικανοποιητικά.

11) Τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να συμβάλλουν στη λειτουργία της Κοινής Κυβερνομονάδας και να διασφαλίσουν ότι η έναρξη της επιχειρησιακής της λειτουργίας θα έχει περατωθεί έως τις **30 Ιουνίου 2023**. Αυτή θα πρέπει να πραγματοποιηθεί σε τέσσερα στάδια, τα οποία θα αποσκοπούν στην ολοκλήρωση των ακόλουθων δραστηριοτήτων:

α) Στάδιο 1 — Αξιολόγηση των οργανωτικών πτυχών της Κοινής Κυβερνομονάδας και προσδιορισμός των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ έως τις **31 Δεκεμβρίου 2021**·

β) Στάδιο 2 — Εκπόνηση σχεδίων αντιμετώπισης περιστατικών και κρίσεων και ανάπτυξη κοινών δραστηριοτήτων ετοιμότητας έως τις **30 Ιουνίου 2022**·

γ. Στάδιο 3 — Έναρξη επιχειρησιακής λειτουργίας της Κοινής Κυβερνομονάδας έως τις **31 Δεκεμβρίου 2022**·

δ. Στάδιο 4 — Επέκταση της συνεργασίας στο πλαίσιο της Κοινής Κυβερνομονάδας σε οντότητες του ιδιωτικού τομέα και υποβολή εκθέσεων σχετικά με την πρόοδο που έχει σημειωθεί έως τις **30 Ιουνίου 2023**.

Οι λεπτομερέστερες δράσεις που θα πρέπει να αναληφθούν στο πλαίσιο των τεσσάρων διαδοχικών σταδίων περιγράφονται στο παράρτημα της παρούσας σύστασης.

([31]) COM(2020) 823 final

([32]) Σύμφωνα με τον κανονισμό (ΕΕ) 2016/794.

12) Στο πλαίσιο των δύο πρώτων σταδίων, ο ENISA θα πρέπει να οργανώσει και να στηρίξει την προετοιμασία της Κοινής Κυβερνομονάδας. Οι υπηρεσίες της Επιτροπής θα πρέπει να συστήσουν ομάδα εργασίας, στην οποία θα συμμετέχουν οι επιχειρησιακοί συμμετέχοντες και οι συμμετέχοντες υποστήριξης, προκειμένου να ολοκληρωθούν οι εν λόγω προπαρασκευαστικές εργασίες. Οι υπηρεσίες της Επιτροπής θα πρέπει να ορίσουν έναν εκπρόσωπο ως συμπρόεδρο της ομάδας εργασίας. Θα πρέπει επίσης να καλέσουν έναν εκπρόσωπο που θα διορίσει ο ύπατος εκπρόσωπος και έναν εκπρόσωπο που θα επιλέξουν τα κράτη μέλη να αναλάβουν χρέη συμπροέδρων. Ο συμπρόεδρος που εκπροσωπεί την Επιτροπή και ο συμπρόεδρος που διορίζει ο ύπατος εκπρόσωπος θα συμβάλλουν στα θέματα της ημερήσιας διάταξης σύμφωνα με τις αντίστοιχες αρμοδιότητές τους.

13) Έως το τέλος του δεύτερου σταδίου, η ομάδα εργασίας θα πρέπει να ολοκληρώσει την αξιολόγηση των οργανωτικών πτυχών της Κοινής Κυβερνομονάδας και των ρόλων και αρμοδιοτήτων των επιχειρησιακών συμμετεχόντων στην εν λόγω πλατφόρμα. Η ομάδα εργασίας θα πρέπει να υποβάλει τα αποτελέσματα της αξιολόγησης αυτής στην Επιτροπή και στον ύπατο εκπρόσωπο. Η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει στη συνέχεια να κοινοποιούν την αξιολόγηση αυτή στο Συμβούλιο. Η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει να συντάξουν κοινή έκθεση με βάση την αξιολόγηση αυτή και να καλέσουν το Συμβούλιο να εγκρίνει την έκθεση μέσω συμπερασμάτων του Συμβουλίου.

14) Η Κοινή Κυβερνομονάδα θα πρέπει να λειτουργεί από το τρίτο στάδιο.

15) Ο ENISA και η Επιτροπή θα πρέπει να διασφαλίσουν τη χρήση των υφιστάμενων πόρων στο πλαίσιο των χρηματοδοτικών προγραμμάτων της ΕΕ, κυρίως του προγράμματος «Ψηφιακή Ευρώπη», σύμφωνα με τους ισχύοντες κανόνες για την κατάρτιση των αντίστοιχων προγραμμάτων εργασίας, για τον εξοπλισμό των συμμετεχόντων στην Κοινή Κυβερνομονάδα με πρόσθετες ικανότητες κατάρτισης, ικανότητες επικοινωνίας και ασφαλείς υποδομές ανταλλαγής πληροφοριών που επιτρέπουν την ανταλλαγή διαβαθμισμένων πληροφοριών, μεταξύ άλλων και μεταξύ των κοινοτήτων.

VI. **ΕΠΑΝΕΞΕΤΑΣΗ**

16) Τα κράτη μέλη θα πρέπει να συνεργαστούν με την Επιτροπή και τον ύπατο εκπρόσωπο, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, για να αξιολογήσουν την αποτελεσματικότητα και την αποδοτικότητα της Κοινής Κυβερνομονάδας έως τις **30 Ιουνίου 2025**, με σκοπό την άντληση συμπερασμάτων για το μέλλον της Κοινής Κυβερνομονάδας. Στην αξιολόγηση αυτή θα πρέπει να ληφθεί υπόψη η εφαρμογή των τεσσάρων προαναφερθέντων σταδίων.

Βρυξέλλες, 23 Ιουνίου 2021.

Για την Επιτροπή
Thierry BRETON
Μέλος της Επιτροπής

ΠΑΡΑΡΤΗΜΑ

Στάδια για τη δημιουργία της Κοινής Κυβερνομονάδας

Το παρόν παράρτημα περιγράφει περαιτέρω τις βασικές και υποστηρικτικές δράσεις που απαιτούνται για τη σύσταση και την έναρξη επιχειρησιακής λειτουργίας της Κοινής Κυβερνομονάδας.

1. *Στάδιο 1 — Αξιολόγηση των οργανωτικών πτυχών της Κοινής Κυβερνομονάδας και προσδιορισμός των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ*

ΒΑΣΙΚΕΣ ΔΡΑΣΕΙΣ

Οι επιχειρησιακοί συμμετέχοντες στην Κοινή Κυβερνομονάδα, οι οποίοι συγκεντρώνονται στο πλαίσιο ομάδας εργασίας που συστάθηκε από την Επιτροπή και με την υποστήριξη του ENISA, θα πρέπει να συλλέγουν πληροφορίες σχετικά με τις υφιστάμενες επιχειρησιακές ικανότητες, συμπεριλαμβανομένου καταλόγου διαθέσιμων αναγνωρισμένων επαγγελματιών, με ένδειξη της σχετικής εμπειρογνωμοσύνης τους, των διαθέσιμων εργαλείων, λειτουργιών και στοιχείων χειρισμού περιστατικών, των διαθέσιμων χαρτοφυλακίων κατάρτισης και ασκήσεων, και των υφιστάμενων πληροφοριών και προϊόντων ανάλυσης πληροφοριών. Με βάση τα στοιχεία αυτά, οι επιχειρησιακοί συμμετέχοντες θα πρέπει να καταρτίσουν **κατάλογο των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ** που είναι έτοιμες να αναπτυχθούν σε περίπτωση κυβερνοπεριστατικών ή κυβερνοκρίσεων, ιδίως μέσω των ομάδων κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ.

Η ομάδα εργασίας θα πρέπει να δρομολογήσει αξιολόγηση των **οργανωτικών πτυχών** της Κοινής Κυβερνομονάδας **και των ρόλων και αρμοδιοτήτων των επιχειρησιακών συμμετεχόντων στην εν λόγω πλατφόρμα**.

Προκειμένου να αποκτηθεί επισκόπηση των ικανοτήτων και να συμφωνηθούν οι διαδικασίες, οι βασικές δράσεις και, στο μέτρο που είναι δυνατόν, οι υποστηρικτικές δράσεις στο πλαίσιο του πρώτου σταδίου θα πρέπει να ολοκληρωθούν έως τις **31 Δεκεμβρίου 2021 [6 μήνες μετά την έγκριση]**.

2. *Στάδιο 2 — Εκπόνηση σχεδίων αντιμετώπισης περιστατικών και κρίσεων και ανάπτυξη κοινών δραστηριοτήτων ετοιμότητας*

ΒΑΣΙΚΕΣ ΔΡΑΣΕΙΣ

Οι επιχειρησιακοί συμμετέχοντες στην ομάδα εργασίας, σε διαβούλευση με τους συμμετέχοντες υποστήριξης, θα πρέπει να εκπονήσουν το **ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας** με βάση τα εθνικά σχέδια αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας. Το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας θα πρέπει να περιλαμβάνει στόχους ετοιμότητας της ΕΕ, καθορισμένες διαδικασίες και ασφαλείς διαύλους ανταλλαγής πληροφοριών, συμπεριλαμβανομένων τρόπων χειρισμού των πληροφοριών, καθώς και κριτήρια για την ενεργοποίηση του μηχανισμού αμοιβαίας συνδρομής με βάση μια συμφωνημένη ταξινόμηση περιστατικών και τον κατάλογο των διαθέσιμων ικανοτήτων της ΕΕ.

Έως το τέλος του δεύτερου σταδίου, η ομάδα εργασίας θα πρέπει να ολοκληρώσει την αξιολόγηση των οργανωτικών πτυχών της Κοινής Κυβερνομονάδας και των ρόλων και αρμοδιοτήτων των επιχειρησιακών συμμετεχόντων στην εν λόγω πλατφόρμα. Η ομάδα εργασίας θα πρέπει να υποβάλει τα αποτελέσματα της αξιολόγησης αυτής στην Επιτροπή και στον ύπατο εκπρόσωπο. Η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει να κοινοποιήσουν την αξιολόγηση αυτή στο Συμβούλιο. Η Επιτροπή και ο ύπατος εκπρόσωπος θα πρέπει να συνεργαστούν, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, για να εκπονήσουν κοινή έκθεση με βάση την εν λόγω αξιολόγηση και να καλέσουν το Συμβούλιο να εγκρίνει την εν λόγω έκθεση μέσω συμπερασμάτων του Συμβουλίου.

ΥΠΟΣΤΗΡΙΚΤΙΚΕΣ ΔΡΑΣΕΙΣ

Το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας θα πρέπει να βασίζεται στα κύρια στοιχεία των εθνικών σχεδίων αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας. Σύμφωνα με την πρόταση οδηγίας της Επιτροπής σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, με την οποία καταργείται η οδηγία (ΕΕ) 2016/1148 ([1]), τα κράτη μέλη θα πρέπει να εγκρίνουν εθνικά σχέδια αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας. Τα εθνικά σχέδια, τα οποία ενδέχεται να υπόκεινται σε αξιολόγηση από ομοτίμους, θα πρέπει να καθορίζουν στόχους και λεπτομέρειες σχετικά με τη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων κυβερνοασφάλειας. Μεταξύ άλλων, τα εθνικά σχέδια θα πρέπει να εξετάζουν τα ακόλουθα ζητήματα:

α) τους στόχους των εθνικών μέτρων και δραστηριοτήτων ετοιμότητας·

β) τους ρόλους και τις αρμοδιότητες των εθνικών αρμόδιων αρχών σε εθνικό επίπεδο·

γ) τις διαδικασίες διαχείρισης κρίσεων και τους διαύλους ανταλλαγής πληροφοριών·

δ) τον προσδιορισμό μέτρων ετοιμότητας, συμπεριλαμβανομένων ασκήσεων και δραστηριοτήτων κατάρτισης·

ε) τον προσδιορισμό σχετικών δημόσιων και ιδιωτικών ενδιαφερόμενων φορέων και υποδομών·

στ) τις εθνικές διαδικασίες και ρυθμίσεις μεταξύ των αρμόδιων εθνικών αρχών και φορέων, συμπεριλαμβανομένων εκείνων που είναι αρμόδιες για όλες τις κυβερνοκοινότητες, ώστε να διασφαλίζεται η αποτελεσματική συμμετοχή και στήριξη των κρατών μελών στη συντονισμένη διαχείριση μεγάλης κλίμακας περιστατικών και κρίσεων κυβερνοασφάλειας σε επίπεδο ΕΕ.

Με βάση τη συμβολή των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, οι επιχειρησιακοί συμμετέχοντες θα πρέπει να εκτελούν τις ακόλουθες υποστηρικτικές δράσεις στο πλαίσιο της Κοινής Κυβερνομονάδας:

α) καθορισμός της πρώτης ολοκληρωμένης έκθεσης της ΕΕ για την κατάσταση με βάση τα εθνικά σχέδια αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας·

([1]) COM(2020) 823 final 2020/0359 (COD), Βρυξέλλες, 16.12.2020.

β) δημιουργία ικανοτήτων επικοινωνίας και ασφαλών εργαλείων ανταλλαγής πληροφοριών·

γ) διευκόλυνση της έγκρισης πρωτοκόλλων αμοιβαίας συνδρομής μεταξύ των συμμετεχόντων·

δ) οργάνωση διακοινοτικών ασκήσεων και προγραμμάτων κατάρτισης για εμπειρογνώμονες που περιλαμβάνονται στον κατάλογο των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ·

ε) εκπόνηση πολυετούς σχεδίου για τον συντονισμό των ασκήσεων.

Όταν χρειάζεται, οι επιχειρησιακοί συμμετέχοντες θα πρέπει να συμβουλεύονται τους συμμετέχοντες υποστήριξης. Ο ENISA, με την υποστήριξη της Επιτροπής, της Ευρωπόλ και της CERT-EU, θα πρέπει να καταστήσει δυνατή την ανταλλαγή πληροφοριών με τη δημιουργία ικανοτήτων επικοινωνίας και ασφαλών εργαλείων ανταλλαγής πληροφοριών.

Για να εξασφαλιστεί η κατάρτιση των αναγκαίων σχεδίων και η έναρξη εκτέλεσης των κοινών δραστηριοτήτων, οι βασικές και, στο μέτρο του δυνατού, οι υποστηρικτικές δράσεις στο πλαίσιο του δεύτερου σταδίου θα πρέπει να ολοκληρωθούν έως τις **30 Ιουνίου 2022 [6 μήνες μετά το τέλος του σταδίου 1]**.

3. *Στάδιο 3 — Έναρξη επιχειρησιακής λειτουργίας της Κοινής Κυβερνομονάδας*

ΒΑΣΙΚΕΣ ΔΡΑΣΕΙΣ

Μετά την έγκριση από το Συμβούλιο των συμπερασμάτων της Επιτροπής σχετικά με την έκθεση του δεύτερου σταδίου, οι επιχειρησιακοί συμμετέχοντες θα πρέπει να συντονίσουν την ανάπτυξη των **ομάδων κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ** στο πλαίσιο της Κοινής Κυβερνομονάδας και να δημιουργήσουν μια **φυσική πλατφόρμα** που θα επιτρέπει στις ομάδες να εκτελούν τεχνικές και επιχειρησιακές δράσεις. Με βάση τις προπαρασκευαστικές εργασίες που διεξάγονται στο πλαίσιο του δεύτερου σταδίου, οι συμμετέχοντες θα πρέπει να οριστικοποιήσουν το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας. Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να διασφαλίζουν ότι οι εμπειρογνώμονες και οι ικανότητες που περιλαμβάνονται στον κατάλογο των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ είναι διαθέσιμοι/-ες και έτοιμοι/-ες να συμβάλουν στη δραστηριότητα των ομάδων κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ.

Για την εφαρμογή του ενωσιακού σχεδίου αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας, οι συμμετέχοντες θα πρέπει να καθορίσουν ετήσιο πρόγραμμα εργασίας.

ΥΠΟΣΤΗΡΙΚΤΙΚΕΣ ΔΡΑΣΕΙΣ

Η Κοινή Κυβερνομονάδα μπορεί να χρησιμοποιηθεί από την κοινότητα της κυβερνοδιπλωματίας για την ευθυγράμμιση της δημόσιας επικοινωνίας. Η πλατφόρμα μπορεί να επιτρέπει στους συμμετέχοντες να συμβάλλουν στον πολιτικό καταλογισμό καθώς και στον καταλογισμό στο πλαίσιο της ποινικής δικαιοσύνης που χρησιμοποιείται σε αστυνομικό και δικαστικό επίπεδο. Επιπλέον, μπορεί να διευκολύνει την ανάκαμψη και να επιτρέψει διαρθρωμένες συνέργειες με εθνικές και διασυνοριακές ικανότητες παρακολούθησης και ανίχνευσης.

Για να εξασφαλιστεί η έναρξη της επιχειρησιακής λειτουργίας της Κοινής Κυβερνομονάδας, οι βασικές και, στο μέτρο του δυνατού, οι υποστηρικτικές δράσεις στο πλαίσιο του τρίτου σταδίου θα πρέπει να ολοκληρωθούν έως τις **31 Δεκεμβρίου 2022 [6 μήνες μετά το τέλος του σταδίου 2]**.

4. *Στάδιο 4 — Διεύρυνση της συνεργασίας στο πλαίσιο της Κοινής Κυβερνομονάδας ώστε να συμπεριληφθούν ιδιωτικοί φορείς και υποβολή εκθέσεων σχετικά με την επιτευχθείσα πρόοδο*

ΒΑΣΙΚΗ ΔΡΑΣΗ

Οι συμμετέχοντες στην Κοινή Κυβερνομονάδα θα πρέπει να συντάξουν **έκθεση δραστηριοτήτων σχετικά με την πρόοδο που έχει σημειωθεί όσον αφορά την εφαρμογή των τεσσάρων σταδίων που προβλέπονται στη σύσταση, στην οποία θα περιγράφονται τα επιτεύγματα και οι προκλήσεις που αντιμετωπίστηκαν**. Η εν λόγω έκθεση θα πρέπει να περιλαμβάνει στατιστικές πληροφορίες σχετικά με τις δραστηριότητες επιχειρησιακής συνεργασίας που διεξήχθησαν και στα τέσσερα στάδια. Η έκθεση θα πρέπει να υποβληθεί στην Επιτροπή και στον ύπατο εκπρόσωπο.

ΥΠΟΣΤΗΡΙΚΤΙΚΕΣ ΔΡΑΣΕΙΣ

Προκειμένου να επεκταθούν οι ικανότητες και οι πληροφορίες που είναι διαθέσιμες στις ομάδες κυβερνοασφάλειας ταχείας αντίδρασης της ΕΕ, οι συμμετέχοντες θα πρέπει να διασφαλίζουν ότι η Κοινή Κυβερνομονάδα συμβάλλει στη σύναψη **συμφωνιών ανταλλαγής πληροφοριών και επιχειρησιακής συνεργασίας μεταξύ συμμετεχόντων και οντοτήτων του ιδιωτικού τομέα** που παρέχουν, μεταξύ άλλων, υπηρεσίες πληροφοριών για απειλές και υπηρεσίες αντιμετώπισης περιστατικών. Θα πρέπει επίσης να διασφαλίζουν, μεταξύ άλλων δραστηριοτήτων, ότι η Κοινή Κυβερνομονάδα στηρίζει σε τακτικό διάλογο και δραστηριότητες ανταλλαγής πληροφοριών σχετικά με απειλές και τρωτά σημεία με τους χρήστες λύσεων κυβερνοασφάλειας, πρωτίστως εκείνες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS ή συγκεντρώνονται σε **κέντρα ανταλλαγής και ανάλυσης πληροφοριών (ISAC) σε επίπεδο ΕΕ**.

Τα κράτη μέλη θα πρέπει να στηρίζουν οντότητες που δραστηριοποιούνται στην επικράτειά τους, ιδίως εκείνες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS, ώστε να έχουν πρόσβαση και να συμβάλλουν σε διαλόγους δημόσιου και ιδιωτικού τομέα με ISAC σε επίπεδο ΕΕ.

Για να εξασφαλιστεί η δέουσα συμμετοχή του ιδιωτικού τομέα, οι βασικές και, στο μέτρο του δυνατού, οι υποστηρικτικές δράσεις στο πλαίσιο του τέταρτου σταδίου θα πρέπει να ολοκληρωθούν έως τις **30 Ιουνίου 2023 [6 μήνες μετά το τέλος του σταδίου 3]**.

ΤΡΟΠΟΙ ΤΑΧΕΙΑΣ ΚΙΝΗΤΟΠΟΙΗΣΗΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΙΚΑΝΟΤΗΤΩΝ ΤΗΣ ΕΕ

ΠΟΙΟΣ ΠΑΡΕΧΕΙ ΙΚΑΝΟΤΗΤΕΣ: Οι επιχειρησιακοί συμμετέχοντες

ΠΟΙΟΣ ΔΙΑΧΕΙΡΙΖΕΤΑΙ ΤΙΣ ΙΚΑΝΟΤΗΤΕΣ: Οι συμμετέχοντες στην Κοινή Κυβερνομονάδα, σύμφωνα με τους συμφωνηθέντες ρόλους και αρμοδιότητες

Στάδιο	**Στόχος**	**Καθήκον**	**Βασική δράση**	**Υποστηρικτική δράση**
Στάδιο 1 — Καθορισμός έως τις **31 Δεκεμβρίου 2021 [6 μήνες μετά την έκδοση]**	ΕΤΟΙΜΟΤΗΤΑ	**Προσδιορισμός ικανοτήτων**	**Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να καταρτίσουν κατάλογο των διαθέσιμων επιχειρησιακών ικανοτήτων της ΕΕ.**	
Στάδιο 2 — Προετοιμασία έως τις **30 Ιουνίου 2022 [6 μήνες μετά το τέλος του σταδίου 1]**	ΕΤΟΙΜΟΤΗΤΑ	**Καθορισμός σχετικών διαδικασιών και ρυθμίσεων για την ενεργοποίηση ικανοτήτων σε περίπτωση ανάγκης**	**Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να καταρτίσουν το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας (πλαίσιο της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο στο προσχέδιο), βάσει των εγκεκριμένων εθνικών σχεδίων**	**Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να εκπονήσουν τις ολοκληρωμένες εκθέσεις κατάστασης της ΕΕ με βάση την έκθεση της ΕΕ για την τεχνική κατάσταση της κυβερνοασφάλειας**
	ΕΤΟΙΜΟΤΗΤΑ	**Άσκηση ικανοτήτων**		**Οι συμμετέχοντες θα πρέπει να διοργανώσουν κοινή άσκηση και κατάρτιση (διακοινοτική)** **Οι συμμετέχοντες θα πρέπει να εκπονήσουν πολυετές σχέδιο για τον συντονισμό των ασκήσεων.**
	ΕΠΙΓΝΩΣΗ ΤΗΣ ΚΑΤΑΣΤΑΣΗΣ	**Δημιουργία εργαλείων για την ανταλλαγή πληροφοριών και αιτημάτων υποστήριξης**		**Οι συμμετέχοντες θα πρέπει να αναπτύξουν ικανότητες ασφαλούς και ταχείας ανταλλαγής πληροφοριών**
Η ΚΟΙΝΗ ΚΥΒΕΡΝΟΜΟΝΑΔΑ ΕΙΝΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΕΤΟΙΜΗ Με βάση τις προπαρασκευαστικές εργασίες των συμμετεχόντων στο πλαίσιο ομάδας εργασίας που θα συσταθεί από την Επιτροπή				
Στάδιο 3 — Ανάπτυξη έως τις **31 Δεκεμβρίου 2022 [6 μήνες μετά το τέλος του σταδίου 2]**	ΕΤΟΙΜΟΤΗΤΑ	**Καθορισμός σχετικών διαδικασιών, ρυθμίσεων και μνημονίων για την ενεργοποίηση ικανοτήτων σε περίπτωση ανάγκης**	**Οι επιχειρησιακοί συμμετέχοντες θα πρέπει να οριστικοποιήσουν το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας και να καθορίσουν την εφαρμογή του μέσω ετήσιων προγραμμάτων εργασίας.**	**Οι συμμετέχοντες θα πρέπει να υποστηρίξουν τη δημιουργία εθνικών και διασυνοριακών ικανοτήτων παρακολούθησης και ανίχνευσης, συμπεριλαμβανομένης της δημιουργίας SOC**
	ΣΥΝΤΟΝΙΣΜΕΝΗ ΑΝΤΙΜΕΤΩΠΙΣΗ	**Ανάπτυξη ικανοτήτων σε περίπτωση ανάγκης**	**Επιχειρησιακοί συμμετέχοντες για τον συντονισμό των επιχειρησιακών ομάδων κυβερνοασφάλειας ταχείας αντίδρασης μέσω της εικονικής και της φυσικής πλατφόρμας της Κοινής Κυβερνομονάδας στις Βρυξέλλες.**	**Οι συμμετέχοντες θα πρέπει να συντονίσουν τη δημόσια επικοινωνία και να συμβάλουν στον πολιτικό καταλογισμό, καθώς και στον καταλογισμό στο πλαίσιο της ποινικής δικαιοσύνης**

Στάδιο 4 — Επέκταση και υποβολή έκθεσης έως τις **30 Ιουνίου 2023 [6 μήνες μετά το τέλος του σταδίου 3]**	ΕΠΙΓΝΩΣΗ ΤΗΣ ΚΑΤΑΣΤΑΣΗΣ ΣΥΝΤΟΝΙΣΜΕΝΗ ΑΝΤΙΜΕΤΩΠΙΣΗ	**Διασφάλιση της δυνατότητας κλιμάκωσης με τη συμμετοχή του ιδιωτικού τομέα για την κάλυψη αναδυόμενων αναγκών**	**Οι συμμετέχοντες θα πρέπει να υποβάλουν έκθεση δραστηριοτήτων σχετικά με την επιτευχθείσα πρόοδο, περιγράφοντας τα επιτεύγματα και τις προκλήσεις, με την υποστήριξη στατιστικών πληροφοριών.**	**Οι συμμετέχοντες θα πρέπει να συνάψουν συμφωνίες ανταλλαγής πληροφοριών, καθώς και συμφωνίες επιχειρησιακής συνεργασίας με παρόχους υπηρεσιών κυβερνοασφάλειας** **Οι συμμετέχοντες θα πρέπει να συνάψουν συμφωνίες ανταλλαγής πληροφοριών με χρήστες κυβερνοασφάλειας, κυρίως οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS και ISAC της ΕΕ**