Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 8 Οκτωβρίου 2021
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

ΣΗΜΕΙΩΜΑ ΣΗΜΕΙΟΥ «I/A»

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Επιτροπή των Μονίμων Αντιπροσώπων (2ο Τμήμα) / Συμβούλιο
Θέμα:	Συμπεράσματα του Συμβουλίου σχετικά με τη διερεύνηση των δυνατοτήτων της πρωτοβουλίας για την Κοινή Κυβερνομονάδα — για τη συμπλήρωση της συντονισμένης αντιμετώπισης σε επίπεδο ΕΕ περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας - Έγκριση

1. Στις 23 Ιουνίου 2021, η Επιτροπή δημοσίευσε τη σύστασή της σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας[1] για την αναχαίτιση του αυξανόμενου αριθμού σοβαρών περιστατικών στον κυβερνοχώρο τα οποία πλήττουν τις δημόσιες υπηρεσίες, καθώς και τις δραστηριότητες των επιχειρήσεων και των πολιτών σε ολόκληρη την Ευρωπαϊκή Ένωση.

2. Η Επιτροπή παρουσίασε τη σύσταση στην Οριζόντια Ομάδα «Θέματα κυβερνοχώρου» (HWPCI) στις 28 Ιουνίου 2021. Επακολούθησαν συζητήσεις υπό τη σλοβενική Προεδρία κατά τις συνεδριάσεις της HWPCI στις 7 και 14 Ιουλίου 2021 για να συγκεντρωθούν οι απόψεις των κρατών μελών σχετικά με τη σύσταση της Επιτροπής.

[1] C(2021) 4520 final (11155/21 και 11155/21 ADD1).

3. Η Προεδρία παρουσίασε ένα πρώτο σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη διερεύνηση των δυνατοτήτων της πρωτοβουλίας για την Κοινή Κυβερνομονάδα — η οποία συμπληρώνει τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας[2] κατά την άτυπη τηλεδιάσκεψη των μελών της HWPCI στις 23 Ιουλίου 2021. Το εν λόγω σχέδιο συμπερασμάτων συζητήθηκε περαιτέρω κατά τις συνεδριάσεις των μελών της HWPCI στις 8 και 29 Σεπτεμβρίου 2021.

4. Κατά τη συνεδρίασή της στις 6 Οκτωβρίου 2021, η HWPCI συμφώνησε επί του σχεδίου συμπερασμάτων του Συμβουλίου ως έχει στο παράρτημα.

5. Βάσει των ανωτέρω, καλείται η Επιτροπή των Μονίμων Αντιπροσώπων να υποβάλει στο Συμβούλιο το σχέδιο συμπερασμάτων του Συμβουλίου ως έχει στο παράρτημα και να εισηγηθεί στο Συμβούλιο να εγκρίνει το σχέδιο συμπερασμάτων ως σημείο «Α» της ημερήσιας διάταξής του.

---

[2] 10975/21.

ΠΑΡΑΡΤΗΜΑ

Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη διερεύνηση των δυνατοτήτων της πρωτοβουλίας για την Κοινή Κυβερνομονάδα — για τη συμπλήρωση της συντονισμένης αντιμετώπισης σε επίπεδο ΕΕ περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με:

– τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[3],

– τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο[4],

– τη διπλωματία στον κυβερνοχώρο[5],

– πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο (εφεξής: εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο)[6],

– την ασφάλεια και την άμυνα[7],

– το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα[8],

– τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης[9],

– την εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ,

---

3 7290/21.
4 10086/18.
5 6122/15 + COR 1.
6 10474/17.
7 8396/21.
8 15585/14.
9 8711/20.

– την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ[10],

– την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ[11],

1. ΤΟΝΙΖΕΙ τη σημασία της ασφάλειας στον κυβερνοχώρο για την οικοδόμηση μιας ανθεκτικής, ψηφιακής και πράσινης Ευρώπης. ΤΟΝΙΖΕΙ ότι η ασφάλεια στον κυβερνοχώρο είναι απαραίτητη για την ευημερία και την ασφάλεια της ΕΕ και των κρατών μελών της, των πολιτών, των επιχειρήσεων και των θεσμών της, καθώς και για τη διαφύλαξη της ακεραιότητας των ελεύθερων και δημοκρατικών κοινωνιών μας.

2. ΑΝΑΓΝΩΡΙΖΕΙ τον διασυνοριακό και διατομεακό χαρακτήρα πολλών απειλών κατά της ασφάλειας στον κυβερνοχώρο, καθώς και τους κινδύνους και τις δυνητικές επιπτώσεις των συνεχών εκστρατειών πιο αποτελεσματικών, εξεζητημένων, στοχευμένων, πολυσύνθετων, επίμονων ή/και εκτεταμένων κακόβουλων δραστηριοτήτων στον κυβερνοχώρο[12]. Η πανδημία COVID-19 αποκάλυψε περισσότερο τα τρωτά σημεία των κοινωνιών μας και τις δυνατότητες πρόκλησης ζημιών από περιστατικά μεγάλης κλίμακας στον κυβερνοχώρο εις βάρος της οικονομίας, της δημοκρατίας, των βασικών υπηρεσιών και των υποδομών ζωτικής σημασίας, ιδιαίτερα στον τομέα της υγείας. Αύξησε επίσης τη σημασία της συνδεσιμότητας και της εξάρτησης της κοινωνίας από αξιόπιστα, έμπιστα και ασφαλή συστήματα δικτύου και πληροφοριών. Τέλος, υπογράμμισε την ανάγκη για ένα παγκόσμιο, ανοικτό, ελεύθερο, σταθερό και ασφαλές διαδίκτυο, καθώς και για εμπιστοσύνη στα προϊόντα, τις διαδικασίες και τις υπηρεσίες της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) και την ασφάλειά τους, συμπεριλαμβανομένης της ανάγκης να εξασφαλιστεί μια ανθεκτική αλυσίδα εφοδιασμού.

---

10 14435/17 + COR 1.
11 7737/19.
12 ENISA Threat Landscape 2020 (Τοπίο των απειλών 2020).

3. ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη σημασία της ανθεκτικότητας στον κυβερνοχώρο και της περαιτέρω ανάπτυξης του πλαισίου διαχείρισης κρίσεων κυβερνοασφάλειας της ΕΕ[13] με στόχο την αποτελεσματική και έγκαιρη αντιμετώπιση σε επίπεδο ΕΕ περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας, καθώς και της περαιτέρω ενσωμάτωσής του στους υπάρχοντες οριζόντιους και τομεακούς μηχανισμούς της ΕΕ για την αντιμετώπιση κρίσεων. ΤΟΝΙΖΕΙ τον ρόλο του Συμβουλίου και των ολοκληρωμένων ρυθμίσεων για την πολιτική αντιμετώπιση κρίσεων (IPCR) στη διασφάλιση έγκαιρου συντονισμού και αντίδρασης σε πολιτικό ενωσιακό επίπεδο έναντι των κρίσεων –είτε εξωενωσιακής είτε ενδοενωσιακής προέλευσης– οι οποίες έχουν ευρύ αντίκτυπο ή πολιτική σπουδαιότητα. ΕΠΙΣΗΜΑΙΝΕΙ ότι είναι σημαντικό τα εν λόγω πλαίσια και μηχανισμοί να δοκιμάζονται με τακτικές ασκήσεις.

4. ΥΠΕΝΘΥΜΙΖΕΙ ότι οι δραστηριότητες σε επίπεδο ΕΕ όσον αφορά μεγάλης κλίμακας περιστατικά και κρίσεις στον κυβερνοχώρο εκτελούνται σύμφωνα με τις αρχές της επικουρικότητας, της αναλογικότητας, της συμπληρωματικότητας, της μη αλληλεπικάλυψης και της εμπιστευτικότητας. ΕΠΑΝΑΛΑΜΒΑΝΕΙ ότι τα κράτη μέλη φέρουν την πρωταρχική ευθύνη για να αντιμετωπίσουν τα περιστατικά και τις κρίσεις κυβερνοασφάλειας μεγάλης κλίμακας εκ των οποίων θίγονται τα ίδια. ΥΠΕΝΘΥΜΙΖΕΙ τη σημασία του σεβασμού των αρμοδιοτήτων των κρατών μελών και της αποκλειστικής ευθύνης τους για την εθνική ασφάλεια, σύμφωνα με το άρθρο 4 παράγραφος 2 της Συνθήκης για την Ευρωπαϊκή Ένωση, όπου περιλαμβάνεται και ο τομέας της κυβερνοασφάλειας.

5. ΥΠΕΝΘΥΜΙΖΕΙ ταυτόχρονα τη σημασία του σεβασμού των αρμοδιοτήτων και των εντολών που έχουν ανατεθεί στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ. Ο ύπατος εκπρόσωπος, η Επιτροπή και άλλα θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ επίσης διαδραματίζουν ουσιαστικό ρόλο, ο οποίος απορρέει από το δίκαιο της Ένωσης, μεταξύ άλλων λόγω των πιθανών επιπτώσεων περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας εις βάρος της ενιαίας αγοράς, καθώς και της λειτουργίας των ίδιων των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ.

[13] 10086/18.

6. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη να αποφεύγονται οι περιττές αλληλεπικαλύψεις και να επιζητούνται συμπληρωματικότητα και προστιθέμενη αξία στην περαιτέρω ανάπτυξη του πλαισίου της ΕΕ για τη διαχείριση κρίσεων κυβερνοασφάλειας, καθώς και να διασφαλίζεται η ευθυγράμμιση προς τους μηχανισμούς, πρωτοβουλίες, δίκτυα, διεργασίες και διαδικασίες που ήδη υπάρχουν σε εθνικό και ευρωπαϊκό επίπεδο. ΤΟΝΙΖΕΙ τη σημασία του εξορθολογισμού των υφιστάμενων διαδικασιών και δομών για τη μείωση της πολυπλοκότητας και υπέρ της συνοχής στην Ένωση, ούτως ώστε να βελτιωθεί η προσβασιμότητα και η ικανότητα ανταπόκρισης σε όσους ζητούν βοήθεια και αλληλεγγύη.

7. ΑΝΑΓΝΩΡΙΖΕΙ την εφαρμοσιμότητα του διεθνούς δικαίου, συμπεριλαμβανομένου του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, του διεθνούς ανθρωπιστικού δικαίου και του δικαίου των ανθρωπίνων δικαιωμάτων στον κυβερνοχώρο, και ΠΡΟΤΡΕΠΕΙ την τήρηση των εθελοντικών, μη δεσμευτικών προτύπων, κανόνων και αρχών υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο που έχουν εγκριθεί από όλα τα κράτη μέλη του ΟΗΕ.

8. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για την πρόοδο που έχει επιτευχθεί τα τελευταία χρόνια στο πλαίσιο του Συμβουλίου, ιδίως στην Οριζόντια Ομάδα «Θέματα Κυβερνοχώρου» (HWPCI) και σε άλλες σχετικές ομάδες του Συμβουλίου, καθώς και στη δημιουργία άλλων πρωτοβουλιών, δικτύων και μηχανισμών συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των κρατών μελών, ιδίως της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS) και του δικτύου CSIRT που συστάθηκαν με την οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, του δικτύου οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο (CyCLONe), καθώς και των σχετικών με την κυβερνοάμυνα έργων που δρομολογήθηκαν στο πλαίσιο της μόνιμης διαρθρωμένης συνεργασίας (PESCO)[14], της κοινής ειδικής ομάδας δράσης για την καταπολέμηση του κυβερνοεγκλήματος (J-CAT), του Ευρωπαϊκού δικαστικού δικτύου για το έγκλημα στον κυβερνοχώρο (EJCN), των εθελοντικών συνεισφορών των κρατών μελών στο Κέντρο ανάλυσης πληροφοριών της ΕΕ (EU INTCEN), και του συντονισμού και της συνεργασίας στο πλαίσιο της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο.

---

14 Ειδικότερα, οι «ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο και η αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο» που συντονίζει η Λιθουανία, το «συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών» που συντονίζει η Γερμανία, η «πλατφόρμα ανταλλαγής πληροφοριών για την αντιμετώπιση απειλών και περιστατικών στον κυβερνοχώρο» που συντονίζει η Ελλάδα.

9. ΥΠΕΝΘΥΜΙΖΕΙ τα υπάρχοντα πλαίσια συνεργασίας μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, όπως η διαρθρωμένη συνεργασία μεταξύ ENISA και CERT-ΕΕ και το μνημόνιο συμφωνίας μεταξύ του ENISA, του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ), του Ευρωπαϊκού Κέντρου για το Κυβερνοέγκλημα της Ευρωπόλ (EC3) και της CERT-ΕΕ. ΤΟΝΙΖΕΙ τη σημασία της συνεχούς τακτικής ανταλλαγής πληροφοριών με το Συμβούλιο σχετικά με τις περαιτέρω εξελίξεις σε αυτά τα πλαίσια συνεργασίας.

10. ΕΞΑΙΡΕΙ τη σημασία αφενός της ενίσχυσης της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των διαφόρων κοινοτήτων στον κυβερνοχώρο εντός της ΕΕ και των κρατών μελών της σε όλα τα αναγκαία επίπεδα —τεχνικό, επιχειρησιακό και στρατηγικό/πολιτικό— και αφετέρου της διασύνδεσης των υφιστάμενων μηχανισμών, δικτύων, δομών, διεργασιών και διαδικασιών διαχείρισης κρίσεων οπουδήποτε υποστηρίζει και βελτιώνει τον χειρισμό περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

11. ΑΝΑΓΝΩΡΙΖΕΙ την πρόοδο που έχει επιτευχθεί από ομάδα κρατών μελών όσον αφορά τη δημιουργία κοινής επιχειρησιακής ικανότητας για τον κυβερνοχώρο «ομάδες ταχείας αντίδρασης» στο πλαίσιο της PESCO, με στόχο την εμβάθυνση της εθελοντικής συνεργασίας στον κυβερνοχώρο μέσω αμοιβαίας συνδρομής, μεταξύ άλλων για την αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

12. ΑΝΑΓΝΩΡΙΖΕΙ την εμπειρία και την ικανότητα της ανά πάσα στιγμή (24/7) αντίδρασης της κοινότητας επιβολής του νόμου στον τομέα της επιχειρησιακής συνεργασίας και της ασφαλούς ανταλλαγής πληροφοριών έναντι σημαντικών διασυνοριακών κυβερνοεπιθέσεων μέσω του πρωτοκόλλου της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου.

13. ΑΝΑΓΝΩΡΙΖΕΙ τη συνεχιζόμενη εφαρμογή του πλαισίου για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο (εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο). ΥΠΕΝΘΥΜΙΖΕΙ ότι κάθε κράτος μέλος είναι ελεύθερο να λαμβάνει δική του κυρίαρχη απόφαση όσον αφορά τον καταλογισμό της ευθύνης κακόβουλης δραστηριότητας στον κυβερνοχώρο ανάλογα με την εκάστοτε περίπτωση. ΥΠΕΝΘΥΜΙΖΕΙ ότι τα μέτρα που λαμβάνονται στο πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο θα πρέπει να βασίζονται σε κοινή επίγνωση της κατάστασης κατά συμφωνία των κρατών μελών. Το EU INTCEN έχει κεντρικό ρόλο ως κόμβος για την παροχή επίγνωσης της κατάστασης και αξιολόγησης των απειλών σε θέματα κυβερνοχώρου για την ΕΕ, βάσει εθελοντικών συνεισφορών πληροφοριών από τα κράτη μέλη και με την επιφύλαξη των αρμοδιοτήτων τους.

14. ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη σημασία της αμοιβαίας συνδρομής και της αλληλεγγύης, σύμφωνα με το άρθρο 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση και το άρθρο 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ΖΗΤΕΙ τη διενέργεια περαιτέρω ασκήσεων με διάσταση κυβερνοχώρου. ΥΠΕΝΘΥΜΙΖΕΙ την ανάγκη προβληματισμού σχετικά με το πώς διαρθρώνονται το πλαίσιο της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο, η εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο και οι διατάξεις των προαναφερόμενων άρθρων σε περίπτωση περιστατικού ή κρίσης μεγάλης κλίμακας στον κυβερνοχώρο. ΥΠΕΝΘΥΜΙΖΕΙ προσέτι ότι οι υποχρεώσεις των κρατών μελών που απορρέουν από το άρθρο 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση δεν θίγουν τον ιδιαίτερο χαρακτήρα της πολιτικής ορισμένων κρατών μελών για την ασφάλεια και την άμυνα. ΥΠΕΝΘΥΜΙΖΕΙ επίσης ότι, για τα κράτη που είναι μέλη του ΝΑΤΟ, το ΝΑΤΟ παραμένει το θεμέλιο της συλλογικής άμυνάς τους..

15. ΑΝΑΓΝΩΡΙΖΕΙ τη συνεργασία ΕΕ-ΝΑΤΟ για την ασφάλεια και την άμυνα στον κυβερνοχώρο, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών μεταξύ της CERT-ΕΕ και της ομάδας αντιμετώπισης συμβάντων πληροφορικής του ΝΑΤΟ (NCIRC), με πλήρη σεβασμό των αρχών της διαφάνειας, της αμοιβαιότητας και της συμμετοχικότητας, καθώς και της αυτονομίας λήψεως αποφάσεων αμφοτέρων των οργανισμών.

16. ΑΝΑΓΝΩΡΙΖΕΙ τη σημασία της συνεργασίας, κατά περίπτωση, με τον ιδιωτικό τομέα όσον αφορά τις δραστηριότητες ανταλλαγής πληροφοριών και την παροχή συναφούς εμπειρογνωσίας, καθώς και αξιόπιστων λύσεων και υπηρεσιών, μεταξύ άλλων επί παραδείγματι για την υποστήριξη της αντιμετώπισης περιστατικών και την ενίσχυση της επίγνωσης της κατάστασης μεταξύ διαφόρων κοινοτήτων του κυβερνοχώρου.

17. ΤΟΝΙΖΕΙ τη σημασία της ύπαρξης ασφαλών διαύλων επικοινωνίας για την ανταλλαγή διαβαθμισμένων και ευαίσθητων πληροφοριών. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη περαιτέρω προόδου.

Εν προκειμένω και λαμβάνοντας υπόψη τα ανωτέρω,

18. ΑΝΑΓΝΩΡΙΖΕΙ τη σύσταση της Επιτροπής σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας, ως πρωτοβουλία που πρέπει να εξεταστεί κατά την περαιτέρω ανάπτυξη του πλαισίου της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο[15].

19. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να συνεχίσουν τις προσπάθειες για ένα πιο ολοκληρωμένο και αποτελεσματικό ενωσιακό πλαίσιο διαχείρισης κρίσεων ασφάλειας στον κυβερνοχώρο, με βάση τους υφιστάμενους μηχανισμούς και την πρόοδο που έχει ήδη επιτευχθεί, και να λάβουν υπόψη τις δυνατότητες της πρωτοβουλίας της Κοινής Κυβερνομονάδας για τη συμπλήρωση των μηχανισμών αυτών με σταδιακή προσέγγιση. ΤΟΝΙΖΕΙ ότι μια κλιμακωτή, διαφανής και συμμετοχική διαδικασία είναι αναγκαία για την επίρρωση της εμπιστοσύνης και, ως εκ τούτου, έχει κρίσιμη σημασία για την περαιτέρω ανάπτυξη ενός ενωσιακού πλαισίου διαχείρισης κρίσεων ασφάλειας στον κυβερνοχώρο. Η διαδικασία αυτή θα πρέπει να σέβεται τους ισχύοντες ρόλους, αρμοδιότητες και εντολές των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, καθώς και τις αρχές που διατυπώνονται στα παρόντα συμπεράσματα, συμπεριλαμβανομένων των αρχών της αναλογικότητας, της επικουρικότητας, της συμμετοχικότητας, της συμπληρωματικότητας, της μη αλληλεπικάλυψης και της εμπιστευτικότητας των πληροφοριών. ΤΟΝΙΖΕΙ, ταυτόχρονα, ότι κάθε ενδεχόμενη συμμετοχή ή συνεισφορά κρατών μελών σε δυνητική Κοινή Κυβερνομονάδα έχει εθελοντικό χαρακτήρα.

---

15 C(2021)4520 final (11155/21 και 11155/21 ADD1).

20. ΤΟΝΙΖΕΙ την ανάγκη θέσπισης κατάλληλων μεθόδων εργασίας και διακυβέρνησης, με σκοπό να καταστεί δυνατή η είσοδος και η συμμετοχή όλων των κρατών μελών στις διαδικασίες συζήτησης, ανάπτυξης και αποτελεσματικής λήψης αποφάσεων σχετικά με το πλαίσιο της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένης της δυνητικής πρωτοβουλίας για Κοινή Κυβερνομονάδα. ΖΗΤΕΙ να γίνονται σεβαστές οι προνομίες του Συμβουλίου βάσει των Συνθηκών και η αρχή της καλόπιστης συνεργασίας.

21. ΥΠΟΓΡΑΜΜΙΖΕΙ τη σημασία του εντοπισμού και της συμμετοχής όλων των σχετικών κοινοτήτων του κυβερνοχώρου εντός της ΕΕ και στα κράτη μέλη της, λαμβάνοντας παράλληλα υπόψη τους διαφορετικούς ρόλους και αρμοδιότητές τους στα διάφορα είδη περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο. ΥΠΟΓΡΑΜΜΙΖΕΙ τον καθοριστικό ρόλο του Συμβουλίου, ιδίως μέσω της HWPCI, στη λειτουργία χάραξης πολιτικής και συντονισμού όσον αφορά την περαιτέρω ανάπτυξη του πλαισίου της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο. ΚΑΛΕΙ, συνεπώς, τα κράτη μέλη, την Επιτροπή, την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ), το EU INTCEN, την CERT-ΕΕ, τον ENISA, την Ευρωπόλ (EC3), την Eurojust (EJCN), το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (ECCC), καθώς και εκπροσώπους από το δίκτυο CSIRT, το CyCLONe, την ομάδα συνεργασίας NIS, τον ΕΟΑ και τα συναφή έργα PESCO, καθώς και άλλους ενδεχομένως ενδιαφερόμενους φορείς, να δραστηριοποιηθούν σε αυτήν τη διαδικασία. Το ενδεχόμενο δημιουργίας ομάδας εργασίας, όπως προτείνεται στη σύσταση της Επιτροπής, θα μπορούσε να εξεταστεί περαιτέρω, με την εξασφάλιση κατάλληλης εκπροσώπησης όλων των κρατών μελών και τη δράση υπό την πολιτική καθοδήγηση του Συμβουλίου· η ομάδα εργασίας θα λειτουργεί ως προσωρινό φόρουμ στο οποίο θα συνέρχονται εκπρόσωποι όλων των σχετικών κοινοτήτων του κυβερνοχώρου στα κράτη μέλη και εντός της ΕΕ. Η εν λόγω ομάδα εργασίας θα πρέπει να υποβάλλει τακτικά εκθέσεις σχετικά με τις δραστηριότητές της καθώς και πιθανές προτάσεις στο Συμβούλιο προς συζήτηση, έγκριση και περαιτέρω καθοδήγηση. Επιπλέον, θα μπορούσαν να καθιερωθούν και άλλες μορφές διαλόγου εντός και μεταξύ των κοινοτήτων, μεταξύ άλλων μέσω εργαστηρίων, σεμιναρίων, κοινής κατάρτισης και ασκήσεων.

22. ΥΠΟΓΡΑΜΜΙΖΕΙ τον ρόλο του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (ECCC) και του δικτύου εθνικών κέντρων συντονισμού σε σχέση με τη δυνητική Κοινή Κυβερνομονάδα, ιδίως αν ληφθεί υπόψη ο ρόλος της για την ουσιαστική αύξηση των τεχνολογικών ικανοτήτων, των τεχνολογικών λύσεων, των δυνατοτήτων και των δεξιοτήτων της Ένωσης στον τομέα της κυβερνοασφάλειας.

23. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να συμμετάσχουν στην περαιτέρω ανάπτυξη του πλαισίου της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο, μεταξύ άλλων διερευνώντας τις δυνατότητες της πρωτοβουλίας για Κοινή Κυβερνομονάδα, καθιερώνοντας και καθορίζοντας τη διαδικασία, μαζί με ορόσημα και χρονοδιάγραμμα, καθώς και διευκρινίζοντας τους στόχους και τους πιθανούς ρόλους και αρμοδιότητες. ΤΟΝΙΖΕΙ την ανάγκη να παγιωθούν, κατά προτεραιότητα, τα υφιστάμενα δίκτυα και οι αλληλεπιδράσεις εντός κάθε κοινότητας, καθώς και να πραγματοποιηθεί διεξοδική χαρτογράφηση των ενδεχόμενων κενών και αναγκών στην ανταλλαγή πληροφοριών εντός και μεταξύ των κοινοτήτων του κυβερνοχώρου, καθώς και εντός και μεταξύ των ευρωπαϊκών θεσμικών και λοιπών οργάνων και οργανισμών, και, στη συνέχεια, να συμφωνηθούν ενδεχόμενοι πρωταρχικοί στόχοι και προτεραιότητες της δυνητικής Κοινής Κυβερνομονάδας. Χωρίς να προδικάζεται το αποτέλεσμα, ΤΟΝΙΖΕΙ την ανάγκη να δοθεί έμφαση στον προσδιορισμό των αναγκών ανταλλαγής πληροφοριών προκειμένου να διαμορφωθεί κοινή επίγνωση της κατάστασης από όλες τις σχετικές κοινότητες. Κατά τον προσδιορισμό των κενών και των αναγκών στην ανταλλαγή πληροφοριών, συμπεριλαμβανομένης της ενδεχόμενης χρήσης εικονικών πλατφορμών, θα πρέπει να εξακολουθήσει να δίδεται η δέουσα προσοχή στην ύπαρξη ασφαλών διαύλων επικοινωνίας για την ανταλλαγή διαβαθμισμένων και ευαίσθητων πληροφοριών, ΤΟΝΙΖΟΝΤΑΣ παράλληλα τη σπουδαιότητα της χρήσης των ήδη υφιστάμενων υποδομών. Η εισαγωγή σταδιακής προσέγγισης αποσκοπεί στην οικοδόμηση εμπιστοσύνης και στη δημιουργία βάσης για ενδεχόμενα περαιτέρω βήματα σχετικά με την ενίσχυση της ετοιμότητας και της επιχειρησιακής συνεργασίας. ΑΝΑΓΝΩΡΙΖΕΙ ότι οι διαφορετικοί στόχοι θα μπορούσαν να δικαιολογήσουν διαφορετικές λύσεις και τη δραστηριοποίηση διαφορετικού συνόλου εκπροσώπων των σχετικών κοινοτήτων του κυβερνοχώρου εντός της ΕΕ και των κρατών μελών της.

24. ΖΗΤΕΙ να εξεταστεί περαιτέρω η νομική βάση για τη δυνητική Κοινή Κυβερνομονάδα καθ' όλη τη διάρκεια της διαδικασίας, συμπεριλαμβανομένης αξιολόγησης των καθηκόντων και των ρόλων έναντι εκείνων που, στη σύσταση, ανατίθενται στον ENISA υπό το πρίσμα του άρθρου 7 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019. ΖΗΤΕΙ περαιτέρω μελέτη επιμέρους στοιχείων της σύστασης σχετικά με τη δημιουργία Κοινής Κυβερνομονάδας, μεταξύ άλλων όσον αφορά την ιδέα των ομάδων ταχείας αντίδρασης της ΕΕ για την κυβερνοασφάλεια, καθώς και το ενωσιακό σχέδιο αντιμετώπισης περιστατικών και κρίσεων κυβερνοασφάλειας. ΤΟΝΙΖΕΙ ότι η δυνητική Κοινή Κυβερνομονάδα πρέπει να σέβεται τις αρμοδιότητες, τις εντολές και τις νομικές εξουσίες των ενδεχόμενων μελλοντικών συμμετεχόντων σε αυτήν.

25. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να εξετάσουν τις δυνατότητες της πρωτοβουλίας για Κοινή Κυβερνομονάδα, μεταξύ άλλων και από τη σκοπιά των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, προς συμπλήρωση των προσπαθειών που καταβάλλονται επί του παρόντος σε επίπεδο κρατών μελών. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για την πρόθεση της Επιτροπής να ενισχύσει την ανθεκτικότητα των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ μέσω της επικείμενης πρότασής της για κανονισμό σχετικά με κοινούς δεσμευτικούς κανόνες κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ.

26. Εν κατακλείδι, ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη δέσμευσή του υπέρ της ενίσχυσης της ανθεκτικότητας στον κυβερνοχώρο και της περαιτέρω ανάπτυξης του πλαισίου της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο, ΘΑ ΠΑΡΑΚΟΛΟΥΘΕΙ ΤΑΚΤΙΚΑ την πρόοδο και θα παρέχει περαιτέρω καθοδήγηση για τη συμπλήρωση του πλαισίου της ΕΕ για τη διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο.