Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 9 Μαρτίου 2021
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

ΣΗΜΕΙΩΜΑ ΣΗΜΕΙΟΥ «I/A»

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Επιτροπή των Μονίμων Αντιπροσώπων / Συμβούλιο
Θέμα:	Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία

1. Στις 16 Δεκεμβρίου 2020, η Επιτροπή και ο ύπατος εκπρόσωπος της Ένωσης για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας δημοσίευσαν την κοινή τους ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με τίτλο «Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία»[1]. Η νέα στρατηγική για την κυβερνοασφάλεια έχει ως στόχο να ενισχύσει τη συλλογική ανθεκτικότητα της Ευρώπης απέναντι σε κυβερνοαπειλές και να εξασφαλίσει ότι θα μπορέσουν να ωφεληθούν πλήρως όλοι οι πολίτες και οι επιχειρήσεις από έγκυρες και αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία.

[1] 14133/20

2. Η Επιτροπή και η ΕΥΕΔ παρουσίασαν την κοινή ανακοίνωση στην άτυπη βιντεοδιάσκεψη της Οριζόντιας Ομάδας για θέματα κυβερνοχώρου (HWPCI) στις 17 Δεκεμβρίου 2020 και στις 12 Ιανουαρίου 2021. Κατά την άτυπη βιντεοδιάσκεψη της HWPCI στις 17 Δεκεμβρίου 2020, η επερχόμενη πορτογαλική Προεδρία ανακοίνωσε την πρόθεσή της να καταρτίσει σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία.

3. Η Προεδρία υπέβαλε ένα πρώτο σχέδιο συμπερασμάτων του Συμβουλίου κατά την άτυπη βιντεοδιάσκεψη της HWPCI στις 2 Φεβρουαρίου 2021. Τα συμπεράσματα αυτά συζητήθηκαν στη συνέχεια σε άτυπες βιντεοδιασκέψεις της HWPCI στις 9 Φεβρουαρίου 2021, στις 19 Φεβρουαρίου 2021, την 1η και στις 9 Μαρτίου 2021.

4. Επειδή το σχέδιο συμπερασμάτων περιέχει επίσης αναφορά στις αμυντικές πολιτικές της ΕΕ (παράγραφος 30), η Πολιτικοστρατιωτική Ομάδα (PMG) συζήτησε τη σχετική παράγραφο κατά τη συνεδρίασή της στις 10 Φεβρουαρίου 2021.

5. Διάφορες παράγραφοι αφορούν την Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας (παράγραφοι 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 και 33) και, ως εκ τούτου, υποβλήθηκαν στην Επιτροπή Πολιτικής και Ασφάλειας η οποία ενέκρινε τις παραγράφους αυτές κατά τη συνεδρίασή της στις 4 Μαρτίου 2021.

6. Κατά την άτυπη βιντεοδιάσκεψη της 9ης Μαρτίου 2021, η HWPCI κατέληξε σε συμφωνία επί του σχεδίου συμπερασμάτων του Συμβουλίου ως έχει στο έγγραφο 6722/21.

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

ΠΑΡΑΡΤΗΜΑ

Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με:

— την κοινή ανακοίνωση της 25ης Ιουνίου 2013 προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με θέμα τη στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: «Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο»[2],

— τη διακυβέρνηση του διαδικτύου[3],

— την κοινή ανακοίνωση της 20ής Νοεμβρίου 2017 προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ»[4],

— την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ[5],

— τη σημασία του 5G για την ευρωπαϊκή οικονομία και την ανάγκη μετριασμού των κινδύνων ασφάλειας που συνδέονται με το 5G[6]

— το μέλλον μιας Ευρώπης ψηφιοποιημένης σε μεγάλο βαθμό μετά το 2020: «Τόνωση της ψηφιακής και οικονομικής ανταγωνιστικότητας σε ολόκληρη την Ένωση και της ψηφιακής συνοχής»[7],

συμπληρωματικές προσπάθειες για την ενίσχυση της ανθεκτικότητας και την αντιμετώπιση των υβριδικών απειλών[8],

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

---

2 12109/13
3 16200/14
4 14435/17 + COR 1
5 7737/19
6 14517/19
7 9596/19
8 14972/19
9 8711/20

— την ψηφιακή διπλωματία[10],

— την ενίσχυση της ανθεκτικότητας και την αντιμετώπιση υβριδικών απειλών, περιλαμβανομένης της παραπληροφόρησης στο πλαίσιο της πανδημίας COVID-19[11],

— τη διπλωματία στον κυβερνοχώρο[12],

— τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο[13],

— ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»)[14],

— τις κατευθυντήριες γραμμές για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο[15],

— μια ανάκαμψη που προωθεί τη μετάβαση προς μια πιο δυναμική, ανθεκτική και ανταγωνιστική ευρωπαϊκή βιομηχανία[16],

— την κυβερνοασφάλεια των συνδεδεμένων συσκευών[17],

— την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας[18],

— και το ψήφισμα του Συμβουλίου σχετικά με την ασφάλεια μέσω κρυπτογράφησης και την ασφάλεια παρά την κρυπτογράφηση[19],

---

10 12804/20
11 14064/20
12 6122/15 + COR 1
13 10086/18
14 10474/17
15 10496/18
16 13004/20
17 13629/20
18 14540/16
19 13084/1/20 REV 1

— και τη δήλωση των κρατών μελών της 15ης Οκτωβρίου 2020 σχετικά με την ανάπτυξη του νέφους επόμενης γενιάς για τις επιχειρήσεις και τον δημόσιο τομέα στην ΕΕ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 1ης και 2ας Οκτωβρίου 2020 σχετικά με την πανδημία COVID-19, την ενιαία αγορά, τη βιομηχανική πολιτική, την ψηφιακή διάσταση και τις εξωτερικές σχέσεις[20] και τα συμπεράσματα σχετικά με την παραπληροφόρηση και τις υβριδικές απειλές, καθώς και σχετικά με ένα νέο στρατηγικό θεματολόγιο 2019-2024 της 20ής Ιουνίου 2019[21],

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τη συνολική στρατηγική της Ευρωπαϊκής Ένωσης για την εξωτερική πολιτική και την πολιτική ασφαλείας «Κοινό όραμα, κοινές δράσεις: μια ισχυρότερη Ευρώπη» της 28ης Ιουνίου 2016,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τις ανακοινώσεις της Ευρωπαϊκής Επιτροπής σχετικά με τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, της 19ης Δεκεμβρίου 2020[22], και με τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας της 24ης Ιουλίου 2020[23],

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ την κοινή ανακοίνωση της Ευρωπαϊκής Επιτροπής και του ύπατου εκπροσώπου σχετικά με ένα νέο θεματολόγιο ΕΕ-ΗΠΑ για παγκόσμια αλλαγή, της 2ας Δεκεμβρίου 2020[24],

1. ΕΠΙΣΗΜΑΙΝΕΙ το γεγονός ότι η κυβερνοασφάλεια είναι απαραίτητη για να οικοδομηθεί μια ανθεκτική, πράσινη και ψηφιακή Ευρώπη και ΧΑΙΡΕΤΙΖΕΙ την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με τίτλο «Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία», στην οποία περιγράφεται το νέο πλαίσιο δράσης της ΕΕ όσον αφορά «την ανθεκτικότητα, την τεχνολογική κυριαρχία και τον ηγετικό ρόλο», καθώς και για να προστατευθούν οι πολίτες, οι επιχειρήσεις και οι θεσμοί της από περιστατικά και απειλές στον κυβερνοχώρο, ενώ παράλληλα θα ενισχύεται η εμπιστοσύνη ατόμων και οργανισμών στην ικανότητα της ΕΕ να προαγάγει ασφαλή και αξιόπιστα συστήματα δικτύων και πληροφοριών, υποδομές και συνδεσιμότητα, καθώς και να προαγάγει και να προστατεύσει έναν παγκόσμιο, ανοιχτό, ελεύθερο, σταθερό και ασφαλή κυβερνοχώρο θεμελιωμένο στα ανθρώπινα δικαιώματα, τις θεμελιώδεις ελευθερίες, τη δημοκρατία και το κράτος δικαίου.

---

20 EUCO 13/20
21 EUCO 9/19
22 19.2.2020 COM(2020) 67 final
23 24.7.2020 COM(2020) 605 final
24 2.12.2020 JOIN(2020) 22 τελικό

2. ΑΝΑΓΝΩΡΙΖΕΙ ότι η πανδημία COVID-19 έφερε στο προσκήνιο της καθημερινής μας ζωής την αυξημένη ανάγκη για εμπιστοσύνη στα εργαλεία και τα συστήματα της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) και την ασφάλειά τους. ΤΟΝΙΖΕΙ ότι η κυβερνοασφάλεια και το παγκόσμιο και ανοικτό διαδίκτυο είναι ζωτικής σημασίας για τη λειτουργία της δημόσιας διοίκησης και των θεσμών τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο, καθώς και για την κοινωνία και την οικονομία μας στο σύνολό της.

3. ΤΟΝΙΖΕΙ την ανάγκη να αυξηθεί η ευαισθητοποίηση σε θέματα κυβερνοχώρου στο πολιτικό και το στρατηγικό επίπεδο λήψης αποφάσεων, παρέχοντας στους φορείς λήψης αποφάσεων σχετικές γνώσεις και πληροφορίες και ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη να ενισχυθεί η ευαισθητοποίηση του ευρέος κοινού και να προωθηθεί η κυβερνοϋγιεινή.

4. ΖΗΤΕΙ την προαγωγή και την προστασία των βασικών ενωσιακών αξιών της δημοκρατίας, του κράτους δικαίου, των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών, περιλαμβανομένου του δικαιώματος στην ελευθερία της έκφρασης και της πληροφόρησης, του δικαιώματος στην ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι και του δικαιώματος στην ιδιωτική ζωή στον κυβερνοχώρο. ΧΑΙΡΕΤΙΖΕΙ, στο πλαίσιο αυτό, περαιτέρω συνεχείς προσπάθειες να προστατευθούν υπερασπιστές των ανθρώπινων δικαιωμάτων, μέλη της κοινωνίας των πολιτών και της ακαδημαϊκής κοινότητας που δουλεύουν σε θέματα όπως η κυβερνοασφάλεια, η προστασία δεδομένων, η παρακολούθηση και η λογοκρισία στο διαδίκτυο, παρέχοντας περαιτέρω πρακτική καθοδήγηση, προωθώντας βέλτιστες πρακτικές και εντείνοντας τις προσπάθειες της ΕΕ να αποτρέψει παραβιάσεις και καταπατήσεις των ανθρώπινων δικαιωμάτων και την κατάχρηση αναδυόμενων τεχνολογιών, ιδίως μέσω της χρήσης διπλωματικών μέτρων όπου απαιτείται, καθώς και μέσω του ελέγχου των εξαγωγών τέτοιων τεχνολογιών. ΑΝΑΔΕΙΚΝΥΕΙ, στο πλαίσιο αυτό, τη σημασία του σχεδίου δράσης της ΕΕ για τα ανθρώπινα δικαιώματα και τη δημοκρατία 2020-2024 και των κατευθυντήριων γραμμών της για τα ανθρώπινα δικαιώματα όσον αφορά την ελευθερία της έκφρασης εντός και εκτός διαδικτύου.
5. ΕΠΙΣΗΜΑΙΝΕΙ ότι η επίτευξη στρατηγικής αυτονομίας με παράλληλη διατήρηση μιας ανοικτής οικονομίας αποτελεί βασικό στόχο της Ένωσης προκειμένου να καθορίσει η ίδια την οικονομική της πορεία και τα συμφέροντά της. Αυτό περιλαμβάνει ενίσχυση της ικανότητας για αυτόνομες επιλογές στον τομέα της κυβερνοασφάλειας με στόχο να ενισχυθεί ο ψηφιακός ηγετικός ρόλος της ΕΕ και οι στρατηγικές της ικανότητες. ΥΠΕΝΘΥΜΙΖΕΙ ότι αυτό περιλαμβάνει εντοπισμό και μείωση στρατηγικών εξαρτήσεων και αύξηση της ανθεκτικότητας στα πιο ευαίσθητα βιομηχανικά οικοσυστήματα και ειδικούς τομείς. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι αυτό μπορεί να περιλαμβάνει διαφοροποίηση των αλυσίδων παραγωγής και εφοδιασμού, ενθάρρυνση και προσέλκυση επενδύσεων και παραγωγής στην Ευρώπη, διερεύνηση εναλλακτικών λύσεων και κυκλικών μοντέλων και προώθηση ευρείας βιομηχανικής συνεργασίας σε όλα τα κράτη μέλη.

6. Λαμβάνοντας υπόψη την έλλειψη ψηφιακών δεξιοτήτων και δεξιοτήτων κυβερνοασφάλειας στο εργατικό δυναμικό, ΤΟΝΙΖΕΙ ότι είναι σημαντικό να καλυφθεί η ζήτηση εκπαιδευμένου εργατικού δυναμικού στον τομέα της ψηφιακής τεχνολογίας και της κυβερνοασφάλειας, ιδίως με ανάπτυξη, διατήρηση και προσέλκυση των καλύτερων ταλέντων, για παράδειγμα μέσω εκπαίδευσης και κατάρτισης, ώστε να καταστεί δυνατή η ψηφιοποίηση της κοινωνίας μας υπό συνθήκες κυβερνοασφάλειας. ΕΝΘΑΡΡΥΝΕΙ τις γυναίκες και τα κορίτσια να έχουν αυξημένη συμμετοχή στην εκπαίδευση σε θετικές επιστήμες, τεχνολογία, μηχανική και μαθηματικά (STEM) και στην αναβάθμιση δεξιοτήτων για θέσεις εργασίας ΤΠΕ και την επανειδίκευση σε ψηφιακές δεξιότητες ως ένα από τα μέσα για να γεφυρωθεί το έμφυλο ψηφιακό χάσμα.

7. ΥΠΕΝΘΥΜΙΖΕΙ ότι η κοινή και ολοκληρωμένη προσέγγιση της ΕΕ στην κυβερνοδιπλωματία αποσκοπεί να συμβάλει στην πρόληψη συγκρούσεων, στον μετριασμό απειλών κατά της κυβερνοασφάλειας και στην ενίσχυση της σταθερότητας στις διεθνείς σχέσεις. Στο πλαίσιο αυτό, ΕΠΙΒΕΒΑΙΩΝΕΙ την προσήλωσή του στην επίλυση διεθνών διαφορών στον κυβερνοχώρο με ειρηνικά μέσα και ότι όλες οι διπλωματικές προσπάθειες της ΕΕ θα πρέπει, κατά προτεραιότητα, να επιδιώκουν να προωθήσουν την ασφάλεια και τη σταθερότητα στον κυβερνοχώρο μέσω αυξημένης διεθνούς συνεργασίας, καθώς και να μειώσουν τον κίνδυνο παρανοήσεων, κλιμάκωσης και συγκρούσεων που ενδέχεται να προκύψουν από περιστατικά ΤΠΕ, ΣΤΗΡΙΖΕΙ δε την περαιτέρω ανάπτυξη και εφαρμογή μέτρων οικοδόμησης εμπιστοσύνης σε περιφερειακό και διεθνές επίπεδο. ΕΠΑΝΑΛΑΜΒΑΝΕΙ την ομόφωνη έκκληση της Γενικής Συνέλευσης των Ηνωμένων Εθνών να καθοδηγούνται τα κράτη μέλη του ΟΗΕ από τις συστάσεις των εκθέσεων της UNGGE όταν χρησιμοποιούν ΤΠΕ και ΕΠΙΒΕΒΑΙΩΝΕΙ την εφαρμογή του διεθνούς δικαίου, ιδίως του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, στον κυβερνοχώρο.

8. ΕΠΙΒΕΒΑΙΩΝΕΙ ότι, προκειμένου να διαμορφωθούν ουσιωδώς διεθνείς κανόνες και πρότυπα στον χώρο των αναδυόμενων τεχνολογιών και της τεχνικής και λογικής υποδομής που είναι απαραίτητη για τη γενική διαθεσιμότητα και ακεραιότητα του δημόσιου πυρήνα του διαδικτύου, ώστε να συνάδουν με τις οικουμενικές αξίες και τις αξίες της ΕΕ, είναι απαραίτητη η περαιτέρω ανάπτυξη κανόνων και προτύπων εντός της Ένωσης, μέσω και μιας προσέγγισης πολλαπλών ενδιαφερομένων. Αυτό θα διασφαλίσει ότι το διαδίκτυο παραμένει παγκόσμιο, ανοικτό, ελεύθερο, σταθερό και ασφαλές και ότι η χρήση και ανάπτυξη ψηφιακών τεχνολογιών σέβεται τα ανθρώπινα δικαιώματα, η δε χρήση τους είναι νόμιμη, ασφαλής και δεοντολογική. ΣΗΜΕΙΩΝΕΙ την επικείμενη στρατηγική τυποποίησης και ΔΕΣΜΕΥΕΤΑΙ να αναλάβει προορατική και συντονισμένη δράση προβολής για να προωθήσει τον ηγετικό ρόλο της ΕΕ και τους στόχους της σε διεθνές επίπεδο, μεταξύ άλλων σε διάφορους διεθνείς οργανισμούς τυποποίησης και μέσω της συνεργασίας με ομοϊδεάτες εταίρους, την κοινωνία των πολιτών, την ακαδημαϊκή κοινότητα και τον ιδιωτικό τομέα.

9. ΣΤΗΡΙΖΕΙ ΣΘΕΝΑΡΑ το μοντέλο των πολλαπλών ενδιαφερομένων για τη διακυβέρνηση του διαδικτύου και την κυβερνοασφάλεια και δεσμεύεται να ενισχύσει τακτικές και διαρθρωμένες ανταλλαγές με ενδιαφερόμενα μέρη, περιλαμβανομένου του ιδιωτικού τομέα, της ακαδημαϊκής κοινότητας και της κοινωνίας των πολιτών σε διεθνή φόρουμ, μεταξύ άλλων στο πλαίσιο της Έκκλησης του Παρισιού για Εμπιστοσύνη και Ασφάλεια στον Κυβερνοχώρο. ΠΡΟΩΘΕΙ καθολική, οικονομικά προσιτή και ισότιμη πρόσβαση στο διαδίκτυο που να γεφυρώνει τα ψηφιακά χάσματα και, ειδικότερα, τη χειραφέτηση των γυναικών και των κοριτσιών και των ατόμων που βρίσκονται σε ευάλωτες ή περιθωριοποιημένες καταστάσεις, τόσο κατά την ανάπτυξη πολιτικής όσο και κατά τη χρήση του διαδικτύου.

10. ΤΟΝΙΖΕΙ την ανάγκη να περιληφθεί η κυβερνοασφάλεια στις ψηφιακές επενδύσεις και πρωτοβουλίες κατά τα προσεχή έτη και να επιτευχθούν σταδιακά ισότιμοι όροι ανταγωνισμού στον τομέα της κυβερνοασφάλειας και ΣΗΜΕΙΩΝΕΙ το σχέδιο της Επιτροπής για αύξηση δημόσιων δαπανών και μόχλευση ιδιωτικών επενδύσεων στο πεδίο της κυβερνοασφάλειας. ΕΠΙΣΗΜΑΙΝΕΙ τη σημασία των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ) στο οικοσύστημα της κυβερνοασφάλειας και ΑΝΑΓΝΩΡΙΖΕΙ τα σχετικά χρηματοδοτικά μέσα που είναι διαθέσιμα για να στηρίξουν μια ισχυρή εστίαση στην κυβερνοασφάλεια εντός του ψηφιακού μετασχηματισμού στη διάρκεια του πολυετούς δημοσιονομικού πλαισίου (ΠΔΠ) 2021-2027, καθώς και στον μηχανισμό ανάκαμψης και ανθεκτικότητας (RRF).

11. ΠΡΟΣΒΛΕΠΕΙ στην ταχεία εφαρμογή του κανονισμού σχετικά με το ευρωπαϊκό βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας και το δίκτυο εθνικών κέντρων συντονισμού (CCCN), περιλαμβανομένης της ταχείας σύστασης και θέσης σε λειτουργία του ευρωπαϊκού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας στο Βουκουρέστι. Η ταχεία έγκριση του θεματολογίου του θα συμβάλει στη μεγιστοποίηση των αποτελεσμάτων των επενδύσεων ώστε να ενισχυθεί ο ηγετικός ρόλος και η στρατηγική αυτονομία της Ένωσης στο πεδίο της κυβερνοασφάλειας και να στηριχθούν τεχνολογικές ικανότητες και δεξιότητες και να αυξηθεί η παγκόσμια ανταγωνιστικότητα της Ένωσης με συμβολή από τη βιομηχανία και τις ακαδημαϊκές κοινότητες στην κυβερνοασφάλεια, περιλαμβανομένων ΜΜΕ και ερευνητικών κέντρων, τα οποία θα επωφεληθούν από μια πιο συστηματική, συμπεριληπτική και στρατηγική συνεργασία, όσον αφορά τη συνοχή της Ένωσης και όλων των κρατών μελών της.

12. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για το συνεχιζόμενο έργο του ENISA, από κοινού με τα κράτη μέλη και τους ενδιαφερόμενους, με σκοπό να καταστούν διαθέσιμα στην ΕΕ συστήματα πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ που θα πρέπει να συμβάλλουν στην αύξηση του συνολικού επιπέδου κυβερνοασφάλειας εντός της ψηφιακής ενιαίας αγοράς. Στο πλαίσιο αυτό, ΠΡΟΣΒΛΕΠΕΙ στο κυλιόμενο πρόγραμμα εργασίας της Ένωσης με στόχο την ανάπτυξη ενωσιακών συστημάτων πιστοποίησης της κυβερνοασφάλειας στο πλαίσιο της πράξης για την κυβερνοασφάλεια (ΠΚΑ). ΑΝΑΓΝΩΡΙΖΕΙ, εν προκειμένω, τον κομβικό ρόλο της ΕΕ στην ανάπτυξη προτύπων που μπορούν να διαμορφώσουν το τοπίο της κυβερνοασφάλειας και που συντελούν στη διασφάλιση θεμιτού ανταγωνισμού εντός της ΕΕ και σε παγκόσμιο επίπεδο, προωθώντας την πρόσβαση στην αγορά, καθώς και αντιμετωπίζοντας τους κινδύνους για την ασφάλεια, διασφαλίζοντας παράλληλα τη δυνατότητα εφαρμογής του νομοθετικού πλαισίου της ΕΕ.

13. ΕΠΑΝΑΛΑΜΒΑΝΕΙ ότι είναι σημαντικό να εξεταστεί αν απαιτείται να θεσπιστεί μακροπρόθεσμα οριζόντια νομοθεσία, η οποία θα ορίζει επίσης τους αναγκαίους όρους διάθεσης στην αγορά, για την κάλυψη όλων των συναφών πτυχών της κυβερνοασφάλειας των συνδεδεμένων συσκευών, όπως η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα. ΘΕΩΡΕΙ ΕΥΠΡΟΣΔΕΚΤΗ, στο πλαίσιο αυτό, μια διερευνητική συζήτηση σχετικά με το πεδίο εφαρμογής τέτοιας νομοθεσίας και της συνάρτησής της με το πλαίσιο πιστοποίησης της κυβερνοασφάλειας, όπως ορίζεται στην ΠΚΑ, με σκοπό την αύξηση του επιπέδου ασφάλειας εντός της ψηφιακής ενιαίας αγοράς. ΤΟΝΙΖΕΙ ότι οι απαιτήσεις κυβερνοασφάλειας θα πρέπει να ορίζονται σύμφωνα με τη σχετική ενωσιακή νομοθεσία, συμπεριλαμβανομένης της ΠΚΑ, του νέου νομοθετικού πλαισίου, του κανονισμού για την ευρωπαϊκή τυποποίηση και της πιθανής μελλοντικής οριζόντιας νομοθεσίας, ώστε να αποφεύγεται η νομοθετική ασάφεια και ο κατακερματισμός.

14. ΑΝΑΓΝΩΡΙΖΕΙ τη σημασία μιας ολοκληρωμένης και οριζόντιας προσέγγισης της κυβερνοασφάλειας στην Ένωση, με πλήρη σεβασμό των αρμοδιοτήτων και των αναγκών των κρατών μελών, καθώς και τη σημασία της συνεχούς στήριξης για τεχνική βοήθεια και συνεργασία ώστε να αναπτυχθούν οι ικανότητες των κρατών μελών. Λαμβάνοντας υπόψη την εξέλιξη του τοπίου των κυβερνοαπειλών, ΣΗΜΕΙΩΝΕΙ τη νέα πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, η οποία βασίζεται στην οδηγία ΑΔΠ, και ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη στήριξή του για την ενίσχυση και την εναρμόνιση των εθνικών πλαισίων κυβερνοασφάλειας και τη σταθερή συνεργασία μεταξύ των κρατών μελών. Επιπλέον, ΤΟΝΙΖΕΙ την ανάγκη ευθυγράμμισης και συνάρθρωσης της τομεακής νομοθεσίας στον τομέα αυτό.

15. ΣΗΜΕΙΩΝΕΙ την πρόταση της Επιτροπής να στηριχθούν τα κράτη μέλη στη δημιουργία και την ενίσχυση κέντρων επιχειρήσεων ασφαλείας (ΚΕΑ) ώστε να συγκροτηθεί ένα δίκτυο ΕΠΣ σε ολόκληρη την ΕΕ, για την περαιτέρω παρακολούθηση και πρόβλεψη των σημάτων επιθέσεων σε δίκτυα. Στο πλαίσιο αυτό, ΑΝΑΜΕΝΕΙ τα λεπτομερή σχέδια της Επιτροπής σχετικά με το δίκτυο ΚΕΑ, σεβόμενο παράλληλα τις αρμοδιότητες των κρατών μελών. ΥΠΕΝΘΥΜΙΖΕΙ τις προσπάθειες που καταβάλλουν τα κράτη μέλη, με την υποστήριξη της ΕΕ, για τη δημιουργία τομεακών, εθνικών και περιφερειακών CSIRT και εθνικών ή ευρωπαϊκών κέντρων ανταλλαγής και ανάλυσης πληροφοριών (ISAC) στο πλαίσιο ενός αποτελεσματικού δικτύου εταιρικών σχέσεων για την κυβερνοασφάλεια στην Ένωση. ΠΡΟΣΒΛΕΠΕΙ στη διερεύνηση των δυνατοτήτων του δικτύου αυτού να ενισχύσει τα ΚΕΑ, καθώς και στη συμπληρωματικότητα και τον συντονισμό τους με υφιστάμενα δίκτυα και φορείς (κυρίως το δίκτυο CSIRT), προκειμένου να προωθηθεί μια αποτελεσματική, ασφαλής και αξιόπιστη νοοτροπία κοινοχρησίας πληροφοριών. ΤΟΝΙΖΕΙ ότι η διαδικασία αυτή θα βασιστεί στο έργο που επιτελείται στο πλαίσιο των πρωτοβουλιών για την τεχνητή νοημοσύνη και την υπολογιστική υψηλών επιδόσεων και από τους ευρωπαϊκούς κόμβους ψηφιακής καινοτομίας.

16. ΣΗΜΕΙΩΝΕΙ την πιθανή ανάπτυξη ενός ασφαλούς συστήματος συνδεσιμότητας, με βάση την ευρωπαϊκή υποδομή κβαντικής επικοινωνίας (EuroQCI) και τις κυβερνητικές δορυφορικές επικοινωνίες της Ευρωπαϊκής Ένωσης (GOVSATCOM), και ΑΝΑΓΝΩΡΙΖΕΙ ότι οποιαδήποτε μελλοντική πιθανή ανάπτυξη θα πρέπει να βασίζεται σε ένα στιβαρό πλαίσιο κυβερνοασφάλειας και να λαμβάνει υπόψη ολόκληρη την υποδομή ηλεκτρονικών επικοινωνιών, όπως τα διαστημικά, τα επίγεια και τα υποβρύχια συστήματα δικτύων.

17. ΠΡΟΣΒΛΕΠΕΙ σε συζητήσεις με την Επιτροπή, τον ENISA, τους δύο διαχειριστές εξυπηρετητή ρίζας DNS της ΕΕ και την πολυσυμμετοχική κοινότητα για την αξιολόγηση του ρόλου των δύο διαχειριστών εξυπηρετητή ρίζας DNS της ΕΕ όσον αφορά τη διασφάλιση ότι το διαδίκτυο παραμένει παγκοσμίως προσβάσιμο και μη κατακερματισμένο. ΘΕΩΡΕΙ ΕΥΠΡΟΣΔΕΚΤΕΣ περαιτέρω συζητήσεις σχετικά με την πρόθεση της Επιτροπής να αναπτύξει μια εναλλακτική ευρωπαϊκή υπηρεσία για πρόσβαση στο παγκόσμιο διαδίκτυο (πρωτοβουλία «DNS4EU»), η οποία θα βασίζεται σε ένα διαφανές μοντέλο που θα συμμορφώνεται με τα τελευταία πρότυπα και κανόνες για την ασφάλεια, την προστασία των δεδομένων και της ιδιωτικής ζωής εκ σχεδιασμού και εξ ορισμού, προκειμένου να συμβάλει στην αύξηση της ανθεκτικότητας, διατηρώντας και ενισχύοντας παράλληλα τη διεθνή συνδεσιμότητα για όλα τα κράτη μέλη.

18. ΑΝΑΓΝΩΡΙΖΕΙ την ανάγκη να καταβληθούν κοινές προσπάθειες από την Επιτροπή και τα κράτη μέλη ώστε να επιταχυνθεί η υιοθέτηση βασικών προτύπων για το διαδίκτυο, συμπεριλαμβανομένου του IPv6, και καθιερωμένων προτύπων ασφάλειας για το διαδίκτυο, δεδομένου ότι αυτά συμβάλλουν καθοριστικά στην αύξηση του συνολικού επιπέδου ασφάλειας, ανθεκτικότητας και διαλειτουργικότητας του παγκόσμιου διαδικτύου, καθώς και στο περαιτέρω άνοιγμά του, αυξάνοντας παράλληλα την ανταγωνιστικότητα της ενωσιακής βιομηχανίας και ιδίως των φορέων εκμετάλλευσης διαδικτυακών υποδομών.

19. ΤΟΝΙΖΕΙ τη σημασία μιας συντονισμένης προσέγγισης, καθώς και της ανάπτυξης και εφαρμογής αποτελεσματικών μέτρων σε εθνικό επίπεδο για την ενίσχυση της κυβερνοασφάλειας των δικτύων 5G. ΥΠΟΣΤΗΡΙΖΕΙ τα επόμενα βήματα που πρέπει να γίνουν για την κυβερνοασφάλεια των δικτύων 5G, όπως παρουσιάζονται στο προσάρτημα της στρατηγικής της ΕΕ για την κυβερνοασφάλεια και με βάση τα αποτελέσματα της έκθεσης σχετικά με τον αντίκτυπο της σύστασης της Επιτροπής για την ασφάλεια των δικτύων 5G, για παράδειγμα όσον αφορά τον καθορισμό μακροπρόθεσμης και ολοκληρωμένης προσέγγισης που θα εξετάζει ολόκληρη την αξιακή αλυσίδα και το οικοσύστημα 5G. Με σκοπό την περαιτέρω ενίσχυση της συντονισμένης προσέγγισης για την ασφάλεια των δικτύων 5G, ΠΡΟΤΡΕΠΕΙ τα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και άλλους σχετικούς ενδιαφερόμενους φορείς να συνεχίσουν τον περιοδικό απολογισμό τους, σε συνδυασμό με την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών στο πλαίσιο του ειδικού προγράμματος εργασιών της ομάδας συνεργασίας NIS για την κυβερνοασφάλεια 5G, καθώς και να υποβάλλουν τακτικά εκθέσεις στο Συμβούλιο σχετικά με την πρόοδο που σημειώνεται. ΤΟΝΙΖΕΙ, δίνοντας παράλληλα έμφαση στην ευθύνη των κρατών μελών για την προστασία της εθνικής ασφάλειας, την ισχυρή του δέσμευση να εφαρμόσει και να ολοκληρώσει ταχέως την εφαρμογή των μέτρων της εργαλειοθήκης 5G της ΕΕ και να συνεχίσει τις προσπάθειες που καταβάλλονται για την εγγύηση της ασφάλειας των δικτύων 5G και την ανάπτυξη των μελλοντικών γενεών δικτύων. Η στενή συνεργασία μεταξύ των κρατών μελών, της Επιτροπής και του ENISA για την ασφάλεια των δικτύων 5G θα μπορούσε να χρησιμεύσει ως παράδειγμα για άλλα ζητήματα στον τομέα της κυβερνοασφάλειας, με ταυτόχρονο σεβασμό των αρμοδιοτήτων των κρατών μελών και των αρχών της επικουρικότητας και της αναλογικότητας.

20. ΑΝΑΓΝΩΡΙΖΕΙ τη σημασία της περαιτέρω ενσωμάτωσης της κυβερνοασφάλειας στους μηχανισμούς της ΕΕ για την αντιμετώπιση κρίσεων και της δοκιμής τους σε σχετικές ασκήσεις, ΤΟΝΙΖΕΙ δε τη σημασία της ενίσχυσης της συνεργασίας και της κοινοχρησίας πληροφοριών μεταξύ των διαφόρων κοινοτήτων στον κυβερνοχώρο εντός της ΕΕ και της διασύνδεσης των υφιστάμενων πρωτοβουλιών, δομών και διαδικασιών (όπως οι IPCR, το δίκτυο CSIRT, η ομάδα συνεργασίας NIS, το CyCLONe, το ευρωπαϊκό κέντρο για τα εγκλήματα στον κυβερνοχώρο, το INTCEN της ΕΕ και άλλοι σχετικοί οργανισμοί της ΕΕ) σε περίπτωση περιστατικών και απειλών μεγάλης κλίμακας και διασυνοριακού χαρακτήρα. ΛΑΜΒΑΝΟΝΤΑΣ ΥΠΟΨΗ την πρόοδο που έχει ήδη επιτευχθεί στον τομέα αυτό, ΑΝΑΜΕΝΕΙ την πρόταση της Επιτροπής σχετικά με τη διαδικασία, τα ορόσημα και το χρονοδιάγραμμα για τον καθορισμό της κοινής μονάδας κυβερνοχώρου προκειμένου να παρασχεθεί προστιθέμενη αξία και σαφής εστίαση και να εξορθολογιστεί το ενωσιακό πλαίσιο διαχείρισης κρίσεων κυβερνοασφάλειας, μεταξύ άλλων μέσω της ετοιμότητας, της κοινής επίγνωσης της κατάστασης, της ενίσχυσης της συντονισμένης αντίδρασης και των ασκήσεων, με διαφανή και βαθμιαίο τρόπο, αποφεύγοντας παράλληλα τις επαναλήψεις και τις αλληλεπικαλύψεις και με σεβασμό των αρμοδιοτήτων των κρατών μελών.

21. ΤΟΝΙΖΕΙ τόσο τη σημασία της προώθησης της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των σχετικών φορέων κυβερνοασφάλειας και των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης —π.χ. των αρχών επιβολής του νόμου και των δικαστικών αρχών— όσο και την ανάγκη επέκτασης και βελτίωσης της ικανότητας των εν λόγω αρχών να διερευνούν και να διώκουν κυβερνοεγκλήματα και να προωθούν τις διεθνείς διαπραγματεύσεις και τους κανόνες της ΕΕ για τη διασυνοριακή πρόσβαση σε ψηφιακά πειστήρια. Ανεξάρτητα από το εκάστοτε τεχνολογικό πλαίσιο, έχει ουσιώδη σημασία να διαφυλαχθούν οι εξουσίες των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης μέσω νόμιμης πρόσβασης για την εκτέλεση των καθηκόντων τους, όπως προβλέπεται και επιτρέπεται από τον νόμο. Κάθε τέτοιος νόμος ο οποίος προβλέπει εξουσίες επιβολής πρέπει πάντα να σέβεται πλήρως την τήρηση της προσήκουσας διαδικασίας και άλλες εγγυήσεις, καθώς και τα θεμελιώδη δικαιώματα, ιδίως το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα.

22. ΕΠΙΒΕΒΑΙΩΝΕΙ ΕΚ ΝΕΟΥ τη στήριξή του στην ανάπτυξη, την εφαρμογή και τη χρήση ισχυρής κρυπτογράφησης ως αναγκαίου μέσου για την προστασία των θεμελιωδών δικαιωμάτων και της ψηφιακής ασφάλειας των ατόμων, των κυβερνήσεων, της βιομηχανίας και της κοινωνίας και, ταυτόχρονα, ΑΝΑΓΝΩΡΙΖΕΙ την ανάγκη να διασφαλιστεί η ικανότητα των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης — π.χ. των αρχών επιβολής του νόμου και των δικαστικών αρχών— να ασκούν τις νόμιμες εξουσίες τους, τόσο στο διαδίκτυο όσο και εκτός διαδικτύου, για την προστασία των κοινωνιών και των πολιτών μας. Οι αρμόδιες αρχές πρέπει να μπορούν να έχουν πρόσβαση στα δεδομένα με νόμιμο και στοχευμένο τρόπο, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων και των σχετικών νόμων περί προστασίας των δεδομένων, διαφυλάσσοντας παράλληλα την κυβερνοασφάλεια. ΤΟΝΙΖΕΙ ότι κάθε δράση που αναλαμβάνεται πρέπει να σταθμίζει προσεκτικά τα συμφέροντα αυτά με τις αρχές της αναγκαιότητας, της αναλογικότητας και της επικουρικότητας.

23. ΥΠΟΣΤΗΡΙΖΕΙ και ΠΡΟΩΘΕΙ τη σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, καθώς και τις εν εξελίξει εργασίες για το δεύτερο πρόσθετο πρωτόκολλο της σύμβασης αυτής. Επιπλέον, εξακολουθεί να συμμετέχει σε πολυμερείς ανταλλαγές σχετικά με το κυβερνοέγκλημα, μεταξύ άλλων σε διαδικασίες που σχετίζονται με το Συμβούλιο της Ευρώπης, το Γραφείο των Ηνωμένων Εθνών για τον Έλεγχο των Ναρκωτικών και την Πρόληψη του Εγκλήματος (UNODC) και την Επιτροπή για την Πρόληψη του Εγκλήματος και την Ποινική Δικαιοσύνη (CCPCJ), ώστε να εξασφαλιστεί ενισχυμένη διεθνής συνεργασία για την καταπολέμηση του κυβερνοεγκλήματος, συμπεριλαμβανομένης της ανταλλαγής βέλτιστων πρακτικών και τεχνικών γνώσεων και της στήριξης της ανάπτυξης ικανοτήτων, με παράλληλο σεβασμό, προώθηση και προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών.

24. Ενώ η εθνική ασφάλεια παραμένει αποκλειστικά ευθύνη κάθε κράτους μέλους, ΑΝΑΓΝΩΡΙΖΕΙ τη σημασία της συνεργασίας στον τομέα των στρατηγικών πληροφοριών σχετικά με απειλές και δραστηριότητες στον κυβερνοχώρο και ΚΑΛΕΙ τα κράτη μέλη, μέσω των αρμόδιων αρχών τους, να συνεχίσουν να συμβάλλουν στο έργο του INTCEN της ΕΕ ως κόμβου για την επίγνωση της κατάστασης και την αξιολόγηση απειλών σε θέματα κυβερνοχώρου στην ΕΕ και να μελετήσουν την πρόταση για ενδεχόμενη σύσταση ομάδας εργασίας των κρατών μελών για τις πληροφορίες στον κυβερνοχώρο, προκειμένου να ενισχυθεί η ειδική ικανότητα του INTCEN σε αυτόν τον τομέα, με βάση σχετικές εθελοντικές συνεισφορές των κρατών μελών και χωρίς να θίγονται οι αρμοδιότητές τους.

25. ΥΠΟΓΡΑΜΜΙΖΕΙ τη σημασία ενός στέρεου και συνεκτικού πλαισίου ασφάλειας για την προστασία όλου του προσωπικού, των δεδομένων, των δικτύων επικοινωνιών, των συστημάτων πληροφοριών και των διαδικασιών λήψης αποφάσεων της ΕΕ βάσει σφαιρικών, συνεπών και ομοιογενών κανόνων. Ειδικότερα, αυτό θα πρέπει να επιτευχθεί με την ενίσχυση της ανθεκτικότητας και τη βελτίωση της νοοτροπίας ασφάλειας της ΕΕ έναντι των κυβερνοαπειλών και με την ισχυροποίηση της ασφάλειας των διαβαθμισμένων και μη διαβαθμισμένων δικτύων της ΕΕ, εξασφαλίζοντας παράλληλα την κατάλληλη διακυβέρνηση και τη διάθεση επαρκών πόρων και ικανοτήτων, μεταξύ άλλων στο πλαίσιο της ενίσχυσης της εντολής της CERT-EU. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ, στο πλαίσιο αυτό, για τις εν εξελίξει συζητήσεις με αντικείμενο τη θέσπιση κοινών κανόνων για την ασφάλεια των πληροφοριών, λαμβάνοντας δεόντως υπόψη τους κανόνες ασφαλείας του Συμβουλίου για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ, καθώς και τον καθορισμό κοινών δεσμευτικών κανόνων για την κυβερνοασφάλεια για όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ.

26. ΜΕ ΒΑΣΗ τις προσπάθειες της ΕΕ για διπλωματία στον κυβερνοχώρο, ΔΕΣΜΕΥΕΤΑΙ να αυξήσει την αποτελεσματικότητα και την αποδοτικότητα της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο και ΠΡΟΣΒΛΕΠΕΙ στην εμβάθυνση των συζητήσεων σχετικά με το πεδίο εφαρμογής και τη χρήση της, που να αξιοποιεί τα διδάγματα από την εφαρμογή του μέσου αυτού μέχρι σήμερα. Οι συζητήσεις αυτές θα πρέπει να συντελούν στην προαγωγή της ασφάλειας σε διεθνές επίπεδο με την προώθηση του διαλόγου και την καλλιέργεια ενός κοινού οράματος σε θέματα κυβερνοασφάλειας, την ενίσχυση της πρόληψης, της σταθερότητας, της συνεργασίας, την προώθηση της εμπιστοσύνης και της δημιουργίας ικανοτήτων και, όπου απαιτείται, την εφαρμογή περιοριστικών μέτρων, με σκοπό την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο που στοχεύουν στην ακεραιότητα και την ασφάλεια της ΕΕ και των κρατών μελών της, συμβάλλοντας με τον τρόπο αυτό στη διεθνή ασφάλεια και σταθερότητα και εδραιώνοντας τη στάση της ΕΕ στον κυβερνοχώρο, με πλήρη σεβασμό των εθνικών αρμοδιοτήτων και προνομίων. Ειδικότερα, θα πρέπει να δοθεί ιδιαίτερη προσοχή στην πρόληψη και την αντιμετώπιση κυβερνοεπιθέσεων με συστημικές συνέπειες που ενδέχεται να επηρεάσουν τις αλυσίδες εφοδιασμού, τις υποδομές ζωτικής σημασίας και τις βασικές υπηρεσίες, τους δημοκρατικούς θεσμούς και διαδικασίες καθώς και να υπονομεύσουν την οικονομική μας ασφάλεια, συμπεριλαμβανομένης της κλοπής διανοητικής ιδιοκτησίας μέσω του κυβερνοχώρου. Τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ θα πρέπει επίσης να εξετάσουν περαιτέρω τη συνάρθρωση μεταξύ του ενωσιακού πλαισίου διαχείρισης κρίσεων κυβερνοασφάλειας, της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο και των διατάξεων του άρθρου 42 παράγραφος 7 της ΣΕΕ και του άρθρου 222 της ΣΛΕΕ, ιδίως μέσω εργασιών βάσει σεναρίων για την ανάπτυξη κοινής αντίληψης των πρακτικών λεπτομερειών εφαρμογής του άρθρου 42 παράγραφος 7 της ΣΕΕ.

27. ΑΝΑΓΝΩΡΙΖΕΙ τη σημασία της ενίσχυσης της συνεργασίας με διεθνείς οργανισμούς και χώρες-εταίρους προκειμένου να προωθηθεί η κοινή αντίληψη του τοπίου των κυβερνοαπειλών, να αναπτυχθούν διάλογοι και μηχανισμοί συνεργασίας, να προσδιοριστούν, όπου κρίνεται σκόπιμο, συνεργατικές διπλωματικές αντιδράσεις, καθώς και να βελτιωθεί η κοινοχρησία πληροφοριών, μεταξύ άλλων μέσω εκπαίδευσης, κατάρτισης και ασκήσεων. Ειδικότερα, ΤΟΝΙΖΕΙ ότι μια ισχυρή διατλαντική εταιρική σχέση στον τομέα της κυβερνοασφάλειας συμβάλλει στην κοινή μας ασφάλεια, σταθερότητα και ευημερία και ΣΗΜΕΙΩΝΕΙ τις διατάξεις της συμφωνίας εμπορίου και συνεργασίας ΕΕ-Ηνωμένου Βασιλείου για τη συνεργασία στον τομέα της κυβερνοασφάλειας. Υπενθυμίζοντας τα κυριότερα επιτεύγματα της συνεργασίας ΕΕ-ΝΑΤΟ στον τομέα της κυβερνοασφάλειας στο πλαίσιο της εφαρμογής των κοινών δηλώσεων της Βαρσοβίας του 2016 και των Βρυξελλών του 2018, επαναλαμβάνει τη σημασία της ενισχυμένης, αμοιβαία ενισχυτικής και επωφελούς συνεργασίας μέσω εκπαίδευσης, κατάρτισης, ασκήσεων και συντονισμένης αντίδρασης σε κακόβουλες δραστηριότητες στον κυβερνοχώρο, με πλήρη σεβασμό της αυτονομίας και των διαδικασιών λήψης αποφάσεων των δύο οργανισμών, με βάση τις αρχές της διαφάνειας, της αμοιβαιότητας και της συμπεριληπτικότητας.

28. Προκειμένου να συμβάλει σε έναν παγκόσμιο, ανοικτό, ελεύθερο, σταθερό και ασφαλή κυβερνοχώρο, η σημασία του οποίου για τη συνεχιζόμενη ευμάρεια, ανάπτυξη, ασφάλεια, ευημερία, συνδεσιμότητα και ακεραιότητα των κοινωνιών μας αυξάνεται διαρκώς, ΔΕΣΜΕΥΕΤΑΙ να συνεχίσει να συμμετέχει σε διαδικασίες καθορισμού προτύπων σε διεθνείς οργανισμούς, ιδίως στις διαδικασίες που σχετίζονται με την πρώτη επιτροπή του ΟΗΕ, προωθώντας και συμβάλλοντας στην αναγνώριση της εφαρμογής του διεθνούς δικαίου στον κυβερνοχώρο και στην τήρηση των προτύπων, των κανόνων και των αρχών της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο, μεταξύ άλλων προωθώντας τον ταχύ καθορισμό προγράμματος δράσης για την προαγωγή της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο, ως εποικοδομητικής, βασισμένης στη συναίνεση και χωρίς αποκλεισμούς συνέχειας σε αμφότερες τις εν εξελίξει διαδικασίες GGE και OEWG του ΟΗΕ.

29. ΥΠΕΝΘΥΜΙΖΕΙ την ισχυρή δέσμευσή του στην αποτελεσματική πολυμέρεια και σε μια παγκόσμια τάξη βασισμένη σε κανόνες με τα Ηνωμένα Έθνη στον πυρήνα της και την αποφασιστικότητά του να ενισχύσει τη συνεργασία και τον συντονισμό με διεθνείς και περιφερειακούς οργανισμούς, συγκεκριμένα το σύστημα του ΟΗΕ, το ΝΑΤΟ, το Συμβούλιο της Ευρώπης, τον ΟΑΣΕ, τον ΟΟΣΑ, την ΑΕ, τον ΟΑΚ, τον ASEAN, το ARF, το ΣΣΚ και τον ΣΑΚ με αντικείμενο συζητήσεις για θέματα που αφορούν τον κυβερνοχώρο, καθώς και τη συνέχιση και επέκταση των διαρθρωμένων διαλόγων και διαβουλεύσεων της ΕΕ για τον κυβερνοχώρο με τρίτες χώρες. ΤΟΝΙΖΕΙ την ενεργό υποστήριξή του προς τον ΟΗΕ, ιδίως σε σχέση με το θεματολόγιο του 2030, συμπεριλαμβανομένων των στόχων βιώσιμης ανάπτυξης, και ΔΕΧΕΤΑΙ ΜΕ ΙΚΑΝΟΠΟΙΗΣΗ τον χάρτη πορείας του Γενικού Γραμματέα του ΟΗΕ για την ψηφιακή συνεργασία και το θεματολόγιο του Γενικού Γραμματέα του ΟΗΕ για τον αφοπλισμό, ο οποίος ενισχύει τη λογοδοσία και την τήρηση των κανόνων στον κυβερνοχώρο και συμβάλλει στην πρόληψη και την ειρηνική διευθέτηση των συγκρούσεων που προκύπτουν από κακόβουλες δραστηριότητες στον κυβερνοχώρο. ΔΕΧΕΤΑΙ ΜΕ ΙΚΑΝΟΠΟΙΗΣΗ την πρόταση να δημιουργηθεί άτυπο δίκτυο κυβερνοδιπλωματίας της ΕΕ από τον ύπατο εκπρόσωπο για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας με σκοπό την περαιτέρω δέσμευση και την ανάπτυξη εμπειρογνωμοσύνης από την ΕΕ και τα κράτη μέλη σε διεθνή ζητήματα κυβερνοχώρου, προκειμένου να ενισχυθεί η συντονισμένη δράση προβολής.

30. ΠΡΟΣΒΛΕΠΕΙ στην επικείμενη πρόταση αναθεώρησης του πλαισίου πολιτικής για την άμυνα στον κυβερνοχώρο και ΔΕΣΜΕΥΕΤΑΙ να συνεχίσει τις προσπάθειες για την ενίσχυση των διαστάσεων κυβερνοασφάλειας και κυβερνοάμυνας, ώστε να διασφαλιστεί η πλήρης ενσωμάτωσή τους στον ευρύτερο τομέα της ασφάλειας και της άμυνας, ιδίως στο πλαίσιο των εργασιών για τον στρατηγικό προσανατολισμό. ΘΕΩΡΕΙ ότι το προσδοκώμενο «Στρατιωτικό όραμα και στρατηγική για τον κυβερνοχώρο ως τομέα επιχειρήσεων» θα συμβάλει στην προώθηση αυτών των συζητήσεων. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για την πρωτοβουλία του Ευρωπαϊκού Οργανισμού Άμυνας να τονώσει τη συνεργασία μεταξύ στρατιωτικών CERT και ΣΤΗΡΙΖΕΙ τις προσπάθειες που καταβάλλονται για την ενίσχυση των πολιτικοστρατιωτικών συνεργειών και του συντονισμού στην κυβερνοάμυνα και την κυβερνοασφάλεια, συμπεριλαμβανομένων πτυχών που αφορούν το διάστημα, μεταξύ άλλων μέσω των ειδικών έργων PESCO.

31. ΔΕΧΕΤΑΙ ΜΕ ΙΚΑΝΟΠΟΙΗΣΗ την πρόταση να αναπτυχθεί ένα θεματολόγιο της ΕΕ για την ανάπτυξη εξωτερικών ικανοτήτων στον κυβερνοχώρο, την πρόταση να δημιουργηθεί ένα συμβούλιο της ΕΕ για την ανάπτυξη ικανοτήτων στον κυβερνοχώρο και τη σύσταση και εφαρμογή του CyberNet της ΕΕ (δίκτυο της ΕΕ για την ανάπτυξη ικανοτήτων στον κυβερνοχώρο) ώστε να αυξηθούν παγκοσμίως η ανθεκτικότητα και οι ικανότητες στον κυβερνοχώρο. Στο πλαίσιο αυτό, ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για τη συνεργασία με τα κράτη μέλη, καθώς και με εταίρους του δημόσιου και του ιδιωτικού τομέα, ιδίως το παγκόσμιο φόρουμ για την εμπειρογνωμοσύνη στον κυβερνοχώρο (GFCE) και άλλους σχετικούς διεθνείς οργανισμούς, ώστε να εξασφαλιστεί ο συντονισμός και να αποφευχθούν οι αλληλεπικαλύψεις. Ειδικότερα, ΕΝΘΑΡΡΥΝΕΙ τη συνεργασία με εταίρους στα Δυτικά Βαλκάνια και στις ανατολικές και νότιες γειτονικές χώρες της ΕΕ.

32. Για να εξασφαλιστεί ότι όλες οι χώρες είναι σε θέση να αποκομίσουν τα κοινωνικά, οικονομικά και πολιτικά οφέλη του διαδικτύου και της χρήσης των τεχνολογιών, ΔΕΣΜΕΥΕΤΑΙ να βοηθήσει τις χώρες-εταίρους να αντιμετωπίσουν την αυξανόμενη πρόκληση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, ιδίως εκείνων που βλάπτουν την ανάπτυξη των οικονομιών ή των κοινωνιών τους και την ακεραιότητα και την ασφάλεια των δημοκρατικών συστημάτων τους, μεταξύ άλλων παράλληλα με τις προσπάθειες στο πλαίσιο του ευρωπαϊκού σχεδίου δράσης για τη δημοκρατία.

33. Προκειμένου να διασφαλιστεί η ανάπτυξη, η εφαρμογή και η παρακολούθηση των προτάσεων που παρουσιάζονται στη στρατηγική της ΕΕ για την κυβερνοασφάλεια, και λαμβανομένου υπόψη του πολυετούς χαρακτήρα ορισμένων από τις πρωτοβουλίες, ΕΝΘΑΡΡΥΝΕΙ την Επιτροπή και τον ύπατο εκπρόσωπο για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας να καταρτίσουν λεπτομερές σχέδιο εφαρμογής που θα καθορίζει τις προτεραιότητες και το χρονοδιάγραμμα των προγραμματισμένων δράσεων. Θα ΠΑΡΑΚΟΛΟΥΘΕΙ την πρόοδο στην εφαρμογή των παρόντων συμπερασμάτων μέσω σχεδίου δράσης το οποίο θα επανεξετάζεται και θα επικαιροποιείται τακτικά από το Συμβούλιο σε στενή συνεργασία με την Ευρωπαϊκή Επιτροπή και τον ύπατο εκπρόσωπο.