Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 20 Νοεμβρίου 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	20 Νοεμβρίου 2017
Αποδέκτης:	Αντιπροσωπίες
αριθ. προηγ. εγγρ.:	13943/17 + COR 1
Αριθ. εγγρ. Επιτρ.:	12210/17, 12211/17
Θέμα:	Συμπεράσματα του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ - Συμπεράσματα του Συμβουλίου (20 Νοεμβρίου 2017)

Διαβιβάζονται συνημμένως στις αντιπροσωπίες τα συμπεράσματα του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ, τα οποία εγκρίθηκαν από το Συμβούλιο Γενικών Υποθέσεων στις 20 Νοεμβρίου 2017.

ΠΑΡΑΡΤΗΜΑ

Σχέδιο συμπερασμάτων του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ

Το Συμβούλιο της Ευρωπαϊκής Ένωσης,

1. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ τη σημασία της ασφάλειας στον κυβερνοχώρο για την ευημερία, την ανάπτυξη και την ασφάλεια της ΕΕ και την ακεραιότητα των ελεύθερων και δημοκρατικών κοινωνιών μας και των σχετικών διαδικασιών στην ψηφιακή εποχή, τόσο με την προστασία του κράτους δικαίου όσο και των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών κάθε ατόμου·

2. ΥΠΟΓΡΑΜΜΙΖΟΝΤΑΣ την ανάγκη να αντιμετωπιστεί η ασφάλεια στον κυβερνοχώρο με μια συνεκτική προσέγγιση σε εθνικό, ενωσιακό και παγκόσμιο επίπεδο, δεδομένου ότι οι απειλές στον κυβερνοχώρο μπορούν να έχουν συνέπειες για τη δημοκρατία, την ευημερία, τη σταθερότητα και την ασφάλεια·

3. ΕΠΙΣΗΜΑΙΝΕΙ ότι ένα υψηλό επίπεδο ανθεκτικότητας στον κυβερνοχώρο σε ολόκληρη την ΕΕ είναι επίσης σημαντικό για να επιτευχθεί η εμπιστοσύνη στην ενιαία ψηφιακή αγορά και την περαιτέρω ανάπτυξη μιας ψηφιακής Ευρώπης·

4. ΕΠΑΝΑΛΑΜΒΑΝΟΝΤΑΣ ότι η ΕΕ θα προωθεί συστηματικά ένα ανοικτό, παγκόσμιας εμβέλειας, ελεύθερο, ειρηνικό και ασφαλές κυβερνοχώρου, όπου τα ανθρώπινα δικαιώματα και οι θεμελιώδεις ελευθερίες, ειδικότερα δε το δικαίωμα της ελευθερίας της έκφρασης, η πρόσβαση σε πληροφορίες, η προστασία των δεδομένων, η ιδιωτική ζωή και η ασφάλεια, καθώς και οι βασικές αξίες και αρχές της ΕΕ, τόσο εντός της ΕΕ όσο και σε παγκόσμιο επίπεδο, εφαρμόζονται και τηρούνται πλήρως και ΥΠΟΓΡΑΜΜΙΖΟΝΤΑΣ τη ζωτική σημασία της διασφάλισης κατάλληλης ισορροπίας μεταξύ των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών, καθώς και της τήρησης των απαιτήσεων της πολιτικής εσωτερικής ασφάλειας της ΕΕ[1],

5. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ ότι το διεθνές δίκαιο, συμπεριλαμβανομένων του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, του διεθνούς ανθρωπιστικού δικαίου και του δικαίου ανθρωπίνων δικαιωμάτων εφαρμόζονται στον κυβερνοχώρο και, ως εκ τούτου, ΤΟΝΙΖΟΝΤΑΣ την ανάγκη να συνεχιστούν οι προσπάθειες για να διασφαλιστεί ότι τηρείται το διεθνές δίκαιο στον κυβερνοχώρο·

[1] Έγγρ. 12650/17.

6. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με την στρατηγική της ΕΕ για τον κυβερνοχώρο[2], για τη διακυβέρνηση του διαδικτύου[3], για την ενίσχυση της ανθεκτικότητας της ΕΕ[4], για τη διπλωματία στον κυβερνοχώρο[5] και σχετικά με ένα πλαίσιο για κοινή διπλωματική ενωσιακή αντιμετώπιση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο[6], για τη βελτίωση της ποινικής δικαιοσύνης στον κυβερνοχώρο[7], για την ασφάλεια και την άμυνα στο πλαίσιο της Παγκόσμιας Στρατηγικής της ΕΕ[8], σχετικά με το κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών[9] και για την ενδιάμεση επανεξέταση της ανανεωμένης Στρατηγικής Εσωτερικής Ασφάλειας της Ευρωπαϊκής Ένωσης για την περίοδο 2015-2020[10]·

7. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ ότι το πλαίσιο που παρέχεται από τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης), παρέχει μια ισχυρή βάση μεταξύ μιας διαφοροποιημένης ομάδας χωρών για τη χρησιμοποίηση ενός αποτελεσματικού νομικού προτύπου για τις διάφορες εθνικές νομοθεσίες και για διεθνή συνεργασία για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο·

8. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ την ανάγκη να δοθεί εκ νέου έμφαση στο πλαίσιο πολιτικής της ΕΕ για την άμυνα στον κυβερνοχώρο 2014 και να επικαιροποιηθεί για την περαιτέρω ενσωμάτωση της ασφάλειας και της άμυνας στον κυβερνοχώρο στην Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ) και για το ευρύτερο θεματολόγιο ασφάλειας και άμυνας·

9. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ ότι μια παγκοσμίως ανταγωνιστική ευρωπαϊκή βιομηχανία αποτελεί σημαντικό στοιχείο για την επίτευξη ενός υψηλού επιπέδου ασφάλειας στον κυβερνοχώρο σε εθνικό επίπεδο όσο και σε επίπεδο ΕΕ·

10. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ ότι, σύμφωνα με το άρθρο 4.2 της ΣΕΕ, η εθνική ασφάλεια αποτελεί αποκλειστική αρμοδιότητα εκάστου κράτους μέλους.

---

2 12109/13 και 6225/13 (κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο (COM JOIN (2013) 1 final)).

3 16200/14 και 6460/14 (ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Πολιτική και διακυβέρνηση του Διαδικτύου - Ο ρόλος της Ευρώπης στη διαμόρφωση του μέλλοντος της διακυβέρνησης του Διαδικτύου (COM(2014) 72 final))

4 14540/16 και 11013/16 (ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών: Πολιτική «Ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας» (COM 2016(410) final).

5 Έγγρ. 6122/15.

6 Έγγρ. 9916/17.

7 Έγγρ. 10007/16.

8 Έγγρ. 9178/17.

9 7688/16 (Κοινή ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Κοινό πλαίσιο για την αντιμετώπιση των υβριδικών απειλών· Απόκριση της Ευρωπαϊκής Ένωσης).

10 Έγγρ. 12650/17.

ΜΕ ΤΟ ΠΑΡΟΝ

11. ΕΚΦΡΑΖΕΙ ΤΗΝ ΙΚΑΝΟΠΟΙΗΣΗ ΤΟΥ για την Κοινή ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο της ΕΕ για την προώθηση ενός φιλόδοξου στόχου για την ενίσχυση της ασφάλειας στον κυβερνοχώρο εντός της ΕΕ. Επίσης συμβάλλει στη στρατηγική αυτονομία της ΕΕ, όπως αναφέρεται στα συμπεράσματά της σχετικά με την παγκόσμια στρατηγική της Ευρωπαϊκής Ένωσης για την εξωτερική πολιτική και την πολιτική ασφαλείας[11], με στόχο να οικοδομήσει μια ψηφιακή Ευρώπη που θα είναι πιο ασφαλής, που θα προκαλεί εμπιστοσύνη, θα έχει επίγνωση των πλεονεκτημάτων της, ανταγωνιστική, ανοικτή στον κόσμο, που θα σέβεται τις κοινές αξίες της ΕΕ σχετικά με ανοικτό, ελεύθερο, φιλειρηνικό και ασφαλές παγκόσμιο διαδίκτυο - και, ως εκ τούτου, θα επιτύχει υψηλότερο επίπεδο ανθεκτικότητας με στόχο την πρόληψη, την αποτροπή, τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο και θα είναι σε θέση να ανταποκρίνεται από κοινού στις απειλές στον κυβερνοχώρο σε ολόκληρη την ΕΕ, και

12. ΚΑΛΕΙ τα κράτη μέλη, τα θεσμικά όργανα, τους οργανισμούς και λοιπά όργανα της ΕΕ της να συνεργασθούν, σεβόμενα το πεδίο αρμοδιοτήτων του καθενός και την αρχή της επικουρικότητας και αναλογικότητας και σύμφωνα με τους στρατηγικούς στόχους που ορίζονται στα παρόντα συμπεράσματα, και

13. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη η Ευρωπαϊκή Ένωση, τα κράτη μέλη της και ο ιδιωτικός τομέας να εξασφαλίσουν επαρκή χρηματοδότηση εντός των διαθέσιμων πόρων, προκειμένου να στηριχθούν οι προσπάθειες έρευνας και ανάπτυξης για την οικοδόμηση ανθεκτικότητας και ασφάλειας στον κυβερνοχώρο στο σύνολο της ΕΕ, καθώς και να ενισχύσουν τη συνεργασία για την πρόληψη, την αποτροπή, τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο και να είναι σε θέση να ανταποκρίνονται από κοινού σε μεγάλης κλίμακας συμβάντα και κακόβουλες δραστηριότητες στον κυβερνοχώρο σε ολόκληρη την ΕΕ·

[11] Έγγρ. 13202/16.

Κεφάλαιο I

ΔΙΑΣΦΑΛΙΣΗ ΜΙΑΣ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΤΗΣ ΕΕ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΤΗΝ ΕΝΙΑΙΑ ΨΗΦΙΑΚΗ ΑΓΟΡΑ

14. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι κάθε κράτος μέλος φέρει την πρωταρχική ευθύνη για τη βελτίωση της ασφάλειας στον κυβερνοχώρο και της αντιμετώπισης περιστατικών και κρίσεων στον κυβερνοχώρο, ενώ η ΕΕ μπορεί να παράσχει ισχυρή προστιθέμενη αξία στηρίζοντας τη συνεργασία μεταξύ των κρατών μελών. Σε αυτό το πλαίσιο, ΤΟΝΙΖΕΙ την ανάγκη όλα τα κράτη μέλη να διαθέσουν τους αναγκαίους πόρους προς τις εθνικές αρχές που είναι αρμόδιες για την ασφάλεια στον κυβερνοχώρο, ούτως ώστε να εξασφαλιστεί η πρόληψη, ο εντοπισμός και η αντιμετώπιση περιπτώσεων συμβάντων και κρίσεων στον κυβερνοχώρο σε ολόκληρη την ΕΕ·

15. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη, όπου είναι δυνατόν, να χρησιμοποιούνται οι υφιστάμενοι μηχανισμοί, οι δομές και οι οργανισμοί σε επίπεδο ΕΕ·

16. ΕΠΙΚΡΟΤΕΊ:

- την πρόοδο που επιτεύχθηκε όσον αφορά τη μεταφορά στο εθνικό δίκαιο των κρατών μελών της οδηγίας ΑΔΠ και ΤΟΝΙΖΕΙ την ανάγκη για την επίτευξη πλήρους και αποτελεσματικής εφαρμογής έως τον Μάιο του 2018 όπως ορίζεται στην εν λόγω οδηγία[12]·
- το έργο που επιτελείται στο πλαίσιο της ομάδας συνεργασίας ΑΔΠ για την ενίσχυση της στρατηγικής συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών·
- το έργο που επιτελείται στο πλαίσιο του δικτύου CSIRT, ιδίως όσον αφορά την ενίσχυση της επιχειρησιακής συνεργασίας των κρατών μελών, την οικοδόμηση εμπιστοσύνης και αξιοπιστίας, για την ανταλλαγή πληροφοριών κατά την αντιμετώπιση μεγάλης κλίμακας συμβάντων ασφάλειας στον κυβερνοχώρο και, με βάση τα συμπεράσματα από τα κράτη μέλη, με την παροχή στοιχείων για μια κοινή αντίληψη της κατάστασης σε ευρωπαϊκό επίπεδο·
- το έργο που επιτελείται στο πλαίσιο της συμβατικής σύμπραξης δημόσιου και ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο (cPPP).

[12] Με την επιφύλαξη της αρμοδιότητας των κρατών μελών για τη μεταφορά στο εθνικό δίκαιο της οδηγίας ΑΔΠ, ιδίως σε ό,τι αφορά τους φορείς εκμετάλλευσης βασικών υπηρεσιών.

17. ΕΚΦΡΑΖΕΙ ΤΗΝ ΙΚΑΝΟΠΟΙΗΣΗ ΤΟΥ για την επιβεβαίωση, στην κοινή ανακοίνωση, ότι η ισχυρή και αξιόπιστη κρυπτογράφηση είναι πολύ σημαντική για την ορθή διασφάλιση των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στην ΕΕ και για την εμπιστοσύνη του κοινού στην ψηφιακή ενιαία αγορά, λαμβάνοντας ταυτόχρονα υπόψη την ανάγκη των αρχών επιβολής του νόμου να έχουν πρόσβαση στα δεδομένα που απαιτούνται για τις έρευνές τους και την επιβεβαίωση ότι η ασφαλής ψηφιακή ταυτοποίηση και η επικοινωνία διαδραματίζουν βασικό ρόλο στη διασφάλιση της αποτελεσματικής ασφάλειας στον κυβερνοχώρο στην ΕΕ·

18. ΧΑΙΡΕΤΙΖΕΙ το σχέδιο εντός της κοινής ανακοίνωσης για αύξηση της φιλοδοξίας κατά τη διεξαγωγή των πανευρωπαϊκών ασκήσεων ασφάλειας στον κυβερνοχώρο σε τακτική βάση, αξιοποιώντας την εμπειρία που έχει αποκτηθεί από τις ασκήσεις «Cyber Europe», συνδυάζοντας την αντίδραση σε διάφορα επίπεδα, δεδομένου ότι αυτό θα αποτελέσει σημαντικό στοιχείο για την προώθηση της ετοιμότητας των κρατών μελών και των θεσμικών οργάνων της ΕΕ για την αντιμετώπιση μεγάλης κλίμακας συμβάντων στον κυβερνοχώρο·

19. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να διεξάγουν τακτικές στρατηγικές ασκήσεις ασφάλειας στον κυβερνοχώρο σε διάφορες συνθέσεις του Συμβουλίου, με βάση την εμπειρία που αποκτήθηκε κατά τη διάρκεια της άσκησης EU CYBRID 2017 και

20. Με την επιφύλαξη της έκβασης της νομοθετικής διαδικασίας:

- ΧΑΙΡΕΤΙΖΕΙ την πρόταση για μια ισχυρή και μόνιμη εντολή για τον ENISA με πρωταρχικό στόχο να υποστηρίξει και να αναπτύξει στενότερη συνεργασία μεταξύ κρατών μελών, για την ενίσχυση των ικανοτήτων τους και την ενίσχυση της εμπιστοσύνης σε μια ψηφιακή Ευρώπη·

- ΕΠΙΒΕΒΑΙΩΝΕΙ ότι το μέλλον του ENISA πρέπει να βασίζεται στην εμπειρία και την εμπειρογνωμοσύνη στο εσωτερικό των κρατών μελών και στην ΕΕ και να στηρίζει τη συνεπή ανάπτυξη και εφαρμογή των υφιστάμενων και μελλοντικών πολιτικών και κανονισμών ασφάλειας στον κυβερνοχώρο της ΕΕ, διασφαλίζοντας ταυτόχρονα ότι όλες οι αρμοδιότητες του ENISA πρέπει να αναπτυχθούν για να συμπληρώνουν τις αντίστοιχες των κρατών μελών·

- ΕΠΙΒΕΒΑΙΩΝΕΙ τον στόχο της ενίσχυσης της εμπιστοσύνης σε μια ψηφιακή Ευρώπη αυξάνοντας την εμπιστοσύνη στις ψηφιακές λύσεις και καινοτομίες, συμπεριλαμβανομένου του Διαδικτύου των Πραγμάτων, του ηλεκτρονικού εμπορίου και της ηλεκτρονικής διακυβέρνησης, ιδίως όσον αφορά το παγκόσμιας εμβέλειας ευρωπαϊκό πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο[13]. Αυτό αποτελεί βασική προϋπόθεση για την ενίσχυση της εμπιστοσύνης και της ασφάλειας στα ψηφιακά προϊόντα και υπηρεσίες, την προστασία των υποδομών ζωτικής σημασίας, των κρατικών δεδομένων και των δεδομένων των πολιτών και των επιχειρήσεων και διαδραματίζει καίριο ρόλο για τη θέσπιση προσέγγισης της ασφάλειας βάσει σχεδιασμού για τα προϊόντα, τις υπηρεσίες και τις διεργασίες στη ψηφιακή ενιαία αγορά·

- ΤΟΝΙΖΕΙ ότι οι νομοθετικές εργασίες για την ενίσχυση της πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ, θα πρέπει να ανταποκρίνονται στις ανάγκες της αγοράς και των χρηστών, να βασίζονται στις εμπειρίες των ικανοτήτων και των διαδικασιών πιστοποίησης που υπάρχουν στην ΕΕ (για παράδειγμα το πλαίσιο SOG-IS) και θα πρέπει να παρέχουν ένα πλαίσιο ικανό να προσαρμόζεται ταχέως στις προηγμένες μελλοντικές ψηφιακές εξελίξεις·

- ΤΟΝΙΖΕΙ ότι κατά την ενίσχυση της πιστοποίησης ασφάλειας του κυβερνοχώρου στην ΕΕ, θα πρέπει να καλύπτεται έως το υψηλότερο επίπεδο, το πλήρες φάσμα των απαιτήσεων ασφαλείας, όπου θα πρέπει να αποδεικνύονται οι δυνατότητες αντίστασης κατά των επιθέσεων. Βασικοί παράγοντες της επιτυχίας θα είναι η διασφάλιση μιας αξιόπιστης, διαφανούς και ανεξάρτητης διαδικασίας πιστοποίησης της ασφάλειας για την προώθηση της διαθεσιμότητας αξιόπιστων και ασφαλών συσκευών, λογισμικού και υπηρεσιών εντός της Ενιαίας Αγοράς όσο και πέραν αυτής· αναγνωρίζοντας την αντίστοιχη εμπειρογνωμοσύνη μέσω ευρωπαϊκών και παγκόσμιων προτύπων της ευρωπαϊκής βιομηχανίας, των κυβερνήσεων και των ειδικών σε θέματα αξιολόγησης[14]· σεβασμός του ρόλου των κρατών μελών στη διαδικασία πιστοποίησης, ιδίως όσον αφορά την αξιολόγηση σε υψηλότερα επίπεδα ασφάλειας και ιδιαίτερα σε σχέση με τις βασικές ανάγκες ασφάλειας και την αξιολόγηση των δεξιοτήτων. Αυτό το πλαίσιο πιστοποίησης πρέπει επίσης να εξασφαλίζει ότι κάθε σύστημα πιστοποίησης σε ενωσιακό επίπεδο είναι αναλογικό προς το επίπεδο διασφάλισης που απαιτείται για τη χρήση προϊόντων, υπηρεσιών και/ή των εμπλεκομένων συστημάτων ΤΠΕ, και να παρέχει τη δυνατότητα διασυνοριακών συναλλαγών για τις επιχειρήσεις όλων των κλιμάκων για την ανάπτυξη και πώληση νέων προϊόντων, τόσο εντός της ΕΕ όσο και εκτός των αγορών της ΕΕ.

---

13 Με τη θέσπιση παγκόσμιων προτύπων σύμφωνα με το πνεύμα του κώδικα δεοντολογίας του ΤΦΕ-ΠΟΕ.

14 Με τη θέσπιση ευρωπαϊκών και παγκόσμιων προτύπων σύμφωνα με το πνεύμα του κώδικα δεοντολογίας του ΤΦΕ-ΠΟΕ.

21. ΧΑΙΡΕΤΙΖΕΙ την πρόθεση της Επιτροπής να δημιουργήσει ένα δίκτυο κέντρων ικανοτήτων για την ασφάλεια στον κυβερνοχώρο για την τόνωση της ανάπτυξης και εξάπλωσης των τεχνολογιών ασφάλειας στον κυβερνοχώρο και να προσφέρει μια πρόσθετη ώθηση στην καινοτομία για τη βιομηχανία της ΕΕ στην παγκόσμια σκηνή για την ανάπτυξη επόμενης γενιάς και καινοτόμων τεχνολογιών, όπως η τεχνητή νοημοσύνη, η κβαντική υπολογιστική, η τεχνολογία blockchain και οι ασφαλείς ψηφιακές ταυτότητες·

22. ΤΟΝΙΖΕΙ την ανάγκη το Δίκτυο κέντρων ικανοτήτων για την ασφάλεια στον κυβερνοχώρο να είναι ανοικτό προς όλα τα κράτη μέλη και τα υφιστάμενα κέντρα αριστείας και ικανοτήτων τους και να δίνει ιδιαίτερη προσοχή στη συμπληρωματικότητα και με αυτό κατά νου ΛΑΜΒΑΝΕΙ ΥΠΟΨΗ ΤΟΥ το προβλεπόμενο Ευρωπαϊκό ερευνητικό κέντρο ασφάλειας στον κυβερνοχώρο, το οποίο θα πρέπει, ως βασικός του ρόλος, να επικεντρωθεί στη διασφάλιση της συμπληρωματικότητας και την αποφυγή επικαλύψεων στο πλαίσιο του δικτύου των Κέντρων και την ασφάλεια στον κυβερνοχώρο και με άλλους οργανισμούς της ΕΕΕ·

23. ΤΟΝΙΖΕΙ ότι το Δίκτυο κέντρων για την ασφάλεια στον κυβερνοχώρο θα πρέπει να αντιμετωπίζει ένα φάσμα θεμάτων από την έρευνα έως τη βιομηχανία, και, ως εκ τούτου, πρέπει να συμβάλλει, μεταξύ άλλων, στην επίτευξη του στόχου της ευρωπαϊκής στρατηγικής αυτονομίας·

24. Ενόψει του προτεινόμενου Δικτύου κέντρων για την ασφάλεια στον κυβερνοχώρο, ΕΠΙΒΕΒΑΙΩΝΕΙ ΕΚ ΝΕΟΥ την ανάγκη η ΕΕ, μέσω των κρατών μελών της, να αναπτύξει ευρωπαϊκή ικανότητα για την αξιολόγηση της ισχύος της κρυπτογράφησης που χρησιμοποιείται σε προϊόντα και υπηρεσίες που διατίθενται για τους πολίτες, τις επιχειρήσεις και τις κυβερνήσεις, στο πλαίσιο της ψηφιακής ενιαίας αγοράς, αναγνωρίζοντας παράλληλα ότι οι πολιτικές για την κρυπτογράφηση αποτελούν βασική πτυχή της εθνικής ασφάλειας και, ως εκ τούτου, εμπίπτουν στην αρμοδιότητα των κρατών μελών·

25. ΚΑΛΕΙ όλους τους ενδιαφερόμενους φορείς να αυξήσουν τις επενδύσεις στις εφαρμογές νέων τεχνολογιών στην ασφάλεια στον κυβερνοχώρο, ώστε να συμβάλλουν στην εξασφάλιση της ασφάλειας στον κυβερνοχώρο σε όλους τους τομείς της ευρωπαϊκής οικονομίας·

26. ΤΟΝΙΖΕΙ τη σημασία αξιόπιστης, έγκυρης και συντονισμένης παροχής υπηρεσιών ασφάλειας στον κυβερνοχώρο για όλα τα όργανα της ΕΕ και ΚΑΛΕΙ την ΕΠΙΤΡΟΠΗ και τα άλλα θεσμικά όργανα της ΕΕ να αναπτύξουν περαιτέρω την ομάδα CERT-ΕΕ σύμφωνα με τους ανωτέρω στόχους και να εξασφαλίσουν επαρκείς πόρους και για αυτές τις ανάγκες·

27. ΧΑΙΡΕΤΙΖΕΙ την έκκληση να αναγνωριστεί ο σημαντικός ρόλος που διαδραματίζουν οι ερευνητές ασφάλειας τρίτων μερών στον εντοπισμό τρωτών σημείων σε προϊόντα και υπηρεσίες που υπάρχουν ήδη και ΚΑΛΕΙ τα κράτη μέλη να ανταλλάσσουν βέλτιστες πρακτικές για τη συντονισμένη δημοσιοποίηση τρωτών σημείων·

28. ΤΟΝΙΖΕΙ τη συλλογική ευθύνη στον τομέα της ασφάλειας στον κυβερνοχώρο και ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να προωθήσουν τις ψηφιακές δεξιότητες και την παιδεία για τα μέσα επικοινωνίας, βοηθώντας τους χρήστες να προστατεύουν τις ψηφιακές πληροφορίες τους στο διαδίκτυο και να είναι ενημερωμένοι σχετικά με τους κινδύνους που διατρέχουν όταν κοινοποιούν προσωπικά δεδομένα στο διαδίκτυο·

29. ΕΚΦΡΑΖΕΙ ΤΗΝ ΙΚΑΝΟΠΟΙΗΣΗ ΤΟΥ για την έμφαση που δίδει η κοινή ανακοίνωση στην παιδεία, στην υγιεινή στον κυβερνοχώρο και στην ευαισθητοποίηση σχετικά με τα θέματα αυτά στα κράτη μέλη και την ΕΕ·

30. ΚΑΛΕΙ ΤΗΝ ΕΠΙΤΡΟΠΗ να υποβάλει χωρίς χρονοτριβή μια εκτίμηση αντικτύπου και να προτείνει έως τα μέσα του 2018 τις σχετικές νομικές πράξεις για την υλοποίηση της πρωτοβουλίας για τη σύσταση του δικτύου κέντρων ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και του Ευρωπαϊκού Κέντρου Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο·

31. ΚΑΛΕΙ τα κράτη μέλη:

- να αποδώσουν προτεραιότητα στην ευαισθητοποίηση σχετικά με τον κυβερνοχώρο κατά τις εκστρατείες ενημέρωσης και να αναδείξουν την ασφάλεια στον κυβερνοχώρο στο πλαίσιο της ακαδημαϊκής εκπαίδευσης και στα προγράμματα επαγγελματικής κατάρτισης. Θα πρέπει να δοθεί ιδιαίτερη έμφαση στην εκπαίδευση των νέων και στην καλλιέργεια των ψηφιακών δεξιοτήτων, με στόχο τη δημιουργία επαγγελματιών έτοιμων να αντιμετωπίσουν τις προκλήσεις που επιφυλάσσει το μέλλον στον τομέα της ασφάλειας, της οικονομίας και της παροχής υπηρεσιών·

- να ενισχύσουν τις προσπάθειες για την έναρξη εξειδικευμένων προγραμμάτων υψηλού επιπέδου στον τομέα της ασφάλειας στον κυβερνοχώρο προκειμένου να καλυφθεί το υπάρχον κενό στους επαγγελματίες αυτού του τομέα στην ΕΕ·

- να δημιουργήσουν ένα αποτελεσματικό δίκτυο συνεργασίας εκπαιδευτικών σημείων επαφής υπό την αιγίδα του ENISA. Το δίκτυο αυτό θα πρέπει να αποσκοπεί στη βελτίωση του συντονισμού και της ανταλλαγής βέλτιστων πρακτικών μεταξύ των κρατών μελών όσον αφορά την εκπαίδευση και την ευαισθητοποίηση του κοινού για την ασφάλεια στον κυβερνοχώρο, καθώς και στους τομείς της κατάρτισης, των ασκήσεων και της δημιουργίας ικανοτήτων·

- να εξετάσουν το ενδεχόμενο εφαρμογής των κανόνων της οδηγίας ΑΔΠ και στις δημόσιες διοικήσεις που συμμετέχουν σε κρίσιμες κοινωνικές ή οικονομικές δραστηριότητες, εάν δεν καλύπτονται ήδη από την εθνική νομοθεσία και εφόσον κρίνεται σκόπιμο, και να παράσχουν κατάρτιση σχετικά με την ασφάλεια στον κυβερνοχώρο και στις δημόσιες διοικήσεις, δεδομένου του ρόλου που διαδραματίζουν στην κοινωνία και την οικονομία μας.

Κεφάλαιο ΙΙ

ΟΙΚΟΔΟΜΗΣΗ ΤΗΣ ΙΚΑΝΟΤΗΤΑΣ ΤΗΣ ΕΕ ΣΤΗΝ ΠΡΟΛΗΨΗ, ΤΗΝ ΑΠΟΤΡΟΠΗ, ΤΟΝ ΕΝΤΟΠΙΣΜΟ ΚΑΙ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΚΟΒΟΥΛΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

32. ΤΟΝΙΖΕΙ ότι τυχόν ιδιαιτέρως σοβαρό συμβάν ή κρίση στον κυβερνοχώρο θα μπορούσε να θεωρηθεί επαρκής λόγος για την επίκληση της ρήτρας αλληλεγγύης[15] της ΕΕ ή/και της ρήτρας αμοιβαίας συνδρομής[16] από κάποιο κράτος μέλος.

33. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για την έγκριση του πλαισίου για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, το οποίο συμβάλλει στην πρόληψη των συγκρούσεων, στη συνεργασία και τη σταθερότητα στον κυβερνοχώρο με τη θέσπιση μέτρων στο πλαίσιο της ΚΕΠΠΑ, όπως, ενδεικτικά, περιοριστικά μέτρα, τα οποία μπορούν να χρησιμοποιηθούν για την πρόληψη και αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο και ΚΑΛΕΙ την ΕΥΕΔ και τα κράτη μέλη να διεξάγουν τακτικά ασκήσεις επί του εν λόγω πλαισίου·

---

15 Άρθρο 222 ΣΛΕΕ

16 Άρθρο 42 παράγραφος 7 ΣΕΕ

34. ΤΟΝΙΖΕΙ την ανάγκη για αποτελεσματική αντίδραση σε επίπεδο ΕΕ όποτε ανακύπτουν μεγάλης κλίμακας συμβάντα και κρίσεις στον κυβερνοχώρο, χωρίς να θίγονται οι αρμοδιότητες των κρατών μελών, και την ανάγκη να ενσωματωθεί η ασφάλεια στον κυβερνοχώρο στους υφιστάμενους μηχανισμούς διαχείρισης κρίσεων σε επίπεδο ΕΕ[17]. Προς τούτο, ΑΠΕΥΘΥΝΕΙ ΕΚΚΛΗΣΗ να κινητοποιείται τακτικά η αντιμετώπιση σε επίπεδο ΕΕ έναντι μεγάλης κλίμακας συμβάντων στον κυβερνοχώρο – από διπλωματικές-στρατηγικές κινήσεις έως καθαρά τεχνικές – έχοντας ως βάση και προσαρμόζοντας κατά περίπτωση τα σχετικά πλαίσια και διαδικασίες[18]·

35. ΤΟΝΙΖΕΙ τη σημασία της επιτυχούς αλληλοσύνδεσης μεταξύ των μηχανισμών αντίδρασης και ανταλλαγής πληροφοριών των διαφόρων φορέων που διαδραματίζουν ζωτικό ρόλο για την ασφάλεια στον κυβερνοχώρο στην Ευρώπη, όπως για παράδειγμα μεταξύ των σχετικών οργάνων της ΕΕ και των αρχών των κρατών μελών. Οι εν λόγω μηχανισμοί θα πρέπει να υποβληθούν σε δοκιμές και ελέγχους στο πλαίσιο ασκήσεων ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ και να τυποποιηθούν με αντίστοιχες συμφωνίες, όπου απαιτείται·

36. ΣΗΜΕΙΩΝΕΙ τη δυνατότητα να εξεταστεί, εφόσον υποβληθεί από την Επιτροπή, πρόταση για τη σύσταση Ταμείου Αντιμετώπισης Έκτακτων Απειλών Κυβερνοασφάλειας, παράλληλα με τις υφιστάμενες προσπάθειες των κρατών μελών και λαμβανομένων υπόψη των διαθέσιμων πόρων (ιδίως στο πλαίσιο του πολυετούς δημοσιονομικού πλαισίου της ΕΕ) ώστε να βοηθηθούν τα κράτη μέλη στην αντιμετώπιση και τον μετριασμό μεγάλης κλίμακας συμβάντων στον κυβερνοχώρο, υπό την προϋπόθεση ότι το ενδιαφερόμενο κράτος μέλος διέθετε ενδεδειγμένο σύστημα για την ασφάλεια στον κυβερνοχώρο πριν από το περιστατικό, συμπεριλαμβανομένης της πλήρους εφαρμογής της οδηγίας ΑΔΠ, και ώριμα πλαίσια διαχείρισης κινδύνου και εποπτείας σε εθνικό επίπεδο·

37. ΑΝΑΓΝΩΡΙΖΕΙ την αυξανόμενη διασύνδεση μεταξύ ασφάλειας στον κυβερνοχώρο και άμυνας και ΖΗΤΕΙ να ενταθεί η συνεργασία στον τομέα της άμυνας στον κυβερνοχώρο, μεταξύ άλλων με την ενθάρρυνση της συνεργασίας μεταξύ μη στρατιωτικών και στρατιωτικών φορέων αντιμετώπισης συμβάντων στον κυβερνοχώρο και να ενισχυθεί περαιτέρω η κυβερνοασφάλεια των αποστολών και επιχειρήσεων της ΚΠΑΑ·

---

17 C/2017/6100 final

18 9916/17 και C/2017/6100 final.

38. ΤΟΝΙΖΕΙ την ανάγκη να αξιοποιηθούν ενδεχομένως στον μέγιστο βαθμό οι προτεινόμενες αμυντικές πρωτοβουλίες ώστε να επιταχυνθεί η ανάπτυξη επαρκών ικανοτήτων στον κυβερνοχώρο στην Ευρώπη και ΑΝΑΓΝΩΡΙΖΕΙ τις ευκαιρίες για πιθανή εκπόνηση σχεδίων κυβερνοάμυνας μέσω της μόνιμης διαρθρωμένης συνεργασίας (PESCO), εφόσον κριθεί αναγκαίο από τα συμμετέχοντα κράτη μέλη της PESCO και ΑΝΑΓΝΩΡΙΖΕΙ τον ρόλο που διαδραματίζει η Ευρωπαϊκή Βιομηχανική και Τεχνολογική Βάση στον τομέα της Άμυνας (EDTIB) και η ευρύτερη, μη στρατιωτική, βιομηχανική βάση στον τομέα της ασφάλειας στον κυβερνοχώρο ως προς την παροχή μέσων στα κράτη μέλη για να διαφυλάσσουν τα συμφέροντά τους στους τομείς της ασφάλειας και της άμυνας στον κυβερνοχώρο·

39. ΣΗΜΕΙΩΝΕΙ την πρόταση της Επιτροπής να θέσει σε εφαρμογή μια πλατφόρμα για την εκπαίδευση και κατάρτιση σε θέματα κυβερνοάμυνας, μέχρι το τέλος του 2018, και ΤΟΝΙΖΕΙ ότι η πλατφόρμα θα πρέπει να αναβαθμίσει τις ευκαιρίες κατάρτισης και εκπαίδευσης εντός των κρατών μελών και θα πρέπει να εξασφαλίζει τη συμπληρωματικότητα με άλλες προσπάθειες και πρωτοβουλίες της ΕΕ, ιδίως με την ΕΑΑΑ και τον ΕΟΑ·

40. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να ανταποκριθούν στην απειλή της χρήσης ΤΠΕ για κλοπή διανοητικής ιδιοκτησίας, συμπεριλαμβανομένων εμπορικών μυστικών ή άλλων εμπιστευτικών επιχειρηματικών πληροφοριών, με σκοπό την εξασφάλιση ανταγωνιστικών πλεονεκτημάτων σε εταιρείες ή βιομηχανικούς κλάδους·

41. ΑΝΑΓΝΩΡΙΖΕΙ την ανάγκη για αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο, συμπεριλαμβανομένων όσων διαπράττονται στο Darkweb, της σεξουαλικής εκμετάλλευσης παιδιών στο Διαδίκτυο, καθώς και της απάτης και της παραχάραξης μέσων πληρωμής πλην των μετρητών, κυρίως επιδιώκοντας τη συλλογή περισσότερων στοιχείων, τη διεξαγωγή κοινών ερευνών και την από κοινού χρήση επιχειρησιακής υποστήριξης·

42. ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για το έργο που έχει επιτελεστεί από τη ΕΕ και τα κράτη μέλη της όσον αφορά την αντιμετώπιση των προκλήσεων που θέτουν τα συστήματα που επιτρέπουν σε εγκληματίες και σε τρομοκράτες να επικοινωνούν με τρόπους στους οποίους οι αρμόδιες αρχές δεν έχουν δυνατότητα πρόσβασης, ΤΟΝΙΖΕΙ ότι στο έργο αυτό πρέπει να λαμβάνεται υπόψη ότι η ισχυρή και αξιόπιστη κρυπτογράφηση είναι υψίστης σημασίας για την ασφάλεια στον κυβερνοχώρο και για την εδραίωση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά καθώς για και την εξασφάλιση του σεβασμού των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών·

43. ΥΠΟΓΡΑΜΜΙΖΕΙ τη σημασία της παροχής στις αρχές επιβολής του νόμου των εργαλείων εκείνων που θα διευκολύνουν τον εντοπισμό, τη διερεύνηση και τη δίωξη του εγκλήματος στον κυβερνοχώρο, ώστε τα εγκλήματα που διαπράττονται στον κυβερνοχώρο να μην μένουν απαρατήρητα ή ατιμώρητα και ΕΚΦΡΑΖΕΙ ΤΗΝ ΙΚΑΝΟΠΟΙΗΣΗ ΤΟΥ για τη συνεισφορά του Ευρωπαϊκού Δικαστικού Δικτύου για το έγκλημα στον κυβερνοχώρο στην καταπολέμηση του εγκλήματος μέσω της συνεργασίας των δικαστικών αρχών·

44. ΤΟΝΙΖΕΙ πόσο σημαντικό είναι να εξασφαλιστεί μια συντονισμένη θέση της ΕΕ για την αποτελεσματική διαμόρφωση των αποφάσεων περί διακυβέρνησης διαδικτύου σε ευρωπαϊκό και παγκόσμιο επίπεδο εντός του πολυσυμμετοχικού πλαισίου, όπως μεταξύ άλλων με την εξασφάλιση βάσεων δεδομένων WHOIS των διευθύνσεων IP και των ονομάτων τομέα οι οποίες να χαρακτηρίζονται από ταχύτητα πρόσβασης και ακρίβεια, προκειμένου να διαφυλαχθεί η ικανότητα επιβολής του νόμου και το δημόσιο συμφέρον·

45. ΤΟΝΙΖΕΙ τη σημασία που έχει η υιοθέτηση του πρωτοκόλλου IPv6 του Διαδικτύου, που είναι ζωτικής σημασίας για την ανάπτυξη του Διαδικτύου των Πραγμάτων σε κλίμακα καθώς και για τη βελτίωση της απόδοσης των εγκλημάτων που διαπράττονται στον κυβερνοχώρο·

46. ΕΝΘΑΡΡΥΝΕΙ τις εν εξελίξει εργασίες σχετικά με τη διασυνοριακή πρόσβαση στα ηλεκτρονικά αποδεικτικά στοιχεία, την αντιμετώπιση της διατήρησης δεδομένων και τις προκλήσεις για τις ποινικές διαδικασίες που τίθενται από τα συστήματα που επιτρέπουν σε εγκληματίες και τρομοκράτες να επικοινωνούν με τρόπους στους οποίους οι αρμόδιες αρχές δεν έχουν δυνατότητα πρόσβασης, έχοντας πάντα υπόψη την ανάγκη σεβασμού των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και την προστασία των δεδομένων·

47. ΚΑΛΕΙ την Επιτροπή:

- να υποβάλει έως τον Δεκέμβριο του 2017 έκθεση προόδου σχετικά με την εφαρμογή των πρακτικών μέτρων για τη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία·
- να υποβάλει στις αρχές του 2018 νομοθετική πρόταση για τη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία·

48. ΚΑΛΕΙ την Ευρωπόλ, τον ENISA και την Eurojust:

- να συνεχίσουν την ενίσχυση της συνεργασίας τους για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, τόσο μεταξύ τους όσο και με άλλους σχετικούς φορείς, συμπεριλαμβανομένης της κοινότητας των CSIRT, της Ιντερπόλ, του ιδιωτικού τομέα και της ακαδημαϊκής κοινότητας για την εξασφάλιση συνεργειών και συμπληρωματικότητας, σύμφωνα με τις αντίστοιχες εντολές και αρμοδιότητές τους.

- να συμβάλουν μαζί με τα κράτη μέλη στη διαμόρφωση συντονισμένης προσέγγισης όσον αφορά την ενωσιακή αντιμετώπιση σε επίπεδο επιβολής του νόμου σε περίπτωση συμβάντων και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο συμπληρωματικά προς τις διαδικασίες που περιγράφονται στα σχετικά πλαίσια[19]·

49. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να συνεχίσουν να εργάζονται για την επίτευξη των ακόλουθων στόχων:

- να αρθούν τα εμπόδια στη διερεύνηση εγκλημάτων και στην αποτελεσματική ποινική δικαιοσύνη στον κυβερνοχώρο, καθώς επίσης να ενισχυθεί η διεθνής συνεργασία και ο διεθνής συντονισμός στην καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο·

- να αντιμετωπιστούν οι προκλήσεις που θέτουν οι τεχνολογίες ανωνυμοποίησης, έχοντας ωστόσο κατά νου ότι η ισχυρή και αξιόπιστη κρυπτογράφηση έχει μεγάλη σημασία για την ασφάλεια στον κυβερνοχώρο και για την εδραίωση της εμπιστοσύνης στην ψηφιακή ενιαία αγορά·

- να διαμορφωθούν κατάλληλα οι αποφάσεις διαδικτυακής διακυβέρνησης, οι οποίες επηρεάζουν την ικανότητα των αρχών επιβολής του νόμου να καταπολεμούν την εγκληματικότητα στον κυβερνοχώρο.

[19] 9916/17 και C/2017/6100 final.

Κεφάλαιο ΙΙΙ

ΕΝΙΣΧΥΣΗ ΤΗΣ ΔΙΕΘΝΟΥΣ ΣΥΝΕΡΓΑΣΙΑΣ ΓΙΑ ΑΝΟΙΚΤΟ, ΕΛΕΥΘΕΡΟ, ΕΙΡΗΝΙΚΟ ΚΑΙ ΑΣΦΑΛΗ ΠΑΓΚΟΣΜΙΟ ΚΥΒΕΡΝΟΧΩΡΟ

50. ΑΝΑΓΝΩΡΙΖΕΙ ότι η ασφάλεια στον κυβερνοχώρο αποτελεί παγκόσμια πρόκληση, η οποία απαιτεί αποτελεσματική παγκόσμια συνεργασία μεταξύ όλων των εμπλεκομένων, και ΑΝΑΓΝΩΡΙΖΕΙ ότι πρέπει να δοθεί ιδιαίτερη έμφαση στον σεβασμό των δημοκρατικών αξιών και των αρχών του ανοικτού, ελεύθερου, ειρηνικού και ασφαλούς κυβερνοχώρου σε παγκόσμιο επίπεδο, και, υπό αυτό το πρίσμα,

51. ΑΠΕΥΘΥΝΕΙ ΕΚΚΛΗΣΗ στην ΕΕ και τα κράτη μέλη της να προωθήσουν την καθιέρωση ενός στρατηγικού πλαισίου για την πρόληψη των συγκρούσεων, τη συνεργασία και τη σταθερότητα στον κυβερνοχώρο που να βασίζεται στην εφαρμογή του ισχύοντος διεθνούς δικαίου, και ιδίως του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, την ανάπτυξη και την εφαρμογή οικουμενικών κανόνων για την υπεύθυνη κρατική συμπεριφορά, και περιφερειακά μέτρα οικοδόμησης εμπιστοσύνης μεταξύ των κρατών·

52. ΑΝΑΓΝΩΡΙΖΕΙ τον ρόλο των Ηνωμένων Εθνών στην περαιτέρω ανάπτυξη προδιαγραφών για την υπεύθυνη κρατική συμπεριφορά στον κυβερνοχώρο και υπενθυμίζει ότι τα αποτελέσματα των εργασιών της Ομάδας Κυβερνητικών Εμπειρογνωμόνων των Ηνωμένων Εθνών κατά τα τελευταία έτη έχουν διαμορφώσει ένα συναινετικό σύνολο κανόνων και συστάσεων [20], το οποίο έχει υποστηριχθεί επανειλημμένα από τη Γενική Συνέλευση των Ηνωμένων Εθνών, και το οποίο τα κράτη πρέπει να λάβουν ως βάση για την υπεύθυνη κρατική συμπεριφορά στον κυβερνοχώρο·

53. ΑΝΑΓΝΩΡΙΖΕΙ ότι οι εν λόγω κανόνες της υπεύθυνης κρατικής συμπεριφοράς προβλέπουν μεταξύ άλλων ότι τα κράτη δεν θα πρέπει εν γνώσει τους να επιτρέπουν να χρησιμοποιείται το έδαφός τους για διεθνείς παράνομες πράξεις, θα πρέπει να ανταποκρίνονται σε δέουσες αιτήσεις συνδρομής από άλλο κράτος μέλος όταν κρίσιμες υποδομές ΤΠΕ του τελευταίου αποτελούν στόχο κακόβουλων πράξεων ΤΠΕ που προέρχονται από το έδαφός τους και ότι τα κράτη θα πρέπει να λαμβάνουν τα κατάλληλα μέτρα για την προστασία των κρίσιμων υποδομών τους από απειλές ΤΠΕ·

54. ΑΝΑΓΝΩΡΙΖΕΙ τις κοινές απειλές και κινδύνους στον κυβερνοχώρο που αντιμετωπίζει η ΕΕ, το ΝΑΤΟ και τα κράτη μέλη αυτών και ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη σημασία της συνέχισης της συνεργασίας μεταξύ ΕΕ και ΝΑΤΟ σχετικά με την ασφάλεια στον κυβερνοχώρο και την άμυνα, τηρουμένων πλήρως των αρχών της συμμετοχικότητας, της αμοιβαιότητας και της αυτονομίας λήψης αποφάσεων της ΕΕ και σύμφωνα με τα συμπεράσματα του Συμβουλίου της 6ης Δεκεμβρίου 2016 σχετικά με την εφαρμογή της κοινής δήλωσης του Προέδρου του Ευρωπαϊκού Συμβουλίου, του Προέδρου της Ευρωπαϊκής Επιτροπής και του Γενικού Γραμματέα του Οργανισμού Βορειοατλαντικού Συμφώνου[20]·

55. ΑΠΕΥΘΥΝΕΙ ΕΚΚΛΗΣΗ στην ΕΕ και τα κράτη μέλη της να στηρίξουν και να ενθαρρύνουν την ανάπτυξη περιφερειακών μέτρων οικοδόμησης εμπιστοσύνης, τα οποία διαδραματίζουν ουσιαστικό ρόλο στην αύξηση της συνεργασίας και της διαφάνειας και στη μείωση του κινδύνου σύγκρουσης. Η εφαρμογή μέτρων οικοδόμησης εμπιστοσύνης για την ασφάλεια στον κυβερνοχώρο στο πλαίσιο του ΟΑΣΕ και σε άλλα περιφερειακά πλαίσια θα αυξήσει την προβλεψιμότητα της κρατικής συμπεριφοράς και θα συμβάλει περαιτέρω στη σταθεροποίηση του κυβερνοχώρου·

56. ΕΠΙΒΕΒΑΙΩΝΕΙ ότι η ΕΕ θα εξακολουθήσει να σέβεται τις θεμελιώδεις αξίες της όσον αφορά την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, με βάση τις κατευθυντήριες γραμμές της ΕΕ για τα ανθρώπινα δικαιώματα σχετικά με την ελευθερία στο διαδίκτυο. Η ΕΕ επισημαίνει επίσης τη σημασία της συμμετοχής όλων των ενδιαφερόμενων φορέων στη διακυβέρνηση του διαδικτύου, περιλαμβανομένης της ακαδημαϊκής κοινότητας, της κοινωνίας των πολιτών και του ιδιωτικού τομέα·

57. ΑΠΕΥΘΥΝΕΙ ΕΚΚΛΗΣΗ στην ΕΕ και τα κράτη μέλη της για την προώθηση της δημιουργίας ικανοτήτων στον κυβερνοχώρο σε τρίτες χώρες, με ιδιαίτερη προτεραιότητα στις γειτονικές και αναπτυσσόμενες χώρες με ταχέως αυξανόμενη συνδεσιμότητα, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και την οικοδόμηση ανθεκτικότητας στον κυβερνοχώρο, σύμφωνα με τις θεμελιώδεις αξίες της ΕΕ. Για την προαγωγή των προσπαθειών της ΕΕ στον εν λόγω τομέα, θα πρέπει να δημιουργηθεί ένα δίκτυο ανάπτυξης ικανοτήτων της ΕΕ στον τομέα του κυβερνοχώρου και να καταρτιστούν κατευθυντήριες γραμμές για την ανάπτυξη των εν λόγω ικανοτήτων, συμπληρωματικά προς τους υφιστάμενους μηχανισμούς και δομές·

[20] Έγγρ. 15283/16.

58. ΕΠΙΣΗΜΑΙΝΕΙ την πρόοδο που έχει σημειωθεί στη συνεργασία ΕΕ-ΝΑΤΟ στον τομέα της άμυνας και της ασφάλειας στον κυβερνοχώρο και της ανάπτυξης της εν λόγω συνεργασίας στην κατάρτιση, την εκπαίδευση και τις έννοιες, με παράλληλη αποφυγή της περιττής επανάληψης των προσπαθειών όπου υπάρχει αλληλεπικάλυψη απαιτήσεων, καθώς και όσον αφορά την προαγωγή της διαλειτουργικότητας μέσω των προδιαγραφών και των προτύπων στον τομέα της κυβερνοάμυνας, και ΑΠΕΥΘΥΝΕΙ ΕΚΚΛΗΣΗ για τη συνέχιση της συνεργασίας σχετικά με την άμυνα στον κυβερνοχώρο (σε επίπεδο προσωπικού) και την ανταλλαγή βέλτιστων πρακτικών όσον αφορά τη διαχείριση κρίσεων, με αποφυγή της περιττής επανάληψης προσπαθειών, όπου υπάρχει αλληλεπικάλυψη απαιτήσεων, με πλήρη σεβασμό της Πολιτικής Ασκήσεων της ΕΕ και των αρχών της συμμετοχικότητας, της αμοιβαιότητας της αυτονομίας λήψης αποφάσεων της ΕΕ·

59. ΑΝΑΓΝΩΡΙΖΕΙ ότι η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης) προσφέρει ένα αποτελεσματικό νομικό πρότυπο στο οποίο μπορεί να βασιστεί η εθνική νομοθεσία για το έγκλημα στον κυβερνοχώρο. ΖΗΤΕΙ από όλες τις χώρες να σχεδιάσουν κατάλληλα εθνικά νομικά πλαίσια και να επιδιώξουν τη συνεργασία εντός του υφιστάμενου διεθνούς πλαισίου που προσφέρει η Σύμβαση της Βουδαπέστης·

60. ΥΠΕΝΘΥΜΙΖΕΙ τα επιτεύγματα από τη διεξαγωγή διμερών διαλόγων σε επίπεδο ΕΕ σχετικά με τον κυβερνοχώρο και ζητεί να καταβληθούν περαιτέρω προσπάθειες για να διευκολυνθεί η συνεργασία με τρίτες χώρες στον τομέα της ασφάλειας στον κυβερνοχώρο·

61. ΥΠΕΝΘΥΜΙΖΕΙ ότι η ΕΕ διαθέτει στιβαρό και νομικά δεσμευτικό μηχανισμό ελέγχου των εξαγωγών με βάση τις αποφάσεις και τις βέλτιστες πρακτικές που εκπονήθηκαν στο πλαίσιο των διεθνών καθεστώτων μη διάδοσης και ΣΗΜΕΙΩΝΕΙ την εν εξελίξει συζήτηση στο Συμβούλιο για την εξεύρεση των βέλτιστων τρόπων ώστε να βελτιωθεί περαιτέρω η λειτουργία των εν λόγω ελέγχων και ΚΑΛΕΙ τα κράτη μέλη να εξακολουθήσουν να θέτουν επί τάπητος, στο συναφές διεθνές καθεστώς ελέγχου των εξαγωγών (π.χ. Διακανονισμός του Wassenaar) τις κρίσιμες εφαρμογές των νέων τεχνολογιών που άπτονται της ασφάλειας στον κυβερνοχώρο, προκειμένου να διασφαλιστεί ο αποτελεσματικός έλεγχος των τεχνολογιών του μέλλοντος που θα είναι κρίσιμες για την ασφάλεια στον κυβερνοχώρο.

62. Σε συνέχεια των συμπερασμάτων του Ευρωπαϊκού Συμβουλίου της 19ης Οκτωβρίου 2017[21], τα παρόντα συμπεράσματα θα εφαρμοστούν μέσω ενός σχεδίου δράσης που θα εγκριθεί από το Συμβούλιο πριν από το τέλος του 2017. Το σχέδιο δράσης θα είναι ένα δυναμικό έγγραφο το οποίο θα υπόκειται σε τακτική επανεξέταση και επικαιροποίηση από το Συμβούλιο.

---

[21] EUCO 14/17.