

Πέμπτη 22 Νοεμβρίου 2012

(συμπεριλαμβανομένων των ΓΔ HOME, ECHO και ΓΔ SANCO) και οι οργανισμοί της Ένωσης (Ευρωπόλ, Frontex, Ευρωπαϊκό Κέντρο Πρόληψης και Ελέγχου Νόσων και άλλοι).

ο

ο ο

48. αναθέτει στον Πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στην Αντιπρόεδρο της Επιτροπής/Υπατη Εκπρόσωπο, το Συμβούλιο, την Επιτροπή, τα κοινοβούλια των κρατών μελών της ΕΕ, την Κοινοβουλευτική Συνέλευση του NATO και τον Γενικό Γραμματέα του NATO.

P7_TA(2012)0457

Ασφάλεια και άμυνα στον κυβερνοχώρο

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 22ας Νοεμβρίου 2012 σχετικά με την ασφάλεια και την άμυνα στον κυβερνοχώρο (2012/2096(INI))

(2015/C 419/22)

Το Ευρωπαϊκό Κοινοβούλιο,

- έχοντας υπόψη την έκθεση σχετικά με την εφαρμογή της Ευρωπαϊκής Στρατηγικής Ασφάλειας που συμφωνήθηκε από το Ευρωπαϊκό Συμβούλιο στις 11 και 12 Δεκεμβρίου 2008,
- έχοντας υπόψη τη σύμβαση για την κυβερνοεγκληματικότητα του Συμβουλίου της Ευρώπης, η οποία υπεγράφη στη Βουδαπέστη στις 23 Νοεμβρίου 2001,
- έχοντας υπόψη τα συμπεράσματα του Συμβουλίου σχετικά με την προστασία των υποδομών πληροφοριών ζωτικής σημασίας της 27ης Μαΐου 2011 και τα προηγούμενα συμπεράσματα του Συμβουλίου σχετικά με την ασφάλεια στον κυβερνοχώρο,
- έχοντας υπόψη το «Ψηφιακό θεματολόγιο για την Ευρώπη» της Επιτροπής της 19ης Μαΐου 2010 (COM(2010)0245),
- έχοντας υπόψη την οδηγία 2008/114/EK του Συμβουλίου της 8ης Δεκεμβρίου 2008 σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους ⁽¹⁾,
- έχοντας υπόψη την πρόσφατη ανακοίνωση της Επιτροπής σχετικά με την ίδρυση ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο ως προτεραιότητα της στρατηγικής εσωτερικής ασφάλειας (COM(2012)0140),
- έχοντας υπόψη το ψήφισμά του της 10ης Μαρτίου 2010 σχετικά με την εφαρμογή της ευρωπαϊκής στρατηγικής ασφάλειας και της κοινής πολιτικής ασφάλειας και άμυνας ⁽²⁾,
- έχοντας υπόψη το ψήφισμά του της 11ης Μαΐου 2011 σχετικά με την ανάπτυξη της κοινής πολιτικής ασφάλειας και άμυνας μετά την έναρξη ισχύος της Συνθήκης της Λισαβόνας ⁽³⁾,
- έχοντας υπόψη το ψήφισμά του της 22ας Μαΐου 2012 σχετικά με τη Στρατηγική Εσωτερικής Ασφάλειας της Ένωσης ⁽⁴⁾,
- έχοντας υπόψη το ψήφισμά του της 27ης Σεπτεμβρίου 2011 σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 1334/2000 περί κοινοτικού συστήματος ελέγχου των εξαγωγών ειδών και τεχνολογίας διπλής χρήσης ⁽⁵⁾,
- έχοντας υπόψη το ψήφισμά του της 12ης Ιουνίου 2012 σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας — επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο ⁽⁶⁾,

⁽¹⁾ ΕΕ L 345 της 23.12.2008, σ. 75.

⁽²⁾ ΕΕ C 349 Ε της 22.12.2010, σ. 63.

⁽³⁾ Κείμενα που εγκρίθηκαν, P7_TA(2011)0228.

⁽⁴⁾ Κείμενα που εγκρίθηκαν, P7_TA(2012)0207.

⁽⁵⁾ Κείμενα που εγκρίθηκαν, P7_TA(2011)0406.

⁽⁶⁾ Κείμενα που εγκρίθηκαν, P7_TA(2012)0237.

Πέμπτη 22 Νοεμβρίου 2012

- έχοντας υπόψη το ψήφισμα του Συμβουλίου Ανθρωπίνων Δικαιωμάτων του ΟΗΕ της 5ης Ιουλίου 2012 σχετικά με την προαγωγή, προάσπιση και απόλαυση των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο ⁽¹⁾, το οποίο αναγνωρίζει τη σημασία της προάσπισης των ανθρωπίνων δικαιωμάτων και της ελεύθερης διαδικτυακής ροής πληροφοριών,
 - έχοντας υπόψη τα συμπεράσματα της Συνόδου Κορυφής του Σικάγου της 20ης Μαΐου 2012,
 - έχοντας υπόψη τον τίτλο V της Συνθήκης ΕΕ,
 - έχοντας υπόψη το άρθρο 48 του Κανονισμού του,
 - έχοντας υπόψη την έκθεση της Επιτροπής Εξωτερικών Υποθέσεων (A7-0335/2012),
- A. εκτιμώντας ότι, στον σημερινό παγκοσμιοποιημένο κόσμο, η ΕΕ και τα κράτη μέλη της βασίζονται σε μεγάλο βαθμό στην κυβερνοασφάλεια, στην ασφαλή χρήση των πληροφοριών και των ψηφιακών τεχνολογιών και σε ευέλικτες και αξιόπιστες υπηρεσίες πληροφόρησης και συναφείς υποδομές,
- B. εκτιμώντας ότι οι τεχνολογίες πληροφοριών και επικοινωνιών χρησιμοποιούνται και ως μέσα καταστολής· εκτιμώντας ότι το πλαίσιο στο οποίο χρησιμοποιούνται οι τεχνολογίες καθορίζει σε μεγάλο βαθμό τον αντίκτυπο που μπορεί να έχουν οι εν λόγω τεχνολογίες ως μοχλός είτε θετικών εξελίξεων είτε καταστολής,
- Γ. λαμβάνοντας υπόψη ότι οι προκλήσεις, οι απειλές και οι επιθέσεις στον κυβερνοχώρο αυξάνονται με δραματικούς ρυθμούς και συνιστούν μείζονος σημασίας απειλή για την ασφάλεια, την άμυνα, τη σταθερότητα και την ανταγωνιστικότητα των εθνικών κρατών, καθώς και του ιδιωτικού τομέα· εκτιμώντας ότι οι εν λόγω απειλές δεν θα πρέπει να θεωρούνται μελλοντικά ζητήματα· εκτιμώντας ότι η πλειοψηφία των άκρως προβεβλημένων συμβάντων στον κυβερνοχώρο που επιφέρουν αναταραχές έχει πλέον πολιτικά υποκινούμενη φύση· εκτιμώντας ότι αν και η συντριπτική πλειοψηφία των συμβάντων στον κυβερνοχώρο εξακολουθεί να έχει απλοϊκή μορφή, οι απειλές κατά περιουσιακών στοιχείων ζωτικής σημασίας καθίστανται ολοένα και πιο επιτηδευμένες και απαιτούν εις βάθος προστασία,
- Δ. εκτιμώντας ότι ο κυβερνοχώρος, με τους σχεδόν δύο δισεκατομμύρια διασυνδεδεμένους χρήστες σε παγκόσμιο επίπεδο, έχει αναδειχθεί σε ένα από τα πιο δυναμικά και αποτελεσματικά μέσα προαγωγής δημοκρατικών ιδεών και οργάνωσης των πολιτών, καθώς επιδιώκουν να πραγματοποιήσουν τις φιλοδοξίες τους για ελευθερία και αγώνα κατά των δικτατοριών· εκτιμώντας ότι η χρήση του κυβερνοχώρου από μη δημοκρατικά και απολυταρχικά καθεστώτα απειλεί όλο και περισσότερο τα ατομικά δικαιώματα της ελευθερίας της έκφρασης και του συνεταιρίζεσθαι· εκτιμώντας ότι είναι, επομένως, κρίσιμης σημασίας να διασφαλισθεί ότι ο κυβερνοχώρος θα παραμείνει ανοικτός στην ελεύθερη ροή ιδεών, πληροφοριών και της έκφρασης,
- Ε. λαμβάνοντας υπόψη ότι υπάρχουν πολλά εμπόδια πολιτικής, νομοθετικής και οργανωτικής φύσης στην ΕΕ και στα κράτη μέλη της όσον αφορά την ανάπτυξη μιας ολοκληρωμένης και ενιαίας προσέγγισης της κυβερνοάμυνας και της κυβερνοασφάλειας· εκτιμώντας ότι υπάρχει έλλειψη κοινού ορισμού, κοινών προτύπων και κοινών μέτρων στον ευαίσθητο και εύαλωτο τομέα της κυβερνοασφάλειας,
- ΣΤ. εκτιμώντας ότι οι ανταλλαγές και ο συντονισμός εντός των θεσμικών οργάνων της ΕΕ και με τα κράτη μέλη και μεταξύ αυτών, καθώς και με τους εξωτερικούς εταίρους, εξακολουθούν να μην επαρκούν,
- Ζ. εκτιμώντας ότι δεν υφίστανται σαφείς και εναρμονισμένοι ορισμοί για την «κυβερνοασφάλεια» και την «κυβερνοάμυνα» σε επίπεδο ΕΕ και κρατών μελών· εκτιμώντας ότι η κατανόηση της κυβερνοασφάλειας και άλλων σημαντικών όρων ποικίλλει σημαντικά μεταξύ των διαφόρων χωρών,
- Η. εκτιμώντας ότι η ΕΕ δεν έχει αναπτύξει ακόμη δικές της συνεκτικές πολιτικές όσον αφορά την προστασία πληροφοριακών υποδομών ζωτικής σημασίας, γεγονός που καθιστά αναγκαία μια διεπιστημονική προσέγγιση, ενισχύοντας έτσι την ασφάλεια και επιδεικνύοντας παράλληλα σεβασμό στα θεμελιώδη δικαιώματα,
- Θ. λαμβάνοντας υπόψη ότι η ΕΕ έχει προτείνει διάφορες πρωτοβουλίες για την καταπολέμηση της κυβερνοεγκληματικότητας σε επίπεδο πολιτών, συμπεριλαμβανομένης της ίδρυσης ενός νέου Ευρωπαϊκού Κέντρου για Κυβερνοεγκλήματα, αλλά δεν διαθέτει συγκεκριμένο σχέδιο σε επίπεδο ασφάλειας και άμυνας,
- Ι. εκτιμώντας ότι η οικοδόμηση πίστης και εμπιστοσύνης μεταξύ του ιδιωτικού τομέα, των αρχών επιβολής του νόμου, των θεσμών άμυνας και των άλλων αρμόδιων θεσμών είναι ύψιστης σημασίας για την καταπολέμηση της κυβερνοεγκληματικότητας,

⁽¹⁾ <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx>.

Πέμπτη 22 Νοεμβρίου 2012

- ΙΑ. εκτιμώντας ότι η πίστη και η αμοιβαία εμπιστοσύνη στις σχέσεις μεταξύ κρατικών και μη κρατικών παραγόντων αποτελεί προϋπόθεση για την ανάπτυξη αξιόπιστης κυβερνοασφάλειας,
- ΙΒ. λαμβάνοντας υπόψη ότι μεγάλος αριθμός συμβάντων στον κυβερνοχώρο τόσο από τον δημόσιο όσο και από τον ιδιωτικό τομέα εξακολουθούν να μην αναφέρονται λόγω της ευαισθητής φύσης των πληροφοριών και της πιθανής ζημιάς στην εικόνα των εμπλεκόμενων εταιρειών,
- ΙΓ. εκτιμώντας ότι μεγάλος αριθμός συμβάντων στον κυβερνοχώρο λαμβάνει χώρα λόγω της έλλειψης ευελιξίας και ανθεκτικότητας των ιδιωτικών και δημόσιων υποδομών δικτύων, της περιορισμένης προστασίας ή ασφάλειας των βάσεων δεδομένων και άλλων μειονεκτημάτων των υποδομών πληροφοριών ζωτικής σημασίας· εκτιμώντας ότι λίγα μόνο κράτη μέλη θεωρούν την προστασία των δικτύων και των συστημάτων πληροφοριών τους, καθώς και των συναφών δεδομένων, μέρος του αντίστοιχου καθήκοντος επιμέλειάς τους, πράγμα που εξηγεί την έλλειψη επενδύσεων σε υπερσύγχρονη τεχνολογία ασφαλείας, κατάρτιση και ανάπτυξη κατάλληλων κατευθυντήριων γραμμών, ότι μεγάλος αριθμός κρατών μελών εξαρτάται από την τεχνολογία ασφαλείας που αναπτύσσουν τρίτες χώρες, και ότι πρέπει να αυξηθούν οι προσπάθειες για μείωση της εν λόγω εξάρτησης,
- ΙΔ. λαμβάνοντας υπόψη ότι οι περισσότεροι δράστες κυβερνοεπιθέσεων υψηλού επιπέδου, που συνιστούν απειλή για την εθνική ή τη διεθνή ασφάλεια και άμυνα, δεν αναγνωρίζονται ποτέ ούτε διώκονται· εκτιμώντας ότι δεν υπάρχει διεθνώς συμφωνημένη απόκριση σε κρατικά υποστηριζόμενη κυβερνοεπίθεση κατά άλλου κράτους, ούτε συμφωνία για το κατά πόσον αυτό θα μπορούσε να θεωρηθεί *casus belli*,
- ΙΕ. εκτιμώντας ότι ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δραστηριοποιείται ως διαμεσολαβητής των κρατών μελών για να στηρίξει την ανταλλαγή ορθών πρακτικών στον τομέα της κυβερνοασφάλειας, προτείνοντας τρόπους ανάπτυξης, υλοποίησης και διατήρησης μιας στρατηγικής για την κυβερνοασφάλεια, και διαδραματίζει υποστηρικτικό ρόλο σε εθνικές στρατηγικές για την κυβερνοασφάλεια, σε εθνικά σχέδια έκτακτης ανάγκης, στη διοργάνωση πανευρωπαϊκών και διεθνών ασκήσεων για την προστασία υποδομών πληροφοριών ζωτικής σημασίας (CIIP) και στην ανάπτυξη σεναρίων εθνικών ασκήσεων,
- ΙΣΤ. εκτιμώντας ότι έως τον Ιούνιο του 2012 μόνο 10 κράτη μέλη της ΕΕ είχαν εγκρίνει επίσημα μια εθνική στρατηγική για την κυβερνοασφάλεια,
- ΙΖ. εκτιμώντας ότι η κυβερνοάμυνα είναι μία από τις κορυφαίες προτεραιότητες του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ), ο οποίος έχει συγκροτήσει, στο πλαίσιο του σχεδίου ανάπτυξης δυνατοτήτων, μια ομάδα έργου σχετικά με την κυβερνοασφάλεια με την πλειονότητα των κρατών μελών, η οποία συλλέγει εμπειρίες και εισηγείται συστάσεις,
- ΙΗ. εκτιμώντας ότι οι επενδύσεις στην έρευνα και ανάπτυξη της κυβερνοασφάλειας και της κυβερνοάμυνας είναι ζωτικής σημασίας για την προαγωγή και τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας και κυβερνοάμυνας· εκτιμώντας ότι οι αμυντικές δαπάνες για έρευνα και ανάπτυξη έχουν μειωθεί, αντί να ανέλθουν στο 2 % των συνολικών αμυντικών δαπανών, όπως είχε συμφωνηθεί,
- ΙΘ. εκτιμώντας ότι η αύξηση της ευαισθητοποίησης και η ενημέρωση των πολιτών σχετικά με την κυβερνοασφάλεια θα πρέπει να αποτελεί τη βάση κάθε ολοκληρωμένης στρατηγικής για την κυβερνοασφάλεια,
- Κ. εκτιμώντας ότι πρέπει να επιτευχθεί σαφής ισορροπία μεταξύ των μέτρων για την ασφάλεια και των δικαιωμάτων των πολιτών σύμφωνα με την ΣΛΕΕ, όπως το δικαίωμα ιδιωτικότητας, η προστασία των δεδομένων και η ελευθερία της έκφρασης, χωρίς κάποιο από αυτά να θυσιάζεται στο όνομα κάποιου άλλου·
- ΚΑ. εκτιμώντας ότι υπάρχει ολοένα και μεγαλύτερη ανάγκη για περισσότερο σεβασμό και προστασία των ατομικών δικαιωμάτων ιδιωτικότητας όπως ορίζονται στον Χάρτη της ΕΕ και στο άρθρο 16 της ΣΛΕΕ· εκτιμώντας ότι η ανάγκη διασφάλισης και προάσπισης του κυβερνοχώρου σε εθνικό επίπεδο για τα θεσμικά όργανα και τους στρατιωτικούς φορείς, αν και σημαντική, δεν θα πρέπει επ' ουδενί να χρησιμοποιείται ως δικαιολογία για τον περιορισμό, με οποιονδήποτε τρόπο, των δικαιωμάτων και ελευθεριών στον κυβερνοχώρο και στον χώρο των πληροφοριών,
- ΚΒ. εκτιμώντας ότι η παγκόσμια και ασύνορη φύση του διαδικτύου απαιτεί νέες μορφές διεθνούς συνεργασίας και διακυβέρνησης με πολλαπλά ενδιαφερόμενα μέρη,
- ΚΓ. εκτιμώντας ότι οι κυβερνήσεις βασίζονται ολοένα περισσότερο σε ιδιωτικούς παράγοντες για την ασφάλεια των υποδομών ζωτικής σημασίας τους,
- ΚΔ. εκτιμώντας ότι η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) δεν έχει ακόμη συμπεριλάβει προδραστικά στις σχέσεις της με τρίτες χώρες την παράμετρο της κυβερνοασφάλειας,

Πέμπτη 22 Νοεμβρίου 2012

- ΚΕ. εκτιμώντας ότι το Μέσο Σταθερότητας αποτελεί μέχρι στιγμής το μοναδικό πρόγραμμα της ΕΕ το οποίο είναι σχεδιασμένο για την αντιμετώπιση επειγουσών κρίσεων ή παγκόσμιων/διαπεριφερειακών προκλήσεων στον τομέα της ασφάλειας, συμπεριλαμβανομένων απειλών της κυβερνοασφάλειας,
- ΚΣΤ. εκτιμώντας ότι η από κοινού αντιμετώπιση –μέσω της ομάδας εργασίας ΕΕ-ΗΠΑ για την κυβερνοασφάλεια και την κυβερνοεγκληματικότητα– απειλών κυβερνοασφάλειας αποτελεί ένα από τα ζητήματα προτεραιότητας των σχέσεων ΕΕ-ΗΠΑ,

Δράσεις και συντονισμός στην ΕΕ

- σημειώνει ότι οι κυβερνοαπειλές και οι κυβερνοεπιθέσεις κατά κυβερνητικών, διοικητικών, στρατιωτικών και διεθνών φορέων αποτελούν ταχέως αυξανόμενη απειλή που σημειώνεται συχνά τόσο στην ΕΕ όσο και διεθνώς και ότι υπάρχουν σημαντικοί λόγοι που γεννούν ανησυχία ότι κρατικοί και μη κρατικοί παράγοντες, ιδίως τρομοκρατικές και εγκληματικές οργανώσεις, είναι σε θέση να πραγματοποιούν επιθέσεις κατά των ζωτικής σημασίας δομών και υποδομών πληροφοριών και επικοινωνιών των θεσμικών οργάνων και των μελών της ΕΕ, με δυνατότητα πρόκλησης σοβαρής βλάβης, συμπεριλαμβανομένων κινητικών επιπτώσεων·
- υπογραμμίζει, επομένως, την ανάγκη μιας καθολικής και συντονισμένης προσέγγισης των προκλήσεων αυτών σε επίπεδο ΕΕ, με την ανάπτυξη μιας ολοκληρωμένης στρατηγικής της ΕΕ για την κυβερνοασφάλεια, η οποία θα πρέπει να εξασφαλίσει έναν κοινό ορισμό της κυβερνοασφάλειας και της κυβερνοάμυνας, καθώς και του τι συνιστά άμυνα σε σχέση με μια κυβερνοεπίθεση, να προσφέρει ένα κοινό επιχειρησιακό όραμα και να λαμβάνει υπόψη την προστιθέμενη αξία των υφιστάμενων υπηρεσιών και οργανισμών, καθώς και τις ορθές πρακτικές και τα διδάγματα από τα κράτη μέλη που ήδη διαθέτουν εθνική στρατηγική· τονίζει τη ζωτική σημασία του συντονισμού και της δημιουργίας συνεργειών στο επίπεδο της Ένωσης για τη συμβολή στον συνδυασμό διαφορετικών πρωτοβουλιών, προγραμμάτων και δραστηριοτήτων, τόσο στρατιωτικών όσο και μη στρατιωτικών· επισημαίνει ότι η εν λόγω στρατηγική θα πρέπει να διασφαλίζει ευελιξία και να ενημερώνεται σε τακτική βάση, προκειμένου να προσαρμόζεται στη ραγδαία μεταβαλλόμενη φύση του κυβερνοχώρου·
- παροτρύνει την Επιτροπή και την Ύπατη Εκπρόσωπο της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας να εξετάσουν, στην επικείμενη πρότασή τους για τις ρυθμίσεις ενόψει της υλοποίησης της Ρήτρας Αλληλεγγύης (Άρθρο 222 ΣΛΕΕ), το ενδεχόμενο σοβαρής κυβερνοεπίθεσης εναντίον κράτους μέλους· υποστηρίζει επιπλέον ότι, αν και εξακολουθεί να υπάρχει ανάγκη να οριστούν με κοινή ορολογία οι κυβερνοεπιθέσεις που θέτουν σε κίνδυνο την εθνική ασφάλεια, αυτές θα μπορούσαν να καλυφθούν από τη Ρήτρα Αμοιβαίας Άμυνας (άρθρο 42.7 ΣΕΕ), χωρίς να θίγεται η αρχή της αναλογικότητας·
- επισημαίνει ότι η ΚΠΑΑ πρέπει να διασφαλίζει ότι οι δυνάμεις που συμμετέχουν σε στρατιωτικές επιχειρήσεις και αποστολές πολιτικού χαρακτήρα της ΕΕ προστατεύονται έναντι κυβερνοεπιθέσεων· υπογραμμίζει ότι η κυβερνοάμυνα θα πρέπει να καταστεί ενεργός δυνατότητα της ΚΠΑΑ·
- τονίζει ότι όλες οι πολιτικές κυβερνοασφάλειας της ΕΕ θα πρέπει να βασίζονται στη μέγιστη προστασία και διατήρηση των ψηφιακών ελευθεριών και στον σεβασμό των ανθρωπίνων δικαιωμάτων στο επιχειρηματικό περιβάλλον και να είναι σχεδιασμένες έτσι ώστε να συμβάλλουν στη διασφάλισή τους· πιστεύει ότι το Διαδίκτυο και οι τεχνολογίες των επικοινωνιών και των πληροφοριών πρέπει να περιλαμβάνονται στην εξωτερική πολιτική και την πολιτική ασφάλειας της ΕΕ έτσι ώστε να προωθηθεί αυτή η προσπάθεια·
- ζητεί από την Επιτροπή και το Συμβούλιο να αναγνωρίσουν απερίφραστα τις ψηφιακές ελευθερίες ως θεμελιώδη δικαιώματα και ως απαραίτητες προϋποθέσεις για την άσκηση των οικουμενικών ανθρωπίνων δικαιωμάτων· τονίζει ότι στόχος των κρατών μελών πρέπει να είναι να μην διακυβευθούν σε καμία περίπτωση τα δικαιώματα και οι ελευθερίες των πολιτών τους κατά τον καθορισμό των τρόπων απόκρισής τους σε κυβερνοαπειλές και κυβερνοεπιθέσεις και ότι θα πρέπει να υπάρχουν επαρκείς νομοθετικές διαφοροποιήσεις μεταξύ κυβερνοσυμβάντων σε στρατιωτικό και μη στρατιωτικό επίπεδο· ζητεί να δοθεί ιδιαίτερη προσοχή όσον αφορά την επιβολή περιορισμών στην ικανότητα των πολιτών να χρησιμοποιούν τα εργαλεία των τεχνολογιών επικοινωνιών και πληροφοριών·
- ζητεί από το Συμβούλιο και την Επιτροπή να εκπονήσουν, σε συνεργασία με τα κράτη μέλη, Λευκή Βίβλο για την κυβερνοάμυνα, καθορίζοντας σαφείς ορισμούς και κριτήρια για τον διαχωρισμό των κυβερνοεπιθέσεων σε στρατιωτικό και μη στρατιωτικό επίπεδο, σύμφωνα με τα κίνητρα και τις επιπτώσεις τους, καθώς και σε επίπεδο αντίδρασης, συμπεριλαμβανομένης της διερεύνησης, του εντοπισμού και της δίωξης των δράστών·
- διακρίνει τη σαφή ανάγκη επικαιροποίησης της Ευρωπαϊκής Στρατηγικής Ασφάλειας για τον εντοπισμό και την εξεύρεση μέσων καταδίωξης και δικαστικής δίωξης ιδιωτών, σχετιζόμενων με δίκτυα και υποστηριζόμενων από κράτη δράστών κυβερνοεπιθέσεων·

Επίπεδο ΕΕ

- τονίζει τη σημασία της συνεργασίας και του συντονισμού σε οριζόντια βάση σχετικά με την κυβερνοασφάλεια στο εσωτερικό των θεσμικών οργάνων και των οργανισμών της ΕΕ και μεταξύ αυτών·

Πέμπτη 22 Νοεμβρίου 2012

10. τονίζει ότι οι νέες τεχνολογίες δημιουργούν προκλήσεις όσον αφορά τον τρόπο με τον οποίο οι κυβερνήσεις εκτελούν τα βασικά τους καθήκοντα· επαναβεβαιώνει ότι οι πολιτικές ασφαλείας και άμυνας βρίσκονται εν τέλει στα χέρια των κυβερνήσεων, συμπεριλαμβανομένης της επαρκούς δημοκρατικής εποπτείας· λαμβάνει υπό σημείωση τον ολοένα σημαντικότερο ρόλο των ιδιωτικών φορέων για την εκτέλεση καθηκόντων στον τομέα της ασφαλείας και της άμυνας, συχνά χωρίς διαφάνεια, λογοδοσία ή μηχανισμούς δημοκρατικής εποπτείας·
11. τονίζει ότι οι κυβερνήσεις πρέπει να τηρούν τις βασικές αρχές του διεθνούς δημόσιου και του ανθρωπιστικού δικαίου, όπως ο σεβασμός της κρατικής κυριαρχίας και των ανθρωπίνων δικαιωμάτων, όταν χρησιμοποιούν νέες τεχνολογίες στο πλαίσιο των πολιτικών ασφαλείας και άμυνας· επισημαίνει την πολύτιμη εμπειρία κρατών μελών της ΕΕ, όπως η Εσθονία, στον καθορισμό και τον σχεδιασμό πολιτικών κυβερνοασφάλειας και κυβερνοάμυνας·
12. αναγνωρίζει την ανάγκη αξιολόγησης του συνολικού επιπέδου των κυβερνοεπιθέσεων κατά των συστημάτων πληροφοριών και υποδομών της ΕΕ· επισημαίνει, στο πλαίσιο αυτό, την ανάγκη συνεχούς αξιολόγησης του βαθμού ετοιμότητας των θεσμικών οργάνων της ΕΕ για την αντιμετώπιση πιθανών κυβερνοεπιθέσεων· εμμένει ιδίως στην ανάγκη ενίσχυσης των υποδομών πληροφοριών ζωτικής σημασίας·
13. τονίζει επίσης την ανάγκη παροχής πληροφοριών ως προς τα τρωτά σημεία, τις ειδοποιήσεις και προειδοποιήσεις για νέες απειλές στα συστήματα πληροφοριών·
14. σημειώνει ότι οι πρόσφατες κυβερνοεπιθέσεις κατά ευρωπαϊκών πληροφοριακών δικτύων και κυβερνητικών συστημάτων πληροφοριών προκάλεσαν σοβαρή ζημία από οικονομική άποψη και από άποψη ασφαλείας, ο βαθμός της οποίας δεν έχει εκτιμηθεί επαρκώς·
15. καλεί όλα τα θεσμικά όργανα της ΕΕ να καταρτίσουν δικές τους στρατηγικές για την κυβερνοασφάλεια και να εκπονήσουν σχέδια έκτακτης ανάγκης όσον αφορά τα συστήματά τους το συντομότερο δυνατό·
16. καλεί όλα τα θεσμικά όργανα της ΕΕ να συμπεριλάβουν στα σχέδιά τους για την ανάλυση κινδύνου και τη διαχείριση κρίσεων το ζήτημα της διαχείρισης κρίσεων στον κυβερνοχώρο· καλεί, επιπλέον, όλα τα θεσμικά όργανα της ΕΕ να προσφέρουν σε όλο τους το προσωπικό σεμινάρια κατάρτισης για την αύξηση της ευαισθητοποίησης σχετικά με την κυβερνοασφάλεια· προτείνει τη διεξαγωγή κυβερνοασκήσεων, μία φορά ετησίως, όπως γίνεται με τις ασκήσεις έκτακτης ανάγκης·
17. υπογραμμίζει τη σημασία της αποτελεσματικής ανάπτυξης της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική της ΕΕ (EU-CERT) και εθνικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική, καθώς και την ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης σε περίπτωση που είναι αναγκαία η ανάληψη δράσης· επιδοκιμάζει το γεγονός ότι, έως το Μάιο του 2012, όλα τα κράτη μέλη είχαν συγκροτήσει ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική· ενθαρρύνει την περαιτέρω ανάπτυξη εθνικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική και μιας ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική της ΕΕ, οι οποίες θα μπορούν να κινητοποιηθούν εντός 24 ωρών, αν παραστεί ανάγκη· επισημαίνει ότι πρέπει να διερευνηθεί η σκοπιμότητα συμπράξεων δημόσιου-ιδιωτικού τομέα στο πεδίο αυτό·
18. αναγνωρίζει ότι η «Cyber Europe 2010», η πρώτη πανευρωπαϊκή άσκηση για την προστασία υποδομών πληροφοριών ζωτικής σημασίας η οποία διεξήχθη με τη συμμετοχή διάφορων κρατών μελών με επικεφαλής τον ENISA, αποδείχθηκε χρήσιμη ενέργεια και παράδειγμα ορθών πρακτικών· τονίζει επίσης την ανάγκη δημιουργίας του δικτύου προειδοποίησης σχετικά με τις υποδομές ζωτικής σημασίας σε ευρωπαϊκό επίπεδο το συντομότερο δυνατόν·
19. τονίζει τη σημασία των πανευρωπαϊκών ασκήσεων προετοιμασίας για περιπτώσεις μεγάλης κλίμακας συμβάντων ασφαλείας δικτύων, και θεωρεί αναγκαίο τον καθορισμό ενιαίας δέσμης προτύπων για την αξιολόγηση απειλών·
20. καλεί την Επιτροπή να διερευνήσει την αναγκαιότητα και τη σκοπιμότητα μιας θέσης Συντονιστή του κυβερνοχώρου σε επίπεδο ΕΕ·
21. θεωρεί ότι, δεδομένου του υψηλού επιπέδου δεξιότητας που απαιτείται τόσο για την επαρκή προάσπιση των συστημάτων και των υποδομών του κυβερνοχώρου όσο και για τις επιθέσεις σε βάρος αυτών, θα πρέπει να αναπτυχθεί μια «Λευκή» (white hat) στρατηγική μεταξύ της Επιτροπής, του Συμβουλίου και των κρατών μελών· επισημαίνει ότι το δυναμικό «διαρροής εγκεφάλων» σε αυτές τις περιπτώσεις είναι υψηλό και ότι, ιδίως οι ανήλικοι που καταδικάζονται για τέτοιου είδους επιθέσεις, έχουν πολλές δυνατότητες τόσο για αποκατάσταση όσο και για ένταξη στους οργανισμούς και φορείς άμυνας·

Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ)

22. επιδοκιμάζει τις πρόσφατες πρωτοβουλίες και τα έργα σχετικά με την κυβερνοάμυνα, ειδικά όσον αφορά τη συγκέντρωση και τη χαρτογράφηση σχετικών δεδομένων, προκλήσεων και αναγκών στον τομέα της κυβερνοασφάλειας και της κυβερνοάμυνας, και παροτρύνει τα κράτη μέλη να συνεργαστούν περισσότερο, μεταξύ άλλων και σε στρατιωτικό επίπεδο, με τον ΕΟΑ για την κυβερνοάμυνα·

Πέμπτη 22 Νοεμβρίου 2012

23. υπογραμμίζει ότι τα κράτη μέλη πρέπει να συνεργαστούν στενά με τον ΕΟΑ για την ανάπτυξη των εθνικών δυνατοτήτων τους στον τομέα της κυβερνοάμυνας· πιστεύει ότι η ανάπτυξη συνεργειών, η συγκέντρωση και η ανταλλαγή σε ευρωπαϊκό επίπεδο είναι κρίσιμης σημασίας για την αποτελεσματική κυβερνοάμυνα σε ευρωπαϊκό και εθνικό επίπεδο·

24. ενθαρρύνει τον ΕΟΑ να εμβαθύνει τη συνεργασία του με το NATO, με εθνικά και διεθνή κέντρα αριστείας, με το Ευρωπαϊκό Κέντρο Κυβερνοεγκληματικότητας της Ευρωπόλ που συμβάλλει στην ταχύτερη αντίδραση σε περίπτωση κυβερνοεπιθέσεων, και ειδικά το Συνεργατικό Κέντρο Αριστείας για την Κυβερνοάμυνα (CCDCOE), και να επικεντρωθεί στην ανάπτυξη ικανοτήτων, την κατάρτιση καθώς και την ανταλλαγή πληροφοριών και πρακτικών·

25. παρατηρεί με ανησυχία ότι μόνο ένα κράτος μέλος κατάφερε να φθάσει στο 2 % των δαπανών για έρευνα και ανάπτυξη στον τομέα της άμυνας έως το 2010 και ότι πέντε κράτη μέλη δεν πραγματοποίησαν καθόλου δαπάνες για έρευνα και ανάπτυξη το 2010· παροτρύνει τον ΕΟΑ, μαζί με τα κράτη μέλη, να συγκεντρώσει πόρους και να επενδύσει αποτελεσματικά σε συνεργατική έρευνα και ανάπτυξη, με ιδιαίτερη έμφαση στην κυβερνοασφάλεια και στην κυβερνοάμυνα·

Κράτη μέλη

26. καλεί όλα τα κράτη μέλη να αναπτύξουν και να ολοκληρώσουν τις αντίστοιχες εθνικές στρατηγικές τους για την κυβερνοασφάλεια και την κυβερνοάμυνα χωρίς να χρονοτριβούν περαιτέρω και να εξασφαλίσουν ένα σταθερό περιβάλλον διαμόρφωσης πολιτικής και ένα σταθερό ρυθμιστικό περιβάλλον, να αναπτύξουν ολοκληρωμένες διαδικασίες διαχείρισης κινδύνου, καθώς και τα απαιτούμενα προπαρασκευαστικά μέτρα και μηχανισμούς· καλεί τον ENISA να συνδράμει τα κράτη μέλη· καλεί τον ENISA να συνδράμει τα κράτη μέλη· εκφράζει την υποστήριξη του προς τον ENISA για την εκπόνηση οδηγού ορθής πρακτικής σχετικά με ορθές πρακτικές και συστάσεις όσον αφορά τον τρόπο ανάπτυξης, υλοποίησης και διατήρησης μιας στρατηγικής για την κυβερνοασφάλεια·

27. ενθαρρύνει όλα τα κράτη μέλη να δημιουργήσουν καθορισμένες μονάδες κυβερνοασφάλειας και κυβερνοάμυνας στο πλαίσιο της στρατιωτικής δομής τους, με σκοπό τη συνεργασία με παρεμφερείς φορείς σε άλλα κράτη μέλη της ΕΕ·

28. ενθαρρύνει τα κράτη μέλη να συστήσουν εξειδικευμένα δικαστήρια σε περιφερειακό επίπεδο με στόχο την αποτελεσματικότερη καταστολή σε περίπτωση επίθεσης κατά των συστημάτων πληροφοριών· εμμένει στην ανάγκη ενθάρρυνσης της προσαρμογής των εθνικών νομοθεσιών έτσι ώστε να ακολουθούν τις εξελίξεις τόσο σε τεχνικό επίπεδο όσο και σε επίπεδο εφαρμογής·

29. καλεί την Επιτροπή να συνεχίσει να εργάζεται για μια συνεκτική και αποτελεσματική ευρωπαϊκή προσέγγιση, προκειμένου να αποφευχθούν οι πλεονασματικές πρωτοβουλίες, ενθαρρύνοντας και στηρίζοντας τα κράτη μέλη στις προσπάθειές τους να αναπτύξουν μηχανισμούς συνεργασίας και να ενισχύσουν την ανταλλαγή πληροφοριών· πιστεύει ότι πρέπει να καθιερωθεί ένα ελάχιστο επίπεδο υποχρεωτικής συνεργασίας και ανταλλαγής μεταξύ των κρατών μελών·

30. ενθαρρύνει τα κράτη μέλη να καταρτίσουν εθνικά σχέδια έκτακτης ανάγκης και να συμπεριλάβουν τη διαχείριση κυβερνοκρίσεων στα σχέδια διαχείρισης κρίσεων και τις αναλύσεις κινδύνων· υπογραμμίζει, εν συνεχεία, τη σημασία της επαρκούς κατάρτισης στην στοιχειώδη κυβερνοασφάλεια για όλο το προσωπικό των δημόσιων φορέων και ιδίως της παροχής κατάλληλης κατάρτισης στα μέλη των δικαστικών φορέων και των φορέων ασφάλειας σε κέντρα κατάρτισης· ζητεί από τον ENISA και άλλα αρμόδια όργανα να συνδράμουν τα κράτη μέλη στη διασφάλιση της συγκέντρωσης και της ανταλλαγής πόρων, καθώς και της αποφυγής των επικαλύψεων·

31. παροτρύνει τα κράτη μέλη να αναδείξουν την έρευνα και ανάπτυξη σε έναν από τους βασικούς πυλώνες της κυβερνοασφάλειας και της κυβερνοάμυνας και να ενθαρρύνουν την κατάρτιση προγραμματιστών με ειδικευση στην προστασία των συστημάτων πληροφοριών· καλεί τα κράτη μέλη να τηρήσουν τη δέσμευσή τους για αύξηση των αμυντικών δαπανών για έρευνα και ανάπτυξη σε τουλάχιστον 2 %, ιδιαίτερα όσον αφορά την κυβερνοασφάλεια και την κυβερνοάμυνα·

32. καλεί την Επιτροπή και τα κράτη μέλη να προτείνουν προγράμματα για την προώθηση και την αύξηση της ευαισθητοποίησης των τελικών χρηστών, ιδιωτών και επιχειρηματιών, για την προώθηση της γενικής ασφαλούς χρήσης του διαδικτύου, των συστημάτων και των τεχνολογιών πληροφοριών· προτείνει να εγκαινιάσει η Επιτροπή μια δημόσια πανευρωπαϊκή εκπαιδευτική πρωτοβουλία από αυτή την άποψη, καλεί τα κράτη μέλη να συμπεριλάβουν την εκπαίδευση σχετικά με την κυβερνοασφάλεια στα προγράμματα σπουδών των σχολείων από όσο το δυνατόν νεαρότερη ηλικία·

Συνεργασία δημόσιου-ιδιωτικού τομέα

33. υπογραμμίζει τον κρίσιμο ρόλο της ουσιαστικής και συμπληρωματικής συνεργασίας στον τομέα της κυβερνοασφάλειας μεταξύ των δημόσιων αρχών και του ιδιωτικού τομέα, τόσο σε επίπεδο ΕΕ όσο και σε εθνικό επίπεδο, με στόχο την ανάπτυξη αμοιβαίας εμπιστοσύνης· γνωρίζει ότι η περαιτέρω ενίσχυση της αξιοπιστίας και της αποτελεσματικότητας των αρμόδιων δημόσιων

Πέμπτη 22 Νοεμβρίου 2012

οργανισμών θα συμβάλει στην ανάπτυξη εμπιστοσύνης και στην ανταλλαγή κρίσιμων πληροφοριών·

34. καλεί τους εταίρους του ιδιωτικού τομέα να εξετάζουν λύσεις «ασφαλείας βάσει σχεδιασμού» κατά την ανάπτυξη νέων προϊόντων, συσκευών, υπηρεσιών και εφαρμογών, και τη θέσπιση κινήτρων για όσους σχεδιάζουν νέα προϊόντα, συσκευές, υπηρεσίες και εφαρμογές με κεντρικό χαρακτηριστικό την ασφάλεια βάσει σχεδιασμού· ζητεί, στη συνεργασία με τον ιδιωτικό τομέα για την πρόληψη και την καταπολέμηση κυβερνοεπιθέσεων, να υπάρχουν ελάχιστα πρότυπα διαφάνειας και μηχανισμοί λογοδοσίας·

35. επισημαίνει ότι η προστασία των υποδομών πληροφοριών ζωτικής σημασίας αποτελεί μέρος της στρατηγικής εσωτερικής ασφάλειας της ΕΕ στο πλαίσιο των αυξανόμενων επιπέδων ασφάλειας για τους πολίτες καθώς και τις επιχειρήσεις στον κυβερνοχώρο·

36. ζητεί να εγκαθιδρυθεί μόνιμος διάλογος με τους εν λόγω φορείς σχετικά με τη βέλτιστη χρήση και την ανθεκτικότητα των συστημάτων πληροφοριών και τη διαμοιρασμένη ευθύνη που απαιτείται για την ασφαλή και καλή λειτουργία των συστημάτων αυτών·

37. θεωρεί ότι τα κράτη μέλη, η ΕΕ και ο ιδιωτικός τομέας, σε συνεργασία με τον ENISA, πρέπει να εγκρίνουν μέτρα προκειμένου να αυξηθεί η ασφάλεια και η ακεραιότητα των συστημάτων πληροφοριών, να προληφθούν οι επιθέσεις και να μειωθεί στο ελάχιστο ο αντίκτυπος των επιθέσεων· στηρίζει την Επιτροπή στις προσπάθειές της να καταρτίσει ελάχιστα πρότυπα κυβερνοασφάλειας και συστήματα πιστοποίησης για εταιρείες και να παράσχει κατάλληλα κίνητρα για την τόνωση των προσπάθειών του ιδιωτικού τομέα όσον αφορά τη βελτίωση της ασφάλειας·

38. καλεί την Επιτροπή και τις κυβερνήσεις των κρατών μελών να ενθαρρύνουν τους φορείς του ιδιωτικού τομέα και της κοινωνίας των πολιτών να συμπεριλάβουν τη διαχείριση κυβερνοκρίσεων στα σχέδιά τους για τη διαχείριση κρίσεων και στις αναλύσεις κινδύνων· ζητεί, επιπλέον, την καθιέρωση κατάρτισης για την αύξηση της ευαισθητοποίησης σχετικά με τη στοιχειώδη κυβερνοασφάλεια και την κυβερνουγιεινή για όλα τα μέλη του προσωπικού τους·

39. καλεί την Επιτροπή, σε συνεργασία με τα κράτη μέλη και τις αρμόδιες υπηρεσίες και τα όργανα, να αναπτύξουν πλαίσια και μέσα για ένα σύστημα ταχείας ανταλλαγής πληροφοριών που θα διασφαλίζει την ανωνυμία κατά την αναφορά κυβερνοπεριστατικών για τον ιδιωτικό τομέα, θα δίνει τη δυνατότητα στους δημόσιους φορείς να ενημερώνονται συνεχώς και θα παρέχει βοήθεια, όποτε είναι αναγκαίο·

40. τονίζει ότι η ΕΕ πρέπει να διευκολύνει την ανάπτυξη μιας ανταγωνιστικής και καινοτόμου αγοράς για την κυβερνοασφάλεια στην ΕΕ, προκειμένου να δώσει τη δυνατότητα στις ΜΜΕ να δραστηριοποιηθούν στο πεδίο αυτό, γεγονός το οποίο θα συμβάλει στην τόνωση της οικονομικής ανάπτυξης και στη δημιουργία νέων θέσεων εργασίας·

Διεθνής συνεργασία

41. καλεί την ΕΥΕΔ να ακολουθήσει προδραστική προσέγγιση όσον αφορά την κυβερνοασφάλεια και να εντάξει την παράμετρο της κυβερνοασφάλειας σε όλες τις δράσεις της, ειδικότερα όσον αφορά τρίτες χώρες· ζητεί την επιτάχυνση της συνεργασίας και της ανταλλαγής πληροφοριών σχετικά με τον τρόπο αντιμετώπισης των ζητημάτων κυβερνοασφάλειας που ανακύπτουν με τρίτες χώρες·

42. τονίζει ότι η κατάρτιση μιας ολοκληρωμένης στρατηγικής της ΕΕ για την κυβερνοασφάλεια αποτελεί προϋπόθεση για την εδραίωση της αποτελεσματικής διεθνούς συνεργασίας στον τομέα της κυβερνοασφάλειας, την οποία απαιτεί η διασυννοριακή φύση των κυβερνοαπειλών·

43. καλεί τα κράτη μέλη τα οποία δεν έχουν ακόμη υπογράψει ή κυρώσει τη σύμβαση για την κυβερνοεγκληματικότητα (Σύμβαση της Βουδαπέστης) του Συμβουλίου της Ευρώπης να το πράξουν χωρίς περαιτέρω καθυστέρηση· στηρίζει την Επιτροπή και την ΕΥΕΔ στις προσπάθειές τους να προωθήσουν τη σύμβαση και τις αξίες της σε τρίτες χώρες·

44. έχει επίγνωση της ανάγκης για διεθνώς συμφωνημένη και συντονισμένη αντιμετώπιση των κυβερνοαπειλών· καλεί, επομένως, την Επιτροπή, την ΕΥΕΔ και τα κράτη μέλη να ηγηθούν σε όλα τα φόρουμ, αρχής γενομένης από τα Ηνωμένα Έθνη, με προσπάθειες για την επίτευξη ευρύτερης διεθνούς συνεργασίας και εντέλει συμφωνίας σχετικά με τον καθορισμό μιας κοινής αντίληψης ως προς τα πρότυπα συμπεριφοράς στον κυβερνοχώρο καθώς και να εντατικοποιήσουν τη συνεργασία για την εκπόνηση συμφωνιών ελέγχου των κυβερνοόπλων·

45. ενθαρρύνει την ανταλλαγή γνώσεων στον τομέα της κυβερνοασφάλειας με τις χώρες BRICS και άλλες χώρες με αναδυόμενες οικονομίες, με σκοπό να διερευνηθούν τρόποι δυνητικής κοινής αντιμετώπισης της αυξανόμενης κυβερνοεγκληματικότητας και των κυβερνοαπειλών και κυβερνοεπιθέσεων τόσο σε στρατιωτικό όσο και σε μη στρατιωτικό επίπεδο·

Πέμπτη 22 Νοεμβρίου 2012

46. απευθύνει έκκληση στην ΕΥΕΔ και την Επιτροπή να ακολουθήσουν προδραστική προσέγγιση στο πλαίσιο των σχετικών διεθνών φόρουμ και οργανισμών, ιδίως του ΟΗΕ, του ΟΑΣΕ, του ΟΟΣΑ και της Παγκόσμιας Τράπεζας, με στόχο την εφαρμογή της ισχύουσας διεθνούς νομοθεσίας και την επίτευξη ομοφωνίας σχετικά με τα πρότυπα υπεύθυνης κρατικής συμπεριφοράς όσον αφορά την κυβερνοασφάλεια και την κυβερνοάμυνα, και συντονίζοντας τις θέσεις των κρατών μελών με στόχο την προώθηση των βασικών αξιών και πολιτικών της ΕΕ στο πεδίο της κυβερνοασφάλειας και της κυβερνοάμυνας·

47. καλεί το Συμβούλιο και την Επιτροπή, κατά τις διαβουλεύσεις και συμφωνίες συνεργασίας με τρίτες χώρες, ιδιαίτερα εκείνες που προβλέπουν τη συνεργασία ή ανταλλαγή σε θέματα τεχνολογίας, να επιμείνουν στην εφαρμογή ελάχιστων απαιτήσεων για την πρόληψη και την καταπολέμηση της κυβερνοεγκληματικότητας και των κυβερνοεπιθέσεων και για την εφαρμογή ελάχιστων προτύπων για την ασφάλεια των συστημάτων πληροφοριών·

48. καλεί την Επιτροπή να διευκολύνει και να συνδράμει τρίτες χώρες, εάν είναι αναγκαίο, στις προσπάθειές τους να αναπτύξουν τις δυνατότητές τους στον τομέα της κυβερνοασφάλειας και της κυβερνοάμυνας·

Συνεργασία με το NATO

49. επαναλαμβάνει ότι, με βάση τις κοινές τους αξίες και τα στρατηγικά συμφέροντα, η ΕΕ και το NATO έχουν ιδιαίτερη υποχρέωση και δυνατότητα να αντιμετωπίσουν τις αυξανόμενες προκλήσεις στον τομέα της κυβερνοασφάλειας αποτελεσματικότερα και σε στενή συνεργασία, αναζητώντας πιθανή συμπληρωματικότητα, χωρίς επικάλυψη, και με σεβασμό των αντίστοιχων ευθυνών τους·

50. υπογραμμίζει την ανάγκη συγκέντρωσης και ανταλλαγής σε πρακτικό επίπεδο, λαμβάνοντας υπόψη τη συμπληρωματική φύση της προσέγγισης της ΕΕ και του NATO στην κυβερνοασφάλεια και την κυβερνοάμυνα· τονίζει την ανάγκη στενότερης συνεργασίας, ειδικότερα σχετικά με το σχεδιασμό, την τεχνολογία, την κατάρτιση και τον εξοπλισμό όσον αφορά την κυβερνοασφάλεια και την κυβερνοάμυνα·

51. παροτρύνει όλα τα αρμόδια όργανα στην ΕΕ που ασχολούνται με την κυβερνοασφάλεια και την κυβερνοάμυνα, αξιοποιώντας τις υφιστάμενες συμπληρωματικές δραστηριότητες στην ανάπτυξη αμυντικών δυνατοτήτων, να εμβαθύνουν την πρακτική συνεργασία τους με το NATO, με στόχο την ανταλλαγή εμπειριών και την απόκτηση γνώσεων σχετικά με τον τρόπο ανάπτυξης ανθεκτικότητας για τα συστήματά της ΕΕ·

Συνεργασία με τις Ηνωμένες Πολιτείες

52. θεωρεί ότι η ΕΕ και οι ΗΠΑ θα πρέπει να εμβαθύνουν την αμοιβαία συνεργασία τους για την αντιμετώπιση των κυβερνοεπιθέσεων και της κυβερνοεγκληματικότητας, καθώς ο στόχος αυτός αποτέλεσε προτεραιότητα της διατλαντικής σχέσης μετά τη σύνοδο κορυφής ΕΕ-ΗΠΑ του 2010 στη Λισαβόνα·

53. χαιρετίζει τη συγκρότηση, στη σύνοδο κορυφής ΕΕ-ΗΠΑ τον Νοέμβριο 2010, της ομάδας εργασίας ΕΕ-ΗΠΑ για την κυβερνοασφάλεια και την κυβερνοεγκληματικότητα και υποστηρίζει τις προσπάθειές της για την ενσωμάτωση θεμάτων κυβερνοασφάλειας στον διατλαντικό πολιτικό διάλογο·

54. χαιρετίζει την από κοινού χάραξη, από την Επιτροπή και την κυβέρνηση των ΗΠΑ και υπό την κάλυψη της ομάδας εργασίας ΕΕ-ΗΠΑ, ενός κοινού προγράμματος και ενός χάρτη πορείας προς την πραγματοποίηση κοινών/συγχρονισμένων διηπειρωτικών κυβερνοασκήσεων το 2012/2013· σημειώνει τη διεξαγωγή της πρώτης άσκησης με τίτλο «Cyber Atlantic» το 2011·

55. υπογραμμίζει την ανάγκη συνεργασίας μεταξύ των ΗΠΑ και της ΕΕ, ως των μεγαλύτερων πηγών τόσο κυβερνοχώρου όσο και χρηστών, για την προστασία των δικαιωμάτων και των ελευθεριών των πολιτών τους να χρησιμοποιούν τον εν λόγω χώρο· υπογραμμίζει ότι, ενώ η εθνική ασφάλεια αποτελεί πρωταρχικής σημασίας στόχο, ο κυβερνοχώρος θα πρέπει να είναι ασφαλής αλλά και προστατευμένος·

ο

ο ο

56. αναθέτει στον πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στο Συμβούλιο και στην Επιτροπή, στην ΥΕ/ΑΕ, στον ΕΟΑ, στον ENISA και στο NATO.