Πέμπτη 12 Σεπτεμβρίου 2013

4. ζητεί από την Επιτροπή να υποστηρίξει τα κράτη μέλη στη μείωση του μισθολογικού χάσματος μεταξύ των δύο φύλων τουλάχιστον κατά 5 ποσοστιαίες μονάδες σε ετήσια βάση, με στόχο την εξάλειψη του χάσματος έως το 2020·

5. αναγνωρίζει ότι για να επιτευχθεί πολυδιάστατη προσέγγιση σε πολλαπλά επίπεδα, η Επιτροπή πρέπει να στηρίξει τα κράτη μέλη στην προώθηση των ορθών πρακτικών και την εφαρμογή πολιτικών για την εξάλειψη των διαφορών στις αμοιβές των δύο φύλων·

6. προτρέπει την Επιτροπή να αναθεωρήσει χωρίς καθυστέρηση την οδηγία 2006/54/ΕΚ και να προτείνει τροποποιήσεις σε αυτήν σύμφωνα με το άρθρο 32 της οδηγίας και βάσει του άρθρου 157 της ΣΛΕΕ σύμφωνα με τις ακόλουθες λεπτομερείς συστάσεις που καθορίζονται στο παράρτημα του ψηφίσματος του Ευρωπαϊκού Κοινοβουλίου της 24ης Μαΐου 2012·

7. αναθέτει στον Πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στο Συμβούλιο, στην Επιτροπή, και στις κυβερνήσεις των κρατών μελών.

P7_TA(2013)0376

Στρατηγική για την ασφάλεια στον κυβερνοχώρο της ΕΕ: ένας ανοιχτός, ασφαλής και προστατευμένος κυβερνοχώρος

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Σεπτεμβρίου 2013 σχετικά με μια στρατηγική για την ασφάλεια στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο (2013/2606(RSP))

(2016/C 093/16)

Το Ευρωπαϊκό Κοινοβούλιο,

— έχοντας υπόψη την κοινή ανακοίνωση της Επιτροπής και της Ύπατης Εκπροσώπου της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας, της 7ης Φεβρουαρίου 2013, με τίτλο «Στρατηγική Ασφάλειας του Κυβερνοχώρου της Ευρωπαϊκής Ένωσης: ένας ανοιχτός, ασφαλής και προστατευμένος κυβερνοχώρος» (JOIN(2013)0001),

— έχοντας υπόψη την πρόταση οδηγίας, της 7ης Φεβρουαρίου 2013, σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση (COM(2013)0048),

— έχοντας υπόψη την ανακοίνωση της Επιτροπής της 19ης Μαΐου 2010 με τίτλο "Το ψηφιακό θεματολόγιο για την Ευρώπη (COM(2010)0245) και της 18ης Δεκεμβρίου 2012 με τίτλο "Το ψηφιακό θεματολόγιο για την Ευρώπη — Η υλοποίηση της ευρωπαϊκής ανάπτυξης ψηφιακά (COM(2012)0784),

— έχοντας υπόψη την ανακοίνωση της Επιτροπής, της 27ης Σεπτεμβρίου 2012, με τίτλο «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη» (COM(2012)0529),

— έχοντας υπόψη την ανακοίνωση της Επιτροπής της 28ης Μαρτίου 2012 με τίτλο «Αντιμετώπιση του εγκλήματος στην ψηφιακή μας εποχή: ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο» (COM(2012)0140) και τα σχετικά συμπεράσματα του Συμβουλίου της 7ης Ιουνίου 2012,

— έχοντας υπόψη την οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου ([1]),

— έχοντας υπόψη την οδηγία 2008/114/ΕΚ 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 ([2]),

([1]) ΕΕ L 218 της 14.8.2013, σ. 8.
([2]) ΕΕ L 345 της 23.12.2008, σ. 75.

— έχοντας υπόψη την οδηγία 2011/92/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 2011 για την καταπολέμηση της σεξουαλικής κακοποίησης, της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας, με την οποία καταργείται η απόφαση πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου ([1]),

— έχοντας υπόψη το πρόγραμμα της Στοκχόλμης ([2]) σχετικά με την ελευθερία, την ασφάλεια και τη δικαιοσύνη, τις ανακοινώσεις της Επιτροπής με τίτλο «Για ένα χώρο ελευθερίας, ασφάλειας και δικαιοσύνης στην υπηρεσία των πολιτών της Ευρώπης — Σχέδιο δράσης για την εφαρμογή του προγράμματος της Στοκχόλμης» (COM(2010)0171) και «Η στρατηγική εσωτερικής ασφάλειας της ΕΕ στην πράξη: πέντε βήματα για μια ασφαλέστερη Ευρώπη» (COM(2010)0673), και το ψήφισμά του της 22ας Μαΐου 2012 σχετικά με τη Στρατηγική Εσωτερικής Ασφάλειας της Ένωσης ([3]),

— έχοντας υπόψη την κοινή πρόταση απόφασης του Συμβουλίου σχετικά με τις ρυθμίσεις για την εφαρμογή εκ μέρους της Ένωσης της ρήτρας αλληλεγγύης (JOIN(2012)0039),

— έχοντας υπόψη την απόφαση πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου της 28ης Μαΐου 2001, που αφορά την καταπολέμηση της απάτης και της πλαστογραφίας όσον αφορά τα μέσα πληρωμών πλην των μετρητών ([4]),

— 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 ([5]) και τα συμπεράσματα του Συμβουλίου της 27ης Μαΐου 2011 για την ανακοίνωση της Επιτροπής με τίτλο «Προστασία υποδομών πληροφοριών ζωτικής σημασίας — επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο» (COM(2011)0163),

— έχοντας υπόψη το ψήφισμά του της 11ης Δεκεμβρίου 2012 σχετικά με την ολοκλήρωση της ενιαίας ψηφιακής αγοράς ([6]),

— έχοντας υπόψη το ψήφισμά του της 22ας Νοεμβρίου 2012 σχετικά με την ασφάλεια και την άμυνα στον κυβερνοχώρο ([7]),

— έχοντας υπόψη τη θέση του της 16ης Απριλίου 2013 σε πρώτη ανάγνωση επί της πρότασης κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) (COM(2010)0521) ([8]),

— έχοντας υπόψη το ψήφισμά του, της 11ης Δεκεμβρίου 2012, σχετικά με τη θέσπιση μιας Στρατηγικής Ψηφιακής Ελευθερίας στο πλαίσιο της εξωτερικής πολιτικής της ΕΕ ([9]),

— έχοντας υπόψη τη σύμβαση του Συμβουλίου της Ευρώπης της 23ης Νοεμβρίου 2001 για το έγκλημα στον κυβερνοχώρο,

— έχοντας υπόψη τις διεθνείς υποχρεώσεις της Ένωσης, ιδίως με βάση τη Διεθνή Συμφωνία για το Εμπόριο και τις Υπηρεσίες (GATS),

— έχοντας υπόψη το άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) και τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, και ιδίως τα άρθρα 6, 8 και 11 αυτού,

— έχοντας υπόψη τις συνεχιζόμενες διαπραγματεύσεις για τη Διατλαντική Εταιρική Σχέση Εμπορίου και Επενδύσεων (TTIP) μεταξύ της Ευρωπαϊκής Ένωσης και των ΗΠΑ,

— έχοντας υπόψη το άρθρο 110, παράγραφος 2 του Κανονισμού του,

Α. λαμβάνοντας υπόψη ότι οι αυξανόμενες προκλήσεις στον κυβερνοχώρο, υπό τη μορφή των όλο και πιό προηγμένων απειλών και επιθέσεων, συνιστούν μείζονα απειλή για την ασφάλεια, τη σταθερότητα και την οικονομική ευημερία των κρατών μελών, καθώς και του ιδιωτικού τομέα και της ευρύτερης κοινότητας· λαμβάνοντας υπόψη ότι, ως εκ τούτου, η προστασία της κοινωνίας και της οικονομίας μας θα αποτελούν συνεχώς μια εξελισσόμενη πρόκληση·

([1]) ΕΕ L 335 της 17.12.2011, σ. 1.
([2]) ΕΕ C 115 της 4.5.2010, σ. 1.
([3]) Κείμενα που εγκρίθηκαν, P7_TA(2012)0207.
([4]) ΕΕ L 149 της 2.6.2001, σ. 1.
([5]) Κείμενα που εγκρίθηκαν, P7_TA(2012)0237.
([6]) Κείμενα που εγκρίθηκαν, P7_TA(2012)0468.
([7]) Κείμενα που εγκρίθηκαν, P7_TA(2012)0457.
([8]) Κείμενα που εγκρίθηκαν, P7_TA(2013)0103.
([9]) Κείμενα που εγκρίθηκαν, P7_TA(2012)0470.

Πέμπτη 12 Σεπτεμβρίου 2013

Β. λαμβάνοντας υπόψη ότι ο κυβερνοχώρος και η ασφάλεια στον κυβερνοχώρο πρέπει να αποτελέσουν έναν από τους στρατηγικούς πυλώνες της πολιτικής της ΕΕ και κάθε κράτους μέλους στον τομέα της ασφάλειας και άμυνας· λαμβάνοντας υπόψη ότι έχει κομβική σημασία να διασφαλιστεί ότι ο κυβερνοχώρος θα παραμείνει ανοικτός στην ελεύθερη κυκλοφορία ιδεών και πληροφοριών και την ελεύθερη έκφραση·

Γ. λαμβάνοντας υπόψη ότι το ηλεκτρονικό εμπόριο και οι επιγραμμικές υπηρεσίες αποτελούν ζωτική δύναμη του Διαδικτύου και έχουν κομβική σημασία για την επίτευξη των στόχων της στρατηγικής Ευρώπη 2020, καθόσον είναι προς όφελος τόσο των πολιτών όσο και του ιδιωτικού τομέα· λαμβάνοντας υπόψη ότι η Ένωση πρέπει να αξιοποιήσει πλήρως τις δυνατότητες και τις ευκαιρίες που παρουσιάζει το Διαδίκτυο για την περαιτέρω ανάπτυξη της ενιαίας αγοράς, όπου περιλαμβάνεται και η ψηφιακή ενιαία αγορά·

Δ. λαμβάνοντας υπόψη ότι οι στρατηγικές προτεραιότητες που περιγράφονται στην κοινή ανακοίνωση για την στρατηγική της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο περιλαμβάνουν την επίτευξη της κυβερνοανθεκτικότητας, τον περιορισμό του εγκλήματος στον κυβερνοχώρο, την ανάπτυξη πολιτικής στον τομέα της κυβερνοάμυνας και ικανότητες στον κυβερνοχώρο που συνδέονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ), και την καθιέρωση συνεκτικής διεθνούς πολιτικής της ΕΕ για τον κυβερνοχώρο·

Ε. λαμβάνοντας υπόψη τη μεγάλη διασύνδεση που υπάρχει μεταξύ των συστημάτων δικτύων και πληροφοριών στην Ένωση· λαμβάνοντας υπόψη ότι, δεδομένης της παγκόσμιας φύσης του Διαδικτύου, πολλά συμβάντα ασφαλείας τον τομέα των δικτύων και των πληροφοριών υπερβαίνουν τα εθνικά σύνορα και μπορούν εν δυνάμει να υπονομεύσουν τη λειτουργία της εσωτερικής αγοράς και την εμπιστοσύνη των καταναλωτών στην ψηφιακή ενιαία αγορά·

ΣΤ. λαμβάνοντας υπόψη ότι το μέτρο της ισχύος της ασφάλειας στον κυβερνοχώρο στην Ένωση, καθώς και στον υπόλοιπο κόσμο, είναι η αντοχή του πλέον αδύναμου κρίκου της, και ότι διαταραχές σε έναν και μόνο τομέα ή κράτος μέλος επηρεάζουν κάποιον άλλον τομέα ή κράτος μέλος, δημιουργώντας φαινόμενα μετάδοσης του αντικτύπου τα οποία επηρεάζουν το σύνολο της οικονομίας της Ένωσης·

Ζ. λαμβάνοντας υπόψη ότι, μέχρι τον Απρίλιο του 2013, μόνο 13 κράτη μέλη είχαν επισήμως θεσπίσει εθνικές στρατηγικές στον τομέα της ασφάλειας στον κυβερνοχώρο· λαμβάνοντας υπόψη ότι, μεταξύ των κρατών μελών, εξακολουθούν να παραμένουν θεμελιώδεις διαφορές όσον αφορά την ετοιμότητά τους, την ασφάλεια, τη στρατηγική κουλτούρα και την ικανότητα να αναπτύξουν και να εφαρμόσουν εθνικές στρατηγικές στον τομέα της ασφάλειας στον κυβερνοχώρο και λαμβάνοντας υπόψη ότι πρέπει να υπάρξει αξιολόγηση των διαφόρων αυτό·

Η. λαμβάνοντας υπόψη ότι η ύπαρξη διαφορετικής κουλτούρας στον τομέα της ασφάλειας καθώς και η έλλειψη νομικού πλαισίου επιφέρουν κατακερματισμό και δημιουργούν σοβαρή ανησυχία στην ψηφιακή ενιαία αγορά· λαμβάνοντας υπόψη ότι η έλλειψη εναρμονισμένης προσέγγισης στον τομέα της ασφάλειας στον κυβερνοχώρο ενέχει σοβαρούς κινδύνους για την οικονομική ευημερία και την ασφάλεια των συναλλαγών και ότι, συνεπώς, είναι απαραίτητο να υπάρξει συντονισμός των προσπαθειών για στενότερη συνεργασία μεταξύ των κυβερνήσεων, του ιδιωτικού τομέα και των υπηρεσιών επιβολής του νόμου και των υπηρεσιών πληροφοριών·

Θ. λαμβάνοντας υπόψη ότι το έγκλημα στον κυβερνοχώρο αποτελεί ένα όλο και πιο δαπανηρό διεθνές πρόβλημα το οποίο, επί του παρόντος, επιβαρύνει — σύμφωνα με το Γραφείο των Ηνωμένων Εθνών για τον Έλεγχο των Ναρκωτικών και την Πρόληψη του Εγκλήματος — την παγκόσμια οικονομία σχεδόν με 295 δισ. ευρώ κάθε χρόνο·

Ι. λαμβάνοντας υπόψη ότι το διεθνές οργανωμένο έγκλημα, αξιοποιώντας τα τεχνολογικά επιτεύγματα, εξακολουθεί να μεταφέρει το επιχειρησιακό του πεδίο στον κυβερνοχώρο, όπου το έγκλημα στον κυβερνοχώρο μεταβάλλει ριζικά την παραδοσιακή δομή των ομάδων του οργανωμένου εγκλήματος· λαμβάνοντας υπόψη ότι τα ανωτέρω είχαν ως αποτέλεσμα να μην εντοπίζεται εύκολα το οργανωμένο έγκλημα και να είναι σε θέση να εκμεταλλεύεται τις διαφορές που υφίστανται μεταξύ των διαφορετικών νομικών συστημάτων και των διαφορετικών εθνικών δικαιοδοτικών αρχών σε παγκόσμιο επίπεδο·

ΙΑ. λαμβάνοντας υπόψη ότι η διερεύνηση του εγκλήματος στον κυβερνοχώρο από τις αρμόδιες αρχές εξακολουθεί να παρακωλύεται από διάφορα εμπόδια μεταξύ των οποίων η χρήση, στις συναλλαγές στον κυβερνοχώρο, των «εικονικών νομισμάτων» που μπορούν να χρησιμοποιηθούν για ξέπλυμα χρήματος, τα ζητήματα της εδαφικότητας και των ορίων δικαιοδοσίας, η ανεπαρκής κατανομή των ικανοτήτων συλλογής πληροφοριών, η έλλειψη καταρτισμένου προσωπικού και η μη τακτική συνεργασία με άλλους φορείς·

ΙΒ. λαμβάνοντας υπόψη ότι η τεχνολογία αποτελεί το θεμέλιο για την ανάπτυξη του κυβερνοχώρου και η συνεχής προσαρμογή στις τεχνολογικές αλλαγές έχει ζωτική σημασία για τη βελτίωση της ανθεκτικότητας και της ασφάλειας του κυβερνοχώρου της ΕΕ· λαμβάνοντας υπόψη ότι πρέπει να ληφθούν μέτρα για να διασφαλιστεί ότι η νομοθεσία θα επικαιροποιείται σε κάθε νέα τεχνολογική εξέλιξη, παρέχοντας δυνατότητα αποτελεσματικού εντοπισμού και δίωξης των εγκληματιών του κυβερνοχώρου καθώς και την προστασία των θυμάτων του εγκλήματος στον κυβερνοχώρο· λαμβάνοντας υπόψη ότι η στρατηγική για την

ασφάλεια στον κυβερνοχώρο της ΕΕ πρέπει να περιλαμβάνει μέτρα που εστιάζουν στη συνειδητοποίηση, την εκπαίδευση, την ανάπτυξη Ομάδων Άμεσης Επέμβασης Πληροφορικής (CERTs), την ανάπτυξη μιας εσωτερικής αγοράς για τα προϊόντα και υπηρεσίες ασφάλειας στον κυβερνοχώρο, και την προώθηση επενδύσεων στην έρευνα, την ανάπτυξη και την καινοτομία·

1. χαιρετίζει την κοινή ανακοίνωση σχετικά με μια στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο και την πρόταση οδηγίας για τα μέτρα που θα διασφαλίζουν υψηλό επίπεδο ασφάλειας στον τομέα των δικτύων και των πληροφοριών στην Ένωση·

2. υπογραμμίζει την τεράστια και εντεινόμενη σημασία που παίζει το Διαδίκτυο και ο κυβερνοχώρος στις πολιτικές, οικονομικές και κοινωνικές συναλλαγές όχι μόνο εντός της Ένωσης αλλά και σε σχέση με άλλους φορείς σε ολόκληρο τον κόσμο·

3. υπογραμμίζει ότι είναι αναγκαίο να αναπτυχθεί μια στρατηγική επικοινωνιακή πολιτική για την ασφάλεια στον Κυβερνοχώρο στην ΕΕ, τις καταστάσεις κρίσεων στον κυβερνοχώρο, τις ανασκοπήσεις της στρατηγικής, τη συνεργασία δημόσιου και ιδιωτικού τομέα και τους συναγερμούς και τις συστάσεις προς τον κοινό·

4. υπενθυμίζει ότι υψηλό επίπεδο της ασφάλειας στον τομέα των δικτύων και των πληροφοριών απαιτείται όχι μόνο για τη διατήρηση των υπηρεσιών που είναι ζωτικής σημασίας για την εύρυθμη λειτουργία της κοινωνίας και της οικονομίας, αλλά και για την εξασφάλιση της φυσικής ακεραιότητας των πολιτών μέσω της ενίσχυσης της αποδοτικότητας, της αποτελεσματικότητας και της ασφαλούς λειτουργίας των ζωτικών υποδομών· επισημαίνει ότι, ενώ η ασφάλεια των δικτύων και των πληροφοριών πρέπει να αντιμετωπιστεί, σημαντικό επίσης ζήτημα είναι η βελτίωση της φυσικής ασφάλειας· επισημαίνει ότι η υποδομή πρέπει να είναι ανθεκτική τόσο στις εκούσιες όσο και τις ακούσιες δυσλειτουργίες· τονίζει ότι, σε σχέση με αυτό, η στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο πρέπει να δώσει μεγαλύτερη έμφαση στις κοινές αιτίες των ακούσιων αστοχιών του συστήματος·

5. επαναλαμβάνει την έκκλησή του προς τα κράτη μέλη να υιοθετήσουν εθνικές στρατηγικές ασφάλεια στον κυβερνοχώρο που θα καλύπτουν τις τεχνικές πτυχές, τον συντονισμό, καθώς επίσης και τις πτυχές των ανθρώπινων πόρων και της χρηματοδότησης, προκειμένου να διασφαλισθεί η συμμετοχή τους, χωρίς περιττές καθυστερήσεις, και να προβλέψουν συνολικές διαδικασίες διαχείρισης κινδύνου, καθώς και διασφάλιση του ρυθμιστικού περιβάλλοντος·

6. σημειώνει ότι μόνο η συντονισμένη ανάληψη πρωτοβουλίας και η πολιτική εγκόλπωση εκ μέρους των θεσμικών οργάνων της Ένωσης και των κρατών μελών θα εξασφαλίσει δυνατότητες για την επίτευξη υψηλού επιπέδου ασφάλειας των δικτύων και των πληροφοριών σε ολόκληρη την Ένωση, συμβάλλοντας έτσι στην ασφαλή και εύρυθμη λειτουργία της ενιαίας αγοράς·

7. επισημαίνει ότι η πολιτική της Ένωσης στον τομέα της ασφάλειας στον Κυβερνοχώρο πρέπει να εξασφαλίζει ασφαλές και αξιόπιστο ψηφιακό περιβάλλον που θα βασίζεται και θα έχει σχεδιαστεί για να διασφαλίζει την προστασία και διατήρηση των ελευθεριών και τον σεβασμό των θεμελιωδών δικαιωμάτων στις επιγραμμικές υπηρεσίες, όπως ορίζει ο Χάρτης της ΕΕ και το άρθρο 16 της ΣΛΕΕ, ιδίως τα δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων· πιστεύει ότι η ιδιαίτερη προσοχή πρέπει να δοθεί στην προστασία των παιδιών στις επιγραμμικές υπηρεσίες·

8. καλεί τα κράτη μέλη και την Επιτροπή να αναλάβουν όλες τις αναγκαίες ενέργειες για την υποβολή προγραμμάτων κατάρτισης που θα αποσκοπούν στην προώθηση και τη βελτίωση της συνειδητοποίησης, των ικανοτήτων και της εκπαίδευσης των ευρωπαίων πολιτών, ιδίως όσον αφορά την προσωπική ασφάλεια, στο πλαίσιο ενός προγράμματος ψηφιακού αλφαβητισμού από τις νεαρή ηλικία· χαιρετίζει την πρωτοβουλία για την διοργάνωση ενός Ευρωπαϊκού Μήνα για την Ασφάλεια στον Κυβερνοχώρο, με την υποστήριξη της ENISA και σε συνεργασία με τις δημόσιες αρχές και τον ιδιωτικό τομέα, προκειμένου να βελτιωθεί η συνειδητοποίηση όσον αφορά τις προκλήσεις που ενέχει η προστασία των δικτυακών και πληροφοριακών συστημάτων·

9. πιστεύει ότι η εκπαίδευση στην ασφάλεια στον κυβερνοχώρο αυξάνει την συνειδητοποίηση της ευρωπαϊκής κοινωνίας όσον αφορά τις απειλές στον κυβερνοχώρο, ενθαρρύνοντας κατ' αυτόν τον τρόπο την υπεύθυνη χρήση του κυβερνοχώρου και συμβάλλοντας στην προώθηση της παροχής ικανοτήτων στον κυβερνοχώρο· αναγνωρίζει τον κομβικό ρόλο της Europol και του νέου Ευρωπαϊκού Κέντρου Εγκλήματος στο'ν Κυβερνοχώρο (EC3), καθώς και της ENISA και της Eurojust, όσον αφορά την παροχή δράσεων κατάρτισης σε επίπεδο ΕΕ στην αξιοποίηση των εργαλείων διεθνούς δικαστικής συνεργασίας και επιβολής του νόμου που αφορούν τις διάφορες πτυχές που εγκλήματος στον κυβερνοχώρο·

10. επαναλαμβάνει την ανάγκη παροχής τεχνικών συμβουλών και νομικής πληροφόρησης, καθώς και της θέσπισης προγραμμάτων για την πρόληψη και καταπολέμηση του εγκλήματος στον κυβερνοχώρο· ενθαρρύνει την κατάρτιση εξειδικευμένων μηχανικών στον τομέα του κυβερνοχώρου για την προστασία των κρίσιμων υποδομών και των πληροφοριακών συστημάτων, καθώς επίσης και χειριστών των συστημάτων ελέγχου των μεταφορών και των κέντρων διαχείρισης της κυκλοφορίας· επισημαίνει ότι είναι επείγουσα ανάγκη να θεσπιστούν τακτικά προγράμματα κατάρτισης στον τομέα της ασφάλειας στον κυβερνοχώρο για το προσωπικό του δημόσιου τομέα σε όλα τα επίπεδα·

Πέμπτη 12 Σεπτεμβρίου 2013

11. επαναλαμβάνει την έκκλησή του για να δοθεί προσοχή στην εφαρμογή περιορισμών όσον αφορά την ικανότητα των πολιτών να αξιοποιούν τα εργαλεία της τεχνολογίας των επικοινωνιών και της πληροφορίας και επισημαίνει ότι τα κράτη μέλη, στα μέτρα που σχεδιάζουν για την αντιμετώπιση των απειλών και επιθέσεων στον κυβερνοχώρο, πρέπει να αποσκοπούν στο να μη θέτουν ποτέ σε κίνδυνο τα δικαιώματα και τις ελευθερίες των πολιτών και πρέπει να διαθέτουν επαρκή νομοθετικά μέτρα για τη διάκριση των στρατιωτικών και μη στρατιωτικών συμβάντων στον κυβερνοχώρο·

12. θεωρεί ότι η ρυθμιστικού χαρακτήρα συμμετοχή στο πεδίο της ασφάλειας στον κυβερνοχώρο πρέπει να είναι προσανατολισμένη στον κίνδυνο, να εστιάζεται στη ζωτικής σημασίας υποδομή της οποίας η ομαλή λειτουργία συνιστά μείζον δημόσιο συμφέρον και πρέπει να εδράζεται στις υφιστάμενες, με βάση την αγορά προσπάθειες της βιομηχανίας προς εξασφάλιση ανθεκτικότητας του δικτύου· υπογραμμίζει ότι είναι ζωτικός ο ρόλος της σε επιχειρησιακό επίπεδο συνεργασίας για να ευνοείται αποτελεσματικότερη ανταλλαγή πληροφοριών περί απειλής στον κυβερνοχώρο μεταξύ των δημοσίων αρχών και του ιδιωτικού τομέα — στο επίπεδο τόσο της Ένωσης όσο και των κρατών μελών, καθώς και με στρατηγικούς εταίρους της Ένωσης — με στόχο την εξασφάλιση της ασφάλειας των δικτύων και των πληροφοριών, χάρις στην επίτευξη αμοιβαίας εμπιστοσύνης, αξίας και ανάληψης δεσμεύσεων, καθώς και στην ανταλλαγή εμπειρογνωμοσύνης· θεωρεί ότι οι εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα πρέπει να βασίζονται στον ουδέτερο χαρακτήρα του δικτύου και της τεχνολογίας, πρέπει δε να εστιάζονται στην καταβολή προσπαθειών για να επιληφθεί κανείς προβλημάτων με υψηλό δημόσιο αντίκτυπο· καλεί την Επιτροπή να ενθαρρύνει όλους τους εμπλεκομένους οικονομικούς παράγοντες που δραστηριοποιούνται στην αγορά να επαγρυπνούν περισσότερο και να επιδεικνύουν μεγαλύτερη διάθεση για συνεργασία με στόχο την προστασία άλλων οικονομικών παραγόντων από ζημίες στις υπηρεσίες τους·

13. αναγνωρίζει ότι ο εντοπισμός και η κοινοποίηση κρουσμάτων στον τομέα ασφαλείας στον κυβερνοχώρο είναι ζωτικού χαρακτήρα για την προαγωγή της ανθεκτικότητας του κυβερνοχώρου εντός της Ένωσης· πιστεύει ότι πρέπει να ισχύουν αναλογικές και αναγκαίες απαιτήσεις γνωστοποίησης για να καθίσταται δυνατή η κοινοποίηση κρουσμάτων με σημαντικές παραβιάσεις ασφαλείας στις αρμόδιες αρχές των κρατών μελών και με τον τρόπο αυτόν να καθίσταται δυνατή η βελτιωμένη παρακολούθηση κρουσμάτων εγκληματικότητας στον κυβερνοχώρο και να διευκολύνονται οι προσπάθειες για καλύτερη επίγνωση σε όλα τα επίπεδα·

14. ενθαρρύνει την Επιτροπή και άλλους παράγοντες να θεσπίσουν πολιτικές για την ασφάλεια στον κυβερνοχώρο και την ανθεκτικότητα στον κυβερνοχώρο που να περιέχουν οικονομικά κίνητρα προς προαγωγή υψηλών επιπέδων ασφάλειας και ανθεκτικότητας στον κυβερνοχώρο·

Ανθεκτικότητα στον κυβερνοχώρο

15. σημειώνει ότι διαφορετικοί τομείς και διαφορετικά κράτη μέλη έχουν διαφορετικά επίπεδα ικανοτήτων και δεξιοτήτων και ότι τούτο εμποδίζει την ανάπτυξη συνεργασίας βάσει εμπιστοσύνης και υπονομεύει τη λειτουργία της ενιαίας αγοράς·

16. θεωρεί ότι οι απαιτήσεις για τις μικρές και μεσαίου μεγέθους επιχειρήσεις πρέπει να ακολουθούν αναλογική και βασιζόμενη στον κίνδυνο προσέγγιση·

17. εμμένει στην ανάπτυξη ανθεκτικότητας στον κυβερνοχώρο για υποδομές ζωτικής σημασίας και υπενθυμίζει ότι οι επικείμενες διευθετήσεις για την υλοποίηση της ρήτρας αλληλεγγύης (άρθρο 222 ΣΛΕΕ) πρέπει να λαμβάνουν ως ενδεχόμενο τον κίνδυνο επίθεσης στον κυβερνοχώρο κατά κράτους μέλους· καλεί την Επιτροπή και την Ύπατη Εκπρόσωπο να λαμβάνουν αυτόν τον κίνδυνο υπόψη στις από κοινού εκθέσεις αξιολόγησης της απειλής και του κινδύνου που θα εκδίδουν από το 2015·

18. τονίζει ότι, για να διασφαλίζεται η ακεραιότητα, το διαθέσιμο και ο εμπιστευτικός χαρακτήρας των ζωτικής σημασίας υπηρεσιών ειδικότερα, ο προσδιορισμός και η κατηγοριοποίηση των ζωτικής σημασίας υποδομών πρέπει να είναι στοιχεία επικαιροποιημένα και ότι πρέπει να ορισθούν οι απαραίτητες ελάχιστες απαιτήσεις ασφαλείας του δικτύου και των συστημάτων πληροφοριών·

19. αναγνωρίζει ότι η πρόταση οδηγίας που να αφορά μέτρα για να εξασφαλίζεται υψηλό κοινό επίπεδο ασφάλειας του δικτύου και των πληροφοριών σε ολόκληρη την Ένωση προβλέπει αυτές τις ελάχιστες απαιτήσεις ασφαλείας για τους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας και τους φορείς εκμετάλλευσης υποδομών ζωτικής σημασίας·

20. καλεί τα κράτη μέλη και την Ένωση να θεσπίσουν επαρκή πλαίσια για ταχέα συστήματα αμφίδρομης ανταλλαγής πληροφοριών, τα οποία θα εξασφαλίζουν ανωνυμία για τον ιδιωτικό τομέα και θα τηρούν τον δημόσιο τομέα σε σταθερή βάση επικαιροποιημένο, και, όπου κρίνεται απαραίτητο, να παρέχουν συνδρομή στον ιδιωτικό τομέα·

21. χαιρετίζει την ιδέα της Επιτροπής να δημιουργήσει μία νοοτροπία διαχείρισης κινδύνου όσον αφορά την ασφάλεια στον κυβερνοχώρο και παροτρύνει τα κράτη μέλη και τα θεσμικά όργανα της Ένωσης να περιλάβουν ταχέως τη διαχείριση κρίσης στον κυβερνοχώρο στα σχέδια διαχείρισης κρίσεων που εκπονούν και τις αναλύσεις κινδύνου στις οποίες προβαίνουν· καλεί περαιτέρω τις κυβερνήσεις των κρατών μελών και την Επιτροπή να ενθαρρύνουν τους παράγοντες του ιδιωτικού τομέα να περιλαμβάνουν τη διαχείριση κρίσης στον κυβερνοχώρο στα σχέδια διαχείρισης που εκπονούν και τις αναλύσεις κινδύνου στις οποίες προβαίνουν και να εκπαιδεύσουν το προσωπικό τους στην ασφάλεια στον κυβερνοχώρο·

22. καλεί όλα τα κράτη μέλη και τα θεσμικά όργανα της Ένωσης να εγκαθιδρύσουν δίκτυο από εύρυθμης λειτουργίας Ομάδες Άμεσης Επέμβασης Πληροφορικής (CERT) που να επιχειρεί 24 ώρες το 24ωρο και 7 ημέρες την εβδομάδα. επισημαίνει ότι οι εθνικές CERT πρέπει να αποτελούν μέρος ενός αποτελεσματικού δικτύου στο οποίο ανταλλάσσονται πληροφορίες σύμφωνα με τα απαραίτητα πρότυπα εμπιστοσύνης και εμπιστευτικότητας· σημειώνει ότι πρωτοβουλίες επιστέγασμα που να συγκεντρώνουν τις CERT και άλλους σχετικούς φορείς ασφαλείας μπορεί να αποτελούν χρήσιμα εργαλεία για την ανάπτυξη εμπιστοσύνης σε διασυνοριακό και διατομεακό πλαίσιο· αναγνωρίζει πόσο σημαντική είναι η αποδοτική και αποτελεσματική συνεργασία μεταξύ των CERT και των φορέων επιβολής του νόμου στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο·

23. στηρίζει τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) στην επιτέλεση των καθηκόντων του όσον αφορά την ασφάλεια δικτύων και πληροφοριών, ειδικότερα με την παροχή καθοδήγησης και την παροχή συμβουλών στα κράτη μέλη καθώς και με τη στήριξη της ανταλλαγής βελτίστων πρακτικών και την ανάπτυξη περιβάλλοντος εμπιστοσύνης·

24. τονίζει πόσο αναγκαίο είναι να υλοποιεί η βιομηχανία τις αρμόζουσες απαιτήσεις επιδόσεων ασφάλειας στον κυβερνοχώρο σε όλη την αλυσίδα αξίας για προϊόντα του τομέα της τεχνολογίας της πληροφορίας και των επικοινωνιών που χρησιμοποιούνται στα δίκτυα μεταφορών και τα συστήματα πληροφοριών, να επιδίδεται στην κατάλληλη διαχείριση κινδύνου, να εγκρίνει πρότυπα και λύσεις ασφαλείας και να αναπτύσσει βέλτιστες πρακτικές και ανταλλαγή πληροφοριών με σκοπό να εξασφαλίζονται συστήματα μεταφοράς με ασφάλεια στον κυβερνοχώρο·

Βιομηχανικοί και τεχνολογικοί πόροι

25. είναι της γνώμης ότι η εξασφάλιση υψηλού επιπέδου ασφαλείας δικτύων και πληροφοριών διαδραματίζει κεντρικό ρόλο στην αύξηση της ανταγωνιστικότητας τόσο εκείνων που παρέχουν λύσεις ασφαλείας όσο και εκείνων που τις χρησιμοποιούν εντός της Ένωσης· θεωρεί ότι ενώ ο τομέας της ασφαλείας στην τεχνολογία της πληροφορίας στην Ένωση έχει σημαντικό ανεκμετάλλευτο δυναμικό, οι χρήστες από τον ιδιωτικό, τον δημόσιο και τον επιχειρηματικό τομέα συχνά είναι απληροφόρητοι όσον αφορά το κόστος και τα οφέλη της επένδυσης στην ασφάλεια στον κυβερνοχώρο και ούτως παραμένουν ευάλωτοι στις επιζήμιες απειλές στον κυβερνοχώρο· τονίζει ότι η υλοποίηση των CERT είναι σχετικός παράγων εν προκειμένω·

26. πιστεύει ότι για μεγάλη προσφορά και ζήτηση λύσεων στον τομέα της ασφάλειας στον κυβερνοχώρο απαιτούνται επαρκείς επενδύσεις σε πανεπιστημιακούς πόρους, έρευνα και ανάπτυξη και διαμόρφωση ικανοτήτων και γνώσεων από πλευράς των αρχών των κρατών μελών που εμπλέκονται σε θέματα τεχνολογίας της πληροφορίας και των επικοινωνιών, για να ενθαρρύνονται οι καινοτομίες και να επιτυγχάνεται επαρκής επίγνωση όσον αφορά τους κινδύνους ασφαλείας των δικτύων και των πληροφοριών που να οδηγεί σε έναν συντονισμένο ευρωπαϊκό τομέα ασφαλείας·

27. καλεί τα θεσμικά όργανα της Ένωσης και τα κράτη μέλη να λάβουν τα αναγκαία μέτρα για την εγκαθίδρυση «ενιαίας αγοράς για την ασφάλεια στον κυβερνοχώρο» στην οποία χρήστες και προμηθευτές να μπορούν να προβαίνουν σε βέλτιστη χρήση των καινοτομιών, των συνεργιών και της συνδυασμένης εμπειρογνωμοσύνης που προσφέρονται και η οποία να επιτρέπει την είσοδο μικρών και μεσαίου μεγέθους επιχειρήσεων σε αυτή·

28. ενθαρρύνει τα κράτη μέλη να εξετάσουν το ενδεχόμενο να προβαίνουν σε από κοινού επενδύσεις στον ευρωπαϊκό τομέα ασφάλειας στον κυβερνοχώρο, ακριβώς όπως έχει επιτευχθεί και σε άλλους τομείς, όπως είναι ο τομέας της αεροπορίας·

Έγκλημα στον κυβερνοχώρο

29. θεωρεί ότι οι εγκληματικές δραστηριότητες στον κυβερνοχώρο είναι εξίσου επιζήμιες για το ευ ζην των κοινωνιών με τη διάπραξη παραβάσεων στον φυσικό κόσμο και ότι αυτές οι μορφές εγκλήματος συχνά αλληλοενισχύονται, όπως μπορεί να παρατηρηθεί επί παραδείγματι στη σεξουαλική εκμετάλλευση παιδιών και το οργανωμένο έγκλημα και τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες·

30. σημειώνει ότι σε μερικές περιπτώσεις νόμιμες και παράνομες επιχειρηματικές δραστηριότητες συνδέονται· τονίζει πόσο σημαντική είναι η σύνδεση, την οποία διευκολύνει το διαδίκτυο, ανάμεσα στη χρηματοδότηση της τρομοκρατίας και το σοβαρό οργανωμένο έγκλημα· τονίζει ότι πρέπει να δοθεί στο κοινό να κατανοήσει πόσο σοβαρή είναι η εμπλοκή στο έγκλημα στον κυβερνοχώρο και τη δυνατότητα εκείνο που από πρώτη ματιά μπορεί να φαίνεται ένα «κοινωνικά αποδεκτό» έγκλημα — όπως είναι η παράνομη μεταφόρτωση ταινιών — συχνά παράγει μεγάλα ποσά χρημάτων για διεθνή συνδικάτα εγκλήματος·

Πέμπτη 12 Σεπτεμβρίου 2013

31. συμφωνεί με την Επιτροπή ότι οι ίδιες σταθερές και αρχές που ισχύουν μη επιγραμμικά (offline) ισχύουν και επιγραμμικά και συνεπώς ότι η καταπολέμηση του εγκλήματος στον κυβερνοχώρο χρειάζεται να ενταθεί με επικαιροποιημένη νομοθεσία και επιχειρησιακές ικανότητες·

32. έχει την άποψη ότι, με δεδομένο ότι έγκλημα στον κυβερνοχώρο δεν γνωρίζει σύνορα, η καταβολή από κοινού προσπαθειών και η προσφορά εμπειρογνωμοσύνης στο επίπεδο της Ένωσης υπεράνω του επιπέδου των μεμονωμένων κρατών μελών έχουν ιδιαίτερη σημασία και ότι στη Eurojust, το EC3 της Europol, τα CERT και τα πανεπιστήμια και τα κέντρα ερευνών πρέπει να παρασχεθούν επαρκείς πόροι και ικανότητες να λειτουργήσουν κατά τρόπο αρμόζοντα ως κέντρα εμπειρογνωμοσύνης, συνεργασίας και ανταλλαγής πληροφοριών·

33. χαιρετίζει θερμά την εγκαθίδρυση του EC3 και ενθαρρύνει τη μελλοντική ανάπτυξη αυτής της υπηρεσίας και του ζωτικού ρόλου της στον συντονισμό της έγκαιρης και αποτελεσματικής διασυνοριακής ανταλλαγής πληροφοριών και εμπειρογνωμοσύνης προς στήριξη των προσπαθειών για πρόληψη, εντοπισμό και διερεύνηση του εγκλήματος στον κυβερνοχώρο·

34. καλεί τα κράτη μέλη να εξασφαλίζουν ότι οι πολίτες μπορούν εύκολα να έχουν πρόσβαση σε πληροφορίες σχετικά με απειλές στον κυβερνοχώρο και με τον τρόπο να τις καταπολεμήσουν· πιστεύει ότι αυτή η καθοδήγηση πρέπει να περιλαμβάνει πληροφορίες σχετικά με το πώς μπορούν οι χρήστες να προστατεύουν την προσωπική τους σφαίρα στο διαδίκτυο, πώς να εντοπίζουν και να αναφέρουν περιπτώσεις άγρας παιδιών μέσω του διαδικτύου (grooming), πώς να εγκαθιστούν στους υπολογιστές τους λογισμικό και τείχη προστασίας (firewalls), πώς να διαχειρίζονται τους προσωπικούς τους κωδικούς και πώς να εντοπίζουν το ηλεκτρονικό «ψάρεμα» (phishing), τη δόλια εκτροπή σε ψευδεπίγραφους ιστοτόπους (pharming) και άλλες επιθέσεις·

35. εμμένει στο να επικυρώσουν τα κράτη μέλη που δεν το έχουν ακόμη πράξει τη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης σχετικά με το Έγκλημα στον Κυβερνοχώρο χωρίς χρονοτριβή· χαιρετίζει τις σκέψεις του Συμβουλίου της Ευρώπης σχετικά με την ανάγκη επικαιροποίησης της σύμβασης υπό το φως των τεχνολογικών εξελίξεων για να εξασφαλίζεται ότι παραμένει αποτελεσματική στην αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και καλεί την Επιτροπή και τα κράτη μέλη να συμμετάσχουν σε αυτόν τον διάλογο· ενθαρρύνει τις προσπάθειες προαγωγής της επικύρωσης της σύμβασης μεταξύ άλλων κρατών και καλεί την Επιτροπή να την προαγάγει ενεργώς εκτός της Ένωσης·

Άμυνα στον κυβερνοχώρο

36. τονίζει ότι οι προκλήσεις, απειλές και επιθέσεις στον κυβερνοχώρο θέτουν τα συμφέροντα των κρατών μελών που σχετίζονται με την άμυνα και την εθνική τους ασφάλεια εν κινδύνω και ότι οι πολιτικές και οι στρατιωτικές προσεγγίσεις του καθήκοντος της προστασίας των ζωτικής σημασίας υποδομών πρέπει να μεγιστοποιούν τα οφέλη σε αμφότερες τις προσεγγίσεις χάρις στην καταβολή προσπαθειών προς επίτευξη συνεργιών·

37. καλεί συνεπώς τα κράτη μέλη σε εντονότερη συνεργασία με τον Ευρωπαϊκό Οργανισμός Άμυνας (EDA) με σκοπό την ανάπτυξη προτάσεων και πρωτοβουλιών για ικανότητες άμυνας στον κυβερνοχώρο αξιοποιώντας τις πρόσφατες πρωτοβουλίες και έργα· υπογραμμίζει την ανάγκη αύξησης της έρευνας και ανάπτυξης μεταξύ άλλων μέσω της συγκέντρωσης και από κοινού χρήσης των πόρων·

38. επαναλαμβάνει ότι μία περιεκτική στρατηγικής ασφαλείας στον κυβερνοχώρο της ΕΕ θα πρέπει να λαμβάνει υπόψη την προστιθέμενη αξία από υφιστάμενες υπηρεσίες και φορείς καθώς και τις βέλτιστες πρακτικές που συγκεντρώνονται από τα κράτη μέλη που έχουν ήδη θεσπίσει αφ' εαυτών εθνικές στρατηγικές ασφαλείας στον κυβερνοχώρο·

39. καλεί την Αντιπρόεδρο/Ύπατη Εκπρόσωπο να περιλάβει τη διαχείριση κρίσεων στον κυβερνοχώρο στον σχεδιασμό για τη διαχείριση κρίσεων, τονίζει δε πόσο αναγκαίο είναι να αναπτύξουν τα κράτη μέλη σε συνεργασία με τον EDA σχέδια προς προστασία των αποστολών και επιχειρήσεων της ΚΠΑΑ από επιθέσεις στον κυβερνοχώρο· καλεί τα κράτη μέλη να συγκροτήσουν κοινή ευρωπαϊκή δύναμη άμυνας στον κυβερνοχώρο·

40. υπογραμμίζει την καλή συνεργασία στην πράξη που υπάρχει με το ΝΑΤΟ στο πεδίο της ασφάλειας στον κυβερνοχώρο και την ανάγκη να καταστεί αυτή η συνεργασία εντονότερη, ειδικότερα μέσω στενότερου συντονισμού στα πεδία του σχεδιασμού, της τεχνολογίας, της κατάρτισης και του εξοπλισμού·

41. ζητεί από την Ένωση να καταβάλει προσπάθειες για να επιτύχει ανταλλαγές με διεθνείς εταίρους, περιλαμβανομένου του ΝΑΤΟ, να εντοπίσει πεδία συνεργασίας, να αποφεύγει την αλληλεπικάλυψη και να επιτυγχάνει τη συμπληρωματικότητα των δραστηριοτήτων, σε όποιον τομέα είναι τούτο δυνατό·

Πέμπτη 12 Σεπτεμβρίου 2013

Διεθνής πολιτική

42. πιστεύει ότι η διεθνής συνεργασία και διεξαγωγή διαλόγου διαδραματίζουν ουσιαστικό ρόλο δημιουργώντας κλίμα εμπιστοσύνης και διαφάνειας και προάγοντας υψηλού επιπέδου δημιουργία δικτύων και ανταλλαγή πληροφοριών σε παγκόσμιο επίπεδο· καλεί ως εκ τούτου την Επιτροπή και την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης να συγκροτήσουν ομάδα διπλωματίας στον κυβερνοχώρο, στις αρμοδιότητες της οποίας θα εντάσσεται η προαγωγή του διαλόγου με χώρες και οργανώσεις της αυτής νοοτροπίας· ζητεί από την ΕΕ να συμμετέχει περισσότερο ενεργά στο ευρύ φάσμα διεθνών υψηλού επιπέδου διασκέψεων σχετικά με την ασφάλεια στον κυβερνοχώρο·

43. θεωρεί ότι πρέπει να επιτευχθεί ισορροπία ανάμεσα στους αντιθέτων κατευθύνσεων στόχους των διασυνοριακών διαβιβάσεων δεδομένων, της προστασίας των δεδομένων και της ασφάλειας στον κυβερνοχώρο σύμφωνα με τις διεθνείς υποχρεώσεις της Ένωσης, κυρίως δυνάμει της GATS·

44. καλεί την Αντιπρόεδρο/Ύπατη Εκπρόσωπο να εγγράψει τη διάσταση της ασφάλειας στον κυβερνοχώρο στον κύριο κορμό δραστηριοτήτων της εξωτερικής δράσης, ειδικά σε σχέση με τρίτα κράτη, για να επιτευχθεί εντονότερη συνεργασία καθώς και την ανταλλαγή εμπειριών και πληροφοριών σχετικά με το πώς να αντιμετωπίζεται η ασφάλεια στον κυβερνοχώρο·

45. ζητεί από την Ένωση να καταβάλει προσπάθειες για να επιτύχει ανταλλαγές με διεθνείς εταίρους με σκοπό να εντοπίσει πεδία συνεργασίας, να αποφεύγει την αλληλεπικάλυψη και να επιτυγχάνει τη συμπληρωματικότητα των δραστηριοτήτων, σε όποιον τομέα είναι τούτο δυνατό· καλεί την Αντιπρόεδρο/Ύπατη Εκπρόσωπο και την Επιτροπή να είναι προορατικές στους διεθνείς οργανισμούς και να συντονίσουν τις θέσεις των κρατών μελών σχετικά με το πώς να προάγουν λύσεις και πολιτικές στο πεδίο του κυβερνοχώρου κατά τρόπο αποτελεσματικό·

46. είναι της γνώμης ότι πρέπει να καταβληθούν προσπάθειες για να εξασφαλισθεί ότι τα υφιστάμενα διεθνή νομικά μέσα, συγκεκριμένα η Σύμβαση του Συμβουλίου της Ευρώπης σχετικά με το Έγκλημα στον Κυβερνοχώρο, επιβάλλονται στον κυβερνοχώρο· θεωρεί ως εκ τούτου ότι επί του παρόντος δεν χρειάζεται να υπάρξουν νέα νομικά μέσα στο διεθνές επίπεδο· χαιρετίζει ωστόσο τη διεθνή συνεργασία για την ανάπτυξη κανόνων συμπεριφοράς για τον κυβερνοχώρο υποστηρίζοντας το κράτος δικαίου στον κυβερνοχώρο· θεωρεί ότι πρέπει να εξετασθεί η επικαιροποίηση των υφισταμένων νομικών μέσων για να αντανακλάται η πρόοδος που σημειώνει η τεχνολογία· έχει την άποψη ότι τα θέματα δικαιοδοσίας απαιτούν εις βάθος συζήτηση σχετικά με το θέμα της δικαστικής συνεργασίας και δίωξης σε ποινικές υποθέσεις σε διεθνική κλίμακα·

47. θεωρεί ότι συγκεκριμένα η Ομάδα Εργασίας ΕΕ-ΗΠΑ σχετικά με την Ασφάλεια στον Κυβερνοχώρο και το Έγκλημα στον Κυβερνοχώρο πρέπει να αποτελέσει μέσο για την ανταλλαγή, όπου αρμόζει, βελτίστων πρακτικών σχετικά με τις πολιτικές ασφαλείας στον κυβερνοχώρο ανάμεσα στην ΕΕ και τις ΗΠΑ· σημειώνει εν προκειμένω ότι τομείς που συνδέονται με την ασφάλεια στον κυβερνοχώρο, όπως είναι οι υπηρεσίες που εξαρτώνται από την ασφαλή λειτουργία του δικτύου και των συστημάτων πληροφοριών, θα περιληφθούν στις επικείμενες διαπραγματεύσεις της Διατλαντικής Εταιρικής Σχέσης στον Τομέα του Εμπορίου και των Επενδύσεων (TTIP), που θα πρέπει να ολοκληρωθεί με τρόπο που θα διασφαλίζει την κυριαρχία και την ανεξαρτησία της ΕΕ και των θεσμικών της οργάνων·

48. σημειώνει ότι οι δεξιότητες ασφαλείας στον κυβερνοχώρο και η ικανότητα πρόληψης, εντοπισμού και ακύρωσης στην πράξη απειλών και δολίων επιθέσεων δεν έχουν ομοιόμορφη ανάπτυξη παγκοσμίως· τονίζει ότι οι προσπάθειες αυξημένης ανθεκτικότητας στον κυβερνοχώρο και καταπολέμησης απειλών στον κυβερνοχώρο δεν πρέπει να περιορίζονται σε ομοφρονούντες εταίρους αλλά πρέπει να απευθύνονται και σε περιοχές με ολιγότερο ανεπτυγμένες ικανότητες, τεχνική υποδομή και νομικά πλαίσια· πιστεύει ότι επί του θέματος είναι ζωτικής σημασίας ο συντονισμός των CERT· καλεί την Επιτροπή να διευκολύνει — και, εάν απαιτείται, να βοηθήσει — τις προσπάθειες που καταβάλλουν τρίτα κράτη για να αποκτήσουν δικές τους ικανότητες ασφάλειας στον κυβερνοχώρο χρησιμοποιώντας κατάλληλα μέσα·

Υλοποίηση

49. ζητεί να διενεργούνται τακτικές αξιολογήσεις της αποτελεσματικότητας των στρατηγικών για την ασφάλεια στον κυβερνοχώρο των κρατών μελών στο ύψιστο πολιτικό επίπεδο με στόχο να εξασφαλίζεται η προσαρμογή στις νέες παγκόσμιες απειλές και να υπάρχουν εχέγγυα για ασφάλεια στον κυβερνοχώρο του ιδίου επιπέδου στα διάφορα κράτη μέλη·

50. ζητεί από την Επιτροπή να εκπονήσει σαφή χάρτη πορείας που να ορίζει τους χρόνους για την επίτευξη στόχων στο επίπεδο της Ένωσης δυνάμει της στρατηγικής ασφάλειας στον κυβερνοχώρο καθώς και για την αποτίμησή τους· καλεί τα κράτη μέλη να συμφωνήσουν ένα παρόμοιο σχέδιο επίτευξης στόχων για τις εθνικές τους δραστηριότητες δυνάμει αυτής της στρατηγικής·

Πέμπτη 12 Σεπτεμβρίου 2013

51. ζητεί τακτικές εκθέσεις — από την Επιτροπή, τα κράτη μέλη, την Europol και το προσφάτως ιδρυθέν EC3, την Eurojust και τον ENISA — με αποτίμηση της προόδου που σημειώνεται σχετικά με τους στόχους που θέτει η στρατηγική ασφαλείας στον κυβερνοχώρο, περιλαμβανομένων βασικών δεικτών επιδόσεων που να μετρούν την πρόοδο της υλοποίησης·

o

o o

52. αναθέτει στον Πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στο Συμβούλιο, την Επιτροπή, τις κυβερνήσεις και τα κοινοβούλια των κρατών μελών, την Europol, την Eurojust και το Συμβούλιο της Ευρώπης.

P7_TA(2013)0377

Ψηφιακό θεματολόγιο για την ανάπτυξη, την κινητικότητα και την απασχόληση

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Σεπτεμβρίου 2013 σχετικά με το ψηφιακό θεματολόγιο για την ανάπτυξη την κινητικότητα και την απασχόληση: Καιρός να ανεβάσουμε ταχύτητα (2013/2593(RSP))

(2016/C 093/17)

Το Ευρωπαϊκό Κοινοβούλιο,

— έχοντας υπόψη την ανακοίνωση της Επιτροπής της 18ης Δεκεμβρίου 2012 με τίτλο «Το Ψηφιακό Θεματολόγιο για την Ευρώπη — ψηφιακή καθοδήγηση της ευρωπαϊκής μεγέθυνσης» — COM(2012)0784,

— έχοντας υπόψη τις ερωτήσεις προς την Επιτροπή και το Συμβούλιο σχετικά «ψηφιακό θεματολόγιο για την ανάπτυξη την κινητικότητα και την απασχόληση: Καιρός να ανεβάσουμε ταχύτητα» (O-000085/– B7-0219/2013 και O-000086 — B7-0220/2013),

— έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 531/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2012, για την περιαγωγή σε δημόσια δίκτυα κινητών επικοινωνιών μέσα στην Ένωση ([1]),

— έχοντας υπόψη την απόφαση αριθ. 243/2012/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Μαρτίου 2012, σχετικά με την καθιέρωση πολυετούς προγράμματος πολιτικής για το ραδιοφάσμα ([2]),

— έχοντας υπόψη τις συνεχείς διαπραγματεύσεις για τη σύσταση της Διευκόλυνσης «Συνδέοντας την Ευρώπη» και ειδικότερα την τροποποιημένη πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με προσανατολισμούς για τα διευρωπαϊκά δίκτυα τηλεπικοινωνιών και την κατάργηση της απόφασης αριθ. 1336/97/ΕΚ — (COM(2013)0329),

— έχοντας υπόψη το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 5ης Μαΐου 2010 σχετικά με ένα νέο ψηφιακό θεματολόγιο για την Ευρώπη: 2015.eu ([3]),

— έχοντας υπόψη την ανακοίνωση της Ευρωπαϊκής Επιτροπής της 27ης Σεπτεμβρίου 2012 με τίτλο «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη» COM(2012)0529),

— έχοντας υπόψη την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Ιανουαρίου 2012, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων) (COM(2012)0011),

---

([1]) ΕΕ L 172 της 30.6.2012, σ. 10.
([2]) ΕΕ L 81 της 21.3.2012, σ. 7.
([3]) ΕΕ C 81 E της 15.3.2011, σ. 45