Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 23 Μαΐου 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	23 Μαΐου 2022
Αποδέκτης:	Αντιπροσωπίες
Θέμα:	Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο – Συμπεράσματα του Συμβουλίου, όπως εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022

Διαβιβάζονται συνημμένως προς τις αντιπροσωπίες τα συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, όπως εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 23 Μαΐου 2022.

ΠΑΡΑΡΤΗΜΑ

Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με:

– την κοινή ανακοίνωση της 25ης Ιουνίου 2013 προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο με θέμα τη στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: «Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο»[1],

– το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα[2],

– τη διακυβέρνηση του διαδικτύου[3],

– τη διπλωματία στον κυβερνοχώρο[4],

– την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας[5],

– την κοινή ανακοίνωση της 20ής Νοεμβρίου 2017 προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ»[6],

– πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»)[7],

– τη συντονισμένη αντιμετώπιση σε επίπεδο ΕΕ συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο[8],

– τις κατευθυντήριες γραμμές για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο[9],

– την εκτελεστική απόφαση (ΕΕ) 2018/1993 του Συμβουλίου, της 11ης Δεκεμβρίου 2018, ως προς τις ρυθμίσεις για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων της ΕΕ[10],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.
10 ΕΕ L 320 της 17.12.2018, σ. 28.

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

– τη σημασία του 5G για την ευρωπαϊκή οικονομία και την ανάγκη μετριασμού των κινδύνων ασφάλειας που συνδέονται με το 5G[12],

– το μέλλον μιας Ευρώπης ψηφιοποιημένης σε μεγάλο βαθμό μετά το 2020: «Τόνωση της ψηφιακής και οικονομικής ανταγωνιστικότητας σε ολόκληρη την Ένωση και της ψηφιακής συνοχής»[13],

– τις συμπληρωματικές προσπάθειες για την ενίσχυση της ανθεκτικότητας και την αντιμετώπιση των υβριδικών απειλών[14],

– τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης[15],

– την κυβερνοασφάλεια των συνδεδεμένων συσκευών[16],

– τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία[17],

– την ασφάλεια και την άμυνα[18],

– τη διερεύνηση των δυνατοτήτων της πρωτοβουλίας για την Κοινή Κυβερνομονάδα — για τη συμπλήρωση της συντονισμένης αντιμετώπισης σε επίπεδο ΕΕ περιστατικών και κρίσεων κυβερνοασφάλειας μεγάλης κλίμακας[19],

– τη στρατηγική πυξίδα για την ασφάλεια και την άμυνα — Για μια Ευρωπαϊκή Ένωση που προστατεύει τους πολίτες, τις αξίες και τα συμφέροντά της και συμβάλλει στη διεθνή ειρήνη και ασφάλεια[20],

---

11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. ΕΠΙΣΗΜΑΙΝΕΙ ότι η κακόβουλη συμπεριφορά στον κυβερνοχώρο, τόσο από κρατικούς όσο και από μη κρατικούς φορείς, έχει ενταθεί τα τελευταία έτη, και σε αυτή περιλαμβάνεται η απότομη και συνεχής έξαρση κακόβουλων δραστηριοτήτων που στοχεύουν τις υποδομές ζωτικής σημασίας, τις αλυσίδες εφοδιασμού και τη διανοητική ιδιοκτησία της ΕΕ και των κρατών μελών της, ο αυξημένος κίνδυνος δευτερογενών επιπτώσεων όπως και η αύξηση των επιθέσεων λυτρισμικού κατά των επιχειρήσεων, των οργανισμών και των πολιτών μας. ΣΗΜΕΙΩΝΕΙ ότι, με την επιστροφή στην πολιτική της ισχύος, ορισμένες χώρες προσπαθούν όλο και περισσότερο να αμφισβητήσουν και να υπονομεύσουν τη βασισμένη σε κανόνες διεθνή τάξη στον κυβερνοχώρο, μετατρέποντας τον κυβερνοχώρο, όπως και την ανοικτή θάλασσα, τον αέρα και το απώτερο διάστημα, σε έναν ολοένα και πιο διαφιλονικούμενο τομέα. ΑΝΑΓΝΩΡΙΖΕΙ ότι οι μεγάλης κλίμακας κυβερνοεπιθέσεις ή οι απόπειρες διείσδυσης, διατάραξης ή καταστροφής των συστημάτων δικτύων και πληροφοριών που προκαλούν συστημικές επιπτώσεις έχουν γίνει συχνότερες, θα μπορούσαν να υπονομεύσουν την οικονομική μας ασφάλεια και να επηρεάσουν τους δημοκρατικούς θεσμούς και διαδικασίες μας, και δείχνουν την ετοιμότητα ορισμένων παραγόντων να θέσουν σε κίνδυνο τη διεθνή ασφάλεια και σταθερότητα. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι η στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας κατέδειξε ότι οι επιθετικές δραστηριότητες στον κυβερνοχώρο μπορούν να διεξαχθούν ως αναπόσπαστο μέρος υβριδικών στρατηγικών που συνδυάζουν εκφοβισμό, αποσταθεροποίηση και οικονομική αναταραχή.

2. ΕΠΑΝΑΛΑΜΒΑΝΕΙ ότι, ενόψει των σημερινών γεωπολιτικών αλλαγών, η ισχύς της Ένωσής μας έγκειται στην ενότητα, την αλληλεγγύη και την αποφασιστικότητα, και ότι η εφαρμογή της στρατηγικής πυξίδας θα ενισχύσει τη στρατηγική αυτονομία της ΕΕ και την ικανότητά της να συνεργάζεται με εταίρους για τη διαφύλαξη των αξιών και των συμφερόντων της, μεταξύ άλλων στον κυβερνοχώρο. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι μια ισχυρότερη και πιο ικανή ΕΕ στον τομέα της ασφάλειας και της άμυνας θα συμβάλει θετικά στην παγκόσμια και τη διατλαντική ασφάλεια και λειτουργεί συμπληρωματικά προς το ΝΑΤΟ, το οποίο παραμένει το θεμέλιο της συλλογικής άμυνας για τα μέλη του. ΕΠΑΝΑΒΕΒΑΙΩΝΕΙ την πρόθεση της ΕΕ να εντείνει την υποστήριξη στη βασιζόμενη σε κανόνες διεθνή τάξη, με τα Ηνωμένα Έθνη στον πυρήνα της.

3. Σύμφωνα με τα συμπεράσματα του Συμβουλίου σχετικά με τη στρατηγική κυβερνοασφάλειας της ΕΕ και στο πνεύμα της στρατηγικής πυξίδας, ΕΠΑΝΑΛΑΜΒΑΝΕΙ την ανάγκη να διαμορφώσουμε τη στάση της Ένωσης στον κυβερνοχώρο, ενισχύοντας την ικανότητά μας να προλαμβάνουμε κυβερνοεπιθέσεις μέσω της δημιουργίας ικανοτήτων, της ανάπτυξης δυνατοτήτων, της κατάρτισης, της διοργάνωσης ασκήσεων, της ενίσχυσης της ανθεκτικότητας και της δυναμικής αντιμετώπισης κυβερνοεπιθέσεων κατά της ΕΕ και των κρατών μελών της, αξιοποιώντας όλα τα διαθέσιμα μέσα της ΕΕ. Αυτό περιλαμβάνει την περαιτέρω επίδειξη της αποφασιστικότητας της ΕΕ να παρέχει άμεσες και μακροπρόθεσμες απαντήσεις σε παράγοντες απειλής που επιδιώκουν να μας στερήσουν την ασφαλή και ανοικτή πρόσβαση στον κυβερνοχώρο και να θίξουν τα στρατηγικά μας συμφέροντα, συμπεριλαμβανομένης της ασφάλειας των εταίρων μας. Στο πλαίσιο αυτό, ΤΟΝΙΖΕΙ ότι η στάση στον κυβερνοχώρο αποσκοπεί να συγκεράσει τις διάφορες πρωτοβουλίες που συντρέχουν τις δράσεις της ΕΕ για την εδραίωση της ειρήνης και της σταθερότητας στον κυβερνοχώρο καθώς και για την υποστήριξη ενός ανοικτού, ελεύθερου, παγκόσμιου, σταθερού και ασφαλούς κυβερνοχώρου, να συντονίσει καλύτερα τις βραχυπρόθεσμες, μεσοπρόθεσμες και μακροπρόθεσμες δράσεις για την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κυβερνοαπειλών και επιθέσεων, καθώς και να κινητοποιήσει δυνατότητες στον κυβερνοχώρο. ΕΠΙΣΗΜΑΙΝΕΙ ότι τα στοιχεία αυτά θα πρέπει να ενσωματωθούν στη στάση της ΕΕ στον κυβερνοχώρο, σύμφωνα με τις πέντε λειτουργίες της ΕΕ στον κυβερνοχώρο: ενίσχυση της ανθεκτικότητας και των ικανοτήτων προστασίας μας στον κυβερνοχώρο· ενίσχυση της αλληλέγγυας και ολοκληρωμένης διαχείρισης κρίσεων· προώθηση του οράματός μας για τον κυβερνοχώρο· ενίσχυση της συνεργασίας με χώρες εταίρους και διεθνείς οργανισμούς· πρόληψη και άμυνα κατά κυβερνοεπιθέσεων και αντιμετώπισή τους.

I. ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΚΑΙ ΤΩΝ ΙΚΑΝΟΤΗΤΩΝ ΠΡΟΣΤΑΣΙΑΣ ΜΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

4. ΕΠΑΝΑΛΑΜΒΑΝΕΙ την ανάγκη να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας της ΕΕ, ΠΡΟΣΒΛΕΠΕΙ στην ταχεία έγκριση του σχεδίου οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (NIS), του σχεδίου κανονισμού σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA) και του σχεδίου οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων (CER) και ΣΗΜΕΙΩΝΕΙ την πρόταση κανονισμού για τον καθορισμό μέτρων για υψηλό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και οργανισμούς της Ένωσης, προκειμένου να προωθηθεί μια Ευρωπαϊκή Ένωση που προστατεύει τους πολίτες, τις δημόσιες υπηρεσίες και τις επιχειρήσεις της στον κυβερνοχώρο. ΕΝΘΑΡΡΥΝΕΙ την Επιτροπή να ολοκληρώσει την έγκριση βασικών προτάσεων για να διασφαλιστεί ότι οι ψηφιακές υποδομές, οι τεχνολογίες, τα προϊόντα και οι υπηρεσίες είναι ασφαλείς, προκειμένου να σταλεί σαφές μήνυμα σχετικά με τις φιλοδοξίες της ΕΕ για αυτά τα θέματα και να καταστεί δυνατή η στήριξη των εταιρειών ώστε να αντεπεξέλθουν στην πρόκληση. ΚΑΛΕΙ την Επιτροπή να προτείνει κοινές ενωσιακές απαιτήσεις κυβερνοασφάλειας για τις συνδεδεμένες συσκευές καθώς και για τις συναφείς διαδικασίες και υπηρεσίες μέσω της πράξης για την κυβερνοανθεκτικότητα, η οποία θα πρέπει να προταθεί από την Επιτροπή πριν από το τέλος του 2022, λαμβάνοντας υπόψη την ανάγκη για οριζόντια και ολιστική προσέγγιση που θα καλύπτει ολόκληρο τον κύκλο ζωής των ψηφιακών προϊόντων καθώς και τις υφιστάμενες ρυθμίσεις, ιδίως στον τομέα της κυβερνοασφάλειας.

5. ΚΑΛΕΙ τις αρμόδιες αρχές, όπως ο Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και η ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS), από κοινού με την Ευρωπαϊκή Επιτροπή, να διατυπώσουν συστάσεις, βάσει αξιολόγησης κινδύνου, προς τα κράτη μέλη και την Ευρωπαϊκή Επιτροπή, προκειμένου να ενισχυθεί η ανθεκτικότητα των δικτύων και των υποδομών επικοινωνιών εντός της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένης της υπό υλοποίηση εργαλειοθήκης 5G της ΕΕ.

6. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να εντείνουν τις προσπάθειες για να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας, για παράδειγμα διευκολύνοντας την ανάδυση αξιόπιστων παρόχων υπηρεσιών κυβερνοασφάλειας, και ΤΟΝΙΖΕΙ ότι η ενθάρρυνση της δημιουργίας τέτοιων παρόχων θα πρέπει να αποτελεί προτεραιότητα για τη βιομηχανική πολιτική της ΕΕ στον τομέα της κυβερνοασφάλειας. Με σκοπό την ενίσχυση της ανθεκτικότητας και την καλύτερη αντιμετώπιση των κυβερνοεπιθέσεων με πιθανές συστημικές επιπτώσεις και αντλώντας διδάγματα από τον χειρισμό των τρωτών σημείων των Solarwinds, Microsoft Exchange και Apache Log4J, ΚΑΛΕΙ την Επιτροπή να προτείνει επιλογές ώστε να ενθαρρυνθεί η ανάδυση ενός αξιόπιστου κλάδου υπηρεσιών κυβερνοασφάλειας, να ενισχυθεί η κυβερνοασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ, να αντιμετωπιστούν οι δυνητικές επιπτώσεις των τρωτών σημείων του λογισμικού για την ΕΕ και τα κράτη μέλη της, μεταξύ άλλων ενόψει της επικείμενης πράξης για την κυβερνοανθεκτικότητα, καθώς και να βελτιωθούν οι δυνατότητες εντοπισμού και κοινοποίησης κυβερνοαπειλών εντός και μεταξύ των κρατών μελών.

7. ΕΠΑΝΑΛΑΜΒΑΝΟΝΤΑΣ ότι οι επενδύσεις στην καινοτομία και η καλύτερη αξιοποίηση της μη στρατιωτικής τεχνολογίας έχουν καίρια σημασία για την ενίσχυση της τεχνολογικής μας κυριαρχίας, μεταξύ άλλων στον κυβερνοχώρο, ΚΑΛΕΙ την Επιτροπή να θέσει ταχέως σε επιχειρησιακή λειτουργία το Ευρωπαϊκό Κέντρο Αρμοδιότητας για Θέματα Κυβερνοασφάλειας για την ανάπτυξη ενός ισχυρού ευρωπαϊκού οικοσυστήματος έρευνας, βιομηχανίας και τεχνολογίας στον κυβερνοχώρο, ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη προώθησης της έρευνας και της καινοτομίας, περισσότερων επενδύσεων σε μη στρατιωτικούς και αμυντικούς τομείς για την ενίσχυση της τεχνολογικής και βιομηχανικής βάσης της ΕΕ στον τομέα της άμυνας (EDTIB), καθώς και την ανάγκη ανάπτυξης των δυνατοτήτων της ΕΕ και των κρατών μελών της στον κυβερνοχώρο, συμπεριλαμβανομένων των δυνατοτήτων στρατηγικής υποστήριξης. ΕΠΙΣΗΜΑΙΝΕΙ τη σημασία της εντατικής αξιοποίησης νέων τεχνολογιών, ιδίως της κβαντικής υπολογιστικής, της τεχνητής νοημοσύνης και των μαζικών δεδομένων, για την επίτευξη συγκριτικών πλεονεκτημάτων, μεταξύ άλλων όσον αφορά τις επιχειρήσεις αντιμετώπισης κυβερνοπεριστατικών.

8. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ ότι η ενίσχυση της κυβερνοασφάλειάς μας είναι ένας τρόπος για να αυξηθεί η αποτελεσματικότητα και η ασφάλεια των προσπαθειών μας στην ξηρά, στον αέρα, στη θάλασσα και στο απώτερο διάστημα, ΕΠΙΣΗΜΑΙΝΕΙ τη σημασία της ενσωμάτωσης των μελημάτων για την κυβερνοασφάλεια σε όλες τις δημόσιες πολιτικές της ΕΕ, συμπεριλαμβανομένης της τομεακής νομοθεσίας με την οποία συμπληρώνεται η οδηγία NIS 2, και ΚΑΛΕΙ την Επιτροπή να διερευνήσει επιλογές για την αύξηση της κυβερνοασφάλειας σε ολόκληρη την αλυσίδα εφοδιασμού της τεχνολογικής και βιομηχανικής βάσης της ΕΕ στον τομέα της άμυνας (EDTIB).

9. ΑΝΑΓΝΩΡΙΖΕΙ ότι η εξασφάλιση επαρκών οικονομικών και ανθρώπινων πόρων για την κυβερνοασφάλεια και μέτρων που αποσκοπούν στη δημιουργία ευνοϊκού περιβάλλοντος για την ανταγωνιστικότητα του ιδιωτικού τομέα έχει ουσιαστική σημασία για τη διαμόρφωση της στάσης της ΕΕ στον κυβερνοχώρο και ότι το ζήτημα της σταθερής και μακροχρόνιας χρηματοδότησης της κυβερνοασφάλειας θα πρέπει επίσης να αντιμετωπιστεί σε επίπεδο ΕΕ με τον σχεδιασμό και την υλοποίηση οριζόντιου μηχανισμού που θα συνδυάζει πολλαπλές πηγές χρηματοδότησης, συμπεριλαμβανομένου του κόστους ανθρώπινων πόρων υψηλής εξειδίκευσης. Ως εκ τούτου, ΚΑΛΕΙ την Επιτροπή να διερευνήσει επιλογές για έναν τέτοιο μηχανισμό πριν από το τέλος του 2022, οι οποίες θα συζητηθούν στα αρμόδια όργανα του Συμβουλίου.

10. ΕΠΙΣΗΜΑΙΝΕΙ την ανάγκη να εντείνουμε τις προσπάθειές μας και να ενισχύσουμε τη συνεργασία για την καταπολέμηση του διεθνούς εγκλήματος στον κυβερνοχώρο, ιδίως του λυτρισμικού, μέσω του μηχανισμού EMPACT (Ευρωπαϊκή Πολυκλαδική Πλατφόρμα κατά των Εγκληματικών Απειλών), με ανταλλαγές μεταξύ του τομέα της κυβερνοασφάλειας, της επιβολής του νόμου και του διπλωματικού κλάδου, καθώς και μέσω της ενίσχυσης των δυνατοτήτων επιβολής του νόμου για την έρευνα και τη δίωξη του εγκλήματος στον κυβερνοχώρο. ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη δέσμευσή του να ενημερώνει το κοινό σχετικά με τις κυβερνοαπειλές και τα μέτρα που λαμβάνονται σε εθνικό και ενωσιακό επίπεδο κατά των απειλών αυτών, με τη συμμετοχή της κοινωνίας των πολιτών, του ιδιωτικού τομέα και της πανεπιστημιακής κοινότητας, με σκοπό την αύξηση της ευαισθητοποίησης και την ενθάρρυνση κατάλληλου επιπέδου κυβερνοπροστασίας και κυβερνοϋγιεινής. ΤΟΝΙΖΕΙ την ανάγκη να επικεντρωθούμε στις δεξιότητες και τις ικανότητες των πολιτών στον τομέα της κυβερνοασφάλειας σε επίπεδο ΕΕ και κρατών μελών, καθώς και την ανάγκη ενεργού εμπλοκής των χρηστών για τη δική τους προστασία.

II. **ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΛΛΗΛΕΓΓΥΑΣ ΚΑΙ ΟΛΟΚΛΗΡΩΜΕΝΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΡΙΣΕΩΝ**

11. Με βάση τις ετήσιες ασκήσεις στον κυβερνοχώρο, άλλες ασκήσεις που εμπεριέχουν τη διάσταση του κυβερνοχώρου και την άσκηση CyCLES 2022 της ΕΕ, ΤΟΝΙΖΕΙ τη σημασία της θέσπισης προγράμματος τακτικών διακοινοτικών και πολυεπίπεδων κυβερνοασκήσεων με σκοπό τη δοκιμή και την ανάπτυξη της εσωτερικής και εξωτερικής αντίδρασης της ΕΕ σε περιστατικά μεγάλης κλίμακας στον κυβερνοχώρο, με τη συμμετοχή του Συμβουλίου, της ΕΥΕΔ, της Επιτροπής και σχετικών ενδιαφερομένων, όπως ο ENISA και ο ιδιωτικός τομέας, και το οποίο θα διαρθρωθεί στο πλαίσιο της γενικής πολιτικής της ΕΕ για τις ασκήσεις και θα συμβάλει σε αυτή. ΕΠΙΣΗΜΑΙΝΕΙ τη σημασία της περαιτέρω ανάπτυξης των ασκήσεων Cyber Europe και BlueOLEx, με συνδυασμένη αντίδραση σε διάφορα επίπεδα. ΑΝΑΓΝΩΡΙΖΕΙ την ανάγκη να αξιολογηθούν και να παγιωθούν οι υφιστάμενες ασκήσεις και να διερευνηθεί το ενδεχόμενο περαιτέρω ασκήσεων για συγκεκριμένα τμήματα του κυβερνοχώρου, ιδίως μια στρατιωτική άσκηση CERT και μια άσκηση που θα επικεντρώνεται στη συνεργασία σε καταστάσεις κρίσης μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. ΑΝΑΓΝΩΡΙΖΕΙ ότι η στάση της Ένωσης στον κυβερνοχώρο θα ενισχύσει την ικανότητά μας για την πρόληψη κυβερνοεπιθέσεων μέσω διαφόρων δράσεων, συμπεριλαμβανομένης της κατάρτισης, και, ως εκ τούτου, ΚΑΛΕΙ τα κράτη μέλη να ενισχύσουν τη συνεργασία του στρατιωτικού και του μη στρατιωτικού τομέα όσον αφορά προγράμματα κυβερνοκατάρτισης και κοινές κυβερνοασκήσεις.

12. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη περαιτέρω δοκιμής και ενίσχυσης της επιχειρησιακής συνεργασίας και της κοινής επίγνωσης της κατάστασης μεταξύ των κρατών μελών, μεταξύ άλλων μέσω καθιερωμένων δικτύων όπως το δίκτυο CSIRT και το δίκτυο οργανισμών σύνδεσης για τις κρίσεις στον κυβερνοχώρο (EU CyCLONe), προκειμένου να προωθηθεί η ετοιμότητα της ΕΕ για την αντιμετώπιση περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι είναι σημαντικό να καταβληθούν προσπάθειες για την ανάπτυξη κοινής γλώσσας μεταξύ των κρατών μελών και με τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ, η οποία θα είναι προσαρμοσμένη για συζήτηση σε πολιτικό επίπεδο, προκειμένου να υποστηριχτεί η θέσπιση ενοποιημένης αξιολόγησης της σοβαρότητας και του αντικτύπου των σχετικών περιστατικών στον κυβερνοχώρο καθώς και των πιθανών σεναρίων εξέλιξης και των αναγκών που προκύπτουν από αυτά, κατά περίπτωση. ΥΠΟΓΡΑΜΜΙΖΕΙ σχετικά την ανάγκη να βελτιωθεί η συμπληρωματικότητα των κοινών εκθέσεων αξιολόγησης της κατάστασης, συμπεριλαμβανομένων των εκθέσεων του EU CyCLONe σχετικά με τον αντίκτυπο και τη σοβαρότητα περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο στο σύνολο των κρατών μελών της ΕΕ, και των αξιολογήσεων απειλών από το EU INTCEN στο πλαίσιο της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο. ΚΑΛΕΙ την Επιτροπή, τον ύπατο εκπρόσωπο και την ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών, σε συντονισμό με τα αρμόδια μη στρατιωτικά και στρατιωτικά όργανα και οργανισμούς και καθιερωμένα δίκτυα, συμπεριλαμβανομένου του δικτύου EU CyCLONe, να διενεργήσουν έως το τέλος του 2022 αξιολόγηση κινδύνου και να εκπονήσουν σενάρια κινδύνου από την άποψη της κυβερνοασφάλειας σε κατάσταση απειλής ή πιθανής επίθεσης κατά κρατών μελών ή χωρών εταίρων και να τα υποβάλουν στα αρμόδια όργανα του Συμβουλίου. ΕΠΙΣΗΜΑΙΝΕΙ την ανάγκη κατάλληλης και συντονισμένης ενημέρωσης του κοινού σχετικά με την αντίδραση της ΕΕ σε περιστατικά μεγάλης κλίμακας στον κυβερνοχώρο.

13. Σε περίπτωση περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο, ΤΟΝΙΖΕΙ την ανάγκη να ενισχυθεί ο συντονισμός και, κατά περίπτωση, με βάση την πρόοδο που έχει επιτευχθεί και το έργο των ομάδων ταχείας αντίδρασης στον κυβερνοχώρο της PESCO καθώς και με βάση τις εργασίες του δικτύου CSIRT και του EU CyCLONe, να ενισχυθεί η εθελοντική συγκέντρωση των ικανοτήτων μας για την αντιμετώπιση περιστατικών μεταξύ των κρατών μελών. ΑΝΑΓΝΩΡΙΖΕΙ ότι η ανάπτυξη δεσμών με τον ιδιωτικό τομέα θα μπορούσε να ενισχύσει τις ικανότητες του δημόσιου τομέα, ιδίως σε ένα περιβάλλον ελλείψεων δεξιοτήτων σε ολόκληρη την ΕΕ, και ότι ο εντοπισμός και ο συντονισμός αυτών των ιδιωτικών εταίρων θα μπορούσαν να συμβάλουν σημαντικά στην περίπτωση περιστατικών μεγάλης κλίμακας. Με σκοπό μια ολοκληρωμένη προετοιμασία για την αντιμετώπιση περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο, ΚΑΛΕΙ την Επιτροπή να υποβάλει πρόταση σχετικά με ένα νέο Ταμείο Αντιμετώπισης Έκτακτων Αναγκών για την Κυβερνοασφάλεια έως το τέλος του τρίτου τριμήνου του 2022.

14. Σύμφωνα με τη στρατηγική πυξίδα, ΕΠΑΝΑΛΑΜΒΑΝΕΙ την ανάγκη να επενδύσουμε στην αμοιβαία συνδρομή που διαθέτουμε δυνάμει του άρθρου 42 παράγραφος 7 της Συνθήκης για την Ευρωπαϊκή Ένωση, καθώς και στην αλληλεγγύη δυνάμει του άρθρου 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, ιδίως μέσω συχνών ασκήσεων. Στο πλαίσιο αυτό, ΤΟΝΙΖΕΙ την ανάγκη να καταβληθούν περαιτέρω προσπάθειες για την παροχή και τον συντονισμό διμερούς μη στρατιωτικής και/ή στρατιωτικής στήριξης, μεταξύ άλλων με τη διερεύνηση πιθανής στήριξης από την ΕΕ κατόπιν ρητού αιτήματος των κρατών μελών, και για τον καθορισμό κατάλληλων μέτρων αντιμετώπισης, μεταξύ άλλων μέσω της ανάπτυξης μιας συντονισμένης επικοινωνιακής στρατηγικής στο πλαίσιο της εφαρμογής του άρθρου 42 παράγραφος 7. ΣΗΜΕΙΩΝΕΙ ότι αυτό θα μπορούσε επίσης να περιλαμβάνει τη διερεύνηση των δεσμών μεταξύ των υφιστάμενων μηχανισμών διαχείρισης κρίσεων της ΕΕ και του μηχανισμού πολιτικής προστασίας της ΕΕ.

15. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι για μια ενισχυμένη στάση της ΕΕ στον κυβερνοχώρο θα απαιτηθούν ενισχυμένες ασφαλείς επικοινωνίες. Για τον σκοπό αυτό, ΕΠΑΝΑΛΑΜΒΑΝΕΙ τους προσανατολισμούς που παρέχει σχετικά η στρατηγική πυξίδα και ΚΑΛΕΙ την Επιτροπή και τα άλλα αρμόδια θεσμικά και λοιπά όργανα και οργανισμούς να προβούν, έως το τέλος του 2022, σε χαρτογράφηση των υφιστάμενων εργαλείων ασφαλούς επικοινωνίας στον τομέα του κυβερνοχώρου, η οποία θα συζητηθεί στα αρμόδια όργανα του Συμβουλίου και με τις αρμόδιες ομάδες συνεργασίας, όπως το δίκτυο CSIRT και το EU CyCLONe.

III. ΠΡΟΩΘΗΣΗ ΤΟΥ ΟΡΑΜΑΤΟΣ ΜΑΣ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

16. ΥΠΕΝΘΥΜΙΖΕΙ ότι η κοινή και ολοκληρωμένη προσέγγιση της ΕΕ στην κυβερνοδιπλωματία αποσκοπεί να συμβάλει στην πρόληψη συγκρούσεων, στον μετριασμό των απειλών κατά της κυβερνοασφάλειας και στην ενίσχυση της σταθερότητας στις διεθνείς σχέσεις. Στο πλαίσιο αυτό, ΕΠΑΝΕΒΑΙΩΝΕΙ την προσήλωση της ΕΕ στην επίλυση διεθνών διαφορών στον κυβερνοχώρο με ειρηνικά μέσα και την εφαρμογή του διεθνούς δικαίου, συμπεριλαμβανομένου του διεθνούς δικαίου για τα ανθρώπινα δικαιώματα και του διεθνούς ανθρωπιστικού δικαίου, στις δράσεις των κρατών στον κυβερνοχώρο. ΥΠΟΓΡΑΜΜΙΖΕΙ τη δέσμευση της ΕΕ και των κρατών μελών της να ενεργούν σύμφωνα με τους προαιρετικούς, μη δεσμευτικούς κανόνες υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο που έχουν συμφωνηθεί από όλα τα κράτη μέλη του ΟΗΕ. ΤΟΝΙΖΕΙ τη σημασία ενός ανοικτού, ελεύθερου, παγκόσμιου, σταθερού και ασφαλούς κυβερνοχώρου στον οποίο εφαρμόζονται πλήρως τα ανθρώπινα δικαιώματα, οι θεμελιώδεις ελευθερίες και το κράτος δικαίου για τη στήριξη της κοινωνικής ευημερίας, της οικονομικής ανάπτυξης, της ευμάρειας και της ακεραιότητας των ελεύθερων και δημοκρατικών κοινωνιών μας και ΕΠΑΝΑΒΕΒΑΙΩΝΕΙ τη δέσμευση της ΕΕ και των κρατών μελών της να συνεχίσουν να προωθούν αυτές τις αξίες και τις αρχές. Με σκοπό την ανάπτυξη διαύλων για εποικοδομητικό, ειλικρινή και ανοικτό διάλογο με βασικούς ενδιαφερομένους του κυβερνοχώρου, ΤΟΝΙΖΕΙ ότι είναι σημαντικό να καταστούν τα ζητήματα κυβερνοχώρου, συμπεριλαμβανομένης της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο, αναπόσπαστο μέρος των διαπραγματεύσεων προσχώρησης στην Ένωση και των στρατηγικών και πολιτικών διαλόγων της ΕΕ με διεθνείς εταίρους ή και ανταγωνιστές, και ταυτόχρονα, ΚΑΛΕΙ τον ύπατο εκπρόσωπο να επανεξετάσει τους υφιστάμενους διμερείς διαλόγους για τον κυβερνοχώρο και, εάν χρειαστεί, να προτείνει την έναρξη παρόμοιας συνεργασίας με επιπλέον χώρες ή σχετικούς διεθνείς οργανισμούς.

17. ΥΠΕΝΘΥΜΙΖΕΙ τη σημασία της πολυμερούς συνεργασίας, καθώς και άλλοι ενδιαφερόμενοι φέρουν ευθύνη για την ασφάλεια στον κυβερνοχώρο, ιδίως όσον αφορά την εφαρμογή των συστάσεων και των αποφάσεων που λαμβάνονται στα διεθνή και περιφερειακά φόρουμ. ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να προωθήσουν περαιτέρω το μοντέλο μας για τον κυβερνοχώρο και το διαδίκτυο με βάση την πολυσυμμετοχική προσέγγιση και μέσω πρωτοβουλιών όπως η έκκληση του Παρισιού για εμπιστοσύνη και ασφάλεια στον κυβερνοχώρο και η διακήρυξη για το μέλλον του διαδικτύου, δίνοντας έμφαση στα κοινά οφέλη της σταθερότητας στον κυβερνοχώρο και αυξάνοντας την ευαισθητοποίηση σε παγκόσμιο επίπεδο σχετικά με τους κινδύνους μιας κρατικοκεντρικής και αυταρχικής αντίληψης του διαδικτύου, και ΚΑΛΕΙ την ΕΕ και τα κράτη μέλη της να ενισχύσουν περαιτέρω τη συνεργασία με την πολυσυμμετοχική κοινότητα, μεταξύ άλλων με την αξιοποίηση σχετικών έργων, όπως η πρωτοβουλία για τη διπλωματία στον κυβερνοχώρο του μέσου εξωτερικής πολιτικής της ΕΕ.

18. ΔΕΣΜΕΥΕΤΑΙ να συνεχίσει να συμμετέχει σε διαδικασίες στο πλαίσιο σχετικών διεθνών οργανισμών, ιδίως στις διαδικασίες που σχετίζονται με την πρώτη επιτροπή και την τρίτη επιτροπή του ΟΗΕ, τονίζοντας παράλληλα ότι το ισχύον διεθνές δίκαιο εφαρμόζεται ανεπιφύλακτα στον κυβερνοχώρο και σε σχετικούς με τον κυβερνοχώρο τομείς. ΤΟΝΙΖΕΙ τη σημασία της συνέχισης των προσπαθειών για την υποστήριξη και την προαγωγή του πλαισίου των Ηνωμένων Εθνών για υπεύθυνη συμπεριφορά των κρατών, ΥΠΟΓΡΑΜΜΙΖΕΙ δε ότι η ΕΕ και τα κράτη μέλη της θα καταβάλουν ενεργές προσπάθειες για την ενισχυμένη υλοποίησή του, μεταξύ άλλων μέσω της θέσπισης του προγράμματος δράσης για την προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA). ΕΠΙΣΗΜΑΙΝΕΙ ότι η ΕΕ και τα κράτη μέλη της θα συμμετέχουν ενεργά στις διαπραγματεύσεις για μια μελλοντική σύμβαση των Ηνωμένων Εθνών που θα χρησιμεύσει ως αποτελεσματικό μέσο για τις αρχές επιβολής του νόμου και τις δικαστικές αρχές στον παγκόσμιο αγώνα κατά του κυβερνοεγκλήματος, λαμβάνοντας πλήρως υπόψη το υφιστάμενο πλαίσιο των διεθνών και περιφερειακών πράξεων στον τομέα αυτό, ιδίως τη σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο. ΤΟΝΙΖΕΙ τη σημασία της περαιτέρω στήριξης της ανάπτυξης και της επιχειρησιακής εφαρμογής μέτρων οικοδόμησης εμπιστοσύνης (ΜΟΕ) σε περιφερειακό και διεθνές επίπεδο, και της περαιτέρω ενθάρρυνσης της χρήσης των υφιστάμενων ΜΟΕ για τον κυβερνοχώρο στον ΟΑΣΕ, μεταξύ άλλων σε καιρούς διεθνών εντάσεων.

19. ΥΠΕΝΘΥΜΙΖΕΙ ότι η υιοθέτηση μιας προορατικής προσέγγισης με βάση τα ανθρώπινα δικαιώματα για τη διασφάλιση των διεθνών προτύπων στους τομείς των αναδυόμενων τεχνολογιών και της βασικής αρχιτεκτονικής του διαδικτύου σύμφωνα με δημοκρατικές αξίες και αρχές έχει ουσιαστική σημασία για να εξασφαλιστεί ότι το διαδίκτυο παραμένει παγκόσμιο, ακατακερμάτιστο και ανοικτό, και ΥΠΟΣΤΗΡΙΖΕΙ την αρχή της χρήσης και ανάπτυξης των τεχνολογιών με σεβασμό των ανθρωπίνων δικαιωμάτων και με εστίαση στην ιδιωτικότητα, καθώς και τη νόμιμη, ασφαλή και δεοντολογική τους χρήση. ΠΑΡΟΤΡΥΝΕΙ τον ύπατο εκπρόσωπο και την Επιτροπή να αναπτύξουν ένα στρατηγικό όραμα για τεχνικά ζητήματα στον ψηφιακό τομέα, τα οποία έχουν επιπτώσεις στην εξωτερική πολιτική και θα μπορούσαν να έχουν αντίκτυπο στη σταθερότητα του κυβερνοχώρου και του διαδικτύου ειδικότερα, μεταξύ άλλων στους σχετικούς εξειδικευμένους διεθνείς οργανισμούς (Διεθνής Ένωση Τηλεπικοινωνιών, κλπ.).

IV. ΕΝΙΣΧΥΣΗ ΤΗΣ ΣΥΝΕΡΓΑΣΙΑΣ ΜΕ ΧΩΡΕΣ ΕΤΑΙΡΟΥΣ ΚΑΙ ΔΙΕΘΝΕΙΣ ΟΡΓΑΝΙΣΜΟΥΣ

20. ΤΟΝΙΖΕΙ την ανάγκη να συνδεθεί καλύτερα η στρατηγική της ΕΕ για τη δημιουργία ικανοτήτων στον κυβερνοχώρο με τους κανόνες του ΟΗΕ για την υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο, μεταξύ άλλων με την ανάπτυξη προσαρμοσμένων προγραμμάτων συνεργασίας και δημιουργίας ικανοτήτων προς στήριξη των προσπαθειών υλοποίησης από τρίτα κράτη και, στο πλαίσιο αυτό, να συνεχιστούν και να επεκταθούν οι προσπάθειές μας με σκοπό την υποστήριξη του προγράμματος δράσης των Ηνωμένων Εθνών για την προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA). ΤΟΝΙΖΕΙ τη σημασία της πλήρους ενσωμάτωσης της δημιουργίας ικανοτήτων στον κυβερνοχώρο στο πλαίσιο της προσφοράς της ΕΕ ως παρόχου ασφάλειας, με επαρκή συντονισμό των προσπαθειών μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, και, ειδικότερα, ΕΚΦΡΑΖΕΙ ΙΚΑΝΟΠΟΙΗΣΗ για τη συνεργασία μεταξύ των κρατών μελών καθώς και με εταίρους του δημόσιου και του ιδιωτικού τομέα, ιδίως μέσω του δικτύου της ΕΕ για τη δημιουργία ικανοτήτων στον κυβερνοχώρο (EU CyberNet) και του παγκόσμιου φόρουμ για την εμπειρογνωμοσύνη στον κυβερνοχώρο (GFCE), προκειμένου να εξασφαλιστεί ο συντονισμός και να αποφευχθούν οι επικαλύψεις.

Καλεί τον ύπατο εκπρόσωπο και την Επιτροπή να συγκροτήσουν έως το τρίτο τρίμηνο του 2022 *συμβούλιο δημιουργίας ικανοτήτων στον κυβερνοχώρο* και να πραγματοποιούν τακτικές ανταλλαγές απόψεων στο πλαίσιο της Οριζόντιας ομάδας για θέματα κυβερνοχώρου. ΚΑΛΕΙ την Επιτροπή και τον ύπατο εκπρόσωπο να κινητοποιήσουν περαιτέρω τον Μηχανισμό Γειτονίας, Ανάπτυξης και Διεθνούς Συνεργασίας (NDICI), τον Μηχανισμό Προενταξιακής Βοήθειας (IPA III) και άλλα χρηματοδοτικά εργαλεία, όπως ο Ευρωπαϊκός Μηχανισμός για

την Ειρήνη (EPF) και η πρωτοβουλία Global Gateway, με σκοπό να υποστηριχτεί η ανθεκτικότητα των εταίρων μας, η ικανότητά τους να εντοπίζουν και να αντιμετωπίζουν κυβερνοαπειλές και να ερευνούν και να διώκουν κυβερνοεγκλήματα, καθώς και η ανάπτυξη έργων συνεργασίας, μεταξύ άλλων στο πλαίσιο κρίσεων, και ειδικότερα, ΕΝΘΑΡΡΥΝΕΙ τη συνεργασία με εταίρους στα Δυτικά Βαλκάνια και στην Ανατολική και Νότια Γειτονία της ΕΕ και την αποστολή εμπειρογνωμόνων της ΕΕ και των κρατών μελών για την παροχή υποστήριξης σε κρίσεις στον κυβερνοχώρο, λαμβάνοντας υπόψη τις ισχύουσες νομικές εντολές.

21. ΤΟΝΙΖΕΙ την ανάγκη να ενταθούν οι προσπάθειες για να αναπτυχθεί μια διαρθρωμένη και ανοικτή ενωσιακή προσέγγιση επικοινωνιακής προβολής όσον αφορά τον τρόπο προώθησης μιας παγκόσμιας συναντίληψης για την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο, για το πλαίσιο των Ηνωμένων Εθνών για την υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο, συμπεριλαμβανομένης της πρωτοβουλίας για ένα πρόγραμμα δράσης για την προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA), καθώς και σχετικά με τη θέση της ΕΕ και των κρατών μελών της στις εν εξελίξει διαπραγματεύσεις σχετικά με τη σύμβαση των Ηνωμένων Εθνών για το έγκλημα στον κυβερνοχώρο, και στο πλαίσιο αυτών των προσπαθειών ΖΗΤΕΙ από τον ύπατο εκπρόσωπο να υποβάλει στο Συμβούλιο σχέδιο επικοινωνιακής προβολής έως το τέλος του 2022. ΕΝΘΑΡΡΥΝΕΙ τον ύπατο εκπρόσωπο και τις υπηρεσίες της Επιτροπής να αξιοποιήσουν με πλήρη και συστηματικό τρόπο τις 145 αντιπροσωπείες και να αναπτύξουν τακτική και εποικοδομητική συνεργασία μεταξύ αυτών και των πρεσβειών των κρατών μελών σε τρίτες χώρες, υπό την εποπτεία του σχεδιαζόμενου δικτύου της ΕΕ για τη διπλωματία στον κυβερνοχώρο. ΚΑΛΕΙ τον ύπατο εκπρόσωπο να δημιουργήσει το δίκτυο της ΕΕ για τη διπλωματία στον κυβερνοχώρο έως το τρίτο τρίμηνο του 2022, το οποίο θα συμβάλει στην ανταλλαγή πληροφοριών, σε κοινές δραστηριότητες κατάρτισης για το προσωπικό της ΕΕ και των κρατών μελών, σε συνεκτικές προσπάθειες δημιουργίας ικανοτήτων και στην ενίσχυση της εφαρμογής του πλαισίου του ΟΗΕ για την υπεύθυνη συμπεριφορά των κρατών καθώς και των μέτρων οικοδόμησης εμπιστοσύνης μεταξύ κρατών.

22. ΤΟΝΙΖΕΙ τη δέσμευσή του για περαιτέρω συνεργασία με διεθνείς οργανισμούς και χώρες εταίρους για την προώθηση της κοινής κατανόησης του τοπίου των κυβερνοαπειλών, την ανάπτυξη μηχανισμών συνεργασίας και τον προορατικό εντοπισμό συνεργατικών διπλωματικών αντιδράσεων. ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα βασικά επιτεύγματα της συνεργασίας ΕΕ-ΝΑΤΟ στον τομέα της κυβερνοασφάλειας στο πλαίσιο της εφαρμογής των κοινών δηλώσεων της Βαρσοβίας του 2016 και των Βρυξελλών του 2018, με πλήρη σεβασμό της αυτονομίας και των διαδικασιών λήψης αποφάσεων των δύο οργανισμών και με βάση τις αρχές της διαφάνειας, της αμοιβαιότητας και της συμπεριληπτικότητας, ΤΟΝΙΖΕΙ την ανάγκη περαιτέρω ενίσχυσης της συνεργασίας με το ΝΑΤΟ σε θέματα κυβερνοχώρου, μέσω ασκήσεων, κοινοχρησίας και ανταλλαγής πληροφοριών μεταξύ εμπειρογνωμόνων, μεταξύ άλλων όσον αφορά την ανάπτυξη δυνατοτήτων, την δημιουργία ικανοτήτων από τους εταίρους και μέσω αποστολών και επιχειρήσεων, καθώς και όσον αφορά την εφαρμοσιμότητα του διεθνούς δικαίου και των κανόνων του ΟΗΕ σχετικά με την υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο, καθώς και την ανάγκη ενίσχυσης πιθανής συντονισμένης αντίδρασης έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

V. ΠΡΟΛΗΨΗ ΚΑΙ ΑΜΥΝΑ ΚΑΤΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥΣ

23. ΑΝΑΓΝΩΡΙΖΕΙ ότι ο κυβερνοχώρος έχει καταστεί μεταξύ άλλων και πεδίο γεωπολιτικού ανταγωνισμού και, ως εκ τούτου, ΕΠΑΝΑΛΑΜΒΑΝΕΙ ότι η ΕΕ πρέπει να είναι σε θέση να αντιδρά γρήγορα και αποφασιστικά σε κυβερνοεπιθέσεις, όπως οι υποκινούμενες από κρατικές αρχές κακόβουλες δραστηριότητες στον κυβερνοχώρο που στοχεύουν την ΕΕ και τα κράτη μέλη της και, συνεπώς, πρέπει να ενισχύσει την εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο και να αξιοποιήσει πλήρως όλα τα μέσα της, συμπεριλαμβανομένων των διαθέσιμων πολιτικών, οικονομικών, διπλωματικών, νομικών και στρατηγικών εργαλείων επικοινωνίας για την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. ΥΠΟΓΡΑΜΜΙΖΕΙ ότι οι εχθρικοί παράγοντες πρέπει να γνωρίζουν ότι οι κυβερνοεπιθέσεις κατά των κρατών μελών και των θεσμικών οργάνων της ΕΕ θα εντοπίζονται εγκαίρως, θα αναγνωρίζονται αμέσως και θα προσκρούουν σε όλα τα αναγκαία εργαλεία και πολιτικές. Με βάση ιδίως τα επιμέρους στοιχεία της στάσης στον κυβερνοχώρο και τα διδάγματα που αντλήθηκαν από την εφαρμογή της εργαλειοθήκης για τη διπλωματία στον κυβερνοχώρο μετά την έναρξή της καθώς και από την άσκηση CyCLES της ΕΕ, ΚΑΛΕΙ τα κράτη μέλη και τον ύπατο εκπρόσωπο, με την υποστήριξη της Επιτροπής, να εργαστούν για την αναθεώρηση των κατευθυντήριων γραμμών εφαρμογής της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο έως το τέλους του πρώτου τριμήνου του 2023, ιδίως μέσω της διερεύνησης πρόσθετων μέτρων αντιμετώπισης.

24. ΥΠΟΓΡΑΜΜΙΖΕΙ την ανάγκη τακτικών ανταλλαγών απόψεων σχετικά με το τοπίο των κυβερνοαπειλών στα αρμόδια όργανα και επιτροπές του Συμβουλίου, διατηρώντας ταυτόχρονα τακτική συνεργασία με τον ιδιωτικό τομέα, και με βάση την αξιολόγηση του αντικτύπου και της σοβαρότητας πρόσφατων περιστατικών, προκειμένου να αυξηθεί η συνολική ευαισθητοποίηση και ετοιμότητα για περαιτέρω εφαρμογές της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο και να αναπτυχθούν περαιτέρω εργαλεία για την υποστήριξη της υλοποίησής της. Μολονότι η εθνική ασφάλεια παραμένει αποκλειστική ευθύνη κάθε κράτους μέλους, ΣΗΜΕΙΩΝΕΙ την ανάγκη ενίσχυσης της ανταλλαγής πληροφοριών και στοιχείων και της συνεργασίας μεταξύ των κρατών μελών καθώς και με το EU INTCEN, προκειμένου να είναι δυνατή η ανταλλαγή στοιχείων κατά την έναρξη της διαδικασίας λήψης αποφάσεων, μεταξύ άλλων όσον αφορά το ζήτημα του καταλογισμού, ώστε να καταστεί δυνατή η ταχεία αποτελεσματική και τεκμηριωμένη αντίδραση σε κακόβουλες δραστηριότητες στον κυβερνοχώρο που στοχεύουν την ΕΕ και τους εταίρους της. ΕΠΑΝΑΛΑΜΒΑΝΕΙ ότι είναι σημαντικό να ενισχυθεί η ικανότητα του INTCEN της ΕΕ στον κυβερνοχώρο, με βάση εθελοντικές συνεισφορές των κρατών μελών και με την επιφύλαξη των αρμοδιοτήτων τους, και να διερευνηθεί η πρόταση για ενδεχόμενη σύσταση ομάδας των κρατών μελών για τη συλλογή στοιχείων κυβερνοχώρου.

25. ΑΝΑΓΝΩΡΙΖΟΝΤΑΣ ότι οι δηλώσεις και τα περιοριστικά μέτρα της ΕΕ που ελήφθησαν στο πλαίσιο της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο έχουν στείλει ισχυρό μήνυμα ότι οι κακόβουλες δραστηριότητες στον κυβερνοχώρο που συνιστούν εξωτερική απειλή για την ΕΕ, τα κράτη μέλη της και τους εταίρους της είναι απαράδεκτες και ότι, ως εκ τούτου, αναγνωρίζοντας ότι συντελούν στην πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, ΕΠΑΝΑΛΑΜΒΑΝΕΙ τη δέσμευσή του να χρησιμοποιήσει τα μέτρα αυτά προκειμένου να υπενθυμίσει τις υποχρεώσεις που ισχύουν για τον κυβερνοχώρο με βάση το διεθνές δίκαιο, συμπεριλαμβανομένου του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, και να προωθήσει το πλαίσιο των Ηνωμένων Εθνών για την υπεύθυνη συμπεριφορά των κρατών στον κυβερνοχώρο, μεταξύ άλλων την υποχρέωση δέουσας επιμέλειας των κρατών μελών να μην επιτρέπουν εν γνώσει τους τη χρήση του εδάφους τους για τη διάπραξη διεθνώς παράνομων πράξεων μέσω ΜΠΕ, με σκοπό την περαιτέρω ανάπτυξη και την προώθηση της κοινής θέσης της ΕΕ σχετικά με την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο. Σημειώνοντας ότι τα κατάλληλα και γρήγορα μηνύματα μετριάζουν τους κινδύνους κλιμάκωσης και μπορούν να αποθαρρύνουν τους επιτιθέμενους που στοχεύουν ευρωπαϊκά συμφέροντα, ΚΑΛΕΙ τον ύπατο εκπρόσωπο να αναπτύξει και να υποβάλει στα κράτη μέλη συνεκτική επικοινωνιακή στρατηγική σχετικά με τη χρήση της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο.

26. ΕΝΘΑΡΡΥΝΕΙ την ανάπτυξη σταδιακών, στοχευμένων και βιώσιμων προσεγγίσεων και αντιδράσεων σε κακόβουλες δραστηριότητες στον κυβερνοχώρο, με τη χρήση του ευρέος φάσματος εργαλείων που παρέχει η εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο, συμπεριλαμβανομένου του καθεστώτος κυρώσεων της ΕΕ στον κυβερνοχώρο, καθώς και με τον σχεδιασμό πρόσθετων μέτρων. ΕΠΙΣΗΜΑΙΝΕΙ την ανάγκη να αυξηθεί η δυνατότητα κινητοποίησης, κατά περίπτωση, όλων των διαθέσιμων εσωτερικών και εξωτερικών εργαλείων, για την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κυβερνοεπιθέσεων, εφαρμόζοντάς τα στο πλαίσιο ταχείας, αποτελεσματικής, σταδιακής, στοχευμένης και βιώσιμης προσέγγισης που θα βασίζεται σε μακροπρόθεσμη στρατηγική δέσμευση. ΚΑΛΕΙ τον ύπατο εκπρόσωπο, σε συνεργασία με την Επιτροπή, να προσδιορίσει πιθανή κοινή αντίδραση της ΕΕ σε κυβερνοεπιθέσεις, συμπεριλαμβανομένων των επιλογών επιβολής κυρώσεων, σε όλο το φάσμα τους, προκειμένου να είμαστε έτοιμοι να αναλάβουμε ταχεία και αποτελεσματική δράση όταν κριθεί αναγκαίο, και να τις υποβάλει στο Συμβούλιο έως το τέλος του πρώτου τριμήνου του 2023.

27. ΣΗΜΕΙΩΝΟΝΤΑΣ ότι η κυβερνοάμυνα αποτελεί πρωτίστως εθνική ευθύνη, ΕΝΘΑΡΡΥΝΕΙ τα κράτη μέλη να αναπτύξουν περαιτέρω τις δυνατότητές τους για τη διεξαγωγή επιχειρήσεων κυβερνοάμυνας, συμπεριλαμβανομένων προορατικών μέτρων για την προστασία, τον εντοπισμό, την άμυνα έναντι κυβερνοεπιθέσεων καθώς και την αποτροπή τους, και ενδεχομένως προς στήριξη άλλων κρατών μελών και της ΕΕ. Κάθε κράτος μέλος ενθαρρύνεται να ενισχύσει, ανάλογα με τις ανάγκες, τις οικείες ικανότητες όσον αφορά την παροχή και τη λήψη βοήθειας και συνδρομής. ΤΟΝΙΖΕΙ ότι η περαιτέρω ανάπτυξη αυτών των δυνατοτήτων θα πρέπει να αποτελέσει έναν από τους βασικούς στόχους της επικείμενης πολιτικής της ΕΕ για την κυβερνοάμυνα. ΣΗΜΕΙΩΝΕΙ ότι η πολιτική της ΕΕ για την κυβερνοάμυνα θα πρέπει να λαμβάνει περισσότερο υπόψη τον ρόλο που μπορούν να διαδραματίσουν τα αρμόδια θεσμικά και λοιπά όργανα της ΕΕ για να ενισχύσουν τη συνεργασία μεταξύ των σχετικών φορέων κυβερνοάμυνας της ΕΕ και των κρατών μελών και να αναπτύξουν τις δικές τους ικανότητες, σύμφωνα με τις αντίστοιχες εντολές τους. ΠΡΟΣΚΑΛΕΙ τον ύπατο εκπρόσωπο, από κοινού με την Επιτροπή, να συμπληρώσει τις εργασίες διαμόρφωσης της στάσης της ΕΕ στον κυβερνοχώρο υποβάλλοντας μια φιλόδοξη πρόταση για μια πολιτική της ΕΕ για την κυβερνοάμυνα εντός του 2022, η οποία θα προετοιμάσει το έδαφος για την περαιτέρω διαμόρφωση αυτής της στάσης στον κυβερνοχώρο από το Συμβούλιο.

28. ΕΠΙΣΗΜΑΙΝΕΙ την ανάγκη να αυξηθεί η διαλειτουργικότητα και η ανταλλαγή πληροφοριών μέσω της συνεργασίας μεταξύ στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (MilCERT). ΚΑΛΕΙ τα κράτη μέλη να δημιουργήσουν, με βάση το έργο του ΕΟΑ, ένα δίκτυο MilCERT για την ανάπτυξη συνεργασίας και τη διευκόλυνση της ανταλλαγής πληροφοριών, το οποίο θα συμβάλει επίσης στην ενίσχυση του συντονισμού με άλλες κυβερνοκοινότητες, καθώς και ενός δικτύου στρατιωτικών διοικητών κυβερνοχώρου προκειμένου να ενισχυθεί η στρατηγική συνεργασία μεταξύ διοικήσεων κυβερνοχώρου των κρατών μελών της ΕΕ ή άλλων αντίστοιχων αρχών. Η δημιουργία αυτών των δικτύων, μαζί με τα έργα της PESCO στον κυβερνοχώρο, θα συμβάλει στην ενίσχυση της κυβερνοάμυνας σε επίπεδο ΕΕ. ΤΟΝΙΖΕΙ τη σημασία της συνεργασίας του προτεινόμενου δικτύου MilCERT με το ήδη υφιστάμενο μη στρατιωτικό δίκτυο (CSIRT) για την ενίσχυση της ανταλλαγής πληροφοριών και τη βελτίωση της επίγνωσης της κατάστασης.

29. Με βάση το στρατιωτικό όραμα και τη στρατηγική της ΕΕ για τον κυβερνοχώρο ως πεδίο επιχειρήσεων και σημειώνοντας τη συνεχιζόμενη ανάπτυξη της στρατιωτικής έννοιας όσον αφορά την κυβερνοάμυνα για στρατιωτικές επιχειρήσεις και αποστολές υπό την ηγεσία της ΕΕ, ΕΠΑΝΑΛΑΜΒΑΝΕΙ την ανάγκη να ενσωματωθεί η διάσταση του κυβερνοχώρου στον σχεδιασμό και τη διεξαγωγή αποστολών και επιχειρήσεων ΚΠΑΑ, μεταξύ άλλων όσον αφορά τις δυνατότητές τους στον κυβερνοχώρο και ΤΟΝΙΖΕΙ ότι αυτό θα συμβάλει στην καλύτερη επίγνωση της κατάστασης στον κυβερνοχώρο σε επίπεδο ΕΕ.

30. Εν κατακλείδι, ΣΗΜΕΙΩΝΕΙ ότι η στάση στον κυβερνοχώρο θα αποτελέσει ένα βήμα προς τη θέσπιση δόγματος της ΕΕ για ανάληψη δράσης στον κυβερνοχώρο, το οποίο θα βασίζεται στην ενίσχυση της ανθεκτικότητας, των δυνατοτήτων και των επιλογών αντίδρασης, καθώς και κοινής θέσης σχετικά με την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο. Το Συμβούλιο ΘΑ ΠΡΟΒΕΙ ΣΕ ΑΠΟΛΟΓΙΣΜΟ της προόδου που θα έχει επιτελεστεί όσον αφορά την εφαρμογή των παρόντων συμπερασμάτων κατά το 2023, προκειμένου να διασφαλιστεί η περαιτέρω διαμόρφωση της στάσης της ΕΕ στον κυβερνοχώρο.