Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 22 Μαΐου 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Αποδέκτης:	Αντιπροσωπίες
αριθ. προηγ. εγγρ.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Θέμα:	Συμπεράσματα του Συμβουλίου σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα

Διαβιβάζονται συνημμένως στις αντιπροσωπίες τα συμπεράσματα του Συμβουλίου σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα, όπως εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδό του στις 22 Μαΐου 2023.

Συμπεράσματα του Συμβουλίου σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα

1. Το Συμβούλιο χαιρετίζει τη φιλόδοξη κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα, στη βάση της οποίας βρίσκεται το πλαίσιο πολιτικής για την κυβερνοάμυνα του 2014 και η επικαιροποίησή του που έγινε το 2018, με σκοπό την περαιτέρω επένδυση στις σύγχρονες και διαλειτουργικές ένοπλες δυνάμεις μας, σε τεχνολογίες αιχμής, σε προηγμένες ικανότητες κυβερνοάμυνας και στην ενίσχυση των εταιρικών σχέσεων για την αντιμετώπιση κοινών προκλήσεων. Ο κυβερνοχώρος έχει καταστεί πεδίο στρατηγικού ανταγωνισμού, σε μια εποχή αυξανόμενης εξάρτησης από τις ψηφιακές τεχνολογίες. Ως εκ τούτου, είναι σημαντικό να διατηρηθεί ανοικτός, ελεύθερος, σταθερός και ασφαλής. Η χρήση κυβερνοεπιχειρήσεων, που κατέστησαν δυνατό και πλαισιώνουν τον απρόκλητο και αδικαιολόγητο επιθετικό πόλεμο της Ρωσίας κατά της Ουκρανίας, επηρεάζει την παγκόσμια σταθερότητα και ασφάλεια, εγκυμονεί σημαντικό κίνδυνο κλιμάκωσης και επιτείνει την ήδη σημαντική αύξηση των κακόβουλων δραστηριοτήτων στον κυβερνοχώρο εκτός του πλαισίου των ένοπλων συγκρούσεων τα τελευταία χρόνια.

2. Με τον πόλεμο στην Ουκρανία έχει διαμορφωθεί ένα νέο στρατηγικό πλαίσιο και επιβεβαιώνεται η ανάγκη η ΕΕ, τα κράτη μέλη της και οι εταίροι τους να ενισχύσουν περαιτέρω την ανθεκτικότητα της ΕΕ για την αντιμετώπιση κυβερνοαπειλών και να αυξήσουν την κοινή μας κυβερνοασφάλεια και κυβερνοάμυνα έναντι κακόβουλων συμπεριφορών και επιθετικών ενεργειών στον κυβερνοχώρο. Η κοινή ανακοίνωση σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα σηματοδοτεί την αποφασιστικότητά μας να λάβουμε άμεσα και μακροπρόθεσμα μέτρα για τη διασφάλιση της ελευθερίας δράσης στον κυβερνοχώρο και να αντιδρούμε σε παράγοντες απειλών που επιδιώκουν, μεταξύ άλλων, να διεισδύσουν, να διαταράξουν ή να καταστρέψουν τα συστήματα δικτύων και πληροφοριών της ΕΕ και των εταίρων της. Συμπληρώνοντας τη στρατηγική της ΕΕ για την κυβερνοασφάλεια και σύμφωνα με τη στρατηγική πυξίδα, η παρούσα κοινή ανακοίνωση αποτελεί σημαντικό βήμα προς την πλήρους φάσματος προσέγγιση της ΕΕ όσον αφορά την ανθεκτικότητα, την αντίδραση, την πρόληψη των συγκρούσεων, τη συνεργασία και τη σταθερότητα στον κυβερνοχώρο. Τούτων δοθέντων, το Συμβούλιο υπογραμμίζει την ανάγκη κατάλληλων και συνεκτικών αντιδράσεων εκ μέρους της ΕΕ, των κρατών μελών της και των εταίρων τους, προσβλέποντας επίσης στην αναθεώρηση των κατευθυντήριων γραμμών εφαρμογής της εργαλειοθήκης της ΕΕ για τη διπλωματία στον κυβερνοχώρο ως ένα ακόμη βασικό βήμα προόδου στο πλαίσιο της διαμόρφωσης της στάσης της ΕΕ στον τομέα του κυβερνοχώρου.

3. Το Συμβούλιο τονίζει ότι οι πρόσφατες κυβερνοεπιθέσεις κατά ευρωπαϊκών υποδομών ζωτικής σημασίας, το ραγδαία εξελισσόμενο τοπίο των κυβερνοαπειλών και ο ταχύς ρυθμός της τεχνολογικής ανάπτυξης καταδεικνύουν επίσης την ανάγκη για ενισχυμένο συντονισμό και συνεργασία μεταξύ του στρατιωτικού και του μη στρατιωτικού τομέα, υπογραμμίζοντας παράλληλα ότι δεν υπάρχει ιεράρχηση μεταξύ μη στρατιωτικών και στρατιωτικών κοινοτήτων.

   Η πολιτική της ΕΕ για την κυβερνοάμυνα δίνει τη δυνατότητα στην ΕΕ και στα κράτη μέλη της να ενισχύσουν την ικανότητά προστασίας, εντοπισμού, άμυνας και αποτροπής των απειλών, αξιοποιώντας κατάλληλα όλο το φάσμα των αμυντικών επιλογών που έχουν στη διάθεσή τους οι μη στρατιωτικές και οι στρατιωτικές κοινότητες για την ευρύτερη ασφάλεια και άμυνα της ΕΕ, σύμφωνα με το διεθνές δίκαιο, συμπεριλαμβανομένου του δικαίου των ανθρωπίνων δικαιωμάτων και του διεθνούς ανθρωπιστικού δικαίου.

4. Ενώ η εθνική ασφάλεια, μεταξύ άλλων στον τομέα του κυβερνοχώρου, παραμένει αποκλειστική ευθύνη κάθε κράτους μέλους, όπως επισημαίνεται στο άρθρο 4 παράγραφος 2 της ΣΕΕ, το Συμβούλιο τονίζει εν τω μεταξύ την ανάγκη να πραγματοποιηθούν σημαντικές επενδύσεις, μεμονωμένα και συλλογικά, στην ενίσχυση της ανθεκτικότητας και της ανάπτυξης αμυντικών ικανοτήτων κυβερνοάμυνας πλήρους φάσματος, καθώς και στην αξιοποίηση των πλαισίων συνεργασίας και των οικονομικών κινήτρων που παρέχει η ΕΕ. Το Συμβούλιο τονίζει την ανάγκη περαιτέρω ενίσχυσης των δράσεων των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ για την προστασία της Ένωσης, των πολιτών μας, των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ και των αποστολών και επιχειρήσεων ΚΠΑΑ στον κυβερνοχώρο. Επιπλέον, υπογραμμίζει τη σημασία της ανθεκτικότητας της ΕΕ στον κυβερνοχώρο μέσω της ανάπτυξης ικανοτήτων κυβερνοάμυνας και της ενίσχυσης της συνεργασίας με ένα αξιόπιστο ιδιωτικό οικοσύστημα.

I. **Από κοινού δράση για ισχυρότερη κυβερνοάμυνα**

5. Το Συμβούλιο επαναλαμβάνει ότι μια σταδιακή, διαφανής και συμπεριληπτική διαδικασία είναι απαραίτητη για την ενίσχυση της εμπιστοσύνης, η οποία είναι ζωτικής σημασίας για την περαιτέρω ανάπτυξη ενός ενωσιακού πλαισίου διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας. Αυτή πρέπει να γίνει σύμφωνα με τον χάρτη πορείας για τη διαχείριση κρίσεων στον κυβερνοχώρο που καταρτίστηκε στο Συμβούλιο. Το Συμβούλιο επαναλαμβάνει την ανάγκη να συνεχιστεί η ενίσχυση της ικανότητας μας όσον αφορά την προστασία, τον εντοπισμό, την άμυνα και την αποτροπή κυβερνοεπιθέσεων μέσω της καλύτερης αντίληψης της κατάστασης, της οικοδόμησης ικανοτήτων, της ανάπτυξης δυνατοτήτων, της κατάρτισης, της διεξαγωγής ασκήσεων και της ενισχυμένης ανθεκτικότητας και μέσω της σθεναρής αντίδρασης στις κυβερνοεπιθέσεις κατά της ΕΕ, των κρατών μελών της, των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, των αποστολών και των επιχειρήσεων ΚΠΑΑ, με χρήση όλων των ενδεδειγμένων μέσων. Στο πλαίσιο αυτό, το Συμβούλιο προτρέπει τον ύπατο εκπρόσωπο και την Επιτροπή να μειώσουν την πολυπλοκότητα στον τομέα του κυβερνοχώρου, να αποφεύγουν τις περιττές επικαλύψεις και να διασφαλίσουν τη συνεργασία και τις συνέργειες με υφιστάμενες πρωτοβουλίες. Αναγκαία είναι η ενίσχυση της συνεργασίας και του συντονισμού μεταξύ των φορέων κυβερνοάμυνας της ΕΕ και των κρατών μελών και εντός αυτών, μεταξύ στρατιωτικών και μη στρατιωτικών κυβερνοκοινοτήτων και μεταξύ ενός δημόσιου και ενός αξιόπιστου ιδιωτικού οικοσυστήματος. Στο πλαίσιο αυτό, τα κράτη μέλη ενθαρρύνονται να διερευνήσουν περαιτέρω και να ενισχύσουν τους εθνικούς στρατιωτικούς και μη στρατιωτικούς συντονιστικούς μηχανισμούς, να διευκολύνουν την κοινή εθελοντική ανταλλαγή πληροφοριών, να ανταλλάξουν διδάγματα, να συμβάλουν στην ανάπτυξη διαλειτουργικών προτύπων, να διενεργήσουν αξιολογήσεις επικινδυνότητας και να καταρτίσουν σενάρια επικινδυνότητας, καθώς και να διεξαγάγουν κοινές ασκήσεις, ιδίως σε ευρωπαϊκό επίπεδο, με πλήρη σεβασμό των διατάξεων της οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (NIS2).

6. Αναγνωρίζοντας τις προσπάθειες περαιτέρω ενίσχυσης της ανθεκτικότητας της Ένωσης με την NIS2 και την οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων (CER), το Συμβούλιο επαναλαμβάνει τη σύστασή του σχετικά με μια συντονισμένη προσέγγιση σε επίπεδο ΕΕ για την ενίσχυση της ανθεκτικότητας των υποδομών ζωτικής σημασίας[1]. Ζητεί να ληφθούν μέτρα για την περαιτέρω ενίσχυση της ανθεκτικότητας των κρίσιμων οντοτήτων, των υποδομών ζωτικής σημασίας, των ψηφιακών προϊόντων και υπηρεσιών, επισημαίνοντας παράλληλα ότι η ορθή εφαρμογή της NIS2 παραμένει το σημαντικότερο βήμα. Παρότι αποτελεί κατά κύριο λόγο μη στρατιωτική υποχρέωση, συμβάλλει επίσης στην ενίσχυση της κυβερνοάμυνας. Στο πλαίσιο αυτό, τα θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ, καθώς και τα κράτη μέλη ενθαρρύνονται να στηρίξουν την περαιτέρω ανάπτυξη και εφαρμογή νέων και υφιστάμενων συντονιστικών μηχανισμών της ΕΕ, εκτιμήσεων, αξιολογήσεων και σεναρίων επικινδυνότητας, κοινών εθελοντικών ανταλλαγών πληροφοριών και ασκήσεων, κατά τρόπο που να προστίθεται αξία και να αποφεύγονται οι περιττές επικαλύψεις με υφιστάμενες πρωτοβουλίες.

7. Με στόχο την περαιτέρω ενίσχυση της εμπιστοσύνης, την εδραίωση της συνεργασίας και τη διευκόλυνση της έγκαιρης ανταλλαγής πληροφοριών σχετικά με σημαντικά και μεγάλης κλίμακας περιστατικά στον κυβερνοχώρο που επηρεάζουν τα αμυντικά συστήματα, το Συμβούλιο χαιρετίζει την πρωτοβουλία για την περαιτέρω ανάπτυξη της διάσκεψης των διοικητών κυβερνοχώρου της ΕΕ υπό τη διοργάνωση της εκάστοτε Προεδρίας του Συμβουλίου της ΕΕ, με την υποστήριξη του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ) και τη συμμετοχή της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ). Το Συμβούλιο ενθαρρύνει όλα τα κράτη μέλη να συμμετάσχουν στις συνεδριάσεις αυτές. Για την ενίσχυση της ανθεκτικότητας της ΕΕ κατά μεγάλων κλίμακας περιστατικών στον κυβερνοχώρο, το Συμβούλιο καλεί το δίκτυο οργανισμών διασύνδεσης της ΕΕ για τις κρίσεις στον κυβερνοχώρο (EU-CyCLONe) και τη διάσκεψη των διοικητών κυβερνοχώρου της ΕΕ να προσδιορίσουν πιθανούς τρόπους συνεργασίας και αποκόμισης ωφελειών από μια κοινή στρατιωτική και μη στρατιωτική προοπτική.

---

[1] Πρόταση σύστασης του Συμβουλίου σχετικά με μια συντονισμένη προσέγγιση της Ένωσης για την ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών (COM/2022/551).

8. Έχοντας ως στόχο την προώθηση μιας πιο σθεναρής και συντονισμένης αντίδρασης σε επίπεδο ΕΕ, το Συμβούλιο εκφράζει ικανοποίηση για τη δημιουργία του ενωσιακού επιχειρησιακού δικτύου των στρατιωτικών ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική (MICNET) και προσβλέπει στην επίτευξη της αρχικής επιχειρησιακής ικανότητάς του έως τα μέσα του 2024, προκειμένου να ενισχυθεί η κοινοχρησία τεχνικών πληροφοριών σχετικά με περιστατικά στον κυβερνοχώρο που επηρεάζουν τα αμυντικά συστήματα ενός ή περισσότερων συμμετεχόντων κρατών μελών. Το Συμβούλιο προτρέπει όλα τα κράτη μέλη να συμμετάσχουν στο MICNET προκειμένου να εξασφαλιστεί η αποτελεσματικότητα του δικτύου. Επιπλέον, το Συμβούλιο καλεί τα κράτη μέλη να αξιοποιήσουν τα διδάγματα που αντλήθηκαν από το δίκτυο Ομάδων Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (CSIRT) και ενθαρρύνει σθεναρά τη δημιουργία ενός αποτελεσματικού μηχανισμού συνεργασίας και συντονισμού μεταξύ των δύο δικτύων σε εύθετο χρόνο, με πλήρη σεβασμό των μηχανισμών διακυβέρνησης και των τομέων ευθύνης κάθε οντότητας.

9. Δεδομένης της αύξησης των κακόβουλων δραστηριοτήτων από κρατικούς και μη κρατικούς παράγοντες κατά αποστολών και επιχειρήσεων ΚΕΠΠΑ της ΕΕ, το Συμβούλιο καλεί την ΕΕ και τα κράτη μέλη της να ενισχύσουν τις ικανότητές τους για την προάσπιση και τη διασφάλιση των αποστολών και των επιχειρήσεων ΚΕΠΠΑ. Στο πλαίσιο αυτό, το Συμβούλιο εκφράζει ικανοποίηση για τους στόχους που έχουν τεθεί ώστε να προωθηθεί περαιτέρω η προστασία των στρατιωτικών δικτύων και δομών της ΕΕ, μεταξύ άλλων σύμφωνα με το στρατιωτικό όραμα και τη στρατηγική της ΕΕ για τον κυβερνοχώρο ως πεδίο επιχειρήσεων[2].

[2] ΕΥΕΔ (2021) 706 REV4

10. Το Συμβούλιο υπενθυμίζει τα συμπεράσματα του Συμβουλίου του Μαΐου 2022[3] και επισημαίνει εκ νέου την ανάγκη να επενδύσουμε στην αμοιβαία συνδρομή μας δυνάμει του άρθρου 42 παράγραφος 7 της ΣΕΕ, καθώς και στη ρήτρα αλληλεγγύης δυνάμει του άρθρου 222 της ΣΛΕΕ. Το Συμβούλιο τονίζει τη σημασία που έχει η ΕΕ και τα κράτη μέλη της να αποκτήσουν βαθύτερη κοινή αντίληψη όσον αφορά την εφαρμογή του άρθρου 42 παράγραφος 7, μεταξύ άλλων σε πολύπλοκα σενάρια που αφορούν κυβερνοεπιθέσεις, σύμφωνα με τις σχετικές αρχές του διεθνούς δικαίου. Χαιρετίζει τη δυνατότητα παροχής στήριξης από την ΕΕ σε περίπτωση κυβερνοεπίθεσης, κατόπιν ρητού αιτήματος του ενδιαφερόμενου κράτους μέλους ή κρατών μελών, με την επιφύλαξη των ιδιαίτερων χαρακτηριστικών της πολιτικής ασφάλειας και άμυνας ορισμένων κρατών μελών.

11. Το Συμβούλιο υπογραμμίζει την πρόοδο που έχει επιτευχθεί στο πλαίσιο του έργου της PESCO «Ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο και την αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο (CRRT)» και την ετοιμότητά του να ενεργεί κατόπιν αιτήματος για να ανταποκριθεί στις ανάγκες των κρατών μελών και της ΕΕ, προς στήριξη των αποστολών και επιχειρήσεων ΚΠΑΑ και για την παροχή βοήθειας στους εταίρους της ΕΕ. Το Συμβούλιο εκφράζει ικανοποίηση για την περαιτέρω ανάπτυξη των δυνατοτήτων των CRRT της PESCO, εθνικών ομάδων αντιμετώπισης περιστατικών στον κυβερνοχώρο και, κατά περίπτωση, πρόσθετων δυνατοτήτων αντιμετώπισης περιστατικών, όπως οι μελλοντικές ομάδες ταχείας αντίδρασης σε υβριδικές ενέργειες, κατά τα προβλεπόμενα στη στρατηγική πυξίδα, μεταξύ άλλων μέσω της προώθησης του συντονισμού και της συνεργασίας τους σε επίπεδο ΕΕ.

[3] Συμπεράσματα του Συμβουλίου σχετικά με τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, 23 Μαΐου 2022, 9364/22.

12. Το Συμβούλιο εκφράζει ικανοποίηση για τις εργασίες στο πλαίσιο του έργου της PESCO «Συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών (CIDCC)», στόχος του οποίου είναι η παροχή στρατιωτικών δυνατοτήτων για τη συλλογή και ανάλυση πληροφοριών που είναι σημαντικές για την επίτευξη κοινής επιχειρησιακής εικόνας του κυβερνοχώρου. Επιπλέον, το Συμβούλιο χαιρετίζει την πρόταση να ενσωματωθεί, από το 2025 κι έπειτα, η απόδειξη του εφικτού της ιδέας, εφόσον είναι επιτυχής υπό τη μορφή συντονιστικού κέντρου πληροφοριών, σε ένα κέντρο συντονισμού της ΕΕ για την κυβερνοάμυνα (EUCDCC), ώστε να βελτιωθεί ο συντονισμός και η αντίληψη της κατάστασης, ιδίως μεταξύ των διοικητών αποστολών και επιχειρήσεων ΚΠΑΑ, και να ενισχυθεί η ενωσιακή αρχιτεκτονική διοίκησης και ελέγχου. Το Συμβούλιο καλεί τον ύπατο εκπρόσωπο να παρουσιάσει μια γενική ιδέα και έναν χάρτη πορείας για τη δημιουργία του EUCDCC, αντλώντας διδάγματα από παρόμοιες διεθνείς οντότητες, προσδιορίζοντας τους απαιτούμενους πόρους, αποφεύγοντας τις περιττές επικαλύψεις και επιδιώκοντας συμπληρωματικότητα με το ευρύτερο πλαίσιο της ΕΕ για την κυβερνοασφάλεια.

13. Το Συμβούλιο τονίζει τη σημασία της στρατηγικής συνεργασίας στον τομέα των πληροφοριών σχετικά με τις απειλές και τις δραστηριότητες στον κυβερνοχώρο και καλεί τα κράτη μέλη, μέσω των αρμόδιων αρχών τους, να συνεχίσουν να συμβάλλουν στο έργο του EU INTCEN, της Διεύθυνσης Πληροφοριών του EUMS και των κρατών μελών, στο πλαίσιο της Ενιαίας Ικανότητας Ανάλυσης Πληροφοριών (SIAC). Το Συμβούλιο τονίζει επίσης τη σημασία της ενίσχυσης των ικανοτήτων μας στον τομέα των πληροφοριών στον κυβερνοχώρο για τη βελτίωση της ανθεκτικότητας και των αντιδράσεών μας στον κυβερνοχώρο και την παροχή αποτελεσματικής στήριξης στις οικείες μη στρατιωτικές και στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ, καθώς και της ικανότητας των ενόπλων δυνάμεών μας και της SIAC στον τομέα του κυβερνοχώρου, με βάση σχετικές εθελοντικές συνεισφορές των κρατών μελών και με την επιφύλαξη των αρμοδιοτήτων τους.

14. Το Συμβούλιο λαμβάνει υπό σημείωση το κέντρο κυβερνοκατάστασης και κυβερνοανάλυσης, το οποίο αποσκοπεί στην καλύτερη επίγνωση της κατάστασης εκ μέρους της Επιτροπής. Το Συμβούλιο τονίζει ότι είναι σημαντικό να καθιερωθεί αμοιβαία επωφελής συνεργασία μεταξύ του κέντρου αυτού και άλλων θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, ιδίως του ENISA και της CERT-ΕΕ. Το Συμβούλιο υπογραμμίζει ότι είναι σημαντικό να διασφαλίζεται η στενή συνεργασία με τα δίκτυα συνεργασίας της ΕΕ κατά τη ανάπτυξη ικανοτήτων επίγνωσης της κατάστασης, καθώς και να τηρείται το απόρρητο. Το Συμβούλιο σημειώνει την ανάγκη ενίσχυσης της κοινής επίγνωσης της κατάστασης σε επίπεδο ΕΕ και περαιτέρω ανάπτυξης του ενωσιακού πλαισίου διαχείρισης κρίσεων στον τομέα της κυβερνοασφάλειας, αποφεύγοντας παράλληλα τις περιττές επικαλύψεις των προσπαθειών.

15. Το Συμβούλιο υπενθυμίζει ότι η εκπαίδευση, η κατάρτιση και οι ασκήσεις στον κυβερνοχώρο είναι ουσιαστικής σημασίας για τη διασφάλιση ετοιμότητας και αποτελεσματικότητας και χαιρετίζει τις δραστηριότητες που αναλαμβάνονται σε εθνικό επίπεδο καθώς και εκείνες που παρέχει η ΕΕ μέσω της Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας (ΕΑΑΑ), του ΕΟΑ, του ENISA και των εν εξελίξει έργων της PESCO, όπως το έργο «Δίκτυο εικονικών περιβαλλόντων κυβερνοτεχνολογίας» και το έργο «Ακαδημία για τον κυβερνοχώρο και κόμβος καινοτομίας της ΕΕ» (CAIH). Προκειμένου να ενισχυθούν περαιτέρω οι προσπάθειες αυτές, το Συμβούλιο προσβλέπει στη θέσπιση του προγράμματος-πλαισίου του ΕΟΑ «CyDef-X» για τον συγχρονισμό και την υποστήριξη ασκήσεων κυβερνοάμυνας. Το Συμβούλιο προτρέπει τον ΕΟΑ να διερευνήσει, σε στενή συνεργασία με τα κράτη μέλη και την ΕΥΕΔ, τρόπους με τους οποίους το «CyDef-X» θα μπορούσε να στηρίξει περαιτέρω ασκήσεις, όπως οι CYBER PHALANX, μεταξύ άλλων όσον αφορά την αμοιβαία συνδρομή δυνάμει του άρθρου 42 παράγραφος 7 της ΣΕΕ και τη ρήτρα αλληλεγγύης δυνάμει του άρθρου 222 της ΣΛΕΕ, και σε στενή συνεργασία με την Επιτροπή και τον ENISA όσον αφορά τις μη στρατιωτικές ασκήσεις. Επιπλέον, το Συμβούλιο ενθαρρύνει τη χρήση και την περαιτέρω ανάπτυξη στο πλαίσιο του «CyDef-X» υφιστάμενων περιβαλλόντων δοκιμών και ασκήσεων κυβερνοάμυνας, όπως είναι το έργο «Δίκτυο εικονικών περιβαλλόντων κυβερνοτεχνολογίας». Προκειμένου να διασφαλιστεί μια ευέλικτη και αποτελεσματική διαδικασία λήψης αποφάσεων σε περίπτωση κρίσης στον κυβερνοχώρο, το Συμβούλιο υπογραμμίζει ότι είναι σημαντικό να διεξάγονται τακτικές ασκήσεις επί χάρτου για τη λήψη αποφάσεων σε επίπεδο κρατών μελών.

16. Το Συμβούλιο σημειώνει την πρόταση πράξης για την αλληλεγγύη στον κυβερνοχώρο και την πρόθεση να ενισχυθούν οι ικανότητες εντοπισμού και αντιμετώπισης απειλών και συμβάντων που αφορούν την κυβερνοασφάλεια στην ΕΕ. Το Συμβούλιο υπογραμμίζει ότι οι προτάσεις στον τομέα αυτό μπορούν να είναι αποτελεσματικές μόνο εάν ευθυγραμμίζονται με τα πλαίσια και τις ανάγκες των κρατών μελών για τη διαχείριση κρίσεων. Το Συμβούλιο υπογραμμίζει τη σημασία του να λαμβάνονται υπόψη οι διαθέσιμες εκτιμήσεις επικινδυνότητας της ΕΕ κατά τη δοκιμή των υποδομών ζωτικής σημασίας για πιθανά τρωτά σημεία, ως εθνική αρμοδιότητα, όταν αυτό κρίνεται επωφελές.

17. Το Συμβούλιο σημειώνει την πρόταση της Επιτροπής για τη δημιουργία μηχανισμού για έκτακτες ανάγκες στον κυβερνοχώρο, ο οποίος θα μπορούσε να στηρίξει τη διαθεσιμότητα υπηρεσιών κυβερνοασφάλειας από αξιόπιστους ιδιωτικούς παρόχους για να συνδράμει, κατόπιν αιτήματος, τα κράτη μέλη σε περίπτωση συμβάντων κυβερνοασφάλειας μεγάλης κλίμακας, υπογραμμίζοντας παράλληλα την ανάγκη να αναβαθμιστεί ένας ευρωπαϊκός κλάδος κυβερνοασφάλειας με την υποστήριξη του ECCC ως βασικού πυλώνα για τη λειτουργία του μηχανισμού αυτού. Το Συμβούλιο υπογραμμίζει τον καίριο ρόλο κάθε κράτους μέλους στην παρακολούθηση και την αξιολόγηση των εθνικών αναγκών του.

II. **Προστασία του αμυντικού οικοσυστήματος της ΕΕ**

18. Το Συμβούλιο υπενθυμίζει ότι προτρέπει τα κράτη μέλη να αναπτύξουν περαιτέρω τις δικές τους ικανότητες για τη διεξαγωγή επιχειρήσεων κυβερνοάμυνας, συμπεριλαμβανομένων, κατά περίπτωση, προληπτικών αμυντικών μέτρων για την προστασία, τον εντοπισμό, την υπεράσπιση και την αποτροπή κυβερνοεπιθέσεων. Δεδομένου ότι η οδηγία NIS2 δεν εφαρμόζεται σε οντότητες δημόσιας διοίκησης που ασκούν τις δραστηριότητές τους στον τομέα της άμυνας, το Συμβούλιο καλεί τον ΕΟΑ, με την υποστήριξη της Επιτροπής και της ΕΥΕΔ, κατά περίπτωση, να συνδράμει τα κράτη μέλη στην ανάπτυξη μη νομικά δεσμευτικών εθελοντικών συστάσεων εμπνευσμένων από τη NIS2 για την αύξηση της κυβερνοασφάλειας στην αμυντική κοινότητα, και καλεί όλα τα κράτη μέλη να συμμετάσχουν ενεργά στην προσπάθεια αυτή. Οι συστάσεις αυτές θα πρέπει να λαμβάνουν υπόψη παρόμοιες προσπάθειες που έχουν αναληφθεί σε άλλα πλαίσια.

19. Όπως αναγνωρίζεται στη στρατηγική πυξίδα, η ικανότητα δράσης της ΕΕ εξαρτάται από την ικανότητά της να μειώσει τις στρατηγικές εξαρτήσεις της σε όλες τις ικανότητες κυβερνοάμυνας και τις αλυσίδες εφοδιασμού της που αφορούν την κυβερνοάμυνα, καθώς και να αναπτύξει και να τελειοποιήσει τεχνολογίες αιχμής στον τομέα της κυβερνοάμυνας. Η προσπάθεια αυτή περιλαμβάνει την ενίσχυση της ευρωπαϊκής βιομηχανικής και τεχνολογικής βάσης στον τομέα της άμυνας (EDTIB) σε ολόκληρη την ΕΕ και της ικανότητάς της να συνεργάζεται με ομονοούντες εταίρους ανά τον κόσμο, σε αμοιβαία βάση, ώστε να διασφαλίζονται αμοιβαία οφέλη. Ως εκ τούτου, το Συμβούλιο καλεί τους κλάδους της κυβερνοασφάλειας και της κυβερνοάμυνας να συνεργαστούν στενά για τη δημιουργία συνεργειών με στόχο την ανάπτυξη και την παροχή δυνατοτήτων κυβερνοάμυνας πλήρους φάσματος. Το Συμβούλιο καλεί την Επιτροπή, σε στενή συνεργασία με το ECCC, κατά περίπτωση, να στηρίξει περαιτέρω την ανάπτυξη μιας ισχυρής, ευέλικτης, παγκοσμίως ανταγωνιστικής και καινοτόμου ευρωπαϊκής βιομηχανικής και τεχνολογικής βάσης στον τομέα της κυβερνοάμυνας, συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ), μέσω περαιτέρω επενδύσεων και δράσεων πολιτικής.

20. Λαμβάνοντας υπόψη τη σημασία της διαλειτουργικότητας και των κοινών χαρακτηριστικών των ικανοτήτων κυβερνοάμυνας, μεταξύ άλλων όσον αφορά τη συνεργατική ανάπτυξη ικανοτήτων κυβερνοάμυνας επόμενης γενιάς, το Συμβούλιο καλεί τον ΕΟΑ και το Στρατιωτικό Επιτελείο της ΕΕ να εργαστούν για ένα σύνολο απαιτήσεων διαλειτουργικότητας της ΕΕ στον τομέα της κυβερνοάμυνας, οι οποίες θα βασίζονται στις υφιστάμενες αρχές, διαδικασίες και πρότυπα που έχουν θεσπιστεί ιδίως στο πλαίσιο του Οργανισμού του Βορειοατλαντικού Συμφώνου (ΝΑΤΟ) και θα είναι συμβατές με αυτές. Επιπλέον, το Συμβούλιο καλεί τα κράτη μέλη να διερευνήσουν, στο πλαίσιο της ευρωπαϊκής επιτροπής τυποποίησης στον τομέα της άμυνας, κατά πόσον θα μπορούσαν να απαιτηθούν ειδικά εθελοντικά πρότυπα για τα αμυντικά συστήματα, σε στενή συνεργασία με όλους τους σχετικούς ενδιαφερόμενους φορείς, συμπεριλαμβανομένων των ευρωπαϊκών οργανισμών τυποποίησης και του ΝΑΤΟ, κατά περίπτωση.

21. Το Συμβούλιο εκφράζει ικανοποίηση για τις προσπάθειες της Επιτροπής να υποβάλει σχέδιο για την προώθηση της χρήσης των υφιστάμενων προτύπων για μη στρατιωτικές χρήσεις στον τομέα της κυβερνοασφάλειας και της κυβερνοάμυνας, καθώς και για την ανάπτυξη νέων εθελοντικών προτύπων. Το Συμβούλιο τονίζει την ανάγκη ευθυγράμμισης των προτύπων κυβερνοασφάλειας και κυβερνοάμυνας, κατά περίπτωση. Το Συμβούλιο αναγνωρίζει ότι τέτοιου είδους εθελοντικά πρότυπα θα μπορούσαν να είναι χρήσιμα για τις βιομηχανίες κυβερνοασφάλειας και κυβερνοάμυνας της ΕΕ και ζητεί στενότερη συνεργασία μεταξύ των μη στρατιωτικών και των αμυντικών οργανισμών τυποποίησης.

22. Το Συμβούλιο ζητεί την ταχεία εκπόνηση συστάσεων που θα βασίζονται στη χαρτογράφηση των υφιστάμενων εργαλείων ασφαλούς επικοινωνίας στον κυβερνοχώρο, η οποία θα πραγματοποιηθεί από την Επιτροπή και τα σχετικά όργανα. Όπου είναι δυνατόν, οι συστάσεις θα πρέπει να ευθυγραμμίζονται με τις υφιστάμενες πρωτοβουλίες για την ανταλλαγή πληροφοριών και θα πρέπει επίσης να λαμβάνουν υπόψη τους κινδύνους που ενέχουν οι αναδυόμενες και ρηξικέλευθες τεχνολογίες στις τρέχουσες μεθόδους κρυπτογράφησης.

23. Επιπλέον, το Συμβούλιο εκφράζει ικανοποίηση για τις αρχικές εργασίες που έχουν αναληφθεί σχετικά με την αξιολόγηση επικινδυνότητας και τα σενάρια επικινδυνότητας που εκπονούν η Επιτροπή, ο ύπατος εκπρόσωπος και η ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS) σε σχέση, αρχικά, με τους τομείς της ενέργειας και των τηλεπικοινωνιών, κατόπιν αιτήματος του Συμβουλίου. Το Συμβούλιο αναγνωρίζει ότι προετοιμάζονται επίσης στοχευμένες εκτιμήσεις επικινδυνότητας για τις υποδομές και τα δίκτυα επικοινωνιών στην ΕΕ όσον αφορά την κυβερνοασφάλεια. Το Συμβούλιο επαναλαμβάνει ότι η κοινή αντίληψη των πιθανών επιπτώσεων των συμβάντων στον κυβερνοχώρο μεταξύ των κρατών μελών, αλλά και μεταξύ των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, είναι υψίστης σημασίας. Ως εκ τούτου, το Συμβούλιο καλεί τους προαναφερόμενους φορείς να διασφαλίσουν ότι οι αξιολογήσεις επικινδυνότητας, τα σενάρια και οι επακόλουθες συστάσεις λαμβάνονται υπόψη κατά τον καθορισμό και την ιεράρχηση των μέτρων και της στήριξης, σε επίπεδο ΕΕ και, κατά περίπτωση, σε εθνικό επίπεδο. Επιπλέον, το Συμβούλιο ζητεί από όλους τους σχετικούς παράγοντες να λάβουν υπόψη τα σενάρια επικινδυνότητας κατά τις διαδικασίες εκτίμησης επικινδυνότητας, καθώς και κατά την εκπόνηση ασκήσεων στον κυβερνοχώρο.

III. **Επενδύσεις σε ικανότητες κυβερνοάμυνας**

24. Το Συμβούλιο παροτρύνει τα κράτη μέλη να αυξήσουν τις επενδύσεις τους για τη δημιουργία, τη διατήρηση και την περαιτέρω ανάπτυξη διαλειτουργικών ικανοτήτων κυβερνοάμυνας. Το Συμβούλιο υποστηρίζει την ανάπτυξη ενός συνόλου εθελοντικών δεσμεύσεων για την περαιτέρω ανάπτυξη των εθνικών ικανοτήτων κυβερνοάμυνας, έχοντας επίγνωση παρόμοιων προσπαθειών που έχουν αναληφθεί σε άλλα πλαίσια.

25. Το Συμβούλιο καλεί τα κράτη μέλη και τον ΕΟΑ να αξιοποιήσουν την ευκαιρία της αναθεώρησης του σχεδίου ανάπτυξης δυνατοτήτων για να θέσουν ψηλά τον πήχη της φιλοδοξίας όσον αφορά την ανάπτυξη συνεργατικής κυβερνοάμυνας σε επίπεδο ΕΕ. Το Συμβούλιο παροτρύνει επίσης τα κράτη μέλη να αξιοποιήσουν το επικαιροποιημένο σύνολο προτεραιοτήτων και τις δεσμεύσεις τους στο πλαίσιο της PESCO για να ενισχύσουν το βαθμό συμμετοχής τους σε συνεργατικά έργα ανάπτυξης ικανοτήτων κυβερνοάμυνας της ΕΕ, αναγνωρίζοντας το άμεσο όφελος των συνεργατικών έργων σε επίπεδο ΕΕ για τη στήριξη της ανάπτυξης εθνικών ικανοτήτων κυβερνοάμυνας.

26. Το Συμβούλιο εκφράζει ικανοποίηση για τις προσπάθειες συνεργατικής έρευνας σε επίπεδο ΕΕ που διερευνούν τις εφαρμογές που ενδέχεται να έχουν οι νέες ρηξικέλευθες τεχνολογίες σε συστήματα συνδεόμενα με τον τομέα της άμυνας και σημειώνει επίσης ότι είναι ανάγκη να διασφαλιστεί η ταχεία ενσωμάτωση αυτών των τεχνολογικών εξελίξεων σε υφιστάμενες και σε μελλοντικές δυνατότητες. Το Συμβούλιο ενθαρρύνει τα κράτη μέλη και τη βιομηχανία της ΕΕ να αξιοποιήσουν με τον καλύτερο δυνατό τρόπο τις δυνατότητες συνεργατικής έρευνας σε επίπεδο ΕΕ, για παράδειγμα στο πλαίσιο του ΕΟΑ, στα εν εξελίξει έργα PESCO, όπως είναι η Ακαδημία για τον κυβερνοχώρο και ο κόμβος καινοτομίας της ΕΕ (CAIH), το Ευρωπαϊκό Ταμείο Άμυνας και, κατά περίπτωση, το πρόγραμμα «Ορίζων Ευρώπη» και το πρόγραμμα «Ψηφιακή Ευρώπη» για έργα διπλής χρήσης. Επιπλέον, το Συμβούλιο εκφράζει ικανοποίηση για την αξιοποίηση των ειδικών πλαισίων για τη στήριξη της αμυντικής καινοτομίας κάνοντας χρήση εισροών τεχνολογίας από τον μη στρατιωτικό τομέα, όπως είναι συγκεκριμένα το ενωσιακό πρόγραμμα καινοτομίας στον τομέα της άμυνας και ο κόμβος καινοτομίας για την άμυνα. Επιπλέον, το Συμβούλιο προτρέπει το Ευρωπαϊκό Κέντρο Αρμοδιότητας για την Κυβερνοασφάλεια (ECCC) και τον ΕΟΑ να αναπτύξουν συμφωνία συνεργασίας για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του εκατέρωθεν προσωπικού σχετικά με τις προτεραιότητες μη στρατιωτικής, διττής χρήσης και αμυντικής τεχνολογίας, αντίστοιχα, με σκοπό τη δημιουργία συνεργειών και την αποφυγή επικαλύψεων.

27. Το Συμβούλιο εκφράζει ικανοποίηση για την πρόθεση της Επιτροπής να εκπονήσει τεχνολογικό χάρτη πορείας για κυβερνοτεχνολογίες κρίσιμης σημασίας, σε συνεργασία με τον ΕΟΑ και το ECCC, σε συνάρτηση με τις αντίστοιχες εντολές τους, με τα κράτη μέλη και σε διαβούλευση με σχετικούς ενδιαφερόμενους φορείς, όπως η βιομηχανία, γεγονός που, χάρη στην ταυτοποίηση των κυβερνοτεχνολογιών κρίσιμης σημασίας και τη χαρτογράφηση των τεχνολογικών εξελίξεων και των στρατηγικών εξαρτήσεων, θα παράσχει τρόπους για να μειωθούν αυτές, στηρίζοντας τη στρατηγική αυτονομία και την τεχνολογική κυριαρχία της ΕΕ και διασφαλίζοντας παράλληλα μια ανοικτή οικονομία. Το Συμβούλιο σημειώνει ότι ο τεχνολογικός χάρτης πορείας για κυβερνοτεχνολογίες κρίσιμης σημασίας ενδεχομένως θα αξιοποιηθεί στην εκπόνηση στρατηγικών προτεραιοτήτων για τα χρηματοδοτικά μέσα της ΕΕ ενώ παράλληλα θα ευθυγραμμίζεται με τις αντίστοιχες πρακτικές ρυθμίσεις που ισχύουν γι’ αυτά. Το Συμβούλιο υπενθυμίζει ότι η ΕΕ οφείλει να επιδιώξει μια φιλόδοξη και δυναμική ευρωπαϊκή βιομηχανική πολιτική για τη δημιουργία βιώσιμου, ελκυστικού και ανταγωνιστικού επιχειρηματικού περιβάλλοντος, κάτι που μπορεί επίσης να δώσει στις ευρωπαϊκές οντότητες στον κυβερνοχώρο τη δυνατότητα να αναβαθμιστούν.

28. Το Συμβούλιο εκτιμά την πρόθεση να αντιμετωπιστεί το σημαντικό χάσμα δεξιοτήτων κυβερνοασφάλειας με προσέλκυση νέων επαγγελματιών, συμπεριλαμβανομένων γυναικών, με αναβάθμιση δεξιοτήτων και επανειδίκευση, καθώς και με επένδυση στην κατάρτιση και στην διοργάνωση εκπαιδευτικών προγραμμάτων και ασκήσεων για την συγκρότηση ενός εργατικού δυναμικού για τον κυβερνοχώρο που θα χαρακτηρίζεται από διαφορετικότητα και συμπερίληψη. Αντιλαμβανόμενο τις προκλήσεις που αντιμετωπίζει η ΕΕ σε επίπεδο ανθρώπινου κεφαλαίου στον χώρο της κυβερνοασφάλειας και της κυβερνοάμυνας, το Συμβούλιο εκφράζει ικανοποίηση για την πρωτοβουλία περί ακαδημίας κυβερνοδεξιοτήτων, από την οποία θα επωφεληθεί ενδεχομένως και το εργατικό δυναμικό για την άμυνα στον κυβερνοχώρο.

29. Το Συμβούλιο ζητεί από τα κράτη μέλη να ανταλλάσσουν πληροφορίες σχετικά με τις βέλτιστες πρακτικές για την ανάπτυξη ειδικευμένων επαγγελματιών στον τομέα της κυβερνοασφάλειας, αξιοποιώντας τις συνέργειες μεταξύ πρωτοβουλιών στρατιωτικού, μη στρατιωτικού και σχετικού με την επιβολή του νόμου χαρακτήρα και καλεί την ΕΑΑΑ, με την υποστήριξη και την εμπειρογνωσία του ΕΟΑ και του ENISA, να εξετάσει με ποιους τρόπους θα ενισχυθούν οι ανταλλαγές βέλτιστων πρακτικών και οι περαιτέρω συνέργειες μεταξύ στρατιωτικών και μη στρατιωτικών τομέων όσον αφορά την κατάρτιση και την ανάπτυξη δεξιοτήτων κυβερνοάμυνας.

30. Το Συμβούλιο υπογραμμίζει πόσο σημαντική είναι η αμοιβαία κατανόηση όσον αφορά τη σύνθεση του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας και τις συναφείς δεξιότητες, προκειμένου να εντοπιστούν και να αντιμετωπιστούν τα κενά στην αγορά εργασίας στον τομέα της κυβερνοασφάλειας, και υπογραμμίζει επίσης την ανάγκη να εξασφαλιστεί η συμμετοχή όλων των ενδιαφερόμενων μερών, συμπεριλαμβανομένων των κρατών μελών και του κλάδου. Το Συμβούλιο αναγνωρίζει ότι η θέσπιση δεικτών για την παρακολούθηση της αγοράς εργασίας στον τομέα της κυβερνοασφάλειας θα συμβάλει στον προσδιορισμό των αναγκών σε δεξιότητες κυβερνοασφάλειας και στην επαρκή διοχέτευση κονδυλίων, συμβάλλοντας παράλληλα στην εκπλήρωση των υποχρεώσεων που σχετίζονται με συγκεκριμένες πολιτικές και συγκεκριμένα όσων απορρέουν από την NIS2. Το Συμβούλιο χαιρετίζει την πρόταση για πλαίσιο πιστοποίησης δεξιοτήτων κυβερνοάμυνας και καλεί τον ύπατο εκπρόσωπο, υπό την ιδιότητά του ως επικεφαλής της ΕΑΑΑ, να την αναπτύξει, σε συνεργασία με την ΕΥΕΔ, την Επιτροπή και τα κράτη μέλη, αξιοποιώντας πρωτοβουλίες μη στρατιωτικού χαρακτήρα.

IV. **Εταιρικές σχέσεις για την αντιμετώπιση κοινών προκλήσεων**

31. Το Συμβούλιο καλεί τον ύπατο εκπρόσωπο και την Επιτροπή να ενισχύσουν και να προωθήσουν τη συνεργασία τους και να διερευνήσουν το ενδεχόμενο αμοιβαία επωφελών και ειδικά προσαρμοσμένων συμπράξεων στον τομέα της χάραξης πολιτικών κυβερνοάμυνας, συμπεριλαμβανομένης της οικοδόμησης ικανοτήτων κυβερνοάμυνας μέσω του Ευρωπαϊκού Μηχανισμού για την Ειρήνη (ΕΜΕ). Για τον σκοπό αυτό, η κυβερνοάμυνα θα πρέπει να προστεθεί ως σημείο στους διαλόγους και τις διαβουλεύσεις της ΕΕ για τον κυβερνοχώρο και στις εν γένει διαβουλεύσεις με εταίρους για την ασφάλεια και την άμυνα. Επιπλέον, θα πρέπει να ενισχυθούν οι διάλογοι και η συνεργασία με τον ιδιωτικό τομέα. Το Συμβούλιο υπογραμμίζει ότι η διεθνής συνεργασία σχετικά με τα πρότυπα και την πιστοποίηση της κυβερνοασφάλειας θα αποτελούσε παράγοντα προστιθέμενης αξίας για την ευρωπαϊκή βιομηχανία. Ως εκ τούτου, χαιρετίζει τη δέσμευση της Επιτροπής να καταστήσει το στοιχείο αυτό ουσιαστικό μέρος των κυβερνοδιαλόγων της ΕΕ με τρίτες χώρες και διεθνείς οργανισμούς.

32. Το Συμβούλιο τονίζει τη σημασία της διεθνούς συνεργασίας για την αποτροπή ή τη μείωση των κινδύνων συγκρούσεων στον κυβερνοχώρο, ιδίως μέσω της περαιτέρω ανάπτυξης και επιχειρησιακής εφαρμογής μέτρων οικοδόμησης εμπιστοσύνης (ΜΟΕ) σε περιφερειακό και διεθνές επίπεδο, όπως μεταξύ άλλων στα Ηνωμένα Έθνη, και μέσω της περαιτέρω ενθάρρυνσης της χρήσης υφιστάμενων ΜΟΕ για τον κυβερνοχώρο, όπως στο πλαίσιο του Οργανισμού για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ), συμπεριλαμβανομένων των περιόδων διεθνών εντάσεων.
Η ΕΕ και τα κράτη μέλη της επισημαίνουν ότι στον κυβερνοχώρο εφαρμόζεται το ισχύον διεθνές δίκαιο και τονίζουν τη σημασία της συνέχισης των προσπαθειών για να στηριχθεί και να προωθηθεί το πλαίσιο των Ηνωμένων Εθνών για την υπεύθυνη συμπεριφορά των κρατών και για να γίνει πραγματικότητα η υλοποίησή του, μεταξύ άλλων μέσω της θέσπισης του προγράμματος δράσης για την προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA).

33. Σύμφωνα με τις κοινές δηλώσεις για τη συνεργασία ΕΕ-ΝΑΤΟ, το Συμβούλιο καλεί τον ύπατο εκπρόσωπο, επίσης υπό την ιδιότητά του ως επικεφαλής του ΕΟΑ, και την Επιτροπή, να ενισχύσουν, να εμβαθύνουν και να επεκτείνουν περαιτέρω την εταιρική σχέση με το ΝΑΤΟ στον κυβερνοχώρο, με πλήρη σεβασμό των αρχών της συμμετοχικότητας, της αμοιβαιότητας, του αμοιβαίου ανοικτού χαρακτήρα και της διαφάνειας, καθώς και της αυτονομίας λήψης αποφάσεων αμφότερων των οργανισμών. Χωρίς να αγνοεί την ανάγκη να εξασφαλιστούν συμπληρωματικές και συντονισμένες προσπάθειες με την πληρέστερη δυνατή συμμετοχή όσων κρατών δεν αποτελούν μέρος του ΝΑΤΟ και για αποφυγή περιττών αλληλοεπικαλύψεων, το Συμβούλιο ζητεί να καθιερωθούν δεσμοί στα σχετικά επίπεδα μεταξύ ΕΕ και ΝΑΤΟ όσον αφορά την κατάρτιση, την εκπαίδευση, την αντίληψη της κατάστασης, τις ασκήσεις και τις πλατφόρμες Ε&Α, και ζητεί να επιδιωχθούν δυνητικές συνέργειες ανάμεσα στις αντίστοιχες προαιρετικές δεσμεύσεις για την ανάπτυξη εθνικών δυνατοτήτων κυβερνοάμυνας και τα πλαίσια διαχείρισης κρίσεων, την προστασία των υποδομών ζωτικής σημασίας και την ενίσχυση των ανταλλαγών σε επίπεδο αντίληψης της κατάστασης, τις συντονισμένες αντιδράσεις σε κακόβουλες κυβερνοδραστηριότητες, καθώς και τις προσπάθειες οικοδόμησης ικανοτήτων σε τρίτες χώρες. Στο πλαίσιο αυτό περιλαμβάνονται η τεχνική συμφωνία μεταξύ της ομάδας αντιμετώπισης συμβάντων πληροφορικής του ΝΑΤΟ (NCIRC) και της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική της ΕΕ (CERT-ΕΕ), καθώς και ο ενισχυμένος πολιτικός διάλογος για θέματα κυβερνοάμυνας που διεξάγεται σε όλα τα επίπεδα.

V. **Συμπέρασμα**

34. Με βάση τα συμπεράσματα του Συμβουλίου σχετικά με την πολιτική της ΕΕ για την κυβερνοάμυνα, το Συμβούλιο καλεί τον ύπατο εκπρόσωπο και την Επιτροπή να εκπονήσουν σχέδιο εφαρμογής της πολιτικής που θα εγκρίνουν τα κράτη μέλη, έως το δεύτερο τρίμηνο του 2023. Το Συμβούλιο καλεί επίσης τα κράτη μέλη, εφόσον το επιθυμούν, να εκθέσουν τις φιλοδοξίες και τις δράσεις τους όσον αφορά την κυβερνοάμυνα στο πλαίσιο της πολιτικής της ΕΕ για την κυβερνοάμυνα και να αξιοποιήσουν πλήρως προαιρετικές μη νομικά δεσμευτικές συστάσεις και δεσμεύσεις για να εντείνουν τις εθνικές και πολυεθνικές προσπάθειές τους στον τομέα της κυβερνοάμυνας, με στόχο τη μεγιστοποίηση αντικτύπου σε επίπεδο ΕΕ. Ο ύπατος εκπρόσωπος, η Επιτροπή και τα κράτη μέλη καλούνται να υποβάλλουν εκθέσεις και να πραγματοποιούν συζήτηση κάθε χρόνο σχετικά με την πρόοδο της υλοποίησης των στοιχείων της κοινής ανακοίνωσης και του σχεδίου εφαρμογής της, αρχής γενομένης από το δεύτερο τρίμηνο του 2024.