Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 19 Νοεμβρίου 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	19 Νοεμβρίου 2018
Αποδέκτης:	Αντιπροσωπίες
Θέμα:	Πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση 2018)

Επισυνάπτεται στο παράρτημα για τις αντιπροσωπίες το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση 2018), που εγκρίθηκε από το Συμβούλιο κατά την 3652η σύνοδό του στις 19 Νοεμβρίου 2018.

ΠΑΡΑΡΤΗΜΑ

ΠΛΑΙΣΙΟ ΠΟΛΙΤΙΚΗΣ ΤΗΣ ΕΕ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΜΥΝΑ

(όπως επικαιροποιήθηκε το 2018)

Πεδίο εφαρμογής και στόχοι

Για να ανταποκριθούν στις μεταβαλλόμενες προκλήσεις που αφορούν την ασφάλεια, η ΕΕ και τα κράτη μέλη της πρέπει να ενισχύσουν την κυβερνοανθεκτικότητά τους και να αναπτύξουν αξιόπιστες ικανότητες κυβερνοασφάλειας και κυβερνοάμυνας.

Το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (CDPF) στηρίζει την ανάπτυξη ικανοτήτων κυβερνοάμυνας των κρατών μελών της ΕΕ καθώς και την ενίσχυση της κυβερνοπροστασίας των υποδομών της ΕΕ για την ασφάλεια και την άμυνα, με την επιφύλαξη της εθνικής νομοθεσίας των κρατών μελών και της νομοθεσίας της ΕΕ, συμπεριλαμβανομένου του πεδίου εφαρμογής της κυβερνοάμυνας, όπου αυτό ορίζεται.

Ο κυβερνοχώρος είναι το πέμπτο πεδίο επιχειρήσεων, μαζί με την ξηρά, τη θάλασσα, τον αέρα και το διάστημα: η επιτυχής υλοποίηση των αποστολών και των επιχειρήσεων της ΕΕ εξαρτάται όλο και περισσότερο από την αδιάλειπτη πρόσβαση σε έναν ασφαλή κυβερνοχώρο και προϋποθέτει, ως εκ τούτου, αξιόπιστες και ανθεκτικές επιχειρησιακές ικανότητες στον κυβερνοχώρο.

Ο στόχος του επικαιροποιημένου CDPF είναι να αναπτυχθεί περαιτέρω η πολιτική της ΕΕ για την κυβερνοάμυνα λαμβάνοντας υπόψη σχετικές εξελίξεις σε άλλα σχετικά φόρουμ και τομείς πολιτικής και την εφαρμογή του CDPF από το 2014. Στο CDPF προσδιορίζονται οι τομείς προτεραιότητας για την κυβερνοάμυνα και διευκρινίζονται οι ρόλοι των διαφόρων ευρωπαϊκών φορέων με πλήρη σεβασμό των αρμοδιοτήτων και ευθυνών των φορέων της Ένωσης και των κρατών μελών καθώς και του θεσμικού πλαισίου της ΕΕ και της αυτονομίας της κατά τη λήψη αποφάσεων.

Πλαίσιο

Στα συμπεράσματα του Ευρωπαϊκού Συμβουλίου του Δεκεμβρίου του 2013 σχετικά με την ΚΠΑΑ, όπως και στα αντίστοιχα συμπεράσματα του Συμβουλίου του Νοεμβρίου του 2013, ζητήθηκε η ανάπτυξη πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα, βάσει πρότασης της Ύπατης Εκπροσώπου, σε συνεργασία με την Ευρωπαϊκή Επιτροπή και τον Ευρωπαϊκό Οργανισμό Άμυνας (ΕΟΑ). Το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα εγκρίθηκε από το Συμβούλιο στις 18 Νοεμβρίου 2014[1] και έκτοτε, χάρη στην εφαρμογή του, απτά αποτελέσματα έχουν συμβάλει ώστε να ενισχυθούν σημαντικά οι ικανότητες κυβερνοάμυνας των κρατών μελών. Στο πλαίσιο της ετήσιας έκθεσης του 2017 για την εφαρμογή του πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα[2] και λαμβάνοντας υπόψη τις πρωτοβουλίες της ΕΕ στον τομέα της ασφάλειας και της άμυνας, ιδίως τη συντονισμένη ετήσια επανεξέταση στον τομέα της άμυνας (CARD), τη μόνιμη διαρθρωμένη συνεργασία (PESCO), το Ευρωπαϊκό Ταμείο Άμυνας (ΕΤΑ) και το σύμφωνο μη στρατιωτικής ΚΠΑΑ καθώς και την αναθεώρηση του σχεδίου ανάπτυξης ικανοτήτων (CDP) και του σχεδίου ανάπτυξης μη στρατιωτικών ικανοτήτων (CCDP) το 2018, τα κράτη μέλη ζήτησαν ενημέρωση για το πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα.

Η κυβερνοασφάλεια είναι προτεραιότητα για τη συνολική στρατηγική της ΕΕ για την εξωτερική πολιτική και την πολιτική ασφαλείας και για το ενωσιακό επίπεδο φιλοδοξίας[3]. Η συνολική στρατηγική τονίζει την ανάγκη να αυξηθούν οι ικανότητες για την προστασία της ΕΕ και των πολιτών της και την αντιμετώπιση εξωτερικών κρίσεων. Η συνολική στρατηγική υπογραμμίζει την ανάγκη να ενισχυθεί η ΕΕ ως κοινότητα ασφάλειας. Στο πλαίσιο αυτό, οι προσπάθειες στον τομέα της ασφάλειας και της άμυνας θα πρέπει επίσης να ενισχύουν τον στρατηγικό ρόλο της ΕΕ και την ικανότητά της να ενεργεί αυτόνομα, όταν και όπου αυτό είναι αναγκαίο, καθώς και με τους εταίρους, όταν αυτό είναι δυνατό. Οι στόχοι αυτοί απαιτούν μεγαλύτερη συνεργασία στην ανάπτυξη ικανοτήτων, που θα προωθήσει την αποτελεσματικότητα και τη διαλειτουργικότητα των ικανοτήτων που θα προκύψουν, στρατιωτικών και μη.

---

1 Έγγραφο του Συμβουλίου 15585/14, 18.11.2014

2 Έγγραφο του Συμβουλίου 15870/17, 19.12.2017

3 Συμπεράσματα του Συμβουλίου σχετικά με την εφαρμογή της συνολικής στρατηγικής της ΕΕ στον τομέα της ασφάλειας και της άμυνας, 14.11.2016

Η κοινή δέσμη προτάσεων για την εφαρμογή της κοινής δήλωσης που υπέγραψαν ο Πρόεδρος του Ευρωπαϊκού Συμβουλίου, ο Πρόεδρος της Ευρωπαϊκής Επιτροπής και ο Γενικός Γραμματέας του Οργανισμού Βορειοατλαντικού Συμφώνου στη Βαρσοβία στις 8 Ιουλίου 2016[4] περιλαμβάνει απτά μέτρα για την επέκταση της συνεργασίας ΕΕ-NATO στον τομέα της κυβερνοασφάλειας και της κυβερνοάμυνας, μεταξύ άλλων στο πλαίσιο αποστολών και επιχειρήσεων, καθώς και σε σχέση με την ανάπτυξη ικανοτήτων κυβερνοάμυνας, έρευνας και τεχνολογίας, κατάρτισης, εκπαίδευσης, ασκήσεων και ενσωμάτωσης της κυβερνοδιάστασης στη διαχείριση κρίσεων. Η συνεργασία αυτή σέβεται πλήρως τις αρχές της δημοσιότητας, της διαφάνειας, της συμμετοχικότητας, της αμοιβαιότητας και της αυτονομίας λήψης αποφάσεων της ΕΕ. Μια τεχνική συμφωνία μεταξύ της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-EU) και της ομάδας αντιμετώπισης συμβάντων πληροφορικής του NATO (NCIRC), που υπεγράφη τον Φεβρουάριο του 2016, διευκολύνει την ανταλλαγή τεχνικών πληροφοριών ώστε να βελτιώνεται η πρόληψη, η ανίχνευση και η αντιμετώπιση κυβερνοσυμβάντων που αφορούν αμφότερους τους οργανισμούς.

Αξίζει να υπενθυμίσουμε ότι αρκετές πολιτικές της ΕΕ συμβάλλουν στους στόχους της πολιτικής κυβερνοάμυνας ως έχουν στο παρόν έγγραφο. Επιπλέον, το παρόν πλαίσιο λαμβάνει υπόψη και τη σχετική νομοθεσία, πολιτική και τεχνολογική στήριξη στο μη στρατιωτικό πεδίο. Για παράδειγμα τον Ιούλιο του 2016, το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ενέκριναν την οδηγία για την ασφάλεια δικτύων και πληροφοριών[5] (NIS), η οποία θα ενισχύσει τη γενική ετοιμότητα των κρατών μελών έναντι κυβερνοαπειλών και την πανευρωπαϊκή συνεργασία. Η οδηγία αυτή θεσπίζει μέτρα που θα επιτύχουν υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών εντός της Ένωσης, με σκοπό την καλύτερη λειτουργία της εσωτερικής αγοράς. Η προθεσμία για τη μεταφορά της οδηγίας στο εθνικό δίκαιο έληξε στις 9 Μαΐου 2018.

---

4 Συμπεράσματα του Συμβουλίου σχετικά με την εφαρμογή της κοινής δήλωσης του Προέδρου του Ευρωπαϊκού Συμβουλίου, του Προέδρου της Ευρωπαϊκής Επιτροπής και του Γενικού Γραμματέα του Οργανισμού Βορειοατλαντικού Συμφώνου (6 Δεκεμβρίου 2016, 15283/16· 5 Δεκεμβρίου 2017, 14802/17)

5 Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

Η πρόταση, του Σεπτεμβρίου 2017, για μια Πράξη για την ασφάλεια στον κυβερνοχώρο περιλαμβάνει νέα εντολή για τον οργανισμό της ΕΕ για την κυβερνοασφάλεια (ENISA) και τη θέσπιση ενός πανευρωπαϊκού πλαισίου πιστοποίησης. Μόλις θεσπιστεί, το πλαίσιο πιστοποίησης θα παρέχει στήριξη για υψηλού επιπέδου διαδικασίες, προϊόντα και υπηρεσίες ΤΠΕ, θα προσδώσει ανταγωνιστικό πλεονέκτημα και θα ενισχύσει την εμπιστοσύνη από πλευράς καταναλωτών και υπεύθυνων προμηθειών. Επιπλέον, τον Σεπτέμβριο του 2017 η Επιτροπή έκανε ένα ακόμη βήμα για να προετοιμάσει την ΕΕ για την περίπτωση διασυνοριακών συμβάντων κυβερνοασφάλειας μεγάλης κλίμακας («Blue Print»). Επί του παρόντος, συνεργάζεται με τα κράτη μέλη και με θεσμικά και λοιπά όργανα και οργανισμούς για να αναπτύξουν την ευρωπαϊκή συνεργασία για τις κρίσεις κυβερνοασφάλειας, θέτοντας σε εφαρμογή την πρακτική επιχειρησιακή λειτουργία και τεκμηρίωση όλων των σχετικών φορέων, μεθόδων και διαδικασιών στο πλαίσιο των υφιστάμενων μηχανισμών της ΕΕ για τη διαχείριση κρίσεων και καταστροφών, ιδίως τις ολοκληρωμένες ρυθμίσεις για την αντιμετώπιση πολιτικών κρίσεων.

Τα συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο, που εγκρίθηκαν τον Νοέμβριο του 2016, περιέγραφαν τον κοινό στόχο να συμβάλλουμε στη στρατηγική αυτονομία της ΕΕ, όπως αναφέρεται στα συμπεράσματα του Συμβουλίου του Νοεμβρίου 2016 σχετικά με τη συνολική στρατηγική για την εξωτερική πολιτική και πολιτική ασφαλείας της Ευρωπαϊκής Ένωσης, μεταξύ άλλων στον κυβερνοχώρο. Το Ευρωπαϊκό Συμβούλιο επανέλαβε το μήνυμα αυτό τον Ιούνιο του 2018, ενώ υπογράμμισε και την ανάγκη να ενισχυθούν οι ικανότητες έναντι των απειλών κυβερνοασφάλειας από χώρες εκτός ΕΕ.

Το 2017 το Συμβούλιο ενέκρινε ένα πλαίσιο για μια κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»)[6]. Το πλαίσιο αναμένεται να ενθαρρύνει τη συνεργασία, να διευκολύνει τον μετριασμό των απειλών και να επηρεάσει τη συμπεριφορά των εν δυνάμει δραστών σε μακροπρόθεσμη βάση. Το πλαίσιο κάνει χρήση των μέτρων της ΚΕΠΠΑ, μεταξύ άλλων των περιοριστικών μέτρων, για την πρόληψη και την αντιμετώπιση κακόβουλων κυβερνοδραστηριοτήτων. Οι δράστες κακόβουλων κυβερνοδραστηριοτήτων πρέπει να λογοδοτούν για τις πράξεις τους· τα κράτη μέλη ενθαρρύνονται να αναπτύσσουν περαιτέρω την ικανότητά τους να απαντούν σε κακόβουλες κυβερνοδραστηριότητες κατά τρόπο συντονισμένο και σύμφωνα με την εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο. Τα κράτη δεν θα πρέπει να προβαίνουν ή εν γνώσει τους να στηρίζουν δραστηριότητες ΤΠΕ κατά παράβαση των υποχρεώσεών τους δυνάμει του διεθνούς δικαίου· επίσης δεν θα πρέπει εν γνώσει τους να επιτρέπουν να χρησιμοποιείται το έδαφός τους για διεθνώς παράνομες πράξεις με χρήση των ΤΠΕ.

Τον Σεπτέμβριο του 2017, η Επιτροπή και η ΥΕ/ΑΕ παρουσίασαν μια κοινή ανακοίνωση[7] για θέματα κυβερνοχώρου ώστε να μετριαστούν οι κίνδυνοι που προκύπτουν από το νέο τοπίο απειλών. Περιλαμβάνει την κυβερνοάμυνα ως έναν από τους βασικούς τομείς δράσης· το CDPF είναι ένας από τους πυλώνες της ουσιαστικής εφαρμογής της[8].

Τα συμπεράσματα του Συμβουλίου του Νοεμβρίου του 2017 για θέματα κυβερνοχώρου αναγνώριζαν την αυξανόμενη διασύνδεση μεταξύ κυβερνοασφάλειας και κυβερνοάμυνας και ζήτησαν να ενταθεί η συνεργασία στον τομέα της κυβερνοάμυνας, μεταξύ άλλων με την ενθάρρυνση της συνεργασίας μη στρατιωτικών και στρατιωτικών φορέων αντιμετώπισης συμβάντων. Τόνιζαν επίσης ότι τυχόν ιδιαιτέρως σοβαρό κυβερνοσυμβάν ή κυβερνοκρίση θα μπορούσε να θεωρηθεί επαρκής λόγος ώστε ένα κράτος μέλος να επικαλεστεί τη ρήτρα αλληλεγγύης της ΕΕ ή/και τη ρήτρα αμοιβαίας συνδρομής.

---

6 Συμπεράσματα του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»), 9916/17, 7 Ιουνίου 2017

7 Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ (13 Σεπτεμβρίου 2017, JOIN(2017) 450 final)

8 Συμπεράσματα του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ (20 Νοεμβρίου 2017, 14435/17)

Στις 11 Δεκεμβρίου 2017 θεσπίστηκε η μόνιμη διαρθρωμένη συνεργασία (PESCO). Αυτό το φιλόδοξο, δεσμευτικό και συμμετοχικό πλαίσιο συνεργασίας θεσπίστηκε μεταξύ 25 κρατών μελών και περιλαμβάνει τη δέσμευσή τους να ενισχύσουν τις προσπάθειες συνεργασίας για θέματα κυβερνοάμυνας, καθώς και σχετικά έργα PESCO. Η πρώτη δέσμη έργων PESCO που ορίστηκε από κράτη μέλη που συμμετέχουν στην PESCO το 2017 περιλαμβάνει δύο έργα σχετικά με την κυβερνοάμυνα: το έργο «Ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο και αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο» και το έργο «Πλατφόρμα ανταλλαγής πληροφοριών για την αντιμετώπιση απειλών και συμβάντων στον κυβερνοχώρο». Προβλέπονται και άλλες δέσμες έργων PESCO. Η PESCO θα αναπτύξει ικανότητες κυβερνοάμυνας, ενισχύοντας έτσι τη συνεργασία μεταξύ συμμετεχόντων κρατών μελών και αυξάνοντας τη διαλειτουργικότητα.

Το επικαιροποιημένο σχέδιο ανάπτυξης ικανοτήτων (CDP) που ενέκρινε το διοικητικό συμβούλιο του ΕΟΑ τον Ιούνιο του 2018 χαρακτηρίζει την κυβερνοάμυνα κομβικό σημείο. Αναγνωρίζει την ανάγκη για αμυντικές κυβερνοεπιχειρήσεις σε οποιοδήποτε επιχειρησιακό πλαίσιο. Αυτές θα πρέπει να βασίζονται σε επίγνωση της τρέχουσας και της προβλεπόμενης κατάστασης στον κυβερνοχώρο η οποία να αξιοποιεί την υψηλή τεχνολογία, συμπεριλαμβανομένης της ικανότητας συνδυασμού μεγάλων ποσοτήτων δεδομένων και πληροφοριών από πολλές πηγές προς υποστήριξη της ταχείας λήψης αποφάσεων και της ενισχυμένης αυτοματοποίησης της διαδικασίας συγκέντρωσης και ανάλυσης δεδομένων και της διαδικασίας στήριξης της λήψης αποφάσεων. Το CDP του 2018 εντοπίζει προτεραιότητες ικανότητας κυβερνοάμυνας στους ακόλουθους τομείς: συνεργασία και συνέργειες με συναφείς φορείς σε όλους τους τομείς της κυβερνοάμυνας και της κυβερνοασφάλειας· έρευνα και τεχνολογικές δραστηριότητες στον τομέα της κυβερνοάμυνας· πλαίσια μηχανοτεχνίας για συστήματα σχετικά με κυβερνοεπιχειρήσεις· εκπαίδευση, κατάρτιση, ασκήσεις και αξιολόγηση (ETEE)· αντιμετώπιση προκλήσεων κυβερνοάμυνας σε αέρα, διάστημα, θάλασσα και ξηρά.

Τέλος, τα λίγα τελευταία χρόνια, έχει γίνει σαφές ότι είναι αναγκαίο η διεθνής κοινότητα να προλαμβάνει τις συγκρούσεις, να συνεργάζεται και να σταθεροποιήσει τον κυβερνοχώρο. Η ΕΕ προωθεί, σε στενή συνεργασία με άλλους διεθνείς οργανισμούς, ιδιαίτερα με τον ΟΗΕ, τον ΟΑΣΕ και το περιφερειακό φόρουμ του ASEAN, ένα στρατηγικό πλαίσιο για την πρόληψη συγκρούσεων, τη συνεργασία και τη σταθερότητα στον κυβερνοχώρο, που περιλαμβάνει (i) την εφαρμογή του διεθνούς δικαίου, και ιδίως του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, στον κυβερνοχώρο· (ii) τον σεβασμό των οικουμενικών μη δεσμευτικών προτύπων, κανόνων και αρχών υπεύθυνης κρατικής συμπεριφοράς· (iii) την ανάπτυξη και εφαρμογή περιφερειακών μέτρων οικοδόμησης εμπιστοσύνης (ΜΟΕ). Το πλαίσιο πολιτικής για την κυβερνοάμυνα θα πρέπει επίσης να στηρίζει αυτή την προσπάθεια.

Προτεραιότητες

Το επικαιροποιημένο CDPF εντοπίζει έξι τομείς προτεραιότητας. Εστιάζει πρωτίστως στην ανάπτυξη ικανοτήτων κυβερνοάμυνας, καθώς και στην προστασία των δικτύων επικοινωνίας και πληροφοριών της ΚΠΑΑ. Στους τομείς προτεραιότητας περιλαμβάνονται: η κατάρτιση και οι ασκήσεις, η έρευνα και η τεχνολογία, η στρατιωτική και μη στρατιωτική συνεργασία και η διεθνής συνεργασία. Στον τομέα της κατάρτισης, έμφαση δίδεται στην αναβάθμιση της κατάρτισης στην κυβερνοάμυνα από τα κράτη μέλη και της κατάρτισης για την κυβερνοευαισθητοποίηση της ιεραρχίας διοίκησης της ΚΠΑΑ. Είναι επίσης σημαντική η κατάλληλη αντιμετώπιση της κυβερνοδιάστασης στις ασκήσεις ώστε να βελτιωθεί η ικανότητα της ΕΕ να αντιδρά στις κυβερνοκρίσεις και στις υβριδικές κρίσεις μέσω της βελτίωσης των διαδικασιών λήψης αποφάσεων και της διαθεσιμότητας των πληροφοριών. Ο κυβερνοχώρος είναι ένα ταχέως αναπτυσσόμενο πεδίο και οι νέες τεχνολογικές εξελίξεις θα πρέπει να υποστηρίζονται, τόσο στο μη στρατιωτικό όσο και στο στρατιωτικό πεδίο. Η στρατιωτική και μη στρατιωτική συνεργασία στον τομέα του κυβερνοχώρου είναι κομβικής σημασίας για να διασφαλίσουμε μια συνεκτική απάντηση στις κυβερνοαπειλές. Τέλος, εξίσου σημαντικό είναι ότι η ενίσχυση της συνεργασίας με διεθνείς εταίρους θα μπορούσε να συμβάλλει ώστε να αυξηθεί η κυβερνοασφάλεια εντός της ΕΕ και πέραν αυτής καθώς και για την προώθηση των αρχών και των αξιών της ΕΕ.

Το πλαίσιο αυτό σκιαγραφεί προτάσεις και ευκαιρίες συντονισμού μεταξύ συναφών θεσμικών και λοιπών οργάνων, και οργανισμών της ΕΕ. Επίσης αποτυπώνει τον σημαντικό ρόλο του ιδιωτικού τομέα για την ανάπτυξη τεχνολογιών για την κυβερνοασφάλεια και την κυβερνοάμυνα.

Επιπροσθέτως, το CDPF στηρίζει περαιτέρω την ένταξη της κυβερνοάμυνας στους μηχανισμούς διαχείρισης κρίσεων της Ένωσης όπου, για την αντιμετώπιση των επιπτώσεων μιας κυβερνοκρίσης, ενδέχεται να ισχύουν οι σχετικές διατάξεις της Συνθήκης για την ΕΕ και της Συνθήκης για τη λειτουργία της ΕΕ[9].

1. Υποστήριξη της ανάπτυξης ικανοτήτων κυβερνοάμυνας των κρατών μελών

Η ανάπτυξη των σχετικών ικανοτήτων και τεχνολογιών θα πρέπει να λαμβάνει υπόψη όλες τις πτυχές της ανάπτυξης ικανοτήτων, όπως θεωρία, ηγεσία, οργάνωση, προσωπικό, εκπαίδευση, βιομηχανία, τεχνολογία, υποδομές, υλικοτεχνική υποστήριξη και διαλειτουργικότητα. Για το σκοπό αυτό, τα κράτη μέλη θα πρέπει να εντείνουν τις προσπάθειές τους για την παροχή αποτελεσματικών ικανοτήτων κυβερνοάμυνας. Η ΕΥΕΔ, η Επιτροπή και ο ΕΟΑ θα πρέπει να συνεργαστούν και να στηρίξουν τις προσπάθειες αυτές.

Απαιτείται συνεχής αξιολόγηση των αδύναμων σημείων των υποδομών πληροφοριών που υποστηρίζουν τις αποστολές και επιχειρήσεις ΚΠΑΑ, μαζί με αντίληψη, σχεδόν σε πραγματικό χρόνο, της αποτελεσματικότητας της προστασίας. Από επιχειρησιακή άποψη, ένας από τους κύριους στόχους των δραστηριοτήτων κυβερνοάμυνας θα είναι η διατήρηση της διαθεσιμότητας, της αρτιότητας και της εμπιστευτικότητας των δικτύων επικοινωνίας και πληροφοριών ΚΠΑΑ, εκτός αν προβλέπεται διαφορετικά στην εντολή των επιχειρήσεων ή των αποστολών. Επιπλέον, η ΕΥΕΔ, σε συνεργασία με τα κράτη μέλη, θα ενσωματώσει περαιτέρω κυβερνοϊκανότητες σε αποστολές και επιχειρήσεις ΚΠΑΑ.

Οι δράστες κακόβουλων δραστηριοτήτων στον κυβερνοχώρο πρέπει να λογοδοτούν για τις πράξεις τους. Είναι σημαντικό τα κράτη μέλη, με την υποστήριξη της ΕΥΕΔ, να ενισχύσουν την αμοιβαία συνεργασία για την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. Η εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο αναπτύχθηκε για να συμβάλει στην επίτευξη τέτοιου είδους κοινής απάντησης. Η ΕΥΕΔ και ο ΕΟΑ θα πρέπει να διοργανώνουν τακτικές ασκήσεις με βάση την εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο, στις οποίες τα κράτη μέλη της ΕΕ να μπορούν να κάνουν πρακτική εξάσκηση.

---

9 Άρθρο 222 της ΣΛΕΕ και άρθρο 42 παράγραφος 7 της ΣΕΕ, λαμβάνοντας δεόντως υπόψη το άρθρο 17 της ΣΕΕ.

Λαμβάνοντας υπόψη ότι στην εθνική νομοθεσία των κρατών μελών καθώς και στη νομοθεσία της ΕΕ το πεδίο εφαρμογής της κυβερνοάμυνας είναι ευρύ και διαφοροποιημένο, όπου και όταν ορίζεται, υπάρχει ανάγκη να αναπτυχθεί μια κοινή συνολική αντίληψη σχετικά με το πεδίο εφαρμογής της κυβερνοάμυνας.

Δεδομένου ότι οι στρατιωτικές επιχειρήσεις της ΚΠΑΑ εξαρτώνται από υποδομή διοίκησης, ελέγχου, επικοινωνιών και υπολογιστών (C4) που παρέχεται από τα κράτη μέλη, απαιτείται ορισμένος βαθμός στρατηγικής σύγκλισης κατά τον σχεδιασμό των απαιτήσεων κυβερνοάμυνας για την υποδομή πληροφοριών.

Για την ανάπτυξη ικανοτήτων κυβερνοάμυνας με βάση τις εργασίες της συναφούς ομάδας έργου του ΕΟΑ, οι ΕΥΕΔ/ΕΟΑ και τα κράτη μέλη:

- Θα χρησιμοποιήσουν το CDP και άλλα μέσα διευκόλυνσης και υποστήριξης της συνεργασίας μεταξύ κρατών μελών, όπως την CARD, προκειμένου να υπάρξει μεγαλύτερη σύγκλιση κατά τον σχεδιασμό των απαιτήσεων κυβερνοάμυνας των κρατών μελών σε στρατηγικό επίπεδο, ιδίως όσον αφορά τα ακόλουθα: παρακολούθηση, επίγνωση της κατάστασης, πρόληψη, ανίχνευση και προστασία, ανταλλαγή πληροφοριών, ικανότητα εγκληματολογικών ερευνών και ανάλυσης κακόβουλου λογισμικού, άντληση διδαγμάτων, περιορισμός ζημίας, ικανότητα δυναμικής ανάκαμψης, αποθήκευση κατανεμημένων δεδομένων και εφεδρικά δεδομένα.
- Θα υποστηρίξουν τα υπάρχοντα και μελλοντικά έργα συνένωσης και κοινής χρήσης στον τομέα της κυβερνοάμυνας για στρατιωτικές επιχειρήσεις (π.χ. στις εγκληματολογικές έρευνες, σε μεγαλύτερη διαλειτουργικότητα, στη θέσπιση προτύπων).
- Θα αναπτύξουν πρότυπο σύνολο στόχων και απαιτήσεων για τον ορισμό του κατώτατου επιπέδου κυβερνοασφαλείας και εμπιστοσύνης που θα πρέπει να επιτύχουν τα κράτη μέλη, με βάση την υπάρχουσα πείρα σε επίπεδο ΕΕ.

Η ΕΥΕΔ και ο ΕΟΑ:

- Θα διευκολύνουν τις ανταλλαγές μεταξύ των κρατών μελών σχετικά με τις εθνικές θεωρίες κυβερνοάμυνας καθώς και σχετικά με τα προγράμματα πρόσληψης, παραμονής στην υπηρεσία και εφέδρων με άξονα την κυβερνοάμυνα.

Ο ΕΟΑ:

- Θα μελετήσει τα διαφορετικά πεδία εφαρμογής των στρατιωτικών απαιτήσεων κυβερνοάμυνας στην εθνική νομοθεσία και τις βέλτιστες πρακτικές των κρατών μελών. Ο κύριος στόχος της μελέτης θα είναι η ανάπτυξη μιας αρχιτεκτονικής επιχειρήσεων για την κυβερνοάμυνα, η οποία θα συμπεριλάβει στην εθνική και την ενωσιακή νομοθεσία το πεδίο εφαρμογής, τις λειτουργίες και τις απαιτήσεις που χρησιμοποιούνται στον τομέα από τα κράτη μέλη.

Τα κράτη μέλη, σε οικειοθελή βάση:

- Θα βελτιώσουν τη συνεργασία μεταξύ των στρατιωτικών CERT με σκοπό τη βελτίωση της πρόληψης και του χειρισμού συμβάντων.
- Θα αξιοποιήσουν την PESCO για περαιτέρω αύξηση της συνεργασίας στον τομέα της κυβερνοάμυνας, συμπεριλαμβανομένης της υλοποίησης νέων έργων.
- Θα αξιοποιήσουν το Ευρωπαϊκό Ταμείο Άμυνας με σκοπό την από κοινού ανάπτυξη ικανοτήτων κυβερνοάμυνας.
- Θα αναπτύξουν κοινή αντίληψη σχετικά με την εφαρμογή της ρήτρας αμοιβαίας συνδρομής στον τομέα του κυβερνοχώρου, με παράλληλη διατήρηση της ευελιξίας της.
- Θα αναπτύξουν βασικές απαιτήσεις κυβερνοάμυνας για την υποδομή πληροφοριών.
- Εφόσον η βελτίωση των ικανοτήτων κυβερνοάμυνας εξαρτάται από μη στρατιωτική εμπειρογνωμοσύνη στον τομέα της ασφάλειας δικτύων και πληροφοριών, θα αξιοποιήσουν την εμπειρογνωμοσύνη του ENISA, των αρχών των κρατών μελών που συμμετείχαν στην ομάδα συνεργασίας NIS και άλλων πιθανών οντοτήτων σε επίπεδο ΕΕ με εμπειρογνωμοσύνη στην κυβερνοασφάλεια πολιτών.

Τα κράτη μέλη, το στρατιωτικό προσωπικό της ΕΥΕΔ/ΕΕ, η ΕΑΑΑ και ο ΕΟΑ:

- Θα εξετάσουν την ανάπτυξη εκπαιδευτικών προγραμμάτων σε θέματα κυβερνοάμυνας, εν όψει της πιστοποίησης των ομάδων μάχης της ΕΕ.

Η Επιτροπή, σε συνεργασία με τα κράτη μέλη:

- Θα εξετάσει την ένταξη της κυβερνοασφάλειας στα προγράμματα εργασίας του ευρωπαϊκού προγράμματος βιομηχανικής ανάπτυξης στον τομέα της άμυνας και του Ευρωπαϊκού Ταμείου Άμυνας.

2. Ενίσχυση της προστασίας των δικτύων επικοινωνίας και πληροφοριών της ΚΠΑΑ που χρησιμοποιούνται από οντότητες της ΕΕ

Με την επιφύλαξη του ρόλου της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ (CERT-EU) ως της κεντρικής υπηρεσίας συντονισμού της αντιμετώπισης κυβερνοσυμβάντων για όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και στο πλαίσιο των οικείων κανόνων περί του προϋπολογισμού της Ένωσης, η ΕΥΕΔ θα αναπτύξει κατάλληλη και αυτόνομη αντίληψη των θεμάτων ασφάλειας και άμυνας δικτύου και θα αναπτύξει ίδια ικανότητα σε θέματα ασφάλειας ΤΠ. Σκοπός της θα είναι η ενίσχυση της ανθεκτικότητας των δικτύων ΚΠΑΑ της ΕΥΕΔ, με επίκεντρο την πρόληψη, την ανίχνευση, την αντιμετώπιση συμβάντων, την επίγνωση της κατάστασης, την ανταλλαγή πληροφοριών και μηχανισμούς έγκαιρης προειδοποίησης.

Υπεύθυνη για την προστασία των συστημάτων επικοινωνίας και πληροφοριών της ΕΥΕΔ και την ανάπτυξη ικανοτήτων για την ασφάλεια της τεχνολογίας πληροφοριών (ΤΠ) είναι η Γενική Διεύθυνση Διαχείρισης Προϋπολογισμού και Διοίκησης (ΒΑ) της ΕΥΕΔ. Θα διατεθούν επίσης πρόσθετοι ειδικοί πόροι και στήριξη από το Στρατιωτικό Επιτελείο της ΕΕ (EUMS), τη Διεύθυνση Διαχείρισης Κρίσεων και Σχεδιασμού (CMPD) και τη Μη Στρατιωτική Δυνατότητα Σχεδιασμού και Διεξαγωγής Επιχειρήσεων (CPCC). Οι ανωτέρω ικανότητες για την ασφάλεια ΤΠ θα καλύπτουν διαβαθμισμένα και μη διαβαθμισμένα συστήματα και θα ενσωματώνονται πλήρως στις υπάρχουσες επιχειρησιακές οντότητες.

Απαιτείται επίσης ο εξορθολογισμός των κανόνων ασφάλειας για τα συστήματα πληροφοριών που παρέχονται από τους διάφορους θεσμικούς φορείς της ΕΕ κατά τη διενέργεια επιχειρήσεων και αποστολών ΚΠΑΑ. Σε αυτό το πλαίσιο, θα μπορούσε να εξεταστεί η πρόβλεψη ενιαίας ιεραρχίας διοίκησης με σκοπό την ενίσχυση της ανθεκτικότητας των δικτύων που χρησιμοποιούνται για την ΚΠΑΑ.

Για τον καλύτερο συντονισμό και για την ενίσχυση της προστασίας και της ανθεκτικότητας των συστημάτων επικοινωνίας και πληροφοριών ΚΠΑΑ, δημιουργήθηκε το 2017 ένα εσωτερικό διοικητικό συμβούλιο της ΕΥΕΔ για θέματα κυβερνοχώρου υπό τον Γενικό Γραμματέα της ΕΥΕΔ.

Η ΕΥΕΔ/ΒΑ:

- Θα ενισχύσει, στο πλαίσιο της ΕΥΕΔ, τις ικανότητες στον τομέα της ασφάλειας ΤΠ με βάση τις υπάρχουσες τεχνικές δυνατότητες και διαδικασίες και με επίκεντρο την πρόληψη, την ανίχνευση, την αντιμετώπιση συμβάντων, την επίγνωση της κατάστασης, την ανταλλαγή πληροφοριών και μηχανισμούς έγκαιρης προειδοποίησης. Θα ενισχύσει περαιτέρω τη στρατηγική συνεργασίας με την CERT-EU και τις υφιστάμενες ικανότητες κυβερνοάμυνας.

Η ΕΥΕΔ/ΒΑ, σε συνεργασία με τα EUMS, CMPD και CPCC MPCC:

- Θα αναπτύξει συνεκτική πολιτική και κατευθυντήριες γραμμές για την ασφάλεια στον τομέα της ΤΠ, συνεκτιμώντας επίσης τις τεχνικές απαιτήσεις για την κυβερνοάμυνα σε πλαίσιο ΚΠΑΑ για τις δομές, αποστολές και επιχειρήσεις, λαμβάνοντας υπόψη τα πλαίσια και τις πολιτικές συνεργασίας που ήδη υπάρχουν εντός της ΕΕ με σκοπό τη σύγκλιση των κανόνων, των πολιτικών και της οργάνωσης.

Η ΕΥΕΔ/Ενιαία Ικανότητα Ανάλυσης Πληροφοριών (SIAC):

- Με βάση τις υφιστάμενες δομές, θα ενισχύσει την ικανότητα συλλογής και αξιολόγησης πληροφοριών όσον αφορά τις κυβερνοαπειλές για την αναγνώριση νέων κινδύνων στον κυβερνοχώρο και την παροχή τακτικών αξιολογήσεων, βάσει της στρατηγικής αξιολόγησης απειλών και της παροχής πληροφοριών περί συμβάντων σε σχεδόν πραγματικό χρόνο, τις οποίες συντονίζουν οι αρμόδιες υπηρεσίες της ΕΕ και οι οποίες καθίστανται προσιτές σε διάφορα επίπεδα διαβάθμισης.

Η ΕΥΕΔ/SIAC και η CERT-EU:

- Θα προωθήσουν την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές, σε πραγματικό χρόνο, μεταξύ των κρατών μελών και των αρμόδιων υπηρεσιών της ΕΕ. Για το σκοπό αυτό, θα αναπτυχθούν μηχανισμοί ανταλλαγής πληροφοριών και μέτρα εμπιστοσύνης μεταξύ των αντίστοιχων εθνικών και ευρωπαϊκών αρχών, με εκούσια προσέγγιση βασιζόμενη στην υπάρχουσα συνεργασία.

Η ΕΥΕΔ/EUMS και η MPCC:

- Θα αναπτύξουν περαιτέρω και θα εντάξουν στο σχεδιασμό στρατηγικού επιπέδου την έννοια της κυβερνοάμυνας για στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ.
- Θα αναπτύξουν, σε συνεργασία με το επιχειρησιακό στρατηγείο, σε γενικό επιχειρησιακό επίπεδο, μια τυποποιημένη επιχειρησιακή διαδικασία για θέματα κυβερνοχώρου.

Η ΕΥΕΔ/CPCC και η CMPD:

- Θα αναπτύξουν περαιτέρω και θα εντάξουν στο σχεδιασμό στρατηγικού επιπέδου την έννοια της κυβερνοάμυνας για μη στρατιωτικές αποστολές ΚΠΑΑ.
- Θα ενισχύσουν τις ικανότητες κυβερνοάμυνας των μη στρατιωτικών αποστολών ΚΠΑΑ, αξιοποιώντας τις υφιστάμενες υποδομές και προωθώντας την τυποποίηση και την εναρμόνιση των τεχνολογιών που χρησιμοποιούνται στο πλαίσιο αποστολών και επιχειρήσεων ΚΠΑΑ, αξιοποιώντας, κατά περίπτωση, την εμπειρογνωσία της CERT-EU, του ENISA και του ΕΟΑ.
- Στο πλαίσιο της διαδικασίας ενίσχυσης της μη στρατιωτικής ΚΠΑΑ, θα διερευνήσουν περαιτέρω την πιθανή παροχή στήριξης στις χώρες υποδοχής σχετικά με την κυβερνοασφάλεια από μη στρατιωτικές αποστολές ΚΠΑΑ.

Η ΕΥΕΔ:

- Θα αναπτύξει περαιτέρω κοινές απαιτήσεις για στρατιωτικές και μη στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ.
- Θα ενισχύσει τον συντονισμό της κυβερνοάμυνας για την πραγματοποίηση στόχων που αφορούν την προστασία των δικτύων που χρησιμοποιούνται από θεσμικούς φορείς της ΕΕ που υποστηρίζουν την ΚΠΑΑ, με βάση την υπάρχουσα σχετική πείρα σε επίπεδο ΕΕ.
- Θα επανεξετάζει τακτικά τις απαιτήσεις πόρων και άλλες συναφείς αποφάσεις πολιτικής με βάση τις μεταβαλλόμενες συνθήκες όσον αφορά τυχόν απειλές, σε διαβούλευση με τις σχετικές ομάδες εργασίας του Συμβουλίου και άλλα θεσμικά όργανα της ΕΕ.

3. Προώθηση πολιτικοστρατιωτικής συνεργασίας

Ο κυβερνοχώρος είναι ένα ταχέως αναπτυσσόμενο πεδίο: οι νέες τεχνολογικές εξελίξεις θα πρέπει να υποστηρίζονται από συστήματα ασφαλείας, τόσο στο μη στρατιωτικό όσο και στο στρατιωτικό πεδίο. Στο μέτρο του δυνατού, θα πρέπει να προβλέπεται συντονισμός μεταξύ του μη στρατιωτικού και του στρατιωτικού τομέα, στις περιπτώσεις που παρόμοιες τεχνολογικές εξελίξεις προσφέρουν λύσεις για μη στρατιωτικές και στρατιωτικές εφαρμογές. Σε άλλες περιπτώσεις, οι στρατιωτικές ικανότητες και τα οπλικά συστήματα είναι τόσο συγκεκριμένα, ώστε δεν υπάρχει περιθώριο διαμερισμού με μη στρατιωτικές τεχνολογίες. Με την επιφύλαξη της εσωτερικής οργάνωσης και της νομοθεσίας των κρατών μελών, η πολιτικοστρατιωτική συνεργασία στον κυβερνοχώρο μπορεί να θεωρηθεί ενδεδειγμένη μεταξύ άλλων για την ανταλλαγή βέλτιστων πρακτικών, για την ανταλλαγή πληροφοριών και για τους μηχανισμούς έγκαιρης προειδοποίησης, για τις αξιολογήσεις κινδύνου για την αντιμετώπιση συμβάντων και για τις δράσεις ευαισθητοποίησης, καθώς και για κατάρτιση και ασκήσεις.

Η βελτίωση της κυβερνοασφάλειας για τους πολίτες είναι σημαντικός παράγοντας, ο οποίος συμβάλλει στη συνολική ανθεκτικότητα της ασφάλειας των δικτύων και των πληροφοριών. Η οδηγία NIS αυξάνει την ετοιμότητα σε εθνικό επίπεδο και ενισχύει τη συνεργασία σε επίπεδο Ένωσης μεταξύ των κρατών μελών σε στρατηγικό και σε επιχειρησιακό επίπεδο. Στη συνεργασία αυτή συμμετέχουν τόσο οι εθνικές αρχές που επιβλέπουν τις πολιτικές ασφάλειας στον κυβερνοχώρο όσο και οι εθνικές CERT και η CERT-EU. Η συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών CERT θα πρέπει να ενισχυθεί, λαμβάνοντας δεόντως υπόψη τις εξελίξεις αυτές. Η νέα ευρωπαϊκή πράξη για την κυβερνοασφάλεια στοχεύει στη βελτίωση της ανθεκτικότητας των κυβερνοεπιθέσεων και στην παροχή ενός πλαισίου πιστοποίησης της κυβερνοασφάλειας για τα προϊόντα και τις υπηρεσίες, αυξάνοντας έτσι την εμπιστοσύνη των πολιτών στο ψηφιακό περιβάλλον.

Ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ), ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) και η CERT-EU, μαζί με άλλα συναφή όργανα και οργανισμούς της ΕΕ, στο πλαίσιο των αντίστοιχων εντολών τους και χωρίς αλληλεπικάλυψη με τις αρμοδιότητες των κρατών μελών, καθώς και τα κράτη μέλη, ενθαρρύνονται να ενισχύσουν περαιτέρω τη συνεργασία τους στους ακόλουθους τομείς:

- Ανάπτυξη κοινών προφίλ αρμοδιοτήτων στους τομείς της ασφάλειας και της άμυνας στον κυβερνοχώρο, με βάση τις διεθνείς βέλτιστες πρακτικές και την πιστοποίηση που χρησιμοποιείται από τα θεσμικά όργανα, τα λοιπά όργανα και τους οργανισμούς της ΕΕ, λαμβάνοντας επίσης υπόψη τα πρότυπα πιστοποίησης του ιδιωτικού τομέα.
- Συμβολή στην περαιτέρω ανάπτυξη και προσαρμογή των οργανωτικών και τεχνικών προτύπων του δημόσιου τομέα για την κυβερνοασφάλεια και την κυβερνοάμυνα, ώστε να χρησιμοποιηθούν στον τομέα της άμυνας και της ασφάλειας. Αξιοποίηση, κατά περίπτωση, των εν εξελίξει εργασιών του ENISA και του ΕΟΑ.
- Θέσπιση ή περαιτέρω ανάπτυξη μηχανισμών εργασίας και ρυθμίσεων για την ανταλλαγή βέλτιστων πρακτικών, ιδίως στον τομέα της εκπαίδευσης, της κατάρτισης και των ασκήσεων, καθώς και στην έρευνα, την τεχνολογία, και σε άλλους τομείς που παρέχουν συνέργειες μεταξύ στρατιωτικών και μη στρατιωτικών μέσων.
- Αξιοποίηση των δυνατοτήτων πρόληψης, έρευνας και εγκληματολογικών ερευνών που υπάρχουν σε επίπεδο ΕΕ στον τομέα του ηλεκτρονικού εγκλήματος και ενισχυμένη χρήση τους στην ανάπτυξη ικανοτήτων κυβερνοάμυνας.

Τα κράτη μέλη, σε οικειοθελή βάση:

- Θα ενισχύσουν τη συνεργασία μεταξύ μη στρατιωτικών και στρατιωτικών CERT μεταξύ των κρατών μελών.

η ΕΥΕΔ, η Επιτροπή και τα κράτη μέλη:

- Θα συμπεριλάβουν στον τομέα της κυβερνοάμυνας της ΕΕ τη διαχείριση των κρίσεων και των καταστροφών (μέσω της διαδικασίας «blueprint»).

4. Έρευνα και τεχνολογία

Οι φορείς υποδομών και υπηρεσιών τεχνολογίας της πληροφορίας και των επικοινωνιών (ΤΠΕ) για μη στρατιωτικούς σκοπούς και σκοπούς άμυνας αντιμετωπίζουν αντίστοιχα προβλήματα ασφάλειας στον κυβερνοχώρο, λόγω των κοινών απαιτήσεων τεχνολογικής και επιχειρησιακής ικανότητας. Η πρόβλεψη κοινών αναγκών E&T και κοινών απαιτήσεων για τα συστήματα θα βελτιώσει μακροπρόθεσμα τη διαλειτουργικότητα των συστημάτων και θα περιορίσει τις δαπάνες ανάπτυξης λύσεων. Η επίτευξη οικονομιών κλίμακας είναι αναγκαία για την αντιμετώπιση του ολοένα αυξανόμενου αριθμού απειλών και αδυναμιών. Το ανωτέρω θα διευκολύνει στη συνέχεια τη διαφύλαξη και ανάπτυξη ενός ανταγωνιστικού κλάδου κυβερνοάμυνας στην Ευρώπη.

Η ανάπτυξη ικανοτήτων στον τομέα της κυβερνοάμυνας έχει σημαντική διάσταση E&T. Στο πλαίσιο του θεματολογίου έρευνας για την κυβερνοάμυνα (CDRA), ο ΕΟΑ έθεσε ισχυρές βάσεις για να δοθεί προτεραιότητα στη μελλοντική χρηματοδότηση της έρευνας και τεχνολογίας και την ανάπτυξη ικανοτήτων τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο. Το επακόλουθο στρατηγικό θεματολόγιο έρευνας στο πλαίσιο της σχετικής ad hoc ομάδας εργασίας του ΕΟΑ παρέχει ξεκάθαρα προτεραιότητα στις τεχνολογίες που σχετίζονται με τον κυβερνοχώρο και που είναι αναγκαίες για το στρατιωτικό τομέα, εντοπίζοντας παράλληλα ευκαιρίες για προσπάθειες και επενδύσεις διπλής χρήσης, τόσο σε εθνικό όσο και πολυεθνικό ή χρηματοδοτούμενο από την ΕΕ επίπεδο.

Η ανάπτυξη τεχνολογικών ικανοτήτων στην Ευρώπη για τον περιορισμό των απειλών και των τρωτών σημείων είναι ουσιαστικής σημασίας. Η βιομηχανία θα παραμείνει ο βασικός μοχλός της τεχνολογίας και της καινοτομίας που αφορούν την κυβερνοάμυνα. Η κρυπτογράφηση, τα ασφαλή ενσωματωμένα συστήματα, η ανίχνευση κακόβουλου λογισμικού, οι τεχνικές προσομοίωσης και απεικόνισης, η προστασία των συστημάτων δικτύων και επικοινωνίας και η τεχνολογία ταυτοποίησης και επαλήθευσης της ταυτότητας είναι μερικά από τα ζητήματα που πρέπει να αντιμετωπιστούν. Είναι επίσης σημαντικό να προωθηθεί μια ανταγωνιστική ευρωπαϊκή βιομηχανική αλυσίδα εφοδιασμού στον τομέα της κυβερνοασφάλειας με την υποστήριξη της συμμετοχής των μικρών και μεσαίων επιχειρήσεων (ΜΜΕ).

Η διασφάλιση ότι η Ευρώπη είναι σε θέση να συμβαδίσει με διεθνείς ανταγωνιστές όσον αφορά τις τεχνολογικές ικανότητες στον κυβερνοχώρο εξαρτάται, επίσης, από την ικανότητά μας να τονώσουμε την καινοτομία αιχμής, με τη χρήση εθνικών μέσων καθώς και των μέσων της ΕΕ, όπως το Ευρωπαϊκό Συμβούλιο Καινοτομίας.

Για να διευκολυνθεί η πολιτικοστρατιωτική συνεργασία για την ανάπτυξη ικανοτήτων κυβερνοάμυνας, να ενισχυθεί Ευρωπαϊκή Βιομηχανική και Τεχνολογική Βάση στον τομέα της Άμυνας (EDTIB)[10], και για να προαχθεί η στρατηγική αυτονομία της ΕΕ και στον τομέα του κυβερνοχώρου, όταν και όπου είναι αναγκαίο και σε συνεργασία με εταίρους, ει δυνατόν**,**

Ο ΕΟΑ, η Επιτροπή και τα κράτη μέλη:

- Θα αναζητήσουν συνέργειες μεταξύ των προσπαθειών Ε&Τ στον στρατιωτικό τομέα με μη στρατιωτικά προγράμματα έρευνας και ανάπτυξης, ιδίως όσα αφορούν καινοτομίες αιχμής, και θα λαμβάνουν υπ' όψιν τις πτυχές ασφάλειας και άμυνας στον κυβερνοχώρο κατά την υλοποίηση της προπαρασκευαστικής δράσης για την έρευνα στον τομέα της άμυνας (PADR).
- Θα έχουν κοινά θεματολόγια έρευνας όσον αφορά την κυβερνοασφάλεια (π.χ. το θεματολόγιο έρευνας για την κυβερνοάμυνα του Ευρωπαϊκού Οργανισμού Άμυνας) και θα ανταλλάσσουν τους σχετικούς οδικούς χάρτες και δράσεις· για τον σκοπό αυτό, θα εκπονηθεί διατομεακό θεματολόγιο έρευνας για την κυβερνοάμυνα, σε στενή συνεργασία με την Επιτροπή και τα κράτη μέλη.
- Θα συμβάλουν ώστε να βελτιωθεί η ενσωμάτωση των διαστάσεων της κυβερνοασφάλειας και της κυβερνοάμυνας στα προγράμματα που έχουν διάσταση ασφάλειας και άμυνας διπλής χρήσης, π.χ. ερευνητικό έργο διαχείρισης της εναέριας κυκλοφορίας στον ενιαίο ευρωπαϊκό ουρανό (SESAR).

[10] Ανακοίνωση με τίτλο «Μετάβαση προς ένα ανταγωνιστικότερο και αποτελεσματικότερο τομέα άμυνας και ασφάλειας», COM (2013) 542

Η Επιτροπή:

- Θα εξετάσει το ενδεχόμενο δημιουργίας ευρωπαϊκού κέντρου βιομηχανικών, τεχνολογικών και ερευνητικών ικανοτήτων στον τομέα της κυβερνοασφάλειας, με ένα δίκτυο εθνικών κέντρων συντονισμού για τη στήριξη των τεχνολογικών και βιομηχανικών ικανοτήτων στον τομέα της κυβερνοασφάλειας και την ενίσχυση της ανταγωνιστικότητας του ενωσιακού κλάδου κυβερνοασφάλειας, τη διασφάλιση της συμπληρωματικότητας και την αποφυγή επικαλύψεων τόσο εντός του δικτύου κέντρων ικανοτήτων στον τομέα της κυβερνοασφάλειας όσο και με άλλους οργανισμούς της ΕΕ. Το εν λόγω κέντρο θα πρέπει, μεταξύ άλλων, να ενισχύσει τη συνεργασία μεταξύ μη στρατιωτικών και αμυντικών τεχνολογιών και εφαρμογών, σε στενή συνεργασία και πλήρη συμπληρωματικότητα με τον Ευρωπαϊκό Οργανισμό Άμυνας στον τομέα της κυβερνοάμυνας.
- Θα υποστηρίξει την ανάπτυξη βιομηχανικών οικοσυστημάτων και καινοτομικών συσπειρώσεων που θα καλύπτουν ολόκληρη την αλυσίδα αξίας της ασφάλειας με βάση τις ακαδημαϊκές γνώσεις, την καινοτομία των ΜΜΕ και τη βιομηχανική παραγωγή.

Η Επιτροπή, σε συνεργασία με τα κράτη μέλη:

- Θα λαμβάνει υπόψη τα ζητήματα που άπτονται της κυβερνοάμυνας στις προσκλήσεις της προπαρασκευαστικής δράσης για την έρευνα στον τομέα της άμυνας (PADR).
- Θα λαμβάνει υπόψη την κυβερνοάμυνα στα θέματα που καλύπτονται από το Ευρωπαϊκό Ταμείο Άμυνας.
- Θα υποστηρίξει τη συνοχή της πολιτικής της ΕΕ για να εξασφαλιστεί ότι η διαμόρφωση πολιτικής και οι τεχνικές πτυχές της προστασίας της ΕΕ στον κυβερνοχώρο θα παραμείνουν στην πρώτη γραμμή της τεχνολογικής καινοτομίας και θα εναρμονιστούν σε ολόκληρη την ΕΕ (ικανότητα ανάλυσης και αξιολόγησης των απειλών στον κυβερνοχώρο, πρωτοβουλίες «ασφάλεια βάσει σχεδιασμού», διαχείριση εξαρτήσεων (dependency) για την πρόσβαση στην τεχνολογία κλπ.).

5. Βελτίωση των δυνατοτήτων κατάρτισης, εκπαίδευσης και ασκήσεων

Για να αυξηθεί η ετοιμότητα για την αντιμετώπιση κυβερνοαπειλών και για να καλλιεργηθεί κοινό πνεύμα κυβερνοάμυνας στο σύνολο της ΕΕ, προς όφελος ταυτόχρονα των αποστολών και των επιχειρήσεων της ΕΕ, πρέπει να βελτιωθούν και να αναβαθμιστούν οι δυνατότητες κατάρτισης στον τομέα της κυβερνοάμυνας. Είναι ουσιαστικής σημασίας να χρησιμοποιούνται αποτελεσματικά οι προϋπολογισμοί εκπαίδευσης και κατάρτισης με διατήρηση της υψηλότερης δυνατής ποιότητας. Η συνένωση και κοινή χρήση προγραμμάτων εκπαίδευσης και κατάρτισης σε θέματα κυβερνοάμυνας σε ευρωπαϊκό επίπεδο θα είναι κρίσιμης σημασίας.

Η Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας (ΕΑΑΑ), η ΕΥΕΔ, ο ΕΟΑ, η Επιτροπή και τα κράτη μέλη:

- Θα καταρτίσουν, με βάση την ανάλυση του ΕΟΑ όσον αφορά τις ανάγκες εκπαίδευσης σε θέματα κυβερνοάμυνας και την πείρα που έχει αποκτηθεί από την παροχή εκπαίδευσης σε θέματα ασφάλειας στον κυβερνοχώρο από την ESDC, προγράμματα εκπαίδευσης και κατάρτισης σε θέματα ΚΠΑΑ που θα απευθύνονται σε διάφορα ακροατήρια, συμπεριλαμβανομένων της ΕΥΕΔ, του προσωπικού των αποστολών και επιχειρήσεων ΚΠΑΑ και υπαλλήλων των κρατών μελών, λαμβάνοντας επίσης υπόψη ζητήματα διατήρησης εξειδικευμένου προσωπικού σε βραχυπρόθεσμη, μεσοπρόθεσμη και μακροπρόθεσμη βάση.
- Θα προτείνουν την καθιέρωση διαλόγου όσον αφορά θέματα κυβερνοάμυνας και συγκεκριμένα πρότυπα κατάρτισης και πιστοποίησης με τα κράτη μέλη, τα θεσμικά όργανα της ΕΕ, τρίτες χώρες και άλλους διεθνείς οργανισμούς, καθώς και με τον ιδιωτικό τομέα.
- Θα έλθουν σε επαφή με ευρωπαϊκούς φορείς παροχής κατάρτισης του ιδιωτικού τομέα καθώς και με πανεπιστημιακά ιδρύματα προκειμένου να αναβαθμίσουν τις ικανότητες και δεξιότητες του προσωπικού που συμμετέχει σε αποστολές και επιχειρήσεις ΚΠΑΑ.

Η ΕΑΑΑ:

- Θα αναπτύξει περαιτέρω την πλατφόρμα εκπαίδευσης, κατάρτισης, αξιολόγησης και ασκήσεων (ΕΚΑΑ) σχετικά με τον κυβερνοχώρο που δημιουργήθηκε στην ΕΑΑΑ.
- Θα δημιουργήσει συνέργειες με τα εκπαιδευτικά προγράμματα άλλων φορέων όπως ο ENISA, η Ευρωπόλ, η Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL) και το Κέντρο αριστείας συλλογικής κυβερνοάμυνας του ΝΑΤΟ.
- Θα διερευνήσει τη δυνατότητα κοινών εκπαιδευτικών προγραμμάτων κυβερνοάμυνας ΕΑΑΑ-ΝΑΤΟ, ανοικτών σε όλα τα κράτη μέλη της ΕΕ, προκειμένου να καλλιεργηθεί κοινό πνεύμα κυβερνοάμυνας.

Η Επιτροπή:

- Θα αξιολογήσει τις επιλογές για την αναβάθμιση των δυνατοτήτων κατάρτισης και εκπαίδευσης εντός των κρατών μελών που προσδιορίζονται από την πλατφόρμα ΕΚΑΑ.

Ο ΕΟΑ:

- Θα αναπτύξει νέα εκπαιδευτικά προγράμματα του ΕΟΑ σε συνεργασία με την ΕΑΑΑ για την κάλυψη των αναγκών των κρατών μελών για εκπαίδευση, κατάρτιση και ασκήσεις στον τομέα της κυβερνοάμυνας.
- Θα υποστηρίξει την πλατφόρμα ΕΚΑΑ μεταξύ άλλων μέσω της προοδευτικής ενοποίησης των ενοτήτων εκπαίδευσης, κατάρτισης, αξιολόγησης και ασκήσεων που αναπτύχθηκαν στο πλαίσιο του ΕΟΑ.

Η ΕΥΕΔ και τα κράτη μέλη:

- Θα ακολουθήσουν τους καθιερωμένους μηχανισμούς πιστοποίησης της ΕΑΑΑ για τα εκπαιδευτικά προγράμματα σε στενή συνεργασία με τις αρμόδιες υπηρεσίες των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, με βάση τα ισχύοντα πρότυπα και γνώσεις. Θα εξετάσουν τη δυνατότητα δημιουργίας ειδικών ενοτήτων για θέματα κυβερνοχώρου στο πλαίσιο της πρωτοβουλίας «Στρατιωτικό Erasmus».

Πρέπει να βελτιωθούν οι δυνατότητες ασκήσεων κυβερνοάμυνας για τους πολιτικοστρατιωτικούς φορείς της ΚΠΑΑ. Οι κοινές ασκήσεις είναι εργαλείο για την ανάπτυξη κοινών γνώσεων και κοινής αντίληψης για την κυβερνοάμυνα. Το ανωτέρω θα επιτρέψει τη μεγαλύτερη ετοιμότητα των εθνικών δυνάμεων να δρουν σε πολυεθνικό περιβάλλον. Η διεξαγωγή κοινών ασκήσεων κυβερνοάμυνας θα συμβάλει επίσης στη δημιουργία διαλειτουργικότητας και εμπιστοσύνης.

Η ΕΥΕΔ, ο ΕΟΑ, η CERT-EU και τα κράτη μέλη θα εστιάσουν στην προώθηση στοιχείων κυβερνοάμυνας στην ΚΠΑΑ και άλλες ασκήσεις:

- Θα ενσωματώσουν τη διάσταση της κυβερνοάμυνας στα σημερινά σενάρια για τις ασκήσεις *MILEX* και *MULTILAYER*.
- Θα διοργανώνουν τακτικά στρατηγικές/πολιτικές ασκήσεις όπως η *CYBRID 2017* σε συντονισμό με την παράλληλη και συντονισμένη άσκηση (PACE) υπό την ηγεσία της ΕΕ και τεχνικο-επιχειρησιακές ασκήσεις όπως η *DEFNET*.
- Θα αναπτύξουν, κατά περίπτωση, ειδική άσκηση κυβερνοάμυνας ΚΠΑΑ της ΕΕ και θα διερευνήσουν τις δυνατότητες συντονισμού με πανευρωπαϊκές ασκήσεις κυβερνοχώρου όπως η *CyberEurope*, που διοργανώθηκε από τον ENISA.
- Θα συνεχίσουν να συμμετέχουν σε άλλες πολυεθνικές ασκήσεις κυβερνοάμυνας, όπως η *Locked Shields*.
- Θα προσκαλούν στις ασκήσεις τους οικείους διεθνείς εταίρους, όπως το ΝΑΤΟ, σύμφωνα με το πλαίσιο πολιτικής της ΕΕ για τις ασκήσεις.
- Θα διοργανώνουν τακτικές ασκήσεις με βάση την εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο οι οποίες θα επιτρέπουν στα κράτη μέλη της ΕΕ να εξασκούνται για την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

6. Ενίσχυση της συνεργασίας με τους οικείους διεθνείς εταίρους

Στο πλαίσιο της διεθνούς συνεργασίας πρέπει να εξασφαλιστεί διάλογος με τους διεθνείς εταίρους, συγκεκριμένα το ΝΑΤΟ και άλλους διεθνείς οργανισμούς, με σκοπό τη συμβολή στην ανάπτυξη αποτελεσματικών ικανοτήτων στον τομέα της κυβερνοάμυνας. Θα πρέπει να επιδιωχθεί ενισχυμένη συμμετοχή στις διεξαγόμενες εργασίες στο πλαίσιο του Οργανισμού για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ) και των Ηνωμένων Εθνών (ΗΕ), με απώτερο σκοπό την ανάδειξη ενός στρατηγικού πλαισίου για την πρόληψη των συγκρούσεων, τη συνεργασία και τη σταθερότητα στον κυβερνοχώρο.

Υπάρχει η πολιτική βούληση στην ΕΕ για περαιτέρω συνεργασία με το ΝΑΤΟ στον τομέα της κυβερνοάμυνας για την ανάπτυξη αξιόπιστων και ανθεκτικών ικανοτήτων κυβερνοάμυνας σύμφωνα με τα προβλεπόμενα στην κοινή δήλωση που υπεγράφη από τον Πρόεδρο του Ευρωπαϊκού Συμβουλίου, τον Πρόεδρο της Ευρωπαϊκής Επιτροπής και τον Γενικό Γραμματέα του Οργανισμού Βορειοατλαντικού Συμφώνου στη Βαρσοβία στις 8 Ιουλίου 2016. Οι τακτικές διαβουλεύσεις σε επίπεδο προσωπικού, η αμοιβαία ενημέρωση καθώς και ενδεχόμενες συναντήσεις μεταξύ της πολιτικο-στρατιωτικής ομάδας και των σχετικών επιτροπών του ΝΑΤΟ θα συμβάλουν στην αποφυγή περιττών επικαλύψεων και θα εξασφαλίσουν τη συνοχή και την αλληλοσυμπλήρωση των προσπαθειών, σύμφωνα με το προαναφερόμενο πλαίσιο.

Η ΕΥΕΔ και ο ΕΟΑ, μαζί με τα κράτη μέλη, θα αναπτύξουν περαιτέρω συνεργασία σε θέματα κυβερνοάμυνας μεταξύ ΕΕ και ΝΑΤΟ, με τον δέοντα σεβασμό του θεσμικού πλαισίου και της αυτονομίας κατά τη λήψη αποφάσεων των επιμέρους οργανισμών:

- Θα επιταχύνουν τις εν εξελίξει δραστηριότητες στο πλαίσιο της εφαρμογής της κοινής δήλωσης του Προέδρου του Ευρωπαϊκού Συμβουλίου, του Προέδρου της Ευρωπαϊκής Επιτροπής και του Γενικού Γραμματέα του Οργανισμού Βορειοατλαντικού Συμφώνου.
- Θα ανταλλάσσουν βέλτιστες πρακτικές στον τομέα της διαχείρισης κρίσεων, καθώς και στον τομέα της κυβερνοάμυνας για στρατιωτικές και μη στρατιωτικές αποστολές και επιχειρήσεις.
- Θα μεριμνήσουν για τη συνοχή των αποτελεσμάτων κατά την εκπόνηση των απαιτήσεων για ικανότητες κυβερνοάμυνας όπου υπάρχουν επικαλύψεις, ιδίως όσον αφορά την μακροπρόθεσμη ανάπτυξη των ανωτέρω ικανοτήτων.
- Θα αξιοποιήσουν περαιτέρω το πλαίσιο συνεργασίας του ΕΟΑ με το Κέντρο αριστείας συλλογικής κυβερνοάμυνας του ΝΑΤΟ ως αρχική πλατφόρμα ενισχυμένης συνεργασίας σε πολυεθνικά σχέδια κυβερνοάμυνας, βάσει κατάλληλων αξιολογήσεων.

Η ΕΑΑΑ, η ΕΥΕΔ και ο ΕΟΑ:

- Θα ενισχύσουν τη συνεργασία όσον αφορά την εκπόνηση γενικών εννοιών για την εκπαίδευση και κατάρτιση σε θέματα κυβερνοάμυνας, καθώς και για ασκήσεις.
- Θα εξασφαλίσουν την αμοιβαία συμμετοχή του προσωπικού σε ασκήσεις σύμφωνα με το συμπεφωνημένο πλαίσιο.

Η CERT-ΕΕ:

- Θα αξιοποιήσει περαιτέρω την τεχνική συμφωνία μεταξύ της CERT-EU και συναφών υπηρεσιών κυβερνοάμυνας της ΕΕ, αφενός, και της NCIRC (υπηρεσία αντιμετώπισης συμβάντων ηλεκτρονικών υπολογιστών του ΝΑΤΟ), αφετέρου, με σκοπό τη βελτίωση της επίγνωσης της κατάστασης, της ανταλλαγής πληροφοριών και των μηχανισμών έγκαιρης προειδοποίησης, και θα διαβλέπει ενδεχόμενες απειλές κατά αμφότερων οργανισμών.

Όσον αφορά άλλους διεθνείς οργανισμούς και συναφείς διεθνείς εταίρους της ΕΕ, η ΕΥΕΔ και τα κράτη μέλη, θα προβούν, κατά περίπτωση, στις ακόλουθες ενέργειες:

- Θα παρακολουθούν τις στρατηγικές εξελίξεις και θα διενεργούν διαβουλεύσεις σε θέματα κυβερνοάμυνας με διεθνείς εταίρους (διεθνείς οργανισμούς και τρίτες χώρες).
- Θα διερευνήσουν τις δυνατότητες συνεργασίας επί θεμάτων κυβερνοάμυνας, μεταξύ άλλων με τρίτες χώρες που συμμετέχουν σε αποστολές και επιχειρήσεις ΚΠΑΑ.
- Θα προωθήσουν στους κόλπους των σχετικών διεθνών οργανισμών, ιδίως στον ΟΗΕ, τον ΟΑΣΕ και το Περιφερειακό Φόρουμ του ASEAN, την εφαρμογή του υπάρχοντος διεθνούς δικαίου, και ιδίως του Χάρτη των Ηνωμένων Εθνών στο σύνολό του, στον κυβερνοχώρο, την ανάπτυξη και την εφαρμογή οικουμενικών μη δεσμευτικών προτύπων υπεύθυνης συμπεριφοράς των κρατών, και περιφερειακά μέτρα οικοδόμησης εμπιστοσύνης (ΜΟΕ) μεταξύ των κρατών για την αύξηση της διαφάνειας και τη μείωση του κινδύνου παρανοήσεων στη στάση των κρατών.

Η Επιτροπή και η ΕΥΕΔ:

- Όπου αρμόζει, θα υποστηρίξουν τη δημιουργία ικανοτήτων στον κυβερνοχώρο για τους εταίρους της ΕΕ μέσω του τροποποιημένου μηχανισμού συμβολής στη σταθερότητα και την ειρήνη (IcSP).

Συνέχεια των εργασιών

Μετά τον συντονισμό από την ΕΥΕΔ της εφαρμογής του CDPF, θα πρέπει να υποβληθεί στην πολιτικο-στρατιωτική ομάδα ετήσια έκθεση προόδου, η οποία θα περιλαμβάνει τους έξι τομείς που προαναφέρθηκαν, με τη συμμετοχή των μελών της Οριζόντιας ομάδας εργασίας για θέματα κυβερνοχώρου, και στην Επιτροπή Πολιτικής και Ασφάλειας, εκ μέρους των ΕΥΕΔ/ΕΟΑ/Επιτροπής, προκειμένου να αξιολογηθεί η εφαρμογή του CDPF. Ανά εξάμηνο, θα πρέπει επίσης να γίνεται μια προφορική παρουσίαση.

Ανάλογα με την εξέλιξη της απειλής στον κυβερνοχώρο, είναι ουσιαστικής σημασίας να προσδιορίζονται νέες απαιτήσεις κυβερνοάμυνας οι οποίες εν συνεχεία θα περιλαμβάνονται στο οικείο πλαίσιο πολιτικής. Η επόμενη αναθεώρηση του CDPF θα πρέπει να υποβληθεί το αργότερο μέχρι τα μέσα του 2022, σε στενή διαβούλευση με τα κράτη μέλη.