ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

ΥΠΑΤΗ ΕΚΠΡΟΣΩΠΟΣ ΤΗΣ
ΕΝΩΣΗΣ ΓΙΑ ΘΕΜΑΤΑ
ΚΟΙΝΗΣ ΕΞΩΤΕΡΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΚΑΙ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Βρυξέλλες, 13.9.2017
JOIN(2017) 450 final

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ

Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ

1. ΕΙΣΑΓΩΓΗ

Η ασφάλεια στον κυβερνοχώρο είναι κρίσιμης σημασίας, τόσο για την ευημερία όσο και για την ασφάλειά μας. Καθώς η καθημερινή μας ζωή και οι οικονομίες μας εξαρτώνται ολοένα και περισσότερο από τις ψηφιακές τεχνολογίες, αυξάνεται αντιστοίχως και η έκθεσή μας στον σχετικό κίνδυνο. Τα περιστατικά που αφορούν την ασφάλεια στον κυβερνοχώρο παρουσιάζουν διαφοροποιήσεις τόσο από την άποψη του προσώπου που ευθύνεται για το περιστατικό όσο και ως προς τον επιδιωκόμενο σκοπό. Οι κακόβουλες δραστηριότητες στον κυβερνοχώρο δεν απειλούν μόνο τις οικονομίες και την πορεία μας προς την ψηφιακή ενιαία αγορά, αλλά και την ίδια τη λειτουργία της δημοκρατίας, τις ελευθερίες και τις αξίες μας. Η μελλοντική μας ασφάλεια εξαρτάται από την προσαρμογή της ικανότητάς μας να προστατεύουμε την ΕΕ από τις απειλές στον κυβερνοχώρο: τόσο οι μη στρατιωτικές υποδομές όσο και η στρατιωτική ικανότητα βασίζονται σε ασφαλή ψηφιακά συστήματα. Αυτό αναγνωρίστηκε στο Ευρωπαϊκό Συμβούλιο του Ιουνίου 2017[1], καθώς και στη συνολική στρατηγική για την εξωτερική πολιτική και την πολιτική ασφαλείας[2].

Οι κίνδυνοι αυξάνονται εκθετικά. Από μελέτες προκύπτει ότι οι οικονομικές επιπτώσεις του εγκλήματος στον κυβερνοχώρο πενταπλασιάστηκαν από το 2013 έως το 2017 και ενδέχεται μάλιστα να τετραπλασιαστούν έως το 2019[3]. Ιδιαίτερη αύξηση έχει διαπιστωθεί στις περιπτώσεις που αφορούν το λογισμικό ransomware[4] (λυτρισμικό), καθώς οι πρόσφατες επιθέσεις[5] αντικατοπτρίζουν τη ραγδαία αύξηση της εγκληματικής δραστηριότητας στον κυβερνοχώρο. Ωστόσο, το λυτρισμικό δεν αποτελεί σε καμία περίπτωση τη μοναδική απειλή.

Οι απειλές στον κυβερνοχώρο προέρχονται τόσο από μη κρατικούς όσο και από κρατικούς παράγοντες: συχνά πρόκειται για εγκληματικές ενέργειες, με κίνητρο το κέρδος, αλλά μπορεί επίσης να έχουν πολιτικό και στρατηγικό χαρακτήρα. Η εγκληματική απειλή εντείνεται λόγω των ασαφών ορίων μεταξύ του εγκλήματος στον κυβερνοχώρο και του «παραδοσιακού» εγκλήματος, δεδομένου ότι οι δράστες χρησιμοποιούν το διαδίκτυο τόσο ως μέσο για την επέκταση των δραστηριοτήτων τους όσο και ως πηγή για την εξεύρεση νέων μεθόδων και εργαλείων τέλεσης εγκλημάτων[6]. Ωστόσο, στη συντριπτική πλειονότητα των περιπτώσεων, οι πιθανότητες εντοπισμού των εγκληματιών είναι ελάχιστες και οι πιθανότητες δίωξης ακόμη λιγότερες.

Ταυτόχρονα, κρατικοί παράγοντες επιτυγχάνουν όλο και περισσότερο τους γεωπολιτικούς τους στόχους κάνοντας χρήση όχι μόνο παραδοσιακών εργαλείων, όπως οι στρατιωτικές δυνάμεις, αλλά και περισσότερο διακριτικών εργαλείων του κυβερνοχώρου, μεταξύ άλλων παρεμβαίνοντας σε εσωτερικές δημοκρατικές διαδικασίες. Η χρήση του κυβερνοχώρου ως πεδίου πολεμικών επιχειρήσεων, είτε αυτόνομα είτε στο πλαίσιο υβριδικής προσέγγισης, αναγνωρίζεται πλέον ευρέως. Τα φαινόμενα των εκστρατειών παραπληροφόρησης, των ψευδών ειδήσεων και των δραστηριοτήτων στον κυβερνοχώρο που έχουν ως στόχο υποδομές ζωτικής σημασίας αυξάνονται συνεχώς και πρέπει να αντιμετωπιστούν. Για τον λόγο αυτό,

---

1 http://www.consilium.europa.eu/el/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Βλέπε, για παράδειγμα: McAfee & Centre for Strategic and International Studies, «Net losses: Estimating the Global Cost of Cybercrime», 2014.

4 Το λυτρισμικό είναι είδος κακόβουλου λογισμικού το οποίο εμποδίζει ή περιορίζει την πρόσβαση των χρηστών στο σύστημά τους, κλειδώνοντας είτε την οθόνη του συστήματος είτε τα αρχεία των χρηστών έως ότου καταβληθούν λύτρα.

5 Τον Μάιο του 2017, η επίθεση του λυτρισμικού WannaCry πρόσβαλε περισσότερους από 400 000 υπολογιστές σε πάνω από 150 χώρες. Έναν μήνα αργότερα, η επίθεση του λυτρισμικού Petya έπληξε την Ουκρανία και διάφορες εταιρείες σε όλον τον κόσμο.

6 Ευρωπόλ, «Serious and Organised Crime Threat Assessment 2017» (Αξιολόγηση απειλών όσον αφορά το σοβαρό και οργανωμένο έγκλημα για το 2017).

στο έγγραφο προβληματισμού σχετικά με το μέλλον της ευρωπαϊκής άμυνας[7], η Επιτροπή υπογράμμισε τη σημασία της συνεργασίας στον τομέα της άμυνας στον κυβερνοχώρο.

Εάν δεν βελτιώσουμε σημαντικά την ασφάλειά μας στον κυβερνοχώρο, ο κίνδυνος θα αυξάνεται παράλληλα με τον ψηφιακό μετασχηματισμό. Έως το 2020 αναμένεται να διαθέτουν σύνδεση στο διαδίκτυο δεκάδες δισεκατομμύρια συσκευές του «διαδικτύου των πραγμάτων», αλλά η ασφάλεια στον κυβερνοχώρο δεν αποτελεί ακόμη προτεραιότητα κατά τον σχεδιασμό τους[8]. Η πιθανή αποτυχία όσον αφορά την προστασία των συσκευών που θα ελέγχουν τα ηλεκτρικά δίκτυα, τα αυτοκίνητα και τα δίκτυα μεταφορών, τα εργοστάσια, τις οικονομικές συναλλαγές, τα νοσοκομεία και τα σπίτια μας θα μπορούσε να έχει καταστροφικές συνέπειες και να βλάψει σε τεράστιο βαθμό την εμπιστοσύνη των καταναλωτών στις αναδυόμενες τεχνολογίες. Ο κίνδυνος επιθέσεων με πολιτικά κίνητρα σε μη στρατιωτικούς στόχους καθώς και ο κίνδυνος που συνδέεται με ελλείψεις στην στρατιωτική άμυνα στον κυβερνοχώρο, αυξάνει ακόμη περισσότερο την απειλή.

Η προσέγγιση που παρατίθεται στην παρούσα κοινή ανακοίνωση θα επιτρέψει στην ΕΕ να είναι καλύτερα προετοιμασμένη για την αντιμετώπιση των απειλών αυτών. Θα αυξήσει την ανθεκτικότητα και τη στρατηγική αυτονομία, μέσω της τόνωσης των ικανοτήτων από πλευράς τεχνολογίας και δεξιοτήτων, καθώς και μέσω της συμβολής της στην οικοδόμηση ισχυρής ενιαίας αγοράς. Για τον σκοπό αυτό απαιτούνται οι κατάλληλες δομές ώστε να δημιουργηθεί ισχυρή ασφάλεια στον κυβερνοχώρο και να εξασφαλίζεται η δυνατότητα αντίδρασης, όταν αυτή κρίνεται αναγκαία, με την πλήρη συμμετοχή όλων των βασικών παραγόντων. Η εν λόγω προσέγγιση θα συμβάλει επίσης στην καλύτερη αποτροπή των επιθέσεων στον κυβερνοχώρο, μέσω της εντατικοποίησης των εργασιών για την ανίχνευση, τον εντοπισμό και τη δίωξη των δραστών. Θα αναγνωρίσει επίσης την παγκόσμια διάσταση μέσω της ανάπτυξης διεθνούς συνεργασίας ως πλατφόρμας για την ανάληψη ηγετικού ρόλου εκ μέρους της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο. Στο πλαίσιο των ενεργειών αυτών θα αξιοποιηθούν οι προσεγγίσεις της ψηφιακής ενιαίας αγοράς, της συνολικής στρατηγικής, του ευρωπαϊκού θεματολογίου για την ασφάλεια[9], του κοινού πλαισίου για την αντιμετώπιση υβριδικών απειλών[10] και της ανακοίνωσης για τη δημιουργία του Ευρωπαϊκού Ταμείου Άμυνας[1112].

Η ΕΕ ασχολείται ήδη με πολλά από τα ζητήματα αυτά: το ζητούμενο είναι τώρα η σύγκλιση των διαφόρων αξόνων εργασίας. Το 2013 η ΕΕ παρουσίασε μια στρατηγική για την ασφάλεια στον κυβερνοχώρο δρομολογώντας μια σειρά βασικών αξόνων εργασίας για τη βελτίωση της ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο[13]. Οι κύριοι στόχοι και οι βασικές αρχές της, όσον αφορά την προώθηση ενός αξιόπιστου, ασφαλούς και ανοικτού οικοσυστήματος του κυβερνοχώρου, εξακολουθούν να ισχύουν. Ωστόσο, το διαρκώς

---

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_el.pdf.

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination [Λύσεις IDC και TXT (2014), SMART 2013/0037 – Συνδυασμός υπολογιστικού νέφους και διαδικτύου των πραγμάτων], μελέτη που εκπονήθηκε για λογαριασμό της Επιτροπής.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Η προσέγγιση αυτή στηρίζεται επίσης σε ανεξάρτητες επιστημονικές συμβουλές που παρασχέθηκαν από την ομάδα επιστημονικών συμβούλων υψηλού επιπέδου της Ευρωπαϊκής Επιτροπής (βλ. παραπομπές κατωτέρω).

13 JOIN(2013) 1 final. Αξιολόγηση της εν λόγω στρατηγικής παρουσιάζεται στο έγγραφο εργασίας των υπηρεσιών της Επιτροπής SWD (2017) 295.

εξελισσόμενο τοπίο των εντεινόμενων απειλών καθιστά αναγκαία την ανάληψη περαιτέρω δράσης για την αντιμετώπιση και την αποτροπή επιθέσεων στο μέλλον[14].

Δεδομένου του πεδίου εφαρμογής των πολιτικών της, καθώς και των εργαλείων, των δομών και των ικανοτήτων που έχει στη διάθεσή της, η ΕΕ είναι σε θέση να αντιμετωπίσει το ζήτημα της ασφάλειας στον κυβερνοχώρο. Παρότι η εθνική ασφάλεια εξακολουθεί να αποτελεί αρμοδιότητα των κρατών μελών, η κλίμακα και ο διασυνοριακός χαρακτήρας της απειλής συνιστούν ισχυρό επιχείρημα για την ανάληψη δράσης εκ μέρους της ΕΕ με σκοπό την παροχή κινήτρων και στήριξης στα κράτη μέλη για την ανάπτυξη και τη διατήρηση περισσότερων και καλύτερων εθνικών ικανοτήτων ασφάλειας στον κυβερνοχώρο, διασφαλίζοντας ταυτόχρονα την ανάπτυξη ικανοτήτων σε επίπεδο ΕΕ. Σκοπός της προσέγγισης αυτής είναι να ενισχυθούν όλοι οι παράγοντες –η ΕΕ, τα κράτη μέλη, η βιομηχανία και οι ιδιώτες– ώστε να δοθεί στην ασφάλεια στον κυβερνοχώρο η προτεραιότητα που απαιτείται για τη δημιουργία ανθεκτικότητας και την εξασφάλιση βελτιωμένης αντιμετώπισης των απειλών στον κυβερνοχώρο από την ΕΕ. Κατά τον τρόπο αυτό θα είναι δυνατή η λήψη συγκεκριμένων μέτρων που θα συμβάλλουν τόσο στον εντοπισμό και τη διερεύνηση κάθε μορφής περιστατικού στον κυβερνοχώρο που στρέφεται κατά της ΕΕ και των κρατών μελών της όσο και στην κατάλληλη αντιμετώπισή του, μεταξύ άλλων μέσω της άσκησης διώξεων κατά των δραστών. Θα μπορέσει η εξωτερική δράση της ΕΕ για την αποτελεσματική προώθηση της ασφάλειας στον κυβερνοχώρο σε παγκόσμιο επίπεδο. Το αποτέλεσμα θα είναι η στροφή της ΕΕ από μια προσέγγιση αντίδρασης σε μια προορατική προσέγγιση για την προστασία της ευημερίας, της κοινωνίας και των αξιών της Ευρώπης, καθώς και των θεμελιωδών δικαιωμάτων και ελευθεριών, μέσω της αντιμετώπισης τόσο των υφιστάμενων όσο και των μελλοντικών απειλών.

2. ΔΗΜΙΟΥΡΓΙΑ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΤΗΣ ΕΕ ΕΝΑΝΤΙ ΑΠΕΙΛΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Για τη δημιουργία ισχυρής κυβερνοανθεκτικότητας απαιτείται συλλογική και ευρεία προσέγγιση. Για τον σκοπό αυτό, απαιτούνται πιο αξιόπιστες και αποτελεσματικές δομές για την προώθηση της ασφάλειας στον κυβερνοχώρο και για την αντιμετώπιση απειλών στον κυβερνοχώρο, τόσο στα κράτη μέλη όσο και στα θεσμικά και λοιπά όργανα και οργανισμούς της ίδιας της ΕΕ. Απαιτείται επίσης η υιοθέτηση συνολικότερης προσέγγισης που θα εφαρμόζεται σε όλες τις πολιτικές για τη δημιουργία κυβερνοανθεκτικότητας και στρατηγικής αυτονομίας, με μια ισχυρή ενιαία αγορά, την επίτευξη σημαντικής προόδου όσον αφορά την τεχνολογική ικανότητα της ΕΕ και πολύ μεγαλύτερο αριθμό εμπειρογνωμόνων υψηλής εξειδίκευσης. Στο επίκεντρο της προσέγγισης αυτής βρίσκεται η ευρύτερη αναγνώριση του γεγονότος ότι η ασφάλεια στον κυβερνοχώρο αποτελεί κοινή κοινωνική πρόκληση και, ως εκ τούτου, θα πρέπει να συμμετέχουν σε αυτή πολλαπλά επίπεδα της διακυβέρνησης, της οικονομίας και της κοινωνίας.

2.1 Ενίσχυση του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών

[14] Εκτός εάν δηλώνεται διαφορετικά, οι προτάσεις στην παρούσα ανακοίνωση είναι ουδέτερες από δημοσιονομική άποψη. Κάθε πρωτοβουλία που έχει δημοσιονομικές επιπτώσεις θα ακολουθεί δεόντως τις διαδικασίες του ετήσιου προϋπολογισμού και δεν μπορεί να προδικάζει το επόμενο πολυετές δημοσιονομικό πλαίσιο για την περίοδο μετά το 2020.

Ο **Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών** (ENISA) καλείται να διαδραματίσει κεντρικό ρόλο στην ενίσχυση της ανθεκτικότητας και της αντίδρασης της ΕΕ όσον αφορά την ασφάλεια στον κυβερνοχώρο, αλλά υπόκειται σε περιορισμούς λόγω της τρέχουσας εντολής του. Ως εκ τούτου, η Επιτροπή παρουσιάζει μια φιλόδοξη πρόταση μεταρρύθμισης, η οποία συμπεριλαμβάνει **μόνιμη εντολή για τον Οργανισμό**[15]. Κατά τον τρόπο αυτό θα διασφαλιστεί ότι ο ENISA μπορεί να παρέχει στήριξη στα κράτη μέλη, στα θεσμικά όργανα της ΕΕ και στις επιχειρήσεις σε βασικούς τομείς, συμπεριλαμβανομένης της εφαρμογής της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών[16] («οδηγία ΑΔΠ») και του προτεινόμενου πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο.

Έπειτα από τη μεταρρύθμιση, ο ENISA θα διαδραματίζει ισχυρό συμβουλευτικό ρόλο στην ανάπτυξη και την εφαρμογή πολιτικής, μεταξύ άλλων όσον αφορά την προώθηση της συνεκτικότητας των τομεακών πρωτοβουλιών και της οδηγίας ΑΔΠ και τη διευκόλυνση της συγκρότησης κέντρων κοινοχρησίας και ανάλυσης πληροφοριών σε τομείς καίριας σημασίας. Ο ENISA θα θέσει ψηλότερα τον πήχη και θα ενισχύσει την ευρωπαϊκή ετοιμότητα μέσω της διοργάνωσης ετήσιων πανευρωπαϊκών ασκήσεων ασφάλειας στον κυβερνοχώρο, με τον συντονισμό της αντιμετώπισης σε διάφορα επίπεδα. Θα στηρίξει επίσης την ανάπτυξη πολιτικής της ΕΕ όσον αφορά την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας των πληροφοριών και επικοινωνιών (ΤΠΕ) και θα διαδραματίσει σημαντικό ρόλο στην εντατικοποίηση τόσο της επιχειρησιακής συνεργασίας όσο και της διαχείρισης κρίσεων σε ολόκληρη την ΕΕ. Ο οργανισμός θα λειτουργεί επίσης ως σημείο αναφοράς πληροφοριών και γνώσεων εντός της κοινότητας της ασφάλειας στον κυβερνοχώρο.

Η ταχεία και από κοινού κατανόηση των απειλών και των περιστατικών κατά τον χρόνο επέλευσής τους αποτελεί προϋπόθεση για τη λήψη απόφασης σχετικά με το αν απαιτείται η ανάληψη κοινής δράσης μετριασμού ή αντιμετώπισης του κινδύνου με τη στήριξη της ΕΕ. Για αυτού του είδους την ανταλλαγή πληροφοριών απαιτείται η συμμετοχή όλων των σχετικών παραγόντων –θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ, καθώς και κράτη μέλη– σε τεχνικό, επιχειρησιακό και στρατηγικό επίπεδο. Ο ENISA, σε συνεργασία με τους αρμόδιους φορείς σε επίπεδο κρατών μελών και ΕΕ, ιδίως με το δίκτυο των ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές[17], την ομάδα CERT-ΕΕ, την Ευρωπόλ και το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (INTCEN), θα συμβάλλει επίσης στην επίγνωση της κατάστασης σε επίπεδο ΕΕ, η οποία μπορεί να τροφοδοτεί τις πληροφορίες για απειλές και να αξιοποιείται για τη χάραξη πολιτικής στο πλαίσιο της τακτικής παρακολούθησης του τοπίου των απειλών και της αποτελεσματικής επιχειρησιακής συνεργασίας, καθώς και για την αντιμετώπιση διασυνοριακών περιστατικών μεγάλης κλίμακας.

2.2 Προς μια ενιαία αγορά στον τομέα της ασφάλειας στον κυβερνοχώρο

Η ανάπτυξη της αγοράς του τομέα της ασφάλειας στον κυβερνοχώρο στην ΕΕ –από πλευράς προϊόντων, υπηρεσιών και διαδικασιών– ανακόπτεται με διάφορους τρόπους. Βασική πτυχή αποτελεί η έλλειψη συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο, τα οποία να αναγνωρίζονται σε ολόκληρη την ΕΕ, για την ενσωμάτωση υψηλότερων προτύπων ανθεκτικότητας στα προϊόντα και για την υποστήριξη της εμπιστοσύνης στην αγορά σε

[15] COM(2017) 477.

[16] 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.

[17] Όπως προβλέπεται στο άρθρο 9 της οδηγίας ΑΔΠ.

ολόκληρη την ΕΕ. Για τον λόγο αυτό, η Επιτροπή υποβάλλει πρόταση για τη θέσπιση **πλαισίου της ΕΕ για την πιστοποίηση της ασφάλειας στον κυβερνοχώρο**[18]. Στο εν λόγω πλαίσιο θα καθορίζεται η διαδικασία για τη δημιουργία συστημάτων πιστοποίησης της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ, τα οποία θα καλύπτουν προϊόντα, υπηρεσίες και/ή συστήματα και θα προσαρμόζουν το επίπεδο διασφάλισης στην αντίστοιχη χρήση (είτε πρόκειται για υποδομές ζωτικής σημασίας είτε για συσκευές καταναλωτών)[19]. Το συγκεκριμένο πλαίσιο θα αποφέρει σαφή οφέλη στις επιχειρήσεις διότι δεν θα χρειάζεται να υποβάλλονται σε διάφορες διαδικασίες πιστοποίησης για την εκτέλεση εμπορικών συναλλαγών σε διασυνοριακό επίπεδο, περιορίζοντας με τον τρόπο αυτό το διοικητικό και οικονομικό κόστος. Η χρήση προγραμμάτων που θα αναπτυχθούν εντός του πλαισίου αυτού θα συμβάλει επίσης στην καλλιέργεια κλίματος εμπιστοσύνης εκ μέρους των καταναλωτών, με τη χρήση πιστοποιητικού συμμόρφωσης που θα ενημερώνει τους αγοραστές και τους χρήστες και θα τους παρέχει διασφαλίσεις για τα χαρακτηριστικά ασφαλείας των προϊόντων και των υπηρεσιών που αγοράζουν και χρησιμοποιούν. Κατά συνέπεια, τα υψηλά πρότυπα για την ασφάλεια στον κυβερνοχώρο θα μετατραπούν σε πηγή ανταγωνιστικού πλεονεκτήματος. Με τον τρόπο αυτόν θα αυξηθεί η ανθεκτικότητα διότι τα προϊόντα και οι υπηρεσίες ΤΠΕ θα αξιολογούνται επισήμως βάσει ενός καθορισμένου συνόλου προτύπων ασφάλειας στον κυβερνοχώρο, το οποίο θα μπορούσε να αναπτυχθεί σε στενή σύνδεση με το ευρύτερο εν εξελίξει έργο σχετικά με τα πρότυπα ΤΠΕ[20].

Τα συστήματα πιστοποίησης που θα προβλέπει το πλαίσιο θα είναι εθελοντικά και δεν θα επιβάλλουν άμεσες κανονιστικές υποχρεώσεις στους πωλητές ή τους παρόχους υπηρεσιών. Τα συστήματα δεν θα έρχονται σε αντίθεση με τυχόν ισχύουσες νομικές απαιτήσεις, όπως η νομοθεσία της ΕΕ για την προστασία των δεδομένων.

Αφού δημιουργηθεί το πλαίσιο, η Επιτροπή θα καλέσει τους σχετικούς ενδιαφερόμενους φορείς να εστιάσουν στους ακόλουθους τρεις τομείς προτεραιότητας:

- Ασφάλεια σε εφαρμογές κρίσιμης σημασίας ή υψηλού κινδύνου[21]: τα συστήματα από τα οποία εξαρτώνται οι καθημερινές μας δραστηριότητες, από τα αυτοκίνητα έως τα μηχανήματα εργοστασίων, από τα μεγαλύτερα συστήματα, όπως αεροσκάφη ή σταθμοί ηλεκτροπαραγωγής, έως τα μικρότερα συστήματα, όπως τα ιατροτεχνολογικά προϊόντα, καθίστανται ολοένα και περισσότερο ψηφιακά και διασυνδεδεμένα. Ως εκ τούτου, για τα βασικά συστατικά στοιχεία ΤΠΕ προϊόντων και συστημάτων αυτού του είδους θα απαιτούνται αυστηρές αξιολογήσεις ασφάλειας.

- Ασφάλεια στον κυβερνοχώρο σε ευρέως διαδεδομένα ψηφιακά προϊόντα, δίκτυα, συστήματα και υπηρεσίες που χρησιμοποιούνται τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα για την προστασία από επιθέσεις και για την εφαρμογή κανονιστικών απαιτήσεων[22] – όπως κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου, τείχη προστασίας και εικονικά ιδιωτικά δίκτυα· είναι καίριας σημασίας να διασφαλιστεί ότι η

[18] COM(2017) 477.

[19] Το επίπεδο διασφάλισης υποδεικνύει τον βαθμό αυστηρότητας της αξιολόγησης ασφάλειας και είναι συνήθως ανάλογο προς το επίπεδο του κινδύνου που συνδέεται με τους τομείς ή τις λειτουργίες της εκάστοτε εφαρμογής (δηλαδή απαιτείται υψηλότερο επίπεδο διασφάλισης για προϊόντα ή υπηρεσίες ΤΠΕ που χρησιμοποιούνται σε τομείς ή λειτουργίες εφαρμογής υψηλού κινδύνου).

[20] COM(2016) 176.

[21] Η εξαίρεση θα ισχύει σε περίπτωση που η υποχρεωτική ή εθελοντική πιστοποίηση διέπεται από άλλες πράξεις της Ένωσης.

[22] Για παράδειγμα, η οδηγία (ΕΕ) 2016/1148, ο κανονισμός (ΕΕ) 2016/679, η οδηγία (ΕΕ) 2015/2366 και άλλες προτάσεις νομοθετικών πράξεων, όπως ο Ευρωπαϊκός Κώδικας Ηλεκτρονικών Επικοινωνιών, επιβάλλουν στους οργανισμούς την υποχρέωση θέσπισης κατάλληλων μέτρων ασφάλειας για την αντιμετώπιση των σχετικών κινδύνων που αφορούν την ασφάλεια στον κυβερνοχώρο.

διαδεδομένη χρήση των εργαλείων αυτών δεν θα έχει ως συνέπεια τη δημιουργία νέων πηγών κινδύνων ή νέων τρωτών σημείων.

- Χρήση μεθόδων «ασφάλειας εκ σχεδιασμού» σε χαμηλού κόστους, ψηφιακές και διασυνδεδεμένες συσκευές μαζικής κατανάλωσης που συναποτελούν το διαδίκτυο των πραγμάτων: θα μπορούσαν να χρησιμοποιούνται προγράμματα εντός του πλαισίου προκειμένου να επισημαίνεται ότι τα προϊόντα κατασκευάζονται με τη χρήση προηγμένων μεθόδων ασφαλούς ανάπτυξης, ότι έχουν υποβληθεί σε κατάλληλες δοκιμές ασφαλείας και ότι οι πωλητές δεσμεύονται για την ενημέρωση του λογισμικού τους σε περίπτωση εμφάνισης νέων τρωτών σημείων ή απειλών.

Στις ανωτέρω προτεραιότητες θα πρέπει να λαμβάνεται ιδιαιτέρως υπόψη το εξελισσόμενο τοπίο όσον αφορά τις απειλές για την ασφάλεια στον κυβερνοχώρο, καθώς και η σημασία βασικών υπηρεσιών, όπως οι μεταφορές, η ενέργεια, η ιατροφαρμακευτική περίθαλψη, οι τράπεζες, οι υποδομές των χρηματοπιστωτικών αγορών, το πόσιμο νερό ή η ψηφιακή υποδομή[23].

Παρότι δεν είναι δυνατή η παροχή εγγύησης πλήρους ασφάλειας για κανένα προϊόν, σύστημα ή υπηρεσία ΤΠΕ, υπάρχουν διάφορα ευρέως γνωστά και άρτια τεκμηριωμένα ελαττώματα στον σχεδιασμό των προϊόντων ΤΠΕ που τα καθιστούν ευάλωτα σε επιθέσεις. Η υιοθέτηση μιας προσέγγισης «ασφάλειας εκ σχεδιασμού» από τους παραγωγούς συνδεδεμένων συσκευών, λογισμικού και εξοπλισμού ΤΠ θα μπορούσε να διασφαλίσει ότι το ζήτημα της ασφάλειας στον κυβερνοχώρο λαμβάνεται υπόψη πριν από τη διάθεση νέων προϊόντων στην αγορά. Η εν λόγω προσέγγιση θα μπορούσε να ενταχθεί στο πλαίσιο της αρχής του «καθήκοντος επιμέλειας», η οποία θα πρέπει να αναπτυχθεί περαιτέρω σε συνεργασία με τη βιομηχανία και θα μπορούσε να μειώσει τα τρωτά σημεία προϊόντων/λογισμικού με την εφαρμογή διαφόρων μεθόδων από τον σχεδιασμό έως τη δοκιμή και την επαλήθευση, συμπεριλαμβανομένης της επίσημης επαλήθευσης κατά περίπτωση, τη μακροχρόνια συντήρηση και τη χρήση ασφαλών διαδικασιών κύκλου ζωής ανάπτυξης, καθώς και με την ανάπτυξη επικαιροποιήσεων και διορθώσεων σφαλμάτων (patches) για την αντιμετώπιση τρωτών σημείων που δεν είχαν ανακαλυφθεί προηγουμένως και με την ταχεία επικαιροποίηση και επιδιόρθωση[24]. Με τον τρόπο αυτό θα αυξηθεί επίσης η εμπιστοσύνη των καταναλωτών στα ψηφιακά προϊόντα.

Επιπλέον, πρέπει να αναγνωριστεί ο σημαντικός ρόλος που διαδραματίζουν οι ερευνητές ασφάλειας τρίτων μερών στον εντοπισμό τρωτών σημείων σε προϊόντα και υπηρεσίες που υπάρχουν ήδη, ενώ θα πρέπει επίσης να δημιουργηθούν οι προϋποθέσεις που θα διευκολύνουν τη συντονισμένη δημοσιοποίηση τρωτών σημείων[25] σε όλα τα κράτη μέλη, με την αξιοποίηση βέλτιστων πρακτικών[26] και σχετικών προτύπων[27].

---

[23] Οι τομείς που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (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.

[24] Cybersecurity in the European Digital Single Market (Ασφάλεια στον κυβερνοχώρο στην ευρωπαϊκή ψηφιακή ενιαία αγορά), Ομάδα επιστημονικών συμβούλων υψηλού επιπέδου, Μάρτιος 2017

[25] Η συντονισμένη δημοσιοποίηση τρωτών σημείων αποτελεί μια μορφή συνεργασίας που διευκολύνει τους ερευνητές ασφάλειας και τους παρέχει τη δυνατότητα να αναφέρουν τρωτά σημεία στον ιδιοκτήτη ή τον πωλητή του συστήματος πληροφοριών, παρέχοντας στον οργανισμό την ευκαιρία να διαγνώσει και να διορθώσει το τρωτό σημείο με ορθό και έγκαιρο τρόπο προτού γνωστοποιηθούν σε τρίτα μέρη ή στο κοινό λεπτομερή στοιχεία σχετικά με το εν λόγω τρωτό σημείο.

[26] Για παράδειγμα: «Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations» (Οδηγός ορθών πρακτικών σχετικά με τη δημοσιοποίηση τρωτών σημείων. Από τις προκλήσεις στη διατύπωση συστάσεων), ENISA, 2016.

Ταυτόχρονα, **ειδικοί τομείς** βρίσκονται αντιμέτωποι με συγκεκριμένα ζητήματα και θα πρέπει να ενθαρρυνθούν να αναπτύξουν τη δική τους προσέγγιση. Με τον τρόπο αυτό, οι γενικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο θα συμπληρωθούν από ειδικές ανά τομέα στρατηγικές για την ασφάλεια στον κυβερνοχώρο σε τομείς όπως οι χρηματοπιστωτικές υπηρεσίες[28], η ενέργεια, οι μεταφορές και η υγεία[29].

Η Επιτροπή έχει ήδη επισημάνει τα ειδικά ζητήματα ως προς την **ευθύνη** που προκύπτουν λόγω των νέων ψηφιακών τεχνολογιών[30] και οι εργασίες για την ανάλυση των επιπτώσεων βρίσκονται σε εξέλιξη. Τα επόμενα βήματα θα ολοκληρωθούν έως τον Ιούνιο του 2018. Η ασφάλεια στον κυβερνοχώρο εγείρει ζητήματα σχετικά με τον καταλογισμό ζημίας για τις επιχειρήσεις και τις αλυσίδες εφοδιασμού, ενώ η μη αντιμετώπιση των ζητημάτων αυτών δεν θα επιτρέψει την ανάπτυξη ισχυρής ενιαίας αγοράς προϊόντων και υπηρεσιών στον τομέα της ασφάλειας στον κυβερνοχώρο.

Τέλος, η ανάπτυξη της ενιαίας αγοράς της ΕΕ εξαρτάται επίσης από την ενσωμάτωση της ασφάλειας στον κυβερνοχώρο στην πολιτική για το εμπόριο και τις επενδύσεις. Η επίδραση ξένων εξαγορών στις τεχνολογίες κρίσιμης σημασίας –χαρακτηριστικό παράδειγμα της οποίας αποτελεί η ασφάλεια στον κυβερνοχώρο– συνιστά βασική πτυχή του πλαισίου για **τον έλεγχο των ξένων άμεσων επενδύσεων στην Ευρωπαϊκή Ένωση**[31], το οποίο αποσκοπεί στη διευκόλυνση του ελέγχου των επενδύσεων από τρίτες χώρες για λόγους ασφάλειας και δημόσιας τάξης. Κατά τον ίδιο τρόπο, οι απαιτήσεις ασφάλειας του κυβερνοχώρου έχουν ήδη δημιουργήσει εμπορικούς φραγμούς για τα προϊόντα και τις υπηρεσίες της ΕΕ σε σημαντικούς τομείς διαφόρων οικονομιών τρίτων χωρών. Το πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο της ΕΕ θα ενισχύσει περαιτέρω τη διεθνή θέση της Ευρώπης και θα πρέπει να συμπληρώνεται με διαρκείς προσπάθειες για την ανάπτυξη παγκόσμιων προτύπων υψηλής ασφάλειας και για τη σύναψη συμφωνιών αμοιβαίας αναγνώρισης.

2.3 Πλήρης εφαρμογή της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών

Δεδομένου ότι τα κυριότερα εργαλεία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο βρίσκονται επί του παρόντος στα χέρια των εθνικών κυβερνήσεων, η ΕΕ έχει αναγνωρίσει την ανάγκη θέσπισης υψηλότερων προτύπων. Δεδομένου του όλο και πιο παγκοσμιοποιημένου, ψηφιακά εξαρτώμενου και διασυνδεδεμένου χαρακτήρα βασικών τομέων, όπως η τραπεζική, η ενέργεια ή οι μεταφορές, τα περιστατικά μεγάλης κλίμακας που συνδέονται με την ασφάλεια στον κυβερνοχώρο σπανίως πλήττουν ένα μόνο κράτος μέλος.

Η οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών («οδηγία ΑΔΠ») είναι η πρώτη νομοθετική πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο[32]. Σκοπός της είναι η δημιουργία ανθεκτικότητας μέσω της βελτίωσης των εθνικών ικανοτήτων ασφάλειας στον κυβερνοχώρο, της προώθησης καλύτερης συνεργασίας μεταξύ των κρατών μελών και

---

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure (Τεχνολογία των πληροφοριών -- Τεχνικές ασφάλειας -- Δημοσιοποίηση τρωτών σημείων).

[28] Οι επικείμενες εργασίες της Επιτροπής σχετικά με τη χρηματοοικονομική τεχνολογία θα καλύπτουν την ασφάλεια στον κυβερνοχώρο για τον χρηματοπιστωτικό τομέα.

[29] Στον τομέα της ενέργειας, για παράδειγμα, ο συνδυασμός παλαιότατων τεχνολογιών πληροφοριών και τεχνολογιών αιχμής, ιδίως με τις απαιτήσεις σε πραγματικό χρόνο του ηλεκτρικού δικτύου.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] 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.

της επιβολής της υποχρέωσης στις επιχειρήσεις που δραστηριοποιούνται σε σημαντικούς οικονομικούς τομείς να εφαρμόζουν αποτελεσματικές πρακτικές διαχείρισης κινδύνου και να κοινοποιούν σοβαρά περιστατικά στις εθνικές αρχές. Οι υποχρεώσεις αυτές ισχύουν επίσης για τρεις τύπους παρόχων βασικών υπηρεσιών διαδικτύου: υπολογιστικό νέφος, μηχανές αναζήτησης και διαδικτυακές αγορές. Η οδηγία έχει ως στόχο την υιοθέτηση ισχυρότερης και συστηματικότερης προσέγγισης, καθώς και τη βελτίωση της ροής πληροφοριών.

Η πλήρης εφαρμογή της οδηγίας από όλα τα κράτη μέλη έως τον Μάιο του 2018 είναι κεφαλαιώδους σημασίας για την κυβερνοανθεκτικότητα της ΕΕ. Η εν λόγω διαδικασία υποστηρίζεται από συλλογικές προσπάθειες των κρατών μελών οι οποίες θα οδηγήσουν, έως το φθινόπωρο του 2017, στην κατάρτιση κατευθυντήριων γραμμών για την υποστήριξη περισσότερο εναρμονισμένης εφαρμογής, ιδίως σε σχέση με τους φορείς παροχής βασικών υπηρεσιών. Στο πλαίσιο της παρούσας δέσμης μέτρων για την ασφάλεια στον κυβερνοχώρο, η Επιτροπή εκδίδει επίσης ανακοίνωση[33] με σκοπό τη στήριξη των προσπαθειών των κρατών μελών μέσω της παροχής, αφενός, βέλτιστων πρακτικών από τα κράτη μέλη όσον αφορά την εφαρμογή της οδηγίας και, αφετέρου, καθοδήγησης σχετικά με τον τρόπο λειτουργίας της οδηγίας στην πράξη.

Ένας τομέας στον οποίο θα είναι αναγκαία η συμπλήρωση της οδηγίας είναι η ροή πληροφοριών. Για παράδειγμα, η οδηγία καλύπτει μόνο βασικούς στρατηγικούς τομείς, ωστόσο θα είναι λογικά αναγκαία η υιοθέτηση παρόμοιας προσέγγισης από όλους τους ενδιαφερόμενους φορείς που δέχονται επιθέσεις στον κυβερνοχώρο, ούτως ώστε να διασφαλίζεται η συστηματική αξιολόγηση των τρωτών σημείων και των σημείων εισόδου των δραστών επιθέσεων στον κυβερνοχώρο. Επιπλέον, διαπιστώνεται πληθώρα προβλημάτων τα οποία εγείρουν φραγμούς στη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ του δημόσιου και του ιδιωτικού τομέα. Οι κυβερνήσεις και οι δημόσιες αρχές διστάζουν να προβούν σε ανταλλαγή πληροφοριών σχετικά με την ασφάλεια στον κυβερνοχώρο, φοβούμενες το ενδεχόμενο υποβάθμισης του οικείου επιπέδου εθνικής ασφάλειας ή ανταγωνιστικότητας. Οι ιδιωτικές επιχειρήσεις είναι επιφυλακτικές ως προς την ανταλλαγή πληροφοριών σχετικά με τα τρωτά σημεία τους και τις συνεπακόλουθες απώλειες, φοβούμενες το ενδεχόμενο διακύβευσης της εμπιστευτικότητας ευαίσθητων επιχειρηματικών πληροφοριών, υποβάθμισης της φήμης τους ή παραβίασης των κανόνων για την προστασία των δεδομένων[34]. Πρέπει να ενισχυθεί η εμπιστοσύνη στις συμπράξεις δημόσιου και ιδιωτικού τομέα, ούτως ώστε να υποστηριχθεί η ευρύτερη συνεργασία και ανταλλαγή πληροφοριών μεταξύ περισσότερων τομέων. Ο ρόλος των κέντρων κοινοχρησίας και ανάλυσης πληροφοριών είναι ιδιαίτερα σημαντικός για τη δημιουργία του αναγκαίου κλίματος εμπιστοσύνης κατά την ανταλλαγή πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα. Έχουν ληφθεί ορισμένα πρώτα μέτρα σχετικά με ειδικούς τομείς κρίσιμης σημασίας, όπως οι αεροπορικές μεταφορές, μέσω της δημιουργίας του Ευρωπαϊκού Κέντρου για την Ασφάλεια στον Κυβερνοχώρο στον Τομέα των Αερομεταφορών[35], και η ενέργεια, με την ανάπτυξη των κέντρων κοινοχρησίας και ανάλυσης πληροφοριών[36]. Η Επιτροπή θα

---

[33] COM(2017) 476.

[34] Cybersecurity in the European Digital Single Market, Ομάδα επιστημονικών συμβούλων υψηλού επιπέδου, Μάρτιος 2017. Ένα ειδικό ζήτημα αφορά τα εμπορικά μυστικά, για τα οποία στην ανακοίνωση του Ιουλίου 2016 με τίτλο «Ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης» επισημαίνονται οι επιφυλάξεις ως προς τη γνωστοποίηση της κλοπής εμπορικών μυστικών στον κυβερνοχώρο, καθώς και η σημασία των αξιόπιστων διαύλων γνωστοποίησης πληροφοριών που διασφαλίζουν την εμπιστευτικότητα.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Πρόκειται για μη κερδοσκοπικές οργανώσεις που τελούν υπό τη διαχείριση των μελών τους και συγκροτούνται από οντότητες του δημόσιου και του ιδιωτικού τομέα με σκοπό την ανταλλαγή πληροφοριών σχετικά με τις απειλές, τους κινδύνους, την πρόληψη, τον μετριασμό και την αντιμετώπιση των κινδύνων

συμβάλει τα μέγιστα στην προσέγγιση αυτή παρέχοντας στήριξη μέσω του ENISA, δεδομένης της ανάγκης ταχύτερης ανάληψης δράσης, ιδίως σε τομείς παροχής βασικών υπηρεσιών, όπως προσδιορίζονται στην οδηγία ΑΔΠ.

2.4 Ανθεκτικότητα μέσω της ταχείας αντιμετώπισης καταστάσεων έκτακτης ανάγκης

Όταν σημειώνεται επίθεση στον κυβερνοχώρο, η άμεση και αποτελεσματική αντιμετώπισή της μπορεί να μετριάσει τις επιπτώσεις της. Το γεγονός αυτό μπορεί επίσης να καταδείξει ότι οι δημόσιες αρχές δεν είναι ανίσχυρες έναντι των επιθέσεων στον κυβερνοχώρο και να συμβάλει στη δημιουργία κλίματος εμπιστοσύνης. Όσον αφορά την αντίδραση των θεσμικών οργάνων της ΕΕ, οι πτυχές που αφορούν τον κυβερνοχώρο θα πρέπει αρχικά να ενσωματωθούν σε υφιστάμενους μηχανισμούς διαχείρισης κρίσεων της ΕΕ: στις ολοκληρωμένες ρυθμίσεις της ΕΕ για την αντιμετώπιση πολιτικών κρίσεων, υπό τον συντονισμό της Προεδρίας του Συμβουλίου[37], και στα γενικά συστήματα έγκαιρης προειδοποίησης της ΕΕ[38]. Η ανάγκη αντιμετώπισης ενός ιδιαιτέρως σοβαρού περιστατικού ή μιας πολύ σοβαρής επίθεσης στον κυβερνοχώρο μπορεί να αποτελέσει επαρκή λόγο για την επίκληση της ρήτρας αλληλεγγύης της ΕΕ από κάποιο κράτος μέλος[39].

Η ταχεία και αποτελεσματική αντιμετώπιση βασίζεται επίσης στην ύπαρξη μηχανισμού άμεσης ανταλλαγής πληροφοριών μεταξύ όλων των βασικών παραγόντων σε εθνικό και ενωσιακό επίπεδο, ο οποίος προϋποθέτει με τη σειρά του σαφήνεια ως προς τους αντίστοιχους ρόλους και τις σχετικές αρμοδιότητες. Η Επιτροπή έχει προβεί σε διαβούλευση με τα θεσμικά όργανα και τα κράτη μέλη σχετικά με την κατάρτιση προσχεδίου για την παροχή μιας αποτελεσματικής διαδικασίας στο πλαίσιο της επιχειρησιακής αντιμετώπισης περιστατικών μεγάλης κλίμακας στον κυβερνοχώρο, τόσο σε ενωσιακό επίπεδο όσο και σε επίπεδο κρατών μελών. Στο **προσχέδιο** που παρουσιάζεται σε σύσταση στο πλαίσιο της παρούσας δέσμης μέτρων[40], αφενός εξηγείται πώς η ασφάλεια στον κυβερνοχώρο μπορεί να ενσωματωθεί σε μόνιμη βάση στους υφιστάμενους μηχανισμούς διαχείρισης κρίσεων σε επίπεδο ΕΕ και, αφετέρου, προσδιορίζονται οι στόχοι και οι μορφές συνεργασίας μεταξύ των κρατών μελών, καθώς και μεταξύ των κρατών μελών και των αρμόδιων θεσμικών και λοιπών οργάνων, οργανισμών και υπηρεσιών της ΕΕ[41], κατά την αντιμετώπιση μεγάλης κλίμακας περιστατικών και κρίσεων ασφάλειας στον κυβερνοχώρο. Η σύσταση καλεί επίσης τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ να θεσπίσουν ένα πλαίσιο της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο, ώστε το προσχέδιο να οδηγήσει στη λήψη συγκεκριμένων μέτρων. Το προσχέδιο θα τίθεται τακτικά σε δοκιμασία στο πλαίσιο ασκήσεων διαχείρισης κρίσεων στον κυβερνοχώρο και σε άλλους τομείς[42] και θα επικαιροποιείται όταν κρίνεται αναγκαίο.

στον κυβερνοχώρο. Βλέπε, π.χ., τα ευρωπαϊκά κέντρα κοινοχρησίας και ανάλυσης πληροφοριών στον τομέα της ενέργειας (http://www.ee-isac.eu).

37 Κατά τον τρόπο αυτό διευκολύνεται ο συντονισμός των δράσεων αντιμετώπισης σημαντικών διατομεακών κρίσεων στο υψηλότερο πολιτικό επίπεδο.

38 Κατά τον τρόπο αυτό διευκολύνεται η εσωτερική ανταλλαγή πληροφοριών και ο συντονισμός σε αναδυόμενες πολυτομεακές κρίσεις ή σε προβλέψιμες ή επικείμενες απειλές για τις οποίες απαιτείται η ανάληψη δράσης σε επίπεδο ΕΕ.

39 Δυνάμει του άρθρου 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης.

40 C(2017) 6100.

41 Συμπεριλαμβανομένης της Ευρωπόλ, του ENISA, της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική της ΕΕ για τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ (CERT-EE) και του Κέντρου Ανάλυσης Πληροφοριών της ΕΕ (INTCEN).

42 Για παράδειγμα, οι ασκήσεις που πραγματοποιεί ο ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Δεδομένου ότι τα περιστατικά ασφάλειας στον κυβερνοχώρο ενδέχεται να έχουν σημαντικές επιπτώσεις στη λειτουργία των οικονομιών και στην καθημερινή ζωή των ανθρώπων, μια επιλογή θα ήταν η διερεύνηση της δυνατότητας σύστασης **Ταμείου Αντιμετώπισης Έκτακτων Απειλών Κυβερνοασφάλειας**, κατά το παράδειγμα παρόμοιων μηχανισμών αντιμετώπισης κρίσεων σε άλλους τομείς πολιτικής της ΕΕ. Με τον τρόπο αυτό, τα κράτη μέλη θα μπορούν να ζητούν βοήθεια σε επίπεδο ΕΕ σε περίπτωση σημαντικού περιστατικού ή μετά από αυτό, υπό την προϋπόθεση ότι το ενδιαφερόμενο κράτος μέλος διέθετε ενδεδειγμένο σύστημα για την ασφάλεια στον κυβερνοχώρο πριν από το περιστατικό, συμπεριλαμβανομένης της πλήρους εφαρμογής της οδηγίας ΑΔΠ, και ώριμα πλαίσια διαχείρισης κινδύνου και εποπτείας σε εθνικό επίπεδο. Το εν λόγω Ταμείο, το οποίο θα συμπληρώνει υφιστάμενους μηχανισμούς διαχείρισης κρίσεων σε επίπεδο ΕΕ, θα μπορούσε να αναπτύξει ικανότητα άμεσης απόκρισης στο πλαίσιο της αλληλεγγύης και να χρηματοδοτεί ειδικές δράσεις αντιμετώπισης καταστάσεων έκτακτης ανάγκης, όπως η αντικατάσταση εξοπλισμού του οποίου διακυβεύεται η ασφάλεια ή η ανάπτυξη εργαλείων μετριασμού ή αντιμετώπισης του κινδύνου, αξιοποιώντας την εθνική εμπειρογνωσία κατά τρόπο ανάλογο με τον μηχανισμό πολιτικής προστασίας της ΕΕ.

2.5 Δίκτυο ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο με τη δημιουργία Ευρωπαϊκού Κέντρου Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο

Τα τεχνολογικά εργαλεία της ασφάλειας στον κυβερνοχώρο συνιστούν στρατηγικούς πόρους, ενώ αποτελούν ταυτόχρονα βασικές τεχνολογίες ανάπτυξης για το μέλλον. Η διατήρηση και η ανάπτυξη εκ μέρους της ΕΕ των αναγκαίων ικανοτήτων για τη διασφάλιση της ψηφιακής της οικονομίας, της κοινωνίας και της δημοκρατίας της, καθώς και για την προστασία υλισμικού και λογισμικού κρίσιμης σημασίας και την παροχή βασικών υπηρεσιών ασφάλειας στον κυβερνοχώρο, είναι προς το στρατηγικό συμφέρον της Ένωσης.

Η σύμπραξη δημόσιου και ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο[43], η οποία δημιουργήθηκε το 2016, αποτέλεσε ένα σημαντικό πρώτο μέτρο, με την κινητοποίηση επενδύσεων ύψους έως 1,8 δισ. EUR μέχρι το 2020. Ωστόσο, η κλίμακα των υπό εξέλιξη επενδύσεων σε άλλες περιοχές του πλανήτη[44] υποδηλώνει ότι η ΕΕ πρέπει να καταβάλει περισσότερες προσπάθειες από πλευράς επενδύσεων και να επιλύσει το πρόβλημα του κατακερματισμού των ικανοτήτων που είναι διάσπαρτες σε ολόκληρη την ΕΕ.

Η ΕΕ έχει να προσφέρει προστιθέμενη αξία, δεδομένης της εξέλιξης της τεχνολογίας για την ασφάλεια στον κυβερνοχώρο, των σημαντικών επενδύσεων που απαιτούνται και της ανάγκης εξεύρεσης λύσεων που θα μπορέσουν να εφαρμοστούν σε ολόκληρη την ΕΕ. Αξιοποιώντας το έργο των κρατών μελών και της σύμπραξης δημόσιου και ιδιωτικού τομέα, ένα επιπλέον βήμα θα είναι η ενίσχυση ικανοτήτων ασφάλειας στον κυβερνοχώρο της ΕΕ μέσω ενός δικτύου **κέντρων ικανοτήτων ασφάλειας στον κυβερνοχώρο**[45], στον πυρήνα του οποίου θα βρίσκεται το **Ευρωπαϊκό Κέντρο Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο**. Το εν λόγω δίκτυο και το Κέντρο του θα τονώσουν την ανάπτυξη και την αξιοποίηση της τεχνολογίας στον τομέα της ασφάλειας στον κυβερνοχώρο και θα

[43] C(2016) 4400 final.

[44] Οι ΗΠΑ θα επενδύσουν 19 δισ. δολάρια στον τομέα της ασφάλειας στον κυβερνοχώρο μόνο το 2017, αυξάνοντας τα σχετικά κονδύλια κατά 35 % σε σύγκριση με το 2016. Λευκός Οίκος, Γραφείο του Εκπροσώπου Τύπου: «Fact Sheet: Cybersecurity National Action Plan» (Ενημερωτικό δελτίο: Εθνικό σχέδιο δράσης για την ασφάλεια στον κυβερνοχώρο), 9 Φεβρουαρίου 2016.

[45] Το δίκτυο θα περιλαμβάνει υφιστάμενα και μελλοντικά κέντρα ασφάλειας στον κυβερνοχώρο που θα έχουν συγκροτηθεί στα κράτη μέλη, ενώ τα μέλη του θα είναι κατά κύριο λόγο δημόσιοι ερευνητικοί οργανισμοί και εργαστήρια.

συμπληρώνουν τις προσπάθειες ανάπτυξης ικανοτήτων στον τομέα αυτό τόσο σε επίπεδο ΕΕ όσο και σε εθνικό επίπεδο. Η Επιτροπή θα δρομολογήσει αξιολόγηση επιπτώσεων για να εξετάσει τις διαθέσιμες εναλλακτικές επιλογές –συμπεριλαμβανομένης της δυνατότητας σύστασης κοινής επιχείρησης– με στόχο να συγκροτήσει την εν λόγω δομή το 2018.

Ως πρώτο βήμα, και ως συμβολή στον μελλοντικό προβληματισμό, η Επιτροπή θα προτείνει τη δρομολόγηση μιας πιλοτικής φάσης στο πλαίσιο του προγράμματος «Ορίζοντας 2020» με σκοπό τη διασύνδεση των εθνικών κέντρων σε ένα δίκτυο ώστε να δοθεί μια νέα ώθηση στην ανάπτυξη ικανοτήτων και τεχνολογίας στον τομέα της ασφάλειας στον κυβερνοχώρο. Προς τον σκοπό αυτό, η Επιτροπή σχεδιάζει να προτείνει τη χορήγηση βραχυπρόθεσμης χρηματοδότησης ύψους 50 εκατ. EUR. Η δραστηριότητα αυτή θα συμπληρώσει την υπό εξέλιξη υλοποίηση της σύμπραξης δημόσιου και ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο.

Η συγκέντρωση και η διαμόρφωση των ερευνητικών προσπαθειών θα τεθούν στο επίκεντρο του δικτύου και θα αποτελούν πρωταρχικό σημείο εστίασης του Κέντρου. Για τη στήριξη της ανάπτυξης βιομηχανικών ικανοτήτων, το Κέντρο θα μπορούσε να λειτουργήσει ως διαχειριστής έργων ικανοτήτων που θα είναι σε θέση να χειρίζεται πολυεθνικά έργα. Κατά τον τρόπο αυτό, θα δοθεί περαιτέρω ώθηση στην καινοτομία και την ανταγωνιστικότητα της βιομηχανίας της ΕΕ στην παγκόσμια σκηνή όσον αφορά την ανάπτυξη ψηφιακών τεχνολογιών νέας γενιάς, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, της κβαντικής υπολογιστικής, της αλυσίδας μπλοκ (blockchain) και των ασφαλών ψηφιακών ταυτοτήτων, καθώς και στη διασφάλιση της πρόσβασης εταιρειών με έδρα στην ΕΕ σε μαζικά δεδομένα, στοιχεία που στο σύνολό τους είναι καίριας σημασίας για την ασφάλεια στον κυβερνοχώρο στο μέλλον. Το Κέντρο θα αξιοποιήσει επίσης το έργο της ΕΕ για την αύξηση των υποδομών πληροφορικής υψηλών επιδόσεων: τούτο είναι αναγκαίο για την ανάλυση μεγάλων όγκων δεδομένων, την ταχεία κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, τον έλεγχο ταυτοτήτων, την προσομοίωση επιθέσεων στον κυβερνοχώρο και την ανάλυση οπτικοακουστικού υλικού[46].

Το δίκτυο των κέντρων ικανοτήτων θα μπορούσε επίσης να διαθέτει δυνατότητες υποστήριξης της βιομηχανίας μέσω της διενέργειας δοκιμών και προσομοιώσεων για την υποστήριξη της πιστοποίησης της ασφάλειας στον κυβερνοχώρο όπως περιγράφεται στην ενότητα 2.2. Η συμμετοχή του στο πλήρες φάσμα των δραστηριοτήτων της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο θα διασφαλίσει τη συνεχή επικαιροποίηση των στόχων του ανάλογα με τις ανάγκες. Το Κέντρο θα έχει ως στόχο την προώθηση της δημιουργίας υψηλών προτύπων ασφάλειας στον κυβερνοχώρο, όχι μόνο για τα συστήματα τεχνολογίας και ασφάλειας στον κυβερνοχώρο, αλλά και για την ανάπτυξη δεξιοτήτων υψηλής ποιότητας για τους επαγγελματίες, μέσω της παροχής λύσεων και υποδειγμάτων για τις εθνικές προσπάθειες ανάπτυξης ψηφιακών δεξιοτήτων. Στο μέτρο αυτό, θα ενισχύσει επίσης τις ικανότητες ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ και θα αξιοποιήσει συνέργειες, ιδίως με τον ENISA, την CERT-ΕΕ, την Ευρωπόλ, το πιθανό μελλοντικό Ταμείο Αντιμετώπισης Έκτακτων Απειλών Κυβερνοασφάλειας και τις εθνικές CSIRT.

Στο πλαίσιο των εργασιών του δικτύου ικανοτήτων θα πρέπει να δοθεί ιδιαίτερη έμφαση στην έλλειψη ευρωπαϊκής ικανότητας στον τομέα της αξιολόγησης της **κρυπτογράφησης** των προϊόντων και των υπηρεσιών που χρησιμοποιούνται από πολίτες, επιχειρήσεις και κυβερνήσεις εντός της ψηφιακής ενιαίας αγοράς. Η ισχυρή κρυπτογράφηση αποτελεί τη βάση για τα ασφαλή συστήματα ψηφιακής ταυτοποίησης που διαδραματίζουν καίριο ρόλο στην

[46] COM(2012) 45 final και COM(2016) 178 final.

αποτελεσματική ασφάλεια στον κυβερνοχώρο[47]· επιπλέον, διατηρεί τη διανοητική ιδιοκτησία ασφαλή και επιτρέπει την προστασία θεμελιωδών δικαιωμάτων, όπως η ελευθερία έκφρασης και η προστασία των δεδομένων προσωπικού χαρακτήρα, ενώ παράλληλα παρέχει εγγυήσεις για την ασφάλεια του ηλεκτρονικού εμπορίου[48].

Δεδομένου ότι η μη στρατιωτική αγορά και η αγορά άμυνας χαρακτηρίζονται από κοινές προκλήσεις[49] και από την τεχνολογία διπλής χρήσης που προϋποθέτουν στενή συνεργασία σε τομείς καίριας σημασίας, μια δεύτερη φάση του δικτύου και του Κέντρου του θα μπορούσε να αναπτυχθεί περαιτέρω με την προσθήκη της διάστασης της κυβερνοάμυνας, τηρουμένων πλήρως των διατάξεων της Συνθήκης που αφορούν την κοινή πολιτική ασφάλειας και άμυνας. Πέραν της τεχνολογικής της εστίασης, η διάσταση της άμυνας θα μπορούσε να συμβάλει στη συνεργασία των κρατών μελών στον τομέα της κυβερνοάμυνας, μεταξύ άλλων μέσω της ανταλλαγής πληροφοριών, της επίγνωσης της κατάστασης, της δημιουργίας εμπειρογνωσίας και συντονισμένων αντιδράσεων, καθώς και μέσω της παροχής στήριξης στα κράτη μέλη για την ανάπτυξη κοινών ικανοτήτων. Θα μπορούσε επίσης να λειτουργήσει και ως πλατφόρμα που θα επιτρέπει στα κράτη μέλη να προσδιορίζουν τις προτεραιότητες της ΕΕ για την κυβερνοάμυνα, διερευνώντας κοινές λύσεις, συμβάλλοντας στην ανάπτυξη κοινών στρατηγικών, διευκολύνοντας τη κοινή εκπαίδευση σε θέματα κυβερνοάμυνας, ασκήσεις και δοκιμές σε ευρωπαϊκό επίπεδο, και στηρίζοντας τις εργασίες σχετικά με ταξινομήσεις και πρότυπα κυβερνοάμυνας, δραστηριότητες στις οποίες το Κέντρο θα έχει υποστηρικτικό και συμβουλευτικό ρόλο. Για να επιτελεί τις προαναφερόμενες δραστηριότητες, το Κέντρο θα πρέπει να λειτουργεί σε στενή συνεργασία και πλήρη συμπληρωματικότητα με τον Ευρωπαϊκό Οργανισμό Άμυνας στον τομέα της κυβερνοάμυνας, καθώς και με τον ENISA στον τομέα της κυβερνοανθεκτικότητας. Η εν λόγω διάσταση της άμυνας θα λαμβάνει υπόψη τη διαδικασία που δρομολογήθηκε με το έγγραφο προβληματισμού για το μέλλον της ευρωπαϊκής άμυνας.

Η διασφάλιση του υψηλού επιπέδου ανθεκτικότητας που απαιτείται για την άμυνα στον κυβερνοχώρο προϋποθέτει τον καθορισμό ειδικών στόχων για τις προσπάθειες έρευνας και τεχνολογίας. Τα έργα ή οι τεχνολογίες στον τομέα της κυβερνοάμυνας που αναπτύσσονται από επιχειρήσεις θα μπορούσαν να λαμβάνουν χρηματοδότηση από το Ευρωπαϊκό Ταμείο Άμυνας, τόσο για το στάδιο της έρευνας όσο και για το στάδιο της ανάπτυξης[50]. Σε αυτό το πλαίσιο, ιδιαιτέρως συναφείς θα μπορούσαν να είναι ειδικοί τομείς, όπως τα συστήματα κρυπτογράφησης που βασίζονται σε κβαντικές τεχνολογίες, η επίγνωση της κατάστασης στον κυβερνοχώρο, τα βιομετρικά συστήματα ελέγχου πρόσβασης, ο εντοπισμός προηγμένων συνεχών απειλών, ή η εξόρυξη δεδομένων. Η Ύπατη Εκπρόσωπος, ο Ευρωπαϊκός Οργανισμός Άμυνας και η Επιτροπή θα παρέχουν στήριξη στα κράτη μέλη για τον προσδιορισμό τομέων στους οποίους θα μπορούσε να εξεταστεί το ενδεχόμενο χρηματοδότησης κοινών έργων ασφάλειας στον κυβερνοχώρο από το Ευρωπαϊκό Ταμείο Άμυνας.

---

[47] Η Επιτροπή θα δρομολογήσει ήδη στο πλαίσιο του προγράμματος «Ορίζοντας 2020» μια νέα πρόκληση για την απονομή βραβείου από το πρόγραμμα, ύψους 4 εκατ. EUR, στην καλύτερη καινοτόμο λύση για απρόσκοπτες μεθόδους ηλεκτρονικής ταυτοποίησης.

[48] Cybersecurity in the European Digital Single Market, Ομάδα επιστημονικών συμβούλων υψηλού επιπέδου, Μάρτιος 2017.

[49] «Study on synergies between the civilian and the defence cybersecurity markets» (Μελέτη σχετικά με τις συνέργειες μεταξύ των μη στρατιωτικών αγορών και των αγορών άμυνας στον τομέα της ασφάλειας στον κυβερνοχώρο) (Optimity, SMART 2014-0059).

[50] Ήδη το πρόγραμμα ανάπτυξης της ευρωπαϊκής βιομηχανίας άμυνας δίνει προτεραιότητα σε έργα για την άμυνα στον κυβερνοχώρο, ενώ ο τομέας της άμυνας στον κυβερνοχώρο θα αποτελέσει επίσης ένα από τα θέματα της πρόσκλησης υποβολής προτάσεων που θα προκηρυχθεί το 2018.

2.6 Ανάπτυξη ισχυρής βάσης δεξιοτήτων της ΕΕ στον κυβερνοχώρο

Η ασφάλεια στον κυβερνοχώρο έχει μια ισχυρή εκπαιδευτική διάσταση. Η αποτελεσματική ασφάλεια στον κυβερνοχώρο βασίζεται σε μεγάλο βαθμό στις δεξιότητες των ενδιαφερόμενων ατόμων. Ωστόσο, προβλέπεται ότι έως το 2022 το έλλειμμα σε επαγγελματίες με δεξιότητες στον τομέα της ασφάλειας στον κυβερνοχώρο για τους επαγγελματίες που δραστηριοποιούνται στον ιδιωτικό τομέα στην Ευρώπη θα ανέλθει σε 350 000[51]. Η εκπαίδευση στον τομέα της ασφάλειας στον κυβερνοχώρο θα πρέπει να αναπτυχθεί σε όλα τα επίπεδα, αρχής γενομένης από την τυπική κατάρτιση του εργατικού δυναμικού για την ασφάλεια στον κυβερνοχώρο, την πρόσθετη κατάρτιση όσον αφορά την ασφάλεια στον κυβερνοχώρο για όλους τους εμπειρογνώμονες στον τομέα των ΤΠΕ, αλλά και τη δημιουργία νέων ειδικών προγραμμάτων σπουδών για την ασφάλεια στον κυβερνοχώρο. Θα πρέπει να συγκροτηθούν ισχυρά ακαδημαϊκά κέντρα ικανοτήτων τα οποία θα ανταποκρίνονται στις απαιτήσεις ταχύτερης εκπαίδευσης και κατάρτισης και θα μπορούσαν να λαμβάνουν καθοδήγηση από το Ευρωπαϊκό Κέντρο Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο και τον ENISA. Η εν λόγω εκπαίδευση θα πρέπει να αποσκοπεί στο να καταστεί αυτονόητος ο σχεδιασμός προϊόντων και συστημάτων ΤΠΕ που ενσωματώνουν αρχές ασφάλειας ευθύς εξαρχής. Η εκπαίδευση όσον αφορά την ασφάλεια στον κυβερνοχώρο δεν θα πρέπει να περιοριστεί στους επαγγελματίες του τομέα ΤΠ, αλλά θα πρέπει να ενσωματωθεί στα προγράμματα σπουδών και άλλων κλάδων, όπως η μηχανική, η διοίκηση επιχειρήσεων ή η νομική, καθώς και ειδικών ανά τομέα εκπαιδευτικών κατευθύνσεων. Τέλος, το διδακτικό προσωπικό και οι μαθητές της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης κατά την απόκτηση ψηφιακών ικανοτήτων στα σχολεία θα πρέπει να ευαισθητοποιούνται σχετικά με το ηλεκτρονικό έγκλημα και την ασφάλεια στον κυβερνοχώρο.

Η ΕΕ, σε συνεργασία με τα κράτη μέλη, θα πρέπει επίσης να συμβάλει στο έργο αυτό αξιοποιώντας τις εργασίες του Συνασπισμού για τις Ψηφιακές Δεξιότητες και Θέσεις Εργασίας·[52] και με τη θέσπιση, για παράδειγμα, προγραμμάτων μαθητείας για τις ΜΜΕ στον τομέα της ασφάλειας στον κυβερνοχώρο.

2.7 Προώθηση της υγιεινής στον κυβερνοχώρο και της ευαισθητοποίησης

Λαμβανομένου υπόψη ότι στο 95 % περίπου των περιπτώσεων πιστεύεται ότι το περιστατικό διευκολύνθηκε «από κάποιου είδος ανθρώπινο σφάλμα – εσκεμμένο ή μη»[53], ο ανθρώπινος παράγοντας διαδραματίζει σημαντικό ρόλο εν προκειμένω. Κατά συνέπεια, η ασφάλεια στον κυβερνοχώρο αποτελεί ευθύνη όλων μας. Αυτό σημαίνει ότι η συμπεριφορά προσώπων, εταιρειών και δημόσιων διοικήσεων πρέπει να αλλάξει προκειμένου να διασφαλιστεί ότι όλοι κατανοούν την απειλή και είναι εξοπλισμένοι με τα εργαλεία και τις δεξιότητες που απαιτούνται για να εντοπίζουν γρήγορα και να αυτοπροστατεύονται ενεργά από τις επιθέσεις. Οι άνθρωποι πρέπει να αποκτήσουν συνήθειες κυβερνοϋγιεινής και οι επιχειρήσεις και οι οργανισμοί, από την πλευρά τους, πρέπει να καταρτίσουν κατάλληλα προγράμματα κυβερνοασφάλειας με βάση τον κίνδυνο και να τα επικαιροποιούν τακτικά ώστε να αντικατοπτρίζουν το εξελισσόμενο τοπίο κινδύνου.

---

[51] Global Information Security Workforce Study 2017 (Μελέτη του 2017 σχετικά με το παγκόσμιο εργατικό δυναμικό στον τομέα της ασφάλειας των πληροφοριών). Η παγκόσμια έλλειψη ανέρχεται σε 1,8 εκατομμύρια.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM, «The Cybersecurity Intelligence Index» (Δείκτης πληροφοριών σχετικά με την ασφάλεια στον κυβερνοχώρο), 2014, αναφορά στο Securitymagazine.com, 19 Ιουνίου 2014.

Στην οδηγία ΑΔΠ καθορίζονται οι αρμοδιότητες των κρατών μελών όσον αφορά τόσο την ανταλλαγή πληροφοριών για τις επιθέσεις στον κυβερνοχώρο σε επίπεδο ΕΕ όσο και την εφαρμογή ώριμων εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο και πλαισίων σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Οι δημόσιες διοικήσεις σε ενωσιακό και εθνικό επίπεδο θα πρέπει να διαδραματίσουν περαιτέρω ηγετικό ρόλο για την προώθηση των προσπαθειών αυτών.

Πρώτον, τα κράτη μέλη θα πρέπει να μεγιστοποιήσουν τη διαθεσιμότητα εργαλείων ασφάλειας στον κυβερνοχώρο για τις επιχειρήσεις και τους ιδιώτες. Ειδικότερα, θα πρέπει να καταβληθούν περισσότερες προσπάθειες για την πρόληψη και τον μετριασμό των επιπτώσεων του εγκλήματος στον κυβερνοχώρο για τους τελικούς χρήστες. Σχετικό παράδειγμα περιλαμβάνεται ήδη στο έργο της Ευρωπόλ με την εκστρατεία «NoMoreRansom»[54] (Όχι άλλα λύτρα), η οποία διοργανώθηκε μέσω της στενής συνεργασίας των αρχών επιβολής του νόμου και των εταιρειών ασφάλειας στον κυβερνοχώρο, με στόχο την παροχή βοήθειας στους χρήστες ώστε να προλαμβάνουν προσβολές από λυτρισμικό και να αποκρυπτογραφούν δεδομένα σε περίπτωση που δεχθούν επίθεση. Τέτοιου είδους προγράμματα θα πρέπει να αναπτυχθούν και για άλλους τύπους κακόβουλων λογισμικών, σε άλλους τομείς, ενώ η ΕΕ θα πρέπει επίσης να δημιουργήσει **ενιαία διαδικτυακή πύλη στην οποία θα συγκεντρωθούν όλα τα σχετικά εργαλεία σε υπηρεσία μίας στάσης**, από την οποία θα παρέχονται στους χρήστες συμβουλές σχετικά με την πρόληψη και τον εντοπισμό κακόβουλων λογισμικών και σύνδεσμοι προς μηχανισμούς γνωστοποίησης.

Δεύτερον, τα κράτη μέλη θα πρέπει να μεριμνήσουν για την ταχύτερη **χρήση περισσότερων εργαλείων ασφάλειας στον κυβερνοχώρο κατά την ανάπτυξη της ηλεκτρονικής διακυβέρνησης** και να αξιοποιήσουν επιπλέον πλήρως τα οφέλη του δικτύου ικανοτήτων. Θα πρέπει να προαχθεί η υιοθέτηση ασφαλών μέσων ταυτοποίησης, με την αξιοποίηση του πλαισίου της ΕΕ σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά, το οποίο έχει τεθεί σε εφαρμογή από το 2016 και παρέχει ένα προβλέψιμο κανονιστικό περιβάλλον που καθιστά δυνατή την ασφαλή και απρόσκοπτη ηλεκτρονική αλληλεπίδραση μεταξύ των επιχειρήσεων, των ιδιωτών και των δημόσιων διοικήσεων[55]. Επιπλέον, οι δημόσιοι οργανισμοί, ιδίως εκείνοι που παρέχουν βασικές υπηρεσίες, θα πρέπει να διασφαλίζουν ότι το προσωπικό τους λαμβάνει κατάρτιση σε τομείς οι οποίοι συνδέονται με την ασφάλεια στον κυβερνοχώρο.

Τρίτον, τα κράτη μέλη θα πρέπει να θέσουν ως προτεραιότητα την ευαισθητοποίηση σχετικά με τον κυβερνοχώρο στο πλαίσιο **εκστρατειών ευαισθητοποίησης**, συμπεριλαμβανομένων εκστρατειών που θα απευθύνονται σε σχολεία, πανεπιστήμια, την επιχειρηματική κοινότητα και σε ερευνητικούς φορείς. Ο μήνας για την ασφάλεια στον κυβερνοχώρο που λαμβάνει χώρα κάθε Οκτώβριο, υπό τον συντονισμό του ENISA, θα ενισχυθεί ώστε να προσεγγίζει ευρύτερο κοινό ως κοινή προσπάθεια επικοινωνίας σε ενωσιακό και εθνικό επίπεδο. Εξίσου σημαντική είναι και η ευαισθητοποίηση όσον αφορά τις διαδικτυακές **εκστρατείες παραπληροφόρησης και τις ψευδείς ειδήσεις** στα μέσα κοινωνικής δικτύωσης που αποσκοπούν ειδικά στην υπονόμευση των δημοκρατικών διαδικασιών και των ευρωπαϊκών αξιών. Μολονότι η πρωταρχική ευθύνη παραμένει σε εθνικό επίπεδο, συμπεριλαμβανομένης της ευθύνης για τις εκλογές του Ευρωπαϊκού Κοινοβουλίου, έχει αποδειχθεί ότι η

[54] https://www.nomoreransom.org/.

[55] Πρόκειται για τον κανονισμό (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (κανονισμός eIDAS), ο οποίος εκδόθηκε στις 23 Ιουλίου 2014. Επιπλέον, η Ευρωπαϊκή Επιτροπή παρέχει δομικά στοιχεία και εργαλεία για τη διαλειτουργικότητα μεταξύ της ηλεκτρονικής ταυτοποίησης και της ηλεκτρονικής υπογραφής (π.χ. κατάλογοι προγραμμάτων περιήγησης εμπιστοσύνης) μέσω του προγράμματος του μηχανισμού «Συνδέοντας την Ευρώπη».

συγκέντρωση εμπειρογνωμοσύνης και η ανταλλαγή εμπειριών σε ευρωπαϊκό επίπεδο προσδίδουν προστιθέμενη αξία διότι επικεντρώνονται στην ανάληψη δράσης[56].

Ισχυρό ρόλο καλείται να διαδραματίσει και ο **κλάδος** εν γένει, με ιδιαίτερη έμφαση ωστόσο στους παρόχους ψηφιακών υπηρεσιών και τους κατασκευαστές. Ο κλάδος θα πρέπει να παρέχει υποστήριξη στους χρήστες (ιδιώτες, επιχειρήσεις και δημόσιες διοικήσεις) με εργαλεία που τους επιτρέπουν να αναλαμβάνουν την ευθύνη για τις ενέργειές τους στο διαδίκτυο, καθιστώντας ταυτόχρονα σαφές ότι η διατήρηση της υγιεινής στον κυβερνοχώρο αποτελεί αναπόσπαστο τμήμα της προσφοράς προς τους καταναλωτές[57]. Για τον εντοπισμό και την εξάλειψη των τρωτών σημείων, ο κλάδος θα πρέπει να καταβάλλει προσπάθειες για την εφαρμογή εσωτερικών διαδικασιών που αφορούν την έρευνα, τη διαλογή και την αντιμετώπιση των τρωτών σημείων, ανεξάρτητα από το αν η πηγή του πιθανού τρωτού σημείου ήταν εξωτερική ή αν προερχόταν από το εσωτερικό της οικείας εταιρείας.

Βασικές δράσεις

- Πλήρης εφαρμογή της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.
- Άμεση έγκριση από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο του κανονισμού σχετικά με τον καθορισμό νέας εντολής για τον ENISA και τη θέσπιση ευρωπαϊκού πλαισίου πιστοποίησης[58].
- Κοινή πρωτοβουλία της Επιτροπής και της βιομηχανίας για τον ορισμό αρχής «καθήκοντος επιμέλειας» με σκοπό τη μείωση των τρωτών σημείων προϊόντων/λογισμικού και την προώθηση της «ασφάλειας εκ σχεδιασμού».
- Άμεση υλοποίηση του προσχεδίου για την αντιμετώπιση σημαντικών διασυνοριακών περιστατικών.
- Δρομολόγηση αξιολόγησης επιπτώσεων για την εξέταση της δυνατότητας να υποβληθεί πρόταση από την Επιτροπή το 2018 για τη δημιουργία, αφενός, δικτύου κέντρων ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και, αφετέρου, Ευρωπαϊκού Κέντρου Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο, βάσει της εφαρμογής άμεσης πιλοτικής φάσης.
- Παροχή στήριξης στα κράτη μέλη για τον προσδιορισμό τομέων στους οποίους θα μπορούσε να εξεταστεί το ενδεχόμενο χρηματοδότησης κοινών έργων ασφάλειας στον κυβερνοχώρο από το Ευρωπαϊκό Ταμείο Άμυνας.
- Δημιουργία υπηρεσίας μίας στάσης για ολόκληρη την ΕΕ, η οποία θα προσφέρει συνδρομή στα θύματα επιθέσεων στον κυβερνοχώρο, παρέχοντας πληροφορίες σχετικά με τις πλέον πρόσφατες απειλές και συγκεντρώνοντας πρακτικές συμβουλές και εργαλεία για την ασφάλεια στον κυβερνοχώρο.
- Ανάληψη δράσης από τα κράτη μέλη για την ενσωμάτωση της ασφάλειας στον κυβερνοχώρο σε προγράμματα δεξιοτήτων, στην ηλεκτρονική διακυβέρνηση και σε εκστρατείες ευαισθητοποίησης.
- Ανάληψη δράσης από τη βιομηχανία για την ενίσχυση της κατάρτισης του προσωπικού

[56] Παράδειγμα αποτελεί η ειδική ομάδα «East StratCom», η οποία συγκροτήθηκε το 2015 από τα κράτη μέλη και την Ύπατη Εκπρόσωπο με σκοπό την αντιμετώπιση των συνεχιζόμενων εκστρατειών παραπληροφόρησης της Ρωσίας. Έργο της ομάδας είναι να αναπτύξει προϊόντα και εκστρατείες επικοινωνίας που εστιάζουν στην επεξήγηση των πολιτικών της ΕΕ στην περιοχή της Ανατολικής Εταιρικής Σχέσης.

[57] Κάποιοι κατασκευαστές έχουν ήδη εξοικειωθεί με την έννοια αυτή, δεδομένου ότι σε ορισμένες νομοθετικές πράξεις για τα ευρωπαϊκά προϊόντα (όπως η οδηγία 2006/42/ΕΚ για τα μηχανήματα) προβλέπονται ήδη οι αρχές της «ασφάλειας εκ σχεδιασμού».

[58] COM(2017) 477.

όσον αφορά την ασφάλεια στον κυβερνοχώρο και υιοθέτηση της προσέγγισης «ασφάλειας εκ σχεδιασμού» για τα προϊόντα, τις υπηρεσίες και τις διαδικασίες τους.

3. ΔΗΜΙΟΥΡΓΙΑ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΑΠΟΤΡΟΠΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΕ ΕΠΙΠΕΔΟ ΕΕ

Αποτελεσματική αποτροπή σημαίνει θέσπιση πλαισίου μέτρων, τα οποία είναι ταυτόχρονα αξιόπιστα και αποτρεπτικά για τους επίδοξους εγκληματίες και δράστες επιθέσεων στον κυβερνοχώρο. Στον βαθμό που οι δράστες επιθέσεων στον κυβερνοχώρο –τόσο κρατικού όσο και μη κρατικού χαρακτήρα– δεν έχουν τίποτε να φοβηθούν εκτός από την αποτυχία, δεν θα έχουν κίνητρο να πάψουν να προσπαθούν. Η διασφάλιση αποτελεσματικότερης αντιμετώπισης σε επίπεδο επιβολής του νόμου, η οποία θα εστιάζει στον εντοπισμό, στην ιχνηλασιμότητα και στη δίωξη εγκληματιών του κυβερνοχώρου, είναι καθοριστικής σημασίας για τη δημιουργία αποτελεσματικής αποτροπής. Στο στοιχείο αυτό προστίθεται και η ανάγκη παροχής στήριξης από την ΕΕ στα κράτη μέλη της για την ανάπτυξη στρατιωτικών ικανοτήτων διπλής χρήσης στον τομέα της ασφάλειας στον κυβερνοχώρο. Η αναχαίτιση των επιθέσεων στον κυβερνοχώρο θα καταστεί δυνατή μόνον όταν αυξήσουμε τις πιθανότητες σύλληψης και τιμωρίας για την τέλεσή τους. Οι επιθέσεις στον κυβερνοχώρο θα πρέπει να διερευνώνται άμεσα και οι δράστες να παραπέμπονται ενώπιον της δικαιοσύνης ή να λαμβάνονται μέτρα που καθιστούν δυνατή την κατάλληλη αντιμετώπιση σε πολιτικό ή διπλωματικό επίπεδο. Σε περίπτωση μείζονος κρίσης με σημαντικές διεθνείς και αμυντικές διαστάσεις, η Ύπατη Εκπρόσωπος θα μπορεί να υποβάλλει στο Συμβούλιο επιλογές κατάλληλης αντιμετώπισης.

Ένα μέτρο για τη βελτίωση της αντιμετώπισης των επιθέσεων στον κυβερνοχώρο από πλευράς ποινικού δικαίου είχε αποτελέσει ήδη η οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών[59], η οποία εκδόθηκε το 2013. Με την εν λόγω οδηγία θεσπίστηκαν ελάχιστοι κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των κυρώσεων στον τομέα των επιθέσεων κατά των συστημάτων πληροφοριών, ενώ προβλέφθηκαν επίσης επιχειρησιακά μέτρα για τη βελτίωση της συνεργασίας μεταξύ των αρχών. Η συγκεκριμένη οδηγία έχει συμβάλει στην επίτευξη ουσιαστικής προόδου όσον αφορά την ποινικοποίηση των επιθέσεων στον κυβερνοχώρο σε συγκρίσιμο επίπεδο μεταξύ των κρατών μελών, γεγονός που διευκολύνει τη διασυνοριακή συνεργασία των αρχών επιβολής του νόμου που ερευνούν τέτοιου είδους αδικήματα. Ωστόσο, υπάρχουν ακόμη περιθώρια για την πλήρη αξιοποίηση των δυνατοτήτων που δημιουργεί η οδηγία, εάν τα κράτη μέλη εφαρμόσουν πλήρως όλες τις διατάξεις της[60]. Η Επιτροπή θα εξακολουθήσει να παρέχει στήριξη στα κράτη μέλη κατά την εφαρμογή της οδηγίας και επί του παρόντος δεν κρίνει σκόπιμο να προτείνει τροποποιήσεις της.

3.1 Εντοπισμός δραστών κακόβουλων ενεργειών

Για να αυξηθούν οι πιθανότητες παραπομπής των δραστών ενώπιον της δικαιοσύνης, πρέπει να βελτιώσουμε επειγόντως την ικανότητά μας να εντοπίζουμε τους υπεύθυνους επιθέσεων στον κυβερνοχώρο. Η εύρεση χρήσιμων πληροφοριών για τη διερεύνηση εγκλημάτων στον κυβερνοχώρο, κυρίως υπό τη μορφή ψηφιακών ιχνών, αποτελεί σημαντική πρόκληση για τις αρχές επιβολής του νόμου. Ως εκ τούτου, πρέπει να αυξήσουμε την τεχνολογική μας ικανότητα αποτελεσματικής διερεύνησης, μεταξύ άλλων μέσω της ενίσχυσης της αρμόδιας

[59] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών.

[60] COM(2017) 474.

μονάδας της Ευρωπόλ για το έγκλημα στον κυβερνοχώρο με εμπειρογνώμονες στον τομέα του κυβερνοχώρου. Η Ευρωπόλ έχει εξελιχθεί σε βασικό παράγοντα όσον αφορά την παροχή στήριξης στο πλαίσιο των ερευνών των κρατών μελών σε πολλαπλές δικαιοδοσίες. Θα πρέπει να καταστεί κέντρο εμπειρογνωμοσύνης για τις αρχές επιβολής του νόμου των κρατών μελών όσον αφορά τις έρευνες στο διαδίκτυο και την εγκληματολογία στον κυβερνοχώρο.

Η ευρέως διαδεδομένη πρακτική τοποθέτησης πολλαπλών χρηστών –ενίοτε χιλιάδων– πίσω από μία διεύθυνση IP καθιστά εξαιρετικά δύσκολη από τεχνική άποψη τη διερεύνηση τυχόν κακόβουλης συμπεριφοράς στο διαδίκτυο. Καθιστά επίσης απαραίτητη ορισμένες φορές –για παράδειγμα σε περιπτώσεις σοβαρών εγκλημάτων, όπως η σεξουαλική κακοποίηση παιδιών– τη διερεύνηση μεγάλου αριθμού χρηστών προκειμένου να εντοπιστεί ένας δράστης κακόβουλων ενεργειών. Ως εκ τούτου, η ΕΕ θα ενθαρρύνει την υιοθέτηση του νέου πρωτοκόλλου (IPv6) διότι επιτρέπει την κατανομή ενός μόνο χρήστη ανά διεύθυνση IP, αποφέροντας σαφή οφέλη για την επιβολή του νόμου και τη διεξαγωγή ερευνών στον τομέα της ασφάλειας στον κυβερνοχώρο. Ως πρώτο βήμα για την ενθάρρυνση της υιοθέτησης του εν λόγω πρωτοκόλλου, η Επιτροπή θα ενσωματώσει την απαίτηση μετάβασης στο IPv6 σε όλες τις πολιτικές της, μέσω της προσθήκης σχετικών απαιτήσεων στις δημόσιες συμβάσεις και όσον αφορά τη χρηματοδότηση έργων και έρευνας, καθώς και μέσω της παροχής στήριξης για τη δημιουργία του αναγκαίου υλικού κατάρτισης. Επιπλέον, τα κράτη μέλη θα πρέπει να εξετάσουν το ενδεχόμενο σύναψης εθελοντικών συμφωνιών με τους παρόχους υπηρεσιών διαδικτύου για την προώθηση της υιοθέτησης του IPv6.

Το Βέλγιο κατέχει ηγετική θέση[61] *όσον αφορά το ποσοστό υιοθέτησης του IPv6, μεταξύ άλλων χάρη στη συνεργασία δημόσιου και ιδιωτικού τομέα: ενδιαφερόμενοι φορείς εξέτασαν το ενδεχόμενο περιορισμού της χρήσης μίας διεύθυνσης IP σε 16 χρήστες κατ' ανώτατο όριο στο πλαίσιο ενός εθελοντικού μέτρου αυτορρύθμισης, εξέλιξη που παρείχε κίνητρα για τη μετάβαση στο IPv6*[62].

Γενικότερα, θα πρέπει να προωθηθεί περαιτέρω η λογοδοσία στο διαδίκτυο. Αυτό σημαίνει ότι πρέπει να προαχθούν μέτρα αποτροπής της κατάχρησης των ονομάτων τομέα για τη διανομή αυτόκλητων μηνυμάτων ή την πραγματοποίηση επιθέσεων ηλεκτρονικού «ψαρέματος». Για τον σκοπό αυτό, η Επιτροπή θα εργαστεί για τη βελτίωση της λειτουργίας και της διαθεσιμότητας και της ακρίβειας των πληροφοριών που παρέχονται στο Σύστημα Ονομάτων Τομέα και στο σύστημα IP WHOIS[63], σε εναρμόνιση με τις προσπάθειες που καταβάλλονται από το «Σώμα του Διαδικτύου για την εκχώρηση ονομάτων και αριθμών»[64].

3.2 Ενίσχυση της αντιμετώπισης σε επίπεδο επιβολής του νόμου

Η αποτελεσματική **διερεύνηση** και **δίωξη** του εγκλήματος στον κυβερνοχώρο αποτελεί βασικό παράγοντα για την αποτροπή των επιθέσεων στον κυβερνοχώρο. Ωστόσο, το

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Πρωτόκολλο ερωτήσεων και απαντήσεων που χρησιμοποιείται ευρέως για την πραγματοποίηση αναζήτησης σε βάσεις δεδομένων στις οποίες αποθηκεύονται οι εγγεγραμμένοι χρήστες ή τα πρόσωπα στα οποία έχει εκχωρηθεί ένας διαδικτυακός πόρος.

[64] Το «Σώμα του Διαδικτύου για την εκχώρηση ονομάτων και αριθμών» (ICANN) είναι ένας οργανισμός μη κερδοσκοπικού χαρακτήρα, ο οποίος είναι αρμόδιος για τον συντονισμό της συντήρησης και των διαδικασιών διαφόρων βάσεων δεδομένων που αφορούν τους χώρους ονομάτων του διαδικτύου.

υφιστάμενο δικονομικό πλαίσιο πρέπει να προσαρμοστεί καλύτερα στην εποχή του διαδικτύου[65]. Η ταχύτητα των επιθέσεων στον κυβερνοχώρο μπορεί να ασκήσει πιέσεις στις διαδικασίες μας, αλλά και να δημιουργήσει ιδιαίτερες ανάγκες άμεσης διασυνοριακής συνεργασίας. Για τον σκοπό αυτό, όπως ανακοινώθηκε στο πλαίσιο του ευρωπαϊκού θεματολογίου για την ασφάλεια, στις αρχές του 2018 η Επιτροπή θα υποβάλει προτάσεις για τη **διευκόλυνση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία**. Παράλληλα, η Επιτροπή εφαρμόζει επί του παρόντος πρακτικά μέτρα για τη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία για τους σκοπούς ποινικών ερευνών, συμπεριλαμβανομένης της χρηματοδότησης της κατάρτισης σχετικά με τη διασυνοριακή συνεργασία, της ανάπτυξης ηλεκτρονικής πλατφόρμας ανταλλαγής πληροφοριών εντός της ΕΕ και της τυποποίησης των εντύπων δικαστικής συνεργασίας που χρησιμοποιούνται μεταξύ των κρατών μελών.

Άλλο ένα εμπόδιο που εγείρεται στην αποτελεσματική άσκηση διώξεων είναι οι διαφορετικές εγκληματολογικές διαδικασίες που εφαρμόζονται στα διάφορα κράτη μέλη όσον αφορά τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων στο πλαίσιο διερεύνησης εγκλημάτων στον κυβερνοχώρο. Το πρόβλημα αυτό θα μπορούσε να περιοριστεί με την καταβολή προσπαθειών για τη θέσπιση κοινών εγκληματολογικών προτύπων. Επιπλέον, για τη στήριξη της ιχνηλασιμότητας και του καταλογισμού ευθυνών, πρέπει να ενισχυθούν οι εγκληματολογικές ικανότητες. Ένα πιθανό μέτρο θα ήταν η περαιτέρω ανάπτυξη της εγκληματολογικής ικανότητας εντός της Ευρωπόλ, μέσω της προσαρμογής των υφιστάμενων δημοσιονομικών και ανθρώπινων πόρων στο Ευρωπαϊκό Κέντρο της Ευρωπόλ για τα εγκλήματα στον κυβερνοχώρο, ούτως ώστε να καλυφθεί η αυξανόμενη ανάγκη επιχειρησιακής υποστήριξης στο πλαίσιο των διασυνοριακών ερευνών για εγκλήματα στον κυβερνοχώρο. Ένα άλλο μέτρο που θα μπορούσε να ληφθεί, παράλληλα με την τεχνολογική εστίαση στην κρυπτογράφηση όπως περιγράφεται ανωτέρω, συνίσταται στην εξέταση του τρόπου με τον οποίο η κατάχρησή της από εγκληματίες δημιουργεί σημαντικές προκλήσεις όσον αφορά την καταπολέμηση σοβαρών εγκλημάτων, μεταξύ των οποίων η τρομοκρατία και το έγκλημα στον κυβερνοχώρο. Η Επιτροπή θα παρουσιάσει τα αποτελέσματα των υφιστάμενων προβληματισμών σχετικά με τον **ρόλο της κρυπτογράφησης στις ποινικές έρευνες**[66] έως τον Οκτώβριο του 2017[67].

Δεδομένου του διασυνοριακού χαρακτήρα του διαδικτύου, το πλαίσιο διεθνούς συνεργασίας, το οποίο παρέχεται από τη **σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο**[68], προσφέρει σε μια ποικιλόμορφη ομάδα χωρών τη δυνατότητα να χρησιμοποιούν ένα βέλτιστο νομικό πρότυπο για τις διάφορες εθνικές νομοθεσίες αντιμετώπισης του εγκλήματος στον κυβερνοχώρο. Επί του παρόντος διερευνάται το ενδεχόμενο προσθήκης πρωτοκόλλου στη σύμβαση[69], εξέλιξη που θα μπορούσε επίσης να

---

[65] Παράδειγμα αποτελεί ο (εικονικός) κεντρικός διακομιστής εντολών και στοιχείων ελέγχου του botnet Avalanche, ο οποίος μετακινούσε υλικούς διακομιστές και τομείς κάθε πέντε λεπτά.

[66] Προεδρία του Συμβουλίου, «Αποτελέσματα της συνεδρίασης του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων της 8ης και 9ης Δεκεμβρίου 2016», αριθ. 15391/16.

[67] Eighth progress report towards an effective and genuine Security Union (Όγδοη έκθεση προόδου προς την κατεύθυνση μιας αποτελεσματικής και πραγματικής Ένωσης Ασφάλειας), COM(2017) 354 final της 29ης Ιουνίου 2017.

[68] Η εν λόγω σύμβαση αποτελεί την πρώτη διεθνή Συνθήκη σχετικά με εγκλήματα που τελούνται μέσω του διαδικτύου και άλλων δικτύων υπολογιστών και διαλαμβάνει ειδικότερα τις παραβιάσεις δικαιωμάτων διανοητικής ιδιοκτησίας, τις περιπτώσεις απάτης που συνδέονται με υπολογιστές, την παιδική πορνογραφία και τις παραβιάσεις της ασφάλειας των δικτύων. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Το 2017, 55 κυβερνήσεις είχαν κυρώσει ή είχαν προσχωρήσει στη σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

[69] Όροι αναφοράς για την κατάρτιση του σχεδίου του δεύτερου πρόσθετου πρωτοκόλλου της σύμβασης της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, T-CY (2017)3.

αποτελέσει χρήσιμη ευκαιρία για την εξέταση του ζητήματος της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία σε διεθνές πλαίσιο. Αντί της θέσπισης νέων διεθνών νομοθετικών πράξεων για ζητήματα που αφορούν το έγκλημα στον κυβερνοχώρο, η ΕΕ καλεί όλες τις χώρες να καταρτίσουν κατάλληλη εθνική νομοθεσία και να επιδιώξουν τη συνεργασία εντός αυτού του υφιστάμενου διεθνούς πλαισίου.

Η εκτεταμένη διαθεσιμότητα εργαλείων ανωνυμοποίησης διευκολύνει τις προσπάθειες των εγκληματιών για την απόκρυψη της ταυτότητάς τους. Το «**σκοτεινό δίκτυο**»[70] (darknet) έχει δημιουργήσει νέους τρόπους πρόσβασης των εγκληματιών σε υλικό σεξουαλικής κακοποίησης παιδιών, ναρκωτικά ή όπλα, ενώ ο κίνδυνος σύλληψης είναι συχνά μικρός[71]. Επί του παρόντος, αποτελεί επίσης βασική πηγή των εργαλείων που χρησιμοποιούνται στο έγκλημα στον κυβερνοχώρο, όπως εργαλεία κακόβουλου λογισμικού και δικτυοπαραβίασης. Η Επιτροπή θα αναλύσει, από κοινού με τους ενδιαφερόμενους φορείς, τις εθνικές προσεγγίσεις με σκοπό τη εξεύρεση νέων λύσεων. Η Ευρωπόλ πρέπει να διευκολύνει και να στηρίζει έρευνες στο σκοτεινό δίκτυο, να αξιολογεί τις απειλές και να συμβάλλει στον προσδιορισμό της δικαιοδοσίας και στην απόδοση προτεραιότητας σε υποθέσεις υψηλού κινδύνου, ενώ η ΕΕ μπορεί να διαδραματίσει ηγετικό ρόλο στον συντονισμό της διεθνούς δράσης[72].

Ένας αναπτυσσόμενος τομέας εγκληματικής δραστηριότητας στον κυβερνοχώρο είναι η δόλια χρήση στοιχείων πιστωτικών καρτών ή άλλων ηλεκτρονικών μέσων πληρωμής. Τα διαπιστευτήρια πληρωμής που αποκτώνται μέσω επιθέσεων στον κυβερνοχώρο κατά διαδικτυακών εμπόρων λιανικής ή άλλων νόμιμων επιχειρήσεων διακινούνται στη συνέχεια στο διαδίκτυο και μπορούν να χρησιμοποιηθούν από εγκληματίες για την τέλεση απάτης[73]. Η Επιτροπή βρίσκεται επί του παρόντος στο στάδιο υποβολής πρότασης για την προώθηση της αποτροπής μέσω **οδηγίας για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν μέσα πληρωμής πλην των μετρητών**[74]. Η εν λόγω οδηγία αποσκοπεί στην επικαιροποίηση των υφιστάμενων κανόνων στον συγκεκριμένο τομέα και στην ενίσχυση της ικανότητας των αρχών επιβολής του νόμου να καταπολεμούν αυτή τη μορφή εγκλήματος.

Παράλληλα, πρέπει να βελτιωθούν οι ικανότητες έρευνας των αρχών επιβολής του νόμου των κρατών μελών όσον αφορά το έγκλημα στον κυβερνοχώρο, όπως επίσης και η κατανόηση των εγκλημάτων στον κυβερνοχώρο και των επιλογών έρευνας από τους εισαγγελείς και το δικαστικό σώμα. Η Eurojust και η Ευρωπόλ συμβάλλουν στην επίτευξη του στόχου αυτού και στην ενίσχυση του συντονισμού, σε στενή συνεργασία με εξειδικευμένες συμβουλευτικές ομάδες εντός του Κέντρου της Ευρωπόλ για τα εγκλήματα στον κυβερνοχώρο και με τα δίκτυα των προϊσταμένων των μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο και των εισαγγελέων που ειδικεύονται στο έγκλημα στον κυβερνοχώρο. Η Επιτροπή θα διαθέσει χρηματοδότηση ύψους 10,5 εκατ. EUR για την καταπολέμηση του εγκλήματος στον

---

[70] Το σκοτεινό δίκτυο αποτελείται από περιεχόμενο σε επικαλυπτικά δίκτυα τα οποία χρησιμοποιούν μεν το διαδίκτυο, αλλά απαιτούν ειδικό λογισμικό, ρυθμίσεις ή άδεια πρόσβασης. Το σκοτεινό δίκτυο αποτελεί μικρό τμήμα του βαθέος ιστού, δηλαδή του τμήματος του ιστού που δεν είναι ευρετηριασμένο από μηχανές αναζήτησης.

[71] Αξιοσημείωτη εξαίρεση αποτελεί η πρόσφατη κατάργηση δύο από τις μεγαλύτερες εγκληματικές αγορές του σκοτεινού ιστού, της Alphabay και της Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Η Ευρωπόλ διαδραματίζει ήδη σημαντικό ρόλο στον συγκεκριμένο τομέα. Για πρόσφατο παράδειγμα, βλέπε: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Τα προϊόντα απάτης αποτελούν σημαντική πηγή εσόδων για το οργανωμένο έγκλημα και, ως εκ τούτου, καθιστούν δυνατή την τέλεση άλλων εγκληματικών δραστηριοτήτων, όπως η τρομοκρατία, η διακίνηση ναρκωτικών και η εμπορία ανθρώπων.

[74] COM(2017) 489.

κυβερνοχώρο στο πλαίσιο του **προγράμματος «Ταμείο Εσωτερικής Ασφάλειας-Αστυνομία»**. Σημαντικό στοιχείο αποτελεί η κατάρτιση και έχει αναπτυχθεί χρήσιμο υλικό από την Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος. Το υλικό αυτό θα πρέπει πλέον να τεθεί ευρέως στη διάθεση των επαγγελματιών του τομέα επιβολής του νόμου, με την υποστήριξη του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κατάρτιση στον Τομέα της Επιβολής του Νόμου (CEPOL).

3.3 Συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα κατά του εγκλήματος στον κυβερνοχώρο

Η αποτελεσματικότητα των παραδοσιακών μηχανισμών επιβολής του νόμου τίθεται υπό αμφισβήτηση από τα χαρακτηριστικά του ψηφιακού κόσμου, ο οποίος αποτελείται κυρίως από υποδομές ιδιωτικής ιδιοκτησίας και πολυάριθμους διαφορετικούς παράγοντες σε ευρύ φάσμα δικαιοδοσιών. Κατά συνέπεια, η συνεργασία με τον ιδιωτικό τομέα, συμπεριλαμβανομένης της βιομηχανίας και της κοινωνίας των πολιτών, είναι θεμελιώδους σημασίας για την αποτελεσματική καταπολέμηση του εγκλήματος από τις δημόσιες αρχές. Στο πλαίσιο αυτό, ο χρηματοπιστωτικός τομέας είναι επίσης σημαντικός και θα πρέπει να εξασφαλιστεί μεγαλύτερη συνεργασία. Για παράδειγμα, θα πρέπει να ενισχυθεί ο ρόλος των μονάδων χρηματοοικονομικών πληροφοριών[75] στο πλαίσιο του εγκλήματος στον κυβερνοχώρο.

Ορισμένα κράτη μέλη έχουν ήδη λάβει βασικά μέτρα. Στις Κάτω Χώρες, τα χρηματοπιστωτικά ιδρύματα και οι αρχές επιβολής του νόμου συνεργάζονται, στο πλαίσιο της ειδικής ομάδας για το ηλεκτρονικό έγκλημα, με στόχο την αντιμετώπιση της ηλεκτρονικής απάτης και του εγκλήματος στον κυβερνοχώρο. Το γερμανικό κέντρο ικανοτήτων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο λειτουργεί ως επιχειρησιακός κόμβος ώστε τα μέλη του να ανταλλάσσουν πληροφορίες σε στενή συνεργασία με τη γερμανική ομοσπονδιακή αστυνομία και να αναπτύσσουν μέτρα για τη διασφάλιση της προστασίας έναντι εγκλημάτων στον κυβερνοχώρο. Δεκαέξι κράτη μέλη[76] έχουν δημιουργήσει κέντρα αριστείας για το έγκλημα στον κυβερνοχώρο, με στόχο τη διευκόλυνση της συνεργασίας μεταξύ των αρχών επιβολής του νόμου, της ακαδημαϊκής κοινότητας και των ιδιωτών εταίρων για την ανάπτυξη και την ανταλλαγή βέλτιστων πρακτικών, κατάρτισης και ανάπτυξης ικανοτήτων.
Η Επιτροπή στηρίζει τη δημιουργία συμπράξεων δημόσιου και ιδιωτικού τομέα, καθώς και μηχανισμών συνεργασίας μέσω ειδικών έργων, όπως το κέντρο ηλεκτρονικής απάτης και δίκτυο εμπειρογνωμόνων[77], τα οποία εφαρμόζουν μοντέλα και πρότυπα ανταλλαγής πληροφοριών με σκοπό την ανάλυση και τον περιορισμό των κινδύνων ηλεκτρονικών εγκλημάτων και απάτης.

Στο πλαίσιο του εγκλήματος στον κυβερνοχώρο, οι ιδιωτικές επιχειρήσεις πρέπει να είναι σε θέση να ανταλλάσσουν με τις αρχές επιβολής του νόμου πληροφορίες σχετικά με συγκεκριμένα περιστατικά –συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα– τηρώντας πλήρως τους κανόνες για την προστασία των δεδομένων. Η μεταρρύθμιση της

[75] Οι μονάδες χρηματοοικονομικών πληροφοριών λειτουργούν ως εθνικά κέντρα για την παραλαβή και την ανάλυση αναφορών ύποπτων συναλλαγών και άλλων πληροφοριών που αφορούν τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες, συναφή βασικά αδικήματα και τη χρηματοδότηση της τρομοκρατίας, καθώς και για τη διάδοση των αποτελεσμάτων της ανάλυσης αυτής.

[76] Αυστρία, Βέλγιο, Βουλγαρία, Γαλλία, Γερμανία, Ελλάδα, Εσθονία, Ηνωμένο Βασίλειο, Ιρλανδία, Ισπανία, Κύπρος, Λιθουανία, Πολωνία, Ρουμανία, Σλοβενία και Τσεχική Δημοκρατία.

[77] Η πρωτοβουλία OF2CEN της ΕΕ έχει ως στόχο να καταστήσει δυνατό να ανταλλάσσονται συστηματικά μεταξύ τραπεζών και υπηρεσιών επιβολής του νόμου σε ολόκληρη την ΕΕ πληροφορίες σχετικές με τη διαδικτυακή απάτη για την αποτροπή πληρωμών προς απατεώνες και παρένθετους μεταφορείς χρημάτων, καθώς και για τη διερεύνηση και ποινική δίωξη των εμπλεκόμενων δραστών. Η πρωτοβουλία συγχρηματοδοτείται από την ΕΕ (πρόγραμμα «Ταμείο Εσωτερικής Ασφάλειας-Αστυνομία»).

προστασίας δεδομένων της ΕΕ, η οποία θα τεθεί σε εφαρμογή τον Μάιο του 2018, προβλέπει κοινή δέσμη κανόνων για τον καθορισμό των προϋποθέσεων συνεργασίας μεταξύ των αρχών επιβολής του νόμου και ιδιωτικών οντοτήτων. Η Ευρωπαϊκή Επιτροπή θα συνεργαστεί με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και ενδιαφερόμενους φορείς με στόχο τον προσδιορισμό βέλτιστων πρακτικών στον συγκεκριμένο τομέα και, κατά περίπτωση, την παροχή καθοδήγησης.

3.4 Ενίσχυση της αντιμετώπισης σε πολιτικό επίπεδο

Στο **πλαίσιο κοινής διπλωματικής αντίδρασης της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο**[78] («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»), το οποίο εγκρίθηκε πρόσφατα, καθορίζονται τα μέτρα που πρέπει να λαμβάνονται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφάλειας, συμπεριλαμβανομένης της λήψης περιοριστικών μέτρων που μπορούν να χρησιμοποιηθούν για την ενίσχυση της αντίδρασης της ΕΕ σε δραστηριότητες που θίγουν τόσο τα πολιτικά και οικονομικά της συμφέροντα όσο και τα συμφέροντά της στον τομέα της ασφάλειας. Το εν λόγω πλαίσιο αποτελεί σημαντικό βήμα προόδου για την ανάπτυξη ικανοτήτων επισήμανσης και αντίδρασης, τόσο σε επίπεδο ΕΕ όσο και σε επίπεδο κρατών μελών. Θα αυξήσει την ικανότητά μας να καταλογίζουμε ευθύνες για κακόβουλες δραστηριότητες στον κυβερνοχώρο, με σκοπό την άσκηση επιρροής στη συμπεριφορά δυνητικών δραστών, λαμβανομένης παράλληλα υπόψη της ανάγκης διασφάλισης κατάλληλων δράσεων αντιμετώπισης. Ο καταλογισμός ευθυνών σε κρατικό ή μη κρατικό παράγοντα εξακολουθεί να αποτελεί κυρίαρχη πολιτική απόφαση που λαμβάνεται σε συνάρτηση με πληροφορίες από όλες τις πηγές. Επί του παρόντος βρίσκονται σε εξέλιξη εργασίες εφαρμογής του πλαισίου σε συνεργασία με τα κράτη μέλη, οι οποίες θα συνεχιστούν σε στενό συντονισμό με το προσχέδιο για την αντιμετώπιση μεγάλης κλίμακας περιστατικών στον κυβερνοχώρο[79]. Η επίγνωση της κατάστασης, η οποία είναι αναγκαία για τη χρήση των μέτρων εντός του πλαισίου, θα πρέπει να ενοποιείται, να αναλύεται και να αποτελεί αντικείμενο κοινοχρησίας από το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (INTCEN)[80], σε στενή συνεργασία με τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ.

3.5 Δημιουργία αποτροπής στον τομέα της ασφάλειας στον κυβερνοχώρο μέσω της αμυντικής ικανότητας των κρατών μελών

Τα κράτη μέλη αναπτύσσουν ήδη ικανότητες άμυνας στον κυβερνοχώρο. Επιπλέον, δεδομένων των ασαφών ορίων μεταξύ της άμυνας και της ασφάλειας στον κυβερνοχώρο και του χαρακτήρα διπλής χρήσης των εργαλείων και των τεχνολογιών στον κυβερνοχώρο, καθώς και των σημαντικών αποκλίσεων μεταξύ των προσεγγίσεων των κρατών μελών, η ΕΕ είναι σε θέση να συμβάλει στην προώθηση συνεργειών μεταξύ των στρατιωτικών και μη στρατιωτικών προσπαθειών[81].

Τα κράτη μέλη που διαθέτουν περισσότερο προηγμένες ικανότητες στον τομέα της ασφάλειας στον κυβερνοχώρο και είναι πρόθυμα να τις συνενώσουν θα μπορούσαν, με την υποστήριξη της Ύπατης Εκπροσώπου, της Επιτροπής και του Ευρωπαϊκού Οργανισμού Άμυνας, να εξετάσουν το ενδεχόμενο να συμπεριληφθεί η ασφάλεια στον κυβερνοχώρο στο πλαίσιο μιας «μόνιμης διαρθρωμένης συνεργασίας» (PESCO). Το πρόγραμμα αυτό θα

[78] http://www.consilium.europa.eu/el/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 final.
[81] Η ΕΕ αντιλαμβάνεται τον κυβερνοχώρο ως χώρο επιχειρήσεων, όπως χερσαίες, εναέριες και θαλάσσιες επιχειρήσεις. Στις προσπάθειες άμυνας στον κυβερνοχώρο περιλαμβάνονται επίσης η προστασία και η ανθεκτικότητα των διαστημικών πόρων και των συναφών επίγειων υποδομών.

μπορούσε να βασιστεί στις εργασίες που αναφέρονται ανωτέρω για την ενθάρρυνση των βιομηχανικών ικανοτήτων και της στρατηγικής αυτονομίας της ΕΕ. Η ΕΕ μπορεί επίσης να προωθήσει τη διαλειτουργικότητα, μεταξύ άλλων, διευκολύνοντας την ανάπτυξη ικανοτήτων, τον συντονισμό της κατάρτισης και της εκπαίδευσης και τις προσπάθειες τυποποίησης διπλής χρήσης.

Παράλληλα, θα πρέπει να αξιοποιηθεί πλήρως το κοινό πλαίσιο αντιμετώπισης υβριδικών απειλών, οι οποίες συχνά περιλαμβάνουν επιθέσεις στον κυβερνοχώρο, κυρίως μέσω της Μονάδας Ανάλυσης Υβριδικών Απειλών της ΕΕ και του προσφάτως συσταθέντος Ευρωπαϊκού Κέντρου Αριστείας για την αντιμετώπιση των υβριδικών απειλών στο Ελσίνκι, αποστολή των οποίων είναι η ενθάρρυνση του στρατηγικού διαλόγου και η διενέργεια έρευνας και ανάλυσης.

Η ΕΕ θα δώσει εκ νέου έμφαση στο πλαίσιο πολιτικής της ΕΕ για την άμυνα στον κυβερνοχώρο 2014[82], ως εργαλείο για την περαιτέρω ενσωμάτωση της ασφάλειας και της άμυνας στον κυβερνοχώρο στην κοινή πολιτική ασφάλειας και άμυνας (ΚΠΑΑ). Η ανθεκτικότητα στον κυβερνοχώρο των αποστολών και επιχειρήσεων της ΚΠΑΑ είναι καθοριστικής σημασίας: θα αναπτυχθούν τυποποιημένες διαδικασίες και τεχνικές ικανότητες οι οποίες θα μπορούν να υποστηρίζουν τόσο τις μη στρατιωτικές όσο και τις στρατιωτικές αποστολές και επιχειρήσεις, καθώς και τις αντίστοιχες δομές δυνατότητας σχεδιασμού και διεξαγωγής επιχειρήσεων και τους παρόχους υπηρεσιών τεχνολογίας των πληροφοριών της ΕΥΕΔ. Για την προώθηση της συνεργασίας μεταξύ των κρατών μελών και την καλύτερη καθοδήγηση των προσπαθειών της ΕΕ στον εν λόγω τομέα, ο Ευρωπαϊκός Οργανισμός Άμυνας και η ΕΥΕΔ, σε συνεργασία με τις υπηρεσίες της Επιτροπής, θα διευκολύνουν τη στρατηγικού επιπέδου συμμετοχή των υπευθύνων χάραξης πολιτικής των κρατών μελών στον τομέα της άμυνας στον κυβερνοχώρο. Η ΕΕ θα στηρίξει παράλληλα την ανάπτυξη ευρωπαϊκών λύσεων ασφάλειας στον κυβερνοχώρο, στο πλαίσιο των προσπαθειών που καταβάλλει για τη δημιουργία ευρωπαϊκής βιομηχανικής και τεχνολογικής βάσης στον τομέα της άμυνας. Στη δράση αυτή περιλαμβάνεται επίσης η προώθηση περιφερειακών συνεργατικών σχηματισμών αριστείας στον τομέα της ασφάλειας και της άμυνας στον κυβερνοχώρο.

Έως το 2018, οι υπηρεσίες της Επιτροπής, σε στενή συνεργασία με την ΕΥΕΔ, τα κράτη μέλη και άλλους αρμόδιους οργανισμούς της ΕΕ, θα θέσουν σε εφαρμογή μια **πλατφόρμα κατάρτισης και εκπαίδευσης στον τομέα της άμυνας στον κυβερνοχώρο** για την αντιμετώπιση της υφιστάμενης έλλειψης δεξιοτήτων που παρατηρείται στον εν λόγω τομέα. Κατά τον τρόπο αυτό θα συμπληρωθούν οι εργασίες του Ευρωπαϊκού Οργανισμού Άμυνας στον συγκεκριμένο τομέα, μέσω της συμβολής στην αντιμετώπιση της υφιστάμενης έλλειψης δεξιοτήτων όσον αφορά την ασφάλεια και την άμυνα στον κυβερνοχώρο.

Βασικές δράσεις

- Πρωτοβουλία της Επιτροπής για τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία (αρχές του 2018).
- Άμεση έγκριση από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της πρότασης οδηγίας για την καταπολέμηση της απάτης και της.πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών.
- Προσθήκη απαιτήσεων σχετικά με το IPv6 στις δημόσιες συμβάσεις της ΕΕ και όσον αφορά τη χρηματοδότηση έρευνας και έργων. Σύναψη εθελοντικών συμφωνιών μεταξύ των κρατών μελών και των παρόχων υπηρεσιών διαδικτύου για την προώθηση της

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

υιοθέτησης του IPv6.
- Ανανέωση/επέκταση της έμφασης που δίνεται στο πλαίσιο της Ευρωπόλ στην εγκληματολογία στον κυβερνοχώρο και στην παρακολούθηση του σκοτεινού δικτύου.
- Εφαρμογή του πλαισίου κοινής διπλωματικής αντίδρασης της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.
- Παροχή ενισχυμένης οικονομικής στήριξης σε εθνικά και διεθνικά έργα για τη βελτίωση της ποινικής δικαιοσύνης στον κυβερνοχώρο.
- Δημιουργία, κατά τη διάρκεια του 2018, εκπαιδευτικής πλατφόρμας σχετικά με την ασφάλεια στον κυβερνοχώρο για την αντιμετώπιση της υφιστάμενης έλλειψης δεξιοτήτων στους τομείς της ασφάλειας και της άμυνας στον κυβερνοχώρο.

4. ΕΝΙΣΧΥΣΗ ΤΗΣ ΔΙΕΘΝΟΥΣ ΣΥΝΕΡΓΑΣΙΑΣ ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Με γνώμονα τις βασικές αξίες της ΕΕ και τα θεμελιώδη δικαιώματα, όπως η ελευθερία έκφρασης και το δικαίωμα στην προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα, καθώς και την προώθηση του ανοικτού, ελεύθερου και ασφαλούς κυβερνοχώρου, η διεθνής πολιτική της ΕΕ για την ασφάλεια στον κυβερνοχώρο έχει σχεδιαστεί με σκοπό, αφενός, την αντιμετώπιση της διαρκώς εξελισσόμενης πρόκλησης που συνιστά η προαγωγή της παγκόσμιας σταθερότητας στον κυβερνοχώρο και, αφετέρου, τη συμβολή στη στρατηγική αυτονομία της ΕΕ στον κυβερνοχώρο.

4.1 Η ασφάλεια στον κυβερνοχώρο στο πλαίσιο των εξωτερικών σχέσεων

Σύμφωνα με διαθέσιμα στοιχεία, άνθρωποι σε όλο τον κόσμο προσδιορίζουν τις κυβερνοεπιθέσεις από άλλες χώρες ως μία από τις σημαντικότερες απειλές για την εθνική ασφάλεια[83]. Λόγω του παγκόσμιου χαρακτήρα της απειλής, η δημιουργία και η διατήρηση ισχυρών συμμαχιών και εταιρικών σχέσεων με τρίτες χώρες είναι καίριας σημασίας για την πρόληψη και την αποτροπή επιθέσεων στον κυβερνοχώρο, οι οποίες μάλιστα διαδραματίζουν ολοένα κεντρικότερο ρόλο στο πλαίσιο της διεθνούς σταθερότητας και ασφάλειας. Στο πλαίσιο των διμερών, περιφερειακών και πολυμερών της δεσμεύσεων, η ΕΕ θα θέσει σε προτεραιότητα τη θέσπιση στρατηγικού πλαισίου για την πρόληψη των συγκρούσεων και τη σταθερότητα στον κυβερνοχώρο.

Η ΕΕ προωθεί σθεναρά τη θέση ότι στον κυβερνοχώρο εφαρμόζεται το διεθνές δίκαιο, και ειδικότερα ο Χάρτης των Ηνωμένων Εθνών. Συμπληρωματικά προς το δεσμευτικό διεθνές δίκαιο, η ΕΕ υιοθετεί τα πρότυπα, τους κανόνες και τις αρχές υπεύθυνης κρατικής συμπεριφοράς που είναι προαιρετικού, μη δεσμευτικού χαρακτήρα και έχουν διατυπωθεί από την ομάδα κυβερνητικών εμπειρογνωμόνων των Ηνωμένων Εθνών[84]· ενθαρρύνει επίσης την ανάπτυξη και την εφαρμογή περιφερειακών μέτρων δημιουργίας εμπιστοσύνης, τόσο στο πλαίσιο του Οργανισμού για την Ασφάλεια και τη Συνεργασία στην Ευρώπη όσο και σε άλλες περιοχές.

Σε διμερές επίπεδο, οι διάλογοι με θέμα τον κυβερνοχώρο[85] θα αναπτυχθούν περαιτέρω και θα πλαισιωθούν από προσπάθειες διευκόλυνσης της συνεργασίας με τρίτες χώρες, με σκοπό την ενίσχυση των αρχών δέουσας επιμέλειας και κρατικής ευθύνης στον κυβερνοχώρο. Στο

[83] Spring 2017 Global Attitudes Survey (Εαρινή έρευνα του 2017 σχετικά με τις παγκόσμιες θέσεις), Pew Research Centre.

[84] A/68/98 και A/70/174.

[85] Τον Σεπτέμβριο του 2017 η ΕΕ πραγματοποίησε διαλόγους με θέμα τον κυβερνοχώρο με τις ΗΠΑ, την Κίνα, την Ιαπωνία, τη Δημοκρατία της Κορέας και την Ινδία.

πλαίσιο των διεθνών της δεσμεύσεων, η ΕΕ θα θέσει σε προτεραιότητα ζητήματα διεθνούς ασφάλειας στον κυβερνοχώρο, λαμβάνοντας παράλληλα μέριμνα ώστε ότι η ασφάλεια στον κυβερνοχώρο να μην αποτελεί πρόσχημα για την προστασία της αγοράς και τον περιορισμό των θεμελιωδών δικαιωμάτων και ελευθεριών, συμπεριλαμβανομένης της ελευθερίας έκφρασης και της πρόσβασης σε πληροφορίες. Για την υιοθέτηση ολοκληρωμένης προσέγγισης όσον αφορά την ασφάλεια στον κυβερνοχώρο απαιτείται σεβασμός των ανθρωπίνων δικαιωμάτων, και η ΕΕ θα συνεχίσει να προασπίζει τις βασικές της αξίες παγκοσμίως, με γνώμονα τις κατευθυντήριες γραμμές της ΕΕ στον τομέα των ανθρωπίνων δικαιωμάτων για την ελευθερία στο διαδίκτυο[86]. Στο πλαίσιο αυτό, η ΕΕ τονίζει τη σημασία που έχει η συμμετοχή όλων των ενδιαφερόμενων μερών στη διακυβέρνηση του διαδικτύου.

Η Επιτροπή έχει επίσης υποβάλει πρόταση[87] για τον εκσυγχρονισμό των ελέγχων των εξαγωγών της ΕΕ, συμπεριλαμβανομένης της επιβολής ελέγχων στην εξαγωγή κρίσιμων τεχνολογιών κυβερνοεπιτήρησης οι οποίες θα μπορούσαν να προκαλέσουν παραβιάσεις των ανθρωπίνων δικαιωμάτων ή να χρησιμοποιηθούν σε βάρος της ίδιας της ασφάλειας της ΕΕ, και θα εντείνει τους διαλόγους με τρίτες χώρες για την προώθηση της σύγκλισης και της υπεύθυνης συμπεριφοράς σε παγκόσμιο επίπεδο στον εν λόγω τομέα.

4.2 Ανάπτυξη ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο

Η παγκόσμια ασφάλεια στον κυβερνοχώρο βασίζεται στην τοπική και εθνική ικανότητα όλων των χωρών να αποτρέπουν και να αντιδρούν σε περιστατικά στον κυβερνοχώρο, καθώς και να διεξάγουν έρευνες και να ασκούν διώξεις σε υποθέσεις τέλεσης εγκλημάτων στον κυβερνοχώρο. Η στήριξη των προσπαθειών για τη δημιουργία εθνικής ανθεκτικότητας σε τρίτες χώρες θα αυξήσει το παγκόσμιο επίπεδο ασφάλειας στον κυβερνοχώρο, με θετικές επιπτώσεις και για την ΕΕ. Για την αντιμετώπιση των ταχέως εξελισσόμενων απειλών στον κυβερνοχώρο χρειάζεται, αφενός, να καταβληθούν προσπάθειες σχετικά με την εκπαίδευση και την ανάπτυξη πολιτικών και νομοθεσίας και, αφετέρου, να λειτουργήσουν αποτελεσματικά σε όλες τις χώρες του πλανήτη τόσο ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική όσο και μονάδες καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

Από το 2013, η ΕΕ πρωταγωνιστεί στην ανάπτυξη διεθνών ικανοτήτων ασφάλειας στον κυβερνοχώρο και συνδέει συστηματικά τις προσπάθειες αυτές με τη συνεργασία της για την ανάπτυξη. Η ΕΕ θα συνεχίσει να υποστηρίζει ένα μοντέλο ανάπτυξης ικανοτήτων με βάση τα δικαιώματα, σύμφωνα με την προσέγγιση Digital4Development[88]. Όσον αφορά την ανάπτυξη ικανοτήτων, προτεραιότητα θα δοθεί στις γειτονικές χώρες της ΕΕ και στις αναπτυσσόμενες χώρες στις οποίες παρατηρείται ταχέως αναπτυσσόμενη συνδεσιμότητα και ταχεία ανάπτυξη απειλών. Οι προσπάθειες της ΕΕ θα πλαισιώσουν το αναπτυξιακό πρόγραμμα της ΕΕ με βάση το θεματολόγιο για τη βιώσιμη ανάπτυξη με ορίζοντα το 2030, καθώς και τις συνολικές προσπάθειες που καταβάλλονται για την ανάπτυξη θεσμικών ικανοτήτων.

Προκειμένου να βελτιωθεί η ικανότητα της ΕΕ όσον αφορά την κινητοποίηση της συλλογικής εμπειρογνωμοσύνης της για τη στήριξη της εν λόγω ανάπτυξης ικανοτήτων, θα πρέπει να δημιουργηθεί ειδικό δίκτυο ανάπτυξης ικανοτήτων της ΕΕ στον τομέα του κυβερνοχώρου, με τη συμμετοχή της ΕΥΕΔ, των αρμόδιων αρχών των κρατών μελών σε θέματα του κυβερνοχώρου, των οργανισμών της ΕΕ, των υπηρεσιών της Επιτροπής, της ακαδημαϊκής κοινότητας και της κοινωνίας των πολιτών. Θα καταρτιστούν κατευθυντήριες

[86] Κατευθυντήριες γραμμές της ΕΕ στον τομέα των ανθρωπίνων δικαιωμάτων για την ελευθερία της έκφρασης εντός και εκτός διαδικτύου.
[87] COM(2016) 616.
[88] SWD(2017) 157.

γραμμές για την ανάπτυξη ικανοτήτων της ΕΕ στον τομέα του κυβερνοχώρου, οι οποίες θα συμβάλουν στη βελτίωση της πολιτικής καθοδήγησης και της ιεράρχησης των προσπαθειών της ΕΕ κατά την παροχή βοήθειας σε τρίτες χώρες.

Επιπλέον, η ΕΕ θα συνεργαστεί με άλλους χορηγούς στον συγκεκριμένο τομέα προκειμένου να αποφευχθεί η αλληλεπικάλυψη των προσπαθειών και να διευκολυνθεί η καλύτερη στοχοθέτηση της ανάπτυξης ικανοτήτων στις διάφορες περιοχές.

4.3 Συνεργασία ΕΕ-NATO

Αξιοποιώντας τη σημαντική πρόοδο που έχει ήδη επιτευχθεί, η ΕΕ θα εμβαθύνει τη συνεργασία μεταξύ της ΕΕ και του NATO στον τομέα της ασφάλειας στον κυβερνοχώρο, των υβριδικών απειλών και της άμυνας, όπως προβλέπεται στην κοινή δήλωση της 8ης Ιουλίου 2016[89]. Στις σχετικές προτεραιότητες περιλαμβάνονται η προώθηση της διαλειτουργικότητας μέσω της θέσπισης συνεκτικών απαιτήσεων και προτύπων για την άμυνα στον κυβερνοχώρο, η ενίσχυση της συνεργασίας στον τομέα της κατάρτισης και των ασκήσεων, καθώς και η εναρμόνιση των απαιτήσεων κατάρτισης.

Η ΕΕ και το NATO θα προωθήσουν επίσης τη συνεργασία τους σε επίπεδο έρευνας και καινοτομίας στον τομέα της άμυνας στον κυβερνοχώρο, ενώ θα αξιοποιήσουν τις ισχύουσες τεχνικές ρυθμίσεις για την ανταλλαγή πληροφοριών στον τομέα της ασφάλειας στον κυβερνοχώρο μεταξύ των αντίστοιχων οργάνων τους που είναι αρμόδια για την ασφάλεια στον κυβερνοχώρο[90]. Οι πρόσφατες κοινές προσπάθειες καταπολέμησης των υβριδικών απειλών, ιδίως η συνεργασία μεταξύ της Μονάδας Ανάλυσης Υβριδικών Απειλών της ΕΕ και της Υπηρεσίας Ανάλυσης Υβριδικών Απειλών του NATO, θα πρέπει να αξιοποιηθούν περαιτέρω για την ενίσχυση της ανθεκτικότητας και της αντιμετώπισης κρίσεων στον κυβερνοχώρο. Θα προαχθεί η περαιτέρω συνεργασία μεταξύ της ΕΕ και του NATO μέσω ασκήσεων στον τομέα της άμυνας στον κυβερνοχώρο, με τη συμμετοχή της ΕΥΕΔ και άλλων οντοτήτων της ΕΕ και σχετικών ομόλογων οργάνων του NATO, συμπεριλαμβανομένου του Συνεργατικού Κέντρου Αριστείας του NATO για την Άμυνα στον Κυβερνοχώρο που βρίσκεται στο Τάλιν. Για πρώτη φορά, το NATO και η ΕΕ θα διεξαγάγουν παράλληλες και συντονισμένες ασκήσεις στο πλαίσιο σεναρίου υβριδικής απειλής· πρώτο θα ξεκινήσει το NATO το 2017 και θα ακολουθήσει στα βήματά του η ΕΕ το 2018. Η επόμενη έκθεση σχετικά με τη συνεργασία ΕΕ-NATO, η οποία θα υποβληθεί στα αντίστοιχα Συμβούλια τον Δεκέμβριο του 2017, θα αποτελέσει ευκαιρία για την εξέταση των δυνατοτήτων περαιτέρω επέκτασης της συνεργασίας, κυρίως μέσω της εξασφάλισης κοινών, ασφαλών και αξιόπιστων μέσων επικοινωνίας μεταξύ όλων των συμμετεχόντων αρμόδιων θεσμικών οργάνων και οργανισμών, συμπεριλαμβανομένου του ENISA.

Βασικές δράσεις

- Προώθηση του στρατηγικού πλαισίου για τη πρόληψη των συγκρούσεων και τη σταθερότητα στον κυβερνοχώρο.
- Δημιουργία νέου δικτύου ανάπτυξης ικανοτήτων για τη στήριξη της ικανότητας τρίτων χωρών να αντιμετωπίζουν απειλές στον κυβερνοχώρο και κατάρτιση κατευθυντήριων γραμμών της ΕΕ για την ανάπτυξη ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο με σκοπό την καλύτερη ιεράρχηση των προσπαθειών της ΕΕ.

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

[90] CERT-ΕΕ και Ικανότητα Αντιμετώπισης Συμβάντων Πληροφορικής του NATO (NCIRC).

- Εμβάθυνση της συνεργασίας μεταξύ της ΕΕ και του ΝΑΤΟ, συμπεριλαμβανομένης της συμμετοχής σε παράλληλες και συντονισμένες ασκήσεις και της ενίσχυσης της διαλειτουργικότητας των προτύπων ασφάλειας στον κυβερνοχώρο.

5. ΣΥΜΠΕΡΑΣΜΑ

Η ετοιμότητα της ΕΕ στον κυβερνοχώρο είναι καίριας σημασίας, τόσο για την ψηφιακή ενιαία αγορά όσο και για την Ευρωπαϊκή Ένωση Ασφάλειας και Άμυνας. Η ενίσχυση της ευρωπαϊκής ασφάλειας στον κυβερνοχώρο και η αντιμετώπιση των απειλών κατά στρατιωτικών και μη στρατιωτικών στόχων συνιστούν πλέον επιτακτική ανάγκη.

Η επικείμενη ψηφιακή σύνοδος κορυφής, η οποία διοργανώνεται από την εσθονική Προεδρία στις 29 Σεπτεμβρίου 2017, παρέχει τη δυνατότητα να επιδειχθεί κοινή αποφασιστικότητα για την τοποθέτηση της ασφάλειας στον κυβερνοχώρο στο επίκεντρο της ΕΕ ως ψηφιακής κοινωνίας. Στο πλαίσιο αυτής της κοινής δέσμευσης, η Επιτροπή καλεί τα κράτη μέλη να δεσμευτούν ως προς τον τρόπο με τον οποίο προτίθενται να ενεργήσουν σε τομείς κύριας ευθύνης τους. Θα πρέπει να συμπεριληφθεί η ενίσχυση της ασφάλειας στον κυβερνοχώρο μέσω των ακόλουθων ενεργειών:

- διασφάλιση της πλήρους και αποτελεσματικής εφαρμογής της οδηγίας ΑΔΠ έως τις 9 Μαΐου 2018, καθώς και των πόρων που απαιτούνται ώστε οι αρμόδιες δημόσιες αρχές για την ασφάλεια στον κυβερνοχώρο να είναι σε θέση να εκτελούν τα καθήκοντά τους με αποτελεσματικό τρόπο·
- εφαρμογή των ίδιων κανόνων στις δημόσιες διοικήσεις, δεδομένου του ρόλου που διαδραματίζουν στην κοινωνία και την οικονομία συνολικά·
- παροχή κατάρτισης σχετικά με την ασφάλεια στον κυβερνοχώρο για τη δημόσια διοίκηση·
- απόδοση προτεραιότητας στην ευαισθητοποίηση σχετικά με τον κυβερνοχώρο στις εκστρατείες ενημέρωσης και ένταξη της ασφάλειας στον κυβερνοχώρο στα ακαδημαϊκά προγράμματα σπουδών και στα προγράμματα επαγγελματικής κατάρτισης·
- χρήση πρωτοβουλιών σχετικά με τη «μόνιμη διαρθρωμένη συνεργασία» (PESCO) και το Ευρωπαϊκό Ταμείο Άμυνας για την υποστήριξη της ανάπτυξης έργων στον τομέα της άμυνας στον κυβερνοχώρο.

Στην παρούσα κοινή ανακοίνωση παρουσιάζεται το μέγεθος της πρόκλησης και το φάσμα των μέτρων που μπορεί να λάβει η ΕΕ. Χρειαζόμαστε μια ανθεκτική Ευρώπη η οποία να μπορεί να προστατεύει αποτελεσματικά τους πολίτες της με την πρόβλεψη πιθανών περιστατικών ασφάλειας στον κυβερνοχώρο, την ενσωμάτωση ισχυρών μηχανισμών προστασίας στις δομές και τη συμπεριφορά της, την ταχεία ανάκαμψη από οποιαδήποτε επίθεση στον κυβερνοχώρο, καθώς και με την αποτροπή όσων σχεδιάζουν τέτοιες επιθέσεις. Στην παρούσα ανακοίνωση προτείνονται στοχευμένα μέτρα τα οποία θα ενισχύσουν περαιτέρω, με συντονισμένο τρόπο, τις δομές και τις ικανότητες της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο, με την πλήρη συνεργασία των κρατών μελών και των διαφόρων σχετικών δομών της ΕΕ, ενώ θα γίνονται παράλληλα σεβαστές οι αρμοδιότητες και οι ευθύνες τους. Με την εφαρμογή της παρούσας ανακοίνωσης θα καταδειχθεί με σαφήνεια ότι η ΕΕ και τα κράτη μέλη θα συνεργαστούν για την εφαρμογή ενός προτύπου ασφάλειας στον κυβερνοχώρο το οποίο θα ανταποκρίνεται πλήρως στις συνεχώς αυξανόμενες προκλήσεις με τις οποίες βρίσκεται αντιμέτωπη σήμερα η Ευρώπη.