ΕΥΡΩΠΑΪΚΟ
ΕΛΕΓΚΤΙΚΟ
ΣΥΝΕΔΡΙΟ

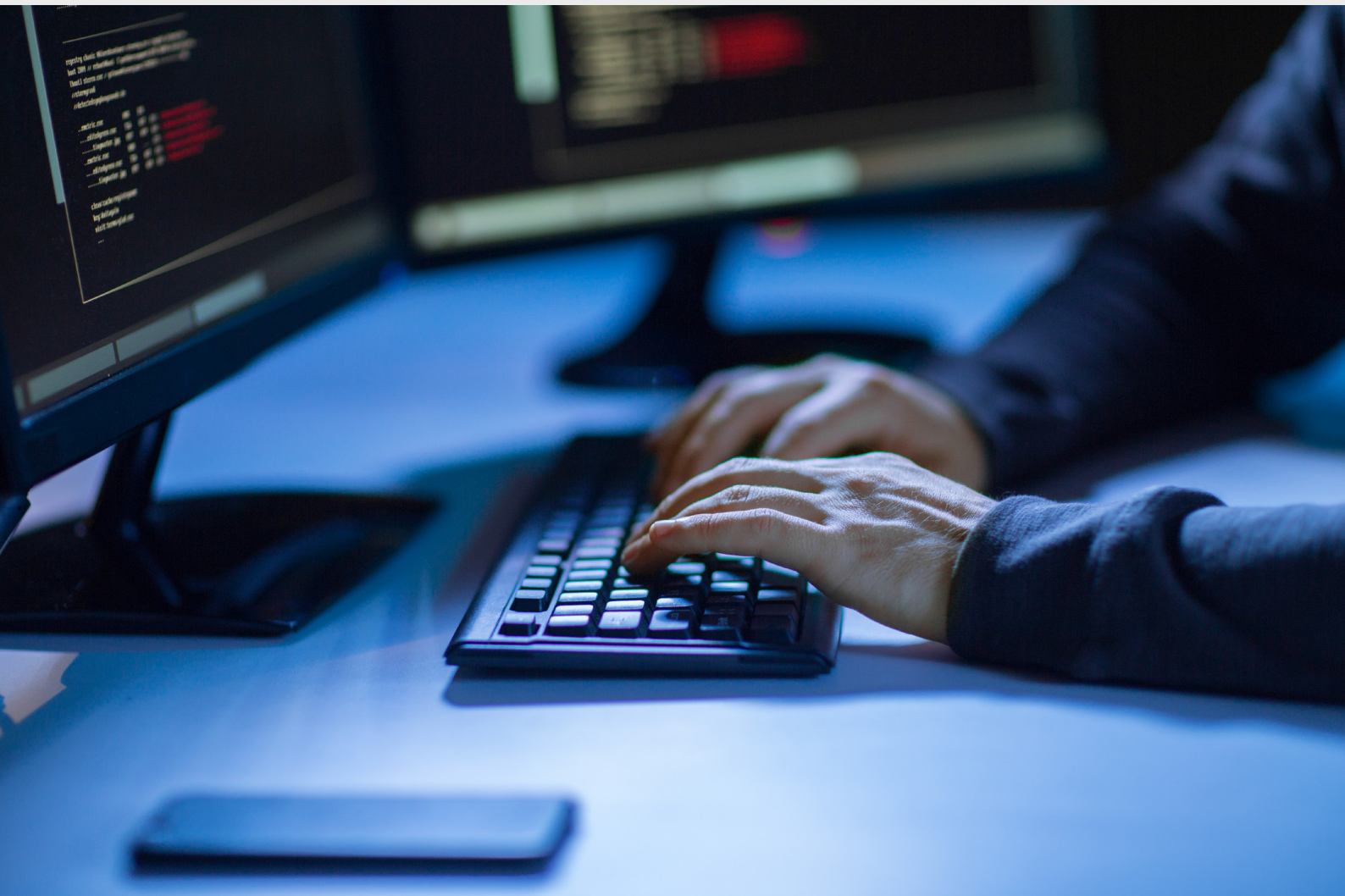
EL

2019

Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια

Ενημερωτικό έγγραφο

Μάρτιος 2019



Τι πραγματεύεται το έγγραφο:

Σκοπός του παρόντος ενημερωτικού εγγράφου, το οποίο δεν συνιστά έκθεση ελέγχου, είναι η επισκόπηση του πολύπλοκου τοπίου της ενωσιακής πολιτικής για την κυβερνοασφάλεια και ο προσδιορισμός των κυριότερων προκλήσεων για την αποτελεσματική εφαρμογή της. Καλύπτει την ασφάλεια δικτύων και πληροφοριών, το κυβερνοέγκλημα, την κυβερνοάμυνα και την παραπληροφόρηση. Θα χρησιμεύσει επίσης ως βάση τυχόν μελλοντικών ελεγκτικών εργασιών στον τομέα αυτό.

Η ανάλυσή μας βασίστηκε στην επισκόπηση δημόσια διαθέσιμων πληροφοριών που περιέχονται σε επίσημα έγγραφα, έγγραφα θέσης και μελέτες τρίτων. Οι επιτόπιες εργασίες μας πραγματοποιήθηκαν μεταξύ Απριλίου και Σεπτεμβρίου 2018, και ελήφθησαν υπόψη οι εξελίξεις μέχρι τον Δεκέμβριο του 2018. Οι εργασίες μας συμπληρώθηκαν με έρευνα που πραγματοποιήσαμε μεταξύ των ανώτατων οργάνων ελέγχου των κρατών μελών και με συνεντεύξεις με πρόσωπα σε θέσεις κλειδιά στα ενωσιακά θεσμικά όργανα, καθώς και με εκπροσώπους του ιδιωτικού τομέα.

Οι προκλήσεις που εντοπίσαμε εμπίπτουν σε τέσσερις ευρείες κατηγορίες: i) πλαίσιο πολιτικής· ii) χρηματοδότηση και δαπάνες· iii) ενίσχυση της κυβερνοανθεκτικότητας· iv) αποτελεσματική αντίδραση σε κυβερνοπεριστατικά. Παραμένει επιτακτική η ανάγκη επίτευξης υψηλότερου επιπέδου κυβερνοασφάλειας στην ΕΕ. Για τον λόγο αυτό, στο τέλος κάθε κεφαλαίου παραθέτουμε μια σειρά ιδεών για περαιτέρω επεξεργασία από τους υπεύθυνους για τη χάραξη πολιτικής, τους νομοθέτες και τους επαγγελματίες των σχετικών κλάδων.

Θα θέλαμε να ευχαριστήσουμε για την εποικοδομητική ανατροφοδότηση που μας παρείχαν τις υπηρεσίες της Επιτροπής, την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, το Συμβούλιο της Ευρωπαϊκής Ένωσης, τον ENISA, την Ευρωπόλ, τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο και τα ανώτατα όργανα ελέγχου των κρατών μελών.

Περιεχομενα

Κλιμάκιο του ΕΕΣ

Σύνοψη

I Η τεχνολογία ανοίγει νέους ορίζοντες ευκαιριών, με τα νέα προϊόντα και τις νέες υπηρεσίες να γίνονται αναπόσπαστο μέρος της καθημερινής μας ζωής. Από την άλλη, όμως, εντείνεται ο κίνδυνος κυβερνοεγκληματικότητας ή κυβερνοεπιθέσεων, ο κοινωνικός και οικονομικός αντίκτυπος των οποίων κλιμακώνεται συνεχώς. Η πρόσφατη εντατικοποίηση, από το 2017, των προσπαθειών της ΕΕ για την ενίσχυση της κυβερνοασφάλειας και της ψηφιακής αυτονομίας της ήρθε σε μια κρίσιμη συγκυρία.

II Επιδίωξη του παρόντος ενημερωτικού σημειώματος, το οποίο δεν συνιστά έκθεση ελέγχου και βασίζεται σε δημόσια διαθέσιμες πληροφορίες, είναι η παροχή μιας συνολικής εικόνας του σύνθετου και άνισου τοπίου στον συγκεκριμένο τομέα πολιτικής και ο προσδιορισμός των βασικών προκλήσεων για την αποτελεσματική εφαρμογή της πολιτικής. Το έγγραφό μας καλύπτει την πολιτική της ΕΕ για την κυβερνοασφάλεια, καθώς και την κυβερνοεγκληματικότητα και την κυβερνοάμυνα, και επίσης τις προσπάθειες για την καταπολέμηση της παραπληροφόρησης. Οι προκλήσεις που εντοπίσαμε κατατάσσονται σε τέσσερις ευρείες κατηγορίες: i) πλαίσιο πολιτικής και νομοθετικό πλαίσιο· ii) χρηματοδότηση και δαπάνες· iii) ενίσχυση της κυβερνοανθεκτικότητας· iv) αποτελεσματική αντίδραση σε κυβερνοπεριστατικά. Κάθε κεφάλαιο περιλαμβάνει ορισμένα σημεία προβληματισμού σχετικά με τις προκλήσεις που παρουσιάζονται.

Πλαίσιο πολιτικής και νομοθετικό πλαίσιο

III Ελλείψει μετρήσιμων στόχων και επαρκών, αξιόπιστων δεδομένων, η ανάπτυξη δράσεων που να ανταποκρίνονται στην απώτερη επιδίωξη της στρατηγικής της ΕΕ για την κυβερνοασφάλεια να καταστεί το ασφαλέστερο παγκοσμίως ψηφιακό περιβάλλον αποτελεί πρόκληση. Τα επακόλουθα σπανίως μετρούνται και αξιολογήσεις έχουν πραγματοποιηθεί σε ελάχιστους τομείς πολιτικής. Βασική πρόκληση συνιστά επομένως **η διασφάλιση ουσιαστικής λογοδοσίας και αξιολόγησης** με τη στροφή προς μια νοοτροπία επιδόσεων, αναπόσπαστο μέρος της οποίας θα αποτελούν πρακτικές αξιολόγησης.

IV Το νομοθετικό πλαίσιο δεν έχει ακόμη ολοκληρωθεί. **Τα κενά που εμφανίζει η ενωσιακή νομοθεσία, σε συνδυασμό με την ασυνεπή μεταφορά της στο εθνικό δίκαιο των κρατών μελών,** μπορούν να δυσχεράνουν την πλήρη εφαρμογή της.

Χρηματοδότηση και δαπάνες

V **Η ευθυγράμμιση του επιπέδου των επενδύσεων με τους στόχους** αποτελεί πρόκληση: απαιτείται όχι μόνο αύξηση των συνολικών επενδύσεων στην κυβερνοασφάλεια –που στην ΕΕ μέχρι στιγμής είναι χαμηλές και κατακερματισμένες– αλλά και κλιμάκωση του αντικτύπου, ιδίως όσον αφορά την καλύτερη αξιοποίηση των αποτελεσμάτων των δαπανών για την έρευνα και τη διασφάλιση της αποτελεσματικής στόχευσης και χρηματοδότησης νεοφυών επιχειρήσεων.

VI **Η ύπαρξη σαφούς συνολικής εικόνας των δαπανών της ΕΕ** είναι αναγκαία προκειμένου τόσο η ΕΕ όσο και τα κράτη μέλη της να γνωρίζουν ποια κενά πρέπει να καλυφθούν προκειμένου να υλοποιηθούν οι στόχοι που έχουν θέσει. Ελλείψει ειδικού προϋπολογισμού της ΕΕ για τη χρηματοδότηση της στρατηγικής για την κυβερνοασφάλεια, δεν υπάρχει σαφής εικόνα του ύψους των πόρων και του τρόπου με τον οποίο αυτοί διατίθενται.

VII Σε μια εποχή κατά την οποία η σημασία των πολιτικών προτεραιοτήτων που επικεντρώνονται στην ασφάλεια αυξάνεται, **οι περιορισμοί που αντιμετωπίζουν οι δραστηριοποιούμενοι στο πεδίο του κυβερνοχώρου οργανισμοί της ΕΕ όσον αφορά την εξασφάλιση πόρων** ενδέχεται να μην επιτρέψουν την υλοποίηση των φιλόδοξων στόχων της ΕΕ. Για την αντιμετώπιση της πρόκλησης αυτής θα χρειαστεί να αναζητηθούν τρόποι προσέλκυσης και διατήρησης ταλέντων.

Ενίσχυση της κυβερνοανθεκτικότητας

VIII Η διακυβέρνηση της κυβερνοασφάλειας, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, στην ΕΕ και διεθνώς, εμφανίζει πληθώρα αδυναμιών. Το γεγονός αυτό υπονομεύει, αφενός, την ικανότητα της παγκόσμιας κοινότητας να αντιδρά σε κυβερνοεπιθέσεις και να τις περιορίζει και, αφετέρου, την εφαρμογή μιας συνεκτικής προσέγγισης σε επίπεδο ΕΕ. Επομένως, η πρόκληση συνίσταται στην **ενίσχυση της διακυβέρνησης της κυβερνοασφάλειας**.

IX Δεδομένου δε του αυξανόμενου ελλείμματος δεξιοτήτων συνολικά στον τομέα της κυβερνοασφάλειας, αποκτά ουσιώδη σημασία η **ενίσχυση των σχετικών δεξιοτήτων και η αύξηση της ενημέρωσης και της ευαισθητοποίησης**. Επί του παρόντος, είναι ελάχιστα τα πανευρωπαϊκά πρότυπα για την εκπαίδευση, την πιστοποίηση ή τις εκτιμήσεις κινδύνου σε σχέση με την κυβερνοασφάλεια.

X Αναγκαίο για την ενίσχυση συνολικά της κυβερνοανθεκτικότητας είναι να δημιουργηθούν προϋποθέσεις εμπιστοσύνης. Η ίδια η Επιτροπή έχει εκτιμήσει ότι ο

συντονισμός γενικά παραμένει ανεπαρκής. Πρόκληση συνιστά και η **βελτίωση της ανταλλαγής πληροφοριών και του συντονισμού** μεταξύ του δημόσιου και του ιδιωτικού τομέα.

Αποτελεσματική αντίδραση σε κυβερνοπεριστατικά

XI Λόγω της αυξανόμενης πολυπλοκότητας των ψηφιακών συστημάτων, είναι αδύνατη η αποτροπή όλων των επιθέσεων. Η απάντηση στην πρόκληση αυτή είναι η **ταχεία ανίχνευση και αντίδραση**. Ωστόσο, η κυβερνοασφάλεια δεν έχει ενσωματωθεί ακόμη πλήρως στους υφιστάμενους σε ενωσιακό επίπεδο μηχανισμούς για την αντιμετώπιση κρίσεων, γεγονός που δυνητικά περιορίζει την ικανότητα της ΕΕ να αντιδρά σε διασυνοριακά κυβερνοπεριστατικά μεγάλης κλίμακας.

XII Καίρια είναι η σημασία της **προστασίας των υποδομών ζωτικής σημασίας και των κοινωνικών λειτουργιών**. Το ενδεχόμενο παρεμβάσεων σε εκλογικές διαδικασίες και πραγματοποίησης εκστρατειών παραπληροφόρησης συνιστά σημαντική πρόκληση.

XIII Οι προκλήσεις που θέτουν σήμερα οι κυβερνοαπειλές που αντιμετωπίζει η ΕΕ και ο κόσμος γενικότερα καθιστούν αναγκαία την σταθερή προσήλωση στις θεμελιώδεις αξίες της ΕΕ και την απαρέγκλιτη τήρησή τους.

Εισαγωγή

01 Η τεχνολογία δημιουργεί πληθώρα νέων ευκαιριών. Τα νέα προϊόντα και οι νέες υπηρεσίες που λανσάρονται γίνονται αναπόσπαστο κομμάτι της καθημερινής ζωής μας. Ωστόσο, με κάθε νέα εξέλιξη, η εξάρτησή μας από την τεχνολογία αυξάνεται, όπως αυξάνεται και η σημασία της κυβερνοασφάλειας. Όσο περισσότερα δεδομένα προσωπικού χαρακτήρα αναρτούμε στο διαδίκτυο και όσο περισσότερο είμαστε συνδεδεμένοι σε αυτό, τόσο αυξάνονται οι πιθανότητες να πέσουμε θύματα κυβερνοεγκλήματος ή κυβερνοεπίθεσης.

Τι είναι η κυβερνοασφάλεια;

02 Δεν υπάρχει τυποποιημένος, καθολικά αποδεκτός ορισμός της κυβερνοασφάλειας[1]. Ο όρος αυτός σε γενικές γραμμές καλύπτει το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών και των χρηστών τους έναντι μη εξουσιοδοτημένης πρόσβασης, επιθέσεων και ζημίας, ώστε να εξασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων.

03 Η κυβερνοασφάλεια καλύπτει την πρόληψη και την ανίχνευση κυβερνοπεριστατικών, την αντίδραση σε αυτά και την ανάκαμψη από αυτά. Τα περιστατικά μπορεί να είναι εσκεμμένα ή μη και κυμαίνονται, ενδεικτικά, από την τυχαία κοινολόγηση πληροφοριών έως επιθέσεις κατά επιχειρήσεων και υποδομών ζωτικής σημασίας και την κλοπή δεδομένων προσωπικού χαρακτήρα, ή ακόμη και έως την παρέμβαση σε δημοκρατικές διαδικασίες. Όλα αυτά τα συμβάντα μπορούν να έχουν πολυποίκιλες επιζήμιες επιδράσεις σε πρόσωπα, οργανισμούς και κοινότητες.

04 Όπως χρησιμοποιείται στους πολιτικούς κύκλους της ΕΕ, ο όρος «κυβερνοασφάλεια» δεν καλύπτει μόνο την ασφάλεια δικτύων και πληροφοριών, αλλά και κάθε παράνομη δραστηριότητα με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Ως εκ τούτου, μπορεί να περιλαμβάνει κυβερνοεγκλήματα όπως την εξαπόλυση επιθέσεων με ιούς υπολογιστών ή την απάτη με μέσα πληρωμής πλην των μετρητών και να αφορά τόσο συστήματα όσο και περιεχόμενο, καθώς και τη διάδοση υλικού σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο. Μπορεί επίσης να καλύπτει εκστρατείες παραπληροφόρησης για την άσκηση επιρροής στον διαδικτυακό διάλογο και υπόνοιες για παρέμβαση σε εκλογικές διαδικασίες. Επιπλέον, η Ευρωπόλ θεωρεί ότι υπάρχει σύγκλιση μεταξύ κυβερνοεγκλήματος και τρομοκρατίας[2].

05 Διάφοροι παράγοντες –μεταξύ άλλων, κράτη, εγκληματικές ομάδες και ακτιβιστές χάκερ– ωθούμενοι από διαφορετικά κίνητρα, προκαλούν κυβερνοπεριστατικά, των οποίων ο αντίκτυπος γίνεται αισθητός σε εθνικό, ευρωπαϊκό ή και διεθνές ακόμη επίπεδο. Εντούτοις, η άυλη και, σε μεγάλο βαθμό, χωρίς σύνορα φύση του διαδικτύου, καθώς και τα εργαλεία και οι τακτικές που χρησιμοποιούνται, συχνά καθιστούν δυσχερή τον εντοπισμό του δράστη μιας επίθεσης (πρόκειται για το επονομαζόμενο «πρόβλημα απόδοσης ευθυνών»).

06 Τα διάφορα είδη απειλών για την κυβερνοασφάλεια μπορούν να ταξινομηθούν είτε σύμφωνα με αυτό που προκαλούν στα δεδομένα –κοινολόγηση, τροποποίηση, καταστροφή ή άρνηση πρόσβασης– είτε σύμφωνα με τις βασικές αρχές ασφάλειας των πληροφοριών που παραβιάζουν, όπως παρουσιάζεται στο ***γράφημα 1*** κατωτέρω. Ορισμένα παραδείγματα επιθέσεων περιγράφονται στο ***πλαίσιο 1***. Αντιστρόφως ανάλογη της αυξανόμενης πολυπλοκότητας των επιθέσεων που εξαπολύονται κατά των συστημάτων πληροφοριών είναι η αποτελεσματικότητα των αμυντικών μηχανισμών μας[3].

Γράφημα 1 – Τα είδη απειλών και οι αρχές ασφάλειας που θέτουν σε κίνδυνο

Πηγή: ΕΕΣ· τροποποιήθηκε από μελέτη του Ευρωπαϊκού Κοινοβουλίου[4]. Λουκέτο = χωρίς αντίκτυπο στην ασφάλεια. Θαυμαστικό = η ασφάλεια σε κίνδυνο.

Πλαίσιο 1

Τα είδη των κυβερνοεπιθέσεων

Κάθε φορά που μια νέα συσκευή συνδέεται στο διαδίκτυο ή με άλλες συσκευές, η λεγόμενη «επιφάνεια επίθεσης» αυξάνεται. Η εκθετική ανάπτυξη του διαδικτύου των πραγμάτων, του υπολογιστικού νέφους, των μαζικών δεδομένων και η ψηφιοποίηση της βιομηχανίας συνοδεύονται από αυξημένη έκθεση των τρωτών σημείων, που παρέχει σε κακόβουλους παράγοντες τη δυνατότητα να στοχεύουν ολοένα και περισσότερα θύματα. Η ποικιλία των ειδών επιθέσεων και η αυξανόμενη πολυπλοκότητά τους δυσχεραίνει εξαιρετικά την παρακολούθηση των εξελίξεων[5].

Το **κακόβουλο λογισμικό** (malware) σχεδιάζεται για να προκαλέσει βλάβες σε συσκευές ή δίκτυα. Μπορεί να περιλαμβάνει ιούς, Δούρειους ίππους, λυτρισμικό, λογισμικά σκουλήκια, προγράμματα διαφημίσεων και κατασκοπευτικό λογισμικό. Το **λυτρισμικό** (ransomware) κρυπτογραφεί τα δεδομένα, εμποδίζοντας την πρόσβαση των χρηστών στα αρχεία τους έως ότου καταβληθούν λύτρα, συνήθως σε κρυπτονόμισμα, ή γίνει κάποια ενέργεια. Σύμφωνα με την Ευρωπόλ, οι επιθέσεις με λυτρισμικό είναι οι συνηθέστερες σε όλους τους τομείς, και τα είδη λυτρισμικού γνώρισαν πρωτοφανή αύξηση στον αριθμό τα τελευταία χρόνια. Αύξηση σημειώνουν επίσης οι επιθέσεις **κατανεμημένης άρνησης υπηρεσίας** (Distributed Denial of Service – DDoS), οι οποίες καθιστούν μη διαθέσιμες υπηρεσίες και πόρους κατακλύζοντάς τους με περισσότερα αιτήματα από όσα μπορούν να διαχειριστούν. Ένα τρίτο των οργανισμών αντιμετώπισε επιθέσεις αυτού του είδους το 2017[6].

Οι χρήστες μπορούν να χειραγωγηθούν ώστε να εκτελέσουν εν αγνοία τους μια ενέργεια ή να καταχωρίσουν εμπιστευτικές πληροφορίες. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για κλοπή δεδομένων ή κυβερνοκατασκοπεία, και είναι γνωστή ως **κοινωνική μηχανική** (social engineering). Αυτό επιτυγχάνεται με διάφορους τρόπους. Μια συνηθισμένη μέθοδος είναι το **ηλεκτρονικό «ψάρεμα»** (phishing). Ο χρήστης λαμβάνει ηλεκτρονικό μήνυμα που μοιάζει να προέρχεται από αξιόπιστη πηγή, σκοπός του οποίου είναι να παραπλανηθεί ώστε να αποκαλύψει πληροφορίες ή να κάνει κλικ σε συνδέσμους που θα μολύνουν τις συσκευές με κακόβουλο λογισμικό. Περισσότερα από τα μισά κράτη μέλη ανέφεραν έρευνες για δικτυακές επιθέσεις[7].

Τα πιο ειδεχθή ίσως είδη απειλών είναι οι **προηγμένες συνεχείς απειλές** (advanced persistent threats, APTs). Πρόκειται για πολύπλοκες επιθέσεις που περιλαμβάνουν μακρόχρονη παρακολούθηση και κλοπή δεδομένων και σε ορισμένες περιπτώσεις έχουν σκοπό και την πρόκληση μεγάλων ζημιών. Το ζητούμενο στην περίπτωσή τους είναι να μην εντοπιστούν για όσο το δυνατόν μεγαλύτερο διάστημα. Οι απειλές αυτές συχνά συνδέονται με δράση κρατικών υπηρεσιών και έχουν στόχο ιδιαίτερα ευαίσθητους τομείς όπως η τεχνολογία, η άμυνα και οι υποδομές ζωτικής σημασίας. Η κυβερνοκατασκοπεία θεωρείται πως αντιπροσωπεύει τουλάχιστον το ένα τέταρτο του συνόλου των κυβερνοπεριστατικών και έχει το μεγαλύτερο κόστος[8].

Πόσο σοβαρό είναι το πρόβλημα;

07 Λόγω της έλλειψης αξιόπιστων στοιχείων, είναι δύσκολο να μετρηθεί ο αντίκτυπος της ανεπαρκούς προετοιμασίας για κυβερνοεπιθέσεις. Ο οικονομικός αντίκτυπος της κυβερνοεγκληματικότητας πενταπλασιάστηκε μεταξύ του 2013 και του 2017[9], πλήττοντας κυβερνήσεις και επιχειρήσεις, ανεξαρτήτως μεγέθους. Ενδεικτική της τάσης αυτής είναι η πρόβλεψη για αύξηση των κυβερνοασφαλίστρων από 3 δισεκατομμύρια ευρώ το 2018 σε 8,9 δισεκατομμύρια ευρώ το 2020.

08 Ενώ ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων συνεχίζει να αυξάνεται, είναι εξαιρετικά ανησυχητική η απόκλιση μεταξύ του κόστους της εξαπόλυσης μιας επίθεσης και του κόστους της πρόληψης, της διερεύνησης και της αποκατάστασης της βλάβης. Παραδείγματος χάριν, μια επίθεση DDoS μπορεί να κοστίσει ακόμη και μόλις 15 ευρώ τον μήνα, ενώ οι ζημίες για τις επιχειρήσεις-στόχο, συμπεριλαμβανομένης της προσβολής της φήμης τους, είναι σημαντικά υψηλότερες[10].

09 Μολονότι το 80 % των επιχειρήσεων της ΕΕ βίωσε τουλάχιστον ένα περιστατικό κυβερνοασφάλειας το 2016[11], η αναγνώριση των κινδύνων παραμένει σε ανησυχητικά χαμηλά επίπεδα. Ποσοστό 69 % των επιχειρήσεων της ΕΕ αγνοεί ή κατανοεί ελάχιστα τους κινδύνους στους οποίους εκτίθεται στον κυβερνοχώρο[12] και ποσοστό 60 % δεν έχει ποτέ προβεί σε εκτίμηση των δυνητικών οικονομικών ζημιών[13]. Επιπλέον, σύμφωνα με παγκόσμια έρευνα, το ένα τρίτο των οργανισμών θα προτιμούσε να καταβάλει τα λύτρα παρά να πραγματοποιήσει επενδύσεις στην ασφάλεια πληροφοριών[14].

10 Από κοινού, οι επιθέσεις με το λυτρισμικό *WannaCry* και το κακόβουλο λογισμικό διαγραφής δεδομένων (wiper) *NotPetya* το 2017 είχαν περισσότερα από 320 000 θύματα σε περίπου 150 χώρες[15]. Οι επιθέσεις αυτές είχαν ως αποτέλεσμα την αφύπνιση της παγκόσμιας κοινότητας σχετικά με την απειλή που συνιστούν οι κυβερνοεπιθέσεις, δημιουργώντας νέα δυναμική για την ενσωμάτωση της διάστασης της κυβερνοασφάλειας στον επίσημο σχεδιασμό πολιτικής. Πλέον, μάλιστα, ποσοστό 86 % των πολιτών της ΕΕ πιστεύει ότι ο κίνδυνος να πέσουν θύματα κυβερνοεγκλήματος αυξάνεται[16].

Η δράση της ΕΕ στον τομέα της κυβερνοασφάλειας

11 Η ΕΕ προσχώρησε στη σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο το 2001[17] (Σύμβαση της Βουδαπέστης) ως οργανισμός με καθεστώς παρατηρητή. Έκτοτε, η ΕΕ μετέρχεται την πολιτική, τη νομοθεσία και τις

δαπάνες για την ενίσχυση της κυβερνοανθεκτικότητάς της. Σε ένα περιβάλλον όπου καταγράφονται ολοένα περισσότερες μείζονες κυβερνοεπιθέσεις και κυβερνοπεριστατικά, χει εντατικοποιήσει τις δραστηριότητές της από το 2013 και έπειτα, όπως διαφαίνεται στο ***γράφημα 2***. Παράλληλα, τα κράτη μέλη κατήρτισαν (και σε ορισμένες περιπτώσεις έχουν ήδη επικαιροποιήσει) τις πρώτες τους εθνικές στρατηγικές κυβερνοασφάλειας.

12 Οι κύριοι παράγοντες που είναι αρμόδιοι για θέματα που άπτονται της κυβερνοασφάλειας σε επίπεδο ΕΕ περιγράφονται στο ***πλαίσιο 2*** και στο ***παράρτημα I***.

Πλαίσιο 2

Ποιοι παράγοντες εμπλέκονται;

Η **Ευρωπαϊκή Επιτροπή** έχει ως στόχο την ενίσχυση των ικανοτήτων και της συνεργασίας στον τομέα της κυβερνοασφάλειας, καθώς και της θέσης της ΕΕ ως παράγοντα στον τομέα αυτό, και την ενσωμάτωση της διάστασης αυτής σε άλλες ενωσιακές πολιτικές. Οι γενικές διευθύνσεις (ΓΔ) που είναι κυρίως αρμόδιες για την πολιτική κυβερνοασφάλειας είναι η **ΓΔ Επικοινωνιακών Δικτύων** (κυβερνοασφάλεια) και η **ΓΔ Μετανάστευσης και Εσωτερικών Υποθέσεων** (κυβερνοεγκληματικότητα), αρμόδιες για την ψηφιακή ενιαία αγορά και την ένωση ασφάλειας αντίστοιχα. Η **ΓΔ Επικοινωνιακών Δικτύων** είναι αρμόδια για την ασφάλεια ΤΠ των συστημάτων της ίδιας της Επιτροπής.

Η Επιτροπή υποστηρίζεται από πλήθος οργανισμών, ιδίως τον **ENISA** (Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών), τον οργανισμό της ΕΕ για την κυβερνοασφάλεια –συμβουλευτικό κυρίως όργανο που στηρίζει την ανάπτυξη πολιτικής, την ανάπτυξη ικανοτήτων και την ενημέρωση και ευαισθητοποίηση για τα σχετικά θέματα. Το ευρωπαϊκό κέντρο για τα εγκλήματα στον κυβερνοχώρο της Ευρωπόλ (**EC3**) δημιουργήθηκε με σκοπό να ενισχύσει τις προσπάθειες επιβολής της νομοθεσίας της ΕΕ για την πάταξη της κυβερνοεγκληματικότητας. Η Επιτροπή φιλοξενεί μια ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (**CERT-EE**), η οποία υποστηρίζει το σύνολο των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης.

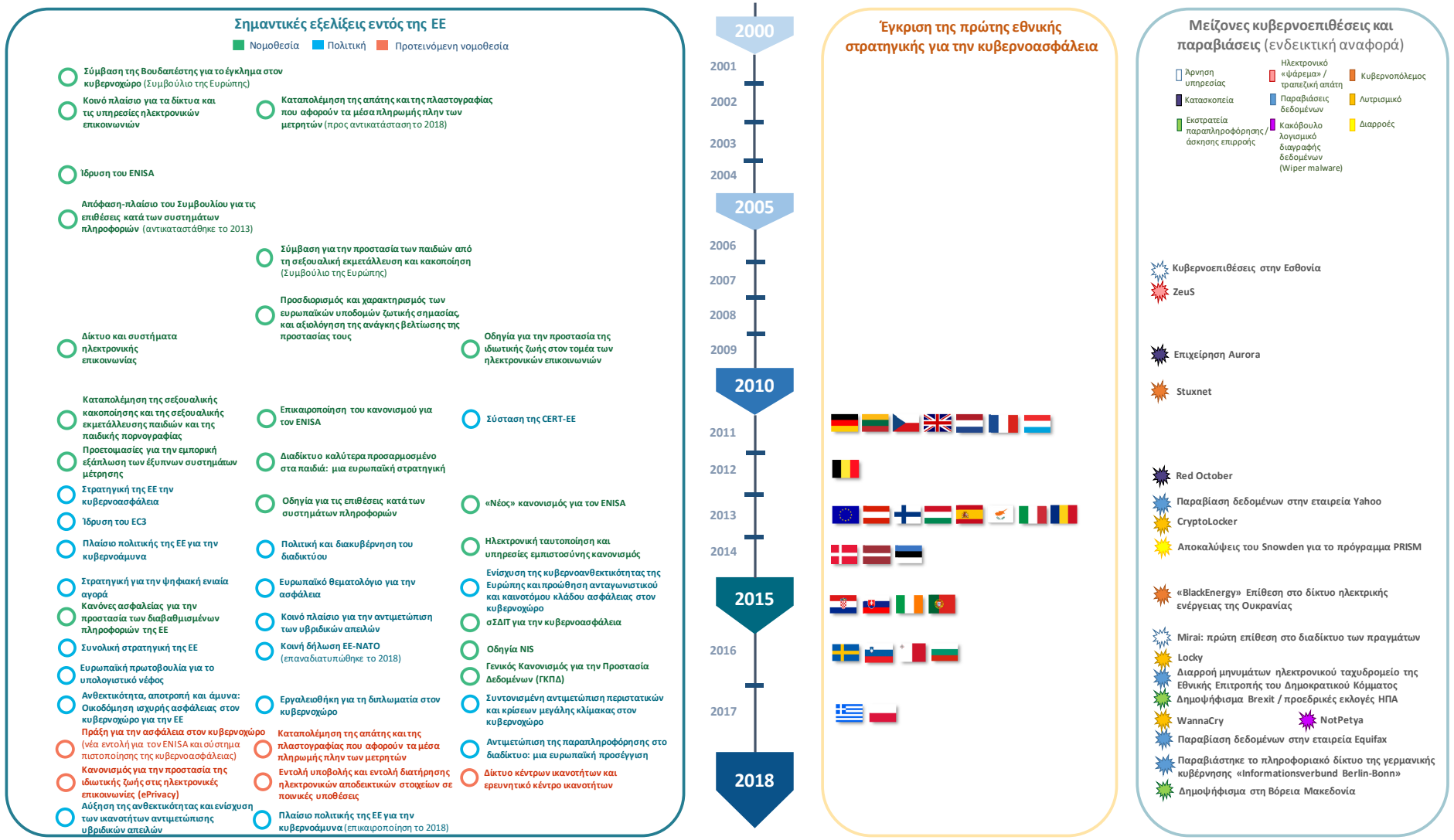
Η **Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης** (ΕΥΕΔ) ηγείται των προσπαθειών στους τομείς της κυβερνοάμυνας, της διπλωματίας στον κυβερνοχώρο και της στρατηγικής επικοινωνίας, και φιλοξενεί κέντρα συλλογής και ανάλυσης πληροφοριών. Ο **Ευρωπαϊκός Οργανισμός Άμυνας** (ΕΟΑ) επιδιώκει την ανάπτυξη ικανοτήτων κυβερνοάμυνας.

Τα **κράτη μέλη** φέρουν την κύρια ευθύνη για την κυβερνοασφάλειά τους και, σε επίπεδο ΕΕ, ενεργούν μέσω του **Συμβουλίου**, το οποίο διαθέτει πληθώρα οργάνων συντονισμού και ανταλλαγής πληροφοριών (μεταξύ αυτών την οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου). Το **Ευρωπαϊκό Κοινοβούλιο** ενεργεί ως

συννομοθέτης.

Οργανώσεις του ιδιωτικού τομέα, συμπεριλαμβανομένων οργανώσεων της βιομηχανίας, φορέων διακυβέρνησης του διαδικτύου, και της πανεπιστημιακής κοινότητας, είναι τόσο εταίροι όσο και συμβάλλοντες στη χάραξη και την εφαρμογή πολιτικών – μεταξύ άλλων μέσω μιας συμβατικής σύμπραξης δημόσιου και ιδιωτικού τομέα (**σΣΔΙΤ**).

Γράφημα 2 – Εντατικοποίηση των προσπαθειών για την ανάπτυξη πολιτικής και νομοθεσίας (κατάσταση ως είχε στις 31 Δεκεμβρίου 2018)



Πηγή: ΕΕΣ.

Πολιτική

13 Το «οικοσύστημα» του κυβερνοχώρου της ΕΕ είναι περίπλοκο και πολυεπίπεδο και εκτείνεται σε μια σειρά τομέων εσωτερικής πολιτικής, όπως οι τομείς της δικαιοσύνης και των εσωτερικών υποθέσεων, της ψηφιακής ενιαίας αγοράς και των πολιτικών για την έρευνα. Στον τομέα της εξωτερικής πολιτικής, η κυβερνοασφάλεια είναι ζήτημα που απασχολεί τη διπλωματία, και αποτελεί όλο και περισσότερο μέρος της αναδυόμενης πολιτικής της ΕΕ στον τομέα της άμυνας.

14 Ακρογωνιαίος λίθος της πολιτικής της ΕΕ είναι η **στρατηγική για την κυβερνοασφάλεια του 2013**[18]. Επιδίωξη της στρατηγικής είναι το ψηφιακό περιβάλλον της ΕΕ να καταστεί το ασφαλέστερο παγκοσμίως, με παράλληλη προάσπιση των θεμελιωδών αξιών και ελευθεριών. Έχει πέντε βασικούς στόχους: i) ενίσχυση της κυβερνοανθεκτικότητας· ii) μείωση της κυβερνοεγκληματικότητας· iii) ανάπτυξη πολιτικών και ικανοτήτων κυβερνοάμυνας· iv) ανάπτυξη βιομηχανικών και τεχνολογικών πόρων κυβερνοασφάλειας· και v) θέσπιση διεθνούς πολιτικής για τον κυβερνοχώρο, σύμφωνη με τις θεμελιώδεις αξίες της ΕΕ.

15 Η στρατηγική για την κυβερνοασφάλεια συνδέεται με τρεις στρατηγικές που εγκρίθηκαν μεταγενέστερα:

— Στόχος του **ευρωπαϊκού θεματολογίου για την ασφάλεια** (2015), είναι η βελτίωση της επιβολής του νόμου και της δικαστικής αντιμετώπισης της κυβερνοεγκληματικότητας, κυρίως μέσω της ανανέωσης και επικαιροποίησης των υφιστάμενων πολιτικών και της ισχύουσας νομοθεσίας[19]. Επιδίωξή του είναι επίσης ο προσδιορισμός των εμποδίων που παρακωλύουν τις ποινικές έρευνες στον τομέα του κυβερνοεγκλήματος και η ανάπτυξη των σχετικών ικανοτήτων.

— Η **στρατηγική για την ψηφιακή ενιαία αγορά**[20] (2015) έχει ως στόχο τη βελτίωση της πρόσβασης σε ψηφιακά προϊόντα και υπηρεσίες, μέσω της δημιουργίας των κατάλληλων συνθηκών για τη μεγιστοποίηση του αναπτυξιακού δυναμικού της ψηφιακής οικονομίας. Για τον σκοπό αυτό, αναγκαία είναι η ενίσχυση της εμπιστοσύνης, της ασφάλειας και της συμμετοχής στο διαδίκτυο.

— Επιδίωξη της **συνολικής στρατηγικής**[21] για το 2016 είναι η ενίσχυση του ρόλου της ΕΕ στον κόσμο. Η κυβερνοασφάλεια αποτελεί κεντρικό πυλώνα της, μέσω της ανανέωσης της δέσμευσης για ενίσχυση των προσπαθειών σε θέματα κυβερνοχώρου, της συνεργασίας με βασικούς εταίρους και της αποφασιστικότητας για την αντιμετώπιση των ζητημάτων του κυβερνοχώρου σε

όλους τους τομείς πολιτικής, συμπεριλαμβανομένης της αντιμετώπισης της παραπληροφόρησης μέσω στρατηγικής επικοινωνίας.

16 Τα τελευταία χρόνια, καθώς ο κυβερνοχώρος στρατιωτικοποιείται ολοένα περισσότερο[22] και προσαρμόζεται για πολεμική χρήση[23], έχει αρχίσει να θεωρείται ως ο πέμπτος τομέας πολέμου[24]. Η κυβερνοάμυνα θωρακίζει τα συστήματα, τα δίκτυα και τις ζωτικές υποδομές του κυβερνοχώρου έναντι επιθέσεων με στρατιωτικά και άλλα μέσα. Το 2014 εγκρίθηκε ένα **πλαίσιο πολιτικής για την άμυνα στον κυβερνοχώρο**, το οποίο επικαιροποιήθηκε το 2018[25]. Κατά την επικαιροποίηση του 2018 προσδιορίστηκαν έξι προτεραιότητες, συμπεριλαμβανομένης της ανάπτυξης αμυντικών ικανοτήτων στον κυβερνοχώρο, καθώς και της προστασίας των δικτύων επικοινωνιών και πληροφοριών της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ) της ΕΕ. Η κυβερνοάμυνα αποτελεί επίσης μέρος του πλαισίου της μόνιμης διαρθρωμένης συνεργασίας (PESCO) και της συνεργασίας ΕΕ-ΝΑΤΟ.

17 Το **κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών** (2016) καλύπτει τις κυβερνοαπειλές τόσο για τις υποδομές ζωτικής σημασίας όσο και για τους ιδιώτες χρήστες, υπογραμμίζοντας ότι οι κυβερνοεπιθέσεις μπορούν να λάβουν και τη μορφή εκστρατειών παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης[26]. Επισημαίνει επίσης την ανάγκη καλύτερης ενημέρωσης και ευαισθητοποίησης αλλά και ενίσχυσης της συνεργασίας μεταξύ της ΕΕ και του ΝΑΤΟ, η οποία έλαβε υπόσταση στις κοινές δηλώσεις ΕΕ-ΝΑΤΟ του 2016 και του 2018[27].

18 Το 2017 η Επιτροπή παρουσίασε μια νέα δέσμη μέτρων για την κυβερνοασφάλεια, η οποία αντανακλά την ολοένα πιο επείγουσα ανάγκη για ψηφιακή προστασία. Η δέσμη αυτή περιελάμβανε μια νέα ανακοίνωση της Επιτροπής για την επικαιροποίηση της στρατηγικής για την κυβερνοασφάλεια του 2013[28], καθώς και προσχέδιο για ταχεία και συντονισμένη ανταπόκριση σε μεγάλης κλίμακας επιθέσεις και την ταχεία εφαρμογή της οδηγίας για την ασφάλεια συστημάτων δικτύου και πληροφοριών (οδηγία NIS)[29]. Επιπλέον, η δέσμη περιελάμβανε σειρά νομοθετικών προτάσεων (βλέπε σημείο ***22***).

Νομοθεσία

19 Από το 2002 έχουν εγκριθεί διάφορες νομοθετικές πράξεις που σχετίζονται, έκαστη σε διαφορετικό βαθμό, με την κυβερνοασφάλεια.

20 Η σημαντικότερη νομοθετική πράξη και κεντρικός πυλώνας της στρατηγικής για την κυβερνοασφάλεια του 2013 είναι η **οδηγία** του 2016 **για την ασφάλεια δικτύων**

και πληροφοριών (οδηγία NIS)[30], η πρώτη σε επίπεδο ΕΕ για την κυβερνοασφάλεια. Η οδηγία, η οποία έπρεπε να μεταφερθεί στο εθνικό δίκαιο έως τον Μάιο του 2018, επιδιώκει να επιτύχει ένα ελάχιστο επίπεδο εναρμονισμένων ικανοτήτων, υποχρεώνοντας τα κράτη μέλη να θεσπίσουν εθνικές στρατηγικές για την ασφάλεια δικτύων και πληροφοριών και να δημιουργήσουν ενιαία κέντρα επαφής και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (computer security incident response team - CSIRT)[31]. Ακόμη, θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών σε κρίσιμους τομείς και για τους παρόχους ψηφιακών υπηρεσιών.

21 Παράλληλα, ο **γενικός κανονισμός για την προστασία των δεδομένων**[32] (ΓΚΠΔ) τέθηκε σε ισχύ το 2016 και σε εφαρμογή τον Μάιο του 2018. Στόχος του είναι η προστασία των δεδομένων προσωπικού χαρακτήρα των ευρωπαίων πολιτών, μέσω του καθορισμού κανόνων για την επεξεργασία και τη διάδοσή τους. Παρέχει στα υποκείμενα των δεδομένων ορισμένα δικαιώματα και συνεπάγεται υποχρεώσεις για τους υπεύθυνους επεξεργασίας δεδομένων (τους παρόχους ψηφιακών υπηρεσιών) σχετικά με τη χρήση και τη διαβίβαση πληροφοριών. Επιπλέον, επιβάλλει απαιτήσεις κοινοποίησης σε περίπτωση παραβίασης και, σε ορισμένες περιπτώσεις, προβλέπει πρόστιμα. Στο ***γράφημα 3*** επεξηγείται πώς η οδηγία NIS και ο ΓΚΠΔ αλληλοσυμπληρώνονται στις επιδιώξεις τους για την ενίσχυση της κυβερνοασφάλειας και τη διασφάλιση της προστασίας των δεδομένων.

22 Στα σχέδια νομοθετικών πράξεων που τελούν υπό συζήτηση περιλαμβάνονται η προτεινόμενη πράξη για την ασφάλεια στον κυβερνοχώρο για την ενίσχυση του ENISA και τη θέσπιση πανευρωπαϊκού μηχανισμού πιστοποίησης[33], η πρόταση κανονισμού σχετικά με τις εντολές υποβολής και διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων[34] και η πρόταση οδηγίας σχετικά με τα ηλεκτρονικά αποδεικτικά στοιχεία[35]. Η πρόταση του 2018 για τη σύσταση του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού (εφεξής «δίκτυο κέντρων ικανοτήτων στον τομέα της κυβερνοασφάλειας και ερευνητικό κέντρο ικανοτήτων») αποτελεί μέρος της δέσμης του 2017 για την κυβερνοασφάλεια[36].

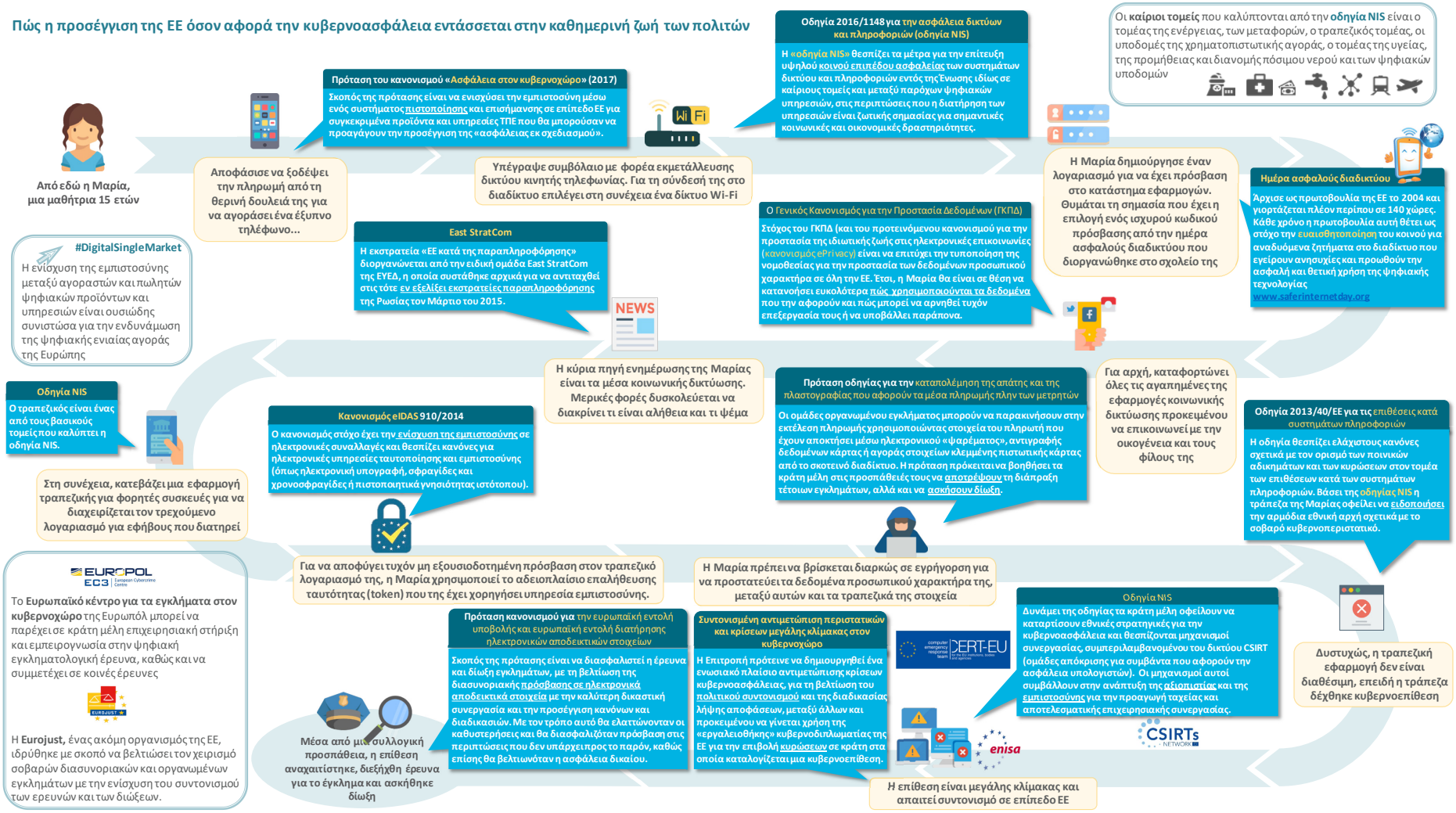
23 Δεν είναι εύκολο να σχηματιστεί σαφής εικόνα του εύρους του πλαισίου πολιτικής και του νομοθετικού πλαισίου που σχετίζεται με την κυβερνοασφάλεια και του τρόπου με τον οποίο επηρεάζει την καθημερινή ζωή μας.

24 Στο ***γράφημα 4*** επιχειρείται να χαρτογραφηθεί ο τρόπος με τον οποίο οι διάφορες νομοθετικές πράξεις και άλλες δραστηριότητες επηρεάζουν τη ζωή ενός φανταστικού ευρωπαίου πολίτη.

Γράφημα 3 – Πώς αλληλοσυμπληρώνονται ο κανονισμός ΓΚΠΔ και η οδηγία NIS

Πηγή: ΕΕΣ.

Γράφημα 4 – Πώς η προσέγγιση της ΕΕ όσον αφορά την κυβερνοασφάλεια εντάσσεται στην καθημερινή ζωή των πολιτών



Πηγή: ΕΕΣ.

Η κατασκευή πλαισίου πολιτικής και νομοθετικού πλαισίου

25 Το «οικοσύστημα» του κυβερνοχώρου της ΕΕ είναι περίπλοκο και πολυεπίπεδο, με τη συμμετοχή πολλών παραγόντων (βλέπε ***παράρτημα Ι***). Η συγκέντρωση όλων των διαφορετικών μερών που το απαρτίζουν συνιστά σημαντική πρόκληση. Από το 2013, καταβάλλονται συντονισμένες προσπάθειες να εξασφαλιστεί συνοχή στον τομέα της κυβερνοασφάλειας της ΕΕ[37].

Πρόκληση 1: Ουσιαστική αξιολόγηση και λογοδοσία

26 Όπως έχει επισημάνει η Επιτροπή, είναι δύσκολο να αποδειχθεί η ύπαρξη τυχόν αιτιώδους σχέσης μεταξύ της στρατηγικής του 2013 και οποιασδήποτε αλλαγής διαπιστώνεται. Οι στόχοι της στρατηγικής του 2013 είχαν διατυπωθεί κατά τρόπο πολύ ευρύ, εκφράζοντας μάλλον ένα όραμα παρά έναν μετρήσιμο στόχο[38]. Η ανάπτυξη δράσης που να ευθυγραμμίζεται με τις εν λόγω γενικές επιδιώξεις συνιστά πρόκληση λόγω της απουσίας μετρήσιμων στόχων. Το επικαιροποιημένο πλαίσιο πολιτικής για την κυβερνοάμυνα (2018) θα επιδιώξει την ανάπτυξη στόχων που θα καθορίζουν το ελάχιστο επίπεδο κυβερνοασφάλειας και εμπιστοσύνης που πρέπει να επιτευχθούν. Ωστόσο, αυτό περιορίζεται στον τομέα της κυβερνοάμυνας. Στόχοι που να καθορίζουν το επιθυμητό επίπεδο ανθεκτικότητας για την ΕΕ στο σύνολό της, δεν έχουν καθοριστεί ακόμη.

27 Τα επακόλουθα σπανίως μετρούνται και αξιολογήσεις έχουν πραγματοποιηθεί σε ελάχιστους τομείς πολιτικής[39]. Αυτό οφείλεται εν μέρει στο γεγονός ότι πολλά από τα μέτρα –νομοθετικά και άλλα– άρχισαν πρόσφατα να εφαρμόζονται, γεγονός που εμποδίζει την πλήρη αξιολόγηση του αντικτύπου τους. Η δυσκολία έγκειται στον προσδιορισμό ουσιαστικών κριτηρίων αξιολόγησης τα οποία να καθιστούν δυνατή τη μέτρηση του αντικτύπου. Επιπλέον, η αυστηρή αξιολόγηση δεν αποτελεί ακόμη τον κανόνα στον τομέα της κυβερνοασφάλειας εν γένει. Ως εκ τούτου, είναι αναγκαία η μετάβαση προς μια νοοτροπία επιδόσεων, αναπόσπαστο μέρος της οποίας θα αποτελούν πρακτικές αξιολόγησης και η τυποποιημένη υποβολή στοιχείων. Η τρέχουσα εντολή του ENISA δεν καλύπτει την αξιολόγηση ή την παρακολούθηση της κατάστασης στον τομέα της κυβερνοασφάλειας και της ετοιμότητας της ΕΕ.

28 Η χάραξη πολιτικών βάσει τεκμηριωμένων στοιχείων εξαρτάται από τη διαθεσιμότητα επαρκών, αξιόπιστων δεδομένων και στατιστικών στοιχείων τα οποία καθιστούν δυνατή την παρακολούθηση και την ανάλυση των τάσεων και των

αναγκών. Απουσία υποχρεωτικού και κοινού συστήματος παρακολούθησης, τα αξιόπιστα στοιχεία σπανίζουν. Επίσης, συχνά οι δείκτες δεν είναι άμεσα διαθέσιμοι και είναι δύσκολο να καθοριστούν[40]. Εντούτοις, σε ορισμένους τομείς έχουν αναπτυχθεί ειδικές μέθοδοι μέτρησης, όπως ο κύκλος πολιτικής της ΕΕ, που χρησιμοποιούνται για την αντιμετώπιση του σοβαρού και οργανωμένου εγκλήματος.

29 Ελάχιστα είναι τα κράτη μέλη που συγκεντρώνουν συστηματικά επίσημα δεδομένα για ζητήματα που σχετίζονται με τον κυβερνοχώρο, γεγονός που αποτελεί τροχοπέδη για τη συγκρισιμότητα. Μέχρι στιγμής, σπανίως έχει η ΕΕ εκδηλώσει ρητά την ανάγκη ενοποίησης των στατιστικών σε ευρωπαϊκό επίπεδο[41]. Ελάχιστες είναι επίσης οι διαθέσιμες ανεξάρτητες αναλύσεις σε επίπεδο ΕΕ σχετικά με βασικά θέματα όπως[42] η οικονομική διάσταση της κυβερνοασφάλειας, συμπεριλαμβανομένων των συμπεριφορικών πτυχών (ακατάλληλα κίνητρα, ασύμμετρη πληροφόρηση), η κατανόηση του αντικτύπου των ελλείψεων ασφάλειας στον κυβερνοχώρο και της κυβερνοεγκληματικότητας, οι μακροοικονομικές στατιστικές σχετικά με τις τάσεις και τις προκλήσεις στον τομέα του κυβερνοχώρου, και οι προσφορότερες λύσεις για την αντιμετώπιση των απειλών.

30 Λόγω της απουσίας ειδικών στόχων και της έλλειψης αξιόπιστων δεδομένων και σαφώς καθορισμένων δεικτών, η αξιολόγηση των επιτευγμάτων της στρατηγικής είναι μέχρι στιγμής κατά κύριο λόγο ποιοτική. Στις εκθέσεις προόδου συχνά περιγράφονται οι πραγματοποιηθείσες δραστηριότητες ή τα επιτευχθέντα ορόσημα, χωρίς ακριβή μέτρηση των αποτελεσμάτων. Επιπλέον, δεν έχουν καθοριστεί ακόμη τα δεδομένα αναφοράς που θα χρησιμοποιούνται για την αξιολόγηση της ανθεκτικότητας των συστημάτων. Ακόμη, ελλείψει ενός κωδικοποιημένου ορισμού του κυβερνοεγκλήματος είναι σχεδόν αδύνατο να βρεθούν σχετικοί δείκτες σε ευρωπαϊκό επίπεδο, οι οποίοι θα συνέβαλλαν στην παρακολούθηση και την αξιολόγηση.

31 Η ανεξάρτητη εποπτεία της εφαρμογής της πολιτικής για την κυβερνοασφάλεια διαφέρει μεταξύ των κρατών μελών. Στο πλαίσιο της έρευνάς μας, ζητήσαμε από τα ανώτατα όργανα ελέγχου των κρατών μελών πληροφορίες για την εμπειρία τους στον έλεγχο στον τομέα αυτό. Τα μισά από όσα απάντησαν[43] δεν είχαν διενεργήσει ποτέ σχετικό έλεγχο. Εξ αυτών που είχαν διενεργήσει ελέγχους, αυτοί είχαν επικεντρωθεί κυρίως στα εξής: διαχείριση των πληροφοριών, προστασία των υποδομών ζωτικής σημασίας, ανταλλαγή πληροφοριών και συντονισμός μεταξύ των βασικών ενδιαφερομένων, ετοιμότητα για την αντιμετώπιση περιστατικών, γνωστοποίηση και αντιμετώπισή τους. Μεταξύ των ζητημάτων που καλύφθηκαν σε μικρότερο βαθμό ήταν τα μέτρα ενημέρωσης/ευαισθητοποίησης και το έλλειμμα ψηφιακών δεξιοτήτων. Για λόγους εθνικής ασφάλειας, τα αποτελέσματα των εν λόγω ελέγχων ή αξιολογήσεων δεν δημοσιοποιούνται πάντοτε. Κατάλογος των εκθέσεων ελέγχου που

έχουν δημοσιεύσει ανώτατα όργανα ελέγχου των κρατών μελών παρατίθεται στο ***παράρτημα III***.

32 Ως κύριες προκλήσεις για τον έλεγχο των μέτρων που λαμβάνουν οι κρατικές αρχές στον τομέα αυτό αναφέρθηκαν οι περιορισμοί στις δεξιότητες που συνδέονται με τον κυβερνοχώρο (βλέπε επίσης σημεία ***82 έως 90***) και οι δυσκολίες στην αξιολόγηση της προόδου στον τομέα της κυβερνοασφάλειας.

Πρόκληση 2: Αντιμετώπιση των κενών στην ενωσιακή νομοθεσία και της άνισης μεταφοράς της στο εθνικό δίκαιο των κρατών μελών

33 Η ταχύτητα με την οποία αναδύονται νέες τεχνολογίες και απειλές υπερβαίνει κατά πολύ την ταχύτητα σχεδιασμού και εφαρμογής της νομοθεσίας της ΕΕ. Οι διαδικασίες της Ένωσης δεν σχεδιάστηκαν για την ψηφιακή εποχή: καίρια προτεραιότητα[44] αποτελεί η ανάπτυξη καινοτόμων και ευέλικτων διαδικασιών, προκειμένου να διασφαλιστεί ένα πολιτικό και νομικό πλαίσιο προσαρμοσμένο στις ανάγκες[45], με στόχο την καλύτερη πρόβλεψη και διαμόρφωση του μέλλοντος.

34 Παρά την προσπάθεια για μεγαλύτερη συνοχή, το νομοθετικό πλαίσιο για την κυβερνοασφάλεια παραμένει ατελές (για παραδείγματα, βλέπε ***πίνακα 1***). Ο κατακερματισμός του και τα κενά αποτελούν πρόσκομμα για την επίτευξη των γενικών στόχων της πολιτικής, ενώ μειώνουν την αποδοτικότητά της. Τα κενά που εντόπισε η Επιτροπή στην αξιολόγηση της στρατηγικής περιλαμβάνουν το διαδίκτυο των πραγμάτων, την ισορροπία των αρμοδιοτήτων μεταξύ χρηστών και παρόχων ψηφιακών προϊόντων, και ορισμένες πτυχές που δεν άγγιξε η οδηγία για την ασφάλεια δικτύων και πληροφοριών. Η πρόταση πράξης για την ασφάλεια στον κυβερνοχώρο επιχειρεί να καλύψει εν μέρει αυτά τα κενά, προάγοντας την «ασφάλεια εκ σχεδιασμού» μέσω ενός συστήματος πιστοποίησης σε επίπεδο ΕΕ. Ορισμένοι ενδιαφερόμενοι εκτιμούν ότι εξακολουθεί να είναι αισθητή η απουσία μιας σαφούς βιομηχανικής πολιτικής για τον κυβερνοχώρο και μιας κοινής προσέγγισης για την κυβερνοκατασκοπεία[46].

Πίνακας 1 - Κενά και άνιση μεταφορά στο νομοθετικό πλαίσιο (ενδεικτικός κατάλογος)

Τομέας πολιτικής	Παραδείγματα
Ψηφιακή ενιαία αγορά	o Η ισχύουσα οδηγία για τις πωλήσεις καταναλωτικών αγαθών δεν καλύπτει την κυβερνοασφάλεια. Οι προτεινόμενες οδηγίες για το ψηφιακό περιεχόμενο[47] και τις διαδικτυακές πωλήσεις[48] αποσκοπούν στην κάλυψη του κενού αυτού. o Τα νομικά πλαίσια των κρατών μελών της ΕΕ για τα καθήκοντα μέριμνας είναι περιορισμένα και εμφανίζουν διαφορές, γεγονός που προκαλεί ανασφάλεια δικαίου και δυσκολίες στην εφαρμογή των μέσων έννομης προστασίας[49]. o Οι πολιτικές για τη γνωστοποίηση τρωτών σημείων των λογισμικών αναπτύσσονται με διαφορετικό ρυθμό στα διάφορα κράτη μέλη, χωρίς να υπάρχει ένα γενικό νομικό πλαίσιο σε επίπεδο ΕΕ το οποίο να διευκολύνει μια συντονισμένη προσέγγιση[50].
Ενίσχυση της ασφάλειας δικτύων και πληροφοριών	o Τα κράτη μέλη είναι ελεύθερα να συμπεριλάβουν τομείς που δεν καλύπτονται από την οδηγία NIS[51]. Οι κλάδοι της φιλοξενίας, οι οποίοι δεν καλύπτονται, μπορεί να αποτελέσουν «κερκόπορτα» για άλλα αδικήματα, συμπεριλαμβανομένης της εμπορίας ανθρώπων, της διακίνησης ναρκωτικών ή της παράνομης μετανάστευσης[52].
Καταπολέμηση του κυβερνοεγκλήματος	o Πολλά κράτη μέλη δεν έχουν συμπεριλάβει ορισμό της έννοιας των ηλεκτρονικών αποδεικτικών στοιχείων στην εθνική νομοθεσία τους[53] (βλέπε επίσης σημείο ***22***). o Η ισχύουσα απόφαση-πλαίσιο σχετικά με την απάτη με μέσα πληρωμής πλην των μετρητών δεν καλύπτει ρητά τα άυλα μέσα πληρωμής, όπως είναι τα εικονικά νομίσματα, το ηλεκτρονικό χρήμα και οι πληρωμές μέσω κινητού τηλεφώνου, ούτε ενέργειες όπως το ηλεκτρονικό «ψάρεμα», η αντιγραφή δεδομένων κάρτας και η κατοχή και ανταλλαγή πληροφοριών πληρωμής[54]. o Η οδηγία για τις επιθέσεις κατά των συστημάτων πληροφοριών, δεν καλύπτει άμεσα την παράνομη εκ των έσω απόκτηση δεδομένων (π.χ. την κυβερνοκατασκοπεία), γεγονός που δυσχεραίνει το έργο των αρχών επιβολής του νόμου[55]. o Στον απόηχο της απόφασης του Δικαστηρίου της Ευρωπαϊκής Ένωσης για τη διατήρηση δεδομένων[56], οι διαφορές στην εφαρμογή του νομικού πλαισίου μεταξύ των κρατών μελών αποτέλεσαν πρόσκομμα για την επιβολή της νομοθεσίας, με αποτέλεσμα να χαθούν ενδεχομένως στοιχεία στο πλαίσιο ερευνών και να υπονομευθεί η αποτελεσματική δίωξη των δραστών ηλεκτρονικών εγκλημάτων[57].

Πηγή: ΕΕΣ.

35 Η εφαρμογή ορισμένων πτυχών της νομοθεσίας εξακολουθεί να είναι προαιρετική, τόσο για τις εθνικές αρχές όσο και για τις ιδιωτικές επιχειρήσεις. Παραδείγματος χάριν, στο πλαίσιο της ομάδας συνεργασίας, η αξιολόγηση των εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και της αποτελεσματικότητας των CSIRT είναι προαιρετική. Επίσης, βάσει του συστήματος πιστοποίησης που προτείνεται στην πράξη για την ασφάλεια στον κυβερνοχώρο, η εφαρμογή της πιστοποίησης για προϊόντα και υπηρεσίες ΤΠΕ θα είναι προαιρετική.

36 Στην ΕΕ, η κυβερνοασφάλεια εμπίπτει στην αρμοδιότητα των κρατών μελών. Εντούτοις, η ΕΕ μπορεί να διαδραματίσει καίριο ρόλο στη δημιουργία των προϋποθέσεων για τη βελτίωση των ικανοτήτων των κρατών μελών και τη μεταξύ τους συνεργασία, καθώς και στην εδραίωση κλίματος εμπιστοσύνης. Ωστόσο, δεδομένων των μεγάλων διαφορών μεταξύ των κρατών μελών όσον αφορά την ικανότητα και τον βαθμό συμμετοχής[58], η παροχή ευαίσθητων πληροφοριών (εθνικής ασφάλειας) θα συνεχίσει να είναι προαιρετική.

37 Η ασυνεπής μεταφορά της ενωσιακής νομοθεσίας στο εθνικό δίκαιο των κρατών μελών μπορεί να οδηγήσει σε νομικές και επιχειρησιακές ανακολουθίες και εμποδίζει την πλήρη επίτευξη των στόχων της νομοθεσίας. Παραδείγματος χάριν, τα κράτη μέλη έχουν υιοθετήσει διαφορετικές ερμηνείες όσον αφορά τον τρόπο εφαρμογής των ελέγχων των εξαγωγών ειδών διπλής χρήσης[59], με συνέπεια ορισμένες επιχειρήσεις που εδρεύουν στην ΕΕ να εξάγουν ενδεχομένως τεχνολογίες και υπηρεσίες που μπορούν να χρησιμοποιηθούν είτε για κυβερνοεπιτήρηση είτε για τη διάπραξη παραβιάσεων των ανθρωπίνων δικαιωμάτων μέσω λογοκρισίας ή υποκλοπής. Το Ευρωπαϊκό Κοινοβούλιο έχει εκφράσει την ανησυχία του για την κατάσταση αυτή[60].

38 Επιπλέον, για την προστασία της ιδιωτικής ζωής και της ελευθερίας της έκφρασης είναι αναγκαία μια προσαρμοσμένη νομοθετική απάντηση, προκειμένου να εξασφαλιστεί η απαιτούμενη ισορροπία μεταξύ της προστασίας των θεμελιωδών αξιών και της επίτευξης των επιταγών ασφάλειας της ΕΕ. Παραδείγματος χάριν, πώς μπορούμε να διασφαλίσουμε τη διατερματική κρυπτογράφηση, στηρίζοντας παράλληλα με τον καλύτερο δυνατό τρόπο την επιβολή της νομοθεσίας; Ή πώς μπορούμε να επιτύχουμε τις επιδιώξεις του ΓΚΠΔ γνωρίζοντας παράλληλα τις επιπτώσεις του στις δημόσια διαθέσιμες πληροφορίες για τους καταχωρίζοντες ονόματα διαδικτυακών χώρων και τους κατόχους ομάδων διευθύνσεων IP; Και με ποιον τρόπο μπορεί αυτό να επηρεάσει αρνητικά τις έρευνες των αρχών επιβολής του νόμου[61];

39 Από μόνη της, η νομοθεσία δεν εγγυάται την ανθεκτικότητα. Παρότι η οδηγία NIS έχει ως στόχο την επίτευξη υψηλού επιπέδου ασφάλειας σε όλη την ΕΕ, επικεντρώνεται ρητά στην επίτευξη μιας ελάχιστης, και όχι της μέγιστης δυνατής, εναρμόνισης[62]. Κενά θα εξακολουθήσουν να εμφανίζονται καθώς το τοπίο του κυβερνοχώρου θα εξελίσσεται.

Σημεία προβληματισμού – πλαίσιο πολιτικής

- Ποια είναι τα κυριότερα βήματα που είναι απαραίτητα προκειμένου να επιτευχθεί η στροφή των φορέων χάραξης πολιτικής και των νομοθετών προς μια νοοτροπία περισσότερο προσανατολισμένη στις επιδόσεις στον τομέα της κυβερνοασφάλειας, μεταξύ άλλων με τον ορισμό της συνολικής ανθεκτικότητας;

- Με ποιον τρόπο μπορεί να συμβάλει καλύτερα η έρευνα στην παραγωγή των αναγκαίων δεδομένων και στατιστικών στοιχείων ώστε να καταστεί δυνατή η ουσιαστική αξιολόγηση;

- Με ποιους τρόπους μπορούν να προσαρμοστούν οι νομοθετικές διαδικασίες της ΕΕ ώστε να αυξηθεί ο βαθμός ευελιξίας τους και να λαμβάνουν περισσότερο υπόψη την ταχύτητα των εξελίξεων της τεχνολογίας και των απειλών;

- Πώς μπορεί η πρακτική της ανάπτυξης μεθόδων μέτρησης (δεικτών, τιμών-στόχου) στο πλαίσιο του κύκλου πολιτικής της ΕΕ να προσαρμοστεί, να επεκταθεί και να αναπαραχθεί στον τομέα της κυβερνοασφάλειας συνολικά;

- Ποια διδάγματα μπορούν να αντλήσουν τα εθνικά ανώτατα όργανα ελέγχου από τις προσεγγίσεις που εφαρμόζουν άλλα ΑΟΕ για τον έλεγχο πολιτικών και των μέτρων κυβερνοασφάλειας;

- Ποιες ανακολουθίες στη μεταφορά στο εθνικό δίκαιο και την εφαρμογή του νομικού πλαισίου της ΕΕ υπονομεύουν την αποτελεσματικότητα της αντιμετώπισης των κενών στην κυβερνοασφάλεια και της κυβερνοεγκληματικότητας, και ποιος θα ήταν ο καλύτερος τρόπος να αντιμετωπιστούν από τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ;

- Πόσο αποτελεσματικοί είναι οι έλεγχοι των ενωσιακών εξαγωγών ειδών και υπηρεσιών του κυβερνοχώρου για την πρόληψη παραβιάσεων των ανθρωπίνων δικαιωμάτων εκτός της ΕΕ;

Χρηματοδότηση και δαπάνες

40 Η ΕΕ φιλοδοξεί το διαδικτυακό περιβάλλον της να καταστεί το ασφαλέστερο στον κόσμο. Αυτό απαιτεί σημαντικές προσπάθειες από πλευράς όλων των ενδιαφερομένων, συμπεριλαμβανομένης μιας στέρεης χρηματοοικονομικής βάσης.

Πρόκληση 3: Ευθυγράμμιση του επιπέδου των επενδύσεων με τους στόχους

Κλιμάκωση των επενδύσεων

41 Οι συνολικές δαπάνες για την κυβερνοασφάλεια ως ποσοστό του ΑΕγχΠ εκτιμώνται σε 0,1 % περίπου. Στις Ηνωμένες Πολιτείες[63], το αντίστοιχο ποσοστό είναι περίπου 0,35 % (συμπεριλαμβανομένου του ιδιωτικού τομέα). Ως ποσοστό, οι δαπάνες της ομοσπονδιακής κυβέρνησης των ΗΠΑ που εγγράφηκαν στον προϋπολογισμό για το 2019 ανέρχονται σε περίπου 0,1 % του ΑΕγχΠ ή σε περίπου 21 δισεκατομμύρια δολάρια[64].

42 Συγκριτικά, οι δαπάνες στην ΕΕ είναι χαμηλές, κατακερματισμένες και συχνά δεν συνοδεύονται από συντονισμένα κυβερνητικά προγράμματα. Η εξασφάλιση ακριβών αριθμητικών στοιχείων είναι δυσχερής, αλλά οι δημόσιες δαπάνες της ΕΕ στον τομέα της κυβερνοασφάλειας εκτιμάται ότι κυμαίνονται μεταξύ ενός και δύο δισεκατομμυρίων ευρώ ετησίως[65]. Οι δαπάνες ορισμένων κρατών μελών, εκφρασμένες ως ποσοστό του ΑΕγχΠ τους, αντιστοιχούν στο ένα δέκατο ή και λιγότερο του επιπέδου των ΗΠΑ[66]. Η ΕΕ και τα κράτη μέλη της χρειάζεται να γνωρίζουν το συνολικό ύψος των συλλογικών επενδύσεών τους, προκειμένου να προσδιορίσουν τις ελλείψεις που πρέπει να αντιμετωπίσουν.

43 Είναι δύσκολο να σχηματιστεί μια συνολική εικόνα ελλείψει σαφών στοιχείων, λόγω του οριζόντιου χαρακτήρα της κυβερνοασφάλειας και του γεγονότος ότι οι δαπάνες στον τομέα αυτό συχνά δεν μπορούν να διαχωριστούν από τις δαπάνες στον τομέα της ΤΠ γενικώς[67]. Με την έρευνά μας επιβεβαιώθηκε ότι είναι δύσκολο να συγκεντρωθούν αξιόπιστα στατιστικά στοιχεία για τις δαπάνες τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Τα τρία τέταρτα των εθνικών ανώτατων οργάνων ελέγχου ανέφεραν ότι δεν διαθέτουν συνολική εικόνα των κρατικών δαπανών που συνδέονται με τον κυβερνοχώρο, και ούτε ένα κράτος μέλος δεν υποχρέωνε τους δημόσιους φορείς να αναφέρουν χωριστά τις δαπάνες για την κυβερνοασφάλεια στα οικονομικά σχέδιά τους.

44 Η κλιμάκωση των δημόσιων και ιδιωτικών επενδύσεων στις ευρωπαϊκές επιχειρήσεις που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας αποτελεί ιδιαίτερη πρόκληση. Δημόσια χρηματοδότηση είναι συχνά διαθέσιμη κατά τα αρχικά στάδια, χωρίς να συμβαίνει συχνά το ίδιο κατά τα στάδια της ανάπτυξης και της επέκτασης[68]. Υφίστανται πολυάριθμες πρωτοβουλίες χρηματοδότησης της ΕΕ, οι οποίες όμως δεν αξιοποιούνται, σε μεγάλο βαθμό λόγω της γραφειοκρατίας[69]. Συνολικά, οι εταιρείες που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας στην ΕΕ υστερούν σε σχέση με τις αντίστοιχες εταιρείες σε διεθνές επίπεδο: καθώς είναι λιγότερες, η μέση χρηματοδότηση που προσελκύουν είναι σημαντικά χαμηλότερη[70]. Είναι επομένως ζωτικής σημασίας για την επίτευξη των στόχων της ψηφιακής πολιτικής της ΕΕ να διασφαλιστεί η αποτελεσματική στόχευση και χρηματοδότηση των νεοσύστατων επιχειρήσεων.

Κλιμάκωση του αντικτύπου

45 Η κάλυψη του επενδυτικού κενού στον τομέα του κυβερνοχώρου θα πρέπει να αποφέρει χρήσιμα επακόλουθα. Παραδείγματος χάριν, παρά το πλεονέκτημα της ΕΕ στον τομέα της έρευνας και της καινοτομίας, τα παραγόμενα αποτελέσματα δεν κατοχυρώνονται, δεν διατίθενται στο εμπόριο ούτε αποκτούν ευρύτερες διαστάσεις ώστε να συμβάλουν στην ενίσχυση της ανθεκτικότητας, της ανταγωνιστικότητας και της ψηφιακής αυτονομίας[71]. Αυτό καθίσταται ιδιαιτέρως εμφανές όταν γίνεται σύγκριση με τους ανταγωνιστές της ΕΕ παγκοσμίως. Η σπανιότητα καταλλήλως αξιοποιηθέντων αποτελεσμάτων οφείλεται σε μια σειρά παραγόντων[72], συμπεριλαμβανομένων των εξής:

- της απουσίας συνεκτικής διακρατικής στρατηγικής για τη διεύρυνση της προσέγγισης ώστε να ανταποκρίνεται στις ευρύτερες ψηφιακές ανάγκες της ΕΕ για ανταγωνιστικότητα και αυξημένη αυτονομία·
- της διάρκειας του κύκλου αλυσίδας αξίας, που έχει ως αποτέλεσμα σύντομα τα εργαλεία να καθίστανται παρωχημένα·
- της έλλειψης βιωσιμότητας, δεδομένου ότι τα έργα ολοκληρώνονται συνήθως με τη διάλυση της ομάδας έργου και τη διακοπή της στήριξης, συμπεριλαμβανομένης της στήριξης για επικαιροποιήσεις και εγκατάσταση επιδιορθώσεων.

46 Η πρόταση της Επιτροπής για τη δημιουργία δικτύου κέντρων ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και κέντρου ερευνητικών ικανοτήτων

αποτελεί μια προσπάθεια να αντιμετωπιστεί ο κατακερματισμός στον τομέα της έρευνας για την κυβερνοασφάλεια και να ενθαρρυνθούν οι επενδύσεις σε μεγάλη κλίμακα[73]. Συνολικά, υπάρχουν περίπου 665 κέντρα εμπειρογνωσίας σε όλη την ΕΕ.

Πρόκληση 4: Σχηματισμός σαφούς εικόνας των δαπανών του προϋπολογισμού της ΕΕ

47 Η ύπαρξη μιας συνολικής εικόνας των δαπανών είναι σημαντική για λόγους διαφάνειας και βελτίωσης του συντονισμού. Απουσία της, οι υπεύθυνοι για τη χάραξη της πολιτικής δύσκολα μπορούν να διαπιστώσουν κατά πόσον οι δαπάνες αντιστοιχούν στις ανάγκες ώστε να επιτευχθούν οι στόχοι προτεραιότητας.

48 Η στρατηγική για την κυβερνοασφάλεια δεν χρηματοδοτείται από ειδικό προϋπολογισμό. Σε ενωσιακό επίπεδο, οι δαπάνες για την κυβερνοασφάλεια καλύπτονται, αφενός, από τον γενικό προϋπολογισμό της ΕΕ και, αφετέρου, από συγχρηματοδότηση των κρατών μελών. Από την ανάλυσή μας προκύπτει μια πολύπλοκη δομή, αποτελούμενη από τουλάχιστον δέκα διαφορετικά μέσα στο πλαίσιο του γενικού προϋπολογισμού της ΕΕ, χωρίς όμως να υπάρχει σαφής εικόνα του ύψους των κονδυλίων και του τρόπου διάθεσής τους (βλέπε ***παράρτημα II***).

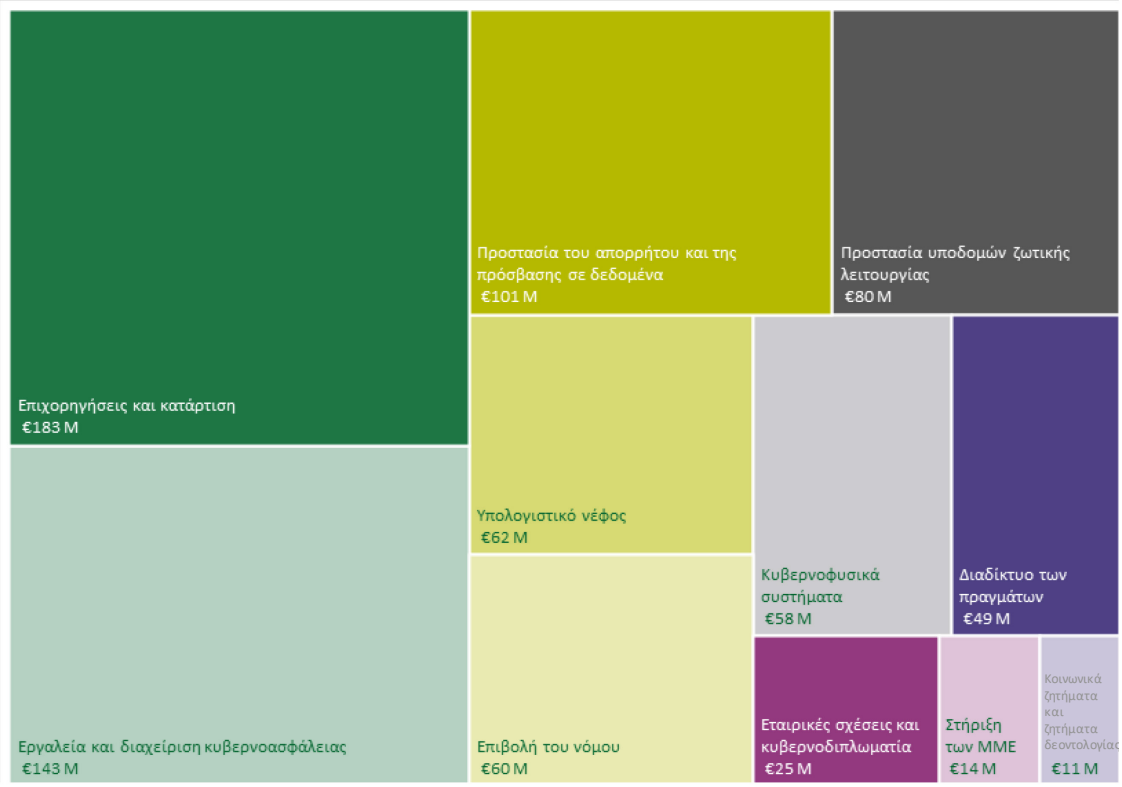
49 Επομένως, η σαφής επισκόπηση των δαπανών σε έναν τομέα που αφορά πολλούς τομείς πολιτικής εμφανίζει σημαντικές δυσκολίες. Αρμόδιες για τη διαχείριση των προγραμμάτων δαπανών είναι διάφορες υπηρεσίες της Επιτροπής, καθεμιά από τις οποίες έχει δικούς της στόχους, κανόνες και χρονοδιαγράμματα. Το ζήτημα περιπλέκεται περισσότερο αν ληφθεί υπόψη η συγχρηματοδότηση από τα κράτη μέλη, όπως στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας - «Αστυνομική συνεργασία»[74].

Ταυτοποιήσιμες δαπάνες για την κυβερνοασφάλεια

50 Κατά την περίοδο 2014-2018, η Επιτροπή διέθεσε τουλάχιστον 1,4 δισεκατομμύρια ευρώ για την εφαρμογή της στρατηγικής[75], το μεγαλύτερο μέρος των οποίων διατέθηκε για το πρόγραμμα «Ορίζων 2020»[76]. Η χρηματοδότηση του προγράμματος «Ορίζων 2020» διοχετεύεται κυρίως στο πλαίσιο των κοινωνικών προκλήσεων «Ασφαλείς κοινωνίες» και «Υπεροχή στις ευρείας εφαρμογής και βιομηχανικές τεχνολογίες»[77]. Εντοπίσαμε 279 έργα σχετικά με την κυβερνοασφάλεια τα οποία είχαν αποτελέσει αντικείμενο σύμβασης έως τα τέλη Σεπτεμβρίου του 2018, με συνολική χρηματοδότηση από την ΕΕ ύψους 786 εκατομμυρίων ευρώ[78]. Στο

γράφημα 5 παρουσιάζεται η τυπολογία των εν λόγω έργων με βάση την ανάλυση αυτή.

Γράφημα 5 – Ερευνητικά έργα στον τομέα της κυβερνοασφάλειας για τα οποία υπεγράφησαν συμβάσεις στο πλαίσιο του προγράμματος «Ορίζων 2020» (σε εκατομμύρια ευρώ)



Πηγή: ΕΕΣ.

51 Το 2016 συνήφθη μια συμβατική σύμπραξη δημόσιου και ιδιωτικού τομέα (σΣΔΙΤ) με σκοπό την προώθηση της ανάπτυξης του ευρωπαϊκού κλάδου της κυβερνοασφάλειας. Επιδίωξη ήταν η διοχέτευση 450 εκατομμυρίων ευρώ από το πρόγραμμα «Ορίζων 2020» στη σΣΔΙΤ και η προσέλκυση πρόσθετου ποσού 1,8 δισεκατομμυρίων ευρώ από τον ιδιωτικό τομέα έως το 2020. Έως τις 31 Δεκεμβρίου 2017, σε διάστημα 18 μηνών, διοχετεύθηκαν στη σΣΔΙΤ 67,5 εκατομμύρια ευρώ από το πρόγραμμα «Ορίζων 2020» και οι επενδύσεις του ιδιωτικού τομέα ανήλθαν σε 1 δισεκατομμύριο ευρώ[79].

52 Η καταπολέμηση του κυβερνοεγκλήματος υποστηρίζεται επίσης από τον τομέα «Αστυνομική συνεργασία» του Ταμείου Εσωτερικής Ασφάλειας. Το Ταμείο Εσωτερικής Ασφάλειας - «Αστυνομική συνεργασία» χρηματοδοτεί μελέτες, συνεδριάσεις εμπειρογνωμόνων και δραστηριότητες επικοινωνίας, για τις οποίες

διέθεσε σχεδόν 62 εκατομμύρια ευρώ κατά το διάστημα 2014-2017. Στο πλαίσιο της επιμερισμένης διαχείρισης, τα κράτη μέλη μπορούν επίσης να λαμβάνουν επιχορηγήσεις για την προμήθεια εξοπλισμού, καθώς και για δραστηριότητες κατάρτισης, έρευνας και συλλογής δεδομένων. Δεκαεννέα κράτη μέλη έχουν λάβει τέτοιες επιχορηγήσεις ύψους 42 εκατομμυρίων ευρώ.

53 Οι πόροι για τη στήριξη της δικαστικής συνεργασίας και της λειτουργίας των συμβάσεων αμοιβαίας δικαστικής συνδρομής, με ιδιαίτερη έμφαση στην ανταλλαγή ηλεκτρονικών δεδομένων και χρηματοοικονομικών πληροφοριών, ανήλθαν σε 9 εκατομμύρια ευρώ στο πλαίσιο του προγράμματος «Δικαιοσύνη» που διαχειρίζεται η ΓΔ Δικαιοσύνης και Καταναλωτών.

54 Η οδηγία για την ασφάλεια δικτύων και πληροφοριών αναφέρει ρητά ότι οι CSIRT πρέπει να διαθέτουν επαρκείς πόρους για την αποτελεσματική εκτέλεση των καθηκόντων τους[80]. Μεταξύ του 2016 και του 2018, διετίθεντο ετησίως 13 εκατομμύρια ευρώ από τον μηχανισμό «Συνδέοντας την Ευρώπη», στον οποίο τα κράτη μέλη μπορούσαν να υποβάλουν αίτηση προκειμένου να λάβουν χρηματοδότηση για να συμμορφωθούν με τις απαιτήσεις της οδηγίας. Δεν έχει πραγματοποιηθεί μελέτη που να προσδιορίζει τις πραγματικές οικονομικές ανάγκες του δικτύου CSIRT και της ομάδας συνεργασίας ώστε το έργο τους να έχει αντίκτυπο.

55 Αρκετές από τις επιχειρησιακές δαπάνες των οργανισμών αποσκοπούν ειδικά στην ενίσχυση της κυβερνοασφάλειας και την αντιμετώπιση του κυβερνοεγκλήματος. Ωστόσο, είναι δύσκολο να εξαχθούν ακριβή αριθμητικά στοιχεία από τις δημόσια διαθέσιμες πληροφορίες.

56 Η Σύμβαση της Βουδαπέστης (βλέπε σημείο ***11***) αποτελεί τη βάση των εξωτερικών δαπανών της ΕΕ για τον κυβερνοχώρο. Κατά την περίοδο 2014-2018, η ΕΕ δαπάνησε περίπου 50 εκατομμύρια ευρώ για την ενίσχυση της κυβερνοασφάλειας εκτός των συνόρων της. Σχεδόν το ήμισυ του ποσού αυτού διατέθηκε μέσω του μηχανισμού συμβολής στη σταθερότητα και την ειρήνη, και κυρίως σε ένα έργο (το ύψους 13,5 εκατομμυρίων ευρώ έργο GLACY+) με στόχο την ενίσχυση των ικανοτήτων σε παγκόσμιο επίπεδο για την ανάπτυξη και την εφαρμογή της νομοθεσίας για την κυβερνοεγκληματικότητα και την ενίσχυση της διεθνούς συνεργασίας[81]. Σε άλλες περιπτώσεις, οι δαπάνες στο πλαίσιο άλλων χρηματοοικονομικών μέσων της ΕΕ επικεντρώθηκαν σε μεγάλο βαθμό στα Δυτικά Βαλκάνια[82], καθώς και στην ευρωπαϊκή γειτονία. Παραδείγματος χάριν, το έργο Cybercrime@EaP που υλοποιείται από κοινού με τις χώρες της ανατολικής εταιρικής σχέσης αποσκοπεί στη βελτίωση της διεθνούς συνεργασίας όσον αφορά την κυβερνοεγκληματικότητα και τα ηλεκτρονικά αποδεικτικά στοιχεία.

Άλλες δαπάνες για την κυβερνοασφάλεια

57 Δεν είναι πάντα ευχερής ο εντοπισμός των δαπανών που σχετίζονται ειδικά με την κυβερνοασφάλεια στο πλαίσιο των προγραμμάτων της ΕΕ:

- Η χρηματοδότηση του προγράμματος «Ορίζων 2020» διοχετεύεται επίσης μέσω της Κοινής Επιχείρησης «Ηλεκτρονικά συστατικά στοιχεία και συστήματα για την ευρωπαϊκή πρωτοπορία» (ECSEL) για τα κυβερνοφυσικά συστήματα. Ωστόσο, δεν κατέστη δυνατό να προσδιορίσουμε μεταξύ των 27 έργων συνολικού ύψους 437 εκατομμυρίων ευρώ των ετών 2015 και 2016 τι ακριβώς αφορούσε την κυβερνοασφάλεια.

- Στο πλαίσιο των Ευρωπαϊκών Διαρθρωτικών και Επενδυτικών Ταμείων είναι διαθέσιμα έως και 400 εκατομμύρια ευρώ για δαπάνες σχετικές με την κυβερνοασφάλεια και τις υπηρεσίες εμπιστοσύνης. Το ποσό αυτό αφορά επενδύσεις για την ασφάλεια και την προστασία των δεδομένων με σκοπό την ενίσχυση της διαλειτουργικότητας και της διασύνδεσης των ψηφιακών υποδομών και τη βελτίωση της ηλεκτρονικής ταυτοποίησης και των υπηρεσιών εμπιστοσύνης και προστασίας της ιδιωτικής ζωής.

58 Στο επιχειρησιακό σχέδιό της για το 2018, η Ευρωπαϊκή Τράπεζα Επενδύσεων ανακοίνωσε την πρόθεσή της να αυξήσει τη χρηματοδότηση των τομέων της τεχνολογίας διπλής χρήσης, της κυβερνοασφάλειας και της μη στρατιωτικής ασφάλειας ώστε να αγγίξει τα 6 δισεκατομμύρια ευρώ σε διάστημα τριών ετών[83].

Μελλοντικές προοπτικές

59 Το ποσό των 2 δισεκατομμυρίων ευρώ που προβλέπεται για τη συνιστώσα της κυβερνοασφάλειας στο πλαίσιο του προτεινόμενου νέου προγράμματος «Ψηφιακή Ευρώπη»[84] για την περίοδο 2021-2027, έχει ως στόχο την ενίσχυση του τομέα της κυβερνοασφάλειας στην ΕΕ και της κοινωνικής προστασίας συνολικά, μεταξύ άλλων, συμβάλλοντας στην εφαρμογή της οδηγίας NIS. Το δίκτυο κέντρων ικανοτήτων στον τομέα της κυβερνοασφάλειας και το ερευνητικό κέντρο ικανοτήτων που προτείνεται να δημιουργηθούν με στόχο την υιοθέτηση μιας πιο εξορθολογισμένης προσέγγισης, αναμένεται να αποτελέσουν τον κύριο μηχανισμό εκτέλεσης των ενωσιακών δαπανών στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη».

60 Πρόσφατα, οι αμυντικές δαπάνες από τον προϋπολογισμό της ΕΕ αυξήθηκαν μέσω του ευρωπαϊκού προγράμματος βιομηχανικής ανάπτυξης στον τομέα της άμυνας, για το οποίο πρόκειται να διατεθούν 500 εκατομμύρια ευρώ κατά την

περίοδο 2019-2020[85]. Το πρόγραμμα αυτό θα επικεντρωθεί στη βελτίωση του συντονισμού και της αποδοτικότητας των αμυντικών δαπανών των κρατών μελών μέσω κινήτρων για από κοινού ανάπτυξη. Αποσκοπεί στην κινητοποίηση επενδύσεων συνολικού ύψους 13 δισεκατομμυρίων ευρώ για τον τομέα της αμυντικής ικανότητας μετά το 2020 μέσω του Ευρωπαϊκού Ταμείου Άμυνας, μέρος των οποίων αφορά την κυβερνοάμυνα[86].

Πρόκληση 5: Οι ελλείψεις πόρων που αντιμετωπίζουν οι οργανισμοί της ΕΕ

61 Οι τρεις βασικοί φορείς που βρίσκονται στο επίκεντρο της πολιτικής της ΕΕ για την κυβερνοασφάλεια –ENISA, κέντρο EC3 της Ευρωπόλ και CERT-ΕΕ (βλέπε ***πλαίσιο 2***)– αντιμετωπίζουν ελλείψεις πόρων σε μια περίοδο κατά την οποία η σημασία των πολιτικών προτεραιοτήτων που επικεντρώνονται στην ασφάλεια αυξάνεται. Οι ελλείψεις σε ανθρώπινους και οικονομικούς πόρους που αντιμετωπίζουν επί του παρόντος οι οργανισμοί της ΕΕ δεν τους επιτρέπουν να ανταποκριθούν στις προσδοκίες[87].

62 Τα αιτήματα των οργανισμών για πρόσθετους πόρους προκειμένου να ανταποκριθούν στην αυξανόμενη ζήτηση δεν έχουν ικανοποιηθεί πλήρως, γεγονός που μπορεί να υπονομεύσει την (έγκαιρη) επίτευξη των στόχων πολιτικής. Ενδεικτικά αναφέρονται οι εξής:

- Η έλλειψη πόρων συνετέλεσε στην αδυναμία του ENISA να επιτύχει πλήρως τους στόχους του το 2017[88]. Στη δέσμη του 2017 προτάθηκε η αύξηση των πόρων, προκειμένου να δοθεί στον οργανισμό η δυνατότητα να ανταποκριθεί στη νέα εντολή του.

- Οι προσλήψεις αναλυτών και οι επενδύσεις σε ικανότητες ΤΠΕ στο κέντρο EC3 της Ευρωπόλ δεν συμβαδίζουν με τη ζήτηση[89]. Ακόμη, η κοινή ειδική ομάδα δράσης για την καταπολέμηση του κυβερνοεγκλήματος (J-CAT) της Ευρωπόλ στελεχώνεται από εμπειρογνώμονες των κρατών μελών και τρίτων χωρών για υποστήριξη κατά τη διενέργεια ερευνών βάσει εμπιστευτικών πληροφοριών. Ωστόσο, το κόστος βαρύνει σε μεγάλο βαθμό τα κράτη προέλευσης, γεγονός που λειτουργεί ανασταλτικά για την αποστολή μεγαλύτερου αριθμού εμπειρογνωμόνων. Προκειμένου να διευκολυνθεί η συμμετοχή περισσότερων χωρών, αναπτύχθηκε μια προσωρινή, κατά περίπτωση, διαδικασία απόσπασης, με χρηματοδότηση από την Ευρωπόλ ή τον κύκλο πολιτικής της ΕΕ.

63 Για ορισμένους από τους περιορισμούς ευθύνονται οι ίδιοι οι οργανισμοί. Πολλοί υπάλληλοι της CERT-ΕΕ και του ENISA είναι συμβασιούχοι, οι διαδικασίες πρόσληψης των οποίων είναι συνήθως βραδείες. Άλλοι πάλι περιορισμοί, όπως η προσέλκυση και η διατήρηση ταλέντων, απορρέουν από την αδυναμία των οργανισμών να ανταγωνιστούν τους μισθούς του ιδιωτικού τομέα ή οφείλονται στις περιορισμένες προοπτικές επαγγελματικής ανέλιξης που προσφέρουν. Για τους λόγους αυτούς, ο ENISA ανέθεσε σε τρίτους την εκτέλεση μεγάλου μέρους των εργασιών του κατά την περίοδο 2014-2016[90].

64 Οι ελλείψεις προσωπικού και των αναγκαίων εργαλείων μπορεί να ενέχουν σημαντικούς κινδύνους, ιδίως όσον αφορά τη συλλογή πληροφοριών για τις απειλές. Ο όγκος των δεδομένων που προέρχονται από ανοικτές και κλειστές πηγές διαρκώς αυξάνεται και υπάρχει κίνδυνος υπέρβασης των ικανοτήτων των αναλυτών να διεξάγουν ορθές αναλύσεις απειλών. Χωρίς τις κατάλληλες ικανότητες και τα κατάλληλα εργαλεία για την επιτυχή ενοποίηση και διασύνδεση των εν λόγω δεδομένων, δεν πρόκειται να καταστεί δυνατό να μεταφραστούν τα δεδομένα αυτά σε αξιοποιήσιμες πληροφορίες για τις απειλές που θα μπορούν να ανταλλάσσονται και να αναλύονται μεταξύ των αρμόδιων φορέων σε ολόκληρη την ΕΕ[91].

Σημεία προβληματισμού – Χρηματοδότηση και δαπάνες

- Με ποιους τρόπους μπορούν η Επιτροπή και οι νομοθέτες να εξορθολογίσουν τις δαπάνες της ΕΕ στον τομέα της κυβερνοασφάλειας και να τις αντιστοιχίσουν σε σαφώς καθορισμένους στόχους;
- Πώς μπορούν να αντιμετωπιστούν κατά τρόπο συνολικό οι ελλείψεις πόρων των οργανισμών της ΕΕ, λαμβανομένων υπόψη των αναγκών και των στόχων της Ένωσης;
- Ποια μέτρα λαμβάνονται σε επίπεδο ΕΕ και κρατών μελών για τη μείωση των φραγμών που αντιμετωπίζουν οι ΜΜΕ στην πρόσβασή τους σε επενδυτικά κεφάλαια, ώστε να επεκτείνουν τις δραστηριότητές τους;
- Ποια συγκεκριμένα και βιώσιμα αποτελέσματα επιτυγχάνονται με τα κεφάλαια του προγράμματος «Ορίζων 2020» για την παραγωγή λύσεων στον τομέα της κυβερνοασφάλειας;
- Με ποιον τρόπο συμβάλλουν οι δραστηριότητες της ΕΕ για ενίσχυση των ικανοτήτων στην ενίσχυση των ικανοτήτων πέρα από τα σύνορά της, τηρουμένων των αξιών της ΕΕ;

Δημιουργία μιας κυβερνοανθεκτικής κοινωνίας

65 Η διακυβέρνηση στον τομέα της κυβερνοασφάλειας αφορά τη διαχείριση των απειλών και των κινδύνων, την ενίσχυση της ικανότητας και της ενημέρωσης και ευαισθητοποίησης, καθώς και τον συντονισμό και την ανταλλαγή πληροφοριών που βασίζονται σε θεμέλια εμπιστοσύνης.

Πρόκληση 6: Ενίσχυση της διακυβέρνησης και των προτύπων

Διακυβέρνηση της ασφάλειας των πληροφοριών

66 Η διακυβέρνηση της ασφάλειας των πληροφοριών αφορά τη δημιουργία δομών και τη χάραξη πολιτικών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων. Δεν περιορίζεται στα τεχνικά ζητήματα· απαιτεί αποτελεσματική ηγεσία, αξιόπιστες διαδικασίες και στρατηγικές που ευθυγραμμίζονται με τους στόχους του οργανισμού[92]. Υποσύνολό της αποτελεί η διακυβέρνηση της κυβερνοασφάλειας, η οποία καλύπτει όλα τα είδη των απειλών που σχετίζονται με τον κυβερνοχώρο, συμπεριλαμβανομένων των στοχευμένων, σύνθετων επιθέσεων, παραβιάσεων ή περιστατικών που είναι δύσκολο να εντοπιστούν ή να αντιμετωπιστούν.

67 Τα μοντέλα διακυβέρνησης της κυβερνοασφάλειας διαφέρουν μεταξύ των κρατών μελών, στο εσωτερικό των οποίων η ευθύνη για την κυβερνοασφάλεια συχνά επιμερίζεται μεταξύ πολλών φορέων. Οι διαφορές αυτές μπορούν να παρεμποδίσουν τη συνεργασία που απαιτείται για την αντιμετώπιση διασυνοριακών συμβάντων μεγάλης κλίμακας και την ανταλλαγή πληροφοριών σχετικά με τις απειλές τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο. Από την έρευνά μας μεταξύ των ανώτατων οργάνων ελέγχου προέκυψε ότι μεγαλύτεροι κίνδυνοι θεωρούνται οι αδυναμίες στις ρυθμίσεις διακυβέρνησης των δημόσιων αρχών και στη διαχείριση των κινδύνων.

68 Μολονότι οι συνέπειες για τους οργανισμούς του ιδιωτικού τομέα μπορεί να είναι σοβαρές, οι αδυναμίες στη διακυβέρνηση του κυβερνοχώρου είναι πάρα πολλές. Σχεδόν εννέα στους δέκα οργανισμούς δηλώνουν ότι οι δραστηριότητές τους στον τομέα της κυβερνοασφάλειας δεν ανταποκρίνονται πλήρως στις ανάγκες τους[93], και οι υπεύθυνοι για την κυβερνοασφάλεια απέχουν συχνά τουλάχιστον δύο ιεραρχικά επίπεδα από το ανώτατο όργανο διοίκησης[94].

69 Οι οδηγίες της ΕΕ για το εταιρικό δίκαιο δεν προβλέπουν ειδικές απαιτήσεις για τη γνωστοποίηση πληροφοριών σχετικά με τους κινδύνους που συνδέονται με τον κυβερνοχώρο. Στις Ηνωμένες Πολιτείες, η Επιτροπή Κεφαλαιαγοράς εξέδωσε πρόσφατα μη δεσμευτικές κατευθυντήριες γραμμές προκειμένου να διευκολύνει τις εισηγμένες επιχειρήσεις στην επιλογή των πληροφοριών προς γνωστοποίηση σχετικά με τους κινδύνους και τα συμβάντα που συνδέονται με την κυβερνοασφάλεια[95]. Η μικτή επιτροπή των ευρωπαϊκών εποπτικών αρχών[96] (ΕΕΑ) προειδοποίησε για την αύξηση των κινδύνων που συνδέονται με τον κυβερνοχώρο και ενθάρρυνε τα χρηματοπιστωτικά ιδρύματα να βελτιώσουν τα ευάλωτα συστήματα ΤΠ και να αναλύσουν τους εγγενείς κινδύνους για την ασφάλεια των πληροφοριών, τη συνδεσιμότητα και την εξωτερική ανάθεση[97].

70 Η ενίσχυση της διακυβέρνησης της ασφάλειας των πληροφοριών στο επίπεδο των ΜΜΕ αποτελεί ιδιαίτερα δύσκολο εγχείρημα δεδομένου ότι, στις περισσότερες περιπτώσεις, οι επιχειρήσεις αυτές αδυνατούν να εφαρμόσουν τα κατάλληλα συστήματα. Δεν διαθέτουν κατάλληλες κατευθυντήριες γραμμές για την εφαρμογή των απαιτήσεων όσον αφορά την ασφάλεια των πληροφοριών και την προστασία της ιδιωτικής ζωής και για τον μετριασμό των τεχνολογικών κινδύνων[98]. Ως εκ τούτου, οι βασικές προκλήσεις συνίστανται στην καλύτερη κατανόηση των αναγκών τους και στην παροχή των κινήτρων και τη λήψη των μέτρων στήριξης που είναι αναγκαία.

71 Η απουσία συνεκτικού πλαισίου διακυβέρνησης για την κυβερνοασφάλεια σε διεθνές επίπεδο επηρεάζει αρνητικά την ικανότητα της διεθνούς κοινότητας να αντιδρά σε κυβερνοεπιθέσεις και να τις περιορίζει. Ως εκ τούτου, είναι σημαντικό να επιτευχθεί συναίνεση επί ενός τέτοιου πλαισίου διακυβέρνησης, το οποίο θα αντικατοπτρίζει με τον καλύτερο δυνατό τρόπο τα συμφέροντα και τις αξίες της ΕΕ[99]. Οι προσπάθειες για τον καθορισμό δεσμευτικών διεθνών κανόνων για τον κυβερνοχώρο κλυδωνίζονται ολοένα περισσότερο, όπως μαρτυρά η αδυναμία επίτευξης συναίνεσης στο πλαίσιο της ομάδας κυβερνητικών εμπειρογνωμόνων των Ηνωμένων Εθνών το 2017 σχετικά με τον τρόπο με τον οποίο το διεθνές δίκαιο θα πρέπει να εφαρμόζεται στα μέτρα αντίδρασης που λαμβάνουν τα κράτη έναντι περιστατικών.

72 Προκειμένου να ενισχύσει το πρόγραμμα δράσης της σχετικά με τη διακυβέρνηση του κυβερνοχώρου, η ΕΕ έχει επίσης επισημοποιήσει έξι εταιρικές σχέσεις σχετικά με θέματα κυβερνοχώρου, για τη διεξαγωγή τακτικών διαλόγων πολιτικής με στόχο την οικοδόμηση εμπιστοσύνης και τη δημιουργία κοινών πεδίων συνεργασίας[100]. Τα αποτελέσματα είναι ανάμεικτα. Ωστόσο, συνολικά, σε διεθνές

επίπεδο, η ΕΕ δεν μπορεί ακόμη να θεωρηθεί «σημαντικός παράγοντας στον τομέα της κυβερνοασφάλειας» παρότι έχει βελτιώσει την εικόνα της[101].

Ασφάλεια των πληροφοριών στα θεσμικά όργανα της ΕΕ

73 Κάθε θεσμικό όργανο της ΕΕ διαθέτει δικούς του κανόνες για τη διακυβέρνηση της ασφάλειας των πληροφοριών. Μια διοργανική συμφωνία προβλέπει ότι η Επιτροπή συντρέχει τα άλλα θεσμικά όργανα και τους οργανισμούς σε θέματα ασφάλειας των πληροφοριών. Τα θεσμικά και λοιπά όργανα της ΕΕ έχουν αναγνωρίσει την ανάγκη ανάπτυξης των ικανοτήτων τους σε θέματα κυβερνοχώρου, καθώς και προσεγγίσεων για τη διαχείριση των κινδύνων κατά τρόπο συνεκτικό. Η Επιτροπή, το Συμβούλιο και η ΕΥΕΔ πρέπει να υποβάλουν το 2020 έκθεση στην οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου σχετικά με τη διακυβέρνηση και την πρόοδο που έχει σημειωθεί όσον αφορά την αποσαφήνιση και την εναρμόνιση της διακυβέρνησης στον τομέα της κυβερνοασφάλειας σε επίπεδο θεσμικών οργάνων και οργανισμών της ΕΕ[102].

74 Στους κόλπους της Επιτροπής, αρμόδια για την ασφάλεια των υποδομών και υπηρεσιών ΤΠ είναι η Γενική Διεύθυνση Πληροφορικής (βλέπε ***πλαίσιο 3***). Κύριοι στόχοι της ψηφιακής στρατηγικής της Επιτροπής στον τομέα της ασφάλειας ΤΠ είναι η ενσωμάτωσή της στις διαδικασίες διαχείρισης, η παροχή (οικονομικά) αποδοτικών υποδομών και η εξασφάλιση ανθεκτικότητας, η διεύρυνση των δυνατοτήτων ανίχνευσης και αντιμετώπισης περιστατικών, και η ενοποίηση της διακυβέρνησης της ΤΠ και της ασφάλειας[103]. Στο πλαίσιο της σύμβασής της παροχής υπηρεσιών, η Επιτροπή διασφαλίζει την ενεργή συντήρηση του συνόλου σχεδόν των λογισμικών και τη χρήση μόνον λογισμικού που τυγχάνει υποστήριξης από τον προμηθευτή[104].

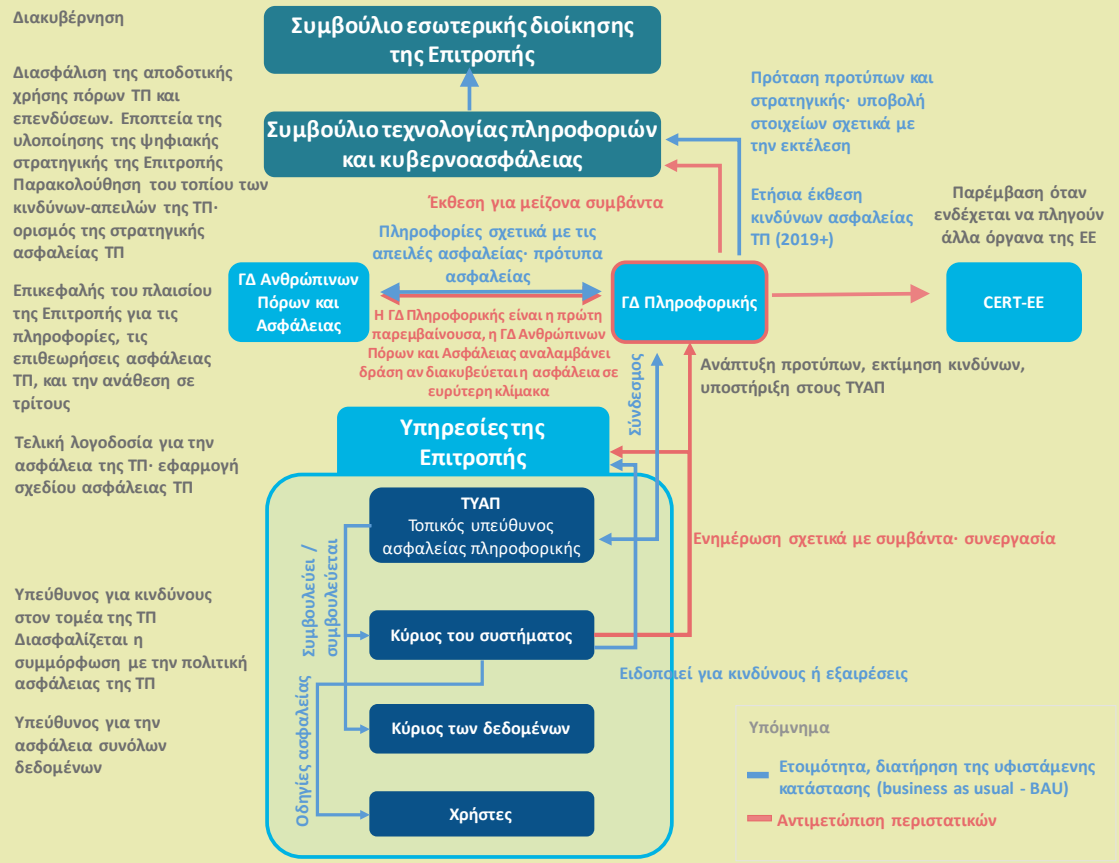
75 Η ανάγκη προστασίας των θεσμικών οργάνων εκτείνεται και στις αποστολές και τις δομές της ΚΠΑΑ ανά τον κόσμο. Μία από τις προτεραιότητες του πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση του 2018) είναι η ενίσχυση της προστασίας των συστημάτων επικοινωνίας και πληροφοριών της ΚΠΑΑ που χρησιμοποιούν οντότητες της ΕΕ. Έχει πλέον συγκροτηθεί στους κόλπους της ΕΥΕΔ ένα εσωτερικό συμβούλιο για τη διακυβέρνηση στον κυβερνοχώρο, το οποίο συνεδρίασε για πρώτη φορά τον Ιούνιο του 2017[105].

Πλαίσιο 3

Προστασία των συστημάτων πληροφοριών της Επιτροπής

Τα περίπου 1 300 συστήματα και οι 50 000 συσκευές της Επιτροπής αποτελούν συνεχώς στόχο κυβερνοεπιθέσεων. Η ευθύνη για θέματα πληροφορικής είναι

αποκεντρωμένη, όπως προκύπτει από το παρακάτω γράφημα. Η ασφάλεια των πληροφοριών και η ασφάλεια στον τομέα της ΤΠ βασίζονται σε κοινό σχέδιο ασφάλειας ΤΠ που έχει καταρτίσει η ΓΔ Πληροφορικής. Το συμβούλιο τεχνολογίας των πληροφοριών και κυβερνοασφάλειας ενεργεί ως το εκ των πραγμάτων υπεύθυνο για την ασφάλεια των πληροφοριών όργανο της Επιτροπής και συνδέει την επιχειρησιακή πλευρά της ασφάλειας ΤΠ με τα ανώτατα κλιμάκια της διοίκησης του θεσμικού οργάνου, που εκπροσωπούνται από το συμβούλιο εσωτερικής διοίκησης της Επιτροπής.



Πηγή: ΕΕΣ, βάσει των αποφάσεων της Επιτροπής[106].

Κύριο καθήκον της ΓΔ Ανθρώπινων Πόρων και Ασφάλειας είναι η προστασία του προσωπικού, των πληροφοριών και των στοιχείων ενεργητικού της Επιτροπής. Διενεργεί επίσης έρευνες ασφάλειας για περιστατικά στα οποία η διάσταση της ασφάλειας δεν συνδέεται αποκλειστικά με την ΤΠ και που, ως εκ τούτου, σχετίζονται με τις δραστηριότητές της στους τομείς της αντικατασκοπείας και της καταπολέμησης της τρομοκρατίας.

Η ΓΔ Πληροφορικής είναι αρμόδια για την ασφάλεια ΤΠ και φιλοξενεί την ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-EE). Η ομάδα αυτή συγκροτήθηκε το 2011 με ετήσιο προϋπολογισμό περίπου 2,5 εκατομμυρίων ευρώ και έχει περίπου 30 υπαλλήλους. Παρότι είναι η πρώτη παρεμβαίνουσα σε κάθε περιστατικό που σχετίζεται με την ασφάλεια των πληροφοριών και αφορά περισσότερα θεσμικά όργανα, δεν λειτουργεί ακόμη σε εικοσιτετράωρη βάση, επτά

ημέρες την εβδομάδα. Φιλοξενεί πλατφόρμα ανταλλαγής πληροφοριών. Το 2018, η CERT-ΕΕ υπέγραψε μη δεσμευτικό μνημόνιο συμφωνίας με τον ENISA, το κέντρο EC3 και τον Ευρωπαϊκό Οργανισμό Άμυνας για την ενίσχυση της συνεργασίας και του συντονισμού. Έχει επίσης συνάψει τεχνική συμφωνία με την ομάδα αντιμετώπισης συμβάντων πληροφορικής του ΝΑΤΟ (NCIRC).

Εκτιμήσεις απειλών και κινδύνων

76 Οι τεκμηριωμένες και συνεχείς εκτιμήσεις απειλών και κινδύνων αποτελούν σημαντικά εργαλεία για τους οργανισμούς τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Ωστόσο, δεν υπάρχει τυποποιημένη προσέγγιση για την ταξινόμηση και τη χαρτογράφηση των κυβερνοαπειλών ή για την εκτίμηση των κινδύνων, με αποτέλεσμα το περιεχόμενο των εκτιμήσεων να ποικίλλει σημαντικά, γεγονός που δυσχεραίνει την υιοθέτηση μιας συνεκτικής προσέγγισης σε επίπεδο ΕΕ όσον αφορά την κυβερνοασφάλεια[107]. Επιπλέον, συχνά βασίζονται στις ίδιες πηγές ή ακόμη και σε εκτιμήσεις απειλών τρίτων, με αποτέλεσμα να δημιουργείται ένας «θάλαμος αντήχησης» όπου επαναλαμβάνονται οι ίδιες διαπιστώσεις[108], με κίνδυνο να μην δίδεται επαρκής προσοχή σε άλλες απειλές. Η κατάσταση αυτή επιδεινώνεται από τη συνεχιζόμενη απροθυμία ανταλλαγής πληροφοριών και την ελλιπή αναφορά των περιστατικών.

77 Η Μονάδα Ανάλυσης Υβριδικών Απειλών[109] που λειτουργεί στους κόλπους της ΕΥΕΔ συστάθηκε προκειμένου να βελτιωθεί η επίγνωση της κατάστασης και να υποστηριχθεί η λήψη αποφάσεων μέσω της ανταλλαγής αναλύσεων. Ωστόσο, πρέπει να διευρύνει το πεδίο εμπειρογνωσίας της, προκειμένου να συμπεριλάβει, μεταξύ άλλων, τον τομέα της κυβερνοασφάλειας. Παράλληλα, η CERT-ΕΕ παρέχει στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ εκθέσεις και ενημερωτικά σημειώματα σχετικά με τις κυβερνοαπειλές των οποίων αποτελούν στόχο.

78 Ο ENISA έχει επισημάνει στο παρελθόν ότι πολλά κράτη μέλη περιγράφουν τις απειλές με ποιοτικούς όρους και ότι υπάρχει ανάγκη για αύξηση της μοντελοποίησης των κυβερνοαπειλών[110]. Η παρακολούθηση των ικανοτήτων στρατηγικής ανάλυσης θα ενισχύσει τη συνολική κατανόηση. Ωστόσο, οι εκτιμήσεις απειλών θα μπορούσαν να καλύπτουν όχι μόνο τις τεχνολογικές, αλλά και τις κοινωνικοπολιτικού και οικονομικού χαρακτήρα απειλές, ώστε να παρέχεται μια πιο ολοκληρωμένη εικόνα, καθώς και τους παράγοντες που ωθούν στην εξαπόλυση απειλών και τα κίνητρα των αυτουργών τους.

Κίνητρα

79 Τα νομικά και οικονομικά κίνητρα που παρέχονται σε οργανισμούς προκειμένου να γνωστοποιούν τα συμβάντα και να μοιράζονται πληροφορίες σχετικά με αυτά εξακολουθούν να είναι υπερβολικά περιορισμένα. Φοβούμενοι την ενδεχόμενη προσβολή της φήμης τους, πολλοί οργανισμοί προτιμούν ακόμη να χειρίζονται τις κυβερνοεπιθέσεις που υφίστανται με διακριτικότητα ή να καταβάλλουν στους δράστες τα ποσά που ζητούν. Μένει να διαπιστωθεί η αποτελεσματικότητα της οδηγίας για την ασφάλεια δικτύων και πληροφοριών στην αύξηση του αριθμού των κοινοποιήσεων. Η Επιτροπή προσβλέπει σε βελτιώσεις κυρίως σε εθνικό επίπεδο, αλλά η πράξη για την ασφάλεια στον κυβερνοχώρο θα προσθέσει μια πανενωσιακή προοπτική[111].

80 Ως αγοραστές ψηφιακών προϊόντων και υπηρεσιών, οι δημόσιες αρχές ασκούν σημαντική πίεση στους προμηθευτές, περιλαμβάνοντας ορισμένα πρότυπα στους όρους των δημόσιων συμβάσεων που συνάπτουν, ενώ το ίδιο ισχύει και με τη χρηματοδότηση προγραμμάτων έρευνας (παραδείγματος χάριν, απαιτώντας την υιοθέτηση συγκεκριμένων τεχνικών προτύπων, όπως το πρωτόκολλο ίντερνετ IPv6 για την καταπολέμηση της κυβερνοεγκληματικότητας). Επί του παρόντος, ωστόσο, δεν υπάρχει κοινό πλαίσιο για τις δημόσιες συμβάσεις που αφορούν υποδομές στον τομέα της κυβερνοασφάλειας[112]. Η Επιτροπή μπορεί να κάνει πολλά στον τομέα αυτό. Το πρόγραμμα «Ψηφιακή Ευρώπη» που προτείνεται για το επόμενο πολυετές δημοσιονομικό πλαίσιο έχει ως στόχο να αντιμετωπίσει το πρόβλημα των περιορισμένων μέχρι στιγμής επενδύσεων για την προμήθεια των πλέον σύγχρονων τεχνολογιών στον τομέα της κυβερνοασφάλειας.

81 Χάρη στη ρυθμιστική ικανότητά της, η Επιτροπή μπορεί να διασφαλίσει την ανάπτυξη των κατάλληλων προτύπων, τα οποία εν συνεχεία θα υιοθετηθούν ευρέως προκειμένου να ενισχυθεί η ασφάλεια. Η Επιτροπή και η Ευρωπόλ συνεργάζονται με φορείς διακυβέρνησης του διαδικτύου, όπως το ICANN (βλέπε σημείο ***38***) και το REIPE-NCC[113], κάτι που είναι αναγκαίο για την ανάπτυξη κατάλληλων δομών για την καταπολέμηση του κυβερνοεγκλήματος, οι οποίες θα διευκολύνουν το έργο των αρχών επιβολής του νόμου και των δικαστικών αρχών.

Πρόκληση 7: Ενίσχυση των δεξιοτήτων και αύξηση της ενημέρωσης και ευαισθητοποίησης

82 Ο ENISA έχει επισημάνει ότι οι χρήστες διαδραματίζουν καίριο ρόλο στην αντιμετώπιση των κυβερνοεπιθέσεων και ότι η ενίσχυση των δεξιοτήτων και η αύξηση

της εκπαίδευσης και της ενημέρωσης είναι ουσιώδους σημασίας για τη δημιουργία μιας κυβερνοανθεκτικής κοινωνίας[114]. Είτε στο πλαίσιο της εργασίας τους είτε στην προσωπική τους ζωή, όσοι είναι ικανοί να εντοπίζουν τις προειδοποιητικές ενδείξεις και γνωρίζουν τις κατάλληλες τεχνικές, μπορούν να καθυστερήσουν ή να αποτρέψουν επιθέσεις.

83 Ιδιαίτερη ανησυχία προκαλεί η αυξανόμενη ασυμμετρία μεταξύ, αφενός, της τεχνογνωσίας που απαιτείται για τη διάπραξη ενός κυβερνοεγκλήματος ή για την εξαπόλυση μιας κυβερνοεπίθεσης και, αφετέρου, των δεξιοτήτων που απαιτούνται για την αντιμετώπιση ενός τέτοιου συμβάντος. Το μοντέλο «crime-as-a-service» έχει μειώσει τους φραγμούς εισόδου στην αγορά του κυβερνοεγκλήματος: άτομα που δεν διαθέτουν τις τεχνικές γνώσεις για την κατασκευή τέτοιων εργαλείων, μπορούν πλέον να νοικιάζουν δίκτυα προγραμμάτων ρομπότ (botnets), εργαλεία εκμετάλλευσης ατελειών (exploit kits) ή πακέτα λυτρισμικού.

Κατάρτιση, δεξιότητες και ανάπτυξη ικανοτήτων

84 Ο κόσμος βρίσκεται αντιμέτωπος με μια αυξανόμενη έλλειψη δεξιοτήτων στον τομέα της κυβερνοασφάλειας. Το έλλειμμα εξειδικευμένου εργατικού δυναμικού αυξήθηκε κατά 20 % από το 2015[115]. Οι παραδοσιακές μέθοδοι προσλήψεων δεν αρκούν για την κάλυψη της ζήτησης, μεταξύ άλλων για τις διευθυντικές θέσεις ή τις θέσεις για τις οποίες απαιτούνται δεξιότητες και γνώσεις σε περισσότερους τομείς[116]. Σχεδόν το 90 % του εργατικού δυναμικού στον τομέα της κυβερνοασφάλειας παγκοσμίως είναι άνδρες. Αυτή η μη ισόρροπη εκπροσώπηση των φύλων περιορίζει περαιτέρω τη δεξαμενή άντλησης ταλέντων[117]. Επιπλέον, στα πανεπιστήμια δεν διδάσκεται επαρκής αριθμός μαθημάτων σχετικών με τον κυβερνοχώρο στο πλαίσιο μη τεχνικών προγραμμάτων σπουδών.

85 Οι ανάγκες για εκπαίδευση και κατάρτιση είναι μεγάλες σε όλα τα επίπεδα, μεταξύ των δημόσιων υπαλλήλων, των στελεχών των αρχών επιβολής του νόμου, των δικαστικών λειτουργών, των μελών των ενόπλων δυνάμεων και των εκπαιδευτικών. Παραδείγματος χάριν, τα δικαστήρια πρέπει να είναι σε θέση να αντιμετωπίζουν τις ταχέως μεταβαλλόμενες τεχνικές ιδιαιτερότητες της κυβερνοεγκληματικότητας και των θυμάτων της[118]. Επί του παρόντος, δεν υπάρχουν πανευρωπαϊκά πρότυπα για την επιμόρφωση και την πιστοποίηση[119]. Σε επίπεδο θεσμικών οργάνων της ΕΕ, είναι σημαντικό να διασφαλίζεται η ύπαρξη υπαλλήλων με το σωστό μείγμα δεξιοτήτων. Σε αντίθετη περίπτωση, τα θεσμικά όργανα ενδέχεται να μην είναι σε θέση να καθορίζουν ορθά την εμβέλεια των προγραμμάτων ή να προσδιορίζουν τους κατάλληλους εταίρους και τις ανάγκες ασφάλειας ή να μην διαθέτουν επαρκή ικανότητα διαχείρισης των προγραμμάτων. Οι ελλείψεις αυτές με τη σειρά τους είναι

δυνατό να υπονομεύσουν την αποτελεσματικότητα των προγραμμάτων ή την ανάπτυξη των πολιτικών της ΕΕ.

86 Παρά το γεγονός ότι αρμόδια για τις εκπαιδευτικές πολιτικές είναι τα κράτη μέλη, σε ενωσιακό επίπεδο πραγματοποιούνται ήδη πολυάριθμες δραστηριότητες κατάρτισης (βλέπε ***πίνακα 2***) και ασκήσεις (βλέπε ***πλαίσιο 4***). Η ΕΕ μπορεί να διευκολύνει την ενσωμάτωση ευρωπαϊκών προτύπων στα εκπαιδευτικά προγράμματα που καλύπτουν όλους τους σχετικούς κλάδους[120]. Στον τομέα της ψηφιακής εγκληματολογικής έρευνας, παραδείγματος χάριν, είναι αναγκαία η ύπαρξη κοινών προτύπων κατάρτισης, προκειμένου να διευκολύνεται η συγκέντρωση αποδεικτικών στοιχείων που θα είναι παραδεκτά στα κράτη μέλη. Λόγω του διασυνοριακού χαρακτήρα της κυβερνοεγκληματικότητας, στη διερεύνηση και τη δίωξη ενός εγκλήματος είναι δυνατό να εμπλέκονται οι αρχές πολλών κρατών μελών, γεγονός που καθιστά αναγκαία μια κοινή κατάρτιση σε επίπεδο ΕΕ. Ωστόσο, ο CEPOL, ο οργανισμός της ΕΕ για την κατάρτιση στον τομέα της επιβολής του νόμου, έχει επισημάνει ότι πάνω από τα δύο τρίτα των κρατών μελών δεν παρέχουν τακτική κατάρτιση για τα ζητήματα του κυβερνοχώρου στους υπαλλήλους των αρχών επιβολής του νόμου[121]. Η ΕΕ θα μπορούσε επίσης ενδεχομένως να αναζητήσει τρόπους ανάπτυξης συνεργιών στους τομείς της στρατιωτικής και μη στρατιωτικής εκπαίδευσης και κατάρτισης[122]. Τούτου λεχθέντος, ο ENISA διαπίστωσε ότι, παρά την πληθώρα δυνατοτήτων κατάρτισης σε κρίσιμους τομείς, αυτές δεν καλύπτουν επαρκώς την ανθεκτικότητα των υποδομών ζωτικής σημασίας[123].

Πίνακας 2 - Ορισμένες από τις πρωτοβουλίες κατάρτισης της ΕΕ που συνδέονται με τον κυβερνοχώρο

Έργα του Ευρωπαϊκού Οργανισμού Άμυνας, π.χ. στήριξη ασκήσεων του ιδιωτικού τομέα και το έργο Cyber Ranges	Δίκτυο Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας (που παρέχει πολιτικο-στρατιωτική κατάρτιση), συμπεριλαμβανομένης της πλατφόρμας εκπαίδευσης, ασκήσεων κατάρτισης και αξιολόγησης για τον κυβερνοχώρο	Προγράμματα κατάρτισης του ENISA σε τομείς που ενδεχομένως δεν καλύπτονται από τα αντίστοιχα προγράμματα που προσφέρονται στην αγορά
Προγράμματα κατάρτισης της Ευρωπόλ, του CEPOL ή της ECTEG[124] συμπεριλαμβανομένου του μοντέλου διακυβέρνησης στον τομέα της κατάρτισης και του πλαισίου ικανοτήτων κατάρτισης (συμπεριλαμβανομένης της πιστοποίησης)	Δίκτυο κέντρων ικανοτήτων και ερευνητικό κέντρο ικανοτήτων (πρόταση)	Μέτρα για την κρυπτογράφηση που προτείνονται στην 11η έκθεση προόδου για την Ένωση Ασφάλειας
Συνεργασία ΕΕ-ΝΑΤΟ σχετικά με την κατάρτιση και την εκπαίδευση στον τομέα της κυβερνοάμυνας	Στρατιωτικό πρόγραμμα Erasmus	Ευρωπαϊκό Δίκτυο Κατάρτισης Δικαστικών

Πηγή: ΕΕΣ.

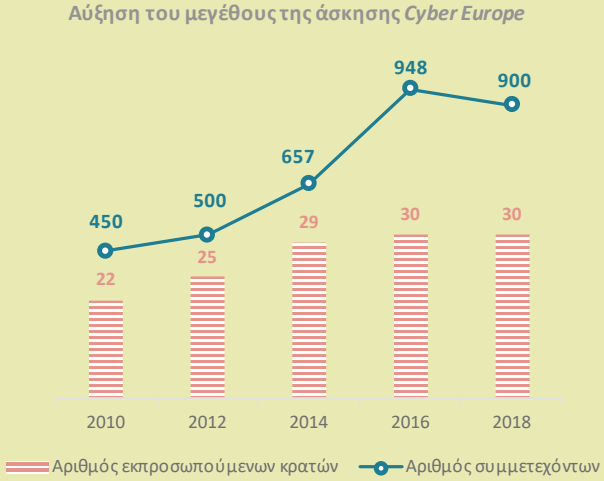
87 Η ΕΕ έχει τοποθετήσει ειδικούς σε θέματα ασφάλειας και καταπολέμησης της τρομοκρατίας σε 17 αντιπροσωπείες προκειμένου να ενισχύσει τη σύνδεση μεταξύ της εσωτερικής και της εξωτερικής ασφάλειας της ΕΕ[125]. Παρά τους περιορισμούς σε επίπεδο πόρων, η ενίσχυση της τεχνογνωσίας στους τομείς που συνδέονται με τον κυβερνοχώρο θα μπορούσε να συμβάλει στην υλοποίηση των κατάλληλων έργων, καθώς και στον εντοπισμό συνεργιών με άλλα προγράμματα ή πηγές χρηματοδότησης[126]. Θα αναδείκνυε επίσης τη θεματολογία της κυβερνοασφάλειας στο πλαίσιο του πολιτικού διαλόγου, παρά τον ανταγωνισμό με πολλές άλλες προτεραιότητες, όπως η μετανάστευση, το οργανωμένο έγκλημα ή η επιστροφή αλλοδαπών μαχητών.

Πλαίσιο 4

Ασκήσεις

Οι ασκήσεις αποτελούν σημαντικές συνιστώσες της εκπαίδευσης και κατάρτισης σχετικά με τον κυβερνοχώρο, καθώς προσφέρουν εξαιρετικές ευκαιρίες για τη βελτίωση της ετοιμότητας μέσω της υποβολής των ικανοτήτων σε δοκιμές, της δοκιμής αντιδράσεων σε πραγματικές συνθήκες και της δημιουργίας δικτύων σχέσεων συνεργασίας. Από το 2010, η συχνότητά τους έχει αυξηθεί αισθητά.

Οι συμμετέχοντες λαμβάνουν μέρος είτε με φυσική παρουσία είτε εξ αποστάσεως. Μετά τις ασκήσεις πραγματοποιούνται αξιολογήσεις προκειμένου να εντοπιστούν τα διδάγματα που αντλήθηκαν, αν και αυτά μπορεί να μην έχουν ακόμη διαχυθεί στα στρατηγικά/πολιτικά, επιχειρησιακά και τεχνικά στρώματα[127].



Πηγή: ΕΕΣ, βάσει εγγράφων του ENISA.

Οι εμβληματικές ασκήσεις της ΕΕ και του ΝΑΤΟ –η ανά διετία άσκηση Cyber Europe (επιχειρησιακή) και η ετήσια άσκηση «Locked Shields» (τεχνική)– προσελκύουν περισσότερους από 1 000 συμμετέχοντες από περίπου 30 συμμετέχοντα κράτη. Και οι δύο διαδικασίες επικεντρώνονται στην προστασία και τη διατήρηση υποδομών ζωτικής σημασίας στο πλαίσιο σεναρίων προσομοίωσης επιθέσεων. Η εμβέλεια των ασκήσεων διευρύνθηκε σημαντικά, καθώς αμφότερες πλέον περιλαμβάνουν στοιχεία πολιτικής από τους τομείς των μέσων ενημέρωσης, της νομικής και των οικονομικών, προκειμένου επαγγελματίες του χώρου να αποκτήσουν επίγνωση της κατάστασης. Οι παράλληλες και συντονισμένες (στρατηγικές) ασκήσεις PACE έχουν ως στόχο την υποβολή της αλληλεπίδρασης ΕΕ-ΝΑΤΟ σε δοκιμασίες στο πλαίσιο ενός σεναρίου υβριδικής κρίσης.

Αυτές δεν είναι οι μόνες διεθνείς ασκήσεις. Ο ENISA διοργανώνει ετησίως την άσκηση cyber challenge, στο πλαίσιο της οποίας ομάδες ανταγωνίζονται να επιλύσουν προβλήματα που σχετίζονται με την ασφάλεια, τα οποία αφορούν π.χ. προβλήματα ασφάλειας του διαδικτύου και των κινητών τηλεφώνων, κρυπτογραφικά παζλ, ανάδρομη τεχνική έρευνα, ζητήματα δεοντολογίας και εγκληματολογίας. Η EU CYBRID, η πρώτη άσκηση σε επίπεδο υπουργών, πραγματοποιήθηκε τον Σεπτέμβριο του 2017 και επικεντρώθηκε στη λήψη στρατηγικών αποφάσεων. Το 2018 δρομολογήθηκε η άσκηση Crossed Swords που συνδιοργανώνεται από το ΝΑΤΟ, για τη βελτίωση των προβληματικών στοιχείων

της άσκησης Locked Shields. Το NATO διοργανώνει επίσης τις ασκήσεις Cyber Coalition.

Μια βασική πρόκληση είναι να εξασφαλίζεται η ενεργός συμμετοχή όλων των σημαντικών παραγόντων και ο συντονισμός όλων των ασκήσεων, να αποφεύγονται οι αλληλοεπικαλύψεις και να ανταλλάσσονται κατά τρόπο αποδοτικό τα διδάγματα που αντλούνται.

Ενημέρωση και ευαισθητοποίηση

88 Είναι συχνό το φαινόμενο οι πολίτες να χρησιμοποιούνται για την πραγματοποίηση επιθέσεων και να γίνονται φορείς διάδοσης της παραπληροφόρησης, καθώς είναι πιθανό να εκτεθούν εν αγνοία τους σε κενά ασφάλειας χρησιμοποιώντας φθηνές και ευρέως διαδεδομένες συσκευές και λογισμικά ή να πέσουν θύματα κοινωνικής μηχανικής. Ως εκ τούτου, η ενημέρωση και η ευαισθητοποίηση είναι καίριας σημασίας για την ανάπτυξη κυβερνοανθεκτικότητας. Αυτό, ωστόσο δεν είναι καθόλου εύκολο, δεδομένου ότι είναι δύσκολο για τους μη ειδικούς να κατανοήσουν την πολυπλοκότητα της κυβερνοασφάλειας και τους συναφείς κινδύνους.

89 Ο Ευρωπαϊκός μήνας για την ασφάλεια στον κυβερνοχώρο (European Cyber Security Awareness Month, ECSM) που διοργανώνεται ετησίως, καθώς και η Ημέρα Ασφαλέστερου Διαδικτύου αποτελούν ενδεικτικές προσπάθειες αύξησης της ενημέρωσης και της ευαισθητοποίησης. Επτά χώρες εκτός της ΕΕ συμμετέχουν πλέον στον ECSM[128]. Η εκστρατεία «Say No!» της Ευρωπόλ επιδιώκει τη μείωση του κινδύνου που διατρέχουν τα παιδιά να πέσουν θύματα σεξουαλικού εξαναγκασμού και εκβιασμού στο διαδίκτυο. Η μείωση του κινδύνου έχει μεγάλη σημασία καθώς προς το παρόν είναι λίγα τα θύματα επιθέσεων που καταγγέλλουν τα εγκλήματα αυτά στην αστυνομία[129]. Η Επιτροπή αναγνωρίζει ότι η στρατηγική για την κυβερνοασφάλεια υπήρξε μόνον μερικώς αποτελεσματική όσον αφορά την ενημέρωση και την ευαισθητοποίηση πολιτών και επιχειρήσεων για τα ζητήματα αυτά[130]. Αυτό οφείλεται στην κλίμακα του εγχειρήματος, τους περιορισμένους πόρους, την άνιση δέσμευση των κρατών μελών, καθώς και στην έλλειψη επιστημονικών αποδεικτικών στοιχείων σχετικά με τον βέλτιστο τρόπο αύξησης και μέτρησης της ενημέρωσης.

90 Η πρόκληση για την Επιτροπή και τους αρμόδιους οργανισμούς είναι να διασφαλίζουν ότι τα μέτρα ενημέρωσης είναι καλά στοχευμένα και τυγχάνουν της κατάλληλης προβολής, προάγουν τη συμμετοχικότητα, παρακολουθούν τις εξελίξεις στο τοπίο των απειλών και αποφεύγουν ανεπιθύμητες παρενέργειες όπως η «κόπωση

ασφάλειας»[131], καθώς και να αναπτύξουν μεθόδους και δείκτες μέτρησης για την αξιολόγηση της αποτελεσματικότητας των μέτρων αυτών. Αυτό θα πρέπει να ισχύει εξίσου στους κόλπους των ίδιων των θεσμικών οργάνων της ΕΕ, όπου επίσης πρέπει να αυξηθεί η εγρήγορση[132].

Πρόκληση 8: Βελτίωση της ανταλλαγής πληροφοριών και του συντονισμού

91 Απαραίτητη προϋπόθεση για την κυβερνοασφάλεια είναι η συνεργασία μεταξύ του δημόσιου και του ιδιωτικού τομέα, κυρίως όσον αφορά την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών. Η εμπιστοσύνη είναι καίριας σημασίας σε όλα τα επίπεδα για τη δημιουργία του κατάλληλου περιβάλλοντος για τη διασυνοριακή ανταλλαγή ευαίσθητων πληροφοριών. Ο ανεπαρκής συντονισμός οδηγεί σε κατακερματισμό, αλληλοεπικάλυψη προσπαθειών και απώλεια εμπειρογνωσίας λόγω της διασποράς της. Ο αποτελεσματικός συντονισμός μπορεί να οδηγήσει σε απτές επιτυχίες, όπως το κλείσιμο αγορών που λειτουργούν στο σκοτεινό διαδίκτυο (darkweb)[133]. Παρά την πρόοδο που επιτεύχθηκε τα τελευταία χρόνια, τα επίπεδα εμπιστοσύνης εξακολουθούν να είναι «ανεπαρκή»[134] σε επίπεδο ΕΕ και σε ορισμένα κράτη μέλη[135].

Συντονισμός μεταξύ των θεσμικών οργάνων και με τα κράτη μέλη της ΕΕ

92 Ένας από τους στόχους της στρατηγικής για την κυβερνοασφάλεια και των συνεργατικών δομών που θεσπίστηκαν με την οδηγία NIS, ήταν η ενίσχυση της εμπιστοσύνης μεταξύ των ενδιαφερομένων. Κατά την αξιολόγηση της στρατηγικής αναγνωρίστηκε ότι έχουν τεθεί τα θεμέλια για τη στρατηγική και επιχειρησιακή συνεργασία σε επίπεδο ΕΕ[136]. Εντούτοις, ο συντονισμός γενικώς είναι ανεπαρκής[137]. Η πρόκληση είναι να διασφαλιστεί ότι η ανταλλαγή πληροφοριών δεν είναι απλώς ουσιαστική, αλλά καθιστά επίσης δυνατή την απόκτηση ολοκληρωμένης εικόνας. Για τον σκοπό αυτό σημαντικός παράγοντας είναι η επίτευξη κοινής αντίληψης βάσει αποδεκτής ορολογίας (βλέπε ***πλαίσιο 5***).

93 Στην αξιολόγηση του ENISA επισημάνθηκε, ωστόσο, ότι η προσέγγιση της ΕΕ όσον αφορά την κυβερνοασφάλεια δεν ήταν επαρκώς συντονισμένη, με αποτέλεσμα την απουσία συνεργιών μεταξύ των δραστηριοτήτων του ENISA και εκείνων άλλων ενδιαφερομένων. Οι μηχανισμοί συνεργασίας δεν έχουν ακόμη ωριμάσει αρκετά[138]. Με την πράξη για την ασφάλεια στον κυβερνοχώρο επιδιώκεται να αντιμετωπιστεί το πρόβλημα αυτό μέσω της ενίσχυσης του συντονιστικού ρόλου του ENISA. Η επιθυμία

για ενίσχυση της συνεργασίας ήταν το σκεπτικό στο οποίο βασίστηκε το μνημόνιο συνεννόησης που υπογράφηκε το 2018 μεταξύ του ENISA, του EOA, του κέντρου EC3 της Ευρωπόλ και της CERT-EE[139]. Προτεραιότητα της Επιτροπής κατά τα προσεχή έτη θα είναι η εξασφάλιση της ευθυγράμμισης των πολιτικών πρωτοβουλιών, των αναγκών και των επενδυτικών προγραμμάτων, προκειμένου να αντιμετωπιστεί ο κατακερματισμός και να δημιουργηθούν συνεργίες[140].

94 Τα καθήκοντα συντονισμού βαρύνουν διάφορους θεσμικούς φορείς. Η ειδική ομάδα για την Ένωση Ασφάλειας συστάθηκε για να διαδραματίσει κεντρικό ρόλο στον συντονισμό των διαφόρων Γενικών Διευθύνσεων της Επιτροπής με σκοπό την προώθηση της ημερήσιας διάταξης της Ένωσης για την ασφάλεια[141]. Η ΓΔ Επικοινωνιακών Δικτύων, Περιεχομένου και Τεχνολογιών προεδρεύει της επιμέρους ομάδας εργασίας της ειδικής ομάδας, για την κυβερνοασφάλεια.

95 Στο Συμβούλιο, τα ζητήματα κυβερνοασφάλειας χειρίζεται η οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου (HWP), η οποία συντονίζει τις εργασίες για τα στρατηγικά και οριζόντια ζητήματα που άπτονται του κυβερνοχώρου και συμβάλλει στην προετοιμασία ασκήσεων και στην αξιολόγηση των αποτελεσμάτων τους. Συνεργάζεται στενά με την Επιτροπή Πολιτικής και Ασφάλειας, η οποία διαδραματίζει κεντρικό ρόλο στη λήψη αποφάσεων σχετικά με τυχόν διπλωματικά μέτρα που αφορούν τον κυβερνοχώρο (βλέπε ***πλαίσιο 6*** στο επόμενο κεφάλαιο). Δεδομένου ότι η κυβερνοασφάλεια αποτελεί οριζόντιο θέμα, ο συντονισμός όλων των σχετικών συμφερόντων δεν είναι απλός: το τελευταίο διάστημα 24 διαφορετικές ομάδες εργασίας και προπαρασκευαστικά όργανα ασχολήθηκαν με θέματα που αφορούν τον κυβερνοχώρο[142].

96 Οι δύο τελευταίες νομοθετικές προτάσεις για την ενίσχυση του ENISA (2017) και για τη δημιουργία δικτύου κέντρων ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και ερευνητικού κέντρου ικανοτήτων (2018) σχεδιάστηκαν ειδικά προκειμένου να αντιμετωπιστεί ο κατακερματισμός και η αλληλοεπικάλυψη των προσπαθειών. Κινητήρια δύναμη πίσω από το δίκτυο κέντρων ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και του ερευνητικού κέντρου ικανοτήτων ήταν η ανάγκη να καλυφθεί το κενό που δεν καλύπτουν οι δομές συνεργασίας της οδηγίας NIS, οι οποίες δεν σχεδιάστηκαν για να στηρίξουν την ανάπτυξη λύσεων «αιχμής».

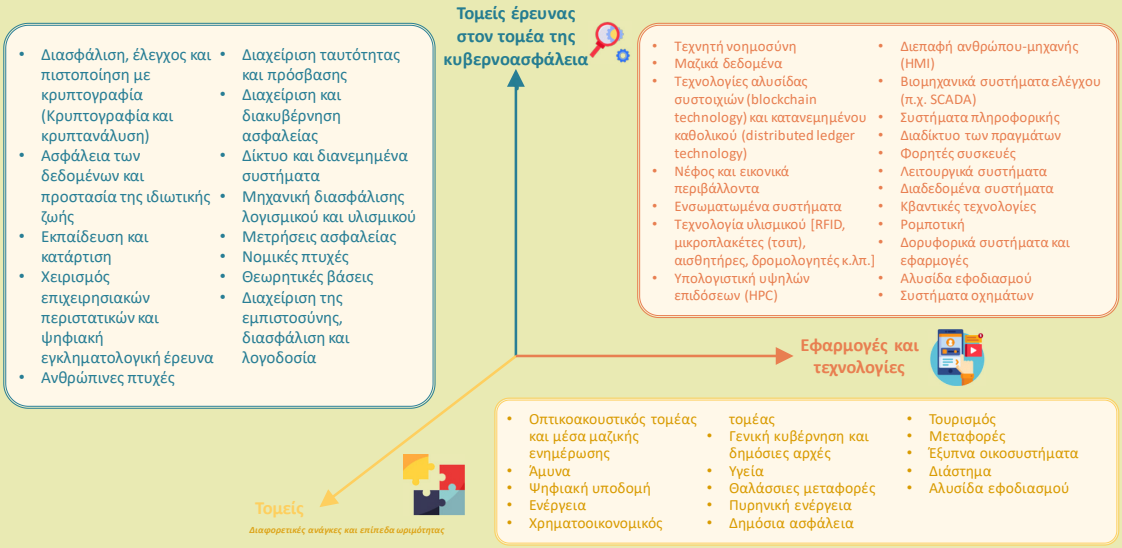
Πλαίσιο 5

Προσπάθεια συνεννόησης στην ίδια κυβερνογλώσσα: *τεχνολογική συνοχή*

Η ορολογική σαφήνεια βελτιώνει την επίγνωση της κατάστασης και τον συντονισμό[143] και συμβάλλει στον προσδιορισμό του τι ακριβώς συνιστά απειλή και κίνδυνο.

Το Κοινό Κέντρο Ερευνών (JRC) της Επιτροπής ανέπτυξε πρόσφατα μια αναθεωρημένη ερευνητική ταξινομία αντλώντας στοιχεία από διάφορα διεθνή πρότυπα[144]. Στόχος της είναι να αποτελέσει σημείο αναφοράς για τους ερευνητικούς φορείς σε όλη την Ευρώπη.

Ταξινομία κυβερνοασφάλειας



Πηγή: ΕΕΣ, προσαρμογή από στοιχεία της Ευρωπαϊκής Επιτροπής.

Μέχρι πρόσφατα, τα θεσμικά όργανα και οι οργανισμοί της ΕΕ δεν χρησιμοποιούσαν κοινούς ορισμούς. Η κατάσταση αυτή αλλάζει. Στο πλαίσιο του σχεδίου στρατηγικής της, η ομάδα συνεργασίας ανέπτυξε ταξινομία συμβάντων με στόχο τη διευκόλυνση της αποδοτικής διασυνοριακής συνεργασίας.

Συνεργασία και ανταλλαγή πληροφοριών με τον ιδιωτικό τομέα

97 Η συνεργασία μεταξύ των δημόσιων αρχών και του ιδιωτικού τομέα είναι ουσιώδους σημασίας για την ενίσχυση του επιπέδου κυβερνοασφάλειας συνολικά.

Παρ' όλα αυτά, όπως διαπίστωσε η Επιτροπή στην αξιολόγηση της στρατηγικής για την ασφάλεια στον κυβερνοχώρο το 2017, η ανταλλαγή πληροφοριών μεταξύ ιδιωτικών φορέων και μεταξύ δημόσιου και ιδιωτικού τομέα δεν ήταν ακόμη η βέλτιστη δυνατή λόγω της απουσίας αξιόπιστων μηχανισμών αναφοράς και κινήτρων για την ανταλλαγή πληροφοριών[145], γεγονός που εμποδίζει την επίτευξη των στρατηγικών στόχων. Η Επιτροπή επεσήμανε επίσης την απουσία αποδοτικού μηχανισμού συνεργασίας στο πλαίσιο του οποίου τα κράτη μέλη θα συνεργάζονταν για τη στρατηγική ενίσχυση των βιώσιμων βιομηχανικών ικανοτήτων στην κατάλληλη κλίμακα[146].

98 Τα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) είναι οργανισμοί που συστάθηκαν για να παρέχουν πλατφόρμες και πόρους για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του δημόσιου και του ιδιωτικού τομέα, καθώς και για τη συγκέντρωση πληροφοριών σχετικά με τις κυβερνοαπειλές. Στόχος τους είναι η οικοδόμηση εμπιστοσύνης μέσω της ανταλλαγής εμπειριών, γνώσεων και αναλύσεων, ιδίως όσον αφορά τα βαθύτερα αίτια, τα συμβάντα και τις απειλές. Εθνικά και τομεακά ISAC υπάρχουν ήδη σε πολλά κράτη μέλη, αλλά σε ευρωπαϊκό επίπεδο είναι ακόμη σχετικά περιορισμένα[147]. Ωστόσο, αντιμετωπίζουν ορισμένες προκλήσεις (περιορισμούς σε επίπεδο πόρων, δυσκολίες στην αξιολόγηση των επιτευγμάτων τους, διασφάλιση των κατάλληλων δομών για τη συμμετοχή τόσο του δημόσιου όσο και του ιδιωτικού τομέα, συμμετοχή των αρχών επιβολής του νόμου) που θα πρέπει να ξεπεραστούν προκειμένου να μπορέσουν να συμβάλουν στην εφαρμογή της οδηγίας NIS και στην οικοδόμηση ικανοτήτων ασφάλειας σε ευρωπαϊκό επίπεδο[148].

99 Η στενή συνεργασία με τον ιδιωτικό τομέα είναι ιδιαίτερα σημαντική για την καταπολέμηση του σύνθετου κυβερνοεγκλήματος, αλλά ο βαθμός αποδοτικότητας ποικίλλει μεταξύ των κρατών μελών και εξαρτάται από το επίπεδο εμπιστοσύνης[149]. Ωστόσο, το κέντρο EC3 της Ευρωπόλ έχει συγκροτήσει μια σειρά συμβουλευτικών ομάδων με φορείς του ιδιωτικού τομέα, θεσμικά όργανα και οργανισμούς της ΕΕ και άλλους διεθνείς οργανισμούς για τη βελτίωση της συνεργασίας μέσω της δικτύωσης, της ανταλλαγής στρατηγικών πληροφοριών και της συνεργασίας. Οι εν λόγω ομάδες εργάζονται σύμφωνα με σχέδια ευθυγραμμισμένα με τους στόχους του κύκλου πολιτικής της ΕΕ[150]. Η κατάχρηση της κρυπτογράφησης για εγκληματικούς σκοπούς είναι ένας τομέας που βρίθει προκλήσεων που καθιστούν αναγκαία τη μεγαλύτερη συνεργασία με τον ιδιωτικό τομέα. Το κέντρο EC3 της Ευρωπόλ εξετάζει επί του παρόντος εναλλακτικές επιλογές για τη φιλοξενία στη J-CAT (βλέπε σημείο ***62***) εμπειρογνωμόνων από τον ιδιωτικό τομέα και την πανεπιστημιακή κοινότητα για σύντομα χρονικά διαστήματα.

100 Η απουσία αποδοτικών μηχανισμών συνεργασίας επηρεάζει αρνητικά τις μη στρατιωτικές και τις αμυντικές κοινότητες, τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Μερικοί από τους τομείς που συνιστούν κοινή πρόκληση είναι η κρυπτογράφηση, τα ασφαλή ενσωματωμένα συστήματα, η ανίχνευση κακόβουλου λογισμικού, οι τεχνικές προσομοίωσης και απεικόνισης, η προστασία των συστημάτων δικτύων και επικοινωνίας και η τεχνολογία ταυτοποίησης. Η προώθηση της πολιτικοστρατιωτικής συνεργασίας και η στήριξη της έρευνας και της τεχνολογίας (ιδίως μέσω της υποστήριξης των ΜΜΕ) είναι δύο από τις προτεραιότητες του επικαιροποιημένου πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση του 2018).

Σημεία προβληματισμού – Ενίσχυση της ανθεκτικότητας

- Πώς μπορεί να επιτευχθεί η κατάλληλη ισορροπία σε ενωσιακό επίπεδο μεταξύ, αφενός, της ανάγκης να ενσωματωθεί η διάσταση της κυβερνοασφάλειας σε άλλες ενωσιακές πολιτικές και να διασφαλιστεί ο αποδοτικός συντονισμός μεταξύ των διαφόρων παραγόντων και, αφετέρου, της διασποράς των αρμοδιοτήτων;
- Πόσο επαρκώς προετοιμασμένα είναι τα θεσμικά όργανα και οι οργανισμοί της ΕΕ για την επόμενη μείζονα επίθεση που θα εξαπολυθεί άμεσα εναντίον τους;
- Πώς μπορούν οι οργανισμοί της ΕΕ που ασχολούνται με θέματα του κυβερνοχώρου να καταστούν ελκυστικότεροι ώστε να προσελκύσουν ταλέντα;
- Ποια περαιτέρω μέτρα πρέπει να ληφθούν για τη διασφάλιση επαρκούς ικανότητας στα θεσμικά όργανα και τους οργανισμούς της ΕΕ ώστε να δημιουργηθεί ένα συνεκτικό πλαίσιο για την αξιολόγηση των κινδύνων και των απειλών;
- Με ποιους τρόπους αντιμετωπίζουν οι ευρωπαϊκές εποπτικές αρχές (Ευρωπαϊκή Αρχή Τραπεζών, Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών και Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων) τα εγγενή τρωτά σημεία του χρηματοπιστωτικού τομέα στον κυβερνοχώρο, και ποια διδάγματα μπορούν να αντληθούν για άλλους τομείς;
- Δεδομένης της συνολικής έλλειψης εμπειρογνωσίας, πώς μπορεί να χρησιμοποιηθεί με τον καλύτερο τρόπο η τεχνική βοήθεια που χορηγεί η ΕΕ σε δημόσιες αρχές ώστε να βελτιωθεί κατά το μέγιστο δυνατό η κυβερνοανθεκτικότητα;
- Πώς μπορούν η ΕΕ και τα κράτη μέλη να εξασφαλίσουν εποικοδομητική παρουσία στις διεθνείς συζητήσεις για τη διαμόρφωση της διακυβέρνησης και των προτύπων του κυβερνοχώρου, καθώς και την προώθηση των αξιών της ΕΕ;
- Ποια μέτρα ενημέρωσης και ευαισθητοποίησης σε επίπεδο ΕΕ και κρατών μελών (συμπεριλαμβανομένων των προσπαθειών πρόληψης) είναι πράγματι αποτελεσματικά, και τι μπορεί να κάνει η ΕΕ για να εφαρμοστούν σε ευρύτερη κλίμακα;
- Με ποιον τρόπο μπορεί να συμβάλει η ΕΕ στην προώθηση της ισόρροπης εκπροσώπησης των φύλων στον τομέα της κυβερνοασφάλειας;
- Πώς μπορούν η ΕΕ και τα κράτη μέλη να ενισχύσουν τις συνεργίες μεταξύ των μη στρατιωτικών και των αμυντικών κοινοτήτων, σύμφωνα με το πλαίσιο πολιτικής για την κυβερνοάμυνα (επικαιροποίηση του 2018);

Αποτελεσματική αντίδραση σε κυβερνοπεριστατικά

101 Ο σχεδιασμός μιας αποτελεσματικής αντιμετώπισης των κυβερνοεπιθέσεων έχει θεμελιώδη σημασία για την όσο το δυνατόν ταχύτερη αναχαίτισή τους. Είναι ιδιαίτερα σημαντικό οι κρίσιμοι τομείς, τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ να είναι σε θέση να αντιδράσουν τάχιστα και κατά τρόπο συντονισμένο. Για τον σκοπό αυτό είναι απαραίτητη η έγκαιρη ανίχνευση.

Πρόκληση 9: Αποτελεσματική ανίχνευση και αντιμετώπιση

Ανίχνευση και γνωστοποίηση

102 Τα κοινά εργαλεία ανίχνευσης καθιστούν δυνατή την αντιμετώπιση της συντριπτικής πλειονότητας των επιθέσεων καθημερινά[151]. Εντούτοις, λόγω της ολοένα μεγαλύτερης πολυπλοκότητας των ψηφιακών συστημάτων, είναι αδύνατη η αποτροπή όλων των επιθέσεων. Ο βαθμός πολυπλοκότητάς τους σημαίνει ότι συχνά μπορεί να παρέλθει σημαντικό χρονικό διάστημα μέχρι να αποκαλυφθούν επιθέσεις. Σύμφωνα με τους εμπειρογνώμονες, πρέπει συνεπώς να δοθεί έμφαση στην ταχεία ανίχνευση και την άμυνα[152]. Ωστόσο, ορισμένα εργαλεία ανίχνευσης, όπως η αυτοματοποίηση, η μηχανική μάθηση και η συμπεριφορική ανάλυση, που επιδιώκουν τη μείωση των κινδύνων και την ανάλυση και άντληση διδαγμάτων από τη συμπεριφορά του συστήματος, εμφανίζουν χαμηλά ποσοστά υιοθέτησης από τις επιχειρήσεις[153]. Αυτό οφείλεται εν μέρει στην παραγωγή ψευδώς θετικών αποτελεσμάτων, βάσει των οποίων μη απειλητικές δραστηριότητες παρουσιάζονται εσφαλμένα ως κακόβουλες.

103 Μετά την ανίχνευση και την ανάλυση της παραβίασης, είναι απαραίτητη η ταχεία γνωστοποίηση και αναφορά της, ούτως ώστε και άλλοι δημόσιοι και ιδιωτικοί φορείς να λάβουν προληπτικά μέτρα, και οι αρμόδιες αρχές να παράσχουν στήριξη σε εκείνους που επλήγησαν. Πολλοί οργανισμοί είναι απρόθυμοι να αναγνωρίσουν και να γνωστοποιήσουν κυβερνοπεριστατικά[154]. Μεγάλη είναι επίσης η σημασία της έγκαιρης συμμετοχής των αρχών επιβολής του νόμου στην αρχική αντίδραση σε πιθανολογούμενα κυβερνοεγκλήματα, και η προληπτική ανταλλαγή πληροφοριών με τις CSIRT.

104 Η απουσία μέχρι τούδε κοινών απαιτήσεων σε επίπεδο ΕΕ σχετικά με τη γνωστοποίηση περιστατικών ενείχε τον κίνδυνο της καθυστέρησης της κοινοποίησης των παραβάσεων και της παρεμπόδισης της αντίδρασης, πρόβλημα το οποίο επιδιώχθηκε να αντιμετωπιστεί με τη θέσπιση της οδηγίας για την ασφάλεια δικτύων και πληροφοριών (βλέπε σημείο ***20***). Μετά τις επιθέσεις με το λυτρισμικό WannaCry του 2017, η Επιτροπή κατέληξε στο συμπέρασμα ότι το σύστημα του δικτύου CSIRT δεν ήταν ακόμη πλήρως λειτουργικό[155]. Δεδομένου ότι η οδηγία βρίσκεται ακόμη στο στάδιο της πλήρους μεταφοράς, μένει να διαπιστωθεί κατά πόσον οι κατευθυντήριες γραμμές που κατήρτισε η ομάδα συνεργασίας θα συμβάλουν κατά τρόπο αποτελεσματικό στην υπέρβαση της διστακτικότητας για την αναφορά συμβάντων[156].

105 Σε ορισμένους τομείς, σύμφωνα με τους ισχύοντες κανονισμούς της ΕΕ, οι πάροχοι βασικών υπηρεσιών υπέχουν πολλαπλές υποχρεώσεις γνωστοποίησης (μεταξύ άλλων και στους καταναλωτές), γεγονός που μπορεί να επηρεάσει αρνητικά την αποδοτικότητα της διαδικασίας. Παραδείγματος χάριν, οι δραστηριοποιούμενοι στον χρηματοπιστωτικό και τον τραπεζικό τομέα φορείς υπόκεινται σε διαφορετικά κριτήρια, πρότυπα, κατώτατα όρια και χρονοδιαγράμματα γνωστοποίησης στο πλαίσιο του ΓΚΠΔ, της οδηγίας NIS, της οδηγίας για τις υπηρεσίες πληρωμών, της ΕΚΤ / του ΕΕΜ, του στόχου 2 και του κανονισμού eIDAS[157]. Ως εκ τούτου, οι υποχρεώσεις αυτές είναι σημαντικό να εξορθολογιστούν, δεδομένου ότι, πέρα από το γεγονός ότι προκαλούν αδικαιολόγητη διοικητική επιβάρυνση, η ετερογένεια μπορεί να έχει ως αποτέλεσμα τον κατακερματισμό των στοιχείων που υποβάλλονται.

Συντονισμένη αντίδραση

106 Η ανάπτυξη ενός ευρωπαϊκού πλαισίου συνεργασίας για τις κρίσεις ασφάλειας στον κυβερνοχώρο βρίσκεται ακόμη σε εξέλιξη. Για τον λόγο αυτό, εγκρίθηκε το σχετικό «σχέδιο στρατηγικής»[158] (βλέπε σημείο ***18***), προκειμένου να εισαχθεί η διάσταση του κυβερνοχώρου στον μηχανισμό ολοκληρωμένων ρυθμίσεων για την αντιμετώπιση πολιτικών κρίσεων (IPCR), να βελτιωθεί η επίγνωση της κατάστασης και να διασφαλιστεί η καλύτερη ολοκλήρωση με άλλους ενωσιακούς μηχανισμούς διαχείρισης κρίσεων[159]. Το σχέδιο στρατηγικής περιλαμβάνει τα θεσμικά όργανα, τους οργανισμούς και τα κράτη μέλη της ΕΕ. Η ομαλή ενοποίηση όλων αυτών των μηχανισμών αντιμετώπισης κρίσεων αποτελεί πρόκληση[160]. Η απουσία κοινού ασφαλούς δικτύου επικοινωνιών σε όλα τα θεσμικά όργανα της ΕΕ αποτελεί επίσης σημαντική αδυναμία[161].

107 Η ικανότητα της ΕΕ να αντιδρά σε κυβερνοεπιθέσεις σε επιχειρησιακό και πολιτικό επίπεδο σε περίπτωση διασυνοριακών περιστατικών μεγάλης κλίμακας έχει

χαρακτηριστεί «περιορισμένη», εν μέρει επειδή η διάσταση της κυβερνοασφάλειας δεν έχει ενσωματωθεί ακόμη στους υφιστάμενους μηχανισμούς συντονισμού για την αντιμετώπιση κρίσεων σε επίπεδο ΕΕ[162]. Η οδηγία NIS δεν κάλυψε το ζήτημα αυτό.

108 Η πρόσφατη πρόταση για μεταρρύθμιση του ENISA, που προέβλεπε μεγαλύτερο επιχειρησιακό ρόλο στη διαχείριση περιστατικών μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας, δεν έτυχε της στήριξης των κρατών μελών, τα οποία προτιμούσαν ο ρόλος του οργανισμού να περιορίζεται στην υποστήριξη και τη συμπλήρωση της δικής τους επιχειρησιακής δράσης[163]. Στο επίπεδο των κρατών μελών υπάρχουν ήδη πολλές CERT/CSIRT, οι οποίες παρουσιάζουν μεγάλες διαφορές όσον αφορά τις ικανότητές τους. Το γεγονός αυτό συνιστά εμπόδιο για την αποτελεσματική διασυνοριακή συνεργασία που απαιτείται για την αντιμετώπιση συμβάντων μεγάλης κλίμακας[164].

109 Προσπαθήσαμε να χαρτογραφήσουμε τους διαφορετικούς ρόλους που ανατίθενται στους διάφορους παράγοντες που προσδιορίζονται στο σχέδιο στρατηγικής, αλλά εντοπίσαμε κενά τα οποία θα πρέπει να καλυφθούν κατά το στάδιο της υλοποίησης. Ένας τομέας που αρχικώς δεν είχε καλυφθεί επαρκώς ήταν η επιβολή του νόμου, παρόλο που το πρωτόκολλο για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου τέθηκε σε ισχύ τον Δεκέμβριο του 2018[165]. Καίριας σημασίας για την επιτυχία του σχεδίου στρατηγικής είναι να διασφαλιστεί, αφενός, η πρακτικότητά του, και, αφετέρου, ότι όλοι οι εμπλεκόμενοι γνωρίζουν τι πρέπει να κάνουν. Για τον σκοπό αυτό θα απαιτηθεί η διενέργεια εκτενών δοκιμών τα προσεχή έτη.

110 Η αποτελεσματική αντίδραση δεν περιορίζεται στον μετριασμό των ζημιών: μεγάλη είναι και η σημασία του προσδιορισμού των υπευθύνων για τις επιθέσεις. Η παρακολούθηση και ο εντοπισμός των δραστών, κυρίως σε περίπτωση υβριδικής επίθεσης, μπορεί να παρουσιάζουν μεγάλες δυσκολίες λόγω της αυξανόμενης χρήσης εργαλείων ανωνυμοποίησης, κρυπτονομισμάτων και της κρυπτογράφησης. Το πρόβλημα αυτό είναι γνωστό ως πρόβλημα απόδοσης ευθυνών. Το ζήτημα δεν είναι μόνο τεχνικό, αλλά δημιουργεί προκλήσεις και για την ποινική δικαιοσύνη. Οι ποινικές έρευνες και η δίωξη των υπόπτων μπορεί να προσκρούουν στις νομικές και διαδικαστικές διαφορές μεταξύ των διαφόρων χωρών. Για την αντιμετώπιση του προβλήματος αυτού θα απαιτηθεί, παραδείγματος χάριν, μια πιο τυποποιημένη επιχειρησιακή ανταλλαγή πληροφοριών, στο πλαίσιο σαφέστερων διαδικασιών, με την Ευρωπόλ ή με το Ευρωπαϊκό δικαστικό δίκτυο για το έγκλημα στον κυβερνοχώρο της Eurojust.

111 Σε πολιτικό επίπεδο, αναπτύχθηκε η «εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο» (βλέπε ***πλαίσιο 6***) προκειμένου να διευκολύνει την επίλυση διεθνών διαφορών στον κυβερνοχώρο με ειρηνικά μέσα. Η δημιουργία ομάδων ταχείας αντίδρασης για τον κυβερνοχώρο και η οργάνωση μιας πρωτοβουλίας για αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο είναι δύο έργα που υλοποιούνται στο πλαίσιο της PESCO και προωθούν την ενισχυμένη ανταλλαγή πληροφοριών[166].

Πλαίσιο 6

Η εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο

Η «κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο»[167], ή αλλιώς «εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο» προέκυψε από τα συμπεράσματα του Συμβουλίου του 2015 για τη διπλωματία στον κυβερνοχώρο[168]. Η διπλωματία στον κυβερνοχώρο αποσκοπεί στην ανάπτυξη και την εφαρμογή μιας κοινής και ολοκληρωμένης προσέγγισης του κυβερνοχώρου βασισμένης στις αξίες της ΕΕ, το κράτος δικαίου, την ανάπτυξη ικανοτήτων και τις εταιρικές σχέσεις, την προώθηση του πολυμερούς μοντέλου διακυβέρνησης του διαδικτύου και τον μετριασμό των απειλών για την κυβερνοασφάλεια και τη μεγαλύτερη σταθερότητα στις διεθνείς σχέσεις.

Η εργαλειοθήκη παρέχει στην ΕΕ και τα κράτη μέλη της τη δυνατότητα να οργανώνουν μια κοινή διπλωματική αντίδραση σε κακόβουλες δραστηριότητες στον κυβερνοχώρο, αξιοποιώντας πλήρως τα μέτρα που προβλέπονται στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφάλειας. Τα μέτρα αυτά μπορεί να είναι προληπτικά (π.χ. ενημέρωση-ευαισθητοποίηση, ανάπτυξη ικανοτήτων), συνεργασίας, σταθερότητας ή περιοριστικά (π.χ. ταξιδιωτικές απαγορεύσεις, απαγορεύσεις εξαγωγών όπλων, δέσμευση κεφαλαίων) ή μέτρα στήριξης της αντίδρασης των κρατών μελών[169]. Βασίζεται στην ιδέα ότι η μεγαλύτερη συνεργασία για τον μετριασμό των απειλών και η κατάδειξη των πιθανών συνεπειών θα αποτρέπει (δυνητικά) επιθετικές συμπεριφορές.

Η κοινή αντίδραση της ΕΕ σε κακόβουλες δραστηριότητες στον κυβερνοχώρο θα είναι ανάλογη προς το εύρος, την κλίμακα, τη διάρκεια, την ένταση, την πολυπλοκότητα, την ιδιομορφία και τις επιπτώσεις της εκάστοτε δραστηριότητας.

Η επιτυχία της εργαλειοθήκης θα κριθεί και από τον βαθμό ενσωμάτωσής της στο σχέδιο στρατηγικής και τις IPCR (βλέπε σημείο ***106***), τον βαθμό επίγνωσης της κατάστασης μέσω της ταχείας και συνεχούς ανταλλαγής πληροφοριών (συμπεριλαμβανομένων στοιχείων σχετικά με την απόδοση ευθυνών)[170] και, τέλος, από την αποτελεσματικότητα της συνεργασίας. Βασικό επίσης συστατικό της επιτυχούς εφαρμογής της εργαλειοθήκης είναι η αποτελεσματική και συντονισμένη επικοινωνία. Μέχρι στιγμής, η εργαλειοθήκη έχει χρησιμοποιηθεί σε δύο περιπτώσεις: προκειμένου να δρομολογηθεί διάλογος με τις Ηνωμένες Πολιτείες μετά την επίθεση *Wannacry*[171] και για τη σύνταξη των συμπερασμάτων του Συμβουλίου με τα οποία καταδικάζεται η κακόβουλη χρήση των ΤΠΕ[172]. Η θέση της

εργαλειοθήκης σε εφαρμογή βρίσκεται σε εξέλιξη και μένει να διαπιστωθεί σε ποιον βαθμό θα επιτύχει τους στόχους της.

Πρόκληση 10: Προστασία των υποδομών ζωτικής σημασίας και των κοινωνικών λειτουργιών

Προστασία των υποδομών

112 Μεγάλο μέρος των υποδομών ζωτικής σημασίας της ΕΕ λειτουργεί μέσω βιομηχανικών συστημάτων ελέγχου (industrial control systems, ICS)[173]. Πολλά από αυτά σχεδιάστηκαν ως αυτόνομα συστήματα, με περιορισμένη δυνατότητα σύνδεσης με τον έξω κόσμο. Η σύνδεση ορισμένων συνιστωσών των ICS στο διαδίκτυο τα έχει καταστήσει περισσότερο ευάλωτα σε εξωτερικές παρεμβάσεις. Η συντήρηση των υπαρχόντων συστημάτων και η επιδιόρθωσή τους μπορεί να μην είναι πλέον δυνατή, αλλά η αναβάθμισή τους συνεπάγεται καθυστερήσεις και κόστος. Ως εκ τούτου, οι προσπάθειες για την ενίσχυση της ασφάλειας των υποδομών ζωτικής σημασίας πρέπει να περιλαμβάνουν την αναβάθμιση των ICS.

113 Καθώς η βιομηχανία εξακολουθεί να ψηφιοποιείται (διαδικασία γνωστή ως «τέταρτη βιομηχανική επανάσταση»), ο αντίκτυπος ενός περιστατικού μεγάλης κλίμακας σε έναν κλάδο της βιομηχανίας μπορεί να έχει αλυσιδωτές αντιδράσεις σε άλλους. Ο ENISA επεσήμανε τη σημασία της χαρτογράφησης του αντικτύπου της αμοιβαίας εξάρτησης που υπάρχει μεταξύ κρίσιμων τομέων[174]. Η διαδικασία αυτή είναι απαραίτητη προκειμένου να γίνει κατανοητός ο ρυθμός ενδεχόμενης εξάπλωσης ενός περιστατικού και αποτελεί προϋπόθεση για την οργάνωση καλά συντονισμένων αντιδράσεων.

114 Η οδηγία NIS αποσκοπεί στην ενίσχυση της ετοιμότητας σε βασικούς τομείς, κρίσιμους για τις υποδομές ζωτικής σημασίας. Ωστόσο, δεν καλύπτονται όλοι οι τομείς (βλέπε ***πίνακα 1***)[175], γεγονός που περιορίζει την αποτελεσματικότητα της στρατηγικής[176]: μία από τις σημαντικότερες πηγές προβληματισμού εν προκειμένω είναι η προστασία της δημοκρατικής ακεραιότητας των εκλογών από παρεμβάσεις στις εκλογικές υποδομές και από την παραπληροφόρηση (βλέπε ***πλαίσιο 7***). Ως εκ τούτου, πέραν της αναθεώρησης της ισχύουσας νομοθεσίας, μια βασική πρόκληση συνίσταται στην εξασφάλιση της αποτελεσματικής αντίδρασης των τομέων αυτών σε περιστατικά μεγάλης κλίμακας.

115 Τα τρωτά σημεία των υποδομών ζωτικής σημασίας δεν σταματούν στα σύνορα της Ευρώπης. Μια σημαντική πρόκληση για την Επιτροπή είναι να ενθαρρύνει τις υποψήφιες χώρες να υιοθετήσουν τα ίδια πρότυπα με τα κράτη μέλη, παραδείγματος χάριν σε τομείς όπως η νομοθεσία που σχετίζεται με τον κυβερνοχώρο ή η προστασία των υποδομών ζωτικής σημασίας.

Πλαίσιο 7

Προστασία κρίσιμων κοινωνικών λειτουργιών: *καταπολέμηση των παρεμβάσεων στις εκλογές*

Τον Μάιο του 2019, περίπου 400 εκατομμύρια ψηφοφόροι θα προσέλθουν στις κάλπες για την ανάδειξη των μελών του Ευρωπαϊκού Κοινοβουλίου. Θα είναι οι πρώτες εκλογές μετά τη θέση σε ισχύ του ΓΚΠΔ και θα διεξαχθούν στον απόηχο σκανδάλων που σχετίζονταν με την κατάχρηση δεδομένων προσωπικού χαρακτήρα για μικροστόχευση ψηφοφόρων και πρωτοφανών συντονισμένων εκστρατειών παραπληροφόρησης («Fake News»). Η Επιτροπή έχει προειδοποιήσει για το ενδεχόμενο κυβερνοπαρεμβάσεων σε αυτές τις εκλογές[177], για την αποτροπή των οποίων είναι αναγκαία η υιοθέτηση μιας προσέγγισης που να βασίζεται στην καθολική στήριξη από το σύνολο των κρατικών αρχών και της κοινωνίας.

Εκλογικές υποδομές

Η διοργάνωση των εκλογών είναι περίπλοκη υπόθεση και η διασφάλιση της προστασίας και της ακεραιότητάς τους εμπίπτει στην αρμοδιότητα των κρατών μελών. Οι παρεμβάσεις στις εκλογές και τις εκλογικές υποδομές μπορεί να έχουν ως στόχο να επηρεάσουν τις προτιμήσεις των ψηφοφόρων, το ποσοστό συμμετοχής ή την ίδια την εκλογική διαδικασία, συμπεριλαμβανομένων των διαδικασιών της ψηφοφορίας, της καταμέτρησης των ψήφων και της ανακοίνωσης των αποτελεσμάτων. Στις εκλογές για το Ευρωπαϊκό Κοινοβούλιο, η προστασία του λεγόμενου «τελευταίου χιλιομέτρου» (της ανακοίνωσης των αποτελεσμάτων από τις πρωτεύουσες των κρατών μελών στις Βρυξέλλες) συνιστά ιδιαίτερα κρίσιμη πρόκληση, δεδομένου ότι δεν υπάρχει μια κοινή προσέγγιση όσον αφορά την ασφάλεια και δεν έχουν πραγματοποιηθεί σχετικές δοκιμές[178].

Η πρόσφατη δέσμη μέτρων της Επιτροπής για τις εκλογές περιελάμβανε μέτρα για την ενίσχυση της κυβερνοασφάλειας των εκλογών, όπως τον καθορισμό εθνικών σημείων επαφής για τον συντονισμό και την ανταλλαγή πληροφοριών κατά το διάστημα πριν από τη διεξαγωγή των εκλογών. Ιδιαίτερη σημασία έχει και η ανταλλαγή βέλτιστων πρακτικών και αντληθέντων διδαγμάτων[179].

Τα εκλογικά συστήματα δεν θεωρούνται μέρος των υποδομών ζωτικής σημασίας[180] ούτε καλύπτονται από την οδηγία για την ασφάλεια δικτύων και πληροφοριών. Ωστόσο, η ομάδα συνεργασίας έχει εκδώσει πρακτικές κατευθυντήριες οδηγίες απευθυνόμενες στις δημόσιες αρχές σχετικά με την ασφάλεια της εκλογικής τεχνολογίας. Μια συνεδρίαση των εθνικών σημείων επαφής αναμένεται να πραγματοποιηθεί στις αρχές του 2019[181]. Ενθαρρύνεται επίσης η διενέργεια εκτιμήσεων κινδύνου από τα κράτη μέλη σχετικά με τις κυβερνοαπειλές για την εκλογική διαδικασία τους.

Παραπληροφόρηση

Η παραπληροφόρηση αποτελεί μια ολοένα αυξανόμενης σημασίας συνιστώσα των υβριδικών επιθέσεων και συνδυάζει κυβερνοεπιθέσεις και παραβίαση δικτύων. Μπορεί να χρησιμοποιηθεί για τη διαίρεση των κοινωνιών, τη δημιουργία κλίματος δυσπιστίας και την υπονόμευση της εμπιστοσύνης στις δημοκρατικές διαδικασίες ή όσον αφορά άλλα θέματα (παραδείγματος χάριν, κατά του εμβολιασμού ή σχετικά με την αλλαγή του κλίματος). Η κλίμακα, η ταχύτητα και η εμβέλεια της παραπληροφόρησης έχουν αυξηθεί σε τέτοιο βαθμό που πλέον συνιστά γνήσια απειλή για την ασφάλεια της ΕΕ.

Η ΕΕ έλαβε πρόσφατα σειρά μέτρων για την αντιμετώπιση του εν λόγω προβλήματος. Το 2015 συγκροτήθηκε η ειδική ομάδα East StratCom της ΕΥΕΔ για να αντιταχθεί στις εκστρατείες παραπληροφόρησης της Ρωσίας[182]. Εμπειρογνώμονες εξαίρουν το έργο της όσον αφορά την προαγωγή των πολιτικών της ΕΕ, την υποστήριξη των ανεξάρτητων μέσων ενημέρωσης στις χώρες της γειτονίας και την πρόβλεψη, την παρακολούθηση και την αντιμετώπιση της παραπληροφόρησης[183]. Ωστόσο, οι πόροι της ειδικής ομάδας είναι περιορισμένοι σε σχέση με την κλίμακα και την πολυπλοκότητα των εκστρατειών παραπληροφόρησης[184]. Είναι αναγκαία μια πιο συστηματική αλληλεπίδραση με τις υφιστάμενες δομές της ΕΕ και καλύτερη στρατηγική συνεργασία στον τομέα της επικοινωνίας[185]. Το Ευρωπαϊκό Συμβούλιο ενέκρινε ένα νέο σχέδιο δράσης[186] τον Δεκέμβριο του 2018.

Πιο πρόσφατα, η Επιτροπή, σε συνέχεια της ανακοίνωσής της του Απριλίου του 2018 σχετικά με την αντιμετώπιση της παραπληροφόρησης στο διαδίκτυο[187], κατήρτισε έναν κώδικα ορθής πρακτικής εθελοντικής αυτορρύθμισης[188], βάσει υφιστάμενων μέσων πολιτικής τα οποία εφαρμόζουν διαδικτυακές πλατφόρμες και η διαφημιστική βιομηχανία[189]. Μεταξύ άλλων, αποσκοπεί στην ενίσχυση της αξιοπιστίας του περιεχομένου και στην υποστήριξη των προσπαθειών προώθησης του γραμματισμού στα μέσα ενημέρωσης και τις ειδήσεις. Έχει επίσης δρομολογηθεί η δημιουργία ενός ανεξάρτητου ευρωπαϊκού δικτύου ελέγχου εγκυρότητας γεγονότων.

Η Επιτροπή έχει δηλώσει ότι, εάν ο κώδικας ορθής πρακτικής δεν τηρηθεί, μπορεί εν συνεχεία να ληφθούν περαιτέρω ρυθμιστικά μέτρα. Σημαντικό ρόλο θα διαδραματίσει επίσης ο καθορισμός του τρόπου μέτρησης της

αποτελεσματικότητας των μέτρων, ιδίως του τρόπου μέτρησης των βελτιώσεων όσον αφορά την εμπιστοσύνη, τη διαφάνεια και την υποχρέωση λογοδοσίας.

Πρόκληση θα αποτελέσει ακόμη η εξεύρεση τρόπων για τη βελτίωση της ανίχνευσης, της ανάλυσης και της ανάδειξης περιπτώσεων παραπληροφόρησης[190]. Επιπλέον, απαιτείται ενεργή και στρατηγική παρακολούθηση και ανάλυση των πηγών ανοικτών δεδομένων[191]. Οι προσπάθειες για καλύτερη κατανόηση του περιβάλλοντος απειλών θα πρέπει επίσης να καλύπτουν τις αναδυόμενες τάσεις, όπως τα «deepfakes» (βαθιά ψευδείς πληροφορίες - βίντεο που παράγονται με τη βοήθεια τεχνητής νοημοσύνης και βαθιάς μηχανικής μάθησης), καθώς και τα εργαλεία που απαιτούνται για την ανίχνευσή τους.

Ενίσχυση της αυτονομίας

116 Η ΕΕ είναι καθαρός εισαγωγέας προϊόντων και υπηρεσιών κυβερνοασφάλειας, γεγονός που αυξάνει τον κίνδυνο τεχνολογικής εξάρτησης από παρόχους από τρίτες χώρες, καθώς και τον κίνδυνο ευπάθειας[192]. Ειδικότερα, το γεγονός αυτό υπονομεύει την ασφάλεια των υποδομών ζωτικής σημασίας της ΕΕ, η οποία επίσης στηρίζεται σε πολύπλοκες παγκόσμιες αλυσίδες εφοδιασμού. Ο κίνδυνος εντείνεται στις περιπτώσεις που οι εν λόγω τρίτοι πάροχοι αποκτούν τον έλεγχο ευρωπαϊκών εταιρειών κυβερνοασφάλειας. Τα κράτη μέλη είναι υπεύθυνα για τον έλεγχο των άμεσων ξένων επενδύσεων (ΑΞΕ), και επί του παρόντος δεν υπάρχει μηχανισμός ελέγχου σε επίπεδο ΕΕ[193].

117 Η ενίσχυση της στρατηγικής αυτονομίας αποτελεί στόχο της συνολικής στρατηγικής της ΕΕ, καθώς και της ανακοίνωσης του 2017 για την ανθεκτικότητα, την αποτροπή και την άμυνα[194]. Η αντιμετώπιση των πολυάριθμων προκλήσεων που παρουσιάζονται στο παρόν έγγραφο θα συμβάλει στην επίτευξη του στόχου αυτού, καθώς δεν πρόκειται για κάτι που μπορεί να επιτευχθεί με επιμέρους μέτρα.

Σημεία προβληματισμού – Αποτελεσματική αντιμετώπιση

- Με ποιον τρόπο βελτίωσε η οδηγία για την ασφάλεια δικτύων και πληροφοριών την κοινοποίηση κυβερνοπεριστατικών σε κρίσιμους τομείς και όχι μόνο;
- Σε ποιον βαθμό ενσωματώνουν τα θεσμικά όργανα της ΕΕ στις διαδικασίες τους τον συντονισμό της αντιμετώπισης κρίσεων σε περιπτώσεις σοβαρών κυβερνοπεριστατικών;
- Πώς μπορεί η διπλωματία στον κυβερνοχώρο να διαδραματίσει σημαντικότερο ρόλο στις εξωτερικές δράσεις της ΕΕ;
- Είναι οι υφιστάμενες δομές και δράσεις της ΕΕ για την αντιμετώπιση της παραπληροφόρησης ανάλογες προς την κλίμακα και την πολυπλοκότητα του προβλήματος;

Τελικές παρατηρήσεις

118 Τα τελευταία χρόνια, η κυβερνοασφάλεια έχει καταλάβει σημαντικότερη θέση στην ημερήσια διάταξη της ΕΕ και των κρατών μελών της, με σκοπό την ενίσχυση της κυβερνοανθεκτικότητας συνολικά. Εντούτοις, η επίτευξη υψηλότερου επιπέδου κυβερνοασφάλειας στην ΕΕ συνιστά κολοσσιαίο εγχείρημα. Στο παρόν ενημερωτικό έγγραφο επιδιώξαμε να επισημάνουμε ορισμένες από τις κύριες προκλήσεις που πρέπει να αντιμετωπίσει η ΕΕ προκειμένου να επιτύχει τον φιλόδοξο στόχο της να καταστεί το ασφαλέστερο ψηφιακό περιβάλλον παγκοσμίως.

119 Από την επισκόπησή μας προκύπτει ότι η μετάβαση προς μια νοοτροπία επιδόσεων, αναπόσπαστο μέρος της οποίας θα αποτελούν πρακτικές αξιολόγησης, είναι απαραίτητη για να εξασφαλιστεί ουσιαστική **λογοδοσία και αξιολόγηση**. **Η νομοθεσία εξακολουθεί να εμφανίζει κενά και δεν μεταφέρεται με συνέπεια στο εσωτερικό δίκαιο των κρατών μελών**. Το γεγονός αυτό δυσχεραίνει σε ορισμένες περιπτώσεις την πλήρη επίτευξη των στόχων της νομοθεσίας. Μια άλλη πρόκληση που εντοπίστηκε αφορά την **ευθυγράμμιση του επιπέδου των επενδύσεων με τους στρατηγικούς στόχους**, που καθιστά αναγκαία όχι μόνο την αύξηση του επιπέδου των επενδύσεων αλλά και την κλιμάκωση του αντικτύπου τους. Η κατάσταση επιδεινώνεται εκ του γεγονότος ότι η ΕΕ και τα κράτη μέλη της δεν **έχουν σαφή εικόνα των ενωσιακών δαπανών** για την κυβερνοασφάλεια. Διαπιστώνεται ακόμη ότι υπάρχουν **περιορισμοί όσον αφορά την εξασφάλιση πόρων από τους οργανισμούς που ασχολούνται με θέματα κυβερνοχώρου,** συμπεριλαμβανομένων δυσκολιών στην προσέλκυση και τη διατήρηση ταλέντων.

120 Διαθέσιμες μελέτες καταλήγουν στο συμπέρασμα ότι η **διακυβέρνηση της κυβερνοασφάλειας μπορεί να ενισχυθεί** προκειμένου να αυξηθεί η ικανότητα της παγκόσμιας κοινότητας να αντιδρά σε κυβερνοεπιθέσεις και κυβερνοπεριστατικά. Από την άλλη πλευρά, η αποτροπή κάθε επίθεσης είναι αδύνατη. Ως εκ τούτου, οι βασικές προκλήσεις που πρέπει να αντιμετωπιστούν αφορούν την **ταχεία ανίχνευση και αντίδραση** και την **προστασία των υποδομών ζωτικής σημασίας και των κοινωνικών λειτουργιών**, καθώς και τη βελτίωση της **ανταλλαγής πληροφοριών και του συντονισμού** μεταξύ του δημόσιου και του ιδιωτικού τομέα. Τέλος, το αυξανόμενο έλλειμμα δεξιοτήτων στον τομέα της κυβερνοασφάλειας καθιστά την **ενίσχυση των σχετικών δεξιοτήτων και την αύξηση της ενημέρωσης και της ευαισθητοποίησης** σε κάθε τομέα και σε όλα τα επίπεδα της κοινωνίας ακόμη μία πρόκληση καίριας σημασίας.

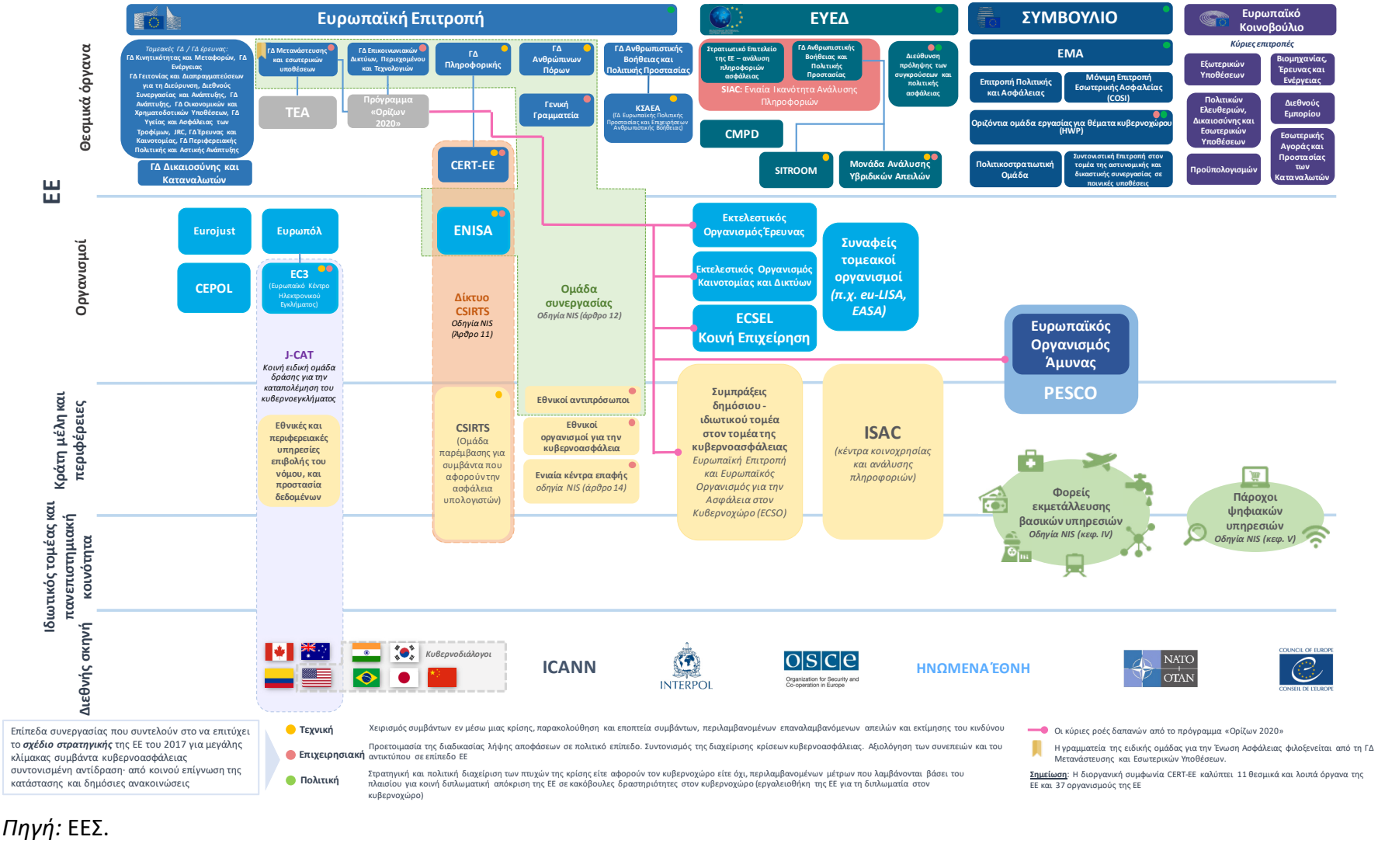
121 Οι προκλήσεις που θέτουν σήμερα οι κυβερνοαπειλές που αντιμετωπίζει η ΕΕ και το ευρύτερο παγκόσμιο περιβάλλον καθιστούν αναγκαία τη σταθερή προσήλωση στις αξίες της ΕΕ και την απαρέγκλιτη τήρησή τους.

Το παρόν ενημερωτικό έγγραφο εγκρίθηκε από το Τμήμα III, κατά τη συνεδρίασή του της 14ης Φεβρουαρίου 2019.

Για το Ελεγκτικό Συνέδριο

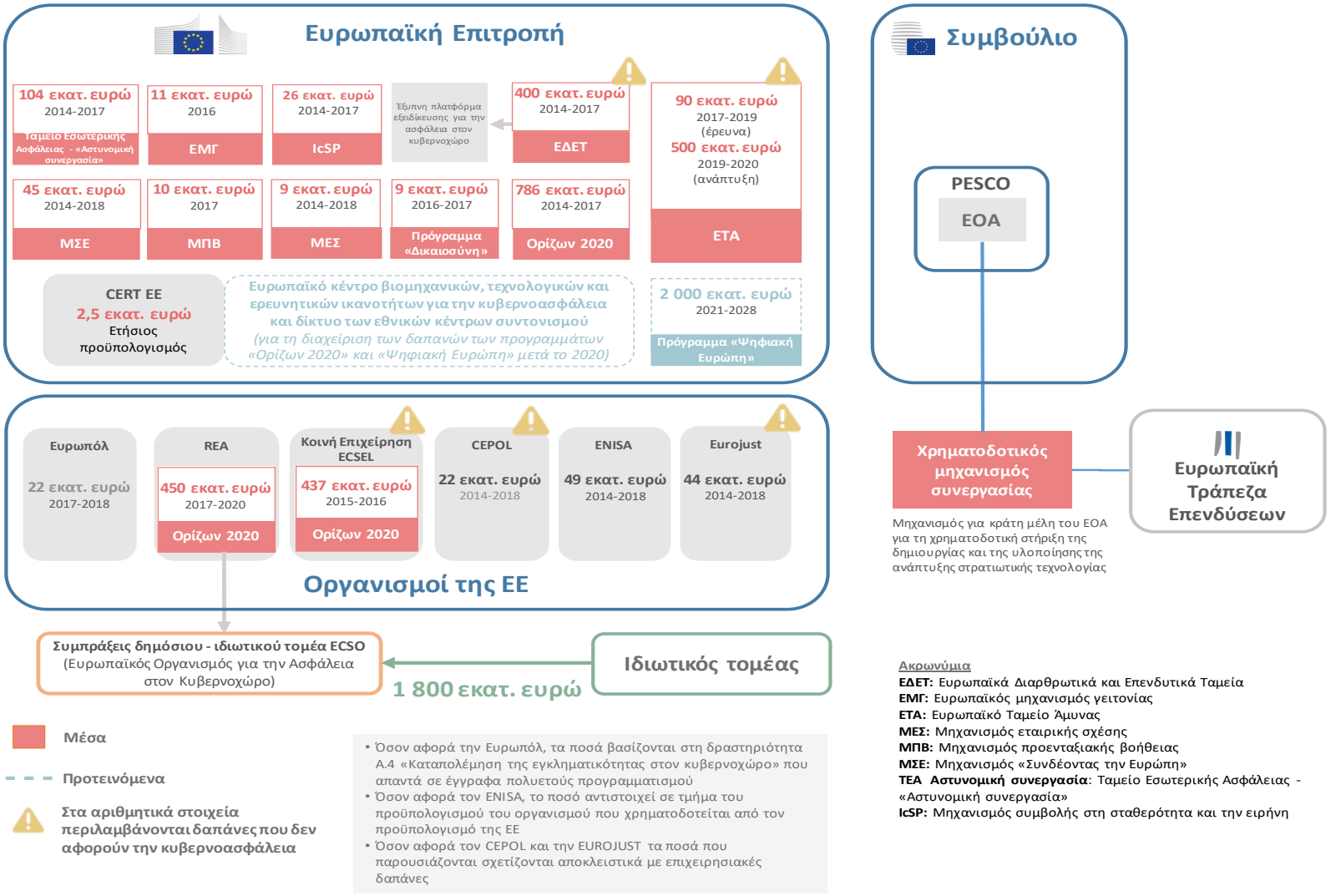
Klaus-Heiner Lehne
Πρόεδρος

Παράρτημα I — Ένα σύνθετο, πολυεπίπεδο τοπίο με πολλούς παράγοντες



Πηγή: ΕΕΣ.

Παράρτημα ΙΙ — Οι δαπάνες της ΕΕ για την κυβερνοασφάλεια από το 2014



Πηγή: ΕΕΣ, βάσει εγγράφων της Ευρωπαϊκής Επιτροπής και οργανισμών της ΕΕ

Παράρτημα III — Εκθέσεις οργάνων ελέγχου των κρατών μελών της ΕΕ

Είδος	Τίτλος (και υπερσύνδεσμος)	Έτος	Κράτος μέλος
Έλεγχοι συμμόρφωσης	Σημείωμα αξιολόγησης εσωτερικού ελέγχου	2014	FR
	Έκθεση πιστοποίησης των λογαριασμών του γενικού συστήματος κοινωνικής ασφάλισης (άμυνα, εξωτερικές υποθέσεις)	2016	FR
	Πιστοποίηση των λογαριασμών του Δημοσίου	2016	FR
	Διασφάλιση της ασφάλειας και της διατήρησης των βάσεων δεδομένων ζωτικής σημασίας της Εσθονίας	Τέλος 2018 / Δεν έχει δημοσιευθεί ακόμη.	EE
	Αποτελεσματικότητα των εσωτερικών ελέγχων όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στις εθνικές βάσεις δεδομένων	2008	EE
Έλεγχοι επιδόσεων / οικονομικής αποδοτικότητας	Έκθεση σχετικά με τον περιορισμό των κυβερνοεπιθέσεων	2013	DK
	RiR 2014:23 Ασφάλεια πληροφοριών στη δημόσια διοίκηση	2014	SE
	Έκθεση σχετικά με την από μέρους της κυβέρνησης επεξεργασία απόρρητων δεδομένων για πρόσωπα και εταιρείες	2014	DK
	Το εθνικό πρόγραμμα κυβερνοασφάλειας	2014	UK
	Έκθεση προς την επιτροπή προϋπολογισμού του γερμανικού ομοσπονδιακού κοινοβουλίου, σύμφωνα με το άρθρο 88, παράγραφος 2, του ομοσπονδιακού κώδικα προϋπολογισμού – ενοποίηση ΤΠ σε επίπεδο ομοσπονδιακής κυβέρνησης	2015	DE
	Έκθεση σχετικά με την πρόσβαση σε συστήματα ΤΠ που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών στην κοινωνία της Δανίας	2015	DK
	Δημόσιος οργανισμός χωροταξίας Plaine de France	2015	FR
	«Το περιβάλλον κυβερνοασφάλειας στη Λιθουανία» στα λιθουανικά και σύνοψη μεταφρασμένη στα αγγλικά	2015	LT
	Η εκτέλεση των καθηκόντων των δημόσιων φορέων στον τομέα της κυβερνοασφάλειας στην Πολωνία (στην πολωνική γλώσσα)	2015	PL
	RiR 2015:21 Κυβερνοεγκληματικότητα – υπάρχουν περιθώρια βελτίωσης της αποδοτικότητας των αστυνομικών και εισαγγελικών αρχών	2015	SE
	Έλλειμμα ψηφιακών δεξιοτήτων στο Δημόσιο (Έρευνα)	2015	UK
	Έκθεση προς το ομοσπονδιακό κοινοβούλιο: Είσπραξη φόρου κληρονομιάς από την ομοσπονδιακή υπηρεσία οικονομικών	2016	BE
	Έκθεση σχετικά με τη διαχείριση της ασφάλειας ΤΠ στα συστήματα που ανατίθενται σε εξωτερικούς προμηθευτές	2016	DK
	Έκθεση ελέγχου σχετικά με τη δανειοδοτική δραστηριότητα του Επίσημου Πιστωτικού Ιδρύματος του 2016	2016	ES

Είδος	Τίτλος (και υπερσύνδεσμος)	Έτος	Κράτος μέλος
	Συντονισμός του δικτύου ασφάλειας της δημόσιας διοίκησης	2016	FI
	Διασφάλιση της ασφάλειας των συστημάτων ΤΠ που χρησιμοποιούνται για την άσκηση δημόσιων καθηκόντων	2016	PL
	Πρόληψη και καταπολέμηση του κυβερνοεκφοβισμού στα παιδιά και τους νέους	2016	PL
	Εργασίες στον τομέα της ασφάλειας των πληροφοριών σε εννέα οργανισμούς - Ένας ακόμη έλεγχος σχετικά με την ασφάλεια των πληροφοριών. RiR 2016:8	2016	SE
	Προστασία των πληροφοριών στη δημόσια διοίκηση	2016	UK
	Έκθεση σχετικά με την προστασία των συστημάτων ΤΠ και των δεδομένων υγείας σε τρεις περιφέρειες της Δανίας	2017	DK
	Σημείωμα σχετικά με τα αποτελέσματα του διεθνούς παράλληλου ελέγχου για την αποτελεσματικότητα των εσωτερικών δικλίδων ελέγχου όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στις εθνικές βάσεις δεδομένων.	2017	EE
	Ρυθμίσεις για την προστασία στον κυβερνοχώρο	2017	FI
	Καθοδήγηση σχετικά με τη λειτουργική αξιοπιστία των ηλεκτρονικών υπηρεσιών	2017	FI
	Δίκτυο γεωργικών επιμελητηρίων (συγκεφαλαιωτική έκθεση)	2017	FR
	Εμπορικό και βιοτεχνικό επιμελητήριο Vaucluse (του περιφερειακού Τμήματος ελέγχου - PACA)	2017	FR
	Διασφάλιση της ασφάλειας και της διατήρησης των βάσεων δεδομένων ζωτικής σημασίας της Εσθονίας	Τέλος 2018 / Δεν έχει δημοσιευθεί ακόμη.	EE
	Ανάπτυξη των κρατικών υποδομών ηλεκτρονικών επικοινωνιών στα λιθουανικά και σύνοψη μεταφρασμένη στα αγγλικά	2017	LT
	Έλεγχος στον τομέα της τεχνολογίας πληροφοριών: η κυβερνοασφάλεια στη δημόσια διοίκηση	2017	MT
	Το σύστημα των εθνικών μητρώων: ασφάλεια, επιδόσεις και χρηστικότητα	2017	PL
	Το περιστατικό WannaCry	2017	UK
	Διαδικτυακή απάτη	2017	UK
	Έκθεση σχετικά με την προστασία από επιθέσεις με λυτρισμικό	2018	DK
	Νοσοκομείο της Arpajon (από το περιφερειακό Τμήμα ελέγχου του Île-de-France)	2018	FR
	Διαχείριση πόρων πληροφοριών ζωτικής σημασίας	2018	LT
	«Ηλεκτρονικό έγκλημα»	2019	LT
	Ασφάλεια των πληροφοριών στην Πολωνία	2019	PL
Άλλοι έλεγχοι	Βάση δεδομένων δημόσιων φορέων	μ.δ.	BE

Είδος	Τίτλος (και υπερσύνδεσμος)	Έτος	Κράτος μέλος
	Ερωτηματολόγιο σχετικά με την πολιτική ασφάλειας και ανάλυσης κινδύνου (σε εξέλιξη)	μ.δ.	BE

Ακρωνύμια και συντομογραφίες

ΑΞΕ: Άμεσες ξένες επενδύσεις

ΑΟΕ: Ανώτατο όργανο ελέγχου

ΓΚΠΔ: Γενικός κανονισμός για την προστασία δεδομένων

ΔΕΑΠ: Διοικούσα επιτροπή ασφάλειας πληροφοριών

ΕΔΕΤ: Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΑ: Ευρωπαϊκή εποπτική αρχή

ΕΕΣ: Ευρωπαϊκό Ελεγκτικό Συνέδριο

ΕΟΑ Ευρωπαϊκός Οργανισμός Άμυνας

ΕΥΕΔ: Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης

Κέντρο EC3: Ευρωπαϊκό κέντρο για τα εγκλήματα στον κυβερνοχώρο της Ευρωπόλ

ΚΠΑΑ: Κοινή Πολιτική Ασφάλειας και Άμυνας

ΜΜΕ: Μικρή και μεσαία επιχείρηση

Οδηγία NIS: Οδηγία για την ασφάλεια δικτύων και πληροφοριών

σΣΔΙΤ: Συμβατική σύμπραξη δημόσιου και ιδιωτικού τομέα

ΤΑΕ - «Αστυνομική συνεργασία»: Ταμείο Εσωτερικής Ασφάλειας - «Αστυνομική συνεργασία»

ΤΥΑΠ: Τοπικός υπεύθυνος ασφάλειας πληροφορικής

CERT: - ΕΕ: Ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική

CSIRT: Ομάδα παρέμβασης για συμβάντα που αφορούν την ασφάλεια υπολογιστών

DDoS: Κατανεμημένη άρνηση υπηρεσίας

ECSEL: Ηλεκτρονικά συστατικά στοιχεία και συστήματα για την ευρωπαϊκή πρωτοπορία

ECSM: Ευρωπαϊκός μήνας για την ασφάλεια στον κυβερνοχώρο

ECSO: Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο

ENISA: Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών

HWPCI: Οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου

ICS: Βιομηχανικά συστήματα ελέγχου

JRC: Κοινό Κέντρο Ερευνών

NCIRC: Ομάδα αντιμετώπισης συμβάντων πληροφορικής του ΝΑΤΟ

PESCO: Μόνιμη διαρθρωμένη συνεργασία

Γλωσσάριο:

Αντιγραφή δεδομένων κάρτας (skimming): Η κλοπή δεδομένων πιστωτικής ή χρεωστικής κάρτας κατά την καταχώρισή τους στο διαδίκτυο.

Ακεραιότητα: Προστασία των πληροφοριών από καταχρηστική τροποποίηση ή καταστροφή και διασφάλιση της γνησιότητάς τους.

Ακτιβιστής χάκερ: Άτομο ή ομάδα που αποκτά μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα πληροφοριών με σκοπό την προώθηση κοινωνικών ή πολιτικών στόχων.

Ασφάλεια δικτύων: Επιμέρους τμήμα της κυβερνοασφάλειας που αφορά την προστασία των δεδομένων που αποστέλλονται μέσω συσκευών συνδεδεμένων στο ίδιο δίκτυο, ώστε να διασφαλίζεται ότι οι πληροφορίες δεν παρακολουθούνται ούτε αλλοιώνονται.

Ασφάλεια των πληροφοριών: Το σύνολο των διεργασιών και των εργαλείων που προστατεύουν τα δεδομένα σε φυσική και ψηφιακή μορφή από μη εξουσιοδοτημένη πρόσβαση, χρήση, κοινολόγηση, διαταραχή, τροποποίηση, καταχώριση ή καταστροφή.

Δεδομένα πρόσβασης: Πληροφορίες σχετικά με τη δραστηριότητα σύνδεσης και αποσύνδεσης ενός χρήστη για την πρόσβαση σε υπηρεσία, όπως η ώρα, η ημερομηνία και η διεύθυνση IP.

Δεδομένα προσωπικού χαρακτήρα: Πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο.

Διαδίκτυο των πραγμάτων: Το δίκτυο αντικειμένων καθημερινής χρήσης που είναι εξοπλισμένα με ηλεκτρονικά συστήματα, λογισμικό και αισθητήρες έτσι ώστε να μπορούν να επικοινωνούν και να ανταλλάσσουν δεδομένα μέσω του διαδικτύου.

Διαθεσιμότητα: Διασφάλιση της ταχείας και αξιόπιστης πρόσβασης σε πληροφορίες και της χρήσης τους.

Διανυσματοποίηση κειμένου: Η διαδικασία της μετατροπής λέξεων, προτάσεων ή ολόκληρων εγγράφων σε αριθμητικούς φορείς ώστε να είναι δυνατή η χρήση τους από αλγόριθμους μηχανικής μάθησης.

Διαχείριση τρωτών σημείων: Αναπόσπαστο μέρος της ασφάλειας υπολογιστών και δικτύων. Αποσκοπεί στον προληπτικό μετριασμό ή την αποτροπή της εκμετάλλευσης

τρωτών σημείων συστημάτων και λογισμικών, μέσω της ανίχνευσης, της ταξινόμησης και της διόρθωσής τους.

Δίκτυο προγραμμάτων ρομπότ (botnet): Δίκτυο υπολογιστών που έχουν προσβληθεί από κακόβουλο λογισμικό και ελέγχονται εξ αποστάσεως, χωρίς γνώση των χρηστών, για την αποστολή ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam), την κλοπή πληροφοριών ή την εξαπόλυση συντονισμένων κυβερνοεπιθέσεων.

Εγκατάσταση επιδιορθώσεων (patching): Η εγκατάσταση σειράς τροποποιήσεων σε λογισμικό ή η επικαιροποίηση, η διόρθωση ή η βελτίωσή του, συμπεριλαμβανομένης της αντιμετώπισης τρωτών σημείων ασφάλειας.

Έγκλημα που διευκολύνεται από τον κυβερνοχώρο: Παραδοσιακό έγκλημα που διαπράττεται σε μεγαλύτερη κλίμακα με τη χρήση συστημάτων πληροφορικής.

Έγκλημα που εξαρτάται από τον κυβερνοχώρο: Έγκλημα που μπορεί να διαπραχθεί μόνο με τη χρήση συσκευών ΤΠ.

Εκλογική υποδομή: Περιλαμβάνει τα συστήματα πληροφορικής και τις βάσεις δεδομένων των προεκλογικών εκστρατειών, τις ευαίσθητες πληροφορίες σχετικά με τους υποψηφίους και τα συστήματα εγγραφής και διαχείρισης των ψηφοφόρων.

Εμπιστευτικότητα: Η προστασία πληροφοριών, δεδομένων ή περιουσιακών στοιχείων από μη εξουσιοδοτημένη πρόσβαση ή κοινολόγηση.

Εργαλεία εκμετάλλευσης ατελειών (exploit kit): Ένα είδος εργαλειοθήκης που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου με το οποίο εκμεταλλεύονται τρωτά σημεία των δικτύων και των συστημάτων πληροφοριών προκειμένου να διανέμουν κακόβουλο λογισμικό ή για άλλου είδους κακόβουλες δραστηριότητες.

Ηλεκτρονικό «ψάρεμα» (phishing): Η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου που μοιάζει να προέρχονται από αξιόπιστη πηγή, προκειμένου να παραπλανηθούν οι αποδέκτες τους να κάνουν κλικ σε κακόβουλους συνδέσμους ή να καταχωρίσουν πληροφορίες προσωπικού χαρακτήρα.

Κακόβουλο λογισμικό (malware): Πρόγραμμα πληροφορικής σχεδιασμένο να βλάπτει υπολογιστές, εξυπηρετητές ή δίκτυα.

Κακόβουλο λογισμικό διαγραφής δεδομένων (wiper malware): Είδος κακόβουλου λογισμικού που έχει στόχο τη διαγραφή όλων των δεδομένων από τον σκληρό δίσκο του υπολογιστή που προσβάλλει.

Κατανεμημένη άρνηση υπηρεσίας (Distributed Denial of Service, DDoS): Κυβερνοεπίθεση που εμποδίζει την πρόσβαση των νόμιμων χρηστών σε υπηρεσία ή

πόρο που διατίθεται μέσω του διαδικτύου κατακλύζοντάς τα με περισσότερα αιτήματα από όσα μπορούν να διαχειριστούν.

Κληροδοτημένο σύστημα: Παρωχημένο ή απαρχαιωμένο σύστημα, εφαρμογή ή γλώσσα προγραμματισμού που χρησιμοποιείται ακόμη, αλλά για το οποίο ενδέχεται να μην διατίθενται πλέον αναβαθμίσεις και στήριξη από τον προμηθευτή, συμπεριλαμβανομένης της στήριξης στον τομέα της ασφάλειας.

Κοινωνική μηχανική: Στο πλαίσιο της ασφάλειας των πληροφοριών, η ψυχολογική χειραγώγηση για την εξαπάτηση προσώπων ώστε να προβούν σε ενέργεια ή να αποκαλύψουν εμπιστευτικές πληροφορίες.

Κρυπτογράφηση: Η μετατροπή αναγνώσιμων πληροφοριών σε μη αναγνώσιμο κώδικα για την προστασία τους. Προκειμένου να αποκρυπτογραφήσει τις πληροφορίες, ο χρήστης πρέπει να έχει πρόσβαση σε μυστικό κλειδί ή κωδικό πρόσβασης.

Κρυπτονόμισμα: Ψηφιακό περιουσιακό στοιχείο που εκδίδεται και ανταλλάσσεται με τη χρήση τεχνικών κρυπτογράφησης, ανεξάρτητα από κάθε κεντρική τράπεζα. Γίνεται δεκτό ως μέσο πληρωμής μεταξύ των μελών μιας εικονικής κοινότητας.

Κυβερνοάμυνα: Επιμέρους τμήμα της κυβερνοασφάλειας που αποσκοπεί στην προστασία του κυβερνοχώρου με στρατιωτικά και άλλα πρόσφορα μέσα για την επίτευξη στρατιωτικο-στρατηγικών στόχων.

Κυβερνοανθεκτικότητα: Η ικανότητα αποτροπής κυβερνοεπιθέσεων και κυβερνοπεριστατικών, προετοιμασίας για την αντιμετώπισή τους, αντίστασης και ανάκαμψης.

Κυβερνοασφάλεια: Το σύνολο των διασφαλίσεων και μέτρων που υιοθετούνται για την προστασία των συστημάτων πληροφοριών και των χρηστών τους από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και ζημίες, ώστε να εξασφαλίζεται η διαθεσιμότητα, το απόρρητο και η ακεραιότητα των δεδομένων.

Κυβερνοέγκλημα: Διάφορες εγκληματικές δραστηριότητες με τους ηλεκτρονικούς υπολογιστές και τα συστήματα ΤΠ είτε ως βασικό εργαλείο είτε ως πρωταρχικό στόχο. Στις δραστηριότητες αυτές περιλαμβάνονται οι εξής: παραδοσιακά αδικήματα (π.χ. απάτη, πλαστογραφία και κλοπή ταυτότητας)· αδικήματα σχετικά με το περιεχόμενο (π.χ. διανομή υλικού παιδικής πορνογραφίας μέσω του διαδικτύου ή υποκίνηση φυλετικού μίσους)· και αδικήματα που αφορούν ειδικά τους ηλεκτρονικούς υπολογιστές και τα συστήματα πληροφοριών (π.χ. επιθέσεις κατά συστημάτων πληροφοριών, επιθέσεις άρνησης υπηρεσίας και επιθέσεις με κακόβουλο λογισμικό).

Κυβερνοεπίθεση: Απόπειρα υπονόμευσης ή καταστροφής του απορρήτου, της ακεραιότητας και της διαθεσιμότητας δεδομένων ή συστήματος πληροφορικής μέσω του κυβερνοχώρου.

Κυβερνοοικοσύστημα: Μια πολύπλοκη κοινότητα συσκευών, δεδομένων, δικτύων, προσώπων, διαδικασιών και οργανισμών που αλληλεπιδρούν, καθώς και το περιβάλλον διεργασιών και τεχνολογιών που επηρεάζει και υποστηρίζει τις εν λόγω αλληλεπιδράσεις.

Κυβερνοπεριστατικό: Περιστατικό το οποίο, άμεσα ή έμμεσα, βλάπτει ή απειλεί την ανθεκτικότητα και την ασφάλεια ενός συστήματος ΤΠ και των δεδομένων που αυτό επεξεργάζεται ή τα οποία είναι αποθηκευμένα σε αυτό ή διαβιβάζονται από αυτό.

Κυβερνοχώρος: Το άυλο παγκόσμιο περιβάλλον στο οποίο πραγματοποιείται διαδικτυακή επικοινωνία μεταξύ προσώπων, λογισμικού και υπηρεσιών, μέσω δικτύων ηλεκτρονικών υπολογιστών και τεχνολογικών συσκευών.

Λυτρισμικό: Κακόβουλο λογισμικό που εμποδίζει την πρόσβαση των θυμάτων σε σύστημα πληροφορικής ή καθιστά μη αναγνώσιμα τα αρχεία, συνήθως μέσω κρυπτογράφησης. Εν συνεχεία, ο δράστης της επίθεσης κατά κανόνα εκβιάζει το θύμα, αρνούμενος να αποκαταστήσει την πρόσβαση έως ότου καταβληθούν λύτρα.

Μοντέλο «crime-as-a-service» (Caas): Εγκληματικό επιχειρηματικό μοντέλο στο οποίο βασίζεται η ψηφιακή υπόγεια οικονομία, που παρέχει ένα ευρύ φάσμα εμπορικών υπηρεσιών και εργαλείων τα οποία παρέχουν τη δυνατότητα σε κυβερνοεγκληματίες χωρίς ειδικές γνώσεις να διαπράττουν κυβερνοεγκλήματα.

Παραπληροφόρηση: Επαληθεύσιμα ψευδής ή παραπλανητική πληροφορία που δημιουργείται, παρουσιάζεται και διαδίδεται με σκοπό τον προσπορισμό οικονομικού οφέλους ή την εσκεμμένη εξαπάτηση του κοινού και μπορεί να προκαλέσει δημόσια ζημία.

Πρόγραμμα διαφημίσεων (adware): Κακόβουλο λογισμικό προβολής διαφημιστικών πλαισίων ή αναδυόμενων παραθύρων (pop-ups) που περιλαμβάνουν κώδικα για την παρακολούθηση της συμπεριφοράς των θυμάτων στο διαδίκτυο.

Υβριδική απειλή: Εκδήλωση εχθρικής πρόθεσης με τη χρήση μείγματος συμβατικών και μη συμβατικών τεχνικών πολέμου (π.χ. στρατιωτικών, πολιτικών, οικονομικών και τεχνολογικών μεθόδων) με σκοπό τη σθεναρή επιδίωξη των στόχων τους.

Υπηρεσίες εμπιστοσύνης: Υπηρεσίες που ενισχύουν τη νομική εγκυρότητα μιας ηλεκτρονικής συναλλαγής, όπως οι ηλεκτρονικές υπογραφές, οι ηλεκτρονικές

σφραγίδες, οι χρονοσφραγίδες, οι υπηρεσίες ηλεκτρονικής παράδοσης και η εξακρίβωση της γνησιότητας των ιστοσελίδων.

Υποδομές ζωτικής σημασίας: Κάθε φυσικός πόρος, υπηρεσία, σύστημα πληροφορικής και υποδομή, της οποίας η διακοπή ή καταστροφή θα είχε σοβαρό αντίκτυπο στη λειτουργία της οικονομίας και της κοινωνίας.

Υπολογιστικό νέφος: Η παροχή πόρων ΤΠ κατά παραγγελία –όπως αποθήκευση, υπολογιστική ισχύς ή ικανότητα κοινοχρησίας δεδομένων– στο περιβάλλον του διαδικτύου, μέσω φιλοξενίας σε απομακρυσμένους εξυπηρετητές.

Ψηφιακό περιεχόμενο: Κάθε είδους δεδομένα –όπως κείμενο, ήχος, εικόνες ή βίντεο– που αποθηκεύονται σε ψηφιακή μορφή.

[1] Στο σχέδιο πράξης της ΕΕ για την ασφάλεια στον κυβερνοχώρο, ορίζεται ως «όλες οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών τους και των προσώπων που υφίστανται τις συνέπειες κυβερνοαπειλών». Η πράξη αναμένεται να εγκριθεί από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις αρχές του 2019.

[2] Ευρωπόλ, *«Internet Organised Crime Threat Assessment 2017»*.

[3] Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο (ECSO), *«European Cybersecurity Industry Proposal for a contractual Public-Private Partnership»*, Ιούνιος 2016.

[4] Ευρωπαϊκό Κοινοβούλιο, *«Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses»*, Μελέτη για την Επιτροπή Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων, Σεπτέμβριος 2015.

[5] ENISA, *«ENISA Threat Landscape Report 2017»*, 18 Ιανουαρίου 2018.

[6] Ευρωπόλ, *«Internet Organised Crime Threat Assessment 2018»*.

[7] Ευρωπόλ, *όπ.π.*, 2018.

[8] European Centre for Political Economy, *«Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?»*, έκτακτο έγγραφο αριθ. 2/18, Φεβρουάριος 2018.

[9] Ομιλία του Προέδρου της Ευρωπαϊκής Επιτροπής για την κατάσταση της Ένωσης, 2017.

[10] Ευρωπόλ, *«World's Biggest Marketplace selling internet paralysing DDoS attacks taken down»*, δελτίο Τύπου, 25 Απριλίου 2018.

[11] Ευρωπόλ, *«Internet Organised Crime Threat Assessment 2017»*.

[12] Ενημερωτικό δελτίο της Ευρωπαϊκής Επιτροπής για την κυβερνοασφάλεια, Σεπτέμβριος 2017.

[13] Το κόστος μπορεί να περιλαμβάνει: απώλεια εσόδων, κόστος αποκατάστασης βλαβών συστημάτων, πιθανές υποχρεώσεις για κλεμμένα περιουσιακά στοιχεία ή πληροφορίες, παροχή κινήτρων για τη διατήρηση πελατών, υψηλότερα ασφάλιστρα, αυξημένες δαπάνες προστασίας (νέα συστήματα, εργαζόμενοι, κατάρτιση), δυνητικό κόστος συμμόρφωσης ή δικαστικά έξοδα.

[14] NTT Security, *«Risk:Value 2018 Report»*.

[15] Το λυτρισμικό *WannaCry* εκμεταλλευόταν κενά ασφάλειας ενός πρωτοκόλλου των Windows της Microsoft που επέτρεπαν την εξ αποστάσεως απόκτηση του ελέγχου οποιουδήποτε υπολογιστή. Μετά τον εντοπισμό του κενού ασφάλειας, η εταιρεία εξέδωσε μια πρόχειρη τροποποίηση (patch). Ωστόσο, τα συστήματα εκατοντάδων χιλιάδων υπολογιστών δεν είχαν ακόμη ενημερωθεί, και πολλοί από αυτούς στη συνέχεια μολύνθηκαν. Πηγή: A. Greenberg, *«Hold North Korea Accountable For Wannacry—and the NSA, too»*, WIRED, 19 Δεκεμβρίου 2017.

[16] Ευρωπαϊκή Επιτροπή, «*Europeans' attitudes towards cybersecurity*», Ειδικό Ευρωβαρόμετρο 464α, Σεπτέμβριος 2017. Μια συμπληρωματική έρευνα αναμένεται να δημοσιευτεί στις αρχές του 2019.

[17] Η σύμβαση της Βουδαπέστης είναι μια δεσμευτική διεθνής κατευθυντήρια γραμμή για τις χώρες που καταρτίζουν νομοθεσία για την καταπολέμηση του κυβερνοεγκλήματος. Παρέχει ένα πλαίσιο για τη διεθνή συνεργασία μεταξύ των συμβαλλομένων κρατών. Επί του παρόντος, η ΕΕ εκπροσωπείται από την Επιτροπή, το Συμβούλιο της Ευρωπαϊκής Ένωσης, την Ευρωπόλ, τον ENISA και την Eurojust.

[18] Ευρωπαϊκή Επιτροπή, *«Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο»*, JOIN (2013) 1 final, 7 Φεβρουαρίου 2013.

[19] Ευρωπαϊκή Επιτροπή, *Το ευρωπαϊκό θεματολόγιο για την ασφάλεια*, COM (2015) 185 final της 28ης Απριλίου 2015.

[20] Ευρωπαϊκή Επιτροπή, *Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης*, COM (2015) 192 final της 6ης Μαΐου 2015.

[21] ΕΥΕΔ *«Κοινό όραμα, κοινές δράσεις: Μια ισχυρότερη Ευρώπη. Μια συνολική στρατηγική για την εξωτερική πολιτική και την πολιτική ασφάλειας της Ευρωπαϊκής Ένωσης»*, Ιούνιος 2016.

[22] Κέντρο Ευρωπαϊκών Πολιτικών Μελετών, *«Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force»*, Νοέμβριος 2018.

[23] Το κακόβουλο λογισμικό που χρησιμοποιήθηκε στην επίθεση με το λυτρισμικό WannaCry, για το οποίο οι Ηνωμένες Πολιτείες, το Ηνωμένο Βασίλειο και η Αυστραλία θεώρησαν υπεύθυνη τη Βόρεια Κορέα, αναπτύχθηκε αρχικά και φυλασσόταν προς μελλοντική χρήση από την Υπηρεσία Εθνικής Ασφαλείας των ΗΠΑ. Στόχος του ήταν η εκμετάλλευση τρωτών σημείων των Windows. Πηγή: A. Greenberg, όπ.π.., WIRED, 19 Δεκεμβρίου 2017. Στον απόηχο των επιθέσεων, η Microsoft καταδίκασε την πρακτική των κυβερνήσεων να εντοπίζουν αλλά να μην γνωστοποιούν τρωτά σημεία των λογισμικών και επανέλαβε την έκκλησή της για μια σύμβαση της Γενεύης για ψηφιακά θέματα.

[24] Επιπλέον της ξηράς, της θάλασσας, του αέρα και του διαστήματος.

[25] Πλαίσιο πολιτικής της ΕΕ για την κυβερνοάμυνα (επικαιροποίηση 2018), 14413/18, 19 Νοεμβρίου 2018.

[26] Ευρωπαϊκή Επιτροπή / Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, *«Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών: απόκριση της Ευρωπαϊκής Ένωσης»*, JOIN (2016) 18 final της 6ης Απριλίου 2016.

[27] Κοινή δήλωση του Προέδρου του Ευρωπαϊκού Συμβουλίου, του Προέδρου της Ευρωπαϊκής Επιτροπής και του Γενικού Γραμματέα του Οργανισμού Βορειοατλαντικού Συμφώνου, της 8ης Ιουλίου 2016 και της 10ης Ιουλίου 2018.

[28] Ευρωπαϊκή Επιτροπή / Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, *«Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ»*, JOIN (2017) 450 final της 13ης Σεπτεμβρίου 2017.

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

[30] 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.

[31] Αυτές είναι ενσωματωμένες σε δομές συνεργασίας που θεσπίζει η οδηγία, το δίκτυο CSIRTS (δίκτυο αποτελούμενο από τις CSIRT που έχουν ορίσει τα κράτη μέλη της ΕΕ και τη CERT-ΕΕ· ο ENISA φιλοξενεί τη γραμματεία του δικτύου) και την ομάδα συνεργασίας (που υποστηρίζει και διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών, και της οποίας η γραμματεία φιλοξενείται από την Επιτροπή).

[32] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

[33] Ευρωπαϊκή Επιτροπή, *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο», και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»),* COM (2017) 477 final της 13ης Σεπτεμβρίου 2017.

[34] Ευρωπαϊκή Επιτροπή, *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ευρωπαϊκή εντολή υποβολής και την ευρωπαϊκή εντολή διατήρησης ηλεκτρονικών αποδεικτικών στοιχείων σε ποινικές υποθέσεις,* COM (2018) 225 final της 17ης Απριλίου 2018.

[35] Ευρωπαϊκή Επιτροπή, *Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση εναρμονισμένων κανόνων για τον ορισμό νόμιμων εκπροσώπων με σκοπό τη συγκέντρωση αποδεικτικών στοιχείων στο πλαίσιο ποινικών διαδικασιών.* COM (2018) 226 final της 17ης Απριλίου 2018.

[36] Ευρωπαϊκή Επιτροπή, *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη σύσταση του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού,* COM (2018) 630 final της 12ης Σεπτεμβρίου 2018.

[37] H. Carrapico και A. Barrinha, *«The EU as a Coherent (Cyber)Security Actor?»*, Journal of Common Market Studies, τόμος 55, αριθ. 6, 2017.

[38] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[39] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, *«Transatlantic cyber-insecurity and cybercrime».«Economic impact and future prospects»*, PE 603.948, Δεκέμβριος 2017.

[40] ENISA, *«An evaluation framework for Cyber Security Strategies»*, 27 Νοεμβρίου 2014.

[41] Εξαίρεση αποτελεί το άρθρο 14 (Παρακολούθηση και στατιστικές) της οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013 , για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.

[42] Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, *«Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks»*, Μάρτιος 2018. Ειδική ομάδα του Κέντρου Μελετών Ευρωπαϊκής Πολιτικής και του ECRI (European Credit Research Institute), «Cybersecurity in Finance: Getting the policy mix right!», Ιούνιος 2018.

[43] Επί συνόλου 28 ανώτατων οργάνων ελέγχου, 24 απάντησαν στην έρευνά μας.

[44] Μηχανισμός επιστημονικών συμβουλών της Ευρωπαϊκής Επιτροπής, «Scientific Opinion 2/2017», 24 Μαρτίου 2017.

[45] Ήτοι βασιζόμενο σε αρχές και –στο μέτρο του δυνατού– τεχνολογικά ουδέτερο.

[46] L. Rebuffi, *«EU Digital Autonomy: A possible approach»*, Digma Zeitschrift für Datenrecht und Informationssicherheit, Σεπτέμβριος 2018. European Centre for Political Economy, όπ.π., «Occasional Paper No 2/18», Φεβρουάριος 2018.

[47] Ευρωπαϊκή Επιτροπή, *Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για την προμήθεια ψηφιακού περιεχομένου*, COM(2015) 634 finalτης 9ης Δεκεμβρίου 2015.

[48] Ευρωπαϊκή Επιτροπή, *Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες πτυχές που αφορούν τις συμβάσεις για τις διαδικτυακές και άλλες εξ αποστάσεως πωλήσεις αγαθών*, COM(2017) 635 final, της 9ης Δεκεμβρίου 2015.

[49] Ολλανδικό Συμβούλιο Κυβερνοασφάλειας, *European Foresight Cyber Security Meeting 2016: «Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care»*, 2016.

[50] Κέντρο Μελετών Ευρωπαϊκής Πολιτική, *«Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force»*, Ιούνιος 2018.

[51] Ευρωπαϊκή Επιτροπή, *Αξιοποιώντας την ΑΔΠ στο έπακρον – Για την αποτελεσματική εφαρμογή της οδηγίας (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*, COM(2017) 476 final/2 της 4ης Οκτωβρίου 2017.

[52] Ευρωπόλ, όπ.π., 2017.

[53] Συμβούλιο της Ευρωπαϊκής Ένωσης, *Τελική έκθεση του έβδομου γύρου αμοιβαίων αξιολογήσεων σχετικά με την «Πρακτική εφαρμογή και λειτουργία των ευρωπαϊκών πολιτικών για την πρόληψη και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο»*, 12711/1/17 REV 1, 9 Οκτωβρίου 2017.

[54] Ευρωπαϊκή Επιτροπή, Εκτίμηση επιπτώσεων που συνοδεύει την πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την καταπολέμηση της απάτης και της

πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών, SWD/2017/0298 final της 13ης Σεπτεμβρίου 2017. Πολιτική συμφωνία σχετικά με τη νέα νομοθεσία επιτεύχθηκε τον Δεκέμβριο του 2018 και αναμένεται να εγκριθεί στις αρχές του 2019.

[55] Ευρωπόλ, όπ.π., 2017.

[56] C-362/14: Maximillian Schrems κατά Data Protection Commissioner (Ιρλανδία), 6 Οκτωβρίου 2015.

[57] Ευρωπόλ/Eurojust, *«Common challenges in combating cybercrime»*, 7021/17 της 13ης Μαρτίου 2017.

[58] Ευρωπαϊκή Επιτροπή, *«Αξιολόγηση της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο»*, SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[59] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, *«Briefing: EU Legislation in Progress – Review of dual-use export controls»*, *PE589.832*.

[60] Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου, της 8ης Σεπτεμβρίου 2015, *ανθρώπινα δικαιώματα και την τεχνολογία: ο αντίκτυπος των συστημάτων παρείσφρησης και παρακολούθησης στα ανθρώπινα δικαιώματα στις τρίτες χώρες*, (2014/2232(INI)), 8 Σεπτεμβρίου 2015. Τα είδη και οι υπηρεσίες διπλής χρήσης, στα οποία συμπεριλαμβάνονται λογισμικό και τεχνολογία, μπορούν να χρησιμοποιηθούν τόσο σε μη στρατιωτικές όσο και σε στρατιωτικές εφαρμογές.

[61] Οι δημόσια διαθέσιμες πληροφορίες αποθηκεύονται στη βάση δεδομένων WHOIS, την οποία διαχειρίζεται το ICANN (Σώμα του Διαδικτύου για την εκχώρηση ονομάτων και αριθμών). Το ICANN διαχειρίζεται το σύστημα ονομάτων χώρου (Domain Name System). Η κατάχρηση ονομάτων χώρου διευκολύνει την κυβερνοεγκληματικότητα.

[62] Άρθρο 3 της οδηγίας NIS, όπ.π.

[63] Συμβούλιο του Ατλαντικού, *«Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures»*, 10 Σεπτεμβρίου 2015.

[64] The White House, *«Cybersecurity spending fiscal year 2019»*.

[65] Ευρωπαϊκή Επιτροπή, *Έγγραφο εργασίας των υπηρεσιών της Επιτροπής: Εκτίμηση επιπτώσεων που συνοδεύει το έγγραφο «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη για την περίοδο 2021-2027»*, SWD(2018) 305 final της 6ης Ιουνίου 2018.

[66] Κέντρο στρατηγικών μελετών της Χάγης, *«Dutch investments in ICT and cybersecurity: putting it in perspective»*, Δεκέμβριος 2016.

[67] Ευρωπαϊκή Επιτροπή, όπ.π., COM(2018) 630 final της 12ης Σεπτεμβρίου 2018.

[68] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, Μονάδα Διερεύνησης Επιστημονικών Προοπτικών, *«Achieving a sovereign and trustworthy ICT industry in the EU»*, Δεκέμβριος 2017.

[69] European Digital SME Alliance, *«Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem»*, 31 Ιουλίου 2017.

[70] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, Μονάδα Διερεύνησης Επιστημονικών Προοπτικών, όπ.π., Δεκέμβριος 2017.

[71] Όπ.π..

[72] Ευρωπαϊκή Επιτροπή, *«Impact assessment on the proposed research competence centre and network of national coordination centres»*, SWD(2018) 403 final (Μέρος 1/4) της 12ης Σεπτεμβρίου 2018.

[73] Ευρωπαϊκή Επιτροπή, όπ.π., COM(2018) 630 final της 12ης Σεπτεμβρίου 2018.

[74] Ειδική έκθεση αριθ. 13/2018 του ΕΕΣ: «Αντιμετώπιση της ριζοσπαστικοποίησης που οδηγεί στην τρομοκρατία».

[75] Τα αριθμητικά στοιχεία που παρατίθενται στην παρούσα ενότητα προέρχονται από δημόσια διαθέσιμα έγγραφα της Επιτροπής, εξαιρουμένου του ποσού των 42 εκατομμυρίων ευρώ που αναφέρεται στο σημείο ***51***, το οποίο μας παρέσχε απευθείας η Επιτροπή.

[76] Το πρόγραμμα «Ορίζων 2020» είναι το ύψους 80 δισεκατομμυρίων ευρώ πρόγραμμα της ΕΕ για την έρευνα και την καινοτομία που στηρίζει την Ένωση καινοτομίας, στόχος της οποίας είναι η διασφάλιση της παγκόσμιας ανταγωνιστικότητας της ΕΕ.

[77] Κοινωνική πρόκληση αριθ. 7 του προγράμματος «Ορίζων 2020»: «ασφαλείς κοινωνίες — προστασία της ελευθερίας και της ασφάλειας της Ευρώπης και των πολιτών της».

[78] Αναλύσαμε τα έργα του προγράμματος «Ορίζων 2020» βάσει του συνόλου δεδομένων του CORDIS. Υποβάλαμε σε διανυσματοποίηση την περιγραφή κάθε έργου, βάσει της ταξινομίας της κυβερνοασφάλειας του JRC (βλέπε ***πλαίσιο 5*** στο επόμενο κεφάλαιο), για τον εντοπισμό έργων που είναι πιθανόν να σχετίζονται με την κυβερνοασφάλεια. Εν συνεχεία, ελέγξαμε με μη αυτοματοποιημένο τρόπο και αναλύσαμε τα αποτελέσματα.

[79] Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο, *«ECS cPPP Progress Monitoring Report 2016-2017»* της 29ης Οκτωβρίου 2018.

[80] Άρθρο 9, παράγραφος 2, της οδηγίας NIS, όπ.π.

[81] Το έργο GLACY+ (Global Action on Cybercrime+) υλοποιείται από κοινού με το Συμβούλιο της Ευρώπης. Στηρίζει δώδεκα χώρες στην Αφρική και σε περιοχές της Ασίας-Ειρηνικού, της Λατινικής Αμερικής και της Καραϊβικής, οι οποίες με τη σειρά τους μπορούν να χρησιμεύσουν ως κόμβοι για την ανταλλαγή των αποκομισθεισών εμπειριών με άλλες χώρες της περιοχής τους.

[82] Το Ευρωπαϊκό Κέντρο Πολιτικής Στρατηγικής (European Political Strategy Centre, EPSC), η ομάδα προβληματισμού της Επιτροπής, προειδοποίησε για το ενδεχόμενο να προκύψει «ψηφιακό τυφλό σημείο» εάν το χάσμα μεταξύ της ΕΕ και των γειτόνων της στα Δυτικά Βαλκάνια συνεχίσει να διευρύνεται. Χώρες όπως η Κίνα και η Ρωσία επενδύουν μεγάλα ποσά στην περιοχή, γεγονός που ενέχει τον κίνδυνο περιθωριοποίησης της ΕΕ ως παράγοντα του κυβερνοχώρου στην περιφέρεια αυτή. Πηγή: EPSC, *«Engaging with the Western Balkans: an investment in Europe's security»*, 17 Μαΐου 2018.

[83] Ευρωπαϊκή Τράπεζα Επενδύσεων, *«The EIB Group Operating Framework and Operational Plan 2018»* της 12ης Δεκεμβρίου 2017. Κατά τον χρόνο της σύνταξης δεν ήταν διαθέσιμες περαιτέρω πληροφορίες.

[84] Ευρωπαϊκή Επιτροπή, *Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση του προγράμματος Ψηφιακή Ευρώπη για την περίοδο 2021-2027*, COM(2018) 434 final της 6ης Ιουνίου 2018.

[85] Ευρωπαϊκή Επιτροπή, *Κανονισμός (ΕΕ) 2018/1092 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Ιουλίου 2018, για τη θέσπιση του ευρωπαϊκού προγράμματος βιομηχανικής ανάπτυξης στον τομέα της άμυνας, που αποσκοπεί στη στήριξη της ανταγωνιστικότητας και της καινοτόμου ικανότητας της αμυντικής βιομηχανίας της Ένωσης* (ΕΕ L 200 της 7.8.2018, σ. 30). Επιπλέον, το 2017 οργανώθηκε μια προπαρασκευαστική δράση για την έρευνα στον τομέα της άμυνας, συνολικού ύψους 90 εκατομμυρίων ευρώ για την περίοδο 2017-2019, η οποία χρηματοδοτείται από το πρόγραμμα «Ορίζων 2020». Δεν είναι σαφές αν περιλαμβάνει δαπάνες σχετικές με τον κυβερνοχώρο.

[86] Το 2019 το ΕΕΣ προγραμματίζει να δημοσιεύσει χωριστό ενημερωτικό έγγραφο σχετικά με την άμυνα της ΕΕ.

[87] Το κέντρο EC3 της Ευρωπόλ, ο ENISA, η ΕΥΕΔ, ο Ευρωπαϊκός Οργανισμός Άμυνας και η CERT-ΕΕ διαθέτουν από κοινού 159 υπαλλήλους. Στον συνολικό αυτό αριθμό δεν περιλαμβάνονται οι υπάλληλοι που ασχολούνται με θέματα κυβερνοχώρου σε επίπεδο Ευρωπαϊκής Επιτροπής ή κρατών μελών. Πηγή: Κέντρο Ευρωπαϊκών Πολιτικών Μελετών, όπ.π., Νοέμβριος 2018.

[88] *«ENISA evaluation»*, 2017.

[89] Στο πολυετές σχέδιο για την περίοδο 2018-2020, η Ευρωπόλ ζήτησε ετήσια αύξηση του προσωπικού κατά 70 έκτακτους υπαλλήλους. Εντούτοις, για το 2018 εγκρίθηκε αύξηση κατά μόλις 26 θέσεις. Στο επόμενο προσχέδιο πολυετούς σχεδίου για την περίοδο 2019-2021, η Ευρωπόλ πρότεινε μια συγκρατημένη αύξηση, υποθέτοντας ότι αίτημα για μεγαλύτερη αύξηση δεν θα γινόταν δεκτό. Πηγή: Διαβούλευση για το σχέδιο πολυετούς προγραμματισμού 2019-2021 που υποβλήθηκε στη μικτή ομάδα κοινοβουλευτικού ελέγχου, A 000834, 1 Φεβρουαρίου 2018.

[90] *«ENISA evaluation»*, 2017. Κατά την περίοδο 2014-2016, περίπου το 80 % του επιχειρησιακού προϋπολογισμού του ENISA χρησιμοποιήθηκε για την εκπόνηση μελετών από τρίτους.

[91] ENISA, *«Exploring the opportunities and limitations of current Threat Intelligence Platforms»*, Δεκέμβριος 2017.

[92] ISACA (γνωστή παλαιότερα ως Ένωση Ελέγχων Πληροφοριακών Συστημάτων), *«Information Security Governance: Guidance for Boards of Directors and Executive Management»*, 2η έκδοση., 2006.

[93] ΕΥ, *«Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017»*, σ. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy και H. Lung), *«Hit or myth? Understanding the true costs and impact of cybersecurity programs»*, Ιούλιος 2017.

[95] Επιτροπή Κεφαλαιαγοράς, *«Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures»*, 21 Φεβρουαρίου 2018.

[96] Φόρουμ συνεργασίας μεταξύ της Ευρωπαϊκής Αρχής Τραπεζών, της Ευρωπαϊκής Αρχής Κινητών Αξιών και Αγορών και της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων.

[97] Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών, *«Joint Committee report on risks and vulnerabilities in the EU financial system»*, Απρίλιος 2018.

[98] ENISA, *«Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs»*, Δεκέμβριος 2015.

[99] Όσον αφορά τα κράτη μέλη της ΕΕ, ο μηχανισμός επιστημονικών συμβουλών της Επιτροπής επισήμανε τον σημαντικό και μοναδικό βαθμό συμφωνίας επί των θεμελιωδών αρχών και αξιών, καθώς και το κοινό στρατηγικό συμφέρον που μπορεί να βρίσκεται στο επίκεντρο της αποτελεσματικής διακυβέρνησης της κυβερνοασφάλειας σε επίπεδο ΕΕ. Πηγή: «Scientific Opinion 2/2017», 24 Μαρτίου 2017.

[100] Ηνωμένες Πολιτείες, Κίνα, Ιαπωνία, Νότια Κορέα, Ινδία και Βραζιλία.

[101] Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας. (T. Renard και A. Barrinha), *Handbook on cyber security, κεφάλαιο 3.4 «The EU as a partner in cyber diplomacy and defence»*, 23 Νοεμβρίου 2018.

[102] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Σχέδιο δράσης για την εφαρμογή των συμπερασμάτων του Συμβουλίου ως προς την κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ»*, JOIN (15748) 17 final της 12ης Δεκεμβρίου 2017.

[103] Ευρωπαϊκή Επιτροπή, *«European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final της 21ης Νοεμβρίου 2018.

[104] Απάντηση του Επιτρόπου Gabriel σε γραπτή κοινοβουλευτική ερώτηση (E-004294-17) της 28ης Ιουνίου 2017.

[105] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Ετήσια έκθεση του 2017 για την εφαρμογή του πλαισίου πολιτικής της ΕΕ για την κυβερνοάμυνα»*, 15870/17, 19 Δεκεμβρίου 2017.

[106] Οι αποφάσεις 2015/443, 2015/444 και 2017/46 διέπουν την ασφάλεια των συστημάτων επικοινωνίας και πληροφοριών της Επιτροπής. Με την απόφαση C(2018) 7706 της Επιτροπής, της 21ης Νοεμβρίου 2018, συγκροτείται συμβούλιο τεχνολογίας των πληροφοριών και κυβερνοασφάλειας, που συγχωνεύει το παλαιότερο συμβούλιο τεχνολογίας των πληροφοριών και τη διοικούσα επιτροπή ασφάλειας πληροφοριών.

[107] Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, όπ.π., Μάρτιος 2018.

[108] Ευρωπαϊκό Κοινοβούλιο, όπ.π., Σεπτέμβριος 2015.

[109] Η Μονάδα Ανάλυσης Υβριδικών Απειλών συστάθηκε το 2016 στο πλαίσιο του Κέντρου Ανάλυσης Πληροφοριών της ΕΕ στους κόλπους της ΕΥΕΔ. Λαμβάνει και αναλύει διαβαθμισμένες πληροφορίες και πληροφορίες ανοικτής πηγής από διάφορα ενδιαφερόμενα μέρη σχετικά με υβριδικές απειλές.

[110] ENISA, *«National-level Risk Assessments: An Analysis Report»*, Νοέμβριος 2013.

[111] Ευρωπαϊκή Επιτροπή, *«Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act»*, SWD(2017) 500 final (Μέρος 1/6) της 13ης Σεπτεμβρίου 2017.

[112] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2018) 403 final της 12ης Σεπτεμβρίου 2018.

[113] Κέντρο Διαδικτυακού Συντονισμού RIPE (Résaux IP Européens Network Coordination Centre), το περιφερειακό διαδικτυακό μητρώο για την Ευρώπη που επιβλέπει την εκχώρηση και καταχώριση των πόρων αριθμών διαδικτύου.

[114] ENISA, *«EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs»*, Νοέμβριος 2012.

[115] Centre for Cyber Safety and Education, σε συνεργασία με τις Booz Allen Hamilton, Alta Associates και Frost & Sullivan, *«2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk»*.

[116] Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, όπ.π., Μάρτιος 2018.

[117] Βουλή των Λόρδων, *«House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19»*, 16 Ιουλίου 2018.

[118] Ευρωπόλ/Eurojust, *«Common challenges in combatting cybercrime»*, 7021/17 της 13ης Μαρτίου 2017.

[119] Ευρωπόλ/Eurojust, όπ.π., 7021/17, 13 Μαρτίου 2017.

[120] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2018) 403 final της 12ης Σεπτεμβρίου 2018.

[121] CEPOL, *«Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022»* της 20ής Νοεμβρίου 2018.

[122] Παραδείγματος χάριν, η συνεργασία μεταξύ της ΕΥΕΔ, των κρατών μελών, και οργανισμών και φορέων όπως ο CEPOL, η Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος (ECTEG) ή η Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας (EAAA).

[123] ENISA, *«Stock-taking of information security training needs in critical sectors»*, Δεκέμβριος 2017.

[124] Ευρωπαϊκή Ομάδα για την Εκπαίδευση και Κατάρτιση στον τομέα του Κυβερνοεγκλήματος.

[125] Ευρωπαϊκή Επιτροπή, Δέκατη τρίτη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας, COM(2018) 46 final της 24ης Ιανουαρίου 2018.

[126] Βάσει των παρατηρήσεων που διατυπώνονται στην Ειδική έκθεση αριθ. 14/2018, όπ.π.

[127] Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου, της 13ης Ιουνίου 2018, σχετικά με την άμυνα στον κυβερνοχώρο (2018/2004(INI)). Συμβούλιο της Ευρωπαϊκής Ένωσης, όπ.π., 15870/17 της 19ης Δεκεμβρίου 2017.

[128] Ελβετία, Βόρεια Μακεδονία, Ουκρανία, Βοσνία-Ερζεγοβίνη, Κοσσυφοπέδιο (η ονομασία αυτή χρησιμοποιείται με την επιφύλαξη των θέσεων ως προς το καθεστώς και συνάδει με το ψήφισμα 1244/1999 του Συμβουλίου Ασφαλείας των Ηνωμένων Εθνών και τη γνώμη του Διεθνούς Δικαστηρίου σχετικά με τη διακήρυξη της ανεξαρτησίας του Κοσσυφοπεδίου), Τουρκία και Ηνωμένες Πολιτείες.

[129] Ευρωπόλ, *«Internet Organised Crime Threat Assessment 2018»*.

[130] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman και S. Furman, *«Security Fatigue»*, «IT Professional», τόμος 18, αριθ. 5, 2016, σ. 26-32. Βλέπε επίσης NIST.

[132] Ευρωπαϊκή Επιτροπή/Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, *«Increasing resilience and bolstering capabilities to address hybrid threats»*, JOIN(2018) 16 final της 13ης Ιουνίου 2018.

[133] Παραδείγματος χάριν, η διακοπή της λειτουργίας των Alphabay και Hansa χάρη σε κοινές επιχειρήσεις υπό την ηγεσία του FBI και της ολλανδικής εθνικής αστυνομίας με την υποστήριξη της Ευρωπόλ. Πρόκειται για δύο από τα μεγαλύτερα κρυπτοκαταστήματα διακίνησης παράνομων εμπορευμάτων, όπως ναρκωτικά, πυροβόλα όπλα και εργαλεία κυβερνοεγκληματικότητας, π.χ. κακόβουλο λογισμικό. Πηγή: Ευρωπόλ, *«Crime on the Dark Web: Law Enforcement coordination is the only cure»*, Δελτίο Τύπου της 29ης Μαΐου 2018.

[134] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2018) 403 final της 12ης Σεπτεμβρίου 2018.

[135] Συμβούλιο της Ευρωπαϊκής Ένωσης, όπ.π., 12711/1/17 REV 1 της 9ης Οκτωβρίου 2017.

[136] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[137] Ευρωπαϊκή Επιτροπή/Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, όπ.π., JOIN(2018) 16 της 13ης Ιουνίου 2018.

[138] Ευρωπαϊκή Επιτροπή, SWD (2017) 500 final της 13ης Σεπτεμβρίου 2017.

[139] *Μνημόνιο συνεννόησης – ENISA, EOA, κέντρο EC3 της Ευρωπόλ και CERT-EE* της 23ης Μαΐου 2018.

[140] Ευρωπαϊκή Επιτροπή, πρόσκληση υποβολής προσφορών: *«Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap»* της 27ης Οκτωβρίου 2017.

[141] Jean-Claude Juncker, Επιστολή ανάθεσης καθηκόντων που απευθύνεται στον Επίτροπο για την Ένωση Ασφάλειας της 2ας Αυγούστου 2016. Η άμυνα δεν εμπίπτει στην αρμοδιότητα της ειδικής ομάδας.

[142] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«EU cybersecurity roadmap»*, 8901/17 της 11ης Μαΐου 2017.

[143] Friends of Europe, *«Debating Security Plus: Crowdsourcing solutions to the world's security issues», 5η έκδοση*, Νοέμβριος 2017.

[144] Τεχνικές εκθέσεις του Κοινού Κέντρου Ερευνών, «European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy».* «Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres», SWD(2018) 403 final της 12ης Σεπτεμβρίου 2018.

[145] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[146] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2018) 403 final της 12ης Σεπτεμβρίου 2018.

[147] Παραδείγματος χάριν, στο ISAC των ευρωπαϊκών χρηματοπιστωτικών ιδρυμάτων συμμετέχουν εκπρόσωποι του χρηματοπιστωτικού τομέα, εθνικές CERT, υπηρεσίες επιβολής του νόμου, ο ENISA, η Ευρωπόλ, η Ευρωπαϊκή Κεντρική Τράπεζα, το Ευρωπαϊκό Συμβούλιο Πληρωμών και η Ευρωπαϊκή Επιτροπή.

[148] ENISA, *«Information Sharing and Analysis Centres (ISACs) Cooperative models»* της 14ης Φεβρουαρίου 2018.

[149] Συμβούλιο της Ευρωπαϊκής Ένωσης, όπ.π., 12711/1/17 REV 1, 9 Οκτωβρίου 2017.

[150] https://www.europol.europa.eu/empact.

[151] Στο πλαίσιο μελέτης που διενήργησε η Accenture το 2018 σε 15 χώρες διαπιστώθηκε ότι το 87 % των στοχευμένων κυβερνοεπιθέσεων αντιμετωπίζονταν: *«2018 State of Cyber Resilience»* της 10ης Απριλίου 2018.

[152] P. Timmers, *«Cybersecurity is Forcing a Rethink of Strategic Autonomy»*, Oxford University Politics Blog, 14 Σεπτεμβρίου 2018.

[153] Caroline Preece, *«Three reasons why cyber threat detection is still ineffective»*, IT Pro, 14 Ιουλίου 2017.

[154] Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, *όπ.π.*, Μάρτιος 2018.

[155] Ευρωπαϊκή Επιτροπή, *Όγδοη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας,*, COM(2017) 354 final της 29ης Ιουνίου 2017.

[156] Βλέπε τις διάφορες δημοσιεύσεις της ομάδας συνεργασίας NIS.

[157] PSD2: Οδηγία για τις υπηρεσίες πληρωμών, ΕΚΤ/ΕΕΜ: Ευρωπαϊκή Κεντρική Τράπεζα/Ενιαίος εποπτικός μηχανισμός, Στόχος 2: Διευρωπαϊκό Αυτοματοποιημένο Σύστημα Ταχείας Μεταφοράς Κεφαλαίων και Διακανονισμού σε Συνεχή Χρόνο (δεύτερης γενιάς), κανονισμός αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά. Πηγή: Ειδική ομάδα του Κέντρου Μελετών Ευρωπαϊκής Πολιτικής και του ECRI (European Credit Research Institute), όπ.π., Ιούνιος 2018.

[158] Ευρωπαϊκή Επιτροπή, *Σύσταση σχετικά με τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο*, C(2017) 6100 final της 13ης Σεπτεμβρίου 2017.

[159] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017. Υπάρχουν διάφοροι μηχανισμοί διαχείρισης κρίσεων, συμπεριλαμβανομένων του μηχανισμού ολοκληρωμένων ρυθμίσεων για την αντιμετώπιση πολιτικών κρίσεων (IPCR), του Argus (μηχανισμός της Επιτροπής για την αντιμετώπιση κρίσεων), του μηχανισμού αντιμετώπισης κρίσεων της ΕΥΕΔ, του μηχανισμού πολιτικής προστασίας της Ένωσης και του πρωτοκόλλου για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου.

[160] Επιπλέον, αυτό μπορεί επίσης να οδηγήσει σε επίκληση του άρθρου 42, παράγραφος 7, της Συνθήκης για την Ευρωπαϊκή Ένωση (ρήτρα αμοιβαίας συνδρομής) ή του άρθρου 222 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ρήτρα αλληλεγγύης).

[161] Ευρωπαϊκή Επιτροπή/Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, όπ.π., JOIN(2018) 16, 13 Ιουνίου 2018. Τον Δεκέμβριο του 2018, δημοσιεύματα έκαναν λόγο για παραβιάσεις του COREU, του δικτύου διπλωματικών επικοινωνιών της ΕΥΕΔ (πηγή: *«New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran»*, 18 Δεκεμβρίου 2018). Το ζήτημα επί του παρόντος διερευνάται.

[162] Απαιτείται περαιτέρω ανάπτυξη της συνεργασίας σχετικά με τις έγκαιρες προειδοποιήσεις και την αμοιβαία συνδρομή: *Συμπεράσματα του Συμβουλίου για τη συντονισμένη ενωσιακή αντιμετώπιση συμβάντων και κρίσεων ασφάλειας μεγάλης κλίμακας στον κυβερνοχώρο*, 10085/18 της 26ης Ιουνίου 2018.

[163] Υπηρεσία Έρευνας του Ευρωπαϊκού Κοινοβουλίου, *«Briefing EU Legislation in Progress: ENISA and a new cybersecurity act»*, PE 614.643, Σεπτέμβριος 2018.

[164] Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, όπ.π., Μάρτιος 2018.

[165] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks»*, 14893/18, Δεκέμβριος 2018.

[166] Ομάδες ταχείας αντίδρασης για τον κυβερνοχώρο και αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο· πλατφόρμα ανταλλαγής πληροφοριών για την αντιμετώπιση απειλών και συμβάντων στον κυβερνοχώρο. Πηγή: Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview»* της 19ης Νοεμβρίου 2018.

[167] Συμβούλιο της Ευρωπαϊκής Ένωσης, «Συμπεράσματα σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο», 9916/17 της 7ης Ιουνίου 2017.

[168] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Συμπεράσματα του Συμβουλίου για τη διπλωματία στον κυβερνοχώρο»*, 6122/55 της 11ης Φεβρουαρίου 2015.

[169] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities»*, 13007/17.

[170] Η απόδοση ευθυνών για ένα συμβάν εξακολουθεί να αποτελεί κυρίαρχη πολιτική απόφαση που λαμβάνεται από τα κράτη μέλη. Δεν προϋποθέτουν όλα τα μέτρα της εργαλειοθήκης απόδοση ευθυνών.

[171] Η χρησιμοποίηση της εργαλειοθήκης δεν είχε ως αποτέλεσμα κοινή δράση. Διάφορα κράτη μέλη υιοθέτησαν τη θέση των ΗΠΑ.

[172] Συμβούλιο της Ευρωπαϊκής Ένωσης, *«Συμπεράσματα σχετικά με τις κακόβουλες δραστηριότητες στον κυβερνοχώρο»*, 7925/18 της 16ης Απριλίου 2018.

[173] Συστήματα πληροφορικής που χρησιμοποιούνται για τον έλεγχο διεργασιών σε διάφορους κλάδους, όπως οι υπηρεσίες κοινής ωφελείας, η χημική και μεταποιητική βιομηχανία, η επεξεργασία τροφίμων, τα συστήματα και οι κόμβοι μεταφορών, και οι υπηρεσίες υλικοτεχνικής υποστήριξης.

[174] ENISA, όπ.π., Δεκέμβριος 2017.

[175] Παραδείγματος χάριν, η δημόσια διοίκηση, η χημική και πυρηνική βιομηχανία και οι τομείς της μεταποίησης, της μεταποίησης τροφίμων, του τουρισμού, της εφοδιαστικής και της πολιτικής προστασίας.

[176] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2017) 295 final της 13ης Σεπτεμβρίου 2017.

[177] Ομιλία της Επιτρόπου Jourová κατά τη σύνοδο ολομέλειας του Ευρωπαϊκού Κοινοβουλίου *«Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign»*, της 14ης Νοεμβρίου 2018.

[178] Ίδρυμα Carnegie για τη Διεθνή Ειρήνη, *«Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks»*, 23 Μαΐου 2018.

[179] Ευρωπαϊκό Κέντρο Πολιτικής Στρατηγικής (L. Past), «Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses», στη δημοσίευση με τίτλο: «Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts», 2018.

[180] Σύμφωνα με την οδηγία 2008/114/ΕΚ του Συμβουλίου σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους.

[181] Σύσταση της Ευρωπαϊκής Επιτροπής σχετικά με τα δίκτυα εκλογικής συνεργασίας, τη διαφάνεια στο διαδίκτυο και την προστασία από επιθέσεις στον κυβερνοχώρο και την καταπολέμηση των εκστρατειών παραπληροφόρησης στο πλαίσιο της εκλογικής διαδικασίας για το Ευρωπαϊκό Κοινοβούλιο, C(2018) 5949 final της 12ης Σεπτεμβρίου 2018.

[182] Συμπεράσματα του Ευρωπαϊκού Συμβουλίου , EUCO 11/15 της 20ής Μαρτίου 2015. Έκτοτε έχουν προστεθεί δύο ακόμη ειδικές ομάδες, για τα Δυτικά Βαλκάνια και τη Νότια Γειτονία.

[183] Μια έκθεση του Συμβουλίου του Ατλαντικού καλούσε την ΕΕ να ζητήσει από όλα τα κράτη μέλη να αποστείλουν εθνικούς εμπειρογνώμονες στην ειδική ομάδα. Βλέπε: D. Fried και A. Polyakova, *«Democratic Defense Against Disinformation»*, 5 Μαρτίου 2018.

[184] Αρχικά δεν διέθετε δικό της προϋπολογισμό. Ωστόσο, το 2018 έλαβε 1,1 εκατομμύρια ευρώ από το Ευρωπαϊκό Κοινοβούλιο για μια προπαρασκευαστική ενέργεια «StratCom Plus».

[185] Ίδρυμα Carnegie για τη Διεθνή Ειρήνη (E. Brattberg, T. Maurer), όπ.π., 23 Μαΐου 2018.

[186] Ευρωπαϊκή Επιτροπή, Ύπατη Εκπρόσωπος της Ένωσης για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας, *«Σχέδιο δράσης κατά της παραπληροφόρησης»*, JOIN(2018) 36 final. Το σχέδιο εστιάζει στα εξής: στη βελτίωση των ικανοτήτων των θεσμικών οργάνων της ΕΕ όσον αφορά τον εντοπισμό, την ανάλυση και την αποκάλυψη υλικού παραπληροφόρησης· στην ενίσχυση των συντονισμένων και κοινών αντιδράσεων στην παραπληροφόρηση· στην κινητοποίηση του ιδιωτικού τομέα· και στην αύξηση της ευαισθητοποίησης και τη βελτίωση της ανθεκτικότητας της κοινωνίας.

[187] Ευρωπαϊκή Επιτροπή, *«Αντιμετώπιση της παραπληροφόρησης στο διαδίκτυο: μια ευρωπαϊκή προσέγγιση»*, COM(2018) 236 final της 26ης Απριλίου 2018.

[188] Δεν πρέπει να συγχέεται με τον κώδικα δεοντολογίας για την καταπολέμηση της παράνομης ρητορικής μίσους στο διαδίκτυο.

[189] JRC, *«The digital transformation of news media and the rise of disinformation and fake news*, Τεχνικές εκθέσεις του Κοινού Κέντρου Ερευνών, έγγραφο εργασίας σχετικά με την ψηφιακή οικονομία 2018-02, Απρίλιος 2018.

[190] ENISA, *«Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")»,* Απρίλιος 2018

[191] Ευρωπαϊκό Κέντρο Πολιτικής Στρατηγικής (C. Frutos López), *«A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats»*, όπ.π., 2018.

[192] Ευρωπαϊκή Επιτροπή, όπ.π., SWD (2018) 403 final της 12ης Σεπτεμβρίου 2018.

[193] Η πρόταση κανονισμού (COM(2017) 487 final της 13ης Σεπτεμβρίου 2017) για τον έλεγχο των ΑΞΕ, που υποβλήθηκε τον Σεπτέμβριο του 2017, εξετάζεται επί του παρόντος στο πλαίσιο της νομοθετικής διαδικασίας. Ειδικότερα, καλύπτει τις τεχνολογίες καίριας σημασίας, συμπεριλαμβανομένης της τεχνητής νοημοσύνης, την κυβερνοασφάλεια και τις εφαρμογές διπλής χρήσης.

[194] Ευρωπαϊκή Επιτροπή/Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης, όπ.π.,JOIN(2017) 450 της 13ης Σεπτεμβρίου 2017.

Κλιμάκιο του ΕΕΣ

Το παρόν ενημερωτικό έγγραφο, με τίτλο *«Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια»*, εγκρίθηκε από το Τμήμα Ελέγχου III, το οποίο είναι αρμόδιο για τον έλεγχο των δαπανών που αφορούν τις εξωτερικές δράσεις, την ασφάλεια και τη δικαιοσύνη και του οποίου προεδρεύει η Bettina Jakobsen, Μέλος του ΕΕΣ. Επικεφαλής του συγκεκριμένου έργου ήταν ο Baudilio Tomé Muguruza, Μέλος του ΕΕΣ, συνεπικουρούμενος από τον Daniel Costa de Magalhaes, προϊστάμενο του ιδιαίτερου γραφείου του και τον Ignacio Garcia de Parada, σύμβουλο στο ιδιαίτερο γραφείο του, τον Alejandro Ballester-Gallardo, ανώτερο διοικητικό στέλεχος, τον Michiel Sweerts, υπεύθυνο έργου, τους Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, ελεγκτές και τον Johannes Bolkart, ασκούμενο. Η Hannah Critoph παρείχε γλωσσική υποστήριξη.

Από αριστερά: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ

Υπηρεσία Εκδόσεων

ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
12, rue Alcide De Gasperi
1615 Luxembourg
ΛΟΥΞΕΜΒΟΥΡΓΟ

Τηλ. +352 4398-1

Πληροφορίες: eca.europa.eu/el/Pages/ContactForm.aspx
Ιστότοπος: eca.europa.eu
Twitter: @EUAuditors