Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 16 Δεκεμβρίου 2020
(OR. en)

14133/20

Διοργανικός φάκελος:
2020/0305(NLE)

CYBER 280	RECH 529
JAI 1118	COMPET 642
JAIEX 121	IND 273
EJUSTICE 107	COTER 115
COSI 254	ENFOPOL 350
DATAPROTECT 154	COPS 485
COPEN 387	MI 578
TELECOM 269	IXIM 139
PROCIV 99	POLMIL 201
CSC 367	HYBRID 48
CIS 65	CSCI 96
RELEX 1019	POLGEN 234

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	16 Δεκεμβρίου 2020
Αποδέκτης:	κ. Jeppe TRANHOLM-MIKKELSEN, Γενικός Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	JOIN(2020) 18 final
Θέμα:	ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - JOIN(2020) 18 final.

συνημμ.: JOIN(2020) 18 final

ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ

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

Βρυξέλλες, 16.12.2020
JOIN(2020) 18 final

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ

Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ

Η στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία

I. ΕΙΣΑΓΩΓΗ: ΚΥΒΕΡΝΟΑΣΦΑΛΗΣ ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ ΣΕ ΕΝΑ ΣΥΝΘΕΤΟ ΠΕΡΙΒΑΛΛΟΝ ΑΠΕΙΛΩΝ

Η κυβερνοασφάλεια αποτελεί αναπόσπαστο μέρος της ασφάλειας των Ευρωπαίων. Είτε χρησιμοποιούν συνδεδεμένες συσκευές ή δίκτυα ηλεκτρικής ενέργειας, είτε εξυπηρετούνται από τράπεζες, αεροσκάφη, δημόσιες διοικήσεις ή νοσοκομεία, οι πολίτες πρέπει να έχουν την εγγύηση ότι προστατεύονται από κυβερνοαπειλές. Η οικονομία, η δημοκρατία και η κοινωνία της ΕΕ εξαρτώνται περισσότερο από ποτέ από την ασφάλεια και την αξιοπιστία των ψηφιακών εργαλείων και της συνδεσιμότητας. Ως εκ τούτου, η κυβερνοασφάλεια είναι θεμελιώδης για την οικοδόμηση μιας ανθεκτικής, πράσινης και ψηφιακής Ευρώπης.

Οι μεταφορές, η ενέργεια και η υγεία, οι τηλεπικοινωνίες, ο χρηματοοικονομικός τομέας, η ασφάλεια, οι δημοκρατικές διαδικασίες, ο τομέας του διαστήματος και της άμυνας εξαρτώνται σε μεγάλο βαθμό από συστήματα δικτύων και πληροφοριών που είναι όλο και περισσότερο διασυνδεδεμένα. Οι διατομεακές αλληλεξαρτήσεις είναι πολύ ισχυρές, διότι τα δίκτυα και τα συστήματα πληροφοριών, με τη σειρά τους, εξαρτώνται για τη λειτουργία τους, από τη σταθερή παροχή ηλεκτρικής ενέργειας. Οι συνδεδεμένες συσκευές είναι ήδη περισσότερες από τους κατοίκους του πλανήτη μας και ο αριθμός τους προβλέπεται να αυξηθεί στα 25 δισεκατομμύρια έως το 2025[1]: το ένα τέταρτο από αυτές θα βρίσκεται στην Ευρώπη. Η ψηφιοποίηση του τρόπου εργασίας επιταχύνθηκε από την πανδημία COVID-19, κατά τη διάρκεια της οποίας το 40 % των εργαζομένων της ΕΕ μεταστράφηκε στην τηλεργασία, γεγονός που θα έχει πιθανώς μόνιμες επιπτώσεις στην καθημερινή ζωή[2]. Το φαινόμενο αυτό αυξάνει τα σημεία που είναι τρωτά σε κυβερνοεπιθέσεις[3]. Τα συνδεδεμένα αντικείμενα συχνά αποστέλλονται στους καταναλωτές με γνωστά τρωτά σημεία, γεγονός που αυξάνει περαιτέρω την επιφάνεια έκθεσης σε κακόβουλες κυβερνοδραστηριότητες[4]. Το βιομηχανικό τοπίο της ΕΕ ψηφιοποιείται και συνδέεται όλο και περισσότερο· αυτό συνεπάγεται επίσης ότι οι κυβερνοεπιθέσεις μπορούν

[1] Εκτίμηση της εμπορικής ένωσης τηλεπικοινωνιών GSMA· https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). Η International Data Corporation προβλέπει 42,6 δισεκατομμύρια συνδεδεμένες μηχανές, αισθητήρες και κάμερες· https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Σύμφωνα με έρευνα που δημοσιεύτηκε τον Ιούνιο του 2020, το 47 % των επικεφαλής επιχειρήσεων δήλωσαν ότι σκόπευαν να επιτρέπουν στους εργαζόμενους να τηλεργάζονται με πλήρες ωράριο ακόμα κι αν καταστεί δυνατή η επιστροφή στον χώρο εργασίας· το 82 % σκόπευε να επιτρέψει την εξ αποστάσεως εργασία, τουλάχιστον εν μέρει· https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Ενα από τα πιο επιβλαβή κακόβουλα λογισμικά, το Mirai, δημιούργησε δίκτυο προγραμμάτων ρομπότ (μπότνετ) με περισσότερες από 600 000 συσκευές που προκάλεσαν μεγάλα προβλήματα στη λειτουργία πολλών σημαντικών ιστότοπων στην Ευρώπη και στις Ηνωμένες Πολιτείες.

να έχουν πολύ μεγαλύτερο αντίκτυπο στις βιομηχανίες και στα οικοσυστήματα απ' ό,τι στο παρελθόν.

Το τοπίο των απειλών επιδεινώνεται από τις γεωπολιτικές εντάσεις σχετικά με το παγκόσμιο και ανοικτό διαδίκτυο και τον έλεγχο των τεχνολογιών σε ολόκληρη την αλυσίδα εφοδιασμού[5]. Οι εντάσεις αυτές αντικατοπτρίζονται στον αυξανόμενο αριθμό κρατών που εγείρουν ψηφιακά σύνορα. Οι περιορισμοί του διαδικτύου και στο διαδίκτυο απειλούν τον παγκόσμιο και ανοικτό κυβερνοχώρο, καθώς και το κράτος δικαίου, τα θεμελιώδη δικαιώματα, την ελευθερία και τη δημοκρατία, δηλαδή τις βασικές αξίες της ΕΕ. Ο κυβερνοχώρος αξιοποιείται ολοένα και περισσότερο για πολιτικούς και ιδεολογικούς σκοπούς, ενώ η εντεινόμενη πόλωση σε διεθνές επίπεδο παρεμποδίζει την πραγματική πολυμέρεια. Οι υβριδικές απειλές συνδυάζουν εκστρατείες παραπληροφόρησης με κυβερνοεπιθέσεις σε υποδομές, οικονομικές διαδικασίες και δημοκρατικούς θεσμούς, και μπορούν να προκαλέσουν υλικές βλάβες, να επιτρέψουν την παράνομη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, να οδηγήσουν σε κλοπή βιομηχανικών ή κρατικών μυστικών, να σπείρουν τη δυσπιστία και να αποδυναμώσουν την κοινωνική συνοχή. Οι δραστηριότητες αυτές υπονομεύουν τη διεθνή ασφάλεια και σταθερότητα και τα οφέλη του κυβερνοχώρου για την οικονομική, κοινωνική και πολιτική ανάπτυξη.

Η κακόβουλη στόχευση κρίσιμων υποδομών αποτελεί μείζονα παγκόσμιο κίνδυνο[6]. Το διαδίκτυο έχει αποκεντρωμένη αρχιτεκτονική, χωρίς κεντρική δομή, και πολυσυμμετοχική διακυβέρνηση. Κατάφερε να στηρίξει τις εκθετικές αυξήσεις του όγκου της κυκλοφορίας, ενώ αποτελεί σταθερό στόχο κακόβουλων προσπαθειών διατάραξης[7]. Ταυτόχρονα, αυξάνεται η εξάρτηση από τις βασικές λειτουργίες του παγκόσμιου και ανοικτού διαδικτύου, όπως το σύστημα ονομάτων τομέα (DNS), και από βασικές υπηρεσίες διαδικτύου για τις επικοινωνίες και τη φιλοξενία, τις εφαρμογές και τα δεδομένα. Οι υπηρεσίες αυτές συγκεντρώνονται όλο και περισσότερο στα χέρια μερικών ιδιωτικών επιχειρήσεων[8]. Αυτό καθιστά την ευρωπαϊκή οικονομία και κοινωνία ευάλωτη σε ανατρεπτικά γεωπολιτικά ή τεχνικά συμβάντα που επηρεάζουν τον πυρήνα του διαδικτύου ή μία ή περισσότερες από αυτές τις επιχειρήσεις. Η αυξημένη χρήση του διαδικτύου και οι αλλαγές στον τρόπο

[5] Συμπεριλαμβανομένων των ηλεκτρονικών εξαρτημάτων, της ανάλυσης δεδομένων, του υπολογιστικού νέφους, των ταχύτερων και εξυπνότερων δικτύων με το 5G και τις μελλοντικές τεχνολογίες, της κρυπτογράφησης, της τεχνητής νοημοσύνης (ΤΝ) και νέων υποδειγμάτων υπολογιστικής και αξιόπιστης επεξεργασίας δεδομένων, όπως η τεχνολογία blockchain, η υπολογιστική νέφους προς παρυφή (cloud-to-edge) και η κβαντική υπολογιστική.

[6] Παγκόσμιο Οικονομικό Φόρουμ, Global Risks Report 2020.

[7] Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης, η πανδημία οδήγησε σε αύξηση της κίνησης στο διαδίκτυο κατά 60 %· https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Ο Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες και η Επιτροπή δημοσιεύουν τακτικά εκθέσεις σχετικά με την κατάσταση της χωρητικότητας του διαδικτύου κατά τη διάρκεια των μέτρων περιορισμού της κυκλοφορίας λόγω του κορονοϊού. Σύμφωνα με έκθεση του ENISA, κατά το τρίτο τρίμηνο του 2019 σημειώθηκε αύξηση κατά 241 % του συνολικού αριθμού των κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) σε σύγκριση με το τρίτο τρίμηνο του 2018. Οι επιθέσεις DDoS αυξάνονται σε ένταση, και η μεγαλύτερη επίθεση που σημειώθηκε ποτέ πραγματοποιήθηκε τον Φεβρουάριο του 2020 και έφτασε σε κορύφωση κυκλοφορίας 2,3 terabit ανά δευτερόλεπτο. Στη διακοπή λειτουργίας του «CenturyLink» τον Αύγουστο του 2020, ένα πρόβλημα δρομολόγησης στον πάροχο υπηρεσιών διαδικτύου των ΗΠΑ οδήγησε σε μείωση της παγκόσμιας διαδικτυακής κίνησης κατά 3,5 %· https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy· https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

εργασίας λόγω της πανδημίας έχουν αποκαλύψει περαιτέρω την ευπάθεια των αλυσίδων εφοδιασμού που εξαρτώνται από αυτή την ψηφιακή υποδομή.

Οι ανησυχίες για την ασφάλεια αποτελούν σημαντικό αντικίνητρο για τη χρήση επιγραμμικών υπηρεσιών[9]. Περίπου τα δύο πέμπτα των χρηστών στην ΕΕ έχουν αντιμετωπίσει προβλήματα που σχετίζονται με την ασφάλεια και τα τρία πέμπτα νιώθουν ότι δεν είναι σε θέση να προστατευθούν από το κυβερνοέγκλημα[10]. Τα τελευταία τρία χρόνια, το ένα τρίτο έλαβε δόλια μηνύματα ηλεκτρονικού ταχυδρομείου ή δέχθηκε δόλιες τηλεφωνικές κλήσεις που προσπαθούσαν να εκμαιεύσουν προσωπικά στοιχεία, αλλά το 83 % δεν έκανε ποτέ καταγγελία για κυβερνοέγκλημα. Μία στις οκτώ επιχειρήσεις έχει πληγεί από κυβερνοεπιθέσεις[11]. Περισσότεροι από τους μισούς προσωπικούς υπολογιστές επιχειρήσεων και καταναλωτών που μολύνθηκαν μία φορά από κακόβουλο λογισμικό, μολύνονται εκ νέου εντός του ίδιου έτους[12]. Εκατοντάδες εκατομμύρια αρχεία χάνονται κάθε χρόνο λόγω παραβιάσεων δεδομένων· το μέσο κόστος ανά παραβίαση για μία μόνο επιχείρηση ξεπέρασε τα 3,5 εκατ. EUR το 2018[13]. Ο αντίκτυπος μιας κυβερνοεπίθεσης συχνά δεν μπορεί να απομονωθεί και μπορεί να προκαλέσει αλυσιδωτές αντιδράσεις σε ολόκληρη την οικονομία και την κοινωνία, επηρεάζοντας εκατομμύρια ανθρώπους[14].

Οι έρευνες σχεδόν όλων των μορφών εγκληματικότητας έχει μια ψηφιακή συνιστώσα. Το 2019 ο αριθμός των περιστατικών που αναφέρθηκαν τριπλασιάστηκε σε σχέση με το προηγούμενο έτος. Εκτιμάται ότι υπάρχουν 700 εκατομμύρια νέα δείγματα κακόβουλου λογισμικού – το συχνότερο μέσο για την εκδήλωση κυβερνοεπίθεσης[15]. Το 2020 το ετήσιο κόστος του κυβερνοεγκλήματος για την παγκόσμια οικονομία εκτιμάται σε 5,5 τρισεκατομμύρια ευρώ, ποσό διπλάσιο από εκείνο του 2015[16]. Πρόκειται για τη μεγαλύτερη μεταβίβαση οικονομικού πλούτου στην ιστορία, μεγαλύτερη από το παγκόσμιο εμπόριο ναρκωτικών. Για ένα σοβαρό περιστατικό, όπως η επίθεση με το λυτρισμικό WannaCry το 2017, το κόστος για την παγκόσμια οικονομία εκτιμάται ότι ξεπέρασε τα 6,5 δισ. EUR[17].

Οι ψηφιακές υπηρεσίας και ο τομέας των χρηματοπιστωτικών υπηρεσιών είναι μεταξύ των συνηθέστερων στόχων κυβερνοεπιθέσεων, μαζί με τον δημόσιο τομέα και τη μεταποίηση. Ωστόσο η κυβερνοετοιμότητα και η κυβερνοευαισθητοποίηση των

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[10] Δείκτης Ψηφιακής Οικονομίας και Κοινωνίας 2020· https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Δελτίο Τύπου της Eurostat, «Μέτρα ασφάλειας ΤΠΕ που λαμβάνονται από τη συντριπτική πλειονότητα των επιχειρήσεων στην ΕΕ», 6/2020-13 Ιανουαρίου 2020. «Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation» (Οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές έχουν καταστεί η νέα κανονικότητα σε διάφορους τομείς όπως η ενέργεια, η υγειονομική περίθαλψη και οι μεταφορές)· WEF, The Global Risks Report 2020.

[12] Πηγή: Comparitech.

[13] «Annual Cost of a Data Breach Report», 2020 Ponemon Institute, με βάση την ποσοτική ανάλυση 524 πρόσφατων παραβιάσεων σε 17 γεωγραφικές περιοχές και 17 κλάδους· https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Έκθεση του Κοινού Κέντρου Ερευνών (ΚΚΕ) με τίτλο «Cybersecurity, our digital anchor» (Κυβερνοασφάλεια, ψηφιακή μας άγκυρα)· https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Πηγή: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Πηγή: Cyence.

επιχειρήσεων και των ιδιωτών παραμένουν σε χαμηλά επίπεδα[18] και, μεταξύ των εργαζομένων, υπάρχει σοβαρή έλλειψη δεξιοτήτων κυβερνοασφάλειας[19]. Το 2019 σημειώθηκαν σχεδόν 450 περιστατικά κυβερνοασφάλειας που αφορούσαν ευρωπαϊκές υποδομές ζωτικής σημασίας, όπως ο χρηματοπιστωτικός τομέας και η ενέργεια[20]. Οι οργανισμοί και οι επαγγελματίες του κλάδου της υγειονομικής περίθαλψης έχουν πληγεί ιδιαίτερα σοβαρά κατά τη διάρκεια της πανδημίας. Καθώς η τεχνολογία καθίσταται άρρηκτα συνδεδεμένη με τον πραγματικό κόσμο, οι κυβερνοεπιθέσεις θέτουν σε κίνδυνο τη ζωή και την ευημερία των πλέον ευάλωτων[21]. Πάνω από τα δύο τρίτα των επιχειρήσεων, ιδίως οι ΜΜΕ, θεωρούνται «αρχάριες» στον τομέα της κυβερνοασφάλειας, και οι ευρωπαϊκές επιχειρήσεις θεωρούνται λιγότερο καλά προετοιμασμένες από τις επιχειρήσεις στην Ασία και την Αμερική[22]. Εκτιμάται ότι, στην Ευρώπη, 291 000 θέσεις εργασίας επαγγελματιών κυβερνοασφάλειας παραμένουν κενές. Η πρόσληψη και η κατάρτιση ειδικών κυβερνοασφάλειας είναι μια αργή διαδικασία, που συνεπάγεται μεγαλύτερους κινδύνους κυβερνοασφάλειας για τους οργανισμούς[23].

Η ΕΕ δεν διαθέτει συλλογική επίγνωση της κατάστασης όσον αφορά τις κυβερνοαπειλές. Αυτό οφείλεται στο γεγονός ότι οι εθνικές αρχές δεν συλλέγουν και δεν ανταλλάσσουν συστηματικά πληροφορίες —όπως αυτές που διατίθενται από τον ιδιωτικό τομέα— οι οποίες θα μπορούσαν να συμβάλουν στην αξιολόγηση της κατάστασης κυβερνοασφάλειας στην ΕΕ. Τα κράτη μέλη αναφέρουν μόνο ένα μικρό ποσοστό των περιστατικών και η ανταλλαγή πληροφοριών δεν είναι ούτε συστηματική ούτε ολοκληρωμένη[24]· οι κυβερνοεπιθέσεις μπορεί να αποτελούν μία μόνο πτυχή συντονισμένων κακόβουλων επιθέσεων κατά των ευρωπαϊκών κοινωνιών. Επί του παρόντος, η αμοιβαία επιχειρησιακή συνδρομή μεταξύ των κρατών μελών είναι περιορισμένη και δεν υπάρχει επιχειρησιακός μηχανισμός μεταξύ των κρατών μελών και των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ, σε περίπτωση μεγάλης κλίμακας διασυνοριακών κυβερνοπεριστατικών ή κρίσης στον κυβερνοχώρο[25].

Ως εκ τούτου, η βελτίωση της κυβερνοασφάλειας είναι απαραίτητη προκειμένου οι πολίτες να εμπιστεύονται, να χρησιμοποιούν και να ωφελούνται από την καινοτομία, τη συνδεσιμότητα και την αυτοματοποίηση, καθώς και για να διασφαλίζονται τα θεμελιώδη δικαιώματα και ελευθερίες, συμπεριλαμβανομένων των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και η

---

[18] Η ευαισθητοποίηση των επιχειρήσεων παραμένει χαμηλή, ιδίως μεταξύ των ΜΜΕ, και όσον αφορά την κυβερνοκλοπή εμπορικών μυστικών· PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

[19] Βλ. ENISA Threat Landscape 2020. Βλ. επίσης, Verizon Data Breach Investigations Report 2020· https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Λυτρισμικό χρησιμοποιήθηκε για την επίθεση σε νοσοκομεία και μητρώα υγείας, π.χ. Ρουμανία (Ιούνιος 2020), Ντίσελντορφ (Σεπτέμβριος 2020) και Vastaamo (Οκτώβριος 2020).

[22] PwC, «The Global State of Information Security» 2018· ESI Thoughtlab, «The Cybersecurity Imperative», 2019.

[23] Οργανισμός της ΕΕ για την κυβερνοασφάλεια, «Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database», Δεκέμβριος 2019.

[24] Τα κράτη μέλη οφείλουν να υποβάλλουν ετήσια συνοπτική έκθεση στην ομάδα συνεργασίας σχετικά με τις κοινοποιήσεις που λαμβάνουν σύμφωνα με το άρθρο 10 παράγραφος 3 της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (οδηγία (ΕΕ) 2016/1148).

[25] Εφαρμόζονται τυποποιημένες επιχειρησιακές διαδικασίες για την αμοιβαία συνδρομή μεταξύ των μελών του δικτύου CSIRT.

ελευθερία έκφρασης και πληροφόρησης. Η κυβερνοασφάλεια είναι απαραίτητη για τη συνδεσιμότητα του δικτύου και για το παγκόσμιο και ανοικτό διαδίκτυο που πρέπει να στηρίξουν τον μετασχηματισμό της οικονομίας και της κοινωνίας κατά τη δεκαετία του 2020. Συμβάλλει σε καλύτερες και περισσότερες θέσεις εργασίας, πιο ευέλικτους χώρους εργασίας, πιο αποδοτικές και βιώσιμες μεταφορές και γεωργία, καθώς και σε ευκολότερη και δικαιότερη πρόσβαση σε υπηρεσίες υγείας. Σύμφωνα με την Ευρωπαϊκή Πράσινη Συμφωνία[26], είναι επίσης σημαντική για τη μετάβαση σε καθαρότερη ενέργεια, μέσω διασυνοριακών δικτύων και έξυπνων μετρητών και για την αποφυγή περιττών επικαλύψεων όσον αφορά την αποθήκευση δεδομένων. Τέλος, είναι θεμελιώδης για τη διεθνή ασφάλεια και σταθερότητα, καθώς και για την ανάπτυξη των οικονομιών, των δημοκρατιών και των κοινωνιών σε παγκόσμιο επίπεδο. Ως εκ τούτου, οι κυβερνήσεις, οι επιχειρήσεις και τα άτομα πρέπει να χρησιμοποιούν τα ψηφιακά εργαλεία με υπεύθυνο τρόπο, και έχοντας επίγνωση των πτυχών που σχετίζονται με την ασφάλεια. Η ευαισθητοποίηση ως προς την κυβερνοασφάλεια και η κυβερνοϋγιεινή πρέπει να διέπουν τον ψηφιακό μετασχηματισμό των καθημερινών δραστηριοτήτων.

Η νέα στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία αποτελεί βασική συνιστώσα του εγγράφου με τίτλο «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης»[27], του σχεδίου ανάκαμψης για την Ευρώπη, που έχει εκπονήσει η Επιτροπή[28], της στρατηγικής για την Ένωση Ασφάλειας 2020-2025[29], της συνολικής στρατηγικής της ΕΕ για την εξωτερική πολιτική και την πολιτική ασφαλείας[30], και του στρατηγικού θεματολογίου του Ευρωπαϊκού Συμβουλίου 2019-2024[31]. Η στρατηγική καθορίζει τον τρόπο με τον οποίο η ΕΕ θα προστατεύει τους πολίτες, τις επιχειρήσεις και τα θεσμικά της όργανα από κυβερνοαπειλές, καθώς και τον τρόπο με τον οποίο θα προωθήσει τη διεθνή συνεργασία και θα ηγηθεί της διασφάλισης ενός ανοικτού και παγκόσμιου διαδικτύου.

II. ΣΚΕΨΟΥ ΟΙΚΟΥΜΕΝΙΚΑ, ΔΡΑΣΕ ΕΥΡΩΠΑΪΚΑ

Η παρούσα στρατηγική αποσκοπεί στο να διασφαλίσει ένα παγκόσμιο και ανοικτό διαδίκτυο με ισχυρές δικλίδες ασφαλείας, ώστε να αντιμετωπίζονται οι κίνδυνοι για την ασφάλεια και τα θεμελιώδη δικαιώματα και τις ελευθερίες των πολιτών στην Ευρώπη. Μετά την πρόοδο που σημειώθηκε στο πλαίσιο των προηγούμενων στρατηγικών, η στρατηγική περιλαμβάνει συγκεκριμένες προτάσεις για την ανάπτυξη **τριών κύριων μέσων —ρυθμιστικών, επενδυτικών και μέσων πολιτικής**— για **τρεις τομείς δράσης της ΕΕ: 1) ανθεκτικότητα, τεχνολογική κυριαρχία και ηγετικός ρόλος, 2) ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντίδρασης, και 3) προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου.** Η ΕΕ έχει δεσμευτεί να στηρίξει τη στρατηγική αυτή με **ένα άνευ προηγουμένου επίπεδο επενδύσεων στην ψηφιακή μετάβαση της ΕΕ κατά την επόμενη επταετία**– με δυνάμει τετραπλασιασμό των προηγούμενων επιπέδων – στο πλαίσιο των νέων τεχνολογικών και βιομηχανικών πολιτικών και του θεματολογίου ανάκαμψης[32].

---

[26] Η Ευρωπαϊκή Πράσινη Συμφωνία, COM(2019) 640 final.
[27] Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, COM(2020) 67 final.
[28] Η ώρα της Ευρώπης: Ανασύνταξη και προετοιμασία για την επόμενη γενιά , COM (2020) 98 final.
[29]Στρατηγική της ΕΕ για την Ένωση Ασφάλειας 2020-2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#
[32] Οι επενδύσεις σε ολόκληρη την αλυσίδα εφοδιασμού ψηφιακής τεχνολογίας, οι οποίες συμβάλλουν στην ψηφιακή μετάβαση ή στην αντιμετώπιση των προκλήσεων που απορρέουν από αυτήν, θα πρέπει να ανέρχονται σε τουλάχιστον 20 % –δηλ. 134,5 δισ. EUR– του Μηχανισμού Ανάκαμψης και Ανθεκτικότητας ύψους 672,5 δισ. EUR, αποτελούμενες από επιχορηγήσεις και δάνεια. Στο πολυετές δημοσιονομικό πλαίσιο 2021-2027

Η κυβερνοασφάλεια πρέπει να ενσωματωθεί σε όλες αυτές τις ψηφιακές επενδύσεις, ιδίως σε βασικές τεχνολογίες όπως η τεχνητή νοημοσύνη (ΤΝ), η κρυπτογράφηση και η κβαντική υπολογιστική, με τη χρήση κινήτρων, υποχρεώσεων και δεικτών αναφοράς. Αυτό μπορεί να τονώσει την ανάπτυξη του ευρωπαϊκού κλάδου της κυβερνοασφάλειας και να παράσχει τη βεβαιότητα που απαιτείται για τη διευκόλυνση της σταδιακής κατάργησης των κληροδοτημένων συστημάτων. Το Ευρωπαϊκό Ταμείο Άμυνας (ΕΤΑ) θα στηρίξει ευρωπαϊκές λύσεις κυβερνοάμυνας, στο πλαίσιο της ευρωπαϊκής τεχνολογικής και βιομηχανικής βάσης στον τομέα της άμυνας. Η κυβερνοασφάλεια περιλαμβάνεται στα εξωτερικά χρηματοδοτικά μέσα για τη στήριξη των εταίρων μας, ιδίως στον Μηχανισμό Γειτονίας, Ανάπτυξης και Διεθνούς Συνεργασίας. Η πρόληψη της κατάχρησης τεχνολογιών, η προστασία υποδομών ζωτικής σημασίας και η διασφάλιση της ακεραιότητας των αλυσίδων εφοδιασμού επιτρέπουν επίσης τη συμμόρφωση της ΕΕ με τα πρότυπα, τους κανόνες και τις αρχές υπεύθυνης κρατικής συμπεριφοράς των Ηνωμένων Εθνών[33].

1. ΑΝΘΕΚΤΙΚΟΤΗΤΑ, ΤΕΧΝΟΛΟΓΙΚΗ ΚΥΡΙΑΡΧΙΑ ΚΑΙ ΗΓΕΤΙΚΗ ΘΕΣΗ

Οι κρίσιμες υποδομές και οι βασικές υπηρεσίες της ΕΕ είναι ολοένα και πιο αλληλεξαρτώμενες και ψηφιοποιημένες. Όλα τα συνδεόμενα με το διαδίκτυο πράγματα στην ΕΕ, είτε πρόκειται για αυτοματοποιημένα αυτοκίνητα, για βιομηχανικά συστήματα ελέγχου ή για οικιακές συσκευές, καθώς και το σύνολο των αλυσίδων εφοδιασμού που τα καθιστούν διαθέσιμα, πρέπει να είναι ασφαλή εκ σχεδιασμού, ανθεκτικά σε κυβερνοπεριστατικά και γρήγορα επιδιορθώσιμα όταν εντοπίζονται τρωτά σημεία. Αυτό έχει θεμελιώδη σημασία για να δοθεί στον ιδιωτικό και στον δημόσιο τομέα της ΕΕ η δυνατότητα επιλογής μεταξύ των πλέον ασφαλών υποδομών και υπηρεσιών. Η επόμενη δεκαετία είναι η ευκαιρία της ΕΕ να αποκτήσει ηγετική θέση στην ανάπτυξη ασφαλών τεχνολογιών σε ολόκληρη την αλυσίδα εφοδιασμού. Η διασφάλιση της ανθεκτικότητας και η ενίσχυση των βιομηχανικών και τεχνολογικών ικανοτήτων κυβερνοασφάλειας θα πρέπει να κινητοποιήσουν όλα τα αναγκαία κανονιστικά, επενδυτικά και πολιτικά μέσα. Η εκ σχεδιασμού κυβερνοασφάλεια των βιομηχανικών διαδικασιών, λειτουργιών και συσκευών μπορεί να μετριάσει τους κινδύνους, να μειώσει δυνητικά το κόστος για τις επιχειρήσεις, καθώς και για την ευρύτερη κοινωνία και, ως εκ τούτου, να αυξήσει την ανθεκτικότητα.

1.1 Ανθεκτικές υποδομές και υπηρεσίες ζωτικής σημασίας

Οι **κανόνες της ΕΕ για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (NIS)** βρίσκονται στο επίκεντρο της ενιαίας αγοράς κυβερνοασφάλειας. Η Επιτροπή προτείνει τη μεταρρύθμιση των κανόνων αυτών στο πλαίσιο μιας αναθεωρημένης οδηγίας NIS, ώστε να αυξηθεί το επίπεδο **κυβερνοανθεκτικότητας όλων των σχετικών τομέων, δημόσιων και ιδιωτικών, που επιτελούν σημαντική λειτουργία για την οικονομία και την κοινωνία[34].** Η επανεξέταση είναι αναγκαία για να μειωθούν οι ασυνέπειες εντός της εσωτερικής αγοράς μέσω της ευθυγράμμισης του πεδίου εφαρμογής, των απαιτήσεων ασφάλειας και αναφοράς περιστατικών, της εθνικής εποπτείας και επιβολής και των αρμοδιοτήτων των αρμόδιων αρχών.

προβλέπεται ενωσιακή χρηματοδότηση της κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» και της έρευνας στον τομέα της κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη», με ιδιαίτερη έμφαση στη στήριξη ΜΜΕ· η χρηματοδότηση αυτή θα μπορούσε να ανέλθει συνολικά σε 2 δισ. EUR συν τις επενδύσεις των κρατών μελών και του κλάδου.

[33] https://undocs.org/A/70/174

[34] [*να προστεθεί παραπομπή στην πρόταση NIS*]

Η αναθεώρηση της οδηγίας NIS θα αποτελέσει τη βάση για πιο συγκεκριμένους κανόνες, οι οποίοι είναι επίσης αναγκαίοι για τομείς στρατηγικής σημασίας, μεταξύ άλλων για τους τομείς της ενέργειας, των μεταφορών και της υγείας. Για να διασφαλιστεί συνεκτική προσέγγιση, όπως ανακοινώθηκε στο πλαίσιο της στρατηγικής για την Ένωση Ασφάλειας 2020-2025, η αναθεώρηση της οδηγίας προτείνεται μαζί με επανεξέταση της νομοθεσίας για την ανθεκτικότητα των υποδομών ζωτικής σημασίας[35]. Οι ενεργειακές τεχνολογίες που ενσωματώνουν ψηφιακές συνιστώσες και η ασφάλεια των σχετικών αλυσίδων εφοδιασμού είναι σημαντικές για να εξασφαλίσουν τη συνέχεια των βασικών υπηρεσιών και τον στρατηγικό έλεγχο των ενεργειακών υποδομών ζωτικής σημασίας. Ως εκ τούτου, η Επιτροπή θα προτείνει, έως τα τέλη του 2022, τη θέσπιση μέτρων, συμπεριλαμβανομένου ενός «κώδικα δικτύου» για τον καθορισμό κανόνων κυβερνοασφάλειας για τις διασυνοριακές ροές ηλεκτρικής ενέργειας. Όπως έχει προτείνει η Επιτροπή, ο χρηματοπιστωτικός τομέας πρέπει επίσης να ενισχύσει την ψηφιακή επιχειρησιακή ανθεκτικότητά του και να διασφαλίσει την ικανότητα να ανθίσταται σε παντοειδείς διαταραχές και απειλές που σχετίζονται με τις ΤΠΕ[36]. Στον τομέα των μεταφορών, η Επιτροπή πρόσθεσε στη νομοθεσία της ΕΕ για την ασφάλεια της αεροπορίας[37] διατάξεις σχετικές με την κυβερνοασφάλεια και θα συνεχίσει τις προσπάθειές της για την ενίσχυση της κυβερνοανθεκτικότητας όλων των τρόπων μεταφοράς. Η ενίσχυση της κυβερνοανθεκτικότητας **των δημοκρατικών διαδικασιών και θεσμών** αποτελεί βασική συνιστώσα του ευρωπαϊκού σχεδίου δράσης για τη δημοκρατία, για τη διασφάλιση και την προώθηση ελεύθερων εκλογών, του δημοκρατικού λόγου και της πολυφωνίας των μέσων ενημέρωσης[38]. Τέλος, για την ασφάλεια των υποδομών και των υπηρεσιών στο πλαίσιο του μελλοντικού διαστημικού προγράμματος, η Επιτροπή θα εξακολουθήσει να εμβαθύνει τη στρατηγική κυβερνοασφάλειας του Galileo για την επόμενη γενιά υπηρεσιών του Παγκόσμιου Δορυφορικού Συστήματος Πλοήγησης και άλλων νέων συνιστωσών του διαστημικού προγράμματος[39].

1.2 Οικοδόμηση μιας ευρωπαϊκής κυβερνοασπίδας

Με την εξάπλωση της συνδεσιμότητας και την αυξανόμενη εξειδίκευση των κυβερνοεπιθέσεων, τα κέντρα ανταλλαγής και ανάλυσης πληροφοριών, ή ISAC, επιτελούν πολύτιμο έργο, μεταξύ άλλων σε τομεακό επίπεδο, επιτρέποντας την ανταλλαγή πληροφοριών για κυβερνοαπειλές μεταξύ πολλαπλών ενδιαφερόμενων μερών[40]. Επιπλέον, τα δίκτυα και τα συστήματα πληροφορικής απαιτούν συνεχή παρακολούθηση και ανάλυση για να εντοπίζονται εισβολές και ανωμαλίες σε πραγματικό χρόνο. Ως εκ τούτου, πολλές ιδιωτικές επιχειρήσεις, δημόσιοι οργανισμοί και εθνικές αρχές έχουν συστήσει ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT) και κέντρα επιχειρήσεων ασφάλειας, ή «SOC».

---

[35][να προστεθεί παραπομπή σε *πρόταση* οδηγίας σχετικά με την ανθεκτικότητα οντοτήτων ζωτικής σημασίας]

[36] Πρόταση κανονισμού για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014, COM/2020/595 final.

[37] Εκτελεστικός κανονισμός 2019/1583 της Επιτροπής.

[38] Ανακοίνωση σχετικά με το ευρωπαϊκό σχέδιο δράσης για τη δημοκρατία COM(2020) 790. Βάσει του σχεδίου, του Ευρωπαϊκού Δικτύου Συνεργασίας για τις Εκλογές, τα εκλογικά δίκτυα των κρατών μελών θα στηρίξουν την ανάπτυξη κοινών ομάδων ειδικών για την αντιμετώπιση απειλών —συμπεριλαμβανομένων κυβερνοαπειλών— εναντίον των εκλογικών διαδικασιών· https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

[39] Αυτό περιλαμβάνει νέα κυβερνητική πρωτοβουλία δορυφορικών επικοινωνιών (GOVSATCOM) και διαστημικών αποβλήτων (SST)

[40]https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Τα κέντρα επιχειρήσεων ασφάλειας έχουν ζωτική σημασία για τη συλλογή αρχείων καταγραφής[41] και την απομόνωση ύποπτων συμβάντων στα δίκτυα επικοινωνιών που παρακολουθούν. Αυτό επιτυγχάνεται μέσω της ταυτοποίησης σημάτων και μοτίβων και της εξαγωγής γνώσεων σχετικών με απειλές από τις μεγάλες ποσότητες δεδομένων που πρέπει να αξιολογηθούν. Τα επιχειρησιακά κέντρα ασφάλειας έχουν συμβάλει στον εντοπισμό των δραστηριοτήτων κακόβουλων εκτελέσιμων αρχείων και, με τον τρόπο αυτόν, έχουν συμβάλει στην ανάσχεση των κυβερνοεπιθέσεων. Οι εργασίες που απαιτείται να πραγματοποιούν τα κέντρα αυτά είναι εξαιρετικά απαιτητικές και ταχύρρυθμες και, γι' αυτόν τον λόγο, η τεχνητή νοημοσύνη και ιδίως οι τεχνικές μηχανομάθησης μπορούν να παράσχουν πολύτιμη στήριξη στους επαγγελματίες του τομέα[42].

Η Επιτροπή προτείνει να δημιουργηθεί **δίκτυο κέντρων επιχειρήσεων ασφάλειας σε ολόκληρη την ΕΕ[43]** και να στηριχθεί η βελτίωση των υφιστάμενων κέντρων, καθώς και η ίδρυση νέων. Θα στηρίξει επίσης την κατάρτιση και την ανάπτυξη δεξιοτήτων του προσωπικού που διαχειρίζεται τα κέντρα αυτά. Θα μπορούσε να δεσμεύσει, βάσει ανάλυσης αναγκών που θα διεξαχθεί με τους σχετικούς ενδιαφερόμενους φορείς και με την υποστήριξη του οργανισμού της ΕΕ για την κυβερνοασφάλεια (ENISA), περισσότερα από 300 εκατ. ευρώ για τη στήριξη της συνεργασίας δημόσιου-ιδιωτικού τομέα και της διασυνοριακής συνεργασίας για τη δημιουργία εθνικών και τομεακών δικτύων, με τη συμμετοχή και των ΜΜΕ, με βάση κατάλληλη διακυβέρνηση, ανταλλαγή δεδομένων και διατάξεις ασφάλειας.

Τα κράτη μέλη ενθαρρύνονται να συνεπενδύσουν σε αυτό το έργο. Στη συνέχεια, τα κέντρα θα είναι σε θέση να ανταλλάσσουν και να συσχετίζουν αποτελεσματικότερα τα σήματα που εντοπίζονται και να δημιουργούν υψηλής ποιότητας πληροφορίες σχετικά με απειλές, τις οποίες θα κοινοποιούν στα ISAC και στις εθνικές αρχές, καθιστώντας έτσι δυνατή την πληρέστερη επίγνωση της κατάστασης. Στόχος θα είναι η σταδιακή σύνδεση όσο το δυνατόν περισσότερων κέντρων σε ολόκληρη την ΕΕ για τη δημιουργία συλλογικών γνώσεων και την ανταλλαγή βέλτιστων πρακτικών. Στα εν λόγω κέντρα θα παρασχεθεί στήριξη για τη βελτίωση της ανίχνευσης, της ανάλυσης και της ταχύτητας αντιμετώπισης συμβάντων μέσω υπερσύγχρονων ικανοτήτων τεχνητής νοημοσύνης και μηχανομάθησης και θα συμπληρωθεί από υποδομές υπερυπολογιστικής που αναπτύχθηκαν στην ΕΕ από την κοινή επιχείρηση για την ευρωπαϊκή υπολογιστική υψηλών επιδόσεων[44].

Με συνεχή συνεργασία, το εν λόγω δίκτυο θα παρέχει έγκαιρες προειδοποιήσεις σχετικά με περιστατικά κυβερνοασφάλειας στις αρχές και σε όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένης της Κοινής Μονάδας Κυβερνοχώρου (βλ. τμήμα 2.1). **Το δίκτυο αυτό θα λειτουργεί ως πραγματική ασπίδα κυβερνοασφάλειας για την ΕΕ**, παρέχοντας ένα στέρεο πλέγμα παρατηρητηρίων, ικανών να εντοπίζουν δυνητικές απειλές πριν προκληθούν ζημίες μεγάλης κλίμακας.

[41]Με τρόπο που επιτρέπει στις αρχές επιβολής του νόμου και στις δικαστικές αρχές να μπορούν να τα χρησιμοποιούν ως αποδεικτικά στοιχεία.

[42]Πηγή: έρευνα του Ponemon Institute Research, «Improving the Effectiveness of the SOC, 2019»· για μελέτες σχετικά με τη χρήση της τεχνητής νοημοσύνης στα επιχειρησιακά κέντρα ασφάλειας, βλ. για παράδειγμα: Khraisat, A., Gondal, I., Vamplew, P. κ.ά, «Survey of intrusion detection systems: techniques, datasets and challenges», *Cybersecur* 2**,** 20 (2019).

[43]Θα αναπτυχθούν λεπτομερέστερες ρυθμίσεις για τη διακυβέρνηση, τις αρχές λειτουργίας και τη χρηματοδότηση των εν λόγω κέντρων, καθώς και για τον τρόπο με τον οποίο τα κέντρα αυτά θα συμπληρώσουν τις υφιστάμενες δομές, όπως οι κόμβοι ψηφιακής καινοτομίας.

[44]https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

1.3 Εξαιρετικά ασφαλής υποδομή επικοινωνιών

Οι κυβερνητικές δορυφορικές επικοινωνίες της Ευρωπαϊκής Ένωσης[45], που αποτελούν συνιστώσα του διαστημικού προγράμματος, θα παράσχουν ασφαλείς και οικονομικά αποδοτικές διαστημικές επικοινωνιακές ικανότητες για τη διασφάλιση αποστολών και επιχειρήσεων που είναι κρίσιμες για την ασφάλεια συστημάτων και προσώπων και τελούν υπό τη διαχείριση της ΕΕ και των κρατών μελών της, συμπεριλαμβανομένων των εθνικών φορέων ασφάλειας και των θεσμικών οργάνων και οργανισμών της ΕΕ.

Τα κράτη μέλη έχουν δεσμευτεί να συνεργαστούν με την Επιτροπή για την ανάπτυξη ασφαλούς υποδομής κβαντικής επικοινωνίας (QCI) για την Ευρώπη[46]. Η QCI θα προσφέρει στις δημόσιες αρχές έναν εντελώς νέο τρόπο διαβίβασης εμπιστευτικών πληροφοριών με μια εξαιρετικά ασφαλή μορφή κρυπτογράφησης, κατασκευασμένη με ευρωπαϊκή τεχνολογία, για την προστασία από κυβερνοεπιθέσεις. Θα έχει δύο κύριες συνιστώσες: τα υφιστάμενα επίγεια δίκτυα επικοινωνίας με οπτικές ίνες, τα οποία συνδέουν στρατηγικές τοποθεσίες σε εθνικό και διασυνοριακό επίπεδο· και συνδεδεμένους διαστημικούς δορυφόρους που καλύπτουν ολόκληρη την ΕΕ, συμπεριλαμβανομένων των υπερπόντιων εδαφών της[47]. Η πρωτοβουλία αυτή για την ανάπτυξη και χρήση νέων και ασφαλέστερων μορφών κρυπτογράφησης, καθώς και για τον σχεδιασμό νέων τρόπων προστασίας των δομών επικοινωνίας και των δεδομένων ζωτικής σημασίας, μπορεί να συμβάλει στη διατήρηση της ασφάλειας των ευαίσθητων πληροφοριών και, ως εκ τούτου, των υποδομών ζωτικής σημασίας.

Σε αυτό το πλαίσιο, αλλά και στο μέλλον, η Επιτροπή θα διερευνήσει το ενδεχόμενο ανάπτυξης ενός συστήματος ασφαλούς συνδεσιμότητας πολλαπλών τροχιών. Με βάση το GOVSATCOM και την QCI, το σύστημα αυτό θα ενσωματώνει τεχνολογίες αιχμής (κβαντική τεχνολογία, 5G, τεχνητή νοημοσύνη, υπολογιστική παρυφών) και θα συμμορφώνεται με το πλέον περιοριστικό πλαίσιο κυβερνοασφάλειας, προκειμένου να υποστηρίζει ασφαλείς βάσει σχεδιασμού υπηρεσίες, όπως η αξιόπιστη, ασφαλής και οικονομικά αποδοτική συνδεσιμότητα και η κρυπτογραφημένη επικοινωνία για κυβερνητικές δραστηριότητες ζωτικής σημασίας.

[45]Το πρόγραμμα GOVSATCOM αποτελεί συνιστώσα του διαστημικού προγράμματος της Ένωσης.

[46]Η δήλωση EuroQCI υπογράφηκε από την πλειονότητα των κρατών μελών και η ανάπτυξη και εγκατάσταση της υποδομής πρόκειται να πραγματοποιηθούν κατά την περίοδο 2021-2027, με χρηματοδότηση από τα προγράμματα «Ορίζων Ευρώπη» και «Ψηφιακή Ευρώπη», καθώς και από τον Ευρωπαϊκό Οργανισμό Διαστήματος, στο πλαίσιο κατάλληλων ρυθμίσεων διακυβέρνησης· https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[47]Η ανάπτυξη διαστημικής συνιστώσας είναι απαραίτητη για την επίτευξη διασημειακών συνδέσεων μεγάλων αποστάσεων (> 1 000 km), οι οποίες δεν μπορούν να υποστηριχθούν από τις επίγειες υποδομές. Αξιοποιώντας τις ιδιότητες της κβαντικής μηχανικής, η QCI θα επιτρέψει αρχικά στα μέρη να ανταλλάσσουν με ασφάλεια τυχαία μυστικά κλειδιά που θα χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση μηνυμάτων. Θα συμπεριλάβει επίσης την εγκατάσταση υποδομής δοκιμών και συμμόρφωσης, για την αξιολόγηση της συμμόρφωσης των ευρωπαϊκών συσκευών και συστημάτων κβαντικής επικοινωνίας με την υποδομή QCI, καθώς και για την πιστοποίηση και επικύρωσή τους πριν από την ενσωμάτωσή τους στην QCI. Θα σχεδιαστεί με τρόπο ώστε να μπορεί να υποστηρίξει πρόσθετες εφαρμογές, όταν αυτές φθάνουν στο αναγκαίο επίπεδο τεχνολογικής ωριμότητας. Το τρέχον πιλοτικό πρόγραμμα OpenQKD (https://openqkd.eu/) αποτελεί πρόδρομο αυτής της υποδομής δοκιμών και συμμόρφωσης.

1.4 Ασφαλέστερα ευρυζωνικά κινητά δίκτυα επόμενης γενιάς

Οι πολίτες και οι εταιρείες της ΕΕ που χρησιμοποιούν προηγμένες και καινοτόμες εφαρμογές που καθίστανται εφικτές με **το 5G και τις μελλοντικές γενιές δικτύων** θα πρέπει να προστατεύονται με τα υψηλότερα πρότυπα ασφάλειας. Με την εργαλειοθήκη της ΕΕ για το 5G[48] που εκδόθηκε τον Ιανουάριο του 2020, τα κράτη μέλη, από κοινού με την Επιτροπή και με την υποστήριξη του ENISA, δημιούργησαν μια ολοκληρωμένη και αντικειμενική προσέγγιση βάσει κινδύνου για την κυβερνοασφάλεια του 5G, η οποία βασίζεται σε αξιολόγηση πιθανών σχεδίων μετριασμού και στον προσδιορισμό των πλέον αποτελεσματικών μέτρων. Επιπλέον, η ΕΕ εδραιώνει τις ικανότητές της στο πεδίο του 5G και των μελλοντικών τεχνολογιών, ώστε να αποφύγει τις εξαρτήσεις και να προωθήσει μια βιώσιμη και διαφοροποιημένη αλυσίδα εφοδιασμού.

Τον Δεκέμβριο του 2020, η Επιτροπή δημοσίευσε έκθεση σχετικά με τις επιπτώσεις της σύστασης της 26ης Μαρτίου 2019 σχετικά με την κυβερνοασφάλεια των δικτύων 5G[49]. Διαπιστώθηκε ότι έχει σημειωθεί σημαντική πρόοδος από την έγκριση της εργαλειοθήκης και ότι τα περισσότερα κράτη μέλη βρίσκονται σε καλό δρόμο για την ολοκλήρωση σημαντικού μέρους της εφαρμογής της εργαλειοθήκης στο εγγύς μέλλον, αν και με ορισμένες παραλλαγές και εναπομένοντα κενά, όπως έχει ήδη επισημανθεί στην έκθεση προόδου που δημοσιεύτηκε τον Ιούλιο του 2020[50].

Τον Οκτώβριο του 2020, το Ευρωπαϊκό Συμβούλιο κάλεσε την ΕΕ και τα κράτη μέλη «να αξιοποιήσουν πλήρως την εργαλειοθήκη για την ασφάλεια των δικτύων 5G στον κυβερνοχώρο» και «να εφαρμόσουν τους σχετικούς περιορισμούς στους προμηθευτές υψηλού κινδύνου για βασικά στοιχεία ενεργητικού που ορίζονται ως ζωτικής σημασίας και ευαίσθητα στις συντονισμένες από την ΕΕ εκτιμήσεις κινδύνου, βάσει κοινών αντικειμενικών κριτηρίων»[51].

Στο μέλλον, η ΕΕ και τα κράτη μέλη της θα πρέπει να διασφαλίσουν ότι οι εντοπισθέντες κίνδυνοι έχουν μετριαστεί επαρκώς και με συντονισμένο τρόπο, ιδίως όσον αφορά τους στόχους της ελαχιστοποίησης της έκθεσης σε προμηθευτές υψηλού κινδύνου και της αποφυγής της εξάρτησης από τους εν λόγω προμηθευτές σε εθνικό και ενωσιακό επίπεδο, καθώς και ότι λαμβάνουν υπόψη κάθε νέα σημαντική εξέλιξη ή κίνδυνο. Τα κράτη μέλη καλούνται να αξιοποιήσουν πλήρως την εργαλειοθήκη στο πλαίσιο των επενδύσεών τους σε ψηφιακές ικανότητες και συνδεσιμότητα.

Με βάση την έκθεση σχετικά με τις επιπτώσεις της σύστασης του 2019, η Επιτροπή ενθαρρύνει τα κράτη μέλη να εντείνουν τις προσπάθειες για την ολοκλήρωση της εφαρμογής των βασικών μέτρων της εργαλειοθήκης έως το δεύτερο τρίμηνο του 2021. Καλεί, επίσης, τα κράτη μέλη να εξακολουθήσουν να παρακολουθούν από κοινού την πρόοδο που σημειώνεται και να εξασφαλίζουν την περαιτέρω ευθυγράμμιση των προσεγγίσεών τους. Σε επίπεδο ΕΕ, θα επιδιωχθούν τρεις κύριοι στόχοι για την υποστήριξη της διαδικασίας αυτής: εξασφάλιση περαιτέρω σύγκλισης των διαφόρων προσεγγίσεων μετριασμού των κινδύνων στην ΕΕ, στήριξη της συνεχούς ανταλλαγής γνώσεων και της ανάπτυξης ικανοτήτων, και προώθηση

[48]Ανακοίνωση σχετικά με την ασφαλή εγκατάσταση του 5G στην ΕΕ — Εφαρμογή της εργαλειοθήκης της ΕΕ, COM(2020) 50.
[49]Εκθεση της Επιτροπής σχετικά με τις επιπτώσεις της σύστασης της Επιτροπής, της 26ης Μαρτίου 2019, σχετικά με την κυβερνοασφάλεια των δικτύων 5G, της 15ης Δεκεμβρίου 2020.
[50]Εκθεση της ομάδας συνεργασίας NIS σχετικά με την εφαρμογή της εργαλειοθήκης, της 24ης Ιουλίου 2020.
[51]EUCO 13/20, Έκτακτη σύνοδος του Ευρωπαϊκού Συμβουλίου (1 και 2 Οκτωβρίου 2020) — Συμπεράσματα.

της ανθεκτικότητας της αλυσίδας εφοδιασμού και άλλων στρατηγικών στόχων της ΕΕ στον τομέα της ασφάλειας. Συγκεκριμένες δράσεις που σχετίζονται με αυτούς τους βασικούς στόχους καθορίζονται στο ειδικό προσάρτημα της παρούσας ανακοίνωσης.

Η Επιτροπή θα εξακολουθήσει να συνεργάζεται στενά με τα κράτη μέλη για την εφαρμογή αυτών των στόχων και δράσεων με την υποστήριξη του ENISA (βλ. παράρτημα).

Επιπλέον, η προσέγγιση της εργαλειοθήκης 5G της ΕΕ έχει προσελκύσει το ενδιαφέρον τρίτων χωρών που αναπτύσσουν επί του παρόντος τις προσεγγίσεις τους για τη διασφάλιση των δικτύων επικοινωνίας τους. Οι υπηρεσίες της Επιτροπής, από κοινού με την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης και το δίκτυο των αντιπροσωπειών της ΕΕ, είναι έτοιμες να παράσχουν στις αρχές παγκοσμίως, εάν τους ζητηθεί, πρόσθετες πληροφορίες σχετικά με την ολοκληρωμένη, αντικειμενική και βασιζόμενη στον κίνδυνο προσέγγιση της ΕΕ.

1.5 Το διαδίκτυο των ασφαλών πραγμάτων

Κάθε συνδεδεμένο πράγμα περιέχει τρωτά σημεία τα οποία μπορούν να εκμεταλλευτούν τρίτοι με δυνητικά εκτεταμένες συνέπειες. Οι κανόνες της εσωτερικής αγοράς περιλαμβάνουν διασφαλίσεις έναντι επισφαλών προϊόντων και υπηρεσιών. Η Επιτροπή καταβάλλει ήδη προσπάθειες για να εξασφαλίσει **διαφανείς λύσεις ασφάλειας και πιστοποίησης στο πλαίσιο της πράξης για την κυβερνοασφάλεια** και να παράσχει κίνητρα για ασφαλή προϊόντα και υπηρεσίες χωρίς να υπονομεύει τις επιδόσεις τους[52]. Το πρώτο τρίμηνο του 2021 θα εγκρίνει το πρώτο κυλιόμενο πρόγραμμα εργασίας της Ένωσης (το οποίο θα επικαιροποιείται τουλάχιστον κάθε τρία έτη), ώστε να δώσει τη δυνατότητα στον κλάδο, στις εθνικές αρχές και στους οργανισμούς τυποποίησης να προετοιμαστούν εκ των προτέρων για τα μελλοντικά ευρωπαϊκά σχήματα πιστοποίησης της κυβερνοασφάλειας[53]. Καθώς το διαδίκτυο των πραγμάτων εξαπλώνεται, οι εφαρμοστέοι κανόνες πρέπει να ενισχυθούν για να διασφαλιστεί η συνολική ανθεκτικότητα, αλλά και για να ενδυναμωθεί περαιτέρω η κυβερνοασφάλεια.

Η Επιτροπή θα εξετάσει μια ολοκληρωμένη προσέγγιση, συμπεριλαμβανομένων πιθανών **νέων οριζόντιων κανόνων για τη βελτίωση της κυβερνοασφάλειας όλων των συνδεδεμένων προϊόντων και συναφών υπηρεσιών που διατίθενται στην εσωτερική αγορά**[54]. Στους κανόνες αυτούς θα μπορούσε να περιλαμβάνεται **νέο καθήκον μέριμνας των κατασκευαστών συνδεδεμένων συσκευών** για την αντιμετώπιση των τρωτών σημείων του λογισμικού, συμπεριλαμβανομένης της συνέχισης των ενημερώσεων λογισμικού και ασφαλείας, καθώς και τη διασφάλιση της διαγραφής προσωπικών και άλλων ευαίσθητων δεδομένων στο τέλος του κύκλου ζωής των συσκευών. Οι εν λόγω κανόνες θα ενισχύσουν

[52]Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια). Η πράξη για την κυβερνοασφάλεια προάγει την πιστοποίηση ΤΠΕ σε επίπεδο ΕΕ, με ένα ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας για τη θέσπιση εθελοντικών ευρωπαϊκών σχημάτων πιστοποίησης της κυβερνοασφάλειας με σκοπό να διασφαλιστεί επαρκές επίπεδο κυβερνοασφάλειας των προϊόντων ΤΠΕ, των υπηρεσιών ΤΠΕ και των διαδικασιών ΤΠΕ στην Ένωση, καθώς και να περιοριστεί ο κατακερματισμός της εσωτερικής αγοράς όσον αφορά τα σχήματα πιστοποίησης της κυβερνοασφάλειας στην Ένωση. Παράλληλα, οι εταιρείες «αξιολογήσεων» κυβερνοασφάλειας συνήθως εδρεύουν εκτός της ΕΕ και λειτουργούν με περιορισμένη διαφάνεια και εποπτεία· https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53]Απαιτείται βάσει του άρθρου 47 παράγραφος 5 της πράξης για την κυβερνοασφάλεια.

[54]Στα συμπεράσματα του Συμβουλίου ζητείται η λήψη οριζόντιων μέτρων για την κυβερνοασφάλεια των συνδεδεμένων συσκευών· 13629/20, 2 Δεκεμβρίου 2020.

την πρωτοβουλία για το «δικαίωμα επισκευής απαρχαιωμένου λογισμικού» η οποία παρουσιάστηκε στο σχέδιο δράσης για την κυκλική οικονομία και θα συμπληρώσουν τα ισχύοντα μέτρα που αφορούν συγκεκριμένα είδη προϊόντων, όπως οι υποχρεωτικές απαιτήσεις που πρόκειται να προταθούν για την πρόσβαση στην αγορά ορισμένων ασύρματων προϊόντων (μέσω της θέσπισης κατ' εξουσιοδότηση πράξης στο πλαίσιο της οδηγίας για τον ραδιοεξοπλισμό[55]), και ο στόχος εφαρμογής κανόνων κυβερνοασφάλειας για τα μηχανοκίνητα οχήματα σε όλους τους νέους τύπους οχημάτων από τον Ιούλιο του 2022[56]. Επιπλέον, θα βασιστούν στην προτεινόμενη αναθεώρηση των κανόνων για τη γενική ασφάλεια των προϊόντων, οι οποίοι δεν εξετάζουν άμεσα τις πτυχές της κυβερνοασφάλειας[57].

1.6 Ενίσχυση της ασφάλειας του διαδικτύου παγκοσμίως

Η λειτουργικότητα και η ακεραιότητα του διαδικτύου παγκοσμίως διασφαλίζονται με ένα σύνολο βασικών πρωτοκόλλων και υποστηρικτικών υποδομών[58]. Το σύνολο αυτό περιλαμβάνει το DNS και το ιεραρχικό και κατανεμημένο σύστημα ζωνών του, το οποίο ξεκινά, στην κορυφή της ιεραρχίας, με τη ζώνη ρίζας και τους δεκατρείς εξυπηρετητές ρίζας DNS[59] στους οποίους βασίζεται ο Παγκόσμιος Ιστός. Η Επιτροπή σκοπεύει να αναπτύξει **σχέδιο έκτακτης ανάγκης, με την υποστήριξη της ενωσιακής χρηματοδότησης, για την αντιμετώπιση ακραίων σεναρίων που επηρεάζουν την ακεραιότητα και τη διαθεσιμότητα του παγκόσμιου συστήματος ρίζας DNS**. Θα συνεργαστεί με τον ENISA, τα κράτη μέλη, τους δύο διαχειριστές εξυπηρετητών ρίζας DNS της ΕΕ[60] και την πολυσυμμετοχική κοινότητα, για να αξιολογήσει τον ρόλο των εν λόγω διαχειριστών στη διασφάλιση της δυνατότητας πρόσβασης στο διαδίκτυο ανά πάσα στιγμή και από όλο τον κόσμο.

Για να αποκτήσει ένας πελάτης πρόσβαση σε έναν πόρο με συγκεκριμένο όνομα τομέα στο διαδίκτυο, το αίτημά του (συνήθως για ενιαίο εντοπιστή πόρου ή URL) πρέπει να μεταφραστεί ή να «επιλυθεί» σε διεύθυνση IP μέσω εξυπηρετητών ονομάτων DNS. Ωστόσο, οι ιδιώτες και οι οργανισμοί της ΕΕ βασίζονται όλο και περισσότερο σε λίγους δημόσιους επιλυτές DNS τους οποίους εκμεταλλεύονται οντότητες εκτός ΕΕ. Αυτή η συγκέντρωση της επίλυσης ονομάτων τομέα DNS στα χέρια λίγων εταιρειών[61] καθιστά ευάλωτη την ίδια τη διαδικασία επίλυσης σε περίπτωση σημαντικών συμβάντων που επηρεάζουν έναν μεγάλο

---

[55]Οδηγία 2014/53/ΕΕ

[56]Σε συνέχεια του κανονισμού του ΟΗΕ που εγκρίθηκε τον Ιούνιο του 2020· http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[57]Αναθεώρηση των ισχυόντων κανόνων για τη γενική ασφάλεια των προϊόντων (οδηγία 2001/95/ΕΚ)· σχεδιάζεται, επίσης να υποβληθεί πρόταση για την προσαρμογή των κανόνων σχετικά με την ευθύνη των παραγωγών στο ψηφιακό πλαίσιο εντός του πεδίου εφαρμογής του κανονιστικού πλαισίου ευθύνης της ΕΕ

[58]«Ο δημόσιος πυρήνας του ανοιχτού διαδικτύου, δηλαδή τα κύρια πρωτόκολλα και οι υποδομές του που είναι παγκόσμιο δημόσιο αγαθό, παρέχει τη βασική λειτουργικότητα του διαδικτύου στο σύνολό του και στηρίζει την κανονική του λειτουργία. Ο ENISA θα πρέπει να στηρίζει την ασφάλεια του δημόσιου πυρήνα του ανοιχτού διαδικτύου και τη σταθερότητα της λειτουργίας του, συμπεριλαμβανομένων, χωρίς να περιορίζεται σε αυτά, των βασικών πρωτοκόλλων (ιδίως DNS, BGP και IPv6), της λειτουργίας του συστήματος ονομάτων τομέα (όπως η λειτουργία όλων των τομέων ανωτάτου επιπέδου) και της λειτουργίας της βασικής ζώνης»· Αιτιολογική σκέψη 23 της πράξης για την κυβερνοασφάλεια.

[59]https://www.iana.org/domains/root/servers

[60]Οι i.root-servers που διαχειρίζεται η Netnod στη Σουηδία και οι k.root-servers που διαχειρίζεται η RIPE NCC στις Κάτω Χώρες.

[61]Consolidation in the DNS resolver market – how much, how fast how dangerous? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ( )

πάροχο, και δυσχεραίνει τις προσπάθειες των αρχών της ΕΕ να αντιμετωπίσουν πιθανές κακόβουλες κυβερνοεπιθέσεις και σοβαρά γεωπολιτικά και τεχνικά περιστατικά[62].

Προκειμένου να περιοριστούν τα ζητήματα ασφάλειας που σχετίζονται με τη συγκέντρωση της αγοράς, η Επιτροπή θα ενθαρρύνει τα σχετικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των επιχειρήσεων της ΕΕ, των παρόχων υπηρεσιών διαδικτύου και των πωλητών προγραμμάτων περιήγησης, να υιοθετήσουν στρατηγική διαφοροποίησης της επίλυσης ονομάτων τομέα DNS. Η Επιτροπή σκοπεύει, επίσης, να συμβάλει στη διασφάλιση της συνδεσιμότητας στο διαδίκτυο στηρίζοντας την ανάπτυξη δημόσιας **ευρωπαϊκής υπηρεσίας επίλυσης DNS**. Αυτή η πρωτοβουλία «DNS4EU» θα προσφέρει μια εναλλακτική, ευρωπαϊκή υπηρεσία για την πρόσβαση στο παγκόσμιο διαδίκτυο. Η DNS4EU θα είναι διαφανής, θα συμμορφώνεται με τα πλέον πρόσφατα πρότυπα και τους κανόνες ασφάλειας, προστασίας των δεδομένων και της ιδιωτικής ζωής ήδη από τον σχεδιασμό και εξ ορισμού και θα συμμετέχει στην ευρωπαϊκή βιομηχανική συμμαχία για τα δεδομένα και το υπολογιστικό νέφος[63].

Η Επιτροπή, σε συνεργασία με τα κράτη μέλη και τις επιχειρήσεις του κλάδου, **θα επιταχύνει επίσης την εφαρμογή βασικών προτύπων του διαδικτύου, συμπεριλαμβανομένου του IPv6[64], καθώς και αναγνωρισμένων προτύπων ασφάλειας του διαδικτύου και ορθών πρακτικών για την ασφάλεια του DNS, της δρομολόγησης και του ηλεκτρονικού ταχυδρομείου[65]**, χωρίς να αποκλείεται η λήψη κανονιστικών μέτρων, όπως μια ευρωπαϊκή ρήτρα λήξης ισχύος για το IPv4 με σκοπό την καθοδήγηση της αγοράς εάν δεν σημειωθεί επαρκής πρόοδος όσον αφορά την υιοθέτησή τους. Η ΕΕ θα πρέπει να προωθήσει (όπως, για παράδειγμα, στο πλαίσιο της στρατηγικής ΕΕ-Αφρικής[66]) την εφαρμογή αυτών των προτύπων στις χώρες εταίρους για να στηρίξει την ανάπτυξη του παγκόσμιου και ανοικτού διαδικτύου και να αντιταχθεί στα κλειστά μοντέλα του διαδικτύου που βασίζονται σε ελέγχους. Τέλος, η Επιτροπή θα εξετάσει την ανάγκη δημιουργίας ενός μηχανισμού για τη συστηματικότερη παρακολούθηση και συλλογή συγκεντρωτικών δεδομένων σχετικά με την κίνηση στο διαδίκτυο και για την παροχή συμβουλών σχετικά με πιθανές διαταραχές[67].

1.7 Ενισχυμένη παρουσία στην τεχνολογική αλυσίδα εφοδιασμού

Χάρη στην προγραμματισμένη χρηματοδοτική στήριξη για τον κυβερνοασφαλή ψηφιακό μετασχηματισμό κατά τη διάρκεια του πολυετούς δημοσιονομικού πλαισίου 2021-2027, η

[62]Υπάρχουν επίσης στοιχεία που αποδεικνύουν ότι τα δεδομένα DNS μπορούν να χρησιμοποιηθούν για σκοπούς κατάρτισης προφίλ, γεγονός που έχει επιπτώσεις στην ιδιωτική ζωή και στα δικαιώματα προστασίας των δεδομένων.

[63]Κοινή δήλωση: Οικοδόμηση του νέφους της επόμενης γενιάς για τις επιχειρήσεις και τον δημόσιο τομέα στην ΕΕ· https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64]Η χρήση του IPv6 έχει πλέον επεκταθεί λόγω της μεγάλης μείωσης της προσφοράς και της αύξησης του κόστους των διευθύνσεων IPv4. Ωστόσο, η χρήση του IPv6 δεν είναι ομοιόμορφη σε όλες τις χώρες της ΕΕ.

[65]Στα πρότυπα αυτά περιλαμβάνονται τα DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE, καθώς και κανόνες και ορθές πρακτικές δρομολόγησης, π.χ. τα αμοιβαία συμφωνηθέντα πρότυπα για ασφαλή δρομολόγηση (MANRS).

[66]Κοινή ανακοίνωση με τίτλο «Προς μια ολοκληρωμένη στρατηγική με την Αφρική», 9.3.2020 JOIN(2020) 4 final.

[67]Αυτό το «παρατηρητήριο του διαδικτύου» θα μπορούσε να εμπίπτει στο πεδίο των δραστηριοτήτων του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας· Πρόταση κανονισμού 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.

ΕΕ έχει τη μοναδική ευκαιρία να συνδυάσει τους πόρους της για να δώσει ώθηση στη βιομηχανική στρατηγική της[68] και στην ηγετική της θέση στους τομείς των ψηφιακών τεχνολογιών και της κυβερνοασφάλειας σε ολόκληρη την ψηφιακή αλυσίδα εφοδιασμού (συμπεριλαμβανομένων των δεδομένων και του υπολογιστικού νέφους, των τεχνολογιών επεξεργαστών επόμενης γενιάς, της εξαιρετικά ασφαλούς συνδεσιμότητας και των δικτύων 6G), σύμφωνα με τις αξίες και τις προτεραιότητές της. Η παρέμβαση του δημόσιου τομέα θα πρέπει να βασίζεται στα εργαλεία που παρέχει το κανονιστικό πλαίσιο της ΕΕ για τις δημόσιες συμβάσεις και τα «σημαντικά έργα κοινού ευρωπαϊκού ενδιαφέροντος». Πέραν τούτου, μπορούν να αποδεσμευτούν ιδιωτικές επενδύσεις μέσω συμπράξεων δημόσιου και ιδιωτικού τομέα (μεταξύ άλλων με την αξιοποίηση της πείρας που αποκτήθηκε από τη συμβατική σύμπραξη δημόσιου και ιδιωτικού τομέα για την ασφάλεια στον κυβερνοχώρο και την υλοποίησή της μέσω του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο), κεφαλαίων επιχειρηματικού κινδύνου για τη στήριξη ΜΜΕ ή βιομηχανικών συμμαχιών και στρατηγικών για τις τεχνολογικές ικανότητες.

Ιδιαίτερη έμφαση θα δοθεί επίσης στο μέσο τεχνικής υποστήριξης[69] και στη βέλτιστη χρήση των πλέον πρόσφατων εργαλείων κυβερνοασφάλειας από τις ΜΜΕ —ιδίως εκείνες που δεν εμπίπτουν στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας NIS— μεταξύ άλλων μέσω ειδικών δραστηριοτήτων στο πλαίσιο των κόμβων ψηφιακής καινοτομίας του προγράμματος «Ψηφιακή Ευρώπη». Στόχος είναι να κινητοποιηθούν επενδύσεις αντίστοιχου ύψους από τα κράτη μέλη, οι οποίες θα συνδυαστούν με ισόποσες επενδύσεις του κλάδου στο πλαίσιο εταιρικής σχέσης υπό κοινή διακυβέρνηση με τα κράτη μέλη στο προτεινόμενο **βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας και στο προτεινόμενο δίκτυο κέντρων συντονισμού (CCCN)**. Το CCCN θα πρέπει να διαδραματίσει καίριο ρόλο, με τη συμβολή του κλάδου και των πανεπιστημιακών κύκλων, στην ανάπτυξη της τεχνολογικής κυριαρχίας της ΕΕ στον τομέα της κυβερνοασφάλειας, στην οικοδόμηση ικανοτήτων για τη διασφάλιση ευαίσθητων υποδομών, όπως το 5G, και στη μείωση της εξάρτησης από άλλα μέρη του πλανήτη για τις πλέον κρίσιμες τεχνολογίες.

Η Επιτροπή σκοπεύει να στηρίξει, ενδεχομένως με το CCCN, την ανάπτυξη ειδικού μεταπτυχιακού προγράμματος στην κυβερνοασφάλεια και να συμβάλει στην επεξεργασία κοινού ευρωπαϊκού χάρτη πορείας για την έρευνα και την καινοτομία στον τομέα της κυβερνοασφάλειας μετά το 2020. Οι επενδύσεις που θα πραγματοποιηθούν μέσω του CCCN θα βασιστούν, επίσης, στη συνεργασία σε έργα έρευνας και ανάπτυξης που εκτελούνται από δίκτυα κέντρων αριστείας στον τομέα της κυβερνοασφάλειας, στο πλαίσιο των οποίων οι καλύτερες ερευνητικές ομάδες της Ευρώπης και οι επιχειρήσεις του κλάδου έρχονται σε επαφή για τον σχεδιασμό και την υλοποίηση κοινών θεματολογίων έρευνας, σύμφωνα με τον χάρτη πορείας του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο[70]. Η Επιτροπή θα συνεχίσει να βασίζεται στο ερευνητικό έργο του ENISA και της Ευρωπόλ και θα συνεχίσει, επίσης, να στηρίζει, στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη», μεμονωμένους διαδικτυακούς φορείς καινοτομίας που αναπτύσσουν ασφαλείς τεχνολογίες επικοινωνιών οι οποίες ενισχύουν την προστασία της ιδιωτικής ζωής και βασίζονται σε λογισμικό και υλισμικό ανοικτού κώδικα, όπως συμβαίνει επί του παρόντος στο πλαίσιο της πρωτοβουλίας «Διαδίκτυο επόμενης γενιάς».

[68]Ανακοίνωση σχετικά με μια νέα βιομηχανική στρατηγική για την Ευρώπη, COM/2020/102 final.
[69]https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=COM:2020:0409:FIN# .
[70]https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies

1.8 Ένα εργατικό δυναμικό της ΕΕ με κυβερνοδεξιότητες

Οι προσπάθειες της ΕΕ να αναβαθμίσει τις δεξιότητες του εργατικού δυναμικού, να αναπτύξει, να προσελκύσει και να διατηρήσει τα καλύτερα ταλέντα στον τομέα της κυβερνοασφάλειας και να επενδύσει σε έρευνα και καινοτομία παγκόσμιας κλάσης αποτελούν σημαντική συνιστώσα της προστασίας από τις κυβερνοαπειλές εν γένει. Ο τομέας αυτός προσφέρει μεγάλες δυνατότητες. Ως εκ τούτου, πρέπει να δοθεί ιδιαίτερη προσοχή στην ανάπτυξη, την προσέλκυση και τη διατήρηση περισσότερο διαφοροποιημένων ταλέντων. Το αναθεωρημένο σχέδιο δράσης για την ψηφιακή εκπαίδευση θα προωθήσει τις δραστηριότητες ευαισθητοποίησης σε θέματα κυβερνοασφάλειας μεταξύ των ατόμων, ιδίως των παιδιών και των νέων, καθώς και μεταξύ των οργανισμών, ιδίως των ΜΜΕ[71]. Θα ενθαρρύνει επίσης τη συμμετοχή των γυναικών στην εκπαίδευση, στους τομείς της επιστήμης, της τεχνολογίας, της μηχανικής και των μαθηματικών (τομείς «STEM»), καθώς και την αναβάθμιση των δεξιοτήτων στις θέσεις εργασίας του τομέα ΤΠΕ και την επανειδίκευση στις ψηφιακές δεξιότητες. Επιπλέον, η Επιτροπή, από κοινού με το Γραφείο Διανοητικής Ιδιοκτησίας της ΕΕ στην Ευρωπόλ, τον ENISA, τα κράτη μέλη και τον ιδιωτικό τομέα, θα αναπτύξει εργαλεία ευαισθητοποίησης και κατευθυντήριες γραμμές για την ενίσχυση της ανθεκτικότητας των επιχειρήσεων της ΕΕ **έναντι της κλοπής διανοητικής ιδιοκτησίας που διευκολύνεται από τον κυβερνοχώρο**[72].

Η εκπαίδευση, καθώς και η επαγγελματική εκπαίδευση και κατάρτιση (ΕΕΚ), η ευαισθητοποίηση και οι ασκήσεις, θα πρέπει επίσης να αυξήσουν περαιτέρω τις δεξιότητες κυβερνοασφάλειας και κυβερνοάμυνας σε επίπεδο ΕΕ. Για τον σκοπό αυτό, οι σχετικοί φορείς της ΕΕ, όπως ο ENISA, ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ) και η Ευρωπαϊκή Ακαδημία Ασφάλειας και Άμυνας (ΕΑΑΑ)[73], θα πρέπει να επιδιώκουν συνέργειες μεταξύ των αντίστοιχων δραστηριοτήτων τους.

Στρατηγικές πρωτοβουλίες

Η ΕΕ θα πρέπει να διασφαλίσει τα εξής:

- την έκδοση της αναθεωρημένης οδηγίας NIS·
- τη θέσπιση κανονιστικών μέτρων για το διαδίκτυο των ασφαλών πραγμάτων·
- τη διάθεση, μέσω των επενδύσεων του CCCN στην κυβερνοασφάλεια (ιδίως μέσω του προγράμματος «Ψηφιακή Ευρώπη», του προγράμματος «Ορίζων Ευρώπη» και του μηχανισμού ανάκαμψης), έως και 4,5 δισ. EUR σε δημόσιες και ιδιωτικές επενδύσεις κατά την περίοδο 2021-2027·
- τη δημιουργία ενός ενωσιακού δικτύου κέντρων επιχειρήσεων ασφαλείας, βασιζόμενων στην τεχνητή νοημοσύνη, και μιας εξαιρετικά ασφαλούς υποδομής επικοινωνιών που θα αξιοποιεί κβαντικές τεχνολογίες·
- την ευρεία υιοθέτηση των τεχνολογιών κυβερνοασφάλειας, μέσω ειδικής στήριξης προς τις ΜΜΕ στο πλαίσιο των κόμβων ψηφιακής καινοτομίας·
- την ανάπτυξη μιας ενωσιακής υπηρεσίας επίλυσης DNS, ως ασφαλούς και ανοικτής

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_el
[72] https://ec.europa.eu/commission/presscorner/detail/el/IP_20_2187
[73] Μέσω της πλατφόρμας εκπαίδευσης, κατάρτισης, ασκήσεων και αξιολόγησης (ΕΚΑΑ) για τον κυβερνοχώρο.

εναλλακτικής λύσης για την πρόσβαση των πολιτών, των επιχειρήσεων και της δημόσιας διοίκησης της ΕΕ στο διαδίκτυο· και

- την ολοκλήρωση της εφαρμογής της εργαλειοθήκης για το 5G έως το δεύτερο τρίμηνο του 2021 (βλ. παράρτημα).

2. ΑΝΑΠΤΥΞΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΙΚΑΝΟΤΗΤΑΣ ΠΡΟΛΗΨΗΣ, ΑΠΟΤΡΟΠΗΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Τα κυβερνοπεριστατικά, είτε πρόκειται για τυχαία περιστατικά είτε για εκούσιες ενέργειες εγκληματιών ή κρατικών και άλλων μη κρατικών φορέων, μπορούν να προκαλέσουν τεράστιες ζημίες. Λόγω της κλίμακας και της πολυπλοκότητά τους, που συχνά συνίστανται στην εκμετάλλευση υπηρεσιών, υλικού και λογισμικού τρίτων για την υπονόμευση ενός τελικού στόχου, είναι δύσκολο να αντιμετωπιστεί το συλλογικό περιβάλλον απειλών της ΕΕ χωρίς συστηματική και ολοκληρωμένη ανταλλαγή πληροφοριών και συνεργασία για κοινή αντίδραση. Η ΕΕ επιδιώκει, **μέσω της πλήρους αξιοποίησης των ρυθμιστικών εργαλείων, της κινητοποίησης και της συνεργασίας**, να στηρίξει τα κράτη μέλη στην προστασία των πολιτών τους, καθώς και των οικονομικών τους συμφερόντων και των συμφερόντων εθνικής ασφάλειας, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων και ελευθεριών και του κράτους δικαίου. Διάφορες κοινότητες, αποτελούμενες από δίκτυα, θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ, καθώς και αρχές των κρατών μελών, είναι υπεύθυνες για την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση των κυβερνοαπειλών, χρησιμοποιώντας τα οικεία μέσα και τις οικείες πρωτοβουλίες[74]. Οι κοινότητες αυτές περιλαμβάνουν: i) αρχές NIS, όπως οι CSIRT, και την αντιμετώπιση καταστροφών· ii) αρχές επιβολής του νόμου και δικαστικές αρχές· iii) την κυβερνοδιπλωματία· και iv) την κυβερνοάμυνα.

2.1 Μια Κοινή Μονάδα Κυβερνοχώρου

Μια Κοινή Μονάδα Κυβερνοχώρου θα μπορούσε να χρησιμεύσει ως εικονική και φυσική πλατφόρμα συνεργασίας για τις διάφορες κοινότητες κυβερνοασφάλειας της ΕΕ, με έμφαση στον επιχειρησιακό και τεχνικό συντονισμό για την αντιμετώπιση σοβαρών διασυνοριακών κυβερνοπεριστατικών και κυβερνοαπειλών**.**

Η Κοινή Μονάδα Κυβερνοχώρου θα αποτελέσει σημαντικό βήμα προς την ολοκλήρωση του **ευρωπαϊκού πλαισίου για τη διαχείριση κρίσεων κυβερνοασφάλειας**. Όπως περιγράφεται στις πολιτικές κατευθυντήριες γραμμές της Προέδρου της Επιτροπής[75], η μονάδα αυτή θα πρέπει να δώσει στα κράτη μέλη και στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ

[74]Συμπεριλαμβανομένων της υποστήριξης του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) για την επιχειρησιακή συνεργασία και τη διαχείριση κρίσεων· του δικτύου CSIRT· του δικτύου CyCLONe (δίκτυο οργανώσεων διασύνδεσης για τις κρίσεις στον κυβερνοχώρο, που θα μετονομαστεί σε EU-CyCLONe, όπως προτείνεται στο πλαίσιο της αναθεωρημένης οδηγίας NIS)· της ομάδας συνεργασίας NIS· του «rescEU»· του Ευρωπαϊκού Κέντρου για τα εγκλήματα στον κυβερνοχώρο και της κοινής ομάδας δράσης για το κυβερνοέγκλημα της Ευρωπόλ, καθώς και του πρωτοκόλλου αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου· του κέντρου ανάλυσης πληροφοριών της ΕΕ (EU INTCEN) και της εργαλειοθήκης για την κυβερνοδιπλωματία· της Ενιαίας Ικανότητας Ανάλυσης Πληροφοριών (SIAC)· και των έργων που σχετίζονται με τον κυβερνοχώρο στο πλαίσιο της μόνιμης διαρθρωμένης συνεργασίας (PESCO), ιδίως το έργο «Ομάδες ταχείας αντίδρασης στον κυβερνοχώρο και αμοιβαία συνδρομή στην κυβερνοασφάλεια» (CRRT).

[75]«Μια Ένωση που επιδιώκει περισσότερα: Το πρόγραμμά μου για την Ευρώπη», πολιτικές κατευθύνσεις για την επόμενη Ευρωπαϊκή Επιτροπή 2019-2024 της υποψήφιας προέδρου της Ευρωπαϊκής Επιτροπής Ursula von der Leyen.

τη δυνατότητα να αξιοποιούν πλήρως υφιστάμενες δομές, πόρους και ικανότητες και να προάγει μια νοοτροπία «**ανάγκης για ανταλλαγή**». Θα παράσχει τα μέσα για την εδραίωση της προόδου που έχει σημειωθεί μέχρι στιγμής στο πλαίσιο της εφαρμογής της σύστασης του 2017 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (προσχέδιο)[76]. Θα παράσχει επίσης την ευκαιρία να ενισχυθεί περαιτέρω η συνεργασία γύρω από την αρχιτεκτονική του προσχεδίου και να αξιοποιηθεί η πρόοδος που έχει επιτευχθεί ιδίως στο πλαίσιο της ομάδας συνεργασίας NIS και του δικτύου CyCLONe.

Με τον τρόπο αυτό θα μπορούσαν να αντιμετωπιστούν **δύο βασικά κενά**, τα οποία επί του παρόντος αυξάνουν τα τρωτά σημεία και δημιουργούν ανεπάρκειες στην αντιμετώπιση διασυνοριακών απειλών και περιστατικών που επηρεάζουν την Ένωση. Πρώτον, οι μη στρατιωτικές, διπλωματικές, αστυνομικές και αμυντικές **κοινότητες** κυβερνοασφάλειας δεν διαθέτουν ακόμη κοινό χώρο για την προώθηση της διαρθρωμένης συνεργασίας και τη διευκόλυνση της επιχειρησιακής και τεχνικής συνεργασίας. Δεύτερον, οι ενδιαφερόμενοι φορείς στον τομέα της κυβερνοασφάλειας δεν έχουν κατορθώσει ακόμη να αξιοποιήσουν πλήρως τις **δυνατότητες** της επιχειρησιακής συνεργασίας και της αμοιβαίας συνδρομής στο πλαίσιο των υφιστάμενων δικτύων και κοινοτήτων. Σ' αυτό προστίθεται και το γεγονός ότι δεν υφίσταται κάποια πλατφόρμα που να επιτρέπει την επιχειρησιακή συνεργασία με τον ιδιωτικό τομέα. Η μονάδα θα πρέπει να βελτιώσει και να επιταχύνει τον συντονισμό και να επιτρέψει στην ΕΕ να αντιμετωπίζει και να αντιδρά σε κυβερνοπεριστατικά και κυβερνοκρίσεις μεγάλης κλίμακας.

Η Κοινή Μονάδα Κυβερνοχώρου δεν θα είναι ένας πρόσθετος, αυτόνομος φορέας, ούτε θα επηρεάζει τις αρμοδιότητες και τις εξουσίες των εθνικών αρχών κυβερνοασφάλειας ή των συμμετεχόντων της ΕΕ. Αντιθέτως, θα λειτουργεί ως μηχανισμός ασφαλείας, στο πλαίσιο του οποίου οι συμμετέχοντες θα μπορούν να στηρίζονται στην υποστήριξη και την εμπειρογνωσία των υπολοίπων, ιδίως σε περιπτώσεις που οι διάφορες κυβερνοκοινότητες πρέπει να συνεργάζονται στενά. Ταυτόχρονα, τα πρόσφατα γεγονότα καταδεικνύουν την ανάγκη να αυξήσει η ΕΕ το επίπεδο φιλοδοξίας και την ετοιμότητά της για να αντιμετωπίσει το τοπίο και την πραγματικότητα των κυβερνοαπειλών. Επομένως, στο πλαίσιο της συμβολής τους στην Κοινή Μονάδα Κυβερνοχώρου, οι φορείς της ΕΕ (η Επιτροπή και οι οργανισμοί και τα όργανα της ΕΕ) θα είναι έτοιμοι να αυξήσουν σημαντικά τους πόρους και τις ικανότητές τους, ώστε να ενισχύσουν την ετοιμότητα και ανθεκτικότητά τους.

Η Κοινή Μονάδα Κυβερνοχώρου θα εκπληρώσει τρεις κύριους στόχους. Πρώτον, θα διασφαλίσει την **ετοιμότητα** όλων των κοινοτήτων κυβερνοασφάλειας· δεύτερον, μέσω της ανταλλαγής πληροφοριών, θα παρέχει συνεχή και κοινή **επίγνωση** της κατάστασης· και τρίτον, θα ενισχύσει τη συντονισμένη **αντίδραση** και ανάκαμψη. Για την επίτευξη των στόχων αυτών, η μονάδα θα πρέπει να βασιστεί σε σαφώς καθορισμένα **δομικά στοιχεία και στόχους**, όπως η εγγύηση **ασφαλούς και ταχείας ανταλλαγής πληροφοριών**, η βελτίωση της **συνεργασίας** μεταξύ των συμμετεχόντων, συμπεριλαμβανομένης της αλληλεπίδρασης μεταξύ των κρατών μελών και των σχετικών οντοτήτων της ΕΕ, η σύναψη δομημένων **εταιρικών σχέσεων με αξιόπιστη βιομηχανική βάση** και η διευκόλυνση συντονισμένης προσέγγισης για τη **συνεργασία με εξωτερικούς εταίρους**. Για τον σκοπό αυτό, με βάση τη χαρτογράφηση των διαθέσιμων ικανοτήτων σε εθνικό και ενωσιακό επίπεδο, η μονάδα θα μπορούσε να διευκολύνει την ανάπτυξη ενός πλαισίου συνεργασίας.

[76]Σύσταση C(2017) 6100 final της 13.9.2017 για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

Για να καταστεί η Κοινή Μονάδα Κυβερνοχώρου ο πυρήνας της επιχειρησιακής συνεργασίας της ΕΕ στον τομέα της κυβερνοασφάλειας, η Επιτροπή θα συνεργαστεί με τα κράτη μέλη και τα σχετικά θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ, συμπεριλαμβανομένων του ENISA, της CERT-EU και της Ευρωπόλ, για την προώθηση μιας **σταδιακής και χωρίς αποκλεισμούς προσέγγισης**, με πλήρη σεβασμό των αρμοδιοτήτων και των εντολών όλων των εμπλεκομένων. Σύμφωνα με την προσέγγιση αυτή, η μονάδα θα μπορούσε να συνεισφέρει στην περαιτέρω συνεργασία μεταξύ των συστατικών μερών μιας συγκεκριμένης κοινότητας κυβερνοασφάλειας, εφόσον τα εν λόγω συστατικά μέρη το κρίνουν απαραίτητο.

Για τη δημιουργία της Κοινής Μονάδας Κυβερνοχώρου προτείνονται τέσσερα βασικά στάδια:

- *Καθορισμός*, μέσω της χαρτογράφησης των διαθέσιμων ικανοτήτων σε εθνικό και ενωσιακό επίπεδο·
- *Προετοιμασία*, μέσω της θέσπισης πλαισίου διαρθρωμένης συνεργασίας και συνδρομής·
- *Ανάπτυξη*, μέσω της εφαρμογής του πλαισίου, με βάση τους πόρους που παρέχουν οι συμμετέχοντες, έτσι ώστε να καταστεί επιχειρησιακή η Κοινή Μονάδα Κυβερνοχώρου·
- *Επέκταση*, μέσω της ενίσχυσης της συντονισμένης ικανότητας αντίδρασης με τη συμβολή του κλάδου και των εταίρων.

Η Επιτροπή, βασιζόμενη στα αποτελέσματα της διαβούλευσης με τα κράτη μέλη, τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ[77], και με τη συμμετοχή του ύπατου εκπροσώπου σύμφωνα με τις αρμοδιότητές του, θα παρουσιάσει έως τον Φεβρουάριο του 2021 τη διαδικασία, τα ορόσημα και το χρονοδιάγραμμα για τον **καθορισμό, την προετοιμασία, την ανάπτυξη και την επέκταση της Κοινής Μονάδας Κυβερνοχώρου**.

2.2 Καταπολέμηση του κυβερνοεγκλήματος

Η εξάρτησή μας από τα διαδικτυακά εργαλεία έχει αυξήσει εκθετικά την επιφάνεια έκθεσής μας σε επιθέσεις από κυβερνοεγκληματίες και έχει διαμορφώσει μια κατάσταση στην οποία η διερεύνηση σχεδόν όλων των τύπων εγκλημάτων περιέχει μια ψηφιακή συνιστώσα. Επιπλέον, οι δράστες κυβερνοεγκλημάτων και όσοι χρησιμοποιούν εργαλεία του κυβερνοχώρου για τον σχεδιασμό και την εκτέλεση των παράνομων ενεργειών τους απειλούν βασικά τμήματα της κοινωνίας μας. Ως εκ τούτου, υπάρχουν στενοί δεσμοί με τη γενική πολιτική ασφάλειας της ΕΕ, όπως αντικατοπτρίζεται στα σχετικά με την κυβερνοασφάλεια στοιχεία που περιέχονται στη στρατηγική της ΕΕ του 2020 για την Ένωση Ασφάλειας και στο θεματολόγιο της ΕΕ για την καταπολέμηση της τρομοκρατίας[78].

Η αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος αποτελεί βασικό παράγοντα για τη διασφάλιση της κυβερνοασφάλειας: η αποτροπή δεν μπορεί να επιτευχθεί μόνο μέσω της

[77]Η διαβούλευση με τα κράτη μέλη (μεταξύ άλλων κατά την άσκηση Blue OLEx20, η οποία έφερε σε επαφή τους επικεφαλής των εθνικών αρχών κυβερνοασφάλειας) και με τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ πραγματοποιήθηκε μεταξύ Ιουλίου και Νοεμβρίου 2020.

[78]Ανακοίνωση με τίτλο «Θεματολόγιο της ΕΕ για την καταπολέμηση της τρομοκρατίας: πρόβλεψη, πρόληψη, προστασία και αντιμετώπιση» της 9.12.2020, COM(2020) 795 final.

ανθεκτικότητας· απαιτεί επίσης τον εντοπισμό και την ποινική δίωξη των δραστών. Επομένως, είναι σημαντικό να ενισχυθούν η συνεργασία και οι ανταλλαγές μεταξύ των παραγόντων κυβερνοασφάλειας και των αρχών επιβολής του νόμου. Ως εκ τούτου, σε επίπεδο ΕΕ, η Ευρωπόλ και ο ENISA έχουν ήδη αναπτύξει ισχυρή συνεργασία, στο πλαίσιο της οποίας έχουν διοργανώσει κοινές διασκέψεις και εργαστήρια και έχουν υποβάλει κοινές εκθέσεις στην Επιτροπή, στα κράτη μέλη και σε άλλους ενδιαφερόμενους φορείς σχετικά με τις απειλές και τις τεχνολογικές προκλήσεις στον τομέα της κυβερνοασφάλειας. Η Επιτροπή θα συνεχίσει να υποστηρίζει αυτή την ολοκληρωμένη προσέγγιση για τη διασφάλιση συνεκτικής και αποτελεσματικής αντίδρασης, βασιζόμενης σε μια ολοκληρωμένη εικόνα πληροφοριών.

Ως σημαντικό στοιχείο της εν λόγω αντίδρασης, οι αρχές της ΕΕ και των κρατών μελών πρέπει να επεκτείνουν και να βελτιώσουν την ικανότητα των αρχών επιβολής του νόμου να διερευνούν τα κυβερνοεγκλήματα, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων και επιδιώκοντας την απαιτούμενη ισορροπία μεταξύ των διαφόρων δικαιωμάτων και συμφερόντων. Η ΕΕ θα πρέπει να είναι σε θέση να αντιμετωπίσει το κυβερνοέγκλημα χάρη στην πλήρη εφαρμογή νομοθεσίας κατάλληλης για τον επιδιωκόμενο σκοπό, με ιδιαίτερη έμφαση στην καταπολέμηση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο και στις ψηφιακές έρευνες, συμπεριλαμβανομένης της εγκληματικότητας στο «σκοτεινό δίκτυο» (darknet). Οι αρχές επιβολής του νόμου πρέπει να είναι πλήρως εξοπλισμένες για τη διεξαγωγή ψηφιακών ερευνών. Ως εκ τούτου, η Επιτροπή θα υποβάλει σχέδιο δράσης για τη βελτίωση της ψηφιακής ικανότητας των υπηρεσιών επιβολής του νόμου, με την παροχή σε αυτές των αναγκαίων δεξιοτήτων και εργαλείων. Επιπλέον, η Ευρωπόλ θα αναπτύξει περαιτέρω τον ρόλο της ως κέντρου εμπειρογνωσίας για την υποστήριξη των εθνικών αρχών επιβολής του νόμου στην καταπολέμηση του εγκλήματος που διευκολύνεται ή εξαρτάται από τον κυβερνοχώρο, συμβάλλοντας με τον τρόπο αυτόν στον καθορισμό κοινών εγκληματολογικών προτύπων (μέσω του εργαστηρίου καινοτομίας και του κόμβου της Ευρωπόλ). Όλες αυτές οι δραστηριότητες πρέπει να υιοθετηθούν με κατάλληλο τρόπο από τα κράτη μέλη, τα οποία ενθαρρύνονται να χρησιμοποιούν τα εθνικά προγράμματα του Ταμείου Εσωτερικής Ασφάλειας και να προτείνουν έργα τα οποία ανταποκρίνονται στις προσκλήσεις υποβολής προτάσεων στο πλαίσιο του θεματικού μέσου.

Η Επιτροπή θα χρησιμοποιήσει όλα τα κατάλληλα μέσα, συμπεριλαμβανομένων των διαδικασιών επί παραβάσει, ώστε να διασφαλίσει την πλήρη μεταφορά και εφαρμογή της οδηγίας του 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών[79], συμπεριλαμβανομένης της παροχής στατιστικών στοιχείων από τα κράτη μέλη. Θα φροντίσει να αποτρέψει με τον καλύτερο δυνατόν τρόπο την κατάχρηση των ονομάτων τομέα, μεταξύ άλλων όσον αφορά τη διανομή παράνομου περιεχομένου, και θα επιδιώξει να εξασφαλίσει τη διαθεσιμότητα ακριβών δεδομένων καταχώρισης, συνεχίζοντας να συνεργάζεται με το Σώμα του Διαδικτύου για την Εκχώρηση Ονομάτων και Αριθμών (ICANN) και με άλλους ενδιαφερόμενους φορείς του συστήματος διακυβέρνησης του διαδικτύου, ιδίως μέσω της ομάδας εργασίας για τη δημόσια ασφάλεια της Κυβερνητικής Συμβουλευτικής Επιτροπής του ICANN. Η πρόταση στο πλαίσιο της αναθεωρημένης οδηγίας NIS προβλέπει επομένως να τηρούνται ακριβείς και πλήρεις βάσεις δεδομένων ονομάτων τομέα και δεδομένων καταχώρισης, ή «δεδομένων WHOIS», και να παρέχεται νόμιμη πρόσβαση στα εν λόγω

[79]Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών.

δεδομένα, τα οποία είναι απαραίτητα για την εγγύηση της ασφάλειας, της σταθερότητας και της ανθεκτικότητας του συστήματος ονομάτων τομέα (DNS).

Η Επιτροπή θα εξακολουθήσει επίσης να καταβάλλει προσπάθειες για την παροχή κατάλληλων διαύλων και την αποσαφήνιση των κανόνων σχετικά με τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία για ποινικές έρευνες (τα οποία απαιτούνται στο 85 % των ερευνών, ενώ το 65 % των συνολικών αιτήσεων απευθύνεται σε παρόχους που εδρεύουν σε άλλη δικαιοδοσία), διευκολύνοντας την έγκριση και την επακόλουθη εφαρμογή της «δέσμης μέτρων για τα ηλεκτρονικά αποδεικτικά στοιχεία» και πρακτικών μέτρων[80]. Η ταχεία έγκριση των προτάσεων για τα ηλεκτρονικά αποδεικτικά στοιχεία από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο είναι καίριας σημασίας για την παροχή ενός αποτελεσματικού εργαλείου στους επαγγελματίες του τομέα. Τα ηλεκτρονικά αποδεικτικά στοιχεία πρέπει να είναι αναγνώσιμα και, ως εκ τούτου, η Επιτροπή θα συνεχίσει τις εργασίες της για τη στήριξη της ικανότητας των υπηρεσιών επιβολής του νόμου στον τομέα των ψηφιακών ερευνών, καθώς και για τη διαχείριση της κρυπτογράφησης κατά τις ποινικές έρευνες, φροντίζοντας να διαφυλαχθεί πλήρως η λειτουργία της κρυπτογράφησης για την προστασία των θεμελιωδών δικαιωμάτων και της κυβερνοασφάλειας.

2.3 Εργαλειοθήκη της ΕΕ για την κυβερνοδιπλωματία

Η ΕΕ χρησιμοποιεί την **εργαλειοθήκη της για την κυβερνοδιπλωματία**[81] με σκοπό την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. Μετά τη θέσπιση, τον Μάιο του 2019, του νομικού πλαισίου για την επιβολή στοχευμένων περιοριστικών μέτρων κατά κυβερνοεπιθέσεων[82], η ΕΕ επέβαλε κυρώσεις, τον Ιούλιο του 2020, στο πλαίσιο του εν λόγω καθεστώτος, σε έξι πρόσωπα και σε τρεις οντότητες που ευθύνονται για κυβερνοεπιθέσεις που έπληξαν την ΕΕ και τα κράτη μέλη της ή που συμμετείχαν σε τέτοιες επιθέσεις[83]. Τον Οκτώβριο του 2020 καταχωρίστηκαν στον κατάλογο άλλα δύο πρόσωπα και ένας φορέας[84]. Οι κακόβουλες δραστηριότητες στον κυβερνοχώρο, συμπεριλαμβανομένων των δραστηριοτήτων βραδείας

[80]COM(2018) 225 και 226· C(2020) 2779 final. Ειδικότερα, το έργο SIRIUS έλαβε πρόσφατα πρόσθετη χρηματοδότηση στο πλαίσιο του μέσου εταιρικής σχέσης για τη βελτίωση των διαύλων νόμιμης διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία για ποινικές έρευνες (τα οποία απαιτούνται στο 85 % των ερευνών για σοβαρά εγκλήματα, ενώ το 65 % των συνολικών αιτήσεων απευθύνεται σε παρόχους που εδρεύουν σε άλλη δικαιοδοσία), και για τη θέσπιση συμβατών κανόνων σε διεθνές επίπεδο.

[81] https://www.consilium.europa.eu/el/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82]Απόφαση (ΚΕΠΠΑ) 2019/797 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 13)· και κανονισμός (ΕΕ) 2019/796 του Συμβουλίου,
της 17ης Μαΐου 2019, σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 1).

[83]Απόφαση (ΚΕΠΠΑ) 2020/1127 του Συμβουλίου, της 30ής Ιουλίου 2020, για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ST/9564/2020/INIT) (ΕΕ L 246 της 30.7.2020, σ. 12-17)· και εκτελεστικός κανονισμός (ΕΕ) 2020/1125 του Συμβουλίου, της 30ής Ιουλίου 2020, για την εφαρμογή του κανονισμού (ΕΕ) 2019/796 σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ST/9568/2020/INIT) (ΕΕ L 246 της 30.7.2020, σ. 4-9).

[84] Απόφαση (ΚΕΠΠΑ) 2020/1537 του Συμβουλίου, της 22ας Οκτωβρίου 2020, για την τροποποίηση της απόφασης (ΚΕΠΠΑ) 2019/797 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 351 I της 22.10.2020, σ. 5-7)· και εκτελεστικός κανονισμός (ΕΕ) 2020/1536 του Συμβουλίου, της 22ας Οκτωβρίου 2020, για την εφαρμογή του κανονισμού (ΕΕ) 2019/796 σχετικά με περιοριστικά μέτρα κατά κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 351 I της 22.10.2020, σ. 1-4).

εξέλιξης, θα πρέπει να καταπολεμούνται μέσω αποτελεσματικής και ολοκληρωμένης κοινής διπλωματικής αντίδρασης της ΕΕ, χρησιμοποιώντας όλα τα μέτρα που είναι διαθέσιμα σε επίπεδο ΕΕ.

Για μια ταχεία και αποτελεσματική κοινή διπλωματική αντίδραση της ΕΕ απαιτείται ισχυρή και κοινή επίγνωση της κατάστασης, καθώς και η ικανότητα ταχείας εκπόνησης κοινής θέσης της ΕΕ. Ο ύπατος εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας θα ενθαρρύνει και θα διευκολύνει τη σύσταση **ομάδας εργασίας των κρατών μελών για τις κυβερνοπληροφορίες**,στο πλαίσιο του κέντρου ανάλυσης πληροφοριών της ΕΕ (INTCEN), για την προώθηση της στρατηγικής συνεργασίας όσον αφορά τις πληροφορίες σχετικά με τις κυβερνοαπειλές και άλλες δραστηριότητες στον κυβερνοχώρο. Οι εργασίες της ομάδας θα ενισχύσουν περαιτέρω την επίγνωση της κατάστασης σε επίπεδο ΕΕ και την ικανότητα λήψης αποφάσεων για κοινή διπλωματική αντίδραση. Η ομάδα εργασίας θα συνεργάζεται με υφιστάμενες δομές[85], συμπεριλαμβανομένων, όπου απαιτείται, εκείνων που καλύπτουν την ευρύτερη απειλή υβριδικών και ξένων παρεμβάσεων, για να συγκεντρώσει πληροφορίες και να εκτιμήσει την κατάσταση.

Για να ενισχύσει την ικανότητά της να προλαμβάνει, να αποθαρρύνει, να αποτρέπει και να αντιμετωπίζει κακόβουλες συμπεριφορές στον κυβερνοχώρο, ο ύπατος εκπρόσωπος, με τη συμμετοχή της Επιτροπής σύμφωνα με τις αρμοδιότητές της, θα υποβάλει πρόταση για τον περαιτέρω καθορισμό της **θέσης της ΕΕ για την κυβερνοαποτροπή**. Με βάση το έργο που έχει επιτελεστεί μέχρι στιγμής στο πλαίσιο της εργαλειοθήκης για την κυβερνοδιπλωματία, η θέση αυτή θα πρέπει να συμβάλει στην υπεύθυνη συμπεριφορά και συνεργασία των κρατών στον κυβερνοχώρο και να παράσχει ιδιαίτερη κατεύθυνση για την καταπολέμηση των κυβερνοεπιθέσεων που προκαλούν τον μεγαλύτερο αντίκτυπο, ιδίως εκείνων που επηρεάζουν τις υποδομές ζωτικής σημασίας, τους δημοκρατικούς θεσμούς και τις δημοκρατικές διαδικασίες μας[86], καθώς και των επιθέσεων στις αλυσίδες εφοδιασμού και της κλοπής διανοητικής ιδιοκτησίας που διευκολύνεται από τον κυβερνοχώρο. Η στάση αυτή θα πρέπει να περιγράφει τον τρόπο με τον οποίο η ΕΕ και τα κράτη μέλη θα μπορούσαν να αξιοποιήσουν τα εργαλεία τους σε επίπεδο πολιτικής, οικονομίας, διπλωματίας, νομικού πλαισίου και στρατηγικής επικοινωνίας έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο, καθώς και τον τρόπο με τον οποίο η ΕΕ και τα κράτη μέλη θα μπορούσαν να ενισχύσουν την ικανότητά τους να καταλογίζουν ευθύνες για κακόβουλες δραστηριότητες στον κυβερνοχώρο. Επιπλέον, ο ύπατος εκπρόσωπος, από κοινού με το Συμβούλιο και την Επιτροπή, σκοπεύει να εξετάσει **πρόσθετα μέτρα στο πλαίσιο της εργαλειοθήκης για την κυβερνοδιπλωματία**, συμπεριλαμβανομένης της δυνατότητας περαιτέρω επιλογών για περιοριστικά μέτρα, καθώς και της δυνατότητας **ψηφοφορίας με ειδική πλειοψηφία για καταχωρίσεις στο πλαίσιο του καθεστώτος οριζόντιων κυρώσεων κατά των κυβερνοεπιθέσεων.** Επιπλέον, η ΕΕ θα πρέπει να καταβάλει περαιτέρω προσπάθειες για την **ενίσχυση της συνεργασίας με διεθνείς εταίρους**, συμπεριλαμβανομένου του ΝΑΤΟ, ώστε να προωθηθεί η επίτευξη κοινής αντίληψης του τοπίου των απειλών, να αναπτυχθούν μηχανισμοί συνεργασίας και να προσδιοριστούν συνεργατικές διπλωματικές αντιδράσεις.

[85]Όπως η Ενιαία Ικανότητα Ανάλυσης Πληροφοριών (SIAC) της ΕΕ και, όπου απαιτείται, τα σχετικά έργα που καταρτίζονται στο πλαίσιο της PESCO, καθώς και το σύστημα έγκαιρης προειδοποίησης (RAS) του 2018, το οποίο έχει δημιουργηθεί για να στηρίζει τη συνολική προσέγγιση της ΕΕ για την αντιμετώπιση της παραπληροφόρησης.

[86] Ιδίως μέσω της επιδίωξης συνεργειών με τις πρωτοβουλίες στο πλαίσιο του ευρωπαϊκού σχεδίου δράσης για τη δημοκρατία.

Ο ύπατος εκπρόσωπος, με τη συμμετοχή της Επιτροπής, θα προτείνει επίσης την επικαιροποίηση των **κατευθυντήριων γραμμών εφαρμογής της εργαλειοθήκης για την κυβερνοδιπλωματία**[87], μεταξύ άλλων με σκοπό την αύξηση της αποδοτικότητας της διαδικασίας λήψης αποφάσεων, και θα εξακολουθήσει να διοργανώνει ασκήσεις καθώς και αξιολογήσεις της εργαλειοθήκης για την κυβερνοδιπλωματία σε τακτική βάση. Επιπλέον, η ΕΕ θα πρέπει να **ενσωματώσει περαιτέρω την εργαλειοθήκη για την κυβερνοδιπλωματία στους μηχανισμούς αντιμετώπισης κρίσεων της ΕΕ** και να επιδιώξει συνέργειες με τις προσπάθειες για την καταπολέμηση των υβριδικών απειλών, της παραπληροφόρησης και των ξένων παρεμβάσεων υπό το κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών[88] και το ευρωπαϊκό σχέδιο δράσης για τη δημοκρατία. Στο πλαίσιο αυτό, η ΕΕ θα πρέπει να εξετάσει την αλληλεπίδραση μεταξύ της εργαλειοθήκης για την κυβερνοδιπλωματία και της πιθανής χρήσης του άρθρου 42 παράγραφος 7 της ΣΕΕ και του άρθρου 222 της ΣΛΕΕ[89].

2.4 Ενίσχυση των ικανοτήτων κυβερνοάμυνας

Η ΕΕ και τα κράτη μέλη πρέπει να αυξήσουν την ικανότητά τους όσον αφορά την πρόληψη και την αντιμετώπιση κυβερνοαπειλών, σύμφωνα με το επίπεδο φιλοδοξίας της ΕΕ που απορρέει από τη συνολική στρατηγική της ΕΕ του 2016[90]. Για τον σκοπό αυτόν, ο ύπατος εκπρόσωπος, σε συνεργασία με την Επιτροπή, θα παρουσιάσει την **επανεξέταση του πλαισίου πολιτικής για την κυβερνοάμυνα (CDPF)** προκειμένου να ενισχυθούν ο συντονισμός και η συνεργασία μεταξύ των παραγόντων της ΕΕ[91], καθώς και με τα κράτη μέλη και μεταξύ αυτών, όσον αφορά επίσης θέματα όπως οι αποστολές και οι επιχειρήσεις της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ). Το πλαίσιο πολιτικής για την κυβερνοάμυνα θα πρέπει να αποτελέσει τη βάση για τον επικείμενο στρατηγικό προσανατολισμό[92], διασφαλίζοντας ότι η κυβερνοασφάλεια και η κυβερνοάμυνα θα ενσωματωθούν περισσότερο στο ευρύτερο θεματολόγιο για την ασφάλεια και την άμυνα.

Το 2018 η ΕΕ χαρακτήρισε τον κυβερνοχώρο ως πεδίο επιχειρήσεων[93]. Το επικείμενο **«Στρατιωτικό όραμα και στρατηγική για τον κυβερνοχώρο ως πεδίο επιχειρήσεων»** της Στρατιωτικής Επιτροπής της ΕΕ θα πρέπει να καθορίσει περαιτέρω τον τρόπο με τον οποίο ο κυβερνοχώρος, ως πεδίο επιχειρήσεων, καθιστά δυνατές τις στρατιωτικές αποστολές και επιχειρήσεις ΚΠΑΑ της ΕΕ. Το **δίκτυο στρατιωτικών CERT**[94], που θα δημιουργηθεί από τον Ευρωπαϊκό Οργανισμό Άμυνας (ΕΟΑ), θα συμβάλει περαιτέρω στη σημαντική αύξηση της συνεργασίας μεταξύ των κρατών μελών. Επιπλέον, για να διασφαλιστεί η κυβερνοασφάλεια των διαστημικών υποδομών ζωτικής σημασίας υπό την ευθύνη του διαστημικού προγράμματος, θα ενισχυθεί ο ευρωπαϊκός οργανισμός για το διαστημικό πρόγραμμα, ιδίως το κέντρο παρακολούθησης της ασφάλειας του Galileo, και η εντολή του θα επεκταθεί και σε άλλους κρίσιμους πόρους του διαστημικού προγράμματος.

---

[87] 13007/17.

[88] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[89] Η ρήτρα αμοιβαίας άμυνας και η ρήτρα αλληλεγγύης, αντίστοιχα.

[90] Συμπεράσματα του Συμβουλίου (14149/16) σχετικά με την εφαρμογή της συνολικής στρατηγικής της ΕΕ στον τομέα της ασφάλειας και της άμυνας.

[91] Κυρίως μεταξύ της ΕΥΕΔ, συμπεριλαμβανομένου του Στρατιωτικού Επιτελείου της ΕΕ (EUMS), της Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας (ΕΑΑΑ), της Επιτροπής και των οργανισμών της ΕΕ, ιδίως του Ευρωπαϊκού Οργανισμού Άμυνας (ΕΟΑ).

[92] Συμπεράσματα του Συμβουλίου για την ασφάλεια και την άμυνα, της 17ης Ιουνίου 2020 (8910/20)

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/el/pdf

[94] Η σύσταση ενός δικτύου στρατιωτικών CERT της ΕΕ ανταποκρίνεται σε έναν στόχο που προσδιορίζεται στο πλαίσιο πολιτικής για την κυβερνοάμυνα του 2018 και αποσκοπεί στην προώθηση της ενεργού αλληλεπίδρασης και της ανταλλαγής πληροφοριών μεταξύ των στρατιωτικών CERT των κρατών μελών της ΕΕ.

Η ΕΕ και τα κράτη μέλη θα πρέπει να δώσουν περαιτέρω ώθηση στην **ανάπτυξη υπερσύγχρονων ικανοτήτων κυβερνοάμυνας** μέσω διαφόρων πολιτικών και μέσων της ΕΕ, ιδίως μέσω του πλαισίου πολιτικής για την κυβερνοάμυνα και, κατά περίπτωση, αξιοποιώντας το έργο του ΕΟΑ. Για να επιτευχθεί αυτό απαιτείται ιδιαίτερη έμφαση στην ανάπτυξη και τη χρήση βασικών τεχνολογιών, όπως η τεχνητή νοημοσύνη, η κρυπτογράφηση και η κβαντική υπολογιστική. Σύμφωνα με τις προτεραιότητες ανάπτυξης δυνατοτήτων της ΕΕ του 2018[95] και με βάση τα πορίσματα της πρώτης πλήρους έκθεσης για τη συντονισμένη ετήσια επανεξέταση στον τομέα της άμυνας[96], η ΕΕ θα πρέπει να προωθήσει τη συνεργασία μεταξύ των κρατών μελών όσον αφορά **την έρευνα, την καινοτομία και την ανάπτυξη ικανοτήτων στον τομέα της κυβερνοάμυνας**, ενθαρρύνοντας τα κράτη μέλη να αξιοποιήσουν το πλήρες δυναμικό της **μόνιμης διαρθρωμένης συνεργασίας (PESCO)[97]** και **του Ευρωπαϊκού Ταμείου Άμυνας[98].**

Το προσεχές **σχέδιο δράσης της Επιτροπής για τις συνέργειες μεταξύ πολιτικών, αμυντικών και διαστημικών βιομηχανιών**, το οποίο θα παρουσιαστεί το πρώτο τρίμηνο του 2021, θα συμπεριλάβει δράσεις για την περαιτέρω στήριξη συνεργειών σε επίπεδο προγραμμάτων, τεχνολογιών, καινοτομίας και νεοφυών επιχειρήσεων, σύμφωνα με τη διακυβέρνηση των αντίστοιχων προγραμμάτων[99].

Επιπλέον, θα πρέπει να αναπτυχθούν σχετικές συνέργειες και διεπαφές μεταξύ των πρωτοβουλιών κυβερνοάμυνας που υλοποιούνται σε άλλα πλαίσια, συμπεριλαμβανομένων των συνεργατικών έργων που σχετίζονται με τον κυβερνοχώρο[100] και πραγματοποιούνται από τα κράτη μέλη στο πλαίσιο της PESCO, καθώς και με τις δομές της ΕΕ για την κυβερνοασφάλεια, με σκοπό την υποστήριξη της ανταλλαγής πληροφοριών και της αμοιβαίας υποστήριξης.

Στρατηγικές πρωτοβουλίες

Η ΕΕ θα πρέπει:

- να ολοκληρώσει το ευρωπαϊκό πλαίσιο διαχείρισης κρίσεων κυβερνοασφάλειας και να καθορίσει τη διαδικασία, τα ορόσημα και το χρονοδιάγραμμα για τη σύσταση της Κοινής Μονάδας Κυβερνοχώρου·
- να εξακολουθήσει να εφαρμόζει το θεματολόγιο για το κυβερνοέγκλημα στο πλαίσιο της στρατηγικής για την Ένωση Ασφάλειας·

[95] Τον Ιούνιο του 2018 τα κράτη μέλη συμφώνησαν, στο διοικητικό συμβούλιο του ΕΟΑ, να καθοδηγήσουν την αμυντική συνεργασία σε επίπεδο ΕΕ.
[96] Εγκρίθηκε από τους υπουργούς Άμυνας στο διοικητικό συμβούλιο του ΕΟΑ τον Νοέμβριο του 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)
[97] Επί του παρόντος υπάρχουν διάφορα έργα PESCO που σχετίζονται με τον κυβερνοχώρο, και συγκεκριμένα η πλατφόρμα ανταλλαγής πληροφοριών για την αντιμετώπιση κυβερνοαπειλών και κυβερνοσυμβάντων, οι ομάδες ταχείας αντίδρασης στον κυβερνοχώρο και η αμοιβαία συνδρομή στην ασφάλεια στον κυβερνοχώρο, η ακαδημία για τον κυβερνοχώρο και κόμβος καινοτομίας της ΕΕ και το συντονιστικό κέντρο κυβερνοχώρου και χώρου πληροφοριών (CIDCC).
[98] Στο πλαίσιο του Ευρωπαϊκού Ταμείου Άμυνας, η Επιτροπή έχει ήδη εντοπίσει ευκαιρίες για δυνητικές συνεργατικές δράσεις έρευνας και ανάπτυξης στον τομέα της κυβερνοάμυνας, με στόχο την ενίσχυση της συνεργασίας, της ικανότητας καινοτομίας και της ανταγωνιστικότητας της αμυντικής βιομηχανίας.
[99] Όπως το πρόγραμμα «Ορίζων Ευρώπη», το πρόγραμμα «Ψηφιακή Ευρώπη» και το Ευρωπαϊκό Ταμείο Άμυνας.
[100] https://pesco.europa.eu/

- να ενθαρρύνει και να διευκολύνει τη σύσταση ομάδας εργασίας των κρατών μελών για τις κυβερνοπληροφορίες, εντός του πλαισίου του κέντρου ανάλυσης πληροφοριών της ΕΕ (EU INTCEN)·
- να προωθήσει τη θέση της ΕΕ για την κυβερνοαποτροπή με σκοπό την πρόληψη, την αποθάρρυνση, την αποτροπή και την αντιμετώπιση κακόβουλων κυβερνοδραστηριοτήτων·
- να επανεξετάσει το πλαίσιο πολιτικής για την κυβερνοάμυνα·
- να διευκολύνει την ανάπτυξη ενός «στρατιωτικού οράματος και μιας στρατηγικής για τον κυβερνοχώρο ως πεδίο επιχειρήσεων» για τις στρατιωτικές αποστολές και επιχειρήσεις της ΚΠΑΑ·
- να στηρίξει συνέργειες μεταξύ πολιτικών, αμυντικών και διαστημικών βιομηχανιών· και
- να ενισχύσει την κυβερνοασφάλεια των διαστημικών υποδομών ζωτικής σημασίας στο πλαίσιο του διαστημικού προγράμματος.

3. ΠΡΟΩΘΗΣΗ ΕΝΟΣ ΠΑΓΚΟΣΜΙΟΥ ΚΑΙ ΑΝΟΙΚΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

Η ΕΕ θα πρέπει να εξακολουθήσει να συνεργάζεται με τους διεθνείς εταίρους για την προώθηση ενός πολιτικού μοντέλου και ενός οράματος για τον κυβερνοχώρο βασισμένων στο κράτος δικαίου, στα ανθρώπινα δικαιώματα, στις θεμελιώδεις ελευθερίες και στις δημοκρατικές αξίες που επιφέρουν κοινωνική, οικονομική και πολιτική ανάπτυξη σε παγκόσμιο επίπεδο και συμβάλλουν σε μια Ένωση Ασφάλειας. Η διεθνής συνεργασία είναι ουσιαστικής σημασίας για να παραμένει ο κυβερνοχώρος παγκόσμιος, ανοικτός, σταθερός και ασφαλής. Για τον σκοπό αυτόν, η ΕΕ θα πρέπει να συνεχίσει να συνεργάζεται με τρίτες χώρες, με διεθνείς οργανισμούς και με την πολυσυμμετοχική κοινότητα προκειμένου να αναπτύξει και να εφαρμόσει μια συνεκτική και ολιστική διεθνή πολιτική για τον κυβερνοχώρο, λαμβάνοντας υπόψη την αυξανόμενη διασύνδεση μεταξύ των οικονομικών πτυχών των νέων τεχνολογιών, της εσωτερικής ασφάλειας, της εξωτερικής πολιτικής και της πολιτικής ασφάλειας και άμυνας. Η ΕΕ, ως ισχυρός οικονομικός και εμπορικός συνασπισμός που έχει ως θεμέλιο τις βασικές δημοκρατικές αξίες και τον σεβασμό του κράτους δικαίου και των θεμελιωδών δικαιωμάτων, βρίσκεται επίσης σε μοναδική θέση ώστε να πρωτοστατήσει στον καθορισμό και στην προώθηση διεθνών κανόνων και προτύπων.

3.1. Ηγετικός ρόλος της ΕΕ όσον αφορά τα πρότυπα, τους κανόνες και τα πλαίσια στον κυβερνοχώρο

Ενίσχυση της διεθνούς τυποποίησης

Για να προωθήσει και να υπερασπιστεί το όραμά της για τον κυβερνοχώρο σε διεθνές επίπεδο, η ΕΕ πρέπει να **ενισχύσει τη δέσμευσή της και τον ηγετικό της ρόλο όσον αφορά τις διαδικασίες διεθνούς τυποποίησης, καθώς και την εκπροσώπησή της σε διεθνείς και ευρωπαϊκούς οργανισμούς τυποποίησης και άλλους οργανισμούς ανάπτυξης προτύπων**[101]. Καθώς οι ψηφιακές τεχνολογίες αναπτύσσονται με ταχύ ρυθμό, τα διεθνή

[101]Π.χ. ο Διεθνής Οργανισμός Τυποποίησης (ISO), η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC), η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), η Ευρωπαϊκή Επιτροπή Τυποποίησης (CEN), η Ευρωπαϊκή Επιτροπή Ηλεκτροτεχνικής Τυποποίησης (CENELEC), το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI),

πρότυπα αποκτούν όλο και μεγαλύτερη σημασία για τη συμπλήρωση των παραδοσιακών ρυθμιστικών προσπαθειών σε τομείς όπως η τεχνητή νοημοσύνη, το υπολογιστικό νέφος, η κβαντική υπολογιστική και η κβαντική επικοινωνία. Η διεθνής τυποποίηση χρησιμοποιείται όλο και περισσότερο από τρίτες χώρες για την προώθηση του πολιτικού και ιδεολογικού τους προγράμματος, το οποίο συχνά δεν ανταποκρίνεται στις αξίες της ΕΕ. Επιπλέον, υπάρχει αυξανόμενος κίνδυνος λόγω ανταγωνιστικών πλαισίων διεθνούς τυποποίησης, που προκαλούν κατακερματισμό.

Η διαμόρφωση διεθνών προτύπων στους τομείς των αναδυόμενων τεχνολογιών και της βασικής αρχιτεκτονικής του διαδικτύου σύμφωνα με τις αξίες της ΕΕ είναι ουσιαστικής σημασίας προκειμένου να διασφαλιστεί ότι το διαδίκτυο παραμένει παγκόσμιο και ανοικτό, ότι οι τεχνολογίες είναι ανθρωποκεντρικές, εστιασμένες στην προστασία της ιδιωτικής ζωής και ότι η χρήση τους είναι νόμιμη, ασφαλής και δεοντολογική. Στο πλαίσιο της επικείμενης στρατηγικής για την τυποποίηση, η ΕΕ θα πρέπει να καθορίσει **τους στόχους της όσον αφορά τη διεθνή τυποποίηση** και να διεξαγάγει προδραστικές και συντονισμένες δραστηριότητες ευαισθητοποίησης για την προώθησή τους σε διεθνές επίπεδο. Θα πρέπει να επιδιώκεται στενότερη συνεργασία και κατανομή των βαρών με εταίρους που συμμερίζονται τις ίδιες απόψεις και με ευρωπαϊκούς ενδιαφερόμενους φορείς.

Προώθηση της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο

Η ΕΕ εξακολουθεί να συνεργάζεται με τους διεθνείς εταίρους για την προαγωγή και την προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου στον οποίο **τηρείται το διεθνές δίκαιο, ιδίως ο Χάρτης των Ηνωμένων Εθνών[102],** καθώς και τα **εθελοντικά μη δεσμευτικά πρότυπα, κανόνες και αρχές της υπεύθυνης συμπεριφοράς των κρατών**[103]. Καθώς οι προοπτικές μιας αποτελεσματικής πολυμερούς συζήτησης σχετικά με τη διεθνή ασφάλεια στον κυβερνοχώρο έχουν επιδεινωθεί, υπάρχει σαφής ανάγκη η ΕΕ και τα κράτη μέλη να υιοθετήσουν μια πιο προδραστική στάση στο πλαίσιο των συζητήσεων στα Ηνωμένα Έθνη και σε άλλα σχετικά διεθνή φόρουμ. Η ΕΕ είναι η πλέον κατάλληλη για **να προωθήσει, να συντονίσει και να εδραιώσει τις θέσεις των κρατών μελών στα διεθνή φόρουμ** και θα πρέπει να **διαμορφώσει τη θέση της σχετικά με την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο**. Ο ύπατος εκπρόσωπος, από κοινού με τα κράτη μέλη, έχει επίσης ως στόχο να προωθήσει την χωρίς αποκλεισμούς και συναινετική πρότασή τους για πολιτική δέσμευση σχετικά με ένα **πρόγραμμα δράσης για την προαγωγή της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA)**[104] στο πλαίσιο των Ηνωμένων Εθνών. Το πρόγραμμα δράσης, με βάση το υφιστάμενο κεκτημένο, όπως αυτό εγκρίθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών[105], προσφέρει μια πλατφόρμα συνεργασίας και ανταλλαγής βέλτιστων πρακτικών εντός των Ηνωμένων Εθνών και

η Ομάδα Μελέτης του Διαδικτύου (IETF), το έργο εταιρικής συνεργασίας 3ης γενιάς (3rd Generation Partnership Project) και το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Όπως αποτυπώνεται στις σχετικές εκθέσεις των ομάδων κυβερνητικών εμπειρογνωμόνων για τις εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας (UNGGEs), οι οποίες εγκρίθηκαν από τη Γενική Συνέλευση των Ηνωμένων Εθνών, και συγκεκριμένα στις εκθέσεις του 2015, του 2013 και του 2010.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Όπως αποτυπώνεται στις σχετικές εκθέσεις των ομάδων κυβερνητικών εμπειρογνωμόνων για τις εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας (UNGGEs), οι οποίες εγκρίθηκαν από τη Γενική Συνέλευση των Ηνωμένων Εθνών, και συγκεκριμένα στις εκθέσεις του 2015, του 2013 και του 2010.

προτείνει τη δημιουργία μηχανισμού για την εφαρμογή των κανόνων υπεύθυνης συμπεριφοράς των κρατών στην πράξη, καθώς και την προώθηση της ανάπτυξης ικανοτήτων. Επιπλέον, ο ύπατος εκπρόσωπος έχει ως στόχο να ενισχύσει και να ενθαρρύνει την εφαρμογή **μέτρων οικοδόμησης εμπιστοσύνης** μεταξύ των κρατών, συμπεριλαμβανομένης της ανταλλαγής βέλτιστων πρακτικών σε περιφερειακό και πολυμερές επίπεδο και της συμβολής στη διαπεριφερειακή συνεργασία.

Η αυξημένη παγκόσμια συνδεσιμότητα δεν θα πρέπει να οδηγήσει σε λογοκρισία, μαζική επιτήρηση, παραβιάσεις του απορρήτου των δεδομένων και καταστολή της κοινωνίας των πολιτών, του πανεπιστημιακού κόσμου και των πολιτών. Η ΕΕ θα πρέπει να εξακολουθήσει να διαδραματίζει ηγετικό ρόλο όσον αφορά την προστασία και την προαγωγή **των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών** στο διαδίκτυο. Για τον σκοπό αυτόν, η ΕΕ θα πρέπει να προωθήσει περαιτέρω τη συμμόρφωση με το διεθνές δίκαιο και με τα διεθνή πρότυπα για τα ανθρώπινα δικαιώματα[106], να θέσει σε εφαρμογή το σχέδιο δράσης της για τα ανθρώπινα δικαιώματα και τη δημοκρατία 2020-2024[107] και να προωθήσει τις κατευθυντήριες γραμμές της στον τομέα των ανθρωπίνων δικαιωμάτων για την ελευθερία της έκφρασης εντός και εκτός διαδικτύου[108], **δίνοντας νέα ώθηση στην πρακτική εφαρμογή των μέσων της ΕΕ**. Η ΕΕ θα πρέπει να καταβάλλει συνεχείς προσπάθειες για την **προστασία των υπερασπιστών των ανθρωπίνων δικαιωμάτων, της κοινωνίας των πολιτών και του πανεπιστημιακού κόσμου που ασχολούνται με θέματα όπως η κυβερνοασφάλεια, το απόρρητο των δεδομένων, η επιτήρηση και η λογοκρισία στο διαδίκτυο.** Για τον σκοπό αυτόν, η ΕΕ θα πρέπει να παράσχει περαιτέρω πρακτική καθοδήγηση, να προωθήσει τις βέλτιστες πρακτικές και να εντείνει τις προσπάθειές της για την πρόληψη της κατάχρησης αναδυόμενων τεχνολογιών, ιδίως με τη χρήση διπλωματικών μέτρων, όπου απαιτείται, καθώς και με τον έλεγχο των εξαγωγών των εν λόγω τεχνολογιών. Η ΕΕ θα πρέπει επίσης να εξακολουθήσει να αγωνίζεται για την προστασία των πλέον ευάλωτων μελών της κοινωνίας στο διαδίκτυο, προτείνοντας νομοθεσία για την καλύτερη προστασία των παιδιών από τη σεξουαλική κακοποίηση και εκμετάλλευση, καθώς και στρατηγική για τα δικαιώματα του παιδιού.

Η Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο

Η ΕΕ εξακολουθεί να στηρίζει τις τρίτες χώρες που επιθυμούν να προσχωρήσουν στη **Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο** και να εργάζεται με σκοπό την ολοκλήρωση του **δεύτερου πρόσθετου πρωτοκόλλου της Σύμβασης της Βουδαπέστης,** το οποίο περιλαμβάνει μέτρα και διασφαλίσεις για τη βελτίωση της διεθνούς συνεργασίας μεταξύ των αρχών επιβολής του νόμου και των δικαστικών αρχών, καθώς και μεταξύ αρχών και παρόχων υπηρεσιών σε άλλες χώρες, και για το οποίο η Επιτροπή συμμετέχει στις διαπραγματεύσεις εξ ονόματος της ΕΕ[109]. Η τρέχουσα πρωτοβουλία για ένα νέο νομικό μέσο σχετικά με το κυβερνοέγκλημα σε επίπεδο ΟΗΕ ενέχει τον κίνδυνο διεύρυνσης της διάστασης απόψεων και επιβράδυνσης πολύ αναγκαίων εθνικών μεταρρυθμίσεων και των σχετικών προσπαθειών ανάπτυξης ικανοτήτων, παρεμποδίζοντας, ενδεχομένως, την αποτελεσματική διεθνή συνεργασία κατά του κυβερνοεγκλήματος: η ΕΕ δεν θεωρεί αναγκαίο ένα νέο νομικό μέσο για το κυβερνοέγκλημα

[106] Ιδίως με τον Χάρτη των Ηνωμένων Εθνών και την Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου.

[107] https://www.consilium.europa.eu/el/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

[109] Απόφαση του Συμβουλίου του Ιουνίου 2019 (αριθ. αναφ. 9116/19)

σε επίπεδο ΟΗΕ. Η ΕΕ εξακολουθεί να συμμετέχει στις **πολυμερείς ανταλλαγές σχετικά με το κυβερνοέγκλημα** για να διασφαλίσει τον σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, μέσω της συμμετοχικότητας και της διαφάνειας και λαμβάνοντας υπόψη τη διαθέσιμη εμπειρογνωσία, με στόχο την παροχή προστιθέμενης αξίας για όλους.

3.2 Συνεργασία με τους εταίρους και την πολυσυμμετοχική κοινότητα

Η ΕΕ θα πρέπει **να ενισχύσει και να επεκτείνει τον κυβερνοδιάλογο με τρίτες χώρες** με σκοπό την προώθηση των αξιών και του οράματός της για τον κυβερνοχώρο, την ανταλλαγή βέλτιστων πρακτικών και την επιδίωξη αποτελεσματικότερης συνεργασίας. Η ΕΕ θα πρέπει επίσης να καθιερώσει **διαρθρωμένες ανταλλαγές με περιφερειακούς οργανισμούς** όπως η Αφρικανική Ένωση, το Περιφερειακό Φόρουμ του ASEAN, ο Οργανισμός Αμερικανικών Κρατών και ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη. Ταυτόχρονα, η ΕΕ θα πρέπει να καταβάλει προσπάθειες ώστε να βρεθούν πιθανά σημεία σύγκλισης με άλλους εταίρους, όπου αυτό είναι δυνατό και σκόπιμο, με βάση ζητήματα κοινού ενδιαφέροντος. Σε συνεργασία με τις αντιπροσωπείες της ΕΕ και, κατά περίπτωση, με τις πρεσβείες των κρατών μελών σε ολόκληρο τον κόσμο, η ΕΕ θα πρέπει να δημιουργήσει ένα άτυπο **δίκτυο κυβερνοδιπλωματίας της ΕΕ** για την προώθηση του οράματος της ΕΕ για τον κυβερνοχώρο, την ανταλλαγή πληροφοριών και τον τακτικό συντονισμό των εξελίξεων στον κυβερνοχώρο[110].

Με βάση τις κοινές δηλώσεις της 8ης Ιουλίου 2016[111] και της 10ης Ιουλίου 2018[112], η ΕΕ θα πρέπει να εξακολουθήσει να προωθεί τη **συνεργασία ΕΕ-NATO,** ιδίως όσον αφορά τις απαιτήσεις διαλειτουργικότητας στον τομέα της κυβερνοάμυνας. Στο πλαίσιο αυτό, η ΕΕ θα πρέπει να επιδιώξει περαιτέρω τη σύνδεση των σχετικών δομών ΚΠΑΑ με την πρωτοβουλία «Federated Mission Networking» του NATO, ώστε να καταστεί δυνατή η διαλειτουργικότητα του δικτύου με το NATO και τους εταίρους, όταν αυτό είναι απαραίτητο. Επιπλέον, θα πρέπει να διερευνηθεί περαιτέρω η συνεργασία μεταξύ της ΕΕ και του NATO όσον αφορά την εκπαίδευση, την κατάρτιση και τις ασκήσεις, μεταξύ άλλων με την αναζήτηση συνεργειών μεταξύ της Ευρωπαϊκής Ακαδημίας Ασφάλειας και Άμυνας και του Συνεργατικού Κέντρου Αριστείας του NATO για την Άμυνα στον Κυβερνοχώρο.

Η ΕΕ, σύμφωνα με τις αξίες της, υποστηρίζει σθεναρά και προωθεί το **πολυσυμμετοχικό μοντέλο διακυβέρνησης του διαδικτύου**. Καμία μεμονωμένη οντότητα, κυβέρνηση ή διεθνής οργανισμός, δεν θα πρέπει να επιδιώκει τον έλεγχο του διαδικτύου. Η ΕΕ θα πρέπει να εξακολουθήσει να συμμετέχει σε φόρουμ[113] για την ενίσχυση της συνεργασίας και τη διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως του δικαιώματος στην αξιοπρέπεια, στην ιδιωτικότητα και στην ελευθερία της έκφρασης και της πληροφόρησης. Για την προώθηση της πολυμερούς συνεργασίας σε θέματα κυβερνοασφάλειας, η Επιτροπή και ο ύπατος εκπρόσωπος, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, έχουν ως στόχο την ενίσχυση των **τακτικών και διαρθρωμένων ανταλλαγών με τα ενδιαφερόμενα μέρη**, συμπεριλαμβανομένου του ιδιωτικού τομέα, των

[110] Θα μπορούσε επίσης, κατά περίπτωση, να αξιοποιήσει τις δραστηριότητες του άτυπου δικτύου ψηφιακής διπλωματίας της ΕΕ, στο οποίο συμμετέχουν τα υπουργεία Εξωτερικών των κρατών μελών.
[111] https://www.consilium.europa.eu/el/press/press-releases/2016/07/08/eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/el/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Όπως το Σώμα του Διαδικτύου για την Εκχώρηση Ονομάτων και Αριθμών (ICANN) και το Φόρουμ για τη Διακυβέρνηση του Διαδικτύου (IGF).

πανεπιστημίων και της κοινωνίας των πολιτών, τονίζοντας ότι, λόγω του διασυνδεδεμένου χαρακτήρα του κυβερνοχώρου, όλα τα ενδιαφερόμενα μέρη πρέπει να ανταλλάσσουν απόψεις και να αναλαμβάνουν τις ευθύνες που τους αναλογούν, με σκοπό τη διατήρηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου. Οι προσπάθειες αυτές θα παράσχουν πολύτιμες πληροφορίες για πιθανές βασικές δράσεις σε επίπεδο ΕΕ.

3.3. Ενίσχυση των παγκόσμιων ικανοτήτων για την αύξηση της παγκόσμιας ανθεκτικότητας

Για να διασφαλιστεί ότι όλες οι χώρες είναι σε θέση να αποκομίσουν τα κοινωνικά, οικονομικά και πολιτικά οφέλη του διαδικτύου και της χρήσης των τεχνολογιών, η ΕΕ εξακολουθεί να στηρίζει τους εταίρους της ώστε να αυξήσουν την κυβερνοανθεκτικότητά τους και τις ικανότητές τους να διερευνούν και να διώκουν το κυβερνοέγκλημα και να αντιμετωπίζουν τις κυβερνοαπειλές. Προκειμένου να διασφαλιστεί η συνολική συνοχή, η ΕΕ θα πρέπει να εκπονήσει **θεματολόγιο της ΕΕ για την ανάπτυξη των εξωτερικών κυβερνοϊκανοτήτων**, ώστε να προσανατολίσει τις προσπάθειες αυτές σύμφωνα με τις κατευθυντήριες γραμμές της για την ανάπτυξη των εξωτερικών κυβερνοϊκανοτήτων[114] και το θεματολόγιο του 2030 για τη Βιώσιμη Ανάπτυξη[115]. Το θεματολόγιο θα πρέπει να αξιοποιεί την εμπειρογνωσία των κρατών μελών και των σχετικών θεσμικών και λοιπών οργάνων και οργανισμών καθώς και των πρωτοβουλιών της ΕΕ, συμπεριλαμβανομένου του δικτύου της ΕΕ για την ανάπτυξη των κυβερνοϊκανοτήτων[116], σύμφωνα με τις αντίστοιχες εντολές τους. Θα δημιουργηθεί **συμβούλιο της ΕΕ για την ανάπτυξη των κυβερνοϊκανοτήτων,** το οποίο θα περιλαμβάνει τους σχετικούς θεσμικούς φορείς της ΕΕ και θα παρακολουθεί την πρόοδο, καθώς και τον εντοπισμό νέων συνεργειών και ενδεχόμενων κενών. Θα μπορεί επίσης να στηρίζει την ενισχυμένη συνεργασία με τα κράτη μέλη, καθώς και με εταίρους του δημόσιου και του ιδιωτικού τομέα και άλλους σχετικούς διεθνείς φορείς, ώστε να εξασφαλιστεί ο συντονισμός των προσπαθειών και να αποφευχθούν οι αλληλεπικαλύψεις.

Η ανάπτυξη των κυβερνοϊκανοτήτων εκ μέρους της ΕΕ θα πρέπει να εξακολουθήσει να επικεντρώνεται στα Δυτικά Βαλκάνια και στις γειτονικές χώρες της ΕΕ, καθώς και στις χώρες εταίρους στις οποίες σημειώνεται ταχεία ψηφιακή ανάπτυξη. Η ΕΕ θα πρέπει να στηρίξει με τις ενέργειές της την ανάπτυξη νομοθεσίας και πολιτικών στις χώρες εταίρους σύμφωνα με τις σχετικές πολιτικές και τα πρότυπα της ΕΕ για την κυβερνοδιπλωματία. Στο πλαίσιο αυτό, οι προσπάθειες της ΕΕ για την ανάπτυξη ικανοτήτων στον τομέα της ψηφιοποίησης θα πρέπει να περιλαμβάνουν την κυβερνοασφάλεια ως σύνηθες χαρακτηριστικό. Για τον σκοπό αυτό, η ΕΕ θα πρέπει να εκπονήσει πρόγραμμα κατάρτισης ειδικά για το προσωπικό της ΕΕ που είναι υπεύθυνο για την υλοποίηση των προσπαθειών της ΕΕ όσον αφορά την ανάπτυξη ψηφιακών ικανοτήτων και των εξωτερικών κυβερνοϊκανοτήτων. Η ΕΕ θα πρέπει επίσης να βοηθήσει τις χώρες αυτές να αντιμετωπίσουν την αυξανόμενη πρόκληση των κακόβουλων κυβερνοδραστηριοτήτων που βλάπτουν την ανάπτυξη των κοινωνιών τους και την **ακεραιότητα και την ασφάλεια των δημοκρατικών συστημάτων,** σύμφωνα με τις προσπάθειες που καταβάλλονται στο πλαίσιο του ευρωπαϊκού σχεδίου δράσης για τη δημοκρατία. Η διομότιμη μάθηση μεταξύ των κρατών μελών της ΕΕ, των σχετικών οργανισμών της ΕΕ και των τρίτων χωρών, θα μπορούσε να είναι ιδιαίτερα χρήσιμη εν προκειμένω.

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

Τέλος, στο πλαίσιο του συμφώνου μη στρατιωτικής ΚΠΑΑ του 2018[117], οι μη στρατιωτικές αποστολές ΚΠΑΑ μπορούν επίσης να συμβάλλουν στην ευρύτερη αντίδραση της ΕΕ για την αντιμετώπιση των προκλήσεων κυβερνοασφάλειας, ιδίως με την ενίσχυση του κράτους δικαίου στις χώρες εταίρους, καθώς και των ικανοτήτων των αρχών επιβολής του νόμου και των μη στρατιωτικών διοικήσεων.

Στρατηγικές πρωτοβουλίες

Η ΕΕ θα πρέπει:

- να καθορίσει ένα σύνολο στόχων στις διεθνείς διαδικασίες τυποποίησης και να τους προωθήσει σε διεθνές επίπεδο·
- να προωθήσει τη διεθνή ασφάλεια και σταθερότητα στον κυβερνοχώρο, ιδίως μέσω της πρότασης της ΕΕ και των κρατών μελών της σχετικά με πρόγραμμα δράσης για την προαγωγή της υπεύθυνης συμπεριφοράς των κρατών στον κυβερνοχώρο (PoA) στο πλαίσιο των Ηνωμένων Εθνών·
- να παρέχει πρακτική καθοδήγηση σχετικά με την εφαρμογή των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στον κυβερνοχώρο·
- να προστατεύει καλύτερα τα παιδιά από τη σεξουαλική κακοποίηση και τη σεξουαλική εκμετάλλευση, καθώς και να παρουσιάσει στρατηγική για τα δικαιώματα του παιδιού·
- να ενισχύσει και να προωθήσει τη Σύμβαση της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, μεταξύ άλλων μέσω των εργασιών για το δεύτερο πρόσθετο πρωτόκολλο της Σύμβασης της Βουδαπέστης·
- να επεκτείνει τον κυβερνοδιάλογο της ΕΕ με τρίτες χώρες, περιφερειακούς και διεθνείς οργανισμούς, μεταξύ άλλων μέσω άτυπου δικτύου της ΕΕ για την κυβερνοδιπλωματία·
- να ενισχύσει τις ανταλλαγές με την πολυσυμμετοχική κοινότητα, ιδίως μέσω τακτικών και δομημένων ανταλλαγών με τον ιδιωτικό τομέα, την πανεπιστημιακή κοινότητα και την κοινωνία των πολιτών· και
- να προτείνει θεματολόγιο της ΕΕ για την ανάπτυξη των εξωτερικών κυβερνοϊκανοτήτων και συμβούλιο της ΕΕ για την ανάπτυξη των κυβερνοϊκανοτήτων της ΕΕ .

III. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΑ ΘΕΣΜΙΚΑ ΚΑΙ ΛΟΙΠΑ ΟΡΓΑΝΑ ΚΑΙ ΤΟΥΣ ΟΡΓΑΝΙΣΜΟΥΣ ΤΗΣ ΕΕ

Δεδομένου του υψηλού πολιτικού προφίλ τους, των κρίσιμων αποστολών τους για τον συντονισμό ιδιαίτερα ευαίσθητων ζητημάτων και του ρόλου τους στη διαχείριση μεγάλων ποσών δημόσιου χρήματος, **τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ αποτελούν τακτικούς στόχους των κυβερνοεπιθέσεων**, ιδίως της κυβερνοκατασκοπείας. Ωστόσο, το επίπεδο κυβερνοανθεκτικότητας και ικανότητας εντοπισμού και αντιμετώπισης κακόβουλων κυβερνοδραστηριοτήτων ποικίλλει σημαντικά μεταξύ των εν λόγω οντοτήτων,

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/en/pdf

ανάλογα με την ωριμότητά τους. Ως εκ τούτου, είναι αναγκαίο να βελτιωθεί το συνολικό επίπεδο κυβερνοασφάλειας μέσω συνεκτικών και ομοιογενών κανόνων.

Στον τομέα της ασφάλειας των πληροφοριών, έχει σημειωθεί πρόοδος προς μεγαλύτερη συνοχή των **κανόνων για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ, καθώς και των ευαίσθητων μη διαβαθμισμένων πληροφοριών**. Ωστόσο, η διαλειτουργικότητα των διαβαθμισμένων συστημάτων πληροφοριών παραμένει περιορισμένη, εμποδίζοντας την απρόσκοπτη διαβίβαση πληροφοριών μεταξύ των διαφόρων οντοτήτων. Θα πρέπει να σημειωθεί περαιτέρω πρόοδος προκειμένου να καταστεί δυνατή μια διοργανική προσέγγιση όσον αφορά τον χειρισμό των διαβαθμισμένων πληροφοριών της ΕΕ και των ευαίσθητων μη διαβαθμισμένων πληροφοριών, η οποία θα μπορούσε επίσης να χρησιμεύσει ως μοντέλο διαλειτουργικότητας μεταξύ των κρατών μελών. Θα πρέπει επίσης να καθοριστεί μια γραμμή βάσης για την απλούστευση των διαδικασιών με τα κράτη μέλη. Η ΕΕ οφείλει επίσης να αναπτύξει περαιτέρω την ικανότητά της να επικοινωνεί με τους σχετικούς εταίρους με ασφαλή τρόπο, βασιζόμενη, στο μέτρο του δυνατού, στις υφιστάμενες ρυθμίσεις και διαδικασίες.

Ως εκ τούτου, όπως ανακοινώθηκε στη στρατηγική για την Ένωση Ασφάλειας, η Επιτροπή θα υποβάλει, το 2021, προτάσεις **κοινών δεσμευτικών κανόνων σχετικά με την ασφάλεια των πληροφοριών και κοινών δεσμευτικών κανόνων σχετικά με την κυβερνοασφάλεια για όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ**, με βάση τις εν εξελίξει διοργανικές συζητήσεις της ΕΕ για την κυβερνοασφάλεια[118].

Οι τρέχουσες και μελλοντικές τάσεις της τηλεργασίας θα απαιτήσουν επίσης περαιτέρω επενδύσεις σε ασφαλείς εξοπλισμούς, υποδομές και εργαλεία που θα επιτρέψουν την εξ αποστάσεως εργασία σε ευαίσθητους και διαβαθμισμένους φακέλους.

Επιπλέον, το όλο και πιο εχθρικό τοπίο των κυβερνοαπειλών και η αυξημένη συχνότητα πιο εξελιγμένων κυβερνοεπιθέσεων που πλήττουν τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ ενισχύουν την ανάγκη για αυξημένες επενδύσεις ώστε να επιτευχθεί υψηλό επίπεδο κυβερνοωριμότητας. Επί του παρόντος καταρτίζεται πρόγραμμα κυβερνοευαισθητοποίησης το οποίο απευθύνεται σε όλα τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ και αποσκοπεί στην ευαισθητοποίηση του προσωπικού, στην κυβερνοϋγιεινή και την υποστήριξη μιας κοινής νοοτροπίας κυβερνοασφάλειας.

Η **ενίσχυση της CERT-ΕΕ με βελτιωμένο μηχανισμό χρηματοδότησης** είναι απαραίτητη προκειμένου να ενισχυθεί η ικανότητά της να βοηθά τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ να εφαρμόζουν τους νέους κανόνες για την κυβερνοασφάλεια και να βελτιώνουν την κυβερνοανθεκτικότητά τους. Η εντολή της CERT-ΕΕ πρέπει επίσης να ενισχυθεί ώστε να της παρασχεθεί ένα σταθερό μέσο για την επίτευξη αυτών των στόχων.

Στρατηγικές πρωτοβουλίες

1. Κανονισμός σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ

2. Κανονισμός σχετικά με τους κοινούς κανόνες κυβερνοασφάλειας για τα θεσμικά

[118]Οι τακτικές διοργανικές συζητήσεις της ΕΕ για την κυβερνοασφάλεια αποτελούν μέρος ευρύτερων ανταλλαγών σχετικά με τις ευκαιρίες και τις προκλήσεις του ψηφιακού μετασχηματισμού για τα θεσμικά όργανα της ΕΕ.

και λοιπά όργανα και τους οργανισμούς της ΕΕ

3. Νέα νομική βάση για την CERT-ΕΕ με σκοπό την ενίσχυση της εντολής και της χρηματοδότησής της.

IV. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η συντονισμένη εφαρμογή της παρούσας στρατηγικής θα συμβάλει σε μια κυβερνοασφαλή ψηφιακή δεκαετία για την ΕΕ, στην επίτευξη Ένωσης Ασφάλειας και στην ενίσχυση της θέσης της ΕΕ παγκοσμίως.

Η ΕΕ θα πρέπει να καθορίσει πρότυπα και κανόνες για παγκόσμιες λύσεις και πρότυπα κυβερνοασφάλειας για βασικές υπηρεσίες και υποδομές ζωτικής σημασίας, καθώς και για την ανάπτυξη και την εφαρμογή νέων τεχνολογιών. Κάθε οργανισμός και κάθε άτομο που χρησιμοποιεί το διαδίκτυο αποτελεί μέρος της λύσης για την εξασφάλιση κυβερνοασφαλούς ψηφιακού μετασχηματισμού.

Η Επιτροπή και ο ύπατος εκπρόσωπος, σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, θα παρακολουθούν την πρόοδο στο πλαίσιο της παρούσας στρατηγικής και θα αναπτύξουν κριτήρια αξιολόγησης. Η παρακολούθηση αυτή θα πρέπει να βασίζεται στις εκθέσεις του ENISA και στις τακτικές εκθέσεις της Επιτροπής για την Ένωση Ασφάλειας. Τα αποτελέσματα θα συμβάλουν στην επίτευξη των επικείμενων στόχων της ψηφιακής δεκαετίας[119]. Σύμφωνα με τις αντίστοιχες αρμοδιότητές τους, η Επιτροπή και ο ύπατος εκπρόσωπος θα εξακολουθήσουν να συνεργάζονται με τα κράτη μέλη προκειμένου να καθοριστούν πρακτικά μέτρα για την προσέγγιση των τεσσάρων κοινοτήτων κυβερνοασφάλειας στην ΕΕ των υποδομών ζωτικής σημασίας και της ανθεκτικότητας της εσωτερικής αγοράς, της δικαιοσύνης και επιβολής του νόμου, της κυβερνοδιπλωματίας και της κυβερνοάμυνας, όπου απαιτείται. Επιπλέον, η Επιτροπή και ο ύπατος εκπρόσωπος θα εξακολουθήσουν να συνεργάζονται με την πολυσυμμετοχική κοινότητα, τονίζοντας ότι όλοι οι χρήστες του διαδικτύου θα πρέπει να συμβάλουν στη διατήρηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου, όπου καθένας θα μπορεί να ζει με ασφάλεια την ψηφιακή του ζωή.

[119] Όπως ανακοινώθηκε στο πρόγραμμα εργασίας της Επιτροπής για το 2021.

Προσάρτημα: τα επόμενα βήματα όσον αφορά την κυβερνοασφάλεια των δικτύων 5G

Με βάση τα αποτελέσματα της επανεξέτασης της σύστασης της Επιτροπής σχετικά με την κυβερνοασφάλεια των δικτύων 5G[120], τα επόμενα στάδια των συντονισμένων εργασιών σε επίπεδο ΕΕ θα πρέπει να επικεντρωθούν σε τρεις βασικούς στόχους και στις κύριες βραχυπρόθεσμες και μεσοπρόθεσμες δράσεις που παρατίθενται στον πίνακα κατωτέρω, που θα υλοποιηθούν από τις αρχές των κρατών μελών, την Επιτροπή και τον ENISA.

Πρώτον, η προτεραιότητα για την επόμενη φάση είναι η **ολοκλήρωση της εφαρμογής της εργαλειοθήκης σε εθνικό επίπεδο και η αντιμετώπιση των ζητημάτων που θίγονται στην έκθεση προόδου του Ιουλίου 2020** . Στο πλαίσιο αυτό, ορισμένα από τα στρατηγικά μέτρα της εργαλειοθήκης θα ωφεληθούν από τις **ενισχυμένες εργασίες συντονισμού ή την ενισχυμένη ανταλλαγή πληροφοριών** στο πλαίσιο του άξονα εργασίας της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS), όπως έχει ήδη επισημανθεί στην έκθεση προόδου, γεγονός που θα μπορούσε ενδεχομένως να οδηγήσει στην ανάπτυξη **βέλτιστων πρακτικών ή καθοδήγησης**. Όσον αφορά τα τεχνικά μέτρα, ο ENISA θα μπορούσε να παράσχει περαιτέρω στήριξη, βασιζόμενος στο έργο που έχει ήδη επιτελέσει και διερευνώντας ορισμένα θέματα περισσότερο εις βάθος, καθώς και **καταρτίζοντας μια ολοκληρωμένη επισκόπηση όλων των σχετικών κατευθυντήριων γραμμών σχετικά με τις απαιτήσεις κυβερνοασφάλειας 5G για τους φορείς εκμετάλλευσης κινητών δικτύων.**

Δεύτερον, τα κράτη μέλη τόνισαν ότι είναι σημαντικό να συμβαδίζουν με τις **εξελίξεις της τεχνολογίας, της αρχιτεκτονικής 5G, των απειλών και των διαφόρων χρήσεων και εφαρμογών 5G, καθώς και των εξωτερικών παραγόντων, μέσω της συνεχούς παρακολούθησής τους,** προκειμένου να είναι σε θέση να **εντοπίζουν και να αντιμετωπίζουν νέους ή αναδυόμενους κινδύνους**. Επιπλέον, θα πρέπει να εξεταστούν περαιτέρω ορισμένες πτυχές της αρχικής ανάλυσης κινδύνου, ιδίως για να διασφαλιστεί ότι η εν λόγω ανάλυση καλύπτει ολόκληρο το οικοσύστημα 5G, συμπεριλαμβανομένων όλων των σχετικών τμημάτων της υποδομής δικτύου και της αλυσίδας εφοδιασμού 5G. Παρότι η εργαλειοθήκη έχει σχεδιαστεί ως ευέλικτο και προσαρμόσιμο μέσο, εάν χρειαστεί, θα μπορούσαν να ληφθούν μεσοπρόθεσμα μέτρα για τη διεύρυνση ή την τροποποίησή της, προκειμένου να διασφαλιστεί ότι παραμένει πλήρης και επικαιροποιημένη.

Τρίτον, θα πρέπει να συνεχιστεί η ανάληψη **δράσεων σε επίπεδο ΕΕ** για τη στήριξη και συμπλήρωση των στόχων της εργαλειοθήκης και για την πλήρη ενσωμάτωσή τους στις σχετικές πολιτικές της Ένωσης και της Επιτροπής, ιδίως σε συνέχεια των δράσεων που εξήγγειλε η Επιτροπή στην ανακοίνωσή της σχετικά με την εργαλειοθήκη της 29ης Ιανουαρίου 2020[121] σε ευρύ φάσμα τομέων (π.χ. χρηματοδότηση της ΕΕ για ασφαλή δίκτυα 5G, επενδύσεις σε τεχνολογίες 5G και μετά το 5G, μέσα εμπορικής άμυνας και ανταγωνισμός για την αποφυγή στρεβλώσεων στην αγορά εφοδιασμού 5G κ.λπ.).

Στις αρχές του 2021 θα πρέπει, κατά περίπτωση, να συμφωνηθούν από τους επικεφαλής φορείς λεπτομερείς ρυθμίσεις και ορόσημα για τις κύριες δράσεις που καθορίζονται κατωτέρω.

[120] Έκθεση της Επιτροπής σχετικά με τις επιπτώσεις της σύστασης 2019/534 της Επιτροπής, της 26ης Μαρτίου 2019, για την κυβερνοασφάλεια των δικτύων 5G.

[121] Ανακοίνωση της Επιτροπής COM (2020)50, Ασφαλής εγκατάσταση του 5G στην ΕΕ — Εφαρμογή της εργαλειοθήκης της ΕΕ, 29 Ιανουαρίου 2020.

Βασικός στόχος 1: διασφάλιση σύγκλισης των εθνικών προσεγγίσεων για τον αποτελεσματικό μετριασμό των κινδύνων σε ολόκληρη την ΕΕ		
Τομείς	**Κύριες βραχυπρόθεσμες και μεσοπρόθεσμες δράσεις**	**Επικεφαλής φορείς**
Εφαρμογή της εργαλειοθήκης από τα κράτη μέλη	Ολοκλήρωση της εφαρμογής των μέτρων που συνιστώνται στα συμπεράσματα της εργαλειοθήκης έως το δεύτερο τρίμηνο του 2021, με περιοδικό απολογισμό στο πλαίσιο του άξονα εργασίας της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS).	Αρχές των κρατών μελών
Ανταλλαγή πληροφοριών και βέλτιστων πρακτικών σχετικά με τα στρατηγικά μέτρα που αφορούν τους προμηθευτές	Εντατικοποίηση της ανταλλαγής πληροφοριών και εξέταση πιθανών βέλτιστων πρακτικών, ιδίως όσον αφορά: - τους περιορισμούς για τους προμηθευτές υψηλού κινδύνου (ΣΜ03), καθώς και τα μέτρα σχετικά με την παροχή διαχειριζόμενων υπηρεσιών (ΣΜ04)· - την ασφάλεια και την ανθεκτικότητα της αλυσίδας εφοδιασμού, ιδίως σε συνέχεια της έρευνας που διεξήγαγε ο BEREC (Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες) σχετικά με τα ΣΜ05-ΣΜ06.	Αρχές των κρατών μελών, Επιτροπή
Ανάπτυξη ικανοτήτων και κατευθυντήριες γραμμές σχετικά με τα τεχνικά μέτρα	Διεξαγωγή ενδελεχών τεχνικών ερευνών και ανάπτυξη κοινών κατευθυντήριων γραμμών και εργαλείων, μεταξύ των οποίων: - ολοκληρωμένος και δυναμικός πίνακας ελέγχων ασφάλειας και βέλτιστων πρακτικών για την ασφάλεια 5G· κατευθυντήριες γραμμές για τη στήριξη της εφαρμογής επιλεγμένων τεχνικών μέτρων από την εργαλειοθήκη.	ENISA, αρχές των κρατών μελών
Βασικός στόχος 2: στήριξη της συνεχούς ανταλλαγής γνώσεων και της ανάπτυξης ικανοτήτων		
Τομείς	**Κύριες βραχυπρόθεσμες και μεσοπρόθεσμες δράσεις**	**Επικεφαλής φορείς**
Συνεχής ανάπτυξη γνώσεων	Οργάνωση δραστηριοτήτων ανάπτυξης γνώσεων σχετικά με την τεχνολογία και τις συναφείς προκλήσεις (ανοικτές αρχιτεκτονικές, χαρακτηριστικά 5G — π.χ. εικονικοποίηση, εγκιβωτισμός, τεμαχισμός κ.λπ.), εξελίξεις στο τοπίο των απειλών, συμβάντα στην πραγματική ζωή κ.λπ.	ENISA, αρχές των κρατών μελών, άλλοι ενδιαφερόμενοι φορείς
Εκτίμηση επικινδυνότητας	Επικαιροποίηση και ανταλλαγή πληροφοριών σχετικά με επικαιροποιημένες εθνικές εκτιμήσεις επικινδυνότητας	Αρχές των κρατών μελών, Επιτροπή, ENISA
Κοινά έργα χρηματοδοτούμενα από την ΕΕ για τη στήριξη της εφαρμογής της εργαλειοθήκης	Παροχή χρηματοδοτικής στήριξης σε έργα που στηρίζουν την εφαρμογή της εργαλειοθήκης με χρηματοδότηση της ΕΕ, ιδίως στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη» (π.χ. έργα ανάπτυξης ικανοτήτων για τις εθνικές αρχές, κλίνες δοκιμών ή άλλες προηγμένες ικανότητες κ.λπ.)	Αρχές των κρατών μελών, Επιτροπή
Συνεργασία μεταξύ των ενδιαφερόμενων	Προώθηση της συνεργασίας μεταξύ των εθνικών αρχών που είναι αρμόδιες για την κυβερνοασφάλεια των	Αρχές των κρατών μελών,

μερών	δικτύων 5G [π.χ. ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS), αρχές κυβερνοασφάλειας, ρυθμιστικές αρχές τηλεπικοινωνιών] και με ιδιωτικούς ενδιαφερόμενους φορείς	Επιτροπή, ENISA
Βασικός στόχος 3: προώθηση της ανθεκτικότητας της αλυσίδας εφοδιασμού και άλλων στρατηγικών στόχων ασφάλειας της ΕΕ		
Τομείς	**Κύριες βραχυπρόθεσμες και μεσοπρόθεσμες δράσεις**	**Επικεφαλής φορείς**
Τυποποίηση	Καθορισμός και εφαρμογή συγκεκριμένου σχεδίου δράσης για την ενίσχυση της εκπροσώπησης της ΕΕ σε φορείς καθορισμού προτύπων στο πλαίσιο των επόμενων σταδίων των εργασιών της υποομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών (NIS) για την τυποποίηση προκειμένου να επιτευχθούν συγκεκριμένοι στόχοι ασφάλειας, συμπεριλαμβανομένης της προώθησης διαλειτουργικών διεπαφών για τη διευκόλυνση της διαφοροποίησης των προμηθευτών.	Αρχές των κρατών μελών
Ανθεκτικότητα της αλυσίδας εφοδιασμού	— Διενέργεια ενδελεχούς ανάλυσης του οικοσυστήματος και της αλυσίδας εφοδιασμού 5G με σκοπό τον καλύτερο προσδιορισμό και την παρακολούθηση βασικών πάγιων στοιχείων και δυνητικών κρίσιμων εξαρτήσεων — Διασφάλιση της λειτουργίας της αγοράς και της αλυσίδας εφοδιασμού 5G σύμφωνα με τους κανόνες και τους στόχους της ΕΕ για το εμπόριο και τον ανταγωνισμό, όπως καθορίζονται στην ανακοίνωση της Επιτροπής της 29ης Ιανουαρίου, και της εφαρμογής του ελέγχου των άμεσων ξένων επενδύσεων σε επενδυτικές εξελίξεις που ενδέχεται να επηρεάσουν την αξιακή αλυσίδα 5G, λαμβανομένων υπόψη των στόχων της εργαλειοθήκης. — Παρακολούθηση των υφιστάμενων και των αναμενόμενων τάσεων της αγοράς και εκτίμηση των κινδύνων και των ευκαιριών στον τομέα του ανοικτού RAN, ιδίως μέσω ανεξάρτητης μελέτης	Αρχές των κρατών μελών, Επιτροπή
Πιστοποίηση	Έναρξη προετοιμασιών του/των σχετικού/-ων υποψήφιου/-ων συστήματος/-ων πιστοποίησης για τις βασικές συνιστώσες των δικτύων 5G και τις διαδικασίες των προμηθευτών, ώστε να αντιμετωπιστούν ορισμένοι κίνδυνοι που σχετίζονται με τρωτά σημεία τεχνικού χαρακτήρα, όπως ορίζεται στα σχέδια μετριασμού των κινδύνων της εργαλειοθήκης.	Επιτροπή, ENISA, εθνικές αρχές, άλλα ενδιαφερόμενα μέρη
Ικανότητες της ΕΕ και ανάπτυξη ασφαλών δικτύων	— Επένδυση στην Ε&Κ και στις ικανότητες, ιδίως με τη θέσπιση της εταιρικής σχέσης για τα έξυπνα δίκτυα και τις υπηρεσίες. — Εφαρμογή των σχετικών όρων ασφάλειας για τα χρηματοδοτικά προγράμματα και τα χρηματοδοτικά μέσα της ΕΕ (εσωτερικά και εξωτερικά), όπως ανακοινώθηκε στην ανακοίνωση της Επιτροπής της 29ης Ιανουαρίου.	Κράτη μέλη, Επιτροπή, ενδιαφερόμενα μέρη του κλάδου 5G
Εξωτερικές πτυχές	Θετική ανταπόκριση σε αιτήματα τρίτων χωρών που επιθυμούν να κατανοήσουν και ενδεχομένως να χρησιμοποιήσουν την προσέγγιση «εργαλειοθήκης» που ανέπτυξε η ΕΕ.	Κράτη μέλη, Επιτροπή, ΕΥΕΔ, Αντιπροσωπείες

		της ΕΕ