Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 30 Ιουλίου 2020
(OR. en)

10010/20

JAI 624	**DROIPEN 61**
COSI 121	**COPEN 215**
ENFOPOL 190	**FREMP 51**
ENFOCUSTOM 95	**JAIEX 72**
IXIM 79	**CFSP/PESC 644**
CT 61	**COPS 256**
CRIMORG 66	**HYBRID 20**
FRONT 207	**DISINFO 16**
ASIM 55	**TELECOM 121**
VISA 84	**DIGIT 63**
CYBER 140	**COMPET 347**
DATAPROTECT 71	**RECH 286**
CATS 56	

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για την Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, ο κ. Jordi AYET PUIGARNAU, Διευθυντής
Ημερομηνία Παραλαβής:	27 Ιουλίου 2020
Αποδέκτης:	κ. Jeppe TRANHOLM-MIKKELSEN, Γενικός Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	COM(2020) 605 final
Θέμα:	ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφάλειας

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο COM(2020) 605 final.

συνημμ.: COM(2020) 605 final

ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 24.7.2020
COM(2020) 605 final

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφάλειας

I. Εισαγωγή

Οι πολιτικές κατευθυντήριες γραμμές της Επιτροπής κατέστησαν σαφές ότι, όταν πρόκειται για την προστασία των πολιτών μας, πρέπει να καταβάλλουμε κάθε δυνατή προσπάθεια. Η ασφάλεια από εξωτερικές ενέργειες δεν αποτελεί μόνο τη βάση για την προσωπική ασφάλεια, αλλά προστατεύει επίσης τα θεμελιώδη δικαιώματα και παρέχει τη βάση για εμπιστοσύνη και δυναμισμό στην οικονομία μας, στην κοινωνία μας και τη δημοκρατία μας. Το τοπίο με το οποίο βρίσκονται αντιμέτωποι σήμερα οι Ευρωπαίοι στον τομέα της ασφάλειας είναι ρευστό και επηρεάζεται από εξελισσόμενες απειλές, καθώς και άλλους παράγοντες, μεταξύ των οποίων η κλιματική αλλαγή, οι δημογραφικές τάσεις και η πολιτική αστάθεια πέραν των συνόρων μας. Η παγκοσμιοποίηση, η ελεύθερη κυκλοφορία και ο ψηφιακός μετασχηματισμός εξακολουθούν να φέρνουν ευημερία, να διευκολύνουν τη ζωή μας και να δίνουν ώθηση στην καινοτομία και την ανάπτυξη. Ωστόσο, παράλληλα με τα οφέλη αυτά προκύπτουν εγγενείς κίνδυνοι και κόστος. Οι καταστάσεις αυτές είναι δυνατό να χειραγωγηθούν από την τρομοκρατία, το οργανωμένο έγκλημα, το εμπόριο ναρκωτικών και την εμπορία ανθρώπων, που όλα συνιστούν άμεσες απειλές για τους πολίτες και τον ευρωπαϊκό τρόπο ζωής μας. Οι κυβερνοεπιθέσεις και το κυβερνοέγκλημα εξακολουθούν να αυξάνονται. Οι απειλές κατά της ασφάλειας γίνονται επίσης πιο περίπλοκες: επωφελούνται από τη δυνατότητα διασυνοριακής συνεργασίας, αλλά και από τη διασυνδεσιμότητα· εκμεταλλεύονται την ασάφεια των ορίων μεταξύ του φυσικού και του ψηφιακού κόσμου· εκμεταλλεύονται ευάλωτες ομάδες, καθώς και κοινωνικές και οικονομικές αποκλίσεις. οι επιθέσεις μπορεί να συμβούν σε μια στιγμή και ίσως να αφήνουν λίγα ίχνη ή να μην αφήνουν καθόλου ίχνη· τόσο κρατικοί όσο και μη κρατικοί παράγοντες μπορούν να χρησιμοποιούν διάφορες υβριδικές απειλές[1]· και ό,τι συμβαίνει εκτός της ΕΕ μπορεί να έχει καθοριστικό αντίκτυπο στην ασφάλεια εντός της ΕΕ.

Η κρίση της COVID-19 αναδιαμόρφωσε επίσης την αντίληψή μας όσον αφορά τις απειλές για την ασφάλεια και την προστασία, καθώς και τις αντίστοιχες πολιτικές μας. Τόνισε την ανάγκη κατοχύρωσης της ασφάλειας τόσο στο φυσικό όσο και στο ψηφιακό περιβάλλον. Υπογράμμισε τη σημασία της ανοικτής στρατηγικής αυτονομίας για τις αλυσίδες εφοδιασμού μας όσον αφορά τα προϊόντα, τις υπηρεσίες, τις υποδομές και τις τεχνολογίες κρίσιμης σημασίας. Έχει ενισχύσει την ανάγκη για συμμετοχή κάθε τομέα και κάθε ατόμου σε μια κοινή προσπάθεια να διασφαλιστεί ότι η ΕΕ είναι εξαρχής περισσότερο προετοιμασμένη και ανθεκτική και διαθέτει καλύτερα εργαλεία για να ανταποκρίνεται, όταν χρειαστεί.

Οι πολίτες δεν είναι δυνατό να προστατεύονται μόνο μέσω κρατών μελών που ενεργούν μεμονωμένα. Η ανάγκη για συνεργασία μεταξύ μας, με βάση τα πλεονεκτήματά μας, δεν ήταν ποτέ πιο ουσιώδης, ούτε η ΕΕ είχε ποτέ περισσότερες δυνατότητες να κάνει τη διαφορά. Μπορεί να δώσει πρώτη το παράδειγμα, ενισχύοντας το συνολικό σύστημά της για τη διαχείριση κρίσεων και καταβάλλοντας προσπάθειες εντός και εκτός των συνόρων της για να συμβάλει στην παγκόσμια σταθερότητα. Μολονότι η πρωταρχική ευθύνη για την ασφάλεια ανήκει στα κράτη μέλη, τα τελευταία χρόνια ενισχύεται όλο και περισσότερο η αντίληψη ότι η ασφάλεια ενός κράτους μέλους είναι η ασφάλεια όλων. Η ΕΕ μπορεί να

[1] Αν και οι ορισμοί των υβριδικών απειλών ποικίλλουν, σκοπός της έννοιας είναι να καλύψει τον συνδυασμό καταναγκαστικής και ανατρεπτικής δραστηριότητας, συμβατικών και μη συμβατικών μεθόδων (π.χ. διπλωματικών, στρατιωτικών, οικονομικών και τεχνολογικών) που χρησιμοποιούνται με συντονισμένο τρόπο από κρατικούς ή μη κρατικούς παράγοντες για την επίτευξη ειδικών στόχων (παραμένοντας ωστόσο κάτω από το όριο της επίσημης κήρυξης πολέμου). Βλ. JOIN(2016)18 (final).

δώσει μια πολυτομεακή και ολοκληρωμένη απάντηση, βοηθώντας παράγοντες στον τομέα της ασφάλειας στα κράτη μέλη με τα εργαλεία και τις πληροφορίες που χρειάζονται[2].

Η ΕΕ μπορεί επίσης να μεριμνήσει ώστε η πολιτική για την ασφάλεια να παραμείνει θεμελιωμένη στις κοινές ευρωπαϊκές αξίες μας —με σεβασμό και τήρηση του κράτους δικαίου, της ισότητας[3] και των θεμελιωδών δικαιωμάτων και διασφάλιση της διαφάνειας, της λογοδοσίας και του δημοκρατικού ελέγχου— για να αποκτήσουν οι πολιτικές τη σωστή βάση εμπιστοσύνης. Μπορεί να οικοδομήσει μια αποτελεσματική και πραγματική Ένωση Ασφάλειας στην οποία θα προστατεύονται καλά τα δικαιώματα και οι ελευθερίες των ατόμων. Η ασφάλεια και ο σεβασμός των θεμελιωδών δικαιωμάτων δεν αποτελούν στόχους αλληλοσυγκρουόμενους, αλλά συνεκτικούς και αλληλοσυμπληρούμενους. Οι αξίες και τα θεμελιώδη δικαιώματά μας πρέπει να αποτελούν τη βάση των πολιτικών ασφάλειας, ώστε να κατοχυρώνονται οι αρχές της αναγκαιότητας, της αναλογικότητας και της νομιμότητας, και με τις κατάλληλες διασφαλίσεις για λογοδοσία και δικαστική προσφυγή, ενώ παράλληλα να παρέχεται η δυνατότητα αποτελεσματικής απόκρισης για την προστασία των ατόμων, ιδίως των πλέον ευάλωτων.

Υπάρχουν ήδη σημαντικά νομικά, πρακτικά και υποστηρικτικά εργαλεία, αλλά πρέπει και να ενισχυθούν και να εφαρμοστούν καλύτερα. Έχει σημειωθεί μεγάλη πρόοδος ως προς τη βελτίωση της ανταλλαγής πληροφοριών και της συνεργασίας με τα κράτη μέλη στον τομέα των πληροφοριών ασφάλειας και ως προς τον περιορισμό του χώρου στον οποίο δρουν οι τρομοκράτες και οι εγκληματίες. Ωστόσο, εξακολουθεί να υπάρχει κατακερματισμός.

Επίσης, οι προσπάθειες πρέπει να υπερβαίνουν τα όρια της ΕΕ. Η προστασία της Ένωσης και των πολιτών της δεν αφορά πλέον μόνο την εγγύηση της ασφάλειας εντός των συνόρων της ΕΕ, αλλά και την συμπερίληψη της εξωτερικής διάστασης της ασφάλειας. Η προσέγγιση της ΕΕ όσον αφορά την εξωτερική ασφάλεια στο πλαίσιο της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (ΚΕΠΠΑ) και της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ) θα εξακολουθήσει να αποτελεί βασική συνιστώσα των προσπαθειών της ΕΕ για την ενίσχυση της ασφάλειας εντός της ΕΕ. Η συνεργασία με τρίτες χώρες και σε παγκόσμιο επίπεδο για την αντιμετώπιση των κοινών προκλήσεων έχει καθοριστική σημασία για την αποτελεσματική και ολοκληρωμένη απόκριση, καθώς η σταθερότητα και η ασφάλεια στη γειτονιά της ΕΕ είναι κρίσιμης σημασίας για την ασφάλεια της ίδιας της ΕΕ.

Με βάση το έργο που έχει προηγηθεί από το Ευρωπαϊκό Κοινοβούλιο[4], το Συμβούλιο[5] και την Επιτροπή[6], η νέα αυτή στρατηγική δείχνει ότι μια πραγματική και αποτελεσματική Ένωση Ασφάλειας χρειάζεται να συνδυάζει έναν ισχυρό πυρήνα μέσων και πολιτικών για την επίτευξη ασφάλειας στην πράξη, αναγνωρίζοντας ότι η ασφάλεια επηρεάζει όλα τα μέρη της κοινωνίας και όλες τις δημόσιες πολιτικές. Η ΕΕ χρειάζεται να μεριμνήσει για ένα

---

[2] Για παράδειγμα, μέσω των υπηρεσιών που παρέχονται από το διαστημικό πρόγραμμα της ΕΕ, όπως η υπηρεσία Copernicus, παρέχοντας δεδομένα και εφαρμογές γεωσκόπησης για την επιτήρηση των συνόρων, την ασφάλεια στη θάλασσα, την επιβολή του νόμου, την καταπολέμηση της πειρατείας, την αποτροπή της παράνομης διακίνησης ναρκωτικών και τη διαχείριση καταστάσεων έκτακτης ανάγκης.

[3] Μια Ένωση ισότητας: Στρατηγική για την ισότητα των φύλων 2020-2025, COM(2020) 152.

[4] Για παράδειγμα, το έργο της επιτροπής TERR του Ευρωπαϊκού Κοινοβουλίου, η οποία υπέβαλε έκθεση τον Νοέμβριο του 2018.

[5] Από τα συμπεράσματα του Συμβουλίου του Ιουνίου του 2015 σχετικά με μια «ανανεωμένη στρατηγική εσωτερικής ασφάλειας» έως τα πιο πρόσφατα αποτελέσματα του Συμβουλίου του Δεκεμβρίου του 2019.

[6] «Υλοποίηση του Ευρωπαϊκού Θεματολογίου για την Ασφάλεια για την καταπολέμηση της τρομοκρατίας και την οικοδόμηση μιας αποτελεσματικής και πραγματικής Ένωσης Ασφάλειας», COM (2016) 230 final της 20.4.2016. Βλ. την πρόσφατη αξιολόγηση της εφαρμογής της νομοθεσίας στον τομέα της εσωτερικής ασφάλειας: εφαρμογή της νομοθεσίας εσωτερικών υποθέσεων στον τομέα της εσωτερικής ασφάλειας - 2017-2020 [SWD(2020)135].

ασφαλές περιβάλλον για όλους, ανεξαρτήτως φυλετικής ή εθνοτικής καταγωγής, θρησκείας, πεποιθήσεων, φύλου, ηλικίας ή γενετήσιου προσανατολισμού.

Η στρατηγική αυτή καλύπτει την περίοδο 2020-2025 και επικεντρώνεται στην ανάπτυξη ικανοτήτων και δυνατοτήτων ώστε να διασφαλιστεί ένα διαχρονικά βιώσιμο περιβάλλον ασφάλειας. Καθορίζει μια συνολική κοινωνική προσέγγιση όσον αφορά την ασφάλεια, η οποία μπορεί να ανταποκρίνεται αποτελεσματικά στο ταχέως μεταβαλλόμενο τοπίο των απειλών με συντονισμένο τρόπο. Καθορίζει τις στρατηγικές προτεραιότητες και τις αντίστοιχες δράσεις για την αντιμετώπιση ψηφιακών και φυσικών κινδύνων με ολοκληρωμένο τρόπο σε ολόκληρο το οικοσύστημα της Ένωσης Ασφάλειας, εστιάζοντας στα σημεία όπου η ΕΕ μπορεί να προσθέσει επιπλέον αξία. Στόχος της είναι να προσφέρει ένα αντίκρισμα από την άποψη της ασφάλειας για την προστασία όλων στην ΕΕ.

II. Ένα ταχέως μεταβαλλόμενο ευρωπαϊκό τοπίο απειλών κατά της ασφάλειας

Το αίσθημα ασφάλειας, η ευμάρεια και η ευημερία των πολιτών εξαρτώνται από την ασφάλεια από εξωτερικές ενέργειες. Οι απειλές για αυτήν την ασφάλεια εξαρτώνται από τον βαθμό στον οποίο η ζωή και τα μέσα βιοπορισμού τους είναι ευάλωτα. Όσο πιο ευάλωτα είναι, τόσο μεγαλύτερος είναι ο κίνδυνος εκμετάλλευσης αυτής της ευπάθειας. Τόσο οι ευπάθειες όσο και οι απειλές βρίσκονται σε κατάσταση συνεχούς εξέλιξης και η ΕΕ πρέπει να προσαρμόζεται.

Η καθημερινή μας ζωή εξαρτάται από ευρύ φάσμα υπηρεσιών —όπως η ενέργεια, οι μεταφορές και οι χρηματοπιστωτικές υπηρεσίες, καθώς και η υγεία. Οι υπηρεσίες αυτές εξαρτώνται τόσο από φυσικές όσο και από ψηφιακές υποδομές, γεγονός που επιδεινώνει την ευπάθεια και την πιθανότητα ανατρεπτικών εξελίξεων. Κατά την πανδημία της COVID-19, πολλές επιχειρήσεις και δημόσιες υπηρεσίες έχουν συνεχίσει να λειτουργούν χάρη σε νέες τεχνολογίες, είτε αυτές μας διατηρούν συνδεδεμένους μέσω της τηλεργασίας είτε διατηρούν την υλικοτεχνική υποστήριξη της αλυσίδας εφοδιασμού. Η κατάσταση αυτή όμως έχει ανοίξει επίσης την Κερκόπορτα σε πρωτοφανή αύξηση κακόβουλων επιθέσεων, με τις οποίες επιχειρείται εκμετάλλευση των ανατρεπτικών εξελίξεων εξαιτίας της πανδημίας και της μετάβασης στην ψηφιακή κατ' οίκον εργασία, για εγκληματικούς σκοπούς[7]. Οι ελλείψεις αγαθών έχουν δημιουργήσει νέα πεδία δράσης για το οργανωμένο έγκλημα. Οι συνέπειες θα ήταν ενδεχομένως θανατηφόρες, διαταράσσοντας βασικές υπηρεσίες υγείας σε μια χρονική περίοδο με εντονότατες πιέσεις.

Οι όλο και περισσότεροι τρόποι με τους οποίους οι ψηφιακές τεχνολογίες ωφελούν τη ζωή μας έχουν επίσης καταστήσει την **κυβερνοασφάλεια** των τεχνολογιών ζήτημα στρατηγικής σημασίας[8]. Τα νοικοκυριά, οι τράπεζες, οι χρηματοπιστωτικές υπηρεσίες και οι επιχειρήσεις (ιδίως οι μικρές και μεσαίες επιχειρήσεις) πλήττονται σοβαρά από κυβερνοεπιθέσεις. Οι δυνητικές ζημίες πολλαπλασιάζεται ακόμη περισσότερο εξαιτίας της αλληλεξάρτησης φυσικών και ψηφιακών συστημάτων: κάθε φυσική επίπτωση επηρεάζει αναπόφευκτα τα ψηφιακά συστήματα, ενώ οι κυβερνοεπιθέσεις σε συστήματα πληροφοριών και ψηφιακές

[7] Ευρωπόλ: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (Ευρωπόλ, Πέρα από την πανδημία. Πώς η νόσος COVID-19 θα διαμορφώσει το τοπίο του σοβαρού και οργανωμένου εγκλήματος στην ΕΕ – Απρίλιος 2020)..

[8] Σύσταση της Επιτροπής σχετικά με την κυβερνοασφάλεια δικτύων 5G, C(2019) 2335· ανακοίνωση σχετικά με την ασφαλή εγκατάσταση του 5G στην ΕΕ — Εφαρμογή της εργαλειοθήκης της ΕΕ, COM(2020) 50.

υποδομές μπορούν να παραλύσουν βασικές υπηρεσίες[9]. Η ανάπτυξη του διαδικτύου των πραγμάτων και η αυξημένη χρήση τεχνητής νοημοσύνης θα αποφέρει νέα οφέλη, αλλά και νέους κινδύνους.

Ο κόσμος μας εξαρτάται από ψηφιακές υποδομές, τεχνολογίες και διαδικτυακά συστήματα, που μας επιτρέπουν να δημιουργούμε επιχειρήσεις, να καταναλώνουμε προϊόντα και να απολαμβάνουμε υπηρεσίες. Όλα εξαρτώνται από την επικοινωνία και την αλληλεπίδραση. Η εξάρτηση από το διαδίκτυο έχει ανοίξει την Κερκόπορτα σε ένα κύμα **κυβερνοεγκλήματος**[10]. Το «κυβερνοέγκλημα ως υπηρεσία» και η παραοικονομία του κυβερνοεγκλήματος παρέχουν εύκολη πρόσβαση σε προϊόντα και υπηρεσίες κυβερνοεγκλήματος. Οι εγκληματίες προσαρμόζονται γρήγορα ώστε να χρησιμοποιούν νέες τεχνολογίες για τους δικούς τους σκοπούς. Για παράδειγμα, παραποιημένα και πλαστά φάρμακα έχουν διεισδύσει στη νόμιμη αλυσίδα εφοδιασμού φαρμακευτικών προϊόντων[11]. Η εκθετική αύξηση του υλικού σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο[12] έχει καταδείξει τις κοινωνικές επιπτώσεις των μεταβαλλόμενων μοτίβων του εγκλήματος. Σύμφωνα με πρόσφατη έρευνα οι περισσότεροι άνθρωποι στην ΕΕ (55 %) ανησυχούν για την πρόσβαση που έχουν στα δεδομένα τους εγκληματίες και απατεώνες[13].

Οι απειλές αυτές επιτείνονται επίσης λόγω του **παγκόσμιου περιβάλλοντος**. Οι επιθετικές βιομηχανικές πολιτικές τρίτων χωρών, σε συνδυασμό με τη συνεχιζόμενη και διευκολυνόμενη από τον κυβερνοχώρο κλοπή διανοητικής ιδιοκτησίας, μεταβάλλουν το στρατηγικό πρότυπο για την προστασία και την προώθηση των ευρωπαϊκών συμφερόντων. Η κατάσταση αυτή επιτείνεται από την ανάπτυξη των εφαρμογών διπλής χρήσης —γεγονός που καθιστά έναν ισχυρό κλάδο μη στρατιωτικής τεχνολογίας ισχυρό πλεονέκτημα για την ικανότητα άμυνας και ασφάλειας. Η οικονομική κατασκοπεία έχει σημαντικές επιπτώσεις στην οικονομία, την απασχόληση και την ανάπτυξη στην ΕΕ: Η κυβερνοκλοπή εμπορικών απορρήτων εκτιμάται ότι κοστίζει στην ΕΕ 60 δισ. EUR[14]. Απαιτείται λοιπόν ενδελεχής εξέταση του τρόπου με τον οποίο οι εξαρτήσεις και η αυξημένη έκθεση σε κυβερνοαπειλές επηρεάζουν τη δυνατότητα της ΕΕ να προστατεύει τόσο τα άτομα όσο και τις επιχειρήσεις.

Η κρίση της COVID-19 τόνισε επίσης τον τρόπο με τον οποίο οι κοινωνικές διαιρέσεις και οι αβεβαιότητες δημιουργούν ευπάθειες ασφάλειας. Η εξέλιξη αυτή αυξάνει τις δυνατότητες

---

[9] Τον Μάρτιο του 2020 το πανεπιστημιακό νοσοκομείο του Μπρνο στην Τσεχία δέχτηκε κυβερνοεπίθεση η οποία το ανάγκασε να παραπέμψει εκ νέου ασθενείς και να αναβάλει χειρουργεία (Ευρωπόλ: Pandemic Profiteering. How criminals exploit the COVID-19 crisis) (Ευρωπόλ: Κερδοσκοπία λόγω πανδημίας: πώς οι εγκληματίες εκμεταλλεύονται την κρίση της COVID-19). Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί καταχρηστικά για ψηφιακές, πολιτικές και σωματικές επιθέσεις, καθώς και για παρακολούθηση. Η συλλογή δεδομένων στο πλαίσιο του διαδικτύου των πραγμάτων μπορεί να χρησιμοποιηθεί για την παρακολούθηση ατόμων (έξυπνα ρολόγια, εικονικοί βοηθοί κ.λπ.).

[10] Σύμφωνα με ορισμένες προβολές, το κόστος των παραβιάσεων δεδομένων θα ανέλθει σε 5 τρισ. δολάρια ΗΠΑ ετησίως έως το 2024, από 3 τρισ. δολάρια ΗΠΑ το 2015 (Juniper Research, The Future of Cybercrime & Security).

[11] Σύμφωνα με μία μελέτη του 2016 (Legiscript), εκτιμάται ότι, σε παγκόσμιο επίπεδο, μόνο το 4 % των διαδικτυακών φαρμακείων λειτουργεί νόμιμα, ενώ οι Ευρωπαίοι καταναλωτές αποτελούν τους συνηθέστερους στόχους για τα 30 000 - 35 000 παράνομα φαρμακεία που δραστηριοποιούνται στο διαδίκτυο.

[12] Η στρατηγική της ΕΕ για μια πιο αποτελεσματική καταπολέμηση της παιδικής σεξουαλικής κακοποίησης, COM(2020) 607.

[13] Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2020), Your rights matter: Security concerns and experiences, (Τα δικαιώματά σας έχουν σημασία: προβληματισμοί και εμπειρίες σχετικά με την ασφάλεια) Έρευνα για τα θεμελιώδη δικαιώματα, Λουξεμβούργο, Υπηρεσία Εκδόσεων.

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber (Η κλίμακα και οι επιπτώσεις της βιομηχανικής κατασκοπείας και της κλοπής εμπορικών απορρήτων μέσω του κυβερνοχώρου), 2018.

για πιο εξελιγμένες και **υβριδικές επιθέσεις** από κρατικούς και μη κρατικούς παράγοντες, καθώς ένας συνδυασμός κυβερνοεπιθέσεων, ζημιών σε υποδομές ζωτικής σημασίας[15], εκστρατειών παραπληροφόρησης και ριζοσπαστικοποίησης του πολιτικού αφηγήματος εκμεταλλεύεται τις ευπάθειες.[16]

Ταυτόχρονα, πιο παραδοσιακές απειλές εξακολουθούν να εξελίσσονται. Το 2019 σημειώθηκε πτωτική τάση των **τρομοκρατικών επιθέσεων** στην ΕΕ. Ωστόσο, η απειλή για τους πολίτες της ΕΕ από τζιχαντιστικές επιθέσεις που προέρχονται ή εμπνέονται από το Da'esh και την Αλ Κάιντα και τις συνδεόμενες ομάδες τους παραμένει υψηλή[17]. Παράλληλα, αυξάνεται επίσης η απειλή του βίαιου δεξιού εξτρεμισμού[18]. Οι επιθέσεις με ρατσιστικά κίνητρα πρέπει να αποτελούν πηγή σοβαρής ανησυχίας: οι φονικές αντισημιτικές τρομοκρατικές επιθέσεις στο Halle υπενθύμισαν την ανάγκη να ενταθεί η αντίδραση σύμφωνα με τη δήλωση του Συμβουλίου του 2018[19]. Ένα στα πέντε άτομα στην ΕΕ ανησυχεί ιδιαίτερα για τρομοκρατική επίθεση κατά τους επόμενους 12 μήνες[20]. Η μεγάλη πλειονότητα των πρόσφατων τρομοκρατικών επιθέσεων ήταν επιθέσεις «χαμηλής τεχνολογίας», από μοναχικούς δράστες που στοχεύουν άτομα σε δημόσιους χώρους, ενώ η διαδικτυακή τρομοκρατική προπαγάνδα απέκτησε νέα σημασία με τη ζωντανή μετάδοση των επιθέσεων στο Christchurch[21]. Η απειλή από τα ριζοσπαστικοποιημένα άτομα παραμένει υψηλή —ενισχυμένη δυνητικά από επιστρέφοντες αλλοδαπούς τρομοκράτες μαχητές και από εξτρεμιστές που αποφυλακίζονται[22].

Η κρίση κατέδειξε επίσης πώς οι υφιστάμενες απειλές μπορούν να εξελιχθούν στο πλαίσιο νέων περιστάσεων. Οι ομάδες **οργανωμένου εγκλήματος** έχουν εκμεταλλευτεί τις ελλείψεις αγαθών που δημιουργούν πεδίο δράσης για τη δημιουργία νέων παράνομων αγορών. Το εμπόριο παράνομων ναρκωτικών ουσιών παραμένει η μεγαλύτερη εγκληματική αγορά στην ΕΕ, της οποίας η εκτιμώμενη ελάχιστη λιανική αξία ανέρχεται σε 30 δισ. EUR ετησίως στην ΕΕ[23]. Η εμπορία ανθρώπων συνεχίζεται: σύμφωνα με εκτιμήσεις, τα ετήσια παγκόσμια κέρδη για όλες τις μορφές εκμετάλλευσης ανέρχονται σε περίπου 30 δισ. EUR[24].

---

[15] Οι υποδομές ζωτικής σημασίας είναι βασικές για ζωτικές κοινωνικές λειτουργίες, την υγεία, την ασφάλεια, την ασφάλεια από εξωτερικές ενέργειες, την οικονομική ή κοινωνική ευημερία, των οποίων η διαταραχή/καταστροφή έχει σημαντικές επιπτώσεις (οδηγία 2008/114/ΕΚ του Συμβουλίου).

[16] Το 97 % των πολιτών της ΕΕ έχει έρθει σε επαφή με ψευδείς ειδήσεις, το 38 % σε καθημερινή βάση. Βλ. JOIN(2020)8 final.

[17] 13 κράτη μέλη της ΕΕ ανέφεραν συνολικά 119 πραγματοποιηθείσες, αποτυχημένες και αποτραπείσες τρομοκρατικές επιθέσεις, με δέκα θανάτους και 27 τραυματισμούς (Ευρωπόλ, Έκθεση για την κατάσταση και τις τάσεις της τρομοκρατίας στην Ευρωπαϊκή Ένωση, 2020).

[18] Το 2019 σημειώθηκαν έξι ακροδεξιές τρομοκρατικές επιθέσεις (μία πραγματοποιήθηκε, μία απέτυχε, τέσσερις απετράπησαν: σε τρία κράτη μέλη), σε σύγκριση με μόνο μία το 2018, ενώ περαιτέρω θάνατοι υπήρξαν σε υποθέσεις μη χαρακτηριζόμενες ως τρομοκρατικές (Ευρωπόλ, 2020).

[19] Βλ. επίσης τη δήλωση του Συμβουλίου για την καταπολέμηση του αντισημιτισμού και την ανάπτυξη κοινής προσέγγισης για την ασφάλεια με σκοπό την καλύτερη προστασία των εβραϊκών κοινοτήτων και ιδρυμάτων στην Ευρώπη.

[20] Οργανισμός Θεμελιωδών Δικαιωμάτων της ΕΕ: Your rights matter: Security concerns and experiences (Τα δικαιώματά σας έχουν σημασία: προβληματισμοί και εμπειρίες σχετικά με την ασφάλεια), 2020.

[21] Από τον Ιούλιο του 2015 έως το τέλος του 2019, ο Ευρωπόλ εντόπισε τρομοκρατικό περιεχόμενο σε 361 πλατφόρμες (Ευρωπόλ, 2020).

[22] Ευρωπόλ: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism (Επισκόπηση των Διατλαντικών Βέλτιστων Πρακτικών για την αντιμετώπιση της ριζοσπαστικοποίησης στις φυλακές και της υποτροπής τρομοκρατών), 2019.

[23] Ευρωπαϊκό Κέντρο Παρακολούθησης Ναρκωτικών και Τοξικομανίας (ΕΚΠΝΤ) και έκθεση του Ευρωπόλ για την αγορά ναρκωτικών της ΕΕ 2019.

[24] Έκθεση του Ευρωπόλ για το χρηματοοικονομικό επιχειρηματικό μοντέλο εμπορίας ανθρώπων (2015).

Το διεθνές εμπόριο παραποιημένων φαρμακευτικών προϊόντων ανήλθε σε 38,9 δισ. EUR[25]. Ταυτόχρονα, τα χαμηλά ποσοστά κατασχέσεων επιτρέπουν στους εγκληματίες να συνεχίσουν την επέκταση των εγκληματικών τους δραστηριοτήτων και τη διείσδυση στη νόμιμη οικονομία[26]. Οι εγκληματίες και οι τρομοκράτες έχουν ευκολότερη πρόσβαση σε πυροβόλα όπλα, από τη διαδικτυακή αγορά και μέσω νέων τεχνολογιών, όπως η τρισδιάστατη εκτύπωση[27]. Η χρήση τεχνητής νοημοσύνης, οι νέες τεχνολογίες και η ρομποτική θα αυξήσουν περαιτέρω τον κίνδυνο εκμετάλλευσης των οφελών της καινοτομίας από εγκληματίες για κακόβουλους σκοπούς[28].

Οι απειλές αυτές αφορούν όλες τις κατηγορίες και πλήττουν διάφορα μέρη της κοινωνίας με διάφορους τρόπους. Συνιστούν όλες μείζονα απειλή για άτομα και επιχειρήσεις και απαιτείται συνολική και συνεκτική αντιμετώπισή τους σε επίπεδο ΕΕ. Όταν ευπάθειες ασφάλειας είναι δυνατό να προκύψουν ακόμη και από μικρά διασυνδεόμενα είδη οικιακής χρήσης, όπως ένα ψυγείο ή μια καφετιέρα συνδεδεμένη με το διαδίκτυο, δεν μπορούμε πλέον να βασιζόμαστε μόνο σε παραδοσιακούς κρατικούς παράγοντες για την κατοχύρωση της ασφάλειάς μας. Οι οικονομικοί φορείς πρέπει να αναλάβουν μεγαλύτερη ευθύνη για την κυβερνοασφάλεια των προϊόντων και των υπηρεσιών που διαθέτουν στην αγορά, ενώ τα άτομα πρέπει επίσης να έχουν τουλάχιστον μια βασική αντίληψη της κυβερνοασφάλειας, ώστε να μπορούν να αυτοπροστατεύονται.

III. Συντονισμένη αντίδραση της ΕΕ για ολόκληρη την κοινωνία

Η ΕΕ έχει ήδη δείξει πώς μπορεί να προσφέρει πραγματική προστιθέμενη αξία. Από το 2015 μέχρι σήμερα, η Ένωση Ασφάλειας έχει καθιερώσει νέες διασυνδέσεις όσον αφορά το πώς αντιμετωπίζονται οι πολιτικές ασφάλειας σε επίπεδο ΕΕ. Ωστόσο, πρέπει να εντείνουμε τις προσπάθειες για συμμετοχή ολόκληρης της κοινωνίας, συμπεριλαμβανομένων των κυβερνήσεων σε όλα τα επίπεδα, των επιχειρήσεων σε όλους τους τομείς και των ατόμων σε όλα τα κράτη μέλη. Η αυξανόμενη ευαισθητοποίηση σχετικά με τους κινδύνους της εξάρτησης[29] και η ανάγκη ισχυρής ευρωπαϊκής στρατηγικής για τη βιομηχανία[30] απαιτούν μια ΕΕ με κρίσιμη μάζα όσον αφορά τη βιομηχανία, την παραγωγή τεχνολογίας και την ανθεκτικότητα της αλυσίδας εφοδιασμού. Η δύναμη συνεπάγεται επίσης τον πλήρη σεβασμό των θεμελιωδών δικαιωμάτων και των αξιών της ΕΕ, που αποτελούν προϋπόθεση για νομιμοποιημένες, αποτελεσματικές και βιώσιμες πολιτικές ασφάλειας. Η παρούσα

---

[25] Γραφείο Διανοητικής Ιδιοκτησίας της ΕΕ και έκθεση του ΟΟΣΑ σχετικά με το εμπόριο παραποιημένων φαρμακευτικών προϊόντων

[26] Έκθεση σχετικά με την ανάκτηση και δήμευση περιουσιακών στοιχείων: Μέτρα που διασφαλίζουν ότι το έγκλημα δεν είναι προσοδοφόρο, COM(2020) 217.

[27] Το 2017, χρησιμοποιήθηκαν πυροβόλα όπλα στο 41 % του συνόλου των τρομοκρατικών επιθέσεων (Ευρωπόλ, 2018).

[28] Τον Ιούλιο του 2020, οι διωκτικές και δικαστικές αρχές της Γαλλίας και των Κάτω Χωρών, μαζί με τον Ευρωπόλ και τον Eurojust, παρουσίασαν την κοινή έρευνα για την εξάρθρωση του EncroChat, ενός δικτύου κρυπτογραφημένης τηλεφωνίας που χρησιμοποιείται από εγκληματικά δίκτυα τα οποία εμπλέκονται σε βίαιες επιθέσεις, διαφθορά, απόπειρες δολοφονίας και μεγάλης κλίμακας διακινήσεις ναρκωτικών.

[29] Οι κίνδυνοι ξένης εξάρτησης συνεπάγονται αυξημένη έκθεση σε δυνητικές απειλές: εκμετάλλευση των τρωτών σημείων των πληροφοριακών υποδομών που θέτουν σε κίνδυνο τις κρίσιμες υποδομές (π.χ. ενέργεια, μεταφορές, τραπεζικές υπηρεσίες, υγεία), έλεγχο των συστημάτων βιομηχανικού ελέγχου ή αύξηση της ικανότητας κλοπής δεδομένων ή κατασκοπείας.

[30] Ανακοίνωση της Επιτροπής με τίτλο «Μια νέα βιομηχανική στρατηγική για την Ευρώπη», COM (2020) 102.

στρατηγική για την Ένωση Ασφάλειας καθορίζει συγκεκριμένες ροές εργασίας για την προώθησή τους, οικοδομείται δε γύρω από τους ακόλουθους κοινούς στόχους:

- ***Δημιουργία δυνατοτήτων και ικανοτήτων για την έγκαιρη ανίχνευση, την πρόληψη και την ταχεία αντίδραση στις κρίσεις:*** Η Ευρώπη πρέπει να είναι ανθεκτικότερη για την πρόληψη μελλοντικών κλυδωνισμών, την προστασία από αυτούς και την αντιμετώπισή τους. Είναι αναγκαίο να δημιουργήσουμε δυνατότητες και ικανότητες για την έγκαιρη ανίχνευση και την ταχεία αντίδραση στις κρίσεις ασφάλειας, μέσω ολοκληρωμένης και συντονισμένης προσέγγισης, τόσο συνολικά όσο και με τομεακές πρωτοβουλίες (π.χ. χρηματοπιστωτικές, ενεργειακές, απονομής δικαιοσύνης, επιβολής το νόμου, υγείας, ναυτιλιακές, μεταφορών) και με βάση τα υφιστάμενα εργαλεία και πρωτοβουλίες.[31]. Η Επιτροπή θα υποβάλει επίσης προτάσεις για ευρείας εμβέλειας σύστημα διαχείρισης κρίσεων εντός της ΕΕ, το οποίο θα μπορούσε να αφορά και την ασφάλεια.

- ***Εστίαση στα αποτελέσματα***: Μια στρατηγική που βασίζεται στις επιδόσεις πρέπει να στηρίζεται σε προσεκτική αξιολόγηση των απειλών και των κινδύνων ώστε οι προσπάθειές μας να στοχοθετηθούν με τον καλύτερο δυνατό τρόπο. Πρέπει να καθορίζει και να εφαρμόζει τους κατάλληλους κανόνες και τα κατάλληλα εργαλεία. Απαιτεί αξιόπιστες στρατηγικές πληροφορίες ως βάση για τις πολιτικές ασφάλειας της ΕΕ. Όταν απαιτείται νομοθεσία της ΕΕ, πρέπει να δίνεται συνέχεια σε αυτήν, έτσι ώστε να εφαρμόζεται πλήρως και να αποφεύγονται ο κατακερματισμός και τα κενά που μπορεί κάποιος να εκμεταλλευτεί. Η αποτελεσματική εφαρμογή της στρατηγικής αυτής θα εξαρτηθεί επίσης από την εξασφάλιση της κατάλληλης χρηματοδότησης κατά την επόμενη περίοδο προγραμματισμού 2021-2027, συμπεριλαμβανομένων των συναφών οργανισμών της ΕΕ.

- ***Σύνδεση όλων των φορέων του δημόσιου και του ιδιωτικού τομέα σε μια κοινή προσπάθεια:*** Οι βασικοί παράγοντες, τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, επιδεικνύουν απροθυμία όσον αφορά την ανταλλαγή πληροφοριών σχετικά με την ασφάλεια, από φόβο μήπως αυτό υπονομεύσει την εθνική ασφάλεια ή την ανταγωνιστικότητα.[32] Είμαστε όμως πιο αποτελεσματικοί όταν όλοι αλληλοϋποστηριζόμαστε. Πρώτον, αυτό σημαίνει εντατικότερη συνεργασία μεταξύ των κρατών μελών, με τη συμμετοχή των αρχών επιβολής του νόμου, των δικαστικών αρχών και των δημόσιων αρχών, καθώς και με τα θεσμικά όργανα και τους οργανισμούς της ΕΕ, ώστε να οικοδομηθεί η κατανόηση και η ανταλλαγή που είναι αναγκαίες για κοινές λύσεις. Η συνεργασία με τον ιδιωτικό τομέα είναι επίσης καθοριστικής σημασίας, δεδομένου ότι ο κλάδος κατέχει σημαντικό μέρος της ψηφιακής και μη ψηφιακής υποδομής που είναι κεντρικής σημασίας για την αποτελεσματική καταπολέμηση του εγκλήματος και της τρομοκρατίας. Τα ίδια τα άτομα μπορούν επίσης να συνεισφέρουν, για παράδειγμα μέσω της ανάπτυξης των δεξιοτήτων και της ευαισθητοποίησης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο ή της παραπληροφόρησης. Τέλος, αυτή η κοινή προσπάθεια πρέπει να

[31] Για παράδειγμα, οι ολοκληρωμένες ρυθμίσεις για την πολιτική αντιμετώπιση κρίσεων (IPCR), το Κέντρο Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών, η σύσταση της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (C/2017/6100), το επιχειρησιακό πρωτόκολλο για την αντιμετώπιση υβριδικών απειλών (EU Playbook – Εγχειρίδιο στρατηγικής της ΕΕ) SWD (2016) 227.

[32] Κοινή ανακοίνωση με τίτλο «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ», JOIN(2017) 450.

επεκταθεί πέραν των συνόρων μας, δημιουργώντας στενότερους δεσμούς με ομοϊδεάτες εταίρους.

IV. Προστασία όλων των πολιτών στην ΕΕ: Στρατηγικές προτεραιότητες για την Ένωση Ασφάλειας

Η ΕΕ είναι στην πλέον κατάλληλη θέση να ανταποκριθεί σε αυτές τις νέες παγκόσμιες απειλές και προκλήσεις. Η ανωτέρω ανάλυση των απειλών επισημαίνει τέσσερις αλληλεξαρτώμενες στρατηγικές προτεραιότητες που πρέπει να υλοποιηθούν σε επίπεδο ΕΕ, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων: i) ένα μελλοντικά βιώσιμο περιβάλλον ασφάλειας, ii) αντιμετώπιση των εξελισσόμενων απειλών, iii) προστασία των Ευρωπαίων από την τρομοκρατία και το οργανωμένο έγκλημα, iv) ισχυρό ευρωπαϊκό οικοσύστημα ασφαλείας.

1. Διαχρονικό περιβάλλον ασφάλειας

Προστασία και ανθεκτικότητα των υποδομών ζωτικής σημασίας

Τα άτομα βασίζονται σε βασικές υποδομές στην καθημερινή τους ζωή, όταν ταξιδεύουν, εργάζονται, επωφελούνται από βασικές δημόσιες υπηρεσίες όπως τα νοσοκομεία, οι μεταφορές, ο ενεργειακός εφοδιασμός ή ασκούν τα δημοκρατικά τους δικαιώματα. Εάν οι υποδομές αυτές δεν είναι επαρκώς προστατευμένες και ανθεκτικές, οι επιθέσεις μπορούν να προκαλέσουν τεράστια αναστάτωση —είτε στον πραγματικό είτε στον ψηφιακό κόσμο— τόσο σε μεμονωμένα κράτη μέλη όσο και σε ολόκληρη την ΕΕ.

Το υφιστάμενο πλαίσιο της ΕΕ για την προστασία και την ανθεκτικότητα των υποδομών ζωτικής σημασίας[33] δεν συμβαδίζει με τους εξελισσόμενους κινδύνους. Η αύξηση των αλληλεξαρτήσεων σημαίνει ότι οι διαταραχές σε έναν τομέα μπορεί να έχουν άμεσο αντίκτυπο στη λειτουργία άλλων: μια επίθεση κατά της παραγωγής ηλεκτρικής ενέργειας θα μπορούσε να παραλύσει τις τηλεπικοινωνίες, τα νοσοκομεία, τις τράπεζες ή τα αεροδρόμια, ενώ μια επίθεση στην ψηφιακή υποδομή θα μπορούσε να οδηγήσει σε διαταραχές λειτουργίας στα δίκτυα ηλεκτρικής ενέργειας ή χρηματοδότησης. Καθώς η οικονομία και η κοινωνία μας κινούνται ολοένα και περισσότερο στο διαδίκτυο, κίνδυνοι, όπως οι παραπάνω, αυξάνονται ακόμη περισσότερο. Το νομοθετικό πλαίσιο πρέπει να αντιμετωπίσει αυτή την αυξημένη διασύνδεση και αλληλεξάρτηση, με μέτρα στιβαρής προστασίας και ανθεκτικότητας των υποδομών ζωτικής σημασίας, τόσο στον κυβερνοχώρο όσο και εκτός αυτού. Οι βασικές υπηρεσίες, συμπεριλαμβανομένων των υπηρεσιών που βασίζονται σε διαστημικές υποδομές, πρέπει να προστατεύονται επαρκώς από τις τρέχουσες και τις αναμενόμενες απειλές, αλλά και να είναι ανθεκτικές. Τούτο συνεπάγεται την ικανότητα ενός συστήματος να προετοιμάζεται για την αντιμετώπιση ανεπιθύμητων συμβάντων, να σχεδιάζει την αντίδρασή του σε αυτά, να τα απορροφά, να ανακάμπτει και να προσαρμόζεται με μεγαλύτερη επιτυχία σε αυτά.

Ταυτόχρονα, τα κράτη μέλη άσκησαν το περιθώριο διακριτικής τους ευχέρειας εφαρμόζοντας την ισχύουσα νομοθεσία με διαφορετικούς τρόπους. Ο κατακερματισμός που προκύπτει μπορεί να υπονομεύσει την εσωτερική αγορά και να καταστήσει δυσχερέστερη τη διασυνοριακή συνεργασία —προφανέστερα στις παραμεθόριες περιοχές. Οι φορείς

[33] Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ΕΕ L 194 της 19.7.2016. Οδηγία 2008/114/ΕΚ του Συμβουλίου σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους.

εκμετάλλευσης που παρέχουν βασικές υπηρεσίες σε διάφορα κράτη μέλη είναι υποχρεωμένοι να συμμορφώνονται με διαφορετικά καθεστώτα υποβολής εκθέσεων. Η Επιτροπή εξετάζει κατά πόσον τα **νέα πλαίσια τόσο για τις υλικές όσο και για τις ψηφιακές υποδομές** θα μπορούσαν να προσφέρουν μεγαλύτερη συνοχή και πιο συνεκτική προσέγγιση για τη διασφάλιση της αξιόπιστης παροχής βασικών υπηρεσιών. Το πλαίσιο αυτό πρέπει να συνοδεύεται από **τομεακές πρωτοβουλίες** για την αντιμετώπιση των ειδικών κινδύνων που αντιμετωπίζουν οι κρίσιμες υποδομές, όπως στους τομείς των μεταφορών, του διαστήματος, της ενέργειας, των οικονομικών και της υγείας[34]. Δεδομένης της υψηλής εξάρτησης του χρηματοπιστωτικού τομέα από τις υπηρεσίες ΤΠ και της υψηλής ευαισθησίας του σε κυβερνοεπιθέσεις, ένα πρώτο βήμα θα είναι μια πρωτοβουλία για την ψηφιακή λειτουργική ανθεκτικότητα των χρηματοπιστωτικών τομέων. Λόγω των ιδιαίτερων ευαισθησιών και του αντικτύπου του ενεργειακού συστήματος, μια ειδική πρωτοβουλία θα στηρίξει την ενίσχυση της ανθεκτικότητας των υποδομών ενέργειας κρίσιμης σημασίας έναντι των φυσικών απειλών, κυβερνοαπειλών και υβριδικών απειλών, εξασφαλίζοντας ίσους όρους ανταγωνισμού για τους φορείς εκμετάλλευσης ενέργειας σε διασυνοριακό επίπεδο.

Τα σχετικά με την ασφάλεια αποτελέσματα των άμεσων ξένων επενδύσεων που ενδέχεται να επηρεάσουν υποδομές ζωτικής σημασίας ή κρίσιμες τεχνολογίες θα υπόκεινται επίσης στις αξιολογήσεις που διενεργούνται από τα κράτη μέλη της ΕΕ και την Επιτροπή στο πλαίσιο του νέου ευρωπαϊκού πλαισίου για τον έλεγχο των άμεσων ξένων επενδύσεων[35].

Η ΕΕ μπορεί επίσης να δημιουργήσει νέα εργαλεία για τη στήριξη της ανθεκτικότητας των υποδομών ζωτικής σημασίας. Το παγκόσμιο διαδίκτυο έχει μέχρι στιγμής επιδείξει υψηλό επίπεδο ανθεκτικότητας, ιδίως όσον αφορά την ικανότητα στήριξης του αυξημένου όγκου κυκλοφορίας. Ωστόσο, πρέπει να είμαστε προετοιμασμένοι για πιθανές μελλοντικές κρίσεις που απειλούν την ασφάλεια, τη σταθερότητα και την ανθεκτικότητα του διαδικτύου. Διασφάλιση της αδιάλειπτης λειτουργίας του διαδικτύου σημαίνει στιβαρότητα έναντι κυβερνοπεριστατικών και κακόβουλων διαδικτυακών δραστηριοτήτων και περιορισμό της εξάρτησής του από τις υποδομές και τις υπηρεσίες που βρίσκονται εκτός Ευρώπης. Τούτο θα απαιτήσει συνδυασμό νομοθεσίας, με αναθεώρηση των υφιστάμενων κανόνων, ώστε να εξασφαλιστεί υψηλό κοινό επίπεδο ασφάλειας των συστημάτων δικτύων και πληροφοριών στην ΕΕ· περισσότερες επενδύσεις σε έρευνα και καινοτομία· και μέριμνα για ανάπτυξη ή ενίσχυση των βασικών υποδομών και πόρων του διαδικτύου, ιδίως του συστήματος ονομάτων τομέα[36].

---

[34] Δεδομένου ότι ο τομέας της υγείας έχει υποστεί πιέσεις, ιδίως κατά τη διάρκεια της κρίσης COVID-19, η Επιτροπή θα εξετάσει επίσης πρωτοβουλίες για την ενίσχυση του πλαισίου ασφάλειας της υγείας της ΕΕ και των αρμόδιων οργανισμών της ΕΕ για την αντιμετώπιση σοβαρών διασυνοριακών απειλών κατά της υγείας.

[35] Με την πλήρη εφαρμογή του, στις 11 Οκτωβρίου 2020, ο κανονισμός (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαρτίου 2019, για τη θέσπιση πλαισίου για τον έλεγχο των άμεσων ξένων επενδύσεων στην Ένωση θα παράσχει στην ΕΕ έναν νέο μηχανισμό συνεργασίας για τις άμεσες επενδύσεις από χώρες εκτός της ΕΕ που ενδέχεται να επηρεάσουν την ασφάλεια ή τη δημόσια τάξη. Βάσει του κανονισμού, τα κράτη μέλη και η Επιτροπή θα αξιολογούν τους πιθανούς κινδύνους που συνδέονται με τις εν λόγω άμεσες ξένες επενδύσεις και, όταν ενδείκνυται, σε σχέση με περισσότερα του ενός κράτη μέλη, θα προτείνουν επαρκή μέσα για τον μετριασμό των εν λόγω κινδύνων.

[36] Το σύστημα ονομάτων τομέα (DNS) είναι ένα ιεραρχικό και αποκεντρωμένο σύστημα ονοματοδοσίας για υπολογιστές. υπηρεσίες ή άλλους πόρους που συνδέονται στο διαδίκτυο ή σε ιδιωτικό δίκτυο. Μεταφράζει ονόματα τομέα στις διευθύνσεις IP που απαιτούνται για τον εντοπισμό και την ταυτοποίηση των υπηρεσιών και των συσκευών πληροφορικής.

Κύριο στοιχείο για την προστασία των βασικών ψηφιακών περιουσιακών στοιχείων της ΕΕ και των κρατών μελών είναι η παροχή διαύλου ασφαλών επικοινωνιών για τις υποδομές ζωτικής σημασίας. Η Επιτροπή συνεργάζεται με τα κράτη μέλη για να δημιουργήσει πιστοποιημένη ασφαλή διατερματική κβαντική υποδομή, επίγεια και διαστημική, σε συνδυασμό με το ασφαλές σύστημα κυβερνητικών δορυφορικών επικοινωνιών που προβλέπεται στον κανονισμό για το διαστημικό πρόγραμμα[37].

Κυβερνοασφάλεια

Ο αριθμός των κυβερνοεπιθέσεων εξακολουθεί να αυξάνεται[38]. Οι επιθέσεις αυτές είναι πιο εξελιγμένες από ποτέ, προέρχονται από ευρύ φάσμα πηγών εντός και εκτός της ΕΕ, και στοχεύουν τομείς μέγιστης τρωτότητας. Σε αυτές συμμετέχουν συχνά κρατικοί ή υποστηριζόμενοι από κράτη φορείς, και στοχεύουν βασικές ψηφιακές υποδομές, όπως είναι οι μεγάλοι πάροχοι υπηρεσιών υπολογιστικού νέφους[39]. Οι κίνδυνοι στον κυβερνοχώρο έχουν εξελιχθεί σε σημαντική απειλή και για το χρηματοπιστωτικό σύστημα. Το Διεθνές Νομισματικό Ταμείο έχει υπολογίσει την ετήσια ζημία από κυβερνοεπιθέσεις στο 9 % του καθαρού εισοδήματος των τραπεζών σε παγκόσμιο επίπεδο, ήτοι σε περίπου 100 δισ. δολάρια ΗΠΑ[40]. Η στροφή προς τις συνδεδεμένες συσκευές θα αποφέρει σημαντικά οφέλη στους χρήστες. Ωστόσο, καθώς θα αποθηκεύονται και θα υποβάλλονται σε επεξεργασία λιγότερα δεδομένα στα κέντρα δεδομένων, ενώ η επεξεργασία τους θα γίνεται εγγύτερα στον χρήστη «στις παρυφές»[41], η κυβερνοασφάλεια δεν θα μπορεί πλέον να επικεντρώνεται στην προστασία των κεντρικών σημείων.[42]

Το 2017 η ΕΕ πρότεινε μια προσέγγιση για την κυβερνοασφάλεια, βασιζόμενη στη δημιουργία ανθεκτικότητας, στην ταχεία αντίδραση και στην αποτελεσματική αποτροπή.[43] Η ΕΕ πρέπει τώρα να εξασφαλίσει ότι η δυναμικότητά της στον τομέα της κυβερνοασφάλειας συμβαδίζει με την πραγματικότητα, για την επίτευξη τόσο ανθεκτικότητας όσο και αντίδρασης. Τούτο απαιτεί μια προσέγγιση που θα συνδέει πραγματικά όλες τις συνιστώσες της κοινωνίας, ενώ τα θεσμικά και λοιπά όργανα και οργανισμοί της ΕΕ, τα κράτη μέλη, ο βιομηχανικός κλάδος, η πανεπιστημιακή κοινότητα και οι ιδιώτες θα δίνουν στην κυβερνοασφάλεια την προτεραιότητα που απαιτείται[44]. Η οριζόντια αυτή προσέγγιση, πάλι, πρέπει να συμπληρωθεί με τομεακές προσεγγίσεις για την κυβερνοασφάλεια σε τομείς όπως η ενέργεια, οι χρηματοπιστωτικές υπηρεσίες, οι μεταφορές ή η υγεία. Η επόμενη φάση των εργασιών της ΕΕ θα πρέπει να αποτυπωθεί από κοινού στην αναθεωρημένη ευρωπαϊκή στρατηγική για την κυβερνοασφάλεια.

---

37 Πρόταση κανονισμού για τη θέσπιση του διαστημικού προγράμματος της Ένωσης και του Οργανισμού της Ευρωπαϊκής Ένωσης για το διαστημικό πρόγραμμα. COM(2018) 447.

38 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

39 Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS) εξακολουθούν να αποτελούν μόνιμη απειλή: οι μεγάλοι πάροχοι υποχρεώθηκαν να αμβλύνουν τις επιπτώσεις μαζικών επιθέσεων DDoS, όπως ήταν η επίθεση κατά των διαδικτυακών υπηρεσιών της Amazon τον Φεβρουάριο του 2020.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

41 Η υπολογιστική παρυφών είναι μία κατανεμημένη, ανοιχτή αρχιτεκτονική ΤΠ, με αποκεντρωμένη επεξεργαστική ισχύ, που καθιστά δυνατή την κινητή υπολογιστική και τις τεχνολογίες του διαδικτύου των πραγμάτων (IoT). Στην υπολογιστική παρυφών τα δεδομένα υποβάλλονται σε επεξεργασία από την ίδια τη συσκευή ή από τοπικό υπολογιστή ή εξυπηρετητή, αντί να διαβιβάζονται σε κέντρο δεδομένων.

42 Ανακοίνωση με τίτλο «Ευρωπαϊκή στρατηγική για τα δεδομένα», COM (2020) 66 final.

43 Κοινή ανακοίνωση με τίτλο «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ», JOIN(2017) 450.

44 Η έκθεση με τίτλο «Cybersecurity — our digital Anchor» («Κυβερνοασφάλεια: η ψηφιακή μας άγκυρα») του Κοινού Κέντρου Ερευνών παρέχει πολυδιάστατες πληροφορίες για την ανάπτυξη της κυβερνοασφάλειας κατά τα τελευταία 40 έτη.

Η διερεύνηση νέων και ενισχυμένων μορφών συνεργασίας μεταξύ των υπηρεσιών πληροφοριών, του INTCEN της ΕΕ και άλλων οργανισμών που δραστηριοποιούνται στον τομέα της ασφάλειας θα πρέπει να αποτελεί μέρος των προσπαθειών για την ενίσχυση της κυβερνοασφάλειας, καθώς και για την καταπολέμηση της τρομοκρατίας, του εξτρεμισμού, του ριζοσπαστισμού και των υβριδικών απειλών.

Δεδομένης της εν εξελίξει εγκατάστασης της **υποδομής 5G** ανά την ΕΕ και της δυνητικής εξάρτησης πολλών υπηρεσιών κρίσιμης σημασίας από τα δίκτυα 5G, οι συνέπειες μιας συστημικής και ευρείας έκτασης διακοπής λειτουργίας θα ήταν ιδιαίτερα σοβαρές. Η διαδικασία που θεσπίστηκε με τη σύσταση της Επιτροπής του 2019 για την κυβερνοασφάλεια δικτύων 5G[45] έχει πλέον οδηγήσει σε συγκεκριμένα μέτρα των κρατών μελών σχετικά με τα βασικά μέτρα που ορίζονται στην εργαλειοθήκη 5G[46].

Μία από τις σημαντικότερες μακροπρόθεσμες ανάγκες είναι η ανάπτυξη μιας νοοτροπίας για την **κυβερνοασφάλεια ήδη από τον σχεδιασμό**, με την πτυχή της ασφάλειας να ενσωματώνεται εξ αρχής σε προϊόντα και υπηρεσίες. Σε αυτό θα συμβάλει σημαντικά το νέο πλαίσιο πιστοποίησης της κυβερνοασφάλειας δυνάμει της πράξης για την ασφάλεια στον κυβερνοχώρο[47]. Το πλαίσιο βρίσκεται ήδη σε εξέλιξη: δύο συστήματα πιστοποίησης είναι ήδη στο στάδιο της προετοιμασίας και οι προτεραιότητες για περαιτέρω συστήματα αναμένεται να οριστούν αργότερα εντός του έτους. Η συνεργασία μεταξύ του οργανισμού της ΕΕ για την κυβερνοασφάλεια (ENISA), των αρχών προστασίας των δεδομένων και του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[48] έχει καίρια σημασία σε αυτόν τον τομέα.

Η Επιτροπή έχει ήδη επισημάνει την ανάγκη για μια **Κοινή Μονάδα Κυβερνοχώρου** που θα εξασφαλίζει διαρθρωμένη και συντονισμένη επιχειρησιακή συνεργασία. Σε αυτή θα μπορούσε να περιλαμβάνεται ένας μηχανισμός αμοιβαίας συνδρομής σε περιόδους κρίσης σε επίπεδο ΕΕ. Με βάση την εφαρμογή της σύστασης[49], η Κοινή Μονάδα Κυβερνοχώρου θα μπορούσε να οικοδομήσει εμπιστοσύνη μεταξύ των διαφόρων παραγόντων του ευρωπαϊκού οικοσυστήματος κυβερνοασφάλειας και να προσφέρει μια βασική υπηρεσία στα κράτη μέλη. Η Επιτροπή θα ξεκινήσει συζητήσεις με τους σχετικούς ενδιαφερόμενους φορείς (αρχής γενομένης από τα κράτη μέλη) και θα καθορίσει σαφή διαδικασία, ορόσημα και χρονοδιάγραμμα έως το τέλος του 2020.

Το ίδιο σημαντικοί είναι οι κοινοί κανόνες για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια για όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ. Στόχος θα πρέπει να είναι η δημιουργία υποχρεωτικών και υψηλών κοινών προτύπων για την ασφαλή ανταλλαγή πληροφοριών και την ασφάλεια των ψηφιακών υποδομών και συστημάτων σε όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ. Το νέο αυτό πλαίσιο θα πρέπει να στηρίζει μια ισχυρή και αποτελεσματική επιχειρησιακή συνεργασία για την κυβερνοασφάλεια σε όλα τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ, με

[45] Σύσταση της Επιτροπής για την κυβερνοασφάλεια δικτύων 5G, COM (2019) 2335 final. Η σύσταση προβλέπει την επανεξέτασή της κατά το τελευταίο τρίμηνο του 2020.

[46] Βλ. την έκθεση της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών σχετικά με την εφαρμογή της εργαλειοθήκης, της 24ης Ιουλίου 2020.

[47] Κανονισμός 2019/881 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών (πράξη για την κυβερνοασφάλεια).

[48] Ανακοίνωση με τίτλο: «Η προστασία των δεδομένων ως πυλώνας της ενδυνάμωσης των πολιτών και της προσέγγισης της ΕΕ στην ψηφιακή μετάβαση — δύο έτη εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων», COM(2020) 264.

[49] Σύσταση 2017/1584 της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

επίκεντρο τον ρόλο της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-EU) για τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ.

Δεδομένου του παγκόσμιου χαρακτήρα τους, η οικοδόμηση και διατήρηση ισχυρών **διεθνών εταιρικών σχέσεων** είναι θεμελιώδους σημασίας για την περαιτέρω πρόληψη, αποτροπή και αντιμετώπιση των κυβερνοεπιθέσεων. Το πλαίσιο για μια κοινή διπλωματική αντίδραση της ΕΕ σε κακόβουλες δραστηριότητες στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»)[50] καθορίζει μέτρα στο πλαίσιο της κοινής εξωτερικής πολιτικής και πολιτικής ασφάλειας, συμπεριλαμβανομένων των περιοριστικών μέτρων (κυρώσεων), τα οποία μπορούν να χρησιμοποιηθούν για την αντιμετώπιση δραστηριοτήτων που βλάπτουν τα πολιτικά και οικονομικά συμφέροντά της καθώς και τα συμφέροντά της στον τομέα της ασφάλειας. Η ΕΕ θα πρέπει επίσης να εμβαθύνει τις εργασίες της μέσω ταμείων ανάπτυξης και συνεργασίας για τη δημιουργία ικανοτήτων με σκοπό τη στήριξη των κρατών εταίρων ώστε να ενισχύσουν τα ψηφιακά οικοσυστήματά τους, να υλοποιήσουν εθνικές νομοθετικές μεταρρυθμίσεις και να τηρήσουν τα διεθνή πρότυπα. Με τον τρόπο αυτό ενισχύονται η ανθεκτικότητα της συνολικής κοινότητας και η ικανότητά της να αντιδρά και να αντιμετωπίζει αποτελεσματικά τις κυβερνοαπειλές. Αυτό περιλαμβάνει ειδικές εργασίες για την προώθηση των προτύπων της ΕΕ και της σχετικής νομοθεσίας για την αύξηση της κυβερνοασφάλειας των χωρών εταίρων στις γειτονικές χώρες[51].

Προστασία των δημόσιων χώρων

Οι πρόσφατες τρομοκρατικές επιθέσεις έθεσαν στο στόχαστρο **δημόσιους χώρους**, συμπεριλαμβανομένων τόπων λατρείας και συγκοινωνιακών κόμβων, εκμεταλλευόμενες τον ανοικτό και προσβάσιμο χαρακτήρα τους. Η άνοδος της τρομοκρατίας που πυροδοτήθηκε από τον πολιτικό ή τον ιδεολογικά υποκινούμενο εξτρεμισμό επέτεινε αυτή την απειλή. Αυτό απαιτεί αφενός μεγαλύτερη φυσική προστασία των τόπων αυτών και αφετέρου επαρκή συστήματα ανίχνευσης, χωρίς να υπονομεύονται οι ελευθερίες των πολιτών[52]. Η Επιτροπή θα ενισχύσει τη συνεργασία δημόσιου και ιδιωτικού τομέα για την προστασία των δημόσιων χώρων, με χρηματοδότηση, ανταλλαγή πείρας και ορθών πρακτικών, ειδική καθοδήγηση[53] και συστάσεις[54]. Η προσέγγιση που θα υιοθετηθεί θα περιλαμβάνει επίσης ευαισθητοποίηση, απαιτήσεις επιδόσεων, δοκιμές του εξοπλισμού ανίχνευσης και ενίσχυση των ελέγχων ιστορικού για την αντιμετώπιση απειλών εκ των έσω. Μια σημαντική πτυχή που πρέπει να ληφθεί υπόψη είναι το γεγονός ότι οι μειονότητες και τα ευάλωτα άτομα μπορούν να πλήττονται δυσανάλογα, συμπεριλαμβανομένων των προσώπων που αποτελούν στόχο λόγω της θρησκείας ή του φύλου τους και τα οποία, ως εκ τούτου, χρήζουν ιδιαίτερης προσοχής. Οι περιφερειακές και τοπικές δημόσιες αρχές καλούνται να διαδραματίσουν σημαντικό ρόλο στη βελτίωση της ασφάλειας των δημόσιων χώρων. Η Επιτροπή συμβάλλει επίσης στην ενίσχυση της καινοτομίας των πόλεων στον

---

50 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

51 Βλ. τις κατευθυντήριες γραμμές για την ανάπτυξη των εξωτερικών ικανοτήτων της ΕΕ στον κυβερνοχώρο, 26 Ιουνίου 2018.

52 Τα συστήματα εξ αποστάσεως βιομετρικής ταυτοποίησης απαιτούν ειδική εξέταση. Οι αρχικές απόψεις της Επιτροπής περιγράφονται στη Λευκή Βίβλο της Επιτροπής, της 19ης Φεβρουαρίου 2020, για την τεχνητή νοημοσύνη, COM(2020) 65.

53 Όπως για παράδειγμα, οι κατευθυντήριες γραμμές για την επιλογή κατάλληλων λύσεων φραγμάτων ασφαλείας για την προστασία του δημόσιου χώρου (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 Κατευθυντήριες γραμμές για τις ορθές πρακτικές παρέχονται στο SWD(2019) 140, συμπεριλαμβανομένης μιας ενότητας για τη συνεργασία δημόσιου και ιδιωτικού τομέα. Η χρηματοδότηση στο πλαίσιο του ΤΕΑ-Ασυνομική συνεργασία επικεντρώνεται ιδιαίτερα στην ενίσχυση της συνεργασίας δημόσιου και ιδιωτικού τομέα.

τομέα της ασφάλειας σε δημόσιους χώρους[55]. Η δρομολόγηση της νέας εταιρικής σχέσης του αστικού θεματολογίου[56] για την «ασφάλεια σε δημόσιους χώρους», τον Νοέμβριο του 2018, είναι ενδεικτική της ισχυρής δέσμευσης των κρατών μελών, της Επιτροπής και των πόλεων να αντιμετωπίσουν καλύτερα τις απειλές κατά της ασφάλειας στον αστικό χώρο.

Η αγορά των **δρόνων** εξακολουθεί να επεκτείνεται, με πολλές πολύτιμες και νόμιμες χρήσεις. Ωστόσο, οι δρόνοι μπορούν επίσης να χρησιμοποιηθούν με κακούς σκοπούς από εγκληματίες και τρομοκράτες, και οι δημόσιοι χώροι είναι ιδιαίτερα εκτεθειμένοι σε απειλές. Οι στόχοι μπορούν να περιλαμβάνουν άτομα, συναθροίσεις, υποδομές ζωτικής σημασίας, αρχές επιβολής του νόμου, σύνορα ή δημόσιους χώρους. Οι γνώσεις σχετικά με τη χρήση δρόνων σε διενέξεις θα μπορούσαν να επιστρέψουν στην Ευρώπη είτε απευθείας (μέσω της επιστροφής αλλοδαπών τρομοκρατών μαχητών) είτε μέσω του διαδικτύου. Οι κανόνες που έχουν ήδη αναπτυχθεί από τον Ευρωπαϊκό Οργανισμό Ασφάλειας της Αεροπορίας αποτελούν ένα σημαντικό πρώτο βήμα σε τομείς όπως η καταγραφή των φορέων εκμετάλλευσης δρόνων και η υποχρεωτική εξ αποστάσεως ταυτοποίηση των δρόνων. Δεδομένου ότι οι δρόνοι γίνονται όλο και πιο ευρέως διαθέσιμοι, πιο προσιτοί από οικονομική άποψη και πιο ικανοί, υπάρχει ανάγκη για περαιτέρω δράση. Αυτή θα μπορούσε να περιλαμβάνει την ανταλλαγή πληροφοριών, την καθοδήγηση και την ορθή πρακτική για χρήση από όλους, συμπεριλαμβανομένων των αρχών επιβολής του νόμου, καθώς και περισσότερες δοκιμές για αντίμετρα έναντι των δρόνων[57]. Επιπλέον, θα πρέπει να αναλυθούν περαιτέρω και να αντιμετωπιστούν οι επιπτώσεις από τη χρήση δρόνων σε δημόσιους χώρους για την προστασία της ιδιωτικής ζωής και των δεδομένων.

Βασικές δράσεις

- Νομοθεσία σχετικά με την προστασία και την ανθεκτικότητα των υποδομών ζωτικής σημασίας
- Αναθεώρηση της οδηγίας για τα συστήματα δικτύου και πληροφοριών
- Πρωτοβουλία για την επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα.
- Προστασία και κυβερνοασφάλεια των υποδομών ενέργειας ζωτικής σημασίας και κώδικας δικτύου για την κυβερνοασφάλεια για διασυνοριακές ροές ηλεκτρικής ενέργειας
- Ευρωπαϊκή στρατηγική κυβερνοασφάλειας
- Επόμενα βήματα προς τη δημιουργία μιας Κοινής Μονάδας Κυβερνοχώρου
- Κοινοί κανόνες για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ
- Ενίσχυση της συνεργασίας για την προστασία των δημόσιων χώρων, συμπεριλαμβανομένων των χώρων λατρείας
- Ανταλλαγή βέλτιστων πρακτικών για την αντιμετώπιση της κακής χρήσης των δρόνων

[55] Τρεις πόλεις (ο Πειραιάς στην Ελλάδα, το Tampere στη Φινλανδία και το Τορίνο στην Ιταλία) θα δοκιμάσουν νέες λύσεις στο πλαίσιο των αστικών καινοτόμων δράσεων, οι οποίες συγχρηματοδοτούνται από το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης (ΕΤΠΑ).

[56] Το Αστικό Θεματολόγιο για την ΕΕ αποτελεί μια νέα πολυεπίπεδη μέθοδο εργασίας για την προώθηση της συνεργασίας μεταξύ των κρατών μελών, των πόλεων, της Ευρωπαϊκής Επιτροπής και άλλων ενδιαφερόμενων φορέων με σκοπό την τόνωση της ανάπτυξης, της ποιότητας ζωής και της καινοτομίας στις πόλεις της Ευρώπης και τον προσδιορισμό και την επιτυχή αντιμετώπιση των κοινωνικών προκλήσεων.

[57] Πρόσφατα θεσπίστηκε πολυετές πρόγραμμα δοκιμών για τη στήριξη των κρατών μελών στην ανάπτυξη κοινής μεθοδολογίας και πλατφόρμας δοκιμών στον εν λόγω τομέα.

2. Αντιμετώπιση των εξελισσόμενων απειλών

Κυβερνοέγκλημα

Η τεχνολογία δημιουργεί νέες δυνατότητες για την κοινωνία. Παρέχει επίσης νέα εργαλεία στις δικαστικές αρχές και στις αρχές επιβολής του νόμου. Ταυτόχρονα όμως προσφέρει ευκαιρίες δράσης στους εγκληματίες. Το κακόβουλο λογισμικό, η κλοπή προσωπικών ή επιχειρηματικών δεδομένων με δικτυοπαραβίαση (hacking), και η διακοπή της ψηφιακής δραστηριότητας που προκαλεί οικονομική ζημία ή ζημία για τη φήμη αυξάνονται. Το ανθεκτικό περιβάλλον που δημιουργεί η ισχυρή κυβερνοασφάλεια είναι η πρώτη γραμμή άμυνας. Οι αρχές επιβολής του νόμου πρέπει να είναι σε θέση να εργάζονται στον τομέα των ψηφιακών ερευνών με σαφείς κανόνες, για να μπορούν να διερευνούν και να διώκουν τα εγκλήματα και να προσφέρουν στα θύματα την αναγκαία προστασία. Οι εργασίες αυτές θα πρέπει να βασιστούν στην κοινή ομάδα δράσης για το κυβερνοέγκλημα του Ευρωπόλ και στο πρωτόκολλο αντιμετώπισης καταστάσεων έκτακτης ανάγκης στον τομέα της επιβολής του νόμου, το οποίο δημιουργήθηκε με σκοπό τον συντονισμό της αντιμετώπισης κυβερνοεπιθέσεων μεγάλης κλίμακας. Καθοριστικής σημασίας είναι επίσης οι αποτελεσματικοί μηχανισμοί που επιτρέπουν τις συμπράξεις και τη συνεργασία δημόσιου και ιδιωτικού τομέα.

Παράλληλα, η καταπολέμηση του κυβερνοεγκλήματος θα πρέπει να αποτελέσει στρατηγική επικοινωνιακή προτεραιότητα σε ολόκληρη την ΕΕ, ώστε να ενημερωθούν οι Ευρωπαίοι πολίτες για τους κινδύνους και τα προληπτικά μέτρα που μπορούν να λάβουν. Αυτό θα πρέπει να αποτελεί μέρος μιας προληπτικής προσέγγισης. Ένα ουσιαστικό βήμα είναι επίσης η πλήρης εφαρμογή του ισχύοντος νομικού πλαισίου[58]: η Επιτροπή θα είναι έτοιμη να χρησιμοποιήσει διαδικασίες επί παραβάσει κατά περίπτωση, καθώς και να διατηρήσει το παρόν πλαίσιο υπό επανεξέταση, ώστε να διασφαλιστεί ότι εξακολουθεί να είναι κατάλληλο για τον επιδιωκόμενο σκοπό. Η Επιτροπή θα διερευνήσει επίσης, από κοινού με τον Ευρωπόλ και τον ENISA, δηλαδή τον Οργανισμό κυβερνοασφάλειας της ΕΕ, τη σκοπιμότητα ενός ενωσιακού συστήματος έγκαιρης προειδοποίησης σχετικό με το κυβερνοέγκλημα, το οποίο θα μπορούσε να διασφαλίσει τη ροή πληροφοριών και την ταχεία αντίδραση στα κυβερνοεγκλήματα.

Το κυβερνοέγκλημα αποτελεί παγκόσμια πρόκληση για τη οποία απαιτείται αποτελεσματική διεθνής συνεργασία. Η ΕΕ στηρίζει τη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, η οποία αποτελεί ένα αποτελεσματικό, εδραιωμένο πλαίσιο που επιτρέπει σε όλες τις χώρες να προσδιορίζουν τι συστήματα και διαύλους επικοινωνίας χρειάζονται για να μπορούν να συνεργάζονται αποτελεσματικά μεταξύ τους.

Σχεδόν το ήμισυ των πολιτών της ΕΕ ανησυχούν για την κακή χρήση των δεδομένων[59] και η **κλοπή ταυτότητας** αποτελεί μείζον πρόβλημα[60]. Η δόλια χρήση ταυτότητας για οικονομικό κέρδος είναι μία πτυχή, αλλά μπορεί επίσης να υπάρξει σημαντικός προσωπικός και ψυχολογικός αντίκτυπος, με παράνομες αναρτήσεις εκ μέρους του καταχραστή της

---

58 Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών.

59 46 % (Ευρωβαρόμετρο για τη στάση των Ευρωπαίων απέναντι στην κυβερνοασφάλεια, Ιανουάριος 2020).

60 Η συντριπτική πλειονότητα όσων απάντησαν στο Ευρωβαρόμετρο του 2018 με τίτλο «Η στάση των Ευρωπαίων απέναντι στην ασφάλεια στο Διαδίκτυο» (95 %) θεωρούσαν ότι η κλοπή ταυτότητας συνιστά σοβαρό έγκλημα, και επτά στους δέκα δηλώνουν ότι πρόκειται για πολύ σοβαρό έγκλημα. Το Ευρωβαρόμετρο που δημοσιεύτηκε τον Ιανουάριο του 2020 επιβεβαίωσε τις ανησυχίες σχετικά με το κυβερνοέγκλημα, την ηλεκτρονική απάτη και την κλοπή ταυτότητας: τα δύο τρίτα όσων απάντησαν εξέφρασαν ανησυχία σχετικά με την τραπεζική απάτη (67 %) ή την κλοπή ταυτότητας (66 %)

ταυτότητας που μπορούν να μείνουν στο δίκτυο επί πολλά έτη. Η Επιτροπή θα διερευνήσει πιθανά πρακτικά μέτρα για την προστασία των θυμάτων από όλες τις μορφές κλοπής ταυτότητας, λαμβάνοντας υπόψη την επικείμενη πρωτοβουλία για την ευρωπαϊκή ψηφιακή ταυτότητα[61].

Η αντιμετώπιση του κυβερνοεγκλήματος απαιτεί να κοιτάμε μπροστά. Καθώς η κοινωνία αξιοποιεί τις νέες τεχνολογικές εξελίξεις για την ενίσχυση της οικονομίας και της κοινωνίας, οι κακοποιοί προσπαθούν επίσης να αξιοποιήσουν τα εργαλεία αυτά για να επιτύχουν δόλιους στόχους. Για παράδειγμα, οι κακοποιοί μπορούν να χρησιμοποιήσουν την τεχνητή νοημοσύνη για να εντοπίσουν και να αναγνωρίσουν κωδικούς πρόσβασης ή για να απλουστεύσουν τη δημιουργία κακόβουλου λογισμικού, για να εκμεταλλευτούν εικόνες και αρχεία ήχου που μπορούν στη συνέχεια να χρησιμοποιηθούν για την κλοπή ταυτότητας ή για απάτη.

Σύγχρονες μέθοδοι επιβολής του νόμου

Οι επαγγελματίες στους τομείς της επιβολής του νόμου και της δικαιοσύνης πρέπει να προσαρμοστούν στη νέα τεχνολογία. Οι τεχνολογικές εξελίξεις και οι αναδυόμενες απειλές απαιτούν από τις αρχές επιβολής του νόμου να έχουν πρόσβαση σε νέα εργαλεία, να αποκτούν νέες δεξιότητες και να αναπτύξουν εναλλακτικές τεχνικές έρευνας. Συμπληρωματικά προς τις νομοθετικές δράσεις που αποσκοπούν στη βελτίωση της διασυνοριακής πρόσβασης σε ηλεκτρονικά αποδεικτικά στοιχεία για ποινικές έρευνες, η ΕΕ μπορεί να βοηθήσει τις αρχές επιβολής του νόμου να αναπτύξουν την αναγκαία ικανότητα για τον εντοπισμό, την προστασία και την ανάγνωση των δεδομένων που απαιτούνται για τη διερεύνηση εγκλημάτων και τη χρήση των δεδομένων αυτών ως αποδεικτικών στοιχείων στο δικαστήριο. Η Επιτροπή θα διερευνήσει μέτρα για την **ενίσχυση της ικανότητας επιβολής του νόμου στις ψηφιακές έρευνες**, καθορίζοντας τον τρόπο βέλτιστης χρήσης της έρευνας και της ανάπτυξης για τη δημιουργία νέων εργαλείων επιβολής του νόμου· και τον τρόπο με τον οποίο η κατάρτιση μπορεί να προσφέρει το κατάλληλο σύνολο δεξιοτήτων στις αρχές επιβολής του νόμου και τις δικαστικές αρχές. Εν προκειμένω θα περιλαμβάνεται επίσης η παροχή αυστηρών επιστημονικών αξιολογήσεων και μεθόδων δοκιμών από το Κοινό Κέντρο Ερευνών της Επιτροπής.

Οι κοινές προσεγγίσεις μπορούν επίσης να διασφαλίσουν ότι **η τεχνητή νοημοσύνη, οι διαστημικές ικανότητες, τα μαζικά δεδομένα** και η **υπολογιστική υψηλών επιδόσεων** ενσωματώνονται στην πολιτική ασφάλειας κατά τρόπο αποτελεσματικό τόσο για την καταπολέμηση των εγκλημάτων όσο και για τη διασφάλιση των θεμελιωδών δικαιωμάτων. Η τεχνητή νοημοσύνη θα μπορούσε να λειτουργήσει ως ένα ισχυρό εργαλείο για την καταπολέμηση του εγκλήματος, δημιουργώντας τεράστιες ερευνητικές ικανότητες μέσω της ανάλυσης μεγάλου όγκου πληροφοριών και της ταυτοποίησης μοτίβων και ανωμαλιών[62]. Μπορεί επίσης να παρέχει συγκεκριμένα εργαλεία, όπως να συμβάλει στον εντοπισμό τρομοκρατικού περιεχομένου στο διαδίκτυο ή ύποπτων συναλλαγών στις πωλήσεις επικίνδυνων προϊόντων ή να παρέχει βοήθεια σε πολίτες σε καταστάσεις έκτακτης ανάγκης. Για την αξιοποίηση αυτού του δυναμικού απαιτείται συγκέντρωση της έρευνας, της καινοτομίας και των χρηστών της τεχνητής νοημοσύνης με τη σωστή διακυβέρνηση και τεχνική υποδομή, και την ενεργό συμμετοχή του ιδιωτικού τομέα και των πανεπιστημίων. Απαιτείται επίσης η τήρηση των υψηλότερων προτύπων συμμόρφωσης με τα θεμελιώδη δικαιώματα, με παράλληλη διασφάλιση της αποτελεσματικής προστασίας των πολιτών.

[61] Ανακοίνωση της 19ης Φεβρουαρίου 2020 με τίτλο «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης», COM (2020) 67.

[62] Για παράδειγμα, σε οικονομικά εγκλήματα.

Ειδικότερα, οι αποφάσεις που επηρεάζουν τα άτομα πρέπει να υποβάλλονται σε έλεγχο από ανθρώπους και να συμμορφώνονται με το σχετικό ισχύον δίκαιο της ΕΕ[63].

Ηλεκτρονικές πληροφορίες και ηλεκτρονικά αποδεικτικά στοιχεία χρειάζονται στο 85 % περίπου των ερευνών για σοβαρά εγκλήματα, ενώ το 65 % των συνολικών αιτήσεων απευθύνεται σε παρόχους που εδρεύουν σε άλλη δικαιοδοσία[64]. Το γεγονός ότι τα παραδοσιακά φυσικά ίχνη έχουν μεταφερθεί πλέον στο διαδίκτυο διευρύνει περαιτέρω το χάσμα μεταξύ των ικανοτήτων των αρχών επιβολής του νόμου και των ικανοτήτων των εγκληματιών. Η θέσπιση σαφών κανόνων για τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία για ποινικές έρευνες είναι ουσιαστικής σημασίας. Αυτός είναι ο λόγος για τον οποίο η ταχεία έγκριση από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο των προτάσεων για τα ηλεκτρονικά αποδεικτικά στοιχεία είναι καίριας σημασίας για την παροχή ενός αποτελεσματικού εργαλείου στους επαγγελματίες. Η διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία μέσω πολυμερών και διμερών διεθνών διαπραγματεύσεων είναι επίσης ιδιαίτερα σημαντική για τη θέσπιση συμβατών κανόνων σε διεθνές επίπεδο[65].

Η πρόσβαση σε ψηφιακά αποδεικτικά στοιχεία εξαρτάται επίσης από τη διαθεσιμότητα των πληροφοριών. Εάν τα δεδομένα διαγράφονται υπερβολικά γρήγορα, ενδέχεται να χαθούν σημαντικά αποδεικτικά στοιχεία, με αποτέλεσμα να μην υπάρχει πλέον η δυνατότητα εντοπισμού υπόπτων και εγκληματικών δικτύων (καθώς και θυμάτων). Από την άλλη πλευρά, τα συστήματα διατήρησης δεδομένων εγείρουν ζητήματα προστασίας της ιδιωτικής ζωής. Ανάλογα με την έκβαση των υποθέσεων που εκκρεμούν ενώπιον του Δικαστηρίου της Ευρωπαϊκής Ένωσης, η Επιτροπή θα αξιολογήσει τη μελλοντική πορεία όσον αφορά τη διατήρηση δεδομένων.

Η πρόσβαση σε πληροφορίες καταχώρισης ονομάτων τομέα («δεδομένα WHOIS»)[66] είναι σημαντική για τις ποινικές έρευνες, την κυβερνοασφάλεια και την προστασία των καταναλωτών. Ωστόσο, η πρόσβαση σε αυτές τις πληροφορίες καθίσταται δυσχερέστερη, εν αναμονή της έγκρισης μιας νέας πολιτικής WHOIS από το Σώμα του Διαδικτύου για την Εκχώρηση Ονομάτων και Αριθμών (ICANN). Η Επιτροπή θα συνεχίσει να συνεργάζεται με το ICANN και την πολυμερή κοινότητα ενδιαφερομένων προκειμένου να διασφαλιστεί ότι οι νόμιμοι αιτούντες πρόσβαση, συμπεριλαμβανομένων των αρχών επιβολής του νόμου, μπορούν να αποκτήσουν αποτελεσματική πρόσβαση στα δεδομένα WHOIS σύμφωνα με τους ενωσιακούς και τους διεθνείς κανονισμούς προστασίας των δεδομένων. Η συνεργασία αυτή θα περιλαμβάνει την αξιολόγηση πιθανών λύσεων, συμπεριλαμβανομένης της ενδεχόμενης θέσπισης νομοθεσίας για την αποσαφήνιση των κανόνων για την πρόσβαση σε τέτοιες πληροφορίες.

Οι αρχές επιβολής του νόμου και οι δικαστικές αρχές πρέπει επίσης να είναι εξοπλισμένες για να αποκτούν τα απαραίτητα δεδομένα και αποδεικτικά στοιχεία μόλις αναπτυχθεί

---

[63] Αυτό σημαίνει συμμόρφωση με την ισχύουσα νομοθεσία, συμπεριλαμβανομένου του γενικού κανονισμού (ΕΕ) 2016/679 για την προστασία των δεδομένων, καθώς και της οδηγίας (ΕΕ) 2016/680 για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, η οποία ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

[64] Commission SWD(2018) 118 final.

[65] Ειδικότερα, το δεύτερο πρόσθετο πρωτόκολλο στη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και μια συμφωνία μεταξύ της ΕΕ και των Ηνωμένων Πολιτειών σχετικά με τη διασυνοριακή πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία.

[66] Αποθηκεύονται σε βάσεις δεδομένων που τηρούνται από 2 500 φορείς εκμετάλλευσης μητρώου και καταχωριστών, σε όλο τον κόσμο.

πλήρως στην ΕΕ η **αρχιτεκτονική 5G για τις κινητές τηλεπικοινωνίες**, κατά τρόπο που να σέβεται το απόρρητο των επικοινωνιών. Η Επιτροπή θα υποστηρίξει μια ενισχυμένη και συντονισμένη προσέγγιση κατά τη διαμόρφωση διεθνών προτύπων, τον ορισμό βέλτιστων πρακτικών, διαδικασιών και τεχνικής διαλειτουργικότητας σε βασικούς τεχνολογικούς τομείς, όπως η τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων ή οι τεχνολογίες αλυσίδας συστοιχιών (blockchain).

Σήμερα, σημαντικό μέρος των ερευνών για όλες τις μορφές εγκλήματος και τρομοκρατίας περιλαμβάνει **κρυπτογραφημένες πληροφορίες**. Η κρυπτογράφηση είναι απαραίτητη στον ψηφιακό κόσμο, καθώς προστατεύει τα ψηφιακά συστήματα και τις συναλλαγές, και διαφυλάσσει μια σειρά θεμελιωδών δικαιωμάτων, μεταξύ των οποίων η ελευθερία της έκφρασης, η προστασία της ιδιωτικής ζωής και η προστασία των δεδομένων. Ωστόσο, εάν χρησιμοποιείται για εγκληματικούς σκοπούς, μπορεί επίσης να καλύπτει την ταυτότητα των εγκληματιών και να αποκρύπτει το περιεχόμενο των επικοινωνιών τους. Η Επιτροπή θα διερευνήσει και θα υποστηρίξει ισορροπημένες τεχνικές, επιχειρησιακές και νομικές λύσεις για τις προκλήσεις και θα προωθήσει μια προσέγγιση που θα διασφαλίζει τόσο την αποτελεσματικότητα της κρυπτογράφησης για την προστασία της ιδιωτικής ζωής και της ασφάλειας των επικοινωνιών, όσο και την αποτελεσματική αντιμετώπιση του εγκλήματος και της τρομοκρατίας.

Καταπολέμηση του παράνομου περιεχομένου στο διαδίκτυο

Για την εναρμόνιση της ασφάλειας του διαδικτυακού και του φυσικού περιβάλλοντος απαιτείται συνεχής πρόοδος όσον αφορά την **αντιμετώπιση του παράνομου περιεχομένου στο διαδίκτυο**. Βασικές απειλές για τους πολίτες, όπως η τρομοκρατία, ο εξτρεμισμός ή η σεξουαλική κακοποίηση παιδιών, βασίζονται ολοένα και περισσότερο στο ψηφιακό περιβάλλον, γεγονός το οποίο απαιτεί συγκεκριμένη δράση και ένα πλαίσιο για τη διασφάλιση του σεβασμού των θεμελιωδών δικαιωμάτων. Ένα ουσιαστικό πρώτο βήμα είναι η ταχεία ολοκλήρωση των διαπραγματεύσεων για την προτεινόμενη νομοθεσία σχετικά με το τρομοκρατικό περιεχόμενο στο διαδίκτυο[67] και η διασφάλιση της εφαρμογής της. Η ενίσχυση της εθελοντικής συνεργασίας μεταξύ των αρχών επιβολής του νόμου και του ιδιωτικού τομέα στο **Φόρουμ της ΕΕ για το διαδίκτυο** είναι επίσης καθοριστικής σημασίας για την καταπολέμηση της κατάχρησης του διαδικτύου από τρομοκράτες, βίαιους εξτρεμιστές και εγκληματίες. Η μονάδα της ΕΕ για την αναφορά διαδικτυακού περιεχομένου του Ευρωπόλ θα εξακολουθήσει να διαδραματίζει καίριο ρόλο στην παρακολούθηση της δραστηριότητας των τρομοκρατικών ομάδων στο διαδίκτυο και της δράσης που αναλαμβάνουν οι πλατφόρμες[68], καθώς και στην περαιτέρω ανάπτυξη του **πρωτοκόλλου διαχείρισης κρίσεων της ΕΕ**[69]. Επιπλέον, η Επιτροπή θα εξακολουθήσει να συνεργάζεται με διεθνείς εταίρους, μεταξύ άλλων συμμετέχοντας στο **παγκόσμιο φόρουμ για το διαδίκτυο και την καταπολέμηση της τρομοκρατίας**, προκειμένου να αντιμετωπιστούν οι προκλήσεις αυτές σε παγκόσμιο επίπεδο. Θα συνεχιστούν οι εργασίες για τη στήριξη της ανάπτυξης εναλλακτικών επιχειρημάτων και αντεπιχειρημάτων μέσω του προγράμματος ενδυνάμωσης της κοινωνίας των πολιτών[70].

---

[67] Πρόταση σχετικά με την πρόληψη της διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο, COM (2018) 640, 12 Σεπτεμβρίου 2018.

[68] Ευρωπόλ, Νοέμβριος 2019.

[69] Μια Ευρώπη που προστατεύει – Πρωτόκολλο διαχείρισης κρίσεων της ΕΕ: αντιμετώπιση του τρομοκρατικού περιεχομένου στο διαδίκτυο. (Οκτώβριος 2019).

[70] Συνδέεται με το έργο του προγράμματος ευαισθητοποίησης σχετικά με τη ριζοσπαστικοποίηση, βλ. ενότητα IV.3 κατωτέρω.

Για την πρόληψη και την αντιμετώπιση της διάδοσης της παράνομης ρητορικής μίσους στο διαδίκτυο, η Επιτροπή εγκαινίασε το 2016 τον κώδικα δεοντολογίας για την καταπολέμηση της παράνομης ρητορικής μίσους στο διαδίκτυο, ενώ οι διαδικτυακές πλατφόρμες δεσμεύτηκαν εθελοντικά να αφαιρούν τυχόν περιεχόμενο ρητορικής μίσους. Σύμφωνα με την τελευταία αξιολόγηση, οι εταιρείες αξιολογούν το 90 % του επισημασμένου περιεχομένου εντός 24 ωρών και αφαιρούν το 71 % του περιεχομένου που θεωρείται παράνομη ρητορική μίσους. Ωστόσο, οι πλατφόρμες πρέπει να βελτιώσουν περαιτέρω τη διαφάνεια και την ανατροφοδότηση προς τους χρήστες και να διασφαλίσουν τη συνεπή αξιολόγηση του επισημασμένου περιεχομένου[71].

Το φόρουμ της ΕΕ για το Διαδίκτυο θα διευκολύνει επίσης τις ανταλλαγές απόψεων όσον αφορά τις υφιστάμενες και τις αναπτυσσόμενες τεχνολογίες αντιμετώπισης των προκλήσεων που σχετίζονται με τη σεξουαλική κακοποίηση παιδιών στο διαδίκτυο. Η αντιμετώπιση της σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο βρίσκεται στο επίκεντρο μιας νέας στρατηγικής για την ενίσχυση της **καταπολέμησης της σεξουαλικής κακοποίησης παιδιών**[72], με την οποία επιδιώκεται να μεγιστοποιηθεί η χρήση των διαθέσιμων μέσων σε επίπεδο ΕΕ για την καταπολέμηση αυτών των εγκλημάτων. Οι εταιρείες πρέπει να είναι σε θέση να συνεχίσουν τις εργασίες τους για τον εντοπισμό και την αφαίρεση υλικού σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο, η δε ζημία που προκαλεί το υλικό αυτό απαιτεί ένα πλαίσιο που θα καθορίζει σαφείς και διαρκείς υποχρεώσεις για την αντιμετώπιση του προβλήματος. Η στρατηγική θα ανακοινώσει επίσης την έναρξη εκπόνησης, από την Επιτροπή, ειδικής τομεακής νομοθεσίας για να αντιμετωπιστεί αποτελεσματικότερα η σεξουαλική κακοποίηση παιδιών στο διαδίκτυο, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων.

Γενικότερα, η προσεχής νομοθετική πράξη για τις ψηφιακές υπηρεσίες θα αποσαφηνίσει και θα αναβαθμίσει επίσης τους κανόνες περί ευθύνης και ασφάλειας των ψηφιακών υπηρεσιών και θα άρει τα αντικίνητρα που αποθαρρύνουν ενέργειες για την αντιμετώπιση του παράνομου περιεχομένου και των παράνομων αγαθών ή υπηρεσιών.

Επιπλέον, η Επιτροπή θα εξακολουθήσει να συνεργάζεται με διεθνείς εταίρους και με το **παγκόσμιο φόρουμ για το διαδίκτυο και την καταπολέμηση της τρομοκρατίας**, μεταξύ άλλων μέσω της ανεξάρτητης συμβουλευτικής επιτροπής, με σκοπό να συζητηθεί ο τρόπος αντιμετώπισης αυτών των προκλήσεων σε παγκόσμιο επίπεδο, ενώ παράλληλα θα διαφυλάσσονται οι αξίες της ΕΕ και τα θεμελιώδη δικαιώματα. Θα πρέπει επίσης να εξεταστούν νέα θέματα, όπως οι αλγόριθμοι ή τα διαδικτυακά παιχνίδια[73].

Υβριδικές απειλές

Η κλίμακα και η ποικιλομορφία των σημερινών υβριδικών απειλών είναι πρωτοφανείς. Εκδηλώθηκαν ακόμη περισσότερο κατά την κρίση της COVID-19, καθώς πολλοί κρατικοί και μη κρατικοί παράγοντες προσπάθησαν να εκμεταλλευτούν την πανδημία, κυρίως χειραγωγώντας το περιβάλλον πληροφοριών και προκαλώντας προβλήματα σε βασικές υποδομές. Η κατάσταση αυτή ενέχει τον κίνδυνο αποδυνάμωσης της κοινωνικής συνοχής και υπονόμευσης της εμπιστοσύνης στα θεσμικά όργανα της ΕΕ και στις κυβερνήσεις των κρατών μελών.

---

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

72 Στρατηγική της ΕΕ για την αποτελεσματικότερη καταπολέμηση της σεξουαλικής κακοποίησης παιδιών, COM(2020) 607.

73 Οι τρομοκράτες χρησιμοποιούν όλο και περισσότερο το σύστημα ανταλλαγής μηνυμάτων των πλατφορμών παιχνιδιών για τις ανταλλαγές τους, ενώ οι νεαροί τρομοκράτες αναπαράγουν βίαιες επιθέσεις σε βιντεοπαιχνίδια.

Η προσέγγιση της ΕΕ για τις υβριδικές απειλές ορίζεται στο κοινό πλαίσιο του 2016[74] και στην κοινή ανακοίνωση του 2018 σχετικά με την ενίσχυση της ανθεκτικότητας για την αντιμετώπιση υβριδικών απειλών[75]. Η δράση σε επίπεδο ΕΕ υποστηρίζεται από μια σημαντική εργαλειοθήκη που καλύπτει το πλέγμα των εσωτερικών-εξωτερικών πτυχών, με βάση μια προσέγγιση για το σύνολο της κοινωνίας και τη στενή συνεργασία με στρατηγικούς εταίρους, ιδίως με το ΝΑΤΟ και την ομάδα των 7 (G7). Μαζί με την παρούσα στρατηγική δημοσιεύεται έκθεση σχετικά με την εφαρμογή της προσέγγισης της ΕΕ για τις υβριδικές απειλές[76]. Με βάση τη χαρτογράφηση[77] που παρουσιάζεται παράλληλα με την παρούσα στρατηγική, οι υπηρεσίες της Επιτροπής και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης θα δημιουργήσουν μια **διαδικτυακή πλατφόρμα περιορισμένης πρόσβασης**, την οποία θα μπορούν να συμβουλεύονται τα κράτη μέλη όσον αφορά το υλικό και τα μέτρα αντιμετώπισης των υβριδικών απειλών σε επίπεδο ΕΕ.

Μολονότι την ευθύνη για την αντιμετώπιση των υβριδικών απειλών φέρουν πρωτίστως τα κράτη μέλη —λόγω της εγγενούς σχέσης με τις εθνικές πολιτικές ασφάλειας και άμυνας— ορισμένα τρωτά σημεία είναι κοινά για όλα τα κράτη μέλη και ορισμένες απειλές είναι διασυνοριακές, όπως η στόχευση διασυνοριακών δικτύων ή υποδομών. Η Επιτροπή και ο Ύπατος Εκπρόσωπος θα καθορίσουν μια προσέγγιση της ΕΕ για τις υβριδικές απειλές που θα ενσωματώνει την εξωτερική και την εσωτερική διάσταση σε ένα πλαίσιο αδιάλειπτης ροής και θα συγκεντρώνει εθνικές και ενωσιακές εκτιμήσεις. Η προσέγγιση αυτή πρέπει να καλύπτει όλο το φάσμα της δράσης —από τον έγκαιρο εντοπισμό, την ανάλυση, την ευαισθητοποίηση, την οικοδόμηση ανθεκτικότητας και την πρόληψη έως την αντιμετώπιση κρίσεων και τη διαχείριση συνεπειών.

Πέρα από την ενίσχυση της εφαρμογής, δεδομένης της συνεχούς εξέλιξης των υβριδικών απειλών, θα δοθεί ιδιαίτερη έμφαση στην **ενσωμάτωση υβριδικών εκτιμήσεων στη χάραξη πολιτικής**, ώστε να συμβαδίζει με τις δυναμικές εξελίξεις και να διασφαλίζει ότι δεν παραβλέπεται καμία δυνητικά σημαντική πρωτοβουλία. Υπό το πρίσμα των υβριδικών απειλών θα αξιολογούνται επίσης τα αποτελέσματα των νέων πρωτοβουλιών, συμπεριλαμβανομένων των πρωτοβουλιών σε τομείς που μέχρι σήμερα δεν καλύπτονταν από το πλαίσιο αντιμετώπισης υβριδικών απειλών, όπως η εκπαίδευση, η τεχνολογία και η έρευνα. Στο πλαίσιο της προσέγγισης αυτής θα μπορούσαν να αξιοποιηθούν οι εργασίες που αφορούν τον εννοιολογικό ορισμό των υβριδικών απειλών, οι οποίες παρέχουν πλήρη εικόνα των διαφόρων εργαλείων που χρησιμοποιούνται, ενδεχομένως, από τους αντιπάλους[78]. Ο στόχος θα πρέπει να είναι να διασφαλιστεί ότι η διαδικασία λήψης αποφάσεων στηρίζεται σε τακτική, ολοκληρωμένη και βάσει πληροφοριών υποβολή εκθέσεων σχετικά με την εξέλιξη των υβριδικών απειλών. Οι εκθέσεις αυτές θα βασίζονται

[74] Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών – Απόκριση της Ευρωπαϊκής Ένωσης, JOIN (2016) 18.

[75] Αύξηση της ανθεκτικότητας και ενίσχυση των ικανοτήτων για την αντιμετώπιση υβριδικών απειλών, JOIN (2018) 16.

[76] SWD(2020) 153 Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats («Εκθεση σχετικά με την εφαρμογή του κοινού πλαισίου του 2016 για την αντιμετώπιση υβριδικών απειλών και της κοινής ανακοίνωσης του 2018 σχετικά με την αύξηση της ανθεκτικότητας και την ενίσχυση των ικανοτήτων για την αντιμετώπιση υβριδικών απειλών»)

[77] SWD (2020) 152 Mapping of the measures related to enhancing resilience and countering hybrid threats («Χαρτογράφηση των μέτρων που σχετίζονται με τη βελτίωση της ανθεκτικότητας και την αντιμετώπιση των υβριδικών απειλών»).

[78] The Landscape of Hybrid Threats: A conceptual Model, JRC117280 («Το τοπίο των υβριδικών απειλών: εννοιολογικό μοντέλο»), μοντέλο το οποίο εκπονήθηκε από κοινού από το Κοινό Κέντρο Ερευνών και από το κέντρο αριστείας για την καταπολέμηση των υβριδικών απειλών.

σε μεγάλο βαθμό στις πληροφορίες των κρατών μελών και στην περαιτέρω ενίσχυση της συνεργασίας με τις αρμόδιες υπηρεσίες των κρατών μελών στον τομέα των πληροφοριών, μέσω του κέντρου ανάλυσης πληροφοριών της ΕΕ (EU INTCEN).

Για την ανάπτυξη της **επίγνωσης των καταστάσεων**, οι υπηρεσίες της Επιτροπής και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης θα διερευνήσουν επιλογές για τον εξορθολογισμό των ροών πληροφοριών από διάφορες πηγές, συμπεριλαμβανομένων των κρατών μελών, καθώς και από οργανισμούς της ΕΕ, όπως ο ENISA, ο Ευρωπόλ και ο Frontex. Η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ θα παραμείνει το σημείο εστίασης της ΕΕ για τις αξιολογήσεις υβριδικών απειλών. Η **οικοδόμηση της ανθεκτικότητας** είναι καίριας σημασίας για την πρόληψη των υβριδικών απειλών και την προστασία από αυτές. Επομένως, η συστηματική παρακολούθηση και η αντικειμενική μέτρηση της προόδου στον εν λόγω τομέα είναι ζωτικής σημασίας. Το πρώτο βήμα θα είναι ο προσδιορισμός των τομεακών βασικών παραμέτρων ανθεκτικότητας στις υβριδικές απειλές, τόσο για τα κράτη μέλη όσο και για τα θεσμικά όργανα και οργανισμούς της ΕΕ. Τέλος, για να επιταχυνθεί η **ετοιμότητα για την αντιμετώπιση των υβριδικών κρίσεων**, θα πρέπει να επανεξεταστεί το ισχύον πρωτόκολλο, όπως ορίζεται στο εγχειρίδιο στρατηγικής της ΕΕ του 2016 (EU Playbook)[79], ώστε να ληφθεί υπόψη η ευρύτερη επανεξέταση και ενίσχυση του υπό εξέταση συστήματος αντιμετώπισης κρίσεων της ΕΕ[80]. Στόχος είναι να μεγιστοποιηθεί το αποτέλεσμα της δράσης της ΕΕ με την άμεση συγκέντρωση τομεακών απαντήσεων και τη διασφάλιση της συνεχούς συνεργασίας με τους εταίρους μας, και κυρίως με το ΝΑΤΟ.

Βασικές δράσεις
• Διασφάλιση της εφαρμογής και της καταλληλότητας της νομοθεσίας για το έγκλημα στον κυβερνοχώρο • Στρατηγική για την αποτελεσματικότερη καταπολέμηση της σεξουαλικής κακοποίησης παιδιών • Προτάσεις για τον εντοπισμό και την αφαίρεση υλικού σεξουαλικής κακοποίησης παιδιών • Προσέγγιση της ΕΕ για την αντιμετώπιση υβριδικών απειλών • Επανεξέταση του επιχειρησιακού πρωτοκόλλου της ΕΕ για την αντιμετώπιση υβριδικών απειλών (EU Playbook – Εγχειρίδιο στρατηγικής της ΕΕ) • Αξιολόγηση του τρόπου ενίσχυσης της ικανότητας επιβολής του νόμου στις ψηφιακές έρευνες

3. Προστασία των Ευρωπαίων από την τρομοκρατία και το οργανωμένο έγκλημα

Τρομοκρατία και ριζοσπαστικοποίηση

Το επίπεδο τρομοκρατικής απειλής στην ΕΕ παραμένει υψηλό. Παρά τη συνολική μείωση του αριθμού των επιθέσεων, οι συνέπειες που μπορεί να έχουν οι επιθέσεις αυτές παραμένουν καταστροφικές. Η ριζοσπαστικοποίηση μπορεί επίσης να προκαλέσει ευρύτερη

[79] Επιχειρησιακό πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών (EU Playbook – Εγχειρίδιο στρατηγικής της ΕΕ), SWD(2016) 227.

[80] Σε συνέχεια της τηλεδιάσκεψης της 26ης Μαρτίου 2020, τα μέλη του Ευρωπαϊκού Συμβουλίου εξέδωσαν δήλωση σχετικά με τις δράσεις της ΕΕ για την αντιμετώπιση της έξαρσης της νόσου COVID-19, με την οποία καλούσαν την Επιτροπή να υποβάλει προτάσεις για ένα πιο φιλόδοξο και ευρύτερο σύστημα διαχείρισης κρίσεων εντός της ΕΕ.

πόλωση και να αποσταθεροποιήσει την κοινωνική συνοχή. Τα κράτη μέλη εξακολουθούν να φέρουν την κύρια ευθύνη για την καταπολέμηση της τρομοκρατίας και της ριζοσπαστικοποίησης. Ωστόσο, η ολοένα και μεγαλύτερη διασυνοριακή/διατομεακή διάσταση της απειλής απαιτεί τη λήψη περαιτέρω μέτρων για τη συνεργασία και τον συντονισμό σε επίπεδο ΕΕ. Η αποτελεσματική εφαρμογή της νομοθεσίας της ΕΕ για την καταπολέμηση της τρομοκρατίας, συμπεριλαμβανομένων των περιοριστικών μέτρων[81], αποτελεί προτεραιότητα. Η επέκταση της εντολής της Ευρωπαϊκής Εισαγγελίας στα διασυνοριακά τρομοκρατικά εγκλήματα παραμένει στόχος προς επίτευξη.

Η καταπολέμηση της τρομοκρατίας ξεκινά με την αντιμετώπιση των βαθύτερων αιτίων της. Η πόλωση της κοινωνίας, οι πραγματικές ή εικαζόμενες διακρίσεις και άλλοι ψυχολογικοί και κοινωνιολογικοί παράγοντες μπορούν να καταστήσουν τους ανθρώπους πιο ευάλωτους στη ριζοσπαστική ρητορική. Στο πλαίσιο αυτό, η αντιμετώπιση της **ριζοσπαστικοποίησης** συμβαδίζει με την προώθηση της κοινωνικής συνοχής σε τοπικό, εθνικό και ευρωπαϊκό επίπεδο. Την τελευταία δεκαετία αναπτύχθηκαν διάφορες αποτελεσματικές πρωτοβουλίες και πολιτικές, ιδίως μέσω του δικτύου για την ευαισθητοποίηση σχετικά με τη ριζοσπαστικοποίηση και της πρωτοβουλίας «Οι πόλεις της ΕΕ κατά της ριζοσπαστικοποίησης».[82] Είναι πλέον καιρός να εξεταστούν δράσεις για τον εξορθολογισμό των πολιτικών, των πρωτοβουλιών και των κονδυλίων της ΕΕ με σκοπό την αντιμετώπιση της ριζοσπαστικοποίησης. Οι εν λόγω δράσεις μπορούν να στηρίξουν την ανάπτυξη ικανοτήτων και δεξιοτήτων, να βελτιώσουν τη συνεργασία, να ενισχύσουν τη βάση τεκμηρίωσης και να συμβάλουν στην αξιολόγηση της προόδου, με τη συμμετοχή όλων των σχετικών ενδιαφερόμενων φορέων, συμπεριλαμβανομένων των επαγγελματιών της πρώτης γραμμής, των υπεύθυνων χάραξης πολιτικής και των πανεπιστημίων[83]. Οι ήπιες πολιτικές, όπως η εκπαίδευση, ο πολιτισμός, η νεολαία και ο αθλητισμός, θα μπορούσαν να συμβάλουν στην πρόληψη της ριζοσπαστικοποίησης, παρέχοντας ευκαιρίες για τους νέους που διατρέχουν κίνδυνο, καθώς και συνοχή εντός της ΕΕ[84]. Μεταξύ των τομέων προτεραιότητας περιλαμβάνονται οι εργασίες για τον έγκαιρο εντοπισμό και τη διαχείριση κινδύνων, την οικοδόμηση ανθεκτικότητας και την απεμπλοκή, καθώς και για την αποκατάσταση και την επανένταξη στην κοινωνία.

Οι τρομοκράτες επιδιώκουν να αποκτούν και να χρησιμοποιούν ως όπλα **χημικά, βιολογικά, ραδιολογικά και πυρηνικά (ΧΒΡΠ) υλικά**[85], καθώς και να αναπτύσσουν τις γνώσεις και τις ικανότητες που απαιτούνται για τη χρήσης τους[86]. Το ενδεχόμενο ΧΒΡΠ επιθέσεων διαδραματίζει κυρίαρχο ρόλο στην τρομοκρατική προπαγάνδα. Δεδομένου ότι η ζημία που μπορεί να προκαλέσουν είναι τεράστια, χρήζουν ιδιαίτερης προσοχής. Με βάση την προσέγγιση που χρησιμοποιείται για τη ρύθμιση της πρόσβασης σε πρόδρομες ουσίες

---

81 Το Συμβούλιο ενέκρινε περιοριστικά μέτρα για το ISIL (Da'esh) και την Αλ Κάιντα, καθώς και ειδικά περιοριστικά μέτρα κατά ορισμένων προσώπων και οντοτήτων, με σκοπό την καταπολέμηση της τρομοκρατίας. Για την επισκόπηση όλων των περιοριστικών μέτρων, βλέπε τον χάρτη κυρώσεων της ΕΕ (https://www.sanctionsmap.eu/#/main).

82 Η πιλοτική πρωτοβουλία «Οι πόλεις της ΕΕ κατά της ριζοσπαστικοποίησης» έχει τον διττό στόχο να προωθήσει την ανταλλαγή εμπειρογνωσίας μεταξύ των πόλεων της ΕΕ και να συγκεντρώσει παρατηρήσεις σχετικά με τον καλύτερο τρόπο στήριξης των τοπικών κοινοτήτων σε επίπεδο ΕΕ.

83 Για παράδειγμα, χρηματοδότηση στο πλαίσιο του Ευρωπαϊκού Ταμείου Ασφάλειας και του προγράμματος «Δικαιώματα, Ισότητα και Ιθαγένεια».

84 Δράσεις της ΕΕ όπως οι εικονικές ανταλλαγές στο πλαίσιο του Erasmus+ και η ηλεκτρονική αδελφοποίηση (e-twinning).

85 Για παράδειγμα, τα τελευταία δύο χρόνια υπήρξαν αρκετές περιπτώσεις χρήσης βιολογικών παραγόντων (συνήθως φυτικών τοξινών), τόσο στην Ευρώπη (Γαλλία, Γερμανία, Ιταλία) όσο και αλλού (Τυνησία, Ινδονησία).

86 Το Συμβούλιο έλαβε περιοριστικά μέτρα κατά της διάδοσης και της χρήσης χημικών όπλων.

εκρηκτικών υλών, η Επιτροπή θα εξετάσει το ενδεχόμενο περιορισμού της πρόσβασης σε ορισμένα επικίνδυνα χημικά προϊόντα που θα μπορούσαν να χρησιμοποιηθούν για την πραγματοποίηση επιθέσεων. Η ανάπτυξη των ικανοτήτων αντίδρασης σε επίπεδο πολιτικής προστασίας της ΕΕ (rescEU) στον τομέα των ΧΒΡΠ θα είναι επίσης καίριας σημασίας. Η συνεργασία με τρίτες χώρες είναι επίσης σημαντική για την ενίσχυση μιας κοινής νοοτροπίας όσον αφορά την ασφάλεια και προστασία στον τομέα των ΧΒΡΠ, με πλήρη αξιοποίηση των κέντρων αριστείας ΧΒΡΠ της ΕΕ σε όλο τον κόσμο. Η συνεργασία αυτή θα περιλαμβάνει εθνικές αξιολογήσεις όσον αφορά τις ελλείψεις και τους κινδύνους, την υποστήριξη των εθνικών και περιφερειακών σχεδίων δράσης στον τομέα των ΧΒΡΠ, την ανταλλαγή ορθών πρακτικών και τις δραστηριότητες ανάπτυξης ικανοτήτων στον τομέα των ΧΒΡΠ.

Η ΕΕ έχει θεσπίσει την πιο προηγμένη νομοθεσία παγκοσμίως όσον αφορά τον περιορισμό της πρόσβασης σε **πρόδρομες ουσίες εκρηκτικών υλών**[87] και τον εντοπισμό ύποπτων συναλλαγών που αποσκοπούν στην κατασκευή αυτοσχέδιων εκρηκτικών μηχανισμών. Ωστόσο, η απειλή από την κατασκευή αυτοσχέδιων εκρηκτικών παραμένει σε υψηλό επίπεδο, καθώς τα εκρηκτικά αυτά χρησιμοποιήθηκαν σε πολλαπλές επιθέσεις σε ολόκληρη την ΕΕ[88]. Ως πρώτο βήμα, πρέπει να εφαρμόζονται οι κανόνες, καθώς και να διασφαλίζεται ότι το διαδικτυακό περιβάλλον δεν επιτρέπει την παράκαμψη των ελέγχων.

Η αποτελεσματική δίωξη όσων έχουν διαπράξει τρομοκρατικά εγκλήματα, συμπεριλαμβανομένων των **αλλοδαπών τρομοκρατών μαχητών** που βρίσκονται επί του παρόντος στη Συρία και στο Ιράκ, αποτελεί επίσης σημαντικό στοιχείο της πολιτικής για την καταπολέμηση της τρομοκρατίας. Μολονότι τα ζητήματα αυτά αντιμετωπίζονται πρωτίστως σε επίπεδο κρατών μελών, ο συντονισμός και η στήριξη της ΕΕ μπορούν να βοηθήσουν τα κράτη μέλη στην αντιμετώπιση των κοινών προκλήσεων. Σημαντικό βήμα συνιστούν τα υπό εξέλιξη μέτρα σχετικά με την πλήρη εφαρμογή της νομοθεσίας για την ασφάλεια των συνόρων[89] και την πλήρη αξιοποίηση όλων των σχετικών βάσεων δεδομένων της ΕΕ για την ανταλλαγή πληροφοριών σχετικά με γνωστούς υπόπτους. Πέρα από την ταυτοποίηση ατόμων υψηλού κινδύνου, απαιτείται πολιτική επανένταξης και αποκατάστασης. Η διεπαγγελματική συνεργασία, μεταξύ άλλων και με το σωφρονιστικό προσωπικό και το προσωπικό της δικαστικής επιτήρησης, θα ενισχύσει τη δικαστική αντίληψη των διαδικασιών ριζοσπαστικοποίησης που οδηγούν στον βίαιο εξτρεμισμό, καθώς και την προσέγγιση του δικαστικού τομέα ως προς την επιβολή ποινών και τις εναλλακτικές λύσεις αντί της κράτησης.

Η πρόκληση που συνιστούν οι αλλοδαποί τρομοκράτες μαχητές είναι χαρακτηριστική της σχέσης μεταξύ της εσωτερικής και της **εξωτερικής ασφάλειας.** Η συνεργασία για την καταπολέμηση της τρομοκρατίας και για την πρόληψη και την αντιμετώπιση της ριζοσπαστικοποίησης και του βίαιου εξτρεμισμού είναι καίριας σημασίας για την ασφάλεια εντός της ΕΕ[90]. Απαιτούνται περαιτέρω ενέργειες προκειμένου να αναπτυχθούν εταιρικές

---

[87] Χημικά προϊόντα που θα μπορούσαν να χρησιμοποιηθούν για την κατασκευή αυτοσχέδιων εκρηκτικών. Διέπονται από τον κανονισμό (ΕΕ) 2019/1148 σχετικά με την κυκλοφορία στην αγορά και τη χρήση πρόδρομων ουσιών εκρηκτικών υλών.

[88] Οι επιθέσεις στο Όσλο (2011), στο Παρίσι (2015), στις Βρυξέλλες (2016) και στο Μάντσεστερ (2017) αποτελούν παραδείγματα τέτοιων καταστροφικών επιθέσεων. Επίθεση με αυτοσχέδιο εκρηκτικό στη Λυών (2019) είχε ως αποτέλεσμα να τραυματιστούν 13 άτομα.

[89] Συμπεριλαμβανομένης της νέας εντολής του Ευρωπαϊκού Οργανισμού Συνοριοφυλακής και Ακτοφυλακής (Frontex).

[90] Στα συμπεράσματα του Συμβουλίου της 16ης Ιουνίου 2020 τονίστηκε η ανάγκη να προστατευθούν οι πολίτες της ΕΕ από την τρομοκρατία και τον βίαιο εξτρεμισμό, σε όλες τις μορφές τους και ανεξάρτητα από την προέλευσή τους, και να ενισχυθεί περαιτέρω η εξωτερική συμμετοχή και δράση της ΕΕ για την

σχέσεις για την καταπολέμηση της τρομοκρατίας και της συνεργασίας με χώρες που βρίσκονται στις γειτονικές περιοχές και πέραν αυτών, με βάση την εμπειρογνωσία του δικτύου εμπειρογνωμόνων της ΕΕ για θέματα αντιτρομοκρατίας/ασφαλείας. Το κοινό σχέδιο δράσης για την καταπολέμηση της τρομοκρατίας στα Δυτικά Βαλκάνια αποτελεί καλό πλαίσιο αναφοράς για την εν λόγω στοχευμένη συνεργασία. Ειδικότερα, θα πρέπει να καταβληθούν προσπάθειες για τη στήριξη της ικανότητας των χωρών εταίρων να ταυτοποιούν και να εντοπίζουν αλλοδαπούς τρομοκράτες μαχητές. Η ΕΕ θα συνεχίσει επίσης να προωθεί την πολυμερή συνεργασία με τους κυριότερους παγκόσμιους παράγοντες σε αυτόν τον τομέα, όπως τα Ηνωμένα Έθνη, το ΝΑΤΟ, το Συμβούλιο της Ευρώπης, ο Ιντερπόλ και ο ΟΑΣΕ. Θα συνεργαστεί επίσης με το Παγκόσμιο Φόρουμ κατά της Τρομοκρατίας και με τον Παγκόσμιο Συνασπισμό για την καταπολέμηση του Da'esh, καθώς και με συναφείς φορείς της κοινωνίας των πολιτών. Τα μέσα εξωτερικής πολιτικής της Ένωσης, συμπεριλαμβανομένης της ανάπτυξης και της συνεργασίας, διαδραματίζουν επίσης σημαντικό ρόλο στη συνεργασία με τρίτες χώρες όσον αφορά την πρόληψη της τρομοκρατίας και της πειρατείας. Η διεθνής συνεργασία είναι επίσης απαραίτητη για την εξάλειψη όλων των πηγών **χρηματοδότησης της τρομοκρατίας**, για παράδειγμα μέσω της ομάδας χρηματοοικονομικής δράσης.

Οργανωμένο έγκλημα

Το οργανωμένο έγκλημα έχει τεράστιο οικονομικό και προσωπικό κόστος. Η οικονομική ζημία που οφείλεται στο οργανωμένο έγκλημα και τη διαφθορά εκτιμάται ότι ανέρχεται σε 218 έως 282 δισ. EUR ετησίως.[91] Το 2017, πάνω από 5 000 ομάδες οργανωμένου εγκλήματος αποτελούσαν αντικείμενο ερευνών στην Ευρώπη —δηλ. αύξηση κατά 50 % σε σύγκριση με το 2013.[92] Το οργανωμένο έγκλημα δραστηριοποιείται όλο και περισσότερο σε διασυνοριακό επίπεδο, μεταξύ άλλων και στην άμεση γειτονία της ΕΕ, γεγονός που απαιτεί την εντατικοποίηση της επιχειρησιακής συνεργασίας και την ανταλλαγή πληροφοριών με εταίρους στις γειτονικές χώρες.

Νέες προκλήσεις αναδύονται και μεταφέρουν το έγκλημα στο διαδίκτυο: κατά την πανδημία COVID-19 αυξήθηκαν σημαντικά οι διαδικτυακές απάτες που στόχευαν ευάλωτες ομάδες αλλά και την υγεία και τα υγειονομικά προϊόντα που αποτέλεσαν αντικείμενο κλοπών και διαρρήξεων.[93] Η ΕΕ πρέπει να εντείνει τις εργασίες της για την καταπολέμηση του οργανωμένου εγκλήματος, μεταξύ άλλων και σε διεθνές επίπεδο, με περισσότερα εργαλεία για την εξάρθρωση του επιχειρηματικού μοντέλου του οργανωμένου εγκλήματος. Η καταπολέμηση του οργανωμένου εγκλήματος απαιτεί επίσης στενή συνεργασία με τις τοπικές και περιφερειακές διοικήσεις, καθώς και με την κοινωνία των πολιτών, που είναι βασικοί εταίροι στην πρόληψη του εγκλήματος και στην παροχή βοήθειας και στήριξης στα θύματα, ενώ είναι ιδιαίτερα αναγκαία η συνεργασία μεταξύ διοικήσεων σε παραμεθόριες περιοχές. Οι εργασίες αυτές θα συγκεντρωθούν σε μια **ατζέντα για την αντιμετώπιση του οργανωμένου εγκλήματος**.

Πάνω από το ένα τρίτο των ομάδων οργανωμένου εγκλήματος που δραστηριοποιούνται στην ΕΕ εμπλέκονται στην παραγωγή, διακίνηση ή διανομή ναρκωτικών. Η τοξικομανία είχε ως αποτέλεσμα τον θάνατο οκτώ χιλιάδων ανθρώπων από υπερβολική δόση στην ΕΕ το

καταπολέμηση της τρομοκρατίας στο πλαίσιο ορισμένων γεωγραφικών και θεματικών τομέων προτεραιότητας.

[91] Ως ποσοστό του ακαθάριστου εγχώριου προϊόντος (ΑΕΠ), Έκθεση του Ευρωπόλ με τίτλο: «Does crime still pay?» – Criminal asset recovery in the EU, 2016.

[92] Ευρωπόλ, Αξιολόγηση απειλής όσον αφορά το σοβαρό και οργανωμένο έγκλημα (SOCTA), 2013 και 2017.

[93] Ευρωπόλ, 2020.

2019. Το μεγαλύτερο μέρος της **διακίνησης ναρκωτικών** γίνεται στα σύνορα και πολλά από τα κέρδη παρεισφρέουν στη νόμιμη οικονομία.[94] Ένα νέο θεματολόγιο της ΕΕ για τα ναρκωτικά[95] θα ενισχύσει τις προσπάθειες της ΕΕ και των κρατών μελών όσον αφορά τη μείωση της ζήτησης και της προσφοράς ναρκωτικών, καθορίζοντας κοινές δράσεις για την αντιμετώπιση ενός κοινού προβλήματος και ενισχύοντας τον διάλογο και τη συνεργασία μεταξύ της ΕΕ και των εξωτερικών εταίρων σε ζητήματα ναρκωτικών. Έπειτα από αξιολόγηση του Ευρωπαϊκού Κέντρου Παρακολούθησης Ναρκωτικών και Τοξικομανίας, η Επιτροπή θα αξιολογήσει κατά πόσον η εντολή της πρέπει να αναπροσαρμοστεί ώστε να ανταποκριθεί στις νέες προκλήσεις.

Οι ομάδες οργανωμένου εγκλήματος και οι τρομοκράτες αποτελούν επίσης βασικούς παράγοντες του εμπορίου **παράνομων πυροβόλων όπλων**. Μεταξύ 2009 και 2018, σημειώθηκαν 23 περιστατικά μαζικών πυροβολισμών στην Ευρώπη, στα οποία έχασαν τη ζωή τους πάνω από 340 άτομα.[96] Η διακίνηση πυροβόλων όπλων στην ΕΕ γίνεται συχνά μέσω της άμεσης γειτονίας της.[97] Αυτό καταδεικνύει την ανάγκη ενίσχυσης του συντονισμού και της συνεργασίας τόσο εντός της ΕΕ όσο και με τους διεθνείς εταίρους, ιδίως τον Ιντερπόλ, ώστε να εναρμονιστούν η συλλογή πληροφοριών και η υποβολή εκθέσεων σχετικά με τις κατασχέσεις όπλων. Είναι επίσης σημαντικό να βελτιωθεί η ιχνηλασιμότητα των όπλων, μεταξύ άλλων και στο διαδίκτυο, και να διασφαλιστεί η ανταλλαγή πληροφοριών μεταξύ των αρχών αδειοδότησης και των αρχών επιβολής του νόμου. Η Επιτροπή παρουσιάζει ένα νέο **σχέδιο δράσης της ΕΕ για την καταπολέμηση της παράνομης διακίνησης πυροβόλων όπλων**[98] και θα αξιολογήσει επίσης κατά πόσον οι κανόνες για την άδεια εξαγωγής και τα μέτρα εισαγωγής και διαμετακόμισης για τα πυροβόλα όπλα εξακολουθούν να ενδείκνυνται για τον επιδιωκόμενο σκοπό[99].

Οι εγκληματικές οργανώσεις αντιμετωπίζουν τους μετανάστες και τα άτομα που χρήζουν διεθνούς προστασίας ως εμπορεύματα. Το 90 % των παράτυπων μεταναστών που φτάνουν στην ΕΕ έχουν διακινηθεί από κάποιο εγκληματικό δίκτυο.[100] Η παράνομη διακίνηση μεταναστών συνδέεται επίσης συχνά με άλλες μορφές οργανωμένου εγκλήματος, ιδίως με την εμπορία ανθρώπων.[101]. Πέρα από το τεράστιο ανθρώπινο κόστος της εμπορίας ανθρώπων, ο Ευρωπόλ εκτιμά ότι, σε παγκόσμιο επίπεδο, τα προκύπτοντα ετήσια κέρδη για όλες τις μορφές εκμετάλλευσης από την εμπορία ανθρώπων ανέρχονται σε 29,4 δισ. EUR. Πρόκειται για διεθνικό έγκλημα που τροφοδοτεί την παράνομη ζήτηση εντός και εκτός της ΕΕ και επηρεάζει όλα τα κράτη μέλη της ΕΕ. Η ανεπαρκής καταγραφή όσον αφορά την ταυτοποίηση, τη δίωξη και την καταδίκη αυτών των εγκλημάτων απαιτεί μια νέα προσέγγιση για την ενίσχυση της δράσης. Μια νέα **ολοκληρωμένη προσέγγιση για την εμπορία ανθρώπων** θα συγκεντρώσει όλες τις πτυχές δράσης. Επιπλέον, η Επιτροπή θα παρουσιάσει ένα **νέο σχέδιο δράσης της ΕΕ κατά της λαθραίας διακίνησης μεταναστών**

---

[94] Έκθεση του Ευρωπαϊκού Κέντρου Παρακολούθησης Ναρκωτικών και Τοξικομανίας (ΕΚΠΝΤ) και του Ευρωπόλ για την αγορά ναρκωτικών της ΕΕ 2019. (Νοέμβριος 2019).

[95] Θεματολόγιο και σχέδιο δράσης της ΕΕ για τα ναρκωτικά 2021-2025, COM(2020) 606.

[96] Flemish Peace Institute, Armed to kill. (Οκτώβριος 2019).

[97] Η ΕΕ έχει χρηματοδοτήσει τους φορείς καταπολέμησης της διάδοσης και της διακίνησης φορητών όπλων και ελαφρού οπλισμού στην περιοχή από το 2002. Έχει χρηματοδοτήσει κυρίως το δίκτυο εμπειρογνωμόνων για τα πυροβόλα όπλα της ΝΑ Ευρώπης (SEEFEN). Από το 2019, οι εταίροι των Δυτικών Βαλκανίων συμμετέχουν πλήρως στην προτεραιότητα της Ευρωπαϊκής Πολυκλαδικής Πλατφόρμας κατά των Εγκληματικών Απειλών (EMPACT) όσον αφορά τα πυροβόλα όπλα.

[98] COM(2020) 608.

[99] Κανονισμός (ΕΕ) αριθ. 258/2012 για την εφαρμογή του άρθρου 10 του πρωτοκόλλου των Ηνωμένων Εθνών σχετικά με την καταπολέμηση της παράνομης κατασκευής και διακίνησης πυροβόλων όπλων.

[100] Πηγή: Ευρωπόλ.

[101] Ευρωπόλ, EMSC, 4η Ετήσια Έκθεση.

για την περίοδο 2021-2025. Και τα δύο σκέλη θα επικεντρωθούν στην καταπολέμηση των εγκληματικών δικτύων, την ενίσχυση της συνεργασίας και την υποστήριξη του έργου των φορέων επιβολής του νόμου.

Οι ομάδες οργανωμένου εγκλήματος —καθώς και οι τρομοκράτες— αναζητούν επίσης ευκαιρίες σε άλλους τομείς, ιδίως σε εκείνους που παράγουν υψηλά κέρδη με χαμηλό κίνδυνο εντοπισμού, όπως το **περιβαλλοντικό έγκλημα**. Το παράνομο κυνήγι και η εμπορία άγριων ειδών, η παράνομη εξόρυξη, η παράνομη υλοτομία και η παράνομη διάθεση και μεταφορά αποβλήτων έχουν καταστεί η τέταρτη μεγαλύτερη εγκληματική δραστηριότητα σε ολόκληρο τον κόσμο.[102]. Παρατηρήθηκε επίσης η εγκληματική εκμετάλλευση των συστημάτων εμπορίας δικαιωμάτων εκπομπών και των συστημάτων πιστοποιητικών ενέργειας, καθώς και η κατάχρηση της χρηματοδότησης που διατίθεται για την περιβαλλοντική ανθεκτικότητα και τη βιώσιμη ανάπτυξη. Πέρα από την προώθηση της δράσης της ΕΕ, των κρατών μελών και της διεθνούς κοινότητας για την ενίσχυση των προσπαθειών καταπολέμησης του περιβαλλοντικού εγκλήματος[103], η Επιτροπή αξιολογεί κατά πόσον η οδηγία για το περιβαλλοντικό έγκλημα[104] εξακολουθεί να είναι κατάλληλη για τον επιδιωκόμενο σκοπό. Η αυξανόμενη **εμπορία πολιτιστικών αγαθών** έχει επίσης καταστεί μία από τις επικερδέστερες εγκληματικές δραστηριότητες και αποτελεί πηγή χρηματοδότησης τόσο για τους τρομοκράτες όσο και για το οργανωμένο έγκλημα. Θα πρέπει να διερευνηθούν μέτρα για τη βελτίωση της εντός και εκτός διαδικτύου ιχνηλασιμότητας των πολιτιστικών αγαθών στην εσωτερική αγορά και της συνεργασίας με τρίτες χώρες στις οποίες λεηλατούνται τα πολιτιστικά αγαθά, καθώς και για την παροχή ενεργού στήριξης στις αρχές επιβολής του νόμου και τις ακαδημαϊκές κοινότητες.

Τα **οικονομικά και χρηματοπιστωτικά εγκλήματα** είναι εξαιρετικά πολύπλοκα, αλλά επηρεάζουν εκατομμύρια πολίτες και χιλιάδες εταιρείες στην ΕΕ κάθε χρόνο. Η καταπολέμηση της απάτης είναι ζωτικής σημασίας και απαιτεί την ανάληψη δράσης σε επίπεδο ΕΕ. Ο Ευρωπόλ, μαζί με τον Eurojust, την Ευρωπαϊκή Εισαγγελία και την Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Απάτης, στηρίζουν τα κράτη μέλη και την ΕΕ για την προστασία των οικονομικών και χρηματοπιστωτικών αγορών και για τη διασφάλιση των χρημάτων των φορολογουμένων της ΕΕ. Η Ευρωπαϊκή Εισαγγελία θα καταστεί πλήρως λειτουργική στο τέλος του 2020 και θα διερευνά, θα ασκεί διώξεις και θα προσάγει ενώπιον της δικαιοσύνης τα εγκλήματα που διαπράττονται εις βάρος του προϋπολογισμού της ΕΕ, όπως η απάτη, η διαφθορά και η νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Επίσης, θα αντιμετωπίσει τις διασυνοριακές φορολογικές απάτες στον τομέα του ΦΠΑ, οι οποίες κοστίζουν στους φορολογούμενους τουλάχιστον 50 δισ. EUR ετησίως.

Η Επιτροπή θα στηρίξει επίσης την ανάπτυξη εμπειρογνωσίας και ενός νομοθετικού πλαισίου για τους αναδυόμενους κινδύνους, όπως τα κρυπτονομίσματα και τα νέα συστήματα πληρωμών. Ειδικότερα, η Επιτροπή θα προσπαθήσει να αντιμετωπίσει την εμφάνιση κρυπτογραφικών στοιχείων ενεργητικού, όπως το bitcoin, και τις επιπτώσεις που θα έχουν οι εν λόγω νέες τεχνολογίες στον τρόπο έκδοσης, ανταλλαγής και από κοινού χρήσης των χρηματοοικονομικών περιουσιακών στοιχείων, καθώς και στην πρόσβαση σε αυτά.

Η ανοχή για το παράνομο χρήμα στην Ευρωπαϊκή Ένωση θα πρέπει να είναι μηδενική. Από τριακονταετίας και πλέον, η ΕΕ έχει αναπτύξει ένα σταθερό κανονιστικό πλαίσιο για την

[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, Ιούνιος 2016.
[103] Βλ.: Η Ευρωπαϊκή Πράσινη Συμφωνία COM(2019) 640 final.
[104] Οδηγία 2008/99/ΕΚ σχετικά με την προστασία του περιβάλλοντος μέσω του ποινικού δικαίου.

πρόληψη και την καταπολέμηση της **νομιμοποίησης εσόδων από παράνομες δραστηριότητες** και της χρηματοδότησης της τρομοκρατίας, με πλήρη σεβασμό της ανάγκης προστασίας των δεδομένων προσωπικού χαρακτήρα. Ωστόσο, υπάρχει αυξανόμενη συναίνεση ως προς την ανάγκη σημαντικής βελτίωσης του ισχύοντος πλαισίου. Είναι αναγκαίο να αντιμετωπιστούν οι σημαντικές αποκλίσεις στον τρόπο με τον οποίο εφαρμόζεται, καθώς και οι σοβαρές αδυναμίες στην επιβολή των κανόνων. Όπως αναφέρεται λεπτομερώς στο σχέδιο δράσης του Μαΐου 2020[105], εργασίες βρίσκονται σε εξέλιξη για την αξιολόγηση των δυνατοτήτων ενίσχυσης του πλαισίου της ΕΕ για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας. Στους τομείς που πρέπει να διερευνηθούν περιλαμβάνονται η διασύνδεση των εθνικών κεντρικών μητρώων τραπεζικών λογαριασμών, που θα μπορούσε να επιταχύνει σημαντικά την πρόσβαση στις χρηματοοικονομικές πληροφορίες για τις μονάδες χρηματοοικονομικών πληροφοριών και τις αρμόδιες αρχές.

Τα **κέρδη των ομάδων του οργανωμένου εγκλήματος** εκτιμώνται σε 110 δισ. EUR ετησίως στην ΕΕ. Η τρέχουσα αντίδραση περιλαμβάνει την εναρμόνιση της νομοθεσίας για τη δήμευση και την ανάκτηση περιουσιακών στοιχείων,[106] τη βελτίωση της δέσμευσης και της δήμευσης των περιουσιακών στοιχείων που προέρχονται από εγκληματικές δραστηριότητες στην ΕΕ και τη διευκόλυνση της αμοιβαίας εμπιστοσύνης και της αποτελεσματικής διασυνοριακής συνεργασίας μεταξύ των κρατών μελών. Ωστόσο, μόνο το 1 % περίπου των κερδών αυτών δημεύονται[107], γεγονός που επιτρέπει στις ομάδες οργανωμένου εγκλήματος να επενδύουν στην επέκταση των εγκληματικών τους δραστηριοτήτων και στη διείσδυση στη νόμιμη οικονομία, ενώ ιδίως οι μικρές και μεσαίες επιχειρήσεις, οι οποίες αντιμετωπίζουν δυσκολίες όσον αφορά την πρόσβαση σε πιστώσεις, αποτελούν βασικό στόχο για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες. Η Επιτροπή θα αναλύσει την εφαρμογή της νομοθεσίας[108] και την ενδεχόμενη ανάγκη για περαιτέρω κοινούς κανόνες, συμπεριλαμβανομένης της μη βασιζόμενης σε καταδίκη δήμευσης. Οι υπηρεσίες ανάκτησης περιουσιακών στοιχείων[109], που είναι βασικοί παράγοντες στη διαδικασία ανάκτησης περιουσιακών στοιχείων, θα μπορούσαν επίσης να εξοπλιστούν με καλύτερα εργαλεία για τον έγκαιρο εντοπισμό και την ανίχνευση περιουσιακών στοιχείων σε ολόκληρη την ΕΕ, προκειμένου να ενισχυθούν τα ποσοστά δήμευσης.

Υπάρχει στενή σχέση μεταξύ του οργανωμένου εγκλήματος και της **διαφθοράς**. Σύμφωνα με εκτιμήσεις, μόνο η διαφθορά κοστίζει στην οικονομία της ΕΕ 120 δισ. EUR ετησίως.[110] Η πρόληψη και η καταπολέμηση της διαφθοράς θα εξακολουθήσουν να υπόκεινται σε τακτική παρακολούθηση στο πλαίσιο του μηχανισμού για το κράτος δικαίου, καθώς και του

[105] Σχέδιο δράσης για την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας COM(2020) 2800.

[106] Σύμφωνα με το δίκαιο της ΕΕ, υπηρεσίες ανάκτησης περιουσιακών στοιχείων πρέπει να συγκροτηθούν σε όλα τα κράτη μέλη.

[107] Έκθεση σχετικά με την ανάκτηση και δήμευση περιουσιακών στοιχείων: Μέτρα που διασφαλίζουν ότι το έγκλημα δεν είναι προσοδοφόρο, COM(2020) 217 final.

[108] Οδηγία 2014/42/ΕΕ σχετικά με τη δέσμευση και τη δήμευση οργάνων και προϊόντων εγκλήματος στην Ευρωπαϊκή Ένωση.

[109] Απόφαση 2007/845/ΔΕΥ του Συμβουλίου σχετικά με τη συνεργασία των υπηρεσιών ανάκτησης περιουσιακών στοιχείων στα κράτη μέλη προς ανίχνευση και εντοπισμό προϊόντων εγκλήματος ή άλλων συναφών περιουσιακών στοιχείων.

[110] Είναι δύσκολο να εκτιμηθεί το συνολικό οικονομικό κόστος της διαφθοράς, αν και έχουν καταβληθεί προσπάθειες από φορείς όπως το Διεθνές Εμπορικό Επιμελητήριο, η Διεθνής Διαφάνεια, το Παγκόσμιο Σύμφωνο του ΟΗΕ και το Παγκόσμιο Οικονομικό Φόρουμ, γεγονός που υποδηλώνει ότι η διαφθορά ισοδυναμεί με το 5 % του παγκόσμιου ΑΕΠ.

Ευρωπαϊκού Εξαμήνου. Το Ευρωπαϊκό Εξάμηνο έχει αξιολογήσει τις προκλήσεις όσον αφορά την καταπολέμηση της διαφθοράς, όπως οι δημόσιες συμβάσεις, η δημόσια διοίκηση, το επιχειρηματικό περιβάλλον ή η υγειονομική περίθαλψη. Η νέα ετήσια έκθεση της Επιτροπής για το κράτος δικαίου θα καλύπτει θέματα καταπολέμησης της διαφθοράς και θα επιτρέπει τη διεξαγωγή προληπτικού διαλόγου με τις εθνικές αρχές και τα ενδιαφερόμενα μέρη σε επίπεδο ΕΕ και σε εθνικό επίπεδο. Οι οργανώσεις της κοινωνίας των πολιτών μπορούν επίσης να διαδραματίσουν καίριο ρόλο στην ενίσχυση της δράσης των δημόσιων αρχών για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος και της διαφθοράς, και οι ομάδες αυτές θα μπορούσαν να συγκεντρωθούν επωφελώς σε ένα κοινό φόρουμ. Λόγω του διασυνοριακού χαρακτήρα τους, μια άλλη βασική διάσταση είναι η συνεργασία και η παροχή βοήθειας για την αντιμετώπιση του οργανωμένου εγκλήματος και της διαφθοράς με τις γειτονικές περιοχές της ΕΕ.

Βασικές δράσεις
• Πρόγραμμα για την καταπολέμηση της τρομοκρατίας της ΕΕ, συμπεριλαμβανομένων νέων δράσεων κατά της ριζοσπαστικοποίησης στην ΕΕ • Νέα συνεργασία με σημαντικές τρίτες χώρες και διεθνείς οργανισμούς για την καταπολέμηση της τρομοκρατίας • Ατζέντα για την αντιμετώπιση του οργανωμένου εγκλήματος, συμπεριλαμβανομένης της εμπορίας ανθρώπων • Θεματολόγιο και σχέδιο δράσης της ΕΕ για τα ναρκωτικά 2021-2025 • Αξιολόγηση του Ευρωπαϊκού Κέντρου Παρακολούθησης Ναρκωτικών και Τοξικομανίας • Σχέδιο δράσης της ΕΕ κατά της διακίνησης πυροβόλων όπλων για την περίοδο 2020-2025 • Επανεξέταση της νομοθεσίας σχετικά με τη δέσμευση και τη δήμευση, καθώς και με τις υπηρεσίες ανάκτησης περιουσιακών στοιχείων • Αξιολόγηση της οδηγίας για το περιβαλλοντικό έγκλημα • Σχέδιο δράσης της ΕΕ κατά της λαθραίας διακίνησης μεταναστών, 2021-2025

4. Ισχυρό ευρωπαϊκό οικοσύστημα ασφάλειας

Μια πραγματική και αποτελεσματική Ένωση Ασφάλειας πρέπει να είναι το κοινό εγχείρημα όλων των τμημάτων της κοινωνίας. Οι κυβερνήσεις, οι φορείς επιβολής του νόμου, ο ιδιωτικός τομέας, η εκπαίδευση και οι ίδιοι οι πολίτες πρέπει να δεσμευτούν, να εξοπλιστούν και να διασυνδεθούν κατάλληλα για την οικοδόμηση της ετοιμότητας και της ανθεκτικότητας για όλους, ιδίως τους πιο ευάλωτους, τα θύματα και τους μάρτυρες.

Όλες οι πολιτικές χρειάζονται μια διάσταση ασφάλειας και η ΕΕ μπορεί να συμβάλει σε όλα τα επίπεδα. Κατ' οίκον, η ενδοοικογενειακή βία αποτελεί έναν από τους σοβαρότερους κινδύνους για την ασφάλεια. Το 22 % των γυναικών στην ΕΕ έχουν υποστεί βία από τον σύντροφό τους.[111]. Η προσχώρηση της ΕΕ στη Σύμβαση της Κωνσταντινούπολης για την πρόληψη και την καταπολέμηση της βίας κατά των γυναικών και της ενδοοικογενειακής βίας παραμένει βασική προτεραιότητα. Αν οι διαπραγματεύσεις παραμείνουν σε εκκρεμότητα, η Επιτροπή θα λάβει άλλα μέτρα για την επίτευξη των ίδιων στόχων με τη Σύμβαση, μεταξύ άλλων προτείνοντας να προστεθεί η βία κατά των γυναικών στον κατάλογο των ποινικών αδικημάτων της ΕΕ που ορίζονται στη Συνθήκη.

[111] Μια Ένωση ισότητας: Στρατηγική για την ισότητα των φύλων 2020-2025, COM(2020) 152.

Συνεργασία και ανταλλαγή πληροφοριών

Μία από τις πιο καίριες συνεισφορές της ΕΕ στην προστασία των πολιτών είναι να βοηθήσει την εύρυθμη συνεργασία των αρμοδίων για την ασφάλεια. Η συνεργασία και η ανταλλαγή πληροφοριών είναι τα ισχυρότερα εργαλεία για την καταπολέμηση του εγκλήματος και της τρομοκρατίας και για την απονομή δικαιοσύνης. Για να είναι αποτελεσματικές, πρέπει να είναι στοχευμένες και έγκαιρες. Για να είναι αξιόπιστες, πρέπει να χρησιμοποιούνται με κοινές διασφαλίσεις και ελέγχους.

Έχουν δημιουργηθεί διάφορα μέσα και ειδικές τομεακές στρατηγικές της ΕΕ[112] για την περαιτέρω ανάπτυξη της **επιχειρησιακής συνεργασίας** μεταξύ των κρατών μελών **στον τομέα της επιβολής του νόμου**. Ένα από τα κύρια μέσα που διαθέτει η ΕΕ για να στηρίζει τη συνεργασία μεταξύ των κρατών μελών στον τομέα της επιβολής του νόμου είναι το σύστημα πληροφοριών Σένγκεν, το οποίο χρησιμοποιείται για την ανταλλαγή δεδομένων σχετικά με καταζητούμενα και αγνοούμενα πρόσωπα και αντικείμενα σε πραγματικό χρόνο. Τα αποτελέσματα έχουν γίνει αισθητά με τις συλλήψεις εγκληματιών, τις κατασχέσεις ναρκωτικών και τις διασώσεις πιθανών θυμάτων[113]. Ωστόσο, το επίπεδο συνεργασίας μπορεί να βελτιωθεί περαιτέρω με τον εξορθολογισμό και την αναβάθμιση των διαθέσιμων μέσων. Οι περισσότερες νομοθετικές πράξεις της ΕΕ που διέπουν την επιχειρησιακή συνεργασία στον τομέα της επιβολής του νόμου σχεδιάστηκαν πριν από 30 χρόνια. Υπάρχει κίνδυνος κατακερματισμού εξαιτίας του πολύπλοκου πλέγματος διμερών συμφωνιών μεταξύ των κρατών μελών, πολλές εκ των οποίων είναι παρωχημένες ή δεν χρησιμοποιούνται επαρκώς. Σε μικρότερες ή περίκλειστες χώρες, τα όργανα επιβολής του νόμου που εργάζονται σε διασυνοριακό επίπεδο πρέπει να εκτελούν επιχειρησιακά καθήκοντα ακολουθώντας, σε ορισμένες περιπτώσεις, έως και επτά διαφορετικά σύνολα κανόνων: ως εκ τούτου, ορισμένες επιχειρήσεις, όπως οι καταδιώξεις υπόπτων πέραν των εσωτερικών συνόρων, απλώς δεν πραγματοποιούνται. Το υφιστάμενο πλαίσιο της ΕΕ δεν καλύπτει ούτε την επιχειρησιακή συνεργασία σε νέες τεχνολογίες, όπως οι δρόνοι.

Η επιχειρησιακή αποτελεσματικότητα μπορεί να στηριχθεί με ειδική συνεργασία στον τομέα της επιβολής του νόμου, η οποία μπορεί επίσης να συμβάλει με καίριο τρόπο στην επίτευξη άλλων στόχων πολιτικής, όπως η παροχή στοιχείων που άπτονται της ασφάλειας για τη νέα αξιολόγηση των άμεσων ξένων επενδύσεων. Η Επιτροπή θα εξετάσει τον τρόπο με τον οποίο θα μπορούσε να στηρίξει τον ως άνω στόχο ένας Κώδικας Αστυνομικής Συνεργασίας. Οι αρχές επιβολής του νόμου των κρατών μελών χρησιμοποιούν όλο και περισσότερο τη στήριξη και την εμπειρογνωσία σε επίπεδο ΕΕ, ενώ το κέντρο ανάλυσης πληροφοριών της ΕΕ (EU INTCEN) διαδραματίζει καθοριστικό ρόλο στην προώθηση της ανταλλαγής στρατηγικών πληροφοριών μεταξύ των υπηρεσιών πληροφοριών και ασφάλειας των κρατών μελών και παρέχει πληροφορίες επίγνωσης των καταστάσεων προς όφελος των θεσμικών οργάνων της ΕΕ[114]. Ο **Ευρωπόλ**, επεκτείνοντας τη συνεργασία του με τρίτες χώρες, μπορεί επίσης να διαδραματίσει καθοριστικό ρόλο στην καταπολέμηση του εγκλήματος και της τρομοκρατίας, σε συνοχή με άλλες εξωτερικές πολιτικές και εργαλεία της ΕΕ. Ωστόσο, ο Ευρωπόλ αντιμετωπίζει σήμερα σειρά σοβαρών περιορισμών —ιδίως όσον αφορά την άμεση ανταλλαγή δεδομένων προσωπικού χαρακτήρα με ιδιωτικούς

[112] Όπως το σχέδιο δράσης για την ενωσιακή στρατηγική ασφάλειας στη θάλασσα το οποίο οδήγησε σε σημαντικά επιτεύγματα χάρη στη συνεργασία μεταξύ αρμόδιων οργανισμών της ΕΕ όσον αφορά καθήκοντα ακτοφυλακής.

[113] Η καταπολέμηση του οργανωμένου εγκλήματος στην ΕΕ το 2019 (Συμβούλιο, 2020).

[114] Το EU INTCEN αποτελεί τη μοναδική πύλη μέσω της οποίας οι υπηρεσίες πληροφοριών και ασφάλειας των κρατών μελών μπορούν να παρέχουν στην ΕΕ επίγνωση των καταστάσεων βασιζόμενη σε πληροφορίες.

φορείς— οι οποίοι δεν του επιτρέπουν να στηρίξει αποτελεσματικά τα κράτη μέλη στην καταπολέμηση της τρομοκρατίας και του εγκλήματος. Επί του παρόντος, αξιολογείται η εντολή του Ευρωπόλ για να διερευνηθεί πως θα πρέπει να βελτιωθεί, ώστε να διασφαλίζεται ότι ο Οργανισμός μπορεί να εκτελεί τα καθήκοντά του στο ακέραιο. Σε αυτό το πλαίσιο, οι αρμόδιες αρχές σε επίπεδο ΕΕ (όπως η OLAF, ο Ευρωπόλ, ο Eurojust και η Ευρωπαϊκή Εισαγγελία) θα πρέπει επίσης να συνεργάζονται στενότερα και να βελτιώνουν την ανταλλαγή πληροφοριών.

Μια άλλη βασική σύνδεση είναι η περαιτέρω ανάπτυξη του **Eurojust** για να μεγιστοποιηθεί η συνέργεια μεταξύ της συνεργασίας στον τομέα της επιβολής του νόμου και της δικαστικής συνεργασίας. Η ΕΕ θα ωφεληθεί επίσης από μεγαλύτερη στρατηγική συνοχή: η **EMPACT**[115], ο κύκλος πολιτικής της ΕΕ για το σοβαρό και διεθνές οργανωμένο έγκλημα, παρέχει στις αρχές μια μεθοδολογία βασιζόμενη σε εγκληματολογικές πληροφορίες, ώστε να αντιμετωπίζουν από κοινού τις πλέον σημαντικές εγκληματικές απειλές που επηρεάζουν την ΕΕ. Την τελευταία δεκαετία έχει αποφέρει σημαντικά επιχειρησιακά αποτελέσματα[116]. Με βάση την πείρα των επαγγελματιών του κλάδου, ο υφιστάμενος μηχανισμός θα πρέπει να εξορθολογιστεί και να απλουστευθεί, ώστε να αντιμετωπίζει καλύτερα τις πλέον πιεστικές και εξελισσόμενες εγκληματικές απειλές για έναν νέο κύκλο πολιτικής την περίοδο 2022-2025.

Η έγκαιρη και σχετική **πληροφόρηση** είναι καίριας σημασίας για τις καθημερινές εργασίες δίωξης του εγκλήματος. Παρά την ανάπτυξη νέων βάσεων δεδομένων σε επίπεδο ΕΕ για την ασφάλεια και τη διαχείριση των συνόρων, πολλές πληροφορίες εξακολουθούν να βρίσκονται σε εθνικές βάσεις δεδομένων ή να ανταλλάσσονται εκτός αυτών των εργαλείων. Αυτό έχει ως αποτέλεσμα σημαντικό πρόσθετο φόρτο εργασίας, καθυστερήσεις και αυξημένο κίνδυνο απώλειας βασικών πληροφοριών. Η βελτίωση, η επιτάχυνση και η απλούστευση των διαδικασιών, με τη συμμετοχή ολόκληρης της κοινότητας ασφάλειας, θα αποφέρουν καλύτερα αποτελέσματα. Τα σωστά εργαλεία είναι απαραίτητα προκειμένου να αξιοποιούνται πλήρως οι δυνατότητες της ανταλλαγής πληροφοριών με σκοπό την αποτελεσματική δίωξη του εγκλήματος, ενώ παράλληλα θα πρέπει να προβλέπονται οι απαραίτητες διασφαλίσεις, ώστε η ανταλλαγή δεδομένων να σέβεται τη νομοθεσία για την προστασία των δεδομένων και τα θεμελιώδη δικαιώματα. Υπό το πρίσμα των εξελίξεων στον τομέα της τεχνολογίας, της εγκληματολογίας και της προστασίας των δεδομένων, καθώς και της μεταβολής των επιχειρησιακών αναγκών, η ΕΕ θα μπορούσε να εξετάσει αν χρειάζεται να εκσυγχρονιστούν μέσα, όπως οι **αποφάσεις Prüm του 2008** με τις οποίες θεσπίζεται η αυτόματη ανταλλαγή δεδομένων DNA, δακτυλικών αποτυπωμάτων και αδειών κυκλοφορίας οχημάτων, ώστε να καταστεί εφικτή η αυτοματοποιημένη ανταλλαγή πρόσθετων κατηγοριών δεδομένων που είναι ήδη διαθέσιμα σε βάσεις ποινικών ή άλλων δεδομένων των κρατών μελών για τους σκοπούς ποινικών ερευνών. Επιπλέον, η Επιτροπή θα εξετάσει τη δυνατότητα ανταλλαγής ποινικών μητρώων, ώστε να διαπιστώνεται αν υπάρχει ποινικό μητρώο για ένα πρόσωπο σε άλλα κράτη μέλη και να διευκολύνεται η πρόσβαση στα εν λόγω μητρώα, μόλις εντοπιστούν, με όλες τις απαραίτητες διασφαλίσεις.

Οι **πληροφορίες για τους ταξιδιώτες** συμβάλλουν στη βελτίωση των συνοριακών ελέγχων, στη μείωση της παράτυπης μετανάστευσης και στον εντοπισμό προσώπων που συνεπάγονται κινδύνους για την ασφάλεια. Τα δεδομένα εκ των προτέρων πληροφοριών σχετικά με τους επιβάτες είναι τα βιογραφικά δεδομένα κάθε επιβάτη που συλλέγεται από τους αερομεταφορείς κατά τον έλεγχο εισιτηρίων και αποστέλλονται εκ των προτέρων στις

[115] EMPACT σημαίνει Ευρωπαϊκή Πολυκλαδική Πλατφόρμα κατά των Εγκληματικών Απειλών.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

αρχές ελέγχου των συνόρων στη χώρα προορισμού. Η αναθεώρηση του νομικού πλαισίου[117] θα μπορούσε να βελτιώσει την αποτελεσματική αξιοποίηση των πληροφοριών, διασφαλίζοντας παράλληλα τη συμμόρφωση με τη νομοθεσία για την προστασία των δεδομένων και διευκολύνοντας τη ροή των επιβατών. Οι καταστάσεις ονομάτων επιβατών (PNR) είναι τα δεδομένα που παρέχουν οι επιβάτες κατά την κράτηση πτήσεων. Η εφαρμογή της οδηγίας για τις καταστάσεις ονομάτων επιβατών[118] έχει καίρια σημασία και η Επιτροπή θα συνεχίσει να στηρίζει και να επιβάλλει την εφαρμογή της. Επιπλέον, ως ενδιάμεση δράση, η Επιτροπή θα προβεί σε επανεξέταση της τρέχουσας προσέγγισης όσον αφορά τη **διαβίβαση δεδομένων PNR σε τρίτες χώρες**.

Η **δικαστική συνεργασία** αποτελεί απαραίτητο συμπλήρωμα των προσπαθειών της αστυνομίας για την καταπολέμηση του διασυνοριακού εγκλήματος. Τα τελευταία 20 έτη η δικαστική συνεργασία έχει διέλθει ριζικότερες αλλαγές. Είναι αναγκαίο φορείς, όπως η **Ευρωπαϊκή Εισαγγελία** και ο **Eurojust**, να διαθέτουν τα μέσα για να λειτουργούν στον μέγιστο βαθμό ή να ενισχυθούν. Θα μπορούσε επίσης να ενισχυθεί η συνεργασία μεταξύ επαγγελματιών του τομέα της δικαιοσύνης με τη λήψη περαιτέρω μέτρων όσον αφορά την αμοιβαία αναγνώριση δικαστικών αποφάσεων, την κατάρτιση των δικαστικών και την ανταλλαγή πληροφοριών. Στόχος θα πρέπει να είναι η αύξηση της αμοιβαίας εμπιστοσύνης μεταξύ των δικαστών και των εισαγγελέων, η οποία είναι κεντρικής σημασίας για την ομαλή διεξαγωγή διασυνοριακών διαδικασιών. Η χρήση **ψηφιακών τεχνολογιών** μπορεί επίσης να βελτιώσει την αποδοτικότητα των δικαστικών μας συστημάτων. Με τη στήριξη του Eurojust, συστήνεται επί του παρόντος νέο ψηφιακό σύστημα ανταλλαγής για τη διαβίβαση ευρωπαϊκών εντολών έρευνας, αιτημάτων αμοιβαίας δικαστικής συνδρομής και σχετικών ανακοινώσεων μεταξύ των κρατών μελών. Η Επιτροπή θα συνεργαστεί με τα κράτη μέλη για να επιταχυνθεί η εγκατάσταση των απαραίτητων συστημάτων ΤΠ σε εθνικό επίπεδο.

Η διεθνής συνεργασία είναι επίσης καίριας σημασίας για την αποτελεσματική επιβολή του νόμου και τη δικαστική συνεργασία. Οι διμερείς συμφωνίες με βασικούς εταίρους διαδραματίζουν καθοριστικό ρόλο στην εξασφάλιση πληροφοριών και αποδεικτικών στοιχείων πέραν της ΕΕ. Σημαντικός είναι επίσης ο ρόλος του **Ιντερπόλ**, ενός από τους μεγαλύτερους διακυβερνητικούς οργανισμούς εγκληματολογικής αστυνομίας. Η Επιτροπή θα εξετάσει πιθανούς τρόπους ενίσχυσης της συνεργασίας με τον Ιντερπόλ, όπως, για παράδειγμα, η ενδεχόμενη πρόσβαση σε βάσεις δεδομένων του Ιντερπόλ και η ενίσχυση της επιχειρησιακής και στρατηγικής συνεργασίας. Οι αρχές επιβολής του νόμου στην ΕΕ βασίζονται επίσης σε βασικές χώρες-εταίρους σημασίας για τον εντοπισμό και τη διερεύνηση εγκληματιών και τρομοκρατών. Θα μπορούσαν να ενισχυθούν οι **εταιρικές σχέσεις στον τομέα της ασφάλειας μεταξύ της ΕΕ και τρίτων χωρών**, με στόχο να ενισχυθεί η συνεργασία για την αντιμετώπιση κοινών απειλών, όπως η τρομοκρατία, το οργανωμένο έγκλημα, το κυβερνοέγκλημα, η σεξουαλική κακοποίηση παιδιών και η εμπορία ανθρώπων. Η προσέγγιση αυτή θα βασίζεται σε κοινά συμφέροντα στον τομέα της ασφάλειας και σε καθιερωμένους διαύλους επικοινωνίας περί συνεργασίας και ασφάλειας.

Επιπροσθέτως της ανταλλαγής πληροφοριών, η ανταλλαγή εμπειρογνωσίας μπορεί να είναι ιδιαίτερα σημαντική για αυξημένη ετοιμότητα της επιβολής του νόμου έναντι **μη παραδοσιακών απειλών**. Η Επιτροπή θα ενθαρρύνει την ανταλλαγή βέλτιστων πρακτικών

[117] Οδηγία 2004/82/ΕΚ του Συμβουλίου σχετικά με την υποχρέωση των μεταφορέων να κοινοποιούν τα στοιχεία των επιβατών.

[118] Οδηγία 2016/681 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

και θα διερευνήσει επίσης έναν πιθανό **μηχανισμό συντονισμού των αστυνομικών δυνάμεων σε επίπεδο ΕΕ** σε καταστάσεις ανωτέρας βίας, όπως πανδημίες. Η πανδημία απέδειξε επίσης ότι η ψηφιακή αστυνομία της γειτονιάς, σε συνδυασμό με νομικά πλαίσια για τη διευκόλυνση της αστυνόμευσης στο διαδίκτυο, θα είναι θεμελιώδους σημασίας για την καταπολέμηση του εγκλήματος και της τρομοκρατίας. Οι εταιρικές σχέσεις μεταξύ αστυνομίας και κοινοτήτων, τόσο στο διαδίκτυο όσο και εκτός αυτού, μπορούν να αποτρέψουν την εγκληματικότητα και να μετριάσουν τις επιπτώσεις του οργανωμένου εγκλήματος, της ριζοσπαστικοποίησης και των τρομοκρατικών δραστηριοτήτων. Η σύνδεση των λύσεων αστυνόμευσης σε τοπικό, περιφερειακό, εθνικό και ενωσιακό επίπεδο αποτελεί βασικό παράγοντα επιτυχίας για την Ένωση Ασφάλειας της ΕΕ στο σύνολό της.

Η συμβολή των ισχυρών εξωτερικών συνόρων

Η σύγχρονη και αποδοτική διαχείριση των εξωτερικών συνόρων έχει το διττό όφελος της διατήρησης της ακεραιότητας του Σένγκεν και της παροχής ασφάλειας στους πολίτες μας. Η συμμετοχή όλων των σχετικών φορέων για τη μέγιστη αξιοποίηση της ασφάλειας στα σύνορα μπορεί να έχει πραγματικό αντίκτυπο στην πρόληψη του διασυνοριακού εγκλήματος και της τρομοκρατίας. Οι κοινές επιχειρησιακές δραστηριότητες της πρόσφατα ενισχυμένης Ευρωπαϊκής Συνοριοφυλακής και Ακτοφυλακής[119] συμβάλλουν στην πρόληψη και την ανίχνευση του διασυνοριακού εγκλήματος στα **εξωτερικά σύνορα** και πέραν της ΕΕ. Οι τελωνειακές δραστηριότητες, αφενός, για τον εντοπισμό κινδύνων που αφορούν την ασφάλεια και την ασφάλεια από εξωτερικές ενέργειες σε όλα τα εμπορεύματα πριν από την άφιξή τους στην ΕΕ και, αφετέρου, για τον έλεγχο εμπορευμάτων κατά την άφιξή τους, είναι ζωτικής σημασίας για την καταπολέμηση του διασυνοριακού εγκλήματος και της τρομοκρατίας. Στο προσεχές σχέδιο δράσης για την τελωνειακή ένωση θα εξαγγελθούν δράσεις που επίσης έχουν ως στόχο την ενίσχυση της διαχείρισης κινδύνων και την αύξηση της εσωτερικής ασφάλειας, μεταξύ άλλων, ιδίως με την αξιολόγηση της σκοπιμότητας σύνδεσης των σχετικών συστημάτων πληροφοριών για σκοπούς ανάλυσης κινδύνων για την ασφάλεια.

Τον Μάιο του 2019 εγκρίθηκε το πλαίσιο **διαλειτουργικότητας μεταξύ των συστημάτων πληροφοριών της ΕΕ** στον τομέα της δικαιοσύνης και των εσωτερικών υποθέσεων. Η νέα αυτή αρχιτεκτονική αποσκοπεί στη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των νέων ή αναβαθμισμένων συστημάτων πληροφοριών[120]. Το πλαίσιο διαλειτουργικότητας θα οδηγήσει σε ταχύτερη και συστηματικότερη πληροφόρηση των υπαλλήλων επιβολής του νόμου, των συνοριοφυλάκων και των υπαλλήλων των υπηρεσιών μετανάστευσης. Θα συμβάλει στην ορθή ταυτοποίηση και στην καταπολέμηση της πλαστοπροσωπίας. Για να υλοποιηθούν οι ως άνω επιδιώξεις, η εφαρμογή της διαλειτουργικότητας θα πρέπει να αποτελέσει προτεραιότητα, τόσο σε πολιτικό όσο και σε τεχνικό επίπεδο. Η στενή συνεργασία μεταξύ των οργανισμών της ΕΕ και όλων των κρατών μελών θα είναι υψίστης σημασίας για την επίτευξη του στόχου της πλήρους διαλειτουργικότητας έως το 2023.

Η **πλαστογράφηση ταξιδιωτικών εγγράφων** θεωρείται μία από τις αξιόποινες πράξεις που διαπράττονται συχνότερα. Διευκολύνει την παράνομη μετακίνηση εγκληματιών και τρομοκρατών και διαδραματίζει μείζονα ρόλο στην εμπορία ανθρώπων και στο εμπόριο

[119] Αποτελούμενης από τον Ευρωπαϊκό Οργανισμό Συνοριοφυλακής και Ακτοφυλακής (Frontex) και τις αρχές συνοριοφυλακής και ακτοφυλακής των κρατών μελών.

[120] Το σύστημα εισόδου/εξόδου (ΣΕΕ), το Ευρωπαϊκό Σύστημα Πληροφοριών και Αδειοδότησης Ταξιδιού (ETIAS), το εκτεταμένο Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου (ECRIS-TCN), το σύστημα πληροφοριών Σένγκεν, το σύστημα πληροφοριών για τις θεωρήσεις και το μελλοντικό επικαιροποιημένο σύστημα Eurodac.

ναρκωτικών[121]. Η Επιτροπή θα εξετάσει τρόπους επέκτασης των εργασιών που ήδη εκπονούνται στον τομέα των προτύπων ασφάλειας των ενωσιακών εγγράφων διαμονής και ταξιδιού, μεταξύ άλλων, μέσω της ψηφιοποίησης. Από τον Αύγουστο του 2021, τα κράτη μέλη θα αρχίσουν να εκδίδουν δελτία ταυτότητας και έγγραφα διαμονής σύμφωνα με εναρμονισμένα πρότυπα ασφάλειας, συμπεριλαμβανομένου μικροκυκλώματος που θα περιέχει βιομετρικά αναγνωριστικά στοιχεία τα οποία θα μπορούν να επαληθεύονται από όλες τις συνοριακές αρχές της ΕΕ. Η Επιτροπή θα παρακολουθεί την εφαρμογή των εν λόγω νέων κανόνων, όπως, για παράδειγμα, η σταδιακή αντικατάσταση εγγράφων που βρίσκονται επί του παρόντος σε κυκλοφορία.

Ενίσχυση της έρευνας και της καινοτομίας στον τομέα της ασφάλειας

Οι εργασίες για την κατοχύρωση της κυβερνοασφάλειας και την καταπολέμηση του οργανωμένου εγκλήματος, του κυβερνοεγκλήματος και της τρομοκρατίας εξαρτώνται σε μεγάλο βαθμό από τη μελλοντική ανάπτυξη εργαλείων με σκοπό: τη συμβολή στη δημιουργία ασφαλέστερων και καλύτερα προστατευμένων νέων τεχνολογιών, την αντιμετώπιση των προκλήσεων που προκύπτουν από τις τεχνολογίες και την υποστήριξη του έργου των φορέων επιβολής του νόμου. Αυτό, με τη σειρά του, βασίζεται στους εταίρους του ιδιωτικού τομέα και στις βιομηχανίες.

Η καινοτομία θα πρέπει να θεωρείται στρατηγικό εργαλείο για την αντιμετώπιση των υφιστάμενων απειλών και την πρόβλεψη τόσο μελλοντικών κινδύνων όσο και ευκαιριών. Οι καινοτόμες τεχνολογίες μπορούν να δημιουργήσουν νέα εργαλεία για να βοηθήσουν τους φορείς επιβολής του νόμου και άλλους παράγοντες στον τομέα της ασφάλειας. Η τεχνητή νοημοσύνη και η ανάλυση μαζικών δεδομένων θα μπορούσαν να αξιοποιήσουν την υπολογιστική υψηλών επιδόσεων για την προσφορά καλύτερου εντοπισμού και γρήγορης και ολοκληρωμένης ανάλυσης[122]. Βασική προϋπόθεση για την ανάπτυξη αξιόπιστων τεχνολογιών είναι η ύπαρξη συνόλων δεδομένων υψηλής ποιότητας, τα οποία έχουν στη διάθεσή τους οι αρμόδιες αρχές για την εκπαίδευση, τη δοκιμή και την επικύρωση των αλγορίθμων[123]. Γενικότερα, ο κίνδυνος τεχνολογικής εξάρτησης είναι σημαντικός σήμερα —η ΕΕ είναι, για παράδειγμα, καθαρός εισαγωγέας προϊόντων και υπηρεσιών κυβερνοασφάλειας, με ό,τι αυτό συνεπάγεται για την οικονομία και τις υποδομές ζωτικής σημασίας. Για τον έλεγχο της τεχνολογίας και τη διασφάλιση της συνέχειας του εφοδιασμού, ακόμη και σε περίπτωση δυσμενών συμβάντων και κρίσεων, η Ευρώπη πρέπει να έχει παρουσία και ικανότητα στα κρίσιμα σημεία των σχετικών αξιακών αλυσίδων.

Η **έρευνα, η καινοτομία και η τεχνολογική ανάπτυξη** της ΕΕ προσφέρουν την ευκαιρία να ληφθεί υπόψη η διάσταση της ασφάλειας, καθώς αναπτύσσονται οι τεχνολογίες αυτές και η εφαρμογή τους. Η επόμενη γενιά προτάσεων χρηματοδότησης της ΕΕ μπορεί να λειτουργήσει καταλυτικά από την άποψη αυτή[124]. Οι πρωτοβουλίες για ευρωπαϊκούς χώρους δεδομένων και υποδομές υπολογιστικού νέφους συνυπολογίζουν την ασφάλεια από

[121] Η ύπαρξη δεσμού μεταξύ της πλαστογράφησης εγγράφων και της εμπορίας ανθρώπων περιγράφεται στη δεύτερη έκθεση σχετικά με την πρόοδο που σημειώνεται στις ενέργειες για την καταπολέμηση της εμπορίας ανθρώπων, COM(2018) 777 και στο συνοδευτικό έγγραφο εργασίας των υπηρεσιών της Επιτροπής SWD(2018) 473, όπως επίσης και στην έκθεση του Ευρωπόλ με τίτλο «Situation Report – Trafficking in Human Beings in the EU» (Έκθεση για την επικρατούσα κατάσταση όσον αφορά την εμπορία ανθρώπων στην ΕΕ) του 2016.

[122] Αυτό θα πρέπει να βασιστεί στη στρατηγική της Επιτροπής για την τεχνητή νοημοσύνη.

[123] Ευρωπαϊκή στρατηγική για τα δεδομένα, COM(2020) 66 final.

[124] Οι προτάσεις της Επιτροπής για το πρόγραμμα «Ορίζων Ευρώπη», το Ταμείο Εσωτερικής Ασφάλειας, το Ταμείο για την ολοκληρωμένη διαχείριση των συνόρων, το πρόγραμμα EUInvest, το Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης και το πρόγραμμα «Ψηφιακή Ευρώπη» θα στηρίξουν την ανάπτυξη και τη χρήση καινοτόμων τεχνολογιών και λύσεων ασφάλειας σε ολόκληρη την αξιακή αλυσίδα της ασφάλειας.

την αρχή. Το ευρωπαϊκό βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας και το δίκτυο εθνικών κέντρων συντονισμού[125] αποσκοπούν στη δημιουργία μιας αποτελεσματικής και αποδοτικής δομής μέσω της οποίας θα συγκεντρώνονται και θα ανταλλάσσονται οι ερευνητικές ικανότητες και τα αποτελέσματα στον τομέα της κυβερνοασφάλειας. Το διαστημικό πρόγραμμα της ΕΕ παρέχει υπηρεσίες που στηρίζουν την ασφάλεια της ΕΕ, των κρατών μελών της και των πολιτών[126].

Η χρηματοδοτούμενη από την ΕΕ έρευνα στον τομέα της ασφάλειας, στο πλαίσιο της οποίας δρομολογήθηκαν από το 2007 περισσότερα από 600 έργα συνολικής αξίας σχεδόν 3 δισ. EUR, αποτελεί βασικό μέσο για την προώθηση της τεχνολογίας και της γνώσης για τη στήριξη λύσεων ασφάλειας. Στο πλαίσιο της επανεξέτασης της εντολής του Ευρωπόλ, η Επιτροπή θα εξετάσει τη δημιουργία ενός **ευρωπαϊκού κόμβου καινοτομίας για την εσωτερική ασφάλεια**[127], με αποστολή την εξεύρεση κοινών λύσεων σε κοινές προκλήσεις και ευκαιρίες στον τομέα της ασφάλειας, τις οποίες τα κράτη μέλη ενδέχεται να μην είναι σε θέση να αξιοποιήσουν μόνα τους. Η συνεργασία είναι θεμελιώδους σημασίας για τη βέλτιστη εστίαση των επενδύσεων και την ανάπτυξη καινοτόμων τεχνολογιών με όφελος τόσο στον τομέα της ασφάλειας όσο και της οικονομίας.

Δεξιότητες και ευαισθητοποίηση

Η ευαισθητοποίηση σε θέματα ασφάλειας και η απόκτηση των δεξιοτήτων για την αντιμετώπιση πιθανών απειλών είναι ουσιαστικής σημασίας για την οικοδόμηση μιας πιο ανθεκτικής κοινωνίας, όπου οι επιχειρήσεις, οι διοικητικές υπηρεσίες και τα άτομα θα είναι καλύτερα προετοιμασμένα. Οι προκλήσεις όσον αφορά την υποδομή ΤΠ και τα ηλεκτρονικά συστήματα ανέδειξαν την ανάγκη βελτίωσης της ανθρώπινης ικανότητάς μας για ετοιμότητα και αντίδραση στον τομέα της κυβερνοασφάλειας. Η πανδημία ανέδειξε επίσης τη σημασία της ψηφιοποίησης σε όλους τους τομείς της οικονομίας και της κοινωνίας της ΕΕ.

Ακόμη και **βασικές γνώσεις σχετικά με τις απειλές κατά της ασφάλειας** και τον τρόπο αντιμετώπισής τους μπορούν να έχουν πραγματικό αντίκτυπο στην ανθεκτικότητα της κοινωνίας. Η επίγνωση των κινδύνων του κυβερνοεγκλήματος και η ανάγκη προστασίας από τους κινδύνους αυτούς μπορούν να λειτουργήσουν σε συνδυασμό με την προστασία από παρόχους υπηρεσιών για την αντιμετώπιση κυβερνοεπιθέσεων. Οι πληροφορίες σχετικά με τους κινδύνους που ενέχει η διακίνηση ναρκωτικών μπορούν να δυσχεράνουν ακόμη περισσότερο την επιτυχία των εγκληματιών. Η ΕΕ μπορεί να τονώσει τη διάδοση βέλτιστων πρακτικών, για παράδειγμα μέσω του δικτύου Κέντρων Ασφαλούς Διαδικτύου[128], και να διασφαλίσει ότι οι στόχοι αυτοί λαμβάνονται υπόψη στα δικά της προγράμματα.

---

[125] Πρόταση, της 12ης Σεπτεμβρίου 2018, για τη σύσταση του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού, COM(2018) 630.

[126] Για παράδειγμα, το πρόγραμμα Copernicus παρέχει υπηρεσίες που επιτρέπουν την επιτήρηση των εξωτερικών συνόρων της ΕΕ και τη θαλάσσια επιτήρηση, πράγμα που συμβάλλει στη δράση κατά της πειρατείας και της παράνομης διακίνησης, καθώς και στη στήριξη υποδομών ζωτικής σημασίας. Μόλις καταστεί πλήρως λειτουργικό, το πρόγραμμα αυτό θα αποτελέσει καταλυτικό παράγοντα για τις πολιτικές και στρατιωτικές αποστολές και επιχειρήσεις.

[127] Ο εν λόγω κόμβος θα συνεργάζεται επίσης με τον EBCGA/Frontex, τον CEPOL, τον eu-LISA και το Κοινό Κέντρο Ερευνών.

[128] Βλ. www.betterinternetforkids.eu: η κεντρική πύλη και τα εθνικά Κέντρα Ασφαλούς Διαδικτύου χρηματοδοτούνται επί του παρόντος στο πλαίσιο του τηλεπικοινωνιακού προγράμματος του μηχανισμού «Συνδέοντας την Ευρώπη», και έχει προταθεί μελλοντική χρηματοδότηση στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη».

Το μελλοντικό σχέδιο δράσης για την ψηφιακή εκπαίδευση θα πρέπει να περιλαμβάνει στοχευμένα μέτρα για την απόκτηση δεξιοτήτων ΤΠ στον τομέα της ασφάλειας για το σύνολο του πληθυσμού. Το θεματολόγιο δεξιοτήτων[129] που εγκρίθηκε πρόσφατα υποστηρίζει την απόκτηση δεξιοτήτων καθ' όλη τη διάρκεια της ζωής. Περιλαμβάνει ειδικές δράσεις για την αύξηση του αριθμού των πτυχιούχων στους τομείς των φυσικών επιστημών, της τεχνολογίας, της μηχανικής, των τεχνών και των μαθηματικών που απαιτούνται σε τομείς αιχμής, όπως η κυβερνοασφάλεια. Πρόσθετες δράσεις, που χρηματοδοτούνται από το πρόγραμμα «Ψηφιακή Ευρώπη», θα επιτρέψουν στους επαγγελματίες να συμβαδίζουν με τις εξελίξεις στο τοπίο των απειλών κατά της ασφάλειας και, ταυτόχρονα, να καλύπτουν τις ελλείψεις στον τομέα αυτόν στην αγορά εργασίας της ΕΕ. Ο συνολικός αντίκτυπος θα είναι η παροχή της δυνατότητας στα άτομα να αποκτήσουν δεξιότητες για την αντιμετώπιση των απειλών κατά της ασφάλειας και στις επιχειρήσεις να βρίσκουν τους επαγγελματίες που χρειάζονται στον τομέα αυτόν. Οι μελλοντικοί Ευρωπαϊκοί Χώροι Έρευνας και Εκπαίδευσης θα προωθούν επίσης τις σταδιοδρομίες στους τομείς των φυσικών επιστημών, της τεχνολογίας, της μηχανικής, των τεχνών και των μαθηματικών.

Επίσης σημαντική είναι η πρόσβαση των **θυμάτων** στα δικαιώματά τους· πρέπει να λαμβάνουν την αναγκαία βοήθεια και υποστήριξη, ανάλογα με τις ιδιαίτερες περιστάσεις στις οποίες βρίσκονται. Ιδιαίτερες προσπάθειες απαιτούνται όσον αφορά τις μειονότητες και για τα πιο ευάλωτα θύματα, όπως παιδιά ή γυναίκες που διακινούνται με σκοπό τη σεξουαλική εκμετάλλευση ή που εκτίθενται σε ενδοοικογενειακή βία[130].

Η ενίσχυση των **δεξιοτήτων στον τομέα της επιβολής του νόμου** μπορεί να διαδραματίσει ιδιαίτερο ρόλο. Λόγω των τρεχουσών και των νέων τεχνολογικών απειλών απαιτούνται περισσότερες επενδύσεις στην αναβάθμιση των δεξιοτήτων του προσωπικού επιβολής του νόμου στο αρχικό στάδιο και καθ' όλη τη διάρκεια της σταδιοδρομίας του. Ο CEPOL είναι βασικός εταίρος για την παροχή συνδρομής στα κράτη μέλη στο έργο αυτό. Η κατάρτιση των υπηρεσιών επιβολής του νόμου σε θέματα ρατσισμού και ξενοφοβίας, και ιδίως σε θέματα δικαιωμάτων των πολιτών γενικότερα, πρέπει να αποτελούν ουσιώδη συνιστώσα της ενωσιακής νοοτροπίας ασφάλειας. Τα εθνικά συστήματα απονομής δικαιοσύνης και οι επαγγελματίες της δικαιοσύνης πρέπει επίσης να είναι εφοδιασμένοι για να προσαρμόζονται και να ανταποκρίνονται σε άνευ προηγουμένου προκλήσεις. Η κατάρτιση είναι απαραίτητη για να μπορούν οι επιτόπιες αρχές να αξιοποιούν στο έπακρο τα εργαλεία υπό επιχειρησιακές συνθήκες. Επιπλέον, θα πρέπει να καταβληθεί κάθε δυνατή προσπάθεια για την ενίσχυση της συνεκτίμησης της ισότητας των φύλων, καθώς και της συμμετοχής των γυναικών στην επιβολή του νόμου.

Βασικές δράσεις
• Ενίσχυση της εντολής του Ευρωπόλ • Διερεύνηση ενός «Κώδικα αστυνομικής συνεργασίας» και του αστυνομικού συντονισμού σε περιόδους κρίσης • Ενίσχυση του Eurojust για τη διασύνδεση των δικαστικών αρχών και των αρχών επιβολής του νόμου

[129] Ευρωπαϊκό Θεματολόγιο δεξιοτήτων για βιώσιμη ανταγωνιστικότητα, κοινωνική δικαιοσύνη και ανθεκτικότητα, COM(2020) 274 final.

[130] Βλ. Στρατηγική για την ισότητα των φύλων, COM(2020) 152· Στρατηγική για τα δικαιώματα των θυμάτων, COM(2020) 258· και Διαδίκτυο καλύτερα προσαρμοσμένο στα παιδιά: μια ευρωπαϊκή στρατηγική, COM(2012) 196.

- Αναθεώρηση της οδηγίας για τις εκ των προτέρων πληροφορίες για τους επιβάτες
- Ανακοίνωση σχετικά με την εξωτερική διάσταση των καταστάσεων ονομάτων επιβατών
- Ενίσχυση της συνεργασίας μεταξύ της ΕΕ και του Ιντερπόλ
- Πλαίσιο διαπραγματεύσεων με βασικές τρίτες χώρες για την ανταλλαγή πληροφοριών
- Καλύτερα πρότυπα ασφάλειας για τα ταξιδιωτικά έγγραφα
- Διερεύνηση ενός ευρωπαϊκού κόμβου καινοτομίας για την εσωτερική ασφάλεια

V. Συμπεράσματα

Σε έναν κόσμο όλο και μεγαλύτερων αναταράξεων, η Ευρωπαϊκή Ένωση εξακολουθεί να θεωρείται ευρέως ένας από τους ασφαλέστερους και πιο προστατευμένους χώρους. Ωστόσο, αυτό δεν μπορεί να θεωρηθεί δεδομένο.

Η νέα στρατηγική για την Ένωση Ασφάλειας θέτει τα θεμέλια για ένα οικοσύστημα ασφάλειας που εκτείνεται σε όλο το εύρος της ευρωπαϊκής κοινωνίας. Βασίζεται στη γνώση ότι η ασφάλεια αποτελεί κοινή ευθύνη. Η ασφάλεια είναι ζήτημα που αφορά όλους. Όλα οι κρατικοί φορείς, οι επιχειρήσεις, οι κοινωνικές οργανώσεις, τα θεσμικά όργανα και οι πολίτες πρέπει να εκπληρώσουν τις υποχρεώσεις τους, ώστε να καταστούν ασφαλέστερες οι κοινωνίες μας.

Τα ζητήματα ασφάλειας πρέπει πλέον να εξετάζονται από πολύ ευρύτερη προοπτική απ' ό,τι στο παρελθόν. Πρέπει να ξεπεραστούν οι ψευδείς διακρίσεις μεταξύ φυσικού και ψηφιακού κόσμου. Η στρατηγική της ΕΕ για την Ένωση Ασφάλειας συνενώνει ολόκληρο το φάσμα των αναγκών ασφάλειας και επικεντρώνεται στους τομείς που θα είναι οι πλέον κρίσιμοι για την ασφάλεια της ΕΕ κατά τα επόμενα έτη. Αναγνωρίζει επίσης ότι οι απειλές για την ασφάλεια δεν σταματούν στα γεωγραφικά σύνορα, και λαμβάνει επίσης υπόψη τη συνεχώς αυξανόμενη διασύνδεση μεταξύ εσωτερικής και εξωτερικής ασφάλειας[131]. Στο πλαίσιο αυτό, θα είναι σημαντικό η ΕΕ να συνεργάζεται με τους διεθνείς εταίρους για την προστασία όλων των πολιτών της και να διατηρεί στενό συντονισμό με την εξωτερική δράση της ΕΕ κατά την υλοποίηση της εν λόγω στρατηγικής.

Η ασφάλειά μας συνδέεται με τις θεμελιώδεις αξίες μας. Όλες οι προτεινόμενες δράσεις και πρωτοβουλίες της εν λόγω στρατηγικής θα σέβονται πλήρως τα θεμελιώδη δικαιώματα και τις ευρωπαϊκές αξίες μας. Αυτά συνιστούν τα θεμέλια του ευρωπαϊκού τρόπου ζωής μας και πρέπει να παραμείνουν στο επίκεντρο του έργου μας.

Τέλος, η Επιτροπή έχει πλήρη επίγνωση του γεγονότος ότι κάθε πολιτική ή δράση αποκτά νόημα μόνον όταν εφαρμόζεται και επιβάλλεται στην πράξη. Για τον λόγο αυτόν, είναι αναγκαίο να τονίζουμε συνεχώς τη σημασία της ορθής εφαρμογής και επιβολής της ισχύουσας και της μελλοντικής νομοθεσίας. Η πτυχή αυτή θα παρακολουθείται μέσω τακτικών εκθέσεων για την Ένωση Ασφάλειας, και η Επιτροπή θα ενημερώνει πλήρως το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και τα ενδιαφερόμενα μέρη για όλες τις σχετικές δράσεις, ενώ θα ενθαρρύνει τη συμμετοχή τους σε αυτές. Επιπλέον, η Επιτροπή είναι έτοιμη να συμμετάσχει σε κοινές συζητήσεις με τα θεσμικά όργανα σχετικά με τη στρατηγική για την Ένωση Ασφάλειας, καθώς και να διοργανώσει τέτοιες συζητήσεις, ώστε να προβεί από κοινού με τα άλλα θεσμικά όργανα σε απολογισμό της επιτευχθείσας προόδου, εξετάζοντας συγχρόνως με αυτά τις μελλοντικές προκλήσεις.

[131] Βλ. συνολική στρατηγική της ΕΕ

Η Επιτροπή καλεί το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο να εγκρίνουν την παρούσα στρατηγική για την Ένωση Ασφάλειας ως βάση για τη συνεργασία και την κοινή δράση στον τομέα της ασφάλειας κατά την επόμενη πενταετία.