CENTER
FOR
CYBER
RESILIENCE

ΠΟΛΙΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΨΗΦΙΑΚΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ

ΑΠΟ ΤΗΝ ΚΑΤΑΚΕΡΜΑΤΙΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΑ ΣΤΗΝ ΚΟΙΝΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΙΚΟΝΑ ΚΑΙ ΣΤΟΝ ΕΝΙΑΙΟ ΣΤΡΑΤΗΓΙΚΟ ΣΧΕΔΙΑΣΜΟ

DELPHI ECONOMIC FORUM

POLICY PAPERS

ΜΕ ΤΗΝ ΥΠΟΣΤΗΡΙΞΗ ΤΗΣ BAT HELLAS

BAT
A BETTER TOMORROW

ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Το παρόν Policy Paper συνδυάζει τη συζήτηση στρογγυλής τραπέζης με τίτλο «Anti-illicit strategies in the online environment» που διοργάνωσε το Delphi Economic Forum υπό τον κανόνα Chatham House στις 15 Ιουλίου 2026 στην Αθήνα με συμπληρωματική ανάλυση στοιχείων από επίσημες πηγές της Ευρωπαϊκής Ένωσης, του ΟΟΣΑ, του EUIPO, της Europol και του Παγκόσμιου Οργανισμού Τελωνείων.

Τα αριθμητικά στοιχεία της συζήτησης διατηρούνται μόνο όπου συμβάλλουν στην ελληνική επιχειρησιακή εικόνα και διακρίνονται από τις διεθνώς επαληθεύσιμες εκτιμήσεις. Επειδή δεν υπάρχει ενιαίος διεθνής δείκτης για το σύνολο του ψηφιακού παράνομου εμπορίου, η συγκεκριμένη έκθεση αποφεύγει την άθροιση διαφορετικών αγορών και χρησιμοποιεί τα δεδομένα για παραποιημένα προϊόντα ως ισχυρή, αλλά όχι εξαντλητική, ένδειξη της κλίμακας.

ΛΕΙΤΟΥΡΓΙΚΟΣ ΟΡΙΣΜΟΣ

Ως ψηφιακό παράνομο εμπόριο νοείται η αξιοποίηση ιστοτόπων, marketplaces, μέσων κοινωνικής δικτύωσης, εφαρμογών, υπηρεσιών ηλεκτρονικών πληρωμών και ψηφιακών εργαλείων επικοινωνίας για την προώθηση, πώληση, πληρωμή ή οργάνωση της διακίνησης λαθραίων, παραποιημένων, μη ασφαλών, μη συμμορφούμενων ή άλλως παράνομων προϊόντων. Ο όρος περιγράφει ένα λειτουργικό οικοσύστημα και όχι ένα ενιαίο ποινικό αδίκημα.

Επιτελική σύνοψη

Το ψηφιακό παράνομο εμπόριο δεν αποτελεί μια πλήρως νέα μορφή παρανομίας. Αποτελεί τον μετασχηματισμό παραδοσιακών παράνομων αγορών μέσα από την διείσδυση στις υποδομές του νόμιμου ηλεκτρονικού εμπορίου. Η διαφήμιση, η συναλλαγή και η πληρωμή μπορούν να γίνονται ψηφιακά, ενώ η παραγωγή, η αποθήκευση και η παράδοση παραμένουν φυσικές. Η υβριδικότητα αυτή του ψηφιακού εμπορίου κατακερματίζει την πληροφορία και επιτρέπει σε πολλές μικρές και επιμέρους λειτουργίες να αποκρύπτουν ένα οργανωμένο δίκτυο μεγάλης κλίμακας.

Η διεθνής και ευρωπαϊκή εικόνα επιβεβαιώνει τη μετάβαση προς τις μαζικές μικρές αποστολές. Σύμφωνα με την έκθεση του OECD–EUIPO, τα παραποιημένα και πειρατικά προϊόντα αντιστοιχούσαν το 2021 σε έως 2,3% του παγκόσμιου εμπορίου και 4,7% των εισαγωγών της ΕΕ. Το 79% των σχετικών κατασχέσεων αφορούσε αποστολές με λιγότερα από δέκα τεμάχια. Στην ΕΕ, οι μικρές αποστολές αποτελούσαν το 97% του συνόλου το 2025, καθιστώντας τον καθολικό φυσικό έλεγχο ανέφικτο.

Το φαινόμενο συνδέεται συστηματικά με το οργανωμένο και το οικονομικό έγκλημα, την απάτη, τη νομιμοποίηση εσόδων, τις φορολογικές και τελωνειακές παραβάσεις, τις παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και τη διαφθορά. Σε ορισμένες αγορές εμφανίζονται επίσης συνέργειες με το κυβερνοέγκλημα ως υπηρεσία, εκμετάλλευση ανηλίκων ως money mules ή διακινητών και παράνομες αγορές φαρμάκων, ουσιών ντόπινγκ, καπνικών προϊόντων και όπλων. Η σύνδεση με τη χρηματοδότηση της τρομοκρατίας πρέπει να αξιολογείται με βάση συγκεκριμένα αποδεικτικά στοιχεία και συγκεκριμένες υποθέσεις και όχι να θεωρείται αυτομάτως δεδομένη.

Η αποτελεσματική απάντηση δεν εξαντλείται στην αύξηση των ελέγχων. Απαιτεί κοινή επιχειρησιακή εικόνα, έγκαιρη και νόμιμη ανταλλαγή δεδομένων, στόχευση βάσει κινδύνου και οντότητας, σαφή ταυτοποίηση πωλητών, ταχεία συνεργασία με πλατφόρμες και παρόχους πληρωμών και συστηματική οικονομική διερεύνηση. Η Τεχνητή Νοημοσύνη μπορεί να λειτουργεί ως πολλαπλασιαστής ισχύος, όχι ως αυτόνομος μηχανισμός απόδειξης ή κύρωσης.

Για την Ελλάδα, η πρόκληση είναι ταυτόχρονα ποσοτική και θεσμική. Η εκρηκτική αύξηση των κινήσεων ηλεκτρονικού εμπορίου από τρίτες χώρες επιβαρύνει τις τελωνειακές πύλες, ενώ η πληροφορία παραμένει κατανεμημένη μεταξύ τελωνείων, φορολογικών και αστυνομικών αρχών, εποπτικών φορέων, πλατφορμών, παρόχων πληρωμών και επιχειρήσεων μεταφοράς. Τα διαθέσιμα στοιχεία δεν συγκροτούν ακόμη ενιαία εθνική μέτρηση του φαινομένου, αποτυπώνουν όμως ουσιαστική έκθεση: η Ελλάδα περιλαμβανόταν το 2024 στις δέκα χώρες της ΕΕ με τη μεγαλύτερη τελωνειακή δέσμευση παραποιημένων προϊόντων τόσο ως προς τον αριθμό όσο και ως προς την εκτιμώμενη αξία.

Η καταπολέμηση απαιτεί να μετατραπούν οι υφιστάμενες δυνατότητες σε σταθερό σύστημα συνεργασίας: κοινή επιχειρησιακή εικόνα, διαλειτουργικά και ασφαλή δεδομένα, σαφή σημεία επαφής, προκαθορισμένοι χρόνοι ανταπόκρισης και αξιολόγηση με δείκτες αποτελέσματος. Προτεραιότητα πρέπει να δοθεί στη διακοπή ολόκληρου του δικτύου –πωλητή, ψηφιακής παρουσίας, πληρωμής και φυσικής διανομής– και στην παράλληλη δέσμευση του παράνομου οικονομικού οφέλους, με αναλογικότητα και δικαστικό έλεγχο.

ΤΑΥΤΟΤΗΤΑ
POLICY PAPER

Το Policy Paper «Πολιτικές αντιμετώπισης του ψηφιακού παράνομου εμπορίου: Από την κατακερματισμένη πληροφορία στην κοινή επιχειρησιακή εικόνα και στον ενιαίο στρατηγικό σχεδιασμό» συνοψίζει και επεκτείνει τα βασικά σημεία της συζήτησης στογγυλής τραπέζης που διοργανώθηκε από το Delphi Economic Forum υπό τον κανόνα Chatham House στις 15 Ιουλίου 2026.

Στη συζήτηση στρογγυλής τραπέζης συμμετείχαν οι: Μιχάλης Χρυσοχοΐδης – Υπουργός Προστασίας του Πολίτη, Δημοσθένης Αναγνωστόπουλος – Γενικός Γραμματέας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης, Υπουργείο Ψηφιακής Διακυβέρνησης, Γιώργος Πιτσιλής – Διοικητής Ανεξάρτητης Αρχής Δημοσίων Εσόδων (ΑΑΔΕ), Μιχάλης Μπλέτσας – Διοικητής, Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ), Δημήτριος Μπουρίκος – Γενικός Διευθυντής Τελωνείων και Ειδικών Φόρων Κατανάλωσης, Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ), Νικόλας Χατζηδάκης – Διευθύνων Σύμβουλος (CEO), AfterSalesPro, Κατερίνα Φραϊδάκη – Πρόεδρος Δ.Σ., GRECA (Ελληνικός Σύνδεσμος Ηλεκτρονικού Εμπορίου), Αντώνης Γιαννακόδημος – Partner, Δικηγορική Εταιρεία Ζέπος & Γιαννόπουλος, Σταύρος Καφούνης – Πρόεδρος Ελληνικής Συνομοσπονδίας Εμπορίου και Επιχειρηματικότητας (ΕΣΕΕ), Ηρακλής Καναβάρης, Partner Cyber της Deloitte, Δρ. Τριαντάφυλλος Καρατράντος, Επιστημονικός συνεργάτης στο Ελληνικό Ίδρυμα Ευρωπαϊκής & Εξωτερικής Πολιτικής (ΕΛΙΑΜΕΠ), Δημήτρης Καραβάς – Partner, Δικηγορική Εταιρεία Δρυλλεράκης & Συνεργάτες, Κάθριν Ελέανορ Καραβιώτη – Senior Government Affairs Manager, VISA Ελλάδα, Κύπρος & Ισραήλ, Παναγιώτης Κουκουλομμάτης – Πρόεδρος Συντονιστικού Επιχειρησιακού Κέντρου (ΣΕΚ), Γρηγόρης Λαζαράκος – Managing Partner, Δικηγορική Εταιρεία L&L, Γιάννης Μαστροκώστας – Διευθυντής Εταιρικών Υποθέσεων, PMI Ελλάδα / Παπαστράτος, Τηλέμαχος Μωραΐτης – Government Affairs Director, Microsoft Ελλάδα, Κύπρος & Μάλτα, Αναστάσιος Παπαθανασίου – Υποδιευθυντής, Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, Ελληνική Αστυνομία, Γιάννης Ψωμάς – Head of Legal, Compliance & Public Affairs, Pernod Ricard Hellas, Κατερίνα Σιπητάνου – Head of Corporate & Regulatory Affairs Greece, Malta, Cyprus, Israel, BAT Hellas, Κάτια Σταθάκη – Διευθύνουσα Σύμβουλος (CEO), Nexi Greece, Ιωάννης Σταυρακάκης – Υποστράτηγος & Υποδιευθυντής, Διεύθυνση Αντιμετώπισης Οργανωμένου Εγκλήματος, Ελληνική Αστυνομία και Παναγιώτης Τσανάκας, Κοσμήτορας, Καθηγητής Πληροφορικής και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ).

Τη συζήτηση συντόνισε η δημοσιογράφος Μαριλένα Γεραντώνη.

Το policy paper συνέγραψε ο Λουκάς Βελιδάκης και επιμελήθηκε ο Δρ Τριαντάφυλλος Καρατράντος, επιστημονικός συνεργάτης του ΕΛΙΑΜΕΠ.

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ Α
ΤΟ ΠΡΟΒΛΗΜΑ
– σ.10 –

ΜΕΡΟΣ Β
ΤΟ ΔΙΕΘΝΕΣ, ΕΥΡΩΠΑΪΚΟ
ΚΑΙ ΕΛΛΗΝΙΚΟ ΠΛΑΙΣΙΟ
– σ.28 –

ΜΕΡΟΣ Γ
ΣΥΓΚΡΙΤΙΚΕΣ ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ
ΚΑΙ ΔΙΔΑΓΜΑΤΑ
– σ.34 –

ΜΕΡΟΣ Δ
ΠΡΟΤΑΣΕΙΣ ΠΟΛΙΤΙΚΗΣ
ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ
– σ.38 –

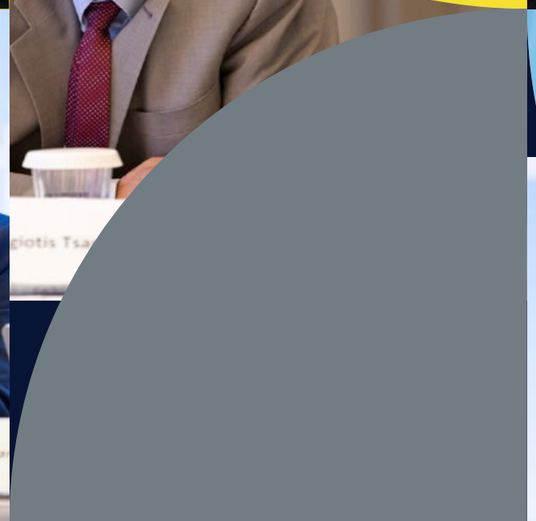
ΣΥΜΠΕΡΑΣΜΑΤΑ
– σ.42 –

ΒΑΣΙΚΕΣ ΠΗΓΕΣ
– σ.43 –



















CENTER FOR CYBER RESILIENCE

ΤΟ ΨΗΦΙΑΚΟ ΠΑΡΑΝΟΜΟ ΕΜΠΟΡΙΟ ΜΕ ΜΙΑ ΜΑΤΙΑ

Ο όρος περιγράφει ένα λειτουργικό οικοσύστημα και όχι ένα ενιαίο ποινικό αδίκημα.

Αφορά τον μετασχηματισμό παραδοσιακών παράνομων αγορών μέσα από τη διείσδυση στις υποδομές του νόμιμου ηλεκτρονικού εμπορίου.





ΑΠΟ ΠΕΡΙΠΟΥ
200.025
ΤΟ 2021 ΣΕ ΠΕΡΙΣΣΟΤΕΡΕΣ ΑΠΟ
23.000.000
ΑΥΞΗΘΗΚΑΝ ΤΟ 2025 ΟΙ ΚΙΝΗΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΑΠΟ ΤΡΙΤΕΣ ΧΩΡΕΣ ΣΤΗΝ ΕΛΛΑΔΑ

2,3%
ΤΟΥ ΠΑΓΚΟΣΜΙΟΥ ΕΜΠΟΡΙΟΥ ΚΑΙ
4,7%
ΤΩΝ ΕΙΣΑΓΩΓΩΝ ΤΗΣ ΕΕ ΑΦΟΡΟΥΝ ΠΑΡΑΠΟΙΗΜΕΝΑ ΚΑΙ ΠΕΙΡΑΤΙΚΑ ΠΡΟΪΟΝΤΑ
(ΓΙΑ ΤΟ ΕΤΟΣ 2021)

ΣΤΟ ΠΡΟΓΡΑΜΜΑ ΤΟΥ 2026 ΟΙ ΕΛΕΓΧΟΙ ΔΙΩΞΗΣ ΣΕ ΔΕΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΑΥΞΗΘΗΚΑΝ ΣΤΙΣ
5.000
ΠΕΡΙΠΤΩΣΕΙΣ, ΕΝΑΝΤΙ ΠΕΡΙΠΟΥ
2.500 ΕΩΣ 3.500
ΤΑ ΠΡΟΗΓΟΥΜΕΝΑ ΧΡΟΝΙΑ

ΤΟ ΒΑΣΙΚΟ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΕΛΛΕΙΜΜΑ ΕΙΝΑΙ ΟΤΙ ΚΑΝΕΝΑΣ ΦΟΡΕΑΣ ΔΕΝ ΒΛΕΠΕΙ ΜΟΝΟΣ ΤΟΥ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΙΚΟΝΑ

ΤΟ 2024 Η ΕΛΛΑΔΑ ΠΕΡΙΛΑΜΒΑΝΟΤΑΝ ΣΤΙΣ ΔΕΚΑ ΧΩΡΕΣ ΤΗΣ ΕΕ ΜΕ ΤΗ ΜΕΓΑΛΥΤΕΡΗ ΤΕΛΩΝΕΙΑΚΗ ΔΕΣΜΕΥΣΗ ΠΑΡΑΠΟΙΗΜΕΝΩΝ ΠΡΟΪΟΝΤΩΝ

ΣΕ
467
ΔΙΣ. ΔΟΛΑΡΙΑ ΑΝΗΛΘΕ ΤΟ ΠΑΓΚΟΣΜΙΟ ΕΜΠΟΡΙΟ ΠΑΡΑΠΟΙΗΜΕΝΩΝ ΚΑΙ ΠΕΙΡΑΤΙΚΩΝ ΠΡΟΪΟΝΤΩΝ
(ΓΙΑ ΤΟ ΕΤΟΣ 2021)

Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΗΣ ΣΥΝΟΛΙΚΗΣ ΑΠΑΝΤΗΣΗΣ ΕΞΑΡΤΑΤΑΙ ΑΠΟ ΤΗ ΣΥΝΔΕΣΗ ΟΛΩΝ ΤΩΝ ΚΡΙΚΩΝ ΤΗΣ ΑΛΥΣΙΔΑΣ

CENTER FOR CYBER RESILIENCE

ΜΕΡΟΣ Α

ΤΟ ΠΡΟΒΛΗΜΑ

1.
Η ΚΛΙΜΑΚΑ ΚΑΙ Η ΕΞΕΛΙΞΗ ΤΟΥ ΨΗΦΙΑΚΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ

Η ΕΚΘΕΣΗ OECD–EUIPO ΤΟΥ 2025 ΕΚΤΙΜΑ ΟΤΙ ΤΟ ΠΑΓΚΟΣΜΙΟ ΕΜΠΟΡΙΟ ΠΑΡΑΠΟΙΗΜΕΝΩΝ ΚΑΙ ΠΕΙΡΑΤΙΚΩΝ ΠΡΟΪΟΝΤΩΝ ΑΝΗΛΘΕ ΤΟ 2021 ΣΕ ΠΕΡΙΠΟΥ 467 ΔΙΣ. ΔΟΛΑΡΙΑ. Η ΕΙΚΟΝΑ ΔΕΝ ΚΑΛΥΠΤΕΙ ΤΟ ΣΥΝΟΛΟ ΤΩΝ ΛΑΘΡΑΙΩΝ Ή ΜΗ ΣΥΜΜΟΡΦΟΥΜΕΝΩΝ ΠΡΟΪΟΝΤΩΝ, ΑΠΟΤΥΠΩΝΕΙ ΟΜΩΣ ΤΗΝ ΟΙΚΟΝΟΜΙΚΗ ΚΛΙΜΑΚΑ ΚΑΙ ΤΗΝ ΠΡΟΣΑΡΜΟΣΤΙΚΟΤΗΤΑ ΤΩΝ ΔΙΚΤΥΩΝ.

1.1 Παγκόσμια κλίμακα και μετασχηματισμός των ροών

Η ανάπτυξη του διασυνοριακού ηλεκτρονικού εμπορίου αύξησε την πρόσβαση των καταναλωτών και μείωσε το κόστος εισόδου στις διεθνείς αγορές. Τα ίδια χαρακτηριστικά, όμως, αξιοποιούνται από παράνομους πωλητές: χαμηλό κόστος δημιουργίας λογαριασμού, παγκόσμιο αγοραστικό κοινό, πολλαπλές ψηφιακές ταυτότητες, ευέλικτες πληρωμές και δυνατότητα αποστολής μικρών δεμάτων απευθείας στον καταναλωτή.

Η έκθεση OECD–EUIPO του 2025 εκτιμά ότι το παγκόσμιο εμπόριο παραποιημένων και πειρατικών προϊόντων ανήλθε το 2021 σε περίπου 467 δισ. δολάρια. Η εικόνα δεν καλύπτει το σύνολο των λαθραίων ή μη συμμορφούμενων προϊόντων, αποτυπώνει όμως την οικονομική κλίμακα και την προσαρμοστικότητα των δικτύων. Η μεταφορά της παραγωγής πλησιέστερα στις αγορές προορισμού, η εισαγωγή χωριστών εξαρτημάτων και συσκευασιών και η τελική συναρμολόγηση σε τοπικό επίπεδο δυσχεραίνουν περαιτέρω την επιβολή.

1.2 Η Ευρωπαϊκή Ένωση ως ενιαία αγορά και ενιαίο πεδίο κινδύνου

Η ΕΕ αποτελεί ιδιαίτερα ελκυστική αγορά λόγω αγοραστικής δύναμης, ενιαίας αγοράς και ελεύθερης κυκλοφορίας μετά την πρώτη είσοδο. Οι διαφορές στην ένταση των εθνικών ελέγχων ενδέχεται να επηρεάζουν την επιλογή των διαδρομών εισόδου, καθώς τα δίκτυα μπορούν να προτιμούν σημεία που θεωρούν λιγότερο αυστηρά και στη συνέχεια να διακινούν τα προϊόντα στην εσωτερική αγορά.

Η πανευρωπαϊκή επιχείρηση τελωνειακού ελέγχου που δημοσιοποιήθηκε τον Ιανουάριο του 2026 εξέτασε 20.000 παιχνίδια και μικρές ηλεκτρονικές συσκευές: περισσότερα από τα μισά δεν συμμορφώνονταν με τα ευρωπαϊκά πρότυπα και, από τα προϊόντα που υποβλήθηκαν σε εργαστηριακό έλεγχο, το 84% κρίθηκαν επικίνδυνα. Το εύρημα καταδεικνύει ότι η πρόκληση δεν είναι μόνο δημοσιονομική ή σχετική με την παραποίηση, αλλά αφορά άμεσα την υγεία και την ασφάλεια των καταναλωτών.

1.3 Τρεις δομικές μεταβολές των εμπορικών ροών

- Από τα μεγάλα φορτία στις μαζικές μικρές αποστολές, με χαμηλή αξία ανά δέμα αλλά μεγάλη σωρευτική επίπτωση.
- Από τον εμφανή εισαγωγέα σε αλυσίδες πλατφορμών, πωλητών, παρόχων πληρωμών, αποστολέων και ενδιάμεσων.
- Από τον μεμονωμένο φυσικό έλεγχο στην προληπτική ανάλυση δεδομένων, δικτύων και συμπεριφοράς.

1.4 Η ελληνική περίπτωση

Η ελληνική περίπτωση χαρακτηρίζεται από απότομη αύξηση των κινήσεων ηλεκτρονικού εμπορίου, σημαντική πίεση στις τελωνειακές πύλες και κατακερματισμό της σχετικής πληροφορίας. Για βασική πύλη εισόδου παρουσιάστηκε αύξηση των κινήσεων ηλεκτρονικού εμπορίου από τρίτες χώρες, από περίπου 200.025 το 2021 σε περισσότερες από 23 εκατομμύρια το 2025. Παρά τα προβλήματα με τον συνολικό προσδιορισμό και τη μονάδα μέτρησης των διαφορετικών κινήσεων, αυτή η διαφοροποίηση αποτυπώνει όμως τη μεταβολή κλίμακας που αντιμετωπίζουν οι υπηρεσίες.

ΣΤΗΝ ΚΟΙΝΗ ΕΚΘΕΣΗ ΕΥΡΩΠΑΪΚΗΣ ΕΠΙΤΡΟΠΗΣ–EUIPO ΓΙΑ ΤΟ 2024, Η ΕΛΛΑΔΑ ΣΥΓΚΑΤΑΛΕΓΕΤΑΙ ΣΤΑ ΔΕΚΑ ΚΡΑΤΗ ΜΕΛΗ ΜΕ ΤΙΣ ΜΕΓΑΛΥΤΕΡΕΣ ΤΕΛΩΝΕΙΑΚΕΣ ΔΕΣΜΕΥΣΕΙΣ ΠΑΡΑΠΟΙΗΜΕΝΩΝ ΠΡΟΪΟΝΤΩΝ, ΤΟΣΟ ΣΕ ΠΛΗΘΟΣ ΟΣΟ ΚΑΙ ΣΕ ΕΚΤΙΜΩΜΕΝΗ ΑΞΙΑ. ΤΟ ΕΥΡΗΜΑ ΑΦΟΡΑ ΠΑΡΑΒΙΑΣΕΙΣ ΔΙΚΑΙΩΜΑΤΩΝ ΔΙΑΝΟΗΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΣΤΑ ΕΞΩΤΕΡΙΚΑ ΣΥΝΟΡΑ ΚΑΙ ΔΕΝ ΤΑΥΤΙΖΕΤΑΙ ΜΕ ΤΟ ΣΥΝΟΛΟ ΤΟΥ ΨΗΦΙΑΚΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ, ΛΕΙΤΟΥΡΓΕΙ ΟΜΩΣ ΩΣ ΣΥΓΚΡΙΣΙΜΟΣ ΔΕΙΚΤΗΣ ΤΕΛΩΝΕΙΑΚΗΣ ΠΙΕΣΗΣ.

Η δημόσια στατιστική εικόνα δεν επιτρέπει ακόμη τον υπολογισμό ενός ενιαίου μεγέθους για το ψηφιακό παράνομο εμπόριο στην Ελλάδα. Διαθέσιμοι δείκτες, ωστόσο, επιβεβαιώνουν την έκθεση της χώρας. Στην κοινή έκθεση Ευρωπαϊκής Επιτροπής–EUIPO για το 2024, η Ελλάδα συγκαταλέγεται στα δέκα κράτη-μέλη με τις μεγαλύτερες τελωνειακές δεσμεύσεις παραποιημένων προϊόντων, τόσο σε πλήθος όσο και σε εκτιμώμενη αξία. Το εύρημα αφορά παραβιάσεις δικαιωμάτων διανοητικής ιδιοκτησίας στα εξωτερικά σύνορα και δεν ταυτίζεται με το σύνολο του ψηφιακού παράνομου εμπορίου, λειτουργεί όμως ως συγκρίσιμος δείκτης τελωνειακής πίεσης.

Η επιχειρησιακή κλίμακα αποτυπώνεται και σε πρόσφατες υποθέσεις. Τον Ιούνιο του 2026 η Ελληνική Αστυνομία ανακοίνωσε την εξάρθρωση δικτύου παράνομης παραγωγής και διαδικτυακής προώθησης φαρμακευτικών σκευασμάτων και ουσιών ντόπινγκ. Από την έρευνα προέκυψαν περισσότερες από 15.000 αποστολές στην Ελλάδα και σε 90 χώρες, κατασχέθηκαν 40.856 τεμάχια και η εκτιμώμενη παράνομη πρόσοδος υπερέβαινε το 1 εκατ. ευρώ. Η υπόθεση δεν αποτελεί μέτρο της συνολικής αγοράς, δείχνει όμως πώς η ψηφιακή προβολή, η εγχώρια παραγωγή, η ταχυδρομική διανομή και η διασυνοριακή πελατεία μπορούν να συγκροτούν ενιαίο δίκτυο.

Η χώρα διαθέτει τελωνειακές, φορολογικές, αστυνομικές, οικονομικές και ψηφιακές δυνατότητες, χωρίς κανένας φορέας να έχει από μόνος του την πλήρη εικόνα. Το πρόβλημα επομένως δεν είναι απλώς η έλλειψη αρμοδιοτήτων, αλλά η αδυναμία σταθερής σύνδεσης των πληροφοριών για το προϊόν, τον πωλητή, την πληρωμή, τον αποστολέα, τον παραλήπτη καθώς και των δεδομένων από τις σχετικές υποθέσεις.

2.
ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΤΟ ΨΗΦΙΑΚΟ ΠΑΡΑΝΟΜΟ ΕΜΠΟΡΙΟ ΚΑΙ ΟΙ ΠΡΟΚΛΗΣΕΙΣ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ

2.1 Η επιχειρησιακή αλυσίδα

Η παρούσα ενότητα εξετάζει τη λειτουργική ακολουθία μιας υπόθεσης. Η αλυσίδα περιλαμβάνει την ψηφιακή προβολή, την ταυτότητα του πωλητή, την παραγγελία, την πληρωμή, την αποθήκευση, τη μεταφορά και την παράδοση. Σε κάθε στάδιο παράγονται διαφορετικά δεδομένα και εμπλέκονται διαφορετικοί φορείς.

Η αξία της χαρτογράφησης της δράσης των παρανόμων βρίσκεται στη δυνατότητα εντοπισμού του κατάλληλου σημείου παρέμβασης. Η αφαίρεση μιας αγγελίας μπορεί να περιορίσει προσωρινά την ορατότητα, αλλά δεν διακόπτει το δίκτυο όταν ο πωλητής, ο λογαριασμός πληρωμών, το απόθεμα και η υποδομή διανομής παραμένουν ενεργά.

ΤΟ ΠΑΡΑΝΟΜΟ ΕΜΠΟΡΙΟ ΜΠΟΡΕΙ ΝΑ ΟΡΓΑΝΩΝΕΤΑΙ ΚΑΙ ΝΑ ΠΡΑΓΜΑΤΟΠΟΙΕΙΤΑΙ ΨΗΦΙΑΚΑ, ΟΜΩΣ Η ΔΙΑΚΙΝΗΣΗ ΤΩΝ ΠΡΟΪΟΝΤΩΝ ΠΑΡΑΜΕΝΕΙ ΦΥΣΙΚΗ. ΤΟ ΠΡΟΪΟΝ ΠΡΕΠΕΙ ΝΑ ΑΠΟΘΗΚΕΥΤΕΙ, ΝΑ ΜΕΤΑΦΕΡΘΕΙ ΚΑΙ ΤΕΛΙΚΑ ΝΑ ΠΑΡΑΔΟΘΕΙ ΣΤΟΝ ΑΓΟΡΑΣΤΗ. ΟΙ ΕΤΑΙΡΕΙΕΣ COURIER ΚΑΙ LOGISTICS ΑΠΟΤΕΛΟΥΝ, ΕΠΟΜΕΝΩΣ, ΚΡΙΣΙΜΟΥΣ ΚΡΙΚΟΥΣ ΤΗΣ ΑΛΥΣΙΔΑΣ ΚΑΙ Η ΕΝΤΑΞΗ ΤΟΥΣ ΣΤΟΥΣ ΜΗΧΑΝΙΣΜΟΥΣ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΑΝΤΑΛΛΑΓΗΣ ΠΛΗΡΟΦΟΡΙΩΝ ΕΙΝΑΙ ΑΠΑΡΑΙΤΗΤΗ.

Το παράνομο προϊόν μπορεί να προβάλλεται σε κανονικούς ιστοτόπους, marketplaces, social media, κλειστές ομάδες ή υπηρεσίες μηνυμάτων. Το dark web αποτελεί μία μόνο εκδοχή και όχι κατ' ανάγκην το βασικό κανάλι. Νόμιμες και τεχνικά ασφαλείς πλατφόρμες μπορούν να χρησιμοποιούνται για παράνομους σκοπούς, γεγονός που διακρίνει την ασφάλεια ενός πληροφοριακού συστήματος από τη νομιμότητα της δραστηριότητας που φιλοξενεί. Η ίδια προσφορά μπορεί να μετακινείται γρήγορα ανάμεσα σε λογαριασμούς και πλατφόρμες. Επομένως, το ζητούμενο δεν είναι μόνο η αφαίρεση του μεμονωμένου listing, αλλά η σύνδεσή του με τον πραγματικό πωλητή, προηγούμενες αναρτήσεις, σχετικούς λογαριασμούς και επαναλαμβανόμενα στοιχεία επικοινωνίας ή πληρωμής.

Η αξιοπιστία της αλυσίδας εξαρτάται από το κατά πόσο μπορεί να προσδιοριστεί ποιος πραγματικά προσφέρει το προϊόν και ποιος έχει δυνατότητα παρέμβασης. Η απλή καταχώριση ενός ονόματος ή email δεν επαρκεί όταν ένας πωλητής μπορεί να επανεμφανίζεται με νέα στοιχεία. Χρειάζονται αναλογικές διαδικασίες Know Your Business Customer, έλεγχος συνδεδεμένων λογαριασμών και σαφής κατανομή ευθύνης ανάμεσα σε πωλητή, πλατφόρμα και άλλους ενδιαμέσους. Η παραγγελία και η πληρωμή συνδέουν την ψηφιακή προσφορά με συγκεκριμένο αγοραστή, έμπορο και μέσο πληρωμής. Τα δεδομένα αυτά μπορούν να επιβεβαιώσουν ότι πολλές φαινομενικά ασύνδετες πωλήσεις αποτελούν μέρος του ίδιου δικτύου.

Το παράνομο εμπόριο μπορεί να οργανώνεται και να πραγματοποιείται ψηφιακά, όμως η διακίνηση των προϊόντων παραμένει φυσική. Το προϊόν πρέπει να αποθηκευτεί, να μεταφερθεί και τελικά να παραδοθεί στον αγοραστή. Οι εταιρείες courier και logistics αποτελούν, επομένως, κρίσιμους κρίκους της αλυσίδας και η ένταξή τους στους μηχανισμούς συνεργασίας και ανταλλαγής πληροφοριών είναι απαραίτητη.

Επίσης, είναι σημαντική η διαφορετική χαρτογράφηση της αλυσίδας ανά κατηγορία προϊόντος. Καπνικά, αλκοολούχα, φάρμακα, αναβολικά και άλλες κατηγορίες υψηλού κινδύνου δεν ακολουθούν κατ' ανάγκην τις ίδιες διαδρομές, ούτε εμφανίζουν τις ίδιες ευπάθειες. Η αποτύπωση των επιμέρους σταδίων –από την ψηφιακή προώθηση και την πληρωμή έως τη μεταφορά και την παράδοση– μπορεί να επιτρέψει πιο στοχευμένες παρεμβάσεις και αποτελεσματικότερους ελέγχους.

Οι courier και οι επιχειρήσεις logistics δεν πρέπει να μετατραπούν σε γενικούς ελεγκτές του περιεχομένου των δεμάτων. Η συνεισφορά τους βρίσκεται κυρίως στην αξιόπιστη ταυτοποίηση του αποστολέα, στην ποιότητα των δεδομένων αποστολής και στην αναγνώριση επαναλαμβανόμενων μοτίβων που υποδεικνύουν συστηματική εμπορική δραστηριότητα.

2.2 Δίκτυα, ψηφιακά αποτυπώματα, κρυπτοστοιχεία, διασυνοριακότητα

Η ψηφιοποίηση της φορολογικής πληροφορίας επιτρέπει την εξέταση όχι μόνο μιας μεμονωμένης συναλλαγής, αλλά και των σχέσεων ανάμεσα σε πολλές συναλλαγές και επιχειρήσεις. Στόχος της ανάλυσης δεν είναι μόνο η διακοπή μιας επιμέρους παράνομης πράξης, αλλά ο εντοπισμός και η εξάρθρωση του ευρύτερου δικτύου. Η αξία των δεδομένων βρίσκεται στη δυνατότητα αναγνώρισης μοτίβων και συνδεδεμένων οντοτήτων.

ΟΙ ΨΗΦΙΑΚΕΣ ΠΛΗΡΩΜΕΣ ΠΡΟΣΦΕΡΟΥΝ ΕΝΑ ΑΠΟ ΤΑ ΠΛΟΥΣΙΟΤΕΡΑ ΣΥΝΟΛΑ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΤΗΝ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ, ΚΑΘΩΣ ΚΑΘΕ ΣΥΝΑΛΛΑΓΗ ΔΗΜΙΟΥΡΓΕΙ ΑΞΙΟΠΟΙΗΣΙΜΟ ΨΗΦΙΑΚΟ ΑΠΟΤΥΠΩΜΑ. Η ΧΩΡΑ ΕΚΔΟΣΗΣ ΤΗΣ ΚΑΡΤΑΣ, Η ΓΕΩΓΡΑΦΙΚΗ ΠΡΟΕΛΕΥΣΗ, Η ΔΙΕΥΘΥΝΣΗ IP, Η ΤΑΧΥΤΗΤΑ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ ΚΑΙ Η ΑΠΟΚΛΙΣΗ ΑΠΟ ΤΗ ΣΥΝΗΘΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΕΝΟΣ ΕΜΠΟΡΟΥ ΜΠΟΡΟΥΝ ΝΑ ΑΞΙΟΠΟΙΟΥΝΤΑΙ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ.

Οι ψηφιακές πληρωμές προσφέρουν ένα από τα πλουσιότερα σύνολα δεδομένων για την ανάλυση κινδύνου, καθώς κάθε συναλλαγή δημιουργεί αξιοποιήσιμο ψηφιακό αποτύπωμα. Η χώρα έκδοσης της κάρτας, η γεωγραφική προέλευση, η διεύθυνση IP, η ταχύτητα των συναλλαγών και η απόκλιση από τη συνήθη δραστηριότητα ενός εμπόρου μπορούν να αξιοποιούνται σε πραγματικό χρόνο.

Ενδεικτικά, μεγάλος διεθνής πάροχος επεξεργάζεται περισσότερες από 300 δισ. συναλλαγές ετησίως σε περισσότερες από 200 χώρες και διαθέτει ορατότητα σε συναλλαγές περισσότερων από 150 εκατ. εμπόρων. Ένας τέτοιος όγκος δεδομένων επιτρέπει την αναγνώριση μοτίβων απάτης και αποκλίσεων σε πραγματικό χρόνο που δεν θα ήταν ορατές σε έναν μεμονωμένο φορέα.

Τα συστήματα παρακολούθησης απάτης και συναλλαγών μπορούν να οδηγούν σε άμεση αναστολή συναλλαγών, προσωρινό πάγωμα λογαριασμού αποδοχής πληρωμών, καθυστέρηση εκκαθάρισης και πρόσθετο έλεγχο ταυτοποίησης. Σε χαρακτηριστική περίπτωση εντοπίστηκαν και διακόπηκαν συναλλαγές ύψους 75.000 ευρώ μέσα σε λίγες ώρες.

Η επιχειρησιακή ανθεκτικότητα των συστημάτων πληρωμών εντάσσεται πλέον σε συγκεκριμένο ευρωπαϊκό κανονιστικό πλαίσιο. Η Πράξη για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (Digital Operational Resilience Act – DORA) ενισχύει τις απαιτήσεις διαχείρισης τεχνολογικού και κυβερνοκινδύνου για φορείς του χρηματοπιστωτικού τομέα. Με τον τρόπο αυτό ενισχύεται και η ανθεκτικότητα κρίσιμων συστημάτων παρακολούθησης και εντοπισμού απάτης υπό συνθήκες σοβαρής ψηφιακής επίθεσης.

2.3 Νέα δεδομένα, νέες στρατηγικές

Η πραγματική πρόκληση είναι η ταχύτητα με την οποία η πληροφορία μπορεί να φτάσει από έναν ιδιωτικό πάροχο προς την αρμόδια αρχή. Η περιοδική διαβίβαση στοιχείων δεν επαρκεί όταν η απάτη μπορεί να εντοπίζεται σε δευτερόλεπτα. Χρειάζονται ασφαλείς δίαυλοι πληροφορίας σε πραγματικό ή σχεδόν πραγματικό χρόνο μεταξύ παρόχων πληρωμών, τραπεζών, εποπτικών και διωκτικών αρχών.

Η ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΤΟΥ ΨΗΦΙΑΚΟΥ ΕΜΠΟΡΙΟΥ ΣΥΓΚΕΝΤΡΩΝΕΤΑΙ ΣΕ ΤΡΕΙΣ ΒΑΣΙΚΕΣ ΓΚΡΙΖΕΣ ΖΩΝΕΣ: ΤΗΝ ΙΧΝΗΛΑΣΙΜΟΤΗΤΑ ΤΩΝ ΠΡΟΪΟΝΤΩΝ, ΤΗΝ ΙΧΝΗΛΑΣΙΜΟΤΗΤΑ ΤΩΝ ΠΡΟΣΩΠΩΝ ΚΑΙ ΤΗΝ ΙΧΝΗΛΑΣΙΜΟΤΗΤΑ ΤΗΣ ΕΥΘΥΝΗΣ. Η ΠΟΛΙΤΙΚΗ ΛΟΙΠΟΝ ΠΡΕΠΕΙ ΝΑ ΜΠΟΡΕΙ ΝΑ ΑΠΑΝΤΑ ΤΙ ΔΙΑΚΙΝΗΘΗΚΕ, ΠΟΙΟΣ ΠΡΑΓΜΑΤΙΚΑ ΣΥΜΜΕΤΕΙΧΕ ΚΑΙ ΠΟΙΟΣ ΕΙΧΕ ΕΥΘΥΝΗ ΉΔΥΝΑΤΟΤΗΤΑ ΠΑΡΕΜΒΑΣΗΣ ΣΕ ΚΑΘΕ ΣΤΑΔΙΟ ΤΗΣ ΣΥΝΑΛΛΑΓΗΣ.

Η κλασική αρχή follow the money επεκτείνεται πλέον και στα κρυπτοστοιχεία, καθιστώντας αναγκαία την ανάπτυξη αντίστοιχων δυνατοτήτων παρακολούθησης και ανάλυσης. Η χρήση mixing services, unhosted wallets και διαφορετικών ψηφιακών υποδομών καθιστά την ιχνηλάτηση δυσκολότερη και απαιτεί τεχνική εξειδίκευση, διεθνή συνεργασία και πρόσβαση σε δεδομένα που συχνά βρίσκονται εκτός εθνικής δικαιοδοσίας.

Η διασυνοριακή ανταλλαγή φορολογικών πληροφοριών διευρύνεται περαιτέρω μέσω της DAC8, η οποία επεκτείνει το ευρωπαϊκό πλαίσιο διοικητικής συνεργασίας στα κρυπτοστοιχεία. Η εφαρμογή της μπορεί να ενισχύσει την ανταλλαγή πληροφοριών μεταξύ των κρατών-μελών, σε ένα πεδίο όπου οι συναλλαγές κινούνται διασυνοριακά ταχύτερα από τις παραδοσιακές διοικητικές διαδικασίες. Το παράνομο εμπόριο είναι από τη φύση του διασυνοριακό. Πάροχοι πληρωμών ή άλλες ψηφιακές υπηρεσίες μπορούν να εδρεύουν σε διαφορετικό κράτος-μέλος και να δραστηριοποιούνται μέσω passporting. Οι πάροχοι που δραστηριοποιούνται διασυνοριακά δεν πρέπει να παραμένουν αδιαφανείς για τις αρμόδιες διωκτικές αρχές. Η πρόσβαση στα αναγκαία δεδομένα πρέπει να γίνει ταχύτερη, περισσότερο προβλέψιμη και συμβατή με τις θεσμικές εγγυήσεις.

Η αύξηση από περίπου 200.025 κινήσεις e-commerce το 2021 σε πάνω από 23 εκατομμύρια το 2025 καταδεικνύει ότι το σύστημα έχει περάσει σε διαφορετική κλίμακα. Η παραδοσιακή λογική φυσικού ελέγχου κάθε ύποπτου φορτίου δεν μπορεί να εφαρμοστεί σε δεκάδες εκατομμύρια αποστολές. Η τελωνειακή στρατηγική πρέπει να βασίζεται σε ανάλυση κινδύνου, πληροφορίες από άλλες τελωνειακές διοικήσεις, ευρωπαϊκούς μηχανισμούς και ειδικά επιχειρησιακά σχέδια.

Η μετάβαση αποτυπώνεται και επιχειρησιακά: στο πρόγραμμα του 2026 οι έλεγχοι δίωξης σε δέματα ηλεκτρονικού εμπορίου αυξήθηκαν στις 5.000 περιπτώσεις, έναντι περίπου 2.500 έως 3.500 τα προηγούμενα χρόνια. Η αύξηση δεν συνιστά επιστροφή στη λογική του μαζικού ελέγχου, αλλά ενίσχυση της στοχευμένης επιβολής βάσει κινδύνου.

Η λογική του Authorized Economic Operator προσφέρει ένα μοντέλο στο οποίο ο φορέας αξιολογείται συνολικά και όχι σε κάθε συναλλαγή ξεχωριστά. Το μοντέλο αυτό δημιουργεί εμπιστοσύνη ανάμεσα σε τελωνειακές αρχές και νόμιμες επιχειρήσεις και επιτρέπει την καλύτερη κατανομή των ελεγκτικών πόρων.

Οι εταιρείες courier αποτελούν κρίσιμο κρίκο της αλυσίδας, χωρίς αυτό να σημαίνει ότι πρέπει να αναλάβουν τον ρόλο ελεγκτή του περιεχομένου των δεμάτων. Αντίθετα, η αξία τους βρίσκεται στην ισχυρότερη ταυτοποίηση του αποστολέα, στην ανάλυση μοτίβων και στον εντοπισμό περιπτώσεων όπου ένας ιδιώτης εμφανίζει συστηματική εμπορική συμπεριφορά ή μια εταιρεία δημιουργείται, εξαφανίζεται και επανεμφανίζεται με διαφορετικά στοιχεία.

Η πολυπλοκότητα του ψηφιακού εμπορίου συγκεντρώνεται σε τρεις βασικές γκρίζες ζώνες: την ιχνηλασιμότητα των προϊόντων, την ιχνηλασιμότητα των προσώπων και την ιχνηλασιμότητα της ευθύνης. Η πολιτική λοιπόν πρέπει να μπορεί να απαντά τι διακινήθηκε, ποιος πραγματικά συμμετείχε και ποιος είχε ευθύνη ή δυνατότητα παρέμβασης σε κάθε στάδιο της συναλλαγής.

3.
Η ΘΕΣΗ ΤΟΥ ΨΗΦΙΑΚΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ ΣΤΟ ΕΥΡΥΤΕΡΟ ΕΓΚΛΗΜΑΤΙΚΟ ΟΙΚΟΣΥΣΤΗΜΑ

ΤΟ ΨΗΦΙΑΚΟ ΠΑΡΑΝΟΜΟ ΕΜΠΟΡΙΟ ΛΕΙΤΟΥΡΓΕΙ ΩΣ ΚΟΜΒΟΣ ΣΥΓΚΛΙΣΗΣ ΔΙΑΦΟΡΕΤΙΚΩΝ ΜΟΡΦΩΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ. ΟΙ ΙΔΙΕΣ ΥΠΟΔΟΜΕΣ – ΕΤΑΙΡΙΚΑ ΣΧΗΜΑΤΑ, ΛΟΓΑΡΙΑΣΜΟΙ ΠΛΗΡΩΜΩΝ, MONEY MULES, ΑΠΟΘΗΚΕΣ, ΜΕΤΑΦΟΡΙΚΕΣ ΕΤΑΙΡΕΙΕΣ, ΠΛΑΣΤΑ ΕΓΓΡΑΦΑ, DOMAINS ΚΑΙ ΨΗΦΙΑΚΗ ΔΙΑΦΗΜΙΣΗ– ΜΠΟΡΟΥΝ ΝΑ ΥΠΟΣΤΗΡΙΖΟΥΝ ΠΕΡΙΣΣΟΤΕΡΕΣ ΑΠΟ ΜΙΑ ΠΑΡΑΝΟΜΕΣ ΑΓΟΡΕΣ. Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΝΟΣ ΠΡΟΪΟΝΤΟΣ ΧΩΡΙΣ ΧΑΡΤΟΓΡΑΦΗΣΗ ΤΟΥ ΔΙΚΤΥΟΥ ΚΙΝΔΥΝΕΥΕΙ ΕΠΟΜΕΝΩΣ ΝΑ ΔΙΑΚΟΨΕΙ ΜΟΝΟ ΕΝΑ ΚΑΝΑΛΙ ΚΑΙ ΟΧΙ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΗ ΥΠΟΔΟΜΗ.

Το ψηφιακό παράνομο εμπόριο λειτουργεί ως κόμβος σύγκλισης διαφορετικών μορφών εγκληματικότητας. Οι ίδιες υποδομές –εταιρικά σχήματα, λογαριασμοί πληρωμών, money mules, αποθήκες, μεταφορικές εταιρείες, πλαστά έγγραφα, domains και ψηφιακή διαφήμιση– μπορούν να υποστηρίζουν περισσότερες από μία παράνομες αγορές. Η αντιμετώπιση ενός προϊόντος χωρίς χαρτογράφηση του δικτύου κινδυνεύει επομένως να διακόψει μόνο ένα κανάλι και όχι την εγκληματική υποδομή.

Τα δίκτυα οργανωμένου εγκλήματος δεν εξειδικεύονται κατ' ανάγκην σε μία μόνο κατηγορία προϊόντος. Μετακινούν κεφάλαια, τεχνογνωσία και δίκτυα logistics ανάμεσα σε παραποιημένα προϊόντα, λαθραία καπνικά και αλκοόλ, φάρμακα, ουσίες ντόπινγκ, ναρκωτικά και άλλες παράνομες αγορές. Η πολυεγκληματικότητα επιτρέπει διαφοροποίηση του κινδύνου και αξιοποίηση των ίδιων διαδρομών για διαφορετικά αγαθά.

Η απόκρυψη του πραγματικού δικαιούχου, η κατάτμηση συναλλαγών, οι εικονικές επιχειρήσεις, οι λογαριασμοί τρίτων και η γρήγορη μεταφορά κεφαλαίων μετατρέπουν το πεδίο σε αντικείμενο οικονομικής έρευνας. Η αρχή follow the money πρέπει να εφαρμόζεται από την έναρξη της υπόθεσης και να επεκτείνεται σε κρυπτοστοιχεία, παρόχους υπηρεσιών πληρωμών και διασυνοριακά δεδομένα.

Phishing, social engineering, κλοπή ταυτότητας, παραβίαση λογαριασμών και κακόβουλη διαφήμιση μπορούν να χρησιμοποιούνται τόσο για την εξαπάτηση καταναλωτών όσο και για τη λειτουργία παράνομων καταστημάτων. Το crime as a service μειώνει το τεχνικό κατώφλι: εγκληματικές ομάδες μπορούν να αγοράζουν έτοιμες υποδομές, υπηρεσίες απόκρυψης, domains, πλαστά reviews και εργαλεία δημιουργίας παραπλανητικού περιεχομένου.

Η διαφθορά μπορεί να διευκολύνει την είσοδο, αποθήκευση ή διακίνηση προϊόντων, ενώ η ανάμειξη νόμιμων και παράνομων ροών δυσχεραίνει τον εντοπισμό. Η νόμιμη επιχείρηση μπορεί να είναι θύμα, ακούσιος ενδιάμεσος ή, σε ορισμένες περιπτώσεις, ενεργός συνεργός. Αυτό επιβάλλει διαφοροποιημένη αξιολόγηση οντοτήτων και όχι συλλογική αντιμετώπιση ολόκληρων κλάδων ως υπόπτων.

Οι ανήλικοι μπορεί να εμφανίζονται ως καταναλωτές προϊόντων υψηλού κινδύνου, αλλά και ως money mules, παραλήπτες δεμάτων, μεταπωλητές ή ψηφιακοί προωθητές. Η στρατολόγηση μέσω κοινωνικών δικτύων και η

κανονικοποίηση μικρών πράξεων παρανομίας απαιτούν σύνδεση πολιτικών επιβολής, πρόληψης και ψηφιακού γραμματισμού.

Παράνομες εμπορικές δραστηριότητες μπορούν, σε συγκεκριμένες υποθέσεις, να χρηματοδοτούν τρομοκρατικούς φορείς ή βίαια δίκτυα. Δεν είναι όμως ορθό να χαρακτηρίζεται κάθε παράνομη αγορά ως πηγή χρηματοδότησης τρομοκρατίας χωρίς αποδεικτική σύνδεση. Η πολιτική πρέπει να στηρίζεται σε δείκτες, οικονομική διερεύνηση και ανταλλαγή πληροφοριών, αποφεύγοντας γενικεύσεις που αποδυναμώνουν την αναλυτική ακρίβεια.

PHISHING, SOCIAL ENGINEERING, ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ, ΠΑΡΑΒΙΑΣΗ ΛΟΓΑΡΙΑΣΜΩΝ ΚΑΙ ΚΑΚΟΒΟΥΛΗ ΔΙΑΦΗΜΙΣΗ ΜΠΟΡΟΥΝ ΝΑ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΤΟΣΟ ΓΙΑ ΤΗΝ ΕΞΑΠΑΤΗΣΗ ΚΑΤΑΝΑΛΩΤΩΝ ΟΣΟ ΚΑΙ ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΠΑΡΑΝΟΜΩΝ ΚΑΤΑΣΤΗΜΑΤΩΝ. ΤΟ CRIME AS A SERVICE ΜΕΙΩΝΕΙ ΤΟ ΤΕΧΝΙΚΟ ΚΑΤΩΦΛΙ: ΕΓΚΛΗΜΑΤΙΚΕΣ ΟΜΑΔΕΣ ΜΠΟΡΟΥΝ ΝΑ ΑΓΟΡΑΖΟΥΝ ΕΤΟΙΜΕΣ ΥΠΟΔΟΜΕΣ, ΥΠΗΡΕΣΙΕΣ ΑΠΟΚΡΥΨΗΣ, DOMAINS, ΠΛΑΣΤΑ REVIEWS ΚΑΙ ΕΡΓΑΛΕΙΑ ΔΗΜΙΟΥΡΓΙΑΣ ΠΑΡΑΠΛΑΝΗΤΙΚΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ.

ΣΥΝΑΦΗΣ ΜΟΡΦΗ	ΚΟΙΝΕΣ ΥΠΟΔΟΜΕΣ/ΕΝΔΕΙΞΕΙΣ	ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΑΠΑΝΤΗΣΗ
ΟΡΓΑΝΩΜΕΝΟ ΕΓΚΛΗΜΑ	ΚΟΙΝΑ LOGISTICS, ΑΠΟΘΗΚΕΣ, ΠΟΛΛΑΠΛΑ ΠΡΟΪΟΝΤΑ	ΑΝΑΛΥΣΗ ΔΙΚΤΥΟΥ ΚΑΙ ΚΟΙΝΕΣ ΕΡΕΥΝΕΣ
ΝΟΜΙΜΟΠΟΙΗΣΗ ΕΣΟΔΩΝ	MONEY MULES, ΕΙΚΟΝΙΚΕΣ ΕΤΑΙΡΕΙΕΣ, CRYPTO	ΠΑΡΑΛΛΗΛΗ ΟΙΚΟΝΟΜΙΚΗ ΕΡΕΥΝΑ ΚΑΙ ΔΕΣΜΕΥΣΗ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ
ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ/ΑΠΑΤΗ	PHISHING, ΚΛΕΜΜΕΝΟΙ ΛΟΓΑΡΙΑΣΜΟΙ, CRIME AS A SERVICE	ΣΥΝΔΕΣΗ FRAUD INTELLIGENCE ΚΑΙ ΨΗΦΙΑΚΩΝ ΕΡΕΥΝΩΝ
ΔΙΑΦΘΟΡΑ	ΠΑΡΑΚΑΜΨΗ ΕΛΕΓΧΩΝ, ΕΣΩΤΕΡΙΚΗ ΠΛΗΡΟΦΟΡΗΣΗ	INTEGRITY CONTROLS ΚΑΙ ΕΡΕΥΝΑ ΚΡΙΣΙΜΩΝ ΚΟΜΒΩΝ
ΕΚΜΕΤΑΛΛΕΥΣΗ ΑΝΗΛΙΚΩΝ	MONEY MULES, ΠΑΡΑΛΗΠΤΕΣ, ΜΕΤΑΠΩΛΗΤΕΣ	ΠΡΟΣΤΑΣΙΑ, ΠΡΟΛΗΨΗ ΚΑΙ ΣΤΟΧΕΥΜΕΝΗ ΕΠΙΒΟΛΗ
ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΤΡΟΜΟΚΡΑΤΙΑΣ	ΥΠΟΠΤΕΣ ΡΟΕΣ ΚΑΙ ΤΕΚΜΗΡΙΩΜΕΝΟΙ ΔΕΣΜΟΙ	CASE-BY-CASE ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ

4.
ΓΙΑΤΙ Η ΣΗΜΕΡΙΝΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΔΕΝ ΕΠΑΡΚΕΙ

Η πρόκληση δεν προκύπτει από ένα μοναδικό θεσμικό ή τεχνικό κενό. Προκύπτει από τον συνδυασμό όγκου, ταχύτητας, κατακερματισμένων αρμοδιοτήτων και ασύνδετων δεδομένων. Οι παρακάτω αδυναμίες εξηγούν γιατί τα διαθέσιμα εργαλεία δεν μετατρέπονται πάντοτε σε αποτελεσματική διατάραξη των δικτύων.

ΤΑ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΑ ΣΥΣΤΗΜΑΤΑ ΜΠΟΡΟΥΝ ΝΑ ΠΑΡΑΓΟΥΝ ΕΝΔΕΙΞΕΙΣ ΚΙΝΔΥΝΟΥ, ΟΧΙ ΑΠΟΔΕΙΚΤΙΚΕΣ ΚΡΙΣΕΙΣ Ή ΑΠΟΦΑΣΕΙΣ ΕΝΟΧΗΣ. Η ΕΝΔΕΙΞΗ ΤΗΣ ΜΗΧΑΝΗΣ ΠΡΕΠΕΙ ΝΑ ΑΝΤΙΜΕΤΩΠΙΖΕΤΑΙ ΩΣ ΑΦΕΤΗΡΙΑ ΠΕΡΑΙΤΕΡΩ ΕΛΕΓΧΟΥ ΚΑΙ ΝΑ ΜΗΝ ΥΠΟΝΟΜΕΥΕΙ ΤΟ ΤΕΚΜΗΡΙΟ ΑΘΩΟΤΗΤΑΣ. ΓΙΑ ΤΟΝ ΛΟΓΟ ΑΥΤΟ, ΣΥΣΤΗΜΑΤΑ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ ΠΡΕΠΕΙ ΝΑ ΛΕΙΤΟΥΡΓΟΥΝ ΜΕ ΑΝΘΡΩΠΙΝΗ ΕΠΟΠΤΕΙΑ, AUDIT TRAILS, ΚΑΤΑΓΡΑΦΗ ΕΝΕΡΓΕΙΩΝ ΚΑΙ ΔΥΝΑΤΟΤΗΤΑ ΕΛΕΓΧΟΥ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ.

4.1 Τεχνητή Νοημοσύνη και περιορισμοί των αυτοματοποιημένων μοντέλων

Η Τεχνητή Νοημοσύνη μπορεί να βελτιώσει σημαντικά τη δυνατότητα των αρχών και των ιδιωτικών φορέων να επεξεργάζονται μεγάλους όγκους δεδομένων. Μπορεί να εντοπίζει ασυνήθιστες συμπεριφορές, μοτίβα συναλλαγών, σχέσεις ανάμεσα σε οντότητες και σήματα που θα ήταν πρακτικά αδύνατο να εντοπιστούν χειροκίνητα. Η ΤΝ δεν αντικαθιστά την ανθρώπινη κρίση, αλλά ενισχύει την ικανότητα ανάλυσης και στόχευσης. Ο ελεγκτής ή ο ερευνητής αποκτά πρόσβαση σε περισσότερα δεδομένα και καλύτερα σήματα κινδύνου, χωρίς να εκχωρεί την τελική απόφαση στη μηχανή.

Όταν η πραγματική παρανομία είναι πολύ σπάνια σε σχέση με τον συνολικό όγκο των δεδομένων, ακόμη και ένας πολύ καλός αλγόριθμος μπορεί να παράγει περισσότερα ψευδώς θετικά αποτελέσματα (false positives), δηλαδή νόμιμες περιπτώσεις που το σύστημα χαρακτηρίζει λανθασμένα ως ύποπτες ή παράνομες. Η χαμηλή συχνότητα της παράνομης δραστηριότητας μέσα σε πολύ μεγάλους όγκους δεδομένων δημιουργεί ιδιαίτερη στατιστική πρόκληση. Σε έκθεση της Ευρωπαϊκής Επιτροπής του Νοεμβρίου 2025, η αναλογία παράνομου υλικού προς το σύνολο του ελεγχόμενου περιεχομένου για μεγάλο πάροχο αναφέρθηκε σε μόλις 0,00027%. Υπό αυτές τις συνθήκες, ακόμη και ένα ιδιαίτερα ακριβές σύστημα μπορεί να παράγει σημαντικό αριθμό ψευδώς θετικών ενδείξεων και να επιβαρύνει δυσανάλογα νόμιμες περιπτώσεις.

Τα αυτοματοποιημένα συστήματα μπορούν να παράγουν ενδείξεις κινδύνου, όχι αποδεικτικές κρίσεις ή αποφάσεις ενοχής. Η ένδειξη της μηχανής πρέπει να αντιμετωπίζεται ως αφετηρία περαιτέρω ελέγχου και να μην υπονομεύει το τεκμήριο αθωότητας. Για τον λόγο αυτό, συστήματα υψηλού κινδύνου πρέπει να λειτουργούν με ανθρώπινη εποπτεία, audit trails, καταγραφή ενεργειών και δυνατότητα ελέγχου της διαδικασίας.

Η προστασία της ιδιωτικότητας και η αποτελεσματική ασφάλεια δεν αποτελούν κατ’ ανάγκην αντικρουόμενους στόχους. Το ζητούμενο είναι η ανάπτυξη αποτελεσματικών μηχανισμών με σεβασμό στα προσωπικά δεδομένα και στις εγγυήσεις του κράτους δικαίου.

Δεν υπάρχει πραγματικό έλλειμμα ώριμων τεχνολογιών ιχνηλασιμότητας. RFID, NFC, QR codes, κρυπτογραφικά QR codes και κατανεμημένα μητρώα μπορούν να χρησιμοποιούνται ώστε οι ελεγκτές, αλλά και οι ίδιοι οι καταναλωτές, να ελέγχουν τη γνησιότητα ενός προϊόντος. Το πρόβλημα συνεπώς δεν βρίσκεται αποκλειστικά στην έρευνα. Βρίσκεται στη διάδοση, στην εφαρμογή και στο εάν οι επιχειρήσεις και οι καταναλωτές έχουν κίνητρο να χρησιμοποιήσουν αυτά τα εργαλεία. Η χαμηλή συχνότητα μιας παράνομης κατηγορίας αυξάνει τον κίνδυνο ψευδώς θετικών ενδείξεων, αλλά η πραγματική θετική προγνωστική αξία εξαρτάται επίσης από την ευαισθησία, την ειδικότητα, την ποιότητα των δεδομένων και το επιχειρησιακό κατώφλι. Για τον λόγο αυτό, τα μοντέλα πρέπει να αξιολογούνται με μετρήσεις ακρίβειας, bias, explainability και πραγματικής επιχειρησιακής χρησιμότητας.

4.2 Νομοθετικό ή εφαρμοστικό έλλειμμα;

Ως προς το θεσμικό πλαίσιο, αναδεικνύονται δύο διαφορετικές προσεγγίσεις. Η πρώτη θεωρεί ότι το ουσιαστικό δίκαιο είναι σε μεγάλο βαθμό επαρκές, καθώς η νομική φύση της λαθρεμπορίας δεν αλλάζει ανάλογα με το τεχνολογικό μέσο και εντοπίζει το κύριο πρόβλημα στην εφαρμογή και στη συνεργασία. Η δεύτερη προσέγγιση εντοπίζει ουσιαστικά θεσμικά κενά στη σύνδεση του λαθρεμπορίου με το ηλεκτρονικό εμπόριο και υποστηρίζει την ανάγκη ειδικότερων ρυθμίσεων. Η σύνθεση των δύο θέσεων οδηγεί σε στοχευμένη κάλυψη αποδεδειγμένων κενών και όχι σε γενικευμένη επανεγγραφή του πλαισίου.

Η σύνθεση πρέπει να είναι περιορισμένη: όχι γενικευμένη νομοθετική επανεγγραφή, αλλά στοχευμένη διόρθωση συγκεκριμένων κενών και πολύ καλύτερη εφαρμογή. Η τεχνολογία εξελίσσεται ταχύτερα από τη νομοθεσία. Αν ο νόμος περιγράφει συγκεκριμένες τεχνολογίες αντί να ορίζει το επιδιωκόμενο αποτέλεσμα, μπορεί να καταστεί παρωχημένος μέσα σε ένα ή δύο χρόνια.

Η έλλειψη συγκεκριμένης αρμοδιότητας μπορεί να έχει άμεσο επιχειρησιακό αποτέλεσμα. Χαρακτηριστική είναι περίπτωση απατηλού ιστοτόπου που μιμούνταν κρατική πλατφόρμα, για τον οποίο δεν υπήρχε ρητή δυνατότητα αποκλεισμού και απαιτήθηκε νομοθετική παρέμβαση.

Η ανάγκη αυστηροποίησης των ποινών δεν προκύπτει ως κύρια προτεραιότητα, καθώς ορισμένες από τις υφιστάμενες κυρώσεις είναι ήδη ιδιαίτερα αυστηρές. Μεγαλύτερη σημασία έχει η ταχύτητα και η συνέπεια της εφαρμογής. Το βασικό πρόβλημα είναι ότι, όταν η τελική δικαστική κρίση έρχεται πολλά χρόνια αργότερα, η αποτρεπτική ισχύς της κύρωσης μειώνεται.

Η γραφειοκρατική επιβάρυνση των εξειδικευμένων υπηρεσιών περιορίζει τον διαθέσιμο επιχειρησιακό χρόνο και μπορεί να μειώνει την αποτελεσματικότητα των ερευνών. Η ομαδοποίηση συναφών καταγγελιών και η προτεραιοποίηση με βάση μοτίβα και κίνδυνο μπορούν να απελευθερώσουν επιχειρησιακούς πόρους και να βελτιώσουν την έρευνα.

Το βασικό επιχειρησιακό έλλειμμα είναι ότι κανένας φορέας δεν βλέπει μόνος του ολόκληρη την εικόνα. Η αστυνομία βλέπει ένα τμήμα, τα τελωνεία ένα άλλο, οι πάροχοι πληρωμών τις συναλλαγές, οι courier τις αποστολές και οι πλατφόρμες την ψηφιακή δραστηριότητα. Η σύνδεση αυτών των πληροφοριών μπορεί να αποκαλύψει μοτίβα και δίκτυα που κανένας φορέας δεν θα εντόπιζε μόνος του.

ΤΟ ΒΑΣΙΚΟ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΕΛΛΕΙΜΜΑ ΕΙΝΑΙ ΟΤΙ ΚΑΝΕΝΑΣ ΦΟΡΕΑΣ ΔΕΝ ΒΛΕΠΕΙ ΜΟΝΟΣ ΤΟΥ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΙΚΟΝΑ. Η ΑΣΤΥΝΟΜΙΑ ΒΛΕΠΕΙ ΕΝΑ ΤΜΗΜΑ, ΤΑ ΤΕΛΩΝΕΙΑ ΕΝΑ ΑΛΛΟ, ΟΙ ΠΑΡΟΧΟΙ ΠΛΗΡΩΜΩΝ ΤΙΣ ΣΥΝΑΛΛΑΓΕΣ, ΟΙ COURIER ΤΙΣ ΑΠΟΣΤΟΛΕΣ ΚΑΙ ΟΙ ΠΛΑΤΦΟΡΜΕΣ ΤΗΝ ΨΗΦΙΑΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ. Η ΣΥΝΔΕΣΗ ΑΥΤΩΝ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΜΠΟΡΕΙ ΝΑ ΑΠΟΚΑΛΥΨΕΙ ΜΟΤΙΒΑ ΚΑΙ ΔΙΚΤΥΑ ΠΟΥ ΚΑΝΕΝΑΣ ΦΟΡΕΑΣ ΔΕΝ ΘΑ ΕΝΤΟΠΙΖΕ ΜΟΝΟΣ ΤΟΥ.

Υπάρχει ήδη θεσμική υποδομή συνεργασίας. Το ζητούμενο δεν είναι κατ' ανάγκην η δημιουργία νέου θεσμού, αλλά η επέκταση και εμβάθυνση του υφιστάμενου μηχανισμού. Η περιστασιακή επικοινωνία μεταξύ στελεχών πρέπει να μετατραπεί σε θεσμοθετημένο κόμβο με σαφείς όρους, προϋποθέσεις και διαδικασίες λειτουργίας.

4.3 Ψηφιακές πλατφόρμες, σήματα εμπιστοσύνης, προστασία ανηλίκων

Οι ψηφιακές πλατφόρμες πρέπει να έχουν κεντρικότερο ρόλο τόσο στη διαμόρφωση πολιτικής όσο και στην επιχειρησιακή αντιμετώπιση του παράνομου εμπορίου. Η συνεργασία και η συνυπευθυνότητά τους πρέπει να στηρίζονται σε σαφείς διαδικασίες ανταπόκρισης, χορήγησης στοιχείων και ταχείας αφαίρεσης παράνομου περιεχομένου, ώστε να λειτουργούν ως ενεργοί κρίκοι της ψηφιακής αλυσίδας.

Η Πράξη για τις Ψηφιακές Υπηρεσίες (Digital Services Act – DSA) ενισχύει το πλαίσιο συνεργασίας και χορήγησης στοιχείων προς τις αρμόδιες αρχές, χωρίς να υποκαθιστά τις ειδικές τελωνειακές, εποπτικές και διωκτικές αρμοδιότητες. Το κρίσιμο ζήτημα είναι πλέον η ταχύτητα. Σε ένα περιβάλλον όπου η παράνομη δραστηριότητα μπορεί να μετακινείται σχεδόν σε πραγματικό χρόνο από έναν λογαριασμό, ένα site ή μια πλατφόρμα σε άλλο, η αποτελεσματικότητα της συνεργασίας εξαρτάται όχι μόνο από το αν θα δοθούν τα στοιχεία ή θα αφαιρεθεί το παράνομο περιεχόμενο, αλλά και από το πόσο γρήγορα θα γίνει αυτό.

Η αποτελεσματικότητα της συνολικής απάντησης εξαρτάται από τη σύνδεση όλων των κρίκων της αλυσίδας και όχι μόνο από την επιμέρους ισχύ κάθε φορέα.

Δεν υπάρχει ουσιαστική σύγκρουση ανάμεσα στο φυσικό και το ψηφιακό εμπόριο, καθώς οι νόμιμες επιχειρήσεις λειτουργούν και στα δύο κανάλια. Η πραγματική ασυμμετρία βρίσκεται ανάμεσα στους φορείς που συμμορφώνονται με το φορολογικό και κανονιστικό πλαίσιο και σε όσους το παρακάμπτουν. Για τον λόγο αυτό, η προσθήκη νέων κανόνων πρέπει να εξετάζεται σε συνδυασμό με τη μείωση περιττής γραφειοκρατίας για τη νόμιμη αγορά.

Κάθε νέα υποχρέωση πρέπει να εξετάζεται ως προς το εάν μπορεί πραγματικά να επιβληθεί στους παραβάτες ή αν απλώς αυξάνει το κόστος όσων ήδη τηρούν τον νόμο.

Το ηλεκτρονικό εμπόριο χρειάζεται απλά και αναγνωρίσιμα σήματα εμπιστοσύνης. Ένα σύστημα trust mark που βασίζεται σε σαφή κριτήρια μπορεί να βοηθά τον καταναλωτή να αναγνωρίζει αξιόπιστα ηλεκτρονικά καταστήματα. Τα ίδια κριτήρια μπορούν να αξιοποιούνται προληπτικά για τον αυτοματοποιημένο έλεγχο ιστοτόπων, πάντοτε με ανθρώπινη εποπτεία.

Η προστασία των ανηλίκων απαιτεί αξιόπιστη επιβεβαίωση ηλικίας και ταυτότητας, ώστε να είναι γνωστή η πραγματική ταυτότητα των μερών μιας συναλλαγής. Το κρίσιμο ζήτημα δεν είναι η διαθεσιμότητα της τεχνολογίας, αλλά η συνεπής εφαρμογή της στα φυσικά και ψηφιακά

ΟΙ ΨΗΦΙΑΚΕΣ ΠΛΑΤΦΟΡΜΕΣ ΠΡΕΠΕΙ ΝΑ ΕΧΟΥΝ ΚΕΝΤΡΙΚΟΤΕΡΟ ΡΟΛΟ ΤΟΣΟ ΣΤΗ ΔΙΑΜΟΡΦΩΣΗ ΠΟΛΙΤΙΚΗΣ ΟΣΟ ΚΑΙ ΣΤΗΝ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ. Η ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ Η ΣΥΝΥΠΕΥΘΥΝΟΤΗΤΑ ΤΟΥΣ ΠΡΕΠΕΙ ΝΑ ΣΤΗΡΙΖΟΝΤΑΙ ΣΕ ΣΑΦΕΙΣ ΔΙΑΔΙΚΑΣΙΕΣ ΑΝΤΑΠΟΚΡΙΣΗΣ, ΧΟΡΗΓΗΣΗΣ ΣΤΟΙΧΕΙΩΝ ΚΑΙ ΤΑΧΕΙΑΣ ΑΦΑΙΡΕΣΗΣ ΠΑΡΑΝΟΜΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ, ΩΣΤΕ ΝΑ ΛΕΙΤΟΥΡΓΟΥΝ ΩΣ ΕΝΕΡΓΟΙ ΚΡΙΚΟΙ ΤΗΣ ΨΗΦΙΑΚΗΣ ΑΛΥΣΙΔΑΣ.

κανάλια. Η προστασία επεκτείνεται και στον κίνδυνο στρατολόγησης νέων από εγκληματικές ομάδες.

Η διαρκής ενημέρωση αποτελεί βασική γραμμή άμυνας και πρέπει να αφορά πολίτες, επιχειρήσεις, εργαζομένους και δημόσιες αρχές. Καθώς τα πρότυπα ψηφιακής απάτης μεταβάλλονται συνεχώς, η εκπαίδευση δεν μπορεί να είναι εφάπαξ.

Η κοινωνική απονομιμοποίηση του λαθρεμπορίου αποτελεί αναγκαίο μέρος της πρόληψης. Όσο οι μικρές παράνομες αγορές αντιμετωπίζονται ως κοινωνικά αθώες ή ασήμαντες, η ζήτηση θα συνεχίσει να τροφοδοτεί τα δίκτυα. Οι πολίτες πρέπει να αντιλαμβάνονται ότι ακόμη και περιορισμένης αξίας παράνομες αγορές μπορούν να βλάπτουν τη δημόσια υγεία, τα δημόσια έσοδα και τη νόμιμη οικονομία.

Η αντιμετώπιση της ζήτησης δεν εξαντλείται στην ενημέρωση και στην αλλαγή κουλτούρας. Σε ορισμένες αγορές, η μεγαλύτερη διαθεσιμότητα, ευκολία και ελκυστικότητα της νόμιμης εναλλακτικής μπορεί να περιορίζει τον χώρο ανάπτυξης της παράνομης αγοράς. Η καταστολή της παράνομης προσφοράς και η ενίσχυση της νόμιμης επιλογής μπορούν επομένως να λειτουργούν συμπληρωματικά.

ΗΚΟΙΝΩΝΙΚΗ ΑΠΟΝΟΜΙΜΟΠΟΙΗΣΗ ΤΟΥ ΛΑΘΡΕΜΠΟΡΙΟΥ ΑΠΟΤΕΛΕΙ ΑΝΑΓΚΑΙΟ ΜΕΡΟΣ ΤΗΣ ΠΡΟΛΗΨΗΣ. ΟΣΟ ΟΙ ΜΙΚΡΕΣ ΠΑΡΑΝΟΜΕΣ ΑΓΟΡΕΣ ΑΝΤΙΜΕΤΩΠΙΖΟΝΤΑΙ ΩΣ ΚΟΙΝΩΝΙΚΑ ΑΘΩΕΣ Ή ΑΣΗΜΑΝΤΕΣ, Η ΖΗΤΗΣΗ ΘΑ ΣΥΝΕΧΙΣΕΙ ΝΑ ΤΡΟΦΟΔΟΤΕΙ ΤΑ ΔΙΚΤΥΑ. ΟΙ ΠΟΛΙΤΕΣ ΠΡΕΠΕΙ ΝΑ ΑΝΤΙΛΑΜΒΑΝΟΝΤΑΙ ΟΤΙ ΑΚΟΜΗ ΚΑΙ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΑΞΙΑΣ ΠΑΡΑΝΟΜΕΣ ΑΓΟΡΕΣ ΜΠΟΡΟΥΝ ΝΑ ΒΛΑΠΤΟΥΝ ΤΗ ΔΗΜΟΣΙΑ ΥΓΕΙΑ, ΤΑ ΔΗΜΟΣΙΑ ΕΣΟΔΑ ΚΑΙ ΤΗ ΝΟΜΙΜΗ ΟΙΚΟΝΟΜΙΑ.

5. Τα βασικά κενά πολιτικής

ΚΕΝΟ	ΠΡΑΚΤΙΚΗ ΣΥΝΕΠΕΙΑ	ΑΝΑΓΚΗ ΠΟΛΙΤΙΚΗΣ
ΚΟΙΝΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΙΚΟΝΑ	ΚΑΝΕΝΑΣ ΦΟΡΕΑΣ ΔΕΝ ΒΛΕΠΕΙ ΟΛΟΚΛΗΡΟ ΤΟ ΔΙΚΤΥΟ.	ΣΤΑΘΕΡΗ ΣΥΝΔΕΣΗ ΤΕΛΩΝΕΙΑΚΩΝ, ΑΣΤΥΝΟΜΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΙΔΙΩΤΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
ΤΑΧΥΤΗΤΑ	Η ΠΑΡΑΝΟΜΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΜΕΤΑΚΙΝΕΙΤΑΙ ΠΡΙΝ ΟΛΟΚΛΗΡΩΘΕΙ Η ΔΙΟΙΚΗΤΙΚΗ ΑΝΤΙΔΡΑΣΗ.	ΜΕΤΡΗΣΙΜΟΙ ΧΡΟΝΟΙ ΑΠΟΚΡΙΣΗΣ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΚΛΙΜΑΚΩΣΗΣ
ΙΧΝΗΛΑΣΙΜΟΤΗΤΑ	ΔΕΝ ΣΥΝΔΕΟΝΤΑΙ ΠΑΝΤΑ ΠΡΟΪΟΝ, ΠΩΛΗΤΗΣ ΚΑΙ ΥΠΕΥΘΥΝΟΣ ΕΝΔΙΑΜΕΣΟΣ.	KNOW YOUR BUSINESS CUSTOMER ΚΑΙ ΚΟΙΝΑ ΑΝΑΓΝΩΡΙΣΤΙΚΑ
ΟΙΚΟΝΟΜΙΚΗ ΔΙΕΡΕΥΝΗΣΗ	ΔΙΑΚΟΠΤΕΤΑΙ ΕΝΑ ΚΑΝΑΛΙ ΧΩΡΙΣ ΝΑ ΠΛΗΤΤΕΤΑΙ ΤΟ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟ ΜΟΝΤΕΛΟ.	FOLLOW THE MONEY ΑΠΟ ΤΗΝ ΑΡΧΗ ΤΗΣ ΥΠΟΘΕΣΗΣ
ΑΞΙΟΛΟΓΗΣΗ	ΜΕΤΡΩΝΤΑΙ ΕΛΕΓΧΟΙ ΚΑΙ ΚΑΤΑΣΧΕΣΕΙΣ, ΟΧΙ Η ΣΥΣΤΗΜΙΚΗ ΔΙΑΤΑΡΑΞΗ.	KPIs ΑΚΡΙΒΕΙΑΣ, ΤΑΧΥΤΗΤΑΣ, ΥΠΟΤΡΟΠΗΣ ΚΑΙ ΑΝΑΚΤΗΣΗΣ ΕΣΟΔΩΝ

CENTER FOR CYBER RESILIENCE

ΜΕΡΟΣ Β

ΤΟ ΔΙΕΘΝΕΣ, ΕΥΡΩΠΑΪΚΟ ΚΑΙ ΕΛΛΗΝΙΚΟ ΠΛΑΙΣΙΟ

6.
ΤΟ ΔΙΕΘΝΕΣ ΠΛΑΙΣΙΟ

Το Framework of Standards on Cross-Border E-Commerce του Παγκόσμιου Οργανισμού Τελωνείων παρέχει τη βασική διεθνή αναφορά. Οι δεκαπέντε αρχές του επικεντρώνονται στην έγκαιρη ηλεκτρονική πληροφόρηση, στη διαχείριση κινδύνου, στην απλούστευση των νόμιμων ροών, στην είσπραξη εσόδων, στη διυπηρεσιακή συνεργασία, στις συμπράξεις με τον ιδιωτικό τομέα και στη μέτρηση των αποτελεσμάτων.

6.1 Αναβαθμισμένα ηλεκτρονικά δεδομένα και διαχείριση κινδύνων

Η έγκαιρη πρόσβαση σε ακριβή δεδομένα πριν από την άφιξη της αποστολής επιτρέπει στο τελωνείο να διαχωρίζει υψηλό και χαμηλό κίνδυνο. Η προσέγγιση αυτή είναι κρίσιμη σε περιβάλλον εκατομμυρίων μικρών δεμάτων, όπου ο φυσικός έλεγχος μπορεί να είναι μόνο επιλεκτικός.

6.2 Συνεργασία και κατανομή ευθύνης

Το διεθνές πλαίσιο αντιμετωπίζει πλατφόρμες, ταχυδρομεία, courier, παρόχους υπηρεσιών και τελωνεία ως αλληλεξαρτώμενα μέρη. Η συνεργασία πρέπει να στηρίζεται σε σαφείς ρόλους, ποιότητα δεδομένων, προστασία προσωπικών πληροφοριών και αξιολόγηση των πραγματικών αποτελεσμάτων.

6.3 Διεθνής τελωνειακή και αστυνομική συνεργασία

Η διασυνοριακή φύση του προβλήματος απαιτεί ανταλλαγή δεικτών κινδύνου, κοινές επιχειρήσεις και ταχεία πρόσβαση σε στοιχεία που βρίσκονται σε άλλη δικαιοδοσία. OECD, EUIPO, WCO, Interpol και Europol παράγουν διαφορετικού τύπου γνώση, η οποία πρέπει να μετατρέπεται σε εθνικά προφίλ κινδύνων και επιχειρησιακές προτεραιότητες.

7.
ΤΟ ΠΛΑΙΣΙΟ ΠΟΛΙΤΙΚΗΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Η ΕΕ δεν διαθέτει ένα μοναδικό νομοθέτημα για το ψηφιακό παράνομο εμπόριο. Η αντιμετώπιση προκύπτει από τη συνδυασμένη λειτουργία τελωνειακού δικαίου, εποπτείας αγοράς, ασφάλειας προϊόντων, ψηφιακών υπηρεσιών, προστασίας καταναλωτή, φορολογικής συνεργασίας, καταπολέμησης της νομιμοποίησης εσόδων και αστυνομικής συνεργασίας. Η αποτελεσματικότητα εξαρτάται συνεπώς από τη διαλειτουργικότητα των μηχανισμών.

Η πολιτική συμφωνία του Μαρτίου 2026 για τη μεταρρύθμιση της Τελωνειακής Ένωσης προβλέπει μία περισσότερο ενιαία και data-driven αρχιτεκτονική. Η νέα EU Customs Authority θα εποπτεύει το EU Customs Data Hub, το οποίο θα συγκεντρώνει δεδομένα αλυσίδων εφοδιασμού και θα υποστηρίζει κοινή ανάλυση κινδύνου με ΤΝ και ανθρώπινη παρέμβαση. Το Hub προβλέπεται να ανοίξει για αποστολές ηλεκτρονικού εμπορίου το 2028.

Από την 1η Ιουλίου 2026 εφαρμόζεται προσωρινός δασμός τριών ευρώ ανά είδος για αποστολές κάτω των 150 ευρώ, έως την πλήρη εφαρμογή του νέου καθεστώτος. Η μεταρρύθμιση μεταφέρει σταδιακά μεγαλύτερη ευθύνη στις πλατφόρμες και στους πωλητές, αντί να αντιμετωπίζει τον μεμονωμένο καταναλωτή και τον μεταφορέα ως κύριους φορείς της τελωνειακής υποχρέωσης.

Η Ανακοίνωση της Επιτροπής του Φεβρουαρίου 2025 συνδέει τελωνεία, εποπτεία αγοράς, προστασία καταναλωτή, πλατφόρμες και περιβαλλοντική συμμόρφωση. Η αξία της βρίσκεται στην προσέγγιση ολόκληρου του κύκλου: δεδομένα πριν από την άφιξη, έλεγχος στα σύνορα, εποπτεία των προσφορών online, δράση μετά τη διάθεση στην αγορά και ενημέρωση των καταναλωτών.

Η ΕΕ ΔΕΝ ΔΙΑΘΕΤΕΙ ΕΝΑ ΜΟΝΑΔΙΚΟ ΝΟΜΟΘΕΤΗΜΑ ΓΙΑ ΤΟ ΨΗΦΙΑΚΟ ΠΑΡΑΝΟΜΟ ΕΜΠΟΡΙΟ. Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΡΟΚΥΠΤΕΙ ΑΠΟ ΤΗ ΣΥΝΔΥΑΣΜΕΝΗ ΛΕΙΤΟΥΡΓΙΑ ΤΕΛΩΝΕΙΑΚΟΥ ΔΙΚΑΙΟΥ, ΕΠΟΠΤΕΙΑΣ ΑΓΟΡΑΣ, ΑΣΦΑΛΕΙΑΣ ΠΡΟΪΟΝΤΩΝ, ΨΗΦΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ, ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑΝΑΛΩΤΗ, ΦΟΡΟΛΟΓΙΚΗΣ ΣΥΝΕΡΓΑΣΙΑΣ, ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΤΗΣ ΝΟΜΙΜΟΠΟΙΗΣΗΣ ΕΣΟΔΩΝ ΚΑΙ ΑΣΤΥΝΟΜΙΚΗΣ ΣΥΝΕΡΓΑΣΙΑΣ. Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΕΞΑΡΤΑΤΑΙ ΣΥΝΕΠΩΣ ΑΠΟ ΤΗ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ.

Ο DSA θεσπίζει υποχρεώσεις ιχνηλασιμότητας επαγγελματιών πωλητών, notice-and-action, συνεργασία με trusted flaggers, διαφάνεια και διαχείριση συστημικών κινδύνων για τις πολύ μεγάλες πλατφόρμες. Δεν καθιερώνει γενική ευθύνη των ενδιάμεσων για κάθε παράνομο προϊόν ούτε υποκαθιστά τις αρμόδιες αρχές. Δημιουργεί, όμως, σαφέστερα σημεία επαφής και διαδικασίες αντίδρασης.

Ο General Product Safety Regulation, ο Κανονισμός για την εποπτεία της αγοράς, το Safety Gate και το τελωνειακό πλαίσιο προστασίας δικαιωμάτων πνευματικής ιδιοκτησίας συγκροτούν κρίσιμα εργαλεία. Το κεντρικό ζητούμενο είναι η σύνδεση πληροφοριών για επικίνδυνα προϊόντα με τελωνειακά δεδομένα και δεδομένα από τις πλατφόρμες, ώστε ένα εύρημα να οδηγεί σε ταχεία προληπτική δράση σε όλα τα κανάλια.

Το IOSS, το CESOP, η DAC7 και η DAC8 ενισχύουν τη φορολογική ορατότητα στις ψηφιακές πλατφόρμες, τις διασυνοριακές πληρωμές και τα κρυπτοστοιχεία. Το ευρωπαϊκό πλαίσιο AML και η συνεργασία χρηματοπιστωτικών και διωκτικών αρχών προσφέρουν τη βάση για follow-the-money έρευνες. Το DORA συνεισφέρει στην επιχειρησιακή ανθεκτικότητα των χρηματοπιστωτικών υποδομών, αλλά δεν αποτελεί ειδικό μηχανισμό καταπολέμησης του παράνομου εμπορίου.

Europol, OLAF, EUIPO, Eurojust και οι προτεραιότητες EMPACT μπορούν να συνδέσουν εθνικές έρευνες, τελωνειακές επιχειρήσεις, οικονομικά δεδομένα και διεθνή αιτήματα. Η πρόκληση είναι να μετατραπούν οι ευρωπαϊκές δυνατότητες σε σταθερή εθνική ροή εργασίας και όχι να ενεργοποιούνται μόνο σε μεγάλες ή ήδη ώριμες υποθέσεις.

8. ΤΟ ΕΛΛΗΝΙΚΟ ΠΛΑΙΣΙΟ ΚΑΙ ΤΑ ΚΕΝΑ ΕΦΑΡΜΟΓΗΣ

ΔΕΝ ΥΠΑΡΧΕΙ ΑΜΕΣΗ ΑΝΑΓΚΗ ΝΕΑΣ ΝΟΜΟΘΕΣΙΑΣ ΣΤΗΝ ΕΛΛΑΔΑ. ΠΡΕΠΕΙ ΝΑ ΔΟΘΕΙ ΕΜΦΑΣΗ ΣΤΗΝ ΑΝΑΓΝΩΡΙΣΗ ΣΥΓΚΕΚΡΙΜΕΝΩΝ ΚΕΝΩΝ –ΑΡΜΟΔΙΟΤΗΤΑ ΜΠΛΟΚΑΡΙΣΜΑΤΟΣ, ΠΡΟΣΒΑΣΗ ΣΕ ΔΕΔΟΜΕΝΑ, ΣΥΝΔΕΣΗ ΚΑΤΑΓΓΕΛΙΩΝ, ΧΡΟΝΟΙ ΔΙΚΑΣΤΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ– ΚΑΙ Η ΤΕΧΝΟΛΟΓΙΚΑ ΟΥΔΕΤΕΡΗ ΔΙΟΡΘΩΣΗ ΤΟΥΣ.

Στην Ελλάδα το πεδίο τέμνει αρμοδιότητες τελωνειακών και φορολογικών αρχών, Ελληνικής Αστυνομίας, οικονομικών και εισαγγελικών αρχών, φορέων κυβερνοασφάλειας, εποπτείας της αγοράς και προστασίας καταναλωτή. Υπάρχει ήδη θεσμική υποδομή συντονισμού· η βασική ανάγκη είναι η αναβάθμισή της σε σταθερό επιχειρησιακό μηχανισμό και όχι η αυτόματη δημιουργία νέου φορέα.

8.1 Υφιστάμενες δυνατότητες

- Τελωνειακή ανάλυση κινδύνου και στοχευμένοι έλεγχοι μικροδεμάτων.
- Φορολογικά και συναλλακτικά δεδομένα για αναγνώριση δικτύων οντοτήτων.
- Εξειδικευμένες αστυνομικές δυνατότητες για κυβερνοέγκλημα και οργανωμένο έγκλημα.
- Μηχανισμοί συνεργασίας με Europol, OLAF, Eurojust, EUIPO και άλλες τελωνειακές διοικήσεις.

8.2 Κενά εφαρμογής

- Απουσία μόνιμης κοινής επιχειρησιακής εικόνας και ενιαίας ταξινόμησης υποθέσεων.
- Ανταλλαγή πληροφοριών που συχνά εξαρτάται από προσωπικά δίκτυα και όχι από θεσμοθετημένη ροή.
- Μη τυποποιημένοι χρόνοι ανταπόκρισης πλατφορμών, παρόχων πληρωμών και άλλων ενδιαμέσων.
- Περιορισμένη συστηματική αξιολόγηση υποθέσεων μετά την ολοκλήρωσή τους.

8.3 Νομοθετικά και διαδικαστικά ζητήματα

Δεν υπάρχει άμεση ανάγκη νέας νομοθεσίας. Πρέπει να δοθεί έμφαση στην αναγνώριση συγκεκριμένων κενών –αρμοδιότητα μπλοκαρίσματος, πρόσβαση σε δεδομένα, σύνδεση καταγγελιών, χρόνοι δικαστικής διαχείρισης– και η τεχνολογικά ουδέτερη διόρθωσή τους.

CENTER FOR CYBER RESILIENCE

ΜΕΡΟΣ Γ

ΣΥΓΚΡΙΤΙΚΕΣ ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ ΚΑΙ ΔΙΔΑΓΜΑΤΑ

9.
ΕΠΙΛΕΓΜΕΝΕΣ ΔΙΕΘΝΕΙΣ ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ

9.1 Επαναλαμβανόμενες αρχές

Οι παρακάτω πρακτικές δεν αποτελούν έτοιμα μοντέλα προς αντιγραφή. Αναδεικνύουν όμως τέσσερις επαναλαμβανόμενες αρχές: σαφή υπευθυνότητα των ενδιαμέσων, ταχεία απόκριση, αξιοποίηση προηγμένων δεδομένων και μόνιμη δημόσια–ιδιωτική συνεργασία.

Η επιλογή των παραδειγμάτων βασίζεται στη συνάφειά τους με τα βασικά σημεία παρέμβασης του paper: ταυτοποίηση και λογοδοσία πωλητών, διακοπή ψηφιακών υποδομών, ανάλυση κινδύνου σε ροές μικρών δεμάτων και οργανωμένη συνεργασία δημόσιου και ιδιωτικού τομέα. Ο πίνακας διακρίνει το κύριο χαρακτηριστικό κάθε πρακτικής από το στοιχείο που μπορεί να προσαρμοστεί στην Ελλάδα. Η μεταφορά δεν αφορά αυτούσια αντιγραφή θεσμών, αλλά αξιοποίηση λειτουργικών μηχανισμών συμβατών με τις εθνικές αρμοδιότητες, το ενωσιακό δίκαιο και τις εγγυήσεις προστασίας δεδομένων.

9.2 Κριτήρια αξιολόγησης μιας καλής πρακτικής

- Σαφής νομική αρμοδιότητα και σημείο επαφής.
- Προκαθορισμένοι χρόνοι ανταπόκρισης και δυνατότητα ελέγχου της απόφασης.
- Ταυτοποίηση πωλητή και αποτροπή της άμεσης επανεμφάνισης με νέα στοιχεία.
- Αξιολόγηση της ακρίβειας των μοντέλων και όχι απλή μέτρηση του αριθμού ελέγχων.
- Σταθερή συνεργασία με δικαιούχους, πλατφόρμες, πληρωμές, courier και τελωνεία.

10.
ΟΡΙΖΟΝΤΙΑ ΔΙΔΑΓΜΑΤΑ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ

Η συγκριτική επισκόπηση δεν υποδεικνύει ένα ενιαίο μοντέλο. Αναδεικνύει, όμως, επαναλαμβανόμενα χαρακτηριστικά που μπορούν να προσαρμοστούν στο ελληνικό θεσμικό περιβάλλον.

- Αξιόπιστη ταυτοποίηση του πραγματικού πωλητή και αποτροπή άμεσης επανεμφάνισης.
- Προκαθορισμένοι και μετρήσιμοι χρόνοι απόκρισης για listings, domains και αιτήματα στοιχείων.
- Αξιοποίηση δεδομένων πριν από την άφιξη της αποστολής και κοινά risk profiles.
- Συνδυασμός τελωνειακής, ψηφιακής και οικονομικής διερεύνησης.
- Μόνιμη δημόσια/ιδιωτική συνεργασία με σαφείς όρους, δικλείδες και λογοδοσία.
- Μέτρηση hit rate, false positives, υποτροπής πωλητών και συστημικής διατάραξης.

Τα διδάγματα αυτά αποτελούν τα κριτήρια σχεδιασμού των προτάσεων που ακολουθούν. Δεν μεταφέρονται μηχανιστικά, αλλά συνδέονται με τα κενά πολιτικής που εντοπίστηκαν στο Μέρος Α και με τις δυνατότητες του ελληνικού πλαισίου στο Μέρος Β.

CENTER FOR CYBER RESILIENCE

ΜΕΡΟΣ Δ

ΠΡΟΤΑΣΕΙΣ ΠΟΛΙΤΙΚΗΣ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ – ΣΥΜΠΕΡΑΣΜΑΤΑ

11.
ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ

Ο στρατηγικός στόχος είναι η μετατροπή της υφιστάμενης συνεργασίας σε μόνιμη κοινή επιχειρησιακή υποδομή για την πρόληψη, τον εντοπισμό και τη διατάραξη του ψηφιακού παράνομου εμπορίου. Η υποδομή αυτή πρέπει να συνδέει την εικόνα του προϊόντος, του πωλητή, της πληρωμής και της διανομής, χωρίς να καταργεί τις αρμοδιότητες των επιμέρους αρχών ή τις εγγυήσεις προστασίας δικαιωμάτων.

Αρχές σχεδιασμού

- Αξιοποίηση και αναβάθμιση υφιστάμενων θεσμών πριν από τη δημιουργία νέων.
- Στόχευση βάσει κινδύνου, οντότητας και δικτύου, όχι αδιαφοροποίητη αύξηση ελέγχων.
- Privacy by design, ανθρώπινη εποπτεία και ελεγξιμότητα των αυτοματοποιημένων εργαλείων.
- Συνυπευθυνότητα χωρίς μετατροπή των νόμιμων ενδιαμέσων σε γενικούς διωκτικούς μηχανισμούς.
- Αξιολόγηση με βάση τη διατάραξη δικτύων και όχι μόνο τον αριθμό ενεργειών.

ΧΩΡΑ/ΠΡΑΚΤΙΚΗ	ΒΑΣΙΚΟ ΧΑΡΑΚΤΗΡΙΣΤΙΚΟ	ΔΥΝΑΤΟΤΗΤΑ ΠΡΟΣΑΡΜΟΓΗΣ ΣΤΗΝ ΕΛΛΑΔΑ
ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ – PIPCU / OPERATION ASHIKO	ΕΞΕΙΔΙΚΕΥΜΕΝΗ ΑΣΤΥΝΟΜΙΚΗ ΜΟΝΑΔΑ ΚΑΙ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟ NOMINET ΓΙΑ ΑΝΑΣΤΟΛΗ DOMAINS	ΜΟΝΙΜΟ ΠΡΩΤΟΚΟΛΛΟ ΑΣΤΥΝΟΜΙΑΣ, ΑΡΜΟΔΙΩΝ ΑΡΧΩΝ ΚΑΙ REGISTRIES
ΒΕΛΓΙΟ – NOTICE & ACTION ΓΙΑ .BE	ΔΥΝΑΤΟΤΗΤΑ ΑΝΑΣΤΟΛΗΣ ΚΑΙ ΑΝΑΚΑΤΕΥΘΥΝΣΗΣ DOMAIN ΕΝΤΟΣ ΜΙΑΣ ΕΡΓΑΣΙΜΗΣ ΗΜΕΡΑΣ	ΜΕΤΡΗΣΙΜΟ SLA ΚΑΙ ΠΡΟΕΙΔΟΠΟΙΗΤΙΚΗ ΣΕΛΙΔΑ ΠΡΟΣ ΤΟΝ ΚΑΤΑΝΑΛΩΤΗ
ΗΠΑ – INFORM CONSUMERS ACT	ΥΠΟΧΡΕΩΤΙΚΗ ΣΥΛΛΟΓΗ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΣΤΟΙΧΕΙΩΝ ΠΩΛΗΤΩΝ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ	KNOW YOUR BUSINESS CUSTOMER ΚΑΙ ΑΠΟΤΡΟΠΗ ΕΠΑΝΕΓΓΡΑΦΗΣ ΚΑΚΟΒΟΥΛΩΝ ΠΩΛΗΤΩΝ
ΝΟΤΙΑ ΚΟΡΕΑ – UNI-PASS ΚΑΙ RISK ANALYTICS	ΠΡΟΗΓΜΕΝΑ ΔΕΔΟΜΕΝΑ, ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΣΤΟΧΕΥΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΛΥΣΙΔΑΣ ΕΦΟΔΙΑΣΜΟΥ	ΕΝΟΠΟΙΗΣΗ ΤΕΛΩΝΕΙΑΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΕΠΙΔΟΣΕΩΝ ΤΩΝ ΜΟΝΤΕΛΩΝ
ΟΛΛΑΝΔΙΑ–ΒΕΛΓΙΟ – PROFILE	ΚΟΙΝΗ ΑΝΑΠΤΥΞΗ ANALYTICS ΚΑΙ ΤΝ ΓΙΑ ΤΕΛΩΝΕΙΑΚΟ RISK MANAGEMENT	ΔΙΑΚΡΑΤΙΚΑ ΜΟΝΤΕΛΑ ΚΙΝΔΥΝΟΥ ΚΑΙ ΑΝΤΑΛΛΑΓΗ ΔΕΙΚΤΩΝ ΓΙΑ ΒΑΣΙΚΕΣ ΠΥΛΕΣ ΕΙΣΟΔΟΥ

12. ΠΥΛΩΝΕΣ ΠΑΡΕΜΒΑΣΗΣ

12.1 Διακυβέρνηση και κοινή επιχειρησιακή εικόνα

- Μόνιμη διυπηρεσιακή δομή με τελωνειακές, φορολογικές, αστυνομικές, οικονομικές, κυβερνοασφαλείας και εποπτικές αρχές.
- Θεσμοθετημένα σημεία επαφής με πλατφόρμες, παρόχους πληρωμών, τράπεζες, courier, logistics και κλαδικούς φορείς.
- Κοινό λεξιλόγιο κινδύνων, taxonomy υποθέσεων και διαδικασία escalation.

12.2 Δεδομένα, risk intelligence και ΤΝ

- Ασφαλείς δίαυλοι για σχεδόν άμεση ανταλλαγή σημάτων κινδύνου και όχι ανεξέλεγκτη συγκέντρωση δεδομένων.
- Risk-based και entity-based μοντέλα που συνδυάζουν προϊόν, πωλητή, πληρωμή, αποστολέα, παραλήπτη και ιστορικό συμμόρφωσης.
- Human-in-the-loop, audit trails, περιοδικός έλεγχος false positives και μηχανισμός αμφισβήτησης.

12.3 Διακοπή του εγκληματικού επιχειρηματικού μοντέλου

- Παράλληλη ψηφιακή, τελωνειακή και οικονομική έρευνα από τα πρώτα στάδια.
- Ταχεία αναστολή παράνομων listings και domains με εγγυήσεις και αποτροπή επανεμφάνισης.
- Follow the money, δέσμευση εγκληματικών εσόδων και αξιοποίηση δεδομένων πληρωμών και κρυπτοστοιχείων.

12.4 Στοχευμένες θεσμικές και διαδικαστικές παρεμβάσεις

- Αναδρομική εξέταση σημαντικών υποθέσεων για εμπειρικό εντοπισμό κενών.
- Τεχνολογικά ουδέτερες διορθώσεις εκεί όπου αποδεικνύεται συγκεκριμένο κενό αρμοδιότητας ή διαδικασίας.
- Ομαδοποίηση συναφών καταγγελιών και επιτάχυνση της δικαστικής διαχείρισης υποθέσεων υψηλής επίπτωσης.

12.5 Πρόληψη, καταναλωτής και νόμιμη αγορά

- Συνεχής ενημέρωση για αξιόπιστα e-shops, επικίνδυνα προϊόντα και μοτίβα εξαπάτησης.
- Ισχυρότερη ηλικιακή επαλήθευση για ρυθμιζόμενα προϊόντα, με προστασία προσωπικών δεδομένων.
- Αξιολόγηση κάθε νέας υποχρέωσης ως προς το πραγματικό αποτέλεσμα και το βάρος για τις ήδη σύννομες επιχειρήσεις.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το ψηφιακό παράνομο εμπόριο είναι πρόβλημα αλυσίδας. Χρησιμοποιεί τις ίδιες υποδομές με τη νόμιμη οικονομία, τέμνει αρμοδιότητες και συνδέεται με ένα ευρύτερο εγκληματικό οικοσύστημα. Η αποτελεσματική αντίδραση πρέπει να συνδέει πληροφορίες χωρίς να καταργεί τις εγγυήσεις, να αξιοποιεί την τεχνολογία χωρίς να εκχωρεί την κρίση στη μηχανή και να επιβάλλει υποχρεώσεις χωρίς να τιμωρεί δυσανάλογα τη νόμιμη αγορά.

Το κρίσιμο βήμα για την Ελλάδα δεν είναι η δημιουργία ενός ακόμη θεσμού, αλλά η μετατροπή της υπάρχουσας συνεργασίας σε σταθερή επιχειρησιακή υποδομή, με κοινή εικόνα, σαφείς ρόλους, ασφαλή δεδομένα, μετρήσιμους χρόνους, οικονομική έρευνα και διαρκή μάθηση από πραγματικές υποθέσεις. Οι διαθέσιμες δυνατότητες πρέπει να χρησιμοποιηθούν συντονισμένα, έξυπνα και στοχευμένα.

Η εφαρμογή πρέπει να ξεκινήσει από ένα περιορισμένο σύνολο κοινών προτεραιοτήτων: ενιαίο επιχειρησιακό πρωτόκολλο, κοινά ελάχιστα πεδία δεδομένων, ταχεία διαβίβαση αιτημάτων προς πλατφόρμες και παρόχους πληρωμών και υποχρεωτική οικονομική διερεύνηση στις σοβαρές υποθέσεις. Μια πιλοτική εφαρμογή σε επιλεγμένες κατηγορίες υψηλού κινδύνου και σε βασικές πύλες εισόδου μπορεί να ελέγξει τη λειτουργικότητα του μοντέλου πριν από την ευρύτερη κλιμάκωσή του.

Παράλληλα, η Ελλάδα χρειάζεται συνεκτικό πλαίσιο μέτρησης. Η συστηματική δημοσίευση συγκρίσιμων στοιχείων για αποστολές, ελέγχους, ευρήματα, αποσύρσεις, δεσμεύσεις περιουσιακών στοιχείων και χρόνο απόκρισης θα επιτρέψει να διαχωρίζεται η αύξηση της ανίχνευσης από την πραγματική αύξηση του φαινομένου. Η επιτυχία δεν πρέπει να αποτιμάται μόνο από τον αριθμό κατασχέσεων, αλλά από τη μείωση της επαναλαμβανόμενης παραβατικότητας, τη διακοπή δικτύων, την ανάκτηση παράνομων εσόδων και την προστασία καταναλωτών και νόμιμων επιχειρήσεων.

ΒΑΣΙΚΕΣ ΠΗΓΕΣ

European Commission (2026). EU Customs Reform. https://taxation-customs.ec.europa.eu/customs/eu-customs-reform_en

European Commission (2025). A comprehensive EU toolbox for safe and sustainable e-commerce, COM(2025) 37. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0037

European Commission (2026). Large-scale EU customs control action on third-country e-commerce goods. https://taxation-customs.ec.europa.eu/news/large-scale-eu-customs-control-action-shows-most-third-country-e-commerce-goods-do-not-follow-2026-01-07_en

OECD/EUIPO (2025). Mapping Global Trade in Fakes 2025. https://doi.org/10.1787/94d3b29f-en

OECD/EUIPO (2021). Misuse of E-Commerce for Trade in Counterfeits. https://www.oecd.org/en/publications/misuse-of-e-commerce-for-trade-in-counterfeits_1c04a64e-en.html

Europol (2023). The Other Side of the Coin: An Analysis of Financial and Economic Crime. https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime

Europol (2025). EU Serious and Organised Crime Threat Assessment. https://www.europol.europa.eu/publications-events/main-reports/socta-report

World Customs Organization. Framework of Standards on Cross-Border E-Commerce. https://www.wcoomd.org/en/topics/facilitation/activities-and-programmes/ecommerce.aspx

World Customs Organization (2025). Illicit Trade Report 2025. https://www.wcoomd.org/en/topics/enforcement-and-compliance/resources/publications.aspx

UK Government (2022). Intellectual Property Counter-Infringement Strategy 2022–2027. https://www.gov.uk/government/publications/ip-counter-infringement-strategy-2022-to-2027

US Federal Trade Commission. INFORM Consumers Act. https://www.ftc.gov/business-guidance/resources/INFORMAct

World Customs Organization (2025). Korea Customs Service's digital innovation and e-commerce. https://mag.wcoomd.org/magazine/wco-news-108-issue-3-2025/korea-customs-services-e-commerce/

EUIPO (2021). Domain Names: Challenges and Good Practices. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf

European Commission & EUIPO (2025). Report on the EU enforcement of intellectual property rights in 2024. https://taxation-customs.ec.europa.eu/customs/prohibitions-restrictions/counterfeit-piracy-other-ipr-violations/ipr-facts-and-figures_en

Ελληνική Αστυνομία (2026). Εξάρθρωση κυκλώματος παράνομης παραγωγής και διακίνησης φαρμακευτικών σκευασμάτων και ουσιών ντόπινγκ, 11.6.2026. https://www.astynomia.gr/2026/06/11/11-6-2026-d-a-o-e-exarthrothike-kykloma-pou-drastiriopoiountan-stin-paranomi-paragogi-kai-diakinisi-farmakeftikon-skevasmaton-kai-ousion-ntopingk/

CENTER
FOR
CYBER
RESILIENCE

DELPHI
ECONOMIC
FORUM

POLICY
PAPERS

ΛΕΞΙΛΟΓΙΟ ΟΡΩΝ ΨΗΦΙΑΚΟΥ ΠΑΡΑΝΟΜΟΥ ΕΜΠΟΡΙΟΥ

- **OECD (ΟΟΣΑ):** Διεθνής οργανισμός που ποσοτικοποιεί το ψηφιακό λαθρεμπόριο και χαρτογραφεί τα εγκληματικά δίκτυα στο ηλεκτρονικό εμπόριο (e-commerce), διαμορφώνοντας παγκόσμια πρότυπα διαφάνειας.
- **EUIPO:** Ευρωπαϊκός οργανισμός αρμόδιος για τη διανοητική ιδιοκτησία, που αναλύει τη διακίνηση παραποιημένων προϊόντων (counterfeits) σε ψηφιακές αγορές και μέσα κοινωνικής δικτύωσης.
- **DAC8:** Ευρωπαϊκή οδηγία που αίρει την ανωνυμία των εγκληματικών συναλλαγών, επιβάλλοντας την υποχρεωτική αναφορά δεδομένων για κρυπτοστοιχεία (crypto-assets) και NFTs.
- **AML:** Το ρυθμιστικό πλαίσιο κατά του ξεπλύματος χρήματος που στοχεύει στον εντοπισμό και τη διακοπή των παράνομων χρηματοοικονομικών ροών από το ψηφιακό έγκλημα.
- **DORA:** Ευρωπαϊκός κανονισμός για την ψηφιακή ανθεκτικότητα των χρηματοπιστωτικών υποδομών, που θωρακίζει τις πύλες πληρωμών (payment gateways) απέναντι σε κυβερνοαπειλές.

