

ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES



ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ»

Ο ρόλος του Darknet στο Οργανωμένο Έγκλημα :

Επίπεδο ερευνών και Προβλήματα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Παπαφραγκίσκου Τατιανή

Αθήνα, 2025

Στους γονείς μου

Τριμελής Επιτροπή

Λαμπροπούλου Ευσταθία, Καθηγήτρια Παντείου Πανεπιστημίου

Ζιούβας Δημήτρης, Επίκουρος Καθηγητής Παντείου Πανεπιστημίου

Λάζος Γρηγόρης, Ομότιμος Καθηγητής Παντείου Πανεπιστημίου



Copyright © Παπαφραγκίσκου Τατιανή, 2025

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες, αρχικά στην επιβλέπουσα της διπλωματικής μου εργασίας, καθηγήτρια Λαμπροπούλου Ευσταθία, καθηγήτρια Κοινωνιολογίας του Παντείου Πανεπιστημίου, με επίκεντρο τον κοινωνικό έλεγχο του εγκλήματος. Της οφείλω ιδιαίτερη ευγνωμοσύνη, καθώς μου έδωσε τη δυνατότητα να ασχοληθώ με αυτό το άκρως ενδιαφέρον και σύγχρονο θέμα, μέσα από το οποίο άντλησα πολύτιμες γνώσεις και πληροφορίες που σίγουρα θα αξιοποιήσω στο μέλλον της επιστημονικής μου πορείας. Η καθοδήγηση της ήταν πάντα κατατοπιστική και υποστηρικτική κατά την συγγραφή και την ευχαριστώ για τις συμβουλές και την εμπιστοσύνη που μου έδειξε.

Επίσης, θα ήθελα να ευχαριστήσω τους πολύ κοντινούς μου ανθρώπους, οι οποίοι με τη συναισθηματική και ψυχολογική υποστήριξη που μου προσέφεραν όλον αυτόν τον καιρό, καθώς και με τη διαρκή πίστη που μου έδειχναν, με βοήθησαν να φέρω εις πέρας αυτό το ιδιαίτερα απαιτητικό αλλά εξαιρετικά ενδιαφέρον εγχείρημα, τη συγγραφή της διπλωματικής μου εργασίας.

Πίνακας περιεχομένων

Περίληψη.....	σελ. 1
Abstract.....	σελ. 2
1. Πρόλογος.....	σελ. 3
2. Διαδίκτυο και Darknet.....	σελ. 4
2.1. Τεχνολογία, Διαδίκτυο και Έγκλημα.....	σελ. 4
2.1.1. Το διαδικτυακό έγκλημα.....	σελ. 6
2.1.2. SCAREM.....	σελ. 7
2.2. Darknet – Ιστορική αναδρομή.....	σελ. 8
2.2.1. Η ανωνυμία στο darknet.....	σελ. 10
3. Το οργανωμένο έγκλημα.....	σελ. 12
3.1. Ιστορική αναδρομή.....	σελ. 12
3.1.1. Η Καμόρα της Ιταλίας.....	σελ. 12
3.1.2. Η Γιακούζα της Ιαπωνίας.....	σελ. 13
3.2. Σύγχρονες όψεις της οργανωμένης εγκληματικότητας.....	σελ. 14
3.2.1. Νομοθετικός ορισμός.....	σελ. 14
3.2.2. Μορφές του οργανωμένου εγκλήματος.....	σελ. 16
4. Ο ρόλος του darknet στο οργανωμένο έγκλημα.....	σελ. 20
4.1. Τα σκοτεινά δωμάτια.....	σελ. 21
4.2. Νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες.....	σελ. 23
4.3. Η ερμηνεία της δράσης του οργανωμένου εγκλήματος στο darknet βάσει εγκληματολογικών θεωριών.....	σελ.28
4.4. Mirroring.....	σελ. 30
4.5. Η δομή του οργανωμένου εγκλήματος στο darknet.....	σελ. 31
4.6. Κατηγορίες εγκλημάτων στο darknet.....	σελ. 35
4.6.1. Διακίνηση ναρκωτικών και πώληση όπλων.....	σελ. 35
4.6.1.1. Επιχείρηση «Spector»	σελ. 37
4.6.2. Πορνογραφία και e-trafficking.....	σελ. 39
4.6.2.1. Υπόθεση Play-Pen.....	σελ. 42
4.6.3. Έγκλημα ως υπηρεσία και κυβερνοέγκλημα.....	σελ. 43
4.6.3.1. Υπόθεση REvil.....	σελ. 45
4.6.4. Hitman for hire.....	σελ. 47

4.6.4.1. Η περίπτωση του Besa Mafia	σελ. 48
5. Επιστημολογικά ζητήματα και δυσκολίες στη μελέτη του οργανωμένου εγκλήματος στο Darknet.....	σελ. 49
5.1. Πληροφόρηση από ΜΜΕ, κρατικούς φορείς και διωκτικές αρχές σελ.	σελ. 50
5.2. Στατιστικές αβεβαιότητες ,έλλειψη εγκυρότητας δεδομένων και μεθοδολογικά ζητήματα.....	σελ. 51
5.3. Νομικά και Ηθικά ζητήματα.....	σελ. 51
5.4. Ο ρόλος της τεχνολογίας.....	σελ. 53
6. Προβλήματα αντιμετώπισης του οργανωμένου εγκλήματος στο darknet από τις αρχές επιβολής του νόμου.....	σελ. 53
6.1. Δυσκολίες εντοπισμού και εξάρθρωσης εγκληματικών οργανώσεων στο Darknet.....	σελ. 53
6.2. Νομοθεσία και διακρατική συνεργασία.....	σελ. 56
6.3. Ο ρόλος της τεχνητής νοημοσύνης.....	σελ. 58
7. Αντιμετώπιση.....	σελ. 61
7.1. Καταπολέμηση του Οργανωμένου Εγκλήματος στο Darknet.....	σελ. 61
7.1.1. Europol.....	σελ. 62
7.1.2. FBI (Federal Bureau of Investigation)	σελ. 64
7.1.3. Interpol.....	σελ. 65
7.1.4. Γραφείο Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC)	σελ. 67
7.2. Διακρατική συνεργασία	σελ.68
7.3. Νομοθεσίες και κανονιστικά πλαίσια.....	σελ. 70
7.4. Τεχνολογίες ανίχνευσης και παρακολούθησης δραστηριοτήτων στο Darknet.....	σελ. 72
8. Επίλογος.....	σελ. 74
Βιβλιογραφία.....	σελ. 76

Περίληψη

Από τα παλαιότερα χρόνια, το οργανωμένο έγκλημα αποτελούσε σημαντικό κίνδυνο για τις κοινωνίες και ήταν ικανό να αποσταθεροποιήσει κράτη και θεσμούς, θέτοντας τις αρχές επιβολής του νόμου σε διαρκή εγρήγορση προκειμένου να το αντιμετωπίσουν. Η δομή, οργάνωση και ιεραρχία του οργανωμένου εγκλήματος το καθιστούσαν παραδοσιακά ιδιαίτερα πολύπλοκο τόσο ως προς την αντιμετώπιση του από τις δικτικές αρχές όσο και ως προς την μελέτη και ανάλυση του από την επιστημονική κοινότητα. Βασικό του χαρακτηριστικό είναι η προσαρμοστικότητα, γεγονός που του επιτρέπει να παραμένει διαχρονικά ενεργό και επίκαιρο. Σήμερα, το οργανωμένο έγκλημα ακολουθεί τις τεχνολογικές εξελίξεις, εκμεταλλευόμενο τις δυνατότητες που προσφέρει η ψηφιακή εποχή προκειμένου να δραστηριοποιηθεί και να εξυπηρετήσει τον βασικό του σκοπό: την επίτευξη κέρδους. Ανάμεσα στα σύγχρονα τεχνολογικά εργαλεία που αξιοποιεί το οργανωμένο έγκλημα, συγκαταλέγεται το darknet, μία «σκοτεινή» περιοχή του διαδικτύου, όπου μπορεί να οργανώνεται, να επικοινωνεί και να διακινεί τις υπηρεσίες του με τη μέγιστη δυνατή ανωνυμία. Χάριν στο darknet, το οργανωμένο έγκλημα, πλέον δραστηριοποιείται σε παγκόσμια κλίμακα, γεγονός που καθιστά την διασυνοριακή δικαστική και αστυνομική συνεργασία, πιο επιτακτική από ποτέ.

Λέξεις-κλειδιά: Οργανωμένο έγκλημα, ανωνυμία, προσαρμογή, παγκόσμια διάσταση, διαδίκτυο, darknet, διαδικτυακό έγκλημα, κυβερνοέγκλημα, διακρατική συνεργασία, ψηφιακή εγκληματολογία, επιστημολογία, κρυπτονομίσματα, τεχνητή νοημοσύνη, τεχνολογία

Abstract

Since ancient times, organized crime has posed a significant threat to societies and has been capable of destabilizing states and institutions, placing law enforcement authorities on constant alert in order to combat it. The structure, organization and hierarchy of organized crime have traditionally made it particularly complex both in terms of its treatment by law enforcement authorities and in terms of its study and analysis by the scientific community. Its main characteristic is adaptability, which allows it to remain vibrant and relevant over time. Today, organized crime follows technological developments, taking advantage of the possibilities offered by the digital age in order to operate and serve its main purpose: making a profit. Among the modern technological tools utilized by organized crime is the darknet, a "dark" area of the internet where it can organize, communicate and distribute its services with the greatest possible anonymity. Thanks to the darknet, the organized network now operates on a global scale, which makes cross-border judicial and police cooperation more imperative than ever.

Key-words: Organized crime, anonymity, adaptation, global dimension, internet, darknet, cybercrime, cybercrime, transnational cooperation, digital forensics, epistemology, cryptocurrencies, artificial intelligence, technology

1. Πρόλογος

Το οργανωμένο έγκλημα, αποτελεί μία από τις σοβαρότερες μορφές εγκληματικής δραστηριότητας με βασικό του χαρακτηριστικό την προσαρμοστικότητα στις εξελίξεις των καιρών, ακολουθώντας γρήγορα την τεχνολογική ανάπτυξη και κατά συνέπεια τη συνεχή εμφάνιση νέων ποικίλων δυνατοτήτων που προσφέρει ο ψηφιακός κόσμος στην εποχή μας. Στις σύγχρονες κοινωνίες, το darknet, ως βασικός παρονομαστής ανωνυμίας και κρυπτογράφησης, έχει οδηγήσει το οργανωμένο έγκλημα σε νέες μορφές επιχειρηματικής δράσης, δηλαδή απόκτησης υψηλού κέρδους, που είναι και ο βασικός του σκοπός, με βασικό πλεονέκτημα τη δυσκολία εντοπισμού των μελών του. Το γεγονός αυτό, με τη μετάβαση από τον παραδοσιακό και κάπως ελέγξιμο από τις διωκτικές αρχές τρόπο δράσης του οργανωμένου εγκλήματος στο οργανωμένο κυβερνοέγκλημα, καλούνται να αντιμετωπίσουν οι υπηρεσίες πρόληψης και καταστολής, οι οποίες οφείλουν να λαμβάνουν με την πάροδο του χρόνου υπόψιν όλο και περισσότερες προκλήσεις και παραμέτρους.

Μπορεί η αρχική σκέψη πίσω από το darknet να εστίαζε στην προστασία της ιδιωτικότητας και την ελευθερία της πληροφορίας, όμως έχει καταλήξει να αποτελεί το βασικό χώρο αλληλοεπίδρασης, επικοινωνίας και δράσης του οργανωμένου εγκλήματος, καθώς έχει τη δυνατότητα να οργανώνεται και να προσφέρει τις υπηρεσίες και τα προϊόντα του με ελάχιστες πιθανότητες εντοπισμού και σύλληψης, αφού βασικό χαρακτηριστικό του darknet είναι η ανωνυμία, οι συναλλαγές με κρυπτονομίσματα και η έλλειψη ελέγχου από διωκτικές αρχές και κυβερνήσεις.

Η παρούσα διπλωματική εργασία, λοιπόν, εξετάζει τη διερεύνηση και τη συμβολή του darknet στη λειτουργία και δράση του οργανωμένου εγκλήματος σήμερα, καθώς και τους τρόπους με τους οποίους τα οργανωμένα εγκληματικά δίκτυα εξαπολύουν τη δράση τους. Επίσης, εξετάζονται οι ερευνητικές και κατασταλτικές δυσκολίες των ενδιαφερόμενων, καθώς από τη μία υπάρχει ιδιαίτερα μεγάλη επιστημονική δυσχέρεια να μελετηθεί το φαινόμενο με ακρίβεια και αξιοπιστία και από την άλλη υπάρχουν προβλήματα εντοπισμού, προσέγγισης και εξάρθρωσης των εγκληματικών δικτύων, ανάγκη συνεχούς θεσμικής και τεχνολογικής προόδου προκειμένου να επιτευχθεί τόσο πρόληψη όσο και αντιμετώπιση, αλλά και έμφαση στην αποτελεσματική διακρατική και υπερκρατική συνεργασία.

Στο πρώτο μέρος, η μελέτη εστιάζει σε μία γενική εικόνα της τεχνολογίας και της σημασίας του διαδικτύου στην ανάπτυξη σύγχρονων μορφών ψηφιακού εγκλήματος, στο δεύτερο μέρος αναλύεται το φαινόμενο του οργανωμένου εγκλήματος, με βασικό στόχο την πλήρη κατανόηση του φαινομένου και τελικά το τελευταίο μέρος αντανακλά στην αλληλεπίδραση διαδικτύου και οργανωμένου εγκλήματος, στο ψηφιακό και άκρως πολύπλοκο περιβάλλον του darknet. Μέσα από την ανάλυση παραδειγμάτων, παρεμβάσεων των διωκτικών αρχών αλλά και επιστημονικών προκλήσεων, επιχειρείται να δοθεί μία συνολική άποψη σχετικά με το παρόν ζήτημα ώστε να κατανοηθεί με τον καλύτερο δυνατό τρόπο.

2. Διαδίκτυο και Darknet

2.1. Τεχνολογία, Διαδίκτυο και Έγκλημα

Από την αρχαιότητα έως σήμερα, η τεχνολογία υπήρξε η κινητήριος δύναμη της ανθρώπινης εξέλιξης, διαμορφώνοντας τη ζωή των ανθρώπων και διευκολύνοντας καθημερινές δραστηριότητες που αφορούν την επικοινωνία, τη ψυχαγωγία, την παραγωγή και γενικότερα την επιβίωση. Ο ρόλος και η επιρροή της τεχνολογίας εξελίσσονται όλο και περισσότερο με το πέρασ του χρόνου, δημιουργώντας την ανάγκη επιστημονικής ή μη κατανόησης των θετικών ή αρνητικών επιπτώσεων της τεχνολογίας αλλά και της αξιοποίησης της για την επίλυση των ζητημάτων που προκύπτουν από τη χρήση της. Η τεχνολογία, ως όρος, προέρχεται από τις λέξεις «τέχνη» και «λογία» (=λόγος) και περιγράφει το άθροισμα των τεχνικών, των δεξιοτήτων και των διαδικασιών που αξιοποιούνται από τους ανθρώπους προκειμένου να παράξουν αγαθά ή υπηρεσίες, με σκοπό να βελτιώσουν τη ζωή τους και να επιτύχουν τους βασικούς προς υλοποίηση στόχους τους. Η αδιάκοπη εξέλιξη της τεχνολογίας, λοιπόν, δεν έχει μόνο βελτιώσει τις συνθήκες διαβίωσης, αλλά έχει επίσης οδηγήσει σε επαναστατικές αλλαγές στον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν, εργάζονται και αλληλεπιδρούν, με πιο χαρακτηριστικό παράδειγμα την ανάπτυξη και τη διάδοση του διαδικτύου.¹

¹ Lane A., What is technology?, 2019, <https://www.open.edu/openlearn/science-maths-technology/engineering-technology/what-technology>

Το διαδίκτυο αποτελεί το πιο σημαντικό επίτευγμα της τεχνολογίας, καθώς μετά την ανακάλυψη και λειτουργία του, έχει μεταβληθεί πλήρως η καθημερινή ζωή των ανθρώπων. Πρόκειται για ένα παγκόσμιο σύστημα διασυνδεδεμένων μεταξύ τους δικτύων υπολογιστών, οι οποίοι χρησιμοποιώντας μία καθιερωμένη ομάδα πρωτοκόλλων, που ακούει στο όνομα TCP/IP, μπορούν και εξυπηρετούν παγκόσμια, καθημερινώς, πολλούς δισεκατομμύρια χρήστες.

Οι διασυνδεδεμένοι λοιπόν μεταξύ τους υπολογιστές, ανταλλάσσουν μεταξύ τους μηνύματα με την μορφή των πακέτων δεδομένων (Data Packets), σε επίπεδο υλικού και λογισμικού, μέσα σε ένα κοινό δίκτυο επικοινωνίας, το οποίο λέγεται διαδίκτυο.

Αρχικά, το διαδίκτυο αξιοποιήθηκε ως ένα δίκτυο επικοινωνίας ανάμεσα στις στρατιωτικές δυνάμεις των ΗΠΑ κατά την διάρκεια του Ψυχρού Πολέμου με την Σοβιετική Ένωση.

Το πρώτο διαδίκτυο, γνωστό ως ARPANET, λειτούργησε το 1969 συνδέοντας τέσσερις υπολογιστές από τέσσερα πανεπιστήμια μεταξύ τους. Το 1973, οι τέσσερις υπολογιστές έγιναν είκοσι τρεις και τότε λειτούργησε για πρώτη φορά το ηλεκτρονικό ταχυδρομείο.

Λίγο αργότερα και συγκεκριμένα το 1989, ο καθηγητής, του ερευνητικού ιδρύματος Cern, Tim Berners-Lee, αξιοποίησε τον κυβερνοχώρο για πρώτη φορά με τρόπο όχι πολύ διαφορετικό από αυτό που γνωρίζουν οι άνθρωποι σήμερα.²

Ο κυβερνοχώρος, έχει κάνει τη ζωή πιο αποτελεσματική, λειτουργική και γρήγορη. Αναφορικά με τα προηγούμενα χρόνια, έχει διευκολυνθεί η επικοινωνία, η άντληση πληροφοριών, το εμπόριο, η εκπαίδευση, η αλληλεπίδραση μεταξύ των ανθρώπων κ.α., διαμορφώνοντας τον τρόπο που οι άνθρωποι ζουν, εργάζονται και ψυχαγωγούνται.³

Με το πέρασ του χρόνου οι άνθρωποι συνεχίζουν να εισέρχονται στον κυβερνοχώρο και να πραγματοποιούν όλο και περισσότερες καθημερινές δραστηριότητες διαδικτυακά, γεγονός που έχει οξύνει τις ευκαιρίες για

² PCEDU, Η ιστορία του διαδικτύου, 2022, <https://www.pcedugr.com/post/η-ιστορία-του-διαδικτύου>

³ AnuMeena Care Foundation, The transformative impact of the Internet on Society, 2023 <https://www.linkedin.com/pulse/transformative-impact-internet-society-anumeenacare#:~:text=Since%20its%20inception%2C%20the%20internet,areas%20impacted%20by%20the%20internet.>

κυβερνοεγκλήματα, τα οποία περιλαμβάνουν τόσο νέους τύπους και μορφές εγκλημάτων όσο και νέες μεθόδους διάπραξης των ήδη υπαρχόντων και «παραδοσιακών» εγκλημάτων.

2.1.1. Το διαδικτυακό έγκλημα

Το διαδικτυακό έγκλημα αποτελεί μία υποκατηγορία του ηλεκτρονικού εγκλήματος. Η διαφορά μεταξύ τους έγκειται κυρίως στο πεδίο εφαρμογής τους. Το ηλεκτρονικό έγκλημα αφορά το έγκλημα που λαμβάνει χώρα μέσω υπολογιστών και συστημάτων, ανεξαρτήτως αν θα γίνει χρήση του διαδικτύου ή όχι, ενώ το διαδικτυακό έγκλημα, αφορά εγκλήματα που έχουν πραγματοποιηθεί μέσω του διαδικτύου. Ένα χαρακτηριστικό παράδειγμα είναι η παιδική πορνογραφία, η οποία μπορεί να τελεστεί τόσο «online» όσο και «offline», ωστόσο το διαδίκτυο διευκολύνει ιδιαιτέρως τη διάδοση της.⁴

Τα βασικά χαρακτηριστικά των διαδικτυακών εγκλημάτων είναι ο διασυνοριακός χαρακτήρας, καθώς τα εγκλήματα στον κυβερνοχώρο μπορούν να διαπραχθούν οπουδήποτε, χωρίς γεωγραφικούς περιορισμούς με αποτέλεσμα τη δυσκολία εύρεσης του δράστη, η ανωνυμία, οι δράστες συχνά παραμένουν ανώνυμοι ή χρησιμοποιούν ψευδώνυμα καθιστώντας ιδιαίτερη δύσκολη την ανίχνευση τους και τέλος, η ευκολία πρόσβασης αφενός, αλλά και η τεχνολογική πολυπλοκότητα αφετέρου, καθώς πολλές φορές τα εγκλήματα αυτά απαιτούν εξειδικευμένες γνώσεις και προηγμένα τεχνικά μέσα, τα οποία θα αναλυθούν στη συνέχεια. Τα εγκλήματα αυτά φέρουν πολυδιάστατες επιπτώσεις αφού επηρεάζουν οικονομικούς, κοινωνικούς, προσωπικούς αλλά και πολιτικούς φορείς.⁵

⁴ LawSpot.gr, Ηλεκτρονικό Έγκλημα, 2014, <https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/ilektroniko-egklima>

⁵ Δαλακούρα Ι. Θεοχάρης, Ηλεκτρονικό Έγκλημα, 2019, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης, σελ. 5-6

2.1.2. SCAREM

Οι David M. Newman και Simon Clarke, καθηγητές Κοινωνιολογίας, συνόψισαν τους παράγοντες που γεννούν το διαδικτυακό έγκλημα στο ακρώνυμο «SCAREM», στο οποίο το «S» συμβολίζει την αγγλική λέξη «Stealth», δηλαδή την ευκολία τέλεσης εγκλημάτων στον κυβερνοχώρο, το «C» τη λέξη «Challenge», καθώς το διαδικτυακό έγκλημα αποτελεί πρόκληση για τους εν προκειμένω δράστες να δοκιμάσουν τις ικανότητες και δυνατότητες τους, το «A» αφορά την ανωνυμία («Anonymity»), που συνδέεται άμεσα με την πιθανότητα διαφυγής των δραστών λόγω του ιδιαίτερα δύσκολου χαρακτήρα ως προς τον εντοπισμό τους, το «R» («Reconnaissance») συνάδει με τον αντίστοιχο στρατιωτικό όρο, όπου αναγνώριση του στόχου σημαίνει καλή γνώση του στόχου, το οποίο φανερά απαιτεί τη λήψη εξειδικευμένων γνώσεων και προσαρμοσμένη δράση για να επιτευχθεί, το «E» αντιπροσωπεύει το «Escape», που είναι συναφές με την ανωνυμία που επιτρέπει τη διαφυγή του δράστη και τέλος, το «M» παραπέμπει στη λέξη «Multiplicity» και συμβολίζει την πολλαπλή δράση σε πολλαπλά θύματα ταυτοχρόνως.

Βλέπουμε, λοιπόν, πως η ευκολία πρόσβασης στον κυβερνοχώρο, η ανωνυμία, η όλο και αυξανόμενη ταχύτητα και η μαζικότητα της επικοινωνίας αποτελούν ορισμένα χαρακτηριστικά που διευκολύνουν ιδιαιτέρως την τέλεση διαδικτυακών εγκλημάτων. Οι δράστες έχουν τη δυνατότητα να δράσουν σε βάρος απροσδιόριστου αριθμού θυμάτων, σε οποιαδήποτε τοποθεσία και οποτεδήποτε το επιθυμούν.⁶ Η ραγδαία εξάπλωση των διαδικτυακών εγκλημάτων, σε συνδυασμό με τις αυξανόμενες δυσκολίες εντοπισμού των δραστών και την συνεχή τεχνολογική πρόοδο, έχουν δημιουργήσει συνθήκες όπου η εγκληματική δραστηριότητα μπορεί να ανθίσει σε περιβάλλοντα με περιορισμένη ρυθμιστική παρέμβαση. Αυτές οι συνθήκες ενδυναμώνονται από τη δυνατότητα ανωνυμίας και το αυξημένο επίπεδο προστασίας των χρηστών, γεγονός που καθιστά την καταπολέμηση αυτών των φαινομένων ιδιαίτερα δύσκολη. Στο επίκεντρο αυτών των εξελίξεων βρίσκεται το darknet.

⁶ Ζαραφονίτου Χ., Κουμεντάκη Ε. και Ερευνητική Ομάδα Φοιτητών Κοινωνιολογίας Παντείου Πανεπιστημίου, Θυματοποίηση και φόβος του εγκλήματος των φοιτητών χρηστών του διαδικτύου, 2024, https://criminology.panteion.gr/files/444/Internet_ZARAFONITOY.pdf

2.2. Darknet – Ιστορική αναδρομή

Στο πλαίσιο της σύγχρονης διαδικτυακής πραγματικότητας, το darknet αναδεικνύεται ως ένας από τους πιο αδιευκρίνιστους και επικίνδυνους τομείς του Παγκόσμιου Ιστού, όπου οι χρήστες μπορούν να διασφαλίσουν την πλήρη ανωνυμία τους μέσω ειδικών δικτύων και λογισμικού. Το darknet, λοιπόν, αποτελείται από σκοτεινά δίκτυα τα οποία εμπεριέχονται στον Παγκόσμιο Ιστό και απαιτεί συγκεκριμένο λογισμικό και ρυθμίσεις για να χρησιμοποιηθεί. Μέσω του darknet, οι υπολογιστές μπορούν να επικοινωνούν μεταξύ τους και να ανταλλάσσουν πληροφορίες ανώνυμα, χωρίς να αποκαλύπτουν ποτέ τα άτομα την ταυτότητα ή την τοποθεσία τους. Δημοφιλή τέτοια δίκτυα αποτελούν το Tor, το Hiphenate, το I2P και το Riffle.

Χρησιμοποιείται από διάφορους ανθρώπους, όπως ακτιβιστές και δημοσιογράφους που θέλουν να προστατεύσουν την ανωνυμία τους, ερευνητές που μελετούν εγκληματικά δίκτυα και άτομα που αναζητούν ιδιωτικότητα. Ωστόσο, φιλοξενεί και παράνομες δραστηριότητες, όπως αγοραπωλησίες ναρκωτικών, όπλων, δεδομένων κ.α. Το darknet προωθείται τόσο για την ανωνυμία και την ελευθερία λόγου που προσφέρει όσο και για τις ευκαιρίες κέρδους μέσω παρανομιών. Παρότι συνδέεται συχνά με την εγκληματικότητα, υπάρχουν και νόμιμες χρήσεις, όπως η ανώνυμη πλοήγηση και η παράκαμψη περιορισμών σε χώρες με αυστηρά καθεστώτα, περιορισμένη ελευθερία λόγου και έντονη λογοκρισία, το whistleblowing, δηλαδή η ανώνυμη καταγγελία αυθαιρεσιών ή καταγγελιών στο χώρο εργασίας ή η ερευνητική δραστηριότητα. Η ανωνυμία του το καθιστά διφορούμενο εργαλείο, με θετικές και αρνητικές πλευρές.⁷

Ο όρος "darknet" εμφανίστηκε για πρώτη φορά τη δεκαετία του '70 στο πλαίσιο του ARPANET, του προδρόμου του σύγχρονου διαδικτύου, όπως προαναφέρθηκε. Χρησιμοποιήθηκε για να περιγράψει δίκτυα που ήταν σκόπιμα απομονωμένα από το κύριο δίκτυο και δεν εμφανίζονταν στις λίστες δρομολόγησης του ARPANET. Ο αρχικός σκοπός αυτών των δικτύων ήταν η διατήρηση της ασφάλειας, η ελευθερία της πληροφορίας και η αποφυγή μη εξουσιοδοτημένης πρόσβασης.

⁷Egan M., What is the Dark Web, What's on it & How to Access it, 2019, <https://www.techadvisor.com/article/727316/what-is-the-dark-web-whats-on-it-how-to-access-it.html>

Ο όρος εμφανίστηκε ξανά το 2002 μέσα από το διάσημο άρθρο "The Darknet and the Future of Content Distribution", που δημοσιεύτηκε από τέσσερις ερευνητές της Microsoft. Στο άρθρο, το darknet χαρακτηρίστηκε ως ένα σύνολο αποκεντρωμένων, ανώνυμων δικτύων που μπορούσαν να χρησιμοποιηθούν για την ανεξέλεγκτη διανομή ψηφιακού περιεχομένου, συμπεριλαμβανομένης της πειρατείας, δηλαδή της κλοπής ή πλαστογράφησης προγραμμάτων λογισμικού χωρίς άδεια ή εξουσιοδότηση.

Ωστόσο, το darknet με τον τρόπο που το γνωρίζουμε σήμερα, δηλαδή ένα δίκτυο που δεν είναι προσβάσιμο μέσω των συνηθισμένων μηχανών αναζήτησης και απαιτεί ειδικό λογισμικό (όπως το Tor, το I2P ή το Freenet), ξεκίνησε να διαμορφώνεται τη δεκαετία του 1990 και συνεχίστηκε και την επόμενη δεκαετία. Το Tor ξεκίνησε ως ερευνητικό πρόγραμμα του U.S. Naval Research Laboratory γύρω στο 1995 και έγινε γνωστό στο κοινό το 2002. Το Freenet, που επιτρέπει την ανώνυμη διανομή περιεχομένου, αναπτύχθηκε από τον Ian Clarke, Ιρλανδό φοιτητή, το 1999, στο πλαίσιο της πτυχιακής του εργασίας με τίτλο "A Distributed Decentralised Information Storage and Retrieval System" και η μελέτη του αφορούσε πως το διαδίκτυο μπορεί να χρησιμοποιηθεί ανώνυμα με σκοπό τη προστασία της ελευθερίας του λόγου και τη διατήρηση της ιδιωτικότητας.

Η ανωνυμία και η απουσία κεντρικού ελέγχου που προσέφεραν αυτά τα δίκτυα δεν άργησαν να προσελκύσουν και παράνομες δραστηριότητες, καθώς η αποκέντρωση σε συνδυασμό με τη δυσκολία εντοπισμού των χρηστών δημιούργησαν το κατάλληλο πλαίσιο για την ανάπτυξη παράνομων αγορών και εγκληματικών δραστηριοτήτων. Από τις αρχές της δεκαετίας του 2000, το darknet άρχισε να χρησιμοποιείται για την ανταλλαγή παράνομων αγαθών και υπηρεσιών, όπως ναρκωτικά, όπλα, πλαστά έγγραφα και υπηρεσίες hacking. Η δημιουργία του Silk Road το 2011 αποτέλεσε σημείο καμπής, καθώς ήταν η πρώτη μεγάλη αγορά στην οποία αξιοποιήθηκαν το Tor και τα κρυπτονομίσματα, καθιστώντας επιτρεπτές ανώνυμες συναλλαγές χωρίς κρατικό έλεγχο.

⁸ Επρόκειτο, με λίγα λόγια, για μία «μαύρη» αγορά, η οποία, μάλιστα, αποκαλείται ως η «Amazon» ή το «Ebay» των παράνομων εξαρτησιογόνων ουσιών.

⁸ Stoval J., Darknet, 2023, <https://www.britannica.com/technology/computer-security>

2.2.1. Η ανωνυμία στο darknet

Η πρόσβαση στο darknet, είναι ένα εγχείρημα ιδιαίτερα δυσχερές, το οποίο απαιτεί ειδικές γνώσεις προκειμένου κάποιος να «εισέλθει», καθώς η είσοδος δεν μπορεί να πραγματοποιηθεί με απλά λογισμικά προγράμματα, π.χ. Google Chrome ή Safari, αλλά απαιτείται χρήση ειδικών μηχανών αναζήτησης και περιηγητή, διαμόρφωση του εκάστοτε προγράμματος, εγκατάσταση συγκεκριμένων «εργαλείων» και προσθήκη ειδικών ρυθμίσεων προκειμένου να αποκτήσει κάποιος πρόσβαση, όπως το Tor (The Onion Router) και το DuckDuckGo, τα οποία επιτρέπουν την ασφαλή και ανώνυμη πλοήγηση.

Η ανωνυμία σχετίζεται άμεσα με το λεγόμενο IP address (Internet Protocol address), δηλαδή το μοναδικό αριθμό που φέρει μία συσκευή προκειμένου να αναγνωριστεί και να μπορέσει να επικοινωνήσει με άλλους υπολογιστές. Στο darknet, αυτός ο μοναδικός αριθμός εναλλάσσεται διαρκώς, αφού μέχρι να φτάσει στον τελικό διακομιστή, έχει χρησιμοποιήσει IP διευθύνσεις πολλών διαφορετικών συσκευών που χρησιμοποιούν το darknet, οι οποίες μάλιστα βρίσκονται σε πολλές διαφορετικές περιοχές στον κόσμο. Αυτό που επιτρέπει απόκρυψη της πραγματικής τοποθεσίας του χρήστη, είναι το VPN (Virtual Private Network) , καθώς αναδρομολογεί την κίνησή του μέσω διακομιστών σε διαφορετικές χώρες, αποκρύπτοντας τη διεύθυνση IP του και καθιστώντας δύσκολο τον εντοπισμό της πραγματικής γεωγραφικής του θέσης. Οι εναλλαγές αυτές δεν είναι σταθερές και πολλές φορές πραγματοποιούνται το ίδιο δευτερόλεπτο. Όσοι περισσότεροι είναι οι χρήστες στο darknet, τόσο πιο δύσκολη είναι η ανίχνευση των δραστών από τις διωκτικές αρχές και τόσο μεγαλύτερη είναι η ανωνυμία τους. Η διαδικασία αυτή πραγματοποιείται στον περιηγητή «Tor», ο οποίος έχει λάβει την ονομασία του από τα φύλλα επικάλυψης του κρεμμυδιού (onion routing = δρομολόγηση κρεμμυδιού). Ο περιηγητής «Tor» δημιουργεί κρυπτογραφημένα σημεία εισόδου και διαδρομές, εξασφαλίζοντας ότι κάθε κόμβος στο σύστημα μπορεί να αποκρυπτογραφήσει μόνο ένα σημείο των δεδομένων, καθιστώντας σχεδόν ουτοπικό να παρακολουθηθεί κάποιος την πραγματική διαδρομή των δεδομένων. Αυτή η μέθοδος,

γνωστή και ως «Tor over VPN», είναι καθοριστικής σημασίας για τη διατήρηση της ιδιωτικότητας και της ανωνυμίας κατά την πλοήγηση στο darknet.⁹

Η ανωνυμία, όπως προαναφέρθηκε, καθιστά ιδιαίτερα δυσχερή τον εντοπισμό των δραστών και συνεπώς τη σύλληψη και ποινική τους καταδίκη, με αποτέλεσμα τα στατιστικά που προκύπτουν σχετικά με τα εγκλήματα και τους δράστες στο σκοτεινό διαδίκτυο (darknet) να μην είναι καθόλου αντιπροσωπευτικά και να οδηγούν σε λανθασμένα συμπεράσματα. Μεταξύ, λοιπόν, της καταγεγραμμένης εγκληματικότητας, που παρουσιάζουν οι επίσημες στατιστικές της αστυνομίας και της πραγματικής εγκληματικότητας, υπάρχει ένας σκοτεινός αριθμός της εγκληματικότητας, ο οποίος δεν μπορεί να οδηγήσει σε ασφαλή συμπεράσματα καθώς είναι γνωστός μόνο ένας μικρός εμφανής αριθμός εγκλημάτων. Σύμφωνα μάλιστα με τον Andre Davidovich, οι στατιστικές εμπεριέχουν περιορισμούς και η αξία τους έχει σχέση με τη δραστηριότητα και την παρεμβατική ικανότητα των αντίστοιχων υπηρεσιών επιβολής του νόμου. Συνεπώς, το ζήτημα αυτό θα μπορούσε να βελτιωθεί σε έναν βαθμό με περαιτέρω τεχνολογική εξέλιξη και εξειδίκευση των τελευταίων.¹⁰

Συνεπώς, τα άτομα οδηγούνται ευκολότερα στο έγκλημα, καθώς δεν φοβούνται τον εντοπισμό τους.

Η διαρκώς εξελισσόμενη τεχνολογία, λοιπόν, και οι δυνατότητες που προσφέρει το σκοτεινό διαδίκτυο δεν έχουν επηρεάσει μόνο την ατομική παραβατικότητα, αλλά έχουν επίσης δημιουργήσει τις προϋποθέσεις για τη συγκρότηση πιο πολύπλοκων και οργανωμένων δομών. Σε αυτό το περιβάλλον, οι οργανωμένες εγκληματικές ομάδες βρίσκουν πρόσφορο έδαφος για να επεκτείνουν τις δραστηριότητές τους, αξιοποιώντας την ανωνυμία και τα σύγχρονα μέσα για να ενισχύσουν την ισχύ και την επιρροή τους.

⁹ Ozkaya E.,Islam R, Inside the Dark Web,CRC Press, 2019, σελ. 3-24

¹⁰ Ζαραφωνίτου Χ., Εμπειρική Εγκληματολογία, Νομική Βιβλιοθήκη, Β΄ έκδοση, 2004, Νομική Βιβλιοθήκη, σελ. 37-39

3. Το οργανωμένο έγκλημα

3.1. Ιστορική αναδρομή

Στην ιστορία του οργανωμένου εγκλήματος, η Καμόρα της Ιταλίας, η Γιακούζα της Ιαπωνίας και άλλες αποτελούν κάποιες από τις πρώιμες μορφές του οργανωμένου εγκλήματος. Αυτές οι ομάδες, που συγκροτήθηκαν σε διαφορετικές γεωγραφικές τοποθεσίες και πολιτισμικά περιβάλλοντα, θεωρούνται πρόδρομοι του σύγχρονου οργανωμένου εγκλήματος, δεδομένου ότι καθιέρωσαν τις δομημένες και ιεραρχημένες εγκληματικές οργανώσεις. Τα χαρακτηριστικά τους, όπως η στενή συνεργασία, η ιεραρχία και η στρατηγική διαχείριση εγκληματικών δραστηριοτήτων, αποτέλεσαν το θεμέλιο πάνω στο οποίο θα οικοδομηθούν οι σύγχρονες εγκληματικές οργανώσεις.

3.1.1. Η Καμόρα της Ιταλίας

Η Καμόρα αποτελεί εγκληματική οργάνωση της Ιταλικής μαφίας, η οποία προέκυψε στην περιοχή της Καμπανίας στη Νάπολη.

Αρχικά, η Καμόρα (Camorra: “caro” = αρχηγός + “morra” = παιχνίδι) εμφανίστηκε τον 18^ο αιώνα στη Νάπολη, όταν δημιουργήθηκαν «σπίτια» για τυχερά παιχνίδια που λειτουργούσαν ως πεδίο δράσης μικρών συμμοριών.

Μεταξύ του 1799 και του 1815, η Καμόρα από απλές συμμορίες που δρούσαν ανεξάρτητα, βασισμένες σε κλοπές και εκβιασμούς, απέκτησε ισχυρότερη επιρροή λόγω των κοινωνικών και πολιτικών αναταραχών που επικρατούσαν εκείνη την περίοδο στη Νάπολη και εξελίχθηκε σε οργανωμένη ομάδα με κυριαρχία.

Τον 19^ο αιώνα η Καμόρα συνεργάστηκε με την πολιτική εξουσία, ενώ το 1861 κατέληξε να ελέγχει την πολιτική και την οικονομία της Νάπολης. Λειτουργούσε ως ένα σύστημα φατριών, οι οποίες χρησιμοποιούσαν την εξουσία τους, με σκοπό να εκμεταλλεύονται τις τοπικές κοινωνίες και ουσιαστικά κάθε οικογένεια (φατρία) ήλεγχε και μία περιοχή.

Τον 20^ο αιώνα η Καμόρα ήρθε αντιμέτωπη με απώλειες λόγω μαζικών συλλήψεων και δικαστικών διωγμών και έτσι αναγκάστηκε να αλλάξει μορφή και να προσαρμοστεί. Από

μικρές, τοπικές εγκληματικές ,λοιπόν, ομάδες μετασχηματίστηκε σε ένα αποκεντρωμένο δίκτυο αυτόνομων «φατριών», που δραστηριοποιούνται σε ευρύτερη κλίμακα και σε πιο οργανωμένα εγκλήματα, όπως το λαθρεμπόριο και το ξέπλυμα βρώμικου χρήματος.

Παρ' όλα αυτά η επιρροή της εξακολουθεί να λαμβάνει χώρα έως και σήμερα.¹¹

3.1.2. Η Γιακούζα της Ιαπωνίας

Η Γιακούζα αποτελεί τη μεγαλύτερη εγκληματική οργάνωση τους είδους της με 150.000 μέλη παγκοσμίως. Είναι γνωστή για τους αυστηρούς κώδικες συμπεριφοράς και την οργανωμένη φύση της.

Ο όρος Γιακούζα (ヤクザ) στα Ιαπωνικά σημαίνει «8-9-3» που αποτελεί το χειρότερο φύλλο στο Ιαπωνικό παχνίδι Χάνα Φούντα (花札), παρεμφερές του γνωστού παιχνιδιού Μπλακ Τζακ, όπου ο παίκτης για να κερδίσει πρέπει να συγκεντρώσει 19 πόντους. Σταδιακά, όμως, ο όρος συνδέθηκε με εκείνο του «απόκληρου».

Η Γιακούζα προέρχεται από πρώην Σαμουράι με εκκεντρική εμφάνιση και συμπεριφορά, τους Kabuki-mono (かぶき者). Ωστόσο, όταν έχασαν την κοινωνική τους θέση, μετά την ενοποίηση της Ιαπωνίας, καθώς η ειρήνη μείωσε την ανάγκη για πολεμιστές με αποτέλεσμα να μείνουν χωρίς πόρους, στράφηκαν στο έγκλημα, κυρίως ληστείες και εκβιασμούς.

Στη σύγχρονη, πάλι, εποχή οι Γιακούζα κατέληξαν να προέρχονται από 2 ομάδες, που εμφανίστηκαν την περίοδο των Έντο (徳川時代) (1603-1868). Η πρώτη ήταν οι Tekiya (テキヤ), έμποροι που πουλούσαν λαθραία και χαμηλής ποιότητας αντικείμενα στην αγορά και έσπευσαν να οργανωθούν προκειμένου να προστατεύσουν τις «υπηρεσίες» τους. Έτσι, απέκτησαν ισχύ και έτσι κατέληξαν να έχουν την άδεια να κυκλοφορούν φέροντας σπαθιά νόμιμα, όπως οι Σαμουράι συνήθιζαν να κάνουν στο παρελθόν. Η

¹¹ Tikkanen A., Camorra, 1998, <https://www.britannica.com/topic/organized-crime>

δεύτερη ομάδα ήταν οι Bakuto (バクト), οι οποίοι ασχολούνταν με τα παράνομα τυχερά παιχνίδια και την παροχή προστασίας.

Αργότερα, το 1930, όταν οι κοινωνικές και οικονομικές συνθήκες μεταβλήθηκαν, στράφηκαν στο οργανωμένο έγκλημα και αμέσως μετά τον Β' Παγκόσμιο Πόλεμο ανέλαβαν τις παράνομες αγορές της Ιαπωνίας.

Σε αντίθεση με την Καμόρα, η Γιακούζα δρα ανοιχτά, με γνωστά γραφεία. Παραδοσιακά ασχολείται με την πορνεία, τα τυχερά παιχνίδια, εκβιασμούς και τοκογλυφία, αλλά πλέον επενδύει σε περιουσιακά στοιχεία και το χρηματιστήριο. Μεγάλο μέρος των εσόδων της προέρχεται από την εμπορία πορνογραφικού υλικού, το λαθρεμπόριο όπλων και τη διακίνηση μεταμφεταμίνης.¹²

3.2. Σύγχρονες όψεις της οργανωμένης εγκληματικότητας

3.2.1. Νομοθετικός ορισμός

Ο ορισμός του οργανωμένου εγκλήματος στην ελληνική νομοθεσία περιλαμβάνεται στο άρθρο 187 του Ποινικού Κώδικα, ο οποίος έχει διαμορφωθεί με βάση τη Σύμβαση του Πατέρμο, οπότε αποτελεί το κύριο διεθνές νομικό πλαίσιο για την καταπολέμηση του οργανωμένου εγκλήματος.

Σύμφωνα με το άρθρο 2 της Σύμβασης, ως «Οργανωμένη εγκληματική ομάδα» νοείται «δομημένη ομάδα τριών ή περισσότερων προσώπων που υπάρχει για κάποια χρονική περίοδο και ενεργεί με κοινό σκοπό τέλεσης ενός ή περισσότερων σοβαρών εγκλημάτων, προκειμένου να ποριστεί αμέσως ή εμμέσως οικονομικό ή άλλο υλικό όφελος».

Επιπλέον, ορίζεται ότι «σοβαρό έγκλημα» είναι κάθε αδίκημα που τιμωρείται με ποινή κάθειρξης τουλάχιστον τεσσάρων ετών, ενώ η έννοια της «δομημένης ομάδας» δεν απαιτεί τυπικά προσδιορισμένους ρόλους. Παράλληλα, η Σύμβαση εισάγει έννοιες, όπως εκείνη της «περιουσίας», του «προϊόντος εγκλήματος», καθώς και τις διαδικασίες που

¹² Kaplan D.E., Dubro A., Yakuzo - Japan's Criminal Underworld, University of California Press, 2003, σελ. 31-48

προβλέπονται σχετικά με τη «δέσμευση» και την «κατάσχεση» των περιουσιακών στοιχείων που έχουν αποκτηθεί από εγκληματικές δραστηριότητες. Επιπλέον, καθορίζεται η έννοια του «βασικού εγκλήματος», από το οποίο προκύπτουν τα μη νόμιμα κέρδη, τα οποία ενδεχομένως θα επιχειρηθεί να νομιμοποιηθούν, όπως ορίζεται στο άρθρο 6 της Σύμβασης. Επίσης, προβλέπεται η τεχνική της «ελεγχόμενης παράδοσης», όπου παράνομα ή ύποπτα φορτία επιτρέπεται να διακινούνται με τη γνώση και την επίβλεψη των αρμόδιων αρχών, με σκοπό τη διερεύνηση εγκλήματος και τον εντοπισμό των προσώπων που εμπλέκονται στην τέλεση αυτού. Τέλος, η Σύμβαση περιλαμβάνει τον «Περιφερειακό οργανισμό οικονομικής ενοποίησης», ο οποίος αποτελείται από κράτη που έχουν μεταβιβάσει αρμοδιότητα για ζητήματα που αφορά η παρούσα Σύμβαση.¹³

Σύμφωνα, πάλι, με το άρθρο 187 Π.Κ., όποιος συγκροτεί ή εντάσσεται ως μέλος σε μια επιχειρησιακά δομημένη και με διάρκεια εγκληματική οργάνωση τριών ή περισσότερων μελών, που επιδιώκει την τέλεση κακουργημάτων, τιμωρείται με κάθειρξη έως 10 έτη και χρηματικό πρόστιμο. Όποιος ηγείται της εγκληματικής ομάδας τιμωρείται με κάθειρξη, ενώ όποιος οργανώνει ή στρατολογεί άλλα πρόσωπα για τη διάπραξη αυτών των εγκλημάτων τιμωρείται με φυλάκιση το λιγότερον έξι μηνών. Σε περίπτωση που η οργάνωση επιδιώκει οικονομικό όφελος ή απειλεί τη ζωή, τη σωματική ακεραιότητα ή την ανηλικότητα, η ποινή μπορεί να φτάσει τα τρία έτη φυλάκισης.¹⁴ Επιπλέον, με κάθειρξη τουλάχιστον τριών ετών και χρηματική ποινή τιμωρείται όποιος παρέχει στα μέλη της οργάνωσης οποιοδήποτε είδος περιουσιακών στοιχείων, πληροφοριών ή άλλων μέσων που διευκολύνουν την εγκληματική της δράση.¹⁵ Τέλος, το άρθρο 187 Π.Κ. έχει υπερεθνική ισχύ, καθώς οι διατάξεις των παραγράφων 1,2 και 4 του άρθρου 187 εφαρμόζονται και όταν οι προβλεπόμενες σε αυτό αξιόποινες πράξεις τελέσθηκαν στην αλλοδαπή από ημεδαπό ή στρέφονταν κατά Έλληνα πολίτη ή κατά

¹³ Ν. 3875/2010, Κύρωση και εφαρμογή της Σύμβασης των Ηνωμένων Εθνών κατά του Διεθνικού Οργανωμένου Εγκλήματος και των τριών Πρωτοκόλλων αυτής και συναφείς διατάξεις. ,ΦΕΚ Α' 158/20.9.2010, άρθρο 2, <https://www.lawspot.gr/nomikes-pliροφοries/nomothesia/n3875-2010/arthro-2-nomos-3875-2010>

¹⁴ Όπως τροποποιήθηκε με την Παρ. 1 άρθρ 72 Ν. 4908/2022, ΦΕΚ Α' /52/11.3.2022, https://www.kodiko.gr/nomologia/download_fek?f=fek/2022/a/fek_alpha_52_2022.pdf&t=b86065948aec4e9ff14e17e1b339c68a

¹⁵ Όπως τροποποιήθηκε με την Παρ.9 άρθρ. 3 Ν. 4637/2019, ΦΕΚ Α' 180/18.11.2019, https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/a/fek_alpha_180_2019.pdf&t=50a1accd8eddc3daf21d00bef6b18160

νομικού προσώπου που εδρεύει στην ημεδαπή ή κατά του Ελληνικού Κράτους, ακόμη και αν αυτές δεν είναι αξιόποινες κατά τους νόμους της χώρας στην οποία τελέσθηκαν.¹⁶¹⁷

Τέλος, στις περιπτώσεις καταδίκης για αξιόποινες πράξεις του άρθρου 187, καθώς και για συναφή αδικήματα που συνεκδικάστηκαν με την ίδια απόφαση, η ποινή δεν αναστέλλεται ούτε μετατρέπεται με κανέναν τρόπο, τυχόν ασκηθείσα έφεση δεν έχει αναστέλλουσα ισχύ, εκτός αν το δικαστήριο, σε περίπτωση καταδίκης για το πλημμέλημα της παραγράφου 3 και τα συναφή πλημμελήματα ή κακουργήματα τα οποία επισύρουν πρόσκαιρες στερητικές της ελευθερίας ποινές, κρίνει με ειδική αιτιολογία ότι πρέπει να χορηγηθεί η ανασταλτική δύναμη της έφεσης. Στη τελευταία περίπτωση επιβάλλονται υποχρεωτικά οι κατάλληλοι περιοριστικοί όροι.¹⁸

3.2.2. Μορφές του Οργανωμένου Εγκλήματος

Το οργανωμένο έγκλημα αποτελεί μια από τις μεγαλύτερες απειλές για τη δημόσια ασφάλεια, καθώς δραστηριοποιείται μέσα από πολύπλοκες δομές και ευρύτατα δίκτυα που επηρεάζουν κοινωνίες και κράτη. Παραδοσιακά, οι οργανωμένες εγκληματικές ομάδες χαρακτηρίζονται από αυστηρή δομή και ιεραρχία, μακροχρόνια διάρκεια και σταθερούς εσωτερικούς κανόνες που εξασφαλίζουν τη συνοχή και την επιβίωσή τους στο χρόνο.¹⁹

Η δομή αν και δεν είναι απαραίτητα συγκεκριμένη και διαφέρει από ομάδα σε ομάδα, τηρεί κατά κύριο λόγο την εξής μορφή. Στην κορυφή βρίσκεται ο αρχηγός (boss) , ο οποίος δίνει εντολές, οι οποίες διαβιβάζονται από τον υπαρχηγό στα υπόλοιπα μέλη της ομάδας. Δίπλα στον αρχηγό βρίσκεται ο σύμβουλος (consigliere ή consultant) , ο οποίος τον

¹⁶ Ν. 4619/2019, άρθρο 187, Κύρωση του Ποινικού Κώδικα, ΦΕΚ Α' 95/11.06.2019
<https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-187-poinikos-kodikas-nomos-4619-2019-egklimatiki>

¹⁷ Όπως τροποποιήθηκε με την Παρ. 10 αρθρ. 3 Ν. 4637/2019, Τροποποιήσεις Ποινικού Κώδικα, Κώδικα Ποινικής Δικονομίας και συναφείς διατάξεις, ΦΕΚ Α' 180/18.11.2019,
https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/a/fek_α_180_2019.pdf&t=50α1accd8eddc3dαf21d00bef6b18160

¹⁸ Όπως τροποποιήθηκε με το αρθρ. 37 Ν. 5090/2024, Εκσυγχρονισμός του νομοθετικού πλαισίου για την πρόληψη και την καταπολέμηση της ενδοοικογενειακής βίας, ΦΕΚ Α'/30/24.2.24,
https://www.kodiko.gr/nomologia/download_fek?f=fek/2024/a/fek_α_30_2024.pdf&t=b3d97e1c1ca002298f8a57359b257b4d

¹⁹ Σταμούλη Ε., Εγκλήματα των ισχυρών : Διαφθορά , οικονομικό και οργανωμένο έγκλημα, σελ. 222 επ.

καθοδηγεί αλλά δεν βρίσκεται στην παραδοσιακή ιεραρχία της ομάδας και δεσμεύεται με τον κανόνα της σιωπής, που αφορά την εχεμύθεια μεταξύ όλων των μελών. Κάτω από τον αρχηγό βρίσκεται ο υπαρχηγός (underboss) , ο οποίος μπορεί να λαμβάνει κάποιες πρωτοβουλίες και να δίνει κάποιες διαταγές στα κατώτερα μέλη, πάντοτε, όμως, ακολουθώντας τις εντολές του αρχηγού.

Στη συνέχεια, είναι οι βαθμοφόροι²⁰ (caroregime), όπου κάθε βαθμοφόρος έχει συγκεκριμένη αποστολή και αρμοδιότητα και ο ρόλος τους είναι η διοίκηση των στρατιωτών. Τέλος, οι στρατιώτες (soldiers) είναι τα άτομα, της οργάνωσης που αναλαμβάνουν παράνομες δράσεις , όπως εκβιασμούς, επιθέσεις κλπ, τις λεγόμενες «βρώμικες δουλειές».²¹

Στο οργανωμένο έγκλημα υπάρχει επιχειρησιακός χαρακτήρας , λειτουργεί δηλαδή σαν μία επιχείρηση με αδιάκοπη και αδιάλειπτη δραστηριότητα. Σύμφωνα με την επιχειρηματική θεωρία, στις υστερό-καπιταλιστικές οικονομίες, το οργανωμένο έγκλημα ακολουθεί τους ίδιους τρόπους ανάπτυξης με τις νόμιμες επιχειρήσεις, ακολουθώντας συστηματοποιημένες πρακτικές ως προς τη μεταφορά, τη διάθεση και την προώθηση των προϊόντων της, αλλά και την τοποθέτηση των κεφαλαίων της, θέτοντας το συγκεκριμένο σύστημα σε μία ισορροπία. Οι δομικοί κανόνες, μίας εγκληματικής οργάνωσης, πάλι, υποστηρίζουν πως ο τρόπος διάρθρωσης και κατανομής των εργασιών, ο συντονισμός της δράσης, το πρόγραμμα δράσης και οι κανόνες,, η πολυπλοκότητα κ.α. , αποτελούν μεταβλητά στοιχεία και προσαρμόζονται ανάλογα με το περιβάλλον που εντάσσονται. Επίσης, οι τεχνικές, για τη στρατολόγηση προσωπικού, την προώθηση των συμφερόντων και τη μεγιστοποίηση των κερδών , ο έλεγχος του ανταγωνισμού και η συγκάλυψη των δραστηριοτήτων είναι ίδιες με τις νόμιμες επιχειρήσεις, με κύριο γνώρισμα του επιχειρησιακού χαρακτήρα τους την επιδίωξη οικονομικού κέρδους, το οποίο αποτελεί τον βασικό τους σκοπό.

Συχνά, μάλιστα, παρατηρείται και μερική «απασχόληση» με τα άτομα να μην αποτελούν βασικά μέλη της οργάνωσης, αλλά να επιστρατεύονται για την τέλεση συγκεκριμένων αποστολών και ενεργειών.

²⁰ Οι βαθμοφόροι, συναντώνται και ως ηγέτες, αghματάρχες, πυρηνάρχες κ.α.

²¹ Cellar Door Wiki, Mob Ierarchy, 2008, https://cellar-door.fandom.com/wiki/Mob_Hierarchy

Επίσης, όπως οι νόμιμες επιχειρήσεις έτσι και το οργανωμένο έγκλημα, όπως προαναφέρθηκε, έχει διάρκεια. Δηλαδή όπως μία νόμιμη επιχείρηση δεν θα πουλήσει μόνο ένα προϊόν, έτσι και το οργανωμένο έγκλημα δεν θα συσταθεί για να διαπράξει ένα μόνο έγκλημα .²²

Επίσης, στα εγκληματικά δίκτυα τα μέλη διέπονται από στενούς και σταθερούς δεσμούς, αλλά το δίκτυο μεταξύ των μελών και άλλων ατόμων παραμένει άτυπο και ρευστό. Γενικά, τα άτομα-στελέχη εναλλάσσονται, ώστε να μην αποδιαιρθρώνεται το εγκληματικό δίκτυο με τη σύλληψή τους. Έχει, δηλαδή, πραγματοπαγή χαρακτήρα, δεν εξαρτάται από συγκεκριμένα άτομα αλλά από τον έλεγχο συγκεκριμένων χώρων και δομών. Ακόμη και αν αλλάξουν τα μέλη η δραστηριότητα του οργανωμένου εγκλήματος συνεχίζει να υφίσταται γιατί είναι «προσδεμένη» με συγκεκριμένα σημεία π.χ. γειτονιά, λιμάνι, επιχείρηση ή μία παράνομη αγορά. Παρ' όλα αυτά δεν παύει να υφίσταται το γεγονός πως κάποια μέλη είναι πιο σταθερά από κάποια άλλα. Η προηγούμενη ανάλυση γίνεται από τη θεωρία των εγκληματικών δικτύων που εφαρμόζει ο Carlo Morselli, στο βιβλίο του *Inside Criminal Networks*, όπου εξηγεί πως όντως δεν υπάρχει αυστηρή ιεραρχία, αλλά η συνεργασία μεταξύ των μελών πραγματοποιείται μόνο για την εξυπηρέτηση του κοινού τους σκοπού, τη δημιουργία κέρδους.²³

Για την αποτελεσματικότερη κατανόηση των εγκληματικών δικτύων αξίζει να αναφερθεί και η θεωρία της οργάνωσης, η οποία περιγράφει τη συνεργασία μεταξύ των μελών, προκειμένου να επιτύχουν τους στόχους τους. Η κατανομή των ρόλων είναι ιδιαίτερα σημαντική για την αποτελεσματικότητα και την επιβίωση της οργάνωσης. Τα μέλη αναλαμβάνουν συγκεκριμένους ρόλους για κάθε στάδιο της τελικής εγκληματικής πράξης. Αρχικά, στρατολογούνται νέα μέλη και διαχειρίζονται τις πρώτες εγκληματικές ενέργειες π.χ. λαθρεμπόριο, και η δομή είναι πιο ευέλικτη, ενώ τα παλιότερα μέλη αναλαμβάνουν κυρίως διοικητικούς και συντονιστικούς στα πλαίσια της οργάνωσης ρόλους, καθώς συνήθως αποφεύγουν να εμπλακούν άμεσα σε εγκληματικές ενέργειες με σκοπό να μειώσουν τον κίνδυνο τόσο της έκθεσης όσο και της σύλληψης τους.

²² Σταμούλη Ε., Οργανωμένο έγκλημα, παράνομες αγορές και διαφθορά στην Ελλάδα στο Βιδάλη Σ., Κουλούρης Ν., Παπαχαλαράμπους Χ. (επιμ.), *Εγκλήματα των ισχυρών, Διαφθορά, οικονομικό και οργανωμένο έγκλημα*, Αθήνα, Εκδ. ΕΑΠ, 2019, σελ. 217-218

²³ Ζιούβας Δ., *Οργανωμένο Έγκλημα*, Ευρωπαϊκές Πανεπιστημιακές Εκδόσεις, σελ. 19, 99-103

Μετά την αρχική φάση εδραίωσης της ομάδας όμως, η ιεραρχία γίνεται πιο αυστηρή και το δίκτυο απαιτείται να είναι πιο λειτουργικό ώστε να μπορεί να φέρει εις πέρας όσα είναι αναγκαία και να επιτευχθεί η ακεραιότητα των δραστηριοτήτων.

Άρα, το οργανωμένο έγκλημα συνδυάζει χαρακτηριστικά τόσο δικτύων όσο και επιχειρήσεων.

Σύμφωνα με τον Chambliss, το οργανωμένο έγκλημα, δεν λειτουργεί όπως η «μαφία», όπου ο αρχηγός -ο mafia boss- ελέγχει τα πάντα. Αντίθετα, πρόκειται για ένα δίκτυο χαλαρών σχέσεων μεταξύ επιχειρηματιών, αξιωματούχων επιβολής του νόμου και πολιτικών αφενός, και αφετέρου εγκληματιών, οι οποίοι μέσω του εγκλήματος, εξυπηρετούν τα συμφέροντά τους, καθώς από τη μία επιδιώκουν να μεγιστοποιήσουν τα κέρδη τους και να ελέγξουν τις αγορές, ενώ από την άλλη κατορθώνουν να διατηρούν τα μέλη της ομάδας ενωμένα, μέσω αυστηρών κανόνων, πειθαρχίας και αίσθησης ταυτότητας.²⁴

Το γεγονός αυτό φαίνεται και από το φαινόμενο της «κρίσης σκουπιδιών» στη Νάπολη της Ιταλίας, η οποία άρχισε στις αρχές της δεκαετίας του 1990. Το κράτος, λοιπόν, το 1994 κήρυξε κατάσταση έκτακτης ανάγκης και ανέλαβε να κατασκευάσει νέες χωματερές και να αναβαθμίσει τις υποδομές για αποκομιδή και επεξεργασία αποβλήτων, έργο, όμως, που τελικά δεν υλοποιήθηκε. Έτσι, ενεπλάκη η Καμόρα, εκμεταλλευόμενη την ανάγκη των επιχειρήσεων και την πολιτική αστάθεια, δημιουργώντας χωματερές και εκβιάζοντας επιχειρήσεις να πληρώνουν για να απορρίπτουν τα σκουπίδια τους σε μη εγκεκριμένες περιοχές. Αυτό δημιούργησε σοβαρούς κινδύνους για τη δημόσια υγεία και το περιβάλλον αλλά και τεράστια κέρδη. Τελικά, τα σκουπίδια συσσωρεύτηκαν στους δρόμους για εβδομάδες. Συνεπώς, το οργανωμένο έγκλημα χρησιμοποιεί ως μέσο και τη διαφθορά για να εξυπηρετεί τα συμφέροντά του.²⁵

Επιπλέον, το οργανωμένο έγκλημα έχει υπερεθνικό χαρακτήρα, επειδή τα εγκλήματα που διαπράττει είναι πέρα από τα όρια ενός κράτους και επηρεάζουν πολλές χώρες ταυτόχρονα. Μπορεί, μάλιστα, να αναπτύσσεται τοπικά ή εθνικά, αλλά περιλαμβάνει διεθνείς διασυνδέσεις. Η διακρατική και υπερεθνική του φύση, δυσκολεύει ιδιαίτερα τα όργανα

²⁴ Paoli L., *The paradoxes of organized crime*, 2022, *Crime, Law and Social Change*, σελ. 51-97

²⁵ Giacomo D'A., Burgalassi D., Hali H., Walter M., *Conflict in Campania: Waste emergency or crisis of democracy*, 2010, <https://www.sciencedirect.com/science/article/abs/pii/S0921800910002594?via%3Dihub>

επιβολής μέτρων αντεγκληματικής πολιτικής, καθώς απαιτείται συνεργασία και συντονισμός σε διεθνές επίπεδο. Το οργανωμένο έγκλημα εκμεταλλεύεται τις παγκόσμιες αδυναμίες και τις διαφορές στις νομικές και πολιτικές δομές μεταξύ των χωρών και σε συνδυασμό, μάλιστα, με την εξέλιξη της τεχνολογίας και τη διευκόλυνση της παγκόσμιας επικοινωνίας, επιτρέπεται η δραστηριοποίηση του σε πολλές τοποθεσίες ταυτοχρόνως.²⁶

Γενικά, το οργανωμένο έγκλημα, αξιοποιεί τις κοινωνικές και πολιτικές συνθήκες κάθε περιοχής ή κράτους και διακρίνεται από υψηλή προσαρμοστικότητα στις ανάγκες κάθε εποχής. Οι μέθοδοι και τα είδη των εγκλημάτων που διαπράττουν οι οργανωμένες εγκληματικές ομάδες εξελίσσονται διαρκώς. Για παράδειγμα από παραδοσιακές δραστηριότητες όπως τα τυχερά παιχνίδια και η προστασία, έχουμε περάσει σε πιο σύγχρονες μορφές εγκλημάτων όπως είναι η νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες μέσω κρυπτονομισμάτων και τα κυβερνοεγκλήματα. Αυτό αποδεικνύει τη διάθεση του οργανωμένου εγκλήματος να ανανεώνεται και να προσαρμόζεται στις εξελίξεις των καιρών.²⁷

Χαρακτηριστική απόδειξη αυτής της προσαρμοστικότητας αποτελεί η αξιοποίηση του darknet ως νέου χώρου δράσης, μέσω του οποίου το οργανωμένο έγκλημα εξελίσσει τη δραστηριότητά του και ενισχύει την ανωνυμία και την πολυπλοκότητα των επιχειρήσεών του.

4. Ο ρόλος του darknet στο οργανωμένο έγκλημα

Το οργανωμένο έγκλημα στο darknet έχει δομή αρκετά συναφή με εκείνη του παραδοσιακού οργανωμένου εγκλήματος. Συνεχίζει να έχει αυστηρή ιεραρχία, όπου οι κατώτεροι εκτελούν τις εντολές των ανωτέρων. Σε αντίθεση με το «κλασσικό» οργανωμένο έγκλημα, στο «διαδικτυακό» που δραστηριοποιείται στο darknet, ο αρχηγός υποκινείται από το κίνητρο του κέρδους, ενώ τα μέλη εξυπηρετούν άλλους στόχους και σκοπούς. Η δομή και η εσωτερική λειτουργία αυτών των οργανώσεων, οι οποίες

²⁶ Ζιούβας Δ., Οργανωμένο έγκλημα, Ευρωπαϊκές Πανεπιστημιακές Εκδόσεις, Αθήνα, 2021, σελ. 56-51, 119-120

²⁷ Louise I., Dirty Entanglements: Corruption, Crime, and Terrorism, Cambridge University Press, 2014, σελ. 135-150

βασίζονται κυρίως στην ανωνυμία και την τεχνολογική εξειδίκευση, θα αναλυθεί εκτενέστερα σε μεταγενέστερο κεφάλαιο, με στόχο την πλήρη κατανόηση του τρόπου με τον οποίο προσαρμόζεται το οργανωμένο έγκλημα στο ψηφιακό περιβάλλον του darknet.

Τα μέλη, λοιπόν, συνήθως δεν γνωρίζονται μεταξύ τους, αφού επικρατεί η ανωνυμία και η όλη διαδικασία διέπεται από έναν κώδικα μυστικότητας. Για την επικοινωνία, τις παράνομες συναλλαγές και γενικότερα την επίτευξη οργανωμένων έκνομων δραστηριοτήτων, δημιουργούνται τα λεγόμενα «σκοτεινά δωμάτια» (dark rooms), στα οποία οι δράστες της ίδιας εγκληματικής οργάνωσης δεν γνωρίζονται μεταξύ τους. Αυτή είναι μία διαφορά του οργανωμένου εγκλήματος στο darknet συγκριτικά με το κλασικό οργανωμένο έγκλημα.²⁸

4.1. Τα σκοτεινά δωμάτια

Στο darknet, όπως αναφέρθηκε, υπάρχουν τα σκοτεινά δωμάτια, τα οποία λειτουργούν με παρόμοιο τρόπο με surface net ηλεκτρονικά καταστήματα, όπως το skrutz, με μόνη διαφορά πως στο skrutz το υλικό είναι ανοιχτό και προσβάσιμο σε όλους τους χρήστες. Το υλικό που είναι αναρτημένο στο surface net, αποτελεί το 4% του συνολικού υλικού στο διαδίκτυο.²⁹ Για την είσοδο των χρηστών σε ένα dark room απαιτείται η επαλήθευση μέσω κωδικοποίησης ή φιλτραρίσματος. Αυτό πραγματοποιείται μέσω διαμοιρασμού κρυπτογραφημένου συνδέσμου (link), προκειμένου να μπορέσουν να εισέλθουν και έτσι μέσω αυτού του link δημιουργούνται ομάδες συνομιλίας για ανταλλαγή απόψεων και υλικού.

Η είσοδος, λοιπόν, στα δωμάτια αυτά, διέπεται από πολύ αυστηρούς κανόνες ασφαλείας. Ο διαμοιρασμός του συνδέσμου μπορεί να πραγματοποιηθεί με ποικίλους τρόπους ώστε να ανταποκρίνεται στους μηχανισμούς εμπιστοσύνης.

Ο πρώτος και βασικότερος τρόπος είναι μέσω μεγάλων darknet forums, π.χ. dread. Το dread αποτελεί φόρουμ συζητήσεων όπως το reddit στο surface net και περιλαμβάνει συζητήσεις και ειδήσεις που σχετίζονται με αγορές στο darknet. Σε αυτά τα

²⁸ Γερμανός Γ., Γεωργίου Ν., Κυβερνοέγκλημα: Πρόληψη, Διερεύνηση, Αντιμετώπιση, έκδοση των ιδίων, 2021, σελ. 75-77

²⁹ Razzali N.B., Suradi Nur Biuti Mohd, A nest for cyber criminals: The Dark Web, 2019, σελ. 4

περιβάλλοντα, οι πληροφορίες ανταλλάσσονται μεταξύ συγκεκριμένων χρηστών, οι οποίοι έχουν αποκτήσει καλή φήμη και μπορούν να θεωρηθούν αξιόπιστοι. Συνεπώς, έχει να κάνει με το status quo του χρήστη εντός του φόρουμ.³⁰

Ένας άλλος πολύ συχνός τρόπος απόκτησης του κρυπτογραφημένου συνδέσμου είναι μέσω ειδικής πρόσκλησης προκειμένου να αποκτήσουν είσοδο. Οι προσκλήσεις διακινούνται εφόσον υπάρχει μεταξύ των χρηστών υψηλή και αμοιβαία εμπιστοσύνη και εάν οι λαμβάνοντες χρήστες πληρούν συγκεκριμένα κριτήρια.³¹

Η διανομή μπορεί να πραγματοποιηθεί και με εξωτερικές εφαρμογές για ανταλλαγή μηνυμάτων, οι οποίες επιτρέπουν end-to-end κρυπτογράφηση με αποτέλεσμα οι σύνδεσμοι να κυκλοφορούν με τη μέγιστη δυνατή ασφάλεια.

Επίσης, ο διαμοιρασμός μπορεί να πραγματοποιηθεί και μέσω μίας διαδικασίας που ονομάζεται *στενογραφία*, μέσα από αποστολή εικόνων, «memes» ή αρχείων, ανταλλάσσονται μέσω των μέσων κοινωνικής δικτύωσης και δεν είναι ορατές στο «γυμνό ανθρώπινο μάτι», ούτε και σε αυτοματοποιημένα συστήματα εντοπισμού.³²

Τέλος, ως μέθοδος διαμοιρασμού αξιοποιείται και η προσωρινή ανάρτηση συνδέσμων σε πλατφόρμες ανάρτησης προσωρινού περιεχομένου, όπου η ανάρτηση μετά από συγκεκριμένα λεπτά ή προβολές διαγράφεται και επειδή εξ αρχής ήταν κρυπτογραφημένη, δεν αφήνει και ίχνη.

Επίσης, να επισημανθεί πως οι χρήστες περνούν από μία διαδικασία επίλυσης κρυπτογραφημένων γρίφων προκειμένου να ανοίξουν τον σύνδεσμο και υπογράφουν με το δημόσιο κρυπτογραφικό τους κλειδί για να αποδείξουν την ταυτότητα τους.³³

³⁰ Logie K., Das S., Lessons learned from Dread darknet communities: How and why are fraudsters targeting the elderly to be victims or accomplices?, 2024, <https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12684>

³¹ U.S. Department of Justice, Cyber Security Unit, Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data, 2020, <https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl?inline>

³² Simplilearn, What is Steganography? Types, Techniques, Examples & Applications, 2024, <https://www.simplilearn.com/what-is-steganography-article>

³³ Bursztein E., Bethard S., Fabry C., Mitchell J.C., Jurafsky D., How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation, Stanford University, 2010, https://web.stanford.edu/~jurafsky/burszstein_2010_captcha.pdf

Η χρήση κάθε δωματίου καθορίζεται από τους διαχειριστές και οι χρήστες επικοινωνούν και αλληλοεπιδρούν με κεντρικό θέμα μία μη νόμιμη δραστηριότητα. Έτσι, μ' αυτόν τον τρόπο και τα μέλη μίας εγκληματικής οργάνωσης, χρησιμοποιούν τα dark rooms για θέματα όπως το trafficking, η εμπορία ναρκωτικών, η εμπορία οργάνων κ.α. Κάθε δωμάτιο έχει συγκεκριμένους επισκέπτες που εξυπηρετούνται και ειδικό χαρακτήρα (π.χ. δωμάτια με κεντρικό θέμα την παιδική πορνογραφία εμπεριέχουν παιδεραστές και έχουν στόχο τη διανομή υλικού ή τη δημιουργία κυκλώματος απαγωγής παιδιών). Βλέπουμε, λοιπόν, πως μέσω των σκοτεινών δωματίων, οι δράστες οργανώνονται, μπορούν να συντονίσουν τη δράση τους και τηρούν την ανωνυμία τους. Επομένως, τα dark rooms αποτελούν κομβικό σημείο για όλες τις ομάδες οργανωμένου εγκλήματος που χρησιμοποιούν το darknet.

Επίσης, βάσει των στατιστικών (αν και δεν είναι αντιπροσωπευτικά λόγω του μεγάλου σκοτεινού αριθμού της εγκληματικότητας) έχει προκύψει πως τα πιο συχνά χρησιμοποιούμενα dark rooms από οργανωμένες εγκληματικές ομάδες είναι τα δωμάτια επικοινωνίας μεταξύ των μελών, τα δωμάτια με στόχο την πώληση και διάδοση περιεχομένου παιδικής πορνογραφίας, την απαγωγή παιδιών, το trafficking ατόμων και την παραγωγή, εμπορία και διακίνηση ναρκωτικών.

Συνεπώς, τα δωμάτια αυτά έχουν στόχο είτε την επικοινωνία μεταξύ των μελών της οργάνωσης, είτε την εμπορία των προϊόντων και υπηρεσιών που προσφέρουν και τη νομιμοποίηση των παράνομων κερδών τους.³⁴

4.2. Νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες

Η νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες ή αλλιώς ξέπλυμα βρώμικου χρήματος, χαρακτηρίζεται από μεγάλη ευρηματικότητα. Υπάρχουν τρία στάδια νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες προκειμένου να μπορέσουν να ενταχθούν στη νόμιμη οικονομία.

³⁴ Γερμανός Γ., Γεωργίου Ν., Κυβερνοέγκλημα: Πρόληψη, Διερεύνηση, Αντιμετώπιση, έκδοση των ιδίων, 2021, σελ. 79-100

Το πρώτο είναι η τοποθέτηση, δηλαδή η κατάθεση των κεφαλαίων σε πιστωτικά ιδρύματα. Ουσιαστικά, αφορά τη διάσπαση του ποσού σε μικρότερα μέρη και την τοποθέτηση των χρημάτων σε πολλούς διαφορετικούς τραπεζικούς λογαριασμούς για να μην δημιουργηθούν υποψίες.

Το δεύτερο στάδιο είναι η διαστρωμάτωση. Πρόκειται ουσιαστικά, για ένα πλέγμα οικονομικών συναλλαγών και αφορά τη μεταφορά των κεφαλαίων σε ένα δίκτυο τραπεζικών λογαριασμών, κυρίως σε off-shore (υπεράκτιες/εξωχώριες) εταιρείες. Οι εταιρείες αυτές τηρούν πλήρη ανωνυμία και έχουν πολύ χαμηλούς φόρους (1-2%). Πρόκειται για τους λεγόμενους φορολογικούς παράδεισους, στους οποίους προσφεύγουν οι εγκληματίες των βασικών εγκλημάτων (δηλαδή των κύριων παράνομων πράξεων από τις οποίες προκύπτουν τα παράνομα κέρδη) σε τέτοιες περιπτώσεις. Είναι μία περίπτωση φοροαποφυγής και δεν είναι έγκλημα. Επίσης, στις off-shore εταιρείες δεν υπάρχουν συναλλαγματικοί περιορισμοί, ενώ το τραπεζικό απόρρητο για τους ελέγχους καθιστά την επαφή με τις δικαστικές και αρμόδιες αρχές περιορισμένη έως ανύπαρκτη. Περιοχές που εδρεύουν οι υπεράκτιες εταιρείες είναι η Ανγκόλα, η Κόστα Ρίκα, τα νησιά Κεϊμαν, οι Παρθένοι Νήσοι και άλλα.³⁵

Το τελευταίο στάδιο ξεπλύματος βρώμικου χρήματος είναι η ολοκλήρωση, όπου τα χρήματα που έχουν τοποθετηθεί και διαστρωματωθεί επιστρέφουν πίσω στον αρχικό “ιδιοκτήτη”, ο οποίος τα επενδύει ως νόμιμα κεφάλαια. Αυτό μπορεί να πραγματοποιηθεί με την επένδυση σε μετοχές, με την αγορά κάποιου ακινήτου ή με την εκμετάλλευση κάποιας επιχείρησης, με χαμηλά πάγια έξοδα³⁶, στην οποία θα συγχέονται τα νόμιμα με τα παράνομα έσοδα και θα μπορεί η οργάνωση να δικαιολογήσει την υψηλή συγκέντρωση μετρητών. Τέτοια επιχείρηση θα μπορούσε να είναι κάποιο κατάστημα εστίασης ή ένα πλυντήριο αυτοκινήτων.³⁷

Κατά τον παραδοσιακό τρόπο τέλεσης των εγκλημάτων το σύστημα απονομής της ποινικής δικαιοσύνης είχε την ευκαιρία, αν δεν εντόπιζε τους δράστες κατά την τέλεση

³⁵ Tax Justice Network, Identifying Tax Havens and Offshore Finance Centres, 2007, https://www.taxjustice.net/cms/upload/pdf/Identifying_Tax_Havens_Jul_07.pdf

³⁶ «Χαμηλά πάγια έξοδα» σημαίνει ότι η επιχείρηση έχει χαμηλό κόστος σε σταθερά, μακροχρόνια έξοδα, όπως ενοίκια, τα οποία δεν αλλάζουν σημαντικά με την παραγωγή ή τις πωλήσεις, και έτσι μπορεί να λειτουργεί οικονομικά, διευκολύνοντας την απόκρυψη παράνομων κερδών χωρίς να δημιουργεί υποψίες.

³⁷ Ζιούβας Δ., «Χρηματοπιστωτικό Ποινικό Δίκαιο», Ευρωπαϊκές Πανεπιστημιακές Εκδόσεις, Αθήνα, 2022, σελ 138-140

του εγκλήματος, να το κάνει αργότερα κατά το στάδιο της τοποθέτησης ή της διαστρωμάτωσης. Συνεπώς με προσεκτική εξέταση των ύποπτων συναλλαγών και των επενδύσεων οι διωκτικές αρχές μπορούσαν να αυξήσουν τις πιθανότητες εντοπισμού και αντιμετώπισης του εγκλήματος εκ των υστέρων.³⁸

Σήμερα, όμως η ραγδαία εξέλιξη της τεχνολογίας και η δημιουργία κρυπτονομισμάτων έχει προσδώσει στο ζήτημα αυτό νέες διαστάσεις, καθιστώντας τον εντοπισμό και την καταπολέμηση του από τις διωκτικές αρχές μία ιδιαίτερα σύνθετη και απαιτητική διαδικασία.

Τα κρυπτονομίσματα, είναι ψηφιακά χρήματα, τα οποία αποτελούν χαρακτηριστικό στοιχείο των νέων τεχνολογικών εξελίξεων, στηρίζονται σε πολύπλοκους μαθηματικούς κώδικες και συχνά λειτουργούν αποκεντρωμένα, δηλαδή δεν ελέγχονται από χρηματοπιστωτικά ιδρύματα και κυβερνήσεις, ενώ οι συναλλαγές είναι άμεσες, διασυνοριακές και ανώνυμες. Μέσω ανταλλακτηρίων, οι χρήστες, και στην προκειμένη περίπτωση τα μέλη μίας οργανωμένης εγκληματικής ομάδας, αγοράζουν ή πωλούν κρυπτονομίσματα, ενώ μπορούν να τα χρησιμοποιήσουν και για να αγοράσουν ή να πουλήσουν προϊόντα και υπηρεσίες στο darknet.

Η διαχείριση των κρυπτονομισμάτων πραγματοποιείται από τον κάτοχο του ψηφιακού πορτοφολιού, ενώ όλες οι συναλλαγές καταγράφονται μέσω του λεγόμενου blockchain, το οποίο αποθηκεύει και κρυπτογραφεί όλα τα δεδομένα σε μία αλυσίδα μπλοκ. Η αλυσίδα μπλοκ αποτελεί ένα ασφαλές ψηφιακό αποδεικτικό αρχείο που κρατάει καταγεγραμμένες όλες τις συναλλαγές με τη σειρά που έγιναν σε διαδοχικά ψηφιακά μπλοκ.

Ωστόσο, λόγω του διεθνούς, αποκεντρωμένου και ανώνυμου χαρακτήρα τους, η χρήση τους έχει γίνει ιδιαίτερα ελκυστική από το οργανωμένο έγκλημα. Μέσω των αποκεντρωμένων ανταλλακτηρίων που βρίσκονται στο darknet, τα οποία εννοείται πως δεν χρειάζονται ταυτοποίηση των χρηστών, οι συναλλαγές εντοπίζονται πολύ δύσκολα.³⁹

³⁸ Τραγάκης Γ., «Οργανωμένο Έγκλημα και Ξέπλυμα Βρώμικου Χρήματος», Νομική Βιβλιοθήκη 1996, σελ.254-256

³⁹ Kriptomat, Τι είναι το κρυπτονόμισμα και πως λειτουργεί, 2021, <https://kriptomat.io/gr/kryptonomismata/ti-einai-to-kryptonomisma/>

Το ξέπλυμα βρώμικου χρήματος με κρυπτονομίσματα, ακολουθεί το ίδιο μοτίβο τοποθέτησης – διαστρωμάτωσης – ενσωμάτωσης με μικρές διαφοροποιήσεις. Η τοποθέτηση νοείται όταν το παραστατικό χρήμα μετατραπεί σε κρυπτονομίσματα. Αυτό είναι και το πιο επικίνδυνο για τους δράστες να ανακαλυφθούν από το σύστημα. Ωστόσο, λόγω του γεγονότος ότι το ξέπλυμα πραγματοποιείται στα ήδη «τοποθετημένα» κρυπτονομίσματα και γίνεται κατευθείαν μέσω αυτών, συνήθως το πρώτο βήμα απουσιάζει.

Η διαστρωμάτωση πραγματοποιείται με ποικίλους τρόπους. Ένας τρόπος είναι της κρυπτομίξης. Αυτή συνήθως γίνεται μέσω εξειδικευμένων υπηρεσιών στο darknet , με τη συγκέντρωση πηγών κεφαλαίου από πολλαπλές εισροές για μία μεγάλη και τυχαία χρονική περίοδο και στην πορεία με την επανατοποθέτηση τους προς τις διευθύνσεις προορισμού.

Τα κρυπτονομίσματα, λοιπόν, στέλνονται από πολλές πηγές σε μία διεύθυνση , δηλαδή τον τρέχοντα λογαριασμό. Τα κεφάλαια αναμειγνύονται σε αυτόν τον λογαριασμό και στη συνέχεια χωρίζονται σε διαφορετικές διευθύνσεις. Η διαδικασία αυτή επαναλαμβάνεται πολλές φορές σε τυχαίους χρόνους μέχρι να φτάσουν στον τελικό προορισμό. Ως αποτέλεσμα είναι αδύνατον να συνδεθούν τα κεφάλαια με την αρχική πηγή. Έτσι, λοιπόν, με τις υπηρεσίες κρύπτο - μίξης επιτυγχάνει το οργανωμένο έγκλημα την ανωνυμία , αναμειγνύοντας δυνητικά αναγνωρίσιμα κρυπτονομίσματα με άλλα. Λόγω της επιδιωκόμενης ανωνυμίας, είναι ιδιαίτερα σύνηθες να επιλέγεται αυτός ως τρόπος ξεπλύματος κρυπτονομισμάτων.⁴⁰

Άλλος τρόπος είναι τα «ATM» κρυπτονομισμάτων, τα οποία έχουν ίδια λειτουργία με τα συμβατικά ATM μετρητών χρημάτων, με τη διαφορά ότι δεν υπάρχει κάποια τράπεζα να εποπτεύει τότε πραγματοποιείται ανάληψη ή κατάθεση. Επίσης δεν πραγματοποιείται κανένας έλεγχος στοιχείων και σε περίπτωση καταχώρησης πλαστών στοιχείων, δεν υπάρχει κάποιο φυσικό πρόσωπο ή κάποιος αυτοματοποιημένος μηχανισμός να το ελέγξει.⁴¹

⁴⁰ Antonopoulos, A., «Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Sebastopol», California: O'Reilly, 2015, σελ. 30-31

⁴¹ Becker B., What is a bitcoin ATM? ,2023, <https://builtin.com/cryptocurrency/what-is-a-bitcoin-atm>

Με τον τρίτο τρόπο, τα κρυπτονομίσματα μετατρέπονται σε διαφορετικούς τύπους κρυπτονομισμάτων μέσα από εργαλεία και ανταλλακτήρια του darknet, μέχρι να χαθεί η αρχική τους προέλευση. Για παράδειγμα, ένα bitcoin, μπορεί να ανταλλαχθεί ή να μετατραπεί σε άλλα κρυπτονομίσματα, όπως το ethereum ή το peercoin, όπως για παράδειγμα μετατρέπεται το ευρώ σε δολάρια ή άλλα νομίσματα.

Ένας τέταρτος τρόπος που αξιοποιείται από το οργανωμένο έγκλημα είναι τα δίκτυα peer-to-peer (P2P), τα οποία οργανώνονται και συντονίζονται μέσω αγγελιών ή forums στο darknet. Σε αυτή την περίπτωση επιστρατεύονται πρόσωπα που δεν κινούν την υποψία, τα οποία στέλνουν τα παράνομα χρήματα σε ανταλλακτήρια σε άλλες χώρες με χαλαρούς μηχανισμούς ελέγχου και τελικά μετατρέπονται στο τοπικό νόμισμα αυτής της χώρας.

Μια πέμπτη μέθοδος περιλαμβάνει τη χρήση των λεγόμενων Αρχικών Προσφορών Νομισμάτων (Initial Coin Offerings) ή αλλιώς ICO. Οι εγκληματίες στην περίπτωση αυτή, παρουσιάζονται ως επενδυτές και μετατρέπουν για παράδειγμα τα bitcoin τους, σε άλλα κρυπτονομίσματα.

Στο τελευταίο στάδιο, εκείνο της ενσωμάτωσης, τα έσοδα από τις εγκληματικές δραστηριότητες παρουσιάζονται συχνά ως κέρδη από τυχερά παιχνίδια ή επενδύσεις ICO. Πολλές φορές, μάλιστα, επενδύονται σε εικονικές επιχειρήσεις στο διαδίκτυο.

Κάθε λογαριασμός, δηλαδή κάθε ψηφιακό πορτοφόλι δεν μπορεί να χρησιμοποιηθεί πάνω από δύο φορές. Συνεπώς τα κρυπτονομίσματα λαμβάνονται και κατόπιν μεταφέρονται σε άλλο λογαριασμό. Είναι δυνατόν να πραγματοποιηθούν χιλιάδες συναλλαγές, με μικρό κόστος μέσω της τροποποίησης της «γλώσσας» του εκάστοτε υπό χρήση προγράμματος. Λόγω της ραγδαίας μεταβλητότητας των κρυπτονομισμάτων, δηλαδή των συχνών και απότομων αλλαγών στην αξία τους, είναι εύκολο να δικαιολογηθεί κάποιος απροσδόκητος πλούτος από κρυπτονομίσματα.

Τέλος, στις αποκεντρωμένες συναλλαγές, όπου οι συναλλαγές γίνονται αμέσως μεταξύ των χρηστών χωρίς κάποιον κεντρικό έλεγχο και μεσάζοντες, κυριαρχούν τα ανώνυμα και ιδιωτικά κρυπτονομίσματα, τα οποία είναι απόρρητα και συναλλάσσονται με μεγαλύτερη ανωνυμία στο blockchain, σ' αντίθεση με τα δημόσια όπως τα bitcoin που καταγράφουν τις συναλλαγές ανοιχτά. Τα ιδιωτικά κρυπτονομίσματα είναι λιγότερο

ανιχνεύσιμα, καθώς η ανωνυμία επιτυγχάνεται μέσω της απόκρυψης των λεπτομερειών της διεύθυνσης χρηστών από την οποία έγινε η αποστολή. Έτσι δεν μπορεί να υπάρξει πρόσβαση σε πληροφορίες όπως το υπόλοιπο ενός λογαριασμού και η προέλευση των νομισμάτων.⁴²

4.3. Η ερμηνεία της δράσης του οργανωμένου εγκλήματος στο darknet με βάση εγκληματολογικές θεωρίες

Η επιλογή του οργανωμένου εγκλήματος να επικοινωνεί, να οργανώνεται και να δρα στο darknet αποτελεί μια στρατηγική που επιτυγχάνει το μέγιστο δυνατό όφελος με τον ελάχιστο δυνατό κίνδυνο, το οποίο μπορεί να εξηγηθεί περαιτέρω με τη θεωρία της ορθολογικής επιλογής του Becker.

Σύμφωνα με τον Becker, οι δράστες οδηγούνται στο έγκλημα κατόπιν συνειδητών αποφάσεων αφού έχουν σταθμίσει τα προσδοκώμενα οφέλη, έναντι των πιθανών κινδύνων σχετικά με τη διάπραξη μίας εγκληματικής πράξης.⁴³ Εφόσον, λοιπόν, το darknet αποτελεί ένα χώρο με υψηλό βαθμό ανωνυμίας και έλλειψη θεσμικής εποπτείας, οι εγκληματίες, επιλέγουν να αξιοποιούν όλα αυτά τα εργαλεία, ακριβώς επειδή μειώνουν τον κίνδυνο εντοπισμού και μεγιστοποιούν το οικονομικό όφελος. Συνεπώς, πρακτικές όπως η νομιμοποίηση των παράνομων εσόδων με κρυπτονομίσματα αποτελεί μία συνειδητή επιλογή εγκληματικής δράσης για την αξιοποίηση των δυνατοτήτων που προσφέρει το σκοτεινό διαδίκτυο.

Η δράση του οργανωμένου εγκλήματος στο darknet μπορεί να εξηγηθεί και από τη θεωρία του Reckless για τον κοινωνικό έλεγχο και τον ευκαιριακό χαρακτήρα των εγκλημάτων. Σύμφωνα με αυτή τη θεωρία, οι δράστες διαπράττουν εγκλήματα όταν οι απωθητικές δυνάμεις, δηλαδή οι κοινωνικοί περιορισμοί και οι θεσμικοί έλεγχοι, είναι

⁴² Antonopoulos, A., «Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Sebastopol», California: O'Reilly, 2015, σελ. 44-45

⁴³ Becker G., Crime and punishment: an economic approach, 1968, σελ. 1-5, http://masonlec.org/site/rte_uploads/files/JEP/Readings/Butler%20Economic%20Analysis%20for%20Lawyers%203rd%20ed/CH%20VII%20Crime.pdf

αδύναμες και οι ωθητικές, δηλαδή οι ευκαιρίες διάπραξης του εγκλήματος, είναι ισχυρές.

44

Στο darknet, τόσο η ανωνυμία, όσο και η έλλειψη ελέγχου απ' τις διωκτικές και ρυθμιστικές αρχές είναι αδύναμα, με αποτέλεσμα οι απωθητικές δυνάμεις να περιορίζονται, δίνοντας το κίνητρο στους δράστες να εγκληματούν παρακάμπτοντας τους κοινωνικούς περιορισμούς και τη κρατική παρέμβαση. Συνεπώς, βλέπουμε, πως στη περίπτωση χρήσης και δράσης του darknet από το οργανωμένο έγκλημα οι ωθητικές δυνάμεις υπερτερούν έναντι των απωθητικών, ενισχύοντας τις ευκαιρίες του οργανωμένου εγκλήματος για δράση.

Τέλος, άλλη μία θεωρία που κρίνεται σκόπιμο να αναλυθεί και συνδεθεί με το θέμα της παρούσας διπλωματικής εργασίας είναι η θεωρία των καθημερινών δραστηριοτήτων των Felson και Cohen (1979). Σύμφωνα με αυτή τη θεωρία, η τέλεση του εγκλήματος διευκολύνεται από την σύμπτωση τριών στοιχείων: έναν ευκαιριακό δράστη, πρόθυμο και ικανό να διαπράξει ένα έγκλημα, έναν κατάλληλο (ευάλωτο) στόχο και απουσία ικανών φυλάκων, δηλαδή έλλειψη φυσικών ή κοινωνικών εμποδίων. Με λίγα λόγια, το έγκλημα δεν εξαρτάται αποκλειστικά από τον χαρακτήρα ή τα κίνητρα του δράστη, αλλά όπως είδαμε και στη θεωρία του Reckless, κυρίως από τις ευκαιρίες που του δίδονται.⁴⁵

Στο πλαίσιο του darknet, όλες αυτές οι προϋποθέσεις ενισχύονται. Τα μέλη μίας εγκληματικής οργάνωσης, έχουν κίνητρο το οικονομικό όφελος, ενώ οι στόχοι, δηλαδή οι ενδιαφερόμενοι πελάτες είναι άμεσα διαθέσιμοι, με βασικό χαρακτηριστικό των συναλλαγών μεταξύ τους την ανωνυμία στις αγορές που αλληλοεπιδρούν. Επίσης, στο darknet απουσιάζει ο ικανός φύλακας, δηλαδή οι κρατικοί ελεγκτικοί μηχανισμοί και η δυνατότητα εντοπισμού απ' τις διωκτικές αρχές, με αποτέλεσμα η παρακολούθηση και ο εντοπισμός των δραστών να καθίσταται ένα ιδιαίτερα απαιτητικό εγχείρημα.

⁴⁴ Χάιδου Α., Θετικιστική εγκληματολογία, αιτιολογικές προσεγγίσεις του εγκληματικού φαινομένου, νομική βιβλιοθήκη, 1996, σελ. 206-210

⁴⁵ Ζαραφωνίτου Χ., Ανίτση Ε., Εισήγηση: «Πόλη και έγκλημα: θεωρητική προσέγγιση και χαρακτηριστικά του φαινομένου», 2020, σελ. 5-6, https://easte.panteion.gr/images/other_files/h_kyklos/zarafonitou_anitsi_151220.pdf

Συνεπώς, το darknet αποτελεί έναν ευνοϊκό και αποτελεσματικό χώρο επιχειρηματικής δράσης για το οργανωμένο έγκλημα, όπως ακριβώς αναλύουν στη θεωρία τους οι Felson και Cohen.

4.4. Mirroring

Πέραν των σκοτεινών δωματίων (dark rooms) , τα μέλη του οργανωμένου εγκλήματος, προκειμένου να επικοινωνούν χρησιμοποιούν και μέσα κοινωνικής δικτύωσης στο darknet. Αυτά αποτελούν αντικατοπτρισμό (mirroring), δηλαδή πιστά αντίγραφα, των διεθνώς διαδεδομένων κοινωνικών μέσων (π.χ. Facebook, Instagram κ.α.), διαμορφωμένα στις απαιτήσεις του darknet.

Η βασική διαφορά με τα κλασικά μέσα κοινωνικής δικτύωσης που βρίσκονται στο surface net, είναι ότι δεν απαιτείται κάποια μορφή ταυτοποίησης και γενικότερα, επαλήθευσης του ψηφιακού χρήστη, όπως για παράδειγμα μέσω της διεύθυνσης ηλεκτρονικού του ταχυδρομείου ή τον αριθμό του τηλεφώνου του, αλλά η συμμετοχή πραγματοποιείται χωρίς απολύτως κανέναν έλεγχο, γεγονός που βοηθά στον μέγιστο δυνατό βαθμό την επικοινωνία μεταξύ των ατόμων που εμπλέκονται στην εγκληματική οργάνωση.

Οι σελίδες αυτές, όπως και τα dark rooms, δεν είναι διαθέσιμα, όμως, για όλους, αλλά απαιτούν πρόσκληση ή επιβεβαίωση μέσω γνωστού μέλους για την συμμετοχή του ατόμου στις ομαδικές συνομιλίες. Επίσης, χρησιμοποιείται end-to-end κρυπτογράφηση και μηνύματα που ύστερα από μια ορισμένη χρονική διάρκεια αυτοκαταστρέφονται, μ' αποτέλεσμα να μην μένει κανένα ίχνος.

Τέλος, πέραν της επικοινωνίας, στις πλατφόρμες αυτές επιδιώκεται και η στρατολόγηση νέων μελών, η διακίνηση ψηφιακού καθοδηγητικού υλικού π.χ. για κατασκευή όπλων, εξαρτησιογόνων ουσιών και πλαστών εγγράφων, αλλά και ανταλλαγή πληροφοριών για τεχνικές παράκαμψης, απόκρυψης και αποφυγής εντοπισμού.⁴⁶

⁴⁶ Glushko, R.- J. ,The Discipline of Organizing: Core Concepts Edition, O'Reilly Media, Inc.,2017, σελ.400 επ.

4.5. Η δομή του οργανωμένου εγκλήματος στο darknet

Το darknet, αν και έχει δημιουργήσει ένα νέο περιβάλλον δράσης για το οργανωμένο έγκλημα, με τα σκοτεινά δωμάτια να αποτελούν τον κυρίαρχο τρόπο οργάνωσης, επικοινωνίας και δράσης, η δομή και η ιεραρχία του, όπως ανέδειξε το Υπουργείο Δικαιοσύνης των ΗΠΑ μετά την εξάρθρωση της εγκληματικής οργάνωσης Infracore⁴⁷ το 2017, εξακολουθεί να διατηρεί το ίδιο μοτίβο δράσης και ρόλων με το παραδοσιακό οργανωμένο έγκλημα, με κάποιες προσθήκες και μεταποιήσεις, προσαρμοσμένες στο ψηφιακό περιβάλλον.

Και πάλι στη κορυφή της πυραμίδας, βρίσκεται ο αρχηγός, ο οποίος στη περίπτωση του darknet, ονομάζεται πλέον *εγκέφαλος ή επικεφαλής*. Πρόκειται για ένα πρόσωπο, χάριν του οποίου δημιουργούνται τα δωμάτια, εφόσον είναι συνήθως δική του η ιδέα ως προς τη θεματολογία, και μπορεί εάν θέλει οποιαδήποτε στιγμή να θέσει ένα δωμάτιο σε παύση και να προκαλέσει αποδιοργάνωση ενός ολόκληρου συστήματος, καθώς κάθε δωμάτιο μπορεί να συσταθεί μόνο μία φορά. Επίσης, η πλειοψηφία των εσόδων από τις εγκληματικές πράξεις καταλήγει στα χέρια του επικεφαλής. Αν και γενικότερα επικρατεί ανωνυμία στο darknet, ο επικεφαλής διατηρεί απόλυτη ανωνυμία, οι χρήστες δεν γνωρίζουν την ύπαρξη του και πολλές φορές ακόμη και ορισμένοι διαχειριστές δεν γνωρίζουν για αυτόν.

Έπειτα, είναι οι *διαχειριστές ή κεντρικοί χειριστές (core operators)*, αντίστοιχοι των υπαρχηγών, οι οποίοι έχουν πλήρη λειτουργική αρμοδιότητα και πρόσβαση σε όλο το υλικό και αναλαμβάνουν την εκπαίδευση, οργάνωση και καθοδήγηση των υπόλοιπων χρηστών. Έχουν πλήρη έλεγχο σε όλους τους χρήστες, αρκετές φορές προσδιορίζουν τα θέματα των δωματίων και δίνουν την απαραίτητη πρόσβαση που χρειάζεται για κάθε χρήστη. Επίσης, μπορούν να εγγράψουν, περιορίσουν ή διαγράψουν κάποιον χρήστη και γενικά, επιμελούνται όλες τις ρυθμιστικές διαδικασίες. Τέλος, διαχειρίζονται τους escrow μηχανισμούς, οι οποίοι αποτελούν βασικό εργαλείο για την επίτευξη της ανωνυμίας, της

⁴⁷ Το Infracore αποτελούσε υπερεθνική εγκληματική οργάνωση, η οποία δρούσε στο darknet και διέπραττε εγκλήματα Phishing, με σκοπό τη κλοπή ταυτοτήτων, δεδομένων πιστωτικών καρτών κ.α.

εμπιστοσύνης και της ασφαλούς συναλλαγής. Πρόκειται για ένα ενδιάμεσο στάδιο, που προστατεύει τόσο τους αγοραστές, όσο και τους πωλητές από απάτες. Συγκεκριμένα, ο αγοραστής καταθέτει το πληρωμένο ποσό, το οποίο είναι σε κρυπτονομίσματα, σε μία ουδέτερη πλατφόρμα του darknet, μέχρι να ολοκληρωθεί η συναλλαγή και μόλις ο αγοραστής λάβει το προϊόν, το ποσό καταλήγει στον πωλητή. Έτσι, οι διαχειριστές λειτουργούν και ως *reputation managers*, αφού «καθαρίζουν» το όνομα της ομάδας απέναντι στους χρήστες.

Στη συνέχεια, αντίστοιχοι των βαθμοφόρων είναι οι *διαβαθμισμένοι χρήστες*, οι οποίοι διαθέτουν προσβασιμότητα σε όλο το υλικό του δωματίου και γενικότερα μοιράζονται με τους διαχειριστές τα ίδια δικαιώματα, με τη μόνη διαφορά πως δεν επιτρέπεται να χειριστούν ζητήματα, όπως η εγγραφή ή διαγραφή των υπόλοιπων χρηστών. Παρ' όλα αυτά, εάν οι διαχειριστές το αποφασίσουν, έχουν τη δυνατότητα να αναθέσουν στους διαβαθμισμένους χρήστες και τέτοια καθήκοντα.⁴⁸

Ένας κρίσιμος ρόλος στο ψηφιακό οργανωμένο έγκλημα είναι των τεχνικών ειδικών (*technical experts*). Αυτοί οι ειδικοί, περιλαμβάνουν τους λεγόμενους «*crackers*», οι οποίοι είναι *hackers*, με την έννοια πως οδηγούνται σε μη εξουσιοδοτημένη πρόσβαση και σε χωρίς άδεια διείσδυση, χρησιμοποιώντας τις γνώσεις τους για κακόβουλους σκοπούς. Ο όρος «*cracking*» χρησιμοποιείται για να περιγράψει έναν *hacker*, ο οποίος δρά κακόβουλα. Οι *crackers* εκμεταλλεύονται τρωτά σημεία ή δημιουργούν κακόβουλο λογισμικό, που συνήθως αναφέρεται ως «*cracks* (=ρωγμές)», το οποίο παρακάμπτει ή απενεργοποιεί τους μηχανισμούς προστασίας που έχουν τεθεί σε εφαρμογή από τους προγραμματιστές ενός λογισμικού ή προγράμματος.⁴⁹ Οι *crackers* ονομάζονται αλλιώς «*Black Hat Hackers*» και δραστηριοποιούνται και στο darknet⁵⁰. Οργανώνονται, λοιπόν, σε ομάδες και δημιουργούν παράνομα λογισμικά π.χ. ιούς. Μερικές από τις ενέργειες τους είναι η διείσδυση σε δίκτυα, η παραβίαση κωδικών ασφαλείας, η κατασκοπεία

⁴⁸ U.S. Department of Justice, Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from Cybercrimes, 2018, <https://www.justice.gov/archives/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>

⁴⁹ Spanakis E.G., Silvia Bonomi S., Cyber-attacks and threats for healthcare – a multi-layer thread analysis, <https://ieeexplore.ieee.org/abstract/document/9176698/authors#authors>

⁵⁰ Οι Black Hat Hackers, δραστηριοποιούνται και εκτός του darknet, στο surface net, καθώς πραγματοποιούν επιθέσεις και παραβιάσεις συστημάτων.

δεδομένων και η καταστροφή ιστοσελίδων.⁵¹ Οι crackers εμπλέκονται σε διαφόρων ειδών παράνομες διαδικτυακές δραστηριότητες, όπως η παραβίαση μηχανισμών προστασίας αντιγραφής σε λογισμικό⁵², η παράτυπη πρόσβαση στα συστήματα με σκοπό την πρόκληση ζημίας, η παραποίηση δεδομένων ή η κλοπή πληροφοριών.

Το κακόβουλο λογισμικό εισέρχεται σε έναν ηλεκτρονικό υπολογιστή με σκοπό να του προκαλέσει ζημιά διαγράφοντας ή τροποποιώντας δεδομένα και προγράμματα, παρεμποδίζοντας τη λειτουργία ενός συστήματος ή υποκλέπτοντας σημαντικά δεδομένα και διακρίνεται στους ιούς, στα σκουλήκια και στους «δούρειους ίππους».

Οι ιοί (viruses) έχουν τη δυνατότητα να μολύνουν έναν υπολογιστή και να πολλαπλασιάζονται ακόμη και σε διαφορετικά υπολογιστικά συστήματα προκαλώντας εκτεταμένες ζημιές. Υπάρχουν διαφορετικές κατηγορίες ιών, όπως τα μολυσμένα αρχεία (file infectors), οι ιοί τομέα εκκίνησης (boot sector viruses), οι μακροϊοί (macroviruses) και οι ιοί σεναρίων (script viruses). Τα μολυσμένα αρχεία μπορούν να εφαρμοστούν σε άλλα αρχεία κατά τη διάρκεια που εκείνα εκτελούνται και έτσι ενεργοποιούνται κάθε φορά που εκείνα ανοίγουν. Οι ιοί τομέα εκκίνησης προσχωρούν στον τομέα εκκίνησης ενός σκληρού δίσκου, ο οποίος σε γενικές γραμμές είναι υπεύθυνος για την εκκίνηση ολόκληρου του υπολογιστικού συστήματος. Οι μακροϊοί παρασιτούν σε έγγραφα και ενεργοποιούνται όταν αυτά ανοίγουν, ενώ οι ιοί σεναρίου μολύνουν ιστοσελίδες στο διαδίκτυο. Μόλις ο ιός ενεργοποιηθεί, ο δράστης μπορεί να υποκλέψει ευαίσθητες πληροφορίες, να καταστρέψει αρχεία και να απενεργοποιήσει μέτρα ασφαλείας.⁵³

Τα σκουλήκια (worms) μπορούν να μολύνουν υπολογιστικά συστήματα και δίκτυα. Σ' αντίθεση με τους ιούς δεν χρειάζονται κάποιο πρόγραμμα για να παρασιτήσουν, αλλά εξαπλώνονται ανεξάρτητα μέσω του διαδικτύου και αναπαράγονται πολλαπλασιάζοντας ανεξέλεγκτα τον εαυτό τους προκαλώντας σοβαρές ζημιές στα συστήματα που εισέρχονται.⁵⁴

⁵¹ Goerzen M., Coleman G., Wearing Many Hats, 2022, https://datasociety.net/wp-content/uploads/2022/03/WMH_final01062022Rev.pdf

⁵² Η παραβίαση μηχανισμών προστασίας αντιγραφής σε λογισμικό αποτελεί τη πράξη κατά την οποία οι crackers παραβιάζουν τα συστήματα προστασίας κάποιου λογισμικού που έχουν σχεδιαστεί για μη εξουσιοδοτημένη χρήση του.

⁵³ Aycok, J. Computer Viruses and Malware ,2006, <https://books.google.gr/books?hl=el&lr=&id=xnW->

⁵⁴ Hsiao, S.C., Kao, D.Y. ,2018, The static analysis of WannaCry Ransomware, <https://ieeexplore.ieee.org/abstract/document/8323680>

Ο δούρειος ίππος (Trojan Horse) αποτελεί έναν τύπο κακόβουλου λογισμικού , ο οποίος όπως και στην αρχαία Τροία, προσφέρεται ως μια φαινομενικά αθώα ή χρήσιμη οντότητα, αλλά στην πραγματικότητα κρύβει έναν κίνδυνο. Σκοπός του είναι η εξαπάτηση των χρηστών να τον εγκαταστήσουν στη συσκευή τους και ύστερα μπορούν οι δράστες να υποκλέψουν προσωπικές πληροφορίες ή να καταστρέψουν αρχεία. Οι δούρειοι ίπποι μεταδίδονται μέσω συνημμένων σε ηλεκτρονικό ταχυδρομείο, λήψης αρχείων ή ενημερώσεων λογισμικού. ⁵⁵

Οι συνέπειες του cracking στο πλαίσιο της οργανωμένης δράσης στο darknet είναι ποίκιλες και ιδιαίτερα επιβλαβείς. Αρχικά, παραμονεύουν σημαντικοί κίνδυνοι για τα άτομα, τις επιχειρήσεις και γενικότερα τη συνολική ασφάλεια του διαδικτύου. Οι επιχειρήσεις υφίστανται οικονομικές απώλειες και απειλείται η φήμη τους, ενώ στα άτομα διακυβεύεται η ιδιωτικότητα τους. Επίσης, υπονομεύεται η εμπιστοσύνη στο ψηφιακό οικοσύστημα και γενικά, ολόκληρη η εθνική ασφάλεια βρίσκεται σε κίνδυνο, καθώς το οργανωμένο έγκλημα επεκτείνεται και εξαπλώνεται πέρα από τα σύνορα.

Δεν πρόκειται απλώς για μεμονωμένες ενέργειες, αλλά οι crackers συνεργάζονται μεταξύ τους μέσω ενός πολύπλοκου συστήματος ανταλλαγής πληροφοριών και εργαλείων, το οποίο φέρει σε δυσχερή θέση τις αρχές σχετικά με την ανίχνευση τους και την εξάρθρωση των εγκληματικών δικτύων.

Τέλος, η συνηθέστερη κατηγορία χρηστών, οι οποίοι βρίσκονται στη βάση της πυραμίδας, είναι οι απλοί χρήστες, αντίστοιχοι των στρατιωτών, οι οποίοι μπορούν ύστερα φυσικά από ειδική άδεια των διαχειριστών ή των διαβαθμισμένων χρηστών, να συμμετέχουν σε οποιαδήποτε σχετική δραστηριότητα θέλουν. Ωστόσο, εάν οι απλοί χρήστες δημιουργήσουν την εντύπωση πως διαταράσσουν την ομαλή λειτουργία, κάποιου ή κάποιων δωματίων, τίθενται υπό περιορισμό και γίνονται περιορισμένοι χρήστες, καθώς παρακολουθούνται ηλεκτρονικά και απαγορεύεται η συμμετοχή τους σε κάποια δωμάτια. ⁵⁶

⁵⁵ Mishra U., An Introduction to Computer Viruses,2010, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916631

⁵⁶Nurse J., Bada M., The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations,2019, <https://arxiv.org/pdf/1901.01914>

Συνεπώς, αν και η δομή του οργανωμένου εγκλήματος στο darknet έχει προσαρμοστεί στο ψηφιακό τοπίο, όπου γενικά τα οργανωμένα εγκληματικά δίκτυα λειτουργούν με χαλαρούς και απρόσωπους δεσμούς, παραμένει σε έναν βαθμό αμετάβλητο το μοτίβο της ιεραρχίας και της συνεργασίας μεταξύ των μελών, όπως παρουσιάσαμε στη περίπτωση του παραδοσιακού οργανωμένου εγκλήματος. Στο πλαίσιο αυτό, η θετική αλληλεπίδραση μεταξύ αγοραστών και πωλητών, μέσω μηχανισμών όπως οι escrow, τους οποίους αναλύσαμε παραπάνω, δημιουργεί έναν επιπλέον παράγοντα εμπιστοσύνης και ασφάλειας.

4.6. Κατηγορίες οργανωμένων εγκλημάτων στο darknet

Το darknet, αποτελεί βάση πραγματοποίησης πολλών διαδικτυακών εγκλημάτων, καθώς πολλές οργανωμένες εγκληματικές δραστηριότητες μεταφέρονται εκεί λόγω των δυνατοτήτων, της ασφάλειας και της «κάλυψης» που προσφέρει.

Ορισμένες κατηγορίες εγκλημάτων εκ των ποικίλων που πραγματοποιούνται στο darknet και θα αναλυθούν ενδεικτικά στη παρούσα διπλωματική εργασία είναι η διακίνηση ναρκωτικών και η πώληση όπλων, η πορνογραφία και το e-trafficking , το έγκλημα ως υπηρεσία και το κυβερνοέγκλημα και οι οργανωμένες ανθρωποκτονίες κατόπιν πληρωμής.

4.6.1. Διακίνηση ναρκωτικών και πώληση όπλων

Το darknet έχει μετατραπεί σε βασικό άξονα σχετικά με την αγοραπωλησία ναρκωτικών ουσιών και όπλων, προσφέροντας στους ενδιαφερόμενους ανωνυμία και απεριόριστη γεωγραφική «συνεργασία». Διακινητές και αγοραστές δρουν σε κρυπτογραφημένα δίκτυα όπως το Tor, καθώς εκεί μπορούν να συναλλάσσονται χωρίς να αποκαλύπτουν ποτέ προσωπικές πληροφορίες. Οι αγορές στο darknet πραγματοποιούνται με κρυπτονομίσματα, επιτρέποντας ασφαλείς και μη ανιχνεύσιμες συναλλαγές, ενώ οι χρήστες εκμεταλλεύονται το όλο σύστημα για να συλλέξουν πληροφορίες σχετικά με μεθόδους απόκρυψης των ιδίων , της διανομής των ναρκωτικών και αποφυγής σύλληψης τους. Η λειτουργία τους βασίζεται σε μία δομή ιδιαίτερα

οργανωμένη, όπου οι διαχειριστές επιβλέπουν και ελέγχουν τις συναλλαγές, οι προμηθευτές φροντίζουν να διανείμουν τα ναρκωτικά και οι αγοραστές συναλλάσσονται κρυπτονομίσματα για να τα αγοράσουν.

Η χρήση του darknet στην εμπορία ναρκωτικών δεν περιορίζεται μόνο στις συναλλαγές, αλλά επεκτείνεται και στην εκπαίδευση των χρηστών, προσφέροντας οδηγίες για την παρασκευή ναρκωτικών, το ξέπλυμα των παράνομων εσόδων και την αποφυγή διώξεων, ενισχύοντας έτσι τη βιωσιμότητα και την ανθεκτικότητα αυτών των παράνομων αγορών.⁵⁷

Η διακίνηση ναρκωτικών και η εμπορία όπλων και εκρηκτικών αποτελεί και τη πιο συνηθισμένη εγκληματική δράση του οργανωμένου εγκλήματος στο darknet.

Σύμφωνα με εκτιμήσεις του 2024, τα ετήσια έσοδα από πωλήσεις εξαρτησιογόνων ουσιών στο darknet ξεπερνούν τα 1,7 δισεκατομμύρια δολάρια, ενώ η τάση είναι ανοδική, ιδιαίτερα στην Ευρώπη και τη Βόρεια Αμερική. Η ανωνυμία του Tor και η χρήση ιδιωτικών κρυπτονομισμάτων ενισχύουν τη δραστηριότητα, καθιστώντας δύσκολη την ανίχνευση εμπόρων και αγοραστών.⁵⁸

Μελέτες, πάλι, έχουν δείξει ότι το συνολικό κόστος του εμπορίου όπλων στο darknet είναι περίπου 80.000 δολάρια το μήνα, με τα πυροβόλα όπλα να αντιπροσωπεύουν σχεδόν το 90% των εσόδων.⁵⁹

Οι κυριότερες εξαρτησιογόνες ουσίες που διακινούνται είναι η κοκαΐνη, η ηρωίνη, οι αμφεταμίνες και οι μεθαμφεταμίνες, η κάνναβη, νέες ψυχοδραστικές ουσίες, αλλά και συνθετικά οπιοειδή.

Η κοκαΐνη προέρχεται κυρίως από χώρες της λατινικής Αμερικής, η ηρωίνη από τη νοτιοανατολική και νοτιοδυτική Ασία, ενώ η κάνναβη από το Μαρόκο, την Ολλανδία, την

⁵⁷ Siuda P., Swieca L, Cheba P., Shi H., "Similar to Legal Companies": Vendor Brands and Other Aspects of Marketing Communication in the Darknet Drug Trade, 2024, <https://www.tandfonline.com/doi/full/10.1080/01639625.2024.2428711#abstract>

⁵⁸ Adejumo O., Russian darknet dominated crypto drug trade in 2024 with \$1.65 billion transactions, 2025, <https://cryptoslate.com/russian-darknet-dominated-crypto-drug-trade-in-2024-with-1-65-billion-transactions>

⁵⁹ RAND, US weapons main source of illegal arms trade on the dark web, 2017, <https://www.rand.org/news/press/2017/07/19.html#:~:text=Sixty%20per%20cent%20of%20weapons,sale%20on%20the%20dark%20web.>

Ισπανία και την Αλβανία. Τέλος , συνθετικές και νέες ψυχοδραστικές ουσίες παράγονται κυρίως στην Ολλανδία, τη Πολωνία και την Κίνα, με τη φαιντανύλη να προέρχεται κυρίως από την Κίνα.

Στην περίπτωση των ναρκωτικών, οι οργανωμένες εγκληματικές ομάδες χρησιμοποιούν βία και διαφθορά προκειμένου να έχουν επιρροή και δύναμη στις αγορές. Συχνά μάλιστα εκμεταλλεύονται πτωχούς αγρότες , οι οποίοι εξαναγκάζονται να καλλιεργούν φυτά κοκαΐνης, καθώς βρίσκονται σε δυσχερή οικονομική κατάσταση και δεν έχουν άλλη επιλογή.

Σχετικά με τις συνθετικές ουσίες, οι οργανωμένες εγκληματικές ομάδες ιδιοποιούνται εργαστήρια παραγωγής ναρκωτικών, ενώ συνεργάζονται και με άλλες εγκληματικές οργανώσεις προκειμένου να παράξουν τα ναρκωτικά.

Γενικά, το πιο κρίσιμο σημείο του όλου εγχειρήματος είναι η μεταφορά επειδή σε αυτό το στάδιο είναι πιθανότερο να εντοπιστούν και να συλληφθούν. Όμως, εργαλεία όπως το darknet έχουν μειώσει και αυτή την πιθανότητα.

Το darknet , μέσω των δυνατοτήτων που προσφέρει, την ανωνυμία , την πρόσβαση στην παγκόσμια αγορά και μη ανιχνεύσιμους τρόπους συναλλαγών, λόγω του αποκεντρωμένου συστήματος που χαρακτηρίζει τα κρυπτονομισματα, έχει βοηθήσει ιδιαίτερα το οργανωμένο έγκλημα να διακινεί ναρκωτικά ενισχύοντας την επιχειρηματική του δράση. Οι πωλητές χρησιμοποιούν εξελιγμένες μεθόδους προκειμένου να κρυπτογραφούν τις διευθύνσεις αποστολής με παραπλανητικά δεδομένα και χρησιμοποιούν ακόμη και υπηρεσίες ταχυδρομείου για να διακινούν τα ναρκωτικά σε όλο τον κόσμο .⁶⁰

4.6.1.1. Επιχείρηση «Spector»

Η επιχείρηση «Spector», η οποία πραγματοποιήθηκε μεταξύ του 2021 με 2023, αποτελεί μια τις μεγαλύτερες διακρατικές δράσεις προκειμένου να καταπολεμηθεί το οργανωμένο έγκλημα στο darknet. Για την υλοποίηση της επιχείρησης συνεργάστηκαν εννέα κράτη: η

⁶⁰Bunea G., Marius I., Organized crime , drug trafficking, and the digital world : a concise perspective, University of Cluj Napoca, 2024, https://cuji.ubv.ro/ssh/article/view/61/70?fbclid=IwY2xjawJpu6JleHRuA2FibQlxMAABHrxeZu_mKxb7DVzGM1CwgKW9uPegCp4Cy2n

Αυστρία, η Γαλλία, η Γερμανία, η Πολωνία, η Ολλανδία, η Βραζιλία, η Ελβετία, το Ηνωμένο Βασίλειο και οι Ηνωμένες Πολιτείες της Αμερικής . Στόχος τους ήταν η αποσταθεροποίηση της πλατφόρμας Monopoly Market, μιας παράνομης αγορά ναρκωτικών στο darknet.

Η Monopoly Market αποδομήθηκε αρχικά το 2021 από τις γερμανικές διωκτικές αρχές, οι οποίες κατόρθωσαν να εισέλθουν στο κεντρικό της σύστημα και να αποκτήσουν πολλές σημαντικές πληροφορίες τόσο για τους αγοραστές όσο και για τους πωλητές. Τα δεδομένα αυτά , λοιπόν, διαδραμάτισαν σημαντικό ρόλο τόσο για τη διεθνή συνεργασία των 9 κρατών όσο και για συλλήψεις που πραγματοποιήθηκαν στη συνέχεια σε ποικίλο αριθμό χωρών. Συγκεκριμένα συνελλήφθησαν 288 άτομα, και κατασχέθηκαν 850 κιλά εξαρτησιογόνων ουσιών, 117 πυροβόλα όπλα και σχεδόν 51 εκατομμύρια δολάρια σε μετρητά και κρυπτονομίσματα.

Η συγκεκριμένη υπόθεση δείχνει πως το οργανωμένο έγκλημα προσαρμόζεται πλήρως στις νέες ψηφιακές καταστάσεις και αξιοποιεί στον μέγιστο δυνατό βαθμό τις τεχνολογίες ανώνυμης επικοινωνίας και συναλλαγών, τονίζοντας την ανάγκη διεθνικής, υπερκρατικής και διακρατικής δικαστικής και αστυνομικής συνεργασίας προκειμένου να εξαρθώνονται τέτοιου είδους κυκλώματα.

Μέσα από το παράδειγμα της επιχείρησης «Spector», λοιπόν, είδαμε πως στην περίπτωση των σκοτεινών αγορών, σε γενικές γραμμές διατηρείται ο σκοπός επίτευξης κέρδους, με τη μόνη διαφορά πως η υψηλή τεχνογνωσία μέσω της κρυπτογράφησης και άλλων μέσων , οδηγεί σε μεγάλη ψηφιακή ασφάλεια και αποφυγή εντοπισμού. Επίσης, η ικανότητα συντονισμού των εγκληματικών δικτύων σε διεθνή κλίμακα, η αποτελεσματική διαχείριση logistics για την αποστολή των ναρκωτικών με courier ,η χρήση πλαστών εγγράφων και ο καταμερισμός της εργασίας, κάνει την επιχειρησιακή δομή του οργανωμένου εγκλήματος ένα εγχείρημα ιδιαίτερα απαιτητικό για τις διωκτικές αρχές. Αυτές πρέπει να εκπαιδεύονται διαρκώς σε νέες τεχνολογίες για να μπορούν να αντιμετωπίζουν τις προκλήσεις του οργανωμένου εγκλήματος.⁶¹

⁶¹Europol, 288 dark web vendors arrested in major marketplace seizure, 2023, <https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure>

4.6.2. Πορνογραφία και e-trafficking

Η παράνομη πορνογραφία, ειδικά όταν περιλαμβάνει ανήλικους, αποτελεί ένα από τα πιο αποτρόπαια εγκλήματα του οργανωμένου εγκλήματος στο darknet. Πρόκειται για εγκληματικά δίκτυα, τα οποία εκμεταλλεύονται την ανωνυμία και την αδυναμία ελέγχου που υπάρχει στο darknet και έχουν μετατρέψει μια ακραία και απάνθρωπη έκνομη πράξη σε ένα κερδοφόρο επιχειρηματικό εγχείρημα.

Η πορνογραφία είναι στενά συνδεδεμένη με το trafficking, καθώς πολλές φορές αποτελεί καθαρό προϊόν εμπορίας ανθρώπων. Τα θύματα trafficking εξαναγκάζονται να επιδίδονται σε σεξουαλικές πράξεις, οι οποίες καταγράφονται και χρησιμοποιούνται για την παραγωγή πορνογραφικού υλικού, ενισχύοντας έτσι τον κύκλο εκμετάλλευσης.

Η εμπορία ανθρώπων είναι η στρατολόγηση, μεταφορά, φιλοξενία ή υποδοχή ατόμων μέσω βίας, απάτης ή εξαναγκασμού με σκοπό την εκμετάλλευση. Αυτή η εκμετάλλευση μπορεί να περιλαμβάνει καταναγκαστική εργασία, σεξουαλική δουλεία ή άλλες μορφές εμπορικής σεξουαλικής εκμετάλλευσης. Συνεπώς, η διεθνής νομοθεσία, οι εθνικές πολιτικές και οι κρατικές οργανώσεις καταβάλουν σημαντική προσπάθεια για την καταπολέμηση της εμπορίας ανθρώπων, αφού αποτελεί σοβαρή παραβίαση των ανθρωπίνων δικαιωμάτων και μία μορφή σύγχρονης δουλείας.⁶²

Στη σύγχρονη εποχή το darknet προσφέρει μοναδικές ευκαιρίες στο trafficking. Τα θύματα προσεγγίζονται μέσω διαδικτυακών πλατφορμών στο surface net και εκεί οι δράστες τους προσφέρουν «θέσεις εργασίας» ή «ερωτικό ενδιαφέρον» για να χτιστεί μία ρομαντική σχέση. Στη συνέχεια, το οργανωμένο έγκλημα χρησιμοποιεί τα προαναφερθέντα σκοτεινά δωμάτια και γενικότερα τα marketplaces του darknet, προκειμένου να διαφημίσουν τις υπηρεσίες που προσφέρουν τα θύματα, να δημοπρατήσουν γυναίκες, μικρά κορίτσια και αγόρια βάσει των εμφανισιακών τους χαρακτηριστικών, να διακινήσουν βίντεο και φωτογραφίες από βιασμούς και σωματικές κακοποιήσεις και να οργανώσουν ζωντανές μεταδόσεις και πάλι κατά τη διάρκεια βιασμού των θυμάτων. Οι εγκληματικές οργανώσεις συνεργάζονται μεταξύ τους και ανταλλάσσουν υλικό και υπηρεσίες. Η μεγάλη ζήτηση που υπάρχει στο darknet για

⁶²Zimmerman C., Kiss L., Human trafficking and exploitation: A global health concern, 2017, <https://pmc.ncbi.nlm.nih.gov/articles/PMC5699819/>

τέτοιου είδους περιεχόμενο , ενισχύει αυτή την εγκληματική δράση του οργανωμένου εγκλήματος δημιουργώντας μία ιδιαίτερα προσοδοφόρα αγορά. Επίσης, η δημιουργία υλικού πολλές φορές γίνεται κατόπιν "παραγγελίας", δηλαδή ύστερα από αιτήματα των ενδιαφερόμενων θεατών προς τους δράστες για την παραγωγή συγκεκριμένου πορνογραφικού περιεχομένου, το οποίο αυξάνει την ήδη υπάρχουσα απειλή.⁶³ Σύμφωνα με το UNODC (2024), ο αριθμός των θυμάτων το 2022 αυξήθηκε κατά 25% συγκριτικά με τα πριν την πανδημία δεδομένα (2019). Γενικά, οι ανήλικοι αποτελούν το 38% των θυμάτων, ενώ οι γυναίκες και τα μικρά κορίτσια αποτελούν το 60% των θυμάτων.⁶⁴

Το δίκτυο Tor χρησιμοποιείται ευρέως τόσο για την αγορά όσο και για τη διακίνηση υλικού και υπηρεσιών παιδικής κακοποίησης και πορνογραφίας (CSAM – Child Sexual Abuse Material). Σύμφωνα με διεθνή έρευνα που πραγματοποιήθηκε από μία ερευνητική ομάδα του Τεχνολογικού Πανεπιστημίου Tampere στη Φινλανδία μεταξύ του 2018 με 2023, όπου εξετάστηκαν 176.683 ιστοσελίδες του Tor, αποκαλύφθηκε ότι περίπου το ένα πέμπτο αυτών των ιστοσελίδων φιλοξενούσε περιεχόμενο CSAM. Επιπλέον, το CSAM βρέθηκε να είναι εύκολα προσβάσιμο μέσω 21 από τις 26 πιο διαδεδομένες μηχανές αναζήτησης που λειτουργούν στο Tor.

Επιπλέον, στην ίδια μελέτη εξετάστηκαν 110.133.715 συνεδρίες αναζήτησης στο Tor⁶⁵, όπου αποδείχθηκε ότι το 11,1% των αναζητήσεων σχετίζονταν με το CSAM. Όσον αφορά το ενδιαφέρον αναζήτησης ανά ηλικία, το 40,5% των αναζητήσεων απευθύνονταν σε παιδιά ηλικίας 11 ετών και κάτω, 11,0% επικεντρώθηκε σε παιδιά ηλικίας 12 ετών, 8,2% σε παιδιά 13 ετών, 11,6% σε 14 ετών, 10,9% σε 15 ετών και 12,7% σε 16 ετών.

Η μελέτη αυτή ,λοιπόν, εισήγαγε αποτελεσματικούς μηχανισμούς φιλτραρίσματος για τις μηχανές αναζήτησης, εφάρμοσε στρατηγικές παρέμβασης και παρουσίασε ένα ερωτηματολόγιο σε χρήστες που αναζητούν ή καταναλώνουν περιεχόμενο CSAM. Μια ανάλυση 11.470 απαντήσεων αποκάλυψε ότι το 65,3% των χρηστών CSAM εκτέθηκαν για πρώτη φορά σε τέτοιο υλικό κατά τη διάρκεια της παιδικής τους ηλικίας. Επιπλέον, οι

⁶³Κάλλιου Ε, E- trafficking, εμπορία ανθρώπων στο διαδίκτυο,2023, <https://www.crimetimes.gr/e-trafficking-εμπορία-ανθρώπων-στο-διαδίκτυο/>

⁶⁴ United Nations Office on Drugs and Crime(UNODC), Global report in trafficking in persons, σελ.39-43 https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

⁶⁵ Ως «συνεδρία αναζήτησης» νοείται το σύνολο των αναζητήσεων που πραγματοποιεί κάποιος στο δίκτυο Tor πριν αποσυνδεθεί.

μισοί από τους ερωτηθέντες ανέφεραν ότι η αρχική τους επαφή με το CSAM έγινε κατά λάθος, υπογραμμίζοντας την ευκολία προσβασιμότητας του υλικού.⁶⁶

Γενικά, η παράνομη διακίνηση πορνογραφικού υλικού είναι ένα φαινόμενο που διαρκώς εξελίσσεται και έχει πλέον λάβει τεράστιες διαστάσεις. Το φαινόμενο αυτό περιλαμβάνει τη δημιουργία, αποθήκευση, διανομή ή πώληση πορνογραφικού υλικού χωρίς τη συναίνεση των ατόμων που απεικονίζονται σε αυτό. Οι εγκληματίες χρησιμοποιούν το darknet, ώστε να έχουν τη δυνατότητα να διακινούν το πορνογραφικό υλικό χωρίς αντιδράσεις. Παρ' όλα αυτά η πρόσβαση δεν είναι εύκολη και ανοιχτή για όλους σε τέτοιου είδους θεάματα, αφού απαραίτητη είναι η καταβολή κάποιου αντιτίμου ή κάποιος ειδικός κωδικός πρόσβασης για την πραγματοποίηση εισόδου.

Η εξέλιξη της τεχνολογίας σε συνδυασμό με την ανωνυμία που δίδει το darknet, έχει επιτρέψει την ταχεία διάδοση του φαινομένου και έχει ως επίκεντρο την παιδική πορνογραφία. Γενικότερα, μέχρι το 1960 η νομοθεσία δεν ήταν ιδιαίτερα αυστηρή και χρειάστηκαν τουλάχιστον 20 έτη μέχρι να αλλάξει αυτό και να αρχίσει να αντιμετωπίζεται το φαινόμενο όπως αρμόζει. Η παιδική πορνογραφία είναι ευρέως διαδεδομένη, αποτελώντας ένα από τα πιο προσοδοφόρα εγκλήματα μετά τη διακίνηση ναρκωτικών, ειδικά σε χώρες όπως οι ΗΠΑ και η Κίνα που παρουσιάζουν ιδιαίτερα μεγάλα ποσοστά παραγωγής και διακίνησης υλικού. Τέλος, όσοι ασχολούνται με αυτό δεν σημαίνει απαραίτητα πως αποσκοπούν στην προσωπική ευχαρίστηση αλλά μπορεί να στοχεύουν αποκλειστικά στο χρηματικό κέρδος. Επίσης, το νομικό κενό λόγω της διαφοροποίησης της νομοθεσίας από κράτος σε κράτος, δίνει έναυσμα για την περεταίρω διασπορά του φαινομένου.

Στην περίπτωση του e-trafficking, τα κέρδη του το οργανωμένου εγκλήματος είναι τεράστια. Σ' αυτό έχει συμβάλει η τεχνογνωσία που διαθέτει τόσο για την απόκρυψη της ταυτότητας των μελών και γενικά των εμπλεκομένων, όσο και για τη στρατολόγηση, διακίνηση και εκμετάλλευση των θυμάτων.

⁶⁶ Nurmi J., Paju A., Brumley B., Insoll T., Ovaska A., Soloveva V., Vaaranen-Valkonen N., Aaltonen M., Arroyo D., Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy, Cornell University ,2024, <https://arxiv.org/abs/2404.14112>

4.6.2.1. Υπόθεση Playpen

Το Playpen αποτελούσε μια από τις μεγαλύτερες ιστοσελίδες διακίνησης περιεχομένου παιδικής πορνογραφίας και αποκάλυψε πολλές πληροφορίες για τον τρόπο που εκμεταλλεύεται το οργανωμένο έγκλημα το darknet προκειμένου να πλουτίσει από τη διάδοση υλικού σεξουαλικής κακοποίησης παιδιών.

Η ιστοσελίδα αυτή είχε πάνω από 215.000 χρήστες και 23.000 αρχεία και ήταν δομημένη ανά ηλικία, φύλο και είδος σεξουαλικής δραστηριότητας.

Το playpen λειτουργούσε ένα καλά οργανωμένο δίκτυο διαχειριστών, είχε συνεχή τεχνική υποστήριξη και μέλη τα οποία διευκόλυναν τη διακίνηση σχετικού υλικού.

Το 2014, το FBI έλαβε πληροφορίες από την Kripos (τη νορβηγική αστυνομία), σχετικά με μια πραγματική διεύθυνση IP, την οποία η Kripos εντόπισε στις ΗΠΑ και έτσι το FBI ξεκίνησε την επιχείρηση «Pacifier», μία μυστική επιχείρηση με σκοπό την αντιμετώπιση της παιδικής πορνογραφίας στο darknet. Αυτή περιελάμβανε τη διαχείριση και τον έλεγχο της ιστοσελίδας και τη χρήση ενός κακόβουλου λογισμικού, το οποίο ονομάστηκε NIT (Network Investigation Technique). Μετά από εκτεταμένη έρευνα, το FBI κατάσχεσε αυτόν τον διακομιστή και συνέλαβε τον Steven W. Chase, δημιουργό και κύριο διαχειριστή του Playpen. Ωστόσο, το FBI συνέχισε να χρησιμοποιεί αυτό το λογισμικό (NIT) , με σκοπό να εντοπίσει και ανακαλύψει και άλλα μέλη του οργανωμένου εγκληματικού δικτύου που εμπλεκόταν στη λειτουργία της ιστοσελίδας. Αυτό είχε ως αποτέλεσμα πάνω από 900 συλλήψεις και τη διάσωση 296 παιδιών.⁶⁷

Τελικά, ο επικεφαλής του Playpen, δηλαδή ο Chase, καταδικάστηκε σε 30 χρόνια κάθειρξης ενώ οι διαχειριστές, Michael Fuckiger και David Browning, σε 20 χρόνια φυλάκισης.⁶⁸

⁶⁷Rumold M., Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation, 2016, <https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation>

⁶⁸United States Attorneys Office, Indiana Man Sentenced To Prison For Engaging In A Child Exploitation Enterprise, 2017, <https://www.justice.gov/usao-wdnc/pr/indiana-man-sentenced-prison-engaging-child-exploitation-enterprise>

4.6.3. Έγκλημα ως υπηρεσία και κυβερνοέγκλημα

Ο ρόλος του διαδικτύου στο οργανωμένο έγκλημα εξελίσσεται και επεκτείνεται με ταχύτατους ρυθμούς με το πρώτο να εκμεταλλεύεται τα ιδιαίτερα χαρακτηριστικά που προσφέρει το darknet προκειμένου να λειτουργήσει τόσο επιχειρησιακά, πωλώντας κακόβουλα προγράμματα, ιούς και αλλά παρεμφερή (ransomware-as-a-service) , όσο και ιδιαίτερα καταστροφικά καθώς εξαπολύονται συχνά επιθέσεις σε τράπεζες, κυβερνητικούς οργανισμούς, επιχειρήσεις, ακόμη και ολόκληρα κράτη.

Όσον αφορά το πρώτο, το έγκλημα που παρέχεται ως υπηρεσία (ransomware-as-a-service), οι δράστες προσφέρουν μέσα, εργαλεία και γνώσεις έναντι αντιτίμου σε κρυπτονομίσματα. Μία από τις πιο συνηθισμένες περιπτώσεις παροχής εγκληματικών υπηρεσιών αποτελούν οι λεγόμενες επιθέσεις DDoS (Distributed Denial of Service), όπου οι δράστες χρησιμοποιούν ένα δίκτυο υπολογιστών (botnet), προκειμένου να στείλουν μαζικά αιτήματα σε ένα διακομιστή και να τον μολύνουν με κακόβουλο λογισμικό ώστε να μη μπορεί να χρησιμοποιηθεί μελλοντικά από τους χρήστες. Το κακόβουλο λογισμικό (malware) εισέρχεται σε έναν ηλεκτρονικό υπολογιστή με σκοπό να του προκαλέσει ζημιά διαγράφοντας ή τροποποιώντας δεδομένα και προγράμματα, παρεμποδίζοντας τη λειτουργία ενός συστήματος ή υποκλέπτοντας σημαντικά δεδομένα.

Αντίστοιχα, μπορούν να προσφερθούν υπηρεσίες για τη δημιουργία malware, που στοχεύουν στη λήψη προσωπικών ή οικονομικών δεδομένων από τα θύματα προς μελλοντική εκμετάλλευση. Αυτό μπορεί να περιλαμβάνει ιούς, δούρειους ίππους (trojan horses) ,τύπο κακόβουλου λογισμικού που κρύβονται πίσω από φαινομενικά αθώα ή χρήσιμα αρχεία ή ransomware ,δηλαδή κακόβουλο λογισμικό που κλειδώνει τα αρχεία ενός χρήστη και ζητά χρηματικό αντίτιμο για τη διόρθωση τους.

Τέλος, στο darknet προσφέρονται υπηρεσίες phishing, δηλαδή μία μορφή διαδικτυακής απάτης κατά την οποία ο χρήστης υποδύεται μια οντότητα ή οργανισμό για να αποσπάσει προσωπικά δεδομένα, κωδικούς πρόσβασης και τραπεζικές πληροφορίες, συνήθως με σκοπό το κέρδος. Οι επιθέσεις phishing μπορούν να λάβουν διάφορες μορφές, συμπεριλαμβανομένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από έγκυρες πηγές, όπως τράπεζες, κυβερνητικές υπηρεσίες ή

και άλλες οργανώσεις με σκοπό την απόσπαση προσωπικών δεδομένων από τους χρήστες.

Πέραν όμως της προσφοράς υπηρεσιών και σύμφωνα με τη UNODC, τα οργανωμένα εγκληματικά δίκτυα δραστηριοποιούνται και τα ίδια μέσω του darknet σε διάφορες μορφές κυβερνοεγκλημάτων π.χ. phishing, δημιουργία και διανομή κακόβουλου λογισμικού, επιθέσεις DDoS κ.α. εκμεταλλευόμενα τις νέες και διαρκώς εξελισσόμενες τεχνολογίες πληροφορικής και επικοινωνίας. Η συμπερίληψη κυβερνοεγκληματιών στο οργανωμένο έγκλημα, δημιουργεί ένα περιβάλλον ιδιαίτερα καταστροφικό και δύσκολα ανιχνεύσιμο με την ενίσχυση της διεθνούς συνεργασίας και την εξειδίκευση των διωκτικών αρχών να καθίσταται πιο έντονα από ποτέ.⁶⁹ Η αιτία έγκειται και πάλι σε έκθεση της UNODC, η οποία τονίζει πως η βιομηχανία όλων αυτών των κυβερνοεγκλημάτων επεκτείνεται παγκόσμια και ραγδαία, φτάνοντας στη Νότια Αμερική, την Αφρική και την Ανατολική Ευρώπη, κάτι που αποδεικνύει τη διασύνδεση του παραδοσιακού οργανωμένου εγκλήματος με τις δυνατότητες που προσφέρει το darknet. Η οργάνωση αυτών πραγματοποιείται κυρίως από ασιατικά εγκληματικά συνδικάτα και περιλαμβάνουν χιλιάδες εργαζόμενους οι οποίοι μάλιστα έχουν εξαναγκαστεί να δραστηριοποιούνται στο χώρο αυτό, παραπέμποντας σε ψηφιακή εμπορία ανθρώπων. Παρά τις προσπάθειες αντεγκληματικής πολιτικής, τα εγκληματικά δίκτυα προσαρμόζονται και μεταφέρουν τις δραστηριότητες τους σε λιγότερο ελεγχόμενες περιοχές, όπως το Λάος και η Καμπότζη.⁷⁰ Συγκεκριμένα, το 2024, οι οικονομικές ζημιές από κυβερνοεγκλήματα ξεπέρασαν τα 16 δισεκατομμύρια δολάρια, παρουσιάζοντας αύξηση 33% συγκριτικά με το 2023, ενώ οι επιθέσεις ransomware, δηλαδή η διασπορά κακόβουλου λογισμικού, έχουν αυξηθεί σε τομείς υγειονομικής περίθαλψης και χρηματοπιστωτικά ιδρύματα κατά 9%.⁷¹

⁶⁹UNODC, Cyber organized crime activities, 2019, <https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html>

⁷⁰ UNODC, Cyberfraud in the Mekong reaches inflection point, UNODC reveals, 2025, <https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html>

⁷¹Vicens A.J., Reports of ransomware attacks on US infrastructure rise nine percent, 2025, <https://www.itnews.com.au/news/reports-of-ransomware-attacks-on-us-infrastructure-rise-9-percent-616744>

4.6.3.1. Υπόθεση REvil

Η REvil (Ransomware Evil) αποτελούσε μια ρωσόφωνη ιδιωτική επιχείρηση τύπου «ransomware-as-a-service» με βάση τη Ρωσία. Μέσω του μοντέλου αυτού η REvil πωλούσε προϊόντα κυβερνοεγκλήματος σε άλλες οργανωμένες ομάδες, με εκείνη να διατηρεί το 20-30% από το χρηματικό αντίτιμο που καταβαλλόταν από τα θύματα (λύτρα).⁷²

Ο τρόπος με τον οποίο ο REvil (ο ιός, ο οποίος ήταν ταυτόνυμος της επιχείρησης) εισερχόταν στα συστήματα των θυμάτων ακολουθούσε την εξής λογική: οι διαδικτυακοί εισβολείς (hackers) μεν εκμεταλλεύονταν «zero-day» ευπάθειες στα λογισμικά τους, δηλαδή κενά ασφαλείας που οι δημιουργοί των λογισμικών (π.χ. Microsoft) δεν είχαν ανιχνεύσει, ενώ παράλληλα παραβίαζαν και διακομιστές RDP (Remote Desktop Protocol), πρωτόκολλο που ξεκίνησε η Microsoft, προκειμένου να μπορούν να έχουν πρόσβαση ακόμη και στους πιο απομακρυσμένους υπολογιστές. Επίσης, χρησιμοποιούσαν τη τεχνική του phishing προκειμένου να εξαπατήσουν τα θύματα τους, τα οποία επέτρεπαν στους δράστες την πρόσβαση σε όλα τα ευαίσθητα δεδομένα στη συσκευή τους. Αυτό πραγματοποιούνταν μέσω της εγκατάστασης ειδικά διαμορφωμένων προγραμμάτων, ικανών πρώτα να εξαγάγουν και μετά να κρυπτογραφήσουν αρχεία π.χ. ενός οργανισμού, μετατρέποντας τα σε μη προσβάσιμο υλικό για τους αρχικούς χρήστες. Μετά την επίθεση οι δράστες ζητούσαν ένα συγκεκριμένο χρηματικό ποσό από τα θύματα σε κρυπτονομίσματα προκειμένου να παρέχουν το απαραίτητο κλειδί αποκρυπτογράφησης για να μπορέσουν τα θύματα να επανακτήσουν τις πληροφορίες πίσω στην κατοχή τους.

Η οργάνωση και η λειτουργία της "επιχείρησης", της επέτρεψε να πραγματοποιεί επιθέσεις με υψηλό ποσοστό επιτυχίας, χωρίς ιδιαίτερα προβλήματα κατά την εγκληματική της δράση και χρησιμοποιούσε κρυπτονομίσματα τόσο για τις εισπράξεις των λύτρων, όσο και για την εξασφάλιση της ανωνυμίας και προστασίας των αρχών από τις διωκτικές αρχές. Η ομάδα είχε επιχειρήσει να εκβιάσει ποικίλα δημόσια πρόσωπα και εταιρείες με τη δημοσιοποίηση ευαίσθητων πληροφοριών στο blog της, Happy Blog, το

⁷² Η REvil πωλούσε κακόβουλο λογισμικό ransomware σε άλλα οργανωμένα εγκληματικά δίκτυα, το οποίο κρυπτογραφούσε σημαντικά αρχεία των θυμάτων και στη συνέχεια, ζητούσε από αυτά (τα θύματα) λύτρα, προκειμένου να τους δώσει το κατάλληλο κλειδί προκειμένου να τα αποκρυπτογραφήσουν και να λάβουν τις σημαντικές πληροφορίες που τα αφορούν πίσω.

οποίο λειτουργούσε στο darknet.⁷³ Για παράδειγμα τον Μάιο του 2020, ζήτησαν από τον πρόεδρο των ΗΠΑ, Donald Trump, 42 εκατομμύρια δολάρια, ισχυριζόμενοι πως εισέβαλαν στη νομική εταιρεία Grubman Shire Meiselas & Sacks , η οποία διαχειριζόταν ευαίσθητα νομικά του έγγραφα, απειλώντας τον ότι θα τα δημοσιοποιήσουν. Προς απόδειξη αυτού, δημοσιοποίησαν ορισμένα δείγματα από άλλους επώνυμους πελάτες της εταιρείας, όπως εκείνα της Lady Gaga και της Madonna, αλλά έγγραφα του Trump τελικά δεν δημοσιεύθηκαν ποτέ και η ίδια η νομική εταιρεία ισχυρίστηκε πως δεν τον είχε ποτέ πελάτη.⁷⁴

Στις 30 Μαΐου του 2021, η REvil επιτέθηκε κατά του παγκόσμιου βιομηχανικού κολοσσού τροφίμων JBS USA, πράξη που εξανάγκασε τη διακοπή λειτουργίας όλων των εργοστασίων βοείου κρέατος στις εταιρείες των ΗΠΑ, καθώς και των εργοστασίων πουλερικών και χοιρινού. Ως αποτέλεσμα η JBS , κατέβαλε στη REvil 11 εκατομμύρια δολάρια ώστε να κατορθώσει να αποκαταστήσει τη ζημιά.⁷⁵

Μια από τις γνωστότερες επιθέσεις της REvil, ήταν εκείνη κατά της Kaseya, εταιρείας παροχής λογισμικού για τη διαχείριση IT υπηρεσιών, τον Ιούλιο του 2021, η οποία επηρέασε σε μεγάλη κλίμακα τουλάχιστον 1.500 επιχειρήσεις σε παγκόσμιο επίπεδο. Αυτή τη φορά ζήτησε λύτρα 70 εκατομμύρια δολάρια σε κρυπτονομίσματα απειλώντας πως θα δημοσιοποιήσει και πάλι ευαίσθητες πληροφορίες των θυμάτων.⁷⁶

Προκειμένου να αντιμετωπιστεί το όλο ζήτημα, τον Ιούλιο του 2021, ο πρόεδρος των ΗΠΑ, Jo Biden, επικοινωνήσε με τον Πρόεδρο της Ρωσίας, Vladimir Putin, ώστε να ληφθούν μέτρα αντιμετώπισης ομάδων ransomware-as-a-service στα ρωσικά εδάφη. Λίγες μέρες αργότερα, στις 13 Ιουλίου, οι υποδομές της REvil εξαφανίστηκαν εντελώς και μυστηριωδώς από το διαδίκτυο. Τον Σεπτέμβριο του 2021, η εταιρεία κυβερνοασφαλείας Bitdefender, παρείχε σε όλα τα θύματα της REvil εργαλεία αποκρυπτογράφησης, με

⁷³ Akamai, What is REvil?, 2024, <https://www.akamai.com/glossary/what-is-revil>

⁷⁴ Winder D., Hackers Publish First 169 Trump 'Dirty Laundry' Emails After Being Branded Cyber-Terrorists, 2020, <https://www.forbes.com/sites/daveywinder/2020/05/17/hackers-publish-first-169-trump-dirty-laundry-emails-after-being-branded-cyber-terrorists/>

⁷⁵ Myre G, How Bitcoin Has Fueled Ransomware Attacks, 2021, <https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks>

⁷⁶ Sason D., REvil Ransomware Attack on Kaseya VSA: What You Need to Know, 2021, <https://www.varonis.com/blog/revil-msp-supply-chain-attack>

τουλάχιστον 14.000 από αυτά να ανακτούν πίσω τα δεδομένα τους. Έτσι, απέτρεψε την καταβολή λύτρων αξίας 550 εκατομμυρίων δολαρίων στη REvil.

Τον Σεπτέμβριο του 2021, η εγκληματική ομάδα επιχείρησε να ανακτήσει τις υποδομές της, που είχαν εξαφανιστεί τον περασμένο Ιούλιο, αλλά εμποδίστηκε από τις διεθνείς αρχές.

Τελικά, στις 14 Ιανουαρίου 2022, η Ομοσπονδιακή Υπηρεσία Ασφαλείας της Ρωσίας (FSB) συνέλαβε 14 άτομα της REvil. Από τα άτομα αυτά κατασχέθηκαν 425 εκατομμύρια ρούβλια (περίπου 5,6 εκατομμύρια δολάρια), περίπου 60 εκατομμύρια δολάρια σε μετρητά, περίπου 500.000 ευρώ, μεγάλος αριθμός κρυπτονομισμάτων και 20 πολυτελή αυτοκίνητα. Στο εγχείρημα αυτό συμμετείχε η Interpol, η Europol και το FBI, ανακηρύσσοντας τη REvil ως μια από τις πιο επικίνδυνες εγκληματικές ομάδες κυβερνοεγκληματος που έχει υπάρξει ποτέ.

Φαίνεται, λοιπόν, πως η ανάγκη διεθνούς συνεργασίας για την αντιμετώπιση του σύγχρονου οργανωμένου εγκλήματος είναι υψίστης σημασίας, αφού πλέον τίθενται στο επίκεντρο οι κρίσιμες υποδομές κρατών, η οικονομία και η ασφάλεια των πολιτών.⁷⁷

4.6.4. Hitman for hire

Η ανωνυμία και η αδιαφάνεια που προσφέρει το darknet, έχει ευνοήσει επικίνδυνες επιχειρηματικές δραστηριότητες. Ένα τέτοιο παράδειγμα είναι η πρόσληψη εκτελεστών για ανθρωποκτονίες, με σκοπό την εξυπηρέτηση προσωπικών ή επιχειρηματικών συμφερόντων. Η συναλλαγή, και σε αυτή τη περίπτωση, γίνεται με κρυπτονομίσματα.

Πολλές φορές, οι αγγελίες αυτές είναι άπατες (scams) και σκοπός τους είναι η αποκόμιση κέρδους χωρίς ποτέ να προσφέρουν όντως την υπηρεσία. Σύμφωνα με μελέτη του Holt (2020), το κόστος για την πρόσληψη εκτελεστή κυμαίνεται στα 20.000 δολάρια

⁷⁷ Spanga N., Russia arrests 14 alleged members of REvil ransomware gang, 2022, <https://www.cbsnews.com/news/ransomware-russia-arrests-revil/>

και τα εγκληματικά δίκτυα διαχωρίζουν καθήκοντα μεταξύ των διαμεσολαβητών⁷⁸ και εφαρμόζουν εσωτερικούς ελεγχους. Τα τεχνικά και οργανωτικά μέσα που χρησιμοποιούν τα εγκληματικά δίκτυα ενισχύονται λόγω της τεχνολογίας και των δυνατοτήτων που προσφέρει το Tor και το ανώνυμο και αποκεντρωμένο σύστημα των κρυπτονομισμάτων.

79

4.6.4.1. Η περίπτωση του Besa Mafia

Ένα από τα πιο διαδεδομένα παραδείγματα πρόσληψης δολοφόνου στο darknet , είναι η ιστοσελίδα Besa Mafia, της οποίας το όνομα προήλθε από την Αλβανική μαφία και το ηθικό δόγμα της "μπέσας", δηλαδή της αξιοπιστίας. Τελικά αποδείχθηκε πως πρόκειται για απάτη και δεν πραγματοποιούνταν οι υποσχόμενες δολοφονίες. Παρ' όλα αυτά οι προθέσεις των πελατών ήταν πραγματικές, γεγονός που οδήγησε σε συλλήψεις.

Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση της Kristy Lynn Felkins, κατοίκου της πόλης Fallon της Nevada, η οποία μέσω της ιστοσελίδας Besa Mafia επιχείρησε να δολοφονήσει τον πρώην σύζυγο της. Παρείχε , λοιπόν στο διαχειριστή πληροφορίες σχετικά με τη διεύθυνση του , τα ταξιδιωτικά του σχέδια και γενικά τοποθεσίες που επισκεπτόταν συχνά, ενώ ταυτόχρονα ισχυρίστηκε πως θα ήταν ευκαίιο να τραυματιστεί και η νυν σύζυγος του κατά την εκτέλεση. Αρχικά προσέφερε 13 bitcoin, αξίας 5.000 δολαρίων εκείνη την εποχή (το 2016) και στη συνέχεια προσέθεσε άλλες 4.000 δολάρια για να επιταχυνθεί η διαδικασία . Τελικά , μετά τον εντοπισμό και την αποκάλυψη της Besa Mafia πως πρόκειται για απάτη, ανιχνεύθηκαν τα μηνύματα της Felkins με τον διαχειριστή και συνελλήφθη. Κατά τη δικαστική διαδικασία δήλωσε ένοχη και το 2023 καταδικάστηκε σε πέντε χρόνια κάθειρξης και τρία χρόνια επιτήρησης μετά την αποφυλάκιση της.⁸⁰

⁷⁸ Οι διαμεσολαβητές αποτελούν μέλη ή εξωτερικούς συνεργάτες της οργάνωσης που συντονίζουν πελάτες και εκτελεστές , εξασφαλίζοντας την ανωνυμία και τη διαχείριση των πληρωμών στο darknet.

⁷⁹ Schondelmayer L., Hiring a hitman on the web: Can contractual violence be added to your online shopping cart?, 2020, <https://socialscience.msu.edu/news-events/news/archives/2020/2020-08-14.html>

⁸⁰ Theguardians.com, US woman who hired hitman using bitcoin to kill ex-husband gets five years in prison, 2023, <https://www.theguardian.com/technology/2023/jul/22/nevada-woman-hired-hitman-kill-ex-husband-sentenced>

Η υπόθεση της Besa Mafia αποκαλύπτει τους κινδύνους που βρίσκονται στο darknet, ακόμη και αν πρόκειται για άπατες, καθώς ενεργοποιεί πραγματικές προθέσεις και ανάγκη για συνεχή επιτήρηση και συνεργασία μεταξύ των διωκτικών αρχών.

5. Επιστημολογικά ζητήματα και δυσκολίες στη μελέτη του οργανωμένου εγκλήματος στο Darknet

Η επιστημολογία αποτελεί την επιστήμη που μελετά τη φύση της γνώσης, πως παράγεται, τι πραγματεύεται, τι μεθόδους και τεχνικές χρησιμοποιεί, ποια διαδικασία χρησιμοποιείται μέχρι ένα αποτέλεσμα και κάτω από ποιες προϋποθέσεις επαληθεύεται. Η γνώση αποκτάται με βάση την επιστημονική έρευνα, δηλαδή συστηματική διερεύνηση, συλλογή δεδομένων, ανάλυση και ερμηνεία. Ωστόσο, από την άλλη πρόκειται για ένα κοινωνικό κατασκεύασμα, αφού οι αξίες του ερευνητή επηρεάζονται από εκείνες του συμμετέχοντος, καθώς και από προσωπικά του βιώματα. Άρα η γνώση είναι υποκειμενική.

Στον τομέα των κοινωνικών επιστημών, όπως είναι εκείνη της εγκληματολογίας, η επιστημολογία βοηθά τον ερευνητή να κατανοήσει ζητήματα γύρω από το έγκλημα, τα εργαλεία που θα χρησιμοποιήσει για να το μελετήσει και το κατά πόσο αξιόπιστα είναι τα δεδομένα που προκύπτουν.⁸¹ Όσον αφορά το θέμα της παρούσας διπλωματικής, η επιστημολογία αποτελεί χρήσιμο εργαλείο και μέσο για να κατανοήσει κανείς τα ερευνητικά όρια: αν υπάρχει η δυνατότητα να γνωρίζουμε τι συμβαίνει με βεβαιότητα, κατά πόσο τα δεδομένα που συλλέγουμε ταυτίζονται με την πραγματικότητα και πως μπορούμε σε έναν βαθμό να αποφύγουμε λανθασμένα συμπεράσματα και προκαταλήψεις.

5.1. Πληροφόρηση από ΜΜΕ, κρατικούς φορείς και διωκτικές αρχές

Τα ΜΜΕ έχουν γενικά τη τάση να δραματοποιούν τα γεγονότα και να τα υπεραπλουστευούν προκειμένου συνήθως είτε να εξυπηρετήσουν πολιτικές σκοπιμότητες είτε να αυξήσουν το κοινό τους. Σπανίως γίνεται αναφορά στους βαθύτερους κοινωνικούς

⁸¹ Λαμπροπούλου Ε., Μεταπτυχιακό Εγκληματολογίας, Πάντειο Πανεπιστήμιο, Μάθημα: Επιστημολογικά ζητήματα εγκληματολογίας, Κοινωνικών και Πολιτικών Επιστημών, Διάλεξη: 14/11/2024

και οικονομικούς παράγοντες ανάπτυξης της εγκληματικότητας, ενώ το συγκινησιακό λεξιλόγιο δημιουργεί άλλοτε φόβο και άλλοτε αγανάκτηση στους πολίτες, οι οποίοι επιζητούν αυστηρότερα μέτρα και ποινές. Η ανασφάλεια και ο φόβος των πολιτών γίνονται αντικείμενο πολιτικής εκμετάλλευσης.⁸²

Επίσης, ορισμένες έρευνες έχουν διαπιστώσει ότι οι κυβερνήσεις, οι υπηρεσίες επιβολής του νόμου και γενικά τα MME προβάλλουν σε υπερβολικό βαθμό απειλές που είναι συνδεδεμένες με κάθε χρήση του Tor, χωρίς να δημοσιοποιούν ποτέ τα πλήρη δεδομένα για λόγους εθνικής ασφαλείας. Ωστόσο τίθεται και το ζήτημα ότι πολλές πληροφορίες συχνά προέρχονται από αποσπασματικές πηγές, όπως screenshots από forums χρηστών, δηλώσεις που έχουν κάνει συλληφθέντες διαχειριστές των αγορών στο darknet και «leaks», δηλαδή πληροφορίες ή δεδομένα που αποκαλύπτονται χωρίς άδεια σε δημόσιες πλατφόρμες για να προκαλέσουν δημόσια αναστάτωση.

Όλες αυτές οι πληροφορίες όμως, όταν δεν επαληθεύονται ή παρουσιάζονται με τρόπο που αποκλίνει από το ευρύτερο πλαίσιο, δημιουργούνται παρερμηνείες σχετικά με τη γενικότερη εικόνα του δικτύου Tor, καθώς, για παράδειγμα, κάποιες φορές παρουσιάζεται ως το μοναδικό μέσο εγκληματικής δράσης στο darknet. Αυτό είναι μία μονοδιάστατη και μη επαρκώς τεκμηριωμένη ανάλυση, η οποία μπορεί να παραπλανήσει τους ερευνητές, οδηγώντας σε λανθασμένα ή υπερβολικά συμπεράσματα σχετικά με το πραγματικό μέγεθος αλλά και τη φύση της απειλής. Για παράδειγμα, όπως προαναφέρθηκε, μερικές φορές η χρήση του Tor, δεν έχει παράνομο χαρακτήρα, καθώς μπορεί να χρησιμοποιείται από ακτιβιστές ή δημοσιογράφους προκειμένου να προστατεύσουν την ιδιωτικότητα τους. Έτσι, οι ερευνητικές προσπάθειες, βασίζονται σε δευτερογενή δεδομένα ή δεδομένα που αποκλίνουν σε μεγάλο βαθμό από την ισχύουσα πραγματικότητα, γεγονός που αποτελεί σοβαρό επιστημολογικό ζήτημα που σχετίζεται την αναξιοπιστία λόγω ολίγων ή στρεβλών πρωτογενών δεδομένων.⁸³

⁸² Ζαραφώνιτου Χ., Εμπειρική Εγκληματολογία, Νομική Βιβλιοθήκη, Β' έκδοση, 2004, Νομική Βιβλιοθήκη, σελ. 244-246

⁸³ Lusthaus, J., Industry of Anonymity: Inside the Business of Cybercrime. Harvard University Press, 2018, σελ. 227-240
[https://books.google.gr/books?id=FVhyDwAAQBAJ&pg=PP1&ots=DPkqyZb2C5&dq=Lusthaus%2C%20J.%20\(2018\).%20%22Industry%20of%20Anonymity%3A%20Inside%20the%20Business%20of%20Cybercrime%22&lr&pg=PP5#v=onepage&q&f=false](https://books.google.gr/books?id=FVhyDwAAQBAJ&pg=PP1&ots=DPkqyZb2C5&dq=Lusthaus%2C%20J.%20(2018).%20%22Industry%20of%20Anonymity%3A%20Inside%20the%20Business%20of%20Cybercrime%22&lr&pg=PP5#v=onepage&q&f=false)

5.2. Στατιστικές αβεβαιότητες ,έλλειψη εγκυρότητας δεδομένων και μεθοδολογικά ζητήματα

Η ανωνυμία του darknet και η χρήση εργαλείων όπως το Tor, τα VPN και τα κρυπτονομίσματα, καθιστά ιδιαίτερα δύσκολη την ανίχνευση της δομής των οργανώσεων, πόσο μάλλον της ταυτότητας των μελών, οι οποίοι υιοθετούν πολλαπλές ταυτότητες. Πολλές φορές μάλιστα, υπάρχουν μεμονωμένα άτομα που προσποιούνται πολυμελή και επικίνδυνα εγκληματικά δίκτυα, το οποίο φέρει την ερευνητική διαδικασία των επιστημόνων αντιμέτωπη με ακόμη ένα εμπόδιο. Οι στατιστικές μελέτες είναι περιορισμένες και ο σκοτεινός αριθμός της εγκληματικότητας μεγάλος, ενώ τα μεθοδολογικά προβλήματα που προκύπτουν κατά την έρευνα είναι ποικίλα. Πολλές φορές σκοτεινές αγορές και forums, εξαφανίζονται όπως έγινε στην περίπτωση της REvil, και έτσι χάνεται οποιαδήποτε ουσιαστική μορφή επαλήθευσης, για συναλλαγές που πραγματοποιήθηκαν. Άλλη μια δυσκολία που αντιμετωπίζουν οι ερευνητές είναι πως τα δεδομένα τους εξαρτώνται από δευτερογενείς και όχι πρωτογενείς πηγές, όπως είναι για παράδειγμα δημοσιογραφικές αναφορές, εργαλεία ανάλυσης της δραστηριότητας στο darknet ή εκθέσεις των διωκτικών αρχών, τα οποία όπως προαναφέρθηκε, ατελή. Άρα, το γεγονός αυτό οδηγεί στο εξής επιστημολογικό ερώτημα: Μπορούμε να γνωρίζουμε τελικά τη φύση, το μέγεθος και τη διάσταση του προβλήματος με βεβαιότητα, ή όχι;⁸⁴

5.3. Νομικά και Ηθικά ζητήματα

Η μελέτη του ρόλου του darknet στο οργανωμένο εγκλήματος έχει εγείρει πολλά νομικά, ηθικά και επιστημολογικά ζητήματα, καθώς πρόκειται για ένα παγκοσμιοποιημένο φαινόμενο, το οποίο χαρακτηρίζεται από ανωνυμία και ετερογένεια στα νομικά πλαίσια των κρατών. Οι διαφορετικές εθνικές νομοθεσίες δεν έχουν κοινή βάση για το τι συνιστά «οργανωμένο κυβερνοέγκλημα». Ως αποτέλεσμα, επικρατεί σύγχυση αναφορικά με το συντονισμό, τη συνεργασία, την επικοινωνία και την από κοινού διεθνική και υπερκρατική

⁸⁴ Tzanetakis, M. , Affect and digital drug markets: Negotiating trust and distrust in anonymous online environments. *International Journal of Drug Policy*, 2018, 54–62.

δράση, γεγονός το οποίο δημιουργεί ερευνητικά εμπόδια στους επιστήμονες κατά τη συλλογή και σύγκριση των δεδομένων.

Κατά συνέπεια, λοιπόν, προκύπτουν ατελείς και ασύμβατοι ορισμοί και κατηγοριοποιήσεις, λόγω της απουσίας κοινών νομοθεσιών μεταξύ των κρατών σχετικά με το πως πρέπει να αντιμετωπιστεί το οργανωμένο έγκλημα στο darknet.

Ενδεικτικά, σε κάποιες χώρες επιτρέπεται η πώληση εργαλείων hacking⁸⁵ και θεωρείται έγκλημα, ενώ σε άλλα κράτη είναι έκνομη πράξη και διώκεται ποινικά. Το γεγονός αυτό δυσχεραίνει τη διεθνή ταξινόμηση και σύγκριση του υπό μελέτη ζητήματος.

Οι συνθήκες αυτές, έχουν αξιοποιηθεί από τα οργανωμένα εγκληματικά δίκτυα, τα οποία εκμεταλλεύονται την ατιμωρησία και τη πολυνομία προκειμένου να συνεχίζουν τη δράση τους σε παγκόσμιο επίπεδο, εκτός του ελέγχου των αρχών επιβολής του νόμου.

Γενικά, η ανωνυμία στο darknet δύναται να προστατεύει δικαιώματα των χρηστών όπως αυτό της ιδιωτικότητας ή της ελευθερίας της έκφρασης. Συνεπώς, στους ερευνητές προκύπτει το εξής ηθικό δίλλημα: μέχρι που μπορεί να φτάσει η έρευνα χωρίς να προκληθεί σύγχυση ανάμεσα στην προστασία των δικαιωμάτων των χρηστών και στην ανοχή απέναντι σε εγκληματικές πρακτικές;

Συνεπώς, η απουσία παγκόσμιας συνεννόησης μεταξύ των κρατών με το τι είναι και τι δεν είναι παράνομο, σε συνδυασμό με την έλλειψη παγκόσμια κοινών τεχνολογικών εργαλείων παρακολούθησης και ανάλυσης του οργανωμένου εγκλήματος στο darknet , προκαλεί σοβαρές ερευνητικές δυσκολίες. Τις δυσκολίες αυτές επιχειρούν να αντιμετωπίσουν παγκόσμιοι οργανισμοί όπως η Interpol, η Europol κ.α., αλλά τα αποτελέσματα παραμένουν περιορισμένα, καθώς η πολυδιάσπαση των εθνικών και νομικών πλαισίων ενισχύει την επιστημολογική αβεβαιότητα.⁸⁶

⁸⁵ Τα εργαλεία hacking είναι λογισμικά ή τεχνικές που μπορούν να αξιοποιηθούν για παραβίαση συστημάτων, αλλά και για νόμιμους σκοπούς όπως είναι οι έλεγχοι ασφάλειας.

⁸⁶ Broadhurst R., Grabosky P., Alazab M., Chon S., Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime, 2014, https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime

5.4. Ο ρόλος της τεχνολογίας

Η τεχνολογία αποτελεί το βασικό μέσο επίτευξης του οργανωμένου εγκλήματος, και για αυτόν τον λόγο η μελέτη των τεχνολογικών μεθόδων που χρησιμοποιούνται στα πλαίσια διάπραξης του είναι απαραίτητη για την κατανόηση της διάρθρωσης και της λειτουργίας τέτοιων δικτύων.

Συνεπώς, απαραίτητη κρίνεται η τεχνολογική επένδυση από την πλευρά των αρχών αντεγκληματικής πολιτικής, καθώς δεν εξυπηρετεί μόνο την αντιμετώπιση του οργανωμένου εγκλήματος, αλλά αποτελεί και καθοριστικό παράγοντα για την διευκόλυνση της επιστημονικής μελέτης. Συνεπώς, όσο πιο εξελιγμένα είναι τα τεχνολογικά μέσα που χρησιμοποιούνται για την ανίχνευση και ανάλυση των εγκληματικών πράξεων, τόσο πιο αξιόπιστα και ακριβή θα είναι και τα πρωτογενή δεδομένα που χρησιμοποιούνται στην εγκληματολογική έρευνα.⁸⁷

6. Προβλήματα αντιμετώπισης του οργανωμένου εγκλήματος στο darknet

6.1. Δυσκολίες εντοπισμού και εξάρθρωσης εγκληματικών οργανώσεων στο darknet από τις αρχές επιβολής του νόμου

Ο εντοπισμός και η εξάρθρωση των εγκληματικών δικτύων γενικά, αλλά και του κυβερνοεγκλήματος ειδικότερα, αποτελεί μια εξαιρετικά περίπλοκη διαδικασία για τις αρχές επιβολής του νόμου. Η σύγχρονη τεχνολογία βοηθά τα μέλη του οργανωμένου εγκλήματος να αποκρύπτουν τόσο την πραγματική τους ταυτότητα όσο και τη φυσική τους τοποθεσία. Εργαλεία όπως η πολυεπίπεδη κρυπτογράφηση (π.χ. Tor) , και η δρομολόγηση των επικοινωνιών μέσω παγκόσμιων κόμβων (VPN), χρησιμοποιούνται ακριβώς για να αποτρέψουν οι δράστες τον εντοπισμό ενοχοποιητικών στοιχείων από τις αρχές, αλλά και να προσπαθήσουν να προστατευθούν από τεχνικές παραβιάσεις τρίτων και ανθρώπινα λάθη που θα μπορούσαν να εκθέσουν τις δραστηριότητες τους κατά τις συναλλαγές. Ειδικά, τεχνικές κρυπτογράφησης όπως η «end-to-end» ή τα απαραίτητα κρυπτογραφικά κλειδιά προκειμένου να επιτευχθεί είσοδος σε κάποια πλατφόρμα, καθιστούν ιδιαίτερα

⁸⁷ Europol , Internet Organised Crime Threat Assessment (IOCTA), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

απαιτητική την παρακολούθηση τόσο των επικοινωνιών όσο και των ψηφιακών αποδεικτικών στοιχείων.⁸⁸

Επιπλέον, οι εγκληματικές ομάδες παρουσιάζουν ιδιαίτερα μεγάλη ανθεκτικότητα. Αν ανακαλυφθούν πλατφόρμες στο darknet και ξεκινήσει έρευνα από τις διωκτικές αρχές, αμέσως το εντοπίζουν, τις απενεργοποιούν και δημιουργούν νέες πλατφόρμες και δωμάτια όπου συνεχίζουν την εγκληματική τους δράση από εκεί που την «είχαν αφήσει». Αυτό καθιστά την επιβολή του νόμου πολύ απαιτητική δεδομένου ότι απαιτείται η συνεχής προσαρμοστικότητα των αρχών για να μπορούν να δραστηριοποιούνται σε έναν βαθμό επί ίσοις όροις με τους δράστες. Για παράδειγμα, η REvil εμφανίστηκε στο προσκήνιο μόλις απενεργοποιήθηκε μια άλλη σκοτεινή διαδικτυακή πλατφόρμα ονόματι GandCrab, και συμπτωματικά μοιραζόταν σε μεγάλο βαθμό κοινούς σημαντικούς κώδικες.⁸⁹

Εκτός αυτού, η τεχνολογική υπεροχή των εγκληματικών δικτύων έναντι των διωκτικών αρχών, καθώς και η τεχνική κατάρτιση, τους έχουν επιτρέψει την αξιοποίηση εξειδικευμένων εργαλείων και γενικότερα τεχνολογίες που τα βοηθούν να αποφύγουν τον εντοπισμό τους. Μερικές από τις μεθόδους και τεχνικές που χρησιμοποιούν είναι η εκμετάλλευση «zero-day» ευπαθειών, η πλαστογράφιση ή απόκρυψη μεταδεδομένων⁹⁰ - με σκοπό την απόκρυψη της πραγματικής ταυτότητας και τοποθεσίας των χρηστών - , διασκορπισμένα hosting services, δηλαδή υπηρεσίες που προσφέρουν αυξημένη προστασία έναντι νομικών αιτημάτων, ψευδώνυμα και γενικά πολλαπλοί λογαριασμοί που καθιστούν ιδιαίτερα δύσκολη την ανίχνευση και σύνδεση των αρχών με την πραγματική ταυτότητα των δραστών.⁹¹

Εκτός αυτού η ανωνυμία ακόμη και μεταξύ των μελών του οργανωμένου εγκλήματος δυσκολεύει ακόμη περισσότερο την αποδόμηση των οργανώσεων.

⁸⁸ Lusthaus, J., Industry of Anonymity: Inside the Business of Cybercrime. Harvard University Press, 2018, σελ. 227-240

⁸⁹ Vijayan J., GandCrab Developers Behind Destructive REvil Ransomware, 2019, <https://www.darkreading.com/cyberattacks-data-breaches/gandcrab-developers-behind-destructive-revil-ransomware>

⁹⁰ Τα μεταδεδομένα είναι τα δεδομένα που δίνουν επιπλέον πληροφορίες για ένα αρχείο, για παράδειγμα τα μεταδεδομένα μιας φωτογραφίας είναι η ημερομηνία, το μέγεθος της, η τοποθεσία που τραβήχτηκε κ.α.

⁹¹ Europol, Internet Organised Crime Threat Assessment (IOCTA), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Λόγω του γεγονότος πως το οργανωμένο έγκλημα στο darknet πρόκειται για φαινόμενο με διεθνική και υπερκρατική διάσταση, οι δράστες και τα θύματα πολλές φορές βρίσκονται σε κράτη όπου εάν θυματοποιηθούν ενδέχεται το έγκλημα στο οποίο εκτέθηκαν να μην ανήκει στη δικαιοδοσία του νομικού πλαισίου της χώρας και να μην ληφθεί υπόψιν, δημιουργώντας ιδιαίτερο πρόβλημα τόσο στην έρευνα όσο και στη συνεργασία των διωκτικών αρχών. Επίσης, πολλές φορές λόγω νομοθετικών αλλαγών - όπως με την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων (Κανονισμός ΕΕ 2016/679) που τέθηκε σε ισχύ το 2018 και εισήγαγε αυστηρούς περιορισμούς στη συλλογή, χρήση και αποθήκευση προσωπικών δεδομένων- οι αρχές επιβολής του νόμου περιορίζονται ιδιαίτερα στα δεδομένα που μπορούν να χρησιμοποιήσουν σχετικά με την έρευνα και τον εντοπισμό των δικτύων, καθώς και την εξιχνίαση της δράσης τους.⁹² Αυτό, δημιουργεί προβλήματα δικαιοδοσίας, δυσχεραίνοντας τον προσδιορισμό του ποιος είναι υπεύθυνος για τη διεξαγωγή των ερευνών.⁹³

Τέλος, είναι χρήσιμο να αναφερθεί ότι η αντιμετώπιση του οργανωμένου εγκλήματος οφείλει να γίνεται χωρίς να καταπατώνται τα δικαιώματα των δραστών π.χ. ηλεκτρονική παρακολούθηση, παγίδευση τηλεφώνων κ.α. Σύμφωνα με τη Σύμβαση του Παλέρμο, υπάρχουν αυστηροί κανόνες για να αποτρέπεται η αυθαιρεσία των αρχών και για αυτό αναγκαίος είναι ο διαρκής έλεγχος της δράσης των διωκτικών αρχών από ανεξάρτητους φορείς. Η καταστολή του εγκλήματος δεν πρέπει να παραβιάζει θεμελιώδη δικαιώματα. Επίσης, τα κράτη οφείλουν να δρουν βάσει της αρχής της νομιμότητας και της αναλογικότητας, επειδή πολλές φορές κάτω από την πίεση για εξιχνίαση των εγκλημάτων και την εξάρθρωση των δικτύων, βρίσκονται συχνά στα όρια σεβασμού των θεμελιωδών δικαιωμάτων των κατηγορουμένων, όπως το δικαίωμα σε μία δίκαιη δίκη.⁹⁴

⁹² Κανονισμός (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR), Άρθρο 5, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4.5.2016. Διαθέσιμο σε: <https://gdpr-info.eu/art-5-gdpr/>

⁹³ Miralis N.G., The 5 key challenges for law enforcement in fighting cybercrime, 2020, <https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4>

⁹⁴ Χλούπης Γ., Η Προστασία Ανθρωπίνων Δικαιωμάτων κατά την αντιμετώπιση του υπερεθνικού εγκλήματος, 2016, <http://crime-in-crisis.com/η-προστασία-ανθρωπίνων-δικαιωμάτων-κα/>

5.2.2. Νομοθεσία και διακρατική συνεργασία

Το οργανωμένο έγκλημα αποτελεί ένα φαινόμενο, το οποίο είναι ιδιαίτερα δύσκολο να αντιμετωπιστεί στη φυσική του μορφή πόσω μάλλον στη ψηφιακή, άκρως ανώνυμη και τεχνολογικά ενισχυμένη. Ωστόσο, πέραν της ήδη περίπλοκης φύσης του, η αντεγκληματική πολιτική έρχεται αντιμέτωπη με σημαντικά νομικά κενά και περιορισμούς στη διεθνή συνεργασία.

Ένα από τα κυριότερα προβλήματα αποτελεί το γεγονός πως δεν υπάρχει ένας ενιαίος και κοινός ορισμός για το «ψηφιακό κυβερνοέγκλημα» μεταξύ των χωρών, με αποτέλεσμα να φέρουν διαφορετική νομοθεσία, και στοιχεία τα οποία θεωρούνται παράνομα σε ένα κράτος, είναι νόμιμα σε ένα άλλο.⁹⁵ Για παράδειγμα η κατοχή και χρήση κρυπτονομισμάτων σε κάποια κράτη, όπως η Ελλάδα, είναι νόμιμη, ενώ σε άλλα κράτη παράνομη και κάθε συναλλαγή απαγορεύεται. Στην κατηγορία αυτή ανήκει η Κίνα, η οποία επέβαλλε το 2017 αυστηρούς περιορισμούς στα κρυπτονομίσματα, απαγορεύοντας τα ανταλλακτήρια και αργότερα περιορίζοντας τα χρηματοπιστωτικά ιδρύματα εξόρυξης, διαχείρισης και συναλλαγής κρυπτονομισμάτων. Ο λόγος έγκειται στους κινδύνους για τη χρηματοπιστωτική σταθερότητα απάτης και φυγής κεφαλαίων. Η Αίγυπτος αποτελεί ακόμη μια περιοριστική χώρα ως προς τη διακίνηση και χρήση κρυπτονομισμάτων, καθώς τα θεωρεί επικίνδυνα, αφού χαρακτηρίζονται από υψηλή μεταβλητότητα και πολλές φορές είναι αποκεντρωμένα, δηλαδή δεν αναθέτονται σε κάποιο κρατικό ή χρηματοπιστωτικό έλεγχο, διευκολύνοντας για αυτούς τους λόγους τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες.⁹⁶

⁹⁵ Broadhurst R., Grabosky P., Alazab M., Chon S., Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime, 2014, https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime

⁹⁶ Nessi L., 10 Countries Where Crypto Remains Banned in 2025, 2025, <https://www.ccn.com/education/crypto/10-countries-where-crypto-remains-banned/>

Στα προαναφερθέντα, δηλαδή των νομικών κενών στη διεθνική συνεργασία, ανήκουν και άλλες μορφές δραστηριοτήτων, όπως το hacking . Υπάρχει, μάλιστα, μια κατηγορία ηθικού, όπως αποκαλείται, hacking , το «white hat hacking», όπου οι «white hat hackers» στοχεύουν στον εντοπισμό τυχόν ευπαθειών ή ζητημάτων ασφαλείας που έχει το τρέχον σύστημα. Το «white hat hacking» αντιπαραβάλλεται με το «black hat hacking». Αυτός ο όρος προέκυψε από τις western Αμερικανικές ταινίες , όπως η «Brokeback Mountain» του 2005, όπου ηρωικοί καουμπόηδες , μπορεί παραδοσιακά να φορούν ένα λευκό και ένα μαύρο καπέλο, αντίστοιχα.⁹⁷ Κράτη όπως το Βέλγιο νομιμοποίησε το «white hat hacking» τον Φεβρουάριο του 2023⁹⁸, ενώ το Ηνωμένο Βασίλειο ισχυρίστηκε πως εάν η πρόσβαση σε ένα σύστημα είναι εξουσιοδοτημένη, η πειρατεία είναι ηθική και νόμιμη. Εάν δεν είναι εξουσιοδοτημένη, υπάρχει αδίκημα βάσει του Νόμου περί Κατάχρησης Υπολογιστών. Έτσι και η Κίνα εκμεταλλεύτηκε την τεχνογνωσία των «white hat hackers» τον Ιούλιο του 2021, τους οποίους και υποχρέωσε να δράσουν προκειμένου να εξυπηρετήσουν τις υπηρεσίες πληροφοριών της χώρας.⁹⁹

Επιπλέον, υπάρχει μεγάλη δυσχέρεια έκδοσης ενταλμάτων έρευνας και σύλληψης που να έχουν διακρατική ισχύ, λόγω των διαφορετικών νομικών πλαισίων, διαδικασιών και πρωτοκόλλων που απαιτούνται για συλλογή αποδεικτικών στοιχείων. Στο ευρωπαϊκό ένταλμα σύλληψης, για παράδειγμα, -το οποίο αποτελεί μια απλουστευμένη διασυνοριακή δικαστική διαδικασία παράδοσης του υπόπτου για την άσκηση ποινικής δίωξης ή της εκτέλεσης ποινής ή μέτρου στερητικού της ελευθερίας και εκδίδεται από τη δικαστική αρχή κάποιου κράτους μέλους της ΕΕ και ισχύει σε ολόκληρη την ΕΕ- υπάρχουν πρακτικά εμπόδια στην προστασία των δικαιωμάτων των ανθρώπων και την διασφάλιση δίκαιων διαδικασιών.¹⁰⁰ Πολλές φορές, μάλιστα, απαιτείται αμοιβαία νομική συνδρομή των διωκτικών αρχών, η οποία συχνά είναι αργή, γραφειοκρατική και έτσι γίνεται

⁹⁷ Goerzen M., Coleman G., Wearing Many Hats, 2022, https://datasociety.net/wp-content/uploads/2022/03/WMH_final01062022Rev.pdf

⁹⁸ Somers C., Vranckaert K., Drechsler L. , Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?, <https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/>

⁹⁹ Brar A., China Raises Private Hacker Army To Probe Foreign Governments, 2024, <https://www.newsweek.com/china-hackers-probe-foreign-governments-computers-online-cybersecurity-1861721>

¹⁰⁰ European Union Agency for Fundamental Rights, European Arrest Warrant: Respecting rights across borders, 2024, https://fra.europa.eu/sites/default/files/fra_uploads/pr-2024-european_arrest_warrant.pdf

αναποτελεσματική στην αντιμετώπιση του οργανωμένου εγκλήματος στο darknet. Η αμοιβαία νομική συνδρομή, αποτελεί μια διαδικασία κατά την οποία τα κράτη μοιράζονται δεδομένα και στοιχεία προκειμένου να συλλέξουν αποδεικτικά στοιχεία. Μάλιστα, η Σύμβαση του ΟΗΕ κατά του Διακρατικού Οργανωμένου Εγκλήματος απαιτεί από τα κράτη μέλη να παρέχουν τη μέγιστη δυνατή νομική συνδρομή.¹⁰¹ Εντούτοις, οι σημαντικές διαφορές μεταξύ των νομικών συστημάτων, δημιουργούν και πάλι εμπόδιο στην αποτελεσματική ανταλλαγή πληροφοριών και τη συνεργασία. Γενικότερα, παρά την προσπάθεια συνεργασίας διεθνών οργανισμών, όπως της Interpol ή της Europol, οι οποίες επιχειρούν να προωθήσουν τη συνεργασία, η κατάσταση παραμένει επιστημολογικά αβέβαιη και πρακτικά προβληματική.

5.2.3. Ο ρόλος της τεχνητής νοημοσύνης

Η τεχνητή νοημοσύνη αποτελεί το πιο σύγχρονο τεχνολογικό εργαλείο και επίτευγμα της σύγχρονης εποχής διευκολύνοντας μεν την ζωή των νομοταγών πολιτών αλλά όμως ενισχύοντας δε, και τη διαδικτυακή εγκληματικότητα και κυρίως τα οργανωμένα εγκληματικά δίκτυα στο darknet.

Σύμφωνα με την τελευταία έκθεση για το οργανωμένο έγκλημα, τον Μάρτιο του 2025, που δημοσιεύεται κάθε τέσσερα χρόνια από την Europol, η τεχνητή νοημοσύνη διαδραματίζει σημαντικό ρόλο τόσο στην εξέλιξη του σύγχρονου οργανωμένου εγκλήματος, καθώς έχει ενισχύσει τις δυνατότητες του και έχει αυξήσει τα έσοδα του, όσο όμως και στην αντιμετώπιση του.

Πολλές φορές βέβαια, οι επιθέσεις του οργανωμένου κυβερνοεγκλήματος δεν έχουν αποκλειστικά οικονομικό κίνητρο, καθώς τα εργαλεία της τεχνητής νοημοσύνης γίνονται αντικείμενο εκμετάλλευσης από κράτη προκειμένου να δημιουργήσουν αναστάτωση σε κοινωνίες και θεσμούς. Αυτό γίνεται με διάδοση ψευδών ειδήσεων, διαρροή ευαίσθητων πληροφοριών και επιθέσεις σε κρίσιμες υποδομές π.χ. νοσοκομεία.

¹⁰¹ UNODC, Mutual legal assistance (MLA), 2018, <https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html>

Ορισμένες επιθέσεις, οι λεγόμενες «υβριδικές επιθέσεις» (proxy attacks) δείχνουν έναν συνδυασμό κινήτρων κέρδους και αποσταθεροποίησης, καθώς είναι ολοένα και πιο κρατικά και ιδεολογικά παρακινημένες. Μια τέτοια επίθεση ήταν και εκείνη της φιλωρωσικής ομάδας, NoName57(16), λίγο μετά την εισβολή της Ρωσίας στην Ουκρανία το 2022, η οποία ξεκίνησε να πραγματοποιεί μαζικές αυτοματοποιημένες επιθέσεις DDoS με τη βοήθεια της τεχνητής νοημοσύνης σε σημαντικές υποδομές της Ουκρανίας, αλλά και άλλων χωρών της Ευρωπαϊκής Ένωσης (όπως τράπεζες, ενεργειακές εταιρείες κ.α.) με σκοπό να στρατολογήσει και υποκινήσει νέους υποστηρικτές υπέρ της Ρωσίας και να προκαλέσει πολιτική επιρροή και αποσταθεροποίηση. Την επίθεση αυτή έσπευσε να αντιμετωπίσει η Europol και η Eurojust, μέσω της επιχείρησης «Eastwood», στην οποία συγκεντρώθηκαν, τουλάχιστον δώδεκα χώρες, καταστρέφοντας τελικά περισσότερους από εκατό διακομιστές των υποδομών της ομάδας. Παρ' όλο, λοιπόν, που δεν αποδείχθηκε εντέλει ως κρατική υπηρεσία, η Europol την εντάσσει στις υβριδικές απειλές και θεωρεί πως δημιουργήθηκε για να εξυπηρετήσει γεωπολιτικές σκοπιμότητες της ίδιας της Ρωσίας.

102

Ο όγκος του υλικού σεξουαλικής κακοποίησης παιδιών που είναι διαθέσιμο στο darknet έχει αυξηθεί σημαντικά λόγω της τεχνητής νοημοσύνης, καθώς επιτρέπει τη ταχεία και αυτόματη παραγωγή τέτοιου περιεχομένου χωρίς να υπάρχει κάποιο αληθινό θύμα, γεγονός που καθιστά πιο δύσκολη την ανάλυση εικόνων και τον εντοπισμό των δραστών, καθώς δημιουργεί ρεαλιστικά μέσα (εικόνες και βίντεο) και καθιστά τους εγκληματίες να είναι σε θέση να μιμηθούν άτομα, να εξαπατήσουν, να εκβιάσουν και να δυσφημίσουν. Το περιεχόμενο παιδικής πορνογραφίας, λοιπόν, αυξάνεται, χωρίς να αφορά πραγματικά άτομα και περιστατικά ή να αποτελεί πραγματική απειλή, δυσχεραίνοντας και πάλι το έργο των διωκτικών αρχών για καταπολέμηση του φαινομένου.

Η Τεχνητή Νοημοσύνη και άλλες τεχνολογίες, αποτελούν καταλύτη για το οργανωμένο έγκλημα αφού ενισχύουν την εγκληματική του δράση με την ταχύτητα, την εμβέλεια και την πολυπλοκότητά που προφέρουν, καθώς και τη λειτουργία του

¹⁰² Carol O' L., Russia using criminal networks to drive increase in sabotage acts, says Europol, 2025, <https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol>

,καθιστώντας την ανάγκη ενσωμάτωσης προηγμένων μέτρων ασφαλείας από τις διωκτικές αρχές πιο μεγάλη από ποτέ.¹⁰³

Ωστόσο, η τεχνητή νοημοσύνη βοηθά, πέραν των μελών του οργανωμένου εγκλήματος, και τις διωκτικές αρχές στην επεξεργασία μεγάλου όγκου δεδομένων γρήγορα και με ακρίβεια.

Μέσω των εργαλείων αυτών οι αρχές είναι σε θέση να ανακαλύψουν τους δυσδιάκριτους μηχανισμούς λειτουργίας των εγκληματικών οργανώσεων στο darknet. Ένας τρόπος εντοπισμού των εγκληματικών δραστηριοτήτων όπως είναι η διακίνηση ναρκωτικών, όπλων και προσωπικών δεδομένων, είναι τα συστήματα μηχανικής μάθησης και ανάλυσης προτύπων, δηλαδή επαναλαμβανόμενων μοτίβων, τα οποία αναγνωρίζουν αυτά τα μοτίβα και εντοπίζουν αποκλίσεις από τη φυσιολογική ροή των δεδομένων.

Η μηχανική μάθηση αποτελεί υποσύνολο της τεχνητής νοημοσύνης και μαθαίνει μοτίβα προκειμένου να βελτιώνει την απόδοση της με τη πάροδο του χρόνου. Η μηχανική μάθηση επιτρέπει στα υπολογιστικά συστήματα να μαθαίνουν από εμπειρικά δεδομένα και να αποκτούν την ικανότητα να αναγνωρίζουν, όπως είπαμε μοτίβα, να λαμβάνουν αποφάσεις και τελικά να προσαρμόζονται αυτόματα σε νέες εξελίξεις. Υποπεδίο, πάλι, της μηχανικής μάθησης, αποτελεί η βαθιά μάθηση, η οποία χρησιμοποιεί τεχνητά νευρωνικά δίκτυα - δηλαδή υπολογιστικά συστήματα εμπνευσμένα από τη λειτουργία του ανθρώπινου εγκεφάλου- για την επίλυση σύνθετων εργασιών. Ονομάζεται βαθιά λόγω του γεγονότος πως τα δίκτυα εκπαιδεύονται σε πολλαπλά στρώματα και έτσι μαθαίνουν αυτόματα να εξάγουν λειτουργίες από ακατέργαστα δεδομένα , καθιστώντας τα κατάλληλα για πολύπλοκες εργασίες όπως αναγνώριση εικόνας, ομιλίας, επεξεργασία φυσικής γλώσσας, δηλαδή κατανόηση της ανθρώπινης γλώσσας, κατορθώνοντας έτσι να επιλύει πολύπλοκα προβλήματα, τα οποία ήταν αδύνατο να λυθούν μέσω των παραδοσιακών προσεγγίσεων.

¹⁰³ Corder M., AI is turbocharging organized crime, EU police agency warns, 2025, <https://apnews.com/article/europe-crime-europol-ai-security-cyber-attack-846847536f6feb2bbb423943fd96e1f1>

Οι τεχνικές αυτές βοηθούν ιδιαίτερα τις διωκτικές αρχές να αναλύουν περίπλοκα δεδομένα και να αναγνωρίζουν μοτίβα, ανακαλύπτοντας συνδέσεις μεταξύ IP διευθύνσεων, ηλεκτρονικών πορτοφολιών και ψευδονύμων ταυτοτήτων, οδηγούμενοι τελικά στα ίχνη των οργανωμένων εγκληματικών δικτύων που δρουν στο darknet.

Επίσης τα συστήματα τεχνητής νοημοσύνης , χρησιμοποιούν γραφήματα ανάλυσης, ή αλλιώς αλγόριθμους γραφημάτων, δηλαδή αναλυτικά εργαλεία που χρησιμοποιούνται για τον προσδιορισμό της ισχύος και της κατεύθυνσης των σχέσεων μεταξύ αντικειμένων σε ένα γράφημα. Αυτή η δυνατότητα βοηθά τις διωκτικές αρχές να οπτικοποιήσουν ευρήματα και αποδεικτικά στοιχεία και έτσι να αυξηθούν τα ενδεχόμενα στοχευμένων παρεμβάσεων και όχι μαζικής καταστολής.

Επίσης , χάριν στα συστήματα τεχνητής νοημοσύνης μέσω της μηχανικής μάθησης, όπως προαναφέρθηκε, έχουν αναπτυχθεί τεχνολογίες επεξεργασίας φυσικής γλώσσας , και έτσι επιτυγχάνεται σε ικανοποιητικό βαθμό η κατανόηση συνομιλιών ή και γενικότερα περιεχομένου και αγγελιών σε ένα σκοτεινό δωμάτιο. Η επεξεργασία φυσικής γλώσσας μπορεί να εντοπίσει λέξεις κλειδιά, εξειδικευμένες ορολογίες ή και υπονοούμενα μεταξύ των μελών ενός οργανωμένου εγκληματικού δικτύου. Παράλληλα τα συστήματα έχουν τη δυνατότητα να μεταφράζουν και να αναλύουν το υπό μελέτη περιεχόμενο σε ποικίλες γλώσσες, εξαλείφοντας από τις αρχές εμπόδια κατανόησης.

Γενικά, η τεχνητή νοημοσύνη έχει τη δυνατότητα να προβλέπει ποιες εγκληματικές υπηρεσίες ή προϊόντα θα τεθούν στο επίκεντρο του οργανωμένου εγκληματικού ενδιαφέροντος στο darknet.¹⁰⁴

6. Αντιμετώπιση

6.1. Καταπολέμηση του Οργανωμένου Εγκλήματος στο Darknet

Οι σύγχρονες μορφές που λαμβάνει το οργανωμένο έγκλημα και τα χαρακτηριστικά του, έχουν δημιουργήσει στις τοπικές και εθνικές αρχές την ανάγκη διεθνούς συνεργασίας

¹⁰⁴ Γεωργούλη Αι., Τεχνητή νοημοσύνη, ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, σελ. 20-25, 127-132, <https://repository.kallipos.gr/handle/11419/3381?locale=el>

προκειμένου να αντιμετωπιστεί το ζήτημα σε έναν ικανοποιητικό βαθμό. Έτσι, ενεργοποιούνται και συνεργάζονται διεθνείς οργανισμοί, η Europol, η Interpol, το FBI, το γραφείο κατά της τρομοκρατίας και του οργανωμένου εγκλήματος του ΟΗΕ, το UNODC, και άλλοι, παρέχοντας εξειδικευμένες υπηρεσίες και τεχνολογικά εργαλεία.

6.1.1. Europol

Η Europol αποτελεί την επίσημη υπηρεσία της Ευρωπαϊκής Ένωσης για τη συνεργασία στον τομέα επιβολής του νόμου. Ιδρύθηκε το 1998, εδρεύει στη Χάγη της Ολλανδίας και είναι ο κεντρικός κόμβος για τον συντονισμό των εγκληματολογικών πληροφοριών και την υποστήριξη των κρατών μελών της Ευρωπαϊκής Ένωσης στις προσπάθειες τους να καταπολεμήσουν διάφορες μορφές σοβαρού οργανωμένου εγκλήματος. Κυριος στόχος της Europol είναι η ενίσχυση της αποτελεσματικότητας και της συνεργασίας των υπηρεσιών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης. Για την επίτευξη αυτού του στόχου, διευκολύνει την ανταλλαγή πληροφοριών και στοιχείων, παρέχει αναλυτική υποστήριξη και προσφέρει εξειδικευμένη εκπαίδευση και εμπειρογνωμοσύνη. Ο οργανισμός δεν έχει εκτελεστικές εξουσίες και οι υπάλληλοι του δεν έχουν το δικαίωμα σύλληψης υπόπτων, αλλά διεξαγωγής ανεξάρτητων ερευνών.¹⁰⁵

Η Europol συνεργάζεται στενά με την Eurojust, οργανισμό της Ευρωπαϊκής Ένωσης που είναι υπεύθυνος για τις δικαστικές υποθέσεις, ενισχύοντας τις διακρατικές έρευνες και κατά συνέπεια τη δίωξη εγκληματικών δικτύων που δραστηριοποιούνται στο darknet.¹⁰⁶

Από το 2013, στην Europol λειτουργεί το «European Cybercrime Centre» (EC3), το οποίο ασχολείται με θέματα κυβερνοασφάλειας. Το EC3 ανέλαβε να βοηθήσει τα κράτη

¹⁰⁵ European Union, Eur-lex, Europol (European Union Agency for Law Enforcement Cooperation), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:europol#:~:text=Glossary%20of%20summaries-,Europol%20\(European%20Union%20Agency%20for%20Law%20Enforcement%20Cooperation\),authorities%20and%20law%20enforcement%20services](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:europol#:~:text=Glossary%20of%20summaries-,Europol%20(European%20Union%20Agency%20for%20Law%20Enforcement%20Cooperation),authorities%20and%20law%20enforcement%20services).

¹⁰⁶ European Union, European Union Agency for Criminal Justice Cooperation (Eurojust), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_en

μέλη να αναπτύξουν εργαλεία και να εκπαιδευτούν πάνω στο συγκεκριμένο ζήτημα.¹⁰⁷ Στο πλαίσιο του EC3 αναπτύχθηκε η μονάδα «Europol Dark Web Team», η οποία βοήθησε ιδιαίτερα την έρευνα και τη συνεργασία των αρχών γύρω από θέματα που αφορούν τις παράνομες αγορές και γενικότερα τις ανώνυμες πλατφόρμες του darknet. Η Europol εστιάζει σε εργαλεία, τακτικές και τεχνικές ανάλυσης μεγάλου όγκου δεδομένων από αγορές, φόρουμ και γενικότερα σκοτεινά δωμάτια επικοινωνίας.¹⁰⁸ Παράλληλα, υποστηρίζει τις έρευνες της μέσω του «Serius Platform», μιας πλατφόρμας στο διαδίκτυο που διευκολύνει τη συλλογή αποδεικτικών στοιχείων¹⁰⁹, ενώ στο τεχνολογικό τομέα, το «Europol Innovation Lab», βοηθά στην ανάπτυξη καινοτόμων και σύγχρονων τεχνολογιών προκειμένου να παρακολουθείται η δραστηριότητα πολλαπλών χρηστών στο darknet και να αναλύονται τα blockchain με σκοπό την ανίχνευση και ανακάλυψη κάθε ύποπτης συναλλαγής.¹¹⁰ Σημαντικότερο όμως πυλώνα στην έρευνα και αντιμετώπιση του οργανωμένου εγκλήματος στο darknet, αποτελεί η «Joint Cybercrime Taskforce» (J-CAT), η οποία είναι υπεύθυνη για τις διεθνείς επιχειρήσεις στον τομέα του κυβερνοεγκλήματος.

111

Η Europol, έχει συμμετάσχει σε συντονισμένες και διεθνείς προσπάθειες κατά του οργανωμένου εγκλήματος στο darknet, όπως η επιχείρηση «Disruptor», το 2020, όπου συνεργάστηκε με άλλους διεθνείς φορές, συμπεριλαμβανομένου του FBI. Η επιχείρηση «Disruptor», πέτυχε την κατάρρευση μεγάλων αγορών στο darknet, 179 συλλήψεις και κατασχέσεις μεγάλου όγκου ναρκωτικών, όπλων και κρυπτονομισμάτων.¹¹²

¹⁰⁷ Europol, European Cybercrime Centre - EC3, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

¹⁰⁸ Europol, Crime on the dark web: law enforcement coordination is the only cure, <https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure>

¹⁰⁹ Europol, Serius Project, <https://www.europol.europa.eu/operations-services-innovation/sirius-project>

¹¹⁰ Europol, Innovation Lab, <https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab>

¹¹¹ Europol, Joint Cybercrime Action Taskforce, <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce#:~:text=J%2DCAT's%20objective%20is%20to,and%20operations%20by%20its%20partners.>

¹¹² Europol, International sting against dark web vendors leads to 179 arrests, <https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests>

6.1.2. FBI (Federal Bureau of Investigation)

Το FBI (Federal Bureau of Investigation) , είναι η ομοσπονδιακή υπηρεσία πληροφοριών και ασφαλείας των Ηνωμένων Πολιτειών της Αμερικής. Αποτελεί έναν κορυφαίο αμερικανικό οργανισμό αντιτρομοκρατίας, αντικατασκοπείας και εγκληματολογικής έρευνας και εστιάζει ιδιαίτερα σε θέματα οργανωμένου εγκλήματος και κυβερνοεγκλήματος. Μέσω της Cyber Division, διεύθυνσης για τη διερεύνηση και δίωξη εγκλημάτων στο Διαδίκτυο και της Joint Criminal Opioid and Darknet Enforcement (J-Code), της επιχείρησης του FBI κατά της παράνομης διανομής οπιοειδών στο darknet, η υπηρεσία οργανώνει και αναπτύσσει στρατηγικές σχετικά με την παρακολούθηση, την ανίχνευση και την ανακάλυψη οργανωμένων εγκληματικών δικτύων στο darknet.¹¹³ Το FBI, χρησιμοποιεί εργαλεία όπως το OSINT (Open Source Intelligence), το οποίο περιλαμβάνει τη συλλογή και ανάλυση δημοσίων αναρτημένων πληροφοριών, οι οποίες μπορούν να χρησιμοποιηθούν είτε παθητικά¹¹⁴ είτε ενεργητικά¹¹⁵ σε θέματα κυβερνοασφάλειας, οικονομικών απειλών και άλλα. Το OSINT χρησιμοποιείται προκειμένου να αξιολογηθεί ο κίνδυνος ,να μειωθεί το ψηφιακό αποτύπωμα και να παρακολουθούνται όλα τα δεδομένα σε πραγματικό χρόνο, λαμβάνοντας ο ερευνητής ειδοποίηση όταν κάποιο δεδομένο αλλάζει. Προσφάτως, μάλιστα, εξελίχθηκε σε OSINT 2.0., περιλαμβάνοντας συστήματα τεχνητής νοημοσύνης και λειτουργίες πιο γρήγορες, ευρείες και προσιτές.¹¹⁶

Επίσης, το FBI, διαθέτει εξειδικευμένες μονάδες, όπως το Regional Computer Forensics Laboratory (RCFL) που προσφέρει τόσο υπηρεσίες όσο και εκπαίδευση γύρω από τη συλλογή και εξέταση αποδεικτικών στοιχείων σχετικά με την καταπολέμηση του οργανωμένου εγκλήματος στο darknet¹¹⁷, αλλά και την CART (Computer Analysis Response Team), που είναι εκπαιδευμένη να ανακτά δεδομένα από κατεστραμμένα μέσα, παρέχοντας σημαντική υποστήριξη σε διάφορες εγκληματολογικές υποθέσεις.¹¹⁸

¹¹³ FBI, FBI and Partners Target Darknet Opioid Traffickers, 2019, <https://www.fbi.gov/video-repository/jcode-htoc-030419.mp4/view>

¹¹⁴ Χωρίς αλληλεπίδραση με το αντικείμενο της έρευνας (π.χ. παρακολούθηση).

¹¹⁵ , Με άμεση εμπλοκή με το αντικείμενο της έρευνας (π.χ. επικοινωνία με στόχους).

¹¹⁶ Riskinsigh.com, OSINT or Intelligence 2.0., <https://www.riskinsight-wavestone.com/en/2022/11/osint-or-intel>

¹¹⁷ FBI, Science and technology, <https://www.fbi.gov/how-we-investigate/science-and-technology#>:

¹¹⁸ FBI, Piecing Together Digital Evidence ,The Computer Analysis Response Team,2019 <https://www.fbi.gov/news/stories/piecing-together-digital-evidence>

Το FBI με τις μονάδες του και τις εξελιγμένες τεχνολογίες που χρησιμοποιεί έχει βοηθήσει ιδιαίτερα στην αποτελεσματικότερη αντιμετώπιση του οργανωμένου εγκλήματος στο darknet. Μια εκ των πολλών υποθέσεων με τις οποίες ασχολήθηκε είναι η υπόθεση «Silk Road». Το FBI, μέσα από την ανάλυση των κρυπτονομισμάτων -κυρίως bitcoins που χρησιμοποιούνταν κατά κύριο λόγο στο «Silk Road» και την παρακολούθηση των σχετικών συναλλαγών, σε συνεργασία με την Europol , κατάφερε να οδηγηθεί στη σύλληψη του Ross Ulbricht, δημιουργού και διαχειριστή της πλατφόρμας, το 2013, ο οποίος ενεργούσε με το ψευδώνυμο «Dread Pirate Roberts» και καταδικάστηκε σε ισόβια κάθειρξη για σειρά αδικημάτων, δηλαδή διακίνηση ναρκωτικών, ξέπλυμα βρώμικου χρήματος και εμπλοκή σε ανθρωποκτονία.¹¹⁹

6.1.3. Interpol

Η Interpol αποτελεί τον αρχαιότερο αστυνομικό οργανισμό. Συνδέει τις αστυνομικές υπηρεσίες 195 κρατών και έχει ως αρμοδιότητα τη συλλογή δεδομένων, την ανάλυση μέσω μίας κεντρικής βάσης δεδομένων, όπου καταγράφονται και επεξεργάζονται δεδομένα και τη βοήθεια των κρατών μελών σε περιπτώσεις οργανωμένου εγκλήματος, συμπεριλαμβανομένου και του οργανωμένου εγκλήματος στο darknet. Η Interpol διαθέτει υπηρεσίες όπως η Cybercrime Directorate, διεύθυνση κυβερνοεγκλήματος με εξειδικευμένα εργαστήρια ψηφιακής εγκληματολογίας για τη μελέτη περιστατικών και απειλών στο darknet. Επίσης, το τεχνολογικό κέντρο της Interpol στη Σιγκαπούρη (Global Complex for Innovation)¹²⁰ ενισχύει τις προσπάθειες κυβερνοασφάλειας μέσω της χρήσης τεχνητής νοημοσύνης και εκπαίδευσης των αστυνομικών. Για την επικοινωνία και την ασφαλή ανταλλαγή πληροφοριών μεταξύ των κρατών σε πραγματικό χρόνο, χρησιμοποιεί την πλατφόρμα I-24/7 και έτσι διευκολύνεται η παγκόσμια συνεργασία και η άμεση

¹¹⁹FBI, Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts, 2015, <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts>

¹²⁰ Interpol, INTERPOL Innovation Centre, <https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre>

ανταπόκριση σε εγκλήματα οργανωμένου χαρακτήρα στο darknet.¹²¹ Επίσης, η Interpol εκδίδει ειδικές ειδοποιήσεις, γνωστές ως «μωβ ειδοποιήσεις», με σκοπό να ενημερώνει τα κράτη μέλη σχετικά με νέες απειλές στο διαδίκτυο, όπως τεχνικές ransomware και άλλες πρακτικές που εντοπίζει να χρησιμοποιούν τα οργανωμένα εγκληματικά δίκτυα. Οι ειδοποιήσεις αυτές βοηθούν ιδιαίτερα στην ετοιμότητα των κρατών μελών σχετικά με τους νέους κινδύνους και την αντιμετώπιση των εγκληματικών δικτύων με μεγαλύτερη αποτελεσματικότητα.¹²²

Μια ιδιαίτερα επιτυχημένη προσπάθεια καταπολέμησης του οργανωμένου εγκλήματος με βασικό συντονιστή την Interpol, ήταν η επιχείρηση «Africa Cyber Surge», που πραγματοποιήθηκε 2022 με σκοπό την εξάρθρωση οργανωμένων εγκληματικών δικτύων στον κυβερνοχώρο της Αφρικής. Η επιχείρηση αποδόμησε πάνω από 200.000 κακόβουλα προγράμματα και υποδομές για άπατες, εκβιασμούς και κλοπές δεδομένων. Τελικά η Interpol, με τη στήριξη 27 κρατών μελών και οργανισμών κυβερνοασφάλειας ιδιωτικού χαρακτήρα, όπως η Group-IB και η Kaspersky, κατάφερε να αναλύσει και ανιχνεύσει την πραγματική IP διεύθυνση των χρηστών και έτσι, να οδηγηθεί στην εξάρθρωση και σύλληψη 11 μελών εκ του εμπλεκόμενου οργανωμένου εγκληματικού δικτύου. Προκειμένου να γίνει αυτό, η Interpol, προσέφερε εκτεταμένη και εξειδικευμένη εκπαίδευση σε αξιωματικούς της αστυνομίας για την ανίχνευση και αντιμετώπιση της εγκληματικότητας στο darknet. Η συγκεκριμένη επιχείρηση ήταν σημαντική τόσο για την αντιμετώπιση του κυβερνοεγκλήματος στην Αφρική όσο και για την ενίσχυση της συνεργασίας και της εκπαίδευσης των αστυνομικών αρχών, καθώς δεν στόχευε μόνο ένα δίκτυο αλλά πολλαπλά εγκληματικά δίκτυα και μεμονωμένους δράστες στον κυβερνοχώρο.¹²³

¹²¹ Interpol, Connecting police: I-24/7, <https://www.yumpu.com/en/document/view/7746807/connecting-police-i-24-7-interpol>

¹²² Interpol, National Strategy Cybercrime Strategy Guidebook, 2021, https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf

¹²³ Interpol, Operation across Africa identifies cyber-criminals and at-risk online infrastructure, 2022, <https://www.interpol.int/en/News-and-Events/News/2022/Operation-across-Africa-identifies-cyber-criminals-and-at-risk-online-infrastructure>

6.1.4. Γραφείο Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (UNODC)

Το «Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα» (UNODC, Γαλλικά: Office des Nations Unies contre la Drogue et le Crime)¹²⁴ ιδρύθηκε το 1997 με την ονομασία «Γραφείο Ελέγχου Ναρκωτικών και Πρόληψης του Εγκλήματος», ως αποτέλεσμα της συγχώνευσης του «Διεθνούς Προγράμματος Ελέγχου Ναρκωτικών» των Ηνωμένων Εθνών (UNDCP) και του ισχύοντος «Γραφείου Πρόληψης του Εγκλήματος και της Ποινικής Δικαιοσύνης». Το 2002, το γραφείο έλαβε την σημερινή του ονομασία, UNODC. Βασικός στόχος του οργανισμού είναι η καταπολέμηση της διακίνησης και κατάχρησης παράνομων ναρκωτικών, η πρόληψη του εγκλήματος, η ποινική δικαιοσύνη, το οργανωμένο έγκλημα, η διεθνής τρομοκρατία και η πολιτική διαφθορά. Η UNODC μέσα από το πρόγραμμα «Global Programme against Organized Crime» στοχεύει στην υποστήριξη των κρατών σχετικά με την εφαρμογή της Σύμβασης του Παλέρμο, την ενίσχυση των θεσμικών και νομοθετικών τους πλαισίων, , αλλά και τη δημιουργία στρατηγικών, πολιτικών και σχεδίων για την αντιμετώπιση του διακρατικού οργανωμένου εγκλήματος. Επίσης, το UNODC διευκολύνει τη διεθνή συνεργασία σε ποινικές υποθέσεις, ενσωματώνει τη διάσταση του φύλου και των ανθρωπίνων δικαιωμάτων στη νομοθεσία και την πολιτική – ιδιαίτερα σε ευαίσθητά θέματα που οι γυναίκες και τα κορίτσια επηρεάζονται δυσανάλογα σε σχέση με τους άντρες (π.χ. εμπορία ανθρώπων) - και είναι υπεύθυνο για τη συγκέντρωση και διάδοση της γνώσης και την εκπαίδευση γύρω από το οργανωμένο έγκλημα. Το τελευταίο, οφείλεται στο γεγονός πως μέσα από την έρευνα διαρκώς συλλέγει κρίσιμες πληροφορίες για το οργανωμένο έγκλημα, προωθώντας πρακτικές ικανές να συμβάλλουν στην αποτελεσματικότερη αντιμετώπιση του.¹²⁵ Μέσω του Global Programme on Cybercrime, το UNODC παρέχει τεχνική βοήθεια και εκπαίδευση στα κράτη-μέλη για την αντιμετώπιση φαινομένων κυβερνοεγκλήματος και κατ' επέκταση των δραστηριοτήτων του οργανωμένου εγκλήματος στο darknet. Σκοπός του είναι να κατανοήσουν τα κράτη-μέλη το μέγεθος της απειλής, να ευαισθητοποιηθεί το κοινό και να αναπτυχθούν

¹²⁴ Ειδικός οργανισμός του ΟΗΕ

¹²⁵ UNODC, Global Programme on Implementing the Organized Crime Convention: from Theory to Practice, 2021, <https://www.unodc.org/unodc/es/organized-crime/intro/implementing-untoc/intro-programme.html>

μακροπρόθεσμες πολιτικές πρόληψης και καταπολέμησης του οργανωμένου εγκλήματος στον κυβερνοχώρο.¹²⁶

Το 2022 το UNODC συνεργάστηκε με την OSCE, τον Οργανισμό για την Ασφάλεια και τη Συνεργασία στην Ευρώπη, προκειμένου να προσφέρει καινοτόμες λύσεις πολιτικής για τον μετριασμό των κινδύνων νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες μέσω εικονικών περιουσιακών στοιχείων και κρυπτονομισμάτων. Με το έργο αυτό, το UNODC υποστήριξε κράτη όπως την Μολδαβία και την Ουκρανία, να αναπτύξουν τεχνογνωσία και μηχανισμούς για την καταπολέμηση τέτοιων κινδύνων.¹²⁷ Τέλος, άλλη μια συνεργασία που αξίζει να αναφερθεί είναι του UNODC με την Trend Micro, μια εταιρεία κυβερνοασφάλειας, για την εκπαίδευση επαγγελματιών κυβερνοασφάλειας σε χώρες της Νοτιοανατολικής Ασίας.¹²⁸

Εν κατακλείδι, λόγω του γεγονότος πως η UNODC υποστηρίζει τη διεθνή αστυνομική συνεργασία, έχει αναπτύξει σχέσεις συνεργασίας με την Interpol, τη Europol και άλλους οργανισμούς.

6.2. Διακρατική συνεργασία

Η διακρατική συνεργασία είναι πολύ σημαντική για την αντιμετώπιση του οργανωμένου εγκλήματος στο darknet.

Η συνεργασία μπορεί να είναι είτε αστυνομική είτε δικαστική. Η συνεργασία μεταξύ των αστυνομικών αρχών επιζητά να περιλαμβάνει την ανταλλαγή αποδεικτικών στοιχείων και γνωστικών δεξιοτήτων σε πραγματικό χρόνο, με αποτέλεσμα τη διεξαγωγή συντονισμένων επιχειρήσεων. Τέτοια περίπτωση είναι η επιχείρηση «Emotet» το 2021,

¹²⁶ UNODC, MODEL OF IMPACTING AND PROMOTING CHANGE IN CYBERCRIME CAPACITIES ,2025,<https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/united-nations-office-drugs-and-crime-unodc>

¹²⁷ OSCE, OSCE and UNODC launch a project to counter money laundering of virtual assets and cryptocurrencies, 2022, <https://www.osce.org/occea/529401>

¹²⁸ newsroom.trendmicro.com, UNODC and Trend Micro Partner to Train Cybersecurity Professionals.2021, <https://newsroom.trendmicro.com/2021-07-05-UNODC-and-Trend-Micro-Partner-to-Train-Cybersecurity-Professionals>

στην οποία συμμετείχαν 8 κράτη, μεταξύ των οποίων οι ΗΠΑ, η Ολλανδία, η Γερμανία και η Ουκρανία, υπό τον συντονισμό της Europol και της Eurojust. Η επιχείρηση μπόρεσε να εξαρθρώσει ένα από τα ισχυρότερα δίκτυα οργανωμένου κυβερνοεγκλήματος «κακόβουλου λογισμικού» που παρείχε προϊόντα και υπηρεσίες σε οργανωμένες εγκληματικές ομάδες στο darknet για επιθέσεις ransomware και κλοπή δεδομένων.¹²⁹ Συνεπώς, φαίνεται πως η συνεργασία μεταξύ των κρατών είναι ιδιαίτερα σημαντική για την αντιμετώπιση του σύγχρονου οργανωμένου εγκλήματος.

Όσον αφορά τη δικαστική συνεργασία, αυτή περιλαμβάνει την αμοιβαία δικαστική συνδρομή, την έκδοση υπόπτων και τη συνεργασία οργανισμών όπως η Eurojust στην Ευρώπη ή το UNODC σε παγκόσμιο επίπεδο. Η αμοιβαία δικαστική συνδρομή είναι μια μορφή συνεργασίας μεταξύ διαφορετικών χωρών με σκοπό τη συλλογή και ανταλλαγή πληροφοριών. Οι αρχές μιας χώρας μπορούν επίσης να ζητήσουν και να παράσχουν αποδεικτικά στοιχεία που βρίσκονται σε αυτήν για να βοηθήσουν ποινικές έρευνες ή διαδικασίες σε μια άλλη χώρα. Στην Ευρωπαϊκή Ένωση, οι μηχανισμοί αμοιβαίας δικαστικής συνδρομής αντικαθίστανται σταδιακά από πράξεις αμοιβαίας αναγνώρισης, δηλαδή την αναγνώριση και αυτόματη αποδοχή δικαστικών και διοικητικών αποφάσεων άλλου κράτους χωρίς να απαιτείται επανεξέταση της υπόθεσης από το δικαστήριο του άλλου κράτους. Ωστόσο, μια συμφωνία μεταξύ των χωρών της ΕΕ εξακολουθεί να ισχύει: η σύμβαση για την αμοιβαία δικαστική συνδρομή σε ποινικές υποθέσεις ενισχύει τη συνεργασία μεταξύ δικαστικών, αστυνομικών και τελωνειακών αρχών.¹³⁰ Τέλος, με την οδηγία 2014/41/ΕΕ της 3^{ης} Ιουλίου του 2014 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της ΕΕ, εισήχθη το Ευρωπαϊκό Ένταλμα Σύλληψης, το οποίο αναλύθηκε παραπάνω. Τα κράτη μέλη της Ευρωπαϊκής Ένωσης μπορούν να εκδίδουν υπόπτους σε άλλη χώρα για την εκδίκαση ή έκτιση ποινής χωρίς να απαιτείται κάποια περαιτέρω διαδικασία έκδοσης ή δικαστικής επανεξέτασης.¹³¹

¹²⁹ Europol, World's most dangerous malware EMOTET disrupted through global action, <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emetet-disrupted-through-global-action>

¹³⁰ Mutual legal assistance and extradition, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en

¹³¹ Οδηγία 2014/41/ΕΕ ΤΟΥ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3ης Απριλίου 2014 περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις, Αρθρ.1,2,3,5, <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014L0041>

6.3. Νομοθεσίες και κανονιστικά πλαίσια

Γενικά, το κυριότερο νομοθετικό πλαίσιο σχετικά με τον ρόλο του darknet στο οργανωμένο έγκλημα, είναι η Σύμβαση της Βουδαπέστης για το κυβερνοέγκλημα του 2001 του Συμβουλίου της Ευρώπης και αποτελεί και το μοναδικό δεσμευτικό διεθνές εργαλείο που ορίζει όλα τα κοινά μέτρα ποινικοποίησης και συνεργασίας δικονομικής μορφής. Ωστόσο, δεν έχει υπογραφεί από όλα τα κράτη, όπως η Κίνα και η Ρωσία.¹³²

Η Ευρωπαϊκή Ένωση, μέσω του Κανονισμού DSA (Digital Services Act)¹³³ και της Οδηγίας NIS2, υποχρεώνει όλους τους παρόχους ψηφιακών υπηρεσιών να διαχειρίζονται περιεχόμενο με ύποπτο και παράτυπο χαρακτήρα με ταχύτερους ρυθμούς, συνεργαζόμενοι με τις διωκτικές αρχές για την αποτελεσματικότερη αντιμετώπιση του φαινομένου.¹³⁴

Στην Ελλάδα, το κανονιστικό πλαίσιο για την αντιμετώπιση του οργανωμένου εγκλήματος στο darknet αποτελούν διεθνείς συνθήκες, συνταγματικές διατάξεις, διατάξεις του κοινού ποινικού δικαίου και νόμοι που έχουν εκδοθεί βάσει κοινοτικών οδηγιών. Γενικά, το οργανωμένο έγκλημα στο darknet ρυθμίζεται από ένα σύνολο κανονιστικών κειμένων στην Ελλάδα και την Ευρωπαϊκή Ένωση, τα οποία στοχεύουν στην αντιμετώπιση αυτής εγκληματικής δραστηριότητας στο ψηφιακό χώρο. Συγκεκριμένα, ορίζεται ένας συνδυασμός ποινών κατά του οργανωμένου εγκλήματος, όπως αναλύθηκε σε ανωτέρω κεφάλαιο, σε συνδυασμό με τον Νόμο 4577/2018 σχετικά με την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών. Η Ελλάδα επίσης εφαρμόζει στη νομοθεσία της τη Σύμβαση της Βουδαπέστης για την ηλεκτρονική εγκληματικότητα και την Οδηγία 2016/1148/ΕΕ.¹³⁵

¹³² Ν. 4411/2016, Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης), ΦΕΚ Α' 149/29.07.2016, <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernochoro-0>

¹³³ European Commission, The Digital Services Act, 2022 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

¹³⁴ European Commission, NIS2 Directive: new rules on cybersecurity of network and information systems, 2022, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

¹³⁵ Ν. 4577/2018, Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις, ΦΕΚ Α' 199/03.12.2018, <https://www.kodiko.gr/nomothesia/document/474449/nomos-4577-2018>

Ενδεικτικά:

Ο Νόμος 4557/2018, προβλέπει μέτρα για την καταπολέμηση της χρηματοοικονομικής απάτης και την πρόληψη του «ξεπλύματος μαύρου χρήματος». Αναφέρεται και στη χρήση ηλεκτρονικών μέσων για την παρακολούθηση ύποπτων συναλλαγών.¹³⁶

Τα εγκλήματα που σχετίζονται με την παρακώληση της λειτουργίας των πληροφοριακών συστημάτων ρυθμίζονται από το άρθρο 292B του Ποινικού Κώδικα (Ν. 4619/2019), με ποινές φυλάκισης από ένα έως τρία έτη και χρηματικό πρόστιμο και αφορά τα άτομα τα οποία χωρίς δικαίωμα παρεμπόδισαν ή διέκοψαν τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης σε αυτά. Η φυλάκιση, λοιπόν, φτάνει και τα τρία χρόνια όταν η απειλή αφορά δημόσιες υποδομές και αγαθά που εξυπηρετούν δημόσια συμφέροντα και ανάγκες, όπως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.¹³⁷

Η παραγωγή, διανομή, δημοσίευση, επίδειξη, μεταφορά, προσφορά, πώληση, αγορά, κατοχή, και διακίνηση υλικού παιδικής πορνογραφίας διέπεται από τον Νόμο 4855/2021, ο οποίος τροποποίησε το άρθρο 348Α του Ποινικού Κώδικα, προβλέποντας αυστηρές ποινές φυλάκισης και χρηματικό πρόστιμο. Ειδικότερα, εάν όλα τα παραπάνω πραγματοποιούνται μέσω πληροφοριακών συστημάτων, ο δράστης τιμωρείται με κάθειρξη μέχρι δύο (2) ετών και χρηματική ποινή.¹³⁸ Αν το θύμα, δεν έχει συμπληρώσει το δωδέκατο έτος της ηλικίας του, τότε επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή, ενώ εάν κατά την εκμετάλλευση του ανηλίκου, ο τελευταίος αποβιώσει, τότε στον δράστη επιβάλλεται ισόβια κάθειρξη. Τέλος, όποιος εν γνώσει αποκτά πρόσβαση

¹³⁶ 4577/2018 ,Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις., ΦΕΚ Α' 199/03.12.2018, https://minfin.gov.gr/wp-content/uploads/2023/09/fek_α_139_2018-v.4557-2018.pdf

¹³⁷ Ν.4619/2019, Κύρωση του Ποινικού Κώδικα, ΦΕΚ Α' 95/11.06.2019, https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/α/fek_α_95_2019.pdf&t=α25c5af089b303113f7f0d472e9a35fc

¹³⁸ Ν.4619/2019, Κύρωση του Ποινικού Κώδικα, Αρθ. 80, ΦΕΚ Α' 95/11.06.2019, https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/α/fek_α_95_2019.pdf&t=α25c5af089b303113f7f0d472e9a35fc

σε τέτοιου είδους υλικό μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση έως τρία (3) έτη ή χρηματική ποινή.¹³⁹

Οι προηγούμενες ρυθμίσεις αποτελούν μόνο ένα τμήμα του κανονιστικού πλαισίου για την προστασία του κοινωνικού συνόλου από την εγκληματικότητα του οργανωμένου εγκλήματος στο darknet.

6.4. Τεχνολογίες ανίχνευσης και παρακολούθησης δραστηριοτήτων στο Darknet

Η τεχνολογική πρόοδος πέραν της ανάπτυξης των δυνατοτήτων των οργανωμένων εγκληματικών δικτύων, με χρήση εργαλείων όπως το Tor ή τα κρυπτονομίσματα, έχει οδηγήσει παράλληλα τις αρχές στην χρήση πιο εξελιγμένων μέσων και εργαλείων , για να αντιμετωπίσουν τις εξελίξεις και την επικινδυνότητα των καιρών.

Μερικά από τα εργαλεία και τις τεχνολογίες που χρησιμοποιούνται σχετικά με την επιτήρηση είναι τα crawler bots, εργαλεία OSINT που αναλύθηκαν παραπάνω και εργαλεία ανάλυσης blockchain , δηλαδή συναλλαγών με κρυπτονομίσματα. Τα crawler bots αποτελούν ειδικά διαμορφωμένα λογισμικά που σαρώνουν αυτόματα τις ιστοσελίδες στο darknet και ελέγχουν αν υπάρχει κάτι παράνομο. Τα crawler bots αποτελούν συχνή μέθοδο κυβερνοεπιτήρησης και έρευνας από τους αρμόδιους φορείς και τις κρατικές υπηρεσίες. Για παράδειγμα, το FBI χρησιμοποίησε εργαλεία crawling, για να εντοπίσει τους διαχειριστές της σκοτεινής αγοραστικής πλατφόρμας Alphabay το 2017, και κατάφερε τελικά την κατάρριψη της.¹⁴⁰ Τα εργαλεία ανάλυσης blockchain από την άλλη , αναλύουν τις συναλλαγές που πραγματοποιούνται στο πλαίσιο αγορών ή πωλήσεων στο darknet και

¹³⁹ Ν.4855/2021, ΦΕΚ Α' 215/12.11.21, Τροποποιήσεις του Ποινικού Κώδικα, του Κώδικα Ποινικής Δικονομίας και άλλες επείγουσες διατάξεις, https://www.kodiko.gr/nomologia/download_fek?f=fek/2021/α/fek_α_215_2021.pdf&t=9cd4566ed78c5ae3a90f5f55ea4607a0

¹⁴⁰ Asoke Nath A., Chatterjee S., Auto-Explore the Web – Web Crawler , 2017, <https://www.researchgate.net/profile/Asoke-Nath-4/publication/3166011>

αν αντιληφθούν κάτι ύποπτο , έχουν τη δυνατότητα μερικές φορές να αποκαλύψουν τη σύνδεση μεταξύ ηλεκτρονικού πορτοφολιού και ύποπτης δραστηριότητας.¹⁴¹

Γενικά, οι απαιτήσεις για εξειδικευμένη και ανανεωμένη γνώση των διωκτικών αρχών σχετικά με το κυβερνοέγκλημα είναι αυξημένες. Η ψηφιακή εγκληματολογία (digital forensics) αποτελεί τον πλέον σύγχρονο κλάδο της αστυνομικής εγκληματολογίας που επικεντρώνεται στην αναγνώριση, την απόκτηση, την επεξεργασία, την ανάλυση και την αναφορά δεδομένων που αποθηκεύονται ηλεκτρονικά.

Τα ηλεκτρονικά αποδεικτικά στοιχεία αποτελούν συστατικό σχεδόν όλων των εγκληματικών δραστηριοτήτων και η υποστήριξη της ψηφιακής εγκληματολογίας είναι ζωτικής σημασίας για τις έρευνες των αρχών επιβολής του νόμου.

Ο κύριος στόχος της ψηφιακής εγκληματολογίας είναι η εξαγωγή δεδομένων από τα ηλεκτρονικά αποδεικτικά στοιχεία, η επεξεργασία τους σε αξιοποιήσιμες πληροφορίες και η οργάνωση των ευρημάτων κατά τέτοιο τρόπο ώστε να είναι εφικτή η δίωξη και αποδεκτά τα ευρήματα στο δικαστήριο.¹⁴²

Λόγω της ταχύτατης εξέλιξης και της επικινδυνότητας, κυρίως του οργανωμένου εγκλήματος στο darknet, οι αρχές οφείλουν να βρίσκονται σε συνεχή εγρήγορση και να εκπαιδεύονται διαρκώς , επικαιροποιώντας τις γνώσεις και δεξιότητες τους. Εκτός από νομικά κενά και διαφοροποιήσεις της νομοθεσίας μεταξύ των κρατών υπάρχει και η ανισότητα πόρων, η οποία δυσκολεύει άλλη μία φορά το εγχείρημα διακρατικής συνεργασίας προκειμένου να αντιμετωπιστεί η κατάσταση. Γί αυτό το λόγο, η συνεργασία μεταξύ ιδιωτικού και δημοσίου θα μπορούσε να βοηθήσει στη ανακάλυψη κρίσιμων πληροφοριών, στη δημιουργία εργαλείων και απόκτηση τεχνογνωσίας, απαραίτητων για

¹⁴¹ Riehle C., Europol Report on Criminal Use of Cryptocurrencies, <https://euclid.eu/news/europol-report-on-criminal-use-of-cryptocurrencies>

¹⁴² Interpol, digital forensics, 2025, <https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations>.

την πρόληψη, ανακάλυψη και καταπολέμηση του οργανωμένου εγκλήματος στο darknet.

143

7. Επίλογος

Το οργανωμένο έγκλημα, συνδέεται με το darknet στενά και πολυεπίπεδα, καθώς το τελευταίο με τη δυνατότητα ανωνυμίας και τεχνολογικής κρυπτογράφησης που προσφέρει, έχει καταστήσει το έγκλημα ιδιαίτερα αποτελεσματικό. Μέσα από τη παρούσα διπλωματική εργασία αναλύθηκαν οι τεχνολογικές, νομικές και εγκληματολογικές πτυχές του ζητήματος και παρουσιάστηκε πως το οργανωμένο έγκλημα χαρακτηρίζεται από τη μέγιστη δυνατή προσαρμοστικότητα, αφού έχει κατορθώσει να περιπλέξει το έργο τόσο των διωκτικών όσο και των ερευνητικών αρχών.

Τα κράτη, όπως σημειώθηκε, δεν είναι ικανά να αντιμετωπίσουν αυτό το κρίσιμο και ιδιαίτερα επικίνδυνο φαινόμενο μόνα τους, αφού το οργανωμένο έγκλημα στο darknet έχει εξαπλωθεί σε όλο τον κόσμο και ως εκ τούτου είναι επιτακτική η ανάγκη διεθνούς συνεργασίας αλλά και η εναρμόνιση των νομικών πλαισίων μεταξύ των κρατών. Επίσης, η ψηφιακή εγκληματολογική εκπαίδευση των διωκτικών αρχών και των αρχών επιβολής του νόμου οφείλει να είναι διαρκής και τα τεχνολογικά εργαλεία και μέσα να ακολουθούν κατά το δυνατόν τη ροή εξέλιξης και προσαρμοστικότητας του οργανωμένου εγκλήματος. Ταυτόχρονα, ιδιαίτερα σημαντική κρίνεται η ανάπτυξη διεπιστημονικών τρόπων προσέγγισης, μελέτης και ανάλυσης του φαινομένου, ώστε να μπορέσουν να αντιμετωπιστούν οι ερευνητικές προκλήσεις, οι οποίες είναι άμεσα συνυφασμένες με τη γενικότερη προσέγγιση και αντιμετώπιση του φαινομένου.

Το οργανωμένο έγκλημα, έχει κατορθώσει να μετατραπεί σε έναν κίνδυνο τεχνολογικά εξελιγμένο, που δημιουργεί στις διωκτικές αρχές την ανάγκη σύγχρονων και καινοτόμων στρατηγικών πρόληψης και καταστολής. Τα εργαλεία της τεχνητής νοημοσύνης και η εκπαίδευση των αρχών επιβολής του νόμου σε ζητήματα

¹⁴³ Eurojust, Common challenges in cybercrime, 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf

κυβερνοασφάλειας, σε συνδυασμό με την συνεργασία ιδιωτικών εταιρειών και κρατικών δομών, μπορούν να βοηθήσουν στην αποτελεσματικότερη αντιμετώπιση του οργανωμένου εγκλήματος στο darknet.

Παρ' όλα, αυτά η πλήρης κατανόηση του οργανωμένου εγκλήματος στο darknet εξακολουθεί να αποτελεί ένα δυσχερές εγχείρημα. Η επιστημονική κοινότητα, οι κρατικοί φορείς και η τεχνολογία βρίσκονται αντιμέτωποι με ένα από τα πιο σύνθετα και επικίνδυνα εγκλήματα που έχουν υπάρξει ποτέ.

Εν κατακλείδι, δεν πρέπει να παραληφθεί η επιρροή που ασκεί τόσο το ίδιο το οργανωμένο έγκλημα στο darknet, όσο και οι επιχειρήσεις που στοχεύουν στην έρευνα, μελέτη και αντιμετώπιση του. Από τη μία ο τρόπος δράσης του οργανωμένου εγκλήματος δημιουργεί ατομικές, κοινωνικές, κρατικές, διακρατικές και υπερκρατικές προκλήσεις. Η εκμετάλλευση ανθρώπων, υπηρεσιών και ολόκληρων κρατών τείνει να υπερισχύει, οδηγώντας συχνά σε αμφισβήτηση των θεσμών λόγω της μερικούς ή πλήρης αναποτελεσματικότητας τους. Από την άλλη, οι αντεγκληματικές πολιτικές μπορεί να καταλήξουν σε καταπάτηση προσωπικών ελευθεριών και δικαιωμάτων, ακόμη και των ίδιων των δραστών. Το γεγονός αυτό έχει εγείρει καίρια ερωτήματα σχετικά με την υπεράσπιση και προστασία των ανθρωπίνων δικαιωμάτων και την ηθική ευθύνη που φέρει η τεχνολογική ανάπτυξη. Συνεπώς, είναι αναγκαία η εύρεση λύσεων, όχι μόνο νομικού ή τεχνικού χαρακτήρα, αλλά και πολιτικού και αξιακού. Μόνο μέσα από μία πολυεπίπεδη προσέγγιση θα μπορέσει να καλυφθεί το παρόν ζήτημα συνολικά, περιλαμβάνοντας όλες τις διαστάσεις του.

Βιβλιογραφία

A. Ελληνική βιβλιογραφία

Γερμανός Γ. , Γεωργίου Ν., Κυβερνοέγκλημα: Πρόληψη, Διερεύνηση, Αντιμετώπιση , έκδοση των ιδίων, 2021

Γεωργούλη Αι., Τεχνητή νοημοσύνη, ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ, <https://repository.kallipos.gr/handle/11419/3381?locale=el>

Δαλακούρα Ι. Θεοχάρης, Ηλεκτρονικό Έγκλημα, 2019, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης

Ζαραφωνίτου Χ. Ανίτση Ε., Εισήγηση: «Πόλη και έγκλημα: θεωρητική προσέγγιση και χαρακτηριστικά του φαινομένου», 2020, https://easte.panteion.gr/images/other_files/h_kyklos/zarafonitou_anitsi_151220.pdf

Ζαραφωνίτου Χ., Εμπειρική Εγκληματολογία, Νομική Βιβλιοθήκη, Β΄ έκδοση, 2004, Νομική Βιβλιοθήκη

Ζαραφωνίτου Χ., Κουμεντάκη Ε. και Ερευνητική Ομάδα Φοιτητών Κοινωνιολογίας Παντείου Πανεπιστημίου, Θυματοποίηση και φόβος του εγκλήματος των φοιτητών χρηστών του διαδικτύου, 2024, https://criminology.panteion.gr/files/444/Internet_ZARAFONITOY.pdf

Ζιούβας Δ., Οργανωμένο Έγκλημα, Ευρωπαϊκές Πανεπιστημιακές Εκδόσεις, Αθήνα, 2021

Ζιούβας Δ., «Χρηματοπιστωτικό Ποινικό Δίκαιο», Ευρωπαϊκές Πανεπιστημιακές Εκδόσεις, Αθήνα, 2022

Κάλλιου Ε., E- trafficking, εμπορία ανθρώπων στο διαδίκτυο, 2023, <https://www.crimetimes.gr/e-trafficking-εμπορία-ανθρώπων-στο-διαδίκτυο/>

Kriptomat, Τι είναι το κρυπτονόμισμα και πως λειτουργεί, 2021, <https://kriptomat.io/gr/kryptonomismata/ti-einai-to-kryptonomisma/>

LawSpot.gr, Ηλεκτρονικό Έγκλημα, 2014, <https://www.lawspot.gr/nomikes-plirofories/voithitika-kemenα/ilektroniko-egklima>

Σταμούλη Ε., Εγκλήματα των ισχυρών : Διαφθορά , οικονομικό και οργανωμένο έγκλημα, εκδόσεις Συλλογικό Έργο, 2025

Σταμούλη Ε., Οργανωμένο έγκλημα, παράνομες αγορές και διαφθορά στην Ελλάδα στο Βιδάλη Σ., Κουλούρης Ν., Παπαχαλαράμπους Χ. (επιμ.), Εγκλήματα των ισχυρών, Διαφθορά, οικονομικό και οργανωμένο έγκλημα, Αθήνα, Εκδ. ΕΑΠ, 2019

Τραγάκης Γ., «Οργανωμένο Έγκλημα και Ξέπλυμα Βρώμικου Χρήματος», Νομική Βιβλιοθήκη, 1996

Χαΐδου Α., Θετικιστική εγκληματολογία, αιτιολογικές προσεγγίσεις του εγκληματικού φαινομένου, νομική βιβλιοθήκη, 1996

Χλούπης Γ., Η Προστασία Ανθρωπίνων Δικαιωμάτων κατά την αντιμετώπιση του υπερεθνικού εγκλήματος, 2016, <http://crime-in-crisis.com/η-προστασία-ανθρωπίνων-δικαιωμάτων-κα/>

Β. Ξένη βιβλιογραφία

Adejumo O., Russian darknet dominated crypto drug trade in 2024 with \$1.65 billion transactions, 2025, <https://cryptoslate.com/russian-darknet-dominated-crypto-drug-trade-in-2024-with-1-65-billion-transactions>

Akamai, What is REvil?, 2024, <https://www.akamai.com/glossary/what-is-revil>

Antonopoulos, A., «Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Sebastopol», California: O'Reilly, 2015

AnuMeena Care Foundation, The transformative impact of the Internet on Society, 2023, <https://www.linkedin.com/pulse/transformative-impact-internet-society-anumeenacare#:~:text=Since%20its%20inception%2C%20the%20internet,areas%20impacted%20by%20the%20internet.>

Asoke Nath A., Chatterjee S., Auto-Explore the Web – Web Crawler , 2017,
<https://www.researchgate.net/profile/Asoke-Nath-4/publication/3166011>

Aycock, J. Computer Viruses and Malware ,2006,
<https://books.google.gr/books?hl=el&lr=&id=xnW->

Becker B., What is a bitcoin ATM? ,2023, <https://builtin.com/cryptocurrency/what-is-a-bitcoin-atm>

Becker G., Crime and punishment: an economic approach, 1968,
http://masonlec.org/site/rte_uploads/files/JEP/Readings/Butler%20Economic%20Analysis%20for%20Lawyers%203rd%20ed/CH%20VII%20Crime.pdf

Brar A., China Raises Private Hacker Army To Probe Foreign Governments,2024,
<https://www.newsweek.com/china-hackers-probe-foreign-governments-computers-online-cybersecurity-1861721>

Broadhurst R., Grabosky P., Alazab M., Chon S., Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime,2014,
https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime

Broadhurst R., Grabosky P., Alazab M., Chon S., Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime,2014,
https://www.researchgate.net/publication/288262190_Organizations_and_cyber_crime_An_analysis_of_the_nature_of_groups_engaged_in_cyber_crime

Bunea G., Marius I., Organized crime , drug trafficking, and the digital world : a concise perspective, University of Cluj Napoca, 2024,
https://cuj.ubv.ro/ssh/article/view/61/70?fbclid=IwY2xjawJpu6JleHRuA2FlbQlXMAABHrxeZu_mKxb7DVzGM1CwgKW9uPegCp4Cy2n

Bursztein E., Bethard S., Fabry C., Mitchell J.C., Jurafsky D., How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation, Stanford University, 2010, https://web.stanford.edu/~jurafsky/burszstein_2010_captcha.pdf

Carol O' L., Russia using criminal networks to drive increase in sabotage acts, says Europol, 2025, <https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol>

Cellar Door Wiki, Mob Hierarchy, 2008, https://cellar-door.fandom.com/wiki/Mob_Hierarchy

Corder M., AI is turbocharging organized crime, EU police agency warns, 2025, <https://apnews.com/article/europe-crime-europol-ai-security-cyber-attack-846847536f6feb2bbb423943fd96e1f1>

Criminal Operations,2019, <https://arxiv.org/pdf/1901.01914>

Egan M., What is the Dark Web, What's on it & How to Access it,2019, <https://www.techadvisor.com/article/727316/what-is-the-dark-web-whats-on-it-how-to-access-it.html>

Eurojust, Common challenges in cybercrime, 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf

European Commission ,The Digital Services Act,2022 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Union Agency for Fundamental Rights, European Arrest Warrant: Respecting rights across borders, 2024, https://fra.europa.eu/sites/default/files/fra_uploads/pr-2024-european_arrest_warrant.pdf

European Union, Eur-lex, Europol (European Union Agency for Law Enforcement Cooperation), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:europol#:~:text=Glossary%20of%20summaries-,Europol%20\(European%20Union%20Agency%20for%20Law%20Enforcement%20Cooperation\),authorities%20and%20law%20enforcement%20services](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:europol#:~:text=Glossary%20of%20summaries-,Europol%20(European%20Union%20Agency%20for%20Law%20Enforcement%20Cooperation),authorities%20and%20law%20enforcement%20services).

European Union, European Union Agency for Criminal Justice Cooperation (Eurojust), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_en

Europol ,Internet Organised Crime Threat Assessment (IOCTA), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Europol, 288 dark web vendors arrested in major marketplace seizure, 2023, <https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure>

Europol, Crime on the dark web: law enforcement coordination is the only cure, <https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure>

Europol, European Cybercrime Centre – EC3, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

Europol, Innovation Lab, <https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab>

Europol, International sting against dark web vendors leads to 179 arrests, <https://www.europol.europa.eu/media-press/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests>

Europol, Joint Cybercrime Action Taskforce, <https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action->

taskforce#:~:text=J%2DCAT's%20objective%20is%20to,and%20operations%20by%20its%20partners.

Europol, Sirius Project, <https://www.europol.europa.eu/operations-services-innovation/sirius-project>

Europol, World's most dangerous malware EMOTET disrupted through global action, <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>

FBI, FBI and Partners Target Darknet Opioid Traffickers, 2019, <https://www.fbi.gov/video-repository/jcode-htoc-030419.mp4/view>

FBI, Piecing Together Digital Evidence ,The Computer Analysis Response Team,2019 <https://www.fbi.gov/news/stories/piecing-together-digital-evidence>

FBI, Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts, 2015, <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts>

FBI, Science and technology, <https://www.fbi.gov/how-we-investigate/science-and-technology#>:

Giacomo D'A., Burgalassi D., Hali H., Walter M., Conflict in Campania: Waste emergency or crisis of democracy, 2010, <https://www.sciencedirect.com/science/article/abs/pii/S0921800910002594?via%3Dihub>

Glushko, R.- J. ,The Discipline of Organizing: Core Concepts Edition, O'Reilly Media, Inc.,2017

Goerzen M., Coleman G., Wearing Many Hats, 2022, https://datasociety.net/wp-content/uploads/2022/03/WMH_final01062022Rev.pdf

Hsiao, S.C., Kao, D.Y. ,2018, The static analysis of WannaCry Ransomware, <https://ieeexplore.ieee.org/abstract/document/8323680>

Interpol, Connecting police: I-24/7, <https://www.yumpu.com/en/document/view/7746807/connecting-police-i-24-7-interpol>

Interpol, digital forensics, 2025,<https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations.>

Interpol, INTERPOL Innovation Centre, <https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre>

Interpol, National Strategy Cybercrime Strategy Guidebook, 2021, https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf

Interpol, Operation across Africa identifies cyber-criminals and at-risk online infrastructure,2022,<https://www.interpol.int/en/News-and-Events/News/2022/Operation-across-Africa-identifies-cyber-criminals-and-at-risk-online-infrastructure>

Kaplan D.E., Dubro A.,Yakuza - Japan's Criminal Underworld, University of California Press, 2003

Lane A., What is technology?,2019,,<https://www.open.edu/openlearn/science-maths-technology/engineering-technology/what-technology>

Louise I., Dirty Entanglements: Corruption, Crime, and Terrorism, Cambridge University Press, 2014

Lusthaus, J.,Industry of Anonymity: Inside the Business of Cybercrime. Harvard University Press,2018

Miralis N.G., The 5 key challenges for law enforcement in fighting cybercrime, 2020, <https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4>

Mishra U., An Introduction to Computer Viruses, 2010, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1916631

Morselli C., Inside Criminal Networks, Εκδ. Springer

Mutual legal assistance and extradition, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en

Myre G, How Bitcoin Has Fueled Ransomware Attacks, 2021, <https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks>

Nessi L., 10 Countries Where Crypto Remains Banned in 2025, 2025, <https://www.ccn.com/education/crypto/10-countries-where-crypto-remains-banned/>

newsroom.trendmicro.com, UNODC and Trend Micro Partner to Train Cybersecurity Professionals. 2021, <https://newsroom.trendmicro.com/2021-07-05-UNODC-and-Trend-Micro-Partner-to-Train-Cybersecurity-Professionals>

Nurmi J., Paju A., Brumley B., Insoll T., Ovaska A., Soloveva V., Vaaranen-Valkonen N., Aaltonen M., Arroyo D., Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy, Cornell University, 2024, <https://arxiv.org/abs/2404.14112>

Nurse J., Bada M., The Group Element of Cybercrime: Types, Dynamics, and

Criminal Operations, 2019, <https://arxiv.org/pdf/1901.01914>

OSCE, OSCE and UNODC launch a project to counter money laundering of virtual assets and cryptocurrencies, 2022, <https://www.osce.org/occea/529401>

Ozkaya E.,Islam R, Inside the Dark Web,CRC Press, 2019

Paoli L.,The paradoxes of organized crime, 2022, Crime, Law and Social Change

PCEDU, Η ιστορία του διαδικτύου, 2022,<https://www.pcedugr.com/post/η-ιστορία-του-διαδικτύου>

RAND, US weapons main source of illegal arms trade on the dark web, 2017, <https://www.rand.org/news/press/2017/07/19.html#:~:text=Sixty%20per%20cent%20of%20weapons,sale%20on%20the%20dark%20web.>

Ransomware, <https://ieeexplore.ieee.org/abstract/document/8323680>

Razzali N.B., Suradi Nur Biuti Mohd, A nest for cyber criminals: The Dark Web, 2019

Riehle C.,Europol Report on Criminal Use of Cryptocurrencies, <https://eucrim.eu/news/europol-report-on-criminal-use-of-cryptocurrencies>

Riskinsigh.com, OSINT or Intelligence 2.0., <https://www.riskinsight-wavestone.com/en/2022/11/osint-or-intel>

Rumold M., Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation, 2016, <https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation>

Sason D., REvil Ransomware Attack on Kaseya VSA: What You Need to Know, 2021, <https://www.varonis.com/blog/revil-mssp-supply-chain-attack>

Schondelmayer L., Hiring a hitman on the web: Can contractual violence be added to your online shopping cart?, 2020, <https://socialscience.msu.edu/news-events/news/archives/2020/2020-08-14.html>

Simplilearn, What is Steganography? Types, Techniques, Examples & Applications, 2024, <https://www.simplilearn.com/what-is-steganography-article>

Siuda P., Swieca L, Cheba P., Shi H., "Similar to Legal Companies": Vendor Brands and Other Aspects of Marketing Communication in the Darknet Drug Trade, 2024, <https://www.tandfonline.com/doi/full/10.1080/01639625.2024.2428711#abstract>

Somers C., Vranckaert K., Drechsler L. , Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?, <https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/>

Spanakis E.G., Silvia Bonomi S., Cyber-attacks and threats for healthcare – a multi-layer thread analysis, <https://ieeexplore.ieee.org/abstract/document/9176698/authors#authors>

Spanga N., Russia arrests 14 alleged members of REvil ransomware gang, 2022, <https://www.cbsnews.com/news/ransomware-russia-arrests-revil/>

Stoval J., Darknet, 2023, <https://www.britannica.com/technology/computer-security>

Tax Justice Network, Identifying Tax Havens and Offshore Finance Centres, 2007, https://www.taxjustice.net/cms/upload/pdf/Identifying_Tax_Havens_Jul_07.pdf

Theguardians.com, US woman who hired hitman using bitcoin to kill ex-husband gets five years in prison, 2023, <https://www.theguardian.com/technology/2023/jul/22/nevada-woman-hired-hitman-kill-ex-husband-sentenced>

Tikkanen A., Camorra, 1998, <https://www.britannica.com/topic/organized-crime>

Tzanetakis, M. , Affect and digital drug markets: Negotiating trust and distrust in anonymous online environments. International Journal of Drug Policy, 2018

U.S. Department of Justice, Cyber Security Unit, Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data, 2020, from Illicit Sources, <https://www.justice.gov/criminal/criminal-ccips/page/file/1252341/dl?inline>

U.S. Department of Justice, Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than \$530 Million in Losses from Cybercrimes, 2018, <https://www.justice.gov/archives/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>

United Nations Office Drugs and Crime (UNODC), Global report in trafficking in persons, https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

United States Attorneys Office, Indiana Man Sentenced To Prison For Engaging In A Child Exploitation Enterprise, 2017, <https://www.justice.gov/usao-wdnc/pr/indiana-man-sentenced-prison-engaging-child-exploitation-enterprise>

UNODC, Cyber organized crime activities, 2019, <https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html>

UNODC, Cyberfraud in the Mekong reaches inflection point, UNODC reveals, 2025, <https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html>

UNODC, Global Programme on Implementing the Organized Crime Convention: from Theory to Practice, 2021, <https://www.unodc.org/unodc/es/organized-crime/intro/implementing-untoc/intro-programme.html>

UNODC, MODEL OF IMPACTING AND PROMOTING CHANGE IN CYBERCRIME CAPACITIES ,2025, <https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/united-nations-office-drugs-and-crime-unodc>

UNODC, Mutual legal assistance (MLA), 2018, <https://www.unodc.org/e4j/en/organized-crime/module-11/key-issues/mutual-legal-assistance.html>

Vicens A.J., Reports of ransomware attacks on US infrastructure rise nine percent, 2025, <https://www.itnews.com.au/news/reports-of-ransomware-attacks-on-us-infrastructure-rise-9-percent-616744>

Vijayan J., GandCrab Developers Behind Destructive REvil Ransomware, 2019, <https://www.darkreading.com/cyberattacks-data-breaches/gandcrab-developers-behind-destructive-revil-ransomware>

Winder D., Hackers Publish First 169 Trump 'Dirty Laundry' Emails After Being Branded Cyber-Terrorists, 2020, <https://www.forbes.com/sites/daveywinder/2020/05/17/hackers-publish-first-169-trump-dirty-laundry-emails-after-being-branded-cyber-terrorists/>

Zimmerman C., Kiss L., Human trafficking and exploitation: A global health concern, 2017, <https://pmc.ncbi.nlm.nih.gov/articles/PMC5699819/>

Γ. Νομοθεσίες και κανονιστικά κείμενα

N. 4577/2018 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών, ΦΕΚ Α' 199/03.12.2018, https://minfin.gov.gr/wp-content/uploads/2023/09/fek_alpha_139_2018-v.4557-2018.pdf

N.4619/2019, Κύρωση του Ποινικού Κώδικα, ΦΕΚ Α' 95/11.06.2019, https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/alpha/fek_alpha_95_2019.pdf&t=alpha25c5af089b303113f7f0d472e9a35fc

N.4619/2019, Κύρωση του Ποινικού Κώδικα, ΦΕΚ Α' 95/11.06.2019, https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/alpha/fek_alpha_95_2019.pdf&t=alpha25c5af089b303113f7f0d472e9a35fc

N.4855/2021, ΦΕΚ Α' 215/12.11.21, Τροποποιήσεις του Ποινικού Κώδικα, του Κώδικα Ποινικής Δικονομίας και άλλες επείγουσες διατάξεις,

https://www.kodiko.gr/nomologia/download_fek?f=fek/2021/α/fek_α_215_2021.pdf&t=9cd4566ed78c5ae3a90f5f55ea4607α0

N. 5090/2024, Παρεμβάσεις στον Ποινικό Κώδικα και τον Κώδικα Ποινικής Δικονομίας για την επιτάχυνση και την ποιοτική αναβάθμιση της ποινικής δίκης - Εκσυγχρονισμός του νομοθετικού πλαισίου για την πρόληψη και την καταπολέμηση της ενδοοικογενειακής βίας, ΦΕΚ Α'/30/24.2.24,

https://www.kodiko.gr/nomologia/download_fek?f=fek/2024/α/fek_α_30_2024.pdf&t=b3d97e1c1ca002298f8a57359b257b4d

N. 4411/2016, Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης), ΦΕΚ Α' 149/29.07.2016, <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0>

N. 4577/2018 , Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ενσωμάτωση της Οδηγίας 2015/849/ΕΕ) και άλλες διατάξεις.

N. 3875/2010 , Κύρωση και εφαρμογή της Σύμβασης των Ηνωμένων Εθνών κατά του Διεθνικού Οργανωμένου Εγκλήματος και των τριών Πρωτοκόλλων αυτής και συναφείς διατάξεις. ,ΦΕΚ Α' 158/20.9.2010,άρθρο 2, <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n3875-2010/arthro-2-nomos-3875-2010>

N. 4908/2022, Μέτρα αντιμετώπισης της οπαδικής βίας, ενίσχυση του θεσμικού πλαισίου λειτουργίας των λεσχών φιλάθλων, αθλητικός εθελοντισμός, πνευματικός αθλητισμός, ηλεκτρονικός αθλητισμός (e-sports), εργασιακός αθλητισμός, άλλες διατάξεις για τον εκσυγχρονισμό της αθλητικής νομοθεσίας και λοιπές διατάξεις, 4908 ΦΕΚ Α 52/11.3.2022,

https://www.kodiko.gr/nomologia/download_fek?f=fek/2022/α/fek_α_52_2022.pdf&t=b86065948aec4e9ff14e17e1b339c68α

N. 4637/2019, Τροποποιήσεις Ποινικού Κώδικα, Κώδικα Ποινικής Δικονομίας και συναφείς διατάξεις, ΦΕΚ Α' 180/18.11.2019,
https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/α/fek_α_180_2019.pdf&t=50α1αccd8eddc3daf21d00bef6b18160

N. 4619/2019, άρθρο 187, Κύρωση του Ποινικού Κώδικα, ΦΕΚ Α' 95/11.06.2019
<https://www.lawspot.gr/nomikes-plirotories/nomothesia/n-4619-2019/arthro-187-poinikos-kodikas-nomos-4619-2019-egklimatiki>

N. 4637/2019, Τροποποιήσεις Ποινικού Κώδικα, Κώδικα Ποινικής Δικονομίας και συναφείς διατάξεις, ΦΕΚ Α' 180/18.11.2019,
https://www.kodiko.gr/nomologia/download_fek?f=fek/2019/α/fek_α_180_2019.pdf&t=50α1αccd8eddc3daf21d00bef6b18160

N. 5090/2024, Εκσυγχρονισμός του νομοθετικού πλαισίου για την πρόληψη και την καταπολέμηση της ενδοοικογενειακής βίας, ΦΕΚ Α'/30/24.2.24,
https://www.kodiko.gr/nomologia/download_fek?f=fek/2024/α/fek_α_30_2024.pdf&t=b3d97e1c1ca002298f8α57359b257b4d

Κανονισμός (ΕΕ) 2016/679 (Γενικός Κανονισμός για την Προστασία Δεδομένων – GDPR), Άρθρο 5, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4.5.2016. Διαθέσιμο σε: <https://gdpr-info.eu/art-5-gdpr/>

Οδηγία 2014/41/ΕΕ ΤΟΥ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 3ης Απριλίου 2014 περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις,

Αρθρ.1,2,3,5, <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014L0041>