ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΣΤΟΙΧΕΙΑ ΔΙΚΑΙΟΥ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

DARK WEB

Αποκρυπτογράφηση του Dark Web

Νομικός Οδηγός

Ελένη Κεχριώτη

Μαρία Σχοινάκη

Αθήνα, 2024

Περιεχόμενα

1. Εισαγωγή

Οι ηλεκτρονικοί υπολογιστές έκαναν την εμφάνιση τους στην Ελλάδα πολύ αργότερα από ότι εμφανίστηκαν στις ΗΠΑ, ενώ το διαδίκτυο άρχισε να χρησιμοποιείται στη χώρα μας μόλις το 1990 από πανεπιστημιακά ιδρύματα και αργότερα από μεμονωμένα άτομα. Τότε το ηλεκτρονικό έγκλημα δεν ήταν διαδεδομένο, ούτε καν στις ΗΠΑ, για αυτό είναι και αναμενόμενο ότι η ελληνική έννομη ποινική τάξη δεν διέθετε ποινικές διατάξεις για την αντιμετώπιση αυτού του νέου φαινομένου, το οποίο εξελισσόταν διαρκώς και εκδηλωνόταν μέσα από νέες μορφές. Αυτές τις νέες μορφές ήρθε και συμπλήρωσε η δημιουργία του DarkNet, το οποίο προσέφερε την γλυκιά ανωνυμία σε όσους το χρησιμοποιούσαν, μια ευκαιρία που δύσκολα θα απέρριπτε ένας εγκληματίας. Λόγω αυτού στο Dark Web έχουν βρει "καταφύγιο" οι περισσότερες παράνομες δραστηριότητες και γίνεται ολοένα και δυσκολότερο τόσο να εξιχνιαστούν τα εγκλήματα που συμβαίνουν εκεί όσο και να καταδικαστούν οι δράστες, αφού στο Σκοτεινό Ιστό οι δράστες βρίσκουν συνεχώς "παραθυράκια" που δεν καλύπτει η νομοθεσία.

Σκοπός της παρούσας εργασίας είναι να κατανοήσει πως το σχετικό νομικό πλαίσιο στοχεύει στη διασφάλιση της δημόσιας τάξης και της προστασίας των πολιτών από τις απειλές που προκύπτουν μέσω του Σκοτεινού Διαδικτύου, καθώς και να εξερευνήσει τις διεθνείς και εγχώριες πρωτοβουλίες που έχουν αναπτυχθεί για την αντιμετώπιση αυτών των προκλήσεων. Μέσω της επιστημονικής αυτής προσέγγισης η εργασία αποσκοπεί στην ενίσχυση της κριτικής σκέψης και στην ανάπτυξη μιας συνειδητοποιημένης κατανόησης για τις διαστάσεις του φαινομένου προτρέποντας την ακαδημαϊκή κοινότητα και τους φορείς επιβολής του νόμου να αναζητήσουν αποτελεσματικές λύσεις σε ένα από τα πλέον περίπλοκα ζητήματα της εποχής της πληροφορίας.

Η εργασία οργανώνεται σε 3 κεφάλαια, καθένα από τα οποία έχουν διαφορετική θεματολογία. Στο δεύτερο κεφάλαιο αναλύεται το Darknet, και συγκεκριμένα ο ορισμός του, η ιδεολογία του και οι μορφές ηλεκτρονικού εγκλήματος που λαμβάνουν μέρος σε αυτό. Στο τρίτο κεφάλαιο αναφέρονται η σχετική νομοθεσία, τα νομικά μέσα αντιμετώπισης του ηλεκτρονικού εγκλήματος, καθώς και νομικές προκλήσεις. Τέλος, στο τέταρτο κεφάλαιο αναλύονται μερικές πρόσφατες και σημαντικές υποθέσεις που συνέβησαν στο Dark Web στην Ελλάδα αλλά και διεθνή. Στο τέλος του εγγράφου παρουσιάζονται τα συμπεράσματα αυτής της μελέτης.

2. Ηλεκτρονικό Έγκλημα & DarkNet

Το Darknet αποτελεί ένα ανατρεπτικό φαινόμενο στον κόσμο του διαδικτύου, αφού έχει αναπτυχθεί ως ένα πολυδιάστατο δίκτυο που λειτουργεί με απόλυτη ανωνυμία και περιορισμένη εμβέλεια. Αν και αρχικά δημιουργήθηκε από αμερικανικές μυστικές υπηρεσίες στις αρχές της δεκαετίας του '90 για λόγους ασφαλείας στις επικοινωνίες του ναυτικού στόλου των ΗΠΑ[1], σύντομα έγινε γνωστό στον υπόκοσμο ως ένας ασφαλής χώρος για παράνομες δραστηριότητες, λόγω της ανωνυμίας που προσφέρει. Αυτή η ανωνυμία διευκολύνει τη διεξαγωγή ηλεκτρονικού εγκλήματος (cybercrime), μέσω της χρήσης ενός υπολογιστή και ενός δικτύου, είτε ο υπολογιστής είναι το μέσο για τη διάπραξη του εγκλήματος είτε αποτελεί τον στόχο.

2.1 Λειτουργία του Darknet

Η λειτουργία του Darknet βασίζεται σε αρχές ανωνυμίας και κρυπτογράφησης, διαφοροποιώντας το σημαντικά από το επιφανειακό web. Αντί για τυπικές απαιτήσεις ταυτοποίησης, το Darknet επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους, χρησιμοποιώντας ειδικά δίκτυα όπως το Tor[1]. Αυτή η ιδιότητα το καθιστά ένα ελκυστικό εργαλείο για την εκτέλεση από απλές διαδικτυακές δραστηριότητες με διατηρημένη την ιδιωτικότητα μέχρι και για πιο αμφιλεγόμενες χρήσεις όπως παράνομες συναλλαγές και επικοινωνίες.

Αν και η ιδεολογία του Darknet παραμένει στα περιθώρια της νομιμότητας του διαδικτύου, σήμερα το φαινόμενο αυτό έχει εξελιχθεί σε έναν παράλληλο κόσμο που υπηρετεί τις ανάγκες της παρανομίας. Το οργανωμένο έγκλημα, η πορνογραφία ανηλίκων και η παραβίαση του απορρήτου είναι μερικά από τα παραδείγματα παράνομων ενεργειών που υποβοηθάει το δίκτυο αυτό. Παρά τις προσπάθειες των αρχών να καταπολεμήσουν τα εγκλήματα στο Darknet, η ανωνυμία που παρέχει αυτό καθιστά δύσκολη την ανίχνευση και την δίωξη των εγκληματιών, ενισχύοντας την παράνομη δραστηριότητα.

[1] *Masayuki Hatta*, Deep web, dark web, dark net: A taxonomy of "hidden" Internet, Annals of Business Administrative Science 19, 2020, σελ 278-281, διαθέσιμο: https://doi.org/10.7880/abas.0200908a

2.2 Μορφές Ηλεκτρονικού Εγκλήματος στο Dark Net

Η αυξανόμενη δημοτικότητα του Darknet έχει δώσει στους εγκληματίες του κυβερνοχώρου έναν πιο ασφαλή χώρο δράσης. Τα εγκλήματα που κυρίως λαμβάνουν χώρο στο DarkNet είναι παραδοσιακά ποινικά αδικήματα που πλαισιώνονται και διενεργούνται, εκμεταλλευόμενα, την ανωνυμία και την απλόχερη προσφορά ευρέα κρυφών δυνατοτήτων που προσφέρει ο Σκοτεινός Ιστός. Το πλαίσιο δράσης των εγκληματιών βασίζεται κυρίως στο γεγονός ότι μπορεί να χρησιμοποιηθεί ως εργαλείο επικοινωνίας και ανταλλαγής δεδομένων, καθώς και διάθεσης προϊόντων εγκλήματος.

2.2.1 Κλοπή Πληροφοριών και Δεδομένων

Η υποκλοπή δεδομένων αποτελεί σήμερα σοβαρή απειλή στον κυβερνοχώρο. Οι εισβολείς μπορούν να αξιοποιήσουν τόσο χειροκίνητες όσο και αυτοματοποιημένες επιθέσεις, στοχεύοντας στην παραβίαση και την εξαγωγή δεδομένων, για να υποκλέψουν πληροφορίες από εταιρείες και άτομα, ακόμα και την ίδια την κυβέρνηση.

Μια από τις κοινότερες τεχνικές υποκλοπής δεδομένων είναι η παραβίαση του DNS, η οποία επιτρέπει στους εισβολείς να ανακατευθύνουν την κυκλοφορία σε κακόβουλους ιστοτόπους. Άλλες μέθοδοι περιλαμβάνουν το Cache Poisoning και το Pharming[2], που αλλοιώνουν τις ρυθμίσεις DNS για να οδηγήσουν τους χρήστες σε παραπλανητικές διευθύνσεις IP.

Οι συνέπειες της υποκλοπής δεδομένων μπορεί να είναι σοβαρές, καθώς ευαίσθητες πληροφορίες πελατών, δεδομένα εργαζομένων και εταιρικά μυστικά, αλλά και κρατικά απόρρητα μπορούν εύκολα να διαρρεύσουν.

2.2.2 Κυβερνοεπιθέσεις & Αγορές Exploit

Τα Exploits, γνωστά και ως kit εκμετάλλευσης[3], είναι μία μορφή κυβερνοεπίθεσης που ενσαρκώνεται μέσω ενός κακόβουλο λογισμικό, εκμεταλλευόμενο ευπάθειες σε άλλο λογισμικό. Μια ειδική κατηγορία αποτελούν τα zero-day exploits, τα οποία εκμεταλλεύονται ευπάθειες που δεν έχουν ακόμα ανακαλυφθεί ή διορθωθεί. Οι προγραμματιστές διερευνούν τα συστήματα,

[2] What is Pharming?, mimecast, https://www.mimecast.com/content/what-is-pharming/, (τελευταία πρόσβαση στις 13/05/2024)
[3] Exploit Kits, Wikipedia, https://en.wikipedia.org/wiki/Exploit_kit, (τελευταία πρόσβαση στις 13/05/2024)

εντοπίζουν τις ευπάθειες και δημιουργούν τα exploit που θα χρησιμοποιηθούν κατά των ευάλωτων συσκευών. Η τιμή των exploit kits ποικίλλει ανάλογα με τον αριθμό των πιθανών θυμάτων.

Οι εγκληματίες μπορούν να αγοράσουν exploit kits μέσω του Darknet για να διεξάγουν ηλεκτρονικές επιθέσεις[4]. Τα exploit kits έχουν μεγάλη ζήτηση εξαιτίας της σπανιότητας των προγραμματιστών που δημιουργούν τέτοια λογισμικά.

2.2.3 Ναρκωτικές Ουσίες

Η διακίνηση ναρκωτικών είναι αναμφίβολα μια από τις πιο διαδεδομένες και κερδοφόρες δραστηριότητες στο Darknet. Σε αυτό τον ψηφιακό υπόκοσμο, η πώληση και η αγορά ναρκωτικών γίνεται μέσω διαφόρων πλατφορμών, όπως παράνομες ηλεκτρονικές αγορές, εφαρμογές συνομιλίας και forum. Παρά το γεγονός ότι οι αρχές (LEAs) καταβάλλουν σημαντικές προσπάθειες για να κλείσουν αυτές τις πλατφόρμες, πολλές νέες εμφανίζονται συνεχώς, διατηρώντας τη δραστηριότητα ζωντανή.

Οι συναλλαγές πραγματοποιούνται με κρυπτονομίσματα, διασφαλίζοντας την ανωνυμία και την ασφάλεια των συναλλαγών. Υπάρχουν δύο κύριοι τρόποι πληρωμής: η άμεση πληρωμή, όπου ο αγοραστής μεταφέρει τα χρήματα απευθείας στον προμηθευτή και η πληρωμή μέσω τρίτου, όπου ο διαχειριστής της πλατφόρμας λαμβάνει τα χρήματα και τα προωθεί στον προμηθευτή[5].

2.2.4 Εμπόριο Όπλων και Πυρομαχικών

Οι χρήστες του Darknet συχνά αναζητούν όπλα και πυρομαχικά από διάφορες παράνομες ιστοσελίδες, οι οποίες προσφέρουν μια μεγάλη ποικιλία όπλων με δυνατότητα παράδοσης κατ' οίκον. Αυτές οι παράνομες αγορές ποικίλλουν στις πολιτικές τους, αλλά η ανώνυμη φύση τους προσελκύει αγοραστές που θέλουν να αποφύγουν την παραδοσιακή αγορά όπλων.

Η εμπορία όπλων και πυρομαχικών αν και αποτελεί ένα μικρό κομμάτι της αγοράς του Darknet, έχει απασχολήσει ιδιαίτερα τις αρχές, λόγω των σημαντικών υποθέσεων και των συνεπειών

4 What is an Exploit Kit?,Startup Defense, https://www.startupdefense.io/blog/what-is-an-exploit-kit, 2023, (Τελευταία πρόσβαση στις 12/05/2024)

5 *Reid Southwick*, Inside the dark web drug trade,2024, https://newsinteractives.cbc.ca/longform/the-new-frontier-of-the-drug-trade/, (Τελευταία πρόσβαση στις 14/05/2024)

τους, που συμβαίνουν ανά τακτά χρονικά διαστήματα. Η εμπλοκή αυτή των αρχών φάνηκε κυρίως μετά το 2016, όπου ένας 18χρονος εισέβαλε οπλισμένος σε ένα εμπορικό κέντρο στο Μόναχο και σκότωσε 9 ανθρώπους[6]. Τα όπλα τα οποία χρησιμοποίησε, τα είχε προμηθευτεί από το Darknet.

Η ανώνυμη φύση του Darknet παρέχει αίσθηση ασφάλειας στους αγοραστές και τους ενθαρρύνει να προμηθεύονται όπλα από εκεί, αντί να αγοράζουν από φυσικά καταστήματα. Αυτό οφείλεται στο γεγονός ότι οι συναλλαγές πραγματοποιούνται με απόλυτη ανωνυμία, χρησιμοποιώντας τεχνολογίες όπως το VPN και το Bitcoin[7].

2.2.5 Σωματεμπορία

Η σωματεμπορία στο Darknet υποβοηθάται από ανώνυμες πλατφόρμες, κρυπτονομίσματα και κρυπτογραφημένες επικοινωνίες, επιτρέποντας στους διακινητές να πωλούν και να διακινούν ανθρώπινα όντα με ασφάλεια. Οι εγκληματικές ομάδες χρησιμοποιούν αυτές τις τεχνολογίες για να διαφημίσουν παράνομες υπηρεσίες και να διευκολύνουν τη μεταφορά θυμάτων. Οι προσπάθειες επιβολής του νόμου εστιάζουν στην ανίχνευση αυτών των δραστηριοτήτων μέσω παγκόσμιας συνεργασίας και περιορισμό της αυτού τεχνολογίας[8].

2.2.6 Τρομοκρατία

Το Dark Web αποτελεί ιδανικό περιβάλλον για την επικοινωνία και την οργάνωση τρομοκρατικών ομάδων λόγω της ανωνυμίας που παρέχει. Οι τρομοκράτες χρησιμοποιούν κρυπτογραφημένες πλατφόρμες για την ανταλλαγή πληροφοριών και την προετοιμασία επιθέσεων, με τη χρήση κρυπτονομισμάτων και κρυπτογραφημένων επικοινωνιών να επιτρέπουν την ανεμπόδιστη δράση τους[9]. Οι προσπάθειες καταπολέμησης των τρομοκρατικών επιθέσεων

---

6 Shooter who killed 9 in Munich was 18-year-old with dual Iranian German nationality, The Washington Post, 2016, (Τελευταία Πρόσβαση στις 11/05/2024)

7 International arms trade on the dark web, Rand, https://www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html (Τελευταία Πρόσβαση στις 13/05/2024)

8 *Campbell C.*, Web of Lives: How Regulating the Dark Web Can Combat Online Human Trafficking, Hein Online, 2018, σελ 136

9 *Καψοκόλη Ε.*, Η χρήση του κυβερνοχώρου από τους τρομοκράτες: Η περίπτωση του ISIS, μέσα στο Βιβλίο Διακυβέρνηση του κυβερνοχώρου και κυβερνοασφάλεια στις διεθνείς σχέσεις, εκδόσεις Παπαζήση, 2022, σελ 211-234

περιλαμβάνουν την παρακολούθηση των διαδικτυακών δραστηριοτήτων του ψηφιακού κόσμου και τη συνεργασία μεταξύ διεθνών φορέων[10].

2.2.7 Πορνογραφία Ανηλίκων

Ακόμα μια σκοτεινή πλευρά του διαδικτύου στην οποία προσφέρει πρόσβαση το Darknet, είναι οι ιστοσελίδες με "πλούσιο" υλικό σεξουαλικής εκμετάλλευσης ανηλίκων. Το ακατάλληλο αυτό περιεχόμενο, μπορεί να περιλαμβάνει κακοποίηση ανηλίκων σε ζωντανή μετάδοση, με την υπόσχεση υψηλών αμοιβών για τους παραγωγούς τους, καθώς και ανάρτηση και λήψη ψηφιακού υλικού[11].

Αν και οι προσπάθειες των αρχών επιβολής του νόμου έχουν οδηγήσει στο κλείσιμο πολλών ιστοσελίδων που προωθούν αυτό το υλικό, η εμπορία πορνογραφίας ανηλίκων στο Darknet παραμένει ένα σοβαρό πρόβλημα. Οι παραβάτες συνεχίζουν να δραστηριοποιούνται, χρησιμοποιώντας forum και κρυπτογραφημένες συνδέσεις για τη διακίνηση παράνομου περιεχομένου, ενώ πολλές ομάδες παραγωγών συνεχίζουν να λειτουργούν κρυφά.

3. Νομοθεσία και Νομικά Ζητήματα

Τα τελευταία χρόνια υπάρχουν ολοένα και περισσότερες αντιφατικές εκκλήσεις για περισσότερη κυβερνητική επιτήρηση στο διαδίκτυο και αυξημένη προστασία της ιδιωτικής ζωής και της ανωνυμίας των ατόμων. Πολλές επιχειρήσεις έχουν κριθεί για την ανταλλαγή δεδομένων με τις υπηρεσίες επιβολής του νόμου και άλλες, για την άρνησή τους, προκειμένου να προστατέψουν τα ιδιωτικά δεδομένα των πελατών τους. Ο σκοτεινός ιστός αντιπροσωπεύει την ελευθερία του λόγου τόσο στην ανωνυμία όσο και στις πιθανές σκοτεινές πλευρές του τι μπορεί να δημιουργούνται όταν η ανωνυμία και ο ανεξέλεγκτος λόγος - συμπεριλαμβανομένης της εμπορίας παράνομων ουσιών και υπηρεσιών - συνδέει[12].

---

10 *ABHISHEK S*,Countering Terrorism through Dark Web Analysis, IEEE, 2012, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6396055&tag=1 (τελευταία πρόσβαση στι1 12/05/2024)

11 *Siniša Franjić*, Child Pornography Is Showing Participation a Person Under the Age of 18 in Sexual Intercourse, Studies in Law and Justice, 2023, σελ 39–45, διαθέσιμο στο https://www.pioneerpublisher.com/slj/article/view/188

12 *Kokolaki E., Daskalaki E., Psaroudaki K., Christodoulaki M, Fragopoulou P.,* Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation, Foundation for Research and Technology, 2020, Διαθέσιμο στο Research Gate

Σε παγκόσμια κλίμακα, η νομοθεσία για τα θέματα που αφορούν το Dark Web είναι θολή έως ανύπαρκτη. Αυτό οφείλεται στο γεγονός ότι το DarkNet δεν καθίσταται παράνομο, όπως παράνομη δεν καθίσταται και η πρόσβαση σε αυτό. Παράνομες είναι οι δραστηριότητες που παίρνουν μέρος σε αυτό και όχι το ίδιο το δίκτυο. Στην Ευρωπαϊκή Ένωση (ΕΕ), η νομοθεσία περί Dark Web ενσωματώνεται σε ευρύτερα νομικά πλαίσια που αφορούν την κυβερνοασφάλεια, την καταπολέμηση της παιδικής πορνογραφίας και την εξάλειψη του οργανωμένου εγκλήματος.

3.1 Προσωπικά Δεδομένα

Η ΕΕ επέβαλε ένα ευρύ φάσμα μέτρων προστασίας της ιδιωτικής ζωής υπό την αιγίδα του Γενικού Κανόνα Προστασίας Δεδομένων (GDPR)[13], ο οποίος διέπει την συλλογή, αποθήκευση και επεξεργασία προσωπικών δεδομένων, συμπεριλαμβανομένων και εκείνων που ανταλλάσσονται στον σκοτεινό ιστό. Ο GDPR επιτρέπει στις εθνικές αρχές προστασίας δεδομένων να επιβάλλει ποινές και κυρώσεις για παραβάσεις που αφορούν την ασφάλεια των δεδομένων που μπορούν να συμβούν στα πλαίσια του σκοτεινού ιστού και αναγκάζει τις επιχειρήσεις να είναι συνεπής με την προστασία των δεδομένων εργαζομένων και πελατών[14].

3.2 Κυβερνοασφάλεια

Άλλος ένας κανονισμός που επιβλήθηκε από την ΕΕ στα πλαίσια της κυβερνοασφάλειας είναι η Οδηγία Ασφάλειας Δικτύων και Πληροφοριών (NIS2 Directive)[15]. Ο σκοτεινός ιστός επηρεάζει την κυβερνοασφάλεια, καθώς μέσου αυτού μπορούν εύκολα να εκτελεστούν κυβερνοεπιθέσεις και άρα υπόκεινται άμεσα στις νομικές διατάξεις του NIS2. Επίσης, λειτουργεί μέσω τρωτών δικτύων που είναι ευάλωτα σε κυβερνοεπιθέσεις και άρα ο NIS2 προκειμένου να προστατέψει κάθε είδους δίκτυο, συμπεριλαμβανομένου και του σκοτεινού ιστού, εφαρμόζει μέτρα

13 https://gdpr-info.eu/, (Τελευταία Πρόσβαση στις 12/05/2024)

14 Γκρίτζαλης Σ., Κάτσικας Σ., Λαμπρινουδάκης Κ., Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, εκδόσεις Νέων Τεχνολογιών, 2021, σελ 91-95

15 NIS Directive, enisa, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (Τελευταία Πρόσβαση στις 15/04/2024)

ασφαλείας όπως παρακολούθηση των δικτύων και ανίχνευση επιθέσεων, με αποτέλεσμα τον άτυπο περιορισμό των δραστηριοτήτων του Dark Web[16].

3.3 Οργανωμένο Έγκλημα

Το οργανωμένο έγκλημα[17] συνίσταται σε εγκληματικές ομάδες που επιδιώκουν κέρδος μέσω παράνομων υπηρεσιών όπως, τρομοκρατικές ενέργειες, παράνομη διάθεση ουσιών καθώς και σωματεμπορία. Οι εγκληματικές αυτές ομάδες εκμεταλλεύονται την τεχνολογία του Darknet για να πραγματοποιούν και να επεκτείνουν τις δραστηριότητές τους με τρόπο που είναι δύσκολο να εντοπιστεί από τις αρχές.

3.3.1 Ναρκωτικές Ουσίες

Άλλη μία μορφή οργανωμένου εγκλήματος που λαμβάνει χώρο στο Dark Web όπως προαναφέρθηκε είναι και το εμπόριο απαγορευμένων ουσιών. Στην Ελλάδα, έχει θεσπιστεί αντίστοιχος νόμος που ποινικοποιεί τέτοιους είδους υποθέσεις. Ειδικότερα, ο νόμος 4139/2013[18] κυρώνει διατάξεις σχετικές με μορφές διακίνησης και εμπορίας εξαρτησιογόνων ουσιών. Σύμφωνα με το άρθρο 2, η διάθεση των ουσιών του πίνακα Α' της παρ. 2 του άρθρου 1 του ν. 3459/2006 (Α' 103)[19], είναι αποκλειστικό δικαίωμα του Κράτους και οποιαδήποτε παράβαση διώκεται ποινικά. Ο σκοτεινός ιστός παρέχει ένα ανώνυμο περιβάλλον όπου οι δραστηριότητες όπως η διακίνηση ναρκωτικών μπορούν να λαμβάνουν χώρα με μεγαλύτερη δυσκολία στην ανίχνευση. Ο νόμος μπορεί να χρησιμοποιηθεί για τη δίωξη και τιμωρία ατόμων και οργανώσεων που διαπράττουν αξιόποινες πράξεις στον σκοτεινό ιστό, συμπεριλαμβανομένης της παράνομης διακίνησης ναρκωτικών.

3.3.2 Όπλα και Πυρομαχικά

Ένα ακόμη έγκλημα που ανήκει στο ευρύ φάσμα του οργανωμένου εγκλήματος είναι το εμπόριο όπλων και πυρομαχικών. Στην Ελλάδα, έχει θεσπιστεί αντίστοιχος νόμος που ποινικοποιεί

---

[16] *Γκρίτζαλης Σ., Κάτσικας Σ., Λαμπρινουδάκης Κ.*, Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, ό.π, σελ. 76-83

[17] Το οργανωμένο έγκλημα Έννοια, χαρακτηριστικά, αντιμετώπιση, Ελληνική Αστυνομία, https://www.astynomia.gr/2009/10/30/organomeno-egklima/ (τελευταία πρόσβαση στις 14/05/2024)

[18] Νόμος 4139/2013 - Νόμος περί εξαρτησιογόνων ουσιών και άλλες διατάξεις, (Τελευταία Πρόσβαση στις 14/05/2024)

[19] Νόμος 3459/2006 (Κωδικοποιημένος) - ΦΕΚ Α 103/25.05.2006

τέτοιους είδους υποθέσεις. Συγκεκριμένα, ο νόμος 2168/1993[20] εγκυροποιεί νομικά διατάξεις σχετικές με το εμπόριο, την κατοχή και χρήση πυρομαχικών και όπλων. Σύμφωνα με το άρθρο 6, η εμπορία και η διάθεση, με οποιονδήποτε τρόπο, όπλων και αντικειμένων, που αναφέρονται στο άρθρο 1 του παρόντος νόμου, απαγορεύεται και διώκεται ποινικά. Η ανωνυμότητα του DarkNet αποτελεί υψηλό θέλγητρο επισκεψιμότητας για την πλαισίωση τέτοιου είδους αδικημάτων, καθώς η ανίχνευση των πράξεων είναι δύσκολη. Ο νόμος μπορεί να χρησιμοποιηθεί για την δίωξη και τιμωρία ατόμων και οργανώσεων που διαπράττουν σχετικά εγκλήματα στον σκοτεινό ιστό, με μόνη απαίτηση την σχετική εξιχνίαση.

3.3.3 Σωματεμπορία

Στον σκοτεινό ιστό η σωματεμπορία μπορεί να λάβει μέρος μέσω πολλών κρυπτογραφημένων επικοινωνιών και αγορών ανθρώπινων όντων για σεξουαλική εκμετάλλευση, δουλεία και πολλές άλλες μορφές εκμετάλλευσης. Η Ελληνική Κυβέρνηση έχει εγκρίνει νόμους ανεξάρτητα, ακόμα και σε συνεργασία με άλλες χώρες προκειμένου να περιορίσουν τέτοιου είδους ενέργειες. Συγκεκριμένα, στο άρθρο 323Α[21] του Ποινικού Κώδικα, κατακριτέα και διώξιμη ποινικά θεωρείται οποιαδήποτε πράξη σχετική με την σωματεμπορία και την σχετική ανθρώπινη εκμετάλλευση. Πιο συγκεκριμένα, το άρθρο αυτό ποινικοποιεί την πράξη της συγκράτησης ή εκφόρτωσης ανθρώπων χωρίς τη συναίνεσή τους, όπως σε περιπτώσεις ανθρώπινης εμπορίας ή εκμετάλλευσης. Άλλη μία μορφή αντιστάθμισης τέτοιου είδους ενεργειών είναι η Συμφωνία μεταξύ της Κυβέρνησης της Ελληνικής Δημοκρατίας και της Κυβέρνησης της Ουκρανίας[22], η οποία προβάλλει την συνεργασία των συμβαλλόμενων χωρών σε θέματα τρομοκρατίας, παράνομης διακίνησης ναρκωτικών, οργανωμένου εγκλήματος και άλλων μορφών εγκληματικότητας, προκειμένου να εξαλειφθούν. Παρόλο που το άρθρο και η Συμφωνία δεν αναφέρονται συγκεκριμένα στον σκοτεινό ιστό, μπορεί να χρησιμοποιηθούν για την δίωξη παραβατών, που ενεργούν μέσω αυτού και άρα να περιοριστούν και να κριθούν ποινικά τέτοιου είδους εγκλήματα.

---

20 https://www.kodiko.gr/nomothesia/document/156460/nomos-3459-2006 (Τελευταία Πρόσβαση στις 16/05/2024)

21 https://www.hellenicparliament.gr/UserFiles/bcc26661-143b-4f2d-8916-0e0e66ba4c50/k-porno-pap.pdf, σελ 1 (Τελευταία Πρόσβαση στις 14/05/2024)

22 Νόμος 3158/2003 - ΦΕΚ 163/Α/26-6-2003 - ΔΙΕΘΝΕΙΣ ΣΥΜΦΩΝΙΕΣ - ΣΥΜΒΑΣΕΙΣ - ΣΥΝΘΗΚΕΣ, (Τελευταία Πρόσβαση στις 14/05/2024)

3.3.4 Τρομοκρατία

Λόγω της ανωνυμίας που υπάρχει στο Dark Web, αναπτύσσεται ένα ανώνυμο περιβάλλον, στο οποίο μπορούν οι εγκληματίες να επικοινωνούν και να σχεδιάζουν παράνομες δραστηριότητες. Μια από τις δραστηριότητες αυτές είναι οι τρομοκρατικές οργανώσεις. Σύμφωνα με τον νόμο 4619/2019, άρθρο 187Α[23], μια τρομοκρατική οργάνωση είναι μια ομάδα ανθρώπων, η οποία τελεί έγκλημα γενικής διακινδύνευσης ή κατά της δημόσιας τάξης με σοβαρό κίνδυνο για την χώρα και τους πολίτες της. Η ένταξη σε αυτές τις ομάδες, όπως και η παρακίνηση για ένταξη άλλων ατόμων τιμωρείται με τουλάχιστον 6 μήνες, ένω η διαρκής δράση τιμωρείται με 10 χρόνια. Ακόμη, για να περιοριστεί το τρομοκρατικό περιεχόμενο στο διαδίκτυο και η διάδοση του, δημοσιεύτηκε πρόσφατα στην εφημερίδα της Κυβερνήσεως, ο νόμος 5067/2023[24], με τον οποίο θεσπίστηκαν νέα μέτρα, έτσι ώστε να μην περιορίζεται η ελευθερία έκφρασης στο διαδίκτυο, αλλά να διασφαλίζεται η προστασία της δημόσιας ασφάλειας.

3.4 Πορνογραφία Ανηλίκων

Στο Dark Web αποτελεί συχνό φαινόμενο η πορνογραφία ανηλίκων, δηλαδή η διακίνηση υλικού παιδικής πορνογραφίας και η μεταφορά πληροφοριών αναφορικά σε αυτές τις πράξεις. Στην Ελλάδα, όπως και σε πολλές άλλες χώρες, αλλά και σε διεθνή επίπεδα, έχουν θεσπιστεί ειδικοί νόμοι για την μείωση αυτών των πράξεων. Συγκεκριμένα, ο νόμος 4619/2019, άρθρο 348Α[25], τονίζει ότι το προαναφερθέν έγκλημα τελούν όσοι α) διαπράττουν το έγκλημα κατ' επάγγελμα, β) παράγουν πορνογραφικό υλικό για την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή της σωματικής δυσλειτουργίας, γ) ο δράστης παραγωγής είναι προσωρινός ή μη κηδεμώνας, δ) αποκτούν εν γνώσει τους πρόσβαση σε υλικό μέσω του διαδικτύου, και διώκονται ποινικά με κάθειρξη και χρηματική ποινή.

---

23 Άρθρο 187Α - Ποινικός Κώδικας (Νόμος 4619/2019) - Τρομοκρατικές πράξεις – Τρομοκρατική οργάνωση, (Τελευταία Πρόσβαση στις 12/05/2024)

24 Δημοσιεύθηκε ο νόμος για την πρόληψη διάδοσης τρομοκρατικού περιεχομένου στο διαδίκτυο (Ν. 5067/2023), (Τελευταία Πρόσβαση στις 14/05/2024)

25 Άρθρο 348Α - Ποινικός Κώδικας (Νόμος 4619/2019) - Πορνογραφία ανηλίκων, (Τελευταία Πρόσβαση στι; 14/05/2024)

3.5 Απόρρητο

Μια ακόμη δραστηριότητα που συμβαίνει στο Dark Web είναι ο διαμοιρασμός στοιχείων ή προγραμμάτων υπολογιστή, τα οποία μπορούν να είναι κρατικά, επιστημονικά, στρατιωτικά, διπλωματικά ή επαγγελματικά απόρρητα. Σύμφωνα με τον νόμο 370Β Π.Κ[26] , οι δράστες οι οποίοι αντιγράφουν, εκτυπώνουν, χρησιμοποιούν, αποκαλύπτουν σε τρίτο ή παραβιάζουν αυτά τα απόρρητα τιμωρούνται με φυλάκιση τουλάχιστον 1 έτους. Με τη διάταξη αυτή, σκοπός είναι να προστατευτούν όλων των ειδών τα απόρρητα από κακόβουλους δράστες, αλλά ακόμα και από το απλό κοινό, ιδίως όταν πρόκειται για κρατικά έγγραφα.

3.6 Διεθνείς Φορείς Επιβολής του Νόμου

Σε περισσότερο διεθνή όρια, η Ελληνική Αστυνομία συνεργάζεται με διάφορες οργανώσεις αλλά και συναρμόδιους φορείς, όπως η Europol, η Interpol, και μέσω αυτής με τις αρχές διαφόρων κρατών, όπως οι ΗΠΑ, η Ολλανδία, το Ισραήλ, η Ρουμανία και άλλες, για την αντιμετώπιση του ηλεκτρονικού εγκλήματος και της παράνομης χρήσης του Darknet.

3.6.1 Europol

Ένας από αυτούς τους οργανισμούς είναι η Europol, η Ευρωπαϊκή Υπηρεσία Καταπολέμησης της Ηλεκτρονικής Εγκληματικότητας, η οποία είναι υπεύθυνη για την συλλογή, ανάλυση και ανταλλαγή πληροφοριών μεταξύ ευρωπαϊκών αρχών επιβολής του νόμου σχετικά με το ηλεκτρονικό έγκλημα, συμπεριλαμβανομένης της δραστηριότητας στο Darknet[27]. Με αυτή της την δράση, η Europol, έχει καταφέρει να αντιμετωπίσει πολλά ηλεκτρονικά εγκλήματα και να διώξει ποινικά τους δράστες.

Ακόμη, η Ευρωπαϊκή Ένωση, και συγκεκριμένα η Europol, έχει αναπτύξει σχέδια δράσης για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας, όπως για παράδειγμα την σεξουαλική εκμετάλλευση ανηλίκων[28] που συμβαίνει στο Dark Web. Τα σχέδια αυτά συμπεριλαμβάνουν

26 Άρθρο 370Β - Ποινικός Κώδικας (Νόμος 4619/2019) - Παράνομη πρόσβαση σε σύστημα πληροφοριών ή σε δεδομένα, (Τελευταία Πρόσβαση στις 13/05/2024)

27 Crime on the dark web: law enforcement coordination is the only cure | Europol (europa.eu) (Τελευταία Πρόσβαση στις 14/05/2024)

28 Child Sexual Exploitation | Europol (europa.eu) (Τελευταία Πρόσβαση στις 14/05/2024)

συνεργασία μεταξύ των ευρωπαϊκών κρατών με στόχο την ανάπτυξη κοινών προτύπων για την αντιμετώπιση του ηλεκτρονικού εγκλήματος.

3.6.2 Interpol

Η Interpol είναι είναι ένας διεθνής οργανισμός που διευκολύνει την παγκόσμια αστυνομική συνεργασία και τον έλεγχο του εγκλήματος. Η Interpol παρέχει ερευνητική υποστήριξη, εμπειρογνωμοσύνη και εκπαίδευση στις αρχές επιβολής του νόμου παγκοσμίως, εστιάζοντας σε τρεις κύριους τομείς του διεθνικού εγκλήματος: την τρομοκρατία, το έγκλημα στον κυβερνοχώρο και το οργανωμένο έγκλημα[29].

3.6.3 Lawful Hacking

Ωστόσο, το ηλεκτρονικό έγκλημα πλέον, ιδίως αυτό που λαμβάνει μέρος στο Dark Web, έχει εξελιχθεί αρκετά, δυσκολεύοντας έτσι τις υπηρεσίες επιβολής του νόμου, να εντοπίσουν τους δράστες και να καταπολεμήσουν το έγκλημα. Έτσι, έχουν εξελιχθεί και τα πρότυπα αντιμετώπισης, περιλαμβάνοντας νέα μέτρα και θεσπίζοντας νέους νόμους.
Ένα από αυτά τα μέτρα είναι η χρησιμοποίηση του hacking ως εργαλείου για την καταπολέμηση του ηλεκτρονικού εγκλήματος[30]. Αν και δεν έχει οριστεί επίσημα από την Europol, η δράση αυτή συνηθίζεται να αναφέρεται ως "νόμιμο Hacking"[31], και οι είναι οι χρησιμοποίηση τεχνικών hacking από LEAs, με σκοπό την απόκτηση πρόσβασης σε συσκευές και δίκτυα, έτσι ώστε να εξιχνιάσουν εγκληματική δραστηριότητα. Η Europol έχει δηλώσει την ανάγκη χρήσης του "νόμιμου Hacking" λόγω της ισχυρής κρυπτογράφησης σε ηλεκτρονικές συσκευές που υπονομεύει την έρευνα και τη δίωξη των οργανωμένων εγκλημάτων, καθώς τα δεδομένα δεν είναι διαθέσιμα ή μη αναγνωρίσιμα. Η χρήση της κρυπτογράφησης έχει αυξήσει τον αριθμό των σοβαρών εγκλημάτων, τα οποία έχουν αναγνωριστεί από την Europol ως απειλή για τη δημόσια τάξη και ασφάλεια, την αποτελεσματικότητα του συστήματος ποινικής δικαιοσύνης και το

29 https://www.interpol.int/fr/Qui-nous-sommes/Qu-est-ce-qu-INTERPOL (Τελευταία Πρόσβαση στις 14/05/2024)

30 *Ghappour A.*, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, Boston University School of Law, 2017, σελ 22-24, Διαθέσιμο στο https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1205&context=faculty_scholarship

31 *An Nhien, Iman, Liudmila, Timothy, Alice*, Hacking for Justice: How Europol Walks the Tightrope Between Fighting Crime and Protecting Fundamental Rights, EU Law Enforcement, 2023, Διαθέσιμο στο https://eulawenforcement.com/?p=8566 (Τελευταία Πρόσβαση στις 14/05/2024)

κράτος δικαίου. Αντίθετα, η ίδια η χρήση "νόμιμου Hacking" μπορεί να εγκυμονεί κινδύνους για την προστασία των θεμελιωδών δικαιωμάτων. Πράγματι, η εφαρμογή αυτής της μεθόδου μπορεί, για παράδειγμα, να επηρεάσει δυνητικά το απόρρητο των ατόμων εάν οι LEA έχουν υπερβολική πρόσβαση σε προσωπικά δεδομένα χωρίς επαρκείς έγκυρους λόγους ή νόμιμους σκοπούς. Ως εκ τούτου, η χρήση "νόμιμου Hacking" εκ μέρους των LEA έχει γίνει ένα επίμαχο ζήτημα στην Ευρωπαϊκή Ένωση (ΕΕ), εγείροντας ερωτήματα σχετικά με την ισορροπία μεταξύ των αναγκών των LEA και των ατομικών δικαιωμάτων απορρήτου.

3.7 Νομικές Προκλήσεις

Παρά τη σημασία της, η ψηφιακή αστυνόμευση του σκοτεινού ιστού παρουσιάζει στους LEA αρκετές νομικές προκλήσεις. Για αρχή, υπάρχει έλλειψη ομοιομορφίας στο διεθνές δίκαιο και όταν ένα έγκλημα συμβαίνει πέρα από τα σύνορα, η ευθύνη είναι κοινή, γεγονός που μπορεί να καταστήσει δύσκολη τη δίκαιη απονομή της δικαιοσύνης. Αυτό δημιουργεί προκλήσεις δικαιοδοσίας, για παράδειγμα, η Κίνα, η οποία είναι κατηγορηματικά αντίθετη στη χρήση των TOR σε οποιαδήποτε κατάσταση, έχει πολιτικές και νόμους σχετικά με τους χρήστες της που είναι αρκετά διαφορετικοί από αυτούς στις Ηνωμένες Πολιτείες και την Ευρώπη.

Λόγω αυτών των διαφορετικών πολιτικών συχνά καθίσταται δύσκολη η εξιχνίαση του εγκλήματος. Για παράδειγμα, στην Αμερική ισχύει η τέταρτη τροπολογία, η οποία προστατεύει τους ανθρώπους από αυθαίρετη έρευνα και κατάσχεση, καθώς ο σεβασμός της ιδιωτικής ζωής του ατόμου, ενώ δεν αισθάνεται ότι όλα παρακολουθούνται από την κυβέρνηση είναι θεμελιώδες ανθρώπινο δικαίωμα. Έτσι, οι συσκευές hacking μπορεί να θεωρηθεί ότι υπονομεύουν αυτή την ελευθερία για πολλούς. Με τη τροπολογία αυτή, καθίσταται δύσκολη η γρήγορη εξιχνίαση του διασυνοριακού εγκλήματος, εφόσον μπορεί να έρχεται σε σύγκρουση με την πολιτική άλλου κράτους.

Επίσης, η εθνική κυριαρχία μπορεί να απειληθεί εάν οι εγκληματίες καταδιώκονται πέρα από τα σύνορα ή εάν υπάρχουν μη εξουσιοδοτημένες έρευνες ξένων κυβερνήσεων. Θεωρείται εισβολή

στην κυριαρχία άλλου κράτους η εκτέλεση λειτουργιών επιβολής του νόμου εντός άλλου κράτους χωρίς τη συγκατάθεση αυτού του κράτους[32].

4. Νομικές Υποθέσεις

4.1 Απάτη με Υπολογιστή

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος ανέλαβε τον Απρίλιο του 2024 τη διερεύνηση μιας υπόθεσης που είχε προκύψει μετά από καταγγελίες πολιτών. Η υπόθεση αφορούσε μιαν ειδικά οργανωμένη εγκληματική ομάδα, η οποία επιδίδονταν σε απάτες και παραβίαση ηλεκτρονικών συστημάτων με σκοπό την παράνομη απόκτηση κερδών[33].

Η ομάδα απαρτίζονταν από 4 άτομα με ειδίκευση και γνώση στον τομέα της τεχνολογίας και συγκεκριμένα του διαδικτύου και του τρόπου λειτουργίας των τραπεζών, των ηλεκτρονικών πλατφορμών ακόμα και των υπηρεσιών Ψηφιακής Διακυβέρνησης (e-GOV). Δρούσαν κυρίως στη Θεσσαλονίκη, ενώ εκτελούσαν εγκληματικές πράξεις σε πανελλαδικό επίπεδο. Με τη βοήθεια 12 ακόμη ατόμων, πραγματοποιούσαν απάτες και παραβιάσεις ασφάλειας, αποκτώντας χρήματα παράνομα, μέσω της εκμετάλλευσης προσωπικών δεδομένων.

Ο τρόπος λειτουργίας τους περιλάμβανε την αναζήτηση και την αγορά προσωπικών δεδομένων από το Darknet, την παραβίαση ασφαλείας διαφόρων υπηρεσιών, και την πραγματοποίηση μη εξουσιοδοτημένων συναλλαγών σε υπηρεσίες e-banking. Η ομάδα προσπάθησε να ξεπλύνει τα χρήματα που αποκόμισε μέσω λογαριασμών σε διάφορα ηλεκτρονικά συστήματα, αλλά η δράση της ανακαλύφθηκε από τις αρχές. Τα μέλη της οργάνωσης έχοντας αποκτήσει 315.948,53 ευρώ, διώχθηκαν ποινικά και μετά την απολογία τους δύο από τους βασικούς κατηγορούμενους κρίθηκαν προφυλακιστέοι.

32 Warner C., Law Enforcement and Digital Policing of the Dark Web: An Assessment of the Technical, Ethical and Legal Issues. In: Montasari, R. Springer, Διαθέσιμο στο https://doi.org/10.1007/978-3-031-40118-3_7 (Τελευταία Πρόσβαση στις 13/05/2024

33 04-04-2024: Από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος διακριβώθηκε η δράση εγκληματικής οργάνωσης, τα μέλη της οποίας διέπρατταν συστηματικά απάτες με υπολογιστή (Τελευταία Πρόσβαση στις 15/05/2024)

4.2 Αγορά Όπλων

Τον Μάρτιο του 2023 ένας 30χρονος Έλληνας από τη Λαμία παρήγγειλε ένα πιστόλι αξίας 1.800 ευρώ μέσω μιας ιστοσελίδας στο Dark Web. Οι αμερικανικές αρχές εντόπισαν την παραγγελία και ανέλαβαν δράση, εμποδίζοντας την αποστολή του όπλου προς την Ελλάδα. Στη συνέχεια, ειδοποίησαν τις ελληνικές αρχές, οι οποίες ταυτοποίησαν τον αγοραστή και τον συνέλαβαν. Ο δράστης κατηγορήθηκε για παράβαση της νομοθεσίας περί όπλων[34].

Στο παρελθόν τα εγκλήματα που σχετίζονταν με το Dark Web στην Ελλάδα ήταν κατά κόρον υποθέσεις διακίνησης ναρκωτικών. Το έναυσμα για την έξαρση της επικινδυνότητας έρχεται να θέσει αυτή η υπόθεση, που είναι η πρώτη επιβεβαιωμένη δραστηριότητα λαθρεμπορίου όπλων, για την οποία σχηματίστηκε δικογραφία με τα στοιχεία του δράστη.

4.3 Διεθνής Αγορά Ναρκωτικών

Το 2019, ο Milomir Desnica , 35 ετών, από την Σερβία, ξεκίνησε και λειτούργησε μια αγορά στο Darknet, γνωστή ως “Monopoly Market”, με σκοπό την πώληση παράνομων ναρκωτικών, συμπεριλαμβανομένων οπιοειδών, διεγερτικών, ψυχεδελικών και συνταγογραφούμενων φαρμάκων, μεταξύ άλλων. Ο Desnica κατηγορείται για συνωμοσία για διανομή και κατοχή με σκοπό τη διανομή μεθαμφεταμίνης και για συνωμοσία για να πλένει νομισματικά μέσα[35].

Η κοινή επιχείρηση με το όνομα SpecTor, στην οποία συμμετείχαν αρχές επιβολής από τις Ηνωμένες Πολιτείες, το Ηνωμένο Βασίλειο, τη Βραζιλία και την Ευρώπη, είχε ως αποτέλεσμα την κατάσχεση της παράνομης αγοράς στο Dark Web και τη σύλληψη 288 ατόμων που εμπλεκόνταν στην εμπορία ναρκωτικών στο σκοτεινό διαδίκτυο. Η Europol ηγήθηκε αυτής της επιχείρησης, η οποία διευκολύνθηκε από πληροφορίες που συγκεντρώθηκαν από προηγούμενη δράση της γερμανικής αστυνομίας κατά της υποδομής του Monopoly Market[36]. Οι συλλήψεις έλαβαν χώρα σε όλη την Ευρώπη, τις ΗΠΑ, το Ηνωμένο Βασίλειο και τη Βραζιλία, με αρκετούς ύποπτους να θεωρούνται ως στόχοι υψηλής αξίας. Αυτή η συνεργατική προσπάθεια οδήγησε σε καταδίκες και σε εκκρεμείς διώξεις, ιδίως εναντίον διακινητών ναρκωτικών. Η επιχείρηση

34 «Σούπερ μάρκετ» όπλων στο Dark Web: Έλληνας έκανε παραγγελία (Τελευταία Πρόσβαση στις 15/05/2024)

35 District of Columbia | Citizen of Croatia and Serbia Charged with Running Monopoly Drug Market on the Darknet | United States Department of Justice (Τελευταία Πρόσβαση στις 15/05/2024)

36 Nearly 300 arrested in US-Europe dark web drug bust (Τελευταία Πρόσβαση στις 15/05/2024)

επίσης επέφερε σημαντικές κατασχέσεις, συμπεριλαμβανομένων μετρητών, εικονικών νομισμάτων και μεγάλης ποσότητας ναρκωτικών. Αποτέλεσμα αυτής της σύλληψης ήταν ο Desnica να καταδικαστεί στις παραπάνω κατηγορίες με φυλάκιση 14 χρόνων[37].

5. Συμπεράσματα

Η έρευνα για το Darknet αποκαλύπτει ένα πρόσφορο έδαφος άνθισης ποινικά διωκόμενων εγκλημάτων, που στηρίζονται στην σχετική δυσκολία ανίχνευσης. Παρά τη νομιμότητα της ίδιας της πλατφόρμας του Darknet, οι δραστηριότητες που λαμβάνουν χώρα σε αυτόν τον χώρο συχνά παραβιάζουν τους νόμους των περισσότερων χωρών. Παρέχοντας ένα περιβάλλον απαλλαγμένο από ταυτοποιήσεις και προσωποποιήσεις, το Darknet εξυμνεί την ανωνυμία και προωθεί εμμέσως την ανομία ενθαρρύνοντας παράνομες δραστηριότητες όπως το οργανωμένο έγκλημα, η παιδική πορνογραφία και η παραβίαση προσωπικών δεδομένων και απορρήτου. Οι αρχές επιβολής του νόμου χρησιμοποιούν προηγμένες τεχνολογίες και διεθνή συνεργασία για να παρακολουθούν και να εξαρθρώνουν παράνομες δραστηριότητες στο Darknet, αλλά η φύση του Darknet καθιστά δύσκολη την πλήρη εξάλειψη αυτών των δραστηριοτήτων.

Η κατάσταση αυτή εγείρει σοβαρές ανησυχίες σχετικά με την ασφάλεια και την ηθική ευθύνη της εποχής της πληροφορίας. Το γεγονός ότι οι εγκληματίες εκμεταλλεύονται τις δυνατότητες του Darknet για να διαπράττουν σοβαρά εγκλήματα χωρίς να εντοπίζονται, προκαλεί έντονη ανησυχία και επιβάλλει την ανάγκη για αποφασιστική δράση. Οι αρχές πρέπει να εντείνουν τις προσπάθειές τους, όχι μόνο μέσω τεχνολογικής απόψεως αλλά και μέσω της εκπαίδευσης και ευαισθητοποίησης του κοινού, για να προστατεύσουν την κοινωνία από τις απειλές που αναδύονται από αυτή τη σκοτεινή πλευρά του διαδικτύου.

Η μάχη κατά της ψηφιακής εγκληματικότητας είναι διαρκής και απαιτεί τη δέσμευση όλων των εμπλεκομένων για να διασφαλιστεί ένας ασφαλέστερος ψηφιακός κόσμος. Υψίστης σημασίας αποτελεί η επανεξέταση -που είθε προκύψει- του υπάρχοντος νομικού πλαισίου που περιορίζει τον Σκοτεινό Ιστό καθώς και η ανάπτυξη στρατηγικών που θα εξισορροπούν την προστασία της ιδιωτικότητας με την ανάγκη διατήρησης της δημόσιας ασφάλειας.

37 District of Columbia | Serbian Citizen Sentenced to 14 Years in Prison for Operating the Monopoly Narcotics Marketplace on the Dark Net | United States Department of Justice (Τελευταία Πρόσβαση στις 15/05/2024)

Συνοψίζοντας, η έρευνα τονίζει την έλλειψη περιοριστικών μέτρων από νομικής απόψεως και κρούει τον κώδωνα του κινδύνου περί ανάγκης σχετικής νομικής πλαισίωσης. Επιτακτική αποτελεί επίσης η ανάγκη για συνεχή και εντατική παρακολούθηση του Darknet σε συνδυασμό με την ενίσχυση των διεθνών συνεργασιών για την αποτελεσματική καταπολέμηση των εγκλημάτων που λαμβάνουν χώρα σε αυτόν τον επικίνδυνα ανώνυμο ψηφιακό χώρο.

Περίληψη

Στην συνολική ανάλυση του DarkWeb και του σχετικού νομικού πλαισίου, προέκυψε ότι ενώ το DarkNet δεν υπόκεινται ανεξάρτητα σε κάποιο νομοθετικό κανόνα, επηρεάζεται από πολλούς ευρείας συγγενικότητας νόμους που υπηρετούν βασικά και θεμελιώδη ζητήματα του φάσματος της εγκληματικότητας. Με στόχαστρο εξάλειψης να αποτελεί το οργανωμένο έγκλημα, η πορνογραφία ανηλίκων καθώς και οι κυβερνοεπιθέσεις, που διενεργούνται μέσω του σκοτεινού ιστού, πολλοί διεθνείς φορείς στηρίζονται στην ύπαρξη αυτών των θεμελιωδών νόμων προκειμένου να διασφαλιστεί η δημόσια ασφάλεια στο διαδίκτυο και η προστασία των πολιτών από τις απειλές του DarkNet. Καθημερινά, λαμβάνουν χώρο χιλιάδες ποινικώς δικάσιμα εγκλήματα που ως βάση έχουν τον σκοτεινό ιστό. Η ενίσχυση του νομικού πλαισίου που αφορά το DarkNet αποτελεί ουσιαστικό βήμα για την αντιμετώπιση των εγκληματικών δραστηριοτήτων σε αυτό το περιβάλλον. Με την αποτελεσματική εφαρμογή αυτών των νόμων, μπορεί να ενισχυθεί η διεθνής συνεργασία για την ασφαλέστερη χρήση του διαδικτύου και την προστασία των πολιτών.