ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΚΟΤΕΙΝΟ ΔΙΑΔΙΚΤΥΟ

ΚΑΙ Η ΣΧΕΣΗ ΤΟΥ ΜΕ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ.

Σύνταξη από: ΠΑΠΑΓΙΑΝΝΟΠΟΥΛΟΥ ΜΑΡΓΑΡΙΤΑ, Α.Μ.: 1621
και ΝΤΑΛΑΓΙΑΝΝΗ ΠΑΡΑΣΚΕΥΗ , Α.Μ.: 0800

Αντίρριο, Οκτώμβριος, 2016

Περιεχόμενα

Πίνακας Πινάκων

Πίνακας Εικόνων

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον καθηγητή μας και επιβλέποντα της πτυχιακής εργασίας κύριο Απόστολο Φούρναρη για την βοήθεια του και την καθοδήγηση του στην εκπόνηση αυτής της πτυχιακής εργασίας, τις οικογένειες μας για την πολύμορφη συμπαράστασή τους στη διάρκεια των ακαδημαϊκών μας σπουδών.

Επίσης και τις κυρίες Δουκέλη και Αυγουστίδου από την Δίωξη ηλεκτρονικού εγκλήματος καθώς επίσης και την κυριά Σταθάκη, τους κυρίους Παπαθανασίου, Γερμανός, Φιλιππίδης και πολλούς ακόμα καταξιωμένους επαγγελματίες στο χώρο της Δίωξης ηλεκτρονικού εγκλήματος. Καθώς και τον κύριο Μικρούλη πρώην μέλος της δίωξής ηλεκτρονικού εγκλήματος οπού μας έφερε σε επαφή με τα υπόλοιπα μέλη της δίωξης.

Abstract

Nowadays , it is a fact that computers and Internet have a great impact on our daily life , as they offer infinite possibilities. However every kind of risk is lurking for its users. The purpose of the following dessertation work is to inform all of us about electronic-online crime .In the first part of this study it will be theoritically analysed the concept and the various forms of cyber crime, but also its legal implications . Furthermore , it will be given advice to Internet users and preventive measures will be mentioned . Internet despite the possibilities that has to offer , as opposed to real world , is an unstable environment where criminal acts can be easily made. The second part refers to a study about dark net In this ever changing environment the concept of cyber crime acquires a new dimension . Moreover we managed to get in touch with reputable people specialised to cyber crime from whom we took a huge amount of information in order to understand it better

Εισαγωγή

Είναι γεγονός ότι στην σύγχρονη εποχή οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο έχουν εισχωρήσει για τα καλά στην καθημερινότητά μας καθώς οι δυνατότητες που προσφέρουν είναι άπειρες. Παρόλα αυτά ελλοχεύει κάθε είδους κίνδυνος για τους χρήστες

του. Σκοπός της επικείμενης πτυχιακής εργασίας είναι η παρουσίαση και η ενημέρωση της κατάστασης στο τομέα του ηλεκτρονικού - διαδικτυακού εγκλήματος.

Στο πρώτο μέρος της μελέτης αυτής θα αναλυθεί σε θεωρητικό πλαίσιο η έννοια του ηλεκτρονικού - διαδικτυακού εγκλήματος, των ποικίλων μορφών του αλλά και των νομικών - ποινικών του προεκτάσεων. Επίσης θα αναφερθούν προληπτικά μέτρα και συμβουλές για τους χρήστες του διαδικτύου. Το διαδίκτυο πάρα τις δυνατότητες που προσφέρει δεν είναι ένας χώρος, όπως ο πραγματικός κόσμος, αλλά ένα μη σταθερό περιβάλλον το οποίο μπορεί δύσκολα να ελεγχθεί και να οριοθετηθεί γεγονός που το καθιστά πόλο έλξης για διάφορες εγκληματικές ενέργειες.

Το δεύτερο μέρος αναφέρεται σε μια μελέτη περίπτωσης το σκοτεινό διαδίκτυο Darknet. Σε αυτό το συνεχώς μεταβαλλόμενο περιβάλλον η έννοια του ηλεκτρονικού - διαδικτυακού εγκλήματος αποκτά μια καινούργια διάσταση. Επίσης μέσα από συνομιλία με καταξιωμένους ανθρώπους πάνω στο ηλεκτρονικό έγκλημα αντλήσαμε διάφορες πληροφορίες έτσι ώστε να το κατανοήσουμε καλύτερα.

Δομή και στόχοι της διπλωματικής εργασίας

Η διπλωματική μας εργασία αποτελείται από δύο εννοιολογικά τμήματα. Το πρώτο αποτελεί το θεωρητικό πλαίσιο, το οποίο καταγράφει τις βασικές έννοιες που σχετίζονται με την εγκληματολογική επιστήμη και την έννοια του εγκλήματος. Ορίζεται το ηλεκτρονικό έγκλημα και τα είδη του και η νομοθεσία που το διέπει, καθώς και η σημασία τους. Συσχετίζονται δε με τα προαναφερόμενα η ασφάλεια και η ιδιωτικότητα στο διαδίκτυο και η δικανική των δικτύων.

Στο δεύτερο μέρος, όπου παρουσιάζεται μια μελέτη περίπτωσης, περιγράφεται το "Σκοτεινό διαδίκτυο", γνωστό και ως Darknet. Ορίσαμε το Darknet και περιγράψαμε την εξέλιξη του και καθορίσαμε τα χαρακτηριστικά του. Αναφέραμε τις μηχανές αναζήτησης που χρησιμοποιούνται και παρουσιάσαμε τους τρόπους χρήσης του Darknet και πιθανής προστασίας των απλών χρηστών από τη χρήση του. Επίσης καταγράψαμε βασικά παραδείγματα από τόσο από την παγκόσμια, όσο και από την ελληνική εμπειρία για το

Darknet. Στόχος δε της διπλωματικής μας αποτελεί η διερεύνηση των απόψεων των άμεσα εμπλεκόμενων υπηρετούντων στην ΕΛ.ΑΣ., ως προς τη χρήση του TOR στον εντοπισμό του ηλεκτρονικού εγκλήματος. Ως συνέπεια, εξετάστηκε ο ρόλος της ΕΛ.ΑΣ στον εντοπισμό του ηλεκτρονικού εγκλήματος και του Darknet., βάσει της συνομιλίας μας καταξιωμένους ανθρώπους στο χώρο της Δίωξής Ηλεκτρονικού Εγκλήματος . Τέλος, συνοψίζονται τα βασικά συμπεράσματα και τα ανοικτά προβλήματα που προκύπτουν από την παρούσα πτυχιακή εργασία.

ΜΕΡΟΣ Ι

ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ

1. Εισαγωγή

Το διαδίκτυο είναι το παγκοσμιοποιημένο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων που εξυπηρετεί εκατομμύρια χρηστών καθημερινά σε ολόκληρο τον κόσμο. Το διαδίκτυο αποτελεί παγκοσμίως το μεγαλύτερο σύστημα υπολογιστών, το οποίο λόγω της ανοικτής δομής και της απεριόριστης εξάπλωσής του συνδέει εκατοντάδες εκατομμύρια χρήστες σε όλο τον κόσμο. Ή εναλλακτικά, το διαδίκτυο μπορεί να παρομοιαστεί ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, το οποίο συνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων. Οι

διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα με τη χρήση διαφόρων πρωτοκόλλων, τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το διαδίκτυο αποτελεί μία από τις βάσεις της σημερινής κοινωνίας. Έχει αλλάξει τον τρόπο με τον οποίο ο κόσμος επικοινωνεί, δουλεύει, μαθαίνει και το σπουδαιότερο ζει. Το διαδίκτυο και κατ' επέκταση οι Η/Υ, έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητας μας, είτε ως μέσα ψυχαγωγίας-ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων (Ζάννη, 2005, σ. 3-12; Κριθαράς, 2009, σ. 10-12).

Αποτελεί την κύρια μηχανή με την οποία άτομα επικοινωνούν μεταξύ τους ταχύτερα πλέον από ποτέ. Οποιεσδήποτε διεργασίες μπορούν να πραγματοποιηθούν με το πάτημα ενός κουμπιού του πληκτρολογίου ή με ένα κλικ του ποντικιού. Στο διαδίκτυο ο χωρόχρονος χάνει την σημασία του. Η σωστή χρήση του διαδικτύου μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών του προσφέροντας τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης. Ταυτόχρονα, η "πληροφορία" στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε αριθμό και όγκο. Επίσης, στις μέρες μας, γίνεται σε μεγάλο βαθμό και χρήση εφαρμογών κοινωνικής δικτύωσης (facebook, twitter, chat rooms). Βασικό χαρακτηριστικό του διαδικτύου αποτελεί το γεγονός ότι δεν υπάρχει ένα συντονιστικό κέντρο, δίνοντας την εντύπωση ενός ενιαίου πλέγματος, και τούτο σημαίνει ότι σε περίπτωση που καταστραφεί κάποιο τμήμα του, οι πληροφορίες ακολουθούν άλλη δίοδο που παρακάμπτει το κατεστραμμένο τμήμα, ώστε να επιτυγχάνεται η συνεχής ροή δεδομένων εντός του συστήματος,. Οι συνδεδεμένοι με το διαδίκτυο Η/Υ συνεργάζονται για να μεταφέρουν πληροφορίες προς διάφορες κατευθύνσεις σε όλο τον κόσμο. Η αποστολή μιας τέτοιας ηλεκτρονικής πληροφορίας, αυτή, χωρίζεται από το TCP (Transmission Control Protocol) και το IP (Internet Protocol) σε μικρότερα κομμάτια που ονομάζονται πακέτα και το καθένα αποκτά τη δική του ταυτότητα και ακολουθεί διαφορετικό δρόμο, για να φτάσει στον προορισμό του. Όταν η πληροφορία φτάσει στον προορισμό της, τότε όλα τα διασπασμένα κομμάτια (πακέτα) της πληροφορίας ενώνονται ξανά και υπεύθυνο για την ασφαλή και ορθή επανένωση αυτή είναι το TCP και το IP. Την κυκλοφορία μέσω του διαδικτύου διευθύνει ένας ειδικός υπολογιστής που ονομάζεται router. Ένα πακέτο μπορεί να περάσει από πολλούς routers ως τον προορισμό του (Ζάννη, 2005, σ. 3-12; Κριθαράς, 2009, σ. 10-12).

Για να αποκτήσει κάποιος πρόσβαση στο διαδίκτυο, ώστε να γίνει δέκτης του πλήθους των υπηρεσιών που προσφέρει, πρέπει να επιλέξει έναν από του εξής τρόπους σύνδεσης (Ζάννη, 2005, σ. 3-12; Κριθαράς, 2009, σ. 10-12):

(i). *Διαρκής σύνδεση* με το διαδίκτυο υφίσταται όταν ο Η/Υ είναι μόνιμα και άμεσα συνδεδεμένος με ένα δίκτυο, το οποίο είναι ακολούθως συνδεδεμένο με το διαδίκτυο. Με αυτόν τρόπο ο χρήστης έχει στη διάθεσή του διαρκώς όλες τις υπηρεσίες που προσφέρει το διαδίκτυο,

(ii). *Προσωρινή άμεση σύνδεση* με το διαδίκτυο επιτυγχάνεται με τη χρήση ενός υπολογιστή, μιας συσκευής modem και μιας τηλεφωνικής γραμμής και μέσω κλήσεως ενός συνδέσμου εισόδου που οδηγεί ευθέως στο διαδίκτυο,

(iii). Ο πιο συνήθης τρόπος σύνδεσης είναι η *προσωρινή έμμεση σύνδεση*, που προϋποθέτει έναν υπολογιστή, μια συσκευή modem, μια τηλεφωνική γραμμή και την πληρωμή συνδρομής σε ένα φορέα παροχής πρόσβασης. Πρακτικά, ο χρήστης καλεί τον αριθμό του παρόχου και μόλις επιτευχθεί η σύνδεση του είναι επιτρεπτή η είσοδος στο διαδίκτυο, όπου μπορεί να κάνει χρήση των διαφόρων λειτουργιών και υπηρεσιών του (Ζάννη, 2005, σ. 3-12; Κριθαράς, 2009, σ. 10-12).

Από την άλλη μεριά, η *εγκληματολογική επιστήμη* σχετίζεται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των πιθανών αποδεικτικών στοιχείων, που συνδέουν μια αξιόποινη πράξη με πρόσωπα και γεγονότα εγκληματικών πράξεων. Η *ηλεκτρονική εγκληματολογία* αποτελεί τον επιστημονικό κλάδο που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο αποδεκτό νομικά. Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης συνδέονται με υπολογιστές. Στην περίπτωση αυτή γίνεται αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, να τις συγκεντρώσουμε και να τις ταξινομήσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές αντιμετωπίζουν το πρόβλημα ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που πιθανόν να οδήγησε στην καταστροφή αποδείξεων σχετικών με την αθωότητα του κατηγορουμένου (Ζάννη, 2005, σ. 3-12; Κριθαράς, 2009, σ. 10-12).

1.1.Η εγκληματολογική επιστήμη

Η εγκληματολογική επιστήμη αποτελεί την εφαρμογή ενός ευρέος φάσματος επιστημών που απαντούν σε ερωτήματα τα οποία αφορούν το νομικό σύστημα. Σχετίζεται τόσο με την πολιτική αγωγή όσο και με τα εγκλήματα. Η εν λόγω επιστήμη διαδραματίζει καίριο ρόλο στο δικαστικό σύστημα, αφού παρέχει τις επιστημονικά αποδεδειγμένες πληροφορίες στους ερευνητές, οι οποίοι αναλύουν τα αποδεικτικά στοιχεία που συνέλεξαν. Η διερεύνηση Η εγκληματολογική επιστήμη περιλαμβάνει τα παρακάτω βήματα: (i). *Συλλογή αποδεικτικών στοιχείων* από το χώρο του εγκλήματος, (ii). *Ανάλυση* των στοιχείων στο εργαστήριο, και (iii). *Παρουσίαση* των αποτελεσμάτων στο δικαστήριο. Βάσει του είδους του εγκλήματος που διερευνάται μπορεί να απαιτούνται η συλλογή, εξέταση και ανάλυση μεγάλου όγκου αποδεικτικών στοιχείων και εξειδικευμένοι επιστήμονες (π.χ., με γνώσεις βιολογίας, χημείας, φυσικής, πληροφορικής και άλλων επιστημών). Οι προαναφερόμενοι ερευνητές εργάζονται ξεχωριστά για την ανάλυση των αποδεικτικών στοιχείων μιας υπόθεσης. Στη συνέχεια συνδυάζονται όλα τα αποτελέσματα που προκύπτουν ώστε να συγκροτηθεί η υπόθεση (Bell, 2008, σ. 5-18).

1.1.1. Κλάδοι της εγκληματολογικής επιστήμης

Στην εγκληματολογική επιστήμη συνδυάζονται οι επιστήμες της ανθρωπολογίας, αρχαιολογίας, οδοντιατρικής, εντομολογίας και παθολογίας. Ανθρωπολογία είναι η εφαρμογή της κλασσικής ανθρωπολογίας στο νομικό περιβάλλον και χρησιμοποιείται συνηθέστερα στην ανεύρεση και αναγνώριση των ανθρώπινων σκελετών. Η δικανική ανθρωπολογία χρησιμοποιείται τις περισσότερες φορές σε ποινικές υποθέσεις όπου τα ανθρώπινα υπολείμματα του θύματος βρίσκονται σε προχωρημένο στάδιο αποσύνθεσης και μπορεί να βοηθήσει στην αναγνώριση αποθανόντων των οποίων τα υπολείμματα έχουν αποσυντεθεί, καεί, ακρωτηριαστεί ή γενικά δεν μπορεί να γίνει η αναγνωριστεί η ταυτότητα του θύματος. Εκτός των παραπάνω η ανθρωπολογία μελετά την ποικιλομορφία, ανάπτυξη, αύξηση και εξέλιξη του ανθρώπινου σκελετού. Οι ερευνητές του κλάδου, συνήθως εργάζονται σε

συνεργασία με παθολόγους, οδοντιάτρους και ερευνητές ανθρωποκτονιών, ώστε να ταχτοποιήσουν το θύμα με κάποιο προγονό του, να ανακαλύψουν αποδεικτικά στοιχεία σε ένα τραύμα και τέλος να καθορίσουν το χρονικό διάστημα από το θάνατο του θύματος (Bell, 2008, σ. 5-18).

Η δικανική αρχαιολογία συνδυάζει τις τεχνικές της αρχαιολογίας και της εγκληματολογικής επιστήμης. Ο εν λόγω τομέας εστιάζει στην ανάλυση των ανθρώπινων υπολειμμάτων, όπως επίσης και στην εύρεση της τοποθεσίας των ανθρώπινων υπολειμμάτων και στην εκσκαφή τους. Έχουν αναπτυχτεί λεπτομερείς και συστηματικές μεθόδους εντοπισμού, έρευνας, ανασκαφής και καταγραφής τόπων ενταφιασμού, ενώ ταυτόχρονα χρησιμοποιούνται οι πληροφορίες που αποκτήθηκαν για να ανακατασκευάσουν πιθανές δραστηριότητες στην τοποθεσία αυτή. Αυτές οι διαδικασίες προσαρμόζονται ώστε να οδηγήσουν στην ανάλυση και ανακατασκευή της σκηνής ενός εγκλήματος, ειδικότερα όταν η σκηνή του εγκλήματος δεν έχει ανακαλυφθεί για μεγάλο χρονικό διάστημα (Bell, 2008, σ. 5-18).

Οι δικανικοί αρχαιολόγοι συμβάλλουν τόσο στην εύρεση της τοποθεσίας και την ανασκαφή των ανθρωπίνων υπολειμμάτων, την ανάκτηση των ανθρώπινων υπολειμμάτων, εγκληματικών πράξεων, κλεμμένων αγαθών ή και όπλων, όπως επίσης και σε άλλα ενδεχόμενα αποδεικτικά στοιχεία ενός εγκλήματος ή δυστυχήματος. Παράλληλα έχουν αναπτυχτεί και τεχνικές που περιλαμβάνουν την διατήρηση των αντικειμένων, λαμβάνοντας υπόψη τις χημικές και βιολογικές διαδικασίες που διενεργούνται κατά την αποδόμηση των υλικών. Ο δικανικός αρχαιολόγος μελετά και προβλέπει την κατάσταση των υλικών που είναι θαμμένα στο έδαφος, ώστε να εξηγήσει το μοτίβο των αποδεικτικών στοιχείων που βρέθηκαν. Η μελέτη του τρόπου αποδόμησης ενός ανθρώπινου πτώματος, σχετίζεται με την κατάσταση των αποδεικτικών στοιχείων που προέκυψαν από τη διερεύνηση, και βρίσκουν χρησιμότητα στην επιβολή του νόμου ή άλλες αρχές. Η δικανική εντομολογία αφορά την διερεύνηση των εντόμων που βρίσκονται εντός, πάνω ή γύρω από τα ανθρώπινα απομεινάρια ώστε να καθοριστεί ο χρόνος ή η τοποθεσία θανάτου ή ακόμη και εάν μεταφέρθηκε το θύμα μετά από το θάνατο του (Bell, 2008, σ. 5-18).

Η δικανική ψυχολογία σχετίζεται με την μελέτη της ψυχολογίας του ατόμου, υπό το πρίσμα της εγκληματολογικής επιστήμης. Με αυτόν τον τρόπο διερευνώνται οι συνθήκες που οδηγούν σε εγκληματικές συμπεριφορές. Μια σημαντική πλευρά της δικανικής ψυχολογίας και ψυχιατρικής είναι η ικανότητα κατάθεσης στο δικαστήριο, αναδιατυπώνοντας τα ψυχολογικά ευρήματα στη νομική γλώσσα του δικαστηρίου, παρέχοντας πληροφορίες στους

νομικούς με σαφέστερο τρόπο. Επιπλέον, βοηθούν τους ψυχολόγους και ψυχιάτρους στην κατανόηση του ποινικού νόμου, ώστε να είναι ικανοί να επικοινωνήσουν σωστά με δικαστές και δικηγόρους. Με τη βοήθεια αυτών των επιστημών καταγράφονται και αποκωδικοποιούνται συμπεριφορικά αποδεικτικά στοιχεία, που συνήθως είναι αόριστα και επιδέχονται διαφορετικές ερμηνείες. Περιλαμβάνουν και τον καθορισμό της εγκληματικής ευθύνης και την εγκυρότητα του ισχυρισμού πιθανής φρενοβλάβειας ή όχι, αξιολογώντας την επικινδυνότητα του ατόμου για την κοινωνία και την πιθανότητα να παραβεί πάλι τον νόμο. Αξιολογούν τόσο τα θύματα όσο και τους παραβάτες, μελετώντας κάθε είδους επιθετική συμπεριφορά, και επαληθεύουν την κατάθεση ενός αυτόπτη μάρτυρα (Bell, 2008, σ. 5-18).

Στην εγκληματολογική επιστήμη ανήκουν και οι επιστήμες της βαλλιστικής, γενετικής, δακτυλοσκοπίας, ποδιατρικής και τοξικολογίας. Η βαλλιστική αποτελεί τη μελέτη των μηχανισμών που ασχολούνται με την πτήση, τη συμπεριφορά και την επίδραση των βλημάτων, όπως των σφαιρών, των βομβών βαρύτητας, των πυραύλων ή ομοειδών βλημάτων. Αποτελεί την επιστήμη ή την τέχνη του σχεδιασμού και επιτάχυνσης των βλημάτων έτσι ώστε να επιτευχθεί η επιθυμητή επίδοση. Μια υποκατηγορία της βαλλιστικής είναι η μελέτη των βαλλιστικών αποτυπωμάτων η οποία αναφέρεται σε ένα σύνολο δικανικών τεχνικών οι οποίες στηρίζονται σε σημάδια που αφήνουν τα όπλα σε σφαίρες, ώστε να αντιστοιχιστεί μια σφαίρα με ένα όπλο από το οποίο βλήθηκε, βασιζόμενη σε αναζητήσεις σε μεγάλες βάσεις δεδομένων. Οι βάσεις δεδομένων, που χρησιμοποιούνται για τα βαλλιστικά αποτυπώματα, συνήθως περιλαμβάνουν εικόνες και εγγραφές από όλα τα νέα όπλα που κυκλοφορούν στην αγορά οπλών (Bell, 2008, σ. 5-18).

Η αναγνώριση δακτυλικών αποτυπωμάτων -γνωστή και ως δακτυλοσκοπία-, είναι η διαδικασία της σύγκρισης δύο αποτυπωμάτων, από τα ανθρώπινα δάκτυλα ή από την παλάμη του χεριού, ώστε να καθοριστεί εάν αυτά τα αποτυπώματα προέρχονται από το ίδιο πρόσωπο. Τα αποδεικτικά στοιχεία που προκύπτουν δύναται να συλλέγουν, να διατηρηθούν και να διανεμηθούν με διαφορετικούς τρόπους, ανάλογα με τις επικρατούσες συνθήκες. Αντικείμενα από την σκηνή ενός εγκλήματος χρησιμοποιούνται για να ληφθούν αποτυπώματα από αυτά. Τα αντικείμενα στο οποίο βρέθηκαν τα αποτυπώματα στέλνονται σε αναλυτές αποτυπωμάτων. Επίσης, αποτυπώματα που αποτεθήκαν πάνω σε αφαιρούμενες επιφάνειες αποκόπτονται και στέλνονται για ανάλυση. Όπως συμβαίνει με όλα τα αποδεικτικά στοιχεία και σε κάθε περίπτωση είναι απαραίτητη η πλήρης και αναλυτική καταγραφή τους, με φωτογράφισή τους, ειδικότερα σε περιπτώσεις που αυτά είναι δύσκολο να αναπαραχθούν ή να μεταφερθούν από το σημείο στο οποίο βρέθηκαν. Αντίστοιχα, η ποδιατρική αποτελεί την

μελέτη των αποτυπωμάτων ενός πέλματος ή ενός υποδήματος και των ιχνών που άφησαν στην τοποθεσία του εγκλήματος ώστε να αποδειχθεί κατά τη διερεύνηση η ταυτότητα ενός προσώπου. Τα αποδεικτικά στοιχεία από τα αποτυπώματα ενός παπουτσιού καταγράφονται με αφθονία στην σκηνή ενός εγκλήματος και στις περισσότερες περιπτώσεις μπορούν να αποδειχθούν ίσης αξίας με τα δακτυλικά αποτυπώματα. Αρχικά οι ερευνητές προσπαθούν να αναγνωρίσουν τον κατασκευαστή και το μοντέλο του υποδήματος από το οποίο προήλθε το αποτύπωμα. Αυτό συνήθως γίνεται συγκρίνοντάς τα με μια βάση δεδομένων. Η επιτυχία αυτών των μεθόδων εξαρτάται από την αναγνώριση του μοτίβου, τα σημάδια της μάρκας και του λογότυπου. Μπορούν να εξαχθούν πληροφορίες σχετικά με τον ιδιοκτήτη του υποδήματος οι οποίες εξαρτώνται από την γωνία της πατημασιάς και την κατανομή του βάρους. Η λεπτομερής ανάλυση των αποτυπωμάτων ενός υποδήματος, συνήθως χρησιμοποιούνται για την ταυτοποίηση ενός συγκεκριμένου υποδήματος με το αποτύπωμά του. Η δικανική οδοντιατρική ασχολείται με την εξέταση και την επαλήθευση των οδοντιατρικών αποδεικτικών στοιχείων, τα οποία εν συνέχεια παρουσιάζονται στη δικαιοσύνη. Τα αποδεικτικά στοιχεία τα οποία εξάγονται από τη μελέτη της ανθρώπινης οδοντοστοιχίας είναι η ηλικία και ταυτοποίηση του ατόμου στον οποίο ανήκει η οδοντοστοιχία. Τα αποτελέσματα προκύπτουν χρησιμοποιώντας οδοντιατρικές τεχνικές οι οποίες περιλαμβάνουν, ακτινογραφίες, προ- και επί-θανάτιες φωτογραφίες καθώς και εξέταση γενετικού υλικού. Επιπρόσθετα αποδεικτικά στοιχεία που μελετά ο εν λόγω κλάδος αποτελούν σημάδια από δαγκωματιές (στο θύμα, στον αυτουργό ή σε αντικείμενα το οποίο σχετίζονται με τη τοποθεσία του εγκλήματος). Οι περιοχές εφαρμογών είναι η ταυτοποίηση θυμάτων από τα ανθρώπινα υπολείμματά τους, ταυτοποίηση προσώπων σε μαζικούς θανάτους, αξιολόγηση των τραυματισμών από δαγκωματιές και αξιολόγηση σε περιπτώσεις κακομεταχείρισης πολιτικών υποθέσεων (Bell, 2008, σ. 5-18).

Η γενετική σχετίζεται με τις τεχνικές που χρησιμοποιούνται για την αναγνώριση υπόπτων από τα αντίστοιχα DNA-προφίλ. Τα DNA-προφίλ αποτελούν κρυπτογραφημένα αριθμητικά σύνολα που αντικατοπτρίζουν το DNA ενός ατόμου, και μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του ατόμου. Η δικανική παθολογία αποτελεί το πεδίο της επιστήμης που καθορίζει την αιτία θανάτου ή τραυματισμού, εφαρμόζοντας της αρχές της φαρμακευτικής και της ιατρικής. Οι δικανικοί παθολόγοι διερευνούν τις σκηνές ενός εγκλήματος για τραυματισμούς ή ασθένειες που τις συνδέει άμεσα ή αποτελούν την αφετηρία για μια σειρά από γεγονότα που οδήγησαν στο θάνατο ενός ατόμου. Ακόμη είναι δυνατόν να καθορίζουν την κύρια αιτία θανάτου, η οποία στις περισσότερες περιπτώσεις είναι ανθρωποκτονία

(τυχαία, φυσική, αυτοκτονία ή απροσδιόριστη). Επίσης, πραγματοποιείται και συλλογή αποδεικτικών στοιχείων ή καθορίζεται η ταυτότητα του αποθανόντος. Εξετάζονται και καταγράφονται, επίσης, οι τραυματισμοί, πραγματοποιείται τοξικολογική ανάλυση στους ιστούς και τα υγρά του πτώματος, για να προσδιοριστούν περιπτώσεις σκόπιμης δηλητηρίασης (Bell, 2008, σ. 5-18).

Η τοξικολογία αποτελεί την μελέτη της ανίχνευσης και αναγνώρισης για παράνομες ναρκωτικές ουσίες, χημικούς καταλύτες οι οποίοι χρησιμοποιούνται σε περιπτώσεις εμπρησμών, εκρηκτικών μηχανισμών και πυροβολισμών. Ο ερευνητής αποσκοπεί στην σωστή εξαγωγή και ερμηνεία των αποτελεσμάτων. Ένας τοξικολόγος συνήθως λαμβάνει υπόψη του το περιεχόμενο μιας διερεύνησης, και συγκεκριμένα κάθε φυσικό σύμπτωμα το οποίο έχει καταγραφεί, ώστε να περιορίσει την αναζήτηση (π.χ., μπουκάλια με χάπια, σκόνες, επαλείμματα ιχνών, καθώς και άλλες διαθέσιμες χημικές ουσίες). Βάσει των πληροφοριών και των δειγμάτων αυτών οι τοξικολόγοι καθορίζουν την παρουσία τοξικών ουσιών, τις συγκεντρώσεις τους, καθώς και τις πιθανές επιπτώσεις στον ανθρώπινο οργανισμό (Bell, 2008, σ. 5-18).

Στην συγκεκριμένη πτυχιακή εργασία παίζει ρόλο Ψηφιακή Δικανική ή αλλιώς Δικανική των Υπολογιστών.

Ο όρος Δικανική Υπολογιστών (Computer Forensics ή αλλιώς Digital Forensics) αναφέρεται σε ένα κλάδο της Δικανικής Επιστήμης (Science Forensic, της επιστήμης δηλαδή που ασχολείται με την συλλογή αποδεικτικών στοιχείων σε εγκληματικές και παραβατικές ενέργειες) ο οποίος αποτελεί τη μεθοδολογία η οποία ακολουθείται για την συλλογή ψηφιακών αποδεικτικών στοιχείων από Ηλεκτρονικούς Υπολογιστές και γενικότερα ψηφιακές αποθηκευτικές συσκευές. Ως Διαδικασία της Δικανικής Υπολογιστών (Computer Forensic Process) θα μπορούσε να χαρακτηριστεί η διαδικασία που ακολουθείται, έτσι ώστε από το υπολογιστικό σύστημα που μας ενδιαφέρει να μπορέσουμε να εξάγουμε κάποια αποδεικτικά στοιχεία. Η μεθοδολογία και ο σκοπός της Δικανικής Υπολογιστών δεν είναι ίδιος με την απλή ανάκτηση χαμένων δεδομένων (data recovery), αλλά να εξαχθούν όσο το δυνατόν περισσότερες πληροφορίες που να αφορούν αυτά τα δεδομένα. Στην περίπτωση παραβίασης ενός υπολογιστικού συστήματος από κάποιο επιτιθέμενο, σκοπός είναι να προσδιοριστεί ο τρόπος με τον οποίο κατάφερε να αποκτήσει πρόσβαση στο σύστημα, ποίες ήταν οι ενέργειες του πάνω σε αυτό και ποιος ήταν ο στόχος-αιτία της επίθεσης. Εν συντομία οι τέσσερεις φάσεις που αποτελούν αυτή τη διαδικασία είναι, η φάση της συλλογής

(Collection), της εξέτασης (Examination), της ανάλυσης (Analysis) και της αναφοράς των αποτελεσμάτων (Reporting).

Η Δικανική Δικτύων (Network Forensics), αποτελεί μια νέα προσέγγιση για την έρευνα περιστατικών ασφαλείας σε ένα δίκτυο και την άμεση αντίδραση, οδηγώντας σε μεγαλύτερη ασφάλεια του δικτύου . Είναι μια επέκταση στο μοντέλο της δικτυακής ασφάλειας, όπου η έμφαση παραδοσιακά δίνεται στην πρόληψη και σε μικρότερο βαθμό στην ανίχνευση. Η εστίαση γίνεται στη σύλληψη, την καταγραφή και την ανάλυση δικτυακών πακέτων και συμβάντων, για διερευνητικούς σκοπούς. Η Δικανική Δικτύων έρχεται να συμπληρώσει τα κενά που λείπουν και να δώσει τα επιπλέον στοιχεία που απαιτούνται για μια πλήρη διερεύνηση των συνθηκών, κάτω από τις οποίες πραγματοποιήθηκε μια επίθεση. Ο όρος Δικανική Δικτύων (Network Forensics) χρησιμοποιείται για να περιγράψει την διαδικασία της ανάλυσης πληροφοριών, οι οποίες έχουν συλλεχθεί σε ένα ενεργό δίκτυο, από διάφορα εργαλεία επιθεώρησης, παρακολούθησης και ανίχνευσης εισβολών, με σκοπό την προστασία.

2. Η έννοια του εγκλήματος

Το έγκλημα χαρακτηρίζεται με φύση σύνθετη, αφού σε αυτήν συναντώνται και την καθορίζουν από την μια μεριά η κοινωνική-βιολογική-ψυχολογική πραγματικότητα του ανθρώπου και από την άλλη η δεοντολογία που διέπει -στο πλαίσιο της κοινωνίας- την συμπεριφορά του. Το έγκλημα αποτελεί αδιαίρετα οντολογικό και αξιολογικό φαινόμενο. Η σύνθετη φύση του εγκλήματος μπορεί να αποδοθεί από τον χαρακτηρισμό του ως ένα

ορισμένου, αρνητικά αξιολογούμενου, φαινομένου της πραγματικότητας (Μαγκάκης, 1984, σ. 3). Αποτελεί δε ένα αναπόσπαστο κομμάτι κάθε κοινωνίας και καταγράφεται ως το φαινόμενο που κατά τη διάρκεια του συνεχώς μεταβάλλονται οι εκφάνσεις, τα μέσα τέλεσης καθώς και το νομικό πλαίσιο που το διέπει. Ανάλογα με τις κοινωνικοπολιτικές συνθήκες και τις ηθικές τάσεις -κάθε εποχής και τόπου- το έγκλημα παραμένει παρόν, κινούμενο πάντα σε τρείς βασικούς άξονες Ως έγκλημα μπορεί να νοηθεί κάθε ενέργεια που παρεκκλίνει από αποδεκτούς κοινωνικούς κανόνες. Δεν υπάρχει κοινωνία η οποία δεν αντιμετωπίζει το πρόβλημα της εγκληματικότητας (Μαγκάκης, 1984, σ. 4).

Οι κλάδοι που ασχολούνται με το έγκλημα είναι η νομική επιστήμη και η επιστήμη της εγκληματολογίας Η νομική, στηρίζεται στον προσδιορισμό του εγκλήματος που σχετίζεται με τον εκάστοτε ισχύον ποινικό νόμο, ενώ η εγκληματολογία εξετάζει το έγκλημα ως κοινωνικό φαινόμενο και προσπαθεί να το ερμηνεύσει σαν τέτοιο. Η νομική έννοια του εγκλήματος όπως αυτή προσδιορίζεται στο άρθρο 14 του ποινικού μας κώδικα. Τον δογματικό ορισμό του εγκλήματος αποτυπώνει ο ίδιος ο ποινικός κώδικας: "*έγκλημα είναι πράξη άδικος και καταλογιστή εις τον πράξαντα, τιμωρούμενη υπό του νόμου*". Το σημαντικότερο περιεχόμενό του αποδίδεται από το γεγονός ότι αποτελεί μια πράξη που θίγει τις αξίες της κοινωνική ζωής και που η τέλεση του αποτυπώνει την έλλειψη σεβασμού του δράστη προς τις αξίες αυτές, έτσι ώστε η ποινική καταστολή της να κρίνεται αναγκαία (Μαγκάκης, 1984, σ. 5-6).

Από τους διάφορους εγκληματολογικούς ορισμούς του εγκλήματος -που στηρίζονται σε διαφορετικά κάθε φορά κριτήρια-, αναφέρουμε ως περισσότερο περιεκτικό εκείνον που δίνεται από τον Αλεξιάδη, (1996, σ. 50) σύμφωνα με τον οποίο: "*Πραγματικό έγκλημα είναι κάθε εκδήλωση ανθρώπινης δράσης η οποία είναι επικίνδυνα αντικοινωνική*". Ο συνολικός αριθμός των εγκλημάτων που διαπράττονται σε ορισμένη τοπικά και χρονικά κοινωνική ομάδα συνιστά την εγκληματικότητα (Αλεξιάδης, 1996, σ. 99) που καταγράφεται σε μια κοινωνία. Το έγκλημα, διαχρονικά, αποτελεί ιστορικό και κοινωνικό φαινόμενο, καθώς συνοδεύει την εξέλιξη των ανθρώπινων κοινωνιών. Καμιά κοινωνία δεν έχει απαλλαχθεί από αυτό, αν και παρατηρείται μια τάση αύξησης της συχνότητας και ταυτόχρονα την εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς (Αλεξιάδης, 1996, σ. 100).

Τα βασικά στοιχεία ενός εγκλήματος αποτελούν: Ο κανόνας, το έγκλημα και η κύρωση-ποινή, που συναποτελούν έναν αδιάσπαστο κύκλο. Η μη ύπαρξη ενός κανόνα δεν καθιστά δυνατή την παράβασή του, αφού δημιουργήθηκε για να οργανώσει και να προστατέψει τα κοινωνικά αγαθά από κάθε προσβολή τους εντός των πλαισίων της κοινωνικής συμβίωσης. Ταυτόχρονα, αν δεν υπήρχε το έγκλημα δεν θα υφίστατο η κύρωση. Η κύρωση αποτελεί

συνέπεια της παράβασης του κανόνα και υποδηλώνει προς τον εγκληματία που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Η ποινή δηλώνει την εκτόνωση της κοινωνικής αντίδρασης ως προς το έγκλημα και ιδεολογία παρουσιάζεται ως αποκατάσταση της διαταραχθείσας από το έγκλημα κοινωνικής τάξης ή ως το μέσο για την ηθική βελτίωση του παραβάτη (Αλεξιάδης, 1996, σ. 101-102).

3. Ηλεκτρονικό έγκλημα

Έχοντας προσδιορίζει κάπως, την έννοια του εγκλήματος, μπορούμε να ισχυριστούμε ότι ηλεκτρονικό έγκλημα, είναι κάθε άδικη πράξη και καταλογιστή, επικίνδυνα αντικοινωνική, που τελείται μέσω ηλεκτρονικού Η/Υ. Ο Τσουραμάνης (2005, σ. 34) καταγραφεί τον ορισμό "*Ψηφιακό έγκλημα είναι κάθε παράνομη πράξη για τη διάπραξη αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας*". Ο όρος ηλεκτρονικό έγκλημα ή ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής

επεξεργασίας δεδομένων. Η ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη, η άνευ άδειας απόκτηση ή παραποίηση δεδομένων και η δολιοφθορά, δηλαδή εγκλήματα όπου ο Η/Υ αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Η εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα τα αδικήματα για την τέλεση των οποίων ο Η/Υ χρησιμοποιείται ως βοηθητικό μέσο (Τσουραμάνης, 2005, σ. 35-36).

Στη σημερινή παγκοσμιοποιημένη εποχή της πληροφορίας και της τεχνολογικής εξέλιξης καταγράφεται η ολοένα αυξανόμενη τάση για την διείσδυση των ευρυζωνικών τεχνολογιών στην κοινωνία. Διαφαίνεται δε και η τάση για σύγκλιση των τηλεπικοινωνιακών δικτύων παροχής υπηρεσιών για πρόσβαση παντού, για πάντα και με οποιοδήποτε τρόπο. Στο συνεχώς μεταβαλλόμενο περιβάλλον αυτό, η έννοια της ασφάλειας των Η/Υ και δικτύων αποκτά νέες διαστάσεις. Οι έννοιες ηλεκτρονικό έγκλημα ή κυβερνό-έγκλημα, όπως επίσης και οι τεχνολογίες που χρησιμοποιούνται για τη διάπραξη, ανίχνευση και αντιμετώπιση κακόβουλων επιθέσεων σε συστήματα και εφαρμογές, αποτελούν αναπόσπαστο κομμάτι της ασφάλειας των πληροφοριακών συστημάτων. Ηλεκτρονικές απειλές, όπως ένα κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και συστήματα, ενοχλητικά ηλεκτρονικά μηνύματα και επιθέσεις κλοπής ηλεκτρονικής ταυτότητας αναμένεται πως θα βρουν νέα, εξίσου γόνιμα, εδάφη για την εξάπλωσή τους. Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπρόσθετα το έργο τους (Τσουραμάνης, 2005, σ. 37-40).

3.1. Ανασκόπηση

Η βιομηχανική επανάσταση έθεσε τις βάσεις για την διεθνοποιημένη κοινωνία, και τον μετασχηματισμό της όπως και της ανθρωπότητας σε σχηματισμούς με εθνικά κράτη που ανταλλάσσουν μεταξύ τους μαζικής παραγωγής τυποποιημένα εμπορεύματα. Μετά το δεύτερο παγκόσμιο πόλεμο και σε ιδιαίτερα σύντομο χρονικό διάστημα ξεκίνησε η πληροφορική επανάσταση. Η ταχύτατη ανάπτυξη και διάδοση και εφαρμογή της πληροφορικής προσφέρει σημαντικά πλεονεκτήματα σε πολλούς τομείς της κοινωνικής ζωής,

ώστε σήμερα γίνεται λόγος για αυξανόμενη εξάρτηση του κράτους, της οικονομίας, της παιδείας και του πολιτισμού από την πληροφορική (Λάζος, 2001, σ. 22).

Η σύγχρονη κοινωνία τείνει προς στο σημείο, όπου τα πάντα θα εξαρτώνται από το λογισμικό. Ο κύριος όγκος των πληροφοριών κάθε είδους που διακινούνται καθημερινά στον πλανήτη, μεταβιβάζεται μέσω συστημάτων πληροφορικής. Αλλά και αντίστροφα, κάθε πληροφορία, άξια λόγου, τείνει να θεωρείται η πληροφορία που μπορεί να μεταβιβασθεί μέσω των συστημάτων αυτών. Όλο και πιο συχνά, ο έλεγχος και η ρύθμιση της παραγωγικής διαδικασίας γίνεται διαμέσω επεξεργασίας δεδομένων. Η πληροφορική επανάσταση με όλα της τα υλικά (hardware) και άυλα (software) συστατικά, αποτελεί μια κοινωνική σχέση και ένα εργαλείο που έχουν στόχο να παραμείνουν στην κοινωνία. Οι τεχνολογικές εξελίξεις-καινοτομίες δημιουργούν προβλήματα μέχρι να ενσωματωθούν στα επικρατούντα πρότυπα των κοινωνικών σχέσεων και εξουσίας και μέχρι να μορφοποιηθούν με τρόπους που θα ελαχιστοποιηθούν ή θα αμβλύνουν τις προοπτικές διάσπασης αυτών των προτύπων (Λάζος, 2001, σ. 24-25).

Το διαδικτυακό έγκλημα ξεκίνα από τα μέσα της δεκαετίας του 1980, και εξασφαλίζει από κάθε άποψη την αυτόνομη ύπαρξή του. Αποτελείται από δράστες και δράσεις, πλαισιώνεται από ένα ιδιαίτερο δίκαιο και προσεγγίζεται από προσαρμοσμένες -στις ιδιαιτερότητές του- κοινωνικές επιστήμες όπως είναι η πληροφορική εγκληματολογία. Στο διαδικτυακό έγκλημα ο Η/Υ έχει διάφορους ρόλους. Μπορεί να αποτελέσει το υλικό σώμα, hardware το αντικείμενο δηλαδή της επίθεσης, να καεί, να πυροβοληθεί, να κλαπεί, είτε ο ίδιος είτε οι περιφερειακές του συσκευές. Με αυτό τον τρόπο, είναι δυνατό να καταστραφούν τα πολύτιμα προγράμματα και δεδομένα που έχει. Μπορεί επίσης να χρησιμοποιηθεί ως εργαλείο, για τη διάπραξη αδικημάτων (Λάζος, 2001, σ. 26-30).

3.2. Η έννοια του ηλεκτρονικού-διαδικτυακού εγκλήματος.

Το διαδίκτυο και οι ηλεκτρονικοί υπολογιστές παρέχουν στους χρήστες αφενός μεν ασύλληπτες δυνατότητες και αφετέρου εισαγάγουν νέες μορφές παραβατικής συμπεριφοράς. Έτσι δημιουργούνται αξιόποινες πράξεις που υφίστανται λόγω τη χρήσης ηλεκτρονικοί υπολογιστές και του διαδικτύου. Έτσι, εγκληματικές πράξεις όπως η εξύβριση ή η δυσφήμιση -μέσω μιας ιστοσελίδας ή ηλεκτρονικού ταχυδρομείου- διαπράττονται πλέον ταχύτερα, με το διαδίκτυο να αποτελεί το βασικό πεδίο τέλεσης τους. Η δυσκολία των διωκτικών αρχών στην

διαλεύκανση της ηλεκτρονικής εγκληματικότητας και η ανωνυμία των δραστών, έχουν ως αποτέλεσμα την ελαχιστοποίηση της τιμωρίας του δράστη. Τα στα στοιχεία αυτά ωθούν τους στην τέλεση αξιόποινων πράξεων μέσω διαδικτύου. Έτσι στις μέρες μας, παρά την εξέλιξη των διωκτικών μηχανισμών, η διαλεύκανση της ηλεκτρονικής εγκληματικότητας παραμένει μια δύσκολη υπόθεση (Βλαχόπουλος, 2007, σ. 12-14).

Είναι επιπρόσθετα είναι αναγκαίο να γίνει διάκριση μεταξύ του λεγόμενου ηλεκτρονικού εγκλήματος και του διαδικτυακού το οποίο παρουσιάζει ποιοτικά σημαντικές διαφορές -από το προαναφερόμενο- λόγω των ιδιαίτερων χαρακτηριστικών του διαδικτύου. Τα χαρακτηριστικά αυτά συνοψίζονται στη δυνατότητα ανταλλαγής δεδομένων και προγραμμάτων μεταξύ όλων των συνδεδεμένων υπολογιστών. Η αδυναμία διατύπωσης ενός ενιαίου ορισμού που να περιλαμβάνει όλες τις εκφάνσεις του διαδικτυακού εγκλήματος οφείλεται στο γεγονός ότι οι παραβάσεις στο διαδικτύου παρουσιάζουν ποικιλομορφία ως προς τις μορφές εκδήλωσης τους. Οι Forester & Morrison (1994) (από Βλαχόπουλος, 2007, σ. 15), αναφέρουν ότι το ηλεκτρονικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά ή εγκληματική πράξη που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων στην οποία ο Η/Υ χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της.

Απαραίτητα στοιχεία για την τέλεση του ηλεκτρονικού εγκλήματος, θεωρούνται η ύπαρξη Η/Υ ή και κινητού τηλέφωνου. Ο Shinder (2002) (από Βλαχόπουλος, 2007, σ. 16), αναφέρει ότι ο ρόλος που διαδραματίζει ο Η/Υ -στα πλαίσια του ηλεκτρονικού εγκλήματος- είναι κυρίαρχος αφού αποτελεί:

- ✓ Στόχο επιθέσεων, δηλαδή ο Η/Υ αποτελεί και το θύμα της επίθεσης,
- ✓ Μέσο για τη διάπραξη κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιείται από το δράστη για την πραγματοποίηση του εγκληματικού εγκλήματος,
- ✓ Βοηθητικό μέσο για τη διάπραξη του εγκλήματος.

Το ηλεκτρονικό έγκλημα εισάγει νέους περιορισμούς, αφού:

(i). Πολλές φορές είναι πολύ δύσκολο να προσδιοριστεί <u>ο τόπος τέλεσης του εγκλήματος</u> και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου Η/Υ ο εγκληματίας μπορεί να το διαπράξει από οποιοδήποτε και,

(ii) <u>Ο ακριβής χρόνος τέλεσης του εγκλήματος</u> και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημιά που προκλήθηκαν πολύ αργότερα από το χρόνο που πραγματοποιηθήκαν,

(iii). Τα εγκλήματα στον κυβερνοχώρο που καταγγέλλονται είναι σχετικά λίγα και αυτό γιατί το θύμα ακόμα και όταν αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, δεν καταφεύγει στις αρμόδιες διωκτικές αρχές.

Μια συσκευή ηλεκτρονικής επεξεργασίας δεδομένων μπορεί να χρησιμοποιηθεί για τη διάπραξη κλοπής, καταπάτησης ή παραβίασης δικαιωμάτων. Ο Η/Υ σχετίζεται ειδικά με την πληροφορική τεχνολογία, και έχει ρόλο που αφορά στις πληροφορικές ιδιότητες των δεδομένων και των προγραμμάτων, που φιλοξενούνται στο σώμα του Η/Υ. Η ειδοποιός διαφορά μεταξύ των πληροφοριών σε μη-ηλεκτρονική μορφή και των πληροφοριών σε ηλεκτρονική μορφή είναι ότι οι πληροφορίες σε ηλεκτρονική μορφή μπορούν να αντιγραφούν, τροποποιηθούν, υπονομευθούν ή διαγραφούν χωρίς οι αναγκαίες ενέργειες να αφήνουν πίσω τους κάποιο φυσικό ίχνος. Δημιουργούν επίσης, ένα μοναδικό περιβάλλον στο οποίο μπορούν να λάβουν χώρα μη-εξουσιοδοτημένες δραστηριότητες, ενώ συγχρόνως ο Η/Υ δημιουργεί μοναδικές μορφές περιουσιακών στοιχείων που μπορούν να υποστούν προσβολές. Ο Η/Υ μπορεί να μην έχει άμεση συμμετοχή σε ανάλογα συμβάντα. Τα ηλεκτρονικά αποθηκευμένα δεδομένα αποτελούν μια εντελώς νέα μορφή -υποκείμενη σε νέες μορφές προσβολής-, που έχει οδηγήσει σε νέα είδη προσβλητικών δραστηριοτήτων. Τα ονόματα των δραστηριοτήτων είναι τα ίδια: απάτη, κλοπή, κατάχρηση, βανδαλισμός, δόλια βλάβη, εκβιασμός, σαμποτάζ και κατασκοπεία (Συκιώτου, 2009, σ. 45-47).

Ο Η/Υ χρησιμοποιείται ως ένα νέο μέσο τέλεσης εγκλημάτων, όπου η χρήση του τεχνικού μέσου επέβαλε απλώς τη συμπλήρωση ή την τροποποίηση των αντίστοιχων διατάξεων, έτσι ώστε να καλύπτει την καινούργια μεθοδολογία τέλεσης: Σε ένα ανταλλακτήριο συναλλάγματος που λειτουργούσε με τον παραδοσιακό τρόπο οι δυνατότητες παράνομης δραστηριότητας του υπαλλήλου συνίστατο στο να ξεγελάσει τον πελάτη σχετικά με το ποσό που αντιστοιχεί, να του δώσει άχρηστα νομίσματα, να τον κλέψει στα ρέστα κλπ. Απαιτούσε δηλαδή μια άμεση προσωπική επαφή δράστη και θύματος και μια κατά τον ένα ή άλλο τρόπο προσβολή του δεύτερου (Συκιώτου, 2009, σ. 46-48).

Το τοπίο του ψηφιακού εγκλήματος μετέβαλε ριζικά η εμφάνιση του διαδικτύου στο οποίο συνδέθηκαν εκατομμύρια άνθρωποι σε όλον τον κόσμο, ανταλλάσσοντας καθημερινά έναν τεράστιο όγκο δεδομένων κειμένου, εικόνας, ήχου, αλλά και προγραμμάτων υπολογιστών χρησιμοποιώντας το ως ένα παγκόσμιο forum ανταλλαγής ιδεών, ειδήσεων, πληροφοριών, ως χώρο διασκέδασης, ως πεδίο εμπορικών και οικονομικών συναλλαγών και αναπόφευκτα, ως χώρο και εγκληματικής δραστηριότητας. Μπορεί δε να περιγραφεί ως ένα παγκόσμιας εμβελείας ψηφιακό πλέγμα, που συνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα

παρέχοντας διάφορες υπηρεσίες και εργαλεία. Η σωστή χρήση του διαδικτύου βοηθά στο να ανέβει το μορφωτικό επίπεδο των χρηστών του προσφέροντας τους επικαιροποιημένα στοιχεία σε όλους τους τομείς της σύγχρονης γνώσης Το διαδίκτυο αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας μας, είτε ως μέσο ψυχαγωγίας και ενημέρωσης, είτε ως εργαλείο πληροφόρησης και διεκπεραίωσης επαγγελματικών και προσωπικών υποχρεώσεων και δραστηριοτήτων. Η πληροφορία στην εποχή του διαδικτύου έχει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται και επεξεργάζονται είναι ανυπολόγιστες τόσο σε όγκο, όσο και σε αριθμό, ενώ σήμερα -σε μεγάλο βαθμό- γίνεται και χρήση εφαρμογών κοινωνικής δικτύωσης, όπως facebook, twitter και chat rooms (Νικολαΐδης, 1999, σ. 22-24).

Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820, όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard, που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. Έτσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα. Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών , οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται.

3.3. Μορφές κυβερνό-εγκλήματος

Λόγω της συνεχούς δικτύωσης των ηλεκτρονικών υπολογιστών τα νομικά ζητήματα -που τα αφορούν- έγιναν πολυπλοκότερα και η ανάγκη της νομικής αντιμετώπισης των συνεχώς νεοεμφανιζόμενων εγκληματικών συμπεριφορών πιο επιτακτική. Ο εντοπισμός των χαρακτηριστικών της νέας γενιάς εγκληματικότητας συνδέεται με την ανάγκη για θέσπιση νέων κανόνων ποινικού δικαίου, αναδεικνύοντας ταυτόχρονα την επικινδυνότητα του νέου αυτού ποινικού φαινομένου. Συνοψίζουμε ορισμένα από τα βασικά χαρακτηριστικά του (Νικολαΐδης, 1999, σ. 24-28, Furnell, 2006, σ. 56-58):

- Το διαδικτυακό έγκλημα διαπράττεται σε ελάχιστο χρόνο. Η αμεσότητα αυτή έχει αποτέλεσμα τέτοια ταχύτητα τέλεσης που πολλές φορές δεν γίνεται αντιληπτό ούτε το ίδιο το θύμα. Ο δράστης, κάνοντας χρήση του Η/Υ που είναι συνδεδεμένος στο διαδίκτυο, επιτίθεται και μπορεί να εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού παγκοσμιοποιημένα.
- Το ηλεκτρονικό έγκλημα πλήττει κυρίως τις πληροφορίες που περιέχονται στα ηλεκτρονικά δεδομένα. Αλλοιώσεις, φθορές και βλάβες προκαλούνται σε ενσώματα αντικείμενα στο Η/Υ, όπως σκληροί δίσκοι και μνήμη είναι απλά δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά τα δεδομένα,
- Η εισβολή σε ένα υπολογιστικό σύστημα διευκολύνεται από το διαδίκτυο και αυτό γιατί διατίθεται ελεύθερα σε αυτό εφαρμογές λογισμικού,
- Για τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτούνται διακρατικές συνεργασίες. Ο χαρακτήρας αυτός του ηλεκτρονικού εγκλήματος οδηγεί συχνά σε διαφορετική αξιολόγηση του περιεχομένου του (αφού αυτό που μπορεί να είναι νόμιμο ένα κράτος που βρίσκεται ο δράστης ή υπάρχουν αποθηκευμένα τα δεδομένα να είναι παράνομο στο άλλο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους),
- Για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής και διαδικτύου, καθώς και συνεχή εκπαίδευση όσων είναι αρμόδιοι για τη δίωξή του (αστυνομικές και δικαστικές αρχές).

Τα αδικήματα που διαπράττονται στον κυβερνοχώρο ταξινομούνται στις ακόλουθες κατηγορίες: Παρεμπόδιση κυβερνό-κυκλοφορίας, τροποποίηση και κλοπή δεδομένων, εισβολή και σαμποτάζ σε δίκτυο, μη εξουσιοδοτημένη πρόσβαση, διασπορά ιών, υπόθαλψη αδικημάτων, πλαστογραφία και απάτη (Νικολαΐδης, 1999, σ. 24-28, Furnell, 2006, σ. 56-58). Οι μορφές των κυβερνό-εγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το τμήμα ηλεκτρονικού εγκλήματος της ΕΛ.ΑΣ. την τελευταία δεκαετία αφορούσαν απάτες μέσω διαδικτύου, παιδική πορνογραφία, cracking και hacking, διακίνηση-πειρατεία λογισμικού, πιστωτικών καρτών και διακίνηση ναρκωτικών και εγκλήματα σε chat rooms (Νικολαΐδης, 1999, σ. 30).

Ο Αργυρόπουλος, (2001) (από Κριθαράς, 2009, σ. 45), κατηγοριοποιεί τις εξής βασικές κατηγορίες ηλεκτρονικών εγκλημάτων:

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον Υ/Η, όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον. Το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.

- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού Η/Υ, αλλά χωρίς την ύπαρξη δικτύωσης, όπως η παράνομη αντιγραφή λογισμικού.
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο, δηλαδή αποτελεί στοιχείο για την εγκληματική συμπεριφορά του δράστη, όπως με τη διασπορά κακόβουλου λογισμικού στο Darknet.

Σύμφωνα με τον Glick (1995, σ. 10) τα ηλεκτρονικά εγκλήματα διακρίνονται στις ακόλουθες κατηγορίες:

4. Απάτη: Για προσωπική ωφέλεια (αλλοίωση των εισαγόμενων με νόμιμο τρόπο, καταστροφή-συμπίεση-ακαταλληλότητα εκροών, αλλοίωση των δεδομένων του Η/Υ, αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρούμενων των προσβολών από τους ιούς),
5. Κλοπή: Των δεδομένων, του λογισμικού,
6. Χρήση λογισμικού χωρίς άδεια: Χρήση παράνομων αντιγράφων λογισμικού,
7. Ιδιωτική εργασία: Μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος,
8. Χάκινγκ: Ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας,
9. Σαμποτάζ: Η διαμεσολάβηση με την πρόκληση ζημιάς στον τρέχοντα κύκλο ή εξοπλισμό,
10. Εισαγωγή: Πορνογραφικού υλικού,
11. Ιοί: Διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής.

Στο σημείο αυτό θα αναλύσουμε τις διάφορες μορφές του ηλεκτρονικού εγκλήματος, τις οποίες έχουμε κατηγοριοποιήσει σε δύο κατηγορίες. Στην πρώτη κατηγορία ανήκουν τα γνήσια ηλεκτρονικά εγκλήματα, των οποίων η εμφάνιση συνδέεται άμεσα με τους Η/Υ και τον κυβερνοχώρο και στη δεύτερη τα συμβατικά -που προϋπήρχαν των Η/Υ- που συνέβαλαν σε μεγάλο βαθμό στους διαφορετικούς, ευκολότερους τρόπους εκτέλεσης τους (Furnell, 2006, σ. 56-58).

Τα πιο διαδεδομένα εγκλήματα που περιλαμβάνονται σε αυτήν την κατηγορία αποτελούν τα (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 33-38; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70): (i). Ηλεκτρονικό ψάρεμα (phising-pharming), (ii). Ανεπιθύμητη αλληλογραφία (spamming), (iii). Κακόβουλες εισβολές σε δίκτυα (hacking, cracking), (iv). Διασπορά κακόβουλου λογισμικού (ιοί-viruses, σκουλήκια-worms, δούρειοι ίπποι-trojan horses), (v). Πειρατεία ονομάτων χώρου (domain names piracy), (vi). Η απάτη με

τη Νιγηριανή επιστολή (Nigerian scam), και (vii). Επιθέσεις άρνησης εξυπηρέτησης (DoS, Denial of Service).

Οι *κακόβουλες εισβολές* σε δίκτυα αποτελούν τις μη εξουσιοδοτημένες προσβάσεις και τις χωρίς δικαίωμα διεισδύσεις σε συστήματα Η/Υ. Σκοπός τους δεν είναι μόνο η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας εισβολής σε ένα υπολογιστικό σύστημα. Μπορεί να αφορούν από το νομικό και έγκριτο πληροφορικό προγραμματισμό έως μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να οριστούν ως παράνομες και εγκληματικές. Η εισβολή σε δίκτυο ακόμα και αν δεν είναι κακόβουλη, ενέχει πάντα κακόβουλο χαρακτήρα. Αυτό συμβαίνει αφού ο επιτιθέμενος (hacker), διεισδύοντας στο σύστημα αποκτά γνώσεις για την ασφάλεια του και εντοπίζει τα πιθανά αδύνατα σημεία του. Έτσι είναι δυνατόν, εν συνεχεία, να διαπραχτούν κακόβουλες επιθέσεις ή ακόμα και να συγκεντρωθούν πληροφορίες για κάποιον τρίτο που θα προχωρήσει στην επίθεση (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Λάζος, 2001, σ. 36-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Συνοπτικά ως *χάκερ (hacker)* μπορεί να χαρακτηριστεί κάθε άτομο το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε Η/Υ ή σε περιφερειακή μνήμη ή μεταδίδονται με συστήματα τηλεπικοινωνιών. Γενικώς, αναγνωρίζονται τρεις κατηγορίες hacker: (i). Οι white hat-hackers, που στόχο έχουν να καταπολεμούν το ηλεκτρονικό έγκλημα, (ii). Οι black hat-hackers είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα και χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν, σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν. Το κίνητρο τους είναι χρηματικό τις περισσότερες φορές και όχι ιδεολογικό, και (iii). Οι grey hat-hackers που παραβιάζουν τον νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Επιπρόσθετα το cracking αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα. Οι αλλαγές των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων καθιστά δυνατή την παράνομη αντιγραφή τους. Βασικό σκοπό αποτελεί η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70)**.**

Ως *ανεπιθύμητη αλληλογραφία (spamming)* χαρακτηρίζεται η μαζική αποστολή μεγάλου αριθμού μηνυμάτων διαμέσω ηλεκτρονικού ταχυδρομείου που απευθύνονται σε παραλήπτες χωρίς οι ίδιοι να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα.

Αναφέρεται δε περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου. Χρησιμοποιείται επίσης για να καταδείξει την αποστολή μηνυμάτων που χαρακτηρίζονται ενοχλητικά για οποίον τα λαμβάνει. Τα κυριότερα χαρακτηριστικά του spamming συνοψίζονται ως ακολούθως: (i). Απρόκλητο, αφού δεν αναγνωρίζεται σχέση μεταξύ παραλήπτη και αποστολέα, (ii). Εμπορικό, αφού σκοπεύει στην προβολή ή διαφήμιση προϊόντων-υπηρεσιών, στη διεύρυνση πελατολογίου και στην πραγματοποίηση πωλήσεων, (iii). Μαζικό, αφού χαρακτηρίζεται από τη μαζική αποστολή μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών. Για να προστατευτεί ο χρήστης, πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Στην περίπτωση του *ηλεκτρονικού ψαρέματος* ο απατεώνας προσπαθεί μέσω μηνυμάτων να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα (τραπεζικού λογαριασμού ή πιστωτικής κάρτας). Αρχικά το υποψήφιο θύμα λαμβάνει ένα e-mail, αποστολέας του οποίου φαίνεται να είναι η τράπεζα του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του, λόγω προβλημάτων στους Η/Υ της τράπεζας ή υποψιών ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιαστεί. Το e-mail συνδέεται με τον δικτυακό τόπο της τράπεζας, οποίος όμως δεν είναι πραγματικός και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα. Το vishing αποτελεί μια προσαρμογή του ηλεκτρονικού ψαρέματος σε χρηστές κινητού τηλέφωνου ή VoIP (Voice over IP tools). Ο χρήστης λαμβάνει e-mail ή SMS με το οποίο του ζητείται να καλέσει έναν αριθμό χωρίς χρέωση με στόχο να επιβεβαιώσει τα στοιχεία του. Μπορεί ακόμα να λάβει ένα τηλέφωνο με μαγνητοφωνημένο μήνυμα που να του ζητά να εισάγει τα προσωπικά του στοιχεία.

Το *pharming* λογίζεται ως η εκμετάλλευση μιας ευπάθειας στην υπηρεσία DNS (Domain Name), που επιτρέπει σε έναν χάκερ να ανακατευθύνει την κυκλοφορία αυτού του δικτυακού τόπου σε άλλο. Στην περίπτωση αυτή οι δράστες δεν επιζητούν να πείσουν το θύμα, αλλά χρησιμοποιούν προγράμματα που, στην πραγματικότητα, επαναδρομολογούν την κυκλοφορία των δεδομένων. Έτσι, ο χρήστης καταχωρεί τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ ουσιαστικά τα αποθηκεύει στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, οι δράστες αποστέλλουν μέσω e-mail προγράμματα, τα οποία μετά την εγκατάστασή τους στον Η/Υ του θύματος, συλλέγουν και αποστέλλουν τα στοιχεία (π.χ., PIN, κωδικούς) τα οποία τους ενδιαφέρουν (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Ο όρος *malware* αποτελεί σύντμηση των λέξεων malicious και software. Αναφέρεται σε προγράμματα τα οποία έχουν ως στόχο να παραβιάσουν την ασφάλεια των προσωπικών υπολογιστών για να προκαλέσουν ζημιά ή για να υποκλέψουν προσωπικά στοιχεία. Οι πιο γνωστοί τρόποι διαδικτυακής παραβατικότητας μέσω δημιουργίας και διασποράς κακόβουλου λογισμικού είναι οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms), καθώς και οι δούρειοι ίπποι (Trojan horses) (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Οι *ιοί* αποτελούν προγράμματα που έχουν σχεδιαστεί ώστε να μολύνει άλλα προγράμματα με αντίγραφά του. Έχουν την δυνατότητα να αναπαράγονται συνεχώς και να μεταδίδονται από ένα σύστημα σε άλλο, με σκοπό τη δυσλειτουργία του Η/Υ ή και την καταστροφή ολόκληρων συστημάτων, την διαγραφή αρχείων ή το σβήσιμο του συνόλου των σκληρών δίσκων. Παρουσιάζουν παρασιτικές συμπεριφορές αφού μολύνουν άλλα αρχεία, ακολουθώντας την συμπεριφορά των βιολογικών. Ο συνηθέστερος τρόπος μετάδοσης των ιών είναι η διανομή τους μέσω ηλεκτρονικού ταχυδρομείου. Με βασικό κριτήριο το προσβαλλόμενο μέρος του Η/Υ (και τις προσπάθειες που καταβάλλουν οι εγκληματίες προκειμένου να μην γίνουν αντιληπτοί) διαχωρίζει τους ιούς ως ακολούθως: (i) Ιοί που μολύνουν τον τομέα εκκίνησης του σκληρού δίσκου, ο οποίος περιέχει εντολές εκκίνησης του Η/Υ (boot viruses), (ii) Ιοί που προσκολλώνται σε διάφορα τμήματα του λογισμικού ή στο πρόγραμμα ελέγχου εφαρμογών και μολύνουν το σύστημα (system cluster viruses), (iii). Ιοί που προσβάλλουν προγράμματα Η/Υ και κρύβονται μέσα σε εκτελέσιμα αρχεία (exe), που τρέχουν μόλις ξεκινήσει το πρόγραμμα που έχουν μολύνει (software viruses), (iv). Ιοί που μπορούν και αναπαράγονται με διάφορους τρόπους, με σκοπό να εξασφαλίζουν την ανθεκτικότητα τους έναντι των διαφόρων προγραμμάτων anti-virus (polymorphous viruses), (v). Ιοί που κρύβουν τις αλλαγές που πραγματοποιούν στον τομέα εκκίνησης ενός συστήματος ή ενός αρχείου, επεμβαίνοντας στο λογισμικό του προσβαλλόμενου συστήματος (stealth viruses), (vi). Ιοί που στόχο έχουν να καταστρέψουν ή να σβήσουν εντελώς τα προγράμματα Anti-Virus (retroviruses) και (vi). Ιοί που προσβάλλουν τις μακροεντολές σύγχρονων προγραμμάτων εφαρμογών (data viruses) (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Ένας *δούρειος ίππος* επίσης, αποτελείται από δύο μέρη, το server και το client. Για να μολυνθεί ένας Η/Υ από έναν δούρειο ίππο θα πρέπει με κάποιον τρόπο να εγκατασταθεί και να εκτελεστεί σε αυτόν το μέρος server. Στη συνέχεια, αφού εκτελεστεί το μέρος client στον Η/Υ του επιτιθέμενου και δοθεί η IP διεύθυνση του Η/Υ που έχει προσβληθεί, ο έλεγχος του

θα είναι πλέον εύκολος. Τα προγράμματα με τα οποία μεταφέρονται οι δούρειοι ίπποι στον Η/Υ λέγονται droppers. Οι δούρειοι ίπποι επικοινωνούν με τον client μέσω διαφόρων θυρών του Η/Υ τις οποίες μπορούμε να απενεργοποιήσουμε με τη χρήση κάποιου τοίχους προστασίας (firewall) (Λάζος, 2001, σ. 37). Ένα τέτοιο κακόβουλο λογισμικό μπορεί να έχει συνήθως την μορφή παιχνιδιού, ενώ αυτό που κάνει όμως στην πραγματικότητα είναι να κλέβει τα ονόματα και τους κωδικούς των ανυποψίαστων χρηστών του διαδικτύου. Ένας δούρειος ίππος δημιουργεί μια κερκόπορτα (trapdoor) στο σύστημα, την οποία μπορεί να χρησιμοποιήσει ο επιτιθέμενος για να συνδεθεί σε αυτή (μυστικό σημείο εισόδου σ' ένα πρόγραμμα, που επιτρέπει σε κάποιον που τη γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης) (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Τα *σκουλήκια* αποτελούν προγράμματα που χρησιμοποιούνται σαν ένας μηχανισμός μεταφοράς άλλων. Χρησιμοποιούν τις δυνατότητες κυκλοφορίας που τους παρέχει ένα δίκτυο με σκοπό να μεταφέρουν κάποιο καταστρεπτικό πρόγραμμα δηλαδή έναν ιό στα διάφορα συστήματα του δικτύου αυτού. Η διαφορά τους από τους ιούς αναφέρεται ότι δεν χρειάζεται ανθρώπινη παρεμβολή για την ενεργοποίηση τους (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Οι *dialers* είναι μια κατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, και στοιχεία λογαριασμών) για τον χρήστη, χωρίς τη γνώση και έγκρισή του, προσκομίζοντας χρήματα εύκολα και γρήγορα. Αλλάζουν τις ρυθμίσεις του δικτύου -μέσω τηλεφώνου- ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο αριθμό που συνήθως είναι μια διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του πάροχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό αυτό και όχι τον αριθμό του δικού του πάροχου υπηρεσιών διαδικτύου (Νικολαΐδης, 1999, σ. 40-50; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Οι *λογικές βόμβες* αποτελούν μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον ή τροποποιούν κάποιον υπάρχοντα κώδικα. Προστίθενται στο πρόγραμμα από χρήστη ο οποίος έχει πρόσβαση στο σύστημα και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους.

Κατασκευάζονται ευκολότερα και έχουν δυνατότητα να προκαλέσουν σοβαρές ζημιές ακόμα και καταστροφές σε σωσμένα αρχεία αλλά και σε ολόκληρο το λογισμικό ενός ηλεκτρονικού Η/Υ (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Τα *rootkits* είναι ένα σύνολο εργαλείων και υπηρεσιών για διατηρήσει κάποιος την πρόσβαση του σε ένα σύστημα, από τη στιγμή που θα εισβάλει σε αυτό. Επιτρέπουν να αναζητηθούν ονόματα χρηστών και κωδικοί πρόσβασης, να εξαπολυθούν επιθέσεις κατά συστημάτων -από απόσταση- και να αποκρυφτούν δράσεις με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος. Μπορούν επίσης, να ελέγχουν την πληκτρολόγηση, να επιτίθενται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσουν κερκόπορτες για την εξυπηρέτηση των εισβολέων. Τα *ransom ware* αποτελούν μια κατηγορία κακόβουλων λογισμικών, που από απόσταση κρυπτογραφούν δεδομένα του χρηστή και για να τα αποκρυπτογραφήσει απαιτεί λύτρα (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Μια *bot* εφαρμογή είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο πάνω σε έναν Η/Υ. Οι υπολογιστές που έχουν μολυνθεί με bot χαρακτηρίζονται ζόμπι. Ο ιδιοκτήτης δεν γνωρίζει ότι έχει εξαπολύσει έναν ιό ή εγκαταστήσει έναν δούρειο ίππο ο οποίος ενεργοποιεί τον Η/Υ να λειτουργήσει ως ζόμπι. Ο εισβολέας μπορεί να χρησιμοποιήσει το μολυσμένο Η/Υ για να επιτεθεί ή να στείλει spam σε άλλους υπολογιστές. Το *scare ware* αποτελούν προγράμματα εξαπάτησης και είναι γνωστά και ως fraud ware. Εμφανίζονται με τη μορφή pop-up παραθύρων, με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. προειδοποιώντας τους ότι ο Η/Υ τους έχει μολυνθεί με κακόβουλο λογισμικό) και να τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου λογισμικού που υποτίθεται πως θα τους προστατέψει από επιθέσεις και απειλές (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Ένα botnet είναι μια συλλογή από υπολογιστές των θυμάτων, που είναι γνωστή ως bots, μη επανδρωμένα αεροσκάφη, ή ζόμπι, που έχουν μολυνθεί και αφομοιωθεί σε μια μεγαλύτερη συλλογική μέσω μιας κεντρικής διοίκησης και ελέγχου (Nazario 2007). Τα botnets μπορούν να χρησιμοποιηθούν για πολλούς φαύλους σκοπούς:

• DDoS επιθέσεις (Distributed Denial of Service)

• Infection(Λιμωξη)

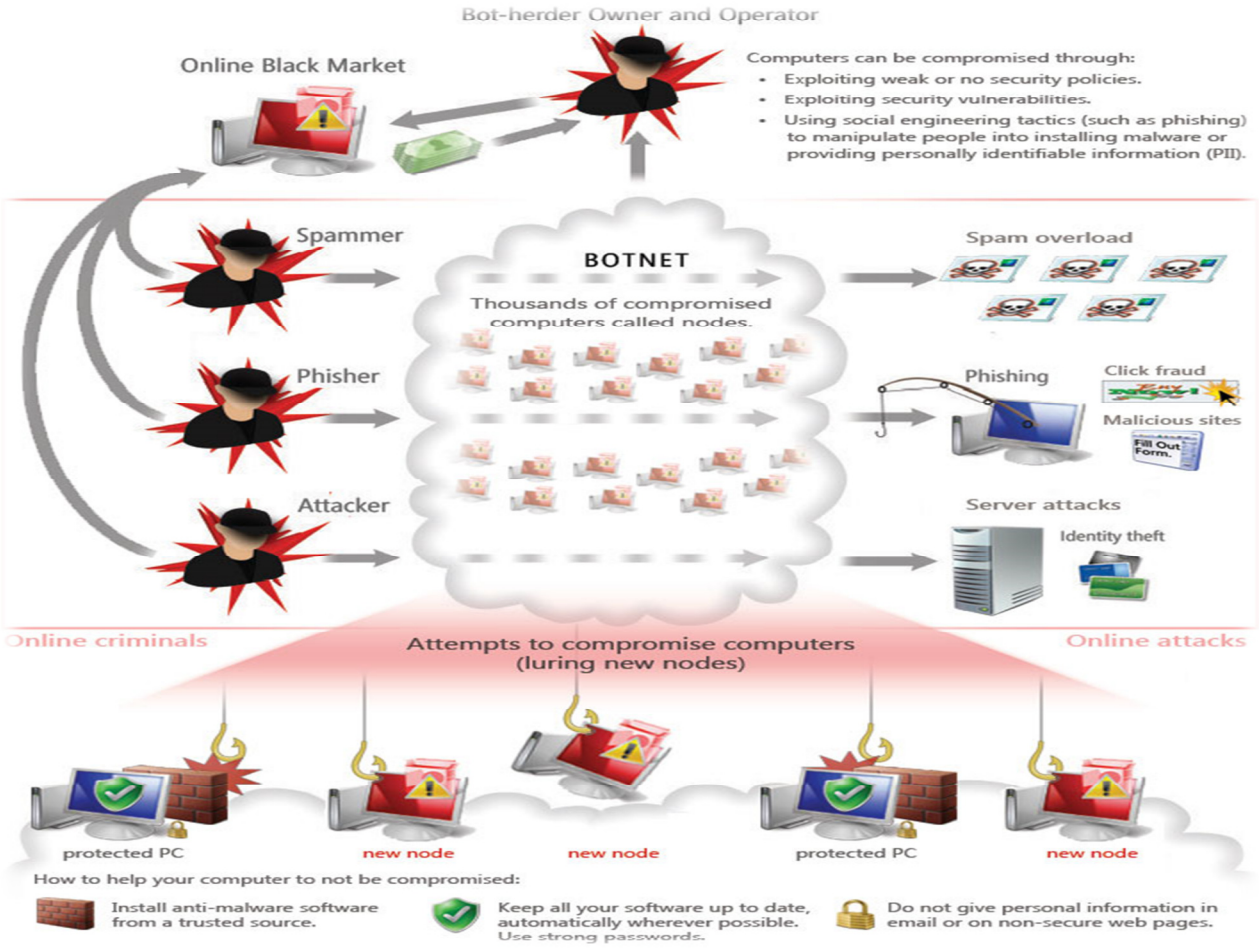
• Spamming

• Κατασκοπεία

• Proxies

Το λογισμικό bot συνεχίσει να εξελίσσεται μπορείτε να το κατεβάσετε δωρεάν από πολλές ιστοσελίδες στο διαδίκτυο hacking.

Κάτω από τα μολυσμένα botnet δικτύα υπολογιστών βρίσκεται ένα κρυφό κοινωνικό δίκτυο ατόμων που ασχολούνται με το ηλεκτρονικό έγκλημα. (Εικονα 1) Ολόκληρα δίκτυα συνομιλίας έχουν εντοπιστεί σύμφωνα με την οποία οι spammers, bot herderss, malware authorss, crackerss web site, και άλλων εγκληματιών συγκεντρώνονται για να συνεργαστούν και να πωλούν τις υπηρεσίες τους σε μια ακμάζουσα μαύρη οικονομία της αγοράς.



Εικονα1. Botnet(http://www.helpsec.net/malware-infected-home-routers-used-to-launch-ddos-attacks)

Τα *βακτήρια (bacteria)* είναι προγράμματα που δεν καταστρέφουν εμφανώς. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο δεν κάνει τίποτε άλλο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα σύστημα Η/Υ. Τότε δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Τα προγράμματα αυτά μπορούν εν συνεχεία να αντιγράψουν τον εαυτό τους. Αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Το μέσο για την είσοδο στο διαδίκτυο αποτελεί το domain name, το οποίο επιτελεί ρόλο ηλεκτρονικής διεύθυνσης. Έτσι επιτρέπεται η επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διεύθυνσης. Το domain name αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (3 έως 24), με χωρίς ή λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία. Διαιρείται σε τρία μέρη: Το πρώτο μέρος είναι κοινό για όλα τα domain names και αποτελείται από τα αρκτικόλεξα http://www και δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο παγκόσμιο διαδίκτυο. Το δεύτερο μέρος ή *μεταβλητό πεδίο* (SLD) αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το όνομα και την διαδικτυακή διεύθυνση. Το τρίτο μέρος είναι το *top level domain* (TLD), που δηλώνει το είδος της ιστοθέσης ή τη γεωγραφική προέλευση (…com, για όσους ασκούν εμπορική δραστηριότητα, …edu, για εκπαιδευτικούς οργανισμούς, …org, για οργανισμούς, …net για παροχές υπηρεσιών διαδικτύου, …gov, για κυβερνητικούς οργανισμούς, …int, για διεθνείς οργανισμούς, …gr» για τη χώρα αρχειακής καταχώρισης-Ελλάδα) (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Το domain name δεν μπορεί να ταυτιστεί με την εμπορική επωνυμία , τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει, ωστόσο, να αποδίδεται σε αυτό μια λειτουργία τόσο διακριτικού τίτλου όσο και σήματος. Όταν δε χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο πρέπει να έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσης οποιασδήποτε ονομασίας, όσο γνωστή και αν είναι, από οποιοδήποτε, προκαλεί ανεπανόρθωτες ζημίες στην επιχείρηση που

καθιερώθηκε στις συναλλαγές με την συγκεκριμένη ονομασία. Με δεδομένο τα ανωτέρω, θα πρέπει να απολαμβάνει προστασίας αντίστοιχης με εκείνη των διακριτικών γνωρισμάτων, αλλά και ένα διακριτικό γνώρισμα θα πρέπει να προστατεύεται από τη χρήση ενός ονόματος διαδικτύου. Παρά το γεγονός ότι προηγήθηκε χρονικά η καταχώριση αυτού στο διαδίκτυο, αρκεί να μην έχει χορηγηθεί το συγκεκριμένο όνομα σε άλλον αιτούντα (First Come First Served). Η καταχώριση γνωστού ξένου διακριτικού γνωρίσματος ως domain name συνιστά και αθέμιτο παρεμποδιστικό ανταγωνισμό (αρ. 1, Ν 146/1914) (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Την *Νιγηριανή απάτη* αποτελούν μηνύματα ηλεκτρονικού ταχυδρομείου (γνωστά και ως 419) που εμπεριέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας. Επικαλούμενος λόγους πολιτικής φύσης, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός Νιγηρίας κάποιο τεράστιο χρηματικό ποσό. Το θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά ζητείται η συγκατάθεση του παραλήπτη και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του ή και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης αρχίζει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Αρχίζει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου, οπότε το θύμα αρχίζει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης χρεώνει τον τραπεζικό λογαριασμό του θύματος με υπέρογκα ποσά (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Οι επιθέσεις *άρνησης εξυπηρέτησης* (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου

(διακομιστής ιστοσελίδας-web server ή διακομιστής αρχείων-file server). Ο Η/Υ- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των ψεύτικων αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου, όπως επίσης και την ακεραιότητα των δεδομένων και τη γενικότερη λειτουργία του συστήματος. Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι: (i). Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες, (ii). Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο, και (iii). Η υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Τέλος, αναφέρουμε και τα συμβατικά εγκλήματα που τελούνται και χωρίς τη χρήση Η/Υ ή του διαδικτύου. Στην κατηγορία αυτή εντάσσονται εγκλήματα που προϋπήρχαν της πληροφορικής τεχνολογίας. Η τεχνολογία έχει δώσει δυνατότητες για νέους και πιο πρόσφορους τρόπους τέλεσης τους. Τα κυριότερα εγκλήματα αυτής της κατηγορίας είναι τα εξής (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κιούπης & Ιωαννίδου, 2007, σ. 23-27; Κριθαράς, 2009, σ. 50-70): (i). Το ξέπλυμα χρήματος, (ii). Η πειρατεία λογισμικού, (iii). Η παιδική πορνογραφία και (iv) η διαδικτυακή τρομοκρατία.

Ο όρος *ξέπλυμα χρήματος* περιγράφει τις διαδικασίες που επιχειρείται η εξαφάνιση χρήματος που έχει προέλθει από παράνομες δραστηριότητες. Με άλλα λόγια τα κέρδη που αποκτήθηκαν μέσω εγκλημάτων ενεργειών υπόκεινται σε μια σειρά διαδικασιών οι οποίες καλύπτουν τις παράνομες προέλευσης τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές. Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια: (i). *Τοποθέτηση*: Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο οικονομικό σύστημα, σε έναν χρηματοοικονομικό οργανισμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις, (ii). *Στρωματοποίηση*: Ο δράστης επιχειρεί σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση. Με τον τρόπο αυτό μεταμφιέζονται οι αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεγκτικά όργανα του φορέα στον οποίο επενδύθηκαν τελικά, (iii). *Ενσωμάτωση*: Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριότητας όπως

για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κ.λπ., έτσι ώστε τα εν λόγω κεφάλαια να επιστρέφουν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια. Το βασικό πλεονέκτημα του ξεπλύματος χρήματος μέσω διαδικτύου αποτελεί το γεγονός ότι δεν υπάρχει προσωπική επαφή μεταξύ των συναλλασσόμενων μερών. Ως αποτέλεσμα οι δράστες νιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από την ανωνυμία τους νομιμοποιούν τα έσοδα των παράνομων δραστηριοτήτων (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Η ανωνυμία του διαδικτύου, δυσχεραίνει την πιστοποίηση της ταυτότητας των πελατών μιας εταιρείας. Ως αποτέλεσμα, πολλές εταιρείες, χωρίς να το γνωρίζουν, διευκολύνουν το ξέπλυμα χρήματος. Για παράδειγμα, έχει διαπιστωθεί η αγορά, μέσω του διαδικτύου, ασυνήθιστα μεγάλων ποσοτήτων αγαθών από συγκεκριμένους πελάτες, που θέλουν, με αυτό τον τρόπο, να προωθήσουν χρήματα, που έχουν περιέλθει στην κατοχή τους από παράνομες δραστηριότητες. Άλλη μέθοδος ξεπλύματος χρημάτων είναι η κατάθεση μέσω του διαδικτύου, σχετικά μικρών ποσών σε πολλαπλούς τραπεζικούς λογαριασμούς (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Επίσης, ο κύριος όγκος των πληροφορικών εγκλημάτων εντάσσεται στην υποκατηγορία των πληροφορικών οικονομικών εγκλημάτων. Η αναλογία δε μεταξύ των διάφορων υποκατηγοριών πληροφορικού εγκλήματος που απασχολούν τους ειδικούς είναι χαρακτηριστική: σε κάθε δώδεκα περιπτώσεις πληροφορικού οικονομικού εγκλήματος αναλογεί μόλις μια περίπτωση των άλλων κατηγοριών. Ένας παράγοντας που συμβάλλει σε αυτή τη δυσαναλογία ως προς ενδιαφέρον αποτελεί το ευκολότερα ανιχνεύσιμο, το χειροπιαστό, του πληροφορικού οικονομικού εγκλήματος: Κατά κανόνα, γίνεται αντιληπτό από τους ενδιαφερόμενους σε σχετικά μικρό χρονικό διάστημα μετά την τέλεσή του. Επιπλέον, από τη στιγμή που θα γίνει αντιληπτό, είναι μετρήσιμο με μεγάλη ακρίβεια, τουλάχιστον όσον αφορά στα άμεσα οικονομικά του μεγέθη. Ένας δεύτερος παράγοντας είναι το γεγονός ότι και οι ίδιες οι επιχειρήσεις έχουν δείξει μεγάλο ενδιαφέρον για αυτόν τον τύπο εγκλήματος και ως συνέπεια έχουν διαθέσει πολύ σημαντικούς πόρους για τη διερεύνησή του. Συνεπώς, η ισχύς των επιχειρήσεων συμβάλλει σε σημαντικό βαθμό στην αύξηση της αντιπροσώπευσης του πληροφοριακού οικονομικού εγκλήματος μέσα στο ευρύτερο πληροφορικό έγκλημα (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Ένας τρίτος παράγοντας είναι ότι συχνά το οικονομικό έγκλημα είναι ευκολότερα αναγνωρίσιμο, τόσο σε σύγκριση με μια σημαντική μερίδα υπερατομικών πληροφορικών εγκλημάτων όπως είναι οι περιπτώσεις κατασκοπείας, όσο και σε σύγκριση με μερίδα των πληροφορικών εγκλημάτων κατά των προσωπικών δικαιωμάτων όπου, συχνά, το ίδιο το θύμα δεν επιθυμεί την αποκάλυψη. Στο πλαίσιο των πληροφορικών οικονομικών εγκλημάτων, η απάτη μέσω Η/Υ περιλαμβάνει την παραποίηση κάποιων δεδομένων ή πληροφοριών που φιλοξενούνται στις βάσεις δεδομένων ή σε προγράμματα με σκοπό το οικονομικό κέρδος. Αφορά κυρίως στην κλοπή, διαγραφή, αλλοίωση ή προσθήκη δεδομένων ή πληροφοριών με σκοπό το βραχυπρόθεσμο ή μακροπρόθεσμο οικονομικό κέρδος. Κεντρικό αντικείμενο- στόχος της συγκεκριμένης μορφής απάτης είναι τα δεδομένα που φιλοξενούνται στον Η/Υ και αφορούν σε οικονομικά μεγέθη. Η συγκεκριμένη απάτη μετεξελίχθηκε στο πέρασμα του χρόνου από ένα ομοιογενές σύνολο αδικημάτων, της εποχής των κεντρικών πληροφορικών συστημάτων, σε μια διαφοροποιημένη ενότητα που περιγράφει ένα μεγάλο φάσμα διαφορετικών υποθέσεων στο πεδίο του οικονομικού εγκλήματος (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Η απάτη σε βάρος μιας επιχείρησης ή ενός ιδιώτη μέσω της εστίασης, και παραποίησης, σε πληροφορίες και δεδομένα, τα οποία τους αφορούν άμεσα και έμμεσα, έχει να κάνει με τους άυλους πόρους, όπως χρηματικές καταθέσεις, οικονομικούς τίτλους, για παράδειγμα, ομόλογα, και λογιστικά μεγέθη, όπως ισολογισμούς. Υπάρχουν περιπτώσεις *βελτίωσης της πίστης* μέσω της παραποίησης των δεδομένων που αναφέρονται σε ένα άτομο ή μια επιχείρηση, αλλά και χειροτέρευσης της φερεγγυότητας ενός ατόμου ή μιας επιχείρησης, για τους αντίθετους λόγους, που μπορεί να πραγματοποιηθεί από κάποιο άτομο ή επιχείρηση εχθρικά διακείμενων ή αντίθετων συμφερόντων (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70):.

Απάτες μέσω Η/Υ με την παρέμβαση στο σύστημα επεξεργασίας δεδομένων ενός οργανισμού ή μιας επιχείρησης απαντώνται συχνά και σχετίζονται με μισθούς-συντάξεις αλλά και τραπεζικές καταθέσεις. Σε ένα ανοχύρωτο σύστημα, η δημιουργία ενός τραπεζικού λογαριασμού πολλών μηδενικών είναι ζήτημα ελάχιστου χρόνου και προσπάθειας. Αν το πληροφορικό σύστημα διαθέτει έναν αμυντικό μηχανισμό προηγούμενης γενιάς και αν ο συγκεκριμένος hacker δε βιάζεται, αλλά αρκείται σε έναν αρχικό λογαριασμό ενός ή δύο μηδενικών, και κατόπιν εισάγει μια ρουτίνα προσθήκης πέντε μηδενικών σε κάποια συχνά μεν, αλλά άτακτα χρονικά διαστήματα, δεν έχει λόγους να φοβάται τις συνέπειες. Πέρα όμως,

από τις περιπτώσεις παράνομης κατασκευής δεδομένων, συχνά παρατηρούνται και περιπτώσεις παραβίασης καρτών συναλλαγής (ATM cards) και ανάλογων μέσων πληρωμής. Ακόμη και αν τέτοιου είδους απάτες οδηγούν σε μικρές συνολικά ζημιές, οι στατιστικές δείχνουν πως η κακοχρησία των καρτών αποτελεί μια από τις πιο συχνές υποθέσεις πληροφορικού εγκλήματος. Μια παραποιημένη πληρωμή διαπράττεται μέσω τράπεζας, που διαθέτει σύστημα αυτόματης ανάληψης ή χορήγησης χρήματος (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70):.

Η *κλοπή ταυτότητας* είναι ένα από τα πλέον σοβαρά εγκλήματα του διαδικτύου (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70). Στην ψηφιακή εποχή που διανύουμε, τεράστιες ποσότητες δεδομένων είναι αποθηκευμένες σε ηλεκτρονικές βάσεις δεδομένων για διάφορους σκοπούς. Είναι εύκολο για τον καθέναν, να βρει στοιχεία ατόμων και να τα χρησιμοποιήσει για την διεκπεραίωση πάσης φύσεως συναλλαγών. Το έγκλημα της κλοπής ταυτότητας, ολοκληρώνεται σε δυο στάδια. Στο πρώτο, ο επιτιθέμενος προσπαθεί να αποκτήσει τα στοιχεία της ταυτότητας ενός ατόμου με διάφορους τρόπους ψηφιακούς, όπως:

- Υποκλέπτοντας την αλληλογραφία, παραβιάζοντας μη ασφαλή κιβώτια αλληλογραφίας, υποβάλλοντας ψευδή αλλαγή διεύθυνσης κατοικίας στο ταχυδρομικό γραφείο των νόμιμων παραληπτών,
- Αποσπώντας τα ενημερωτικά σημειώματα των πιστωτικών καρτών, υποδυόμενο τον υπάλληλο ή συγγενικό πρόσωπο του νόμιμου κατόχου,
- Εισβάλλοντας στις βάσεις δεδομένων εταιρειών και οργανισμών, όπου φυλάσσονται προσωπικά δεδομένα.
- Χρησιμοποιώντας ειδικό λογισμικό, το οποίο, έχει τη δυνατότητα, να αποσπά προσωπικά δεδομένα και άλλες πληροφορίες, παρακολουθώντας την κίνηση των πακέτων στο διαδίκτυο.

Το επόμενο βήμα είναι η χρησιμοποίηση των κλεμμένων στοιχείων, που μπορεί να πραγματοποιηθεί:

- Ανοίγοντας λογαριασμούς πιστωτικών καρτών με τα στοιχεία του θύματος, τους οποίους και χρησιμοποιεί για την αγορά αγαθών μέσω του διαδικτύου,
- Ανοίγοντας τραπεζικούς λογαριασμούς, τους οποίους, χρεώνει με ακάλυπτες επιταγές,

- Δημιουργώντας πλαστές πιστωτικές κάρτες, άδειες οδήγησης, διαβατήρια και ταυτότητες χρησιμοποιώντας τα στοιχεία του θύματος,
- Υποβάλλοντας ψευδείς φορολογικές δηλώσεις (και μέσω Διαδικτύου), για να εισπράξει επιστροφή φόρου.
- Πειρατεία ονομάτων χώρου

Η *πειρατεία ονομάτων χώρου* γνώρισε ιδιαίτερη άνθηση κατά τα πρώτα χρόνια του διαδικτύου. Διάφοροι επιτήδειοι, εκμεταλλευόμενοι το γεγονός πως μεγάλες εταιρείες δεν είχαν κατοχυρώσει, ακόμη, ονόματα χώρων για τους δικτυακούς τους τόπους, προέβαιναν σε κατοχύρωση ονομάτων διάσημων εταιρειών, με αποτέλεσμα να αποκτούν τα δικαιώματα της νέας διεύθυνσης. Στη συνέχεια, μπορούν να δράσουν με δύο διαφορετικούς τρόπους, όπως να παραχωρήσουν την διεύθυνση στην εταιρεία που κατέχει το συγκεκριμένο όνομα, έναντι βέβαια σημαντικού χρηματικού ποσού, είτε να προβούν στην ανάρτηση, στη συγκεκριμένη διεύθυνση, περιεχομένου προσβλητικού, γεγονός που επιφέρει σημαντικές συνέπειες στην εταιρεία Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70):.

Ο όρος *πειρατεία λογισμικού* αναφέρεται στην αναπαραγωγή και διάθεση προγραμμάτων Η/Υ, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους. Η ψηφιακή μορφή των εφαρμογών λογισμικού, καθιστά ιδιαίτερα εύκολη την αναπαραγωγή τους σε πολλαπλά αντίγραφα. Πριν από την έλευση του διαδικτύου, οι εφαρμογές λογισμικού διακινούνταν με δισκέτες ή CD. Η εξάπλωση, όμως, του διαδικτύου και ιδιαίτερα των ευρυζωνικών συνδέσεων άνοιξε νέους ορίζοντες στην πειρατεία λογισμικού. Πλέον, το λογισμικό μπορεί να διακινηθεί με διάφορες υπηρεσίες που προσφέρει το διαδίκτυο, όπως ηλεκτρονικό ταχυδρομείο (e-mail), chat, UseNet, ftp και ιδιαίτερα με τις εφαρμογές P2P ανταλλαγής αρχείων. Οι εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα ώστε να αποτρέψουν την αντιγραφή ή χρήση τους από πολλούς Η/Υ, αν και οι hackers-crackers πάντα βρίσκουν τεχνικές για να παρακάμψουν τα μέτρα αυτά. Χρησιμοποιώντας την τεχνική cracking έχουν τη δυνατότητα να απενεργοποιούν τους κωδικούς, τα κλειδιά και ότι άλλο χρησιμοποιείται για την προστασία ενός προγράμματος (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι ακόλουθες (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70): (I). *Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση*

της αδείας χρήσης: Αποτελεί την συνηθέστερη μορφή παράνομης χρήσης εφόσον απαιτείται ξεχωριστή άδεια για κάθε Η/Υ στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα. Εκδηλώνεται δε ως εξής: (i). Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες, (ii). Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρεία που διαθέτει άδεια για έναν συγκεκριμένο αριθμό χρηστών Η/Υ, (iii). Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών, (iv). Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους, αφού οι πωλητές Η/Υ προκειμένου να κάνουν την αγορά ενός πιο ελκυστική προσφέρουν προγράμματα χωρίς τις άδειες, και (II). *Πλαστογράφηση ή πλήρης απομίμηση του προϊόντος*: Η παράνομη αναπαραγωγή και πώληση λογισμικού -ώστε να θεωρείται νόμιμο-, περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, αναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Τα πλαστά λογισμικά συνήθως κατασκευάζονται και προωθούνται με τέτοιους τρόπους ώστε να ανταγωνίζονται το αυθεντικό προϊόν.

Η παιδική πορνογραφία ως φαινόμενο αποτελεί μάστιγα των σύγχρονων παγκοσμιοποιημένων κοινωνιών που αποκτά ολοένα και μεγαλύτερες διαστάσεις με ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Ο κυβερνοχώρος παρέχει στους παραγωγούς-διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Έτσι με τη χρήση του διαδικτύου: (i). Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτότητά του, (ii). Υπάρχει προσβασιμότητα του πορνογραφικού υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος, (iii). Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων, (iv). Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού το οποίο μέσα σε ελάχιστο χρόνο μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών (Κιούπης & Ιωαννίδου, 2007, σ. 23-27).

Η διακίνηση πορνογραφικού υλικού, δεν αποτελεί ένα καινούργιο έγκλημα. Η εξάπλωση όμως, του διαδικτύου, έχει διευκολύνει τη διάπραξή του. Τα αδικήματα που συνδέονται με τη μορφή αυτή του υλικού, σχετίζονται τόσο με τη δημιουργία του υλικού όσο και με τη μη νόμιμη διακίνησή του. Η παράνομη διακίνηση υλικού παιδικής πορνογραφίας έχει λάβει τεράστιες διαστάσεις, προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές αρχές. Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη επιχείρηση, καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό

υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων, αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε μέσα ικανοποίησης των σεξουαλικών τους ορέξεων. Ο ανήλικος από την πλευρά του, αποτελεί και χρήστη των Η/Υ και του διαδικτύου. Το πρόβλημα μπορεί να προσεγγισθεί από δύο διαφορετικές πλευρές, όσον αφορά το πώς επηρεάζεται η συμπεριφορά των παιδόφιλων με την είσοδό τους σε πορνογραφικές ιστοσελίδες. Ενδέχεται οι ορέξεις του δράστη να ικανοποιηθούν και να εκτονωθούν με τον τρόπο αυτό και να μην εκδηλωθούν οι διαστροφικές του τάσεις στο υπόλοιπο κοινωνικό περιβάλλον. Είναι όμως πολύ πιθανό να του δημιουργηθεί ψύχωση, την οποία θα εκδηλώσει στον κοινωνικό του περίγυρο, κακοποιώντας σεξουαλικά κάποιο ανήλικο άτομο. Επιπλέον οι παιδόφιλοι δημιουργούν τα δικά τους δωμάτια επικοινωνίας, στα οποία είναι μόνο αυτοί ευπρόσδεκτοι, ανταλλάσσοντας ιδέες, εμπειρίες και τακτικές προσέγγισης ανηλίκων (Κιούπης & Ιωαννίδου, 2007, σ. 23-27).

Το πορνογραφικό υλικό, που διακινείται μέσω του διαδικτύου, συνήθως είναι σε μορφή φωτογραφιών, βίντεο ή και οποιοδήποτε μορφή πολυμέσων. Δυστυχώς, υπάρχουν πάρα πολλοί δικτυακοί τόποι που έχουν πορνογραφικό περιεχόμενο και λειτουργούν ως λέσχες παιδεραστών και τα οποία πουλούν φωτογραφίες και βιντεοταινίες ανήλικων πρωταγωνιστών. Υπάρχουν ηλεκτρονικές διευθύνσεις με μαλακό πορνογραφικό υλικό οι ενδιαφερόμενοι μπορούν να τις αναζητήσουν μέσω άλλων ηλεκτρονικών διευθύνσεων ερωτικού ή συναφούς περιεχόμενου. Στις διευθύνσεις εκείνες όμως που έχουν πιο σκληρό πορνό μέσα στο δίκτυο μπορεί να φτάσει κάποιος μόνο αν ψάξει ενδελεχώς στο διαδίκτυο. Οι κωδικοποιημένες πορνογραφικές διευθύνσεις ανακοινώνονται ιδιωτικά, μέσω e-mail, ενώ οι παράνομες υπηρεσίες που προσφέρονται, διαφημίζονται μέσα από διάφορες ομάδες συζητήσεων, που καλύπτονται πίσω από παραπλανητικούς τίτλους και ενδιαφέροντα, όπως μουσική, ταξίδια ή αθλητισμός. Οι μηχανές αναζήτησης σπάνια θα καταδείξουν μια ηλεκτρονική διεύθυνση που έχει ως κύριο περιεχόμενο την παιδική πορνογραφία. Ο καθένας μπορεί εύκολα να το κατεβάσει στον Η/Υ του, χωρίς να χρειαστεί να αποκαλύψει την ταυτότητά του. Τέτοιου είδους υλικό, βρίσκεται σε διάφορους δικτυακούς τόπους, ενώ σε συγκεκριμένους δικτυακούς τόπους, γίνεται ανταλλαγή υλικού, δηλαδή αντί να πληρώσει κάποιος τίμημα για το υλικό που προμηθεύεται, προσφέρει νέο υλικό, ως αντάλλαγμα. Αυξημένη ζήτηση υπάρχει στην κακοποίηση ανηλίκων από υπερήλικες (Κιούπης & Ιωαννίδου, 2007, σ. 23-27).

Στο διαδίκτυο παρουσιάζονται και διακινούνται χιλιάδες φωτογραφίες βασανιστηρίων χωρίς έλεγχο, οι οποίες χωρίς δυσκολία χαρακτηρίζονται αδικαιολόγητα ως ερωτικές. Προκειμένου να στοχεύσουν σε κοινό με συγκεκριμένα ενδιαφέροντα οι έμποροι της παιδικής αθωότητας διαφημίζουν την καταγωγή και την ηλικία των ανήλικων θυμάτων. Η εξάπλωση του φαινομένου της πορνογραφίας και πορνείας ανηλίκων στο διαδίκτυο αλλάζει διαρκώς, και αυτό οφείλεται στο γεγονός ότι αυτός είναι ο ιδανικός χώρος όπου οποιοσδήποτε μπορεί να περάσει από το πραγματικό στο φανταστικό, από έναν κόσμο με κανόνες ηθικής και νόμους σε έναν άλλον, όπου όλα επιτρέπονται, και δεν υπάρχουν ηθικοί ή άλλοι φραγμοί. Εξαιτίας δε του νεαρού της ηλικίας του, δηλαδή της έντονης περιέργειας και του ατίθασου του χαρακτήρα του, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου και να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του (Κιούπης & Ιωαννίδου, 2007, σ. 23-27).

Ο χρήστης του δικτύου που αναζητά πορνογραφικό υλικό, ζει σε έναν κόσμο φανταστικό όπου μπορεί να βγάλει στην επιφάνεια τις ερωτικές και σεξουαλικές του προτιμήσεις ελεύθερα, χωρίς τον κίνδυνο της αποκάλυψης, της κριτικής, του κοινωνικού ελέγχου, ή ακόμα και της ποινικής δίωξης του. Πολλοί από αυτούς τους χρήστες της αναζήτησης υλικού παιδικής πορνογραφίας είναι οικογενειάρχες, επαγγελματίες με υψηλό εισόδημα, ίσως και επιφανή μέλη κάποιας κοινωνίας, που δεν είχαν ευκαιρία να εξωτερικεύσουν ασφαλώς αυτή την ερωτική τους διαστροφή. Μέσω όμως του διαδικτύου δεν ρισκάρουν και νιώθουν ασφαλείς, φυσιολογικοί και νόμιμοι, αφού καλύπτονται πίσω από την ανωνυμία μιας τυχαίας διεύθυνσης ηλεκτρονικού ταχυδρομείου (Κιούπης & Ιωαννίδου, 2007, σ. 23-27).

Προσεγγίζοντας την αιτιολογία του φαινομένου καταλήγουμε ότι η φτώχεια είναι ο κύριος καταλύτης, αλλά δεν μπορεί να εξηγήσει επαρκώς την εμπορική σεξουαλική εκμετάλλευση των παιδιών. Κατά συνέπεια θα πρέπει να εστιάσουμε την προσοχή μας στους ακόλουθους παράγοντες που συμβάλλουν ουσιαστικά σε αυτή την εγκληματική συμπεριφοράς (Κιούπης & Ιωαννίδου, 2007, σ. 23-27; Δήμου, 2002, σ. 18-22):

- Η ενδοοικογενειακή κακοποίηση και παραμέληση παιδιών: Ένα μεγάλο ποσοστό των παιδιών που βρίσκονται υπό σεξουαλική εκμετάλλευση έχουν υποστεί κάποιου είδους σωματική ή ψυχολογική κακοποίηση μέσα στις οικογένειες τους,
- Πόλεμοι: Πολλά παιδιά είναι συχνά χωρισμένα από τους γονείς τους, ενώ άλλα τους χάνουν στο σκληρό περιβάλλον ενόπλων συγκρούσεων και πολεμικών γεγονότων και μένουν ορφανά και απροστάτευτα. Στο πλαίσιο αυτό καθίστανται ιδιαίτερα τρωτά στους εκμεταλλευτές. Είναι πολλές οι περιπτώσεις όπου έχουν αναφερθεί εξαφανίσεις παιδιών από

στρατόπεδα προσφύγων, τα οποία και αποτέλεσαν αντικείμενο εμπορικών συναλλαγών και μεταφέρθηκαν για να ριχθούν στην πορνεία,

- Υπερκαταναλωτισμός: Σε πολλές αναπτυγμένες χώρες κάποια παιδιά ωθούνται στην πορνεία, επιδιώκοντας μεγαλύτερα εισοδήματα με γρήγορους τρόπους. Αυτή την επιθυμία την δημιουργεί ο υπερκαταναλωτισμός, προσελκύει τα ανήλικα παιδιά και τα οδηγεί στο κύκλωμα της παιδικής πορνείας, αφού η επιδίωξη και ο στόχος τους είναι το άμεσο, υψηλό και γρήγορο κέρδος, με το οποίο θα μετέχουν σε απόλαυση αγαθών και υπηρεσιών πολυτελείας,
- Ανήλικα ορφανά παιδιά, λόγω ασθενειών και επιδημιών: Πρόκειται για εκατομμύρια παιδιά με καταγωγή από τριτοκοσμικές χώρες, ηλικίας κάτω των 15 ετών, που έχουν χάσει τον έναν ή και τους δύο γονείς τους από AIDS ή και άλλες αιτίες,
- Τα παιδιά των φαναριών: Τα άστεγα παιδιά που περιφέρονται και ζουν στους δρόμους, καταφεύγουν συχνά στην πορνεία προκειμένου να επιζήσουν, αφού τους αποφέρει υψηλές και εύκολες αποδοχές,
- Εθνοτικές-κοινωνικές διακρίσεις: Δεξαμενή άντλησης ανήλικων παιδιών για εκμετάλλευση, αποτελούν διάφορες εθνοτικές ομάδες και ιδίως μειοψηφίες οικονομικά ασθενέστερων στρωμάτων, με χαμηλό μορφωτικό επίπεδο, και περιορισμένη πρόσβασή στην εκπαίδευση και την εργασία.

Η *κυβερνό-τρομοκρατία* (cyber terrorism) αποτελεί την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υπερεθνικές ομάδες και μυστικούς πράκτορες. Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του. Με τη χρήση του λοιπόν οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Η ηλεκτρονική τρομοκρατία αφορά σε εκρηκτικά και σαμποτάζ, που αν και το περισσότερο από αυτό το υλικό είναι ήδη διαθέσιμο σε δημόσιες βιβλιοθήκες και βιβλιοπωλεία, η ευκολία με την οποία γίνεται προσβάσιμο διαμέσου των ηλεκτρονικών μέσων προσδίδει στο φαινόμενο απειλητικές διαστάσεις. Θεωρείται ως η μέγιστη απειλή στην εμπορική, οικονομική και πολιτική βιωσιμότητα του διαδικτύου. Τόσο στον

ηλεκτρονικό τύπο όσο και στον παραδοσιακό, κάνουν την εμφάνισή τους δημοσιεύματα που ασχολούνται με περιστατικά εκρήξεων και επιθέσεων, για τις οποίες οι δράστες απέκτησαν την αναγκαία ενημέρωση μέσω του διαδικτύου. Στις ΗΠΑ, Καναδά και Αυστραλία, μεταξύ άλλων χωρών, έχει παρατηρηθεί μια αυξητική τάση στην ηλεκτρονική τρομοκρατία, κυρίως δε όσον αφορά στις εκρήξεις (Νικολαΐδης, 1999, σ. 40-50; Λάζος, 2001, σ. 36-40; Καρακώστας, 2003, σ. 20-40; Ζάννη, 2005, σ. 78-85; Κριθαράς, 2009, σ. 50-70).

Σύμφωνα με τους Strassman and Marlow (1996) (από Ζαννή, 2005, σ. 78-85) η τρομοκρατία πληροφοριών μέσω του διαδικτύου, είναι ένα μοναδικό φαινόμενο στην ιστορία του εγκλήματος. Τα εγκλήματα πληροφοριών μπορούν να διαπραχθούν εύκολα χωρίς αποκάλυψη οποιονδήποτε αποδεικτικών στοιχείων. Η θέση αυτή εξηγεί και τους λόγους που χρησιμοποιείται το διαδίκτυο από τους τρομοκράτες. Ο Whine (2000) (από Ζαννή, 2005, σ. 78-85) θεωρεί ότι είναι τέσσερις: (i) Το διαδίκτυο παρέχει τη δυνατότητες αλληλεπίδρασης-επικοινωνία και δικτύωση, (ii). Το διαδίκτυο επιτρέπει την συγκεκαλυμμένη επικοινωνία και την ανωνυμία, πρακτικές που απαιτούνται για την επιτυχημένη δράση εξτρεμιστικών οργανώσεων, (iii). Ένας τρίτος λόγος χρησιμοποίησης του διαδικτύου είναι ότι αποτελεί ένα φτηνό μέσο επικοινωνίας. Η κατοχή ενός Η/Υ επιτρέπει σε έναν τρομοκράτη να γίνει φορέας στα εθνικά και παγκόσμια γεγονότα, με δεδομένο ότι γίνονται όλο και περισσότερο ανέξοδοι, η διάπραξη τρομοκρατικών πράξεων μέσω του διαδικτύου, θα γίνεται όλο και πιο εύκολη υπόθεση, και (iv). Το διαδίκτυο λειτουργεί ως πολλαπλασιαστής της δύναμης που διαθέτουν οι εξτρεμιστικές οργανώσεις, και ταυτόχρονα ως πολλαπλασιαστής της αμεσότητας επικοινωνίας.

Στην ηλεκτρονική τρομοκρατία εντάσσεται και η *προπαγάνδα μίσους* η οποία αναφέρεται σε εξευτελιστικό και υποτιμητικό περιεχόμενο που στρέφεται εναντίον συγκεκριμένων τάξεων ή ομάδων ανθρώπων. Ο πιο συνηθισμένος τύπος που παρουσιάζεται στο διαδίκτυο είναι η ρατσιστική προπαγάνδα, όπως νεοναζιστική και αντισημιτική. Εκτός από αυτόν όμως, δεν είναι ασυνήθιστη η εμφάνιση: (i). περιεχομένου με φανατικό θρησκευτικό χαρακτήρα, που προσβάλλει πιστούς άλλων θρησκειών, (ii) ομοφυλοφοβικού περιεχομένου, το οποίο προσβάλλει ειδικές μειονότητες με βάση τις σεξουαλικές τους προτιμήσεις, και (iii) περιεχομένου με ακραίο πολιτικό στίγμα, όπου γίνεται ευθεία πολεμική ενάντια σε πολιτικούς ή κρατικούς σχηματισμούς. Δεν είναι λίγες οι ανησυχίες που εγείρονται από αυτά τα είδη προπαγάνδας, αφού, συχνά, διαπιστώνονται προκλήσεις για γενοκτονίες και αντεκδικητικές δράσεις (Ζαννή, 2005, σ. 78-85).

Τέλος, μια μορφή ηλεκτρονικής τρομοκρατίας αποτελεί και ο *πολιτιστικός ιμπεριαλισμός*. Καθώς βρίσκεται σε καθεστώς ευρείας διαθεσιμότητας, μπορεί να προκαλεί την προσοχή και να επισκιάζει περιεχόμενα τοπικού χαρακτήρα. Το γεγονός και μόνον ότι ο κυβερνοχώρος είναι αγγλόφωνος προδιαθέτει για μια απώθηση των άλλων γλωσσών στην περιφέρεια της συνείδησης και μια αντικατάσταση τοπικών προϊόντων και θεσμών με προϊόντα και θεσμούς του δυτικού πολιτισμού. Ενδογενείς μορφές έκφρασης, τέχνης και τοπικές αξίες απειλούνται από την ανισομερή ανάπτυξη και προώθηση περιεχομένου με παγκοσμιοποιημένο χαρακτήρα. Πολύ περισσότερο, γίνονται κατανοητές οι ανησυχίες ορισμένων εθνών και κρατών που αντιμετωπίζουν την τηλεπικοινωνιακή επανάσταση ως βασικό μέσο μιας πιο εντατικής και επιθετικής προώθησης του πολιτισμού αναπτυγμένων χωρών στους τοπικούς πολιτισμούς (Ζαννή, 2005, σ. 78-85).

4. Νομοθετική προσέγγιση του ηλεκτρονικού εγκλήματος

Αποτελεί κοινό τόπο, ότι τόσο στην Ελλάδα όσο και σε άλλες χώρες του λεγομένου δυτικού κόσμου, οι νομοθετικές ρυθμίσεις που αφορούν τα ψηφιακά εγκλήματα παρουσιάζουν αδυναμίες. Η νομοθεσία λόγω της ιδιαίτερης φύσης του ηλεκτρονικού εγκλήματος πρέπει να ενημερώνεται συνεχώς για τις εξελίξεις στον τομέα της τεχνολογίας των Η/Υ, προκειμένου να μπορεί ανταποκριθεί στους τρόπους διάπραξης των σχετικών αξιόποινων πράξεων. Το ηλεκτρονικό έγκλημα αποτελεί επίσης, δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που δύναται να διώκονται ποινικά (Κιούπης, 1999, σ. 5, Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 12-21).

Η δίωξη του ηλεκτρονικού εγκλήματος εφόσον και οι καταγγελίες είναι περιορισμένη και κινείται σε χαμηλά επίπεδα. Οι επιχειρήσεις -κυρίως- αποφεύγουν να καταγγείλουν ηλεκτρονικές παραβάσεις, γιατί φοβούνται επανάληψη των αδικημάτων και πλήγμα στη φήμη τους. Επίσης, θέλουν να αποφεύγουν τα υψηλά δικαστικά έξοδα. Οι αστυνομικές και οι

δικαστικές αρχές αντιμετωπίζουν δυσκολίες στον εντοπισμό και την περαιτέρω δίωξη, γεγονός που σχετίζεται, κυρίως, με το χαμηλό επίπεδο πληροφορικής κατάρτισης των στελεχών τους. Ο διεθνής χαρακτήρας των συγκεκριμένων εγκλημάτων δίνει τη δυνατότητα στους δράστες να έχουν γρήγορη πρόσβαση σε συστήματα Η/Υ σε παγκόσμια κλίμακα. Τα ψηφιακά εγκλήματα -από νομική άποψη- χαρακτηρίζονται από τον μεγάλο όγκο των δεδομένων τους, τον μη οπτικό χαρακτήρα των αποδείξεων, τη δυνατότητα κάλυψης των ιχνών τους και την ταχεία εξαφάνιση των αποδεικτικών στοιχείων. Απαιτείται συνήθως αρκετός χρόνος, για να διευκρινιστούν οι υποθέσεις, που είναι συνήθως πολύπλοκες και απαιτούν συνεργασία και με άλλες υπηρεσίες. Πολλές φορές οι δικαστές υποβαθμίζουν τη σημασία των ψηφιακών εγκλημάτων, αφού οι ποινές που επιβάλλουν δεν είναι ικανές ώστε να τους αποτρέψουν από την επανάληψη της πράξης (Κιούπης, 1999, σ. 7).

Επιπρόσθετα, συχνά προκύπτει και πρόβλημα της δικαιοδοσίας, αφού είναι δύσκολο να ορισθεί ο τόπος τέλεσης του αδικήματος και η πιθανή αρμοδιότητα του δικαστηρίου που θα εκδικάσει την υπόθεση. Με δεδομένη όμως, την αύξηση των μορφών των ψηφιακών εγκλημάτων η ειδική και εξειδικευμένη νομοθετική αντιμετώπισή τους θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν παγκοσμίως έχουν θεσπιστεί νομοθετικές διατάξεις, σχετικές με τα ψηφιακά εγκλήματα. Ωστόσο, το νομοθετικό πλαίσιο που να αφορά ειδικότερα το ζήτημα είναι σε αρκετές περιπτώσεις εξαιρετικά ελλιπής και συνήθως γενικόλογος (Βελέντζας, 2008, σ. 33).

Στην Ευρωπαϊκή Ένωση ισχύουν: (i). Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της ομάδας των Οκτώ, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας, (ii). Το Ψήφισμα του Συμβουλίου με αριθμό 2003/C48/01, για την ασφάλεια των δικτύων και των πληροφοριών, (iii). Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής, (iv). Η κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων, (v). Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων, (vi). Το Έγγραφο με αριθμό 2000/C124/01 σχετικά με τη στρατηγική της ΕΕ για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο

έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος, και (vii). Το σχέδιο δράσης με αριθμό 97/C251/01 για την καταπολέμηση του οργανωμένου εγκλήματος (Βελέντζας, 2008, σ. 35-40).

Η "Σύμβαση για το Έγκλημα στον κυβερνοχώρο" με αντικείμενο την καταπολέμηση της εγκληματικής δραστηριότητας στους κόλπους του διαδικτύου, καταρτίστηκε στις 23/11/2001 στη Βουδαπέστη. Η Σύμβαση έως σήμερα έχει υπογραφεί από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου, καθώς και από τις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Νότια Αφρική. Ο βασικότερος σκοπός της εν λόγω σύμβασης είναι η εναρμόνιση των εθνικών νομοθεσιών των κρατών-μελών που έχουν υπογράψει, στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Επίσης, με τη σύμβαση παρέχεται το νομοθετικό πλαίσιο του δικονομικού δικαίου που είναι απαραίτητο για τη διερεύνηση και τη δίωξη των εγκλημάτων του κυβερνοχώρου. Με τη σύμβαση αυτή θέτονται οι βάσεις για μια αποτελεσματική συνεργασία για το ηλεκτρονικό έγκλημα (Βελέντζας, 2008, σ. 40).

4.1. Η Ελληνική νομοθεσία για το ηλεκτρονικό έγκλημα

Στην ελληνική νομοθεσία δεν υπάρχει ακόμη νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου. Στην Ελλάδα ισχύει ο νόμος 2928 του 2001 για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων, και αφορά τα εγκλήματα που διαπράττονται με Η/Υ και στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται σε περιβάλλον διαδικτύου. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της ΕΕ, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων (Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 25-30; Βελέντζας, 2008, σ. 45-47).

Η ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί έναν συνδυασμό διεθνών συνθηκών, συνταγματικών

διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών. Στο ΣτΕ, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι "ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας". Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της (Πίνακας 1) (Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 25-30; Βελέντζας, 2008, σ. 45-47).

Στον Ποινικού Κώδικα (ΠΚ) η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α,370Β και 370Γ. Τα άρθρα 370 και 370Α αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας, αντίστοιχα. Η ανάλογη εφαρμογή των διατάξεων αυτών στο χώρο του διαδικτύου, έχει προκαλέσει έντονο προβληματισμό στους νομικούς κύκλους, ιδιαίτερα όσον αφορά το άρθρο 370Α, το οποίο κατά πολλούς, θεωρείται ότι δεν μπορεί να τύχει εφαρμογής στο διαδίκτυο. Το άρθρο 370Β, παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα. Η πιο ουσιαστική διάταξη, όσον αφορά το χώρο του διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ. Το απόρρητο στην περίπτωση αυτή προστατεύεται υπό μια ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται το δικαίωμα του νόμιμου κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον Η/Υ του (Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 25-30; Βελέντζας, 2008, σ. 45-47).

Τα παραπάνω άρθρα του ΠΚ δεν είναι αρκετά για να καλύψουν τις ανάγκες δίωξης της ηλεκτρονικής εγκληματικότητας, η οποία παράλληλα πάντα με τις τεχνολογικές εξελίξεις εμφανίζεται με νέες μορφές. Άλλωστε στα συγκεκριμένα άρθρα δεν έχει προβλεφθεί η ύπαρξη του διαδικτύου το οποίο πλέον δίνει νέες διαστάσεις στο ζήτημα. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν με βάση την ισχύουσα Ελληνική νομοθεσία. Αυτό το κενό αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, εφόσον ο εικονικός κόσμος του

διαδικτύου θεωρηθεί απλά ως ένα ακόμα μέσο για τη διάπραξη εγκλημάτων (Πίνακας 1) (Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 25-30; Βελέντζας, 2008, σ. 45-47).

Πρόσφατα τέθηκε σε ισχύ το Π.Δ. 47/2005, από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ) το οποίο αφορά και διευκρινίζει τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του. Σύμφωνα με το άρθρο 370Β: *1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους, 2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους, 3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147 και 4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.*

Βάσει του άρθρου 370Γ: *1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) € έως πέντε χιλιάδων εννιακοσίων (5.900) €, 2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα €. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148, 3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του και 4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.*

Τέλος, βάσει του άρθρου 386^{Α}, που άφορα τις απάτες με υπολογιστή: *Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή*

ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

Πίνακας 1. Η νομοθεσία που αφορά το ηλεκτρονικό έγκλημα.

ΑΡΘΡΑ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ

- Άρθρο 337 - Προσβολή της γενετήσιας αξιοπρέπειας
- Άρθρο 348 - Διευκόλυνση ακολασίας άλλων
- Άρθρο 348Α - Πορνογραφία ανηλίκων
- Άρθρο 348Β - Προσέλκυση παιδιών για γενετήσιους λόγους
- Άρθρο 370Α- Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
- Άρθρο 370Β- Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.
- Άρθρο 370Γ- Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.
- Άρθρο 386Α-Απάτη με υπολογιστή

ΝΟΜΟΙ

- Ν. 2472/1997- «Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (ενσωματωμένες τροποποιήσεις)
- Ν. 2867/2000- «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και άλλες διατάξεις»
- Ν. 2819/2000- «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»
- Ν. 3115/2003-«Αρχή Διασφάλισης του απορρήτου των επικοινωνιών»
- Ν. 3431/2006-«Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»
- Ν. 3471/2006-«Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997»
- Ν. 3917/2011-«Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»

ΠΡΟΕΔΡΙΚΑ ΔΙΑΤΑΓΜΑΤΑ

- Π.Δ. 131/2003-«Ηλεκτρονικό εμπόριο κ.λπ. Υπηρεσίες της Κοινωνίας της

Πληροφορίας»

- Π.Δ. 150/2001-«Ηλεκτρονικές Υπογραφές»
- Π.Δ. 47/2005 – «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του»

ΟΔΗΓΙΕΣ ΕΥΡΩΠΑΪΚΗΣ ΈΝΩΣΗΣ

- Οδηγία 87/102/ΕΟΚ του Συμβουλίου της 22ας Δεκεμβρίου 1986 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
- Οδηγία 90/88/ΕΟΚ του Συμβουλίου της 22ας Φεβρουαρίου 1990 για την τροποποίηση της οδηγίας 87/102/ΕΟΚ για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη
- Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (ONP)
- Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών
- Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών
- Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων
- Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις
- Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές
- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά-Οδηγία για το ηλεκτρονικό εμπόριο
- Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους -Οδηγία για την πρόσβαση
- Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την δανειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών -Οδηγία για την δανειοδότηση
- Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών -Οδηγία πλαίσιο
- Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών -Οδηγία καθολικής υπηρεσίας
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών - Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

- Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών

ΔΙΕΘΝΕΙΣ ΣΥΜΒΑΣΕΙΣ

- Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας
- Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001
- Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948
- Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ)

ΑΠΟΦΑΣΕΙΣ

- Η ΥΑ με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».
- Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002-«Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου με κατάληξη .g»
- Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002-«Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»

Συμπληρωματικά, τελευταία έχουν πραγματοποιηθεί συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως, με σκοπό τη συζήτηση και τη λήψη αποφάσεων, σχετικά με το ζήτημα αυτό. Συγκεκριμένα, πραγματοποιήθηκε συνέδριο για το ηλεκτρονικό έγκλημα στη Βουδαπέστη και υπογράφτηκε συνθήκη, στις 23/11/2001, στην οποία εντάσσονται όλα τα σχετικά συμπεράσματα. Αυτή περιλαμβάνει ορισμούς και ρυθμίσεις για όλες τις μορφές των ψηφιακών εγκλημάτων και είναι γνωστή ως “Convention on Cyber Crime 2001”. Στην Ελλάδα δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Internet και ειδικότερα να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από την πλευρά του ποινικού δικαίου. Ο νόμος 1805/1988 αφορά εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές. Συγκεκριμένα, με το άρθρο 3 του νόμου αυτού προστέθηκαν τρία νέα άρθρα στον Ποινικό Κώδικα, τα 370Β, 370Γ και 386Α (Καϊάφα-Γκμπάντι & Συμεωνίδου-Καστανίδου, 2004, σ. 25-30; Βελέντζας, 2008, σ. 45-47).

4.2. Δίκτυα υπολογιστών και νομοθεσία

Η ασφάλεια των πληροφοριακών συστημάτων και ειδικότερα των δικτύων υπολογιστών μιας επιχείρησης είναι μία υποχρέωση που δεν αφορά μόνο την προστασία της επιχείρησης, αλλά και την προστασία των προσώπων, στοιχεία των οποίων έχουν καταχωριστεί στα συστήματα αυτά. Ο νόμος Ν 2472/97 (άρθρο 10) έχει επιβάλει υποχρεώσεις προστασίας της εμπιστευτικότητας-μυστικότητας των πληροφοριών και λήψης μέτρων ασφαλείας. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα ασφαλείας που λαμβάνονται θα πρέπει να είναι ανάλογα προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων

που είναι αντικείμενο της επεξεργασίας. Στις υποχρεώσεις μιας επιχείρησης περιλαμβάνεται η επιλογή συνεργατών που διαθέτουν όχι μόνο τεχνικές γνώσεις αλλά και προσωπική ακεραιότητα που διασφαλίζει την τήρηση του απορρήτου της επεξεργασίας (Μαγκάκης, 1984, σ. 100-120).

Οι άδειες επεξεργασίας ευαίσθητων δεδομένων συνοδεύονται από την επιβολή όρων ασφαλείας των δεδομένων και την υποχρέωση επεξεργασίας τέτοιων σχεδίων. Χωρίς να υπεισέρχεται σε λεπτομέρειες, η Αρχή Προστασίας Προσωπικών Δεδομένων έχει συντάξει ένα κείμενο οδηγιών, όπου αναφέρεται το βασικό περιεχόμενο των σχεδίων ασφαλείας και εκτάκτου ανάγκης, ώστε αυτά να κρίνονται επαρκή από την άποψη της προστασίας της εμπιστευτικότητας. Η συγκέντρωση και επεξεργασία ηλεκτρονικών και μη δεδομένων αντιμετωπίστηκε από νωρίς και συνεχίζει να αντιμετωπίζεται ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική ζωή. Η υπάρχουσα νομοθεσία παρέχει επαρκή προστασία στους πολίτες αλλά με την πάροδο του χρόνου και την περαιτέρω ανάπτυξη της τεχνολογίας χρειάζονται ειδικότερες διατάξεις που θα αντικαταστήσουν τις γενικές και από τις οποίες θα προκύπτει με σαφήνεια ποιος, πότε ακριβώς, σε ποια δεδομένα και με ποιο σκοπό θα έχει δικαίωμα πρόσβασης και επεξεργασίας. Στην προσπάθεια του Ελληνικού κράτους για εξασφάλιση υψηλού βαθμού εμπιστευτικότητας των πολιτών στις νέες τεχνολογίες επικοινωνιών είτε μέσω υπολογιστών είτε μέσω άλλων τηλεπικοινωνιακών μέσων, έχουν ιδρυθεί δύο αρχές προστασίας που σχετίζονται με τα προσωπικά δεδομένα, η Αρχή Προστασίας Προσωπικών Δεδομένων και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Μαγκάκης, 1984, σ. 100-120).

Η αρχή προστασίας προσωπικών δεδομένων (ΑΠΠΔ): Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο. Η αρχή αυτή έχει ποικίλες αρμοδιότητες μεταξύ των οποίων είναι να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Οι σημαντικότερες οδηγίες της ΑΠΠΔ είναι: (i). Η οδηγία 1122.2000 για τα κλειστά κυκλώματα τηλεόρασης και η οδηγία 115/2001 για την επεξεργασία των δεδομένων (Μαγκάκης, 1984, σ. 100-120).

Οι σπουδαιότερες αποφάσεις της ΑΠΠΔ είναι οι εξής (Μαγκάκης, 1984, σ. 100-120): (i). Η απόφαση 50/2000 σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας, (ii). Η απόφαση 120/2001 για την επεξεργασία

προσωπικών δεδομένων σχετικά την παροχή υπηρεσιών καρτοκινητής τηλεφωνίας, (iii). Η απόφαση 1469.2000 για τη συλλογή προσωπικών δεδομένων από εταιρείες τηλεπικοινωνιακών δραστηριοτήτων, (iv). Η απόφαση 147/2001 για την χρήση ευαίσθητων δεδομένων ενώπιον δικαστηρίου και (v). Η απόφαση 8/2003 σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

Η *αρχή διασφάλισης του απορρήτου των επικοινωνιών (ΑΔΑΕ)* προβλέπεται από το Ν.3115/2003. Είναι ανεξάρτητη αρχή με διοικητική αυτοτέλεια και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στο πλαίσιο αυτό, η ΑΔΑΕ είναι η αρμόδια αρχή για τον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Η δράση της διέπεται πάντοτε από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας. Η ΑΔΑΕ αποτελείται από 7 μέλη και ισάριθμα αναπληρωματικά, τα οποία απολαμβάνουν κατά την άσκηση των καθηκόντων τους πλήρη προσωπική και λειτουργική ανεξαρτησία. Ωστόσο, έχουν καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την αποχώρησή τους. Τα πρόσωπα που θα γίνουν μέλη της ΑΔΑΕ, επιλέγονται από τη Βουλή και πρέπει να τυγχάνουν ευρείας κοινωνικής αποδοχής και να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στο νομικό τομέα ή στον τεχνικό τομέα των επικοινωνιών.

Η ΑΔΑΕ στο πλαίσιο εκπλήρωσης του σκοπού της, μπορεί να (Μαγκάκης, 1984, σ. 100-120):

- Διενεργεί αυτεπαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- Καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.
- Συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.
- Γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

- Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., για να διαπιστώσουν παράβαση της νομοθεσίας για την προστασία του απορρήτου, μπορούν να ελέγχουν τα βιβλία και στοιχεία των ελεγχόμενων υπηρεσιών, οργανισμών και επιχειρήσεων, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν. Επιπλέον, έχουν δικαίωμα να ενεργούν έρευνες στα γραφεία και τις λοιπές εγκαταστάσεις των ελεγχόμενων και να διενεργούν ένορκες και μη καταθέσεις, με την επιφύλαξη του επαγγελματικού απορρήτου των εξεταζόμενων προσώπων.
- Σε περίπτωση που κατά τον έλεγχο διαπιστωθεί παραβίαση του απορρήτου, τα μέλη της Α.Δ.Α.Ε. μπορούν να κατασχέσουν τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφουν τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. Για τα μέσα που κατάσχονται, ορίζεται μεσεγγυούχος ωσότου αποφανθούν τα αρμόδια δικαστήρια.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Ε.Τ.) αποτελεί σημαντική αρχή στο χώρο του διαδικτύου καθώς αποτελεί την εθνική ρυθμιστική αρχή σε θέματα τηλεπικοινωνιών. Υποχρεούνται στην τήρηση εμπιστευτικότητας, εμπορικών πληροφοριών για τέσσερα χρόνια μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Ε.Τ. . Η Ε.Ε.Ε.Τ. χορηγεί άδειες σε Πάροχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's), ενώ ρυθμίζει τον τομέα των τηλεπικοινωνιών, ασκώντας παράλληλα και έλεγχο σε αυτό, και εποπτεύεται την τηλεπικοινωνιακή αγορά.

4.3. Παραβάσεις νομοθεσίας περί ασφάλειας δικτύων

Η τήρηση των απαγορεύσεων που σχετίζονται με την επεξεργασία αλλά και την ασφάλεια των προσωπικών δεδομένων επιβάλλεται από την οικεία νομοθεσία. Τυχόν παράβαση των απαγορεύσεων για προστασία και ασφάλεια των δεδομένων ενδέχεται να έχει ως αποτέλεσμα την επιβολή διοικητικών κυρώσεων από την ΑΠΠΔ (πρόστιμα, αναστολή επεξεργασίας και καταστροφή αρχείων) ή/και τη έγερση αξιώσεων και υποχρεώσεων αποζημίωσης ή χρηματικής ικανοποίησης των προσώπων που θίγονται από τις παραβάσεις των νομοθετικών διατάξεων και των υποχρεώσεων ασφαλείας. Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με

ποινή φυλάκισης τουλάχιστον ενός έτους και χρηματική ποινή από 15000-60000€. Σε περίπτωση που ο παραβάτης ανήκει στο προσωπικό υπηρεσίας, οργανισμού, νομικού προσώπου ή επιχείρησης που ασχολείται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση ή την επικοινωνία, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον 2 ετών και η χρηματική ποινή τουλάχιστον 30000 € (Μαγκάκης, 1984, σ. 100-120).

Πίνακας 2. Οι Ελληνικές δικαστικές αποφάσεις που αφορούν το ηλεκτρονικό έγκλημα.

ΑΡΘΡΑ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ
• Η 1129.2001 του Μον.Πρωτ.Τρ. σχετικά με την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα • Η 1988.2002 του Μον.Πρωτ.Αθ. σχετικά με την πώληση προϊόντων εξ αποστάσεως και την παράνομη αποστολή διαφημιστικών εντύπων • Η 2950.2002 του Μον.Πρωτ.Θεσ. σχετικά με την δωσιδικία νομικού προσώπου σε υπόθεση επεξεργασία δεδομένων προσωπικού χαρακτήρα • Η 2279.2001 του ΣτΕ σχετικά με την σύσταση της ΑΠΔΠ χαρακτήρα • Η 2286.2001 του ΣτΕ σχετικά με την άσκηση αίτησης ακυρώσεως κατά πράξης της ΑΠΠΔ από πολιτικό κόμμα • Η 984.2001 του Συμβουλίου Εφετών για την παράνομη γνώση, αλλοίωση και ανακοίνωση ευαίσθητων προσωπικών δεδομένων • Η 3545/2002 του ΣτΕ σχετικά με την συμμετοχή σε συνεδρίαση της ΑΠΠΔ αναπληρωματικού μέλους της, στο οποίο έχουν ανατεθεί καθήκοντα εισηγητή.

Συγκεκριμένες παραβάσεις συνιστούν μάλιστα ποινικά αδικήματα και επισύρουν και ποινικές κυρώσεις. Την μεγαλύτερη κύρωση δε αποτελεί η δυσπιστία των συναλλασσόμενων, αφού πολλοί απέχουν από ηλεκτρονικές συναλλαγές λόγω φόβου για τη μεταχείριση και την τύχη των προσωπικών τους δεδομένων. Η επένδυση σε τεχνολογίες ενίσχυσης της ιδιωτικότητας, η ύπαρξη, τήρηση και διαφήμιση πολιτικών για την προστασία της ιδιωτικότητας δεν είναι απλά συμμόρφωση προς τους νόμους. Είναι ανταγωνιστικό πλεονέκτημα και προϋπόθεση για να αποκτηθεί η εμπιστοσύνη των καταναλωτών (Μαγκάκης, 1984, σ. 100-120).

Εκτός από την ελληνική δικαιοσύνη και την ΑΠΠΔ που επιβάλει κυρώσεις σε περιπτώσεις άρσης του απορρήτου στην επικοινωνία μέσω τηλεπικοινωνιακών δικτύων ή δικτύων υπολογιστών, και η Αρχή Διατήρησης της Ακεραιότητας των Επικοινωνιών (ΑΔΑΕ) μπορεί

να επιβάλει διοικητικές κυρώσεις στους παραβάτες. Η απόφασή της πρέπει να είναι πλήρως αιτιολογημένη και ύστερα από προηγούμενη κλήτευση και ακρόαση του -φερόμενου ως- υπαιτίου, ο οποίος μπορεί να παραστεί μετά ή διά πληρεξουσίου δικηγόρου, εκτός αν διαταχτεί η αυτοπρόσωπη παρουσία του. Οι διοικητικές κυρώσεις που μπορεί να επιβάλει η ΑΔΑΕ είναι (Μαγκάκης, 1984, σ. 100-120):

- Σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής του παραβάτη, και
- Πρόστιμο από 15000-1500000 €.

Παράλληλα με τα παραπάνω νομοθετήματα και την δραστηριότητα των ΑΠΠΔ και ΑΔΑΕ οι πολίτες που γίνονται υποκείμενα επεξεργασίας προσωπικών δεδομένων προστατεύονται και από τα δικαστήρια. Πληθώρα δικαστικών αποφάσεων, ελληνικών και ξένων, αναφέρονται και ρυθμίζουν κάθε είδους διαφορά που ανακύπτει σχετικά με την επεξεργασία προσωπικών δεδομένων (Πίνακας 2) (Μαγκάκης, 1984, σ. 100-120).

4.4. Η δικαιοδοσία στο διαδίκτυο

Η δικαιοδοσία στα εγκλήματα που τελούνται στο διαδίκτυο είναι πολύπλοκο εξαιτίας της παγκοσμιότητας του. Η δικαιοδοσία αποτελεί την αρμοδιότητα ενός δικαστηρίου να δικάσει μια συγκεκριμένη υπόθεση αλλά συγχρόνως και η αντίστοιχη αρμοδιότητα των διωκτικών αρχών να διερευνήσουν μια εγκληματική συμπεριφορά. Η αρμοδιότητα του δικαστηρίου είναι συνυφασμένη με τον καθορισμό του τόπου τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τέλεσης του αδικήματος υποστηρίζονται τέσσερις θεωρίες (Bigelow, 1985, σ. 3-5):

- Η θεωρία του τόπου του αποτελέσματος: Τόπος τέλεσης του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
- Η θεωρία του τόπου ενέργειας: Ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου έχει τελεστεί η ενέργεια που έτεινε στο άδικο αποτέλεσμα.
- Η μικτή θεωρία: Τόπος τέλεσης του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.
- Η θεωρία του βαρύνοντος τόπου: Ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Όμως υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας καθώς είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας. Η επικρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του βαρύνοντος τόπου.

Κυρίαρχο νομικό ζήτημα για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, αποτελεί η νομική ρύθμιση του διαδικτύου. Έως σήμερα, δεν υπάρχουν συγκεκριμένες διατάξεις που να ρυθμίζουν συνολικά τις προσφερόμενες -μέσω του διαδικτύου- υπηρεσίες. Επιπλέον, οποιαδήποτε προσπάθεια ρύθμισης, συναντά φραγμούς, που ανάγονται στις απόψεις δύο αντιμαχόμενων παρατάξεων: αυτών που είναι υπέρ και αυτών που είναι κατά της οποιασδήποτε προσπάθειας ρύθμισης του διαδικτύου (Ζάννη, 2005, σ. 100-105). Τα επιχειρήματα υπέρ της ρύθμισης του διαδικτύου είναι τα ακόλουθα (Ζάννη, 2005, σ. 100-105):

- Είναι ανοιχτό σε όλους και απαιτείται η ρύθμισή του για τον έλεγχο του παράνομου περιεχομένου του,
- Δεν αποτελεί διαφορετικό μέσο επικοινωνίας, σε σχέση με τα ΜΜΕ τα οποία υπόκεινται ήδη σε νομοθετικές ρυθμίσεις,
- Υπάρχει πληθώρα επιβλαβούς υλικού σε αυτό, όπως και αυξανόμενη εγκληματική δραστηριότητα, που δημιουργεί την υποχρέωση της πολιτείας για τον έλεγχο και την αντιμετώπισή της,
- Οι περισσότεροι χρήστες, απαιτούν κάποια μορφή ρύθμισης για την προστασία των δεδομένων τους και των περιουσιακών δικαιωμάτων τους, έναντι επιθέσεων κακόβουλων χρηστών.

Τα επιχειρήματα εναντίον οποιασδήποτε μορφής ρύθμισης συνοψίζονται στα ακόλουθα (Ζάννη, 2005, σ. 100-105):

- Η ελευθερία του λόγου που προσφέρεται μέσω του διαδικτύου είναι απόλυτο δικαίωμα κάθε πολίτη, προστατευόμενο από συνταγματικές διατάξεις,
- Το διαδίκτυο είναι διαφορετικό από τα άλλα μέσα επικοινωνίας, διαθέτοντας ιδιαίτερα χαρακτηριστικά όπως η ελευθερία, η ειλικρίνεια και ο πειραματισμός,
- Το διαδίκτυο δεν μπορεί να ρυθμιστεί, διότι είναι τεράστιο και παγκόσμιο και οποιαδήποτε προσπάθεια, θα έρχεται πάντοτε αντιμέτωπη με το ζήτημα της λογοκρισίας,
- Οι γονείς είναι υπεύθυνοι για να προστατεύσουν τα παιδιά από το παράνομο περιεχόμενο του διαδικτύου και όχι τα κράτη με νομοθετικές ρυθμίσεις.

5. Διαδίκτυο και ασφάλεια

Με τη χρήση ενός δικτύου, είναι εύκολο για δύο ή περισσότερους ανθρώπους, που βρίσκονται σε μεγάλη απόσταση μεταξύ τους να γράψουν μια αναφορά μαζί. Όταν ένας εργαζόμενος πραγματοποιεί μια αλλαγή σε ένα on-line κείμενο οι άλλοι μπορούν να δουν αμέσως την αλλαγή αυτή αντί να περιμένουν αρκετές μέρες για μια επιστολή. Η πρόσβαση σε απομακρυσμένες πληροφορίες είναι πολυμορφική. Μια περιοχή στην οποία ήδη συμβαίνει είναι η πρόσβαση σε τραπεζικούς οργανισμούς. Πολλοί άνθρωποι πληρώνουν τα χρέη τους,

διαχειρίζονται τους τραπεζικούς τους λογαριασμούς και τις επενδύσεις τους ηλεκτρονικά. Οι αγορές από το σπίτι έχουν γίνει δημοφιλείς, με τη δυνατότητα να ανατρέχει κανείς σε on-line καταλόγους χιλιάδων εταιριών. Μια άλλη καινοτομία στα δίκτυα υπολογιστών αποτελεί ο παγκόσμιος ιστός που περιέχει πληροφορίες για τις τέχνες, τις επιχειρήσεις, την κυβέρνηση, την υγεία, την ιστορία, τη διασκέδαση, τις επιστήμες, τα ταξίδια και ένα σωρό άλλα θέματα. Επίσης το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται ήδη από εκατομμύρια ανθρώπων και μεταφέρει εκτός του κειμένου, εικόνα και ήχο (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

Είναι ολοφάνερο ότι το να κάνει κάποιος ένα δίκτυο ασφαλές είναι πολύ πιο απαιτητικό από το να το προστατεύει από λάθη προγραμματισμού. Απαιτεί το να ξεγελάσει κανείς τους συχνά ευφυείς, αφοσιωμένους και μερικές φορές καλά χρηματοδοτημένους αντιπάλους. Είναι επίσης προφανές ότι τα μέτρα που θα σταματήσουν τους περιστασιακούς αντιπάλους θα ασκήσουν λίγη επίδραση στους σοβαρούς. Για το λόγο αυτό, επειδή η δημιουργία ενός ασφαλούς δικτύου φαντάζει ουτοπική, θα πρέπει να υπάρχει πρόληψη για την έγκαιρη ανίχνευση των επιθέσεων από κακόβουλους χρήστες του δικτύου. Συμπεραίνουμε λοιπόν πως το δίκτυο μας θα πρέπει να είναι εφοδιασμένο με ένα εργαλείο ανίχνευσης επιθέσεων. Το εργαλείο αυτό θα πρέπει να είναι σε θέση να ειδοποιεί τον διαχειριστή ασφάλειας του δικτύου όταν γίνεται κάποια επίθεση, προκειμένου αυτός να προσπαθήσει να την αντιμετωπίσει προστατεύοντας το στόχο της επίθεσης (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

5.1. Βασικές αρχές ασφαλείας

Οι στόχοι μιας υλοποίησης ασφαλείας υπολογιστών συνήθως συνοψίζονται σε τρεις έννοιες, γνωστές με το αρκτικόλεξο CIA (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38):

- Εμπιστευτικότητα: Η αρχή του εμπιστευτικότητας (confidentiality) προστατεύει ευαίσθητη πληροφορία από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή της.

- Ακεραιότητα: Η αρχή του ακεραιότητα (integrity) εξασφαλίζει ότι η πληροφορία ή το λογισμικό είναι πλήρες, σωστό και αυθεντικό, με άλλα λόγια ότι δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο.
- Διαθεσιμότητα: Η αρχή του διαθεσιμότητας (availability) εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι προσπελάσιμες και λειτουργικές, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος για πρόσβαση σε αυτές.

Με την αρχή αυτή σχετίζεται και η έννοια της εμπιστοσύνης. Η εμπιστοσύνη έχει να κάνει με το κατά πόσο μπορεί κάποιος χρήστης να εμπιστεύεται ένα υπολογιστικό σύστημα και να είναι εφησυχασμένος ότι το σύστημα κάνει αυτό που ισχυρίζεται και όχι κάποια άλλη ανεπιθύμητη ενέργεια. Διαφορετικά συστήματα, που εξυπηρετούν διαφορετικούς σκοπούς, ρίχνουν μεγαλύτερο βάρος σε κάποια από τις τρεις αυτές αρχές.

Η αρχή του confidentiality (εμπιστευτικότητας) προστατεύει ευαίσθητη πληροφορία από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή της. Συνήθως χρησιμοποιείται κρυπτογράφηση και έλεγχος πρόσβασης, για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων. Η προσπάθεια που θα καταβληθεί για να εξασφαλιστεί η εμπιστευτικότητα των δεδομένων εξαρτάται από το πόσο ευαίσθητα είναι τα δεδομένα του. Υπάρχουν διάφορες εφαρμογές παρέχουν κρυπτογράφηση από άκρο σε άκρο, ωστόσο σε μια τέτοια περίπτωση υπάρχει το μειονέκτημα ότι καθένα από τα άκρα θα πρέπει να υποστηρίζει το ίδιο πρωτόκολλο κρυπτογράφησης (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38), όπως:

- Τα *Ιδεατά Ιδιωτικά Δίκτυα* (VPNs), μπορούν να χρησιμοποιηθούν ως εναλλακτική λύση για δημιουργία ενός ασφαλούς καναλιού επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων.
- *Κρυπτογραφία σε επίπεδο συνδέσμου μετάδοσης δεδομένων του μοντέλου OSI*, ωστόσο είναι δύσκολο στην εφαρμογή του, καθώς απαιτεί κάθε ενδιάμεση συσκευή δικτύωσης στο μονοπάτι επικοινωνίας να συμμετέχει στην κρυπτογράφηση.
- *Προστασία με φυσικά μέσα* εφαρμόζεται παράλληλα για να περιορίσει την μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά κέντρα ή σε μέρη όπου υπάρχει δικτυακός εξοπλισμός.

Η αρχή του integrity (ακεραιότητα) εξασφαλίζει ότι η πληροφορία δεν έχει υποστεί κάποια αλλαγή με κάποιον παράνομο τρόπο κατά την μεταφορά της από τον αποστολέα στον παραλήπτη της. Προστατεύουμε την πληροφορία για να μην τροποποιηθεί από χρήστες ή εφαρμογές που δεν είναι εξουσιοδοτημένες να πράξουν κάτι τέτοιο, ή από χρήστες που είναι

μεν εξουσιοδοτημένοι για προσπέλαση, αλλά τα δικαιώματά τους δεν τους επιτρέπουν να πραγματοποιήσουν καμιά τροποποίηση σε αυτήν. Για να ικανοποιείται η ακεραιότητα των δεδομένων πρέπει να εξασφαλίζεται ότι κάθε μήνυμα που φτάνει σε έναν παραλήπτη είναι αναλλοίωτο σε σχέση με αυτό που έφυγε από τον αποστολέα. Το περιεχόμενο του μηνύματος πρέπει να είναι πλήρες και να μην έχει υποστεί καμιά αλλαγή σε κάποιον ενδιάμεσο κόμβο του δικτύου (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

Η ακεραιότητα μιας σύνδεσης μπορεί να εξασφαλιστεί με χρήση κρυπτογραφίας και έλεγχο δρομολόγησης. Ισχυρές μέθοδοι εξασφάλισης της ακεραιότητας υπάρχουν όταν γίνεται χρήση hash συναρτήσεων, όπως ο αλγόριθμος MD5 ή SHA. Η ακεραιότητα επεκτείνεται και στο λογισμικό των δικτυακών συσκευών, μέσω των οποίων μεταφέρονται δεδομένα. Το λογισμικό πρέπει να πιστοποιείται ώστε να εξασφαλίζεται η προέλευσή του και η ορθή μεταφορά του στην κάθε συσκευή. Όταν το λογισμικό εγκατασταθεί σε κάποια συσκευή πρέπει να πιστοποιείται ότι το checksum που επιστρέφει το λογισμικό με αυτό που δίνει η εταιρία για το λογισμικό αυτό. Έτσι εξασφαλίζεται η ορθή μεταφορά και εγκατάσταση του στην κάθε συσκευή (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

Η αρχή της διαθεσιμότητας εξασφαλίζει ότι η πληροφορία ή οι υπηρεσίες είναι προσπελάσιμες και λειτουργικές, όταν ζητηθούν από κάποιον ο οποίος είναι εξουσιοδοτημένος για πρόσβαση σε αυτές. Η ανοχή σε σφάλματα, ο πλεονασμός, τα εφεδρικά αντίγραφα, οι διαδικασίας ανάκτησης, η ανθεκτικότητα και η εξισορρόπηση φορτίου είναι σχεδιαστικές αρχές του δικτύου, οι οποίες χρησιμοποιούνται για να εξασφαλιστεί η διαθεσιμότητα. Αν τα συστήματα δεν είναι διαθέσιμα όταν πρέπει, τότε οι έννοιες εμπιστευτικότητα και ακεραιότητα δεν έχουν καμιά απολύτως σημασία (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

Εκτός της προαναφερόμενης *τριάδας αρχών CIA*, υπάρχει μια πληθώρα από αρχές ασφαλείας οι οποίες πρέπει οπωσδήποτε να λαμβάνονται υπ' όψιν κατά το σχεδιασμό ή την υλοποίηση ενός πλάνου ασφαλείας. Οι βασικότερες από τις αρχές αυτές είναι: η ιδιωτικότητα, η πιστοποίηση, η εξουσιοδότηση και η υπευθυνότητα (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

Η αρχή της ιδιωτικότητας εξασφαλίζει πως η πληροφορία που ανταλλάσσεται μεταξύ των χρηστών παραμένει απόρρητη και είναι εμφανής μόνο στους νόμιμους χρήστες. Για να είναι ένα δίκτυο υπολογιστών ασφαλές, πρέπει να εξασφαλίζεται πως κανένας κακόβουλος ενδιάμεσος χρήστης δεν μπορεί να δει την πληροφορία που διακινείται πάνω στο δίκτυο. Το

να εμποδίζεται η αλλοίωση των δεδομένων είναι οπωσδήποτε κρίσιμο σε ένα δίκτυο, ωστόσο αυτό δεν αρκεί. Για να μπορεί κάποιος να ισχυρισθεί πως είναι ασφαλής, θα πρέπει να εξασφαλίζεται και το απόρρητο της επικοινωνίας (Γκρίτζαλης κ.α., 2003, σ. 21-25; Κάτσικας κ.α., 2004, σ. 35-38).

5.2. Βασικά προληπτικά εργαλεία

Η διασπορά ιών είναι μια από τις πιο διαδεδομένες μορφές επίθεσης στο διαδίκτυο. Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους. Ένα τέτοιο πρόγραμμα που πρέπει να είναι εγκατεστημένο σε κάθε Η/Υ, επιτελεί τρείς βασικές λειτουργίες. Αυτές είναι (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65):

(i). Ανίχνευση των ιών, που πραγματοποιείται κατόπιν ενέργειας του χρήστη ή μπορεί να γίνεται και αυτόματα.

(ii). Προσδιορισμός ταυτότητας ιών που στην περίπτωση που το σύστημα έχει προσβληθεί από κάποιον ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητα του.

(iii). Καθαρισμός των ιών, που αφού έχει προηγηθεί ο εντοπισμός του ιού, ακολουθεί η αφαίρεσή του. Το λογισμικό antivirus επιδιορθώνει το μολυσμένο από τον ιό αρχείο ή ακόμα μπορεί και να το διαγράψει.

Ακολουθεί η πιστοποίηση της ταυτότητας ενός χρήστη με τη δημιουργία και η χρήση συνθηματικών λέξεων ή συμβόλων. Έτσι το όνομα χρήστη (user ID) και ο κωδικός πρόσβασης (password) είναι απαραίτητα στοιχεία προκειμένου να επιτραπεί η είσοδος του εξουσιοδοτημένου χρήστη στο σύστημα. Στην επιστήμη των Η/Υ ο όρος τείχος προστασίας (firewall) χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Η κύρια λειτουργία ενός τείχος προστασίας είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα τείχος προστασίας παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Στο διαδίκτυο πρέπει να υπάρχει μικρός βαθμό εμπιστοσύνης, οπότε ο σκοπός της τοποθέτησης ενός τείχους προστασίας είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπιση τους. Η σωστή πρακτική είναι το τείχος προστασίας να ρυθμίζεται έτσι ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου. Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μια ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το τείχος προστασίας ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει. Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65).

Τα τείχη προστασίας δρουν ως εμπόδια ανάμεσα στο διαδίκτυο και στο εσωτερικό δίκτυο ή έναν Η/Υ και σταματάει διάφορους κινδύνους και επιθέσεις, συμπεριλαμβανομένων και ορισμένων ιών. Το τείχος προστασίας μπορεί να είναι λογισμικό που τρέχει σε έναν Η/Υ, λογισμικό που προστατεύει το δίκτυο ή συσκευή hardware συνδεμένη στο δίκτυο. Το τείχος προστασίας φιλτράρει την πληροφορία που εισέρχεται στο δίκτυο ή εξέρχεται από αυτό, με

βάση κανόνες τους οποίους έχουμε θέσει. Με τον τρόπο αυτό προστατεύεται το δίκτυο από εισβολείς. Επιπλέον, απαγορεύεται η αποστολή πληροφορίας από τους υπολογιστές του δικτύου, όπως π.χ. ποιοι τύποι αρχείων επιτρέπεται να αποστέλλονται (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65).

Στα μειονεκτήματα των τειχών προστασίας λογίζονται το υψηλό οικονομικό κόστος, η δυσκολία να ρυθμιστούν με τρόπο αποτελεσματικό για την εκπλήρωση της αποστολής τους και τέλος το γεγονός ότι η προστασία που παρέχουν είναι εντελώς σχετική. Ένας σημαντικός τρόπος για προστασία από πολλά είδη επιθέσεων είναι η σχεδίαση της τοπολογίας του δικτύου ώστε να είναι δύσκολο να γίνει εισβολή. Ένα τείχος προστασίας είναι ένα επιπλέον επίπεδο προστασίας τοποθετημένο γύρω από ένα δίκτυο ή από μια συγκεκριμένη εφαρμογή. Ένα τείχος προστασίας που προστατεύει ένα δίκτυο θα περιλαμβάνει συνήθως ένα δρομολογητή που μπορεί να προγραμματιστεί ώστε να μην επιτρέπει επιλεκτικά την πρόσβαση σε ένα δίκτυο, για παράδειγμα θα απορρίπτει πακέτα που δεν στέλνονται σε συγκεκριμένες επιτρεπόμενες θύρες. Όταν ένα πακέτο φτάνει στον δρομολογητή του τείχους προστασίας, αυτός το επεξεργάζεται και αποφασίσει αν θα το αφήσει να περάσει στο δίκτυο που προστατεύει ή όχι. Μια ακόμα ισχυρότερη χρήση ενός τείχους προστασίας είναι σε ένα σενάριο δυο επιπέδων προστασίας, όπου χρησιμοποιείται ένας δρομολογητής που παρακολουθεί την επικοινωνία με το διαδικασία και ένας ακόμη που παρακολουθεί την επικοινωνία στο εσωτερικό δίκτυο (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65).

Η κρυπτογράφηση αποτελεί τη διαδικασία επεξεργασίας και κωδικοποίησης της ψηφιακής πληροφορίας κατά τέτοιο τρόπο ώστε αυτή να παραμένει αναγνώσιμη στην κατανοητή μορφή της μόνο από τους εξουσιοδοτημένους παραλήπτες που διαθέτουν το κατάλληλο «κλειδί» - κώδικα, δηλαδή η πληροφορία καθίσταται εμπιστευτική. Αρχικά η τεχνολογία της κρυπτογράφησης δημιουργήθηκε με σκοπό την προστασία του απορρήτου του μηνύματος. Στην πορεία, η εξέλιξη της κρυπτογράφησης προσφέρει στον αποστολέα του μηνύματος μεγαλύτερη ασφάλεια σχετικά με το ακέραιο αλλά και το απόρρητο του μηνύματος κατά την αποστολή του. Ένα κρυπτογραφικό σύστημα αποτελεί ένα σύνολο λειτουργιών οι οποίες είναι παραμετροποιημένες από κλειδιά και χρησιμοποιούνται για τη διατήρηση εχεμύθειας στην επικοινωνία. Με τις ενσωματωμένες λειτουργίες της έγκρυψης και της απόκρυψης, το σύστημα παρέχει ασφάλεια και προστασία στην ιδιωτικότητα, αποκλείοντας έτσι την χωρίς εξουσιοδότηση πρόσβαση σε υλικό που ορίστηκε να παραμείνει απόρρητο. Το κρυπτογραφικό περιεχόμενο δεν μπορεί να γίνει προσβάσιμο από οποιονδήποτε που θα

προσπαθήσει να το προσπελάσει χωρίς να γνωρίζει τι περιέχει. Συνεπώς, αποκλείεται η έκθεση σε βλαπτικό υλικό για όποιον θα μπορούσε να προσβληθεί ακόμα και αν αυτό συνέβαινε τυχαία (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65).

Ένα σύγχρονο σύστημα κρυπτογράφησης αποτελείται από τέσσερα κύρια σημεία, τα οποία είναι (Γκρίτζαλης κ.α., 2003, σ. 30-40; Κάτσικας κ.α., 2004, σ. 50-65):

- Το αρχικό μήνυμα,
- Το κρυπτογραφικό σύστημα αποτελούμενο από έναν αλγόριθμο κρυπτογράφησης και έναν αποκρυπτογράφησης,
- Το κρυπτογραφημένο μήνυμα, που είναι το αποτέλεσμα της εφαρμογής του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη,
- Το κλειδί, το οποίο είναι μια συμβολοσειρά, που χρησιμοποιείται στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης από τους αλγορίθμους.

Οι βασικότεροι στόχοι που επιτυγχάνονται με την κρυπτογράφηση είναι:

- Η αυθεντικοποίηση, όπου το μήνυμα δε θα διαρρεύσει σε χρήστη που δεν έχει δικαίωμα πρόσβασης,
- Η ακεραιότητα, όπου το μήνυμα θα φτάσει στον παραλήπτη του χωρίς να έχει υποστεί αλλοίωση ή μετατροπή,
- Η μη αποποίηση της παραλαβής-αποστολής, δηλαδή ο αποστολέας ή παραλήπτης του μηνύματος δε θα αρνηθούν ότι έστειλαν το μήνυμα.

5.3. Προληπτικά μέτρα

Τα προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι. Για την ασφάλεια των δικτύων, ορισμένες

συμβουλές είναι οι ακόλουθες (Jansen & Ayers, 2007, σ. 33-39; Βλαχόπουλος, 2007, σ. 80-100):

❖ *Συμβουλές για παιδιά*

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο διαδίκτυο,
- Συζητήστε με τους γονείς σας ή με κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο διαδίκτυο και σας ανησυχούν ή σας φοβίζουν,
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο διαδίκτυο ακόμη και αν σας το ζητήσουν,
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν,
- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο διαδίκτυο,
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα,
- Μην εμπιστεύεστε ότι διαβάζετε στο διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

❖ *Συμβουλές για νέους*

- Μη δίνετε σε κανέναν τον κωδικό πρόσβασης στο διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τον κωδικό είναι οι γονείς σας,
- Μην απαντάτε σε ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεστε άβολα. Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάσετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε,
- Αν αισθανθείτε άβολα την ώρα που συνομιλείτε μέσω chatroom, διακόψτε αμέσως τη συνομιλία,
- Αποφύγετε να στέλνετε τη φωτογραφία σας και τα προσωπικά στοιχεία σας μέσω διαδικτύου σε άγνωστο,
- Μην επιδιώξετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο διαδίκτυο,
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με τον διαδικτυακό σας φίλο. Ενημερώστε τους γονείς σας ή κάποιο άτομο που εμπιστεύεστε και φροντίστε αυτή η συνάντηση να γίνει σε δημόσιο χώρο,

- Αναπτύξτε κριτική διάθεση σε ότι διαβάζετε στο διαδίκτυο. Μην εμπιστεύεστε αμέσως ότι δείτε,
- Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν σερφάρετε στο διαδίκτυο.

❖ *Συμβουλές για γονείς*

- Κρατήστε τον Υ/Η σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον κυβερνοχώρο και μάθετε από αυτά,
- Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του Υ/Η. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους,
- Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms, χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του διαδικτύου χωρίς να είστε και εσείς μαζί,
- Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες,
- Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του διαδικτύου,
- Συζητήστε με τα παιδιά σας για την ασφάλεια του διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους,
- Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο διαδίκτυο.

❖ *Συμβουλές για οικονομικές συναλλαγές*

- Αποφεύγετε να πραγματοποιείται οικονομικές συναλλαγές μέσω διαδικτύου από internet cafe, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές. Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας,

- Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί,
- Αποφεύγετε να χρησιμοποιείται ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα,
- Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπή τους θα διευκολύνετε πολύ τους δράστες,
- Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια κάρτες σας,
- Μη δίνετε τον κωδικό πρόσβασής σας σε οποιονδήποτε κάτω από οιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτήν την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την αστυνομία,
- Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία internet banking,
- Απενεργοποιήστε τη λειτουργία αυτόματης καταχώρησης του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους,
- Κάνετε αγορές μόνο από γνωστές εταιρίες που σας παρέχουν εγγυήσεις ασφάλειας,
- Αν κάνετε συχνά αγορές από το διαδίκτυο, χρησιμοποιείτε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας,
- Φροντίστε να διατηρείται σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας,
- Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρίες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείται και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του,
- Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς και ένα τείχος προστασίας, και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους.
- Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών,

- Μην ανοίγετε τα e-mails για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό σας.
- Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μη στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου,
- Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά,
- Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα ATM (Βλαχόπουλος, 2007, σ. 80-100).

ΜΕΡΟΣ 2

Μελέτη περίπτωσης

6. Το Σκοτεινό διαδίκτυο

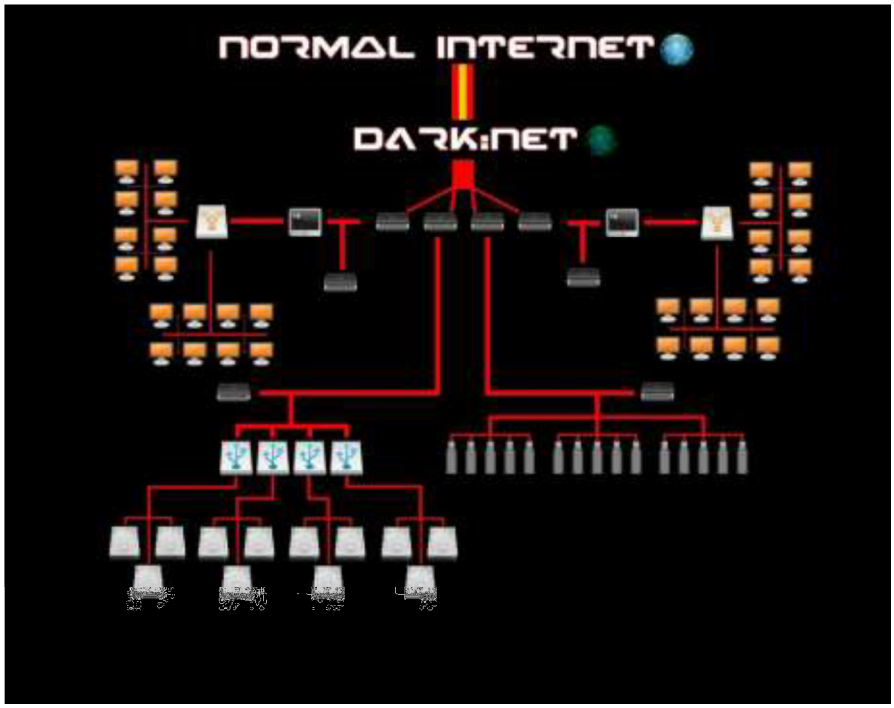
Εισαγωγή

Η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο. Παραδοσιακές ηλεκτρονικές απειλές όπως: Κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και συστήματα, ενοχλητικά ηλεκτρονικά μηνύματα, επιθέσεις κλοπής ηλεκτρονικής ταυτότητας κ.λπ., αναμένεται να βρουν νέα, εξίσου γόνιμα, εδάφη για την εξάπλωσή τους. Μια από τις πλέον σκοτεινές πτυχές του internet το **Darknet**, ένα μυστικό διαδίκτυο που δημιουργήθηκε στις αρχές της δεκαετίας του 90′ από τις αμερικανικές μυστικές υπηρεσίες, προκειμένου να εξασφαλίζεται η μυστικότητα των συνομιλιών στα πλοία του στόλου των ΗΠΑ που ταξίδευαν σε ολόκληρο το κόσμο. Ωστόσο, πολύ γρήγορα αυτό το σκοτεινό διαδικτυακό κόσμο, το ανακάλυψαν και άλλοι χρήστες σε ολόκληρο το κόσμο οπού αρχίσαν να το χρησιμοποιούν για όχι και τόσο κάλους σκοπούς, με αποτέλεσμα να περάσει στα χέρια οργανωμένων εγκληματικών οργανώσεων. Πλέον το σκοτεινό διαδίκτυο έχει εξελιχθεί σε ένα παράλληλο κόσμο. Το ιντερνέτ και οι Η/Υ παρέχουν στους χρήστες αφενός μεν ασύλληπτες δυνατότητες και αφετέρου όμως εισαγάγουν νέες μορφές παραβατικής συμπεριφοράς.

6.1 Ορισμός του Darknet

Βρισκόμαστε στην διάρκεια της τεχνολογικής επανάστασης που έφερε το διαδίκτυο. Η κοινή χρήση αρχείων, τα δίκτυα Η/Υ και οι ψηφιακοί χρήστες έχουν πλέον τη δυνατότητα να κρύψουν τις δραστηριότητα τους στο διαδίκτυο χρησιμοποιώντας ασφαλή, ιδιωτικά και ανώνυμα δίκτυα που συνολικά ονομάστηκαν Darknet (επίσης γνωστό και ως Deepnet, Deepweb, Undernet, το σκοτεινό, αόρατο το κρυμμένο web, Εικόνα 1) αναφέρεται στο περιεχόμενο του www που δεν ανήκει στο επιφανειακό web (surface web), το οποίο δεικτοδοτείται από μία συνηθισμένη μηχανή αναζήτησης. Ο παγκόσμιος ιστός θεωρείται το δίκτυο των συνδεδεμένων υπολογιστών και δικτύων σε παγκόσμια κλίμακα, και το οποίο χρησιμοποιεί μία συγκεκριμένη ομάδα πρωτοκόλλων και επικοινωνίας, γνωστή και ως "http". Κάθε μονάδα του διαδικτύου αποτελείται από συνδεδεμένους υπολογιστές σε τοπικό επίπεδο. Αυτά τα δίκτυα με τη σειρά τους συνδέονται σε ευρύτερα δίκτυα, όπως εθνικά και υπερεθνικά. Το ευρύτερο δίκτυο στον κόσμο λέγεται παγκόσμιος ιστός το οποίο είναι μοναδικό, και συμπεριλαμβάνεται τόσο τα γήινα δίκτυα, όσο και τα δίκτυα των δορυφόρων της και άλλων διαστημικών συσκευών που είναι συνδεδεμένα σε αυτό. Οι κόμβοι σε τοπικά δίκτυα ή δίκτυα μεγάλου εύρους, όπως το διαδίκτυο, είναι ισότιμοι, συνεπώς θα έπρεπε να έχουν δυνατότητα πρόσβασης στο ίδιο σύνολο κόμβων.

Χρησιμοποιείται ως όρος για να περιγράψει ένα από τα πολλά δίκτυα ανταλλαγής αρχείων peer-to-peer σε ευρεία χρήση, δηλαδή το σύνολο των μη προσβάσιμων διευθύνσεων ενός δικτύου (Εικόνα 2). Είναι ένα συνονθύλευμα από: (i). spam sites που οι search engines απορρίπτουν εξαιτίας της χαμηλής ποιότητάς τους, (ii). προσωπικές ιστοσελίδες, boards, forums, και άλλες μορφές ιστοσελίδων που δεν παρουσιάζουν ενδιαφέρον για το ευρύ κοινό, (iii) βάσεις δεδομένων ακαδημαϊκού περιεχομένου που αφορούν ερευνητές (iv). κυβερνητικές υπηρεσίες πάλι με περιορισμένο ενδιαφέρον για τον πολύ κόσμο (v). Το Darknet περιλαμβάνει παράνομα και εγκληματικά sites που δεν θέλουν να προσελκύσουν το ενδιαφέρον των άλλων (Wood, 2010; saferinternet.gr).



Εικονα 2.Η σχέση του Darknet με το επιφανειακό web (https://linuxsecurityblog.com/2016/02/24/the-darknet-faq/).

Το Darknet για έναν υπολογιστή-κόμβο είναι το σύνολο των διευθύνσεων του δικτύου που ανήκει στις οποίες δεν έχει πρόσβαση (Wood, 2010). Αναφέρεται από τον Bergman, M., που επινόησε τον όρο αναφέρει (από Wood, 2010): "Το να ψάχνει κανείς στο internet σήμερα είναι σαν να σέρνει ένα δίχτυ στην επιφάνεια του ωκεανού: πολλά μπορεί να πιαστούν στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκονται βαθιά και επομένως δεν μπορούν να πιαστούν. Οι περισσότερες πληροφορίες του web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες, και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Οι παραδοσιακές μηχανές αναζήτησης δεν μπορούν να ανακτήσουν το περιεχόμενο του Deepweb. Αυτές οι σελίδες δεν υπάρχουν μέχρι να δημιουργηθούν δυναμικά
ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Το Deepweb είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό web".

Η Wood (2010) συμπληρώνει ότι το Darknet δεν αποτελεί ένα ξεχωριστό τύπο διαδικτύου, αλλά η βασική διαφορά του με το www είναι ότι έχει περιορισμένη εμβέλεια και επιπλέον λειτουργεί σε καθεστώς ανωνυμίας, χάρη σε εντελώς διαφορετικά συστήματα και τεχνικές

δομές. Το Darknet δεν είναι ένα συγκεντρωτικό σύστημα, γεγονός που υποδηλώνει πως δεν απαιτείται να γίνει είσοδος σε ηλεκτρονικές πύλες με ταυτοποίηση προσωπικών στοιχείων. Ιδεολογικά, ωστόσο, το εν λόγω δίκτυο εμφανίζεται στα περιθώρια της νομιμότητας του διαδικτύου (Wood, 2010).(Εικονα 3)

Εικονα 3. Το Darknet.(https://witnessthis.wordpress.com/2009/12/14/the-dark-web-explained-2/)

Το Darknet αποτελεί επίσης, ένα αυτόνομο διαδίκτυο που προσφέρει ανώνυμη κάλυψη - χωρίς τη δυνατότητα ανίχνευσης της ηλεκτρονικής ταυτότητας των χρηστών- σε παράνομους και περιθωριακούς κύκλους. Ωστόσο παρά τις τρομακτικές του δυνατότητες, οι ειδικοί επισημαίνουν ότι το Darknet δεν έχει μόνο κακή πλευρά, παρόλο που συχνά το εξισώνουν με τον online υπόκοσμο. Οι πληροφορίες που συνήθως διακινούνται στο Darknet ανήκουν σε μία ή περισσότερες από τις παρακάτω κατηγορίες (Wood, 2010; saferinternet.gr):

(i). *Με δυναμικά παραγόμενο περιεχόμενο*, όπως δυναμικές ιστοσελίδες οι οποίες δημιουργούνται ως αποτέλεσμα της εκτέλεσης κάποιας επερώτησης ή προσπελαύνονται μόνο μέσω κάποιας φόρμας,

(ii). *Με μη συνδεδεμένο περιεχόμενο*, όπως ιστοσελίδες οι οποίες δεν περιέχουν συνδέσμους από άλλες ιστοσελίδες, εμποδίζοντας έτσι τα προγράμματα που κάνουν Web

Crawling επισκεφθούν το περιεχόμενό τους,

(iii). *Ιδιωτικό web*, με ιστότοπους που απαιτούν εγγραφή και κωδικό πρόσβασης,

(iv). *Με περιεχόμενο περιορισμένης πρόσβασης*, με ιστότοπους που περιορίζουν την πρόσβαση στις σελίδες τους με τεχνικό τρόπο (χρησιμοποιώντας το Robots Exclusion Standard, CAPTCHAs, ή το no-cache Pragma στις επικεφαλίδες του πρωτοκόλλου HTTP, τα οποία απαγορεύουν στις μηχανές αναζήτησης να πλοηγούνται στις ιστοσελίδες τους),

(v). *Με περιεχόμενο που δεν είναι σε μορφή HTML*, όπως κείμενα που συμπεριλαμβάνονται σε multimedia αρχεία (εικόνες ή video) ή που έχουν συγκεκριμένη μορφή την οποία δεν μπορούν να χειριστούν οι μηχανές αναζήτησης,

(vi). *Με κείμενα που χρησιμοποιούν το πρωτόκολλο Gopher* και *αρχεία που βρίσκονται σε διακομιστές FTP* και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης, αφού δεν δεικτοδοτούν ιστοσελίδες που βρίσκονται έξω από το πρωτόκολλο HTTP (Wood, 2010).

Οι πληροφορίες στο web είναι κρυμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες (Εικόνα 2). Οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν και ανακτήσουν το περιεχόμενό τους γιατί οι ιστοσελίδες αυτές δεν υπάρχουν για τις μηχανές αναζήτησης μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Αυτό συμβαίνει γιατί οι μηχανές αναζήτησης δεν μπορούν να καταχωρίσουν πληροφορίες που βρίσκονται σε βάσεις δεδομένων, σε δυναμικές ιστοσελίδες που δημιουργούνται από κάποιον κώδικα ή σε ιδιωτικά δίκτυα πληροφοριών. Έτσι, ο μεγαλύτερος όγκος πληροφοριών παραμένει απροσπέλαστος από τους χρήστες που χρησιμοποιούν το www. Η περιήγηση στο Darknet γίνεται ανώνυμα μέσα από την χρήση του TOR, δηλαδή διαρκώς μεταβαλλόμενων δεδομένων τα οποία καθιστούν σχεδόν αδύνατο τον εντοπισμό του χρήστη (Wood, 2010).

6.1.1. Είδη εγκληματικών δραστηριοτήτων στο Deep Web

Θα αναφερθούμε σε ορισμένες κατηγορίες εγκληματικών δραστηριοτήτων που η ανωνυμία του Deep Web διευκολύνει τη διάπραξή τους. Σημειώνεται ότι, σε γενικές γραμμές, δεν πρόκειται για νέα φαινόμενα, παρά για παραδοσιακά εγκλήματα όπου το Deep Web χρησιμοποιείται ως εργαλείο είτε επικοινωνίας και ανταλλαγής δεδομένων, είτε διάθεσης προϊόντων εγκλήματος.

- **Ναρκωτικές ουσίες, όπλα και είδη υπό εξαφάνιση**

Με αντιπροσωπευτικότερο παράδειγμα τον ιστότοπο αγοραπωλησιών Silk Road (το οποίο έχει τεθεί εκτός λειτουργίας από τις διωκτικές Αρχές), στις ανώνυμες online αγορές (marketplaces) μπορεί κανείς να θέσει προς πώληση ή να αγοράσει μια μεγάλη γκάμα προϊόντων, νόμιμων, αλλά και παράνομων: βιβλία, ρούχα, αλλά και ναρκωτικές ουσίες και όπλα. Μοιάζουν με τους συνηθισμένους ιστοτόπους αγγελιών / αγοραπωλησιών.

- **Κλεμμένα αγαθά και πληροφορίες / δεδομένα**

Στις προαναφερθείσες online αγορές μπορεί κάποιος να προβεί σε αγοραπωλησίες υποκλαπέντων αγαθών, δεδομένων οικονομικής φύσεως (αριθμούς και κωδικούς ασφαλείας πιστωτικών καρτών) ή credentials πρόσβασης σε online λογαριασμούς (email, social media, web-banking κ.λπ.), καθώς επίσης και πλαστογραφημένα έγγραφα (ταυτότητες, διαβατήρια και πολλά άλλα).

- **Δολοφονίες**

Πέρα από τους ιστοτόπους όπου μπορεί κάποιος να αναζητήσει και να προσλάβει στην υπηρεσία του έναν "επαγγελματία" δολοφόνο, το πιο απίθανο είναι ότι έχουν δημιουργηθεί ιστότοποι όπου κάποιος μπορεί να στοιχηματίσει για την ημέρα δολοφονίας ενός συγκεκριμένου προσώπου. Αυτό από μόνο του αποτελεί ισχυρό κίνητρο για να διαπράξει κάποιος μια δολοφονία, χωρίς να έχει άμεση σχέση με το θύμα.

- **Τρομοκρατία**

Για προφανείς λόγους, το Deep Web επιλέγεται από τρομοκρατικές οργανώσεις ως μέσο επικοινωνίας, προπαγάνδας, στρατολόγησης νέων μελών, χρηματοδότησης και σχεδιασμού.

- **Hacktivism**

Χαρακτηριστικότερο παράδειγμα στην κατηγορία αυτή αποτελεί η ομάδα Anonymous, που χρησιμοποιούν το Deep Web για σκοπούς ακτιβισμού. Ο διαδικτυακός ακτιβισμός, από ικανότατους hackers, αποτελεί μια νέα τάση διαδήλωσης ενάντια στην εξουσία του κράτους.

- **Αγορές Exploit**

Τα Exploits αποτελούν κακόβουλο λογισμικό βασισμένο στις ευπάθειες λογισμικού. Μια επιμέρους κατηγορία των exploits είναι τα zero-day exploits τα οποία στοχεύουν σε ευπάθειες που δεν έχουν διορθωθεί από τις κατασκευάστριες εταιρείες και που οι προγραμματιστές έχουν "zero-days" προθεσμία για να τις διορθώσουν. Η τιμή διάθεσης των exploit kits διαμορφώνεται με βάση το πλήθος των υποψήφιων (συσκευών) θυμάτων.

- **Παράνομες οικονομικές συναλλαγές**

Σε αυτή την κατηγορία εντάσσεται η νομιμοποίηση εσόδων μέσω διαφόρων προσφερόμενων υπηρεσιών και με τη χρήση ψηφιακών νομισμάτων τύπου Bitcoin, ώστε να αποκρύπτεται η πραγματική προέλευση των χρημάτων. Παράλληλα, μπορεί κάποιος να προμηθευτεί, σε υπόγειες αγορές, υποκλαπέντα δεδομένα πιστωτικών καρτών με απεριόριστο όριο συναλλαγών, καταβάλλοντας ένα συγκεκριμένο αντίτιμο.

- **The Hidden Wiki**

Πρόκειται για τοποθεσία όπου μπορεί κάποιος να βρει πλήθος (εν δυνάμει επικίνδυνων) πληροφοριών (π.χ. κατασκευή εκρηκτικών μηχανισμών) και συνδέσμους προς άλλους ιστοτόπους στο Dark Web (οι οποίοι διαρκώς τροποποιούνται).

- **Πειράματα σε ανθρώπους**

Πριν τεθεί εκτός λειτουργίας το 2011, ο ιστότοπος The Human Experiment περιείχε λεπτομερή αποτελέσματα ιατρικών πειραμάτων που διενεργούνταν σε αγνώστους (κατά βάση άστεγους πολίτες).

- **Κλοπές – διαρρήξεις**

“Επαγγελματίες” κλέφτες προσφέρουν τις υπηρεσίες τους έναντι αμοιβής, η οποία καθορίζεται από το αντικείμενο – στόχο και την επικινδυνότητα της “αποστολής”.

- **Εμπόριο όπλων και πυρομαχικών**

Γνωστότερος ιστότοπος της συγκεκριμένης κατηγορίας αποτελεί ο Euroarms, όπου μπορεί κάποιος να αγοράσει οποιουδήποτε είδους όπλο και να ζητήσει την παράδοσή του κατ' οίκον. Η προμήθεια των πυρομαχικών γίνεται μέσω άλλων ιστοτόπων, επίσης στο Dark Web.

- **Στοιχηματισμός – τζόγος**

Λόγω της ισχύουσας νομοθεσίας σε ορισμένες χώρες και την απαγόρευση πρόσβασης πολιτών σε μη εγκεκριμένους από το Κράτος ιστοτόπους στοιχηματισμού, μπορεί ένας χρήστης να αποκρύψει την πραγματική του IP διεύθυνση και να παρακάμψει τις δικλείδες ασφαλείας των Παρόχων Υπηρεσιών Διαδικτύου (ISPs).

- **Πορνογραφία ανηλίκων**

Στο Dark Web μπορεί κανείς να αποκτήσει πρόσβαση σε ιστοτόπους με “πλούσιο” υλικό σεξουαλικής εκμετάλλευσης ανηλίκων ή ακόμα και ιστοτόπους που προβάλουν κακοποίηση ανηλίκων σε ζωντανή μετάδοση (live streaming), έναντι φυσικά υψηλότατης αμοιβής.

6.2 Τρόποι προσπέλασης του Σκοτεινού διαδικτύου(Darknet)

Το Darknet κρύβει πολλά μυστικά και καθημερινά προστίθενται κι άλλα, με τρόπο ώστε κανείς, στην κυριολεξία, όσο «προχωρημένος» ή έμπειρος κι αν είναι να μην μπορεί να υποθέσει με σχετική ασφάλεια τί άλλο θα μπορούσε να υπάρχει κρυμμένο μέσα στο Darknet, πέρα απ" αυτά που ήδη γνωρίζει ότι υπάρχουν. Τα περισσότερα sites που αναφέρονται στο Darknet ταυτίζουν ανακριβώς το Darknet με το δίκτυο Tor. Πολλά εξ αυτών μάλιστα, υποστηρίζουν λανθασμένα ότι το πρώτο βήμα για να εισέλθει κάποιος στο βαθύ, κρυμμένο ίντερνετ, είναι η θέση σε λειτουργία του Tor browser στον υπολογιστή του. Παρακάτω παραθέτουμε πέντε βασικά εργαλεία προσπέλασης του σκοτεινού διαδικτύου(Darknet).

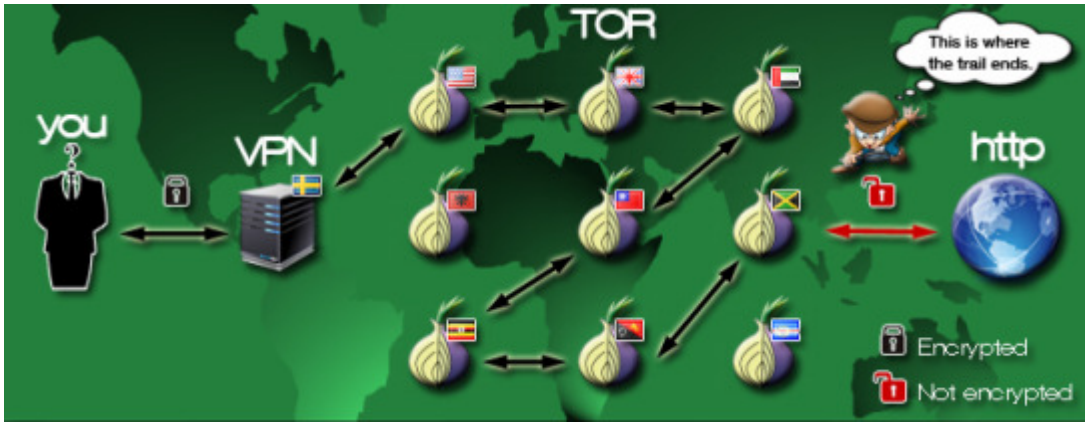
6.2.1. Εργαλείο 1: TOR

Οι πληροφορίες στο web είναι κρυμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες. Οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν και ανακτήσουν το περιεχόμενό τους γιατί οι ιστοσελίδες αυτές δεν υπάρχουν για τις μηχανές αναζήτησης μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Αυτό συμβαίνει γιατί οι μηχανές αναζήτησης δεν μπορούν να καταχωρίσουν πληροφορίες που βρίσκονται σε βάσεις δεδομένων, σε δυναμικές ιστοσελίδες που δημιουργούνται από κάποιον κώδικα ή σε ιδιωτικά δίκτυα πληροφοριών. Έτσι, ο μεγαλύτερος όγκος πληροφοριών παραμένει απροσπέλαστος από τους χρήστες που χρησιμοποιούν το www. Η περιήγηση στο Darknet γίνεται ανώνυμα μέσα από την χρήση του TOR, δηλαδή διαρκώς μεταβαλλόμενων δεδομένων τα οποία καθιστούν σχεδόν αδύνατο τον εντοπισμό του χρήστη (Lemley & Reese, 2004).Το Darknet είναι ένα δίκτυο από σέρβερ, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα. Η πιο διαδεδομένη τεχνολογία γι' αυτό τον σκοπό είναι το TOR, που εγγυάται και τη δική τους ανωνυμία. Χάρης στο TOR, ένα site μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, καμουφλάροντας τον σέρβερ που το φιλοξενεί.

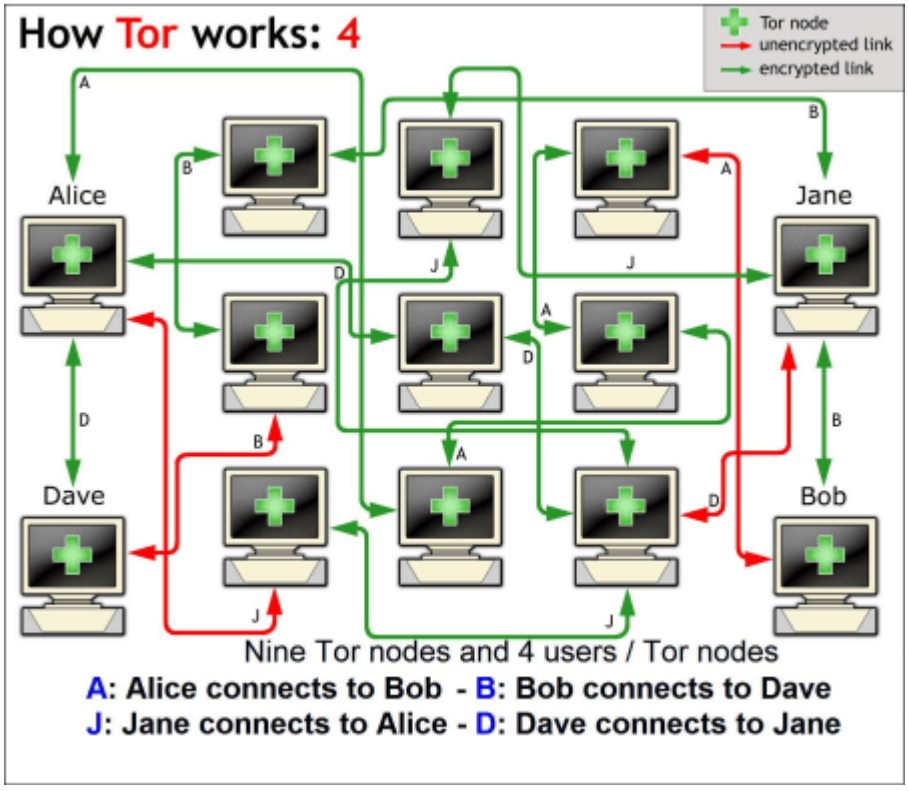
Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Darknet έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους. Οι χρήστες που επιθυμούν να συμμετάσχουν στη κατασκευή της γέφυρας αυτής πρέπει να είναι εγγεγραμμένοι στην υπηρεσία της Amazon. Το γεγονός υποδεικνύει ότι προσφέρεται για χρήση του Darknet,

αφού δημιουργούνται κρυψώνες με τις υπηρεσίες cloud (Lemley & Reese, 2004).Ένα μέρος του Darknet είναι προσβάσιμο μέσω του ανώνυμου δικτύου TOR. Η επίσκεψη σε ένα δικτυακό τόπο μέσω του TOR εκτρέπει τις συνδέσεις μέσα από μια τυχαιοποιημένη πορεία υπολογιστών άλλων χρηστών πριν από την επίτευξη του στόχου του web server, κρύβοντας ουσιαστικά την τοποθεσία σας από αυτόν το διακομιστή. Αντίθετα από τις κανονικές ιστοσελίδες, οι σελίδες του Darknet δεν έχουν φιλικές διευθύνσεις URL. Αντ'αυτού, αποτελούν μια φαινομενικά τυχαία σειρά χαρακτήρων που ακολουθείται από την κατάληξη ".onion" και παρέχει πρόσβαση σε αυτές τις κρυφές ιστοσελίδες. Στο Darknet υπάρχει το "Hidden Wiki" που παρέχει καταχωρήσεις αυτών των διευθύνσεων URL για να διευκολυνθεί η χρήση του Darknet. Το TOR χρησιμοποιείται κυρίως από ακτιβιστές που θέλουν να αποφύγουν τη λογοκρισία, καθώς και από άτομα τα οποία επιζητούν ανωνυμία για πιο ύποπτους σκοπούς. Οι υποστηρικτές του επιθυμούν επέκταση του bandwidth της εν λόγω υπηρεσίας, και για αυτό στρέφονται στην Amazon, ή στην cloud υπηρεσία της οποίας θα κάνει δυσκολότερο για τις κυβερνήσεις να παρακολουθήσουν τα δρώμενα στο Darknet. Σε αυτό το βάθος δεν φτάνουν ποτέ οι μηχανές αναζήτησης και ο κόσμος διαμορφώνεται με άλλους κανόνες. Εμφανίζεται ο κατάλογος ταξινόμησης Hiddenwiki που ταξινομεί σελίδες με κατάληξη onion και παρέχει μια πρώτου επιπέδου διερεύνηση του πυθμένα. Με τη χρήση λογισμικού του TOR ο χρήστης εξασφαλίζοντας την ανωνυμία του, αποκτά πρόσβαση σε πληροφορίες όπως είναι η πώληση και διακίνηση όπλων, ναρκωτικών, παράνομων αγοραπωλησιών και στοιχημάτων, διακίνησης πορνογραφικού υλικού. Σε αυτή την πλευρά του διαδικτύου η ηθική απουσιάζει και εκτός από πλαστά διαβατήρια ή χαρτονομίσματα κανείς μπορεί να προσλάβει μέχρι και μισθωμένους δολοφόνους. Οι χρήστες του TOR ζητούν από τους υποστηρικτές του δικτύου να εγγραφούν στην υπηρεσία προκειμένου να τρέξουν μια γέφυρα (bridge)- ένα εξαιρετικά σημαντικό τμήμα του δικτύου, μέσω του οποίου δρομολογούνται οι επικοινωνίες. Μια τέτοιου τύπου γέφυρα δίνει την δυνατότητα για bandwidth στο δίκτυο TOR ώστε να βελτιώνεται η ασφάλεια και η ταχύτητα με την οποία οι χρήστες μπορούν να έχουν πρόσβαση στο διαδίκτυο (Lemley & Reese, 2004). Στο Deep Web λειτουργούν επίσης διάφορα εικονικά δίκτυα υπολογιστών διασυνδεδεμένων μεταξύ τους Peer to Peer (VPNs – Virtual Private Networks, Intranets, frameworks). Η πληροφορία στα δίκτυα αυτά αποθηκεύεται ολόκληρη ή σε «πακέτα», ανοικτή ή κρυπτογραφημένη, στους σκληρούς δίσκους των υπολογιστών που αποτελούν μέρος του VPN και διακινείται Peer to Peer (P2P), από τον κάθε υπολογιστή απ ευθείας σε κάποιους άλλους υπολογιστές, διαφορετικούς κάθε φορά, χωρίς τη μεσολάβηση κάποιου κεντρικού σέρβερ και χωρίς κάποιον κεντρικό έλεγχο. Με τον τρόπο αυτό, η αποθήκευση και διακίνηση της πληροφορίας

καθώς και η εκάστοτε πλήρης διαδρομή της, καθίσταται πρακτικά κεντρικώς ανεξέλεγκτη και, στις περισσότερες περιπτώσεις, μη ανιχνεύσιμη.(Εικονα4-5) Υπάρχουν όμως και άλλα λογισμικά παρόμοια με το TOR. Αυτά είναι :



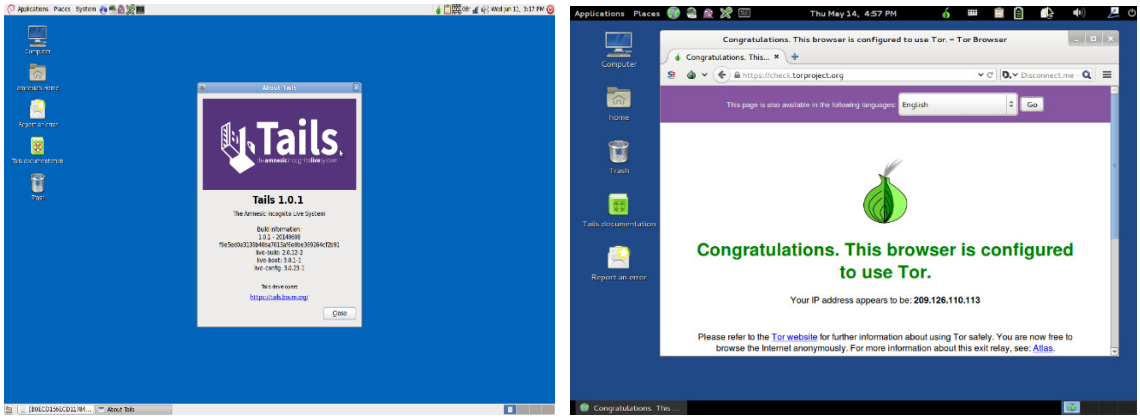
Εικονα 4. Λειτουργία του Tor(http://www.daddy-cool.gr/epikerotita/to-skoteino-internet-dark-deep-web.html)



Εικονα 5.Λειτουργία του Tor(http://www.daddy-cool.gr/epikerotita/to-skoteino-internet-dark-deep-web.html)

6.2.2. Εργαλείο 2:Tails OS

Tails OS είναι ένα ζωντανό σύστημα που έχει ως στόχο να διατηρήσει το απόρρητο και την ανωνυμία του χρήστη. Αυτό σας βοηθά να χρησιμοποιήσετε το Internet ανώνυμα και να παραμείνει η ταυτότητα του χρήστη κρυφή σχεδόν οπουδήποτε και σε οποιονδήποτε υπολογιστή, δεν αφήνει κανένα ίχνος, εκτός αν το ζητήσει ρητώς.(Εικονα 6)



Εικονα 6. Tor μαζι με το Tails(http://waves.pirateparty.gr/node/1187)

Είναι ένα πλήρες λειτουργικό σύστημα που έχει σχεδιαστεί για να χρησιμοποιηθεί από ένα DVD, USB stick, ή κάρτα SD, ανεξάρτητα από το αρχικό λειτουργικό σύστημα του υπολογιστή. Είναι ένα free software (Ελεύθερο Λογισμικό) και βασίζεται σε Debian GNU / Linux.

Βασίζεται στο δίκτυο Tor για την προστασία της ιδιωτικότητας σε απευθείας σύνδεση: όλο το λογισμικό έχει ρυθμιστεί για να συνδεθείτε στο Internet μέσω Tor αν μια εφαρμογή προσπαθεί να συνδεθεί με το Internet, η σύνδεση αυτόματα μπλοκάρει για την ασφάλεια. Επίσης σε θέματα που αφορούν κακόβουλο λογισμικό, δεν υφίσταται κίνδυνος αν δεν υπαρχει πρόσβαση στο Darknet/Deep Web μέσω του Tails OS. Επίσης καθώς το πρόγραμμα τρέχει από την RAM μας και δεν αφήνει ίχνη στον υπολογιστή που το χρησιμοποιούμε, εκτός κι αν το ζητήσουμε οπότε, τεχνικά, (εφόσον κάνουμε ανώνυμη χρήση) δεν τίθεται κάποιο ζήτημα αναγνώρισης της ταυτότητάς μας.

6.2.3. Εργαλείο 3: Το λογισμικό Crowds

Το λογισμικό Crowds επιτρέπει την ανάκτηση πληροφοριών από το διαδίκτυο χωρίς να αποκαλύπτει πληροφορίες ιδιωτικότητας σε τρίτους. Στόχος του Crowds αποτελεί η ανώνυμη φυλλομέτρηση, ώστε είτε η πληροφορία σχετικά με το χρήστη, είτε η ίδια η πληροφορία που ανακτάται από το δίκτυο, να παραμένει κρυφή από άλλους. Αποτρέπει τους εξυπηρετητές να καταγράψουν πληροφορίες, όπως η διεύθυνση IP και το όνομα του domain, οι οποίες δίνουν την δυνατότητα ταυτοποίησης του χρήστη. Επιπρόσθετα, το λογισμικό αυτό έχει τη δυνατότητα να αποκρύβει πληροφορίες όπως τη σελίδα και τον τύπο Η/Υ του χρήστη. (Reiter & Rubin, 1998).

Η φιλοσοφία και σχεδίαση του Crowds βασίζεται στην αρχική ιδέα ότι οι άνθρωποι διατηρούν την ανωνυμία τους εύκολα, αν κινούνται ανώνυμα μέσα στο πλήθος. Το πλήθος που δημιουργείται από τους χρήστες του Crowds, ανεξαρτήτως ανθρωπογεωγραφίας, πραγματοποιεί τις συναλλαγές στο διαδίκτυο εκ μέρους των μελών του. Για να εγγραφεί οποιοδήποτε ως μέλος στο πλήθος, πρέπει να εκτελέσει μια διεργασία στον υπολογιστή που είναι γνωστή ως Jondo (John Doe), η οποία υπονοεί ένα τυχαίο και απρόσωπο άτομο μέσα στο πλήθος (κάθε μέλος στο πλήθος αντιπροσωπεύεται από το Jondo που εκτελείται στον υπολογιστή του) (Reiter & Rubin, 1998).

Συγκεκριμένα, το σύστημα Crowds προστατεύει τις σελίδες που επισκέπτεται ή αιτείται ο χρήστης από οντότητες με δικαιώματα διαχειριστή, αφού η επικοινωνία μεταξύ των Jondos κρυπτογραφείται με χρήση συμμετρικού συστήματος με μυστικό κλειδί το οποίο διαμοιράζονται. Στο Crowds, το μονοπάτι των συνεργαζόμενων πληρεξούσιων υπηρεσιών επιλέγεται τυχαία, βήμα προς βήμα, καθώς η αρχική αίτηση προωθείται μέσω του πλήθους.
Το μονοπάτι επιλέγεται από το πλήθος μονάχα μια φορά και χρησιμοποιείται για όλες τις ανώνυμες επικοινωνίες από έναν αποστολέα ιδρυτής σε κάθε παραλήπτη εντός μιας περιόδου είκοσι τεσσάρων ωρών (Reiter & Rubin, 1998).

Το Crowds διατηρεί την ανωνυμία με την εκτέλεση ενός πρωτοκόλλου αρχικοποίησης. Εφόσον αυτό ολοκληρωθεί, ο αποστολέας κατέχει ένα μυστικό συμμετρικό κλειδί το οποίο γνωρίζουν και όσοι άλλοι Jondo συμπεριλαμβάνονται στο πλήθος. Για την αποστολή

δεδομένων, ο ιδρυτής δημιουργεί και προωθεί ένα πακέτο, το οποίο περιέχει ένα τυχαίο μονοπάτι, την IP διεύθυνση του παραλήπτη, καθώς και τα δεδομένα τα οποία είναι κρυπτογραφημένα με ένα κλειδί, το οποίο διαμοιράζεται με τον τυχαία επόμενο επιλεγμένο Jondo. Όταν ο παραλήπτης παραλάβει το πακέτο, επιστρέφει ένα πακέτο απάντησης διαμέσου του αντίστροφου μονοπατιού της αίτησης. Τα επόμενα πακέτα μεταξύ του αποστολέα και του παραλήπτη ακολουθούν πάντα το ίδιο μονοπάτι. Για να περιοριστεί ο αριθμός των διαθέσιμων μονοπατιών μεταξύ των συνεργατών, το Crowds είναι αρμόδιο να τροποποιεί τα μονοπάτια κάθε είκοσι τέσσερις ώρες (Reiter & Rubin, 1998).

6.2.4. Εργαλειο 4:Το λογισμικό Hordes

Το λογισμικό Hordes χρησιμοποιεί πολλαπλούς πληρεξούσιους παρόμοιους με αυτούς που χρησιμοποιούνται στο πρωτόκολλο Crowds για την ανώνυμη δρομολόγηση ενός πακέτου. Ταυτόχρονα, όμως χρησιμοποιεί και υπηρεσίες πολλαπλής δρομολόγησης για την ανώνυμη δρομολόγηση της απάντησης στον δημιουργό-ιδρυτή του μηνύματος. Αποτελεί δε, το πρώτο πρωτόκολλο ανωνυμίας που εκμεταλλεύεται τα αποτελέσματα της απόδοσης και ανωνυμίας βάσει της πολλαπλής δρομολόγησης IP (IP multicast routing). Σε γενικές γραμμές βασίζεται στην αρχή της πολλαπλής δρομολόγησης, δηλαδή στην ύπαρξη μιας IP διεύθυνσης
για πολλούς Η/Υ. Τα δεδομένα δεν αναφέρονται σε ορισμένο Η/Υ, αλλά σε πολλαπλές διευθύνσεις, οπότε είναι, γενικά, δύσκολο να αποκαλυφθεί με ακρίβεια το μέλος στο οποίο αναφέρονται τα δεδομένα, αφού κάθε ξεχωριστή διεύθυνση αναφέρεται σε πολλά μέλη (Levine & Shields, 2002). Οι βασικές αρχές λειτουργίας του πρωτοκόλλου αυτού είναι (Levine & Shields, 2002):

(i). Όσο αυξάνει ο βαθμός ανωνυμίας δεν αυξάνει και ο βαθμός δυσκολίας εφαρμογής του πρωτοκόλλου στους διάφορους δεσμούς,

(ii). Οι απαιτήσεις παραβίασης του συστήματος αυξάνονται ή τουλάχιστον δεν μειώνονται με την αυξανόμενη χρήση

και

(iii). Οι απαιτήσεις είναι τέτοιες που αποθαρρύνουν τον πιθανό εισβολέα.

Το Hordes χρησιμοποιεί πολλούς πληρεξούσιους για να στέλνει το μήνυμα στον
Παραλήπτη, ενώ για την απάντηση χρησιμοποιεί τεχνικές multicasting. Σε θέματα απόδοσης απαιτεί μέσο χρόνο που υπερβαίνει ελαφρώς του μισού αντιστοίχου του Crowds. Περιλαμβάνονται οι φάσεις της αρχικοποίησης και της μετάδοσης των δεδομένων και σκοπό της φάσης αρχικοποίησης αποτελεί μια αυθεντική λίστα των άλλων μελών του πλήθους (Levine & Shields, 2002).

6.2.5. Εργαλειο 5:Το λογισμικό Freedom

Το λογισμικό Freedom σχεδιάστηκε για να προστατεύσει την ιδιωτικότητα των χρηστών που αποστέλλουν ηλεκτρονικά μηνύματα, φυλλομετρούν στον ιστό, συμμετέχουν σε ομάδες και συνομιλίες μέσω διαδικτύου. Το δίκτυο Freedom εκτελείται υπεράνω του διαδικτύου, και χρησιμοποιεί πολλαπλά επίπεδα κρυπτογράφησης για να επιτρέπεται σε ένα χρήστη-Freedom να εκφράζεται με ποικιλία ψευδώνυμων. Έτσι διασφαλίζεται η απόκρυψη των πραγματικών IP διευθύνσεων των χρηστών, των διευθύνσεων ηλεκτρονικού ταχυδρομείου και άλλων πληροφοριών που θα μπορούσαν να παραβιαστούν από ωτακουστές και από ενεργές επιθέσεις παραβίασης της ιδιωτικότητας των χρηστών (Goldberg & Shostack, 1999).

Οι χρήστες ενθαρρύνονται για τη δημιουργία ψευδωνύμων (nyms) για κάθε περιοχή δραστηριότητας στην οποία είναι επιθυμητή η διατήρηση της ανωνυμίας τους. Τα nyms που χρησιμοποιούνται δεν μπορούν να διασυνδεθούν μεταξύ τους με σκοπό την παραβίαση της ανωνυμίας. Έτσι δεν είναι δυνατόν να γνωρίζει κάποιος αν δύο ηλεκτρονικές διευθύνσεις ανήκουν στο ίδιο ή σε διαφορετικά πρόσωπα. Το Freedom προστατεύει την ιδιωτικότητα των χρηστών διαμέσω των υποστηριζόμενων πρωτοκόλλων της υπηρεσίας πληρεξούσιου. Αποστέλλει τα πακέτα με τη βοήθεια ενός ιδιωτικού δικτύου πριν αυτά προωθηθούν στο διαδίκτυο. Το εν λόγω δίκτυο το διαχειρίζεται και το υποστηρίζει η εταιρεία Zero-Knowledge, Inc και ως συνεπεία οι κόμβοι του δικτύου επεξεργάζονται επίσης από το περιβάλλον της Zero-Knowledge, Inc ή από άλλους συνεργάτες, έτσι ώστε κανένας χειριστής να μην έχει συνολική γνώση για το είδος των δεδομένων που κυκλοφορούν (Goldberg & Shostack, 1999).

“Πλεονεκτήματα” ανώνυμης περιήγησης στο Darknet

Ένας έμπειρος / υποψιασμένος χρήστης του Διαδικτύου, ο οποίος θέλει να προμηθευτεί απαγορευμένα φαρμακευτικά σκευάσματα διαθέσιμα online, θα απέφευγε να πληκτρολογήσει σχετικούς όρους αναζήτησης σε έναν συνηθισμένο περιηγητή (browser). Αντίθετα, θα προτιμούσε να περιηγηθεί online ανώνυμα, έτσι ώστε να είναι (σχεδόν) αδύνατο για τις Αρχές επιβολής του Νόμου να ανακαλύψουν την IP διεύθυνσή του και κατ' επέκταση την τοποθεσία της φυσικής του κατοικίας. Το ίδιο ισχύει και για τους πωλητές των απαγορευμένων σκευασμάτων, που, ομοίως, δεν είναι διατεθειμένοι να θέσουν σε λειτουργία ένα online κατάστημα για το οποίο οι διωκτικές Αρχές θα μπορούσαν να προσδιορίσουν διασυνδέσεις με τον πραγματικό κόσμο (φυσική τοποθεσία, ονοματεπώνυμα διαχειριστών / ιδιοκτητών, κ.λπ.).

Πέρα, βέβαια, από την αγοραπωλησία απαγορευμένων ουσιών ή άλλων προϊόντων σχετιζομένων με εγκλήματα, υπάρχουν κι άλλοι λόγοι που οδηγούν τους χρήστες στο Darknet και στην “ανώνυμη” περιήγηση. Χαρακτηριστικότερα παραδείγματα αποτελούν οι πολίτες που επιδιώκουν τη διασφάλιση του απορρήτου της επικοινωνίας τους (π.χ. καταγραφή δεδομένων επικοινωνίας από κρατικές υπηρεσίες για λόγους ασφάλειας), οι απασχολούμενοι σε οργανισμούς που θέλουν να παραδώσουν κρυφά σε δημοσιογράφους απόρρητη αλληλογραφία που διαχειρίζονται και οι κάτοικοι χωρών που λόγω της επικρατούσας πολιτικής κατάστασης επιθυμούν να εκφραστούν δημόσια ή να επικοινωνήσουν μέσω του “Επιφανειακού Web”, αλλά φοβούνται για τις συνέπειες ανακάλυψής τους. Σημειώνεται ότι στην τελευταία περίπτωση, η χρήση του Darknet εκτιμάται ότι συνδέθηκε στενά με το φαινόμενο της “Αραβικής Άνοιξης”. Ειδικά για τις κατηγορίες εγκληματικών δραστηριοτήτων, όπου η ανωνυμία που διασφαλίζει το Darknet μπορεί να διαδραματίσει καθοριστικό ρόλο, θα αναφερθούμε στη συνέχεια.

6.3. Η εξέλιξη του Darknet

Ο όρος Darknet επινοήθηκε το 2002 εισήχθη από τον Clarke I., στην διπλωματική του εργασία στο Πανεπιστήμιο του Εδιμβούργου το 1995. Ο Clarke δημιούργησε το λογισμικό ανοικτού κώδικα freenet, ένα νέο επαναστατικό τρόπο χρησιμοποίησης του διαδικτύου, χωρίς οι χρήστες του να γίνονται αντιληπτοί.(Εικονα 7) Το Darknet δημιουργήθηκε με σκοπό να αντιμετωπιστούν οι απειλές προσφυγής, η αποκεντρωμένη P2P τεχνολογία και ο αποκλεισμός του έλεγχου από τον φορέα παροχής υπηρεσιών, ώστε να καθίσταται δυσκολότερη η παρακολούθηση των ενεργειών των χρηστών. Τα δίκτυα P2P μπορούν και διατηρούν ένα βασικό χαρακτηριστικό, ότι δεν είναι ανώνυμα. Παρά το γεγονός ότι η κοινή χρήση αρχείων και οι δραστηριότητες των χρηστών στα δημόσια δίκτυα P2P είναι δύσκολο να εντοπιστούν, αυτό δεν είναι αδύνατο. Έτσι στους χρήστες της Gnutella, καθώς και άλλων δικτύων τύπου-BitTorrent, επιτρέπεται ο προσδιορισμός των παραμέτρων του διακομιστή, ενώ στα αποκεντρωμένα δίκτυα αποκαλύπτεται η διεύθυνση IP και δίνεται η ικανότητα ανταλλαγής αρχείων. Έτσι, είναι δυνατόν να ανιχνευθούν παραβατικές συμπεριφορές και να προσδιοριστούν κατηγορίες παράνομων πράξεων. Επιπλέον, τα αποκεντρωμένα δίκτυα δεν παραμένουν ιδιωτικά, με δεδομένο ότι οι χρηστές επικοινωνούν ομαδικά στο διαδίκτυο (Wood, 2010).

Στα τελικά βήματα στη διαδικασία εξέλιξης των P2P προέκυψε η ανάγκη για την μετατόπιση της προσοχής προς τους απλούς χρηστές. Έτσι, η δισκογραφική βιομηχανία RIAA έχει μηνύσει πάνω από 15000 άτομα για παραβίαση πνευματικών δικαιωμάτων. Για να απαλλαγούν από την ευθύνη, οι καταναλωτές απαίτησαν οι P2P προγραμματιστές να βελτιώσουν τα κατανεμημένα δίκτυα ώστε να προστατεύουν οι χρήστες από την ευθύνη. Ταυτόχρονα να τους παρέχουν την ανωνυμία, προστασία της ιδιωτικής ζωής, και αυξημένο έλεγχο ασφαλείας. Αυτές οι νεότερες εκδόσεις των κατανεμημένων δικτύων, γνωστή ως Darknets, συνιστούν σοβαρή απειλή για την επιβολή των πνευματικών δικαιωμάτων στο διαδίκτυο αποκρύπτοντας τη συμπεριφορά των χρηστών από την ανίχνευση (Wood, 2010).

Εικονα 7.Σχηματική απεικόνιση του Darknet.(https://blogstermind.wordpress.com/tag/darknet-conversations/)

Σύμφωνα με εκτιμήσεις που πραγματοποιηθήκαν από το Πανεπιστήμιο Berkeley της Καλιφόρνια το 2011 το Deepweb αποτελούνταν ≈ από 91000 Tbytes. Αντίθετα το επιφανειακό web (που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης) ≈ 167 Tbytes. Την ίδια χρονιά το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200000000 βίντεο, συνολικού μεγέθους 5000 Tbytes (Wood, 2010). Για να κατανοήσουμε καλύτερα τη λειτουργία του Darknet, μπορούμε να φανταστούμε το διαδίκτυο ως ένα τεράστιο παγόβουνο, η κορυφή του οποίου περισσεύει ελάχιστα από τη θάλασσα ενώ ο τεράστιος όγκος του κρύβεται στο βυθό (Εικόνα 7). Σε αυτή την περίπτωση η μύτη του παγόβουνου είναι οι ιστοσελίδες που χρησιμοποιούμε καθημερινά, όπως το Google και το YouTube. Μια τεράστια σωρεία πληροφοριών και ιστοσελίδων κρύβεται στο βυθό και δεν είναι προσβάσιμη από τα συμβατικά browsers. Εισερχόμενοι στο Facebook επί παραδείγματι, η ανταλλαγή μηνυμάτων αλλά και το ανέβασμα φωτογραφιών και άλλων αρχείων αφήνει πάντα πίσω αόρατα ηλεκτρονικά ίχνη, τα οποία καταγράφουν και ταξινομούν όλες αυτές τις πληροφορίες. Από την άλλη πλευρά, ο εντοπισμός αντίστοιχων πληροφοριών είναι σχεδόν αδύνατος στο Darknet. Το Darknet λειτουργεί με πολύ χαμηλές ταχύτητες και η πλοήγηση

γίνεται με όρους άκρας μυστικότητας (Wood, 2010).

Το Διαδίκτυο έχει εξελιχθεί σε μια παγκόσμια πλατφόρμα μέσω της οποίας ο καθένας μπορεί εύκολα να διαδώσει οτιδήποτε και να ανταλλάξει ιδέες. Έχει παρά πολλά πλεονεκτήματα αλλά η κακή χρήση του Διαδικτύου έχει γίνει όλο και πιο σοβαρή. Τρομοκρατικές οργανώσεις, εξτρεμιστικές ομάδες, ομάδες μίσους και φυλετικών ομάδων έχουν διογκωθεί και με τη χρήση του Web προωθούν την ιδεολογία τους. Η χρήση του Web διευκολύνει την εσωτερική επικοινωνία ώστε να επιτεθούν στους εχθρούς τους και να διεξάγουν εγκληματικές δραστηριότητες. Εκεί οι τρομοκράτες μπορούν να εξαπολύσουν επιθέσεις σε τέτοιες κρίσιμες υποδομές, όπως μεγάλα sites ηλεκτρονικού εμπορίου και κυβερνητικά δίκτυα (Gellman 2002). Αντάρτες στο Ιράκ έχουν δημοσιεύσει μηνύματα Web ζητώντας πυρομαχικά, υποστήριξη, χρηματοπιστωτικές και εθελοντές (Blakemore 2004). Ως εκ τούτου, έχει καταστεί σημαντικό να συγκεντρωθούν πληροφορίες από το Web, ώστε επιτρέπει καλύτερη κατανόηση και ανάλυση των τρομοκρατικών και εξτρεμιστικών ομάδων.

Μεγάλο μέρος των πληροφοριών που είναι αποθηκευμένες σε βάσεις δεδομένων των μηχανών αναζήτησης όπου συλλέγονται και αναλύονται για μετασχηματισμό σε νοημοσύνη και γνώση όπου θα ενισχυθεί η κατανόηση των δραστηριοτήτων των τρομοκρατών. Ωστόσο, οι μηχανές αναζήτησης συχνά ξεπερνούν τους χρήστες με την παραγωγή καταλόγων και άσχετα αποτελέσματα και έτσι έχουμε τη δημιουργία προβλημάτων με την υπερφόρτωση πληροφοριών. Σχετικές αλλά αόριστες πληροφορίες καθιστά δύσκολο να αποκτήσουν μια ολοκληρωμένη περιγραφή της τρομοκρατικής ομάδας ή ένα θέμα της τρομοκρατίας.

Πολλοί πόροι στο Web περιέχουν πληροφορίες σχετικά με την τρομοκρατία, αλλά ένα σχετικά μικρό ποσοστό προέρχεται από τους ίδιες τις τρομοκρατικές ομάδες, και τα δεδομένα συχνά μπορεί να είναι παραπλανητικά. Πολλές τρομοκρατικές ιστοσελίδες δεν χρησιμοποιούν τα αγγλικά, έτσι οι ερευνητές οι οποίοι δεν γνωρίζουν τη γλώσσα τους δεν είναι σε θέση να καταλάβουν το περιεχόμενο.

Τα τελευταία χρόνια, έχουν υπάρξει πολλές μελέτες από διάφορες οπτικές γωνίες αναλύοντας την παρουσία του Internet του μίσους και εξτρεμιστικές ομάδες. Η χρήση του Διαδικτύου από αυτές τις ομάδες έχει προκαλέσει το ενδιαφέρον της έρευνας τρομοκρατίας σε διάφορες κοινωνικές επιστήμες συμπεριλαμβανομένης της ψυχολογίας, της κοινωνιολογίας, της εγκληματολογίας, και πολιτικών επιστημών. Επιστήμονες που μελετούν

την εξόρυξη web και εξαγωγή πληροφοριών και αναλυτές ασφαλείας και ασχολούνται με την πατρίδα και τις εθνικές πολιτικές και την ασφάλεια των άλλων.

Ωστόσο, οι ιστοσελίδες και τα φόρουμ των εξτρεμιστικών και τρομοκρατικών ομάδων αναδύονται γρήγορα, συχνά εξίσου γρήγορα εξαφανίζονται.
Έτσι, πολλοί ερευνητές, φοιτητές, αναλυτές, και άλλοι αντιμετωπίζουν δυσχέρειες στον εντοπισμό, τη συλλογή και την ανάλυση αυτού του περιεχομένου.

Ενώ το διαδίκτυο έχει γίνει μια παγκόσμια πλατφόρμα για την επικοινωνία, οι τρομοκράτες μοιράζονται την ιδεολογία τους και επικοινωνούν με τα μέλη βάσει του Darknet. Επί του παρόντος, τα προβλήματα επικοινωνίας και η δυσκολία να αποκτηθεί μια ολοκληρωμένη εικόνα των τρομοκρατικών δραστηριοτήτων εμποδίζουν την αποτελεσματική και αποδοτική ανάλυση των τρομοκρατικών πληροφοριών στο διαδίκτυο. Για να προβλεφθούν και να αποκλειστούν πιθανές τρομοκρατικές δραστηριοτήτων, έχει αναπτυχθεί μια νέα μεθοδολογία για τη συλλογή και την ανάλυση πληροφοριών από το Darknet. Η μεθοδολογία αυτή περιλαμβάνει τη συλλογή πληροφοριών, την ανάλυση τους βάσει τεχνικών πιθανοτήτων και προσπαθεί να εκμεταλλευτεί διάφορες πηγές πληροφοριών. Οι Chen et al., (2006) συνέλεξαν και ανάλυσαν πληροφορίες από 39 ιστοσελίδες Τζιχαντιστών, αναλύοντας την απεικόνιση του περιεχομένου τους τις σχέσεις, και τα επίπεδα δραστηριότητας τους. Η αξιολόγηση των εμπειρογνωμόνων έδειξαν ότι η μέθοδος είναι πολύ χρήσιμη και πολλά υποσχόμενη, έχοντας ένα υψηλό δυναμικό για να βοηθήσει στην έρευνα και την κατανόηση των τρομοκρατικών δραστηριοτήτων και στον εντοπισμό πυρήνων τρομοκρατών. Οι προσπάθειες αυτές θα βοηθήσουν τους ερευνητές να εντοπίζουν και να προλαμβάνουν τρομοκρατικές επιθέσεις (Chen et al., 2006).

Οι αναλυτές αντιτρομοκρατικής νοημοσύνης καταγράφουν την παρουσία στο διαδίκτυο των τρομοκρατών, ομάδων μίσους, και άλλων εξτρεμιστών μέσα από τη μελέτη των πρωτογενών πηγών συμπεριλαμβανομένης και των δικών τους ιστοσελίδων, βίντεο, και φόρουμ συζητήσεων στο Διαδίκτυο. Με προσεκτική ανάλυση, μπορούν να αποκαλυφθούν τάσεις ανάλογα με τα θέματα και τις συζητήσεις, την αλληλουχία των ιδεών, καθώς και τις σχέσεις μεταξύ τους. The DarkWeb φόρουμ κατασκευάστηκε αρχικά για να επιτρέψει την εξέταση, της χρήσης των forums του διαδικτυου από τρομοκρατικές ή εξτρεμιστικές ομάδες. Η βίντεο portal διευκολύνει την μελέτη των βίντεο που χρησιμοποιούν αυτές οι ομάδες. Και

οι δύο πύλες είναι διαθέσιμες για τους ερευνητές κατόπιν αιτήματος. Το εν λόγω βίντεο Portal μόλις πρόσφατα έγινε προσιτό σε ερευνητές και προορίζεται να χρησιμεύσει ως μια άλλη δυνητική πηγή για πληροφορίες. Λαμβάνοντας υπόψη τις δυσκολίες της αναγνώρισης και εντοπισμού της πηγής των βίντεο αυτών, με δεδομένο ότι είναι συνήθως λογοκρίνονται το ενδιαφέρον για τα φόρουμ και τα portal αυτά είναι ιδιαίτερα έντονο. Μια περίοδος αξιολόγησης μπορεί όμως να εξασφαλίσει την πιθανή χρηστικότητα τους (Chen et al.).

6.4. Χαρακτηριστικά του Darknet

Ο κόσμος του Darknet μπορεί να ταξινομηθεί σε τέσσερεις κατηγορίες: (i). Μαύρη αγορά (ναρκωτικά, όπλα, υλικό για τρομοκρατικές ενέργειες, ψεύτικες άδειες-ταυτότητες), (ii).Πειρατικό υλικό (απαγορευμένα λογισμικά, βιβλία, παιχνίδια, μουσική, τηλεοπτικές σειρές), (iii). Ιστοσελίδες προπαγάνδας τρομοκρατικών οργανώσεων που κάνουν κήρυγμα για ιερό πόλεμο και αρκετές από αυτές χρησιμοποιούν κρυπτογραφημένη γλώσσα και πληροφορίες συνάντησης με σκοπό τη στρατολόγηση νέων μελών, και (iv). Απαγορευμένα social media και forums, οπού ομάδες συζητήσεων χάκερ, ακτιβιστών, επιστημόνων, περίεργων ανθρώπων και παιδεραστών έχουν δημιουργήσει τις δικές τους εφαρμογές κοινωνικής δικτύωσης (Wood, 2010; saferinternet.gr).

Ήταν και παραμένει ένα παράλληλο δίκτυο με το διαδίκτυο, το οποίο σβήνει αυτόματα την ταυτότητα του χρήστη. Ωστόσο, πολύ γρήγορα το Darknet πέρασε στα χέρια οργανωμένων εγκληματικών οργανώσεων και διακινητών παράνομων υλικών. Πλέον το Darknet έχει εξελιχθεί σε ένα παράλληλο κόσμο. Ο χρήστης του Darknet, είναι ανώνυμος, καθώς η ταυτότητα του υπολογιστή του, το ID δηλαδή, δεν είναι φανερό. Ακόμα και εάν κάποιος ανακαλύψει την ταυτότητα του υπολογιστή του που περιπλανήθηκε στο σκοτάδι, η πραγματική ταυτότητα του χρήστη είναι αλλοιωμένη με αποτέλεσμα την απόλυτη ανωνυμία (Wood, 2010; saferinternet.gr).

Συνοψίζοντας ορισμένα από τα χαρακτηριστικά του Darknet, αναφέρουμε (Wood, 2010; saferinternet.gr):

- Οι εξήντα, μόνον, από τις μεγαλύτερες βαθιά κρυμμένες τοποθεσίες web περιέχουν συνολικά περίπου 750 terabytes πληροφοριών -ήδη, αυτές από μόνες τους, υπερβαίνουν το μέγεθος του επιφανειακού web κατά σαράντα φορές,
- Το Darknet περιέχει περίπου 550 δισεκατομμύρια μεμονωμένα έγγραφα σε σύγκριση

με το 1 δισεκατομμύριο που υφίστανται στο επιφανειακό,

- Περισσότερες από 200000 βαθιά κρυμμένες ιστοσελίδες υπάρχουν σήμερα,
- Το Darknet είναι η μεγαλύτερη αναπτυσσόμενη κατηγορία των νέων πληροφοριών στο διαδίκτυο και η ενημέρωση του κοινού είναι πολύ μεγαλύτερη, ,
- Οι Darknet ιστοσελίδες τείνουν να είναι περιορισμένες, με βαθύτερο περιεχόμενο, σχετικά με τις αντίστοιχες του επιφανειακού web,
- Το περιεχόμενο Darknet είναι ιδιαίτερα σημαντικό για κάθε ανάγκη πληροφόρησης και αγοράς,
- Περισσότερο από το ήμισυ του περιεχομένου του Darknet βρίσκεται σε

συγκεκριμένες βάσεις δεδομένων, και

- Ένα 95% από το Darknet είναι προσβάσιμες πληροφορίες, που δεν υπόκεινται σε τέλη

ή συνδρομές.

Το Darknet έχει ορισμένα ιδιαίτερα χαρακτηριστικά: (i). *Το περιεχόμενο των βάσεων δεδομένων*: Οι βάσεις δεδομένων περιέχουν πληροφορίες που είναι αποθηκευμένες σε πίνακες που δημιουργούνται από προγράμματα, όπως το Access, Oracle, SQL Server, MySQL. Οι πληροφορίες που αποθηκεύονται σε βάσεις δεδομένων είναι προσβάσιμες μόνο αν αναζητηθούν και με τα δεδομένα που έχουν, να ανακτηθεί και έπειτα εμφανίζονται σε μια ιστοσελίδα. Αυτό είναι ευδιάκριτο από στατικές, αυτόνομες ιστοσελίδες, οι οποίες μπορεί κάποιος να έχει άμεση πρόσβαση. Ένα σημαντικό ποσό των πολύτιμων πληροφοριών στο web παράγεται από τις βάσεις δεδομένων, (ii). *Μη αρχεία κειμένου*, όπως εικόνες πολυμέσων, το λογισμικό και τα έγγραφα σε μορφές όπως η μορφή PDF, το Microsoft Word, Libre/Open Office, (iii). *Συζητήσεις και άλλες δραστηριότητες επικοινωνίας* στους ιστότοπους κοινωνικής δικτύωσης, όπως το Facebook και το Twitter, σελιδοδείκτες και αναφορές αποθηκεύονται σε κοινωνικές bookmarking sites, (iv). *Περιεχόμενο διαθέσιμο στις τοποθεσίες που προστατεύονται από κωδικό πρόσβασης* ή άλλους περιορισμούς. Μερικά από αυτά είναι η αμοιβή με βάση το περιεχόμενο και διατίθενται στους χρήστες τους με βάση διάφορα συστήματα ελέγχου ταυτότητας, και (v). *Η κάθετη αναζήτηση*: Μπορεί να υποβληθεί ερώτημα επικεντρώνοντας σε ένα συγκεκριμένο θέμα, τη βιομηχανία, τον τύπο του περιεχομένου, τη γεωγραφική θέση, τη γλώσσα, τον τύπο του αρχείου ή της ιστοσελίδας, το κομμάτι των δεδομένων και ούτω καθεξής (Wood, 2010; saferinternet.gr).

Το σύνολο των μη κατανεμημένων διευθύνσεων ενός δικτύου καλείται Darkaddress space. Το φαινόμενο του Darknet όμως εμφανίζεται και στο διαδίκτυο, όπου οι μη κατανεμημένες διευθύνσεις είναι πλέον ελάχιστες. Οι αιτίες για τις οποίες οι κόμβοι αυτοί δεν είναι προσβάσιμοι, είναι κατά κύριο λόγο πιο δυσάρεστοι. Το διαδίκτυο είναι χωρισμένο σε επίπεδα, με το υψηλότερο επίπεδο να είναι οι υπολογιστές των χρηστών και το χαμηλότερο οι κεντρικοί δρομολογητές των παροχών -παγκοσμίου κλίμακας-, που αλληλοσυνδέονται και αποτελούν τη ραχοκοκαλιά του διαδικτύου. Σε όσο χαμηλότερο επίπεδο ανήκει ένας δρομολογητής, τόσο περισσότερη κίνηση περνά μέσα από αυτόν εξυπηρετώντας το ανάλογο πλήθος διευθύνσεων. Είναι αντιληπτό πως ένας τέτοιος δρομολογητής λειτουργεί ως πύλη για τις διευθύνσεις που εξυπηρετεί. Αν λοιπόν ο δρομολογητής είναι απορυθμισμένος σε σχέση με είτε την εισερχόμενη είτε την εξερχόμενη κίνηση, αυτό θα τον κάνει μέρος του Darknet

ενός άλλου. Ο κύριος λόγος που κεντρικοί δρομολογητές έχουν ρυθμίσεις που περιορίζουν την προσβασιμότητα είναι η μείωση του φόρτου, με περικοπή του μεγέθους των πινάκων δρομολόγησης. Παρατηρούνται επίσης, όροι των συμβολαίων μεταξύ των παροχών που καθορίζουν σε ποια τμήματα του δικτύου του ενός θα έχουν πρόσβαση οι πελάτες του άλλου, δημιουργώντας έτσι στους πρώτους περιοχές του ιστού που τους απαγορεύεται η πρόσβαση. Μια έρευνα της Arbor Networks έδειξε πως σε αυτό ανήκουν 5% των κόμβων του ιστού, που ανέρχονται ≈ στους 100000000 διακομιστές (Wood, 2010).

Το Darknet δε θα μπορούσε φυσικά να μη γίνει αντικείμενο εκμετάλλευσης διάφορων κακόβουλων επιτήδειων. Αποτελεί ένα από τα μέσα που χρησιμοποιούνται κατεξοχήν για παράνομες ενέργειες όπως επιθέσεις DoS ή spamming. Πολλοί hackers εκμεταλλεύονται τις κακές ρυθμίσεις των δρομολογητών για να διεξάγουν επιθέσεις από Η/Υ που για το υπόλοιπο διαδίκτυο στην ουσία δεν υπάρχουν, καθώς δεν είναι δυνατή η επικοινωνία μαζί τους και εμφανίζονται καθόλου ή ελάχιστα σε πίνακες δρομολόγησης. Συχνά γίνεται επίσης αναδρομολόγηση πακέτων κακόβουλης κίνησης μέσα από διευθύνσεις του Darknet για να αποφευχθεί ο εντοπισμός της πηγής τους. Επιπλέον, hackers μπορούν να δημιουργήσουν τμήματα του Darknet καταλαμβάνοντας δρομολογητές και αλλάζοντας οι ίδιοι τις ρυθμίσεις τους (Wood, 2010).

Για να κατανοήσουμε όμως καλύτερα τους λόγους για τους οποίους ένα μεγάλος μέρος αυτών των πηγών δεν είναι εμφανής, ας δούμε κάποιους σημαντικούς λόγους της απόκρυψης τους:(ι). Το δυναμικά παραγόμενο περιεχόμενο δηλαδή οι δυναμικές ιστοσελίδες οι οποίες δημιουργούνται ως αποτέλεσμα της εκτέλεσης κάποιας ερώτησης ή προσπελαύνονται μόνο μέσω κάποιας φόρμας, (ii). Το μη συνδεδεμένο περιεχόμενο, δηλαδή οι ιστοσελίδες οι οποίες δεν περιέχουν συνδέσμους από ή σε άλλες ιστοσελίδες, και (iii). Το ιδιωτικό web εκείνοι δηλαδή οι ιστότοποι που απαιτούν εγγραφή και κωδικό πρόσβασης. Περιλαμβάνονται και ιστότοποι με περιεχόμενο περιορισμένης πρόσβασης, όπως ιστότοποι που περιορίζουν την πρόσβαση στις σελίδες τους με τεχνικό τρόπο και απαγορεύουν στις μηχανές αναζήτησης να πλοηγούνται στις ιστοσελίδες τους. Έτσι, οποιοδήποτε περιεχόμενο που δεν είναι σε μορφή HTML (κείμενα που συμπεριλαμβάνονται σε multimedia αρχεία ή που έχουν συγκεκριμένη μορφή την οποία δεν μπορούν να χειριστούν οι μηχανές αναζήτησης ή κείμενα που χρησιμοποιούν το πρωτόκολλο Gopher και αρχεία που βρίσκονται σε διακομιστές FTP και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης) δεν μπορεί να ανευρεθεί από τις κοινές μηχανές αναζήτησης όπως η Google. Οι μηχανές αναζήτησης ανακαλύπτουν περιεχόμενο στο διαδίκτυο, χρησιμοποιώντας webcrawlers και ακολουθώντας συνδέσμους και είναι αναποτελεσματική στην εύρεση πληροφοριών από το Darknet. Το

2005, η Yahoo έκανε ένα μικρό κομμάτι του Darknet ερευνήσιμο με τη χρήση των Yahoo Subscriptions. Αυτή η μηχανή αναζήτησης ψάχνει μόνο μέσω λίγων συνδρομητικών ιστοτόπων, και τέτοιοι ιστότοποι εμφανίζουν όλο τους το περιεχόμενο στα robots των μηχανών αναζήτησης, έτσι ώστε να εμφανίζονται στις αναζητήσεις των χρηστών, αλλά μετά εμφανίζουν στους χρήστες μία σελίδα για login ή συνδρομή (Wood, 2010).

Ένα μέρος του Darknet είναι προσβάσιμο μέσω του ανώνυμου δικτύου TOR. Η επίσκεψη σε ένα δικτυακό τόπο μέσω του TOR εκτρέπει τις συνδέσεις μέσα από μια τυχαιοποιημένη πορεία υπολογιστών άλλων χρηστών πριν από την επίτευξη του στόχου του web server, κρύβοντας ουσιαστικά την τοποθεσία σας από αυτόν το διακομιστή. Αντίθετα από τις κανονικές ιστοσελίδες, οι σελίδες του Darknet δεν έχουν φιλικές διευθύνσεις URL. Αντ' αυτού, αποτελούν μια φαινομενικά τυχαία σειρά χαρακτήρων που ακολουθείται από την κατάληξη ".onion" και παρέχει πρόσβαση σε αυτές τις κρυφές ιστοσελίδες. Στο Darknet υπάρχει το "Hidden Wiki" που παρέχει καταχωρήσεις αυτών των διευθύνσεων URL για να διευκολυνθεί η χρήση του Darknet. Επιπλέον, είμαστε σίγουροι πως δεν υπάρχουν υπολογιστές που αντιστοιχούν στις διευθύνσεις του, επομένως δεν είναι δυνατό να προκληθούν επιθέσεις προερχόμενες από αυτό. Οι διευθύνσεις του Darknet δεν είναι καταχωρημένες σε αρχεία καταγραφής κίνησης, ούτε αποστέλλουν πακέτα προς τον ιστό. Αυτό αντιπροσωπεύει μόνο ένα κλάσμα των συνολικών peer-to-peer αρχείων που ανταλλάσσονται, δεδομένου ότι αυτό είναι μόνο ένα χώρο και ένα πρωτόκολλο. Υπάρχουν ακόμη πολλοί χρήστες του σε άλλα δίκτυα ανταλλαγής αρχείων όπως το Kazaa, το Gnutella, και τα παρόμοια. Η καταγραφή και επεξεργασία των εισερχόμενων και εξερχόμενων πακέτων από διευθύνσεις του Darknet, είναι και ο σκοπός του Darknet server (Wood, 2010).

6.4.1. Πόσο μεγάλο είναι το Darknet;

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο Berkeley της Καλιφόρνια (University of California, Berkeley) το 2001 , το Darknet αποτελείται περίπου από 91.000 terabytes. Αντίθετα το επιφανειακό Web, που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης είναι περίπου 167 terabytes.

Η Βιβλιοθήκη του Αμερικάνικου Κονγκρέσου, υπολογίστηκε πως το 1997 είχε 3.000 terabytes. Το 2011, το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200 εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes.

Ο υπολογισμός του μεγέθους του web διαφέρει από πηγή σε πηγή και έτσι υπάρχει ένα μεγάλο περιθώριο λάθους και κανένας αριθμός δε μπορεί να θεωρηθεί ως ακριβής. Ωστόσο σχετικά με τον αριθμό των πηγών του Darknet υπάρχουν πιο ακριβείς εκτιμήσεις: Το 2004 ο He ανακάλυψε 300.000 deep web sites σε ολόκληρο το Web , και σύμφωνα με τον Shestakov, περίπου 14.000 Darknet sites υπήρχαν στο Ρώσικο τμήμα του Web το 2006.

Γενικά θα πρέπει να υπολογίσουμε ότι το βαθύ ίντερνετ όπως και το βαθύ κράτος που λένε οι κομμουνιστές είναι πολλαπλάσιο του επιφανειακού ιστού. Μοιάζει σε μεγάλο βαθμό με το SEO, όπου το SEO* που φαίνεται είναι πολύ μικρό σε αναλογία με το SEO που δεν φαίνεται.
*Οπου **SEO→ Search Engine Optimization - SEO →** οργανική βελτιστοποίηση και η πληρωμένη καταχώριση με τη δημιουργία διαφημιστικής καμπάνιας.

Κανείς δεν μπορεί να υπολογίσει με ακρίβεια σήμερα το μέγεθος του Darknet μια και αυτό είναι συνεχώς μεταβαλλόμενο και αυξανόμενο σε μέγεθος. Συνεχώς καινούριες ιστοσελίδες προστίθενται στις παλιές και επειδή ο στόχος τους είναι να μείνουν κρυφές, είναι αρκετά δύσκολο με τις υπάρχουσες μηχανές αναζήτησης να τις βρούμε.
Θα πρέπει δηλαδή να υπάρξει μια μεγάλη αλλαγή στη δομή του αλγορίθμου της Google, ή να δημιουργηθεί μια νέα μηχανή αναζήτησης για να μπορέσουμε να δούμε το βαθύ ίντερνετ.

Η πληροφορική της τρομοκρατίας στηρίζεται σε μεγάλο βαθμό στη γνώση του τομέα της τρομοκρατίας και βάσεις δεδομένων.

Το Διαδίκτυο ενεργεί ως ιδανική μέθοδος για τις πληροφορίες και τη διάδοση προπαγάνδας(Whine 1997 Gustavson και Sherkat 2004). Μέσω του υπολογιστή η επικοινωνία προσφέρεται με έναν γρήγορο, ανέξοδο, και ανώνυμο τρόπο επικοινωνίας για τις εξτρεμιστικές ομάδες (Crilley 2001). Οι εξτρεμιστικές ομάδες χρησιμοποιούν συχνά τον Ιστό για να προωθήσουν την έχθρα και βία (Glaser 2002). Αυτή η προβληματική άποψη του διαδικτύου και είναι συχνά αναφερόμενος ως σκοτεινό διαδίκτυό (DarkNet) (Chen 2006).

Ένα σημαντικό συστατικό του σκοτεινού διαδικτύου (DarkNet) είναι εξτρεμιστικά φόρουμ που κρύβονται βαθιά μέσα στο διαδίκτυο. Πολλοί έχουν δηλώσει την ανάγκη για συλλογή και ανάλυση των φόρουμ του DarkNet. (Burris και λοιποί 2000 Schafer 2002).

Το Διαδίκτυο έχει εξελιχθεί σε μια παγκόσμια πλατφόρμα μέσω της οποίας ο καθένας μπορεί να εύκολα διαδώσει οτιδήποτε και να ανταλλάξει ιδέες. Έχει παρά πολλά πλεονεκτήματα αλλά η κακή χρήση του Διαδικτύου έχει γίνει όλο και πιο σοβαρή. Τρομοκρατικές οργανώσεις,εξτρεμιστικές ομάδες, ομάδες μίσους και φυλετικών ομάδων έχουν διογκοθεί και με τη χρήση του Web προωθουν την ιδεολογία τους. Η χρήση του Web διευκολύνει την εσωτερική επικοινωνία ώστε να επιτεθούν στους εχθρούς τους και να διεξάγουν εγκληματικές δραστηριότητες. Εκεί οι τρομοκράτες μπορούν να εξαπολύσουν επιθέσεις σε τέτοιες κρίσιμες υποδομές, όπως μεγάλα sites ηλεκτρονικού εμπορίου και κυβερνητικά δίκτυα (Gellman 2002). Αντάρτες στο Ιράκ έχουν δημοσιεύσει μηνύματα Web ζητώντας πυρομαχικά, υποστήριξη, χρηματοπιστωτικές και εθελοντές (Blakemore 2004). Ως εκ τούτου, έχει καταστεί σημαντικό να συγκεντρωθούν πληροφορίες από το Web, ώστε επιτρέπει καλύτερη κατανόηση και ανάλυση των τρομοκρατικών και εξτρεμιστικών ομάδων.

Η πρωτοφανής αύξηση του Διαδικτύου έχει οδηγήσει στην ιδιαίτερη εστίαση επάνω σε crawling /spidering τεχνικές τα τελευταία χρόνια. Οι crawlers είναι ορισμένες τεχνικές που ορίζονται ως «λογισμικό προγράμματα που διαβαίνουν το διάστημα πληροφοριών World Wide Web με την ακολουθία συνδέσεων υπερκειμένων και ανάκτησης των εγγράφων Ιστού από το τυποποιημένο πρωτόκολλο HTTP» (Cheong 1996) . Είναι προγράμματα που μπορούν να δημιουργήσουν μια τοπική συλλογή ή έναν δείκτη των μεγάλων όγκων δεδομένων από μια ιστοσελίδα (Cho και Garcia-Molina 2000).
Μια σημαντική ανησυχία είναι η δυνατότητα πρόσβασης στα δυναμικά φόρουμ του ιστού οπου συχνά απαιτούνται ιδιότητες μέλους. (Florescu και λοιποί 1998 Raghavan και Garcia-Molina 2001) Υπάρχει επίσης πολύγλωσσος ιστός περισσότερο από το 30% του ιστού είναι στις μη-αγγλικές γλώσσες (Chen και Chau 2003). Συνεπώς, το Darknet καλύπτει επίσης πολυάριθμες γλώσσες. Τα σκοτεινά φόρουμ περιέχουν πλούσιο περιεχόμενο που χρησιμοποιείται για στερεότυπες επικοινωνίες και τη διάδοση προπαγάνδας (Abbasi και Chen 2005 Zhou και λοιποί 2005 Qin και λοιποί 2005). Αυτά τα φόρουμ περιέχουν στατικά και δυναμικά αρχεία κειμένων και διάφορες μορφές πολυμέσων (π.χ., εικόνες, ήχος, βιντεο κλπ). Η συλλογή τέτοιων διαφορετικών ικανοποιημένων τύπων εισάγει πολλές μοναδικές

προκλήσεις που δεν αντιμετωπίζονται με τυποποιημένο καταχωρήσιμου αρχείο (κείμενο που βασίζεται).

Ως εκ τούτου ο σκοπός του Dark Web είναι να παρέχει μια ερευνητική υποδομή για χρήση από τους κοινωνικούς επιστήμονες και επιστήμονες πληροφορικής, αναλυτές πολιτικής και ασφάλειας, και άλλοι (Zhang et al. 2009). Το αρχείο αυτή τη στιγμή αποτελείται από 13 εκατομμύρια αποσπάσεις από 29 διεθνείς τζιχάντ φόρουμ . Αυτά τα φόρουμ συλλογικά έχουν φιλοξενήσει 340.000 μέλη των οποίων η συζητήσεις καλύπτουν ένα ευρύ φάσμα κοινωνικοπολιτικών, πολιτιστικών, ιδεολογικών και θρησκευτικών θεμάτων. Τα φόρουμ που συλλέγονται για το έργο αυτό είναι στα αραβικά, αγγλικά, γαλλικά, γερμανικά, και ρωσικα.Τα φορουμ σε αραβική γλώσσα περιλαμβάνουν σημαντικά τζιχάντ web sites, μερικά από τα οποία παρακολουθούνται από το Κέντρο Open Source CIA. Τα φόρουμ σε αγγλική γλώσσα αντιπροσωπεύουν τόσο εξτρεμιστικές και πιο μέτριες ομάδες, προκειμένου να διευκολυνθεί η μελέτη των διαδικασιών ριζοσπαστικοποίησης πάροδο του χρόνου. Τρία γαλλικά φόρουμ, και τα εννιά φόρουμ στα γερμανικά και ρωσικά, παρέχουν αντιπροσωπευτικά περιεχόμενα για εξτρεμιστικές ομάδες. Το περιεχόμενο ενημερώνεται τακτικά, προκειμένου να παραμείνει φρέσκο. Περιλαμβάνει εργαλεία για την αναζήτηση, περιήγηση, τη μετάφραση και την ανάλυση και οπτικοποίηση. Το Dark Web Forum Portal παρέχει web-enabled πρόσβαση σε αυτά τζιχάντ web φόρουμ (Zhang et al. 2009).

6.4.2. Τοπολογική ανάλυση Darknet

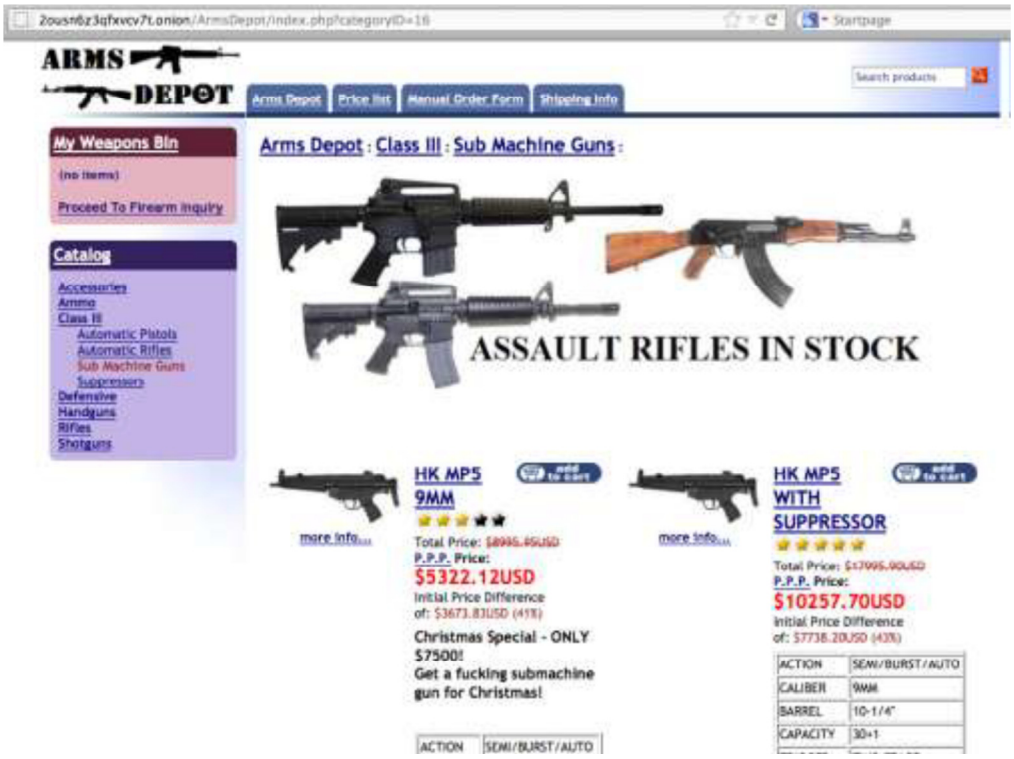
Τα τελευταία χρόνια, οι επιστήμονες έχουν αποκαλύψει τις ιδιότητες μιας ευρείας ποικιλίας των πολύπλοκων συστημάτων που χαρακτηρίζονται ως δίκτυα μεγάλης κλίμακας σε συνεργασία με το World Wide Web, το Διαδίκτυο ηλεκτρικών δικτύων ηλεκτρικής ενέργειας, και βιολογικά δίκτυα, μεταξύ πολλών άλλων. Ένα κομμάτι που λείπει σε αυτή την εικόνα, ωστόσο, είναι η ανάλυση σχετικά με την τοπολογία του "Σκοτεινού Διαδικτύου" δίκτυα που είναι κρυμμένα από την κοινή θέα αλλά θα μπορούσε να έχουν καταστροφικές συνέπειες για την κοινωνία και την οικονομία μας. Τρομοκρατικά δίκτυα, τα ναρκωτικά παράνομη διακίνηση, το λαθρεμπόριο όπλων δίκτυα συμμοριών, και πολλές άλλες μυστικές ομάδες είναι όλα σκοτεινά δίκτυα.

Τοπολογική ανάλυση, η οποία επικεντρώνεται στα στατιστικά χαρακτηριστικά της δομής του δικτύου είναι μια νέα μεθοδολογία για τη μελέτη των δικτύων μεγάλης κλίμακας (Albert και Barabási 2002? Watts και Strogatz 1998).

6.5. Μηχανές αναζήτησης

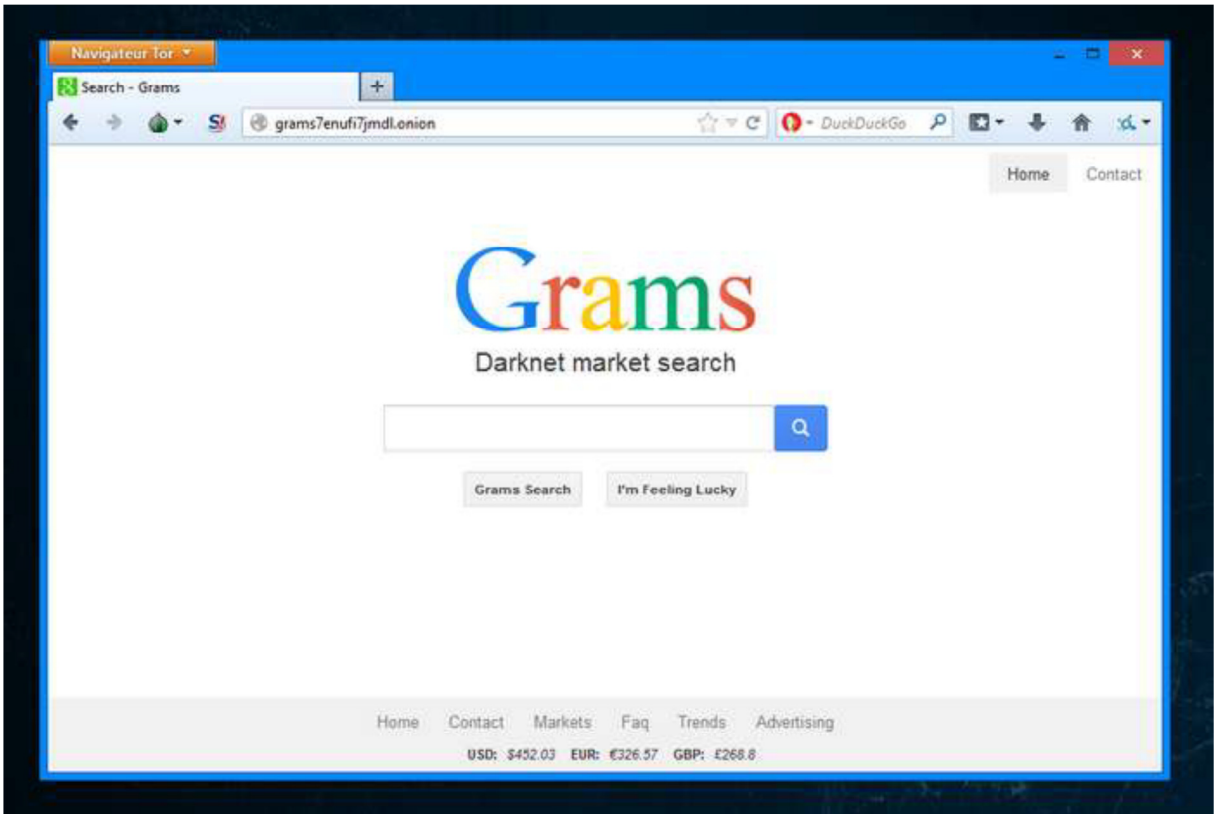
Οι μηχανές αναζήτησης αποτελούν μια λειτουργία ρυθμιστή και προσφέρουν γενική πρόσβαση σε πληροφορίες λόγω της απλότητας, της ταχύτητας αναζήτησης και ευρείας κάλυψης. Η αποκάλυψη του μέρους αυτού του Darknet είναι σημαντική για την επιστημονική κοινότητα. Εντός των τελευταίων ετών, οι επαγγελματίες χρήστες και έμποροι πληροφοριών βρήκαν ότι η τεχνολογία των μηχανών αναζήτησης μπορεί εύκολα να κατασκευάσει ακόμη και ακαδημαϊκό περιεχόμενο (Lewandowski, 2006), που όλο και περισσότερο παρέχεται αποκλειστικά στο διαδίκτυο. Τέτοιου τύπου μηχανές αποτελούν τα Open Access, Google Scholar και Scopus, Z39.50 και Open Archives Initiative (Πρωτόκολλο Συγκομιδής Μεταδεδομένων). Τα υπάρχοντα εργαλεία αναζήτησης και οι προσεγγίσεις δείχνουν τις δυνατότητες για να κάνει ορατό το AIW, όπως η οικοδόμηση μιας συλλογής από τις μεγαλύτερες βάσεις δεδομένων, η χρήση των informetric διανομής και η ταξινόμηση του περιεχόμενου του (Lewandowski, 2006).

Μιλάμε συχνά για underground κοινότητες, παράνομες ιστοσελίδες ή μαύρες αγορές, αλλά λόγω της φύσης των συγκεκριμένων ιστότοπων και υπηρεσιών, οι οποίες είναι προσβάσιμες μέσω του δικτύου TOR, οι χρήστες δεν μπορούν να αποκτήσουν εύκολα πρόσβαση σε αυτές. Οι underground αγορές συνήθως προσφέρουν ναρκωτικά, όπλα, εργαλεία hacking ή παράνομες υπηρεσίες, και για τον εντοπισμό τους οι χρήστες πρέπει να πληκτρολογήσουν περίπλοκες και συγκεκριμένες διευθύνσεις URL στο πρόγραμμα περιήγησης TOR που χρησιμοποιούν (Εικόνα 8). Επίσης οι σκοτεινοί ιστότοποι αλλάζουν συχνά διευθύνσεις URL για λόγους ασφάλειας, κάνοντας ακόμη πιο δύσκολο τον εντοπισμό τους (saferinternet.gr).



Εικονα 8.Αγορές στο Darknet.(http://www.agoradrugs.com/tag/dark-web/)

Η πρώτη μηχανή αναζήτησης με την ονομασία Grams (http://grams7enufi7jmdl.onion), η οποία διευκολύνει τον εντοπισμό παράνομων διαδικτυακών αγορών στο Darknet, κυκλοφορεί σε beta έκδοση. Η μηχανή αναζήτησης Grams λειτουργεί όπως και αυτή της Google και ανιχνεύει αποτελέσματα από οκτώ διαφορετικές μαύρες αγορές, συμπεριλαμβανομένων των Agora, BlackBank, C9, Evolution, Mr.Nice Guy, Pandora, The Pirate Market και SilkRoad2. Μέχρι πρόσφατα, ακόμη κι αν είχε κανείς εγκαταστήσει το software, θα έπρεπε να γνωρίζει επίσης τη συγκεκριμένη διεύθυνση κάθε ιστοσελίδας που θέλει να επισκεφθεί. Ωστόσο, πριν από λίγες εβδομάδες, το Darknet απέκτησε την δική του μηχανή αναζήτησης Grams, που συγκεντρώνει αποτελέσματα από οκτώ online μαύρες αγορές και τις αγγελίες τους. Βέβαια, το κίνητρο του δημιουργού του Grams είναι το κέρδος και σύντομα θα αρχίσει να χρεώνει όσους θέλουν οι αγγελίες τους να εμφανίζονται ψηλότερα στα αποτελέσματα. Οι προγραμματιστές του Grams φαίνεται ότι προσπαθούν να έρθουν σε επαφή με τους κάτοχους και άλλων underground αγορών, προκειμένου να συμπεριλάβουν ακόμη περισσότερες ιστοσελίδες στα αποτελέσματα αναζήτησης (Εικόνα 9, saferinternet.gr).



Εικονα 9.Η μηχανή αναζήτησης Grams.(http://www.cosmara.gr/2014/05/grams-darknets.html)

Μια νέα μηχανή αναζήτησης, την οποία ανάπτυξε η DARPA υπηρεσία του Πενταγώνου έχει στόχο να ρίξει φως στο Darknet, το οποίο δεν αναγνωρίζουν οι συμβατικές μηχανές αναζήτησης, όπως το Google και το Bing. Όπως αναφέρεται σε σχετικό δημοσίευμα του Wired, το εν λόγω project, υπό την κωδική ονομασία Memex, είναι στα σκαριά εδώ και έναν χρόνο και αναπτύσσεται από 17 διαφορετικές ομάδες που συνεργάζονται με την DARPA. Ενδεικτικά, το Google, το Yahoo και το Bing μπορούν να αναγνωρίζουν μόλις το 5% του Διαδικτύου- το Memex επιδιώκει τη δημιουργία ενός καλύτερου χάρτη. Για αυτό τον σκοπό το Memex δεν θα ψάχνει απλά υλικό από τις ιστοσελίδες που αγνοούνται από τις κανονικές μηχανές αναζήτησης, αλλά παράλληλα καταγράφει και χιλιάδες sites από το Darknet -όπως το διαβόητο Silk Road και άλλα που εντάσσονται στο ευρύτερο πλαίσιο του ανώνυμου δικτύου TOR. Οι σελίδες αυτές είναι προσβάσιμες μόνο μέσω του TOR browser και σε αυτούς που γνωρίζουν ακριβώς τις διευθύνσεις τους. Αν και υπάρχουν σελίδες που έχουν καταχωρημένες κάποιες σελίδες τέτοιων Hidden Services, το μεγαλύτερο τμήμα τους παραμένει αόρατο. Επίσης, επιδιώκεται η χρήση αυτοματοποιημένων μεθόδων για την ανάλυση υλικού προκειμένου να βρεθούν κρυμμένοι σύνδεσμοι οι οποίοι είναι χρήσιμοι στις διωκτικές αρχές (saferinternet.gr).

DARPA

Μία νέα μηχανή αναζήτησης, την οποία αναπτύσσει η DARPA (Defense Advanced Research Projects Agency) του αμερικανικού Πενταγώνου έχει στόχο να «ρίξει φως» στη «σκοτεινή πλευρά» του Διαδικτύου: το αποκαλούμενο Dark Web, το οποίο δεν «πιάνουν» οι συμβατικές μηχανές αναζήτησης, όπως το Google και το Bing.(Εικονα 10)

Εικονα 10. D.A.R.P.A (http://truedemocracyparty.net/2013/09/google-is-d-a-r-p-a-defense-advanced-research-projects-agency-head-of-darpa-moves-to-google-old-news-just-a-reminder-the-internet-is-a-u-s-military-concept-t-d-p/)

Όπως αναφέρεται σε σχετικό δημοσίευμα του Wired, το εν λόγω project, υπό την κωδική ονομασία Memex, είναι στα σκαριά εδώ και έναν χρόνο και αναπτύσσεται από 17 διαφορετικές ομάδες που συνεργάζονται με την DARPA. Ενδεικτικά, το Google, το Yahoo και το Bing μπορούν να «βλέπουν» μόλις το 5% του Διαδικτύου- το Memex επιδιώκει τη δημιουργία ενός καλύτερου «χάρτη».

Το βασικό θέμα, όπως ανέφερε ο Dr. Κρις Γουάιτ, υπεύθυνος προγράμματος για το Memex, στην εκπομπή 60 Minutes, είναι να αντιμετωπιστεί η προσέγγιση «one-size-fits-all» όσον αφορά στο Ίντερνετ, όπου τα αποτελέσματα αναζητήσεων βασίζονται στις διαφημίσεις και το ranking.

Για αυτό τον σκοπό το Memex δεν θα ψάχνει απλά υλικό από τα εκατομμύρια ιστοσελίδες που αγνοούνται από τις κανονικές μηχανές αναζήτησης, αλλά παράλληλα θα καταγράφει και χιλιάδες sites από το Dark Web – όπως το διαβόητο Silk Road και άλλα που εντάσσονται στο ευρύτερο πλαίσιο του ανώνυμου δικτύου TOR.Οι σελίδες αυτές είναι προσβάσιμες μόνο μέσω του TOR browser και σε αυτούς που γνωρίζουν ακριβώς τις διευθύνσεις τους.

Αν και υπάρχουν σελίδες που έχουν καταχωρημένες κάποιες σελίδες τέτοιων «Hidden Services» (συχνά γύρω από συγκεκριμένα θέματα) και υπάρχει και μια μηχανή αναζήτησης (Grams) για εντοπισμό σελίδων που πωλούν παράνομες ουσίες και άλλα προϊόντα λαθρεμπορίου, το μεγαλύτερο τμήμα των Hidden Services παραμένει «αόρατο».

Ένας από τους στόχους του εγχειρήματος, κατά τον Γουάιτ, είναι να διαπιστωθεί πόσο μεγάλο τμήμα του traffic του TOR σχετίζεται με ιστοσελίδες των Hidden Services, το περιεχόμενο των οποίων δεν είναι προστατευμένο από κωδικούς μεν, αλλά δεν είναι και προσβάσιμο μέσω συμβατικών μηχανών αναζήτησης δε.

«Προσπαθούμε να κινηθούμε προς την κατεύθυνση ενός αυτοματοποιημένου μηχανισμού εύρεσης τέτοιων σελίδων και να κάνουμε διαθέσιμο το περιεχόμενό τους» σημειώνει σχετικά. Επίσης, επιδιώκεται η χρήση αυτοματοποιημένων μεθόδων για την ανάλυση υλικού προκειμένου να βρεθούν κρυμμένοι συσχετισμοί/ σύνδεσμοι οι οποίοι θα μπορούσαν να είναι χρήσιμοι στην αστυνομία, τις ένοπλες δυνάμεις αλλά και φορείς του ιδιωτικού τομέα.

Σε αυτή τη φάση σχεδιάζεται η δοκιμή του Memex σε συγκεκριμένους τομείς, με πρώτο εξ αυτών την εμπορία ανθρώπων. Ωστόσο, παρεμφερείς τεχνικές θα μπορούσαν να χρησιμοποιηθούν και σε άλλα αντικείμενα, όπως η παρακολούθηση ξεσπασμάτων ασθενειών κ.α.

Όπως είπαμε, οι μηχανές αναζήτησης εμφανίζουν αποτελέσματα χρησιμοποιώντας κάποιους αλγόριθμους που «βάζουν σε λίστες» της ιστοσελίδες και λέγονται crawlers. Οι crawlers όμως δεν βρίσκουν τα πάντα. Υπάρχουν «κρυφοί» πόροι στο διαδίκτυο που χονδρικά, κατατάσσονται στις παρακάτω κατηγορίες :

Δυναμικό περιεχόμενο: δυναμικές σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία.

Μη συνδεδεμένο περιεχόμενο: σελίδες που δεν συνδέονται με άλλες σελίδες. Έτσι, τα crawlers που χρησιμοποιούν οι μηχανές αναζήτησης, δεν μπορούν να τις «βρουν» από άλλες σελίδες που εξετάζουν.

Private Web: ιστοσελίδες που χρειάζεται να κάνετε login με username και password.

Contextual Web: είναι οι σελίδες εκείνες το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτό. Παραδείγματος χάριν, οι σελίδες εκείνες που, αν έχετε πρόσβαση σε αυτές με μία διεύθυνση IP από την Ελλάδα, βλέπετε διαφορετικό περιεχόμενο από το αν θα επισκεπτόσασταν την ίδια σελίδα από μία IP των ΗΠΑ.
Περιεχόμενο περιορισμένης πρόσβασης: ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους (Robots Exclusion Standards, CAPTCHAS κ .α)

Scripted content: σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω π.χ. Flash.

Non-HTML/text content: περιεχόμενο κειμένου που είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats που δεν μπορούν να διαβάσουν οι μηχανές αναζήτησης. Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP/HTTPS.

6.5.1. Ιστοτοποι για την εισαγωγη στο Darknet

Για την περιήγησή στο Darknet/Deepweb υπάρχει παρακάτω μια λίστα με χρήσιμες διευθύνσεις. Αυτές οι διευθύνσεις θα πρέπει να γίνουν αντιγραφή και επικόλληση στον onion browser. Χρειάζεται υπομονή γιατί ο **onion browser** είναι πάρα πολύ αργός.
How To:
Download Tor + Browser

https://www.torproject.org/projects/torbrowser.html.en

Start out:

http://en.wikipedia.org/wiki/.onion#Onion_Sites

The Silk Road για αγορά ναρκωτικών =ο

http://ianxz6zefk72ulzz.onion/index.php

The Hidden Wiki! Μπορείτε να βρείτε τα πάντα εδώ!

http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page

Βιβλιοθήκη Tor

http://am4wuhz3zifexz5u.onion/

Open Vendor Database (αναζητά site με ναρκωτικά !)

http://g7pz322wcy6jnn4r.onion/opensource/ovdb/ac/index.php

The General Store (και άλλα ναρκωτικά)

http://xqz3u5drneuzhaeo.onion/users/generalstore/

A bunch of rather popular boards (like Intel Exchange and

http://4eiruntyxxbgfv7o.onion/snapbbs/sitedex.php

Δημοφιλή chat στο Tor (Arguably) comparable to 4chan

http://b4yrk2nkydqfpzqm.onion/mobile/

Κατάλογος/λίστα με συνδέσμους

http://dppmfxaacucguzpc.onion/

Another chan

http://c7jh7jzl3taek4eh.onion/

pastebin

http://4eiruntyxxbgfv7o.onion/paste/browse.php

http://xqz3u5drneuzhaeo.onion/users/boi/?show=65

Επίσης θα πρέπει να διευκρινίσουμε ότι:

- Τα .onion urls που βλέπει ο Tor browser αποτελούν ένα μέρος μόνο του Darknet/Deep Web.
- Το δίκτυο Tor αποτελεί ένα μικρό υποσύνολο του Darknet/Deep Web. Δεν είναι όλο το Darknet/Deep Web.

6.5.2. BrightPlanet

Το ψάξιμο στο διαδίκτυο σήμερα μπορεί να προσομοιωθεί με ένα δίχτυ ψαρέματος στον ωκεανό. Ενώ ένα μεγάλο μέρος από ψάρια μπορεί να πιαστεί στο δίχτυ, υπάρχει ακόμα ένας θαλάσσιος πλούτος που είναι βαθιά, και ως εκ τούτου, έχασε. Ο λόγος είναι απλός, αφού οι περισσότερες από τις πληροφορίες του διαδικτύου είναι θαμμένες σήμερα κάτω από δυναμικά sites και μηχανές αναζήτησης. Οι μηχανές αναζήτησης δημιουργούν δείκτες spidering, αφού για να ανακαλυφθεί, η σελίδα πρέπει να είναι στατική και συνδέονται με άλλες σελίδες. Παραδοσιακά οι μηχανές αναζήτησης δεν μπορούν να ανακτήσουν το περιεχόμενο του Darknet, αφού τα παραδοσιακά crawlers των μηχανών αναζήτησης δεν μπορεί να το ανιχνεύσουν.

Σήμερα, η τεχνολογία αναζήτησης BrightPlanet αυτοματοποιεί τις διαδικασίες λήψης, χρησιμοποιώντας την τεχνολογία πολλαπλών νημάτων και ως εκ τούτου είναι η μόνη τεχνολογία αναζήτησης, μέχρι στιγμής, που είναι ικανή να ταυτοποιήσει, ανακτήσει και που πληροί τις προϋποθέσεις, για την ασφαλή ανάκτηση πληροφοριών. Η τεχνολογία BrightPlanet έχει ποσοτικοποιήσει το μέγεθος και τη σχετικότητα του Darknet. Ο Bergman (2001) βάσει των ευρημάτων για την προαναφερόμενη τεχνολογία αιχμής, καταλήγει σε μελέτη του (που βασίστηκε σε στοιχεία που συλλέχθηκαν μεταξύ 13-20 Μαρτίου του 2000):

- Η ενημέρωση του κοινού σχετικά με το βαθύ Web είναι σήμερα 400 έως 550 φορές μεγαλύτερη από τη συνήθως ορίζεται από το World Wide Web,
- Το Darknet περιέχει 7.500 Tbyte πληροφοριών σε σχέση με 19 Tbyte πληροφοριών στην επιφάνεια του διαδικτύου,
- Το Darknet περιέχει περίπου 550 δισεκατομμύρια μεμονωμένα έγγραφα σε σύγκριση με το ένα δισεκατομμύριο από την επιφάνεια του Web,
- Υπήρχαν πάνω από 200000 βαθιά κρυμμένες ιστοσελίδες το 2001,
- Κατά μέσο όρο, οι ιστοσελίδες του Darknet λαμβάνουν κατά 50% μεγαλύτερη μηνιαία επισκεψιμότητα από τις αντίστοιχες της επιφάνειας, και
- Το 95% των πληροφοριών του Darknet δεν υπόκεινται σε τέλη ή συνδρομές και είναι δημόσια προσβάσιμες.

Η BrightPlanet ισχυρίζεται ότι έχει αναπτύξει το απαραίτητο λογισμικό, το LexiBot, χάρη στο οποίο κάθε αναζήτηση προχωρά σε μεγαλύτερο βάθος, ψάχνοντας και στις ογκώδεις βάσεις δεδομένων. Η διαδικασία αποδεικνύεται εξαιρετικά χρονοβόρα, αφού μία τυπική αναζήτηση απαιτεί 10-25 λεπτά για να ολοκληρωθεί, ενώ η σύνθετη αναζήτηση αποφέρει αποτελέσματα ύστερα από 90 λεπτά.

6.6. Παραδείγματα του Darknet

Οι πρόσφατες αποκαλύψεις για την ηλεκτρονική κατασκοπεία στις ΗΠΑ και την Ευρώπη έφεραν στο προσκήνιο τις συζητήσεις που αφορούν την ασφάλεια στο διαδίκτυο. Μετά τις πρόσφατες αποκαλύψεις για σκάνδαλα κατασκοπείας στα οποία εμπλέκεται η αμερικανική μυστική υπηρεσία NSA έχει ανοίξει μεγάλος δημόσιος διάλογος παγκοσμίως σε σχέση με την για την ασφάλεια στο διαδίκτυο και τον κόσμο της παρανομίας στο Darknet. Αυτοί που κρύβονται στο Darknet είναι χάκερ, εγκληματίες, παιδόφιλοι, έμποροι και χρήστες ναρκωτικών και αναβολικών ουσιών, ιδιόμορφοι και παρακμιακοί κουλτουριάρηδες, πληρωμένοι δολοφόνοι, επαγγελματίες hackers, επιστήμονες, έμποροι ναρκωτικών, αστρονόμοι, δολοφόνοι, φυσικοί, επαναστάτες, κυβερνητικοί υπάλληλοι, αστυνομικοί, ομοσπονδιακοί, τρομοκράτες, διεστραμμένοι, ανθρακωρύχοι δεδομένων, απαγωγείς, κοινωνιολόγοι κλπ. Το προφίλ όμως των χρηστών είναι αρκετά σκοτεινό. Είναι γνωστό επίσης, ότι σε αυτό το χώρο συντονίζουν τις ενέργειες τους και οι Anonymous, μια παγκόσμια κολεκτίβα δεξιοτεχνών του hacking που έχουν χαρακτηριστεί από τον τύπο ως hacktivists. Την μεγαλύτερη πίτα της συμμετοχής βέβαια διεκδικούν οι τρομοκρατικές οργανώσεις που έχουν βρει τον τρόπο να επικοινωνούν τα μέλη τους σε παγκόσμιο επίπεδο. Η λογική του Darknet είναι να παρέχει ανωνυμία σε όσους το χρησιμοποιούν, που αποτελεί ένα γεγονός που δίνει την ευκαιρία -την οποία δεν θα άφηναν ανεκμετάλλευτη- να δράσουν οι εγκληματίες. Από τις έκνομες δραστηριότητες που έχουν πραγματοποιούνται σε αυτό, ψηλά στη λίστα βρίσκεται η διακίνηση κάθε λογής παράνομου προϊόντος ή υλικού. Darknet επιστρατεύεται κατά κόρον για αγοραπωλησίες παιδικής πορνογραφίας, ναρκωτικών, όπλων, κλεμμένων πιστωτικών καρτών και πλαστών ταυτοτήτων (saferinternet.gr).
Τέτοιου τύπου παραδείγματα αποτελούν τα ακόλουθα (Lemley & Reese, 2004; Wood, 2010; saferinternet.gr):

- Μόνο το 0,00000001% των δεδομένων στο Darknet αφορούν πληροφορίες που οι κανονικοί άνθρωποι είναι σε θέση να έχουν πρόσβαση, να κατανοούν και να χρησιμοποιούν,
- Στις περισσότερες περιπτώσεις, οι παράνομες συναλλαγές γίνονται από online "μαύρες αγορές", δηλαδή ιστοσελίδες όπου οι πωλητές αναρτούν τις αγγελίες τους και δέχονται παραγγελίες. Όπως συμβαίνει και στο νόμιμο ηλεκτρονικό εμπόριο, τα προϊόντα

αποστέλλονται ταχυδρομικά, στη διεύθυνση που θα επιλέξει ο αγοραστής. Με τη διαφορά ότι οι αγοραπωλησίες γίνονται ως επί το πλείστον σε bitcoin. Το bitcoin είναι:

(i). Ένα ψηφιακό συναλλακτικό σύστημα μέσω διαδικτύου και συνεπώς υφίσταται μόνο μέσα σε ψηφιακά συστήματα,

(ii). Δεν έχει κεντρικό έλεγχο και η λειτουργία του βασίζεται στην επικοινωνία των υπολογιστών μεταξύ τους,

(iii). Όσα υπολογιστικά συστήματα συνεισφέρουν την επεξεργαστική τους ισχύ στο δίκτυο του bitcoin, δημιουργούν νομίσματα, προφυλάσσουν το δίκτυο από επιθέσεις κι ελέγχουν την ορθότητα κι εγκυρότητα των συναλλαγών που γίνονται σε αυτό και

(iv). Η δημιουργία των νομισμάτων είναι ελέγξιμη.

Εικονα 11.Η ιστοσελίδα Silk Road. Onion.(https://blogstermind.wordpress.com)

- **<u>Παραδειγμα 1-Η Μαυρη Αγορα ναρκωτικων Silk Road</u>**

Το κέρδος αποτελεί επίσης βασική αιτία που η πλειοψηφία των ιστοσελίδων που εμφανίστηκαν μετά τον περασμένο Οκτώβριο και παρά τη σύλληψη τότε από το FBI του υπεύθυνου για το *Silk Road*, -μια από τις πιο εξελιγμένες online μαύρες αγορές (Εικόνα Εικόνα 11). Κι αυτό γιατί, με βάση τη δικογραφία, τα έσοδα του Silk Road μέσα σε λιγότερο

από 3 χρόνια λειτουργίας άγγιξαν τα 80000000 δολάρια, από την προμήθεια που χρέωνε για κάθε αγοραπωλησία. Μάλιστα, οι συναλλαγές που έγιναν στο διάστημα λειτουργίας του site φαίνεται πως ξεπέρασαν τα 1,2 δισεκατομμύρια $. Σύμφωνα με τις διωκτικές αρχές σε όλο τον κόσμο, το Darknet κάνει δυσκολότερη την αντιμετώπιση του online εγκλήματος, όχι όμως και αδύνατη. Έτσι ενώ ο κατηγορούμενος ως διαχειριστής του Silk Road περιμένει να δικασθεί -αντιμετωπίζοντας ποινή φυλάκισης τουλάχιστον 30 ετών- εξαρθρώθηκε μια ακόμη online μαύρη αγορά, η Utopia, με τη σύλληψη πέντε υπόπτων από την ολλανδική και τη γερμανική αστυνομία. Αποτελεί πάγια τακτική οι διωκτικές αρχές να μην αποκαλύπτουν το είδους των ηλεκτρονικών αντίμετρων που επιστρατεύουν. Έτσι στην περίπτωση του Silk Road, αναφέρθηκε πως η αιτιολογία που οδήγησε σε συλλήψεις ήταν το "ανθρώπινο λάθος". Οι αρχές εκμεταλλεύονται επίσης το γεγονός ότι τα εγκλήματα στον online κόσμο αφήνουν ίχνη και στον πραγματικό. Έτσι, για την εξάρθρωση του Utopia, αστυνομικοί υποδύθηκαν τους πελάτες, αγοράζοντας ναρκωτικά και όπλα.

- **<u>Παραδειγμα 2-Εξασφάλιση ανώνυμής επικοινωνίας</u>**

Στο Darknet έχουν κατά καιρούς φιλοξενηθεί αντίγραφα του GlobalLeaks και του Wikileaks. Το περιοδικό New Yorker έχει δημιουργήσει το Strongbox, μια υπηρεσία στο Darknet που εγγυάται ανωνυμία σε όσους θελήσουν να επικοινωνήσουν με τους συντάκτες του με μεγαλύτερη ασφάλεια από αυτήν που προσφέρουν τα ηλεκτρονικά ταχυδρομεία. Επίσης, η οργάνωση Δημοσιογράφοι Χωρίς Σύνορα συμβουλεύει τα μέλη της να το χρησιμοποιούν για να έρχονται σε επαφή με τις πηγές τους, στην περίπτωση που θέλουν να διασφαλίσουν πως θα μείνει μυστική η ταυτότητα όσων επικοινωνούν.

- **<u>Παραδειγμα 3- Συγγραφείς κακόβουλου λογισμικού(Malware)</u>**

Παρέχει ταυτόχρονα σε συγγραφείς malware έξυπνες μεθόδους για την απόκρυψη κακόβουλων εντολών και ελέγχου. Βοηθάει τους αναλυτές malware στον τομέα της έρευνας τους. Οι διευθύνσεις IP των συγγραφέων κακόβουλου λογισμικού είναι στη μαύρη λίστα από τα γνωστά anti-virus, έτσι συχνά χρησιμοποιούν το TOR για να τα ξεπεράσουν.

- **<u>Παραδειγμα 4- Το Crime Network στο Darknet</u>**

  Το Crime Network, αποτελεί το πραγματικά τρομακτικό περιεχόμενο που βλέπουμε

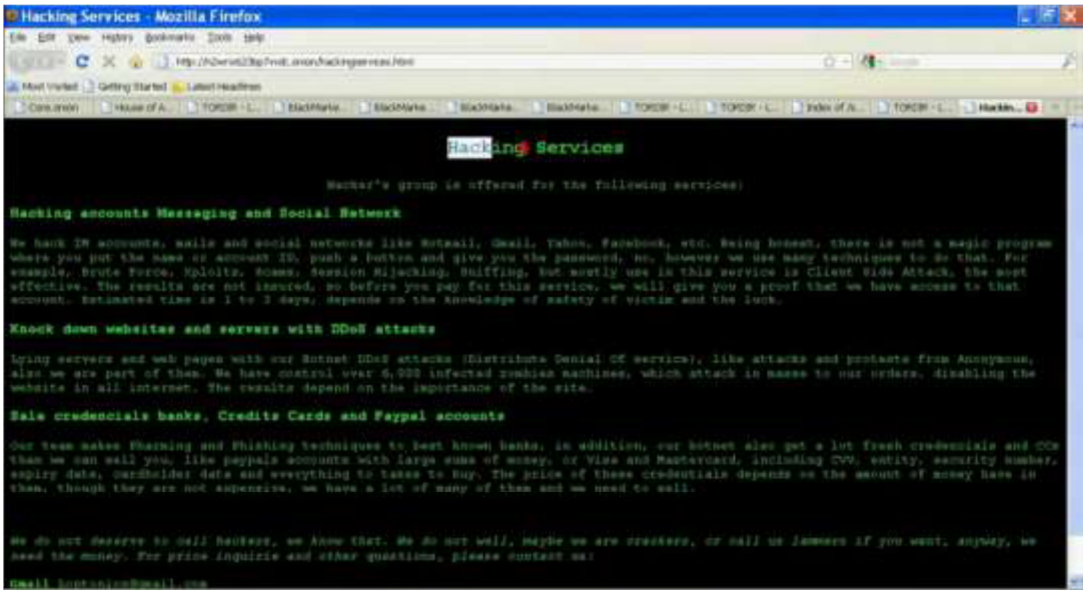
στο Darknet. Όσο βαθύτερα ψάξει κανείς στις ιστοσελίδες του τόσο σκοτεινο γίνεται το περιεχόμενο τους. Οι μαφιόζοι των ΗΠΑ και κυρίως η ιταλική μαφία που δραστηριοποιείται στην Αμερική, πολύ γρήγορα χρησιμοποίησε το Darknet. Έτσι οι πληρωμένοι εκτελεστές της μαφίας, άρχισαν να κλείνουν τα "συμβόλαια θανάτου" διεθνώς μέσω του σκοτεινού κόσμου,

διατηρώντας απόλυτα την ανωνυμία τους,

- **Παραδείγματα**
- Banker & Co και professional service για ξέπλυμα βρώμικου χρήματος,
- PayPal 4free και Hacked PayPal λογαριασμοί προς πώληση, όπου η ιστοσελίδα Eris-

#1 Deepweb Dealer- παρέχει πρόσβαση για αγορά κάνναβης, LSD, DMT, μανιτάρια, ενώ η αντίστοιχη MDMA και οποιουδήποτε άλλου ναρκωτικού,

- All Purpose Identities, δηλαδή ψεύτικες ταυτότητες για ΗΠΑ και Καναδά, άδειες, διαβατήρια και άλλα ταξιδιωτικά έγγραφα,
- Rent-a-Hacker, όπου βρίσκεις επαγγελματίες hackers προς ενοικίαση, για DDOS, hacking, για καταστροφή sites και κατασκοπεία (Εικόνα 12),



Εικονα 12. Rent-a-Hacker. Onion.(http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/)

- Contract killer ή και γνωστό ως "*Σκοτώστε το πρόβλημά σας*" (καταδότης, paparazzi,

πλούσιο άντρα, αστυνομικό, δικαστή, ανταγωνιστή, κλπ) με host: FH,

- Γίνονται ακόμη και υπόγεια τουρνουά στα οποία αγωνίζονται μέχρι θανάτου, όπου λαμβάνουν μέρος πραγματικά εκπαιδευμένοι, επαγγελματίες μαχητές, δηλαδή Dudes (μάγκες) που θεωρούν πραγματική απόλαυση τον αγώνα μέχρι θανάτου. Επίσης, γίνονται σύγχρονες μάχες Gladiator, μεταξύ ανθρώπων ή και ανθρώπων με ζώα,
- Οι βαρόνοι των ναρκωτικών έχουν πια ειδικούς λογαριασμούς στο Darknet και κλείνουν συμφωνίες εκατομμυρίων δολαρίων για την πώληση τους (Εικόνα 9),
- Οι διακινητές παιδικού πορνογραφικού υλικού βρήκαν το απόλυτο εργαλείο για να

πουλάνε το νοσηρό προϊόν τους,

- Παράλληλα, σε εργαλεία και υπηρεσίες που βασίζονται στο TOR βρίσκουν καταφύγιο

απλοί χρήστες που θέλουν να παρακάμψουν τα φίλτρα λογοκρισίας στη χώρα τους και, όπως είναι φυσικό, πολιτικοί ακτιβιστές. Έτσι, σύμφωνα με την ιστοσελίδα του TOR, το Darknet κατακλύσθηκε από blogs κατά τη διάρκεια της Αραβικής Άνοιξης, από ανθρώπους που συμμετείχαν στις εξεγέρσεις και ήθελαν να μεταφέρουν στο εξωτερικό τη μαρτυρία τους,

- **<u>Παραδειγμα 5- Η αναπάντεχη ιστορία ενός φοιτητή στο Darknet</u>**

Η απίστευτη ιστορία φοιτητή που μπλέχτηκε άθελά του σε παγκόσμιο σκοτεινό διαδικτυακό παιχνίδι. Όταν ένας ανυποψίαστος μεταπτυχιακός φοιτητής από το Μπρούκλιν, αποφάσισε ένα βράδυ να περιηγηθεί στο διαδίκτυο, δεν μπορούσε να πιστέψει με τίποτα τι θα ακολουθούσε. Ο νεαρός 32χρονος, διδακτορικός φοιτητής Jeff Kinkl, ο οποίος έβγαζε τα προς το ζην εργαζόμενος ως μεταφραστής και συγγραφέας ήταν μόνος στο διαμέρισμά του στο Μπρούκλιν της Νέας Υόρκης, προσπαθούσε να γράψει μία εργασία με θέμα τη θεσμική μυστικότητα και τους κρατικούς μηχανισμούς εθνικής ασφάλειας. Περιηγούμενος στο διαδίκτυο, άνοιξε τυχαία τη διαβόητη ιστοσελίδα διαμοιρασμού αρχείων και εικόνων 4CHAN που προσελκύει καθημερινά 1000000 επισκέπτες. Καθώς ανοιγόκλεινε το ένα αρχείο μετά το άλλο, έπεσε ξαφνικά σε ένα παράξενο μήνυμα που προσέλκυσε την προσοχή του. Στο παρελθόν είχε διαβάσει κάπου ότι η Υπηρεσία Εθνικής Ασφάλειας (NSA) -η γνωστή πλέον κυβερνητική οργάνωση που δρα στη σκιά της CIA και εμπλέκεται σε επιθετικές και αμυντικές επιχειρήσεις στον κυβερνοχώρο- χρησιμοποιούσε συχνά το 4CHAN με σκοπό την προσέλκυση ταλαντούχων hackers (Εικόνα 13). Ανάμεσα σε εκατοντάδες σχόλια και πεδία συζήτησης, κάποιοι επισκέπτες ανέφεραν ότι το παράξενο μήνυμα ενδεχομένως να ήταν κάποια άσκηση στρατολόγησης, τοποθετημένο από την NSA. Ο Kinkl αποφάσισε να προχωρήσει βαθύτερα. Κοίταζε με επιμονή το μήνυμα, προσπαθώντας να κατανοήσει το νόημά του, όταν ένας σχολιαστής υπέδειξε να ανοιχτεί η εικόνα με το πρόγραμμα επεξεργασίας απλού-κειμένου WordPad. Ο Kinkl δεν κατάφερε να συγκρατηθεί και ακολούθησε την υπόδειξη. Στο κάτω μέρος του κειμένου, βρήκε το ακόλουθο μήνυμα: "*O TIBERIVS CLAVDIVS CAESAR λέει lxxt>33m2mqkyv2gsq3q=w]O2ntk*". Αμέσως βάλθηκε να σπάσει τον κώδικα. Αρχικά, αναγνώρισε ότι το κρυπτογραφημένο κείμενο είχε κωδικοποιηθεί βάσει του "Κώδικα του Καίσαρα", μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Πρόκειται για κώδικα αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Κι εφόσον ο Τιβέριος Κλαύδιος ήταν ο 4ος Ρωμαίος

Αυτοκράτορας, ο Kinkl υπέθεσε ότι το κείμενο έπρεπε να μετατοπιστεί κατά 4 γράμματα του αλφάβητου προς τα πίσω. Το κείμενο αποκάλυψε μία διεύθυνση URL. Όταν όμως πάτησε πάνω στη διεύθυνση, η σελίδα που εμφανίστηκε περιείχε την εικόνα μιας πλαστικής πάπιας και τις λέξεις: "*Αυτό είναι απλό δόλωμα. Φαίνεται πως δεν μπορείς να μαντέψεις πώς να ξετρυπώσεις το μήνυμα*". Η φράση προβλημάτισε τον Kinkl και τους συνοδοιπόρους του στο αινιγματικό παιχνίδι, έως ότου κατάλαβαν ότι οι λέξεις "μαντέψεις" και "ξετρυπώσεις" σχετίζονταν με το λογισμικό αποκρυπτογράφησης OutGuess. Τρέχοντας την εικόνα με το πρόγραμμα OutGuess ανακάλυψαν ένα link που οδηγούσε σε ένα πίνακα μέσα στον ιστότοπο κοινωνικής δικτύωσης reddit. Όταν ο Kinkl άνοιξε το link και είδε την εικόνα μιας σειράς αριθμητικών στοιχείων των Μάγια, αρκετές γραμμές δυσνόητων γραμμάτων και δύο εικόνες με τις ετικέτες "welcome" και "problems".

Εικονα 13.Η ιστοσελίδα της NSA στο Darknet.(https://blogstermind.wordpress.com)

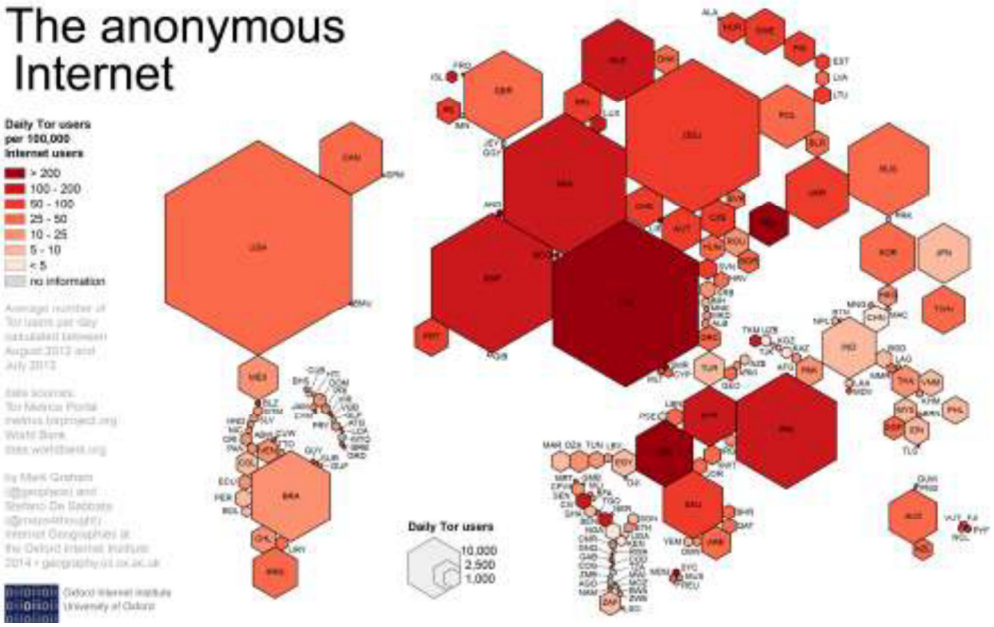
Εκείνη ακριβώς τη στιγμή κάποιος πόσταρε ένα link σε ένα ανώνυμο δωμάτιο συζήτησης στην ιστοσελίδα Mibbit.com. Η ανησυχία του Kinkl είχε αρχίσει να εντείνεται. Είχε αποκλείσει το ενδεχόμενο όλο αυτό να ήταν αποτέλεσμα τρολαρίσματος. Κάτι πιο σοβαρό κρυβόταν από πίσω. Η νύχτα τον βρήκε να λύνει μια σειρά από ενδείξεις που είχαν να κάνουν με κώδικες βιβλίων, τον βασιλιά Αρθούρο και την αναζήτηση του Ιερού Δισκοπότηρου, για να ανακαλύψει τελικά το ακόλουθο μήνυμα: "*κάλεσέ μας στον αριθμό 2143...*". Αμέσως

ειδοποίησε τους φίλους του στο chat-room ότι του δίνουν έναν αριθμό τηλεφώνου. Ξαφνικά, δέχτηκε το ακόλουθο προσωπικό μήνυμα: "*Προπορεύεσαι κατά πολύ των άλλων*", καθώς και μια πρόσκληση σε ένα άλλο μικρότερο δωμάτιο συζήτησης μέσα στο ίδιο δίκτυο. Μπαίνοντας εκεί άρχισε να σχηματίζει τον τηλεφωνικό αριθμό μέσω του Google Voice. Μια προηχογραφημένη φωνή τον καλωσόρισε: "*Πολύ καλά. Τα πήγες περίφημα. Υπάρχουν 3 πρώτοι αριθμοί που σχετίζονται με την αρχική εικόνα jpg. Ο 3301 είναι ένας από αυτούς. Θα πρέπει να βρεις τους άλλους δύο. Πολλαπλασίασε και τους τρεις από αυτούς τους αριθμούς μαζί και πρόσθεσε μία προέκταση .com για να ανακαλύψεις το επόμενο βήμα. Καλή τύχη*". Εν συνεχεία πολλαπλασίασε τους αριθμούς και προέκυψε μια νέα διεύθυνση URL. Στην οθόνη του εμφανίστηκε η εικόνα ενός τζίτζικα και από κάτω ένα ρολόι αντίστροφης μέτρησης που επρόκειτο να λήξει σε 3 μέρες. Τέλος, ανοίγοντας την εικόνα του τζίτζικα με το OutGuess ανακάλυψε άλλο ένα περίεργο μήνυμα: "*Κατάφερες να φτάσεις μέχρι εδώ, Η υπομονή είναι αρετή. Τσέκαρε πάλι στις 5:00 το απόγευμα της Δευτέρας 9/1/2012. UTC*". Ο Kinkl άρχισε πλέον να πανικοβάλλεται, αφού όλο αυτό ξεπερνούσε τα όρια του απλού παιχνιδιού και άρχιζε να λαμβάνει πραγματικές διαστάσεις.

Την Δευτέρα 09/01/2012 και ώρα 4:59, ο Kinkl μαζί με το συγκάτοικό του είχαν καρφωμένο το βλέμμα τους στην οθόνη. Η αντίστροφη μέτρηση είχε φτάσει στο μηδέν και τότε η ιστοσελίδα επαναφορτώθηκε εμφανίζοντας 14 συντεταγμένες GPS, καθώς και τις τοποθεσίες στις οποίες αυτές παρέπεμπαν σε όλο τον πλανήτη: Βαρσοβία, Σεούλ, Παρίσι, Σίδνεϊ, Χαβάη, Μαϊάμι, Νέα Ορλεάνη, Σιάτλ (Εικόνα 14). Τις εβδομάδες που ακολούθησαν χρήστες επισκέφτηκαν τις διευθύνσεις αυτές και πόσταραν στο δωμάτιο συζήτησης εικόνες των ευρημάτων τους: λευκά φύλλα χαρτιού κολλημένα σε φανάρια κυκλοφορίας, τα οποία περιείχαν το καθένα και ένα διαφορετικό κώδικα QR και μία κόκκινη εικόνα ενός τζίτζικα. Οι κωδικοί οδηγούσαν σε διευθύνσεις URL, οι οποίες όταν ανοίχτηκαν με το OutGuess αποκάλυψαν δύο νέα μηνύματα.

Ο Kinkl αδυνατούσε να καταλάβει σε τι αναφέρονταν. Κάποιος άλλος όμως τα κατάφερε: Ήταν ένα ποίημα 300 στροφών γραμμένο από τον συγγραφέα επιστημονικής φαντασίας Ουίλιαμ Γκίμπσον με τίτλο: "Αγρίππας (Βίβλος των Νεκρών)". Χρησιμοποιώντας το ποίημα για να αποκωδικοποιήσουν το περιεχόμενο των μηνυμάτων αποκρυπτογράφησαν μια διεύθυνση TOR. Ο Kinkl κατέβασε το λογισμικό TOR και επισκέφτηκε τη διεύθυνση, η οποία τον καθοδήγησε να δημιουργήσει έναν ανώνυμο λογαριασμό στην υπηρεσία Hotmail. Μερικά λεπτά αργότερα, έλαβε ένα mail. Περιείχε ένα γρίφο που ο Kinkl έπρεπε να λύσει μόνος του. Ήταν όμως αδύνατον, καθώς χρειαζόταν να χρησιμοποιήσει ένα σωρό περίπλοκα λογισμικά αποκρυπτογράφησης. Οι προγραμματιστές φίλοι του δεν μπορούσαν ούτε κι αυτοί

να βοηθήσουν. Δέκα μέρες μετά την έναρξη της περιπέτειάς του ήταν αποφασισμένος να τα εγκαταλείψει. "*Δεν ξανάκουσα τίποτα*", παραδέχεται ο ίδιος ο Kinkl.



Εικονα 14.Η εμβέλεια του Darknet.(https://en.wikipedia.org/wiki/Darknet)

Ωστόσο, μερικές εβδομάδες αφότου είχε εγκαταλείψει την προσπάθεια, αναζήτησε τη λέξη cicada και τον αριθμό 3301, για να ανακαλύψει μία νέα εξέλιξη στο αίνιγμα. Ένα άλλο μυστήριο μήνυμα είχε δημοσιευτεί το Φεβρουάριο του 2012 στον ίδιο πίνακα του site 4CHAN, το οποίο έλεγε: "*Βρήκαμε τα άτομα που αναζητούσαμε. Εδώ, λοιπόν, τελειώνει το μακρύ ταξίδι μας*". Επιπλέον, την επόμενη ακριβώς μέρα, άλλο ένα παράξενο σημείωμα εμφανίστηκε σε ένα ιστότοπο προσωρινής αποθήκευσης κειμένων ονόματι Pastebin. Έμοιαζε με επιστολή συγχαρητηρίων στους νικητές, το οποίο είχε αναδημοσιευτεί από κάποιο μέλος των Anonymous: "*Μην μοιραστείτε αυτη την πληροφορία - Δίχως αμφιβολία, αναρωτιέστε τι είναι αυτό που κάνουμε. Είμαστε κάτι σαν δεξαμενή σκέψης. Πρωταρχικός στόχος μας είναι η έρευνα και η ανάπτυξη τεχνικών υποστήριξης των ιδεών μας. Ελευθερία, ιδιωτικότητα, ασφάλεια*". Το μήνυμα πρόσφερε στους νικητές ελεύθερη συνδρομή μέλους στην ομάδα, εάν και εφόσον απαντούσαν σε μερικές ερωτήσεις του τύπου: "*Πιστεύετε πως η διακίνηση των πληροφοριών θα έπρεπε να είναι ελεύθερη;*". Ο Kinkl δεν μπορούσε να πιστέψει με τίποτα ότι αυτό ήταν το τέλος όλου αυτού του κρυπτικού παιχνιδιού. Μέσα σε 10 μέρες ταξίδεψε τόσο στον παγκόσμιο ιστό όσο δεν έχουν ταξιδέψει άλλοι σε ολόκληρη τη ζωή τους. Μέχρι σήμερα διατηρεί τον TOR περιηγητή του και τις κεραίες του τεντωμένες, περιηγούμενος στα

τρίσβαθα του διαδικτύου, με την ελπίδα ότι μπορεί κάποτε να πέσει πάνω στην αληθινή απάντηση στο αίνιγμα.

6.7. Πιθανή χρήση και προστασία από το Darknet

Η επικοινωνία στο Darknet είναι απλή. Ο τρόπος που επικοινωνούν οι σκοτεινοί χρήστες μεταξύ τους είναι μέσω των προγραμμάτων ανταλλαγής αρχείων σε δίκτυα που ονομάζεται peer-to-peer (P2P). Η απλή δομή, το μηδαμινό κόστος, η άναρχη ροή της πληροφορίας, είναι τα στοιχεία που καθιστούν τα δίκτυα P2P ελκυστικά για τους χρήστες του Darknet. Οι χρηματικές συναλλαγές γίνονται με bitcoins, ένα νομισματικό σύστημα του δικτύου P2P που χρησιμοποίει ισοτιμία με το ευρώ γύρω στα 4 €. Για να αποκτήσετε πρόσβαση στο Darknet, υπάρχουν δυο ενέργειες που πρέπει να γίνουν (Wood, 2010; saferinternet.gr): (i). Η χρήση τον TOR browser, αφού έχει χρησιμοποιηθεί πρώτα ως πρόσθετο η επέκταση TOR για τον Firefox. Κάποιος πρέπει να έχει υπόψη του το TOR δεν είναι 100% ανώνυμο (αφού πολλαπλά proxies απαιτούνται σαν πρόσθετα στον TOR), και βέβαια, ένα τείχος προστασίας καθώς και ένα καλό αντιβιοτικό πρόγραμμα (για τους χρήστες Windows). Καλό θα ήταν να αποσυνδεθεί η κάμερα, να απενεργοποιηθούν τα javascript cookies, τα temp data και να χρησιμοποιήστε ccleaner (για Windows, BleachBit και Linux), (ii). Στη συνέχεια, αποκτήστε πρόσβαση στο Hidden Wiki το οποίο είναι ένα μικρό αλλά χρήσιμο σημείο αναφοράς για να ξεκινήσει η περιήγηση στο Darknet.

Χρησιμοποιήστε μια γενική μηχανή αναζήτησης για να εντοπίσετε μια κάθετη μηχανή αναζήτησης. Αυτό μπορεί να θεωρηθεί ως αναζήτηση επίπεδο split. Στο πρώτο επίπεδο, θα αναζητηθεί η ιστοσελίδα της βάσης δεδομένων. Σε ένα δεύτερο επίπεδο, πηγαίνοντας στην ιστοσελίδα θα αναζητηθεί η ίδια βάση δεδομένων για τις πληροφορίες που θέλετε. Μια σειρά από γενικές μηχανές αναζήτησης θα ψάξει το Darknet για σχετικό περιεχόμενο μετά την αρχική έρευνα.

Ένας ενδεικτικός τρόπος για να εισχωρήσει κάποιος στον απαγορευμένο κόσμο του διαδικτύου είναι να κατεβάσει το λογισμικό TOR ένα σύστημα δηλαδή, που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο διαδίκτυο. Στη συνέχεια πληκτρολογώντας στον browser kpvz7ki2v5agwt35.onion αποκτιέται πρόσβαση στο Hidden Wiki, μία

συγκεντρωτική συλλογή συνδέσεων στο βαθύτερο διαδίκτυο. Οι πληροφορίες που είναι νέο και δυναμικά μεταβαλλόμενο περιεχόμενο, θα εμφανιστούν στο Darknet. Τότε κάποιος εισέρχεται στο Hidden Wiki, οπού εκεί -και σ' αυτό το wiki- υπάρχουν κατηγορίες συνδέσμων που μπορείς να βρεις οτιδήποτε. Υπάρχουν blogs, φόρουμ (από φυσιολογικά, επαναστατικά, επικίνδυνα και παράνομα), TOR-enabled instant messaging και chat, ανώνυμη φιλοξενία αρχείων, χρηματοδότηση, ανατροπή και ανταλλαγή πληροφοριών, πληροφοριών σχετικά με την ασφάλεια-ανωνυμία του Η/Υ, πληροφορίες για wares-cracks-hacking, όλα τα βιβλία, μουσική, και ταινίες. Συνδέει ακόμη με αθλητικά στοιχήματα και τις πληροφορίες του εμπορίου, έχει συνδέσεις στις διεθνείς αγορές ναρκωτικών, κυκλώματα πορνείας, αγορές δολοφόνων, μαύρη αγορά προϊόντων, παιδική πορνογραφία (Wood, 2010; saferinternet.gr). Ορισμένα μέτρα προστασίας, που αφορούν καθαρά το Darknet, μπορεί να είναι τα ακόλουθα (Wood, 2010; saferinternet.gr):

- Πριν ξεκινήσετε την περιήγηση, καλό θα ήταν να γνωρίζετε πώς λειτουργεί το Darknet και τι μπορείτε να κάνετε για να προστατεύσετε τον εαυτό σας καλύτερα ενάντια στους εισβολείς και οτιδήποτε που μπορεί να θέσει σε κίνδυνο την πραγματική ανωνυμία σας,

- Χρησιμοποιήστε μια, οπουδήποτε διανομή Linux η οποία έχει τον Firefox,

- Εγκαταστήστε το TOR, όπως αναφέρεται στα links πιο πάνω και μπείτε στο Darknet

(οι καταλήξεις των σελίδων είναι συνήθως .onion) και κρύψτε την IP σας,

- Μην κάνετε κλικ σε συνδέσμους που βλέπετε στο hiddenwiki,

- Μην περιμένετε να δείτε σελίδες, όπως το Facebook κλπ.,

- Στο Darknet η πληροφορία είναι πληροφορία. Και οι πληροφορίες είναι λέξεις. Θα βρείτε λοιπόν κείμενα, γεμάτα πληροφορίες,

- Στα περισσότερα θέματα, οι πληροφορίες είναι ακριβώς εκεί. Το θέμα η επιλογή, η παραγωγή, η αποθήκευση, η ανταλλαγή και η μεταφορά των πληροφοριών αυτών, που

μπορεί να σας οδηγήσει σε προβλήματα ή και φυλάκιση ακόμη,

- Αν έχετε δεδομένα στον δίσκο του υπολογιστή που τρέχετε live την διανομή, μπορείτε

να τον αποσυνδέσετε και μην συνδέετε καμία εξωτερική συσκευή,

- Ακόμα καλύτερα, μην συνδέεστε από το σπίτι σας, αλλά από κάποιο δημόσιο δίκτυο,

- Αλλαγές και στα DNS είναι θετικές,

- Μπορεί να συναντήσετε και links της μορφής: pipl.com/help/deep-web/ deepwebtech.com/products/exploit-for-government, deepweb.co.nz/online-reviews-good-bador-fake.

- Το Darknet δεν μαθαίνεται από την μια ημέρα στην άλλη. Για την ακρίβεια δεν μαθαίνεται ποτέ. Να είσαστε προσεκτικοί αν αποφασίσετε να το χρησιμοποιείτε,

- Υπάρχουν πλέον ερευνητικά εργαλεία που αποκαλούνται network telescopes, τα οποία παρακολουθούν το Darknet για να εντοπίσουν και να καταγράψουν τέτοιου είδους ενέργειες.

6.7.1. Υπάρχει λόγος να έχω πρόσβαση στο Darknet/Deep Web;

- Ναι αν πιστεύετε πως η ανωνυμία σας πλήττεται και εξακολουθείτε να θέλετε να χρησιμοποιείτε το διαδίκτυο για να αναζητάτε πληροφορίες και να επικοινωνείτε, χωρίς να σας καταγράφει κάποιος.
- Ναι αν ανήκετε σε μία πληθυσμιακή ομάδα που βρίσκεται σε κίνδυνο ή παρακολούθηση και θέλετε να επικοινωνείτε ανώνυμα.
- Ναι αν είστε δημοσιογράφος και δεν θέλετε να απειλείται η ταυτότητα και η ζωή των πηγών σας.

Όχι, δεν υπάρχει κανένας λόγος να ασχοληθείτε με το Darknet/Deep Web, αν πιστεύετε πως το διαδίκτυο είναι τα social media και τα selfies που μοιράζεστε μέσα από αυτά, μαζί με τις κάθε 5 λεπτο αναφορές για το τι σκέφτεστε, τι κάνετε και με ποιον το κάνετε. Επίσης, δεν υπάρχει κανένας λόγος να ασχοληθείτε με το Darknet/Deep Web αν η χρήση που κάνετε στο διαδίκτυο δεν έχει κάποιες πιο «ευρείες» αναζητήσεις. Και όχι, δεν υπάρχει κανένας λόγος να εμπλακείτε με το Darknet/Deep Web, αν δεν μπορείτε να αντιμετωπίσετε την εμπειρία ενός χαοτικού περιεχομένου με ότι προέκταση μπορεί να έχει αυτό. Από ενοχλητικές ή απειλητικές συζητήσεις, μέχρι παράνομο και επικίνδυνο υλικό.

7. Το Darknet ο ρόλος της ΕΛ.ΑΣ.

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί ζήτημα ύψιστης σημασίας για τις αστυνομικές αρχές, όπως άλλωστε και τα κοινά διαπραχθέντα εγκλήματα. Συγκεκριμένα, όσο αφορά τα ηλεκτρονικά εγκλήματα, που έχουν εισέλθει στην καθημερινότητα μας τα τελευταία χρόνια, το ενδιαφέρον της αστυνομίας εστιάζεται περισσότερο στις ασταμάτητες αλλαγές που προκύπτουν στους κόλπους της τεχνολογίας. Οι ταχύτατες αυτές αλλαγές καθιστούν το ηλεκτρονικό έγκλημα δύσκολα ανιχνεύσιμο έγκλημα, τόσο στο εξωτερικό όσο και στην Ελλάδα. Αυτό που φαίνεται να παίζει ρόλο στην αποτελεσματικότητα του έργο των διωκτικών αρχών είναι η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού της αστυνομικής αρχής σε θέματα κυρίως τεχνικής φύσεως σχετικά με τη διερεύνηση και τη δίωξη του ηλεκτρονικού εγκλήματος και κυρίως Darknet. Η Ελληνική Αστυνομία (ΕΛ.ΑΣ.), έχει προχωρήσει στη σύσταση Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΔΗΕ). Οι καταγγελίες των πολιτών που διαπιστώνουν ότι έχουν παραβιαστεί προσωπικά τους δεδομένα ή ότι έπεσαν θύματα κάποια ηλεκτρονικής απάτης ή γενικότερα έχουν αντιληφθεί κάτι ύποπτο σχετικά με το διαδίκτυο ή τη χρήση Η/Υ, θα πρέπει να απευθύνονται άμεσα στην αρμόδια αρχή (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Επιπλέον στην Ελλάδα, σχετικός με καταγγελίες για το ηλεκτρονικό έγκλημα είναι και ο ιστότοπος www.saferinternet.gr. Στο συγκεκριμένο ιστότοπο δράσης, ενημέρωσης και επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου (υπό την αιγίδα της Ε.Ε.) υπάρχουν πολλές, χρήσιμες πληροφορίες και συμβουλές για την ορθή χρήση του διαδικτύου, του κινητού τηλεφώνου και άλλων διαδραστικών τεχνολογιών (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Για την πληρέστερη κατανόηση του ρολού που μπορεί παίξει η γνώση του Darknet στην εξιχνίαση του ηλεκτρονικού εγκλήματος, παραθέτουμε και σχολιάζουμε ορισμένα παραδείγματα από την ελληνική εμπειρία (saferinternet.gr):

- Μόλις το 15% του διαδικτύου λειτουργεί στο φως, το υπόλοιπο 85% κινείται στο

σκοτάδι», υποστηρίζουν εξειδικευμένοι αξιωματικοί της ΕΛ.ΑΣ., προσθέτοντας ότι το εγκληματικό μέλλον αποτυπώνεται πλέον στο Darknet, σε τρομοκρατικές δραστηριότητες, οργανωμένο έγκλημα, αγοραπωλησίες όπλων, ναρκωτικών, υλικού παιδικής πορνογραφίας και άλλων εγκληματικών δραστηριοτήτων, όπως η σύναψη συμβολαίων θανάτου. Έχουν φτιαχτεί κλειστοί κωδικοποιημένοι κόμβοι, μέσα από τους οποίους μιλούν, συνεννοούνται, σχεδιάζουν και ανταλλάσσουν. Έχουν τους δικούς τους Darknet διαδικτυακούς χώρους, που προς το παρόν δύσκολα εντοπίζονται, ισχυρίζονται υψηλόβαθμα στελέχη της ΕΛ.ΑΣ.

- **<u>Παραδειγμα 1- Η πρώτη υπόθεση Darknet στην Ελλάδα διαδραματίζεται στην Πάτρα</u>**

Στο δίκτυο Darknet διακινούνται βιασμοί, κακοποιήσεις, ακόμα και δολοφονίες παιδιών. Εντοπίστηκαν στην Πάτρα δύο άντρες που είχαν ανοίξει λογαριασμό στο Darknet. Το FBI και η Europol έψαχναν συμβόλαια θανάτου της μαφίας σε Ευρώπη και ΗΠΑ και τυχαία βρήκαν τους δύο Πατρινούς. Έτσι, η ΥΔΗΕ πραγματοποίησε τις πρώτες συλλήψεις στην Ελλάδα χρηστών του Darknet, όπου διακινούνται βιασμοί, κακοποιήσεις, ακόμα και δολοφονίες παιδιών. Μετά από κοινή επιχείρηση του FBI, της Europol και βέβαια της ΥΔΗΕ, εντοπίστηκαν στην Πάτρα, οι δυο άνδρες ηλικίας 33 και 35 ετών αντίστοιχα, οι οποίοι διακινούσαν υλικό παιδική πορνογραφίας, κυρίως με κακοποίηση ανηλίκων ακόμα και βρεφών. Ο εντοπισμός των δυο Πατρινών, έγινε έπειτα από μεγάλη επιχείρηση που έχει εξαπολύσει εδώ και μήνες το FBI, σε συνεργασία με την Europol στο Darknet, για την διερεύνηση συμβολαίων θανάτου σε Ευρώπη και ΗΠΑ. Πρόκειται για μια μεγάλη υπόθεση με αιματηρά ξεκαθαρίσματα στους κόλπους της ιταλικής μαφίας που εδρεύει στην Νέα Υόρκη, όπου τα οι ιθύνοντες της διεθνούς εγκληματικής οργάνωσης, έκλειναν συμβόλαια θανάτου, για τους αντιπάλους τους χρησιμοποιώντας τις σελίδες του Darknet προκειμένου να μην εντοπίζονται. Συνολικά το FBI ερεύνησε 20 συμβόλαια θανάτου που ολοκληρώθηκαν στις ΗΠΑ και την Ευρώπη.

Διερευνώντας λοιπόν αυτή την υπόθεση οι δυο υπηρεσίες, έπεσαν επάνω σε ιστοσελίδα του Darknet στην οποία διακινούνταν ιδιαίτερα σκληρό παιδικό πορνό, με κακοποίηση παιδιών ακόμα και δολοφονίες. Δυο από τους διακινητές του υλικού, οι οποίοι μάλιστα διατηρούσαν λογαριασμό σε αυτή τη Darknet ιστοσελίδα, ήταν Έλληνες. Αμέσως ειδοποιήθηκε από το FBI η ΥΔΗΕ προκειμένου να προβεί σε πιο εξειδικευμένες έρευνες για τον εντοπισμό των δυο ατόμων που διατηρούσαν λογαριασμό στο Darknet. Έπειτα από εξειδικευμένη έρευνα στο Darknet, οι αστυνομικοί της ΥΔΗΕ εντόπισαν αρχικά το ηλεκτρονικό ταχυδρομείο των δυο υπόπτων και τελικά ότι δραστηριοποιούνταν στην Πάτρα. Αμέσως κλιμάκιο αστυνομικών της ΥΔΗΕ έφθασε στην Πάτρα οπού και κατάφεραν να

εντοπίσουν το στίγμα των δυο δραστών και να φθάσουν τελικά στα σπίτια τους, αλλά και στους χώρους εργασίας τους, καθώς είναι και οι δυο ιδιωτικοί υπάλληλοι. Στις έρευνες που ακολούθησαν αποδείχτηκε το γεγονός ότι ήταν διαχειριστές συγκεκριμένου λογαριασμού στο Darknet και μάλιστα ιστοσελίδας με σκληρό παιδικό πορνό και κακοποιήσεις ανηλίκων.

- **<u>Παραδειγμα 2- Η Συνωμοσία Πυρήνων της Φωτιάς στο Darknet</u>**

  Στο Darknet η Συνωμοσία Πυρήνων της Φωτιάς, το μανιφέστο του Ξηρού Χ., και η

δολοφονία του ειδικού φρουρού Αμανατίδη, Χ. Έλληνες τρομοκράτες, εγχώριοι βαρώνοι του οργανωμένου εγκλήματος και παιδόφιλοι χρησιμοποιούν το Darknet, για τις παράνομες δραστηριότητές τους, τουλάχιστον από το 2004, όπως αποκαλύπτουν υψηλόβαθμοι αξιωματικοί της ΕΛ.ΑΣ., Περίπου, 20 ελληνικοί κόμβοι του Darknet, χρησιμοποιούνται από μέλη τρομοκρατικών ομάδων, εγκληματικών οργανώσεων και κυκλωμάτων κατοχής και διακίνησης σκληρότατου υλικού παιδικής πορνογραφίας. Η χρησιμοποίηση των δικτύων σέρβερ με τεχνολογίες κρυπτογράφησης TOR και TOR Browser Bundle, έχει διαπιστωθεί στη χώρα μας. Μια από αυτές αφορούσε τη δολοφονία του 33χρονου ειδικού φρουρού Αμανατίδη, Χ., στην Κηφισιά, το 2004. Μια δεύτερη τη σύλληψη μελών της Συνωμοσίας Πυρήνων της Φωτιάς στη Ν. Φιλαδέλφεια, το 2013 και τον Ιανουάριο του 2014 στο αιμοσταγές διαδικτυακό διάγγελμα του "Μανώλη της 17Ν", Ξηρού Χ., μετά την απόδρασή του. Η συγκεκριμένη ενέργεια δεν έχει αποδοθεί σε κάποια τρομοκρατική επωνυμία, ωστόσο η διερεύνησή της απασχολεί ακόμη την Αντιτρομοκρατική Υπηρεσία, αξιωματικοί της οποίας εκτιμούν ότι κάποιοι θιασώτες της εγχώριας τρομοκρατίας, ελεύθεροι και έγκλειστοι φυλακών, επιχείρησαν τη δημιουργία μιας νέας τρομοκρατικής οργάνωσης από εκεί που είχε σταματήσει η «17 Νοέμβρη», όταν σκότωσε τον βρετανό στρατιωτικό ακόλουθο Στίβεν Σόντερς. Στόχος των τρομοκρατών, όπως υποστηρίζουν αξιωματικοί της ΕΛ.ΑΣ., ήταν ο αφοπλισμός του φρουρού και ίσως όχι η δολοφονία του, εκείνος όμως αντέδρασε και δέχθηκε τα πυρά τους, γι αυτό, όπως εξηγούν οι ίδιοι αξιωματικοί, δεν υπήρχε και ανάληψη ευθύνης από κάποια τρομοκρατική επωνυμία. Τέλος, από server χώρας της Βόρειας Ευρώπης ανέβηκε στο διαδίκτυο το διάγγελμα του Ξηρού Χ., όπως διαπιστώθηκε στα εγκληματολογικά εργαστήρια, μέσω προγράμματος κρυφής περιήγησης.

7.1.Επικοινωνία με την Δίωξη Ηλεκτρονικού Συστήματός

Για τις ανάγκες τις πτυχιακής μας θελήσαμε να συνομιλήσουμε με καταξιωμένους ανθρώπους στο χώρο της δίωξης ηλεκτρονικού εγκλήματος Δουκέλη Σταθάκη Παπαθανασίου Γερμανός Φιλιππίδης και πολλούς ακόμα οπού μας βοήθησαν να κατανοήσουμε καλυτέρα κάποια πράγματα.

Αρχικά μας μίλησαν για το ειδικό λογισμικό TLO όπου έτσι εντοπίζουν αρχεία παιδικής πορνογραφίας.
Το TLO είναι ένα πρόγραμμα όπου ψάχνει για peer TO peer p2p προγράμματα το οποίο δουλεύει ταυτόχρονα απ όλες τις αστυνομικές αρχές και δίνει αποτελέσματα ανά χωρά. Η παιδική πορνογραφία έχει αυξηθεί κατά πολύ σε σχέση με το 2014. Συνολικά έχουν 96.334 καταγγελίες για μοναδικά URLs με παιδική πορνογραφία.

Παρόλα αυτά όμως το TLO δεν λειτουργεί στο Darknet. Εκεί η δίωξη ηλεκτρονικού σημαδεύει το hash και το παρακολουθεί.

Έπειτα αναφέρθηκαν σε προγράμματα όπως το Hydra που το εξηγούμε πιο πάνω μας είπαν πως ασχολούνται και με παρόμοια προγράμματα σαν αυτό όπως το GPU, CUDA, CAIN & ADEL JOHN, AIRCRACK, RAINBOW CRACK, OPHCRACK, BRUTUS AET2, LOPHTCRACK, PWDUMP, MEDUSA κ.α.

Η ελληνική δίωξη ηλεκτρονικού μας ενημέρωσε πως δεν υπάρχουν στην Ελλάδα πολλές υποθέσεις σχετικά με το Darknet είναι κάτι σχετικά άγνωστο ακόμα βασικά οι δυνατότητες του είναι άγνωστες ακόμα σε απλούς χρήστες όμως σε σχέση με προηγούμενα χρονιά είναι περισσότερες.

Δεν υπάρχει ακριβής μέθοδος για να βρούνε κάποιον χρήστη στο Darknet διότι οι χρήστες χρησιμοποιούν το Tor όπου τους παρέχει ανωνυμία.
Στο Darknet οι μηχανές αναζήτησης αλλάζουν συνεχώς δεν είναι σταθερές.

Μια βασική διαφορά του Darknet με το DeepNet είναι πως το δεύτερο δεν είναι απαραίτητα παράνομο. Χρησιμοποιείτε επίσης από επιστήμονες ερευνητές green hackers για εγκυκλοπαιδικούς και ερευνητικούς λόγους.

Μηχανές αναζήτησης : redit.com-reddit.com
/r/darknetmarkets.

Site εμπορίας ναρκωτικών όπου πιάστηκαν από την Interpol μετά από 3 χρόνια συστηματικής ερευνάς ώστε να εντοπίσουν την ip τους και κατ΄ επέκταση την φυσική τους διεύθυνση.

Γενικά είναι πολύ δύσκολο το έργο της δίωξης ηλεκτρονικού εγκλήματος σχετικά με το Darknet διότι παρέχεται στους χρήστες ανωνυμία.

Επίσης για απάτες μέσω διαδικτύου απευθυνόμαστε στην
ΔΙ.ΔΗ.Ε. 11188 Δίωξη Ηλεκτρονικού εγκλήματος
Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας:

- Τηλεφωνικά στον αριθμό: 111 88
- Στέλνοντας e-mail στο: **ccu@cybercrimeunit.gov.gr**
- Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smartphones) : CYBERKID για συσκευές iOS και για συσκευές Android g
- Facebook: **www.facebook.com/cyberkid.gov.gr**
- Μέσω Twitter « Γραμμή SOS Cyber Alert»: **@cyberalertGR**
- Ιστότοπος: **www.cyberkid.gr**

7.2.Υποθέσεις που απασχόλησαν τις διωκτικές Αρχές σχετικές με το Dark Web

- **Παραδειγμα 1 : Επιχείρηση Onymous**

Στις 6 Νοεμβρίου 2014 αστυνομικές και δικαστικές Αρχές από διάφορα Κράτη του κόσμου πραγματοποίησαν μια κοινή επιχείρηση, που ονομάστηκε "Onymous", ενάντια σε "σκοτεινές αγορές" (dark markets) που λειτουργούσαν ως υπηρεσίες μέσω του δικτύου ToR. 16 ευρωπαϊκά Κράτη, σε συνεργασία με τις Ηνωμένες Πολιτείες Αμερικής έθεσαν εκτός λειτουργίας μεγάλο αριθμό αγορών. Η επιχείρηση, την οποία συντόνισαν το European Cybercrime Centre (EC3) της Europol, το FBI, το U.S. Immigration and Customs Enforcement's (ICE) του Homeland Security Investigations (HSI) και η Eurojust, οδήγησε στη σύλληψη 17 ατόμων, πωλητών και διαχειριστών online αγορών και στην παύση της λειτουργίας 410 κρυφών ιστοτόπων, μέσω των οποίων διαπιστώθηκε αγοραπωλησία απαγορευμένων αντικειμένων, όπως ναρκωτικών ουσιών και όπλων. Παράλληλα, κατασχέθηκαν bitcoins αξίας σχεδόν ενός εκατομμυρίου δολαρίων, 180.000 ευρώ σε μετρητά, ναρκωτικές ουσίες, χρυσός και ασήμι. Στο πλαίσιο της ίδιας επιχείρησης, το FBI και το U.S. ICE HIS προχώρησε στη θέση εκτός λειτουργίας του ιστοτόπου Silk Road και στη σύλληψη του διαχειριστή του.

- **Παραδειγμα 2: Διαρροή δεδομένων του ιστοτόπου Ashley Madison**

Κυβερνοεγκληματίες δημοσιοποίησαν μεγάλο όγκο δεδομένων χρηστών στο Deep Web. Η πρώτη διαρροή πληροφοριών έλαβε χώρα τον Αύγουστο 2015 και ήταν μεγέθους 9,7 gigabytes. Τα στοιχεία δημοσιεύτηκαν στο Dark Web μέσω διεύθυνσης προσβάσιμης μέσω του Tor (The Onion Router), και περιελάμβαναν στοιχεία λογαριασμών και log-ins για περίπου 32 εκατ. χρήστες της σελίδας - μαζί με στοιχεία καρτών και συναλλαγών που ανάγονται μέχρι και το 2008. Επίσης, διέρρευσαν και «πικάντικες» λεπτομέρειες σχετικά με τις ερωτικές προτιμήσεις των χρηστών.

Η ομάδα των hacker, υπό την ονομασία Impact Team, όμως, δεν σταμάτησε εκεί. Έχοντας ζητήσει το κατέβασμα (που δεν έγινε) του Ashley Madison και του Established Men (επίσης της ίδιας εταιρείας, Avid Life Media), κατηγόρησαν την εταιρεία για τις επιπτώσεις της αποκάλυψης και προχώρησαν σε δεύτερη διαρροή εντός του ίδιου μήνα, η οποία, ανήλθε στα 19 gigabytes.
Ορισμένοι εκμεταλλεύτηκαν τα δεδομένα που διέρρευσαν και προχώρησαν σε διαδικτυακούς εκβιασμούς σε βάρος θυμάτων – χρηστών του ιστοτόπου, προκειμένου να μην αποκαλύψουν σε συγγενικά πρόσωπα των τελευταίων τις δραστηριότητές τους.

- **<u>Παραδειγμα 3 : Επιχείρηση Lecpetex</u>**

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος εξιχνίασε τον Ιούλιο του 2014 την παράνομη διαδικτυακή δράση δύο (2) Ελλήνων, οι οποίοι δημιούργησαν και χρησιμοποίησαν με άνομους σκοπούς (Cracking), το κακόβουλο λογισμικό με την κωδική ονομασία "Lecpetex". Σε βάρος τους σχηματίστηκε δικογραφία, για σύσταση και συμμετοχή σε εγκληματική οργάνωση - συμμορία, απάτη με υπολογιστή, παραβίαση απορρήτου υπολογιστών, καθώς και παράβαση της νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα.
Ειδικότερα, από την ψηφιακή διερεύνηση της υπόθεσης προέκυψε ότι οι δύο εμπλεκόμενοι διέδιδαν το κακόβουλο λογισμικό κυρίως μέσω ιστοσελίδας κοινωνικής δικτύωσης (social media), μολύνοντας μεγάλο αριθμό υπολογιστικών συστημάτων παγκοσμίως. Όπως προέκυψε από την εξέλιξη της έρευνας, οι δράστες χρησιμοποιούσαν τον ιό για συγκεκριμένους ιδιοτελείς σκοπούς, που αφορούν κυρίως:

- Στη χρήση της υπολογιστικής ισχύος των μολυσμένων μηχανημάτων (εκατοντάδων χιλιάδων) για την παραγωγή εικονικού διαδικτυακού χρήματος (bitcoin mining). Συγκεκριμένα το κακόβουλο λογισμικό, μετά την εγκατάσταση του, χρησιμοποιούσε τους μολυσμένους ηλεκτρονικούς υπολογιστές, για να παράγουν ψηφιακά-εικονικά νομίσματα (bitcoin) και
- Στην υποκλοπή ηλεκτρονικών πορτοφολιών (wallets). Οι δράστες με τη χρήση του malware, υπέκλεπταν τους κωδικούς πρόσβασης ηλεκτρονικών πορτοφολιών τα οποία περιείχαν ψηφιακά-εικονικά νομίσματα (bitcoins) και τα μετέφεραν σε άλλα ηλεκτρονικά πορτοφόλια, τα οποία βρίσκονταν υπό τον έλεγχό τους.

Τα διαδικτυακά εικονικά νομίσματα (bitcoins) που συνέλεγαν οι δράστες: α) τα προωθούσαν σε εξειδικευμένες υπηρεσίες μείξης (mixing services), μέσω ειδικού δικτύου (TOR) στο Deep Web. Με τον τρόπο αυτό απέκρυπταν τα ίχνη προέλευσης των παράνομων κερδών που είχαν προέρθει από την παραγωγή bitcoins και από τα ηλεκτρονικά πορτοφόλια που είχαν υποκλέψει και β) τα μετέτρεπαν σε ευρώ με τη χρήση των υπηρεσιών ειδικών ηλεκτρονικών ανταλλακτηρίων τα οποία διατίθενται στο διαδίκτυο, εισπράττοντας, τελικώς, τα παράνομα κέρδη.

- **Παραδειγμα 4 : Επιχείρηση Onymous και Ελληνική Αστυνομία**

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος εντόπισε και συνέλαβε, στο πλαίσιο στοχευμένων ερευνών για την καταπολέμηση της παιδικής πορνογραφίας, χρήστες του Deep Web οι οποίοι διατηρούσαν λογαριασμό σε ιστοσελίδα με υλικό σεξουαλικής κακοποίησης ανηλίκων. Από την ενδελεχή ανάλυση των στοιχείων της επιχείρησης **Onymous**, που κοινοποιήθηκαν στις αστυνομικές υπηρεσίες ανά τον κόσμο, προέκυψε και εμπλοκή Ελλήνων χρηστώνν.

- **Παραδειγμα 5 : Επιχείρηση Scanning Chat της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος**

Εγχειρίδιο που χρησιμοποιείται ως «Κώδικας Επικοινωνίας Παιδόφιλων», στο Διαδίκτυο εντοπίστηκε, έπειτα από έρευνα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, στο Dark Web και για πρώτη φορά στα αστυνομικά χρονικά της χώρας παρουσιάστηκε σε περίληψη, μαζί με τα σύμβολα που χρησιμοποιούν οι παιδόφιλοι για να αναγνωρίζουν τις μεταξύ τους σεξουαλικές προτιμήσεις.

Στο συγκεκριμένο εγχειρίδιο, καλύπτεται σε επτά (7) κεφάλαια οτιδήποτε αφορά στην παιδοφιλία, από την ψυχολογία των παιδιών μέχρι και την προετοιμασία που απαιτείται, ώστε να πραγματοποιήσει ο παιδόφιλος τις ασελγείς του πράξεις. Περιγράφονται, επίσης, τρόποι με τους οποίους ένας παιδόφιλος μπορεί να προσεγγίσει ένα παιδί και να το αποπλανήσει, ενώ αναλύονται και τρόποι με τους οποίους ένας παιδόφιλος μπορεί να προστατέψει τον εαυτό του, αν τυχόν αποκαλυφθεί.

8. Συμπεράσματα

Στο ηλεκτρονικό έγκλημα ο θύτης, λειτουργώντας από την μια πλευρά στην αφάνεια και αφήνοντας ελάχιστα ίχνη και από την άλλη με σύμμαχο την έλλειψη τεχνογνωσίας, καταφέρνει καθημερινά να εισβάλει ακόμα και σε εκείνο το σπίτι με τα τελειότερα συστήματα ασφαλείας έχοντας σχεδόν πάντα σαν σκοπό την απολαβή οικονομικού οφέλους. Παράλληλα οι μορφές των εγκληματικών ενεργειών του καλύπτουν σχεδόν όλο το φάσμα του ποινικού κώδικα, αλλά και των αναφερθέντων νομικών κενών όσον αφορά τον ηλεκτρονικό χώρο δρα ανενόχλητος.

- Στο νέο αυτό περιβάλλον, οι αρχές καλούνται να αντιμετωπίσουν το έγκλημα εκσυγχρονίζοντας της υπηρεσίες της ΥΔΗΕ με τα κατάλληλα τεχνικά μέσα,
- Απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών κριτηρίων για τα ηλεκτρονικά εγκλήματα, που να θέτουν όρια στην συμπεριφορά όσων χρησιμοποιούν το διαδίκτυο
- Κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθούν υπόψη η ελεύθερη διακίνηση ιδεών και οι λοιπές συνταγματικές αρχές.
- Απαραίτητη καθίσταται και η εκπαίδευση όλων των εμπλεκόμενων φορέων (εισαγγελικών, δικαστικών και αστυνομικών αρχών) και κυρίως των αστυνομικών της ΥΔΗΕ σε θέματα διαδικτύου, καθώς και η ενημέρωση των πολιτών στην χρήση του.

Τα συμπεράσματα στα οποία καταλήξαμε καθώς και οι προτάσεις μας για περαιτέρω μελέτη είναι οι εξής:

- Πλέον η ανώνυμη περιήγηση θεωρείται απαραίτητη για κάποιους ανθρώπους όπως για παράδειγμα ερευνητές, δημοσιογράφους κλπ. ώστε να εξασφαλίσουν την ανωνυμία τους για την προσωπική τους ασφάλεια.

- Το Darknet δεν είναι απαραίτητα 'κακό' πολλές φόρες λειτουργεί καλοπροαίρετα ώστε να παρέχει ασφάλεια, εκπαίδευση και ενημέρωση.

- Άξιο σημείωσης είναι πως ένα εργαλείο με αυτές τις άπειρες δυνατότητες χρησιμοποιείται κατά κύριο λόγο για παράνομες πράξεις. Ενώ κάλλιστα θα μπορούσε να προσφέρει πολλά παραπάνω στην κοινωνία μας.

- Όμως απ' την στιγμή που προσφέρει ανωνυμία σε περιβάλλον με άπειρη έκταση και δυνατότητες αποτελεί ένα 'δυνατό egraleio το οποίο δεν θα άφηναν ανεκμετάλλευτο οι εγκληματίες για να εκτελέσουν τις παράνομες πράξεις τους.

- Το Darknet ως απροσπέλαστο από τις μηχανές αναζήτησης καθιστά το έργο των διωκτικών άρχων δύσκολο ως και ακατόρθωτο.

- Το Darknet είναι ευρέως αναπτυγμένο καθώς έχει φτάσει και στην Ελλάδα μη γνωρίζοντας σε πόσο μεγάλο βαθμό και χωρίς την κατάλληλη ενημέρωση και εκπαίδευση των απλών χρηστών.

ΠΑΡΑΡΤΗΜΑ Α.

Εισαγωγή

Το παρακάτω παράρτημα αναφέρεται στη μέθοδο SNA οπού περιγράφεται σε μια γραφική παράσταση διάφορες μετρήσεις που γίνονται πάνω σε ένα δίκτυο. Το δίκτυο είναι ένα διμερές κατευθυνόμενο γράφημα που αποτελείται από κόμβους και συνδέσμους. Κάθε κόμβος αντιπροσωπεύει ένα χρήστη στον διαδικτυακό φόρουμ, και κάθε σύνδεσμος αποτελεί μια απάντηση μεταξύ δύο χρηστών.

SNA

Social network analysis (SNA) είναι μια γραφική παράσταση που βασίζεται στη μέθοδος για την ανάλυση του δικτύου της δομή μιας ομάδας ή του πληθυσμού και τις επιπτώσεις της στην κοινωνική αλληλεπίδραση (Liben- Nowel 2007). SNA έχει χρησιμοποιηθεί ευρέως για τη μελέτη διαφόρων στο πραγματικό κόσμο των δικτύων (Kossinets και Watts 2006). Τα κοινωνικά δίκτυα που σχηματίζονται σε παράνομες οργανώσεις είναι αναφερόμενα ως σκοτεινά δίκτυα (Darknet) (Raab και Milward 2003). Τα σκοτεινά δίκτυα μπορούν να είτε στον πραγματικό κόσμο, όπως τα εγκληματικά δίκτυα που μελετήθηκαν από τον Huetal. (2009), ή στον εικονικό κόσμο, όπως τα κοινωνικά δίκτυα στο φόρουμ που χρησιμοποιούνται από τρομοκράτες (Reid et al. 2004) για να εξαπλωθούν ριζοσπαστικές θρησκευτικές απόψεις, να οργανώσουν τρομοκρατικές δραστηριότητες, ή να μοιραστούν τις γνώσεις για την κατασκευή όπλων. Έτσι, τρομοκρατικά φόρουμ μπορεί να είναι ένας σημαντικός πόρος πληροφοριών για τα καθήκοντα της αντιτρομοκρατικής (Coll και Glasser 2005). Σε φόρουμ στο διαδίκτυο, ένα νήμα είναι μια συλλογή των θέσεων, που εμφανίζεται από χρόνο σε αύξουσα τιμή. Το κοινωνικό δίκτυο στο φόρουμ βασίζεται στη δομή του νήματος και συνήθως αναφέρεται ως "απάντηση δικτύου" (Zhang et al 2007?. Adamic et al 2008).

Οι μετρήσεις στο κοινωνικό δίκτυο είναι διάφορες μετρήσεις των κόμβων που μπορεί να αντανακλά τη σημασία ή τη σύνδεση του κόμβου. Υπάρχουν διάφοροι τύποι των μετρικών

που χρησιμοποιούνται συνήθως σε SNA για διάφορους σκοπούς, όπως για μια κεντρική τοποθεσία, συνοχή, και προσβασιμότητα (Albert και Barabasi 2002). Κεντρικότητα είναι ένα σύνολο μετρήσεων που περιγράφει η σημασία των κόμβων ανάλογα με την ισχύ τους για τη σύνδεση του δικτύου, συμπεριλαμβανομένων των betweenness, βαθμό, και την εγγύτητα. Συνοχή σε ένα κοινωνικό δίκτυο περιγράφει πόσο καλά ένα υποσύνολο των κόμβων συνδέεται με το άλλο από πλευράς ώστε να σχηματίζουν μια κλίκα. Η συνοχή μπορεί να μετρηθεί χρησιμοποιώντας συντελεστής ομαδοποίησης ενός κόμβου, και μια υψηλότερη τιμή υποδεικνύει ότι αν ο κόμβος και οι πρώτες γείτονες του κόμβου σχηματίζουν ένα σύμπλεγμα, είναι πιθανό ότι οι δύο κόμβοι σε αυτό το σύμπλεγμα να έχει μια άμεση σύνδεση.

Η συνδεσιμότητα του δύο κόμβων, συμπεριλαμβανομένων των μετρήσεων όπως η απόσταση, η οποία είναι η αριθμός των ακμών στο μονοπάτι που συνδέει δύο κόμβους. Εκτός από αυτές τις κλασικές μετρήσεις, υπάρχουν και άλλοι αλγόριθμοι και μετρήσεις που αναπτύχθηκε ειδικά για την εκτίμηση της σημασίας σε ένα δίκτυο ιστοσελίδας, όπως βαθμολογίες PageRank και HITS βαθμολογίες.

ΠΑΡΑΡΤΗΜΑ Β.

Εισαγωγή

Σε αυτό το παράρτημα θα αναφέρουμε κάποια σχετικά εργαλεία όπου χρησιμοποιούν διάφοροί επιτήδειοι και τα οποία μπορούμε να τα οποία υπάρχουν ελεύθερα στο internet. Μερικά από αυτά είναι:

- **THC HYDRA**

Το THC Hydra, είναι ένα δυνατό λογισμικό, τ' οποίο ανάμεσα στα άλλα, έχει την δυνατότητα, να εξετάζει την αντοχή των διαφόρων λογαριασμών μας. Στην πράξη, δηλαδή, μπορεί να κάνει επίθεση και να σπάσει κάποιους.

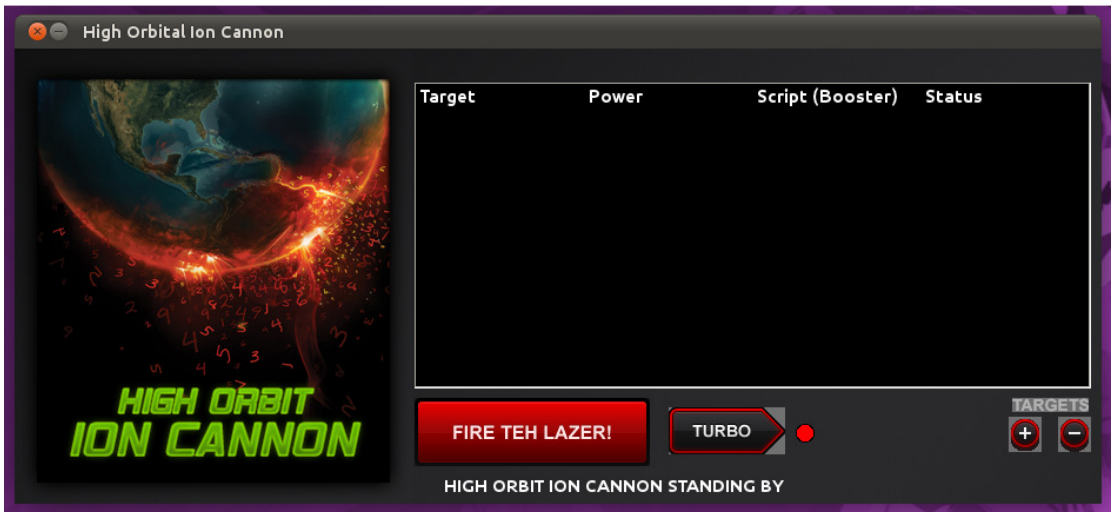
- **HOIC**

Ένα διαδεδομένο εργαλείο που χρησιμοποιούν οι χακτιβιστές (και με αυτό έγιναν και οι παραπάνω επιθέσεις που αναφέρουμε, (μα και άλλες), είναι το γνωστό πλέον HOIC (High Orbit Ion Canon).

Αναλυτικά τι είναι αυτό το HOIC:

Είναι μια εφαρμογή, ένα εκτελέσιμο αρχείο, για Windows, Linux και OSX, δηλαδή και τρέχουν απλά με διπλό κλικ επάνω τους).
Να αναφέρουμε σε αυτό το σημείο πως τόσο η ιστοσελίδα του (hoic.99k.org), όσο και άλλα σημεία που μπορούσε να κατεβεί, έχουν κυριολεκτικά ξηλωθεί από το διαδίκτυο (αν και πάντα υπάρχουν -ακόμα- τρόποι διαμοιρασμού).

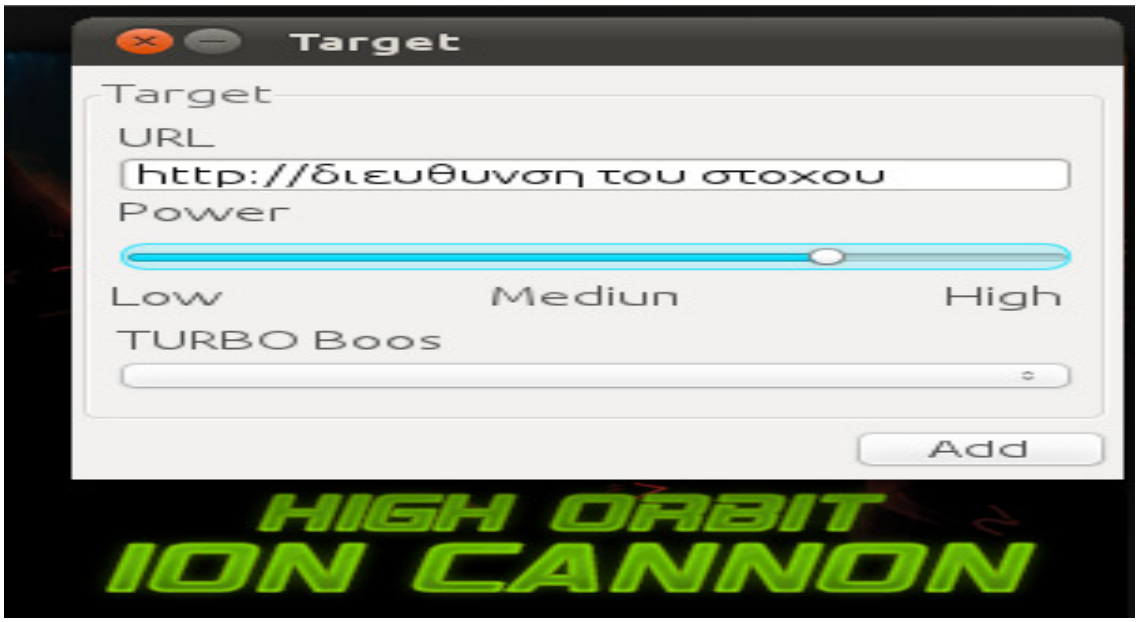
Με το που θα τρέξει κάποιος το HOIC η πρώτη οθόνη που αντικρίζει, είναι η παρακάτω:



Στη συνέχεια αν ο χρήστης (επιτιθέμενος), κάνει κλικ επάνω στο εικονίδιο με σύμβολο συν (+), ανοίγει ένα pop-up παράθυρο, όπου πρέπει να καθοριστούν τα δεδομένα του στόχου και την ισχύ της ταχύτητας επίθεσης (μπορούν να μπουν και περισσότεροι του ενός στόχοι).

Πάνω-κάτω οι μετρήσεις δείχνουν τα εξής:

- Low = ~2 requests/sec, για κάθε url (διεύθυνση στόχου που έχει οριστεί)
- Mediem = ~4 requests/sec, για κάθε url (διεύθυνση στόχου που έχει οριστεί)
- High - ~8 requests/sec, για κάθε url (διεύθυνση στόχου που έχει οριστεί)



Το Booster που έχει πιο κάτω, είναι ένα στοιχείο που καθορίζει τα dynamic request attributes:

Έχοντας κάνει τις επιλογές του αυτές λοιπόν ο επιτιθέμενος αρκεί να πατήσει το κουμπάκι Add και να επιστρέψει στην αρχική οθόνη του HOIC.

Ο εισβολέας, στη συνέχεια, αν θέλει μπορεί να προσαρμόσει περαιτέρω το THREADS Number, ώστε να αυξήσει την ένταση της επίθεσης.

Στη συνέχεια, αρκεί να πατήσει το κουμπάκι: FIRE TEH LAZER!, ώστε να ξεκινήσει η επίθεση.

Να λάβετε υπ' όψην, ότι σε αυτές τις περιπτώσεις χρειάζονται πάρα πολλοί υπολογιστές να κάνουν το ίδιο πράγμα ταυτόχρονα και η οργάνωση αυτή, της ώρας επίθεσης, κανονίζεται από διάφορα κανάλια επικοινωνίας, ανάμεσα τους και το IRC.
Η διαφορά που έχει το HOIC, από το LOIC, έγκειται στις παραπάνω δυνατότητες του δεύτερου, στη καλύτερη "κάλυψη" και πάνω απ' όλα στο booster που αυξάνει την ισχύ της επίθεσης.

- **LOIC**

Παράλληλα, είδαμε και διάφορες δημοσιεύσεις, ιδιαίτερα στο Facebook, σχετικά με τις επιθέσεις και τη προτροπή να κατεβάσουν διάφορα εργαλεία ώστε να μετέχουν και οι απλοί χρήστες. Το δε χειρότερο ήταν πως αυτά τα έλεγαν μέσω του προφίλ τους, στο Facebook.

Σε ένα από αυτά τα εργαλεία με την ονομασία LOIC, τ' οποίο επιτρέπει σε απλούς χρήστες να μετέχουν σε DDoS επιθέσεις, μη κάνοντας τίποτε παραπάνω από το να επικολλήσουν τη δικτυακή διεύθυνση (url) της ιστοσελίδας στόχου.

Το LOIC λοιπόν, είναι Ανοιχτού Κώδικα, διαθέσιμο για Linux, Windows, OSX, FreeBSD και έχει γραφεί στη γλώσσα προγραμματισμού C#. Η δημιουργία της, κρατάει από το Praetox Technologies με σκοπό να είναι ένα stress testing και denial-of-service attack. Στη πορεία άνοιξε τον κώδικα του και τον διέθεσε και αναπτύχθηκε περαιτέρω από χακτιβιστες, κάνοντας το στην ουσία ένα απλό Java script που επιτρέπει τη συμμετοχή οποιοιδήποτε, απλά και μόνο μέσω του browser του.

Το πλήρες όνομα του είναι: Low Orbit Ion Cannon και έτσι (LOIC), ονομαζόταν ένα όπλο από το δημοφιλέστατο παιχνίδι Command & Conquer. Δημοφιλές και γνωστό στο ευρύ κοινό, έγινε κατόπιν της γνωστής κινητοποίησης Operation Global Blackout.

Έχει ενσωματωμένο ένα χαρακτηριστικό που ονομάζεται: Hivemind τ' οποίο και δίνει τη δυνατότητα σε αυτόν που το χρησιμοποιεί, να συνδέσει το αντίγραφο της εφαρμογής που έχει κατεβάσει με κάποιον IRC server. Με αυτό τον τρόπο δίνει την άδεια σε κάποιον άλλο να πάρει τον έλεγχό της εφαρμογής του, δηλαδή την υπολογιστική του ισχύ και να την στρέψει, μαζί με όλους τους υπόλοιπους συνδεδεμένους clients, προς την ιστοσελίδα στόχο.

Για να γίνει αυτό χρειάζονται χιλιάδες LOIC να στοχεύουν προς μια και μόνο ιστοσελίδα ωστε η επίθεση να έχει αποτέλεσμα. Η κεντρική διαχείριση να γίνεται από ένα και μόνο άτομο, ο οποίος και θ' αποφασίσει το πότε ακριβώς θα εξαπολύσει την επίθεση. Αυτό φυσικά συνεπάγεται πως δίνουμε σε κάποιον τρίτο, τον έλεγχο του υπολογιστή μας.

Ένας ασφαλής τρόπος για κάτι τέτοιο είναι η διαδικασία να γίνει με μια διανομή Linux που θα τρέχει σε κάποιο usb στικακι live (η από κάποιο cd). Η δουλειά δηλαδή που κάνουν όλα αυτά τα ενωμένα (χιλιάδες) LOIC, είναι να χρησιμοποιούν τις συνδέσεις των χρηστών, προκείμενου να στέλνουν συνεχόμενα αιτήματα (requests) απευθείας προς τον server που φιλοξενείται η ιστοσελίδα στόχος.

Αν και μόνο ένας υπολογιστής μπορεί να δημιουργήσει κάμποσα αιτήματα TCP, UDP ή HTTP που απαιτούνται ώστε να υπερφορτώσει ένας server, εν τούτοις είναι σχεδόν αδύνατο να τα καταφέρει επειδή τα requests που στέλνονται έτσι, αγνοούνται εύκολα από τον στοχοποιημένο server. Αυτός και ο λόγος που χρειάζεται να είναι ενωμένοι ταυτόχρονα πολλοί υπολογιστές (συνδέσεις + υπολογιστική ισχύς), ώστε οι αιτήσεις (requests) που δέχεται ο επιτιθέμενος server είναι τόσες πολλές και τελικά αδυνατώντας ν' αντέξει, τερματίζει εντελώς τη λειτουργία του, "πέφτοντας" και μη μπορώντας να τον επισκεφθεί κανείς.

Πρακτικά τώρα, αν κάποιος το χρησιμοποιήσει, αν η επίθεση DDoS είναι πετυχημένη τα πάντα από τον server στόχο, βρίσκονται εκτός λειτουργίας. Αυτό έχει και σαν συνέπεια τα αρχεία (log files) που καταγράφουν κάθε εισερχόμενη σύνδεση, να μη δουλεύουν και να έτσι να μη καταγράφουν τίποτε απολύτως. Ακόμη όμως κι αν σε κάποια σπάνια περίπτωση τα log-files προλάβουν και καταγράψουν κάτι, οι χρήστες του LOIC μπορούν άπλα ισχυριστούν πως έπεσαν θύματα, καθώς κάποιος άγνωστος σε αυτούς, κατάφερε και εισήλθε στο δίκτυό τους ή πως ο υπολογιστής τους ήταν θύμα κάποιου bot net (ενός DDoS client) που εγκαταστάθηκε στο σύστημα εν αγνοία τους και συνεπώς αυτό ανάγκασε τον υπολογιστή τους, να έχει τέτοια συμπεριφορά (του LOIC).

Αυτό άλλωστε, είναι κάτι που συμβαίνει καθημερινά και όπως και να έχει σε καμία περίπτωση δεν υπάρχει η δυνατότητα να εξακριβωθεί.

Ανησυχία για το αν το LOIC περιλαμβάνει κακόβουλο κώδικα, δεν πρέπει να υπάρχει, καθώς είναι Ανοιχτού Κώδικα και έτσι ο κίνδυνος είναι ανύπαρκτος. Βασική φυσικά, προϋπόθεση είναι να κατέβει και από την επίσημη σελίδα του και όχι από οπουδήποτε αλλού. Στην ουσία, το μόνο πρόβλημα είναι αυτό που αναφέραμε πιο πάνω, ότι στην ουσία δίνετε τον πλήρη έλεγχο του υπολογιστή σας, σε κάποιο τρίτο άτομο, τ' οποίο και το πιο πιθανό είναι να μη γνωρίζετε, τ' οποίο προσπερνιέται με μια Linux διανομή. όπως αναφέραμε.

Υπάρχουν και άλλα εργαλεία αντίστοιχα, μα το LOIC είναι το πιο διαδεδομένο και αυτό που χρησιμοποιείται καθημερινά, για τον οποιοδήποτε λόγο, στο διαδίκτυο.

Για να το χρησιμοποιήσετέ δοκιμαστικά στην ιστοσελίδα σας, θα πρέπει προηγουμένως, να έχετε επικοινωνήσει με την εταιρεία web-hosting που έχετε.

9.Βιβλιογραφία

Αλεξιάδης, Σ., (1996). *Εγχειρίδιο εγκληματολογίας*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Bell, S., (2008). *Encyclopedia of forensic science, revised edition*. Infobase Publishing.

Bergman, M.K, (2002). White paper, The Deepweb: Surfacing hidden value.

Bigelow, R., (1985). *The challenges of computer law*. Western New England Law Review v. 7, p. 397.

Βελέντζας, ΕΙ., (2008). *Δίκαιο τεχνολογίας και καινοτομίας*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Βλαχόπουλος, Κ., (2007). *Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση*. Αθήνα, Νομική Βιβλιοθήκη.

Caloyannides, M., (2004). *Privacy protection and computer forensics*. 2nd Edition, Artech House.

Casey, E., (2004). *Digital evidence and computer crime: Forensic science, computers, and the internet*. 2nd Edition, Academic Press.

Γκρίτζαλης, Σ., Κάτσικας, Σ., και Γκρίτζαλης Δ., (2003). *Ασφάλεια δικτύων υπολογιστών*. Αθήνα, Παπασωτηρίου.

Δήμου, Γ., (2002). *Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων*, Αθήνα, Παπασωτηρίου.

Ζάννη, Α., (2005). *Το διαδικτυακό έγκλημα*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Furnell, S., (2006). *Κυβερνοέγκλημα-Καταστρέφοντας την κοινωνία της πληροφορίας*. Μετάφραση: Φ. Μηλιώνη, Αθήνα, Εκδόσεις Παπαζήση.

Glick, L, (1995). *Criminology*. Boston, Allyn and Bakon, Editors, p. 120.

Jansen, W., & Ayers, R., (2007) *Guidelines on cell phone forensics. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-101.

Jones, R., (2005). *Internet forensics*. O'Reilly Publishing. ISBN 059610006X.

Kanellis, P., (2006). *Digital crime and forensic science in cyberspace*. Idea Group Inc.

Καϊάφα-Γκμπάντι, Μ., & Συμεωνίδου-Καστανίδου, Ε., (2004). *Ποινικός κώδικας και ειδικοί ποινικοί νόμοι*. Β΄ έκδοση, Αθήνα, Νομική Βιβλιοθήκη.

[90]

Καρακώστας, Ι., (2003). Δίκαιο και internet. Νομικά ζητήματα στο διαδίκτυο. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Κάτσικας, Σ., Γκρίτζαλης, Δ., Γκρίτζαλης Σ., (2004). *Ασφάλεια πληροφοριακών συστημάτων*. Αθήνα, Εκδόσεις Νέων Τεχνολογιών.

Κιούπης, Δ., (1999). Ποινικό δίκαιο και ιντερνέτ. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Κιούπης, Δ., & Ιωαννίδου, Α., (2007). *Η παιδική πορνογραφία στο διαδίκτυο*. Αθήνα, Νομική Βιβλιοθήκη.

Κριθαράς, Θ., (2009). *Ποινικό δίκαιο και διαδίκτυο*. Αθήνα, Νομική Βιβλιοθήκη.

Lemley, M.A., & Reese, R.A., (2004). *Reducing digital copyright without restricting innovation*, 56 Stan. L. Rev. 1345, 1382.

Λάζος, Γ., (2001). *Πληροφορική και έγκλημα*. Αθήνα, Νομική Βιβλιοθήκη.

Mohay, G., (2003). *Computer and intrusion forensics*. Artech House.

Μαγκάκης, Γ.Α., (1984). *Ποινικό δίκαιο*. Έκδοση Γ΄ βελτιωμένη, εκδόσεις Παπαζήση.

Νικολαΐδης, Χ., (1999*). Η σκοτεινή πλευρά του Internet*. Αθήνα, Εκδόσεις Anubis.

Skoudis, E., (2002). *A step-by-step guide to computer attacks and effective defenses*. Prentice-Hall.

Συκιώτου, Α., (2009). *Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Τσουραμάνης, Χ., (2005). *Ψηφιακή εγκληματικότητα. Η (αν)ασφαλής όψη του διαδικτύου*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Wood, J., (2010). The Darknet: A digital copyright revolution. Richmond Journal of Law and Technology 16 (4): 1-60.

Βλαχόπουλου Κ., *Ηλεκτρονικό Έγκλημα*, Εκδ. Νομική Βιβλιοθήκη (2007)

Κιούπη Δ*., Ηλεκτρονικά Οικονομικά Εγκλήματα*, σε Κουράκη Ν., «Τα Οικονομικά Εγκλήματα ΙΙ Ειδικό Μέρος», Εκδ. Αντ. Ν. Σάκκουλα

Λάζος Γ. *Πληροφορική και έγκλημα* , Εκδόσεις Νομική Βιβλιοθήκη , (Αθήνα 2001)

Μαλλέρου Α., *ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ*

Μαρκοπούλου Παγώνα, *Η Σύμβαση για το Κυβερνοέγκλημα*, 2008

Μυλωνόπουλου Χ*., Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο*, Εκδ. Αντ. Ν. Σάκκουλα, (1991)