ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Πτυχιακή Εργασία

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΟΡΦΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

ΑΓΓΕΛΑΚΗΣ ΧΡΗΣΤΟΣ Α.Μ. 14699

ΙΩΣΗΦΕΛΛΗ ΑΣΠΑΣΙΑ Α.Μ. 14306

Μεσολόγγι 2018

ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Πτυχιακή Εργασία

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΟΡΦΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

ΑΓΓΕΛΑΚΗΣ ΧΡΗΣΤΟΣ Α.Μ. 14699

ΙΩΣΗΦΕΛΛΗ ΑΣΠΑΣΙΑ Α.Μ. 14306

Επιβλέπουσα καθηγήτρια

Παναγιώτα Βάθη

Μεσολόγγι 2018

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Διοίκησης Επιχειρήσεων Μεσολογγίου του ΤΕΙ Δυτικής Ελλάδας δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΕΥΧΑΡΙΣΤΙΕΣ

Φτάνοντας στο τέλος των σπουδών μας έχοντας μαζέψει πολλές εμπειρίες και όμορφες στιγμές θα θέλαμε να ευχαριστήσουμε τις οικογένειές μας που βρίσκονται τα χρόνια αυτά δίπλα μας αρωγοί και μας στηρίζουν οικονομικά και προπάντων ηθικά. Η συμβολή τους είναι καθοριστική και τους οφείλουμε το ότι είμαστε σήμερα.

Θα θέλαμε να ευχαριστήσουμε την επιβλέπουσα καθηγήτρια κυρία Βάθη, αρχικά γιατί δέχτηκε να μας αναλάβει στην εκπόνηση της πτυχιακής μας και κατά δεύτερον διότι μας βοήθησε όποια στιγμή τη χρειαστήκαμε παρέχοντας μας τις γνώσεις και συμβουλές της.

Τέλος, ευχαριστούμε τους καθηγητές του τμήματος Διοίκησης Επιχειρήσεων οι οποίοι με περίσσιο σθένος βρίσκονταν πάντα κοντά σε κάθε φοιτητή.

ΠΕΡΙΛΗΨΗ

Στη σημερινή εποχή της πληροφορίας και των τεχνολογικών εξελίξεων παρατηρείται η ολοένα αυξανόμενη διείσδυση των ευρυζωνικών τεχνολογιών στην κοινωνία και διαφαίνεται η τάση για σύγκλιση των τηλεπικοινωνιακών δικτύων παροχής υπηρεσιών καθώς και για πρόσβαση «οποτεδήποτε», «από οπουδήποτε», και «με ο,τιδήποτε».

Σε αυτό το συνεχώς μεταβαλλόμενο περιβάλλον, η έννοια της Ασφάλειας Η/Υ και Δικτύων αποκτά μια καινούρια διάσταση. 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.

Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο. Οι έννοιες «ηλεκτρονικό έγκλημα» ή «κυβερνοέγκλημα» καθώς και οι τεχνολογίες που χρησιμοποιούνται για τη διάπραξη, ανίχνευση και αντιμετώπιση κακόβουλων επιθέσεων σε συστήματα και εφαρμογές, αποτελούν αναπόσπαστο κομμάτι του γνωστικού αντικειμένου της Ασφάλειας Πληροφοριακών Συστημάτων. Η παρούσα πτυχιακή φωτίζει ορισμένες από τις πτυχές που διέπουν το ηλεκτρονικό έγκλημα και τις στρατηγικές για την καταπολέμηση του.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η παρούσα πτυχιακή φωτίζει ορισμένες από τις πτυχές που διέπουν το ηλεκτρονικό έγκλημα και τις στρατηγικές για την αντιμετώπιση του. 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. Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο. Οι έννοιες ηλεκτρονικό έγκλημα ή κυβερνοέγκλημα καθώς και οι τεχνολογίες που χρησιμοποιούνται για τη διάπραξη, ανίχνευση και αντιμετώπιση κακόβουλων επιθέσεων σε συστήματα και εφαρμογές, αποτελούν αναπόσπαστο κομμάτι του γνωστικού αντικειμένου της Ασφάλειας Πληροφοριακών Συστημάτων (Βλαχόπουλος, 2007).

Στο διαδίκτυο υπάρχει –έστω φαινομενικά κάποιες φορές- ανωνυμία. Σύμφωνα με την Ελληνική Αστυνομία (2016) οι κυριότερες μορφές των ηλεκτρονικών εγκλημάτων, που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ, είναι οι απάτες μέσω διαδικτύου, η παιδική πορνογραφία, η διακίνηση και πειρατεία λογισμικού, οι κακόβουλες εισβολές σε δίκτυα (hacking), οι απάτες με πιστωτικές κάρτες, η διακίνηση ναρκωτικών καθώς και ο διαδικτυακός εκφοβισμός που απαντάται συνήθως στα μέσα κοινωνικής δικτύωσης και γενικότερα τα εγκλήματα στα chat rooms[1].

Η ύπαρξη ενός ατόμου με κίνητρο να διαπράξει έγκλημα, ενός κατάλληλου και ευάλωτου στόχου καθώς και η απουσία αποτελεσματικού ελέγχου/αστυνόμευσης είναι τρεις βασικές προϋποθέσεις, που όντας ταυτόχρονα παρούσες χωρικά και χρονικά, δύναται να οδηγήσουν στην εμφάνιση ποινικά κολάσιμων συμπεριφορών τόσο εντός όσο και εκτός της διαδικτυακής ζωής. Το γεγονός ότι το ίδιο το διαδίκτυο είναι από την ύπαρξη του «εγκληματογόνο», ενισχύεται και από τα εγγενή χαρακτηριστικά του, τα οποία και συμβάλλουν στη ραγδαία αύξηση του ηλεκτρονικού εγκλήματος και συνοψίζονται ως κάτωθι (Newman & Clarke, 2003):

[1]Νέες τεχνολογίες και έγκλημα. Θεώνη Γ. Σπαθή. Διαθέσιμο στο: http://www.indeepanalysis.gr/nomika-themata/nees-technologies-kai-egklhma.

ΚΕΦΑΛΑΙΟ 1: ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΔΙΑΚΡΙΣΕΙΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

1.1 Έννοια ηλεκτρονικού εγκλήματος

Το Ηλεκτρονικό Έγκλημα (Computer Crime) είναι μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της (Forester & Morrison, 1994). Ένας τέτοιος ορισμός θα μπορούσε να χαρακτηριστεί υπεραπλουστευμένος. Θα χαρακτηρίζαμε το Ηλεκτρονικό Έγκλημα σαν μια νέα μορφή εγκλήματος με μοναδικό μέσο εκτέλεσης την ιδία τη χρήση των ηλεκτρονικών υπολογιστών. Πρόκειται για μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων με μοναδική διαφορά την εκτέλεση αυτών μέσω ενός υπολογιστή. Στην ελληνική γλώσσα οι οροί που χρησιμοποιούνται είναι ηλεκτρονικό έγκλημα, δικτυακό έγκλημα και έγκλημα του κυβερνοχώρου.

Βασική προϋπόθεση στο ηλεκτρονικό έγκλημα είναι η ύπαρξη ενός ηλεκτρονικού υπολογιστή. Ο υπολογιστής μπορεί να αποτελεί ένα βοηθητικό μέσο για την διάπραξη του εγκλήματος ή να είναι το ίδιο το μέσο με το όποιο θα εκτελεστεί κάποια επίθεση ενώ φυσικά μπορεί να αποτελέσει και το ίδιο το «θύμα» της επίθεσης.

Ο ορισμός του ηλεκτρονικού εγκλήματος έχει να κάνει με την οπτική γωνία από την οποία εξετάζεται. Αυτή η πολυμορφία του εγκλήματος είναι που δυσχεραίνει και τον νομοθέτη, ο όποιος αποφεύγει να του προσδώσει έναν ορισμό και είτε αφήνει αυτήν την αρμοδιότητα στα δικαστήρια και στην παραγόμενη νομολογία, είτε δανείζεται τους χρησιμοποιούμενους από την τεχνολογία όρους.

Σύμφωνα με τον Τσουραμάνη (2006) ένας οργανισμός που έχει δείξει ενδιαφέρον για το κυβερνοέγκλημα είναι η Εξεταστική Επιτροπή της Μεγάλης Βρετανίας ένα ανεξάρτητο σώμα και κυρίως είναι υπεύθυνο για τον έλεγχο των δραστηριοτήτων των τοπικών κυβερνήσεων. Η επιτροπή αυτή διενήργησε έρευνες προκειμένου να εξακριβώσει την έκταση του εγκλήματος μέσω ηλεκτρονικού υπολογιστή τόσο στο δημόσιο όσο και στο ιδιωτικό τομέα και κατέληξε στο συμπέρασμα πως με το πέρασμα του χρόνου διάφορες κατηγορίες εγκλημάτων έχουν

αυξηθεί και χωρίζονται σε δύο μεγάλες κατηγορίες: τα εγκλήματα με τη βοήθεια του Η/Υ και τα εγκλήματα επικεντρωμένα στον Η/Υ.

Το διαδίκτυο πλέον κατέχει ένα σπουδαίο ρολό στη σύγχρονη καθημερινότητα κι αποτελεί βασικό εργαλείο για την πλειοψηφία των χρηστών. Αυτή την διάσταση λοιπόν έρχεται να ακολουθήσει και να εκμεταλλευτεί το ηλεκτρονικό έγκλημα. Η τέλεση ενός τέτοιου εγκλήματος δεν απαιτεί τη φυσική παρουσία του δράστη στον άλλο χώρο αφού μπορεί να γίνει σε ελάχιστα δευτερόλεπτα με τη χρήση ενός δικτυωμένου υπολογιστή. Αυτό αρκεί για να εισβάλει στα υπολογιστικά συστήματα που τον ενδιαφέρουν σε οποιοδήποτε σημείο του κόσμου κι αν βρίσκεται αυτό.

Αυτού του είδους η εισβολή είναι μια απλή υπόθεση που δεν απαιτεί εξειδικευμένη γνώση υπολογιστών αφού στο διαδίκτυο διατίθενται ελευθέρα εφαρμογές λογισμικού που επιτρέπουν στους εισβολείς τη διάπραξη του εν λόγω εγκλήματος. Οι εισβολείς, που είναι γνωστοί και ως hackers, μπορούν να εισέρχονται σε αλλά δίκτυα και υπολογιστικά συστήματα ή ακόμα και να διαχέουν ιούς από τον χώρο τους, σαμποτάροντας πολλές φορές, αυτά τα συστήματα. Αυτό καθίστα αναμφίβολα περισσότερο εύκολη τη διάπραξη του ηλεκτρονικού εγκλήματος σε σχέση με το συμβατικό.

Η επικοινωνία μεταξύ ατόμων από οποιοδήποτε σημείο του πλανήτη σε πραγματικό χρόνο μέσω του ηλεκτρονικού ταχυδρομείου (e-mail) ή των δωματίων συζητήσεων (chat rooms) ή των ομάδων ειδήσεων (newsgroups), αποτελεί μία νέα αδιαμφισβήτητη επανάσταση στον τομέα της επικοινωνίας. Δίνεται η δυνατότητα ταυτόχρονης επικοινωνίας περισσότερων των δύο ατόμων ανέξοδα κι εύκολα. Επομένως δε θα μπορούσε να λείπει σε καμία περίπτωση και ο κίνδυνος του ηλεκτρονικού εγκλήματος, αφού οι δράστες αναζητούν υποψήφια θύματα μέσω αυτών των διαύλων επικοινωνίας. Η πιο διαδεδομένη επίθεση είναι αυτή της ανεπιθύμητης αλληλογραφίας, γνωστή και ως spam. Η παιδική πορνογραφία είναι κι αυτή προϊόν του ηλεκτρονικού εγκλήματος.

Όπως αναφέρθηκε παραπάνω, η τέλεση του εγκλήματος μπορεί να γίνει από οποιοδήποτε σημείο της γης σχετικά εύκολα αρκεί να υπάρχει ηλεκτρονικός υπολογιστής συνδεδεμένος στο διαδίκτυο. Αυτό επομένως καθίστα αδύνατο στις αρμόδιες αρχές δίωξης να εντοπίσουν τον χρόνο και τον τόπο τέλεσης του

εγκλήματος, ενώ συχνά συμβαίνει ο εισβολέας να διαγράφει τα ίχνη του ηλεκτρονικού εγκλήματος, κάτι που καθίστα ακόμα πιο δύσκολο τον εντοπισμό του. Στηριζόμενος λοιπόν στις πιθανές ασάφειες του νόμου ή σε κάποια κενά του αποφεύγει συνήθως την καταδίκη για την πράξη του (Τσουραμάνης, 1996). Για το λόγο αυτό είναι επιτακτική η ανάγκη πληρέστερης και συνεχόμενης εκπαίδευσης - ενημέρωσης των διωκτικών αρχών στις νέες τεχνολογίες.

1.2 Κατηγορίες και ειδικότερες μορφές ηλεκτρονικού εγκλήματος

Οι ειδικοί έχουν προβεί σε μία ταξινόμηση των ηλεκτρονικών εγκληματικών πράξεων σε τρεις κατηγορίες, ανάλογα με τη μορφή τους (Council of Europe, 2005):

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος. Ωστόσο, παρόλο που οι συγκεκριμένες πράξεις έχουν την ίδια αντικειμενική και υποκειμενική υπόσταση ανεξαρτήτως του περιβάλλοντος στο οποίο βρίσκουν εφαρμογή, η αντιμετώπισή τους δεν είναι ίδια λόγω της ιδιαίτερης φύσης τους. Το γεγονός αυτό ανάγκασε τον Έλληνα νομοθέτη να θεσπίσει ειδικούς κανόνες δικαίου για ορισμένες εγκληματικές πράξεις που τελούνται τόσο σε κοινό περιβάλλον όσο και στο περιβάλλον του διαδικτύου.
- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Παραδείγματα αυτής της κατηγορίας αποτελούν οι περιπτώσεις των αδικημάτων που προβλέπονται στα άρθρα 370Β ΠΚ (παράνομη πρόσβαση σε απόρρητα) και 370Γ ΠΚ (η παράνομη αντιγραφή λογισμικού).
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο και η χρήση αυτού αποτελεί το απαραίτητο στοιχείο για την πλήρωση της αντικειμενικής υπόστασης των εγκληματικών πράξεων, ενώ η χρήση του υπολογιστή λειτουργεί συμπληρωματικά καθώς αποτελεί απλά το μέσο τέλεσής τους. Χαρακτηριστικά παραδείγματα της τρίτης κατηγορίας

αποτελούν η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διασπορά κακόβουλου λογισμικού δια του κυβερνοχώρου.

Ωστόσο, σχετικά με την κατηγοριοποίηση των διαφόρων ψηφιακών εγκλημάτων έχουν εκφραστεί και άλλες απόψεις καθώς δεν παρατηρείται ομοφωνία μεταξύ των διαφόρων συγγραφέων που ασχολούνται με τον προσδιορισμό τους. Σύμφωνα λοιπόν, με τον Neil Barrett (1997) τα ηλεκτρονικά εγκλήματα διακρίνονται σε δύο κατηγορίες:

- Σε εκείνα που στρέφονται κατά των Η/Υ και στα οποία περιλαμβάνεται η κλοπή των υλικών μερών ενός Η/Υ, η εισβολή σε ηλεκτρονικά αρχεία και ο ψηφιακός βανδαλισμός καθώς και η διασπορά καταστρεπτικών ιών.
- Σε εκείνα που υποστηρίζονται από Η/Υ και στα οποία περιλαμβάνονται η πορνογραφία, η πειρατεία λογισμικού, οι διάφορες απάτες και το ξέπλυμα μαύρου χρήματος που γίνονται ηλεκτρονικά.

Επίσης κατά την άποψη του Donald Pipkin (2003) τα ηλεκτρονικά εγκλήματα διακρίνονται σε τέσσερις κατηγορίες:

- Τα παραδοσιακά εγκλήματα τα οποία τελούνται με χρήση Η/Υ και ως τέτοια αναφέρει την απάτη, την κλοπή στοιχείων ιδιοκτητών πιστωτικών καρτών και την κλοπή της ηλεκτρονικής ταυτότητας.
- Τα ειδικά εγκλήματα των Η/Υ και σαν τέτοια ο συγγραφέας θεωρεί την επίθεση της άρνησης παροχής υπηρεσιών, την άρνηση πρόσβασης σε πληροφορίες και τη διασπορά καταστρεπτικών ιών.
- Τα αδικήματα που στρέφονται κατά της πνευματικής ιδιοκτησίας όπως είναι η κλοπή πληροφοριών και η εμπορία και καταστροφή πληροφοριών που έχουν κλαπεί.
- Τα εγκλήματα που στρέφονται κατά του προσωπικού απορρήτου, στα οποία εντάσσει τη διακίνηση πορνογραφικού υλικού με ανήλικους που γίνεται μέσω του διαδικτύου.

Ο Σουρής κ.α (2004) διακρίνουν τα ψηφιακά εγκλήματα σε τρεις κατηγορίες. Στην πρώτη κατηγορία εντάσσουν τα εγκλήματα σε υπολογιστή, όπως η μη εξουσιοδοτημένη πρόσβαση, στη δεύτερη εντάσσουν τα εγκλήματα που σχετίζονται

με Η/Υ, όπως η ηλεκτρονική πορνογραφία και η πειρατεία λογισμικού και τέλος, στην τρίτη εντάσσουν τα εγκλήματα που διαπράττονται με τη βοήθεια Η/Υ, όπως η απάτη σε ηλεκτρονικές συναλλαγές, η υποκλοπή στοιχείων πιστωτικών καρτών και η πλαστογράφηση εντύπων.

Ο Τσουραμάνης (2005) εκφράζει την άποψη ότι τα ψηφιακά εγκλήματα, θα πρέπει να ενταχθούν σε δύο μεγάλες κατηγορίες έχοντας ως κριτήριο τα μέσα τέλεσης και εξιχνίασης τους. Δέχεται επομένως ότι στην πρώτη κατηγορία πρέπει να ενταχθούν τα γνήσια ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας. Παραδείγματα αυτής της κατηγορίας αποτελούν σύμφωνα με τον συγγραφέα η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking), η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ, η διασπορά κακόβουλων προγραμμάτων κ.α. Στη δεύτερη κατηγορία δέχεται ότι πρέπει να ενταχθούν τα παραδοσιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, τόσο με την υποστήριξη της ψηφιακής τεχνολογίας όσο και χωρίς τη βοήθειά της. Παραδείγματα αυτής της κατηγορίας αποτελούν τα διάφορα κοινά εγκλήματα, όπως η κλοπή ενός Η/Υ ή τμημάτων του, η απάτη, η εξύβριση, η δυσφήμιση, που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου (e-mail) ή ιστοσελίδων (websites) κ.α., η κατασκοπεία είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική και οι υποκλοπές τηλεφωνικών συνομιλιών που έχουν σαν συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

Μια άλλη ταξινόμηση των ηλεκτρονικών εγκλημάτων προτάθηκε από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα που από την ίδρυση του διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του εγκλήματος μέσω Η/Υ τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Οι κατηγορίες που πρότεινε είναι:

- 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).
- Κλοπή: των δεδομένων, του λογισμικού.
- Χρήση λογισμικού χωρίς άδεια: χρήση παράνομων αντιγράφων λογισμικού.

- Ιδιωτική εργασία: μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος.
- Hacking: ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με την χρήση των δυνατοτήτων της επικοινωνίας.
- Σαμποτάζ: η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό.
- Εισαγωγή: Εισαγωγή πορνογραφικού υλικού, π.χ. πορνογραφικού υλικού μέσω Internet.
- Ιοί: διάχυση ενός προγράμματος με σκοπό την ματαίωση της τρέχουσας εφαρμογής.

Σύμφωνα με τη διεθνή σύμβαση για το κυβερνοέγκλημα του 2001 οι κύριες ψηφιακές παραβάσεις (εγκλήματα) είναι οι ακόλουθες (Council of Europe, 2001)[2]:

- Παράνομη πρόσβαση.
- Παράνομη υποκλοπή.
- Παρεμβολή σε δεδομένα.
- Παρεμβολή σε συστήματα.
- Κακή χρήση συσκευών
- Κλοπή που σχετίζεται με υπολογιστή.
- Απάτη που σχετίζεται με υπολογιστή.
- Παιδική πορνογραφία.
- Κλοπή πνευματικών δικαιωμάτων ηλεκτρονικών πληροφοριών.

Τέλος, κατά την Ανεξάρτητη Αρχή – Συνήγορος του Καταναλωτή (2008)[3] οι μορφές του ηλεκτρονικού εγκλήματος ποικίλουν. Η αντικειμενική υπόσταση του πληρούται με διάφορους τρόπους, ανάλογα με το περιβάλλον στο οποίο εκδηλώνεται και τα τεχνικά μέσα που χρησιμοποιούνται για τη διάπραξή του. Μία συσκευή όπως ο υπολογιστής ή το κινητό τηλέφωνο μπορεί κατά περίπτωση να είναι μέσο διάπραξης ενός αδικήματος (π.χ. πρόσβαση σε παράνομο ρατσιστικό ή πορνογραφικό υλικό, μέσο εξύβρισης, δυσφήμησης, απειλής, εκβίασης, προσβολής απορρήτων, ή

[2] Details of Treaty No.185. Convention on Cybercrime. Διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[3] Συνήγορος του καταναλωτή. Τί πρέπει να γνωρίζουν οι καταναλωτές για την προστασία τους από το ηλεκτρονικό έγκλημα. Διαθέσιμο στο: http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf.

διασποράς ιών) ή να γίνεται η ίδια η συσκευή στόχος της εγκληματικής επίθεσης (αθέμιτη πρόσβαση, υποκλοπή και αλλοίωση δεδομένων, αθέμιτη χρέωση λόγω τηλεπικοινωνιακής απάτης, καταστροφή λειτουργικών προγραμμάτων, παγίδευση ζωτικών λειτουργιών συστημάτων ελεγχομένων από υπολογιστή κλπ).

Το διαπραττόμενο αδίκημα μπορεί να συνίσταται νομικά σε απάτη, πλαστογραφία, παράνομη πρόσβαση, αθέμιτη παγίδευση, αθέμιτη επέμβαση σε σύστημα η δεδομένα, υποκλοπή στοιχείων, παραβίαση κρατικών ή ιδιωτικών απορρήτων. Μπορεί ακόμα να συνιστά αδικήματα σε σχέση με το διακινούμενο επιβλαβές και παράνομο περιεχόμενο (ρατσισμός, τρομοκρατία, παιδική πορνογραφία), προσβολές πνευματικής ή βιομηχανικής ιδιοκτησίας επί έργων και προϊόντων της διανοίας τρίτων κλπ.

1.2.1 Εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών

Στην κατηγορία των εγκλημάτων κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των ηλεκτρονικών υπολογιστών εντάσσονται οι ακόλουθες μορφές ηλεκτρονικού εγκλήματος.

1.2.1.1 Παράνομη πρόσβαση ή εισβολή

Ως παράνομη πρόσβαση χαρακτηρίζεται η εκ προθέσεως και χωρίς εξουσιοδότηση πρόσβαση σε ένα πληροφοριακό σύστημα. Η δραστηριότητα αυτή είναι γνωστότερη ως hacking ή cracking.

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση μέσω διείσδυσης (δηλαδή ηθελημένης παραβίασης των μηχανισμών ελέγχου πρόσβασης) σε υπολογιστικά συστήματα, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η προσωπική ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση των τεχνολογικών γνώσεων και δεξιοτήτων μέσω της εισβολής σε ένα ξένο υπολογιστικό σύστημα[4].

Η έννοια του hacking είναι ευρεία. Μπορεί να αφορά μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν αυξημένες ικανότητες, ορισμένες από τις οποίες μπορούν να χαρακτηριστούν ως παράνομες ή και εγκληματικές. Η

[4] Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα. Διαθέσιμο στο: https://repository.kallipos.gr/bitstream/11419/1037/1/05_chapter_13.pdf.

εισβολή σε ένα τρίτο σύστημα ακόμα και αν δεν είναι κακόβουλη, ενέχει παράνομο χαρακτήρα. Ο επιτιθέμενος, διεισδύοντας σε ένα τρίτο σύστημα αποκτά γνώσεις για το επίπεδο ασφάλειας του, εντοπίζει τα αδύνατα σημεία του και στη συνέχεια μπορεί να διαπράξει κακόβουλη επίθεση ή ακόμα και να δημοσιοποιήσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει αργότερα σε μια ή περισσότερες επιθέσεις.

Ένα πρόσωπο που απολαμβάνει να εξερευνά τις λειτουργίες προγραμμάτων και συστημάτων και να δοκιμάζει τις δυνατότητες τους, σε αντίθεση με τους περισσότερους χρήστες, που προτιμούν να γνωρίζουν τα απολύτως αναγκαία είναι ο hacker (Τσουραμάνης, 2006).

Υπάρχουν, βέβαια, και πολλές άλλες κατηγορίες κακόβουλων χρηστών οι οποίοι έχουν διάφορες ονομασίες στην «αργκό» του Internet: script kiddies, anklebiters, crackers κτλ.

Ενδεικτικά ο Τσουραμάνης (2006) ανέφερε ότι cracker είναι κάποιος που παραβιάζει την ασφάλεια ενός συστήματος. Ο όρος αυτός επινοήθηκε το 1985 από τους hackers προκειμένου να γίνει διαχωρισμός τους από την κακή έννοια του hacker που χρησιμοποιούσαν οι δημοσιογράφοι. Έτσι ενώ οι crackers συχνά αυτοαποκαλούνται hackers, οι πραγματικοί hackers θεωρούν τους crackers ξεχωριστή και υποδεέστερη κατηγορία.

Οι χρήστες αυτοί συνήθως έχουν λίγους υπολογιστικούς πόρους και γνώσεις αλλά τον περισσότερο χρόνο. Επίσης, δεν έχουν και αυτοί κάποιο συγκεκριμένο κίνητρο ή στόχο – είναι απλά η επιθυμία τους να αποδείξουν (τις περισσότερες φορές στους υπόλοιπους) πως είναι ικανοί να παρακάμψουν τα συστήματα ασφάλειας ενός πληροφοριακού συστήματος που τους προτρέπει να προκαλούν ζημιές.

Συνήθως οι χρήστες αυτοί χρησιμοποιούν το Internet για να βρουν τα κατάλληλα εργαλεία και προγράμματα με τα οποία μπορούν και εξαπολύουν διάφορες επιθέσεις. Τα εργαλεία αυτά είναι πλήρως αυτοματοποιημένα, χωρίς να χρειάζεται απολύτως καμία γνώση των πολύπλοκων δικτυακών πρωτοκόλλων και των διαφόρων γλωσσών προγραμματισμού. Αν και γενικά επικρατεί η άποψη ότι τα εργαλεία αυτά είναι πανάκεια και οποιοσδήποτε μπορεί να τα βρει εύκολα και να τα χρησιμοποιήσει κατά βούληση, εμείς θα υποστηρίξουμε πως κάτι τέτοιο δεν είναι

100% αληθές. Τα συγκεκριμένα εργαλεία από μόνα τους δεν μπορούν να προκαλέσουν ζημιές σε ένα σύστημα, μπορούν όμως να γίνουν πραγματικά όπλα (ίσως και μαζικής καταστροφής) αν χρησιμοποιηθούν από άτομα που έχουν τις σχετικές γνώσεις.

Τελευταία κατηγορία παράνομης πρόσβασης ή εισβολής είναι η άρνηση υπηρεσιών (Denial of Sevice (DoS), DoS attack). Μία επίθεση άρνησης υπηρεσιών συνίσταται στον κατακλυσμό ενός δικτύου Η/Υ με τόσο πολλά αιτήματα παροχής υπηρεσιών, ώστε η φυσιολογική ηλεκτρονική κίνηση του δικτύου αυτού να καταστεί εξαιρετικά αργή ή ακόμη και να διακοπεί. Αυτό που χαρακτηρίζει αυτού του είδους την επίθεση είναι η σαφής πρόθεση και επιδίωξη να αποκλειστούν όλοι οι νόμιμοι και φυσιολογικοί χρήστες μίας υπηρεσία δικτύου, από την υπηρεσία αυτή[5].

Πλεονέκτημα του τρόπου αυτού επιθέσεων αποτελεί το γεγονός ότι μπορεί να εκτελεστεί με πολύ περιορισμένα μέσα εναντίον σύγχρονων, τεχνολογικά εξελιγμένων και πολύπλοκων δικτύων και υπολογιστικών συστημάτων και χωρίζεται σε δύο κατηγορίες.

α)Κατανεμημένη άρνηση υπηρεσιών (Distributed denial of service (DDoS), DDoS attack). Στις επιθέσεις που γίνονται με την τεχνική αυτή, ένας μεγάλος αριθμός ηλεκτρονικά μολυσμένων συστημάτων, επιτίθενται εναντίον άλλων Η/Υ, δικτύων ή συστημάτων. Ο επιτιθέμενος χρησιμοποιεί χιλιάδες ή και εκατομμύρια μολυσμένους (με το κατάλληλο λογισμικό) Η/Υ, οι οποίοι συνήθως αναφέρονται ως zombies ή bots και τους ενορχηστρώνει στο να επιτεθούν συγχρόνως σε ένα δίκτυο. Αυτού του είδους οι επιθέσεις είναι δύσκολο να αντιμετωπιστούν διότι τα δεδομένα που κατακλύζουν το δίκτυο – στόχο προέρχονται από πολλούς διαφορετικούς Η/Υ και από πολλές διαφορετικές γεωγραφικές τοποθεσίες (δηλαδή από πολλές διαφορετικές διευθύνσεις internet – IP addresses).

β)Μόνιμη άρνηση υπηρεσιών (Permanent denial of service – PDoS). Μία παραλλαγή της επίθεσης κατανεμημένης άρνησης υπηρεσιών προκαλεί μόνιμα αποτελέσματα στο σύστημα – στόχο και συγκεκριμένα επιφέρει τόσο βαρείες ζημίες ώστε για την επαναφορά του συστήματος απαιτείται πλέον η αντικατάσταση ή η επανεγκατάσταση

[5] Κέντρο διεθνών στρατηγικών αναλύσεων. Κυβερνοχώρος- Κυβερνοεπιθέσεις- Κυβερνοάμυνα. Διαθέσιμο στο: https://kedisa.gr/kybernoxwros-kybernoepitheseis-kybernoamyna-meros-2o-kakoboula-programmata-texnikes-epithesewn/.

τμημάτων του φυσικού εξοπλισμού (hardware) πρόκειται για επιθέσεις PDoS. Οι συνήθεις επιθέσεις DoS ή DDoS αποσκοπούν στην αναστολή των λειτουργιών ή υπηρεσιών ενός δικτύου ή ενός ιστότοπου ή στο να αποκρύψουν την εισαγωγή στο σύστημα κακόβουλου λογισμικού (malware), ενώ οι επιθέσεις PDoS αποτελούν καθαρή προσβολή του υλικού υπόβαθρου των συστημάτων, αλλά με τη χρήση λογισμικού.

1.2.1.2 Αθέμιτη παγίδευση-υποκλοπή

Όπως το ίδιο το όνομα του υπονοεί -παραλλαγή του αγγλικού «fishing» (ψάρεμα)-, το phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα[6].

Το phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam email, το οποίο ισχυρίζεται -ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών.

Τα email αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου σύντομου χρονικού διαστήματος ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να

[6] Νομικά επίλεκτα. Phishing. Διαθέσιμο στο: http://www.nomika-epilekta.gr/arthra/koinonika-arthra/phishing-and-pharming.

πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος.

Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω phishing. Τα email που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικα τους. Το σύστημα Hotmail της Microsoft παρέχει τη διευκόλυνση να μπορεί ο αποδέκτης του email να κάνει έλεγχο (Τσουραμάνης, 2006).

Οι απάτες ψαρέματος μπορεί επίσης να γίνουν και αυτοπροσώπως ή μέσω τηλεφώνου. Στην τελευταία περίπτωση, σε αντίθεση με τα κοινά phishing e-mails, δεν υπάρχει διεύθυνση ή URL για να απαντήσει κανείς, αλλά ένα τηλεφωνικό νούμερο, όπου πρέπει ο παραλήπτης να τηλεφωνήσει και να παράσχει τις ζητούμενες πληροφορίες. Καλώντας το νούμερο αυτό, τους χρήστες καλωσορίζει συνήθως ένα ηχογραφημένο μήνυμα, το οποίο τους καθοδηγεί στην συνέχεια στην παραχώρηση των προσωπικών τους στοιχείων.

1.2.1.3 Επέμβαση σε σύστημα

Οι εκδηλώσεις των κυβερνοεπιθέσεων στο σύστημα γίνονται με δύο μέσα: τον υπολογιστή και τα κακόβουλα προγράμματα. Τα πλέον γνωστά κακόβουλα προγράμματα (κυβερνοόπλα) το κάθε ένα με δικό του τρόπο λειτουργίας, είναι: Trojan Horse, Virus, Worm, Spyware, και Sniffer. Αναλύονται ένα προς ένα παρακάτω[7].

Trojan Horse ή δούρειος ίππος είναι ένα φαινομενικά μη βλαβερό πρόγραμμα, το οποίο, ωστόσο, περιέχει – κατά τρόπο μη εμφανή – κακόβουλο ή επιβλαβή κώδικα λογισμικού και μπορεί να προκαλέσει ζημία ή να εκτελέσει οποιαδήποτε άλλη (κακόβουλη) εργασία για την οποία είναι προορισμένος. Οι χρήστες Η/Υ που λαμβάνουν έναν δούρειο ίππο, παρασύρονται διότι χρησιμοποιούν ένα φαινομενικά αβλαβές πρόγραμμα ή ανοίγουν αρχεία από φαινομενικά «νόμιμη» και γνωστή πηγή προέλευσης. Οι δούρειοι ίπποι μπορούν να προκαλέσουν σοβαρά προβλήματα

[7] What's the Difference Between Viruses, Trojans, Worms, and Other Malware? Διαθέσιμο στο. https://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware.

διαγράφοντας αρχεία ή καταστρέφοντας πληροφορίες. Μπορούν επίσης να δημιουργήσουν ηλεκτρονικές κερκόπορτες στο σύστημα. Σε αντίθεση με τους ιούς και τα ηλεκτρονικά σκουλήκια δεν προσκολλώνται σε αρχεία ή προγράμματα για να τα μολύνουν ούτε αναπαράγουν τους εαυτούς τους.

Ο ιός είναι ένα μικρό πρόγραμμα το οποίο προσκολλά τον εαυτό του σε άλλα προγράμματα ή αρχεία και μεταδίδεται σε δίκτυα, συσκευές αποθήκευσης κ.λπ., φτιάχνοντας αντίγραφα του εαυτού του. Εκτός από αυτό, ένας ιός είναι συνήθως εφοδιασμένος και με ένα εκτελέσιμο κομμάτι λογισμικού το οποίο μπορεί να προγραμματιστεί έτσι ώστε να προκαλέσει κακόβουλα αποτελέσματα, όπως διαγραφές αρχείων, αλλοίωση δεδομένων, διαταραχή λειτουργιών κ.λπ. Σχεδόν όλοι οι ιοί προσαρτώνται σε εκτελέσιμα αρχεία, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει για ένα διάστημα σε κάποιον Η/Υ, χωρίς να είναι ανιχνεύσιμος, μέχρι τη στιγμή που το μολυσμένο εκτελέσιμο αρχείο θα εκτελεστεί (Τσουραμάνης, 2006).

Τα ηλεκτρονικά σκουλήκια (worms) λογισμικού λειτουργούν με τρόπο που μοιάζει με αυτόν των ιών, επειδή μεταδίδονται από υπολογιστή σε υπολογιστή. Σε αντίθεση, όμως, με τους ιούς, τα σκουλήκια λογισμικού έχουν την ικανότητα να ταξιδεύουν χωρίς (έστω και την ακούσια) βοήθεια προσώπων, αυτό επιτυγχάνεται επειδή αυτού του είδους το κακόβουλο λογισμικό εκμεταλλεύεται τα δεδομένα μεταφοράς και κινήσεως των αρχείων εντός του δικτύου. Ωστόσο, ο μεγαλύτερος κίνδυνος που παριστούν τα σκουλήκια συνίσταται στο γεγονός ότι έχουν την ιδιότητα και την ικανότητα να αναπαράγουν τον εαυτό τους εντός του συστήματος. Έτσι ένας μολυσμένος υπολογιστής μπορεί να διαβιβάζει σε άλλους (και κατ' επέκταση σε ολόκληρα δίκτυα ή συστήματα) εκατοντάδες ή και χιλιάδες αντίγραφα ενός ηλεκτρονικού σκουληκιού. Το τελικό αποτέλεσμα στις περισσότερες περιπτώσεις είναι ότι τα ηλεκτρονικά σκουλήκια καταναλώνουν μεγάλα ποσοστά της διαθέσιμης μνήμης ή ακόμη και του εύρους (bandwidth) των γραμμών επικοινωνιών των δικτύων, με συνέπεια μεμονωμένοι υπολογιστές, εξυπηρετητές ιστοσελίδων (web servers) ή και εξυπηρετητές δικτύων (network servers), απλά να μην μπορούν να εκτελέσουν ούτε ένα ποσοστό της φυσιολογικής λειτουργίας τους. Τελευταία έχει παρατηρηθεί και η ύπαρξη σκουληκιών, σχεδιασμένων να εισέρχονται σε δίκτυα Η/Υ και τελικά να επιτρέπουν την εκ του μακρόθεν ανάληψη της λειτουργίας και διαχείρισης των δικτύων αυτών από τρίτους.

Το λογισμικό υποκλοπής spyware είναι λογισμικό που μπορεί να εγκατασταθεί αυτόματα ή να εκτελεστεί στον υπολογιστή χωρίς καμία προειδοποίηση ή έλεγχο και χωρίς τη συγκατάθεσή του χρήστη. Το λογισμικό υποκλοπής spyware μπορεί να μην παρουσιάζει συμπτώματα αφού μολύνει τον υπολογιστή, αλλά πολλοί τύποι λογισμικού κακόβουλης λειτουργίας ή ανεπιθύμητων προγραμμάτων μπορούν να επηρεάσουν τον τρόπο με τον οποίο λειτουργεί ο υπολογιστής. Για παράδειγμα, το πρόγραμμα υποκλοπής μπορεί να παρακολουθεί τη συμπεριφορά του χρήστη στο Web ή να συλλέγει πληροφορίες για εσάς (συμπεριλαμβανομένων πληροφοριών αναγνώρισης ταυτότητας ή ευαίσθητων προσωπικών δεδομένων), να αλλάξει τις ρυθμίσεις του υπολογιστή ή να προκαλέσει μείωση της ταχύτητας λειτουργίας του.

Packet sniffer ή απλώς sniffer, επίσης αποκαλούμενο network monitor ή network analyzer, είναι λογισμικό με δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Όταν γίνει αντιληπτό κάποιο πακέτο το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο. Σε πολλές περιπτώσεις οι μηχανικοί δικτύων, διαχειριστές συστημάτων και επαγγελματίες στον τομέα της ασφάλειας, αλλά και οι hackers κάνουν χρήση ανάλογων εργαλείων (host file hijack). Χρησιμοποιείται νόμιμα από τους πρώτους για καταγραφή και διορθώσεις στην κίνηση (traffic) του δικτύου ενώ από τους δεύτερους για παράνομες δραστηριότητες. Ο σκοπός της παρακολούθησης του δικτύου είναι η «αλίευση» χρήσιμων πληροφοριών που κυκλοφορούν χωρίς κρυπτογράφηση ή με κρυπτογράφηση που μπορεί ο hacker να αποκρυπτογραφήσει.

Τα ανωτέρω κυβερνοόπλα μπορούν να χρησιμοποιηθούν σε διάφορους συνδυασμούς για να υλοποιήσουν μια ποικιλία τεχνικών προσβολής κάποιου στόχου. Η επιλογή της τεχνικής που θα χρησιμοποιηθεί για την προσβολή εξαρτάται από διάφορους παράγοντες, όπως οι δεξιότητες και η εμπειρία του χρήστη, οι δυνατότητες των όπλων, η φύση του στόχου κ.α. (Τσουραμάνης, 2006).

1.2.2 Εγκλήματα σχετιζόμενα με τους ηλεκτρονικούς υπολογιστές

Πρόκειται για τα γνήσια πληροφοριακά εγκλήματα δηλαδή κλασικά ποινικά αδικήματα που τελούνται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών.

1.2.2.1 Πλαστογραφία

Όποιος με πρόθεση και χωρίς δικαίωμα και με σκοπό τη καταδολίευση εισαγάγει, μεταβάλλει, διαγράφει ή αποκρύπτει δεδομένα ηλεκτρονικού υπολογιστή με τρόπον ώστε μη αυθεντικά δεδομένα που δημιουργούνται ως αποτέλεσμα των πιο πάνω παρεμβάσεων να παρουσιάζονται ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά, ανεξάρτητα από το αν τα δεδομένα είναι άμεσα αναγνώσιμα και κατανοητά, διαπράττει αδίκημα που τιμωρείται με φυλάκιση που δεν υπερβαίνει πέντε έτη ή/και με χρηματική ποινή.

Μία από τις σημαντικότερες ποινικές διατάξεις που αφορούν την ακεραιότητα και την ορθότητα της πληροφορίας είναι οι διατάξεις για την πλαστογραφία που εγγυώνται την αυθεντικότητα ενός εγγράφου με την έννοια της εγγύησης του συντάκτη για το περιεχόμενο του εγγράφου. Σε ορισμένες νομοθεσίες απαιτείται υλική ενσωμάτωση του εγγράφου προκειμένου να υφίσταται η προστασία αυτή. Πολλές ευρωπαϊκές νομοθεσίες, μεταξύ των οποίων και η ελληνική, διεύρυναν την έννοια του παραδοσιακού έγγραφου ώστε αυτή να περιλαμβάνει «όλα τα μέσα τα οποία χρησιμοποιούνται από υπολογιστή ή περιφερειακή μνήμη για την με ηλεκτρονικό, μαγνητικό ή κοινό τρόπο εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή πληροφορικών και στοιχείων[8]. Σε αρκετές χώρες μελετάται η εισαγωγή νέας ειδικής νομοθεσίας για την προστασία από την πλαστογραφία νέων μορφών χρήματος όπως το πλαστικό χρήμα ή οι προπληρωμένες κάρτες κλπ.

Χαρακτηριστικές περιπτώσεις πλαστογραφίας με υπολογιστή αποτελούν η κλοπή ταυτότητας, η πειρατεία ονομάτων χώρου (domain name piracy) και η δημιουργία ψεύτικων προφίλ στα μέσα κοινωνικής δικτύωσης (π.χ. facebook).

Κλοπή ταυτότητας δηλαδή η πλαστοποίηση και η χρήση των ψηφιακών στοιχείων ταυτοποίησης άλλους προσώπου, όπως της ψηφιακής υπογραφής, για σκοπό οικονομικού οφέλους μέσω της δημιουργίας νέων τραπεζικών λογαριασμών ή λογαριασμών πιστωτικών καρτών.

Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση

[8] Άρθρο 13 - Ποινικός Κώδικας - Έννοια όρων του Κώδικα. Διαθέσιμο στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-13-poinikos-kodikas-ennoia-oron-toy-kodika.

πελατών και η κατάρτιση των συναλλαγών. Μέσο για την είσοδο στο διαδίκτυο αποτελεί το domain name (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως, επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το domain name αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα domain names και αποτελείται από τα αρκτικόλεξα http://www (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο). Το δεύτερο όμως (second level domain - SLD) ή μεταβλητό πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατεξοχήν όνομα, την κατεξοχήν διαδικτυακή διεύθυνση. Το τρίτο μέρος αποτελεί το επονομαζόμενο top level domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέσης) ή τη γεωγραφική προέλευση (Λάζος, 2001). Το domain name δεν μπορεί καταρχήν να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει ωστόσο να αποδίδεται σε αυτό λειτουργία τόσο διακριτικού τίτλου όσο και σήματος, κατά έμμεσο τρόπο, όταν αυτό χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο, διότι έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσεως οποιασδήποτε ονομασίας, όσο γνωστή και φημισμένη και αν είναι, από τον πρώτο τυχόντα, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση που καθιερώθηκε στις συναλλαγές με την επίμαχη ονομασία. Για τη διαφύλαξη έτσι των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο domain name μια οιονεί λειτουργία διακριτικού τίτλου και σήματος. Τούτο ενισχύεται και από το ότι οι κάτοχοι domain names στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους κατέστησαν γνωστούς στον υλικό κόσμο, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, δεδομένων μάλιστα των περιορισμένων ορίων παροχής domain names για κάθε χρήση αλλά και της επιβαλλόμενης συντομίας γι' αυτού του είδους την επικοινωνία.

1.2.2.2 Απάτη με υπολογιστή

Η συνεχής ανάπτυξη του διαδικτύου ευνόησε την διάπραξη μιας νέας μορφής απάτης, αυτή της απάτης μέσω διαδικτύου ως ειδική περίπτωση οικονομικού εγκλήματος. Συγκεκριμένα, μιλάμε για την πρόθεση και χωρίς δικαίωμα πρόκληση απώλειας περιουσίας σε κάποιον άλλον μέσω α) οποιασδήποτε εισαγωγής, απώλειας, τροποποίησης ή απόκρυψης δεδομένων ηλεκτρονικού υπολογιστή, β) οποιαδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών με σκοπό να επιφέρει οικονομικό όφελος στον εαυτό του ή σε άλλον (Council of Europe, 2005).

Οι κυριότερες μορφές απάτης με υπολογιστή μέσω διαδικτύου είναι απάτη με πιστωτική κάρτα, απάτη με συναλλαγές μέσω ATM ή POS, η Νιγηριανή απάτη, τα πυραμιδικά συστήματα εργασίας, η απάλειψη χρέους και οι ηλεκτρονικές δημοπρασίες. Παρακάτω αναλύονται ορισμένα εξ αυτών.

Στην περίπτωση απάτης με πιστωτική κάρτα, ο απατεώνας προσπαθεί, μέσω των μηνυμάτων που στέλνει, να αποσπάσει από το θύμα του προσωπικά οικονομικά δεδομένα, όπως τα στοιχεία πιστωτικής κάρτας, τραπεζικού λογαριασμού κλπ. Στην αρχή, το υποψήφιο θύμα λαμβάνει ένα e-mail, αποστολές του οποίου φαίνεται να είναι η τράπεζά του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του λογαριασμού του που διακινεί μέσω web. Η σχετική αιτιολογία αναφέρεται σε προβλήματα σε Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δεν γίνει επιβεβαίωση θα κλειδωθεί. Το e-mail αυτό έχει σύνδεσμο προς τον δικτυακό τόπο της τράπεζας, ο οποίος όμως δεν είναι πραγματικός και έτσι, το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα.

Άλλη περίπτωση απάτης με πιστωτική κάρτα είναι οι dialers μια υποκατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, στοιχεία λογαριασμών κλπ.) για τον χρήστη, χωρίς τη γνώση και έγκρισή τους. Σκοπός των δημιουργών προγραμμάτων spyware είναι η προσκόμιση πολλών χρημάτων εύκολα και γρήγορα. Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου, ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου

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 του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου[9].

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντάς τους με τεράστια κέρδη. Ο αποστολέας – απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρείας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος – παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια, το ανυποψίαστο 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 ανταμειφθεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψηφίου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχθεί. Ξεκινάει λοιπόν μια διαδικασία ταχυδρομείου. Το θύμα έχει αρχίσει 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 γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον

[9] Ασφάλεια. Forthnet. Διαθέσιμο στο: http://www.forthnet.gr/Article.aspx?a_id=4393#sthash.iEqIymOH.dpbs.

τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης «419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν[10].

1.2.3 Εγκλήματα σχετιζόμενα με το περιεχόμενο

1.2.3.1 Εγκλήματα σχετικά με την παιδική πορνογραφία

Σύμφωνα με το «Προαιρετικό Πρωτόκολλο της Σύμβασης για τα Δικαιώματα του Παιδιού για την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία» και συγκεκριμένα στο άρθρο 2 «παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες, ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς».

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προϊόντος τους. Οι εγκληματίες διακίνησης πορνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα εκμεταλλευόμενοι την παιδική αθωότητα. Με τη χρήση του διαδικτύου:

- Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη - εγκληματία να αποκρύψει την ταυτότητά του.
- Υπάρχει προσβασιμότητα του επίμαχου υλικού ανά πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος.
- Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο την σεξουαλική κακοποίηση ανηλίκων.
- Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ.) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.

[10] Αστυνομία. Ποιες μορφές διαδικτυακής απάτης συναντώνται συχνότερα; Διαθέσιμο στο: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=3686EN.

Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη «επιχειρηματική» δραστηριότητα. Αποτελεί προϊόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλλουν διόλου ευκαταφρόνητα ποσά. Οι επιπτώσεις σε βάρος των ανηλίκων, μπορούν να ιδωθούν από πολλές οπτικές γωνίες.

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. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους, που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική τους ωρίμανση.

Ο ανήλικος από την πλευρά του, είναι ικανότατος χρήστης των υπολογιστών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου χαρακτήρα του, μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι, μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετάσχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε διαμέσου του ιστού.

Με βάση το άρθρο 348Α του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι[11]:

- Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη, μοντάζ, επεξεργασία εικόνων κλπ.).
- Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού.
- Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη).
- Μεταφορά πορνογραφικού υλικού.
- Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση).

[11] Άρθρο 348Α - Ποινικός Κώδικας - Πορνογραφία ανηλίκων. Διαθέσιμο στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-348a-poinikos-kodikas-pornografia-anilikon.

Έχουμε λοιπόν δυο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο. Από τη μία, τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

1.2.3.2 Εγκλήματα ρατσιστικής και ξενοφοβικής φύσης

Η ελληνική νομοθεσία ενσωμάτωσε το πρωτόκολλο του Στρασβούργου για το διαδικτυακό έγκλημα με το Νόμο 4411/2016[12]. Το "Πρωτόκολλο του Στρασβούργου" το οποίο ενσωματώνει ο νόμος επιχειρεί να βάλει τέλος σε ρατσιστικά, ομοφοβικά και συκοφαντικά σχόλια και αναρτήσεις, στο διαδίκτυο, σε blogs και μέσα κοινωνικής δικτύωσης.

Πάρα πολύς κόσμος και εκτός και εντός διαδικτύου, είναι ανεξέλεγκτος. Υπάρχουν πολλά περιστατικά όπου υπήρξαν άνθρωποι που συκοφαντήθηκαν, λοιδωρήθηκαν έχασαν τη δουλειά τους, επειδή βγήκε μια ομάδα οργανωμένη γνωστών-αγνώστων στο internet και άρχισε να γράφει.

Το πρωτόκολλο αυτό αφορά όλους όσους κάνουν ομοφοβικά σχόλια. Χαρακτηριστικά, δεν μπορείς να αρνηθείς το Ολοκαύτωμα. Γίνεται παράνομη η άρνηση του Ολοκαυτώματος, γίνεται παράνομο το ομοφοβικό σχόλιο, γίνεται παράνομο το ρατσιστικό σχόλιο, γίνεται παράνομη η συκοφαντία.

Με το πρωτόκολλο διευρύνεται το πεδίο εφαρμογής της σύμβασης για το έγκλημα στον κυβερνοχώρο, προκειμένου να αντιμετωπισθούν και ξενοφοβικής και ρατσιστικής φύσης πράξεις, εναρμονίζεται το ισχύον στα συμβαλλόμενα μέρη ουσιαστικό ποινικό δίκαιο, σχετικά με τη διακίνηση, μέσω του Διαδικτύου, υλικού ξενοφοβικής και ρατσιστικής φύσης και παρέχεται σε αυτά η δυνατότητα χρήσης των προβλεπόμενων από τη Σύμβαση για το έγκλημα στον Κυβερνοχώρο δικονομικών μέσων.

Ο ορισμός ρατσιστικό και ξενοφοβικό υλικό περιλαμβάνει κάθε είδους έγγραφο υλικό (κείμενα, βιβλία, περιοδικά, δηλώσεις, μηνύματα) εικόνες (αναπαραστάσεις, φωτογραφίες, σχέδια) και οποιουδήποτε είδους ανάπτυξη ιδεών ή

[12] Τράπεζα Πληροφοριών Νομοθεσίας. Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016. Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html.

θεωριών, ρατσιστικής ή ξενοφοβικής φύσης, με μορφή που να επιτρέπει την αποθήκευση, την επεξεργασία ή τη μετάδοση τους, μέσω συστήματος υπολογιστή.

Η διάταξη του άρθρου 10 της Ευρωπαϊκής Σύμβασης για την προστασία των Δικαιωμάτων του Ανθρώπου, κατοχυρώνει την ελευθερία έκφρασης που περιλαμβάνει τόσο την ελευθερία γνώμης όσο και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών. Σύμφωνα με τη νομολογία του Δικαστηρίου Ανθρωπίνων Δικαιωμάτων η διάταξη αυτή έχει εφαρμογή όχι μόνον στις πληροφορίες ή τις ιδέες, που δεν προξενούν βλάβη σε άλλα άτομα ή που είναι ουδέτερες, αλλά ακόμη και σε εκείνες, που είναι προσβλητικές ή υβριστικές ή προκαλούν ανησυχία στο κράτος ή σε ένα τμήμα του πληθυσμού του[13].

Το Δικαστήριο του Στρασβούργου έχει όμως παραλλήλως δεχθεί, ότι η άσκηση των κατοχυρωμένων από τη διάταξη του άρθρου 10 της ΕΣΔΑ ελευθεριών μπορεί να υπαχθεί σε ορισμένες διατυπώσεις, όρους ή περιορισμούς, εφόσον αυτοί προβλέπονται από το νόμο και αποτελούν αναγκαία μέτρα σε μια δημοκρατική κοινωνία για την προάσπιση της εθνικής ασφαλείας, της εδαφικής ακεραιότητας ή της δημόσιας τάξης και ασφάλειας, την προστασία της ηθικής, της υπόληψης ή των δικαιωμάτων τρίτων κ.λπ. και ότι, εφόσον αποδεικνύεται η συνδρομή των πιο πάνω προϋποθέσεων, οι κρατικές ενέργειες με τις οποίες εισάγονται οι σχετικοί περιορισμοί είναι δυνατόν να θεωρηθούν δικαιολογημένες.

Οι αξιόποινες αυτές πράξεις ρατσιστικής και ξενοφοβικής φύσης πρέπει να τελούνται «χωρίς δικαίωμα» και από πρόθεση. Συνεπώς οι προβλεπόμενοι από τις διατάξεις του πρωτοκόλλου, περιορισμοί στην ελευθερία έκφρασης των ατόμων, σε ό,τι αφορά τη διάδοση ιδεών και πληροφοριών ρατσιστικής και ξενοφοβικής φύσης που βλάπτουν τα δικαιώματα άλλων ατόμων είναι, εν όψει των προεκτεθέντων, συμβατοί τόσο με την ΕΣΔΑ όσο και το Σύνταγμα και εφόσον διαπιστωθεί ότι στη συγκεκριμένη περίπτωση έχουν τηρηθεί οι τασσόμενες από τη νομολογία του Δικαστηρίου του Στρασβούργου προϋποθέσεις, οι σχετικοί περιορισμοί είναι νόμιμοι.

1.2.3.3 Τρομοκρατία μέσω διαδικτύου

Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) ως «την προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών,

[13] Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. Διαθέσιμο στο: http://www.echr.coe.int/Documents/Convention_ELL.pdf.

υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες»[14].

Η χρήση του διαδικτύου παρέχει στους ιδιοκτήτες μια σειρά από πλεονεκτήματα και ειδικότερα:

- Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους.
- Οι ενέργειές τους δύσκολα εντοπίζονται.
- Μπορούν να εξαπολύσουν την επίθεσή τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους.
- Το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί να ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει, διατηρώντας την ανωνυμία του.

Με τη χρήση λοιπόν του διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά Μ.Μ.Ε. και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.

1.2.3.4 Προπαγάνδα-ρητορική μίσους στο διαδίκτυο

Η ρητορική και τα οπτικοακουστικά μέσα του υλικού του μίσους δεν είναι καινούργια. Αυτό που είναι καινούργιο είναι η ευκαιρία που προσφέρει το διαδίκτυο για διαφήμιση του μίσους φτηνά και άμεσα, σε ένα ευρύ κοινό ιδίως στους νέους που είναι οι κύριοι χρήστες του Κυβερνοχώρου.

Ο αριθμός των hate websites αυξάνεται ραγδαία. Κάποιες αντιρατσιστικές οργανώσεις υποστηρίζουν ότι με αυτό τον τρόπο αντανακλάται η αυξανόμενη επιρροή των ρατσιστικών group. Όσον αφορά τους τρόπους αναγνώρισης των hate websites, θα επικαλεστούμε τη λίστα των χαρακτηριστικών του Hatewatch ενός μη κερδοσκοπικού οργανισμού που συνεχώς παρακολουθεί το διαδίκτυο και ειδικότερα τα hate sites[15]. Φυσικά τα κύρια χαρακτηριστικά είναι ότι τα συγκεκριμένα sites ενθαρρύνουν την αναίτια εχθρότητα ή βία εναντίον ενός ανθρώπου ή μαις ομάδας με βάση τη φυλή, το χρώμα, το θρήσκευμα, το φύλο ή την αναπηρία. Σύμφωνα με την

[14] FBI. Cyber Terrorism and Cyber Crimes .Διαθέσιμο στο: https://www.fbi.gov/audio-repository/news-podcasts-inside-cyber-terrorism-and-cyber-crimes.mp3/view.
[15] Πανεπιστήμιο Πειραιώς. Η επίδραση του διαδικτύου στα κοινωνικά κινήματα. Διαθέσιμο στο: http://voidnetwork.gr/wp-content/uploads/2016/09/.

ανωτέρω λίστα ειδικότερα κάποια από τα στοιχεία που έχουν εξακριβωθεί είναι τα εξής:

- Να έχει διεύθυνση ώστε να μπορεί ο κόσμος να ζητήσει συγκεκριμένες πληροφορίες.
- Να έχει τηλεφωνικό αριθμό.
- Να χρησιμοποιεί καταγεγραμμένο domain name και όχι μια σελίδα που παρέχεται δωρεάν.
- Η σχέση του site με ένα μεγαλύτερο group στην πραγματική ζωή.
- Να έχει λίστα με τρέχοντα event ή δραστηριότητες κάποιων γνωστών hate group.
- Να έχει πρωτότυπο περιεχόμενο, το οποίο να έχει δημιουργηθεί ειδικά για το συγκεκριμένο site.
- Να παρουσιάζει συχνή ανανέωση.
- Να συλλέγονται πόροι ή να πραγματοποιείται διαφήμιση μέσω του site.
- Η ενθάρρυνση πράξεων βίας ή παρενόχλησης από μεμονωμένα άτομα που προφανώς ασπάζονται τις ιδέες του site.
    - Η δημοσίευση φωτογραφιών ή ιδιωτικών πληροφοριών στον ιδιοκτήτη του site.
    - Η αναπτυγμένη χρήση της τεχνολογίας όπως βίντεο, διαδικτυακό ραδιόφωνο
    - Η ύπαρξη forum ή γραμμής ειδήσεων.
    - Το site έχει υπερσυνδέσμους σε άλλα διαδικτυακά hate groups ή μεμονωμένα ρατσιστικά άτομα.

Σε Ευρωπαϊκό Επίπεδο κύριος στόχος των δράσεων της Ευρωπαϊκής Ένωσης είναι να προάγουν την ασφαλή χρήση του διαδικτύου και να δημιουργήσουν ένα ευνοϊκό περιβάλλον για την υγιή ανάπτυξη της βιομηχανίας του internet σε πανευρωπαϊκό επίπεδο. Η στόχευση κατευθύνεται στο να εμποδιστεί η χρήση του internet από το να διαπράττονται προσβολές έναντι παιδιών ή να διαδίδονται ιδεολογίες ρατσιστικών διακρίσεων, μίσους ή ξενοφοβίας. Στον άξονα αυτό κινήθηκε και η υπογραφή του Πρόσθετου πρωτοκόλλου στη σύμβαση για το έγκλημα στον κυβερνοχώρο, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων πληροφορικής καθώς και πολλές

αποφάσεις της Ευρωπαϊκής Επιτροπής, που προβλέπουν ότι τα κράτη – μέλη οφείλουν να λάβουν τα αναγκαία μέτρα για τον ποινικό κολασμό πράξεων ρατσισμού και ξενοφοβίας[16].

1.2.3.5 Παρενοχλήσεις ή κυβερνοεκφοβισμός

Ο Διαδικτυακός εκφοβισμός ή κυβερνοεκφοβισμός (Cyberbullying) αποτελεί εξέλιξη του παραδοσιακού εκφοβισμού σε τεχνολογικό επίπεδο, και αφορά «οποιαδήποτε πράξη εκφοβισμού, ψυχολογικής κακοποίησης, επιθετικότητας, απειλής, ταπείνωσης, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς παιδιών, προ εφήβων και εφήβων που πραγματοποιείται μέσω του Διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους και η οποία επαναλαμβάνεται σε βάθος χρόνου ανά τακτά ή άτακτα χρονικά διαστήματα» Ο όρος πρωτοεμφανίστηκε από τον Καναδό παιδαγωγό Bill Belsey (2004)[17] και εντάσσεται, στις συμπεριφορές προληπτικής επιθετικότητας, οι οποίες και δύναται να διεξάγονται από άτομο ή ομάδα ατόμων με απώτερο στόχο την πρόκληση συναισθηματικής ή/και σωματικής βλάβης στο εκάστοτε θύμα.

Ο κυβερνοεκφοβισμός, όπως προαναφέρθηκε, αποτελεί τη συνέχεια του παραδοσιακού εκφοβισμού, με συγκεκριμένες διαφοροποιήσεις οι οποίες και εστιάζονται στα ακόλουθα σημεία:

- Δυνατότητα άμεσης και ταυτόχρονης θυματοποίηση των χρηστών του διαδικτύου μέσα στο προσωπικό τους χώρο, σε παγκόσμιο επίπεδο, με χαμηλό κόστος και εικοσιτετράωρη πρόσβαση από πλευράς θυτών
- Παροχή «ανωνυμίας» από πλευράς διαδικτύου, η οποία και δημιουργεί μια αίσθηση ελευθερίας και ασφάλειας. Ο εκάστοτε θύτης κρυμμένος πίσω από μια ψεύτικη ταυτότητα, μπορεί να διαπράξει την εν λόγω εγκληματική συμπεριφορά, παραμένοντας αόρατος και αφήνοντας ελάχιστα ή και καθόλου ψηφιακά ίχνη με αποτέλεσμα όχι μόνο να γίνεται πιο δύσκολος ο εντοπισμός τους από πλευράς διωκτικών αρχών, αλλά και να αίρονται οι όποιες αρχικές αναστολές τέλεσης του εγκλήματος.

[16]Η Κομισιόν εξετάζει το νομικό πλαίσιο για την πάταξη της ρητορικής μίσους στο διαδίκτυο. Διαθέσιμο στο: http://www.huffingtonpost.gr/2017/04/23/diethnes-tech-media-h-komision-eksetazei-to-nomiko-plaisio-gia-thn-pataksi-ths-ritorikis-misous-sto-diadiktyo_n_16186190.html.

[17] Belsey, B., 2004. Cyberbullying: An Emerging Threat to the "Always On" Generation. Διαθέσιμο στο: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.

- Η έλλειψη προσωπικής επικοινωνίας θύτη-θύματος, η οποία και έχει ως απότοκο τη μη άμεση ενσυναίσθηση των συνεπειών της εκάστοτε επίθεσης από πλευράς θύτη.
- Η ύπαρξη ενός μεγάλου αριθμού ακούσιων ή εκούσιων μαρτύρων (bystanders), οι οποίοι και χωρίζονται σε δυο κύριες κατηγορίες, οι επιβλαβείς για το θύμα, οι οποίοι και μέσω της συμπεριφοράς τους είτε επικροτούν την εγκληματική συμπεριφορά είτε παραμένουν αδιάφοροι και οι βοηθοί παρατηρητές οι οποίοι μέσω της άμεσης αντίδρασής τους κινητοποιούν περισσότερα άτομα για την καταπολέμηση του φαινομένου.
- Η ίδια η φύση του διαδικτύου η οποία και καταρρίπτει την ανάγκη της επαναληψιμότητας, μιας και όποια βίντεο ή αναρτήσεις (σε ένα blog, στο YouTube, στο Facebook και σε άλλα μέσα κοινωνικής δικτύωσης) είναι συνέχεια διαθέσιμα και ορατά από απεριόριστο αριθμό ατόμων οπουδήποτε και οποτεδήποτε, αυξάνοντας έτσι με ευκολία τον αντίκτυπο στο θύμα.
- Η μη ανάγκη ύπαρξης δυσανάλογης δύναμης μεταξύ θύτη και θύματος, μιας και μέσω των ηλεκτρονικών μέσων ακόμη και ένα άτομο χωρίς ιδιαίτερες σωματικές ικανότητες μπορεί να γίνει θύτης σε απεριόριστο αριθμό ατόμων.

Ο ηλεκτρονικός εκφοβισμός μπορεί να λάβει χώρα μέσω του διαδικτύου, του ηλεκτρονικού ταχυδρομείου, δωματίων συνομιλίας (Chat Rooms), σελίδων κοινωνικής δικτύωσης (social networking sites), των ιστολογιών (blogs), μέσω άλλων ιστοσελίδων σχετικών με ηλεκτρονικά παιχνίδια ή υπηρεσιών άμεσης ανταλλαγής μηνυμάτων καθώς και μέσω κινητών τηλεφώνων (Βαφόπουλος, 2012). Πιο συγκεκριμένα, οι μορφές που μπορεί να πάρει μπορούν, βάσει του Willard (2007), να κατηγοριοποιηθούν σε 13 σημεία, τα οποία και εμπίπτουν σε μια από τις 3 μεγάλες κατηγορίες τις δυσφήμισης, της παρενόχλησης και της εξαπάτησης:

1. Flaming (Στην πυρά) – Ηλεκτρονικές αντιπαλότητες μέσω e-mails με σκληρή και χυδαία γλώσσα.
2. Online harassment (Διαδικτυακή παρενόχληση) – Επανειλημμένη αποστολή προσβλητικών μηνυμάτων.
3. Cyberstalking (Καταδίωξη) – Διαδικτυακή παρενόχληση μέσω απειλών πρόκλησης βλάβης ή υπερβολικό εκφοβισμό.

4. Cyberthreats (Απειλές) – Γενικές δηλώσεις μίσους, οι οποίες συνήθως καθιστούν το συντάκτη της δήλωσης συναισθηματικά αναστατωμένο με ενδεχόμενο είτε να βλάψει τον εαυτό του είτε να αυτοκτονήσει.
5. Denigration (Δυσφήμιση) – Αποστολή προς άλλα άτομα επιβλαβών, αναληθών ή σκληρών δηλώσεων σχετικά με ένα πρόσωπο ή δημοσίευση τέτοιου υλικού στο διαδίκτυο με σκοπό τη βλάβη.
6. Impersonation (Μίμηση) – Υιοθέτηση άλλης ταυτότητας και αποστολή επιβλαβούς υλικού με σκοπό τη βλάβη.
7. Outing (Δημοσιοποίηση προσωπικών στοιχείων) – Αποστολή ή δημοσίευση προσωπικών στοιχείων σχετικά με ένα πρόσωπο που περιέχει ευαίσθητες προσωπικές ή ενοχλητικές πληροφορίες, συμπεριλαμβανομένης της προώθησης προσωπικών μηνυμάτων ή εικόνων.
8. Trickery (Εξαπάτηση/Εμπαιγμός) – Ξεγέλασμα του θύματος με απότοκο την αποκάλυψη μυστικών και ενοχλητικών πληροφοριών για να τα μοιραστεί και ο ίδιος διαδικτυακά.
9. Exclusion (Εξοστρακισμός) – Ωμή και σκληρή εξαίρεση ή/και αποβολή κάποιου από ηλεκτρονική ομάδα στο διαδίκτυο.
10. Bash boards (τελειωτικό χτύπημα) – Διαδικτυακοί πίνακες ανακοινώσεων με πρόστυχες και κακόβουλες δημοσιοποιήσεις μίσους.
11. Happy slapping (Χαρωπό χαστούκισμα) – Προσωπική επίθεση σε ανυποψίαστο θύμα, η οποία και βιντεοσκοπείται ή φωτογραφίζεται και μετά το εν λόγω διανέμεται ηλεκτρονικά (ως φάρσα).
12. Text Wars/Attacks (Πόλεμοι κειμένου) – Δημιουργία «συμμορίας» με στοχευμένη αποστολή εκατοντάδων επιβλαβών μηνυμάτων με απότοκο τη συναισθηματική καταπόνηση.
13. Online polls (Διαδικτυακές δημοσκοπήσεις) – Ψήφισμα επί επιβλαβών και υποτιμητικών θεμάτων από τους αναγνώστες της εκάστοτε σελίδας.

Οι θύτες συνήθως παραπέμπουν σε άτομα που υφίστανται και τα ίδια σωματική ή λεκτική βία στο ενδοοικογενειακό περιβάλλον, ή ζουν σε εξαιρετικά πειθαρχημένα περιβάλλοντα. Μπορεί να είναι κυρίαρχες, και ιδιαίτερα δημοφιλείς προσωπικότητες με μεγάλη αυτοπεποίθηση και ιδιαίτερα θετική άποψη για τον εαυτό τους, που συνήθως δυσκολεύονται να ακολουθήσουν κανόνες, ενώ συνήθως παρουσιάζουν και άλλες αντικοινωνικές συμπεριφορές όπως ροπή σε μικροκλοπές,

κατανάλωση αλκοόλ κάπνισμα, προβλήματα αυτοελέγχου, πρόκληση υλικών ζημιών. Τα θύματα από την άλλη πλευρά είναι άτομα ευαίσθητα και εσωστρεφή, ιδιαιτέρως ευάλωτα και ανασφαλή, με χαμηλή αυτοπεποίθηση και δημοφιλία, ενώ δεν εμφανίζουν επιθετική ή προκλητική συμπεριφορά. Συνήθως η σωματική τους αδυναμία και κάποια ιδιαίτερα χαρακτηριστικά τους (παχυσαρκία, τραυλισμός, σεξουαλικές προτιμήσεις, κάποιου είδους αναπηρία) αποτελούν στοιχεία προσέλκυσης εκφοβιστικών επιθέσεων (Γρηγοράκης et al., 2014).

Κύριες αιτίες που μπορεί να οδηγήσουν ένα νέο άτομο να εκτεθεί σε συμπεριφορές διαδικτυακού εκφοβισμού (είτε ως θύμα είτε ως θύτης) είναι η βίωση έντονων συναισθημάτων όπως η συναισθηματική πλήξη, ο θυμός, η απόγνωση, η μοναξιά, η ανάγκη για προσοχή, η ανάγκη επιβολής δύναμης ακόμη και η αντεκδίκηση λόγω πρότερης δικής του θυματοποίησης από άλλο άτομο. Τόσο οι προβληματικές σχέσεις στο οικογενειακό περιβάλλον όσο και μια ευρύτερη κοινωνική δυσλειτουργικότητα του ατόμου σε φιλικό ή/και σχολικό/επαγγελματικό επίπεδο αποτελούν υπόστρωμα πυροδότησης τέτοιων αντικοινωνικών συμπεριφορών. Λιγότερο συχνά μα εξίσου σημαντικό κίνητρο μπορεί να είναι η ευχαρίστηση πρόκλησης πόνου από ένα άτομο σε ένα άλλο με σκοπό απλά την ψυχαγωγία του θύτη[18].

Μια σειρά από επιστημονικές μελέτες παρουσιάζουν στατιστικά ευρήματα τα οποία και υπογραμμίζουν τη σημαντική κατά τα τελευταία χρόνια αύξηση του φαινομένου ειδικότερα μετά την άνοδο των μέσων κοινωνικής δικτύωσης (Facebook, Twitter, YouTube, blog, κτλ.). Ο εκφοβισμός και η παρενόχληση στον κυβερνοχώρο αποτελούν τμήμα της καθημερινότητας παιδιών και εφήβων, με τα δύο φύλα να συμμετέχουν εξίσου αλλά με διαφορετικούς τρόπους εκδήλωσης της επιθετικότητας. Αναφορικά με τη σχέση του διαδικτυακού εκφοβισμού με την ηλικία, η εν λόγω περιγράφεται άριστα με το σχήμα ανεστραμμένου U, μιας και μελέτες έχουν δείξει ότι αυξάνει όταν το άτομο εισέρχεται την εφηβεία, κορυφώνεται στα μέσα αυτής και μετά ακολουθεί φθίνουσα πορεία (Βαφόπουλος, 2012).

[18] Stopbullying.gov, 2017. What is Cyberbylllying. Διαθέσιμο στο: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html.

1.2.4 Εγκλήματα σχετικά με τα πνευματικά δικαιώματα

Η ψηφιοποίηση και η επιγραμμική διάθεση των πολιτιστικών αγαθών διαχωρίζει το περιεχόμενο, μεταφρασμένο σε δυαδική πληροφορία, από το συγκεκριμένο υλικό μέσο. Σαν αποτέλεσμα το πολιτιστικό αγαθό γίνεται πολλαπλασιασμό με μηδενικό κόστος. Ο χαρακτήρας του γίνεται μη-συναγωνιστικός και μη-αποκλειστικός, δηλαδή η χρήση του αγαθού από ένα άτομο δεν επηρεάζει τη χρήση του από άλλα άτομα ούτε μειώνει την ποσότητα του διαθέσιμου αγαθού.

Κατά συνέπεια, η διαθεσιμότητα των αγαθών αυτών δεν επηρεάζεται από τον αριθμό των ατόμων που τα χρησιμοποιούν/καταναλώνουν. Ο συνδυασμός ψηφιοποίησης και επιγραμμικής διανομής πολιτιστικών αγαθών αναιρεί επίσης το πρόβλημα της απόστασης και του χώρου. Η διαδικτυακή προσφορά πολιτιστικών αγαθών δεν περιορίζεται ούτε από την φυσική απόσταση, αφού καθένας μπορεί να επισκεφτεί οποιοδήποτε ιστότοπο από οποιοδήποτε σημείο, ούτε από τον διαθέσιμο αποθηκευτικό χώρο.

Σε ένα δωμάτιο με λίγες δεκάδες ηλεκτρονικούς υπολογιστές μπορούν αποθηκευτούν εκατοντάδες χιλιάδες διαφορετικά βιβλία ή ταινίες. Κατά συνέπεια η ψηφιοποίηση και η επιγραμμική διάθεση αναιρούν την βασική αρχή της σπανιότητας στην οποία στηρίζεται η πολιτιστική βιομηχανία σε ότι αφορά το κομμάτι της αποθήκευσης και της διανομής. Στο διαδίκτυο δεν υπάρχει σπανιότητα πολιτιστικών αγαθών όπως στον φυσικό κόσμο αλλά πληθώρα. Το πρόβλημα είναι λιγότερο το αν μια πληροφορία υπάρχει στο διαδίκτυο αλλά το που ακριβώς βρίσκεται.

Η προστιθέμενη αξία μετακινείται σταδιακά από τους παραγωγούς και τους παραδοσιακούς διανομείς της πληροφορίας όπως η πολιτιστική βιομηχανία και τα ΜΜΕ στους πληροφοριακούς ενδιάμεσους όπως οι μηχανές αναζήτησης και τα κοινωνικά δίκτυα όπως το Facebook, η Google και το The Pirate Bay. Αυτό γίνεται σαφές αν παρατηρήσει κανείς τα οικονομικά μεγέθη αυτών των παικτών στο διαδίκτυο και τα συγκρίνει με αυτά της πολιτιστικής βιομηχανίας (Καλογήρου, 2015). Ταυτόχρονα η ευκολία αντιγραφής και διαμοιρασμού των ψηφιακών αρχείων καθιστά την δυνατότητα αποκλεισμού ενός μέρους του κοινού από αυτά πολύ δύσκολη. Ενώ ο ιδιοκτήτης της πνευματικής ιδιοκτησίας μπορεί να εμποδίσει κάποιον που αρνείται να πληρώσει για ένα βιβλίο να το πάρει στην κατοχή του, ελέγχοντας το δίκτυο διανομής και βάζοντας ας πούμε σεκιούριτι στην πόρτα του

βιβλιοπωλείου, αδυνατεί να εμποδίσει την αντιγραφή και τη διανομή ενός αρχείου όταν αυτή γίνεται με χαμηλό ή μηδενικό κόστος.

Άμεση συνέπεια της ψηφιοποίησης είναι λοιπόν η διάχυση των πολιτισμικών περιεχομένων στο διαδίκτυο σήμερα με τρόπο πολύ πιο αποτελεσματικό και μαζικό από οποιαδήποτε άλλη ιστορική συγκυρία. Από τη μία η εξέλιξη αυτή αποσταθεροποιεί τα οικονομικά μοντέλα της πολιτιστικής βιομηχανίας. Από την άλλη όμως επιτρέπει μια άνευ προηγουμένου δημιουργικότητα για εκατομμύρια απλούς χρήστες σε όλο τον πλανήτη.

Τα μέτρα κατά της ανταλλαγής περιεχομένου στο διαδίκτυο που υποστηρίζει η πολιτιστική βιομηχανία έχουν σαν στόχο την τεχνητή επιβολή στο ψηφιακό περιβάλλον των περιορισμών που ισχύουν στη παραγωγή και διανομή υλικών πολιτιστικών προϊόντων. Με άλλα λόγια, στόχος της βιομηχανίας είναι η επαναφορά του συναγωνιστικού χαρακτήρα στα ψηφιακά προϊόντα ούτως ώστε η αγορά να επανέλθει στην προηγούμενη κατάσταση. Αυτό μπορεί να επιτευχθεί με τους εξής τρεις τρόπους. Με καταστολή των χρηστών που διαμοιράζουν προστατευόμενο περιεχόμενο (πρόστιμο, φυλάκιση, διακοπή σύνδεσης κλπ), με φιλτράρισμα του διαδικτύου (traffic shaping, αποκλεισμός ιστότοπων και υπηρεσιών) και με επιβολή Περιορισμών Ψηφιακής Διαχείρισης (DRM) δηλαδή τεχνολογιών υπαγωγής των χρηστών στον έλεγχο κάποιου τρίτου, ο οποίος παρέχει περιεχόμενο. Το ζήτημα είναι κατά πόσο το ισοζύγιο αυτών των μέτρων μεταξύ προσδοκώμενων αποτελεσμάτων και ανεπιθύμητων παρενεργειών είναι θετικό ή αρνητικό (Καλογήρου, 2015).

Σε γενικές γραμμές οι αρνητικές συνέπειες των παραπάνω μέτρων είναι δυσανάλογες για το δημόσιο συμφέρον, και για τις ατομικές ελευθερίες.

1.2.4.1 Πειρατεία λογισμικού

Πειρατεία λογισμικού είναι η κλοπή προγραμμάτων λογισμικού με την παράνομη αντιγραφή ή πλαστογράφηση γνήσιων προϊόντων και την διανομή πλαστών και παράνομα αντεγραμμένων προϊόντων. Με απλά λόγια, πειρατεία μπορεί να χαρακτηριστεί τόσο η μη συστηματική αντιγραφή προϊόντων χωρίς νόμιμη άδεια χρήσης από ιδιώτες ή επιχειρήσεις, όσο και διανομή ή μεταπώληση προϊόντων λογισμικού χωρίς την νόμιμη άδεια χρήσης.

Σχεδόν οι μισοί από τους χρήστες ηλεκτρονικών υπολογιστών (Η/Υ) παγκοσμίως (47%) αποκτούν το λογισμικό τους με παράνομο τρόπο, σε μόνιμη ή τακτική βάση. Στις αναπτυσσόμενες χώρες δε τα νούμερα είναι πολύ υψηλότερα, σύμφωνα με την πιο ενδελεχή έρευνα, που έχει πραγματοποιηθεί σε χρήστες Η/Υ, σχετικά με τη συμπεριφορά και τη στάση τους απέναντι στην πειρατεία λογισμικού και τα δικαιώματα πνευματικής ιδιοκτησίας.

Η πλειοψηφία των χρηστών Η/Υ στον αναπτυσσόμενο κόσμο αποκτούν συστηματικά το λογισμικό τους με παράνομα μέσα, όπως είναι η αγορά μίας άδειας χρήσης για ένα πρόγραμμα λογισμικού και η μετέπειτα εγκατάσταση του σε πολλαπλούς υπολογιστές ή το κατέβασμα (download) προγραμμάτων από δίκτυα ανταλλαγής (peer to peer), εκφράζοντας, ωστόσο, την υποστήριξή τους στις αξίες των δικαιωμάτων πνευματικής ιδιοκτησίας[19].

Αξίζει επίσης να αναφερθεί ότι σε παγκόσμιο επίπεδο, οι λαμβάνοντες τις επιχειρηματικές αποφάσεις παρουσιάζουν συμπεριφορές και εκφράζουν απόψεις, που συμπίπτουν με εκείνες άλλων χρηστών Η/Υ. Για να μειωθεί η πειρατεία λογισμικού, πρέπει να εκπαιδευτούν οι επιχειρήσεις και οι μεμονωμένοι χρήστες, σχετικά με το τι συνιστά νόμιμη απόκτηση και χρήση λογισμικού, καθώς και να εφαρμοστούν οι νόμοι περί πνευματικής ιδιοκτησίας, αποστέλλοντας, έτσι, ένα ξεκάθαρο και αποτρεπτικό μήνυμα στην αγορά.

Παρότι η πειρατεία λογισμικού είναι αρκετά διαδεδομένη και στη χώρα μας κάτι τέτοιο δε θα μπορούσαμε να το ισχυριστούμε και για τις κλοπές hardware λόγω της ενδεχόμενες άγνοιας των πιθανών παραβατών για την πραγματική τους αξία (Τσουραμάνης, 1996).

[19] Παγκόσμια μελέτη λογισμικού 2016 της BSA. Διαθέσιμο στο: http://www.bsa.org/?sc_lang=el-GR.

ΚΕΦΑΛΑΙΟ 2: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ & ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ Ή ΠΡΟΣΤΑΣΙΑΣ

2.1 Ασφάλεια πληροφοριακών συστημάτων έννοια και αρχές

Η ασφάλεια πληροφοριακών συστημάτων μελετήθηκε για πρώτη φορά στις αρχές της δεκαετίας του 1970. Η πρώτη σχετική δημοσίευση εξέτασε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως μέσω τερματικών, από την ομάδα εργασίας του συμβουλίου αμυντικής επιστήμης του υπουργείου άμυνας των Ηνωμένων Πολιτειών (Τσουραμάνης, 2006). Προηγουμένως, η πρόσβαση στους υπολογιστικούς πόρους προϋπέθετε την φυσική παρουσία και πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή. Η προσέγγιση στην λύση των προβλημάτων ασφάλειας μέχρι τότε βασιζόταν στην φυσική απομόνωση και προστασία του κεντρικού υπολογιστή, καθώς και στον έλεγχο πρόσβασης σε αυτόν.

Ένα από τα συμπεράσματα στην αναφορά της ομάδας εργασίας, ήταν ότι ο χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικό πρόσβασης, μια πρόταση που ποτέ δεν υιοθετήθηκε ευρέως. Άλλες καινοτόμες ιδέες που εκφράστηκαν στην ανάλυση είχαν μεγαλύτερη απήχηση, όπως για παράδειγμα αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει θεμέλιος λίθος στη δημιουργία πολιτικών ασφάλειας[20].

Η ασφάλεια πληροφοριακών συστημάτων συνδέεται με τεχνικές, διαδικασίες, διοικητικά μέτρα και με ηθικές - κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή, τυχαία ή σκόπιμη. Ως βάση μπορεί να οριστεί ο εντοπισμός, η αξιολόγηση και η διαμόρφωση ενός θεωρητικού πλαισίου για το σχεδιασμό πολιτικών ασφάλειας. Το σημαντικότερο σημείο στη διαδικασία σχεδιασμού ασφαλών πολιτικών, είναι ο εντοπισμός και χαρακτηρισμός των πληροφοριών που θα χρησιμοποιηθούν και θα προστατευθούν, ως εμπιστευτικές.

[20] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l33193&from=EL.

Ο στόχος ενός συστήματος πολιτικής ασφάλειας είναι να περιοριστεί η επικινδυνότητα σε αποδεκτό επίπεδο. Το σύστημα περιλαμβάνει αξιολόγηση της επικινδυνότητας και περιορισμό του αποδεκτού επιπέδου ασφαλείας, ανάπτυξη και εφαρμογή μιας πολιτικής ασφαλείας, καθώς και δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της πολιτικής ασφάλειας. Η πολιτική ασφάλεια μαζί με το σύνολο των μέτρων προστασίας αποτελούν το σχέδιο ασφαλείας για τα πληροφοριακά συστήματα. Ο καθορισμός της πολιτικής ασφάλειας του πληροφοριακού συστήματος θα πρέπει να καλύπτεται από: ζητήματα προσωπικού, φυσική ασφάλεια, έλεγχο πρόσβασης στο πληροφοριακό σύστημα, διαχείριση υλικών και λογισμικών, νομικές υποχρεώσεις, διαχείριση της πολιτικής ασφάλειας, οργανωτική δομή και σχέδιο συνέχισης λειτουργίας.

Μείζονος σημασίας είναι και η θεμελίωση της ασφάλειας του πληροφοριακού συστήματος για τα μέλη του οργανισμού, δηλαδή η δημιουργία κουλτούρας ασφαλείας, καθώς πολλές φορές αποτελεί νομική υποχρέωση και αποτελεί παράγοντα εμπιστοσύνης μεταξύ οργανισμού και πελατών. Τα είδη των πολιτικών ασφαλείας είναι: τα τεχνικά και λειτουργικά συστήματα πληροφοριών, τα δίκτυα υπολογιστών, τα οργανωτικά και τα ατομικά συστήματα. Οι απαιτήσεις για την ασφάλεια του πληροφοριακού συστήματος πρέπει να ικανοποιούνται από την πολιτική ασφάλεια[21]. Προέρχονται από όλους τους εμπλεκόμενους στη χρήση και στη λειτουργία του πληροφοριακού συστήματος ενός οργανισμού, δηλαδή από τους χρήστες και τους διαχειριστές του πληροφοριακού συστήματος, τη διοίκηση του οργανισμού, τους πελάτες του οργανισμού, τις νομικές και κανονιστικές διατάξεις που διέπουν την λειτουργία τους.

Με την εφαρμογή πολιτικής ασφαλείας επιδιώκουμε τα εξής: οι οδηγίες και τα μέτρα προστασίας οφείλουν να καλύπτουν το σύνολο των αγαθών και όλες τις λειτουργίες, να ληφθούν υπόψη οι τρέχουσες τεχνολογικές εξελίξεις και να μπορεί η πολιτική να καλύπτει μικρές αλλαγές στο πληροφοριακό σύστημα. Επιπλέον, πρέπει να υπάρχει σαφήνεια και εύκολη κατανόηση, τεχνολογική ανεξαρτησία και καταλληλότητα ανάλογα με τον οργανισμό που απευθύνεται. Για να είναι επιτυχές

[21] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l33193&from=EL.

ένα σύστημα πολιτικής ασφάλειας, πρέπει να υποστηρίζει τους επιχειρηματικούς στόχους, να συμμετέχει η διοίκηση, να είναι κατάλληλο για το περιβάλλον που εφαρμόζεται, οι χρήστες να εκπαιδεύονται κατάλληλα, να υπάρχει αξιολόγηση με εύκολη και άμεση πρόσβαση για όλους τους χρήστες του πληροφοριακού συστήματος και το περιεχόμενο και οι εφαρμογές πρέπει να ανανεώνονται τακτικά.

Οι πολιτικές ασφάλειας προϋποθέτουν την ύπαρξη μίας δέσμης βασικών αρχών, εκφρασμένων με σαφήνεια, η οποία να περιλαμβάνει τους σχεδιαστικούς στόχους των λειτουργικών συστημάτων. Κάθε αντικείμενο του συστήματος θα πρέπει να μπορεί να αναγνωρισθεί μονοσήμαντα και να συνοδεύεται από μία ένδειξη του βαθμού εμπιστευτικότητας. Επιπρόσθετα, η ισχύς των ασφαλιστικών μηχανισμών δεν θα πρέπει να βασίζεται στην άγνοια των χρηστών, σχετικά με τις τεχνικές ασφαλείας που χρησιμοποιούνται, αλλά στην αποτελεσματική τους σχεδίαση. Η ασφάλεια λοιπόν των πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες, την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα (Mcclure et al., 2009).

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Αφορά λοιπόν στην απόλυτη διατήρηση δεδομένων ενός πληροφοριακού συστήματος, χωρίς καμιά μεταβολή, αλλοίωση, ή μεταποίησή τους από μη εξουσιοδοτημένα προς το σύστημα άτομα.

Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι είτε προσωρινά, είτε μόνιμα (Τσουραμάνης, 2006).

Τέλος, η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Δηλαδή η προσπέλαση ευαίσθητων πληροφοριών και δεδομένων γίνεται μόνο από εξουσιοδοτημένα πρόσωπα ή οντότητες.

2.2 Μέτρα ασφαλείας

Τα μέτρα ασφαλείας, ή μέτρα προστασίας, ή αντίμετρα συμπληρώνουν την πολιτική ασφαλείας. Αφορούν όλες τις διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος. Τα μέτρα ασφαλείας χωρίζονται σε τέσσερις μεγάλες κατηγορίες (Mcclure et al., 2009):

- ✓ πρόληψη, όπου τα αντίμετρα προσπαθούν να μειώσουν τον κίνδυνο,
- ✓ διασφάλιση, με εργαλεία, ελέγχους και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων,
- ✓ ανίχνευση, με προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών,
- ✓ επαναφορά, με διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον μετά από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε.

Για την επιτυχή εφαρμογή των μέτρων ασφαλείας, το σχέδιο πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης της εφαρμογής του. Ολοκληρώνοντας το σχέδιο ασφαλείας, θα πρέπει να καταρτισθεί αναλυτικό σχέδιο έκτακτης ανάγκης, το οποίο θα περιλαμβάνει σχέδιο ανάκαμψης από καταστροφή, καθώς και σχέδιο αποκατάστασης λειτουργίας. Η εισαγωγή ασφαλείας σε ένα πληροφοριακό σύστημα είναι ένα δύσκολο και περίπλοκο έργο (Τσουραμάνης, 2005).

2.2.1 Πολιτική και μέτρα ασφαλείας στο διαδίκτυο

Ένα δίκτυο αποτελείται από ένα σύνολο διασυνδεδεμένων υπολογιστικών κόμβων, οι οποίοι έχουν τη δυνατότητα να ανταλλάσσουν μεταξύ τους πληροφορίες, καθώς και τους συνδέσμους μέσω των οποίων διακινούνται οι πληροφορίες αυτές. Υλοποιείται με σκοπό να παρέχει στους χρήστες του τη δυνατότητα να αποκτήσουν διαμοιρασμένη πρόσβαση σε δεδομένα, λογισμικό, συσκευές κ.ά. Η διασύνδεση δύο ή περισσότερων ανομοιογενών δικτύων, με σκοπό τη μεταξύ τους επικοινωνία και τη συνολική λειτουργία τους ως ένα λογικό δίκτυο, υλοποιεί το διαδίκτυο (Internet). Το διαδίκτυο σχεδιάστηκε αρχικά για το υπουργείο άμυνας των ΗΠΑ (δεκαετία του 1960), έχοντας ως σκοπό τη δημιουργία ενός δικτύου μεταγωγής πακέτων που θα μπορεί να λειτουργεί ακόμη και σε περίπτωση ύπαρξης κατεστραμμένων κόμβων ή συνδέσεων, υποστηρίζοντας πολλές εναλλακτικές διαδρομές.

Σήμερα έχει καταφέρει να αποτελέσει ένα παγκόσμιο και χαμηλού κόστους ομοιογενές μέσο για τη διακίνηση πληροφοριών και την παροχή υπηρεσιών, στις οποίες περιλαμβάνονται και εφαρμογές που παρέχουν διακίνηση ευαίσθητων δεδομένων, όπως τραπεζικές συναλλαγές και ηλεκτρονικό εμπόριο. Κατά τη σχεδίαση του διαδικτύου, μέχρι και την τέταρτη έκδοση του πρωτοκόλλου IP, η ασφάλεια δεν αποτελούσε ένα από τα χαρακτηριστικά που λήφθηκαν υπόψη κατά το σχεδιασμό του, καθώς βασικός στόχος ήταν η ανθεκτική λειτουργικότητά του και η ευκολία πρόσβασης σε αυτό. Ως αποτέλεσμα, δεν υπήρξαν μηχανισμοί προστασίας των επικοινωνιών (Mcclure et al., 2009). Έτσι οι μηχανισμοί ασφάλειας θα πρέπει να εφαρμόζονται ως ένα επιπρόσθετο συστατικό. Στην αδυναμία διαμόρφωσης μιας ενιαίας πολιτικής ασφάλειας και διαχείρισης, συμβάλλει και η ετερογένεια των διασυνδεδεμένων δικτύων, καθώς και η φύση της υπόστασης του διαδικτύου που θα πρέπει να μην εξαρτά τη λειτουργία του από ένα ή περισσότερα κέντρα διαχείρισης και ελέγχου.

Η διασφάλιση του απορρήτου των επικοινωνιών στη χώρα μας, υλοποιείται από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ)[22]. Είναι η ανεξάρτητη διοικητική αρχή, η οποία κατά το Σύνταγμα έχει ως αποστολή τη διασφάλιση του απορρήτου των επικοινωνιών[23]. Οι προβλεπόμενες αρμοδιότητες της ΑΔΑΕ διακρίνονται σε: αρμοδιότητες ελέγχου, κανονιστικές αρμοδιότητες, κατασταλτικές αρμοδιότητες, αρμοδιότητες έμμεσης συμμετοχής στη διαδικασία άρσης του απορρήτου, γνωμοδοτικές αρμοδιότητες, αρμοδιότητες επιβολής διοικητικών κυρώσεων, εσωτερικές αρμοδιότητες για την εύρυθμη λειτουργία της και αρμοδιότητες συνεργασίας με άλλους φορείς.

Οι αρμοδιότητες ελέγχου της ΑΔΑΕ αποτελούνται από διενέργεια ελέγχων σε δημόσιους και ιδιωτικούς φορείς, λήψη πληροφοριών από τους φορείς και κλήση σε ακρόαση κάθε προσώπου που κατά την κρίση της μπορεί να συμβάλει στην αποστολή της. Οι κανονιστικές αρμοδιότητές της αφορούν την έκδοση κανονιστικών πράξεων, που δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως, με τις οποίες διασφαλίζεται το απορρήτο των επικοινωνιών. Κατασταλτικές αρμοδιότητες είναι η κατάσχεση των

[22] Απόφαση 165/2011. Διαθέσιμο στο: http://www.adae.gr/fileadmin/docs/KANONISMOS_165.2011.pdf.
[23] ΑΔΑΕ – Παρουσίαση. Διαθέσιμο στο: http://www.adae.gr/i-adae/paroysiasi/.

μέσων παραβίασης του απορρήτου και η καταστροφή πληροφοριών ή στοιχείων ή δεδομένων που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου.

Αρμοδιότητες που αφορούν την έμμεση συμμετοχή της ΑΔΑΕ στη διαδικασία άρσης του απορρήτου είναι: η εξέταση καταγγελιών αναφορικά με τη διαδικασία άρσης του απορρήτου, ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, η τήρηση αρχείου απόρρητης αλληλογραφίας, στο οποίο περιέχονται οι κοινοποιούμενες στην ΑΔΑΕ διατάξεις των δικαστικών αρχών, με τις οποίες αποφασίζεται η άρση του απορρήτου, η δυνητική γνωστοποίηση της επιβολής άρσης του απορρήτου στους θιγόμενους, μετά τη λήξη του μέτρου και εφόσον δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε[24].

Η Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, έχει ως στόχο την προστασία των δεδομένων επικοινωνίας από πιθανούς κινδύνους, ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών. Η υλοποίηση μιας εφαρμογής πολιτικής προστασίας θα πρέπει να είναι σύμφωνη με τον κανονισμό της ΑΔΑΕ, καθώς πραγματοποιείται έλεγχος τήρησης και αποτελεσματικότητας της εκάστοτε πολιτικής.

Εκτός από την πολιτική ασφαλείας είναι απαραίτητη και η εφαρμογή ορισμένων μέτρων ασφαλείας που θα επιτρέπουν στον πάροχο ασφαλή διαδικτυακή επικοινωνία και προστασία των προσωπικών του δεδομένων. Μέτρα ασφαλείας αποτελούν η πιστοποίηση του χρήστη και η χρήση λογισμικού ασφαλείας.

Η πιστοποίηση του χρήστη πραγματοποιείται με τη χρήση κωδικών πρόσβασης, βιομετρικών τεχνικών, είτε με τη χρήση μιας «έξυπνης» κάρτας. Με αυτές τις μεθόδους επιτρέπεται η πιστοποίηση της ταυτότητας του χρήστη, όχι όμως με απόλυτα ασφαλή τρόπο, καθώς υπάρχουν πολλά εργαλεία παραβίασης δεδομένων. Οι κωδικοί πρόσβασης είναι ο πλέον διαδεδομένος τρόπος προστασίας δεδομένων. Είναι απλοϊκή η δημιουργία τους και εύκολη η χρήση τους. Είναι λιγότερο ασφαλείς και αποτελεσματικοί από τις υπόλοιπες μεθόδους, καθώς η παραβίασή τους είναι πλέον εύκολη διαδικασία. Οι βιομετρικές τεχνικές αποτελούν μια μέθοδο πιστοποίησης του χρήστη βασισμένη σε μοναδικά χαρακτηριστικά του με τη χρήση της ψηφιακής τεχνολογίας. Η αναγνώριση προσώπου, η σάρωση δακτυλικού

[24] ΑΔΑΕ - Αυτοτελές Τμήμα Ελέγχου Άρσης του Απορρήτου. Διαθέσιμο στο: http://www.adae.gr/i-adae/organogramma/arsi-toy-aporritoy/.

αποτυπώματος, φωνής, χεριού, ίριδας, υπογραφής, αποτελούν μερικές από τις τεχνικές της συγκεκριμένης μεθόδου, η οποία αποτελεί την πιο αξιόπιστη μέθοδο προστασίας δεδομένων και εφαρμογών ασφαλείας.

Η χρήση λογισμικού ασφαλείας αποτελείται από τρεις μεθόδους: τη χρήση λογισμικών antivirus, firewalls και κρυπτογραφία (Τσουραμάνης, 2005). Η εγκατάσταση ενός λογισμικού antivirus πραγματοποιεί ανίχνευση κακόβουλου λογισμικού, προσδιορίζει την ταυτότητα των ιών, δηλαδή ενημερώνει το λογισμικό για το είδος του ιού που εισήχθη στο σύστημα και το μέγεθος της ζημιάς και τέλος καθαρίζει το σύστημα από τους ιούς εντοπίζοντας αρχεία που τον περιλαμβάνουν, ώστε να επιδιορθωθούν, ή να διαγραφούν. Κάθε antivirus διαθέτει μια βάση δεδομένων γεμάτη με τα χαρακτηριστικά του κώδικα εκατομμυρίων ιών. Τα χαρακτηριστικά αυτά ονομάζονται «υπογραφές ιών». Κάθε αρχείο που ελέγχει το πρόγραμμα, ουσιαστικά διαβάζει τον κώδικά του, και ψάχνει να βρει αν περιέχει ίχνη από τις υπογραφές ιών που το antivirus ήδη γνωρίζει. Επειδή εκατοντάδες νέοι ή παραλλαγμένοι ιοί κυκλοφορούν κάθε μέρα, είναι πολύ σημαντικό το antivirus να είναι συνδεδεμένο στο internet, για να κατεβάσει τις νεότερες ενημερώσεις όσον αφορά τις υπογραφές ιών. Αν το antivirus δεν είναι ενημερωμένο, είναι θέμα χρόνου να βρεθεί κάποιος νέος ιός που ο κώδικάς του να μην ταιριάζει με καμία από τις γνωστές υπογραφές, και να περάσει ανενόχλητος στο σύστημά μας. Η συνηθέστερη μορφή ηλεκτρονικού εγκλήματος που απειλεί λογιστικά συστήματα είναι η είσοδος κακόβουλου λογισμικού και ιών και την προστασία από τα παραπάνω την προσφέρουν τα antivirus[25].

Firewall ή αλλιώς τείχη προστασίας, είναι μια συλλογή κατάλληλων συστημάτων, που τοποθετούνται στο σημείο σύνδεσης της υπό προστασία δικτυακής περιοχής, με τα υπόλοιπα δίκτυα. Επιβάλλει προκαθορισμένη πολιτική ασφαλείας και στόχος του είναι η προστασία των υπολογιστικών πόρων ενός οργανισμού από εξωτερικούς εισβολείς. Επιτελεί δηλαδή έλεγχο προσπέλασης από και προς το δίκτυο, παρέχει τη δυνατότητα καταγραφής της δραστηριότητας στο δίκτυο και δεν αποδίδει πραγματικές διευθύνσεις IP στους εσωτερικούς προστατευόμενους πόρους, καθώς οι εξωτερικοί χρήστες βλέπουν μια ενιαία IP και έτσι αυξάνονται τα επίπεδα ασφαλείας. Ο σκοπός λοιπόν της τοποθέτησης ενός firewall, είναι η πρόληψη επιθέσεων στο

[25] Microsoft. Προστασία του υπολογιστή μου από ιούς. Διαθέσιμο στο: https://support.microsoft.com/el-gr/help/17228/windows-protect-my-pc-from-viruses.

τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι να ρυθμίζεται ούτως 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 μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών[26].

Η κρυπτογραφία είναι ο μετασχηματισμός των δεδομένων σε μορφή που είναι αδύνατο να διαβαστεί από κανέναν, εκτός από εκείνον που κατέχει το κατάλληλο κλειδί, με σκοπό την ασφάλεια ενός συστήματος. Πραγματοποιείται μέσω ενός αλγόριθμου και διακρίνεται σε συμμετρική, όπου χρησιμοποιείται ένα ιδιωτικό κλειδί και σε ασύμμετρη, όπου χρησιμοποιούνται δύο κλειδιά, ένα ιδιωτικό και ένα δημόσιο. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων (Mcclure et al., 2009).

Το ασύμμετρο κρυπτοσύστημα δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι τα δυο είδη κλειδιών του. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι πως ότι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν και στη δημιουργία των ψηφιακών υπογραφών. Σκοπός της κρυπτογραφίας είναι η μεγάλη ασφάλεια ενός συστήματος, η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα και η μη αποποίηση παραλαβής και αποστολής. Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο, να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

2.3 Μέσα εντοπισμού και εξιχνίασης

Η έρευνα για την εξιχνίαση ηλεκτρονικών εγκλημάτων αποτελεί μια δύσκολη και χρονοβόρα διαδικασία, με στόχο τον εντοπισμό των ηλεκτρονικών ιχνών του

[26] ΤΕΙ Κεντρικής Μακεδονίας. Firewalls. Διαθέσιμο στο: http://teachers.teicm.gr/politis/Firewalls_Riverbed.pdf.

δράστη[27]. Τέτοια μέσα είναι: ο εντοπισμός IP, οι συναγερμοί, οι προειδοποιήσεις, οι αναφορές, τα αρχεία καταγραφής, τα emails και τα honeypots.

Ο εντοπισμός IP, δηλαδή το ηλεκτρονικό ίχνος είναι η ηλεκτρονική διεύθυνση IP και αποτελεί ένα ιδιαίτερα χρήσιμο και σημαντικό εργαλείο για τον εντοπισμό ατόμων που χωρίς να έχουν εξουσιοδοτημένη πρόσβαση, πραγματοποιούν ηλεκτρονική επίθεση σε κάποιο υπολογιστή, ή δίκτυο υπολογιστών, ή ακόμα και σε ολόκληρο σύστημα. Για τη διάπραξη ενός τέτοιου είδους εγκλήματος, οι δράστες χρησιμοποιούν ψεύτικες, ή πλαστές διευθύνσεις IP έτσι ώστε να μην είναι δυνατός ο εντοπισμός τους. Ο τρόπος που μπορεί να τελεστεί ένα τέτοιο ηλεκτρονικό έγκλημα είναι εξαιρετικά απλός. Πλαστογραφεί την ηλεκτρονική του διεύθυνση μέσω του συστήματος ονόματος χώρου, ή αλλιώς domain name system[28]. Για την αντιμετώπιση των πλαστών ηλεκτρονικών διευθύνσεων ο αποτελεσματικότερος τρόπος είναι η χρήση των firewalls.

Τα firewalls έχουν τη δυνατότητα αποστολής ηλεκτρονικών μηνυμάτων προς συγκεκριμένους παραλήπτες, ως προς τους οποίους έχει εντοπιστεί εγκληματική δραστηριότητα. Τα μηνύματα αυτά αποστέλλονται στο διαχειριστή του εκάστοτε συστήματος και παράλληλα γίνεται αποθήκευση της δραστηριότητας σε ειδικά αρχεία καταγραφής. Η χρήση του εργαλείου του συναγερμού (alarm) είναι πολύ σημαντική, καθώς μέσω αυτού μπορεί να αποτραπεί μια εγκληματική ηλεκτρονική ενέργεια προτού καν εκδηλωθεί η προσπάθεια παράνομης εισβολής ή μεταφοράς κακόβουλου λογισμικού.

Οι προειδοποιήσεις (alerts) χρησιμοποιούνται από το διαχειριστή του συστήματος. Μέσω των προειδοποιήσεων, ο διαχειριστής ειδοποιείται με email για την πραγματοποίηση επίθεσης και έτσι μπορεί να αντιμετωπίσει μια πιθανή ζημιά του συστήματος λόγω κακόβουλου λογισμικού, έγκαιρα και με αποτελεσματικότητα.

Με τη χρήση του εργαλείου των αναφορών (reports), μπορούν να αντληθούν πληροφορίες για πιθανές ηλεκτρονικές επιθέσεις και κυρίως την προσπάθεια απόκτησης μη εξουσιοδοτημένης πρόσβασης σε έναν ή περισσότερους ηλεκτρονικούς υπολογιστές, ή ακόμη και σε ολόκληρο δίκτυο.

---

[27] Ελληνική Αστυνομία. Αστυνομική Ανασκόπηση. Διαθέσιμο στο: https://www.policemagazine.gr/sites/default/files/pdf/%CE%95%CE%91_2011-06-0267.pdf.

[28] Ασφαλείς Υπηρεσίες και Συναλλαγές σε Περιβάλλοντα Κινητού Εμπορίου. Διαθέσιμο στο: https://repository.kallipos.gr/bitstream/11419/2295/1/02_chapter_07.pdf.

Τα αρχεία καταγραφής ή αλλιώς log files, έχουν τη δυνατότητα να αποθηκεύουν πληροφορίες που είναι σχετικές με λειτουργία ενός συστήματος, ενώ η χρησιμότητά τους είναι ιδιαίτερα μεγάλη από τη στιγμή που θα έχουν ενεργοποιηθεί συγκεκριμένες ενέργειες και πολιτικές. Στην περίπτωση που δεν έχει οριστεί μια συγκεκριμένη πολιτική που να αφορά στην ασφάλεια των χρηστών, τότε τα αρχεία καταγραφής θα παραμένουν κενά, ενώ την ευθύνη για τον καθορισμό των πολιτικών αυτών θα φέρει ο διαχειριστής του συστήματος. Μέσω των αρχείων αυτών, οι διωκτικές αρχές μπορούν να εντοπίσουν και να διερευνήσουν την πιθανότητα διενέργειας κάποιας συγκεκριμένης εφαρμογής από ένα χρήστη, καθώς και αν ο χρήστης αυτός διέθετε την απαιτούμενη εξουσιοδότηση για πρόσβαση σε έναν ηλεκτρονικό υπολογιστή, ή σε ένα σύστημα.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου, δηλαδή τα emails, αποτελούν το βασικότερο μέσο για την αναζήτηση και τον εντοπισμό του δράστη ηλεκτρονικού εγκλήματος. Η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί τον πλέον συνήθη τρόπο τέλεσης ηλεκτρονικών εγκλημάτων. Έχει τη μορφή της αποστολής απειλητικών ηλεκτρονικών μηνυμάτων, ή της αποστολής κακόβουλου λογισμικού, με σκοπό την καταστροφή ηλεκτρονικού υπολογιστή, ή του δικτύου και των αρχείων ενός ατόμου, ή μιας επιχείρησης. Η μετάδοση των μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον αποστολέα στον παραλήπτη διέρχεται από άλλους ενδιάμεσους ηλεκτρονικούς υπολογιστές, κάθε ένας εκ των οποίων μπορεί να προσθέσει τις δικές του πληροφορίες κυρίως στην επικεφαλίδα του. Οι πληροφορίες αυτές καταγράφονται σε διάφορα πεδία και περιλαμβάνουν τις επικεφαλίδες του αποστολέα και τις επικεφαλίδες του παραλήπτη. Έπειτα, μέσω της αναζήτησης του αποστολέα των κακόβουλων ηλεκτρονικών μηνυμάτων, οι πληροφορίες αυτές εντοπίζονται στις επικεφαλίδες του. Με τον τρόπο αυτό μπορεί να εντοπιστεί η διεύθυνση του ηλεκτρονικού ταχυδρομείου του αποστολέα προς όλους τους υπολογιστές που πέρασε το μήνυμα μέχρι να καταλήξει στον παραλήπτη[29].

Το honeypot αποτελεί το πιο σύγχρονο εργαλείο που χρησιμοποιούν οι αρμόδιες αρχές για τον εντοπισμό και την εξιχνίαση του ηλεκτρονικού εγκλήματος. Η λειτουργία και η χρήση του συνίσταται στην ύπαρξη ενός συνόλου συστημάτων που έχουν τη μορφή πραγματικών συστημάτων, ώστε να παραπλανήσουν το δράστη και

[29] Ασφαλείς Υπηρεσίες και Συναλλαγές σε Περιβάλλοντα Κινητού Εμπορίου. Διαθέσιμο στο: https://repository.kallipos.gr/bitstream/11419/2295/1/02_chapter_07.pdf.

να τον οδηγήσουν σε παραβίαση αυτών. Έχουν τη δυνατότητα να παρακολουθούν τις πράξεις του δράστη, έτσι ώστε να διαπιστωθεί στη συνέχεια η μεθοδολογία της επίθεσης. Επιμέρους μορφή των honeypots υψηλής αλληλεπίδρασης αποτελούν τα honeynets, τα οποία παρέχουν ολοκληρωμένα αντίγραφα δικτύων και συστημάτων παραγωγής (Blake et al., 2008).

ΚΕΦΑΛΑΙΟ 3: ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΕΡΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 Ενωσιακό θεσμικό πλαίσιο

Το Συμβούλιο της Ευρώπης συνειδητοποίησε πως επήλθαν σοβαρές και βαθιές αλλαγές στην ψηφιοποίηση, στη σύγκλιση και στη συνεχιζόμενη παγκοσμιοποίηση των ηλεκτρονικών υπολογιστών. Εξέφρασε την ανησυχία του για την ολοένα αυξανόμενη εγκληματικότητα στο κυβερνοχώρο και αναγνώρισε ότι η αποτελεσματική αντιμετώπιση του εγκλήματος αυτού μπορεί να γίνει μόνο με αναπτυγμένη, γρήγορη και καλά εφαρμοσμένη διεθνή συνεργασία σε ποινικά θέματα. Ο σκοπός αυτός επιτεύχθηκε με το Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη στην Βουδαπέστη από όλα σχεδόν τα μέλη της Ευρωπαϊκής Ένωσης, μεταξύ τους και η Ελλάδα, στις 23 Νοεμβρίου 2001[30].

Σκοπός της Σύμβασης είναι η προστασία της κοινωνίας από το έγκλημα στο κυβερνοχώρο με τη θέσπιση της κατάλληλης νομοθεσίας που είναι απαραίτητη για την έρευνα, δίωξη και εκδίκαση των εγκλημάτων του κυβερνοχώρου, καθώς και των εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών, αλλά και για τη συλλογή αποδεικτικών στοιχείων που βρίσκονται σε ηλεκτρονική μορφή, ενώ κύριο χαρακτηριστικό της είναι ότι καθιερώνει την υποχρέωση εναρμόνισης των εθνικών νομοθεσιών σε θέματα εγκλημάτων στο διαδίκτυο, όπως για παράδειγμα η διανομή πορνογραφικού υλικού στο internet, η εμπλοκή ανηλίκου σε ερωτική επαφή με τη χρήση του διαδικτύου, η χωρίς δικαίωμα αντιγραφή έργων πνευματικής ιδιοκτησίας.

Η Σύμβαση της Βουδαπέστης, περιλαμβάνει[31]: α) διατάξεις ουσιαστικού ποινικού δικαίου, β) διατάξεις ποινικού δικονομικού δικαίου και γ) διατάξεις διεθνούς δικαστικής συνεργασίας.

---

[30] Cyber Crime. Κινητοποιήσεις Ευρωπαϊκής Ένωσης σχετικά με το Ηλεκτρονικό Έγκλημα. Διαθέσιμο στο: https://electroniccrime.wordpress.com/.

[31] Lawspot. Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (ελληνικά). Διαθέσιμο στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0.

Οι διατάξεις ουσιαστικού ποινικού δικαίου αφορούν: διατάξεις που αναφέρονται σε εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικού υπολογιστή. Τέτοια αδικήματα είναι η παράνομη πρόσβαση και υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών, διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές, όπως η απάτη μέσω Η/Υ και η πλαστογραφία, διατάξεις για εγκλήματα σχετικά με το περιεχόμενο, όπως το αδίκημα της παιδικής πορνογραφίας, διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων.

Οι διατάξεις ποινικού δικονομικού δικαίου αναφέρονται σε θέματα: ταχείας διαφύλαξης δεδομένων αποθηκευμένων σε σύστημα υπολογιστή, ταχείας διαφύλαξης και γνωστοποίησης διακινουμένων δεδομένων, εντολής παροχής πληροφοριών, έρευνας και κατάσχεσης αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή, πραγματικού χρόνου συλλογής διακινουμένων δεδομένων, παγίδευσης – υποκλοπής περιεχομένου δεδομένων.

Οι διατάξεις διεθνούς δικαστικής συνεργασίας αναφέρονται: στην έκδοση, σε γενικές αρχές σχετικές με την αμοιβαία συνδρομή, σε παροχή αυθόρμητων πληροφοριών, στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών, στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων.

Σε διεθνές επίπεδο οι επιθέσεις κατά συστημάτων πληροφοριών ρυθμίζονται από τις σχετικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα (CETS No. 185, Budapest, 23.XI.2001, σε ισχύ από τις 01.07.2004)[32].

Σε Ενωσιακό επίπεδο οι επιθέσεις κατά συστημάτων πληροφοριών ρυθμίζονται από τις σχετικές διατάξεις της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά

[32] Details of Treaty No.185. Convention on Cybercrime. Διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου[33].

Η οδηγία αφήνει στη διακριτική ευχέρεια των κρατών - μελών να μην ποινικοποιήσουν τις επιθέσεις κατά συστημάτων πληροφοριών, οι οποίες είναι ήσσονος σημασίας. Μία περίπτωση μπορεί να θεωρείται ήσσονος σημασίας όταν, παραδείγματος χάριν, οι ζημίες που προκαλεί το αδίκημα και /ή ο κίνδυνος για το δημόσιο ή το ιδιωτικό συμφέρον, όπως η ακεραιότητα ενός συστήματος υπολογιστών ή ηλεκτρονικών δεδομένων, ή η σωματική ακεραιότητα, τα δικαιώματά ή άλλα συμφέροντα ενός προσώπου, είναι αμελητέα ή τέτοιας φύσης ώστε δεν είναι απαραίτητη η επιβολή ποινικής κύρωσης εντός του νομικού ορίου, ή η απόδοση ποινικής ευθύνης.

Η εύκολη λοιπόν πρόσβαση στο διαδίκτυο, καθώς υπήρξε τάχιστη εξέλιξη της τεχνολογίας, καθιστά αναγκαία τη δημιουργία νομικών κυρώσεων που να καταστέλλουν την εγκληματική δραστηριότητα στο διαδίκτυο. Παρακάτω παραθέτονται οι πράξεις οι οποίες τιμωρούνται ποινικά εφόσον διαπράττονται στο χώρο του διαδικτύου:

Σύμφωνα με το άρθρο 11 του Ν.2867/2000, κατά παράβαση των άρθρων 5 (αναφέρεται στη χορήγηση γενικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) και 6 (αναφέρεται στη χορήγηση ειδικών αδειών τηλεπικοινωνιακών δραστηριοτήτων), η άσκηση τηλεπικοινωνιακών δραστηριοτήτων τιμωρείται με φυλάκιση τουλάχιστον δώδεκα μηνών και με χρηματική ποινή[34].

Επίσης, όποιος παραβαίνει με οποιονδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρησης του απορρήτου των κάθε είδους δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματική ποινή, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις. Σε περίπτωση που ο παραβάτης της παρούσας

[33] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l33193&from=EL.

[34] Νόμος 2867/2000 - ΦΕΚ 273/Α/19-12-2000. Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις. Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-2867-2000.html.

διάταξης ανήκει στο προσωπικό τηλεπικοινωνιακής επιχείρησης, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον τριών ετών και η χρηματική ποινή. Ο τεχνικός εξοπλισμός και τα μέσα που χρησιμοποιήθηκαν για την τέλεση των παραπάνω αξιόποινων πράξεων δημεύονται. Σε περιπτώσεις πολλαπλών ή καθ' υποτροπή παραβάσεων προβλεπόμενων στον παρόντα νόμο, όπως εκάστοτε ισχύει, ή στον Ποινικό Κώδικα, σε σχέση με τα ανωτέρω αδικήματα, επιβάλλονται αθροιστικά οι βαρύτερες ποινές.

Σύμφωνα επίσης με το άρθρο 13 Ν.2774/22.12.99, για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, όποιος κατά παράβαση του νόμου αυτού χρησιμοποιεί, επεξεργάζεται, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα, ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

Όποιος παραλείπει να γνωστοποιήσει στην αρχή, τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορήγησης της άδειας, τιμωρείται με φυλάκιση έως τριών ετών και χρηματική ποινή. Επίσης, όποιος κατά παράβαση του άρθρου 7 του παρόντος νόμου διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της άδειας της αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή. Όποιος κατά παράβαση του άρθρου 8 του παρόντος νόμου προβαίνει σε διασύνδεση αρχείων χωρίς να τη γνωστοποιήσει στην αρχή, τιμωρείται με φυλάκιση έως τριών ετών και χρηματική ποινή. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της αρχής, όπου αυτή απαιτείται, ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών ή τα αφαιρεί, τα αλλοιώνει, τα βλάπτει, τα καταστρέφει, τα επεξεργάζεται, τα μεταδίδει, τα ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα, ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων, ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση και χρηματική ποινή και εάν πρόκειται για ευαίσθητα δεδομένα, με φυλάκιση

τουλάχιστον ενός έτους και χρηματική ποινή, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

Υπεύθυνος επεξεργασίας που δε συμμορφώνεται με τις αποφάσεις της αρχής, που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης, σύμφωνα με το άρθρο 12-4, για την ικανοποίηση του δικαιώματος αντίρρησης, σύμφωνα με το άρθρο 13-2 τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και με χρηματική ποινή. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δεν συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου. Επιπρόσθετα, αν ο υπαίτιος των πράξεων των 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτο, επιβάλλεται κάθειρξη έως δέκα 10 ετών. Τέλος, αν από τις πράξεις των 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή.

Στο δεύτερο μέρος του κεφαλαίου 2 της σύμβασης της Βουδαπέστης, προβλέπεται και απαιτείται από τα κράτη μέλη να υιοθετήσουν συγκεκριμένα και αποτελεσματικά δικονομικά και ανακριτικά μέτρα, τα οποία θα επιτρέπουν και θα διευκολύνουν τη διερεύνηση και τη δίωξη των διαδικτυακών εγκλημάτων. Αυτά είναι: μέτρα για την ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστή. Η υποχρέωση διαφύλαξης και διατήρησης της ακεραιότητας των δεδομένων, ορίζεται για χρονική περίοδο που κρίνεται αναγκαία και δεν υπερβαίνει τις ενενήντα μέρες. Μέτρα για την ταχεία διαφύλαξη και γνωστοποίηση διακινούμενων δεδομένων, ως προς τα οποία η λήψη μέτρων είναι αναγκαία για τη διασφάλιση της έγκαιρης διαφύλαξης διακινούμενων δεδομένων και της έγκαιρης αποκάλυψης ενός ικανοποιητικού συνόλου διακινούμενων δεδομένων προς την αρμόδια αρχή. Μέτρα επίσης σχετικά με την εντολή παροχής πληροφοριών και μέτρα για την έρευνα και κατάσχεση αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή. Επιπρόσθετα, απαιτείται η υιοθέτηση μέτρων σχετικών με τον πραγματικό χρόνο συλλογής διακινούμενων δεδομένων και άλλα σχετικά με την παγίδευση και την υποκλοπή περιεχομένου δεδομένων, τα οποία θα επιτρέπουν στις αρμόδιες αρχές να συγκεντρώνουν, ή να αντιγράφουν μέσω τεχνικών μέσων

δεδομένα περιεχομένου, σε πραγματικό χρόνο, συγκεκριμένων επικοινωνιών που μεταφέρονται μέσω πληροφοριακού συστήματος.

Τα ζητήματα διεθνούς δικαστικής συνεργασίας αναφέρονται στην έκδοση και σε γενικές αρχές σχετικές με την αμοιβαία συνδρομή. Δεδομένης της ανάγκης ευελιξίας του συστήματος της αμοιβαίας δικαστικής συνδρομής και λόγω του ότι το κανονιστικό πλαίσιο για τη συγκέντρωση αποδεικτικών στοιχείων ήταν περίπλοκο, εκδόθηκε η Οδηγία 2014/41/ΕΕ, η οποία προβλέπει και ρυθμίζει την Ευρωπαϊκή Εντολή Έρευνας σε ποινικές υποθέσεις. Σύμφωνα με το πρώτο άρθρο την Οδηγίας, η Ευρωπαϊκή Εντολή Έρευνας είναι δικαστική απόφαση, την οποία εκδίδει ή επικυρώνει δικαστική αρχή κράτους μέλους, με σκοπό την τέλεση ενός ή περισσότερων συγκεκριμένων ερευνητικών μέτρων σε άλλο κράτος μέλος για τη λήψη αποδεικτικών στοιχείων, ή για τη λήψη αποδεικτικών στοιχείων ευρισκόμενων ήδη στην κατοχή των αρμόδιων αρχών του κράτους εκτέλεσης[35].

Η Οδηγία αυτή διευκολύνει σημαντικά τη δικαστική συνεργασία μεταξύ των κρατών μελών στον αγώνα κατά της διασυνοριακής εγκληματικότητας και ιδίως του ηλεκτρονικού εγκλήματος, ενισχύοντας το αίσθημα ελευθερίας, ασφάλειας και δικαιοσύνης στην ΕΕ.

Η δικαιοδοσία ενός κράτους μέλους της ΕΕ αναφορικά με τη δίωξη εγκλημάτων κατά συστημάτων πληροφοριών θεμελιώνεται, εφόσον το αδίκημα έχει διαπραχθεί ολοκληρωτικά ή εν μέρει στο έδαφος του οικείου κράτους μέλους, ή από υπηκόους τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται ποινικό αδίκημα στον τόπο όπου έχει διαπραχθεί (άρθρο 1 του Ν. 4411/2016 και 12 της Οδηγίας).

Το κράτος μέλος, κατά τη θεμελίωση της δικαιοδοσίας του σύμφωνα με την παράγραφο 1, εξασφαλίζει ότι διαθέτει δικαιοδοσία, εφόσον ο δράστης διέπραξε το αδίκημα, όταν βρισκόταν στο έδαφός του, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός του, ή το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός του, ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα βρισκόταν στο έδαφός του. Το κράτος μέλος

[35] Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32014L0041.

ενημερώνει σχετικά την Επιτροπή όταν αποφασίζει να θεμελιώσει δικαιοδοσία για αδίκημα που αναφέρεται στα άρθρα 3 έως 8, το οποίο διαπράττεται εκτός του εδάφους του, όταν μεταξύ άλλων: ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφός του.

Οι αρχές δικαιοδοσίας που παρατίθενται παρακάτω, κατηγοριοποιούν τις περιπτώσεις των ηλεκτρονικών εγκλημάτων:

Η αρχή της εδαφικότητας είναι η βασικότερη και συνηθέστερη αρχή δικαιοδοσίας, η οποία έχει εφαρμογή όταν ένα έγκλημα διαπράττεται στο έδαφος του κυρίαρχου κράτους ανεξαρτήτως εθνικότητας του δράστη ή του θύματος. Η αρχή αυτή θεμελιώνεται στο άρθρο 22 παρ. 1 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

Σε περίπτωση όμως ηλεκτρονικού εγκλήματος, αυτό θεωρείται ότι τελείται στο έδαφος ενός κράτους, εάν ο δράστης έδρασε από το εξωτερικό όταν παρεμβαίνει στο σύστημα υπολογιστή άλλης χώρας. Οι περιπτώσεις αυτές φέρουν στοιχείο ετεροδικίας. Ο ευρύς προσδιορισμός της εδαφικότητας οδηγεί σε πιθανές συγκρούσεις δικαιοδοσίας, δεδομένου ότι για παράδειγμα ένα κακόβουλο λογισμικό μπορεί να βλάψει τα συστήματα υπολογιστών σε πολλές χώρες. Ο κίνδυνος σύγκρουσης δικαιοδοσίας αυξάνεται, αν η αρχή εδαφικότητας εφαρμόζεται και σε περιπτώσεις όπου, παρότι ο δράστης και το θύμα δε βρίσκονται στη χώρα, η υποδομή σε αυτή χρησιμοποιείται για την τέλεση ενός εγκλήματος όπως εάν ένα ηλεκτρονικό μήνυμα με παράνομο περιεχόμενο εστάλη μέσω ενός παρόχου σε μια χώρα, ή ένας ιστότοπος με παράνομο περιεχόμενο είναι αποθηκευμένος στον εξυπηρετητή ενός παρόχου στη χώρα.

Η αρχή της σημαίας, η οποία κατοχυρώνεται στο άρθρο 22 παρ. 1β και 1γ της σύμβασης του Συμβουλίου για το Κυβερνοέγκλημα.

Το δόγμα των συνεπειών, ή αρχή της προστασίας, σύμφωνα με το οποίο η δικαιοδοσία θεμελιώνεται για ένα έγκλημα που διαπράττεται από έναν αλλοδαπό εκτός εδάφους, με κανένα στοιχείο του εγκλήματος να λαμβάνει χώρα εντός του εδάφους, αλλά που το αποτέλεσμα επέρχεται εντός αυτού. Στενά συνδεδεμένη με το δόγμα αυτό είναι η αρχή της προστασίας, η οποία θεμελιώνει δικαιοδοσία σε

περιπτώσεις που ένα θεμελιώδες εθνικό ενδιαφέρον ενεργοποιείται. Εξαιτίας της απουσίας του δράστη, του θύματος και της χρησιμοποιούμενης υποδομής, υπάρχουν μόνο αδύναμες συνδέσεις με μια χώρα και η εφαρμογή της αρχής αυτής είναι υπό αμφισβήτηση.

Η αρχή της ενεργούς εθνικότητας καθορίζει τη δικαιοδοσία βάσει των δραστηριοτήτων ημεδαπών στην αλλοδαπή. Η αρχή αυτή εφαρμόζεται κυρίως στις χώρες αστικού δικαίου παρά στις χώρες εθιμικού δικαίου, με αποτέλεσμα οι τελευταίες να τείνουν να αναπληρώνουν την έλλειψη δικαιοδοσίας που βασίζεται στην αρχή της εθνικότητας με μια πιο διασταλτική ερμηνεία της αρχής εδαφικότητας. Λαμβάνοντας υπόψη ότι τα διαδικτυακά εγκλήματα μπορούν να τελεστούν δίχως να εγκαταλειφθεί το έδαφος της χώρας, η αρχή είναι επουσιώδους σημασίας όταν πρόκειται για κυβερνοεγκλήματα. Ωστόσο, η αρχή αυτή έχει ιδιαίτερη σημασία στις περιπτώσεις παιδικής πορνογραφίας μέσω υπολογιστικών δικτύων. Η αρχή αυτή θεσπίζεται στο άρθρο 22 παρ. 1δ της σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα.

Η αρχή της παθητικής εθνικότητας, σύμφωνα με την οποία η δικαιοδοσία θεμελιώνεται στην εθνικότητα του θύματος. Λαμβάνοντας υπόψη την επικάλυψή της με την αρχή της εδαφικότητας, η αρχή της παθητικής εθνικότητας εφαρμόζεται μόνο εάν ένας ημεδαπός γίνει θύμα ενός εγκλήματος ενώ βρίσκεται εκτός χώρας. παρότι η εφαρμογή της αρχής είναι αμφιλεγόμενη, τις τελευταίες δεκαετίες έχει τύχει ευρείας αποδοχής. Κωδικοποίηση της αρχής, όχι όμως σε επίπεδο διαδικτύου, αποτελεί ο τομέας 7 του Γερμανικού ποινικού Κώδικα.

Τέλος, η αρχή της καθολικότητας, η οποία έχει εφαρμογή σε συγκεκριμένα σοβαρά εγκλήματα διεθνούς ενδιαφέροντος, όπως τα εγκλήματα κατά της ανθρωπότητας και τα εγκλήματα πολέμου. Πολλές χώρες οι οποίες αναγνωρίζουν τη συγκεκριμένη αρχή, προχώρησαν σε επέκταση του πεδίου εφαρμογής της και σε εγκλήματα του διαδικτύου.

3.2 Ισχύον Ελληνικό νομικό πλαίσιο

Στην ελληνική έννομη τάξη δεν υπάρχει νόμος που να αναφέρεται σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου. Ο νόμος ν.1805/88, ο οποίος τροποποίησε και

συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α), αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές, δηλαδή αναφέρεται γενικά στην ηλεκτρονική εγκληματικότητα. Ανεξάρτητα από το εάν ο συγκεκριμένος νόμος επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής, το βέβαιο είναι ότι δεν επαρκεί να καλύψει τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του διαδικτύου.

Για να αποκτήσει κάποιος πρόσβαση στον κυβερνοχώρο απαραίτητη προϋπόθεση αποτελεί η χρήστη των τηλεπικοινωνιών, η οποία επιτυγχάνεται με τη σύνδεση του χρήστη σε μια υπηρεσία παροχής υπηρεσιών. Ο παροχέας υπηρεσιών παίζει σημαντικό ρόλο στην ασφάλεια και στη μυστικότητα του διαδικτύου, καθώς αποτελεί κομβικό σημείο για τον εντοπισμό των παρανομιών και τη συλλογή των αποδεικτικών στοιχείων δεδομένου ότι όλα τα δεδομένα περνούν από τις εγκαταστάσεις του.

Συνεπώς, οι σχετικοί με τις τηλεπικοινωνίες έχουν άμεση ή έμμεση σχέση με τη χρήση του διαδικτύου. Με λίγα λόγια, το διαδίκτυο είναι μια μορφή επικοινωνίας που γίνεται με την βοήθεια ή δια μέσου των τηλεπικοινωνιών. Σχετικοί λοιπόν νόμοι είναι: ο ν.2867/19-12-2000 για την οργάνωση και λειτουργία των τηλεπικοινωνιών, ο ν.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα σε συνδυασμό με το ν.2472/10.4.97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο ν.2225/20.7.94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας, ο ν.2867/19-12-2000 που ρυθμίζει κάθε είδος τηλεπικοινωνιακής δραστηριότητας που αναπτύσσεται εντός της ελληνικής επικράτειας, ο ν.2774/22.12.1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, ο ν.2472/1997 (ΦΕΚ 50 Α/10.4.1997) που προστατεύει το άτομο από την αυτοματοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο ν.2225/94, για την προστασία της ελευθερίας της ανταπόκρισης (Τσουραμάνης, 2005).

3.2.1 Μορφές ηλεκτρονικού εγκλήματος κατά το ελληνικό δίκαιο

Το φαινόμενο της παιδικής πορνογραφίας στο διαδίκτυο αποτελεί μία από τις μορφές του ηλεκτρονικού εγκλήματος. Οποιοσδήποτε μπορεί, πολύ εύκολα και σχετικά γρήγορα, να διαβιβάσει μέσω του διαδικτύου φωτογραφίες παιδικού

σεξουαλικού περιεχομένου σε παραλήπτες σε όλο τον κόσμο είτε σκανάροντας μια φωτογραφία και αποθηκεύοντας την σε κάποιο αρχείο και στη συνέχεια αποστέλλοντας την μέσω ηλεκτρονικού ταχυδρομείου, ή δημοσιεύοντας την σε κάποια ιστοσελίδα, είτε κατεβάζοντας την από κάποια ιστοσελίδα και προωθώντας την μέσω ηλεκτρονικού ταχυδρομείου προς κάθε ενδιαφερόμενο. Τα τελευταία χρόνια βλέπουμε να εξελίσσεται σε μάστιγα, καθώς όλο και περισσότερα κρούσματα και υποθέσεις έρχονται στο φως της δημοσιότητας.

Η παιδική εκμετάλλευση υπήρξε πολύ πριν από το διαδίκτυο, και τα δίκτυα των παραβατών που επικοινωνούσαν πριν από την ανακάλυψη των προσωπικών υπολογιστών ήταν μέρος της καθημερινής ζωής, αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης παιδιών. Η αυξανόμενη χρήση του Διαδικτύου από τους έφηβους και από τα πιο μικρά παιδιά, δημιούργησαν την πιθανότητα δίωξής τους από τους ενήλικους παραβάτες. Καθώς όλο και περισσότερα παιδιά συγκεντρώθηκαν στο διαδίκτυο στη δεκαετία του ’90, οι ενήλικες που επιθυμούσαν να τους δελεάσουν για σεξουαλικές σχέσεις, τους υποδέχθηκαν με χαρά.

Χρονολογικά, το 1962 άρχισε ουσιαστικά να ισχύει η σημερινή αντίληψη για την κακοποίηση των παιδιών και η αντιμετώπισή της ως ιατρό - κοινωνικό πρόβλημα. Τότε χρησιμοποιήθηκε για πρώτη φορά ο όρος Battered Child Syndrome, δηλαδή «Σύνδρομο Κακοποιημένου Παιδιού» στις ΗΠΑ, από τον παιδίατρο Henry Kempe. Ο Kempe αμφισβητήθηκε έντονα, όμως λίγα χρόνια αργότερα, τόσο στην Αμερική όσο και σε άλλες χώρες του κόσμου, οι γιατροί άρχισαν να παραδέχονται ότι οι άνθρωποι που φροντίζουν τα παιδιά, μπορεί και να τα τραυματίζουν.

Σήμερα, σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης η παιδική πορνογραφία έχει τις εξής μορφές:

- ✓ Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
- ✓ Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- ✓ Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο άτομο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Για να γίνουν πλήρως αντιληπτές οι διαστάσεις του προβλήματος, αναφέρονται κάποια στατιστικά στοιχεία που έδωσε στη δημοσιότητα η Unesco σχετικά με την παιδική πορνογραφία στο Διαδίκτυο:

- ✓ Ο τζίρος της βιομηχανίας παιδικής πορνογραφίας ξεπερνά τα 3 δις ευρώ το χρόνο.
- ✓ Ο αριθμός των ιστοσελίδων που φιλοξενούν πορνογραφικό περιεχόμενο με πρωταγωνιστές ανήλικα παιδιά, ακόμη και βρέφη, υπολογίζεται ότι σημείωσε την τελευταία πενταετία ραγδαία αύξηση.
- ✓ Ορισμένες ιστοσελίδες παιδικής πορνογραφίας έχουν ημερησίως επισκεψιμότητα περίπου 150.000.

Προκειμένου να προστατευθούν τα παιδιά από τους κινδύνους του διαδικτύου, δημιουργήθηκε στην έδρα της Unesco, ένα κίνημα που ονομάστηκε Innocence in Danger, δηλαδή Αθωότητα σε κίνδυνο. Το συγκεκριμένο κίνημα δημιουργήθηκε μετά από ένα συνέδριο με θέμα τα κακοποιημένα παιδιά, την παιδική πορνεία και την παιδική πορνογραφία στο διαδίκτυο[36].

Παρά τις κινητοποιήσεις, ωστόσο, που αποβλέπουν στην προστασία των ανήλικων παιδιών στο διαδίκτυο από τους επιτήδειους, συχνά γνωστοποιούνται περιπτώσεις εξαπάτησης ανηλίκων. Παρατηρούνται περιπτώσεις όπου ενήλικες ασελγούν σε ανήλικα παιδιά, τα οποία ψαρεύουν είτε μέσω των λεγόμενων σελίδων κοινωνικής δικτύωσης, είτε από νεανικά στέκια, εξασφαλίζουν από αυτά πορνογραφικό υλικό και τα διακινούν στο διαδίκτυο .

Πέρα από την παιδική πορνογραφία που είναι μία από τις πιο βαριές αλλά και απάνθρωπες μορφές ηλεκτρονικού εγκλήματος υπάρχουν πολλές ακόμη είδους απάτες που πραγματοποιούνται καθημερινά.

Μια από αυτές είναι ο κυβερνοπόλεμος, ο οποίος περιλαμβάνει πολεμικές επιθέσεις ενάντια στο στρατιωτικό σώμα ενός έθνους. Παράδειγμα τέτοιας επίθεσης

[36] Archive for the "Μορφές ηλεκτρονικού εγκλήματος" Category. Παιδική Πορνογραφία. Διαθέσιμο στο: https://electroniccrime.wordpress.com/category/%CE%BC%CE%BF%CF%81%CF%86%CE%AD%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%8D-%CE%B5%CE%B3%CE%BA%CE%BB%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82/.

μπορεί να είναι διακοπή κρίσιμων επικοινωνιακών διαύλων. Οι κυβερνοεπιθέσεις έχουν ως στόχο την υποδομή, είτε αυτή αφορά τις πληροφορίες γενικότερα, τα αποτελέσματα των οποίων μπορεί να είναι πιο επιζήμια για τις χώρες που διαθέτουν σημαντικές υποδομές δικτύων Η/Υ, είτε αφορά δίκτυα κοινά σε όλους τους πολίτες ενός κράτους, όπως για παράδειγμα δίκτυα ενέργειας, μεταφορών, επικοινωνιών κ.τ.λ.

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η διασπορά κακόβουλων προγραμμάτων, δηλαδή η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί είναι ειδικά προγράμματα που έχουν την ικανότητα να μεταδίδονται μεταξύ υπολογιστών και δικτύων και να δημιουργούν αντίγραφα του εαυτού τους χωρίς φυσικά να το γνωρίζει ή να το εγκρίνει ο τελικός χρήστης. Υπάρχουν δύο κατηγορίες ιών: των συστημάτων και των προγραμμάτων. Ένας ιός στοχεύει στη δυσλειτουργία, ή και καταστροφή ολόκληρων συστημάτων, στη διαγραφή αρχείων ή και του συνολικού περιεχομένου των σκληρών δίσκων. Μία μορφή ιών είναι τα σκουλήκια (worms) (Τσουραμάνης, 2006).

Αυτά αποτελούν προγράμματα Η/Υ που χρησιμοποιούνται ως μηχανισμός μεταφοράς άλλων προγραμμάτων. Μία άλλη μορφή είναι οι Δούρειοι Ίπποι (Trojan Horses) που είναι επίσης προγράμματα Η/Υ τα οποία αν και φαίνεται πως λειτουργούν κανονικά, παράλληλα εκτελούν και κάποιες άλλες μη επιτρεπόμενες ενέργειες. Αυτά τα προγράμματα έχουν τη μορφή παιχνιδιών, αυτό που κάνουν όμως, είναι να κλέβουν τα ονόματα και τους κωδικούς πρόσβασης των ανυποψίαστων χρηστών του διαδικτύου. Τέλος, μία ακόμη μορφή κακόβουλων προγραμμάτων είναι εκείνα που καλούν τηλεφωνικούς αριθμούς για την πρόσβαση σε ορισμένες υπηρεσίες υψηλής χρέωσης και ονομάζονται dialers.

Η βλάβη που προκαλεί ένας ιός μπορεί να κυμαίνεται από την εμφάνιση ενός ενοχλητικού μηνύματος στην οθόνη του υπολογιστή, μέχρι και την διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολύνει. Ο πιο συνηθισμένος τρόπος μόλυνσης είναι μέσω email που περιέχουν ένα συνημμένο αρχείο με το πρόγραμμα του ιού, το οποίο αρχίζει και εκτελείται αυτόματα πολλές φορές και έτσι μολύνει τον υπολογιστή του χρήστη.

Κατά τη χρήση του διαδικτύου είναι δυνατόν να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσο τέλεσης της κοινής απάτης,

αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή η ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή, στο πρόγραμμα και στα δεδομένα του. Οι μορφές των πλέον διαδεδομένων απατών που τελούνται τα τελευταία χρόνια μέσω του διαδικτύου είναι οι ακόλουθες (Βλαχόπουλος, 2007):

- ✓ Η απάτη με τα νιγηριανά μηνύματα του ηλεκτρονικού ταχυδρομείου (Nigerian email fraud). Σε αυτή την περίπτωση, το υποψήφιο θύμα λαμβάνει ένα email, με το οποίο ο απατεώνας του υπόσχεται μεγάλη χρηματική αμοιβή αν τον βοηθήσει να μεταφέρει χρήματα από τον τραπεζικό του λογαριασμό στο λογαριασμό του θύματος. Οι λόγοι τους οποίους επικαλείται ο απατεώνας για τη μεταφορά αυτή ποικίλλουν κατά περίπτωση, συνήθως όμως αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή γόνους πλούσιων οικογενειών που θα πρέπει να εγκαταλείψουν τη χώρα τους λόγω πολιτικών συγκρούσεων. Προτού όμως το θύμα εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο απατεώνας, πρέπει να καταβάλλει ορισμένα χρήματα για τα έξοδα μεταφοράς, ή να δώσει για το λόγο αυτό τα στοιχεία του τραπεζικού του λογαριασμού. Στην πρώτη περίπτωση, μετά την αποστολή των χρημάτων θα διακοπεί η επικοινωνία με τον απατεώνα, ενώ στη δεύτερη το θύμα είναι πολύ πιθανό να χάσει όλα τα χρήματα του τραπεζικού του λογαριασμού, είτε έχοντας ο απατεώνας στη διάθεση του τα στοιχεία ταυτότητος του θύματος να του χρεώνει μεγάλα χρηματικά ποσά.
- ✓ Η απάτη με το ηλεκτρονικό μήνυμα ψαρέματος (phishing mail). Στην περίπτωση αυτή, ο απατεώνας προσπαθεί μέσω των μηνυμάτων που αποστέλλει, να αποσπάσει από το θύμα προσωπικά του οικονομικά δεδομένα. Αρχικά, το υποψήφιο θύμα λαμβάνει ένα email, αποστολέας του οποίου φαίνεται να είναι η τράπεζα την οποία πραγματοποιεί συναλλαγές. Η σχετική αιτιολογία αναφέρεται σε προβλήματα στους Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δε γίνει η επιβεβαίωση του θα κλειδωθεί. Το email αυτό περιλαμβάνει σύνδεσμο (link) που οδηγεί στο δικτυακό τόπο της συγκεκριμένης τράπεζας, ο οποίος όμως δεν αποτελεί τον αυθεντικό, αλλά έχει δημιουργηθεί από τον απατεώνα έτσι ώστε να μιμείται τον πραγματικό. Με αυτό τον τρόπο το θύμα αποστέλλει τα στοιχεία του απ' ευθείας στον απατεώνα.

- ✓ Ένας ακόμη τρόπος ψηφιακής απάτης είναι αυτός που αφορά τη λήψη από το θύμα ενός email ή ενός pop-up window που του εμφανίζεται κατά την περιήγησή του στο διαδίκτυο και με το οποίο του γνωστοποιείται πως είναι ένας από τους τυχερούς επισκέπτες που κέρδισε ένα σημαντικό χρηματικό ποσό σε κάποια κλήρωση. Έτσι η επόμενη αναγκαστική κίνηση του θύματος για να παραλάβει τα χρήματα είναι να αφήσει τα προσωπικά του στοιχεία και τα στοιχεία του τραπεζικού του λογαριασμού. Με αυτόν τον τρόπο ο απατεώνας λαμβάνει τα στοιχεία του θύματος, τα οποία μπορεί να τα χρησιμοποιήσει με διάφορους τρόπους εις βάρος του τελευταίου.
- ✓ Η απάτη με τις επιταγές, όπου ο απατεώνας αγοραστής σε μια δικτυακή δημοπρασία είναι δυνατό να συμφωνήσει με τον πωλητή να πληρώσει με επιταγή, αποτελεί μία ακόμη ψηφιακή απάτη. Ο πωλητής αποστέλλει το εμπόρευμα, ενώ ο απατεώνας έχει καταθέσει την επιταγή. Η τράπεζα όμως διαπιστώνει στη συνέχεια πως πρόκειται για πλαστή ή ακάλυπτη επιταγή και έτσι αδυνατεί να περάσει τα χρήματα στο λογαριασμό του θύματος.

Η μορφή Hacking – Cracking, έχει να κάνει με την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα, με παράνομους σκοπούς. Αυτοί οι εγκληματίες του κυβερνοχώρου διακρίνονται σε δύο κατηγορίες, ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα, στους hackers και στους crackers (Τσουραμάνης, 2006).

Hacker ονομάζεται αυτός που αντλεί ευχαρίστηση από την κατανόηση της εσωτερικής λειτουργίας ενός συστήματος. Ειδικότερα, ενός υπολογιστή ή δικτύου υπολογιστών, στον οποίο όμως δεν έχει δικαίωμα πρόσβασης. Στην πραγματικότητα, ο hacker είναι ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων. Η διεθνής κοινότητα των hackers πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοιχτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Έχουν επίσης, την αμφιλεγόμενη πεποίθηση ότι το «σπάσιμο» και η «εξερεύνηση» ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και λογισμικού, είναι ηθικά αποδεκτή εφόσον ο hacker δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση

εμπιστευτικότητας. Οι hackers εμφανίστηκαν για πρώτη φορά στα τηλεπικοινωνιακά δρώμενα τη δεκαετία του 1970 στις Η.Π.Α.

Σε αντίθεση με τους hackers, οι crackers είναι άτομα που κάνουν απόπειρα να αποκτήσουν πρόσβαση σε υπολογιστικό σύστημα για την οποία όχι μόνο δε διαθέτουν εξουσιοδότηση, αλλά με στόχο να το βλάψουν με οποιοδήποτε τρόπο. Οι crackers είναι εξ ορισμού κακόβουλοι, ενώ διαθέτουν και πολλά εργαλεία για τις κακόβουλες ενέργειές τους. Η ουσία του προβλήματος του cracking δεν εντοπίζεται σε επιθέσεις που γίνονται στην αρχική ιστοσελίδα του δικτυακού τόπου μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, κάτι που είναι εύκολο να αντιληφθεί, αλλά στις ύπουλες υποθέσεις. Στην τροποποίηση δηλαδή χωρίς να γίνει αντιληπτό, σημαντικών δεδομένων που τηρούνται από δημόσιες υπηρεσίες, όπως για παράδειγμα η αλλαγή της σειράς επιτυχίας σε έναν διαγωνισμό, η πιστή αντιγραφή ολόκληρων διαδικτυακών τόπων μεγάλων εταιρειών που κάνουν πωλήσεις μέσω διαδικτύου, ή και μεγάλων οργανισμών ή δημόσιων υπηρεσιών και η εξαπάτηση ανυποψίαστων χρηστών των διαδικτυακών τόπων.

3.2.2 Φορείς για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας

Στην Ελλάδα δεν υπάρχει επίσημη εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο. Υπάρχουν όμως φορείς για πρόληψη και καταπολέμηση της ηλεκτρονικής εγκληματικότητας, καθώς και για την τήρηση των αρχών για την ασφάλεια στον κυβερνοχώρο, όπως αυτές ενσωματώθηκαν στον ελληνικό χώρο. Οι φορείς αυτοί είναι:

- ✓ η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας, που ασχολείται με την προστασία των πληροφοριακών δικτύων και υποδομών των ενόπλων δυνάμεων,
- ✓ η Εθνική Υπηρεσία Πληροφοριών, η οποία είναι υπεύθυνη για το CERT (Computer Emergency and Response Team). Αποτελεί την εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και την Αρχή Ασφάλειας πληροφοριών (υπεύθυνη για την ασφάλεια των επικοινωνιών και των συστημάτων πληροφοριών σε εθνικό επίπεδο και την πιστοποίηση του διαβαθμισμένου (απόρρητου) υλικού των εθνικών επικοινωνιών,
- ✓ η Διεύθυνση Ηλεκτρονικού Εγκλήματος, η οποία είναι αρμόδια για τη μελέτη μέτρων αντιμετώπισης του ηλεκτρονικού εγκλήματος, την προετοιμασία

νομοθετικών ρυθμίσεων και διοικητικών πράξεων για την πρόληψη και την καταστολή, την καθοδήγηση των περιφερειακών υπηρεσιών στην εφαρμογή ή βελτίωση μεθόδων καταπολέμησης του εγκλήματος στη χώρα, την ανταλλαγή γνώσεων, πληροφοριών και εμπειριών με αστυνομικές αρχές άλλων χωρών, μέσω της διεύθυνσης Διεθνούς Αστυνομικής Συνεργασίας και την κατάρτιση και εφαρμογή προγραμμάτων πρόληψης και καταστολής. Σε εναρμόνιση με τη Σύμβαση της Βουδαπέστης, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος υπό την εποπτεία του Εισαγγελέα Εφετών, αποτελεί σημείο διαρκούς επαφής για τη διευκόλυνση της ταχείας επεξεργασίας των αιτημάτων συνδρομής που προέρχονται από την αλλοδαπή,

- ✓ το Κέντρο Μελετών Ασφαλείας, το οποίο ανήκει στο Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης και ο ρόλος του είναι η διεξαγωγή θεωρητικής και εφαρμοσμένης έρευνας και η εκπόνηση μελετών στρατηγικής φύσεως σχετικά με την πολιτική Ασφαλείας, καθώς και η παροχή υπηρεσιών γνωμοδοτικού και συμβουλευτικού χαρακτήρα σε ζητήματα ασφαλείας,
- ✓ η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία έχει ως αρμοδιότητά της την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- ✓ η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, που ως βασική αποστολή έχει την προστασία του απορρήτου των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία με κάθε δυνατό τρόπο. Ιδίως ως προς την προστασία του απορρήτου των επικοινωνιών, η ΑΔΑΕ ασκεί έλεγχο τήρησης των όρων διεξαγωγής της επικοινωνίας, καθώς και της διαδικασίας άρσης του απορρήτου,
- ✓ η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, η οποία θεωρείται μια εκ των σημαντικότερων αρχών που εποπτεύουν το χώρο του διαδικτύου, καθώς ρυθμίζει πάσης φύσεως ζητήματα που άπτονται των τηλεπικοινωνιών. Σημαντική είναι η αρμοδιότητα αυτής της αρχής, ως προς τη χορήγηση αδειών προς όλους τους παρόχους τηλεπικοινωνιακών υπηρεσιών και την άσκηση ελέγχου των υπηρεσιών αυτών.

Επίσης, στο πλαίσιο της δράσης για την αντιμετώπιση κινδύνων από χρήση τεχνολογίας ηλεκτρονικών επικοινωνιών, έχει δημιουργηθεί η Ομάδα Ψηφιακής Ασφάλειας. Στόχοι της ομάδας αυτής είναι η πρόληψη ψηφιακών κινδύνων, η

πρόταση πολιτικής για την ασφάλεια, η ενημέρωση για ψηφιακούς κινδύνους και η ανταλλαγή τεχνογνωσίας με φορείς, εμπειρογνώμονες και οργανισμούς στην ελληνική επικράτεια.

3.2.3 Το ζήτημα της δικαιοδοσίας στο διαδίκτυο κατά το ελληνικό δίκαιο

Η δικαιοδοσία ενός κράτους μέλους της ΕΕ αναφορικά με τη δίωξη εγκλημάτων κατά συστημάτων πληροφοριών θεμελιώνεται, εφόσον το αδίκημα έχει διαπραχθεί ολοκληρωτικά ή εν μέρει στο έδαφος του οικείου κράτους μέλους, ή από υπηκόους τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται ποινικό αδίκημα στον τόπο όπου έχει διαπραχθεί (άρθρο 1 του Ν. 4411/2016)[37].

3.2.4 Νομοθετικές ατέλειες του νομοθετικού πλαισίου

Η γρήγορη εξέλιξη της τεχνολογίας καθιστά αδύνατο για τη νομοθεσία να την προφτάσει. Κάπου εδώ γεννάται το ερώτημα αν τελικά ο παγκόσμιος ιστός μπορεί να ελεγχθεί από την άποψη της ποινικής συμπεριφοράς. Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις τόσο σε νομικό όσο και σε τεχνικό επίπεδο, κάτι που αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε κράτους καθώς ελάχιστοι νομικοί τις διαθέτουν.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικά τις καταστάσεις πιεζόμενες από τα πράγματα πριν από δύο περίπου δεκαετίες η συμβατική νομοθεσία δεν αρκούσε για την αντιμετώπισή τους. Στη σημερινή εποχή οι προηγμένες χώρες έχουν καταρτίσει σχετική νομοθεσία για την αντιμετώπιση των εγκλημάτων της πληροφορικής.

Η προσέγγιση των νομικών θεμάτων που αφορούν τον κυβερνοχώρο ενέχει πολλές δυσκολίες καθώς εκτός από νομικές γνώσεις απαιτεί και τεχνικές. Ακόμη, το γεγονός ότι το έγκλημα στον κυβερνοχώρο αποτελεί μία νέα μορφή εγκλήματος προκαλεί δυσχέρεια σε αυτόν που ασχολείται με τη νομική πλευρά του θέματος από ποινική άποψη αφού υπάρχει έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων.

[37] Νόμος 4411/2016 Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξει. Διαθέσιμο στο: https://www.taxheaven.gr/laws/law/index/law/766.

Ένα ακόμη πρόβλημα που καλείται κάποιος να αντιμετωπίσει έχει να κάνει με την ελληνική νομική ορολογία. Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη κατά κανόνα στην αγγλική γλώσσα και η αντίστοιχη μεταφορά αυτών των όρων στα ελληνικά δεν είναι ούτε εύκολη ούτε δόκιμη. Το πρόβλημα αυτό της ορολογίας παρουσιάζεται όχι μόνο στο πεδίο του ουσιαστικού ποινικού δικαίου αλλά και στο αντίστοιχο του ποινικού δικονομικού δικαίου. Αυτό που έχει αποφασισθεί από τα κρατικά νομικά μέσα για την αντιμετώπιση αυτού του θέματος είναι να ακολουθηθεί η παραδοσιακή δικονομική ορολογία και μόνο όπου και όταν κριθεί αναγκαίο να ακολουθηθεί μια μικτή, δηλαδή σε μια υπόθεση ηλεκτρονικού εγκλήματος να αναφερθούν τόσο οι παραδοσιακοί όροι όσο και οι τεχνικοί, για παράδειγμα οι όροι έρευνα ή παρόμοια πρόσβαση, κατάσχεση ή παρόμοια διαφύλαξη.

Τέλος, τα ηλεκτρονικά αποδεικτικά μέσα δεν μπορούν σε καμία περίπτωση να ταυτιστούν με τα παραδοσιακά αποδεικτικά μέσα και αυτό γιατί οι αποδείξεις ενός εγκλήματος που λαμβάνει χώρο στο φυσικό κόσμο, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο χώρο και χρόνο. Αντιθέτως, οι ηλεκτρονικές αποδείξεις δεν είναι χειροπιαστές, μπορεί κάποιος από μακριά να αλλάξει τη μορφή και το περιεχόμενό τους, ή ακόμη και να τις εξαφανίσει με το πάτημα ενός πλήκτρου.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το διαδίκτυο κατέχει ένα σπουδαίο ρολό στη σύγχρονη καθημερινότητα και αποτελεί βασικό εργαλείο για την πλειοψηφία των χρηστών. Το ηλεκτρονικό έγκλημα έρχεται λοιπόν να εκμεταλλευτεί αυτή την διάσταση.

Η επικοινωνία μεταξύ ατόμων από οποιοδήποτε σημείο του πλανήτη σε πραγματικό χρόνο μέσω του διαδικτύου αποτελεί μία νέα αδιαμφισβήτητη επανάσταση στον τομέα της επικοινωνίας.

Η συνεχής ανάπτυξη του διαδικτύου ευνόησε την διάπραξη μιας νέας μορφής απάτης, αυτή της απάτης μέσω διαδικτύου ως ειδική περίπτωση οικονομικού εγκλήματος.

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η παιδική πορνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη επιχειρηματική δραστηριότητα με τεράστια κέρδη, καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων καταβάλλουν υπέρογκα χρηματικά ποσά.

Με τη χρήση του διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά Μ.Μ.Ε. και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων. Συνεπώς το διαδίκτυο παρέχει ευκολία στο έργο της τρομοκρατίας.

Ο διαδικτυακός εκφοβισμός αποτελεί εξέλιξη του παραδοσιακού εκφοβισμού και αφορά πράξεις εκφοβισμού, ψυχολογικής κακοποίησης, επιθετικότητας, απειλής, ταπείνωσης, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς παιδιών, προ εφήβων και εφήβων που πραγματοποιείται μέσω του διαδικτύου.

Ο διαδικτυακός εκφοβισμός αυξάνεται όταν το άτομο εισέρχεται την εφηβεία, κορυφώνεται στα μέσα αυτής και μετά ακολουθεί φθίνουσα πορεία. Η σωματική αδυναμία και κάποια ιδιαίτερα χαρακτηριστικά όπως η παχυσαρκία, ο τραυλισμός, σεξουαλικές προτιμήσεις, κτλ, αποτελούν στοιχεία προσέλκυσης εκφοβιστικών επιθέσεων.

Η ανωνυμία στο διαδίκτυο δημιουργεί μια αίσθηση ελευθερίας και ασφάλειας και έτσι ο θύτης με ψεύτικη ταυτότητα μπορεί να διαπράξει εγκληματική συμπεριφορά παραμένοντας αόρατος, αφήνοντας ελάχιστα ή καθόλου ψηφιακά ίχνη, επομένως γίνεται πιο δύσκολος ο εντοπισμός τους από πλευράς διωκτικών αρχών.

Άμεση συνέπεια της ψηφιοποίησης στις μέρες μας είναι η διάχυση των πολιτισμικών περιεχομένων στο διαδίκτυο, με τρόπο πολύ πιο αποτελεσματικό και μαζικό από οποιαδήποτε άλλη ιστορική συγκυρία.

Η ασφάλεια πληροφοριακών συστημάτων συνδέεται με τεχνικές, διαδικασίες, διοικητικά μέτρα και με ηθικές - κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή, τυχαία ή σκόπιμη. Στηρίζεται σε τρεις βασικές ιδέες, την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα

Οι κωδικοί πρόσβασης είναι ο πλέον διαδεδομένος τρόπος προστασίας δεδομένων. Είναι απλοϊκή η δημιουργία τους και εύκολη η χρήση τους, αλλά λιγότερο ασφαλείς και αποτελεσματικοί από τις υπόλοιπες μεθόδους, καθώς η παραβίασή τους είναι πλέον εύκολη διαδικασία.

Η αναγνώριση προσώπου, η σάρωση δακτυλικού αποτυπώματος, φωνής, χεριού, ίριδας, υπογραφής, είναι μερικές από τις βιομετρικές τεχνικές οι οποίες αποτελούν τις πιο αξιόπιστες μεθόδους προστασίας δεδομένων και εφαρμογών ασφαλείας.

Η χρήση λογισμικού ασφαλείας αποτελείται από τρεις μεθόδους: τη χρήση λογισμικών antivirus, τα firewalls και την κρυπτογραφία.

Η έρευνα για την εξιχνίαση ηλεκτρονικών εγκλημάτων αποτελεί μια δύσκολη και χρονοβόρα διαδικασία, με στόχο τον εντοπισμό των ηλεκτρονικών ιχνών του δράστη. Τέτοια μέσα είναι: ο εντοπισμός IP, οι συναγερμοί, οι προειδοποιήσεις, οι αναφορές, τα αρχεία καταγραφής, τα emails και τα honeypots.

Η εύκολη πρόσβαση στο διαδίκτυο, καθώς υπήρξε τάχιστη εξέλιξη της τεχνολογίας, καθιστά αναγκαία τη δημιουργία νομικών κυρώσεων που να καταστέλλουν την εγκληματική δραστηριότητα στο διαδίκτυο.

Όποιος παραβαίνει με οποιονδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρησης του απορρήτου δεδομένων που

μεταβιβάζονται μέσω διαδικτύου, τιμωρείται με ποινή φυλάκισης και χρηματική ποινή, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις.

Απαιτείται η υιοθέτηση μέτρων σχετικών με τον πραγματικό χρόνο συλλογής διακινούμενων δεδομένων, τα οποία θα επιτρέπουν στις αρμόδιες αρχές να συγκεντρώνουν ή να αντιγράφουν δεδομένα περιεχομένου σε πραγματικό χρόνο, συγκεκριμένων επικοινωνιών που μεταφέρονται μέσω πληροφοριακού συστήματος.

Το γεγονός ότι το έγκλημα στον κυβερνοχώρο αποτελεί μία νέα μορφή εγκλήματος προκαλεί δυσχέρεια σε αυτόν που ασχολείται με τη νομική πλευρά του θέματος από ποινική άποψη αφού υπάρχει έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική

Βαφόπουλος, Μ., (2012). Αλλάζοντας (με) το Διαδίκτυο. Αλλά Προσοχή στις κακοτοπιές. Σε Τσορμπατζούδης, Χ., Λαζούρας, Λ. & Μπαρκούκης, Β., 2012. Κυβερνοεκφοβισμός στην Ελλάδα: Μια διεπιστημονική προσέγγιση. Αριστοτέλειο πανεπιστήμιο Θεσσαλονίκης – Ευρωπαϊκό Πρόγραμμα DAPHNE III .

Βλαχόπουλος, Κ. (2007). Ηλεκτρονικό έγκλημα Μορφές, πρόληψη, αντιμετώπιση. Αθήνα: Εκδόσεις Νομική Βιβλιοθήκη.

Γρηγοράκη, Μ., Περάκη, Φ. & Πολίτη Α., (2014). Ηλεκτρονικός εκφοβισμός στην παιδική και εφηβική ηλικία: διερευνώντας το φαινόμενο όπως εκδηλώνεται στα μέσα κοινωνικής δικτύωσης. Πανελλήνιο Συνέδριο Επιστημών Εκπαίδευσης.

Καλογήρου, Γ. (2015). Κοινωνία της Πληροφορικής και Οικονομία της Γνωσης. Αθήνα: Εκδόσεις Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών Εθνικό Μετσόβιο Πολυτεχνείο.

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

Mcclure, S., Scambray, J. & Kurtz, G. (2009). Ασφάλεια Δικτύων. Αθήνα: Εκδόσεις Γκιούρδας.

Σουρής, Α. Πατσός, Δ. & Γρηγοριάδης, Ν. (2004). Ασφάλεια της Πληροφορίας. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Τσουραμάνης, Χ. (1996). Οικονομική Παραβατικότητα. Αθήνα: Εκδόσεις Έλλην.

Τσουραμάνης, Χ. (2005). Ψηφιακή Εγκληματικότητα. Η α(να)σφαλής όψη του διαδικτύου. Αθήνα: Εκδόσεις Κατσαρός Βασ. Ν.

Τσουραμάνης, Χ. (2006). Κυβερνοέγκλημα. Αθήνα: Εκδόσεις Παπαζήση.

Ξενόγλωσση

Barrett, N. (1997). Digital crime: policing the cybernation. Kogan Page.

Blake, K. W., Converse, V. K., Edmark, R. O. N., & Garrison, J. M. (2008). U.S. Patent No. 7,412,723. Washington, DC: U.S. Patent and Trademark Office.

Clarke, R.V. and Newman, G. (2003) 'Modifying criminogenic products: what role for government?', in R.V. Clarke and G. Newman (eds) Designing out Crime from Products and Systems. Crime Prevention Studies. Vol. 18. Monsey, NY: Criminal Justice Press.

Council of Europe. Octopus Programme. (2005). Organised crime in Europe: the threat of cybercrime: situation report 2004. Council of Europe.

Forester, T., & Morrison, P. (1994). Computer ethics: cautionary tales and ethical dilemmas in computing. Mit Press.

Pipkin, D. L. (2003). Halting the hacker: A practical guide to computer security. Prentice Hall Professional.

Willard, N. (2007). Cyberbullying and Cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Champaign, IL: Research Press.

Ηλεκτρονική

ΑΔΑΕ – Παρουσίαση. Διαθέσιμο στο: http://www.adae.gr/i-adae/paroysiasi/.

ΑΔΑΕ - Αυτοτελές Τμήμα Ελέγχου Άρσης του Απορρήτου. Διαθέσιμο στο: http://www.adae.gr/i-adae/organogramma/arsi-toy-aporritoy/.

Απόφαση 165/2011. Διαθέσιμο στο: http://www.adae.gr/fileadmin/docs/KANONISMOS_165.2011.pdf.

Άρθρο 13 - Ποινικός Κώδικας - Έννοια όρων του Κώδικα. Διαθέσιμο στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-13-poinikos-kodikas-ennoia-oron-toy-kodika.

Archive for the "Μορφές ηλεκτρονικού εγκλήματος" Category. Παιδική Πορνογραφία. Διαθέσιμο στο: https://electroniccrime.wordpress.com/category/%CE%BC%CE%BF%CF%81%CF%86%CE%AD%CF%82-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%8D-%CE%B5%CE%B3%CE%BA%CE%BB%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82/.

Αστυνομία. Ποιες μορφές διαδικτυακής απάτης συναντώνται συχνότερα; Διαθέσιμο στο: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=3686EN.

Ασφάλεια. Forthnet. Διαθέσιμο στο: http://www.forthnet.gr/Article.aspx?a_id=4393#sthash.iEqIymOH.dpbs.

Ασφαλείς Υπηρεσίες και Συναλλαγές σε Περιβάλλοντα Κινητού Εμπορίου. Διαθέσιμο στο: https://repository.kallipos.gr/bitstream/11419/2295/1/02_chapter_07.pdf.

Belsey, B., 2004. Cyberbullying: An Emerging Threat to the "Always On" Generation. Διαθέσιμο στο: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.

Cyber Crime. Κινητοποιήσεις Ευρωπαϊκής Ένωσης σχετικά με το Ηλεκτρονικό Έγκλημα. Διαθέσιμο στο: https://electroniccrime.wordpress.com/.

Details of Treaty No.185. Convention on Cybercrime. Διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Ελληνική Αστυνομία. Αστυνομική Ανασκόπηση. Διαθέσιμο στο: https://www.policemagazine.gr/sites/default/files/pdf/%CE%95%CE%91_2011-06-0267.pdf.

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. Διαθέσιμο στο: http://www.echr.coe.int/Documents/Convention_ELL.pdf.

Η Κομισιόν εξετάζει το νομικό πλαίσιο για την πάταξη της ρητορικής μίσους στο διαδίκτυο. Διαθέσιμο στο: http://www.huffingtonpost.gr/2017/04/23/diethnes-tech-media-h-komision-eksetazei-to-nomiko-plaisio-gia-thn-pataksi-ths-ritorikis-misous-sto-diadiktyo_n_16186190.html.

Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα. Διαθέσιμο στο: https://repository.kallipos.gr/bitstream/11419/1037/1/05_chapter_13.pdf.

Κέντρο διεθνών στρατηγικών αναλύσεων. Κυβερνοχώρος- Κυβερνοεπιθέσεις-Κυβερνοάμυνα. Διαθέσιμο στο: https://kedisa.gr/kybernoxwros-kybernoepitheseis-kybernoamyna-meros-2o-kakoboula-programmata-texnikes-epithesewn/.

Lawspot. Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (ελληνικά). Διαθέσιμο στο: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0.

Microsoft. Προστασία του υπολογιστή μου από ιούς. Διαθέσιμο στο: https://support.microsoft.com/el-gr/help/17228/windows-protect-my-pc-from-viruses.

Νέες τεχνολογίες και έγκλημα. Θεώνη Γ. Σπαθή. Διαθέσιμο στο: http://www.indeepanalysis.gr/nomika-themata/nees-technologies-kai-egklhma.

Νομικά επίλεκτα. Phishing. Διαθέσιμο στο: http://www.nomika-epilekta.gr/arthra/koinonika-arthra/phishing-and-pharming.

Νόμος 2867/2000 - ΦΕΚ 273/Α/19-12-2000. Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις. Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-2867-2000.html.

Νόμος 4411/2016 Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξει. Διαθέσιμο στο: https://www.taxheaven.gr/laws/law/index/law/766.

Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=LEGISSUM:l33193&from=EL.

Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις. Διαθέσιμο στο: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32014L0041.

Παγκόσμια μελέτη λογισμικού 2016 της BSA. Διαθέσιμο στο: http://www.bsa.org/?sc_lang=el-GR.

Πανεπιστήμιο Πειραιώς. Η επίδραση του διαδικτύου στα κοινωνικά κινήματα. Διαθέσιμο στο: http://voidnetwork.gr/wp-content/uploads/2016/09/.

Συνήγορος του καταναλωτή. Τί πρέπει να γνωρίζουν οι καταναλωτές για την προστασία τους από το ηλεκτρονικό έγκλημα. Διαθέσιμο στο: http://www.synigoroskatanaloti.gr/docs/info/info-Hlektroniko-Egklima.pdf.

Stopbullying.gov, 2017. What is Cyberbylllying. Διαθέσιμο στο: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html.

ΤΕΙ Κεντρικής Μακεδονίας. Firewalls. Διαθέσιμο στο: http://teachers.teicm.gr/politis/Firewalls_Riverbed.pdf.

Τράπεζα Πληροφοριών Νομοθεσίας. Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016. Διαθέσιμο στο: https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4411-2016.html.

What's the Difference Between Viruses, Trojans, Worms, and Other Malware? Διαθέσιμο στο. https://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware.