ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ – ΤΟΜΕΑΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ – ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: ΣΥΓΧΡΟΝΗ ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΝΕΕΣ ΜΟΡΦΕΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

ΒΑΣΙΛΕΙΟΣ ΤΑΞΟΠΟΥΛΟΣ
ΑΡΙΘΜΟΣ ΜΗΤΡΩΟΥ: 3214Μ004

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ: ΚΑΘΗΓΗΤΡΙΑ ΑΝΘΟΖΩΗ ΧΑΪΔΟΥ (ΕΠΙΒΛΕΠΟΥΣΑ)
ΚΑΘΗΓΗΤΡΙΑ ΧΡΙΣΤΙΝΑ ΖΑΡΑΦΩΝΙΤΟΥ (ΜΕΛΟΣ)
ΚΑΘΗΓΗΤΗΣ ΓΡΗΓΟΡΗΣ ΛΑΖΟΣ (ΜΕΛΟΣ)

ΑΘΗΝΑ 2016

Περιεχόμενα

Περίληψη

Η σύγχρονη τεχνολογία είναι αναπόσπαστο κομμάτι της ανθρώπινης καθημερινότητας, αλλά χρησιμοποιείται διαφορετικά από τον καθένα. Στο πλαίσιο της χρήσης της σύγχρονης τεχνολογίας παραδοσιακά εγκλήματα μπορούν να τελεστούν με νέα μέσα και εντελώς νέες μορφές εγκλημάτων να κάνουν την εμφάνισή τους. Ως επακόλουθο των εξελίξεων στην εγκληματικότητα εμφανίζονται νέοι νόμοι, για να τις συμπεριλάβουν. Ιδιαίτερο ρόλο στην τέλεση της εγκληματικότητας παίζουν οι υπολογιστές και μαζί με αυτούς και το διαδίκτυο, καθώς ένα μεγάλο μέρος των εγκλημάτων που τελούνται με νέα μέσα, πλέον, τελείται μέσω διαδικτύου. Εντός του κυβερνοχώρου μεγάλο μέρος της εγκληματικότητας εντοπίζεται στον Βαθύ Ιστό, ο οποίος είναι προσβάσιμος μέσα από κατάλληλα εργαλεία ανωνυμοποίησης. Στον Εμφανή Ιστό, που είναι διαθέσιμος από όλους τους χρήστες του διαδικτύου, σημαντικό ρόλο παίζουν και τα κοινωνικά δίκτυα, όπου μπορούν να προσεγγιστούν τα θύματα ευκολότερα. Βεβαίως, τα θύματα μπορούν να προσεγγιστούν και μέσω ενός e-mail ή ενός μηνύματος ή μέσω διαφόρων μηχανισμών παρακολούθησης. Γενικότερα οι δράστες για την απόκτηση οικονομικού οφέλους μπορούν να τελέσουν απάτες εκμεταλλευόμενοι και τεχνολογικά μέσα, όπως οι κάρτες και τα ATM. Ακόμη, οι αστυνομικές αρχές μπορούν να εκμεταλλευτούν τις ίδιες τεχνολογίες με τους δράστες και μέσα από διάφορες επιχειρήσεις να οδηγηθούν στη σύλληψή τους. Από τα πιο διαδεδομένα εγκλήματα που έκαναν την εμφάνισή τους εξαιτίας της αποκλειστικής χρήσης της σύγχρονης τεχνολογίας είναι το hacking, το κακόβουλο λογισμικό και η ψηφιακή πειρατεία. Η κουλτούρα των hackers διέπεται από αξίες και κανόνες. Το κακόβουλο λογισμικό μπορεί να είναι ιδιαίτερα καταστροφικό για τη συσκευή που έχει μολύνει και για τα αποθηκευμένα σε αυτήν αρχεία και προγράμματα. Αντικείμενα ψηφιακής πειρατείας

μπορούν να αποτελέσουν διάφορα μέσα που προστατεύονται από τους νόμους προστασίας πνευματικών δικαιωμάτων. Πιο διαδεδομένη μορφή ψηφιακής πειρατείας είναι η πειρατεία λογισμικού με το φαινόμενο αυτό να υπάρχει σε μεγάλο ποσοστό παγκοσμίως.

Λέξεις-κλειδιά: σύγχρονη τεχνολογία, ηλεκτρονικό έγκλημα, Βαθύς Ιστός, hacking, κακόβουλο λογισμικό, ψηφιακή πειρατεία

Πρόλογος – Εισαγωγικές παρατηρήσεις

Η τεχνολογία έχει εισχωρήσει για τα καλά στην ανθρώπινη καθημερινότητα και είναι πλέον αναπόσπαστο κομμάτι της. Ο τρόπος με τον οποίο τη χρησιμοποιεί ο καθένας είναι διαφορετικός. Τι μπορεί να οριστεί, όμως, ως τεχνολογία και κατ' επέκταση ως σύγχρονη τεχνολογία; Σύμφωνα με το «Λεξικό της νέας ελληνικής γλώσσας» ως τεχνολογία ορίζεται «1. ο τομέας της γνώσης που ασχολείται με την εφαρμοσμένη επιστήμη, τις εφευρέσεις, την ανάπτυξη και πρακτική αξιοποίηση επιστημονικών γνώσεων και μεθόδων, κυρίως στους χώρους της μηχανικής, της βιομηχανίας κλπ., 2. το σύνολο των επιτευγμάτων (εφευρέσεων, διαδικασιών, μεθόδων κ.λπ.) που προκύπτουν μέσω της εφαρμογής επιστημονικών ή τεχνικών γνώσεων για πρακτικούς σκοπούς, καθώς και καθένα από τα παραπάνω επιτεύγματα, 3. το σύνολο των τρόπων με τους οποίους μια κοινωνία εξασφαλίζει τα υλικά αγαθά του πολιτισμού της»[1]. Η σύγχρονη τεχνολογία θα μπορούσε να οριστεί απλώς ως η εξέλιξη της παλαιότερης τεχνολογίας[2]. Συγκεκριμένα θα μπορούσαμε να πούμε ότι η σύγχρονη τεχνολογία αποτελεί το σύνολο των νεότερων επιτευγμάτων μέσα από την εφαρμογή πρόσφατων επιστημονικών ή τεχνικών γνώσεων. Αυτές οι νεότερες επιστημονικές και τεχνικές γνώσεις έχουν οδηγήσει σε ακόμα πιο καινοτόμες εφευρέσεις και διαδικασίες στον τομέα της τεχνολογίας, από τις οποίες αρκετές αποτελούν εξέλιξη των παλαιότερων, ενώ κάποιες άλλες είναι μοναδικές. Παράδειγμα θα μπορούσαν να αποτελέσουν τα smartphones, το live streaming μέσω διαδικτύου, τα tablets και πολλά άλλα. Σε κάθε εποχή κάποιο διαφορετικό τεχνολογικό επίτευγμα μπορεί να θεωρηθεί ως σύγχρονη τεχνολογία. Στη δική μας εποχή θα μπορούσαμε να πούμε πως ως σύγχρονη τεχνολογία

1 Γεώργιος Μπαμπινιώτης 2002, «τεχνολογία», 1760.
2 Karehka Ramey 2012 (http://www.useoftechnology.com/modern-technology-advantages-disadvantages/).

μπορούν να θεωρηθούν οι τεχνολογικές εξελίξεις από τη δεκαετία του ’90 μέχρι σήμερα.

Δεν είναι λίγες οι φορές που η τεχνολογία χρησιμοποιείται για αθέμιτους σκοπούς με αποτέλεσμα την εμφάνιση νέων μορφών εγκληματικότητας. Ως εγκληματικότητα ορίζεται το σύνολο των διαπραττόμενων εγκλημάτων σε κάποια κοινωνική ομάδα που είναι ορισμένη τοπικά και χρονικά[3]. Τι είναι, όμως έγκλημα; Κατά τον Ποινικό Κώδικα αποτελεί «μία πράξη άδικη και καταλογιστή στο δράστη της, η οποία τιμωρείται από το νόμο»[4]. Το έγκλημα αποτελεί την πιο βαριά μορφή παρέκκλισης και προσβάλλει τις αξίες οι οποίες είναι θεμελιώδεις για τη συνέχιση της ύπαρξης μιας κοινωνίας με βάση τις επικρατούσες κοινωνικές και πολιτικές αντιλήψεις και εξαιτίας αυτού η κοινωνία επιζητά να επιβληθούν κυρώσεις, οι οποίες θίγουν σοβαρά ακόμα και σοβαρά αγαθά του δράστη[5]. Για το έγκλημα ο Émile Durkheim αναφέρει ότι παρατηρείται σε όλες τις κοινωνίες όλων των τύπων και ότι μπορεί να αλλάζει μορφή και να μην είναι παντού ίδιες οι πράξεις που χαρακτηρίζονται ως εγκληματικές Επειδή δεν μπορεί να υπάρξει κοινωνία πλήρως απαλλαγμένη από το έγκλημα, αυτό θεωρείται ομαλό, ενώ είναι και χρήσιμο, επειδή έχει κάποια σύνδεση με τις βασικές προϋποθέσεις της κάθε κοινωνικής ζωής, οι οποίες είναι απαραίτητες για την ομαλή εξέλιξη του δικαίου και της ηθικής[6].

Το έγκλημα, λοιπόν, παρατηρείται σε όλες τις κοινωνίες και ανεξαρτήτως περιστάσεων. Με την πάροδο του χρόνου οι οποιεσδήποτε αλλαγές που συντελούνται σε μια κοινωνία επηρεάζουν και το έγκλημα. Μπορεί κάποιες συμπεριφορές να σταματήσουν να νοούνται ως εγκλήματα, να εμφανιστούν νέες μορφές ή οι παλαιότερες να τελούνται με νέα μέσα. Σε αυτό το σημείο μπορούμε να μιλήσουμε για τη συμβολή της

3 Στέργιος Αλεξιάδης, 2011, 115.
4 Άρθρο 14 §1 ΠΚ.
5 Αλίκη Γιωτοπούλου-Μαραγκοπούλου 1984, 39-41.
6 Émile Durkheim 1895 (έκδοση 1978), 130-131, 134.

τεχνολογίας στην εξέλιξη του εγκληματικού φαινομένου και πλέον στις μέρες μας γίνεται λόγος για ηλεκτρονικό έγκλημα. Η Δίωξη Ηλεκτρονικού Εγκλήματος ορίζει το ηλεκτρονικό έγκλημα ως τις «αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία»[7]. Το ηλεκτρονικό έγκλημα μπορεί να χωριστεί σε δύο βασικές κατηγορίες. Η πρώτη αφορά τα γνήσια ηλεκτρονικά εγκλήματα, τα οποία δεν υπήρχαν πριν την εμφάνιση των υπολογιστών και των δικτύων, και τα εγκλήματα τα οποία προϋπήρχαν των υπολογιστών και των δικτύων και πλέον τελούνται και μέσω αυτών[8]. Στα αγγλικά υπάρχουν διάφοροι όροι είτε πιο γενικοί είτε πιο συγκεκριμένοι που μπορούν να περιγράψουν τα εγκλήματα που τελούνται με τεχνολογικά μέσα, όπως οι όροι "electronic crime" ή "e-crime", "cybercrime", "computer crime"[9], "hi-tech crime", "technocrime" κλπ., και συναντώνται με διάφορες αποδόσεις στη βιβλιογραφία. Ο όρος "technocrime", που αποδίδεται κατά λέξη ως «τεχνολογικό έγκλημα», είναι ο πιο γενικός από τους παραπάνω όρους, καθώς περιγράφει γενικά το έγκλημα που τελείται με τεχνολογικά μέσα[10].

Διαχρονικά διαπιστώνεται ότι καθώς εξελίσσεται η τεχνολογία εξελίσσεται και το έγκλημα. Ήδη από τις αρχές του 20ού αιώνα εμφανίστηκαν νέοι για την εποχή τρόποι και τεχνικές για τη διάπραξη εγκλημάτων. Ξεκίνησε η χρήση του τηλεφώνου για τη διάπραξη απατών, η διάπραξη κλοπών και ληστειών διευκολύνθηκε με τα μεταφορικά μέσα, ενώ μέσω της χρήσης και άλλων τεχνολογικών μέσων επήλθε μια αρχική δια-

7 Κωνσταντίνος Γ. Κούρος, χ.χ. (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414).

8 Κωνσταντίνος Βλαχόπουλος 2007, 39.

9 Η διαφορά μεταξύ των όρων «κυβερνοέργκλημα» (cybercrime) και «πληροφορικό έγκλημα» (computer crime) έγκειται στο γεγονός πως το πληροφορικό έγκλημα ορίζεται γενικά ως το έγκλημα που τελείται μέσω υπολογιστή, ενώ το κυβερνοέγκλημα αναφέρεται ευρέως στο έγκλημα που τελείται με υπολογιστή και με τη χρήση της τεχνολογίας δικτύων. (Tom Forester & Perry Morrison 1994, 29-30. David Wall 2001, 2. David Wall 2008, 862-863).

10 Λεπτομερέστερη καταγραφή για το τι περιλαμβάνει το τεχνολογικό έγκλημα στο Stéphane Leman-Langlois 2008, 1.

φοροποίηση στον τρόπο διάπραξης των εγκλημάτων[11].

Η εμφάνιση και η ανάπτυξη των υπολογιστών συνετέλεσε σε αλλαγές αναφορικά με την τέλεση εγκλημάτων. Οι εγκληματικές απειλές, πλέον, στηρίζονται σε μια πιο περίπλοκη τεχνολογία και τα φυσικά όρια καταργούνται. Ο υπολογιστής και άλλες παρόμοιες συσκευές ηλεκτρονικής επεξεργασίας δεδομένων διαδραματίζουν κυρίαρχο ρόλο στο ηλεκτρονικό έγκλημα. Αναζητώντας τις ρίζες του ηλεκτρονικού εγκλήματος, βλέπουμε πως ταυτόχρονα με την εμφάνιση των υπολογιστών έκαναν την εμφάνισή τους και οι επίδοξοι «ηλεκτρονικοί εγκληματίες» προσπαθώντας να βρουν τρόπους να εκμεταλλευτούν αυτές τις νέες τεχνολογίες για τον προσπορισμού οφέλους είτε για τους ίδιους είτε για τρίτους. Στον τομέα του ηλεκτρονικού εγκλήματος η μεγάλη επανάσταση επήλθε με την εμφάνιση των δικτύων, τα οποία δημιούργησαν νέες διόδους για την πρόσβαση στην πληροφορία και κατέστησαν μη αναγκαία τη φυσική παρουσία του επιτιθέμενου στο χώρο φύλαξης της πληροφορίας[12].

Το διαδίκτυο αποτελεί σημαντικό εργαλείο στη διάπραξη εγκλημάτων, είτε νέων είτε παραδοσιακών. Το έγκλημα στο διαδίκτυο λαμβάνει μορφές όπως η παράνομη πρόσβαση σε δεδομένα, η παράνομη οργάνωση και συμμετοχή σε τυχερά παιχνίδια, η διακίνηση ναρκωτικών ουσιών κλπ[13]. Στα πλαίσια του Παγκόσμιου Ιστού (World Wide Web) ένα μεγάλο μέρος της εγκληματικότητας εντοπίζεται σε ιστοτόπους του Βαθέως Ιστού, στον οποίο η πρόσβαση γίνεται με συγκεκριμένα εργαλεία. Ο Βαθύς Ιστός διαθέτει σελίδες οι οποίες δεν είναι διαθέσιμες μέσα από τις τυπικές μηχανές αναζήτησης. Σε μελέτη που έγινε το 2000 από τον Michael K. Bergman βρέθηκε ότι το μέγεθος των πληροφοριών του Βαθέως Ιστού είναι 400 με 550 φορές μεγαλύτερο από το αντίστοιχο του Εμφανούς Ιστού. Τα υπόλοιπα ευρήματα για το μέγεθος λένε πως στον

11 Κωνσταντίνος Βλαχόπουλος 2007, 7.

12 Το ίδιο, 7-9.

13 Περισσότερες μορφές εγκλημάτων στο διαδίκτυο βλ. Ιάκωβος Φαρσεδάκης 2009 (http://criminology.panteion.gr/attachments/article/386/j farsedakis κυβερνοχώρος.pdf).

Βαθύ Ιστό περιέχονται 7500 terabytes πληροφοριών σε σύγκριση με τα μόλις 19 του Εμφανούς Ιστού και 550 δισεκατομμύρια ιδιωτικά έγγραφα σε σχέση με το 1 δισεκατομμύριο που υπάρχει στον Εμφανή Ιστό, υπάρχουν πάνω από 200.000 ιστότοποι με τους 60 μεγαλύτερους να περιέχουν 750 terabytes πληροφοριών. Παράλληλα, οι ιστότοποι του Βαθέως Ιστού λαμβάνουν κατά μέσο όρο 50% μεγαλύτερη μηνιαία κίνηση από τους ιστοτόπους του Εμφανούς Ιστού και τείνουν να είναι πιο περιορισμένου περιεχομένου. Ο Βαθύς Ιστός είναι η μεγαλύτερη αναπτυσσόμενη κατηγορία πληροφοριών μέσα στο διαδίκτυο και το συνολικό ποιοτικό του περιεχόμενο είναι 1000 με 2000 φορές μεγαλύτερο από το περιεχόμενο του Εμφανούς Ιστού. Το περιεχόμενο του Βαθέως Ιστού είναι σε μεγάλο βαθμό συναφές με κάθε ανάγκη πληροφόρησης, αγορά και αρμοδιότητα και παραπάνω από το μισό του Βαθέως Ιστού υπάρχει σε βάσεις δεδομένων για συγκεκριμένα θέματα. Τέλος, το 95% των πληροφοριών εντός του Βαθέως Ιστού είναι δημοσίως διαθέσιμο και δεν απαιτείται κάποια εγγραφή ή πληρωμή[14].

Οι τεχνολογικές εξελίξεις δεν θα μπορούσαν να αφήσουν ανεπηρέαστο τον τομέα της πρόληψης και της αντιμετώπισης των εγκλημάτων. Έχουμε την εμφάνιση νέων τεχνολογιών για την προστασία από τα εγκλήματα και, παράλληλα, κάνουν την εμφάνισή τους νέοι νόμοι, οι οποίοι περιλαμβάνουν τις νέες μορφές εγκληματικότητας, ενώ και οι αστυνομικές αρχές έχουν προσπαθήσει να προσαρμοστούν στα νέα τεχνολογικά δεδομένα με την ίδρυση συγκεκριμένων τομέων που ασχολούνται αποκλειστικά με το έγκλημα που τελείται με τεχνολογικά μέσα. Παράδειγμα μπορεί να αποτελέσει η Δίωξη Ηλεκτρονικού Εγκλήματος, η οποία έχει ως αποστολή «την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας»[15]. Σε διεθνές επίπεδο υπάρχει το European Cybercrime Center (EC3), το οποίο αποτελεί υ-

14 Michael K. Bergman 2001, 1.

15 «Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος», χ.χ. (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194).

πηρεσία της Europol και επικεντρώνεται σε τρεις βασικούς τομείς. Επικεντρώνεται, πρώτον, στα κυβερνοεγκλήματα που τελούνται από οργανωμένες ομάδες και, πιο συγκεκριμένα, σε αυτά που έχουν στόχο την αποκόμιση μεγάλου κέρδους, όπως οι διαδικτυακές απάτες, δεύτερον, στα κυβερνοεγκλήματα που προξενούν σοβαρή βλάβη στο θύμα, όπως η διαδικτυακή σεξουαλική εκμετάλλευση παιδιών, και, τρίτον, στα κυβερνοεγκλήματα που πλήττουν σημαντικές υποδομές και συστήματα πληροφοριών στην Ευρωπαϊκή Ένωση[16].

Η εγκληματολογία ακολούθησε και εκείνη τα νέα τεχνολογικά δεδομένα και δημιουργήθηκε η κατεύθυνση της ψηφιακής ή υπολογιστικής εγκληματολογίας (digital ή computational criminology). Η κατεύθυνση αυτή είναι διεπιστημονική με την έννοια ότι, αφενός, χρησιμοποιεί γνώσεις από την πληροφορική και τα εφαρμοσμένα μαθηματικά (π.χ. αλγορίθμους ή πληροφοριακά συστήματα) και, αφετέρου, χρησιμοποιεί γνώσεις από την εγκληματολογία. Μέσω των προαναφερθέντων η ψηφιακή εγκληματολογία ορίζει εγκληματολογικές έννοιες, συμβάλλει στο να κατανοηθούν σύνθετα εγκληματικά φαινόμενα και προτείνει λύσεις (π.χ. κατασκευή λογισμικού για την πρόληψη των ηλεκτρονικών εγκλημάτων). Η ψηφιακή εγκληματολογία μπορεί να εφαρμοστεί στην περιβαλλοντική εγκληματολογία, στις κλοπές ατομικής ταυτότητας ή αριθμών πιστωτικών καρτών κλπ[17].

Στην παρούσα εργασία θα μας απασχολήσει το θέμα της σύγχρονης τεχνολογίας και της σχέσης της με τις νέες μορφές εγκληματικότητας. Στα περιορισμένα πλαίσια μιας διπλωματικής εργασίας η έμφαση δίνεται στο ηλεκτρονικό έγκλημα, και περισσότερο στο έγκλημα που τελείται με τη βοήθεια του διαδικτύου, το οποίο εξάλλου αποτελεί και το κύριο πεδίο της εγκληματικότητας με τη χρήση της σύγχρονης τεχνολογίας. Το προϋπάρχον ενδιαφέρον αναφορικά με τη μελέτη του εγκλήματος που τε-

16 “Combating cybercrime in a digital age”, χ.χ. (https://www.europol.europa.eu/ec3).
17 Καλλιόπη Δ. Σπινέλλη 2014, 69.

λείται με σύγχρονα τεχνολογικά μέσα συντέλεσε στην επιλογή του θέματος. Η μεθοδολογία που θα ακολουθηθεί είναι η δευτερογενής ανάλυση.

Το πρώτο μέρος της εργασίας αφορά ορισμένες θεωρητικές προσεγγίσεις. Αναφέρονται, αρχικά, προσεγγίσεις για την τεχνολογία, στη συνέχεια, τα εγκλήματα του λευκού κολάρου, περιλαμβάνοντας τα βασικά σημεία της θεωρίας του Sutherland μαζί με κάποιες νεότερες προσεγγίσεις, και, τέλος, τα βασικά σημεία της θεωρίας της ορθολογικής επιλογής των Cornish & Clarke, καθώς και προσεγγίσεις σχετικές με τον κοινωνικό έλεγχο.

Το δεύτερο μέρος της εργασίας αφορά τις νέες μορφές εγκληματικότητας. Αφού αποσαφηνιστεί η έννοια των νέων μορφών εγκληματικότητας και αφού αναφερθούν ενδεικτικά κάποιες εξελίξεις σε νομοθετικό επίπεδο, θα παρατεθούν προβληματισμοί σχετικά με τα παραδοσιακά εγκλήματα που τελούνται με τη βοήθεια της τεχνολογίας και τα εγκλήματα που προκύπτουν αποκλειστικά από τη χρήση της σύγχρονης τεχνολογίας. Στο κεφάλαιο που αφορά τα παραδοσιακά εγκλήματα θα γίνει αναφορά στην εγκληματική δραστηριότητα που εντοπίζεται στον Βαθύ Ιστό και στην εγκληματική δραστηριότητα που τελείται με άλλα τεχνολογικά μέσα δίνοντας μια ιδιαίτερη έμφαση στο έγκλημα της απάτης. Επίσης, θα συμπεριληφθούν και κάποιες πρόσφατες αστυνομικές δράσεις που λήφθηκαν στο πλαίσιο αυτών των τεχνολογιών.

Στο δεύτερο κεφάλαιο του δεύτερου μέρους θα αναφερθούν ορισμένα από τα κυριότερα εγκλήματα που οφείλουν την εμφάνισή τους αποκλειστικά στη χρήση της σύγχρονης τεχνολογίας. Τέτοια εγκλήματα, μεταξύ άλλων, είναι και το hacking και το κακόβουλο λογισμικό και η ψηφιακή πειρατεία. Στα κεφάλαια που αφορούν αυτά τα εγκλήματα θα αναφερθεί από μία περίπτωση, ενώ στο κακόβουλο θα αναφερθούν ξεχωριστές περιπτώσεις για τις τρεις βασικότερες μορφές. Στο κεφάλαιο για το hacking θα αναλυθεί ο όρος “hacker”, η κουλτούρα των hackers, οι τεχνικές που χρησιμοποι-

ούν και το νομοθετικό πλαίσιο. Στο κεφάλαιο για το κακόβουλο λογισμικό εκτός από τις τρεις βασικότερες μορφές του, γίνεται αναφορά σε κάποιες ακόμα μορφές, σε μεθόδους μόλυνσης και στη νομική και τεχνολογική αντιμετώπισή του. Στο κεφάλαιο για την ψηφιακή πειρατεία θα περιληφθούν ο ορισμός και η τυπολογία του φαινομένου, τα επιχειρήματα τα οποία έχουν διατυπωθεί σχετικά, οι έρευνες που αναφέρουν την έκταση που καταλαμβάνει η πειρατεία λογισμικού σε παγκόσμιο επίπεδο και ορισμένες νομοθετικές ρυθμίσεις. Και στα κεφάλαια με τα εγκλήματα που προκύπτουν από τη χρήση της τεχνολογίας η αναφορά στις όποιες νομοθεσίες που παρατίθενται είναι ενδεικτική και όχι εξαντλητική.

Τα ερωτήματα στα οποία θα προσπαθήσουμε να απαντήσουμε στην εργασία και τα οποία θα μας βοηθήσουν στην εξαγωγή συμπερασμάτων, που θα παρατεθούν στο τέλος της εργασίας, είναι τα ακόλουθα:

1. Η τεχνολογία πληροφοριών και τηλεπικοινωνιών μπορεί να αποτελέσει πρόσφορο πεδίο για την ανάπτυξη νέων μορφών εγκληματικότητας;
2. Οι αλλαγές στη νομοθεσία προκλήθηκαν εξαιτίας των αλλαγών που επέφερε η τεχνολογική ανάπτυξη στη διάπραξη εγκλημάτων;
3. Οι τεχνολογικές εξελίξεις συμβάλλουν στην ανάπτυξη μέσων και δράσεων εναντίον των νέων μορφών εγκληματικότητας;
4. Το εύρος της οικονομικής ζημίας από τις απάτες που τελούνται με νέα μέσα είναι μεγαλύτερο από τις αντίστοιχες παραδοσιακές;

1. Θεωρητικές προσεγγίσεις

Ένας τρόπος προσέγγισης της τεχνολογίας γίνεται μέσα από την οπτική που αντιλαμβάνεται την τεχνολογική καινοτομία ως κάτι εγγενώς προοδευτικό. Το επιχείρημα που μπορεί να αντιταχθεί σε αυτή την οπτική είναι η ανάπτυξη των πυρηνικών όπλων. Μια αντίθετη άποψη αναφέρει πως η τεχνολογία είναι εγγενώς κακή. Αυτή η άποψη έχει λίγους υποστηρικτές, αλλά μπορεί να στηριχθεί περισσότερο αν εφαρμοστεί σε συγκεκριμένους τύπους τεχνολογίας, όπως τα πυρηνικά όπλα. Υπάρχει, βέβαια, και η άποψη που αναφέρει πως η τεχνολογία είναι ουδέτερη και ότι μπορεί εξίσου να χρησιμοποιηθεί και για καλούς και για κακούς σκοπούς. Η αδυναμία αυτής της οπτικής γίνεται εμφανής τονίζοντας το ότι οι τεχνολογίες μπορούν να εξυπηρετήσουν κάποιους σκοπούς ευκολότερα σε σχέση με κάποιους άλλους. Για παράδειγμα, τα όπλα έχουν δημιουργηθεί να σκοτώνουν ή να καταστρέφουν, ενώ οι κουβέρτες έχουν δημιουργηθεί να προσφέρουν ζεστασιά[18]. Την άποψη περί τεχνολογικής ουδετερότητας την απορρίπτει και ο Gary Marx, διότι με αυτή την αντίληψη αγνοείται το γεγονός πως η ανάπτυξη και η εφαρμογή της τεχνολογίας λαμβάνουν χώρα πάντα σε κάποιο κοινωνικό πλαίσιο το οποίο ποτέ δεν είναι ουδέτερο[19].

Οι προηγούμενες οπτικές προσδίδουν κάποιο σημαντικό χαρακτηριστικό στην τεχνολογία. Μια διαφορετική προσέγγιση αποδίδει στην τεχνολογία απλώς μια τάση να εξυπηρετεί συγκεκριμένους σκοπούς. Από αυτήν την οπτική η τεχνολογία μπορεί να εκπληρώσει κάποιους σκοπούς ευκολότερα σε σχέση με κάποιους άλλους, αλλά μπορεί, με μεγαλύτερη ή μικρότερη ευκολία, να χρησιμοποιηθεί γενικά για οποιονδήποτε σκοπό. Αυτή η οπτική μπορεί να ονομαστεί και ως «επιλεκτική χρησιμότητα» (selective usefulness). Για παράδειγμα, το τούβλο μπορεί να χρησιμοποιηθεί για τη δημι-

18 Brian Martin 1999, 537.
19 Ronald Corbett & Gary Marx 1991 (http://web.mit.edu/gtmarx/www/critique.html#technical).

ουργία ενός τοίχου, για να σταματήσει μια πόρτα, σαν σφυρί ή σαν όπλο. Άρα το τούβλο είναι επιλεκτικά χρήσιμο για το χτίσιμο ενός τοίχου[20].

Μία άλλη προσέγγιση αναφέρει πως αντί να πάρουμε την τεχνολογία ως δεδομένη και να κοιτάξουμε τις επιπτώσεις της στην κοινωνία, είναι καλύτερα να μελετήσουμε τους παράγοντες που κάνουν την τεχνολογία αυτή που είναι. Μια άλλη δημοφιλής και δυνατή άποψη για την κατανόηση των νέων τεχνολογιών λέει πως η διαδικασία εισαγωγής τους είναι εκτός του ανθρώπινου ελέγχου. Λέει, δηλαδή, πως όταν η τεχνολογία αναπτυχθεί, δεν μπορεί να σταματήσει. Μια λιγότερο ακραία εκδοχή αναφέρει ότι οι σκέψεις για την αποδοτικότητα και τα οικονομικά καθορίζουν σε μεγάλο βαθμό το σχήμα της τεχνολογίας. Εννοεί, δηλαδή, πως από τη στιγμή που σε κάθε εποχή υπάρχει ένας τρόπος που είναι ο καλύτερος για να γίνει κάτι, τότε έτσι θα γίνει. Αυτή η οπτική ονομάζεται τεχνολογικός ντετερμινισμός[21].

Η τεχνολογία μπορεί να τεθεί και στην υπηρεσία εγκληματιών για τη διάπραξη εγκλημάτων αλλά και στην υπηρεσία του επίσημου κοινωνικού ελέγχου για την καταπολέμηση του εγκλήματος. Για την εξήγηση της εγκληματικής συμπεριφοράς έχουν αναπτυχθεί διάφορες θεωρίες. Μεταξύ αυτών των θεωριών είναι και η θεωρία του λευκού κολάρου και η θεωρία της ορθολογικής επιλογής.

Η θεωρία των εγκλημάτων του λευκού κολάρου αναπτύχθηκε από τον Edwin Sutherland. Ο Sutherland ανέφερε πως τα εγκλήματα του λευκού κολάρου έχουν πιθανόν μεγαλύτερο κόστος από τα εγκλήματα που θεωρούνται ως «εγκληματικό πρόβλημα», ενώ όσο μεγάλη και να είναι η οικονομική απώλεια δεν είναι σημαντικότερη από τη ζημιά που προκαλείται στις κοινωνικές σχέσεις. Παραβιάζεται η εμπιστοσύνη και δημιουργείται δυσπιστία, πράγμα το οποίο χαμηλώνει την κοινωνική ηθική και προκαλεί κοινωνική αποδιοργάνωση σε μεγάλη κλίμακα. Ο ίδιος τη συνόψισε σε πέντε

20 Brian Martin 1999, 537-538.
21 Το ίδιο, 538.

βασικά σημεία ως εξής. Πρώτον, η εγκληματικότητα του λευκού κολάρου αποτελεί πραγματική εγκληματικότητα, που υπάρχει σε όλες τις περιπτώσεις παραβίασης του ποινικού νόμου. Δεύτερον, η εγκληματικότητα του λευκού κολάρου διαφέρει από την εγκληματικότητα της κατώτερης τάξης πρωταρχικά στην εφαρμογή του ποινικού νόμου, ο οποίος διαχωρίζει τους εγκληματίες του λευκού κολάρου διοικητικά από τους υπόλοιπους εγκληματίες. Τρίτον, οι θεωρίες των εγκληματολόγων που λένε ότι το έγκλημα οφείλεται σε κάποιες ψυχοπαθολογικές και κοινωνικοπαθολογικές καταστάσεις που σχετίζονται στατιστικά με τη φτώχεια είναι ανυπόστατες, επειδή αποτελούνται από μη αντιπροσωπευτικά δείγματα που επηρεάζονται σε μεγάλο βαθμό από το κοινωνικοοικονομικό status, δεν εφαρμόζονται στους εγκληματίες του λευκού κολάρου και δεν εξηγούν καν την εγκληματικότητα της κατώτερης τάξης λόγω του ότι οι παράγοντες δεν σχετίζονται με μια γενική διαδικασία χαρακτηριστική για όλα τα είδη εγκληματικότητας. Τέταρτον, χρειάζεται μία θεωρία για την εγκληματική συμπεριφοράς που θα εξηγεί και την εγκληματικότητα της κατώτερης τάξης και την εγκληματικότητα του λευκού κολάρου. Πέμπτον, μία υπόθεση τέτοιας φύσης αποδίδεται με τις έννοιες του διαφορικού συγχρωτισμού και της κοινωνική αποδιοργάνωσης[22].

Η θεωρία του Sutherland εξελίχθηκε από μεταγενέστερους ερευνητές. Οι Clinard και Quinney διέκριναν τα εγκλήματα του λευκού κολάρου σε εγκλήματα εργασίας (occupational crime) και σε εγκλήματα επιχείρησης (corporate crime). Ένας πιο σαφής ορισμός, ωστόσο, δόθηκε από τον Edelhertz ο οποίος ανέφερε πως «μια παράνομη πράξη ή μια σειρά από παράνομες πράξεις που διαπράττονται με μη φυσικά μέσα και μέσω απόκρυψης ή δόλου, για την απόκτηση χρημάτων ή περιουσιακών στοιχείων, την αποφυγή πληρωμών ή απωλειών σε χρήμα ή σε περιουσιακά στοιχεία, ή για την απόκτηση εργασίας ή προσωπικού οφέλους συνιστά έγκλημα λευκού περιλαιμί-

22 Edwin H. Sutherland 1940, 5, 11-12.

ου»[23]. Ο Edelhertz εστίασε περισσότερο με τον ορισμό του στα «μέσα» και στα «κίνητρα» των εγκληματιών και επέκτεινε τον ορισμό πέραν της προβληματικής του Sutherland. Ουσιαστικά είπε ότι τα εγκλήματα του λευκού κολάρου μπορούν να λάβουν χώρα και εκτός επιχείρησης[24].

Ο Donn B. Parker στη μελέτη του για το πληροφορικό έγκλημα ανέφερε ότι η κατάχρηση υπολογιστών περιλαμβάνει το έγκλημα του λευκού κολάρου, το βανδαλισμό και τις φθορές ξένης ιδιοκτησίας. Ο Parker ορίζει το έγκλημα του λευκού κολάρου ως «κάθε προσπάθεια ή πρακτική που περιλαμβάνει την κατάπνιξη της ελεύθερης επιχειρηματικότητας ή την προώθηση του αθέμιτου ανταγωνισμού, τη διατάραξη της εμπιστοσύνης εναντίον κάποιου ιδιώτη ή κάποιου θεσμού, την παραβίαση της επαγγελματικής συμπεριφοράς ή τη διακινδύνευση των καταναλωτών και των πελατών»[25]. Ο Parker ήταν από τους πρώτους που συνέδεσαν το πληροφορικό έγκλημα με το έγκλημα του λευκού κολάρου και για την ακρίβεια ότι το λευκό κολάρο αποτελεί ένα μέρος του πληροφορικού εγκλήματος.

Η θεωρία της ορθολογικής επιλογής θεμελιώθηκε από τους Clarke και Cornish τη δεκαετία του 1980. Η θεωρία αυτή βασίζεται στην ιδέα της «αναμενόμενης χρησιμότητας» υποθέτοντας πως τα άτομα προβαίνουν στην πράξη στη βάση της μεγιστοποίησης των κερδών και της ελαχιστοποίησης των απωλειών. Με τη θεωρία της ορθολογικής επιλογής γίνεται επιτρεπτή η αναμόρφωση της δύσκολης ερώτησης σχετικά με τα κίνητρα του εγκληματία ως υπολογισμού, δηλαδή ενός ζυγίσματος μεταξύ κόστους και κερδών. Με αυτόν τον τρόπο μετατίθεται η προσοχή από τον εγκληματία προς το εγκληματικό γεγονός. Το πλεονέκτημα στο να το κάνει αυτό είναι ότι εγκαταλείπει αποτελεσματικά οποιαδήποτε αίσθηση για την ύπαρξη κάποιας χρησιμότητας

23 Herbert Edelhertz 1970, 3.
24 Γρηγόρης Λάζος 2001, 56.
25 Donn B. Parker 1976, 17.

για τη διαφοροποίηση μεταξύ εγκληματιών και μη εγκληματιών[26].

Μεταγενέστερα οι Cornish & Clarke συνόψισαν τη θεωρία τους σε έξι σημεία. Πρώτον, η εγκληματική συμπεριφορά είναι σκόπιμη. Δεύτερον, η εγκληματική συμπεριφορά είναι ορθολογική. Τρίτον, η λήψη απόφασης για το έγκλημα σχετίζεται με το είδος του εγκλήματος. Τέταρτον, οι εγκληματικές επιλογές διαχωρίζονται σε αποφάσεις «εμπλοκής» και σε αποφάσεις «γεγονότος». Πέμπτον, η εμπλοκή αποτελείται από διαφορετικά στάδια. Έκτον, τα εγκληματικά γεγονότα ξεδιπλώνονται σε μια σειρά από στάδια και αποφάσεις[27].

Αρχίζοντας με το ότι η εγκληματική συμπεριφορά είναι σκόπιμη η ορθολογική επιλογή αντιλαμβάνεται τα εγκλήματα ως σκόπιμες και ηθελημένες πράξεις, οι οποίες υλοποιούνται προκειμένου ο δράστης να αποκτήσει κάποιο όφελος. Τα οφέλη που μπορεί να αποκτήσει από αυτή τη συμπεριφορά μπορεί να περιλαμβάνουν την ικανοποίηση συνηθισμένων ανθρωπίνων κινήτρων, όπως επιθυμίες για σεξουαλική ευχαρίστηση, ενθουσιασμό, αυτονομία, θαυμασμό, εκδίκηση, έλεγχο, μείωση της έντασης, υλικά αγαθά κλπ. Η θεωρία συνεχίζει με την ορθολογικότητα της εγκληματικής συμπεριφοράς, πράγμα που σημαίνει ότι τα άτομα δεδομένων των κινήτρων και των στόχων τους θα προσπαθήσουν για την επίτευξη αυτών να επιλέξουν τα καλύτερα διαθέσιμα μέσα. Ωστόσο, δεν μπορούμε να υποθέσουμε πως η ορθολογικότητα είναι τέλεια και έτσι κάνουμε λόγο για περιορισμένη ή οριοθετημένη ορθολογικότητα (limited or bounded rationality), η οποία σχετίζεται με το ότι στον πραγματικό κόσμο χρειάζεται κάποιες φορές να ληφθεί δράση κάτω από περιστάσεις που δεν είναι τέλειες. Φυσικά, η λήψη της απόφασης σχετίζεται με συγκεκριμένα εγκλήματα, δηλαδή οι εγκληματίες δεν διαπράττουν έγκλημα γενικά αλλά συγκεκριμένα εγκλήματα, τα οποία φέρνουν συγκεκριμένα οφέλη στους δράστες και διαπράττονται με συγκεκριμένα κίνητρα. Λό-

26 Tim Newburn 2007, σελίδα 281.
27 Derek B. Cornish & Ronald V. Clarke 2008, 24.

γω του ότι τα εγκλήματα διαφέρουν το ένα από το άλλο, ανάλογα με τη φύση του εγκλήματος θα διαφέρουν πολύ και οι παράγοντες που ζυγίζονται από τους δράστες και οι μεταβλητές που επηρεάζουν τη λήψη αποφάσεων[28].

Οι αποφάσεις οι οποίες λαμβάνονται για το έγκλημα διαχωρίζονται σε αποφάσεις εμπλοκής και σε αποφάσεις γεγονότος. Οι αποφάσεις γεγονότος είναι εγκληματοκεντρικές και επικεντρώνονται στην τέλεση του εγκλήματος, σχετίζονται με το είδος του εγκλήματος και αφορούν επιλογές και αποφάσεις που λαμβάνονται όταν προετοιμάζεται, διενεργείται και τελείται ένας συγκεκριμένος τύπος εγκλήματος. Οι αποφάσεις εμπλοκής αφορούν την εγκληματική καριέρα και περιλαμβάνουν αποφάσεις για την αρχική εμπλοκή (έναρξη), τη συνεχιζόμενη εμπλοκή (εξοικείωση) και την παραίτηση, οι οποίες αποτελούν τα ξεχωριστά στάδια της εγκληματικής εμπλοκής. Αυτός ο διαχωρισμός γίνεται για να τονιστεί το γεγονός πως σε κάθε στάδιο υπάρχουν διαφορετικά σετ μεταβλητών που επηρεάζουν τις αποφάσεις των δραστών. Όσον αφορά την ξεδίπλωση των εγκληματικών γεγονότων σε μία σειρά από στάδια και αποφάσεις, αναφέρουν ότι συχνά δίνεται προσοχή στα κεντρικά στάδια της εγκληματικής ενέργειας χωρίς να δίνεται αντίστοιχη προσοχή στο αρχικό και στο τελικό στάδιο[29].

Διάφορες προσεγγίσεις, βέβαια, έχουν αναπτυχθεί και για τον κοινωνικό έλεγχο. Επελέγησαν σχετικές προσεγγίσεις, καθώς μέσα στην εργασία αναφέρονται και κάποιες δράσεις και μέτρα που έχουν αναληφθεί στο πλαίσιο της σύγχρονης τεχνολογίας για την καταπολέμηση των νέων μορφών εγκληματικότητας. Ο κοινωνικός έλεγχος είναι μια αρκετά ευρεία έννοια της οποίας η χρήση δεν είναι πρόσφατη. Η πρώτη χρήση του όρου σε επιστημονικό κείμενο εντοπίζεται το 1894 στο βιβλίο των Albion Small και George Vincent. Οι Small & Vincent ανέφεραν πως «η αντίδραση της κοινής γνώμης στην εξουσία καθιστά τον κοινωνικό έλεγχο ένα πάρα πολύ λεπτό και δύ-

28 Το ίδιο, 25-27.
29 Το ίδιο, 27-28.

σκολο ζήτημα»[30]. Το 1896 ο George Vincent ορίζει τον κοινωνικό έλεγχο ως την τέχνη η οποία συνδυάζει τις κοινωνικές δυνάμεις με τέτοιον τρόπο ώστε να μπορέσουν να δώσουν στην κοινωνία τουλάχιστον μια ροπή προς το ιδανικό[31]. Μεταγενέστερα το 1925 ο George Herbert Mead αναφέρει πως ο κοινωνικός έλεγχος βασίζεται πάνω στο βαθμό που τα άτομα στην κοινωνία έχουν την ικανότητα να προσλαμβάνουν τις συμπεριφορές των άλλων με τους οποίους συναναστρέφονται, προκειμένου να εκπληρώσουν κοινούς στόχους[32]. Ένας πιο γενικός ορισμός της έννοιας του κοινωνικού ελέγχου δίνεται από τον Stanley Cohen το 1985 και αναφέρει ότι ο κοινωνικός έλεγχος είναι οι οργανωμένοι τρόποι αντίδρασης μια κοινωνίας απέναντι σε συμπεριφορές και ανθρώπους που θεωρούνται με τον ένα ή τον άλλον τρόπο αποκλίνοντες, προβληματικοί, ανησυχητικοί, ενοχλητικοί ή ανεπιθύμητοι. Υπάρχουν διάφοροι όροι, όπως τιμωρία, μεταχείριση, πρόληψη, αποτροπή, δικαιοσύνη κλπ., οι οποίοι μπορούν να εκφράσουν αυτήν την αντίδραση[33].

Ο κοινωνικός έλεγχος βασίζεται σε μια δέσμευση αξιών πάνω σε δύο στοιχεία τουλάχιστον και έτσι μπορεί να γίνει αντιληπτός. Τα στοιχεία αυτά είναι η μείωση του εξαναγκασμού, παρόλο που αναγνωρίζονται τα αμείωτα στοιχεία εξαναγκασμού που υπάρχουν σε ένα νόμιμο σύστημα εξουσίας, και η εξάλειψη της ανθρώπινης δυστυχίας, παρότι αναγνωρίζεται η διατήρηση κάποιου βαθμού ανισότητας. Θα μπορούσε να αναφερθεί και ένα τρίτο στοιχείο, το οποίο είναι η δέσμευση σε διαδικασίες επανακαθορισμού των κοινωνικών στόχων, προκειμένου να βελτιωθεί ο ρόλος της ορθολογικότητας. Αυτό το τρίτο στοιχείο, ωστόσο, θα μπορούσε να θεωρηθεί εγγενές στα δύο πρώτα. Ως αντίθετο του κοινωνικού ελέγχου θα μπορούσε να λογιστεί ο εξαναγκαστι-

30 Albion W. Small & George E. Vincent 1894, 328.
31 George Vincent 1896, 488.
32 George Herbert Mead 1925, 275.
33 Stanley Cohen 1985, 1.

κός έλεγχος, ο οποίος αφορά την κοινωνική οργάνωση που βασίζεται κατά κύριο λόγο στην άσκηση εξαναγκασμού[34].

Το σύστημα για τον έλεγχο της παρεκκλίνουσας συμπεριφοράς καταλαμβάνει χώρο σε όλες τις κοινωνίες και στον πραγματικό χώρο, όπως είναι τα κτίρια, η τεχνολογία, το προσωπικό και οι πελάτες, και στον κοινωνικό χώρο, όπως είναι οι ιδέες, οι επιρροές και τα αποτελέσματα[35]. Ο Gary Marx υποστήριξε πως η κοινωνία γίνεται πορώδης ή διαφανής και λειτουργίες, όπως τα συναισθήματα και η σκέψη, που κάποτε προστατεύονταν πλέον καθίστανται ορατές. Ακόμη, τα εμπόδια και τα όρια που ήταν θεμελιώδη για την αντίληψη της ιδιωτικότητας, της ελευθερίας και της ατομικότητας, όπως είναι η απόσταση, το σκοτάδι, ο χρόνος, οι τοίχοι, τα παράθυρα, ακόμα και το δέρμα, πλέον υποχωρούν[36]. Μέσα από την εφαρμογή συστημάτων εποπτείας μπορεί να ασκηθεί, από τη μία, προληπτικός έλεγχος της τάξης και, από την άλλη, πολιτικός έλεγχος. Ωστόσο, ακόμα και σε επίπεδο διεξαγωγής προληπτικού ελέγχου της συμπεριφοράς του ατόμου στην καθημερινή ζωή δεν γίνεται η τήρηση των ελάχιστων απαιτούμενων εγγυήσεων για τους πολίτες[37].

Ο Gary Marx αναφέρει έξι στρατηγικές για τον κοινωνικό έλεγχο, οι οποίες συνδέονται με την τεχνολογία. Η πρώτη στρατηγική είναι η απομάκρυνση του στόχου (target removal). Σε αυτή τη στρατηγική εδράζεται η λογική της πρόληψης αναφορικά με το γεγονός πως κάτι το οποίο δεν υπάρχει δεν μπορεί να αποτελέσει στόχο. Παράδειγμα μπορεί να αποτελέσει η ολοένα και μικρότερη χρήση μετρητών και έτσι οι έμποροι που δέχονται μόνο πιστωτικές ή χρεωστικές κάρτες δύσκολα μπορούν να πέσουν θύματα ληστείας. Η δεύτερη στρατηγική είναι η υποτίμηση του στόχου (target devaluation). Σε αυτή τη στρατηγική στόχος είναι η υποτίμηση ή η εξάλειψη της αξίας κά-

34 Morris Janowitz 1975, 84.
35 Το ίδιο, 43.
36 Gary T. Marx 1989, 33.
37 Ανθοζωή Χάιδου 2003, 98.

ποιου πιθανού στόχου προς οποιονδήποτε άλλον πέραν των εξουσιοδοτημένων χρηστών. Για την ακρίβεια, ο στόχος παραμένει, αλλά δεν είναι πλέον ελκυστικός προς τους θηρευτές λόγω του ότι έχει αχρηστευτεί. Παράδειγμα μπορούν να αποτελέσουν τα κωδικοποιημένα μηνύματα που στέλνονται ελεύθερα μέσω απροστάτευτων τηλεφωνικών γραμμών, οι οποίες εύκολα μπορούν να υποκλαπούν, αλλά οι πληροφορίες καθίστανται άχρηστες ελλείψει του κωδικού αποκρυπτογράφησης. Η τρίτη στρατηγική είναι η απομόνωση του στόχου (target insulation). Εδώ ο στόχος παραμένει, αλλά είναι προστατευμένος. Παράδειγμα αποτελούν τα διάφορα αντικλεπτικά συστήματα[38].

Η τέταρτη στρατηγική είναι η αχρήστευση του εγκληματία (offender incapacitation). Στόχος είναι ο εγκληματίας να καταστεί ακίνδυνος. Υπάρχουν διάφορα εργαλεία για τον περιορισμό των παραβιάσεων μέσω της αποδυνάμωσης της θέλησης ή της ικανότητας του δράστη να διαπράξει έγκλημα. Υπάρχουν προσπάθειες αχρήστευσης που έχουν να κάνουν με το σώμα του δράστη, όπως είναι ο πραγματικός ή ο χημικός ευνουχισμός για σεξουαλικά εγκλήματα, και προσπάθειες αχρήστευσης που αφορούν τα μέσα τέλεσης του εγκλήματος, όπως η απαγόρευση κατοχής όπλων. Η πέμπτη στρατηγική είναι ο αποκλεισμός του εγκληματία (offender exclusion) και είναι το αντίθετο της απομόνωσης του στόχου. Εδώ περιορίζεται ο εγκληματίας και όχι ο πιθανός στόχος. Παράδειγμα αποτελούν οι ηλεκτρονικές συσκευές εντοπισμού της τοποθεσίας. Η έκτη στρατηγική είναι η αναγνώριση του αδικήματος, του εγκληματία και του στόχου (offense, offender, and target identification). Ο στόχος που τίθεται εδώ είναι η καταγραφή του συμβάντος και η αναγνώριση ή παγίδευση του δράστη. Παράδειγμα μπορούν να αποτελέσουν διάφοροι συναγερμοί και αισθητήρες[39].

Στο δεύτερο μισό του 20ού αιώνα υπήρξε μια σημαντική αύξηση της χρήσης της επιστήμης και της τεχνολογίας για σκοπούς που σχετίζονται με τον κοινωνικό έλεγχο,

38 Gary T. Marx 1995 (http://web.mit.edu/gtmarx/www/bullet.html).
39 Το ίδιο.

όπως είναι η ηλεκτρονική επιτήρηση, η ανάλυση DNA κλπ. Ο έλεγχος έχει γίνει ηπιότερος και λιγότερο ορατός, μερικώς επειδή είναι ενσωματωμένος και μερικώς λόγω του ότι χρησιμοποιούνται πιο υπερσύγχρονες μέθοδοι εξαπάτησης (deception). Παράδειγμα για την ενσωμάτωση μπορούν να αποτελέσουν διάφορα λογισμικά προστασίας και για την εξαπάτηση παράδειγμα μπορούν να αποτελέσουν διάφορες πολύπλοκες μυστικές επιχειρήσεις. Ο σύγχρονος έλεγχος έχει γίνει περισσότερο εκτεταμένος και εκτείνεται σε ένα ευρύτερο δίκτυο σε σχέση με τα μέσα του 20ού αιώνα, περιλαμβάνει πιο ολοκληρωμένα δίκτυα ανταλλαγής πληροφοριών θολώνοντας τα όρια μεταξύ των ιδρυμάτων και των οργανισμών, π.χ. μεταξύ των υπηρεσιών και της κυβέρνησης κλπ[40].

Η αναφορά σε αυτές τις θεωρητικές προσεγγίσεις είναι ενδεικτική και όχι εξαντλητική, καθώς υπάρχουν πάρα πολλές προσεγγίσεις και για την τεχνολογία και για την εγκληματική συμπεριφορά και για τον κοινωνικό έλεγχο. Για το ζήτημα της παρούσας εργασίας έχουν τεθεί κάποια ερωτήματα, τα οποία θα βοηθήσουν στην εξαγωγή συμπερασμάτων. Για τα πρώτα πιο γενικά ερωτήματα που αφορούν την τεχνολογία θα εστιάσουμε στην επιλεκτική χρησιμότητα της τεχνολογίας. Στο πρώτο ερώτημα θα αναφερθούμε ενδεικτικά με βάση τη θεωρία της ορθολογικής επιλογής σε κίνητρα που υπάρχουν πίσω από την τέλεση μιας εγκληματικής πράξης. Στο τρίτο ερώτημα μαζί με την απάντηση θα εστιάσουμε και στον ορισμό του Stanley Cohen για τον κοινωνικό έλεγχο και σε αυτά που αναφέρει ο Gary Marx για το σύγχρονο έλεγχο. Στο τελευταίο ερώτημα θα εστιάσουμε στον ορισμό του Edelhertz.

40 Gary T. Marx 2001, 15506-15507.

2. Νέες μορφές εγκληματικότητας

Στις νέες μορφές εγκληματικότητας θα περιληφθούν, αφενός, τα παραδοσιακά εγκλήματα που τελούνται με νέα τεχνολογικά μέσα και, αφετέρου, τα εγκλήματα των οποίων η ύπαρξη οφείλεται αποκλειστικά στη χρήση της σύγχρονης τεχνολογίας. Στα παραδοσιακά εγκλήματα εντοπίζονται αλλαγές στον τρόπο και στα μέσα τέλεσης, στην προσέγγιση του υποψηφίου θύματος και γενικότερα οι δυσκολίες που μπορεί να υπήρχαν παλαιότερα πλέον κάμπτονται. Ουσιαστικά, τα παραδοσιακά εγκλήματα περνούν σε μια νέα διάσταση και, έτσι, οι απαιτούμενες για τη διάπραξη ενέργειες μπορούν χάρη στην τεχνολογική πρόοδο να ολοκληρωθούν με μεγαλύτερη ευκολία σε σχέση με παλαιότερες εποχές.

Η τεχνολογική εξέλιξη έχει φέρει μεγάλες αλλαγές στον τομέα της εγκληματικότητας με εντελώς νέες μορφές να κάνουν την εμφάνισή τους. Η εμφάνιση των εγκλημάτων αυτών οφείλεται αποκλειστικά στη χρήση της σύγχρονης τεχνολογίας. Η τέλεση αυτών των εγκλημάτων γίνεται αποκλειστικά σε ένα εικονικό περιβάλλον και οι δράστες χρησιμοποιούν όλο και πιο υπερσύγχρονες μεθόδους εκμεταλλευόμενοι την ταχεία τεχνολογική ανάπτυξη. Τα εγκλήματα που τελούνται αποκλειστικά με σύγχρονα τεχνολογικά μέσα και, φυσικά, δεν υπήρχαν πριν την εμφάνιση των υπολογιστών και των δικτύων είναι αρκετά, αλλά αυτά που συναντώνται πιο συχνά είναι το hacking με την έννοια της κακόβουλης εισβολής σε δίκτυο, η διασπορά κακόβουλου λογισμικού και η ψηφιακή πειρατεία. Άλλες μορφές νέων εγκλημάτων αποτελούν διάφορες επιθέσεις εναντίον δικτύων, όπως οι επιθέσεις άρνησης εξυπηρέτησης και οι επιθέσεις σε δικτυακούς τόπους. Οι επιθέσεις άρνησης εξυπηρέτησης αποσκοπούν στο να εξαντληθούν οι πόροι ενός υπολογιστή, ώστε να μην μπορούν να εξυπηρετηθούν άλλοι υπολογιστές και αυτό συχνά ισοδυναμεί με το να διακοπεί η λειτουργία μιας κρίσιμης υ-

πηρεσίας ή ενός συνόλου υπηρεσιών προσφερόμενων από έναν ή περισσότερους διακομιστές. Στις επιθέσεις σε δικτυακούς τόπους ο δράστης μπορεί να διαγράψει ορισμένες σελίδες ή γραφικά και να ανεβάσει δικές του σελίδες με περιεχόμενο που θα ποικίλει από καθαρά χιουμοριστικό μέχρι προπαγανδιστικό. Ο Βλαχόπουλος, ωστόσο, αναφέρει ως γνήσια ηλεκτρονικά εγκλήματα και το phishing, το pharming και το spamming[41]. Αυτά τα τρία, όμως, δεν είναι εγκλήματα, τα οποία προέκυψαν με τη χρήση της τεχνολογίας. Είναι απάτες που απλά τελούνται με νέα μέσα σε ψηφιακό περιβάλλον[42]. Στο κεφάλαιο που αφορά τις εντελώς νέες μορφές εγκληματικότητας θα αναφερθούν το hacking, το κακόβουλο λογισμικό και η ψηφιακή πειρατεία, και πιο συγκεκριμένα η πειρατεία λογισμικού. Αυτά επελέγησαν, επειδή αποτελούν τα πιο συνηθισμένα εγκλήματα που τελούνται με τη βοήθεια της σύγχρονης τεχνολογίας και, επίσης, είναι αυτά που έχουν μελετηθεί περισσότερο σε σχέση με τα υπόλοιπα.

Όπως έχει ήδη αναφερθεί και όπως φαίνεται και από τις παραπάνω μορφές το διαδίκτυο παίζει πολύ σημαντικό ρόλο στη διάπραξη εγκλημάτων. Σε έρευνα που έγινε σε δείγμα φοιτητών για την ανασφάλεια και τη θυματοποίηση στο διαδίκτυο βρέθηκε πως η πλειοψηφία του δείγματος χρησιμοποιούσε πολλά χρόνια το διαδίκτυο, είχε λάβει κάποιας μορφής «εκπαίδευση» για τη χρήση του και αυτοκατατάσσονταν ως «μέσοι χρήστες». Σημειώθηκε ένα σχετικά υψηλό ποσοστό ασφάλειας, πράγμα το οποίο συναρτάται με την εκτεταμένη λήψη μέτρων αυτοπροστασίας, ενώ προέκυψε μια θετική συνάρτηση του φύλου με την ανασφάλεια, με το μεγαλύτερο ποσοστό ανασφάλειας να εντοπίζεται στις γυναίκες. Το ένα πέμπτο του δείγματος ανέφερε πολλαπλή και επαναλαμβανόμενη θυματοποίηση, με τις κυριότερες μορφές να είναι ο εκφοβισμός και η υποκλοπή προσωπικών δεδομένων. Στατιστικά σημαντικές ήταν η συσχέτιση θυματοποίησης και συχνότητας χρήσης, καθώς όσοι χρησιμοποιούσαν καθημερι-

41 Κωνσταντίνος Βλαχόπουλος 2007, 39-62.
42 Περισσότερα βλ. παρακάτω, Choo, Smith & McCusker 2007, 49-51, και "Online fraud: Pharming", χ.χ. (http://us.norton.com/cybercrime-pharming).

νά το διαδίκτυο σημείωσαν τα μεγαλύτερα ποσοστά θυματοποίησης, και η συσχέτιση θυματοποίησης και επαφής με αγνώστους, καθώς αυτοί σημείωσαν το διπλάσιο ποσοστό θυματοποίησης σε σχέση με τους υπόλοιπους. Ως θετικότερο στοιχείο του διαδικτύου αναφέρθηκε η «ενημέρωση/πληροφόρηση» και ως αρνητικότερο τα «διαδικτυακά εγκλήματα» και στη συνέχεια ακολουθούσαν και άλλα αναφερόμενα ως θετικά και αρνητικά στοιχεία[43].

Η δημιουργία νέων μεθόδων στη διάπραξη ήδη υπαρχόντων εγκλημάτων και η εμφάνιση εντελώς καινούριων εγκλημάτων λόγω της τεχνολογικής εξέλιξης κατέστησαν αναγκαία και την προσαρμογή της νομοθεσίας στα νέα δεδομένα. Νέοι νόμοι έρχονται και είτε αντικαθιστούν είτε συμπληρώνουν τους παλαιότερους, ούτως ώστε να συμπεριληφθούν μέσα στο εθνικό δίκαιο κυρώσεις που αφορούν νέες μορφές εγκληματικότητας. Ο ελληνικός Ποινικός Κώδικας βρίθει διαφόρων τέτοιων προσθηκών. Ενδεικτικά μπορούμε να αναφέρουμε τις παραγράφους 3 και 4 του άρθρου 337 για την προσβολή της γενετήσιας αξιοπρέπειας ανηλίκου και το 386Α για την απάτη μέσω υπολογιστή[44]. Σε διεθνές επίπεδο έχουν υπάρξει διάφορες συστάσεις και οδηγίες από το Συμβούλιο της Ευρώπης και την Ευρωπαϊκή Ένωση για τη συμπλήρωση των εθνικών δικαίων των κρατών-μελών. Τα κυριότερα που μπορούμε να αναφέρουμε είναι η «Σύμβαση για το Έγκλημα στον Κυβερνοχώρο» το 2001 και το Πρόσθετο Πρωτόκολλο της Σύμβασης το 2003, τα οποία ήταν από το Συμβούλιο της Ευρώπης, και η Οδηγία 2013/40 από την Ευρωπαϊκή Ένωση. Αυτά τα τρία κυρώθηκαν πρόσφατα από το Ελληνικό Κοινοβούλιο με τον Νόμο 4411/2016[45].

43 Χριστίνα Ζαραφωνίτου 2014, 28-29.
44 Ολόκληρος ο Ποινικός Κώδικας στο http://www.ministryofjustice.gr/site/kodikes/Ευρετήριο/ΠΟΙΝΙΚΟΣΚΩΔΙΚΑΣ/tabid/432/language/el-GR/Default.aspx.
45 Νόμος 4411/2016.

2.1 Παραδοσιακά εγκλήματα και σύγχρονη τεχνολογία

Α. Βαθύς Ιστός και παραδοσιακά εγκλήματα

Αρκετές φορές η διάπραξη εγκλημάτων επιτυγχάνεται με τη διατήρηση της ανωνυμίας των δραστών, ειδικά για τα εγκλήματα που τελούνται μέσα στον Βαθύ Ιστό, χάρη στα κατάλληλα ψηφιακά εργαλεία ανωνυμοποίησης που έχουν εφευρεθεί. Τα εργαλεία ανωνυμοποίησης χρησιμοποιούνται για διάφορους σκοπούς, οι οποίοι μπορεί να είναι είτε απλώς η ιδιωτικότητα είτε η αποφυγή του εντοπισμού, της καταδίωξης (persecution) ή της δίωξης (prosecution). Υπάρχουν διάφορες μεθοδοι για την απόκρυψη της ταυτότητας κάποιου στο διαδίκτυο. Τα εργαλεία που χρησιμοποιούνται μπορούν να χωριστούν σε τρεις κατηγορίες: τους διακομιστές μεσολάβησης (proxies)[46], τα εικονικά ιδιωτικά δίκτυα (virtual private networks – VPNs)[47] και τα Σκοτεινά Δίκτυα (Darknets). Τα Σκοτεινά Δίκτυα είναι δίκτυα τα οποία λειτουργούν εντός του Βαθέως Ιστού. Η εφεύρεση του πρώτου Σκοτεινού Δικτύου, του The Onion Router (Tor) έγινε το 1995 από το Πολεμικό Ναυτικό των ΗΠΑ για την προστασία των επικοινωνιών της κυβέρνησης. Πλέον το Tor είναι παγκοσμίως διαθέσιμο και αποτελεί ένα από τα πιο γνωστά και ευρέως χρησιμοποιημένα εργαλεία ανωνυμοποίησης, ενώ παράλληλα παρέχονται και πρόσθετες υπηρεσίες, όπως το Torchat, το οποίο είναι ασφαλές λογισμικό ανταλλαγής μηνυμάτων. Εκτός από το Tor, αρκετά δημοφιλή εργαλεία ανωνυμοποίησης με παρόμοιες προσφερόμενες υπηρεσίες αποτελούν το Freenet και το Invisible Internet Project (I2P)[48].

46 Ο διακομιστής μεσολάβησης (proxy) ρυθμίζει την πρόσβαση στο internet και εμποδίζει τους εξωτερικούς υπολογιστές να αποκτήσουν πρόσβαση στο δίκτυο [«Ρυθμίσεις διακομιστή μεσολάβησης δικτύου», 2015 (https://support.norton.com/sp/el/gr/home/current/solutions/v66135793_NortonM_Retail_1_el_el)].

47 Το VPN είναι μια τεχνολογία δικτύων για τη δημιουργία μιας ασφαλούς δικτυακής σύνδεσης μέσω ενός δημοσίου δικτύου, όπως το internet, ή ενός ιδιωτικού δικτύου, το οποίο κατέχει ένας πάροχος υπηρεσιών. Η τεχνολογία VPN χρησιμοποιείται από μεγάλες επιχειρήσεις, εκπαιδευτικά ιδρύματα και κυβερνητικές υπηρεσίες για την ασφαλή σύνδεση απομακρυσμένων χρηστών σε κάποιο ιδιωτικό δίκτυο. Προκειμένου ο χρήστης να αποκτήσει πρόσβαση στο ιδιωτικό δίκτυο, πρέπει να αυθεντικοποιηθεί χρησιμοποιώντας μια μοναδική ταυτοποίηση και ένα μοναδικό κωδικό. Η αυθεντικοποίηση γίνεται συνήθως μέσω ενός PIN. ["What is VPN?", χ.χ. (http://whatismyipaddress.com/vpn)].

48 Europol 2014, 55.

Μέσα από τα Σκοτεινά Δίκτυα υπάρχουν και κάποιες προσφερόμενες κρυμμένες υπηρεσίες. Αυτές οι κρυμμένες υπηρεσίες είναι γενικά δύο ειδών: υπόγεια forums (underground forums) και εγκληματικές αγορές (criminal marketplaces). Τα υπόγεια forums λειτουργούν ως τόποι συνάντησης και πίνακες μηνυμάτων για διάφορες κοινότητες και μπορεί κανείς να βρει forums αφιερωμένα στα ναρκωτικά, στο hacking, στη διακίνηση πιστωτικών καρτών και υλικό κακοποίησης ανηλίκων. Παρότι το εμπόριο παράνομων αγαθών υπάρχει μέσα σε αυτά τα forums, η κακή φήμη των Σκοτεινών Δικτύων αυξήθηκε λόγω των αγορών στις οποίες μπορεί κάποιος να έχει πρόσβαση μέσω αυτών. Αυτές οι σκοτεινές αγορές προσφέρουν στους περιηγητές τη δυνατότητα να αποκτήσουν οποιοδήποτε παράνομο προϊόν ή υπηρεσία επιθυμούν, συμπεριλαμβανομένων ναρκωτικών, όπλων, φαρμακευτικών στεροειδών, πιστωτικών καρτών, ακόμα και συμβολαίων θανάτου. Σε αυτές τις αγορές οι πληρωμές γίνονται μέσω εικονικών νομισμάτων, όπως είναι το Bitcoin. Η πιο γνωστή σκοτεινή αγορά είναι το Silk Road[49].

Αρκετές φορές ο Βαθύς Ιστός μπερδεύεται με τον Σκοτεινό Ιστό (Dark Web). Ο Σκοτεινός Ιστός, ωστόσο, αποτελεί μέρος του Βαθέως Ιστού και όχι κάτι ξεχωριστό[50]. Η πλειοψηφία των ιστοτόπων του Σκοτεινού Ιστού χρησιμοποιεί το Tor ως λογισμικό ανωνυμοποίησης, αν και σε κάποιους χρησιμοποιείται το I2P. Μέσω αυτών των συστημάτων η κυκλοφορία του ιστού κωδικοποιείται σε στρώματα και αναπηδά σε τυχαία επιλεγμένους υπολογιστές σε όλο τον κόσμο. Ο Σκοτεινός Ιστός είναι που συνδέεται με εγκληματικές πράξεις, όπως η πώληση ναρκωτικών, όπλων, πλαστών εγγράφων και την παιδική πορνογραφία[51].

Το 2014 διεξήχθη μια έρευνα από τον Gareth Owen, ερευνητή του Πανεπιστημίου του Portsmouth, και την ομάδα του αναφορικά με την επισκεψιμότητα του Σκοτεινού

49 Το ίδιο, 19-20, 42.
50 "Dark web, χ.χ. (http://www.dictionary.com/browse/dark-web?s=t).
51 Andy Greenberg 2014α (https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/).

Ιστού. Η έρευνα διήρκεσε από το Μάρτιο μέχρι το Σεπτέμβριο του 2014 με την εγκατάσταση του Tor σε 40 «εφεδρικούς» υπολογιστές, πράγμα το οποίο τους επέτρεψε να συλλέξουν δεδομένα για όλες τις κρυφές του υπηρεσίες, οι οποίες εκείνη τη στιγμή ανέρχονταν στις 45.000. Στη συνέχεια, χρησιμοποίησαν ένα πρόγραμμα web crawling[52] για την επίσκεψη κάθε σελίδας που βρήκαν και για την ταξινόμησή της. Το 83% της επισκεψιμότητας του Σκοτεινού Δικτύου αφορά ιστοτόπους παιδοφιλικού περιεχομένου. Πολλοί από αυτούς, μάλιστα, ήταν τόσο σαφείς ως προς το περιεχόμενό τους που περιείχαν το πρόθεμα "pedo" στο όνομά τους. Ο αυτόματος web crawler των ερευνητών κατέβασε μόνο κείμενο και όχι εικόνες, ώστε να αποφευχθεί η παράνομη κατοχή υλικού παιδικής πορνογραφίας. Παρότι η επισκεψιμότητα των ιστοτόπων παιδοφιλικού περιεχομένου είναι μεγάλη, αυτοί αντιπροσωπεύουν μόλις το 2% των κρυφών υπηρεσιών του Tor. Το 24% του δικτύου αντιπροσωπεύουν ιστοσελίδες και διαδικτυακές αγορές σχετιζόμενες με τα ναρκωτικά, όπως το Silk Road, το Agora ή το Evolution. Οι επισκέψεις σε ιστοτόπους με τέτοιο περιεχόμενο ανέρχονταν μόλις στο 5% των αναζητήσεων των χρηστών στο Tor. Στη μελέτη αυτή βρέθηκε, ακόμα, πως η συντριπτική πλειοψηφία των κρυφών υπηρεσιών μένουν online για λίγες μέρες ή εβδομάδες, καθώς στο τέλος της έρευνας είχε απομείνει online λιγότερο από το 1/6 των κρυφών υπηρεσιών σε σχέση με το ξεκίνημα[53].

Λόγω του γεγονότος ότι είναι δύσκολη η ακριβής μέτρηση σε οτιδήποτε στον Σκοτεινό Ιστό, τα ευρήματα αφήνουν ένα περιθώριο αμφισβήτησης. Όπως ανέφεραν οι δημιουργοί του Tor, ως «επίσκεψη» στους ιστοτόπους παιδοφιλικού περιεχομένου μπορεί να μετρήσει η μέτρηση και ο εντοπισμός τους από τις υπηρεσίες επιβολής του

52 Web crawling ονομάζεται η διαδικασία των μηχανών αναζήτησης για τη διεξοδική εξέταση των ιστοτόπων, προκειμένου αυτοί να καταλογογραφηθούν. Οι web crawlers σέρνονται συστηματικά σε διάφορους ιστοτόπους κοιτώντας τις λέξεις-κλειδιά, το είδος του περιεχομένου, όλα τα links και στη συνέχεια επιστρέφουν αυτές τις πληροφορίες στους servers της μηχανής αναζήτησης για καταλογογράφηση ["Web crawling", χ.χ. (http:/trackmaven.com/marketing-dictionary/web-crawling/)].

53 Όπως αναφέρεται στο Andy Greenberg 2014β (https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/).

νόμου και από διάφορους οργανισμούς εναντίον της παιδικής κακοποίησης. Ακόμη, μπορεί hackers να εξαπολύσουν επιθέσεις άρνησης εξυπηρέτησης, προκειμένου να ρίξουν έναν ιστότοπο, γεμίζοντάς τον με απατηλές επισκέψεις. Οι ασταθείς ιστότοποι που πέφτουν συνέχεια μπορεί να παράγουν περισσότερες επισκέψεις από τις κανονικές. Τέλος, όσοι χρησιμοποιούν το εργαλείο Tor2Web, το οποίο κάνει τις κρυφές υπηρεσίες του Tor προσβάσιμες σε μη ανώνυμους χρήστες, μπορεί να υποεκπροσωπούνται. [54].

Μια νεότερη έρευνα που αφορά τις κρυφές υπηρεσίες του Tor δημοσιεύτηκε στις αρχές του 2016. Οι ερευνητές συνέλεξαν τα δεδομένα μέσω web crawling και η αξιολόγησή τους έγινε σε δύο βήματα. Αρχικά έφτιαξαν χειροκίνητα κάποιες κατηγορίες που χρησιμοποιήθηκαν για την «εκπαίδευση» ενός ταξινομητή εγγράφων Support Vector Machine[55] και, εν συνεχεία, χρησιμοποιήθηκε αυτός ο ταξινομητής για την ολοκλήρωση των κατηγοριών για τους υπόλοιπους ιστοτόπους. Το σκανάρισμα έγινε σε 5205 ιστοτόπους και η μεθοδολογία βασίστηκε αποκλειστικά σε καταχωρίσεις κειμένων και όχι εικόνες ή οπτικοασκουστικά μέσα, τα οποία απορρίφθηκαν αυτόματα από το web crawler. Τα αποτελέσματα έδειξαν πως η χρήση των κρυμμένων υπηρεσιών του Tor γινόταν κατά κύριο λόγο για εγκληματικούς σκοπούς, συμπεριλαμβανομένων των ναρκωτικών, παράνομων οικονομικών και της παράνομης πορνογραφίας με παιδιά, βία και ζώα[56].

Η κατηγορία με τα οικονομικά (327 ιστότοποι) αποτελούνταν από τρεις εμφανείς υποκατηγορίες. Η πρώτη αφορά τις βασισμένες σε Bitcoin μεθόδους ξεπλύματος χρήματος, η δεύτερη το εμπόριο παράνομα αποκτημένων καρτών και λογαριασμών και η τρίτη το εμπόριο σε πλαστό χρήμα. Τα φαρμακευτικά σκευάσματα και τα ναρκωτικά

54 Το ίδιο.
55 Support Vector Machine ονομάζεται ένας αλγόριθμος στατιστικής ταξινόμησης για την κατηγοριοποίηση περιεχομένου.
56 Daniel Moore & Thomas Rid 2016, 18-21.

(423 ιστότοποι) αποτελούν το πιο συνηθισμένο προϊόν στο δίκτυο του Tor. Οι ουσίες που διατίθενταν ποίκιλαν από μαριχουάνα, μεθαμφεταμίνες, κοκαΐνη και διάφορες μορφές οξέων μέχρι αναβολικά στεροειδή τύπου Viagra. Μεγάλη ποικιλία υπήρχε, επίσης, στο πορνογραφικό περιεχόμενο (122 ιστότοποι). Υπήρχαν άφθονοι ιστότοποι που παρείχαν links σε βίντεο που απεικόνιζαν βιασμό, κτηνοβασία και παιδοφιλία. Ακόμη ήταν διαθέσιμες αρκετές κοινότητες που προσανατολίζονταν στη συζήτηση και την εκμυστήρευση παράνομων φετίχ. Κάποιοι χρήστες αναζητούσαν δικαίωση για τις επιθυμίες τους, αντάλλασσαν εμπειρίες, προτιμήσεις, ακόμα και περιεχόμενο. Άλλες διαθέσιμες παράνομες υπηρεσίες περιλάμβαναν την προμήθεια ψευδών εγγράφων ταυτοποίησης, κλεμμένο ή κατά άλλον τρόπο παράνομα αποκτημένο εξοπλισμό, όπως πυροβόλα όπλα και άλλο σχετιζόμενο εξοπλισμό, ενώ υπήρχαν και αρκετοί ιστότοποι που υποτίθεται ότι παρείχαν δολοφονίες με πολύ μεγάλη αμοιβή. Αντιθέτως με άλλα αγαθά και υπηρεσίες, δεν υπήρχε κάποια ένδειξη πως τελικά είχε κλειστεί κάποιο συμβόλαιο με τους υποτιθέμενους δολοφόνους, με αποτέλεσμα η αξιοπιστία αυτών των ιστοτόπων να είναι ανεπιβεβαίωτη[57].

Σε έρευνα που διεξήχθη από τη Virtual Global Taskforce[58] (VGT) για τη διαδικτυακή σεξουαλική εκμετάλλευση των παιδιών, μέσω άμεσης παρατήρησης 35 ερευνητών και ερωτηματολογίων που δόθηκαν σε συνεργάτες από την επιβολή του νόμου, οι απαντήσεις που μιλούσαν άμεσα για τη διάπραξη εγκληματικών ενεργειών στον Βαθύ Ιστό ήταν λίγες. Ως επί το πλείστον, υπήρχαν γενικές απαντήσεις που, όμως, παρέπεμπαν σε αυτό μιλώντας για τη γενικότερη ανάγκη των δραστών να παραμείνουν ανώνυμοι, τη μετακόμισή τους σε κλειστά δίκτυα ή τη χρήση νέων τεχνολογιών που προσφέρουν περισσότερη ανωνυμία και κρυπτογράφηση. Αυτές οι έμμεσες απαντήσεις

57 Το ίδιο, σελίδες 22-24.
58 Η VGT είναι μια παγκόσμια συνεργασία υπηρεσιών επιβολής του νόμου ενάντια στη διαδικτυακή σεξουαλική κακοποίηση παιδιών (http://virtualglobaltaskforce.com/who-we-are/).

μπορούν να εξηγηθούν από το γεγονός ότι η εμπειρία διεξαγωγής ερευνών σε τέτοια περιβάλλοντα από τις υπηρεσίες επιβολής του νόμου διαφέρει σημαντικά μεταξύ τους. Όσοι μίλησαν ανοιχτά για τον Βαθύ Ιστό είπαν πως το Tor είναι το πιο δημοφιλές Σκοτεινό Δίκτυο ανάμεσα στους παιδόφιλους. Σε πρόσφατη, πριν τη δημοσίευση της έρευνας αυτής, ερευνητική προσπάθεια από τις αρχές αποκτήθηκε το περιθώριο ανασκόπησης κάποιων κρυφών υπηρεσιών του Tor. Η ανασκόπηση έγινε σε 40 κρυφές υπηρεσίες του Tor παρείχαν υλικό σεξουαλικής κακοποίησης παιδιών οδήγησε στην αναγνώριση 300 χιλιάδων πιθανών χρηστών, ενώ σε μία από τις μεγαλύτερες κρυφές υπηρεσίες ήταν συσσωρευμένες πάνω από 1.4 εκατομμύρια εικόνες στην εκτιμώμενη διετή περίοδο μέχρι εκείνη τη στιγμή λειτουργίας του. Αυτοί οι αριθμοί επιβεβαιώνουν την υπόθεση πως οι κρυφές υπηρεσίες του Tor εξελίσσονται προς πιο επικίνδυνες κατευθύνσεις. Χρειάζεται ιδιαίτερη προσοχή στις περιοχές περιορισμένης πρόσβασης, καθώς υπάρχουν υποψίες πως τα μέλη τους είναι εξεζητημένες ομάδες δραστών και ότι το υλικό που υπάρχει εκεί πέρα παράγεται και ανανεώνεται από τα ίδια τα μέλη αυτών των forums. Αυτή η υποψία για την παραγωγή και την ανανέωση από τα ίδια τα μέλη υπάρχει, διότι έχει παρατηρηθεί πως το υλικό που υπάρχει σε αυτά τα forums δεν έχει κυκλοφορήσει πιο πριν[59].

Η διαδικασία της συλλογής παιδικού πορνογραφικού υλικού και η επακόλουθη αναπαραγωγή και διακίνησή του, από τη μία, διαφοροποιεί αυτή την κατηγορία παιδεραστών από αυτούς που διαπράττουν σεξουαλικά εγκλήματα σε βάρος παιδιών και, από την άλλη, αποτελεί την έκφανση σημαντικών ψυχολογικών διαταραχών για το δράστη. Η κατ' επιλογή συλλογή πορνογραφικού υλικού τις περισσότερες φορές γίνεται με σκοπό τη διέγερση της φαντασίας των δραστών και τη σεξουαλική τους ικανοποίηση. Με άλλα λόγια, αποσκοπούν στην αύξηση της σεξουαλικής τους δραστηριότητας μέσα από εικόνες με παιδιά και στη συνέχεια να μοιραστούν τις φαντασιώσεις

59 Europol 2015β, 4, 7, 19.

τους online με άλλους. Ωστόσο, σε έρευνα που διεξήχθη από τους Quayle & Taylor σε δείγμα ανδρών που είχαν κατηγορηθεί για κατοχή υλικού παιδικής πορνογραφίας βρέθηκε πως η συλλογή πορνογραφικού υλικού ανηλίκων μέσω διαδικτύου δεν έχει κάποια απόλυτη σύνδεση με τη σεξουαλική διέγερση και ικανοποίηση του δράστη. Πολλές φορές συλλέγει υλικό με σκοπό να εμπλουτίσει τη συλλογή του με κάτι νέο. Με αυτή τη συμπεριφορά του συλλέκτη αναδεικνύεται και ο ρόλος της παιδικής πορνογραφίας ως προϊόντος εμπορεύσιμου και ως «τροπαίου» [60].

Έχουν υπάρξει αρκετές στοχευμένες αστυνομικές δράσεις εντός του Σκοτεινού Ιστού. Αρκετά μεγάλη ήταν η έρευνα που διεξήγαγε η Αμερικανική Αστυνομία για το Silk Road την περίοδο 2011-2013, η οποία κατέληξε στη σύλληψη του ιδρυτή της αγοράς από το FBI και στο κατέβασμά της από τον Σκοτεινό Ιστό[61]. Το Νοέμβριο του 2014 η Επιχείρηση Onymous, η οποία ήταν διεθνής αστυνομική συνεργασία 21 χωρών με τη συμμετοχή και το FBI και της Europol, στράφηκε εναντίον των αγορών του Σκοτεινού Ιστού που ήταν προσβάσιμες μέσω του Tor. Η επιχείρηση έληξε με την κατάσχεση 617 διευθύνσεων μαζί με Bitcoins αξίας 900.000€ και μετρητά, ναρκωτικά, χρυσό και ασήμι αξίας 180.000€, ενώ εκτός δράσης τέθηκαν 33 δημοφιλείς αγορές και forums, μεταξύ των οποίων και το Silk Road 2[62], και συνελήφθησαν 17 άτομα[63]. Το 2015 στο πλαίσιο της Επιχείρησης Babylon η Europol σε συνεργασία με τις ιταλικές αρχές ξεσκέπασε μια κρυμμένη υπηρεσία στον Σκοτεινό Ιστό που διευκόλυνε την ανταλλαγή υλικού σεξουαλικής κακοποίησης παιδιών. Οι αρχές προχώρησαν στην κατάσχεση 14.000 πορτοφολίων Bitcoin και του παιδοφιλικού υλικού που ανταλλασσόταν[64].

60 Όπως αναφέρεται στο Δανάη Αγγελή κ.ά. 2007, 23-24.
61 Kim Zetter 2013 (https://www.wired.com/2013/11/silk-road/).
62 Το Silk Road 2 ήταν ο διάδοχος του Silk Road. Πλέον είναι διαθέσιμος στον Σκοτεινό Ιστό και ο επόμενος διάδοχος του Silk Road, το Silk Road 3.
63 Europol 2015α, 52.
64 "Darknet hidden service for child sexual abuse material shut down", 2015 (https://www.europol.europa.eu/content/darknet-hidden-service-child-sexual-abuse-material-shut-down).

Β. Διάπραξη παραδοσιακών εγκλημάτων με άλλα τεχνολογικά μέσα με ιδιαίτερη έμφαση στο έγκλημα της απάτης

Η εγκληματικότητα, ωστόσο, δεν περιορίζεται αποκλειστικά στον Σκοτεινό Ιστό και οι δράστες μπορούν να εκμεταλλευτούν τις δυνατότητες όλο και νεότερων τεχνολογικών μέσων. Πλέον, με τη βοήθεια του Bluetooth μπορούν να υποκλαπούν τηλεφωνικές συνομιλίες και γενικά μπορεί να επιτευχθεί απομακρυσμένος έλεγχος του κινητού[65]. Οι τηλεφωνικές συνομιλίες ενός κινητού μπορούν να υποκλαπούν και με τη μέθοδο του cloning, κατά την οποία υποκλέπτονται οι κωδικοί ενός κινητού και αντιγράφεται η κάρτα SIM. Ο ωτακουστής δημιουργεί, ουσιαστικά, ένα αντίγραφο τηλεφώνου με το οποίο λαμβάνει και εκείνος τις κλήσεις που λαμβάνει και το κανονικό κινητό αποκτώντας τη δυνατότητα να ακούσει τη συνομιλία[66].

Η ολοένα και μεγαλύτερη εκμετάλλευση των τεχνολογικών εξελίξεων από τους εγκληματίες επιβεβαιώθηκε και από την προαναφερθείσα έρευνα του VGT, όπου βρέθηκε πως με αυτόν τον τρόπο προκύπτουν διάφορες μορφές διαδικτυακής σεξουαλικής εκμετάλλευσης παιδιών, όπως η αποπλάνηση (grooming) και η προσφορά χρημάτων για σεξ (solicitation), ο σεξουαλικός εκβιασμός, η σεξουαλική κακοποίηση παιδιού σε live streaming, καθώς και η διασπορά αυτοπαραγώμενου τολμηρού υλικού στα κοινωνικά δίκτυα. Τα κοινωνικά δίκτυα χρησιμοποιούνται κυρίως για τις αρχικές επαφές με τα υποψήφια θύματα, οι οποίες στη συνέχεια συνοδεύονται με κατά πρόσωπο εικονικά chats με σεξουαλικούς σκοπούς. Πλέον, η κακοποίηση παιδιών σε live streaming αποτελεί μια καθιερωμένη πραγματικότητα και όχι απλώς μια αναδυόμενη τάση. Οι ερωτηθέντες απάντησαν πως οι δράστες σεξουαλικής κακοποίησης εκμεταλλεύονται τις τεχνολογικές δυνατότητες ζωντανής μετάδοσης εικόνων και βίντεο. Αυ-

65 Κωνσταντίνος Βλαχόπουλος 2007, 73.
66 Μιράντα Λυσάνδρου 2010, 8 (www.efylakas.com/ archives/5623).

τό που συνέβαλε και, μάλιστα, χαρακτηρίστηκε ως σημαντικός παράγοντας στην ευρεία εξάπλωση του φαινομένου της κακοποίησης σε ζωντανή μετάδοση ήταν οι σχετικά υψηλές αμοιβές που παρέχονταν στους διοργανωτές σε αναπτυσσόμενες χώρες. Εκτός αυτού, όμως, αναφέρθηκαν και κάποιες περιπτώσεις μη εμπορικού streaming ανάμεσα σε μέλη ενός κλειστού δικτύου[67].

Απ' ό,τι είδαμε και από την έρευνα του VGT, τα κοινωνικά δίκτυα παίζουν και αυτά το δικό τους ρόλο στη διάπραξη εγκλημάτων. Τα σχετιζόμενα με τα κοινωνικά δίκτυα εγκλήματα είχαν μια αύξηση της τάξης του 780% στο Ηνωμένο Βασίλειο από το 2008 μέχρι το 2012. Το 2012 οι καταγγελίες που αφορούσαν αδικήματα που τελέστηκαν μέσω Facebook και Twitter ανέρχονταν στις 4908 σε σύγκριση με τις 556 που ήταν το 2008. Ανάμεσα στα δημοφιλέστερα αδικήματα που σχετίζονταν με τα κοινωνικά δίκτυα ήταν η παρενόχληση[68] και τα απειλητικά μηνύματα. Σε κάποιες περιοχές που βγήκαν πιο αναλυτικά οι αριθμοί καταγγελιών και τα αδικήματα υπάρχει μια πιο ολοκληρωμένη εικόνα για την έκταση του φαινομένου. Ενδεικτικά αναφέρονται το Tayside, όπου από τις συνολικά 66 καταγγελίες οι 44 περιλάμβαναν αισχρά ή απειλητικά μηνύματα, το Merryside, όπου οι 21 από τις συνολικά 76 καταγγελίες αφορούσαν τη διαδικτυακή παρενόχληση, και το Lancashire, όπου αναφέρθηκαν έξι απειλές δολοφονίας. Αναφέρθηκαν, ακόμη, αμέτρητα σεξουαλικά αδικήματα, συμπεριλαμβανομένης της αποπλάνησης, ρατσιστική συμπεριφορά και απάτες[69].

Το 2015 η Διεθνής Ένωση Αρχηγών της Αστυνομίας (International Association of Chiefs of Police) διεξήγαγε την έκτη ετήσια έρευνα για τη χρήση των κοινωνικών δικτύων από τις υπηρεσίες επιβολής του νόμου. Η διεξαγωγή της έρευνας έγινε σε 553

67 Europol 2015β, 6-7.
68 Η διαδικτυακή παρενόχληση αποτελεί αδίκημα στο Ηνωμένο Βασίλειο από το 1997 με το Protection from Harassment Act 1997 ["Stalking and harassment, χ.χ. (http://www.cps.gov.uk/legal/s_to_u/ stalking_and_harassment/#a02)].
69 Press Association 2012 (https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter).

υπηρεσίες από 44 κράτη. Τα ευρήματα ανέφεραν πως η συντριπτική πλειοψηφία χρησιμοποιεί τα κοινωνικά δίκτυα, ότι έχουν υιοθετήσει πολιτικές αναφορικά με αυτά και ότι βοήθησαν στη βελτίωση των σχέσεων της αστυνομίας με την υπόλοιπη κοινότητα. Τα ευρήματα της έρευνας που αφορούσαν το έγκλημα ήταν τα ακόλουθα. Σε ποσοστό 88.7% ανέφεραν πως η πιο κοινή χρήση των κοινωνικών δικτύων αφορά την αστυνομική έρευνα και σε ποσοστό 83.5% πως τα κοινωνικά δίκτυα τους βοήθησαν στην επίλυση εγκλημάτων εντός της περιοχής δικαιοδοσίας τους[70].

Οι ιστότοποι κοινωνικής δικτύωσης και τα διάφορα chatrooms, μπορούν να βοηθήσουν τους δράστες να προσεγγίσουν τα θύματά τους ευκολότερα. Πριν την εφεύρεση όλων αυτών των δικτύων η προσέγγιση θα έπρεπε να γίνει με φυσικό τρόπο, δηλαδή κατά πρόσωπο. Πλέον, λοιπόν, η προσέγγιση ενός παιδιού και οποιουδήποτε άλλου υποψηφίου θύματος για σεξουαλικούς σκοπούς, για εκβιασμό, για απειλές γενικότερα ή και συγκεκριμένα κατά της ζωής και για εξαπάτηση μπορεί να γίνει απομακρυσμένα μέσα από την οθόνη ενός υπολογιστή χωρίς να είναι απαραίτητη η φυσική παρουσία όλων των εμπλεκόμενων μερών, δηλαδή δράστη και θύματος, στον ίδιο χώρο. Όσον αφορά το έγκλημα της απάτης, το οποίο μπορεί να τελεστεί με πληθώρα τεχνολογικών μέσων προξενώντας οικονομική ζημία, το θύμα, ανάλογα με τη μορφή της απάτης, μπορεί να προσεγγιστεί μέσω ενός e-mail ή ενός SMS ή ακόμα και μέσω διαφόρων μηχανισμών καταγραφής ή παγίδευσης. Το διαδίκτυο βοηθάει πάρα πολύ στην τέλεση απατών και έτσι υπάρχουν πολλών ειδών διαδικτυακές απάτες, όπως αυτές οι οποίες σχετίζονται με τα clicks, με διαδικτυακούς πλειστηριασμούς, το phishing, το spamming κλπ. Άλλες απάτες σχετίζονται με πιστωτικές και χρεωστικές κάρτες και μηχανήματα αυτόματης ανάληψης. Κάθε μορφή απάτης, βέβαια, χωρίζεται και σε διάφορες άλλες υποκατηγορίες.

70 International Association of Chiefs of Police 2015 (http://www.iacpsocialmedia.org/Portals/1/documents/FULL%202015%20Social%20Media%20Survey%20Results.pdf).

Το phishing είναι από τις πιο ευρέως διαδεδομένες μεθόδους διαδικτυακής απάτης. Στόχος είναι η απόσπαση διάφορων εμπιστευτικών πληροφοριών, όπως προσωπικά ή οικονομικά δεδομένα, και η χρήση τους για την πρόκληση βλάβης στην περιουσία των θυμάτων τους[71]. Πιο συγκεκριμένα, οι πληροφορίες που επιχειρεί να αποσπάσει ο δράστης μπορεί να είναι κωδικοί πιστωτικών καρτών, κωδικοί πρόσβασης κλπ. Το υποψήφιο θύμα λαμβάνει ένα e-mail, π.χ. από κάποιον που ισχυρίζεται πως δουλεύει στην υπηρεσία homebanking της τράπεζάς του. Στο μήνυμα τον πληροφορεί πως γίνονται κάποιες εργασίες συντήρησης στο σύστημα και του λέει να επισκεφθεί τον επισυναπτόμενο στο μήνυμα σύνδεσμο, που είναι η σελίδα της υπηρεσίας homebanking, και να επιβεβαιώσει τους κωδικούς πρόσβασης. Το θύμα, πλέον, πατάει στο σύνδεσμο και οδηγείται σε διαδικτυακή τοποθεσία που είναι αντίγραφο της κανονικής και μόλις τα στοιχεία πληκτρολογηθούν, υποκλέπτονται. Πέραν αυτής της κύριας μορφής υπάρχουν και κάποιες παραλλαγές του phishing. Υπάρχει παραλλαγή με e-mail το οποίο στέλνεται μαζί με κακόβουλο λογισμικό και μια άλλη η οποία παίρνει τη μορφή αναδυόμενου παραθύρου στην πραγματική διαδικτυακή τοποθεσία του homebanking. Και οι δύο παραλλαγές, όπως και η κύρια μορφή, έχουν ως σκοπό την υποκλοπή εμπιστευτικών πληροφοριών[72]. Άλλες παραλλαγές του phishing εντοπίζονται σε διαφορετικά τεχνολογικά μέσα.

Μια άλλη μορφή απάτης είναι αυτή που συνδέεται με τις πιστωτικές κάρτες. Η χρήση των πιστωτικών καρτών για διάφορες συναλλαγές στο διαδίκτυο έχει διευκολύνει τη διάπραξη εγκλημάτων. Μέσω της τεχνολογίας “websniffer” η μετάδοση δεδομένων παρακολουθείται και γίνεται αυτόματη ανάκτηση των 16ψήφιων αριθμών πιστωτικών καρτών. Παράλληλα, στο διαδίκτυο υπάρχει και η δυνατότητα αγοραπωλησίας κωδικών που έχουν υποκλαπεί. Τέλος, υπάρχουν εφαρμογές λογισμικού ελεύ-

71 Μαρίνος Παπαδόπουλος 2005, 1-2.
72 Κωνσταντίνος Βλαχόπουλος 2007, 58-60.

θερες στο διαδίκτυο που δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών και επιβεβαιώνουν τη γνησιότητά τους[73].

Τα μηχανήματα αυτόματης ανάληψης δεν θα μπορούσαν να λείπουν από τις απάτες. Έχουν καταγραφεί περιπτώσεις τοποθέτησης μηχανισμών παγίδευσης της κάρτας και τοποθέτησης μικροκαμερών, οι οποίες δε γίνονται αντιληπτές από το χρήστη του μηχανήματος και καταγράφουν το PIN, τον αριθμό της κάρτας και τα δεδομένα που αναγράφονται στην οθόνη. Ακόμη, έχουν αναφερθεί μέχρι και περιπτώσεις τοποθέτησης πρόσθετων πληκτρολογίων που είναι πανομοιότυπα με τα πραγματικά και κλέβουν τα PIN που πληκτρολογεί το θύμα[74].

Αυτό που πρέπει να έχουμε κατά νου είναι ότι αρκετές φορές η οικονομική ζημία που προκαλείται στα θύματα από τις διαφόρων ειδών τεχνολογικά υποβοηθούμενες απάτες μπορεί να είναι πάρα πολύ μεγάλη. Το 2011 το συνολικό κόστος των διαδικτυακών απατών στις ΗΠΑ ανερχόταν στα 485 εκατομμύρια δολάρια[75]. Το 2010 είχε εκτιμηθεί πως οι διαδικτυακές απάτες κόστιζαν ετησίως 100 δισεκατομμύρια δολάρια σε παγκόσμιο επίπεδο, ενώ για το 2013 η αρχική αυτή εκτίμηση ήταν τουλάχιστον διπλάσια[76]. Θεαματική ήταν η άνοδος των απατών σχετικά με ATM μέσα στο 2015 σε όλη την Ευρωπαϊκή Ένωση. Αυτές οι απάτες γίνονταν χάρη στη βοήθεια διαφόρων συσκευών που τοποθετούνταν στο ATM. Συνολικά μέσα στο 2015 έγιναν 18.738 καταγγελίες, οι οποίες αυξήθηκαν κατά 19% σε σχέση με το 2014, και οι συνολικές απώλειες ανέρχονταν στα 327.48 εκατομμύρια ευρώ[77]. Τέλος, σύμφωνα με στοιχεία του Financial Fraud Action UK (FFA UK), οι οικονομικές απώλειες από απάτες που

73 Το ίδιο, 67.
74 Το ίδιο, 75.
75 «Κόστος 485 εκατομμύρια είχαν οι διαδικτυακές απάτες το 2011 στις ΗΠΑ», 2012 (http://www.kathimerini.gr/77278/article/texnologia/diadiktyo/kostos-485-ekat-dolaria-eixan-oi-diadiktyakes-apates-brto-2011-stis-hpa).
76 Henry McDonald 2013 (https://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars).
77 Brian Krebs 2016 (http://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/).

αφορούν κάρτες πληρωμών, τις εξ αποστάσεως τραπεζικές συναλλαγές και τις επιταγές ανήλθαν συνολικά στις 775 εκατομμύρια λίρες για το 2015[78].

Σε διεθνές επίπεδο έχει αναληφθεί δράση και για τις απάτες και κυρίως για αυτές που σχετίζονται με κάρτες πληρωμών. Το 2011 η παγκόσμια επιχείρηση "Night Clone" έληξε επιτυχώς με σχεδόν 70 συλλήψεις στην ΕΕ και εκτός αυτής. Ο αντίκτυπος ήταν τόσο μεγάλος που για αρκετούς μήνες σταμάτησαν οι παράνομες δραστηριότητες άλλων οργανωμένων εγκληματικών ομάδων[79]. Το 2014 το Project Sandpiper, που χρηματοδοτήθηκε από την ΕΕ, κατέληξε σε 59 συλλήψεις μαζί με τη διάλυση πέντε οργανωμένων ομάδων που εκμεταλλεύονταν κλεμμένα στοιχεία από κάρτες. Τα στοιχεία που ανακτήθηκαν προέρχονταν από πάνω από 50.000 κάρτες και η αξία ήταν πάνω από 30 εκατομμύρια ευρώ[80]. Επιτυχείς δράσεις, φυσικά, έχουν αναληφθεί και για άλλου είδους απάτες που τελούνται με νέα μέσα, όπως το phishing[81] και οι απάτες σε ATM[82].

78 FFA UK 2016, 10.
79 Europol 2012, 9.
80 Europol 2015α, 33.
81 Για τη σύλληψη υπόπτων μελών ευρωπαϊκού κυκλώματος voice phishing (παραλλαγή του phishing που τελείται μέσω τηλεφώνου) βλ. το ίδιο, σελίδα 38.
82 Για την εξάρθρωση διεθνούς εγκληματικής ομάδας υπεύθυνης για ATM skimming και ξέπλυμα χρήματος βλ. "International criminal group behind ATM skimming attacks dismantled", 2016 (https://www.europol.europa.eu/content/international-criminal-group-behind-atm-skimming-attacks-dismantled).

2.2. Εγκλήματα που προκύπτουν από τη χρήση της σύγχρονης τεχνολογίας

2.2.1. Hacking

Εξετάζοντας ιστορικά την απαρχή των hackers, βλέπουμε ότι αρχικά δεν αποκαλούσαν τους εαυτούς τους με αυτό το όνομα ή κάποιο άλλο ιδιαίτερο όνομα. Μετά το 1980 επινοήθηκε αναδρομικά από κάποιον δικό τους το προσωνύμιο «Αληθινοί Προγραμματιστές». Από το 1945 και έπειτα η τεχνολογία των υπολογιστών έχει προσεγγίσει τα πιο λαμπρά και τα πιο δημιουργικά μυαλά παγκοσμίως. Οι Αληθινοί Προγραμματιστές προήλθαν από τους χώρους της φυσικής και της μηχανικής, ενώ συχνά ασχολούνταν ερασιτεχνικά με το ραδιόφωνο. Από το τέλος του Β' Παγκοσμίου Πολέμου μέχρι και τις αρχές της δεκαετίας του '70 ήταν η κυρίαρχη κουλτούρα στο χώρο της πληροφορικής[83].

Ο όρος "hacker" εντοπίζεται πρώτη φορά στη Λέσχη Tech Model Rail Road και στο Εργαστήριο Τεχνητής Νοημοσύνης του MIT. Σύμφωνα με αυτόν τον ορισμό, hacker ονομάζονταν όλοι οι ειδήμονες προγραμματιστές υπολογιστών οι οποίοι συνδέονταν με τη δημιουργία του ARPANET[84] και την ανάπτυξη του διαδικτύου. Οι hackers δεν ανταποκρίνονται στην εικόνα που βγάζουν τα μέσα μαζικής ενημέρωσης για αυτούς, δηλαδή άτομα παράτολμα με κλίσεις κοινωνικά αποδοκιμαστέες με στόχο το σπάσιμο κωδίκων, την παράνομη διείσδυση σε συστήματα ή την πρόκληση ολέθρου στην ηλε-

83 Eric S. Raymond, 3.

84 ARPANET (Advanced Research Projects Agency Network) ονομαζόταν το δίκτυο που δημιουργήθηκε από την ARPA (Advanced Research Projects Agency) αρχικά για τη σύνδεση των πανεπιστημιακών υπολογιστών. Η ARPA δημιουργήθηκε στις 7 Φεβρουαρίου 1958 από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών της Αμερικής με σκοπό την προώθηση και την εξασφάλιση της επιστημονικής έρευνας σε όλους τους κλάδους καθώς και για την ανάπτυξη της τεχνολογίας σε όσα επίπεδα μπορούσαν να συσχετιστούν με την άμυνα. Η δημιουργία της ARPA έγινε με αφορμή την εκτόξευση του τεχνητού δορυφόρου Sputnik από τη Σοβιετική Ένωση το 1957, καθώς έτσι φαινόταν ότι οι Ηνωμένες Πολιτείες είχαν έρθει στη δεύτερη θέση όσον αφορά την τεχνολογία. Η ARPA (που αργότερα μετονομάστηκε σε DARPA) χρηματοδότησε ερευνητικά προγράμματα στα πανεπιστήμια σε ολόκληρη τη χώρα. Αρχικά η πρόσβαση στο ARPANET ήταν περιορισμένη σε πανεπιστημιακούς και σε άλλους ερευνητές. Μετά τη χρηματοδότηση ο αριθμός των ερευνητών αυξήθηκε και η ζήτηση υπολογιστών ξεπέρασε τις προμήθειες. Εκείνη την εποχή η πληροφορική ήταν ένας από τους τομείς που είχε πολύ περιορισμένο ανθρώπινο δυναμικό για έρευνα. (Michael A. Banks 2008, σελίδες 2-3).

κτρονική κυκλοφορία. Αυτοί που έχουν έναν τέτοιο τρόπο συμπεριφοράς ονομάζονται “crackers” και απορρίπτονται από την κυρίαρχη κουλτούρα των hackers. Ένας κατά κάποιον τρόπο ταυτολογικός ορισμός που δίνεται για τη λέξη “hacker” είναι πως hackers ονομάζονται εκείνοι που αναγνωρίζονται ως τέτοιοι από την κουλτούρα των hackers[85].

Υπέρτατη αξία της κουλτούρας των hackers είναι η ελευθερία και συγκεκριμένα η ελευθερία της δημιουργίας, η ελευθερία της οικειοποίησης της οποιασδήποτε διαθέσιμης γνώσης και η ελευθερία διανομής της κάτω από οποιαδήποτε μορφή και μέσω ενός οποιουδήποτε καναλιού που επιλέγει ο hacker. Για πολλούς hackers η ελευθερία δεν είναι η μοναδική αξία, αλλά είναι βασικό στοιχείο της αντίληψής τους για τον κόσμο και της πρακτικής που έχουν, ενώ είναι πολλοί και αυτοί που πατώντας σε αυτήν την αρχή της ελευθερίας επικαλούνται το δικαίωμα επιλογής της εμπορικής ανάπτυξης των καινοτομιών τους υπό την προϋπόθεση ότι δεν προδίδουν την πιο θεμελιακή αρχή τους, που είναι η ανοιχτή πρόσβαση σε όλες τις πληροφορίες του προγράμματος ομού με την ελευθερία τροποποίησης του προγράμματος. Η ελευθερία οδηγεί σε μια οικονομία του δώρου λόγω του συνδυασμού της με τη συνεργασία μέσα από την πρακτική της κουλτούρας του δώρου. Ο hacker θα βάλει στο διαδίκτυο τη δική του συμβολή στην ανάπτυξη του εκάστοτε λογισμικού και σαν αποτέλεσμα προσδοκά αμοιβαιότητα. Αυτή η κουλτούρα του δώρου στους hackers έχει μια ξεχωριστή δική της ιδιαιτερότητα, επειδή το κύρος, η υπόληψη και η κοινωνική εκτίμηση είναι συνδεδεμένα με τη σπουδαιότητα του δώρου το οποίο δίδεται στην κοινότητα. Αυτά συνιστούν, εκτός από την αναμενόμενη ανταμοιβή για τη γενναιοδωρία του, και την άμεση ανταμοιβή του αναφορικά με το ότι επέδειξε στους υπόλοιπους την ευφυία του. Ακόμη, υπάρχει ανταμοιβή που είναι συνδεδεμένη με το δώρο, το οποίο εκτός από

85 Manuel Castells 2001 (έκδοση 2005), 69.

ανταλλακτική αξία προσλαμβάνει και αξία χρήσης[86].

Η κουλτούρα των hackers ως σύνολο είναι παγκόσμια και εικονική και έχει ως οργανωτικό θεμέλιο το διαδίκτυο. Οι περισσότεροι γνωρίζονται μεταξύ τους αποκλειστικά με τα ονόματα που χρησιμοποιούν στο διαδίκτυο και αυτό γίνεται όχι επειδή θέλουν να κρύψουν την πραγματική τους ταυτότητα, αλλά επειδή η ταυτότητα που έχουν ως hackers είναι το όνομα που χρησιμοποιούν στο διαδίκτυο. Η ανεπισημότητα και η εικονικότητα είναι βασικά γνωρίσματα της κουλτούρας των hackers, παρόλο που ο μεγαλύτερος βαθμός αναγνώρισης της αξίας τους είναι συνδεδεμένος με την ταυτοποίηση με τα πραγματικά τους ονόματα. Η κουλτούρα των hackers στηρίζεται στην ενεργή συμμετοχή σε μια κοινότητα, που οικοδομείται γύρω από έθιμα και αρχές άτυπης κοινωνικής οργάνωσης. Η κοινότητα αποκλείει το χρήμα, τα επίσημα δικαιώματα ιδιοκτησίας ή τη θεσμική εξουσία σαν πηγές κύρους και υπόληψης. Ουσιαστικά είναι αποδεκτή η ιεραρχία της αξίας και της αρχαιότητας μόνο σε περιπτώσεις που αυτή η μορφή εξουσίας ασκείται για τη συνολική ευδοκίμηση της κοινότητας, με αποτέλεσμα εμφανίζονται συνεχώς νέες φυλές[87].

Την κοινότητα των hackers διέπουν έξι βασικοί ιδιότυποι κανόνες ηθικής, τους οποίους κατέγραψε ο Steven Levy. Οι κανόνες αυτοί έχουν ως εξής: 1. «Η πρόσβαση στους υπολογιστές –καθώς και σε οτιδήποτε που ενδεχομένως θα σε διδάξει κάτι σχετικά με τον τρόπο που λειτουργεί ο κόσμος- θα πρέπει να είναι απεριόριστη και ολοκληρωτική. Πάντα να υπακούς στην προσταγή που σου λέει να έχεις ενεργό ρόλο». 2. «Όλες οι πληροφορίες θα πρέπει να είναι ελεύθερες». 3. «Να μην εμπιστεύεσαι την εξουσία.-Να προωθείς την αποκέντρωση». 4. «Οι hackers θα πρέπει να κρίνονται από τη δράση τους και όχι από μη πραγματικά κριτήρια, όπως πτυχία, ηλικία, φυλή ή κοι-

86 Το ίδιο, 75-76.
87 Το ίδιο, 76-77.

νωνική θέση». 5. «Μπορείς να δημιουργήσεις τέχνη και ομορφιά σε έναν υπολογιστή». 6. «Οι υπολογιστές μπορούν να αλλάξουν τη ζωή σου προς το καλύτερο»[88].

Οι τεχνικές διείσδυσης σε ένα δίκτυο ηλεκτρονικών υπολογιστών, τις οποίες χρησιμοποιούν οι hackers, εξελίσσονται παράλληλα με την ανάπτυξη των υπολογιστικών συστημάτων. Μία αρκετά κοινή τεχνική είναι η εκμετάλλευση των cookies, τα οποία είναι πολύ μικρά αρχεία κειμένου που τοποθετούνται στον υπολογιστή από τις διάφορες επισκέψεις του χρήστη σε διαδικτυακούς ιστοτόπους και περιέχουν πληροφορίες αναφορικά με τις δραστηριότητές του, τα στοιχεία του, τις συνήθειές του κλπ. Αν ένα αρχείο cookie περιλαμβάνει το όνομα χρήστη και τον κωδικό πρόσβασης για κάποια υπηρεσία, ο hacker μπορεί να τα ανακτήσει εκμεταλλευόμενος κάποια ευπάθεια του φυλλομετρητή ή του λειτουργικού συστήματος. Άλλη τεχνική είναι η ανίχνευση των δικτυακών υπηρεσιών συστημάτων (probes, scans). Οι hackers θέλουν να εντοπίσουν πληροφορίες για το σύστημα που θέλουν να επιτεθούν και για να το επιτύχουν αυτό χρησιμοποιούν μια τεχνική που ονομάζεται «σάρωση θυρών» (port scanning). Μέσω της σάρωσης θυρών αποστέλλονται ερωτήματα σε διακομιστές για τη λήψη πληροφοριών αναφορικά με τις προσφερόμενες υπηρεσίες και το χρησιμοποιούμενο επίπεδο ασφάλειας. Αυτές οι πληροφορίες δίνουν τη δυνατότητα στον επιτιθέμενο να παραβιάσει την ασφάλεια του συστήματος, εκμεταλλευόμενος τις αδυναμίες του λειτουργικού συστήματος ή άλλων προσφερόμενων υπηρεσιών[89].

Η τρίτη συχνότερη τεχνική αποτελεί η χρήση ανιχνευτών δικτυακών πακέτων (packet sniffers). Μέσω των packet sniffers μπορούν να ανιχνεύουν όλα τα πακέτα που κυκλοφορούν στο διαδίκτυο και σε περίπτωση που αυτά δεν είναι κρυπτογραφημένα, μπορούν να αποσπάσουν πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών κλπ. Ακόμη μπορούν να λάβουν πληροφορίες για την τοπολογία

88 Steven Levy 1984, 27-33.
89 Κωνσταντίνος Βλαχόπουλος 2007, 40-41.

ενός δικτύου, τις προσφερόμενες υπηρεσίες και τον αριθμό των συνδεδεμένων στο δίκτυο υπολογιστών. Τέταρτη τεχνική είναι οι πλαστές διευθύνσεις IP (IP spoofing). Σε αυτές τις επιθέσεις γίνεται παρέμβαση στις επικεφαλίδες των διακινούμενων σε κάποιο δίκτυο πακέτων και αυτές τροποποιούνται, ώστε το μήνυμα να φαίνεται πως προέρχεται από αξιόπιστη πηγή. Μέσω αυτής της μεθόδου καταφέρνουν να χρησιμοποιήσουν μια διεύθυνση IP εντός του εύρους των διευθύνσεων που εμπιστευόμαστε αποκτώντας πρόσβαση σε υπηρεσίες προοριζόμενες για έμπιστους χρήστες του δικτύου. Τελευταία τεχνική είναι η επίθεση σε επίπεδο εφαρμογής. Σε αυτές τις επιθέσεις εκμεταλλεύονται τις αδυναμίες των δικτυακών εφαρμογών. Παράδειγμα μπορούν να αποτελέσουν τα προβλήματα ασφαλείας που παρουσιάζουν συχνά διάφοροι φυλλομετρητές, ενώ σημαντικές αδυναμίες στον τομέα της ασφάλειας παρουσιάζονται στις σύγχρονες γλώσσες προγραμματισμού για τη δημιουργία δικτύων με δυναμικό περιεχόμενο[90].

Οι hackers εκμεταλλεύονται μια αδυναμία που μπορεί να παρουσιάζει ο στόχος, δηλαδή ένα σημείο που μπορεί να τους δώσει πρόσβαση μέσα σε ένα σύστημα. Σε περιπτώσεις οργανισμών οι ευπάθειες ενός συστήματος δε γίνονται γνωστές από την αρχή, αλλά κυρίως εντοπίζονται και γίνεται η λήψη μέτρων μετά την εκμετάλλευσή τους από κάποιον επιτιθέμενο. Φυσικά, μπορούν να γίνουν γνωστές και από την ενδελεχή μελέτη της ασφάλειας των συστημάτων υπολογιστών και δικτύων του οργανισμού. Ένας ορθολογικός σχεδιασμός για την επίτευξη της ασφάλειας ενός συστήματος περιλαμβάνει τουλάχιστον τη δυνατότητα κρυπτογράφησης των δεδομένων και ασφαλείς τεχνικές ελέγχου πρόσβασης και αυθεντικοποίησης, οι οποίες μπορεί να είναι, π.χ., η επιλογή σωστών συνθηματικών και η χρήση εναλλακτικών μεθόδων ταυτοποίησης, όπως η βιομετρία και η έξυπνη κάρτα[91].

90 Το ίδιο, 41-42.
91 Το ίδιο, 28-29.

Αυτοί που ασκούν το hacking το βλέπουν ως μια νοοτροπία που είναι εμφανής γενικότερα στα επιστημονικά και τεχνολογικά εγχειρήματα και όχι μόνο στον τομέα των υπολογιστών. Όπως ανέφερε ένας Ολλανδός hacker, το hacking δε σχετίζεται μόνο με τους υπολογιστές αλλά με κάθε πεδίο της τεχνολογίας. Όταν, για παράδειγμα, κάποιος δεν έχει μαζί του μια κατσαρόλα να βράσει νερό και χρησιμοποιεί τη μηχανή του καφέ, τότε αυτό είναι hacking. Ουσιαστικά η τεχνολογία χρησιμοποιείται με έναν τρόπο που δεν είναι προβλεπόμενος. Αν κάποιος χρησιμοποιήσει το τηλέφωνο με έναν μη προβλεπόμενο τρόπο, τότε αυτό είναι hacking. Αν κάποιος χρησιμοποιήσει τις ικανότητές του ως μηχανικού αυτοκινήτων προκειμένου να φτιάξει τη μηχανή του με τρόπο που να κάνει πράγματα πέραν αυτών που υποτίθεται ότι πρέπει να κάνει, τότε αυτό είναι hacking. Το hacking, κατά τα λεγόμενά του, μπορεί να αφορά από υπολογιστές, τηλέφωνα, κλειδαριές, μαγνητικές κάρτες μέχρι οτιδήποτε άλλο[92].

Η κύρια νομική αντιμετώπιση του hacking γίνεται μέσω της ποινικής οδού. Η πρώτη χώρα που νομοθέτησε για το πληροφορικό έγκλημα με ποινικοποίηση του hacking από την πρώτη στιγμή της τέλεσής του ήταν οι Ηνωμένες Πολιτείες. Συγκεκριμένα, στη Φλόριντα και στην Αριζόνα υπήρξε ήδη από το 1978 ποινικοποίηση και της απλής παρείσδυσης σε υπολογιστή ασχέτως των κινήτρων ή των ενεργειών που θα ακολουθούσαν. Παράλληλα η ποινικοποίηση όδευε και σε ομοσπονδιακό επίπεδο με τις νομοθετικές πράξεις του 1984 και του 1986[93]. Στο ελληνικό δίκαιο το hacking αντιμετωπίζεται με το άρθρο 370Γ, το οποίο πλέον αφορά σχεδόν εξ ολοκλήρου τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικό σύστημα και ως κυρώσεις προβλέπονται μόνο ποινές φυλάκισης[94].

Με την ποινικοποίηση του hacking εγείρονται έντονοι προβληματισμοί αναφορικά με το αν βρίσκεται εντός των ορίων των κοινωνικών αξιών και της ηθικής της σύγ-

92 Paul A. Taylor 1998, 414.
93 Γρηγόρης Λάζος 2001, 106.
94 Νόμος 4411/2016.

χρονης εποχής. Θα μπορούσε να υποστηριχθεί πως το hacking είναι ανήθικο λόγω της παραβίασης της αξιοπρέπειας αυτών που δούλεψαν, προκειμένου να παράγουν κάτι χρήσιμο για το οποίο προσδοκούν να έχουν κάποιον έλεγχο, ή είναι ανήθικο εξαιτίας της παραβίασης του δικαιώματος της ιδιωτικότητας μια και υπάρχουν προσωπικά δεδομένα μέσα στον υπολογιστή. Ωστόσο, υπάρχει και μία αντίθετη άποψη με την πρόταση μίας «εναλλακτικής ηθικής», σύμφωνα με την οποία το hacking εκφράζει μία θεμελιώδη ανθρώπινη παρόρμηση για το νέο και για την άρνηση του αυτονόητου και του κατεστημένου[95].

Τα κυριότερα επιχειρήματα υπέρ της δημιουργίας αδικήματος για την απρόσκλητη είσοδο σε υπολογιστή είναι πως, δεδομένης της μεγάλης και αυξανόμενης σημαντικότητας των υπολογιστών στη σύγχρονη κοινωνία, είναι καλό για το δημόσιο συμφέρον να μη φοβούνται αυτοί που χρησιμοποιούν υπολογιστές και βασίζονται σε αυτούς για το ότι κάποιοι άλλοι μπορεί να αποκτήσουν πρόσβαση σε υλικό που είναι αποθηκευμένο εκεί και ειδικά αν οι πληροφορίες αυτές είναι ευαίσθητες ή εμπιστευτικές. Μεγάλοι κίνδυνοι τίθενται όταν οι hackers διαταράσσουν τη λειτουργία των υπολογιστών στον τομέα της άμυνας, των πυρηνικών, της εναέριας κυκλοφορίας ή των υπηρεσιών υγείας. Ο hacker, πέρα από οποιαδήποτε δόλια πρόθεση, θα μπορούσε να αλλοιώσει ή να καταστρέψει κατά λάθος πληροφορίες που είναι αποθηκευμένες στον υπολογιστή. Από την άλλη μεριά, ωστόσο, υπάρχει και η άποψη που αναφέρει πως δεν θα έπρεπε να δημιουργηθεί αδίκημα που να αφορά το hacking, Αρκετοί υποστηρίζουν πως το hacking είναι μία σχετικά αβλαβής αναδημιουργία και ότι ίσως παρέχει περισσότερα οφέλη προς τους χρήστες υπολογιστών με το να υποδεικνύουν τις αδυναμίες της ασφάλειας[96].

95 Γρηγόρης Λάζος 2001, 107-108.
96 Martin Wasik 1991, 75.

Μια πολύ γνωστή περίπτωση hacking με διεθνείς διαστάσεις ήταν αυτή του Karl Koch. Ο Karl Koch ήταν υπάλληλος της Χριστιανοδημοκρατικής Ένωσης και στρατολογούσε και άλλους hackers που έκαναν εισβολή σε εργαστήρια στρατιωτικών ερευνών στις Ηνωμένες Πολιτείες και στην Ευρώπη κλέβοντας απόρρητα σχέδια και πουλώντας τα αργότερα στην KGB. Ο Koch και οι υπόλοιποι κατάφεραν να εισβάλουν ακόμα και σε απόρρητες περιοχές της NASA, στην GTE-Thompson -κατασκευάστριας των πυραύλων Exosset- και στη Philips France. Χρησιμοποιούσαν τους υπολογιστές του εργαστηρίου σαν ορμητήριο για την εισβολή τους σε άλλα εργαστήρια της περιοχής. Ξεκίνησε μία μακρόχρονη καταδίωξη στον κυβερνοχώρο, ενώ ήταν ιδιαίτερα δύσκολη η διαδικασία του εντοπισμού τους καθώς πριν φτάσουν το στόχο τους προκειμένου να καλυφθούν συνδέονταν από διαφορετικούς servers από διαφορετικές χώρες, δηλαδή έμπαιναν από τη Γερμανία, συνδέονταν με τη Γαλλία και από εκεί μετά στην Αυστραλία, στις Ηνωμένες Πολιτείες και αλλού. Στο τέλος οι αρχές συνέλαβαν όλη την ομάδα, αλλά ο Koch βρέθηκε νεκρός κάτω από μυστηριώδεις συνθήκες σε ένα δάσος έξω από το Ανόβερο. Επίσημη καταγεγραμμένη αιτία θανάτου από την αστυνομία ήταν η αυτοκτονία[97].

97 Ανθοζωή Χάιδου 2003, 104-105.

2.2.2. Κακόβουλο λογισμικό

Η διασπορά κακόβουλου λογισμικού είναι ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του διαδικτύου και γενικότερα των ηλεκτρονικών υπολογιστών. Μια διαφορετική ονομασία που μπορεί να χρησιμοποιηθεί για το κακόβουλο λογισμικό είναι ο όρος «κακόβουλος κώδικας» (malicious code). Ο κακόβουλος κώδικας είναι ένας υπολογιστικός κώδικας που γράφτηκε με μοναδικό σκοπό να προκαλέσει ζημιά σε κάποιο μηχάνημα ή να εισβάλει στο μηχάνημα και να κλέψει πληροφορίες. Τα κυριότερα είδη του κακόβουλου κώδικα είναι οι ιοί (viruses), τα σκουλήκια (worms) και οι Δούρειοι Ίπποι (Trojans). Κάποιες από αυτές τις μορφές μπορεί να μοιράζονται κοινές τεχνικές ή σκοπούς[98]. Υπάρχουν διάφορα κίνητρα πίσω από τη διασπορά κακόβουλου λογισμικού. Κάποιοι το βλέπουν σαν παιχνίδι και διασκεδάζουν αδιαφορώντας για τις συνέπειες, άλλοι μπορεί να το κάνουν για εκδίκηση (αν πρόκειται, π.χ. για δυσαρεστημένους υπαλλήλους) και άλλοι το κάνουν από πολιτικά ή καθαρά ιδεολογικά κίνητρα[99].

Ένας ορισμός για τους υπολογιστικούς ιούς δόθηκε για πρώτη φορά το 1984 από τον Fred Cohen. Ο Cohen ανέφερε πως ως «ιός» ορίζεται ένα πρόγραμμα που μπορεί να «μολύνει» άλλα προγράμματα τροποποιώντας τα με τέτοιον τρόπο, ώστε να μπορούν να συμπεριλάβουν ένα εξελιγμένο αντίγραφό του[100]. Οι ιοί έχουν δύο βασικές ιδιότητες. Η πρώτη ιδιότητα, η οποία αναφέρεται ήδη από τον ορισμό του Fred Cohen, είναι η «μόλυνση». Η «μόλυνση» είναι η ικανότητα του ιού να αναπαράγεται από μόνος του και στη συνέχεια να προσκολλάται σε άλλα προγράμματα με αποτέλεσμα να πολλαπλασιάζεται εντός του υπολογιστή. Η δεύτερη ιδιότητα των ιών είναι η «λειτουργία». Αυτή η ιδιότητα, όπως αναφέρει και το όνομά της, αφορά μια συγκεκριμένη λειτουργία που εκτελούν οι ιοί, η οποία έχει χαρακτήρα είτε απλώς ενοχλη-

98 Eric J. Sinrod & William P. Reilly 2000, 215.
99 Ανδρέας Αργυρόπουλος 2001, 51.
100 Fred Cohen 1987, 23.

τικό είτε κατάστροφικό. Η «δράση» του ιού ξεκινάει με τη «μόλυνση», συνεχίζει με τη «λειτουργία» και στο τέλος επιστρέφει στο πρόγραμμα στο οποίο είχε αρχικά διεισδύσει. Ο πολλαπλασιασμός του ιού γίνεται συνήθως με ένα συγκεκριμένο τρόπο. Αναζητά ένα πρόγραμμα που δεν έχει μολυνθεί και αφού το βρει, του μεταδίδει ένα αντίγραφό του. Το μολυσμένο πρόγραμμα μετατρέπεται σε «φορέα» του και ακολούθως έχει τη δυνατότητα να μολύνει άλλα «υγιή» προγράμματα[101].

Μια κατηγοριοποίηση των ιών μπορεί να γίνει με βάση τον τρόπο ανάπτυξής τους μέσα στο σύστημα. Η πρώτη κατηγορία αναφέρεται στους ιούς που μεταγράφουν το δικό τους κωδικό προγράμματος σε τμήμα του προγράμματος που διεισδύουν επιτυγχάνοντας τη διατάραξη του προγράμματος αυτού, ώστε αυτό να μην μπορεί να «τρέξει». Η δεύτερη κατηγορία αφορά τους ιούς που παράγουν αντίγραφό τους στην αρχή, στη μέση ή στο τέλος κάποιου προγράμματος. Το πρόγραμμα εξακολουθεί να διατηρεί τη δυνατότητα να «τρέχει», αλλά καταλαμβάνει διαθέσιμο αποθηκευτικό χώρο, πράγμα το οποίο δεν το παρατηρεί ο χρήστης από την αρχή. Η τρίτη κατηγορία αφορά τους ιούς που αρχικά προσκολλώνται στο σκληρό δίσκο και στη συνέχεια εξαπλώνονται στα υπόλοιπα προγράμματα του υπολογιστή. Οι ιοί αυτής της κατηγορίας θεωρούνται «ύπουλοι», επειδή δε γίνονται αμέσως αντιληπτοί, και έχουν τη δυνατότητα ενεργοποίησης με κάθε χρησιμοποίηση του συστήματος και όχι απλώς με το «κατέβασμα» κάποιου μολυσμένου προγράμματος[102].

Φυσικά μπορούν να υπάρξουν και άλλες κατηγοριοποιήσεις των ιών. Μια διαφορετική κατηγοριοποίηση αναφέρει έξι βασικές μορφές ηλεκτρονικών ιών. Η πρώτη μορφή είναι οι file infectors ή parasitic viruses, οι οποίοι μολύνουν ένα πρόγραμμα που εκτελείται προσθέτοντάς του κακόβουλο κώδικα. Την ίδια στιγμή γίνεται τροποποίηση του αρχείου που φιλοξενεί τον ιό, προκειμένου να διασφαλιστεί πως ο κώδικας του ι-

101 Ανδρέας Αργυρόπουλος 2001, 44.
102 Το ίδιο, 45-46.

ού είναι αυτός που θα εκτελεστεί πρώτος. Οι ιοί αυτής της κατηγορίας μπορούν περαιτέρω να διακριθούν σε memory-resident, που παραμένουν στη μνήμη του υπολογιστή διατηρώντας τη δυνατότητα να μολύνουν οποιοδήποτε πρόγραμμα επιλέξει προς εκτέλεση ο χρήστης, και σε non-resident ή direct-action viruses, οι οποίοι αν και δεν παραμένουν στη μνήμη του υπολογιστή, προσκολλώνται σε κάποιο υπάρχον πρόγραμμα και μεταδίδονται μόλις ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα. Δεύτερη βασική μορφή αποτελεί ο boot sector virus, ο οποίος εντοπίζεται σε διάφορες συσκευές βοηθητικής μνήμης (π.χ. δισκέτα), στον Τομέα Εκκίνησης (boot sector) ή στο MBR (Master Boot Record)[103] του σκληρού δίσκου. Αυτός ο ιός φορτώνεται στη μνήμη του υπολογιστή κατά την εκκίνηση (boot) του συστήματος και στη συνέχεια μολύνει κάθε δίσκο ή δισκέτα που θα χρησιμοποιηθεί στον υπολογιστή. Τρίτη βασική μορφή είναι οι multi-partite viruses, οι οποίοι συνδυάζουν επιμέρους χαρακτηριστικά των δύο προαναφερόμενων μορφών. Η τέταρτη βασική μορφή ιών είναι οι companion viruses, οι οποίοι εκμεταλλεύονται μια ευπάθεια των λειτουργικών συστημάτων DOS και σχετίζεται με την ύπαρξη δύο προγραμμάτων με το ίδιο όνομα σε έναν κατάλογο και τη μορφή αυτών των αρχείων. Ο ιός δε μολύνει ένα συγκεκριμένο αρχείο, αλλά δημιουργεί αντίγραφό του, και μόλις ο χρήστης πάει προσπαθήσει να εκτελέσει το πρώτο αρχείο, θα εκτελεστεί πρώτα το αντίγραφό εντός του οποίου εμπεριέχεται ο κακόβουλος κώδικας. Πολλές φορές αυτό το αρχείο μπορεί να είναι «κρυφό» και να παραμένει μέσα στη μνήμη του υπολογιστή. Η μετάδοσή του γίνεται με αποσπώμενα αποθηκευτικά μέσα ή μέσα από το δίκτυο. Η πέμπτη βασική μορφή είναι οι ιοί Link και Flash Bios. Ο ιός Link δε μολύνει το πρόγραμμα καθαυτό, αλλά αλλάζει το σύνδεσμο που «δείχνει» προς ένα πρόγραμμα του υπολογιστή, ώστε να «δείχνει» το σημείο στο οποίο βρίσκεται αυτός ο ιός και να εκτελείται αυτός αντί του

103 Το Master Boot Record (MBR) είναι ο πρώτος τομέας του σκληρού δίσκου που λέει στον υπολογιστή πώς να φορτώσει το λειτουργικό σύστημα και δίνει εντολές για τη διαίρεση του σκληρού δίσκου [“MBR”, χ.χ. (http://www. computerhope.com/jargon/m/mbr.htm)].

προγράμματος. Οι ιοί Flash Bios αντικαθιστούν το πρόγραμμα BIOS που βρίσκεται στη μητρική πλακέτα με αποτέλεσμα να υπάρχουν απρόβλεπτες συνέπειες, όπως είναι η αδυναμία εκκίνησης του υπολογιστή. Τελευταία βασική μορφή είναι οι macro-viruses, οι οποίοι βρίσκονται σε κάποιο αρχείο εικονικού γραφείου, όπως είναι π.χ. το Word του Microsoft Office, και εκτελούν μια μακροεντολή[104], η οποία έχει τη δυνατότητα εκτέλεσης μιας σειράς ανεπιθύμητων ενεργειών[105].

Ως παράδειγμα για τη λειτουργία των ιών μπορούμε να χρησιμοποιήσουμε τον ιό "Brain", ο οποίος δημιουργήθηκε το 1986 στο Πακιστάν. Ο Brain μόλυνε εκείνη την περίοδο τα τμήματα εκκίνησης των υπολογιστών IBM και άλλων συμβατών συστημάτων παγκοσμίως. Αυτός ο ιός ξεκίνησε να υπάρχει σε παράνομα αντίγραφα λογισμικού τα οποία αγοράζονταν από το μαγαζί που παρείχε υπηρεσίες για εγκεφάλους υπολογιστών στη Λαχώρη. Στη συνέχεια, μεταδόθηκε και σε άλλα πειρατικά αντίγραφα λογισμικού παγκοσμίως, και ειδικότερα στις ΗΠΑ, όπου οι υπολογιστές ήταν πιο διαδεδομένοι. Ήταν ένας αρκετά μολυσματικός ιός και δύσκολος στον εντοπισμό λόγω του ιδιαίτερου σχεδιασμού του και είχε τη δυνατότητα να μολύνει ραγδαία οποιαδήποτε δισκέτα τύπου DOS και με αυτόν τον τρόπο ο ιός εξαπλωνόταν. Μετά την ενεργοποίησή του ο "Brain" διέγραφε όλες τις πληροφορίες και τα προγράμματα και μπορούσε να εμφανίσει το ακόλουθο μήνυμα "WELCOME TO THE DUNGEON c 1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 Nizam Block Allama Igbal Town Lahore, Pakistan Phone: 430791, 443248, 2800530 Beware Of This VIRUS Contact Us For Vaccination". Το 1988 ο ιός έφτασε στο απόγειό του έχοντας μολύνει περίπου 200.000 υπολογιστές. Το θετικό που έφερε ήταν η αύξηση των νόμιμων πωλήσεων λογισμικών προγραμμάτων λόγω του φόβου της μόλυνσης από τη

104 Μακροεντολή είναι ένα σύνολο εντολών που μπορούν να εκτελεστούν με μία κίνηση [«Τι πρέπει να γνωρίζετε για τις μακροεντολές», 2010 (http://www.adaeion.gr/word/g/about_macros.html)].
105 Κωνσταντίνος Βλαχόπουλος 2007, 48-49.

μεριά των χρηστών[106].

Παρόμοια προγράμματα με τους ιούς είναι τα σκουλήκια, αλλά η βασική διαφορά τους έγκειται στο ότι τα σκουλήκια δε χρειάζονται κάποια ενέργεια από το χρήστη για τον πολλαπλασιασμό τους. Στην αρχική τους μορφή τα σκουλήκια τροποποιούν ή διαγράφουν αρχεία που είναι αποθηκευμένα σε κάποιον υπολογιστή και εν συνεχεία δημιουργούν πολλαπλά αντίγραφα του εαυτού τους στέλνοντάς τα στους υπολογιστές των υποψηφίων θυμάτων[107]. Διαδίδονται από μόνα τους μέσα από κάποιο δίκτυο ή από κάποιον πίνακα ανακοινώσεων ελισσόμενα συνεχώς από υπολογιστή σε υπολογιστή μέχρι να εξαπλωθούν σε όλα τα συνδεδεμένα συστήματα. Για την πρόκληση ζημιάς χρησιμοποιούν τους μηχανισμούς επικοινωνίας μεταξύ υπολογιστών[108].

Μια περίπτωση σκουληκιού είναι αυτή του Code Red II από το 2001. Το Code Red II προκάλεσε μία από τις μεγαλύτερες καταστροφές στην ιστορία του διαδικτύου προσβάλλοντας σε διάστημα μόλις 14 ωρών 359.000 συστήματα, δηλαδή 2000 συστήματα ανά λεπτό της ώρας. Κάθε 37 λεπτά ο μολυσμένος πληθυσμός συστημάτων διπλασιαζόταν. Σε μικρό χρονικό διάστημα από την εμφάνισή του η συνολική οικονομική ζημιά ανερχόταν σε 2 δισεκατομμύρια δολάρια με ρυθμό 200 εκατομμυρίων ανά ημέρα[109].

Το τρίτο κυριότερο είδος κακόβουλου λογισμικού είναι οι Δούρειοι Ίπποι. Ο Δούρειος Ίππος είναι ένα φαινομενικά αθώο πρόγραμμα, το οποίο, όμως, εμπεριέχει κρυμμένες λειτουργίες. Η φόρτωση του συγκεκριμένου προγράμματος γίνεται στο σκληρό δίσκο του υπολογιστή και εκτελείται μαζί με το κανονικό πρόγραμμα. Μέσα σε αυτό το «αθώο» πρόγραμμα κρύβεται ένα υποπρόγραμμα, που θα εκτελέσει μια λειτουργία άγνωστη προς το χρήστη. Τα προγράμματα των Δούρειων Ίππων μπορούν να λάβουν

106 Robert J. Malone & Reuven R. Levary 1994, 131-132.
107 Κωνσταντίνος Βλαχόπουλος 2007, 50.
108 Γρηγόρης Λάζος 2001, 112.
109 Κωνσταντίνος Βλαχόπουλος 2007, 51.

τη μορφή ενός δημοφιλούς προγράμματος στο οποίο έχουν αλλάξει τον αυθεντικό κώδικα, για να κρύψουν το «φορτίο» τους[110]. Ο επιτιθέμενος χρησιμοποιώντας ένα Δούρειο Ίππο καταφέρνει να αποκτήσει απομακρυσμένο έλεγχο στον υπολογιστή του θύματος και, στη συνέχεια, έχει τη δυνατότητα συλλογής κωδικών πρόσβασης, αριθμών πιστωτικών καρτών ή εξαπόλυσης επίθεσης άρνησης εξυπηρέτησης[111].

Ως παράδειγμα Δούρειου Ίππου μπορούμε να αναφέρουμε το πρόγραμμα "Back Orifice", το οποίο έκανε την εμφάνισή του το 2000. Ο Back Orifice έφθανε στα υποψήφια θύματα μέσω e-mail με τη μορφή συνημμένου αρχείου. Κατά την εκτέλεσή του εγκαθιστούσε στον υπολογιστή του θύματος ένα πρόγραμμα διακομιστή (server) και, εν συνεχεία, ο δράστης εγκαθιστούσε στο δικό του υπολογιστή ένα πρόγραμμα πελάτη (client) δίνοντας εντολές στο server του θύματος. Κατά αυτόν τον τρόπο είχε τη δυνατότητα να αποκτήσει τον πλήρη έλεγχο του υπολογιστή του θύματος και, πέραν τούτου, μπορούσε να διαπράξει άλλα διαδικτυακά εγκλήματα, τα οποία θα φαίνονταν να έχουν διαπραχθεί από το θύμα[112].

Ως υποκατηγορία των Δούρειων Ίππων λογίζονται τα adware και τα spyware, αλλά εξετάζονται χωριστά λόγω της μεγάλης διάδοσής τους. Η χρήση των adware γίνεται για τη διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων προσφερόμενων μέσω διαδικτύου. Κάποιες φορές τα adware ενδέχεται να αποτελούν και νόμιμο λογισμικό, σε περίπτωση που η λειτουργία τους ορίζεται ρητώς στους όρους χρήσης τους οποίους αποδέχεται ο χρήστης κατά την εγκατάστασή τους. Σε κάθε αντίθετη περίπτωση λογίζονται ως κακόβουλο λογισμικό. Τα spyware, σε αντίθεση με τα adware, είναι κατεξοχήν κακόβουλο λογισμικό, το οποίο υποκλέπτει πληροφορίες που αφορούν το χρήστη. Οι πληροφορίες που υποκλέπτονται μέσω του spyware μπορεί να είναι προσωπικά στοιχεία του χρήστη, αριθμοί πιστωτικών καρτών, στοιχεία

110 Eric J. Sinrod & William P. Reilly 2000, 223.
111 Κωνσταντίνος Βλαχόπουλος 2007, 51.
112 Το ίδιο, 51-52.

λογαριασμών και συναλλαγών κλπ. Για την υποκλοπή των δεδομένων γίνεται χρήση διάφορων τεχνικών, π.χ. η χρήση του keylogger, ενός προγράμματος που υποκλέπτει κάθε χαρακτήρα που πληκτρολογείται από το χρήστη[113].

Διαδεδομένα προγράμματα κακόβουλου λογισμικού, πέραν των τριών βασικών, αποτελούν επίσης οι βόμβες (bombs) και οι καταπακτές (trap doors). Η βόμβα είναι ένα πρόγραμμα που εκτελεί ζημιογόνες ενέργειες σε προκαθορισμένο χρόνο. Οι βόμβες διακρίνονται σε λογικές (logic bombs) και ωρολογιακές (time bombs). Οι ωρολογιακές βόμβες είναι προγραμματισμένες να εκτελέσουν τις ενέργειές τους σε μια συγκεκριμένη ημερομηνία ή ώρα. Η ενεργοποίηση των λογικών βομβών γίνεται, όταν συμβαίνει ένα προμελετημένο γεγονός[114]. Οι βόμβες μπορούν να σταματήσουν τη λειτουργία του υπολογιστή, να διαγράψουν αρχεία, να απελευθερώσουν κάποιον ιό ή να προβούν σε διάφορες άλλες ζημιογόνες ενέργειες[115].

Η καταπακτή είναι μια μέθοδος εύκολα προσβάσιμη για την απόκτηση πρόσβασης σε κάποιον υπολογιστή. Μόλις ο χρήστης πατήσει ένα συγκεκριμένο συνδυασμό πλήκτρων, το σύστημα του επιτρέπει να αποκτήσει πρόσβαση σε αρχεία, ακόμα και αν δεν έχει τηρήσει τις κανονικές διαδικασίες ασφαλείας. Αν hackers ανακαλύψουν αυτές τις καταπακτές, έχουν τη δυνατότητα να εισάγουν σε αυτές κακόβουλα προγράμματα χωρίς τις απαιτούμενες εξουσιοδοτήσεις ασφαλείας. Συνήθως οι καταπακτές δημιουργούνται από τους προγραμματιστές για νόμιμους σκοπούς και τις χρησιμοποιούν ως βολικές μεθόδους πρόσβασης σε συστήματα για τη δημιουργία, τη δοκιμή και τη συντήρηση προγραμμάτων χωρίς να χρειαστεί να επηρεάσουν τους χρήστες του συστήματος. Ωστόσο, αρκετές φορές μετά την επίτευξη αυτών των διεργασιών οι καταπακτές ξεχνιούνται και δεν αφαιρούνται[116].

113 Το ίδιο, σελίδα 52.
114 Robert J. Malone & Reuven R. Levary 1994, 135.
115 Κωνσταντίνος Βλαχόπουλος 2007, 53.
116 Robert J. Malone & Reuven R. Levary 1994, 139-140.

Το κακόβουλο λογισμικό ακολουθεί και αυτό τις τεχνολογικές εξελίξεις, με αποτέλεσμα να επεκτείνεται πλέον και σε άλλες συσκευές πέραν των υπολογιστών. Παράλληλα όλο και πιο καινούριες και ζημιογόνες μορφές κακόβουλου λογισμικού κάνουν την εμφάνισή τους. Οι κινητές συσκευές παρέχουν μεγαλύτερες ευκαιρίες επίθεσης ή εκμετάλλευσης. Ακόμη, μοιράζονται κάποιες κοινές μεθόδους μόλυνσης, αν και κάποιες είναι μοναδικές σε κάθε πλατφόρμα. Οι βασικές μέθοδοι μόλυνσης είναι τέσσερις. Η πρώτη είναι το SMS spam, το οποίο δελεάζει τα θύματα να πατήσουν σε ένα link, μέσω του οποίου θα κατέβει στη συσκευή τους κακόβουλο λογισμικό. Η δεύτερη μέθοδος είναι οι spoofed/Trojanised apps. Τα θύματα κατεβάζουν δωρεάν ή σε έκπτωση ή σπασμένες (cracked) εκδόσεις δημοφιλών εφαρμογών, αλλά στην πραγματικότητα κατεβάζουν κακόβουλο λογισμικό. Η τρίτη μέθοδος είναι με τα adware. Οι χρήστες κατεβάζουν μια αβλαβή εφαρμογή, εντός της οποίας οι εγκληματίες ελέγχουν τις διαφημίσεις. Αφού η εφαρμογή κατέβει από αρκετά υποψήφια θύματα, οι δράστες θα αλλάξουν το διαφημιστικό περιεχόμενο κατευθύνοντάς τα σε μολυσμένες ιστοσελίδες. Η τελευταία μέθοδος είναι οι μολυσμένες ενημερώσεις. Οι χρήστες κατεβάζουν κάποια μη κακόβουλη δωρεάν εφαρμογή, στην οποία επιτιθέμενοι σπρώχνουν κάποια ενημέρωση με φορτίο κακόβουλου λογισμικού. Οι μολυσμένες κινητές συσκευές μπορούν να λειτουργήσουν ως φορείς της μόλυνσης, καθώς κάποιες παραλλαγές των κακόβουλων προγραμμάτων έχουν την ικανότητα να εξαπλώνονται σε άλλες συσκευές μέσω Bluetooth. Ακόμη υπάρχει κάποιο είδος κακόβουλου λογισμικού το οποίο απλώνεται πάνω στην επιφάνεια εργασία του υπολογιστή από smartphones και tablets, αφού αυτά συνδεθούν με τον υπολογιστή μέσω USB[117].

Οι χρήστες μπορούν να προστατευθούν από τη διασπορά κακόβουλου λογισμικού με τη χρήση αντιβιοτικών προγραμμάτων (antivirus softwares). Οι τρεις βασικές λειτουργίες αυτών των προγραμμάτων είναι η ανίχνευση των ιών, ο καθορισμός της ταυ-

117 Europol 2014, 24.

τότητάς τους και ο καθαρισμός τους. Μέσω της ανίχνευσης εξακριβώνεται αν πράγματι έχει μολυνθεί το σύστημα από κάποιον ιό. Η ανίχνευση γίνεται είτε μετά από ενέργεια του χρήστη είτε αυτόματα από το ίδιο το σύστημα. Η δυνατότητα προσδιορισμού της ταυτότητας του ιού είναι πολύ σημαντική, γιατί επιτρέπει την εκτίμηση του μεγέθους της προκληθείσας ζημιάς και την εκτέλεση των απαραίτητων ενεργειών, ώστε να αποκατασταθεί η ομαλή λειτουργία του συστήματος. Στο στάδιο του καθαρισμού τα περισσότερα λογισμικά προτείνουν τρεις ενέργειες: την επιδιόρθωση του μολυσμένου αρχείου, να τεθεί το αρχείο σε καραντίνα, ώστε να μην μπορεί να χρησιμοποιηθεί και τη διαγραφή του αρχείου[118]. Παρότι ο όρος "anti-virus" είναι πολύ συγκεκριμένος, τα προγράμματα αυτά είναι σχεδιασμένα να καταπολεμούν και τις άλλες μορφές κακόβουλου λογισμικού[119].

Στην αιτιολογική έκθεση του νόμου 4411/2016 αναφέρεται πως με την υιοθέτηση της Σύμβασης του Συμβουλίου της Ευρώπης για τα εγκλήματα στον κυβερνοχώρο με το άρθρο 6α ποινικοποιείται το κακόβουλο λογισμικό. Ωστόσο, παρακάτω που γίνεται λόγος για τα προστιθέμενα άρθρα του Ποινικού Κώδικα δεν αναφέρεται αν κάποιο από αυτά υιοθετεί το άρθρο 6α της Σύμβασης[120]. Νομοθεσίες για το κακόβουλο λογισμικό θεσπίστηκαν πρώτα στις Ηνωμένες Πολιτείες και στο Ηνωμένο Βασίλειο. Στις ΗΠΑ με το Computer Fraud and Abuse Act του 1986, που αναθεωρούσε ένα νόμο του 1984, έγινε προσπάθεια να δοθούν πιο ευρείς ορισμοί στα ζητήματα του πληροφορικού εγκλήματος και υπήρξε αναφορά και στην έμμεση αντιμετώπιση των ιών. Η απουσία, όμως, ξεκάθαρης αντιμετώπισης προκαλούσε δυσκολίες στα ομοσπονδιακά

118 Κωνσταντίνος Βλαχόπουλος 2007, 89-90.

119 Linda Criddle, χ.χ. (http://www.webroot.com/us/en/home/ resources/tips/pc-security/security-what-is-anti-virus-software).

120 ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ στο σχέδιο νόμου «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 διατάξεις» .

δικαστήρια και υπήρξε μόλις μία καταδίκη κατασκευαστή ιού. Αποφασιστικά βήματα για την αντιμετώπιση της μετάδοσης ιών έγιναν με το Computer Virus Eradication Act του 1989. Σε αυτόν το νόμο έγιναν κάποιες βασικές διευκρινήσεις και προσθήκες του νόμου του 1986. Μέσα στο νόμο του 1989 συμπεριλαμβάνονταν η περιγραφή της δημιουργίας ιών, ο ορισμός των ποινών για τη δημιουργία και τη διάδοση των ιών και η πρόβλεψη χρηματικής αποζημίωσης των θυμάτων σε επίπεδο αστικού δικαίου. Ακόμη, με βάση αυτόν το νόμο, απαιτείται ο προγραμματιστής να έχει τοποθετήσει εν γνώσει του έναν ιό σε κάποιο πρόγραμμα ή υπολογιστικό σύστημα και να γνωρίζει πως αυτός ο ιός θα συμβάλει στην πρόκληση ζημίας με καταστροφή ή απώλεια δεδομένων ή προγραμμάτων. Στο Computer Misuse Act του 1990 στο Ηνωμένο Βασίλειο δε γίνεται κάποια άμεση αναφορά στο κακόβουλο λογισμικό. Κυρίως αναφέρεται σε ποινικοποίηση οποιουδήποτε είδους μη εξουσιοδοτημένης τροποποίησης του υλικού σώματος ή του λογισμικού ενός υπολογιστή[121].

121 Γρηγόρης Λάζος 2001, 118-120.

2.2.3. Ψηφιακή πειρατεία: Το παράδειγμα της πειρατείας λογισμικού

Α. Ορισμός και τυπολογία της ψηφιακής πειρατείας

Ως ψηφιακή πειρατεία ορίζεται μια μορφή παραβίασης πνευματικών δικαιωμάτων και μια μέθοδος παράνομης απόκτησης και διανομής διαφόρων μέσων μέσω της χρήσης των υπολογιστών και των τηλεπικοινωνιακών συσκευών[122]. Αντικείμενα πειρατείας μπορούν να αποτελέσουν τα έργα γραπτού λόγου, τα μουσικά έργα, τα καλλιτεχνικά έργα, οι κινηματογραφικές ταινίες, οι ηχητικές εγγραφές, οι ραδιοφωνικές εκπομπές, τα σήματα μεταφερόμενων προγραμμάτων, οι δημοσιευμένες εκδόσεις και τα προγράμματα υπολογιστών[123].

Μια τυπολογία που αφορά την παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας είναι η ακόλουθη. Πρώτη κατηγορία αποτελεί η παραβίαση των δικαιωμάτων ευρεσιτεχνίας και πνευματικής ιδιοκτησίας του εκδότη (publisher patent and copyright infringement). Αυτό αποτελεί τον παραδοσιακό τύπο κλοπής πνευματικής ιδιοκτησίας, κατά τον οποίο κάποιος παραγωγός αντιγράφει υλικό ή διαδικασία (process) από κάποιον άλλο για την απόκτηση κέρδους. Δεύτερη κατηγορία είναι η βιομηχανική πειρατεία (industrial piracy). Η κατηγορία αυτή αφορά την απόπειρα αντιγραφής και διανομής σε μεγάλη κλίμακα για την απόκτηση κέρδους. Τρίτη κατηγορία είναι η επιχειρησιακή πειρατεία (corporate piracy). Σε αυτήν την κατηγορία ρίζα αποτελεί το εσωτερικό δίκτυο (LAN) της επιχείρησης. Η εγκατάσταση μιας αντιγραμμένης εφαρμογής λογισμικού στον server του εσωτερικού δικτύου της επιχείρησης εκατοντάδες εργαζόμενοι πιθανώς να αποκτήσουν πρόσβαση χωρίς άδεια. Τέταρτη κατηγορία είναι η πειρατεία μεταπώλησης (reseller piracy). Αυτή η κατηγορία αφορά τις επιχειρήσεις που πωλούν εξοπλισμό υπολογιστή με παράνομα αντίγραφα λογισμικού ήδη φορτωμένα στον υπολογιστή τους. Τελευταία κατηγορία είναι η οικιακή πειρατεία

122 Neel Sampat 2009, "Piracy", 143.
123 Γρηγόρης Λάζος 2001, 147-148.

(home piracy). Σε αυτήν την κατηγορία περιλαμβάνονται από την ανταλλαγή αφαιρούμενων δίσκων με φίλους μέχρι την εκτέλεση ενός μη κερδοσκοπικού συστήματος πινάκων ανακοινώσεων για την παράνομη διανομή λογισμικού[124].

Β. Πειρατεία λογισμικού

Η πειρατεία λογισμικού είναι η χωρίς τη γραπτή συναίνεση του δημιουργού αναπαραγωγή ή/και διάθεση προγραμμάτων υπολογιστή, τα οποία υπόκεινται στην προστασία των νόμων περί πνευματικών δικαιωμάτων. Η αναπαραγωγή εφαρμογών λογισμικού σε πολλαπλά αντίγραφα καθίσταται ιδιαίτερα εύκολη λόγω της ψηφιακής τους μορφής. Πριν την εξάπλωση του διαδικτύου η διακίνησή τους γινόταν με φυσικό τρόπο μέσω CD, δισκετών κλπ. Με την εξάπλωση του διαδικτύου, όμως, άνοιξαν νέοι ορίζοντες στην πειρατεία λογισμικού και έτσι το λογισμικό μπορεί, πλέον, να διακινηθεί μέσω διαφόρων υπηρεσιών που προσφέρονται από το διαδίκτυο, όπως e-mail, chat, εφαρμογές ανταλλαγής αρχείων (peer to peer) κλπ[125].

Οι εταιρείες παραγωγής λογισμικού δίνουν μεγάλη σημασία στο ζήτημα των διαφυγόντων κερδών, δηλαδή των κερδών που δεν αποδίδονται στους δημιουργούς ή/και στους ιδιοκτήτες. Στο επιχείρημα της απώλειας κερδών προστίθενται και τα επιχειρήματα της απώλειας φόρων από το κράτος και της απώλειας θέσεων εργασίας. Στα επιχειρήματα αυτά αντιπαρατίθενται θέσεις υπέρ της πρακτικής αυτής. Τα επιχειρήματα της άλλης μεριάς αναφέρουν πως αυτή η πρακτική συμβάλλει στη δημιουργία νέων προτύπων επικοινωνίας, ανταλλαγής και από κοινού μοιράσματος των πληροφοριών[126].

Οι εταιρείες παραγωγής λογισμικού εφαρμόζουν στα προϊόντα τους διάφορα τεχνολογικά μέτρα, προκειμένου να αποτραπεί η αντιγραφή ή η χρήση των προϊόντων τους

124 Peter Troost 1995 (http://www.angelfire.com/on2/darktemplar/piracy.html).
125 Κωνσταντίνος Βλαχόπουλος 2007, 61.
126 Γρηγόρης Λάζος 2001, 140-141.

από πολλούς υπολογιστές. Τέτοια μέτρα είναι το hardware key, το registration key, το όνομα και ο αριθμός της σειράς, η ενεργοποίηση μέσω διαδικτύου και η ενεργοποίηση μέσω τηλεφώνου. Το hardware key είναι μια συσκευή η οποία συνδέεται στον υπολογιστή, συνήθως μέσω της θύρας USB, και μέσα σε αυτήν περιέχεται ένας απαραίτητος για τη λειτουργία του λογισμικού σειριακός αριθμός. Το registration key είναι μια διαδοχική σειρά συμβόλων από γράμματα και αριθμούς που θα πρέπει να εισαχθούν από το χρήστη, προκειμένου να μπορέσει να λειτουργήσει το λογισμικό. Όσον αφορά το μέτρο του ονόματος και του αριθμού σειράς, ο χρήστης, προκειμένου να λειτουργήσει το λογισμικό, πρέπει να εισάγει το όνομά του και έναν αριθμό, πράγματα τα οποία δήλωσε με την αγορά του λογισμικού. Η ενεργοποίηση μέσω τηλεφώνου γίνεται με την πραγματοποίηση μιας κλήσης σε έναν συγκεκριμένο τηλεφωνικό αριθμό, για να δοθεί στο χρήστη ο κωδικός ενεργοποίησης του λογισμικού. Τέλος, η ενεργοποίηση μέσω διαδικτύου γίνεται με τη σύνδεση του χρήστη στο διαδίκτυο με το διακομιστή της εταιρείας λογισμικού[127].

Παρά τη χρήση των διαφόρων τεχνολογικών μέτρων πάντοτε βρίσκονται τεχνικές από τους crackers για την παράκαμψή τους. Μέσω της τεχνικής του cracking, δηλαδή του σπασίματος, μπορούν να προκαλέσουν την απενεργοποίηση των κωδικών, των κλειδιών ή οποιουδήποτε άλλου μέτρου που χρησιμοποιείται. Ακόμα και αν κάποιοι δεν κατέχουν τις εξειδικευμένες γνώσεις που απαιτούνται για την επίτευξη αυτού του σπασίματος, στο διαδίκτυο διατίθενται έτοιμα λογισμικά "crack", τα οποία έχουν τη δυνατότητα να απενεργοποιούν τα μέτρα προστασίας τα οποία τίθενται από τις εταιρείες παραγωγής λογισμικού[128].

Μια εικόνα αναφορικά με την έκταση του φαινομένου δίνεται στις έρευνες που διεξάγει η Business Software Alliance (BSA) παγκοσμίως σε συνεργασία με την In-

127 Κωνσταντίνος Βλαχόπουλος 2007, 61.
128 Το ίδιο, 61-62.

ternational Data Corporation (IDC). Οι δύο τελευταίες έρευνες που έγιναν από την BSA διεξήχθησαν το 2014 και το 2016 για τα έτη 2013 και 2015. Οι έρευνες έγιναν σε δείγμα περίπου 22.000 χρηστών λογισμικού που χρησιμοποιείται είτε στο σπίτι είτε στην επιχείρηση και σε ένα δείγμα 2020 IT managers, οι οποίοι προέρχονται από 20 χώρες. Τα βασικά πορίσματα της έρευνας του 2014 είναι τα εξής. Το ποσοστό χρήσης λογισμικού χωρίς κατάλληλη άδεια για το 2013 ανερχόταν στο 43%, το οποίο ήταν λίγο αυξημένο σε σχέση με το 42% για το 2011 και εξισωμένο με το αντίστοιχο ποσοστό του 2009. Η αξία του μη αδειοδοτημένου λογισμικού ανερχόταν στα 62.7 δισεκατομμύρια δολάρια. Οι IT managers ανέφεραν πως μόλις το 35% των εταιρειών είχε γραπτές πολιτικές που ζητούσαν τη χρήση λογισμικού με την κατάλληλη άδεια. Οι απλοί εργαζόμενοι είναι λιγότερο πιθανόν να πουν ότι στην εταιρεία τους υπάρχει κάποια επίσημη πολιτική αναφορικά με το αδειοδοτημένο λογισμικό σε σχέση με τους IT managers, καθώς υπάρχει ένα κενό επίγνωσης. Ο κυριότερος λόγος για τον οποίο οι χρήστες επιλέγουν να χρησιμοποιήσουν αδειοδοτημένο λογισμικό είναι η προστασία από κακόβουλο λογισμικό. Ανάμεσα στα ρίσκα που αναφέρθηκαν για τη χρήση μη αδειοδοτημένου λογισμικού το 64% ανέφερε ως κύρια ανησυχία τη μη εξουσιοδοτημένη πρόσβαση από τους hackers και ένα 59% ανέφερε την απώλεια δεδομένων[129].

Στην τελευταία έρευνα της BSA διαπιστώθηκε πως το ποσοστό που χρησιμοποιούσε λογισμικό υπολογιστή χωρίς άδεια μειώθηκε από το 43% που ήταν στο 2013 στο 39% για το 2015 και η αξία αυτού του 39% ανερχόταν στα 52.2 δισεκατομμύρια δολάρια. Ακόμα και σε συγκεκριμένες σημαντικές βιομηχανίες, όπου κάποιος θα περίμενε πιο αυστηρούς ελέγχους του ψηφιακού περιβάλλοντος, το ποσοστό χρήσης πειρατικού λογισμικού ήταν παραδόξως υψηλό και ανερχόταν στο 25%, δηλαδή 1 στις 4 βιομηχανίες. Οι βιομηχανίες αυτές ήταν τραπεζικές, ασφαλιστικές και προστασίας. Οι

129 BSA/The Software Alliance 2014, 1, 11.

IT managers δήλωσαν σε ποσοστό 49% πως αναγνωρίζουν ως κυριότερη απειλή του πειρατικού λογισμικού το κακόβουλο λογισμικό. Οι ερευνητές βρήκαν μια αρκετά ισχυρή συσχέτιση μεταξύ του κακόβουλου λογισμικού και του πειρατικού λογισμικού. Διαπίστωσαν πως όσο μεγαλύτερος ο δείκτης χρήσης πειρατικού λογισμικού τόσο μεγαλύτερη και η πιθανότητα να προσβληθούν οι υπολογιστές των χρηστών από κακόβουλο λογισμικό[130].

Σε νομοθετικό επίπεδο γίνεται αναφορά σε ζητήματα πνευματικής ιδιοκτησίας προγραμμάτων υπολογιστών. Η Οδηγία 91/250/ΕΟΚ αναγνωρίζει τα πνευματικά δικαιώματα σε προγράμματα υπολογιστών, ενώ εκτός από το ίδιο το πρόγραμμα προστατεύεται και το προπαρασκευαστικό υλικό. Ακόμη ορίζεται ποιος είναι ο δημιουργός του προγράμματος και ποιες οι πράξεις που υπόκεινται σε άδεια του δικαιούχου[131]. Η Οδηγία αυτή ενσωματώθηκε στο ελληνικό δίκαιο με το νόμο 2121/1993, ο οποίος σχετίζεται με την πνευματική ιδιοκτησία. Μεταξύ άλλων γίνεται ιδιαίτερη μνεία στα πνευματικά δικαιώματα που συνοδεύουν τα προγράμματα ηλεκτρονικών υπολογιστών και η τυχόν παραβίασή τους επισύρει κυρώσεις αστικού και ποινικού χαρακτήρα[132]. Τέλος, η παράγραφος 1 του άρθρου 370Γ του Ποινικού Κώδικα αναφέρεται αναλυτικότερα στις ποινικές κυρώσεις που προβλέπονται από την παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών. Πιο συγκεκριμένα προβλέπονται φυλάκιση 6 μηνών και πρόστιμο ύψους[133].

Μια περίπτωση που μπορούμε είναι αυτή ενός παγκοσμίου κυκλώματος πειρατείας λογισμικού αξίας 100 εκατομμυρίων δολαρίων. Το κύκλωμα αποτελούνταν από έξι άτομα, οι οποίοι πουλούσαν πάνω από 170.000 αντίγραφα προγραμμάτων της Adobe και της Microsoft, συμπεριλαμβανομένων των Windows, του Office, του Photoshop

130 BSA/The Software Alliance 2016, 2-5.
131 Οδηγία 91/250/ΕΟΚ.
132 Νόμος 2121/1993.
133 Νόμος 4411/2016.

και του Creative Suite, μαζί με τους έγκυρους κωδικούς εγγραφής και τα φυσικά πιστοποιητικά γνησιότητας. Τα πειρατικά αντίγραφα λογισμικού πωλούνταν μέσα από διάφορους ιστοτόπους συμπεριλαμβανομένων του Amazon, του Overstock, του eBay, του Craiglist και, σε κάποιες περιπτώσεις, στους δικούς τους ιστοτόπους σε έκπτωση. Ο ένας από τους έξι, μάλιστα, χρησιμοποίησε το μη κερδοσκοπικό οργανισμό Project Contact Africa για την πώληση του πειρατικού λογισμικού στο eBay. Λέγοντας στο e-Bay πως αυτή η επιχείρηση ήταν φιλανθρωπική και υποσχόμενος σε όλους τους πελάτες πως το 100% των πωλήσεων θα πήγαινε σε κάποιο αφρικανικό πρόγραμμα κατάφερε να ενισχύσει το εισόδημά του. Έπεισε, μάλιστα και το eBay να του χρεώνει λιγότερα τέλη για τις πωλήσεις. Μετά τον εντοπισμό τους από τους ερευνητές του Υπουργείου Εσωτερικής Ασφάλειας των ΗΠΑ το Δεκέμβριο του 2015 συνελήφθησαν όλα τα μέλη του κυκλώματος[134].

134 Andy Greenberg 2015 (https://www.wired.com/2015/12/6-men-admit-to-running-a-giant-100m-software-piracy-ring/).

Επίλογος – Συμπεράσματα

Η τεχνολογία αποτελεί αναπόσπαστο κομμάτι της ανθρώπινης καθημερινότητας με την πληροφορική τεχνολογία και τις τηλεπικοινωνίες να έχουν εξαπλωθεί παντού και μαζί με αυτές και το διαδίκτυο. Με τη σύνδεση στο διαδίκτυο έχουμε τον κυβερνοχώρο, για την κοινωνική σημασία του οποίου υπάρχουν διαφορετικές προσεγγίσεις. Μία προσέγγιση αναφέρει ότι είναι ένα είδος εργαλείου, το οποίο συχνά νοείται ως εργαλείο της καπιταλιστικής αγοράς αποκλειστικά. Μία άλλη προσέγγιση αντιλαμβάνεται τον κυβερνοχώρο ως χώρο κοινωνικής επαφής, δηλαδή ως σημείο στο οποίο αναπτύσσονται νέες κοινωνικές σχέσεις με τις οποίες μορφοποιούνται και αναπαράγονται με καινούριο τρόπο οι ήδη υπάρχουσες. Μέσα από τον κυβερνοχώρο δημιουργείται ένας κοινωνικός χώρος ο οποίος μπορεί να χαρακτηριστεί ως άυλος λόγω του ότι τα πρόσωπα μπορούν να εμφανιστούν ως άτομα δίχως σωματική υπόσταση και μπορούν να διατηρούν την ανωνυμία τους. Εντός αυτού του χώρου έχουμε τη δημιουργία όλο και περισσότερων κοινωνικών επαφών, την ύπαρξη εκπαιδευτικών και πολιτισμικών προσφορών καθώς και τη δυνατότητα να διατυπωθούν νομικές συμβουλές. Παράλληλα έχουμε και τη δημιουργία οικονομικών ανταλλαγών, όπως είναι το ηλεκτρονικό εμπόριο[135].

Η σύγχρονη τεχνολογία προσφέρει αρκετά θετικά, όπως η βελτιωμένη επικοινωνία, η άμεση πρόσβαση σε οποιαδήποτε πληροφορία, η ενθάρρυνση της καινοτομίας και της δημιουργικότητας κλπ[136]. Η τεχνολογία πληροφοριών και τηλεπικοινωνιών είναι πεδίο που προσφέρεται για την ανάπτυξη νέων μορφών εγκληματικότητας. Ειδικότερα χάρη στη βοήθεια των υπολογιστών τα εγκλήματα που παλαιότερα χρειάζονταν κατ' ιδίαν προσέγγιση του θύματος από το δράστη για να τελεστούν, πλέον μπορούν

135 Νίκος Κοτζιάς 1999, 17-19.
136 Karehka Ramey 2012.

να διαπραχθούν απομακρυσμένα με σύνδεση στο διαδίκτυο και κάποιες φορές, μάλιστα, σε καθεστώς πλήρους ανωνυμίας. Η πληροφορική τεχνολογία, μάλιστα, έφερε ακόμα περισσότερες αλλαγές στην εγκληματικότητα, καθώς νέα εγκλήματα εμφανίστηκαν και η ύπαρξή τους οφείλεται αποκλειστικά σε αυτήν. Τέτοια εγκλήματα αποτελούν το hacking, το κακόβουλο λογισμικό και η ψηφιακή πειρατεία. Το θύμα, είτε σε εγκλήματα που τελούνται με νέα μέσα είτε σε εντελώς νέα εγκλήματα, προσεγγίζεται πολύ ευκολότερα μέσα από τα κοινωνικά δίκτυα, από τα chatrooms, από ένα e-mail ή ακόμα και από ένα απλό SMS.

Η τεχνολογική εξέλιξη, λοιπόν, επέφερε μεγάλες αλλαγές στη διάπραξη των εγκλημάτων. Οι αλλαγές που επήλθαν επηρέασαν και τη νομοθεσία, η οποία ήταν αναγκαίο να προσαρμοστεί στα νέα δεδομένα, και έτσι νέοι νόμοι έκαναν την εμφάνισή τους. Οι νέοι αυτοί νόμοι αποτελούν προσθήκη ή αντικατάσταση παλαιότερων και περιλαμβάνουν κυρώσεις για τις τεχνολογικές μεθόδους διάπραξης παραδοσιακών εγκλημάτων και για τα εγκλήματα που προέκυψαν αποκλειστικά από τη σύγχρονη τεχνολογία. Η πρώτη χώρα που έκανε τέτοιες προσθήκες ήταν οι ΗΠΑ, ενώ σε επίπεδο διεθνών οργανισμών έχουν υπάρξει κατά την τελευταία δεκαπενταετία συστάσεις και οδηγίες από το Συμβούλιο της Ευρώπης και την Ευρωπαϊκή Ένωση για την προσθήκη ποινικών διατάξεων για τα τεχνολογικά υποβοηθούμενα εγκλήματα μέσα από την ενσωμάτωση των συγκεκριμένων κειμένων.

Οι τεχνολογικές εξελίξεις έχουν συμβάλει και στο να αναπτυχθούν διάφορα τεχνολογικά μέσα για την προστασία από τις νέες μορφές εγκληματικότητας. Συγκεκριμένα μπορούμε να αναφέρουμε την κρυπτογράφηση και τις τεχνικές ελέγχου πρόσβασης και αυθεντικοποίησης για το hacking, τα αντιβιοτικά προγράμματα για το κακόβουλο λογισμικό και τεχνικές όπως το hardware key για την πειρατεία λογισμικού. Παράλληλα οι τεχνολογικές εξελίξεις συμβάλλουν και στη λήψη δράσεων εναντίον των νέ-

ων μορφών εγκληματικότητας, δηλαδή ο επίσημος κοινωνικός έλεγχος εκμεταλλεύεται τις ίδιες τεχνολογίες που εκμεταλλεύονται και οι εγκληματίες οργανώνοντας δράσεις εναντίον τους και με αυτόν τον τρόπο αντιμετωπίζει τις νέες μορφές εγκληματικότητας. Παράδειγμα αποτελούν οι διάφορες αστυνομικές επιχειρήσεις που έχουν γίνει σε διεθνές επίπεδο, όπως η Επιχείρηση Onymous, η Επιχείρηση Babylon, η Επιχείρηση Night Clone κλπ.

Η επαλήθευση των τριών πρώτων ερωτημάτων επαληθεύει και την επιλεκτική χρησιμότητα της τεχνολογίας. Η τεχνολογία μπορεί να εξυπηρετήσει κάποιους σκοπούς πιο εύκολα, αλλά γενικότερα μπορεί να χρησιμοποιηθεί για την εξυπηρέτηση οποιουδήποτε σκοπού. Μπορεί στα χέρια των εγκληματιών η τεχνολογία να εξυπηρετήσει εγκληματικούς σκοπούς, με αποτέλεσμα να δημιουργηθούν νέοι νόμοι, και στα χέρια του επίσημου κοινωνικού ελέγχου να εξυπηρετήσει το σκοπό της καταπολέμησης του εγκλήματος. Ακόμη, η τεχνολογία μπορεί να γίνει επιλεκτικά χρήσιμη και για την προστασία από τις νέες μορφές εγκληματικότητας μέσα από την ανάπτυξη προαναφερθεισών τεχνικών.

Η τεχνολογία, λοιπόν, μπορεί να γίνει επιλεκτικά χρήσιμη για την εξυπηρέτηση εγκληματικών σκοπών. Οι Cornish & Clarke στη θεωρία της ορθολογικής επιλογής αναφέρουν ότι το έγκλημα είναι μια σκόπιμη και ηθελημένη πράξη και υλοποιείται για την απόκτηση οφέλους από το δράστη. Το όφελος αυτό περιλαμβάνει την ικανοποίηση συνηθισμένων ανθρωπίνων κινήτρων. Ως παράδειγμα για αυτά τα κίνητρα μπορούμε να αναφέρουμε τη σεξουαλική ικανοποίηση στην περίπτωση της παιδικής πορνογραφίας ή την εκδίκηση στην περίπτωση της διασποράς κακόβουλου λογισμικού.

Πέραν της χρησιμότητας για την εξυπηρέτηση εγκληματικών σκοπών βλέπουμε και επιλεκτική χρησιμότητα για την αντιμετώπιση των νέων μορφών εγκληματικότητας. Αναφορικά με τον επίσημο κοινωνικό έλεγχο επαληθεύεται, πρώτα από όλα, ο ο-

ρισμός του Cohen για τον οργανωμένο τρόπο αντίδρασης μιας κοινωνίας. Αυτός ο οργανωμένος τρόπος αντίδρασης αντικατοπτρίζεται μέσα από τις οργανωμένες επιχειρήσεις των αστυνομικών αρχών εναντίον των νέων μορφών εγκληματικότητας. Παράλληλα επιβεβαιώνεται το ότι ο σύγχρονος έλεγχος έχει γίνει ηπιότερος και λιγότερο ορατός, αφενός με τα διάφορα λογισμικά από τις εταιρείες και τους προγραμματιστές για την προστασία από τις νέες μορφές εγκληματικότητας και αφετέρου μέσα από τις πολύπλοκες επιχειρήσεις που γίνονται σε καθεστώς ανωνυμίας μέσα στον Σκοτεινό Ιστό μέσα από την εκμετάλλευση των ανώνυμων προγραμμάτων περιήγησης, όπως το Tor.

Τι γίνεται, όμως, με το οικονομικό κόστος από κάποια συγκεκριμένα εγκλήματα; Η οικονομική ζημία από τις απάτες που τελούνται με νέα μέσα μπορεί να είναι πολύ μεγάλη. Μόνο για το 2015 στο Ηνωμένο Βασίλειο οι απάτες που σχετίζονται με κάρτες, τις εξ αποστάσεως τραπεζικές συναλλαγές και τις επιταγές οι απώλειες ξεπέρασαν τα 700 εκατομμύρια λίρες. Οι απάτες που τελούνται με σύγχρονα τεχνολογικά μέσα εμπίπτουν στον ορισμό του Edelhertz για το λευκό κολάρο. Είναι παράνομες πράξεις που τελούνται με μη φυσικά μέσα, όπως είναι ο υπολογιστής και διάφορα ψηφιακά προγράμματα, με δόλο και έχουν σκοπό την απόκτηση χρημάτων με την απόσπασή τους από τα θύματα.

Τα τεχνολογικά υποβοηθούμενα εγκλήματα είναι ένα σημαντικό ζήτημα της σύγχρονης εποχής και η ραγδαία εξέλιξη της τεχνολογίας με το πέρασμα του χρόνου θέτει περισσότερες δυσκολίες στην αντιμετώπισή τους. Κρίνεται αρκετά σημαντική η περαιτέρω εμπειρική διερεύνηση σε ζητήματα που άπτονται των εγκλημάτων που τελούνται με τη βοήθεια της σύγχρονης τεχνολογίας, και ειδικότερα στα εγκλήματα που η ύπαρξή τους οφείλεται αποκλειστικά στη σύγχρονη τεχνολογία, προκειμένου να μπορέσουμε κατανοήσουμε καλύτερα τα κίνητρα πίσω από αυτές τις συμπεριφορές.

Βιβλιογραφία

ΕΛΛΗΝΟΓΛΩΣΣΗ

Αγγελή Δανάη κ.ά., *Η παιδική πορνογραφία στο διαδίκτυο,* επιστημονική εποπτεία Δημήτρης Κιούπης, επιμέλεια Αιμιλία Ιωαννίδου, Νομική Βιβλιοθήκη, Αθήνα 2007.

Αλεξιάδης Στέργιος, *Εγκληματολογία,* 5η έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2011.

Αργυρόπουλος Ανδρέας, *Ηλεκτρονική εγκληματικότητα,* Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2001.

Βλαχόπουλος Κωνσταντίνος, *Ηλεκτρονικό έγκλημα: Μορφές, πρόληψη, αντιμετώπιση*, Νομική Βιβλιοθήκη, Αθήνα 2007.

Γιωτοπούλου-Μαραγκοπούλου Αλίκη, *Εγχειρίδιο εγκληματολογίας,* Νομική Βιβλιοθήκη, Αθήνα 1984.

Ζαραφωνίτου Χριστίνα, «Θυματοποίηση και φόβος του εγκλήματος των φοιτητών χρηστών του διαδικτύου. Σχολιασμένη παρουσίαση ερευνητικών πορισμάτων», *Εγκληματολογία,* τ. 1-2, 2014, σελίδες 21-29.

Κοτζιάς Νίκος, «Κυβερνοχώρος και προβλήματα δημοκρατίας», Πρόλογος στο Ντέιβιντ Μπράουν, *Η δικτατορία στον κυβερνοχώρο: Το τέλος της δημοκρατίας στην εποχή της πληροφορικής,* μετάφραση Πάσχος Μανδραβέλης, Εκδόσεις Καστανιώτη, Αθήνα 1999, σελίδες 9-50 (David Brown, *Cybertrends: Chaos, power and accountability in the information age,* Viking, London 1997).

Λάζος Γρηγόρης, *Πληροφορική και έγκλημα,* Νομική Βιβλιοθήκη, Αθήνα 2001.

Λυσάνδρου Μιράντα, «Ένα τηλεπικοινωνιακό σύστημα είναι ασφαλές μέχρι να εντοπιστεί μια νέα τρύπα: Ευάλωτα σε υποκλοπές τα δίκτυα», *Πολίτης,* 28.2.2010, σελίδα 8 (www.efylakas.com/archives/5623).

Μπαμπινιώτης Γεώργιος, *Λεξικό της νέας ελληνικής γλώσσας,* 2η έκδοση, Κέντρο Λεξικολογίας, Αθήνα 2002.

Παπαδόπουλος Μαρίνος, «Phishing: Η νέα μέθοδος εξαπάτησης στο διαδίκτυο», εισήγηση στο 3ο Πανελλήνιο Συνέδριο «Ηλεκτρονικό Έγκλημα 2005: Δικτυοπειρατεία», Αθήνα 2005, σελίδες 1-24.

Σπινέλλη Καλλιόπη Δ., *Εγκληματολογία: Σύγχρονες και παλαιότερες κατευθύνσεις,* 3η έκδοση, Νομική Βιβλιοθήκη, Αθήνα 2014.

Σπυρόπουλος Φώτιος, *Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking),* Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 2016.

Φαρσεδάκης Ιάκωβος, «Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του», 2009 (http://criminology.panteion.gr/attachments/article/386/j farsedakis κυβερνοχώρος.pdf).

Χάιδου Ανθοζωή, «Σύγχρονη τεχνολογία και κοινωνικός έλεγχος» στο Ανθοζωή Χάιδου, *Εγκληματολογικά κείμενα: Ανήλικοι-ναρκωτικά-κοινωνικός έλεγχος,* Νομική Βιβλιοθήκη, Αθήνα 2003, σελίδες 95-108.

ΞΕΝΟΓΛΩΣΣΗ

Bergman Michael K., "The Deep Web: Surfacing hidden value", *Bright Planet,* 2001, σελίδες 1-17.

BSA/The Software Alliance, *The compliance gap: BSA global software survey,* BSA/The Software Alliance, 2014.

BSA/The Software Alliance, *Seizing opportunity through license compliance: BSA global software survey,* BSA/The Software Alliance, 2016.

Castells Manuel, *The internet galaxy: Reflections on the internet, business and society,* Oxford University Press, Oxford 2001 (*Ο γαλαξίας του διαδικτύου: Στοχασμοί για το διαδίκτυο, τις επιχειρήσεις και την επικοινωνία,* μετάφραση Ελένη Αστερίου, Εκδόσεις Καστανιώτη, Αθήνα 2005).

Choo Kim-Kwang Raymond, Smith Russell G. & McCusker Rob, *Future directions in technology-enabled crime: 2007-09,* Australian Institute of Criminology, Canberra 2007.

Cohen Fred, "Computer viruses: Theory and experiments", *Computers & Security,* vol. 6, no. 1, 1987, σελίδες 22-35.

Cohen Stanley, *Visions of social control: Crime, punishment and classification,* Polity Press, Cambridge 1985.

Corbett Ronald & Marx Gary, "Critique: No soul in the new machine: Technofallacies in the electronic monitoring movement", *Justice Quarterly*, vol. 8, no. 3, 1991, σελίδες 201-216 (http://web.mit.edu/gtmarx/www/critique.html# technical).

Cornish Derek B. & Clarke Ronald V., "The rational choice perspective" στο Richard Wortley & Lorraine Mazerolle (editors), *Environmental criminology and crime analysis,* Willan Publishing, Cullompton, Devon 2008, σελίδες 21-47.

Durkheim Émile, *Les règles de la méthode sociologique,* Félix Alcan, Paris 1895 (*Οι κανόνες της κοινωνιολογικής μεθόδου,* μετάφραση-επιμέλεια Λουκία Μουσούρου, Gutenberg, Αθήνα 1978).

Edelhertz Herbert, *The nature, impact and prosecution of white-collar crime,* National Institute of Law Enforcement and Criminal Justice, Washington, D.C.1970,

Europol, *Payment card fraud: Perspective of law enforcement agencies. Situation Report,* European Police Office, The Hague 2012

Europol, *The internet organized threat assessment (iOCTA) 2014,* European Police Office, The Hague 2014.

Europol, *The internet organized threat assessment (iOCTA) 2015,* European Police Office, The Hague 2015α.

Europol, *Virtual global taskforce child sexual exploitation environmental scan 2015,* European Police Office, The Hague 2015β.

FFA UK, *Fraud the facts 2016: The definitive overview of payment industry fraud,* FFA UK, 2016.

Forester Tom & Morrison Perry, *Computer ethics: Cautionary tales and ethical dilemmas in computing,* 2nd edition, The MIT Press, Cambridge, Massachusetts 1994.

Janowitz Morris, "Sociological theory and social control", *American Journal of Sociology,* vol. 81, no.1, 1975, σελίδες 82-108.

Leman-Langlois Stéphane, "Introduction: technocrime" στο Stéphane Leman-Langlois (editor), *Technocrime: Technology, crime and social control,* Willan Publishing, Cullompton, Devon 2008, σελίδες 1-13.

Malone Robert J. & Levary Reuven R., "Computer viruses: Legal aspects", *University of Miami Business Review,* vol. 4, no. 2/3, 1994, σελίδες 125-157.

Martin Brian, "Social defence strategy: The role of technology", *Journal of Peace Research,* vol. 36, no. 5, 1999, σελ535-552.

Marx Gary T., "Privacy and the home: The king doesn't have to enter your cottage to invade your privacy", *Impact Assessment,* vol. 7, no. 1, 1989, σελίδες 31-59.

Marx Gary T., "Technology and social control" στο Neil J. Smelser & Paul B. Baltes, *International encyclopedia of the social and behavioral sciences (Volume 23),* Elsevier, New York 2001, σελίδες 15506-15512.

Marx Gary T., "The engineering of social control: The search for the silver bullet" στο John Hagan & Ruth D. Peterson (editors), *Crime and inequality,* Stanfornd University Press, Stanford, California 1995, σελίδες 225-246 (http://web.mit.edu/gtmarx/www/bullet.html).

Mead George Herbert, "The genesis of the self and social control", *International Journal of Ethics,* vol. 35, no. 3, 1925, σελίδες 251-277.

Moore Daniel & Rid Thomas, "Cryptopolitik and the Darknet", *Survivor,* vol. 58, no. 1, 2016, σελίδες 7-38.

Newburn Tim, *Criminology,* Willan Publishing, Cullompton, Devon 2007.

Parker Donn B., *Crime by computer,* Charles Scribner's Son, New York 1976.

Sampat Neel, λήμμα "Piracy" στο Samuel C. McQuade (editor), *Encyclopedia of cybercrime,* Greenwood Press, Westport, Connecticut 2009, σελίδες 143-144.

Sinrod Eric J. & Reilly William P., "Cyber-crimes: A practical approach to the application of federal computer crime laws, *Santa Clara High Technology Law Journal,* vol. 16, no. 2, 2000, σελίδες 177-233.

Small Albion W. & Vincent George E., *An introduction to the study of society,* American Book Company, New York 1894.

Sutherland Edwin H., "White-collar criminality", *American Sociological Review,* vol. 5, no. 1, 1940, σελίδες 1-12.

Vincent George, "The province of sociology", *The American Journal of Sociology,* vol. 1, no. 4, 1896, σελίδες 473-491.

Wall David, "Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime", *Information, Communication & Society,* vol. 11, no. 6, 2008, σελίδες 861-884.

Wall David, "Cybercrimes and the internet" στο David Wall (editor), *Crime and the internet,* Routledge, London and New York 2001, σελίδες 1-17.

Wasik Martin, *Crime and the computer,* Clarendon Press, Oxford 1991.

ΠΗΓΕΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

Criddle Linda, "What is anti-virus software?", *Webroot, χ.χ.* (http://www.webroot.com/us/en/home/ resources/tips/pc-security/security-what-is-anti-virus-software).

"Darknet hidden service for child sexual abuse material shut down", *Europol,* 31.7.2015 (https://www.europol.europa.eu/content/darknet-hidden-service-child-sexual-abuse-material-shut-down).

"Dark web", *Dictionary.com, χ.χ.* (http://www.dictionary.com/browse/dark-web?s=t).

"Don't be fooled, be fraud smart", *Barclays, χ.χ.* (http://www.barclays.co.uk/protect-yourself-from-fraud).

Greenberg Andy, "6 men admit to running a global $100M software piracy ring", *Wired,* 17.12.2015 (https://www.wired.com/2015/12/6-men-admit-to-running-a-giant-100m-software-piracy-ring/).

Greenberg Andy, "Hacker lexicon: What is the dark web?", *Wired,* 19.11.2014 (https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/)α.

Greenberg Andy, "Over 80 per cent of Dark-Web visits relate to pedophilia, study finds", *Wired,* 30.12.2014 (https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/)β.

International Association of Chiefs of Police, *2015 social media survey results,* 2015 (http://www.iacpsocialmedia.org/Portals/1/documents/FULL%202015%20Social%20Media%20Survey%20Results.pdf).

"International criminal group behind ATM skimming attacks dismantled", *Europol,* 24.5.2016 (https://www.europol.europa.eu/content/international-criminal-group-behind-atm-skimming-attacks-dismantled).

«Κόστος 485 εκατομμύρια είχαν οι διαδικτυακές απάτες το 2011 στις ΗΠΑ», Η Καθημερινή, 14.5.2012 (http://www.kathimerini.gr/77278/article/texnologia/diadiktyo/kostos-485-ekat-dolaria-eixan-oi-diadiktyakes-apates-brto-2011-stis-hpa).

Κούρος Κωνσταντίνος Γ., «Ηλεκτρονικό έγκλημα», *Ελληνική Αστυνομία,* χ.χ. (http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414).

Krebs Brian, "A dramatic rise in ATM skimming attacks", *Krebs on Security,* 29.4.2016 (http://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/).

McDonald Henry, "Online frauds costs global economy 'many times more than $100 bn'", *The Guardian,* 30.10.2013 (https://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars).

"MBR", *Computer Hope,* χ.χ. (http://www. computerhope.com/jargon/m/mbr.htm)

"Online fraud: Pharming", *Norton,* χ.χ. (http://us.norton.com/cybercrime-pharming).

"Phone scams", *Federal Trade Commission,* February 2014 (https://www.consumer.ftc.gov/articles/0076-phone-scams).

Press Association, "Social media-related crime reports up 780% in four years", *The Guardian,* 27.12.2012 (https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter).

Ramey Karehka, "Modern technology advantages and disadvantages", *Use of Technology,* 6.11.2012 (http://www.useoftechnology.com/modern-technology-advantages-disadvantages/).

«Ρυθμίσεις διακομιστή μεσολάβησης δικτύου», *Norton,* 4.9.2015 (τελευταία ενημέρωση) (https://support.norton.com/sp/el/gr/home/current/solutions/v66135793_NortonM_Retail_1_el_el).

"Stalking and harassment", *The Crown Prosecution Service,* χ.χ. (http://www.cps.gov.uk/legal/s_to_u/stalking_and_harassment/#a02).

«Τι πρέπει να γνωρίζετε για τις μακροεντολές», *Αδαείον,* 17.7.2010 (http://www.adaeion.gr/word/g/about_macros.html).

Troost Peter, "Combating software piracy", 1995 (http://www.angelfire.com/on2/darktemplar/piracy.html).

"Web crawling", *Track Maven, χ.χ.* (http://trackmaven.com/marketing-dictionary/web-crawling).

"What is VPN?", *What Is My IP Address, χ.χ.* (http://whatismyipaddress.com/vpn).

"Who we are", *Virtual Global Taskforce* (http://virtualglobaltaskforce.com/who-we-are/).

Zetter Kim, "How the Feds took down the Silk Road drug Wonderland", *Wired,* 18.11.2013 (https://www.wired.com/2013/11/silk-road/).

ΝΟΜΟΘΕΤΙΚΕΣ ΠΗΓΕΣ

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ στο σχέδιο νόμου «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 διατάξεις».

Νόμος 2121/1993 (ΦΕΚ Α' 25) «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα».

Νόμος 4411/2016 (ΦΕΚ Α' 142) «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 διατάξεις».

Οδηγία 91/250/ΕΟΚ για τη νομική προστασία των προγραμμάτων υπολογιστών.

Ποινικός Κώδικας (http://www.ministryofjustice.gr/site/kodikes/Ευρετήριο/ ΠΟΙΝΙΚΟΣΚΩΔΙΚΑΣ/tabid/432/language/el-GR/Default.aspx).