ΠΑΝΤΕΙΟ ΠΑΝ/ΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

ΘΕΜΑ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ:

«ΠΛΗΡΟΦΟΡΙΚΗ & ΠΑΡΕΚΚΛΙΣΗ: *ΕΝΑ ΝΕΟ ΙΣΤΟΡΙΚΟ ΦΑΙΝΟΜΕΝΟ*»

Διδάκτωρ: **Ρομπόρας Α. Αναστάσιος**
Α.Μ.:302052

Η Τριμελής Συμβουλευτική Επιτροπή:
1) **Ν. Σαρρής**, ως επιβλέπων
2) **Α. Μαγγανάς**, ως μέλος
3) **Γρ. Λάζος**, ως μέλος

ΑΘΗΝΑ 2009

«Η δύναμη της μηχανής ανέκαθεν μας εμπόδιζε να αποδεχτούμε τη μόνη δικαιοσύνη που είναι μία ακριβής στιγμή, ή τη μόνη ηθική που είναι η συνεχής αναγωγή στο πιο απλουστευτικό είναι μας»

Οδ. Ελύτης

Ευχαριστήριο Σημείωμα

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κ. Σαρρή Νεοκλή, επιβλέποντα στην δουλειά μου, καθώς και τα μέλη της επιτροπής κ. Μαγγανά Αντώνη και κ. Λάζο Γρηγόρη για τις διευκολύνσεις που μου παρείχαν σε διάφορα πρακτικού χαρακτήρα θέματα και κυρίως για τις ακαδημαϊκές γνώσεις που μοιράστηκαν μαζί μου τόσο κατά τις μεταπτυχιακές όσο και στις προπτυχιακές μου σπουδές. Το τελευταίο βεβαίως ισχύει για όλους τους καθηγητές μου στο τμήμα Κοινωνιολογίας του Παντείου Πανεπιστημίου μεταξύ άλλων, τον κ. Α. Μαγγανά που με ενθάρρυνε καθ' όλη τη διάρκεια της διδακτορικής μου έρευνας, τον κ. Ι. Φαρσεδάκη, την κ. Ι. Τσίγκανου, την κ. Α. Λυδάκη, την κ. Λαμπροπούλου Έφη.

Επίσης, θέλω να ευχαριστήσω για τον πολύτιμο χρόνο τους και τις πολύωρες συζητήσεις μας, τον κ. Λάζο Γρηγόρη Επίκουρο καθηγητή του τμήματος Κοινωνιολογίας και μέντορα μου σε θέματα πληροφορικής εγκληματικότητας καθώς και τον κ. Σφακιανάκη Μανώλη, Προϊστάμενο - Αστυνόμο Α' του τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος της Γ.Α.Δ.Α, για την αμέριστη συμπαράσταση στη διεξαγωγή της έρευνας.

Ελπίζω με τούτη την έρευνα να προσφέρω κάτι παραπάνω στην, εγκληματολογική, επιστήμη και τον άνθρωπο.

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος – Σκοπός της έρευνας

Αν συμβουλευτούμε ένα ελληνικό λεξικό[1] και αναζητήσουμε τον όρο «Πληροφορική» θα δούμε πως είναι η επιστήμη που ασχολείται με τη συλλογή, την επεξεργασία και τη μεταβίβαση πληροφοριών με μηχανικά μέσα (υπολογιστές) με τρόπο ορθολογικό. Αντίστοιχα, στην αναζήτηση του όρου «παρέκκλιση (diversion)[2]», η απάντηση που θα παίρναμε είναι η απομάκρυνση, η εκτροπή από την αρχική, από την κανονική πορεία ή κατεύθυνση - λοξοδρόμισμα ή η απομάκρυνση, η εκτροπή από (ηθικές, πολιτικές κτλ) αρχές ή κανόνες και η παραβίασή τους. Ως εκ τούτου, η παραβίαση σχετικά με τη σωστή επεξεργασία και μεταβίβαση πληροφοριών μέσω μηχανικών μέσων θα λέγαμε πως είναι ένας πρώτος ετυμολογικός ορισμός της «πληροφορικής παρέκκλισης» στο χώρο της εγκληματολογικής επιστήμης.

Τρεις είναι οι τύποι του εγκλήματος που πρέπει να διακρίνουμε. Πρώτον, υπάρχουν εγκλήματα που πληγώνουν τους ανθρώπους. Τα περισσότερα από αυτά με το πέρασμα των χρόνων έχουν κωδικοποιηθεί εγκληματολογικά, π.χ. ανθρωποκτονία, επίθεση, κλοπή, βιασμός, ληστεία, διάρρηξη κ.τ.λ. Αυτά είναι συνήθως τα εγκλήματα που οι πολίτες φοβούνται περισσότερο, και συχνά συνεργάζονται με την αντίληψη του αυξανόμενου εγκλήματος. Είναι επίσης αυτά που λαμβάνουν σημαντική προσοχή των μέσων μαζικής ενημέρωσης.

Δεύτερον, υπάρχουν ενέργειες που φοβίζουν, ενοχλούν ή προσβάλουν τους ανθρώπους. Μερικοί από αυτούς είναι θύματα εγκλημάτων ή αντιλήψεων του κινδύνου ή ανασφαλούς συμπεριφοράς που μπορεί να επηρεάσει έναν θεατή.

Τρίτον, είναι τα νέα εγκλήματα, εκείνα που έχουν εμφανιστεί πρόσφατα, που έχουν σχέση μερικώς με το οργανωμένο έγκλημα, τη

[1] Βλ., στο http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/index.html
[2] Βλ., Λαμπροπούλου Έφη, «Κοινωνικός Έλεγχος του Εγκλήματος», Αθήνα 1994, Εκδόσεις Παπαζήση, σ.123

διακίνηση ναρκωτικών, το ξέπλυμα χρημάτων, το έγκλημα ενάντια στο περιβάλλον αλλά και το έγκλημα που τελείται μέσω του διαδικτύου.

Η παρούσα βιβλιογραφική συνθετική μελέτη εστιάζει στον τρίτο τύπο εγκλήματος, αυτό του ηλεκτρονικού.

Προσπαθώντας όλο αυτό το διάστημα της έρευνας να σκιαγραφήσουμε το προφίλ αυτού του νέου κοινωνικού φαινομένου διαπιστώσαμε πως τα πράγματα δεν ήταν τόσο απλά. Οι δυσκολίες πολλές, τα διαφορετικά πεδία έρευνας αρκετά και η επίσημη βιβλιογραφία θα λέγαμε «ελλιπής» και «εξελίξιμη».

Σίγουρα το «πάντρεμα» δύο διαφορετικών εννοιών, «πληροφορική» και «παρέκκλιση» φάνταζε παράλογο μερικές δεκαετίες πριν αφού τα κρούσματα πληροφορικής παρέκκλισης ήταν ελάχιστα έως μετρημένα. Σήμερα το διαδίκτυο θα θεωρηθεί, πιθανώς, η μεγαλύτερη τεχνολογική αλλά και κοινωνικοοικονομική επανάσταση με την οποία έκλεισε ο 20ος αιώνας και ξεκίνησε ο 21ος. Σχεδόν όλες οι πλευρές της ζωής και οι κοινωνικές κατηγορίες επηρεάζονται από τις λειτουργίες του. Τα οφέλη είναι πολλά και μεγάλα, χωρίς όμως να λείπουν και οι αρνητικές συνέπειες, όπως και οι κίνδυνοι από την άκριτη και ανεξέλεγκτη χρήση του.

Πάνω σε αυτό το σκεπτικό κτίστηκε η διδακτορική έρευνα αποσκοπώντας στην ανάδειξη και παρουσίαση ενός κοινωνικού φαινομένου που τα τελευταία δέκα χρόνια φαίνεται πως έχει λάβει ανησυχητικές διαστάσεις. Σκοπός της παρούσης, είναι να παρουσιασθούν όσο πιο αναλυτικά και διεξοδικότερα γίνεται τα ιστορικά στοιχεία που οδήγησαν στην εγκληματικότητα μέσω των Ηλεκτρονικών υπολογιστών χρησιμοποιώντας το διαδίκτυο, να ορισθούν και να κατηγοριοποιηθούν τα ηλεκτρονικά εγκλήματα και να παρουσιασθούν οι μορφές τους. Κι αν όλα αυτά ισχύουν για τα ενήλικα και μεγαλύτερα σε ηλικία μέλη της κοινωνίας, οι δυνατότητες και οι απειλές που εμπεριέχει το Ιντερνέτ γίνονται ακόμη πιο κρίσιμες και καθοριστικές για τα παιδιά και τους νέους, τουλάχιστον μέχρι

την ενηλικίωσή τους, στα 18. Πρόκειται δηλαδή για φαινόμενα παιδικής πορνογραφίας. Επίσης έμφαση δίνεται και σε θέματα ασφάλειας στο διαδίκτυο καθώς και στο τρόπο που προσεγγίζουν οι διωκτικές αρχές το έγκλημα στο κυβερνοχώρο. Παράλληλα για την κατανόηση τέτοιων φαινομένων - κρουσμάτων κρίθηκε σκόπιμο – αναγκαίο να παραθέσουμε έρευνες, μελέτες, περιστατικά και πραγματικά γεγονότα που έλαβαν χώρα ανά τον κόσμο και τέλος να προτείνουμε τρόπους αντιμετώπισης και προστασίας από εγκληματικές διαδικτυακές επιθέσεις.

Η δομή της εργασίας

Στις επόμενες παραγράφους παρατίθεται μια συνοπτική περιγραφή της δομής και των περιεχομένων της εργασίας.

Στο πρώτο κεφάλαιο αναφέρονται κάποια εισαγωγικά στοιχεία και εννοιολογικές διασαφηνίσεις περί Κυβερνοχώρου και επιστημονικών τοποθετήσεων για το τι είναι πληροφορική κακοχρησία και τι πληροφορικό έγκλημα.

Στο δεύτερο κεφάλαιο παρουσιάζονται μερικές ριζοσπαστικές και φιλελεύθερες απόψεις για το πληροφορικά ηλεκτρονικό έγκλημα καθώς και μια προσέγγιση αυτού του φαινομένου κοινωνικά και νομικά από την πρώιμη κιόλας εμφάνιση του.

Στο τρίτο κεφάλαιο γίνεται μια σύντομη ιστορική ανασκόπηση των υπολογιστικών εργαλείων από την προϊστορία των ηλεκτρονικών υπολογιστών μέχρι και τις γενιές που έφερε η τεχνολογική εξέλιξη τους.

Το τέταρτο κεφάλαιο περιλαμβάνει την θεματική της έρευνας. Γίνεται μια προσπάθεια απόδοσης του ορισμού και της κατηγοριοποίησης των ηλεκτρονικών εγκλημάτων. Αλλά και των νέων μορφών που έχουν λάβει τα τελευταία χρόνια.

Στο πέμπτο κεφάλαιο αναλύεται το φαινόμενο του Χόκινγκ (hacking). Δίνονται ορισμοί και παρουσιάζεται η σκοτεινή και θετική πλευρά του.

Στο έκτο κεφάλαιο μελετάται το πολυσύνθετο κοινωνικοοικονομικό φαινόμενο της παιδικής πορνογραφίας στο διαδίκτυο, το οποίο έχει έξαρση τα τελευταία χρόνια και εμφανίζεται σε μεγάλη έκταση ανά τον κόσμο κυρίως ως μια μορφή εκμετάλλευσης παιδιών και εφήβων και συνοδεύεται από ποικίλες επιπτώσεις στη σωματική και ψυχική τους υγεία αλλά και στη μελλοντική τους εξέλιξη. Το συγκεκριμένο κεφάλαιο χωρίζεται σε τρία (3) μέρη: Στο Α' μέρος, επιχειρείται αρχικά μια αναδρομή στις ιστορικές διαστάσεις της παιδικής πορνογραφίας. Στη συνέχεια δίνονται στοιχεία για την έκταση της παιδικής πορνογραφίας ανά τον κόσμο σήμερα. Στο Β' μέρος, αναφέρονται διάφορες έρευνες που έχουν πραγματοποιηθεί σχετικά με το θέμα. Παρουσιάζεται η νομοθεσία που αφορά την παιδική πορνογραφία και η οποία έχει θεσμοθετηθεί πρόσφατα. Περιλαμβάνονται επίσης οι τρόποι προστασίας των ανηλίκων και κάποιες συμβουλές. Τέλος, στο Γ' μέρος, παρατίθενται τα συμπεράσματα της μελέτης και προτείνονται μέτρα καταπολέμησης της παιδικής πορνογραφίας οι ιστορικές διαστάσεις και οι προεκτάσεις αυτού.

Στο κεφάλαιο έβδομο αποδίδεται το πρόβλημα της νομικής ορολογίας στον όρο ηλεκτρονικό έγκλημα και παρουσιάζονται αναλυτικά οι προσπάθεια νομικής αντιμετώπισης του θέματος στον Ευρωπαϊκό νομικό χώρο.

Στο κεφάλαιο όγδοο παρουσιάζονται οι βασικές αρχές του όρου «ασφάλεια» στο Διαδίκτυο, η τεχνική διάσταση του όρου ασφάλεια στο διαδίκτυο καθώς και η προσέγγιση του εγκλήματος στον κυβερνοχώρο από τις διωκτικές αρχές.

Στο ένατο κεφάλαιο, παρατίθενται Έρευνες , Μελέτες & Περιστατικά για το Ηλεκτρονικό Έγκλημα καθώς και άρθρα που περιγράφουν πραγματικά γεγονότα από την εξέλιξη του φαινομένου αυτού και τέλος, ακολουθεί το δέκατο κεφάλαιο με τις προτάσεις, τα συμπεράσματα και το λεξικό όρων πληροφορικής.

Εισαγωγή

Οι ηλεκτρονικές επικοινωνίες έχουν αναμφισβήτητα προάγει τη ζωή μας. Μπορούμε πολύ εύκολα να διαπιστώσουμε την παρουσία της υψηλής τεχνολογίας σε κάθε έκφανση της ζωής μας και για κάθε χρήση της. Καθημερινά, όλο και περισσότερος κόσμος χρησιμοποιεί το Διαδίκτυο, τα κινητά τηλέφωνα, τις ψηφιακές φωτογραφικές μηχανές, τα ψηφιακά βίντεο, τους ψηφιακούς αναπαραγωγείς μουσικών τραγουδιών και, φυσικά, τους προσωπικούς ηλεκτρονικούς υπολογιστές.[3]

Η λεγόμενη, ψηφιακή κοινωνία, έχει άμεση επίδραση στη ζωή των ατόμων που αποτελούν μέλη της καθώς, με την παραγωγή πλήθους πληροφοριών, η ροή των οποίων επεκτείνεται συνεχώς, προσφέρει τεράστιες δυνατότητες σε όσους έχουν την γνώση και τη διάθεση να τις εκμεταλλευτούν με οποιοδήποτε τρόπο.[4]

Αναμφισβήτητα, η βάση της τεχνολογίας αυτής της ψηφιακής κοινωνίας είναι το Διαδίκτυο, το οποίο έχει αλλάξει τον τρόπο με τον οποίο ο κόσμος δουλεύει, επικοινωνεί, μαθαίνει αλλά το κυριότερο, ζει. Αποτελεί το κυριότερο εργαλείο με το οποίο ο άνθρωπος επικοινωνεί ταχύτατα όσο ποτέ άλλοτε. Άλλωστε, ένα από τα σπουδαιότερα και πιο σημαντικά χαρακτηριστικά του Διαδικτύου είναι η άνεση και η ταχύτητα που προσφέρει καθώς σχεδόν τα πάντα μπορούν να γίνουν με το πάτημα ενός πλήκτρου ή με τη χρήση του ποντικιού. Για παράδειγμα, μπορεί κανείς να εργάζεται χωρίς να φεύγει από το σπίτι του, να οργανώσει ένα κοινωνικό γεγονός χρησιμοποιώντας το ηλεκτρονικό ταχυδρομείο ή ακόμα και να παίζει σκάκι με κάποιον απομακρυσμένο παίχτη. Στο Διαδίκτυο, ο τόπος χάνει τη σημασία του γιατί η φυσική παρουσία δεν είναι απαραίτητη όταν κάποιος θέλει να

[3] Βλ., ΚΕΝΤΡΟ ΠΛΗ. ΝΕ. Τ. Ν. ΦΛΩΡΙΝΑΣ – «Δίκαιο και Internet» στο dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html

[4] Τσουραμάνης Χρ. στο www.teimes.gr_spoudastirio_yifiaki_eglimatikotita "Ψηφιακή Κοινωνία, Ψηφιακή Εγκληματικότητα και Θυματοποίηση".

ψωνίσει, να πάρει και να δώσει χρήματα, να ψάξει πληροφορίες που τον ενδιαφέρουν, να συνομιλήσει με κάποιον άλλο. Η ανάπτυξη του Παγκόσμιου Ιστού (World Wide Web) έχει κάνει τη διάδοση των πληροφοριών κτήμα του καθενός και το κυριότερο, σε ελάχιστο χρόνο. Μία ακόμα θετική πλευρά του Διαδικτύου και σημαντικό, επίσης, χαρακτηριστικό είναι η τεράστια πηγή πληροφοριών που προσφέρει. Η σωστή χρήση του μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών, προσφέροντας τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης. Επομένως η συμβολή του στην εκπαιδευτική διαδικασία είναι αναμφισβήτητα σημαντική.[5]

Παρ' όλα αυτά, η ψηφιακή κοινωνία είναι αυτή που χωρίζει και διαιρεί τα μέλη της, σε ψηφιακούς εγγράμματους, σε εκείνους δηλαδή που έχουν την δυνατότητα να χρησιμοποιούν το Διαδίκτυο, και στους ψηφιακούς αγράμματους, σε αυτούς δηλαδή που για διάφορους λόγους, είτε οικονομικούς είτε μαθησιακούς κ.τ.λ., δεν έχουν την δυνατότητα χρησιμοποίησης του με αποτέλεσμα κάτι τέτοιο να βοηθάει στην αύξηση των κοινωνικών διακρίσεων.[6]

Το σημαντικότερο, όμως, μειονέκτημα του Διαδικτύου είναι αυτό που αποτελεί και το κυριότερο λειτουργικό πρόβλημα του. Η μη ασφάλεια[7], δηλαδή, του περιεχομένου των πληροφοριών του από αλλοιώσεις και καταστροφές που προέρχονται από μη εξουσιοδοτημένη χρήση των πόρων του με άμεσο αποτέλεσμα την εμφάνιση διαφόρων τύπων ηλεκτρονικών εγκλημάτων.

---

[5] Βλ., Ενότητα 4.1, Κεφάλαιο 4. Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

[6] Βλ., Ενότητα "Collecting And Preserving Evidence On The Internet", Κεφάλαιο 7, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

[7] Η Ζαραφωνίτου Χριστίνα στο «Εμπειρική Εγκληματολογία», 1995 σημειώνει πως στις παραδοσιακές μορφές εγκληματικότητας, έχουν προστεθεί και αρκετές σύγχρονες οι οποίες απορρέουν από την τεχνολογική εξέλιξη, όπως είναι η εγκληματικότητα του τομέα της Πληροφορικής. Διακριτικό γνώρισμα αυτής της μορφής αδικημάτων είναι οι υπολογιστές είτε ως μέσο είτε ως σκοπός του αδικήματος. Βασικό χαρακτηριστικό και αυτών των αδικημάτων, σύμφωνα με τον Parker (1974), αποτελεί ο μεγάλος σκοτεινός αριθμός, ο οποίος δεν μας επιτρέπει να κάνουμε υποθέσεις σχετικά με τις πραγματικέ διαστάσεις του φαινομένου. Η αμερικανική εμπειρία εκτίμησε, μέσα από τη μελέτη 148 περιπτώσεων το 1973, ότι ο αριθμός αυτός δεν αντιπροσώπευε ουτε το 15% των αδικημάτων αυτής της μορφής

Το Διαδίκτυο παρά τις δυνατότητες που προσφέρει δεν είναι ένας χώρος, όπως ο πραγματικός που ζούμε και κινούμαστε καθημερινά. Είναι ένα μη σταθερό περιβάλλον το οποίο κανείς δεν μπορεί να ελέγξει, να χειραγωγήσει και να οριοθετήσει νομικά. Έτσι, το έγκλημα στο Διαδίκτυο αγνοεί τα εδαφικά όρια του πραγματικού χώρου και δεδομένου ότι μπορεί να είναι πλήρως αυτοματοποιημένο, μπορεί να διαπραχθεί σε μια ευρύτερη κλίμακα από το έγκλημα στο πραγματικό χώρο.

Το πολύ μεγάλο ποσοστό της αλματώδης αύξησης των παράνομων δραστηριοτήτων στο Διαδίκτυο, οφείλεται σε δύο από τις πιο διαδεδομένες ανακρίβειες για αυτό: την ανωνυμία και την απόλυτη ελευθερία έκφρασης στους χρήστες του.

Κεφάλαιο 1ο - Εννοιολογικές διασαφηνίσεις

Οι σημερινές τεχνολογικές δυνατότητες επιτρέπουν σε μικρές ομάδες με σχετικά λίγα μέσα να καταφέρουν τεράστιες ζημιές απέναντι σε πολύ μεγαλύτερα και καλύτερα εξοπλισμένα σύνολα. Οι επιτιθέμενοι είναι οργανωμένοι σαν δίκτυο, δηλαδή είναι αποκεντρωμένοι και αόρατοι, αντίθετα οι στόχοι τους είναι σαφώς καθορισμένα κέντρα πολιτικής και οικονομικής δραστηριότητας. Ένα συμπέρασμα του τρομοκρατικού χτυπήματος στους Δίδυμους Πύργους και στο Πεντάγωνο είναι ότι η ύπαρξη τέτοιων κέντρων αρχίζει ν' αποτελεί την αχίλλειο πτέρνα του ισχυρότερου κράτους της Γης.[8]

Η ταχύτατη ανάπτυξη και η αλματώδης αύξηση της χρήσης των ηλεκτρονικών υπολογιστών προσέφεραν απεριόριστες δυνατότητες σε όλους τους τομείς της σύγχρονης οικονομικής και κοινωνικής ζωής. Η τεχνολογία των ηλεκτρονικών υπολογιστών παρέχει σημαντικές δυνατότητες, όπως επιτάχυνση των διαδικασιών, απλοποίηση εργασιών, οργάνωση των πληροφοριών, ακριβή και άμεσο υπολογισμό, διαχείριση ευρύτατου όγκου δεδομένων. Αυτές οι δυνατότητες οδήγησαν σε ριζική αλλαγή των προτύπων δράσης και προγραμματισμού δημόσιων οργανισμών, ιδιωτικών επιχειρήσεων και ιδιωτών. Η διάδοση του Διαδικτύου έδωσε δυνατότητες ενημέρωσης, μέσω του τεράστιου όγκου των πληροφοριών που μεταδίδονται σε ταχύτατους ρυθμούς. Τα δεδομένα που είναι καταχωρημένα στο Internet και οι πληροφορίες που διακινούνται καθημερινά σε παγκόσμια κλίμακα προσφέρουν σημαντικές διευκολύνσεις σε κάθε τομέα της ανθρώπινης δραστηριότητας. Οι αλλαγές αυτές δημιούργησαν κατάλληλες συνθήκες για την εμφάνιση νέων μορφών εγκληματικότητας, ενώ το Διαδίκτυο αποτέλεσε μέσο διάδοσης εγκληματικών φαινομένων και αδικημάτων. Όλες αυτές οι

---

[8] Χρύσανθος Δελλαρόκας, καθηγητής του M.I.T (Massachusetts's Institute of Technology) και αυτόπτης μάρτυρας στο τρομοκρατικό χτύπημα της 11ης Σεπτεμβρίου 2001 στο Παγκόσμιο Κέντρο Εμπορίου.

μορφές εμπεριέχονται στον όρο «ηλεκτρονικό έγκλημα» ή «πληροφορικό έγκλημα» ή όπως έχει επικρατήσει παγκοσμίως «computer crime».

Διεθνώς είναι γνωστό ως «computer crime». Περιλαμβάνει μια ήπειρο εγκλημάτων με μοναδικό όπλο την πρόσβαση από ένα υπολογιστικό σύστημα σε ένα άλλο με τη χρήση του modem.[9] Στις αρχές της δεκαετίας του '80 «το ηλεκτρονικό έγκλημα» ή, όπως το αναφέρει ο, επίκουρος καθηγητής Εγκληματολογίας, Γρηγόρης Λάζος το «πληροφορικό έγκλημα» έκανε μαζική εμφάνιση. Οι ανταλλαγές των πληροφοριών για τα «σπασμένα» δίκτυα και συστήματα γίνονταν μέσω των σχεδόν πρωτόγονων βάσεων δεδομένων των Bulletin Broad Systems (BBS). Ήταν τα πρώτα βήματα για τη δημιουργία μιας underground κοινωνίας χρηστών του Διαδικτύου και τα πρώτα ακούσματα των όρων hacking και phreaking. «Αυτός ο συνδυασμός εξουσίας, τεχνογνωσίας και εξασφαλισμένης ανωνυμίας επέδρασε σαν ακαταμάχητος πειρασμός στα νεαρά αγόρια» έγραφε ο Μπρους Στέρλινγκ[10] στο «The hacker crackdown». Και αν χάκερ στην κυριολεξία σημαίνει «αυτός που πελεκάει το ξύλο με τσεκούρι», είναι σαφές ότι τα τελευταία 20 χρόνια ο όρος έχει λάβει μυθικές διαστάσεις και έχει να κάνει με καταστροφή δικτύων, διασπορά ιών, σπάσιμο κωδικών. Ταυτόχρονα, αυτός που κατέχει την τεχνογνωσία είναι και ο πραγματικά κυρίαρχος. Αυτός ελέγχει μέσω της πληροφορικής τα αρχεία του κράτους - τελωνεία, αρχεία νοσοκομείων, τραπεζών-, άρα τους πολίτες. Είναι το μάτι του «μεγάλου αδελφού» που όσοι νόμοι περί προστασίας της προσωπικότητας και των ατομικών δικαιωμάτων και αν θεσπισθούν πάντα ο πολίτης θα αισθάνεται ότι κάποιοι ελέγχουν τις μύχιες σκέψεις του.

Ο όρος «κυβερνοχώρος» πλάσθηκε από το συντάκτη William Gibson[11] στη Νουβέλα που έγραψε το 1984 με τίτλο «Nuromancer», για να περιγράψει

---

[9] Συντομογραφία του MO-dulator / DEModulator (διαμορφωτής / αποδιαμορφωτής). Το μόντεμ (όπως ονομάζεται πλέον και στα Ελληνικά) επιτρέπει στον υπολογιστή να επικοινωνήσει μέσω τηλεφωνικών γραμμών με άλλους υπολογιστές.

[10] Βλ., Bruce Sterling. «The Hacker Crackdown Law and Disorder on the Electronic Frontier». 1992

[11] Η λέξη κυβερνοχώρος προτάθηκε από τον Γουίλιαμ Γκίμπσον William Gibson, που τον χρησιμοποίησε στο μυθιστόρημά του Νευρομάντης το 1984. Ο Gibson περιέγραψε ένα σενάριο σύμφωνα με το οποίο οι "κάουμπου της κονσόλας" έμπαιναν στον κυβερνοχώρο με τα κράνη τους και πρόβαλλαν τη συνείδησή τους σε τρισδιάστατα 'εικονικά' περιβάλλοντα. Ο Gibson εδώ προσδοκούσε πιθανώς ότι η ανθρώπινη φαντασία θα δημιουργούσε νέες αντιληπτικές «πραγματικότητες» μέσω της τεχνολογίας. Είκοσι δύο χρόνια μετά την έκδοση του Νευρομάντη, το

το περιβάλλον μέσα στο οποίο οι χάκερ των υπολογιστών αναπτύσσουν δραστηριότητες.[12] Σε αυτό το βιβλίο επιστημονικής φαντασίας, η δραστηριότητα της αναρμόδιας πρόσβασης - χάραξης στο περιεχόμενο των συγκροτημάτων ηλεκτρονικών υπολογιστών, εξαπλώνεται στους πολύ φυσικούς όρους.[13] Η εικόνα του χάκερ είναι αυτή που υπερνικά τα φυσικά εμπόδια ασφάλειας, διαπερνώντας την καρδιά των συγκροτημάτων των ηλεκτρονικών υπολογιστών, κάνοντας τις αλλαγές στη φυσική δομή με τέτοιο τρόπο που τροποποιεί τη λειτουργία του συστήματος.[14] Στο τέλος της διαδικασίας ο χάκερ αλλοιώνει ή παίρνει μαζί του τα λογισμικά στοιχεία του συστήματος.[15]

Στο βιβλίο της, «The Pearly Gates of Cyberspace», η συγγραφέας Margaret Wertheim υποστηρίζει ότι το Διαδίκτυο μας παρέχει μια νέα έννοια του χώρου - τον αλληλοσυνδεόμενο «χώρο» ενός παγκόσμιου δικτύου υπολογιστών. Όπως επισημαίνει, τούτη η νέα αντίληψη είναι ένα πολύ πρόσφατο φαινόμενο. Κατά τον 20ο αιώνα, στις αρχές της δεκαετίας του '80 λίγοι άνθρωποι - εκτός από τον στρατιωτικό και ακαδημαϊκό τομέα της

βασίλειο της εικονικής πραγματικότητας έχει καθιερωθεί ήδη ως πολύτιμο εργαλείο σε τομείς όπως την αρχιτεκτονική και η ιατρική.

[12] Στην πραγματικότητα, η συμμετοχή των οργανωμένων ομάδων εγκλήματος στον τομέα της απάτης υπολογιστών διαλευκάνθηκε όταν επιτέθηκε μια ρωσική ομάδα σε μια από τις πιο γνωστές αμερικανικές τράπεζες στη Νέα Υόρκη μέσω των δικτύων δεδομένων το 1994. Λειτουργούσαν από την Αγία Πετρούπολη και η ομάδα κατάφερε να μεταφέρει άνω των $10 εκατομμυρίων σε ξένους λογαριασμούς από την Αμερικανική Τράπεζα. Ο αρμόδιος ανώτερος υπάλληλος ασφάλειας της τράπεζας είπε στο συντάκτη ότι οι συλληφθέντες δράστες κατείχαν πλαστά ελληνικά και ισραηλινά διαβατήρια που ποιοτικώς ήταν τόσο πιστά που μόνο μέλη της πρώην ρωσικής μυστικής υπηρεσίας KGB της Ρωσίας θα μπορούσαν να τα παράγουν. Βλ., M. LYMAN and G. POTTER, *Organized Crime* (New Jersey, Prenhall); U. SIEBER, *Legal Aspects of Computer Related Crime* (European Commission), [1998] p. 25.

[13] Βλ., C. REED, *Computer Law* (U.K, John Angel), [2004] p. 242

[14] Βλ., Mcconnell International, *Cybercrime...and Punishment? Archaic Laws Threaten Global Information* [Dec., 2000].

[15] Πολλές από τις νομικές προκλήσεις που αντιμετωπίζουν οι κατήγοροι στην αναζήτηση εγκληματιών του διαδικτύου, είναι όταν εμφανίζονται μέσω ιών και συγκεκριμένα μέσω του ιού 'I.ove Bug Virus'. Ο συγκεκριμένος ιός κατέστρεψε αρχεία και έκλεψε τους κωδικούς πρόσβασης. Ο ιός που είχε επιπτώσεις επίσης στη NASA και τη CIA και συναγωνίστηκε σε όλο τον κόσμο σε δύο ώρες, τρεις φορές γρηγορότερα από τον ιό Melissa, προκάτοχο του. Όσον αφορά στη ζημία, οι εκτιμήσεις για το ποσό ποικίλουν από $2 δισεκατομμύρια σε $10 δισεκατομμύρια , δεδομένου ότι είναι πάντα δύσκολο να αξιολογηθεί η εκτίμηση η ζημιά που επιβάλλεται από το cybercrime. Βλ., D. HOPPER, *Destructive ILOVEYOU Computer Virus Strikes WorldWide* , διαθέσιμο στο <http://archives.cnn.com/2000/TECH/computing/05/04/iloveyou/>(visited 25/03/2005), J. LEYDEN, *LoveBug Threatens Email Servers* [5 May 2000], <http://www.vnunet.com/news/1100661> (visited 25/03/2005), P. FESTA and J. WILCOX, *Experts Estimate Damages in the Billions for Bug* [5 May 2000], at:
<http://news.com.com/2100-1001-240112.html?legacy=cnet>

πληροφορικής - είχαν πρόσβαση στο δίκτυο. Σήμερα υπάρχουν δισεκατομμύρια δικτυακοί τόποι στο διαδίκτυο. «Το 1998», γράφει η Wertheim, «υπήρχαν πάνω από 100 εκατομμύρια τακτικοί χρήστες του Διαδικτύου και υπολογίζεται ότι στην επόμενη δεκαετία θα υπάρχουν ένα δισεκατομμύριο άνθρωποι σε απευθείας σύνδεση. Όλος αυτός ο 'χώρος' ξεπήδησε μέσα σε 25 χρόνια από το τίποτα».

Όμως, είναι η πραγματική φύση της εμπειρίας του κυβερνοχώρου που βρίσκει συναρπαστική η Wertheim. Όταν επικοινωνεί κανείς με κάποιον άλλο σε απευθείας σύνδεση, δεν υπάρχει καμία αίσθηση του φυσικού χώρου, για τα κυβερνοταξίδια δεν μπορούν να μετρηθούν με την κυριολεκτική έννοια του όρου μέτρηση. «Διασκορπισμένος στο Διαδίκτυο», λέει, «ο χώρος μου δεν μπορεί πλέον να καθοριστεί με καθαρά φυσικά κριτήρια. Το που ακριβώς βρίσκομαι όταν μπαίνω στο Διαδίκτυο είναι ένα ερώτημα προς διερεύνηση, αλλά σίγουρα η θέση μου δεν μπορεί να μετρηθεί μαθηματικά». Έτσι το μόνο που μπορούμε πιθανώς να επιβεβαιώσουμε για τη φύση του κυβερνοχώρου, είναι ότι περιλαμβάνει μια μορφή ψηφιακής επικοινωνίας στην οποία οι πληροφορίες αναμεταδίδονται από τον ένα υπολογιστή στον άλλο, και στην οποία επίσης οι άνθρωποι μοιράζονται το διανοητικό τους έργο.

Αυτό δεν είναι απλά μια επικοινωνία ανταλλαγής πληροφοριών, όμως. Όπως έχουν ανακαλύψει πολλοί ενθουσιώδες θιασώτες του Διαδικτύου, ο κόσμος του κυβερνοχώρου είναι επίσης σφαίρα δραστηριότητας στην οποία μπορούν να διαμορφωθούν φανταστικές προσωπικότητες (personae) μέσω της εικονικής πραγματικότητας. Σε αυτή τη σφαίρα οι ανθρώπινες υπάρξεις αλληλεπιδρούν μεταξύ τους με τρόπους που μπορούν να περιοριστούν ίσως μόνο από τις δυνατότητες της φαντασίας τους.

Ο κυβερνοχώρος φθείρει ριζικά τη σχέση μεταξύ των νομικά σημαντικών φαινομένων και της φυσικής θέσης των.[16] Η άνοδος του παγκόσμιου δικτύου υπολογιστών καταστρέφει τη σύνδεση μεταξύ της γεωγραφικής θέσης και:

(1) της δύναμης των τοπικών κυβερνήσεων να βεβαιώσουν τον έλεγχο της on line συμπεριφοράς

(2) των επιπτώσεων της «on line» συμπεριφοράς στα άτομα ή τα πράγματα

(3) η νομιμότητα των προσπαθειών ενός τοπικού κυρίαρχου να επιβάλει κανόνες εφαρμόσιμους στα παγκόσμια φαινόμενα και

(4) η δυνατότητα της φυσικής θέσης να δώσει πληροφορία της οποίας τα σύνολα των κανόνων ισχύουν.[17]

Αντιμέτωποι με την ανικανότητά τους να ελέγξουν τη ροή των ηλεκτρονίων μέσω των φυσικών συνόρων[18], μερικοί νομοθέτες προσπαθούν να εμβάλουν τα όρια τους στα ηλεκτρονικά μέσα μέσω φιλτραρισμένων μηχανισμών και την καθιέρωση ηλεκτρονικών εμποδίων.[19] Άλλοι έσπευσαν να βεβαιώσουν το δικαίωμα να ρυθμιστεί το εμπόριο με σύνδεση on line στο

[16] Στην πραγματικότητα, η δυσκολία έρχεται στον καθορισμό των νόμων που πρέπει να είναι σε ισχύ για να αποτρέψουν τη συνέχιση των cyber criminals. Ενώ αυτή η επιβολή του νόμου είναι ένας απλός στόχος, προκύπτει πραγματικά μερικές δυσκολίες πάνω σε αυτό. Κάθε χώρα πρέπει να καθορίσει το επίπεδο των παραβάσεων – απατών στο διαδίκτυο αλλά και το βαθμό επιβολής του νόμου ανάλογα με την νομοθεσία της εκάστοτε χώρας. Κατά συνέπεια, είναι απαραίτητο για μια χώρα να θεσπίσει ένα νόμο περί απάτης του διαδικτύου, εάν δεν τον έχει θεσπίσει ήδη. Βλ., M. D. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal Conduct in Cyberspace* (Oxford, International Journal of Law and Information Technology), [200] Vol. 10, n. 2 p. 3.

[17] Στην πραγματικότητα, ο όρος κυβερνοχώρος σημαίνει κυριολεκτικά το «πλεύσιμο διάστημα » και προέρχεται από την ελληνική λέξη kyber (=για να πλοηγήσει). Στο μυθιστόρημα του William Gibson's (1984), η αρχική πηγή του όρου κυβερνοχώρος, αναφέρεται ως ένα πλεύσιμο, ψηφιακό διάστημα των δικτυωμένων υπολογιστών προσιτών από τις κονσόλες υπολογιστών, ένα οπτικό, ζωηρόχρωμο, ηλεκτρονικό, καρτεσιανό datascape γνωστό ως «η μήτρα», όπου οι επιχειρήσεις και τα άτομα αλληλεπιδρούν με πληροφορίες. Έπειτα από τη δημοσίευση αυτού του μυθιστορήματος, ο όρος κυβερνοχώρος ήταν, προσαρμόστηκε και χρησιμοποιήθηκε με ποικίλους τρόπους, από πολλές διαφορετικές εκλογικές περιφέρειες, οι οποίες με κάποιο τρόπο αναφέρονται στην αναδυόμενη μέσω υπολογιστή επικοινωνία και τις τεχνολογίες εικονικής πραγματικότητας. Εδώ, επικεντρώνουμε εκ νέου τον καθορισμό του από μια προηγούμενη εννοιολογική προσέγγιση του Gibson, έτσι ώστε ο κυβερνοχώρος να αναφέρεται στο εννοιολογικό διάστημα μέσα σε ICTs, παρά στην ίδια τη τεχνολογία. *Βλ.*, W. GIBSON, *Neuromancer*, New York, Grafton, 1984; M. DODGE, *Mapping Cyberspace*, N.Y, Routeldge, 2001, σ. 1.

[18] Βλ., C. REED, *Computer Law*, U.K, John Angel, 2004 σ. 242

[19] Βλ., *όπ.π.*

βαθμό που αυτό μπορεί να είναι ενάντια στους τοπικούς πολίτες. Παραδείγματος χάριν ο γενικός εισαγγελέας της Μινεσότα, έχει βεβαιώσει το δικαίωμα να ρυθμίζει το παίξιμο τυχερού παιγνίου που εμφανίζεται σε ξένη ιστοσελίδα η οποία ήταν προσβάσιμη και «παρουσιαζόταν» στο κράτος της Μινεσότα από έναν ντόπιο[20]. Επίσης, η ρυθμιστική αντιπροσωπεία τίτλων του Νιου Τζέρσεϋ έχει βεβαιώσει ομοίως το δικαίωμα να διακόψει τη προσβασιμότητα σε οποιαδήποτε ιστοσελίδα η οποία προσβάλλει το κράτος.[21]

Ο κόσμος του παγκόσμιου εγκλήματος μετά την εξαιρετικά ραγδαία εξέλιξη των νέων τεχνολογιών επικοινωνίας αλλάζει. Τα δεδομένα στο παγκόσμιο έγκλημα εμπλουτίζονται με ρυθμούς γοργούς και εντυπωσιακούς. Η παράνομη δραστηριότητα αποκτά καινούριο πρόσωπο, οικουμενικό και ψηφιοποιημένο. Μέσα από τα άδυτα του Κυβερνοχώρου ξεπηδά η σύγχρονη μορφή του ασύμμετρου εγκλήματος. Οι παράνομοι μπορούν να κρυφτούν καλύτερα, να επικοινωνήσουν με τους συνεργάτες τους ευκολότερα, γρηγορότερα και εφ' όλης της ύλης, θέτοντας με ασύλληπτους ρυθμούς τις βάσεις μιας νέας «Διεθνούς του Εγκλήματος», την οποία οι όχι ανάλογα εξελιγμένες διωκτικές αρχές αδυνατούν να συλλάβουν τόσο εννοιολογικά όσο και κυριολεκτικά. Τουλάχιστον αυτή είναι η κατάσταση που επικρατεί στην πλειοψηφία των περιπτώσεων. Μένουν έτσι, ουραγοί των εξελίξεων, τα νήματα των οποίων κινούν συχνά πυκνά οι δάκτυλοι των ολοένα ισχυρότερων και πιο «δικτυωμένων» εγκληματιών.

Επιπροσθέτως, εγκληματολόγοι, νομικοί και κοινωνιολόγοι όπως η Nelson, ο Hollinger, οι Meier και Thomas συνιστούν την προσοχή σε μια πολύ σημαντική εκκρεμότητα: η κοινωνία δεν έχει ακόμα αποφασίσει ως προς τις ηθικές και πολιτιστικές συντεταγμένες των σχέσεων που δημιουργήθηκαν

---

[20] Βλ., *όπ.π.*

[21] Εντούτοις, το θόλωμα του πραγματικού και του εικονικού επεκτείνεται πέρα από το διανοητό. Οι αναλυτές έχουν αρχίσει πρόσφατα να υποστηρίζουν ότι τα γεωγραφικά περιβάλλοντά μας γίνονται virtualised και ως υπολογιστές χρησιμοποιούνται όλο και περισσότερο για να διαχειριστούν τις πληροφορίες σχετικά με αυτές τις θέσεις. Υπό αυτήν τη μορφή, η δομή πόλεων γίνεται αποτελεσμένη από και ελεγχόμενη από τους υπολογιστές, και μια επαναλαμβανόμενη σχέση εξελίσσεται έτσι ώστε καθώς η πόλη γίνεται με τη χρήση υπολογιστών, το δίκτυο υπολογιστών είναι η πόλη. Εδώ, τα εικονικά διαστήματα των στοιχείων και της διαχείρισης πόλεων και τα πραγματικά διαστήματα των κτηρίων και των οδών γίνονται περιπλεγμένα. Βλ., M. DODGE, *op. cit.* p. 22.

με την ταχύτατη ανάπτυξη των νέων τεχνολογιών, δεν έχει αποφασίσει ως προς το τι είναι πληροφορική κακοχρησία και τι πληροφορικό έγκλημα. Ο νόμος δεν έρχεται τόσο να επικυρώσει κάποια κοινά συμφωνημένα ηθικά και πολιτιστικά πρότυπα για τις σχέσεις και τη χρήση της πληροφορικής, αλλά μάλλον να επιβάλλει τα όρια στα οποία τα πρότυπα αυτά θα πρέπει να αναπτυχθούν.[22]

Στο επόμενο κεφάλαιο παρουσιάζονται μερικές ριζοσπαστικές και φιλελεύθερες απόψεις για το ηλεκτρονικό έγκλημα και οι πιο σημαντικά σύγχρονες κοινωνιολογικές προσεγγίσεις του εγκλήματος. Θα προσπαθήσουμε με τον τρόπο αυτό να κατανοήσουμε καλύτερα τον ορισμό, τη φύση και το περιεχόμενο της απόκλισης.

[22] Βλ., Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2001, σελ. 18.

Κεφάλαιο 2ο - Πληροφορικά Ηλεκτρονικό Έγκλημα: Η προσέγγιση ενός νέου κοινωνικού φαινομένου

2.1. Πληροφορική Παρέκκλιση: Η απροσάρμοστη εγκληματικότητα

Θα μπορούσε κανείς να υποστηρίξει πως το Πληροφορικό έγκλημα αποτελεί ένα κομμάτι της σύγχρονης εγκληματολογίας αν σκεφτεί πως για την σύγχρονη εγκληματολογία, το έγκλημα είναι ένα κοινωνικό πρόβλημα που παρουσιάζεται στο καθένα με πράξεις εγκλήματος. Αυτές οι πράξεις ή τουλάχιστον αυτές που φαινόντουσαν σοβαρές, επαναλαμβανόμενες ή παράλογες, θεωρούνταν συμπτώματα «εγκληματολογίας» και «εγκληματικότητας». Ήταν τα εμφανή συμπτώματα που έκαναν τη διαφορά, συνήθως βρισκόντουσαν σε άτομα αντικοινωνικά ή απροσάρμοστα. Αυτές οι διαφορές και οι όροι που τις παράγουν σχημάτιζαν το κατάλληλο αντικείμενο της εγκληματολογικής γνώσης. Σχημάτισαν επίσης το τέλειο στόχο για επανορθωτική πολιτική που έχουν μείνει για να αντιμετωπίζουν μεγαλύτερα προβλήματα. Όταν αναφερόμαστε στην «μοντέρνα εγκληματολογία»[23] δεν επιδιώκουμε να αναφερόμαστε σε εγκληματολογικές ιδέες που είναι σύγχρονες. Δεν βρισκόμαστε εδώ για παράδειγμα με τις εγκληματολογίες της καθημερινής ζωής ή τις θεωρίες επιλογής και ελέγχου που πρόσφατα είναι και σπουδαίες.[24]. Για τη σύγχρονη εγκληματολογία η απροσάρμοστη εγκληματικότητα ήταν το πρόβλημα, και η επανορθωτική θεραπεία ήταν η λύση.[25] Στην απροσάρμοστη πληροφορική εγκληματικότητα ίσως η επανορθωτική θεραπεία είναι οι ίδιοι οι χρήστες της τεχνολογίας οι οποίοι ίσως μπορέσουν να δώσουν κάποιες πρώτες απαντήσεις στο πρόβλημα που τα τελευταία 15 χρόνια μαστίζει τους κόλπους κάθε κοινωνικού ιστού.

---

[23] Με τον όρο «μοντέρνα εγκληματολογία» εννοούμε το σκελετό των προβλημάτων, εννοιών της πραγματοποίησης της εμφάνισης στα τέλη του δέκατου ένατου (19ου) αιώνα που επαράχθει από τη φαρμακευτική ψυχολογία, εγκληματολογική ανθρωπολογία, στις στατιστικές ανακρίσεις, στη κοινωνική μεταρρύθμιση και στη πειθαρχεία με φυλάκιση, ένας σκελετός που παρείχε συντεταγμένες για ινστιτούτα ποινικής ευημερίας που εξελίχθηκαν κατά τη διάρκεια των επόμενων 70 χρόνων

[24] Βλ. Garlad . D., «The Culture of High Crime Societies: Some Preconditions of Recent "Law and Order" Policies», *British Journal of Criminology*, 2000, 40/3. Επίσης βλ. Garlad . D., «Punishment and Welfare: A History of Penal Strategies», Aldershot: Gower, 1985

[25] Βλ., Garlad . D., «The Limits of the sovereign State:Strategies of Crime Control in Contemporary Society», *British Journal of Criminology*, 1996, 36/4.

2.2. Στοιχεία της παραβατικότητας στην κοινωνία της πληροφορίας

Η απροσάρμοστη πληροφορική εγκληματικότητα ίσως πηγάζει σε αυτό που σήμερα καλούμε ως «κοινωνία της πληροφορίας». Η κοινωνία της πληροφορίας δεν είναι μόνο μία κοινωνία γνώσης και ανάπτυξης. Τα δίκτυα ως ρεπλίκα της κοινωνίας χαρακτηρίζονται και περιέχουν όλες τις πλευρές της. Οι εγκληματίες έχουν επίσης ανακαλύψει τον κυβερνοχώρο. Η εγκληματικότητα αυτή έχει διάφορες μορφές: επίθεση κατά πληροφορικών συστημάτων, διάδοση παιδικής πορνογραφίας, απάτη, παραβιάσεις πνευματικής ιδιοκτησίας, προσβολές της ιδιωτικότητας, υποστήριξη της διάπραξης παραδοσιακών εγκλημάτων όπως η διακίνηση ναρκωτικών ή το δουλεμπόριο. Πρέπει να σημειωθεί ο ιδιαίτερα ευάλωτος χαρακτήρας της σημερινής κοινωνίας της πληροφορίας: η οικονομία, η διοίκηση και η κοινωνία είναι σε πολύ υψηλό βαθμό εξαρτημένες από την αποτελεσματικότητα και την ασφάλεια των πληροφορικών συστημάτων. Είναι μία κοινωνία υψηλών ευκαιριών και ευχερειών αλλά ταυτόχρονα μία κοινωνία κινδύνων.

Η ανωνυμία ως βασικό χαρακτηριστικό του δικτύου έχει σοβαρές συνέπειες για το ποινικό δίκαιο. Δεν δυσχεραίνει απλώς τη διαλεύκανση των εγκλημάτων αλλά δημιουργεί σοβαρό πρόβλημα και ως προς τις αποδείξεις. Ένα άλλο σοβαρό κοινωνιολογικό-εγκληματολογικό στοιχείο είναι ότι η ανωνυμία ενθαρρύνει τους χρήστες του Διαδικτύου να επιχειρήσουν εγκληματικές πράξεις τις οποίες δεν θα επιχειρούσαν παρά μόνο στον κυβερνοχώρο καθώς στον χώρο αυτό δεν φαίνεται να έχει διαμορφωθεί μία ηθική τάξη και δομή με σαφείς κανόνες δεοντολογίας, επιταγές και απαγορεύσεις.

Η διάδοση της τεχνολογίας των υπολογιστών σε όλες τις πλευρές της ζωής, η διασύνδεση των υπολογιστών σε διεθνή δίκτυα έχουν καταστήσει το έγκλημα πιο διαφοροποιημένο, πιο επικίνδυνο και διεθνοποιημένο. Τα νέα συστήματα έχουν ειδικά χαρακτηριστικά που διευκολύνουν τους δράστες

αλλά δυσχεραίνουν το έργο των διωκτικών αρχών (πολλαπλά συστήματα λογισμικού και hardware, έλλειψη εμπειρίας πολλών χρηστών, ανωνυμία, κρυπτογράφηση, διεθνής κινητικότητα). Το αποτέλεσμα:

- Η παραβατικότητα καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο.
- Τα εγκλήματα αυτά μπορούν να πραγματοποιηθούν από τον καθένα και να πλήξουν τον καθένα. Δεν χρειάζεται καν να εγκαταλείψει κανείς τον χώρο του σπιτιού του.
- Το Πληροφορικό Έγκλημα έχει αποκτήσει κινητικότητα και διεθνή χαρακτήρα
- Το Πληροφορικό Έγκλημα και το Διαδίκτυο έχουν αποκτήσει μεγάλη ελκυστικότητα για το οργανωμένο έγκλημα

Οι εξελίξεις αυτές θέτουν σοβαρότατα ζητήματα για το ποινικό δίκαιο καθώς τα μεθοδολογικά του παραδείγματα και οι κατηγορίες του τίθενται σε αμφισβήτηση ως προς τη ρυθμιστική τους ικανότητα.

2.3. Η φύση μιας νέας αποκλίνουσας δραστηριότητας

Σύμφωνα με τον ορισμό του λεξικού κοινωνικών επιστημών της Unesco, ως «αποκλίνουσα συμπεριφορά» (deviant behaviour) ορίζεται «η συμπεριφορά η οποία αποκρούεται ή συγκρούεται με τους γνώμονες (standards) που είναι κοινωνικώς και πολιτιστικώς αποδεκτή από μια κοινωνική ομάδα (social group) ή ένα κοινωνικό σύστημα (social system)»[26]. Απόκλιση (deviance) επομένως, θεωρείται, η μη συμμόρφωση σε κανόνες που είναι αποδεκτοί από ένα σημαντικό αριθμό ανθρώπων σε μια κοινωνία.[27]

Ίσως ένα από τα πλέον αρνητικά στοιχεία της πληροφορικής τεχνολογίας είναι και η δυνατότητα που παρέχει για τη διάπραξη μιας νέας σειράς «αποκλίνουσων δραστηριοτήτων», δραστηριοτήτων που εκτείνονται από το ανήθικο εώς το εγκληματικό. Η πληροφορική τεχνολογία κατέστησε

[26] Βλ., Himmelweit, «Λεξικό κοινωνικών επιστημών (Unesco)», τόμος τρίτος, σελ. 909
[27] Βλ., Giddens, 1989, σελ. 118

δυνατή τη διάπραξη ενός ευρέος φάσματος εγκλημάτων τα οποία, για να τελεσθούν απαιτούν εξειδικευμένη και, συχνά ιδιαίτερα υψηλή κατάρτιση. Η δυνατότητα αυτή αποτέλεσε για πολλούς την ευκαιρία διάπραξης νέων μορφών εγκληματικών ενεργειών.

2.4. Ποια είναι η ταυτότητα του Πληροφορικού Εγκλήματος;

Μέχρι τα μέσα της δεκαετίας του 1970, το πληροφορικό έγκλημα ως πραγματικότητα, έννοια και αντικείμενο συστηματικής εστίασης και ενασχόλησης δεν είχε εξασφαλίσει κάποια διακριτή ταυτότητα. Στην περιορισμένη και περιφερειακής σημασίας ειδική βιβλιογραφία της περιόδου, το πληροφορικό έγκλημα αντιμετωπίζεται κυρίως ως υποκατηγορία του οικονομικού εγκλήματος, του εγκλήματος του λευκού περιλαιμίου, του εγκλήματος της υπαλληλίας, ή ως παραλλαγή ή μετεξέλιξη εγκλημάτων που έχουν σχέση με τις τηλεφωνικές επικοινωνίες.

Μέσα σε λίγα χρόνια, ήδη από τα μέσα της δεκαετίας του 1980, το πληροφορικό έγκλημα εμφανίζεται να έχει εξασφαλίσει την από κάθε άποψη αυτόνομη ύπαρξή του. Κατά την δεκαετία 1975-1985 πραγματοποιήθηκε μια θεαματική αύξηση - ίσως ένας δεκαπλασιασμός - των δημοσιεύσεων αναφορικά με το πληροφορικό έγκλημα. Για παράδειγμα, οι Hollinger και Lanza-Kaduse προτείνουν ως πρώτο έτος για κοινωνική μετατροπή της πληροφορικής εισβολής σε πληροφορικό έγκλημα το 1983.[28]

Πάνω σε αυτές τις σταθερές συνέχειες και αναφορές του 1980 ο Volgyes ήταν πρώτος που αναφέρθηκε σε αυτή την αλλαγή. Συγκεκριμένα διατύπωσε πως «το πληροφορικό έγκλημα έχει μιαν απρόσωπη καθαρότητα. Είναι ένα έγκλημα που στρέφεται απόμακρα, διακριτικά και χωρίς βία ενάντια σε «αντιπαθητικές» κυβερνήσεις και επιχειρήσεις. Γι αυτό το λόγο, και το ευρύ

[28] Βλ., R. Hollinger και L.lanza-Kaduse, «The process of criminalization: The case of computer crime laws", *Criminology*, 1988.26, σσ.101-126

κοινό τείνει να αντιμετωπίζει το ηλεκτρονικό έγκλημα με ανοχή ή ακόμη και με συμπάθεια».[29]

2.5. Νομική και Κοινωνιολογική προσέγγιση του Πληροφορικού Εγκλήματος

Στο βιβλίο του Γρ. Λάζου, «Πληροφορική και Έγκλημα», αναπτύσσονται δύο βασικοί προσανατολισμοί στην προσπάθεια αντιμετώπισης και ελέγχου των συνεχών και θεαματικών ποσοτικών και ποιοτικών αλλαγών στο πληροφορικό έγκλημα.

Ο πρώτος προσανατολισμός εμφανίστηκε συντεταγμένα στο δεύτερο μισό της δεκαετίας του 1970 και επικράτησε κατά τη δεκαετία 1980-90 και θα μπορούσε να ονομασθεί *νομικός προσανατολισμός*. Μια μεγάλη μερίδα επιστημόνων κινήθηκε προς τη κατεύθυνση του να θέσει σε κάποια τάξη το φαινόμενο του πληροφορικού εγκλήματος. Με αφετηρία τους το παραδοσιακό δίκαιο και με την εκτεταμένη χρήση αναλογιών, διατύπωσαν τους πρώτους ορισμούς και σχημάτισαν τυπολογίες πληροφορικού εγκλήματος, επιχειρώντας με αυτό τον τρόπο να αμβλύνουν τη σύγχυση που προκαλούσε ο ραγδαία αυξανόμενος όγκος των εγκλημάτων που περιλάμβαναν στοιχεία ηλεκτρονικής ή, ευρύτερα, πληροφορικής τεχνολογίας. Είναι ο νομικός προσανατολισμός που προσέφερε τους πρώτους ορισμούς του πληροφορικού εγκλήματος, πρότεινε τις τυπολογίες και κατηγοριοποιήσεις που το συνθέτουν και το συσχέτισε με άλλες μορφές εγκλήματος.

Ο *κοινωνιολογικός προσανατολισμός* στην κακοχρησία της πληροφορικής τεχνολογίας και το πληροφορικό έγκλημα ακολούθησε από τις αρχές της δεκαετίας του 1990. Με αφετηρία τον νομικό προσανατολισμό ο κοινωνιολογικός προσανατολισμός εισήγαγε στην agenda της ενασχόλησης με το πληροφορικό έγκλημα πολλά και σημαντικά ζητήματα. Άσκησε κριτική

[29] Βλ., M.R. Volgyes, "The investigation, prosecution and prevention of computer crime: A State-of-the-art review», *Computer and Law Journal*, 1980.2.σ.385

στον προκρούστειο χαρακτήρα των έργων πρώτης και δεύτερης γενιάς του νομικού προσανατολισμού, εντόπισε υπερβολές και σιωπές, έδειξε μεγάλα κοινωνικό-οικονομικά συμφέροντα, άσκησε κριτική στις μεθόδους δίωξης και, γενικότερα, κατέστησε συνθετότερη και πλουσιότερη τη σκέψη πάνω στο πληροφορικό έγκλημα.[30]

Μια μερίδα επιστημόνων που ασχολούνται με το πληροφορικό έγκλημα αποφεύγουν να αποκλίνουν από τους ήδη υπάρχοντες ορισμούς και τις καθιερωμένες κατηγοριοποιήσεις, και διστάζουν να προχωρήσουν σε ριζικές τροποποιήσεις των θεωρητικών εργαλείων τους. Πολλοί βλέπουν πως το πληροφορικό έγκλημα παραμένει ουσιαστικά το ίδιο, και πως μόνες αλλαγές αφορούν στις διακυμάνσεις των μεγεθών, είτε των συνολικών είτε ανά κατηγορία. Άλλοι εκτιμούν πως η αναθεώρηση των αφετηριακών ορισμών και κατηγοριών είναι μεν αναπόφευκτη αλλά πρώιμη. Τέλος μια τρίτη μερίδα επιστημόνων τείνει προς την εκτίμηση ότι οι αλλαγές στο πληροφορικό έγκλημα είναι τόσο καταιγιστικές ώστε κάθε ορισμός και γενίκευση δεσμεύουν τη σκέψη.

2.6. Ορισμός και κατηγοριοποίηση του πληροφορικού εγκλήματος: Μια πρώτη προσπάθεια.

Η περίοδος ανάμεσα στα μέσα της δεκαετίας του 1970 και τα τέλη της δεκαετίας του 1980, αποτελεί μια περίοδο ορισμού και κατηγοριοποίησης του πληροφορικού εγκλήματος. Σε αυτά τα δεκαπέντε χρόνια σύμφωνα με τον Εγκληματολόγο Γρ. Λάζο, το πληροφορικό έγκλημα εντοπίσθηκε, δείχθηκε από επιστήμονες όπως ο Donn Parker, ο Aygust Bequai και ο Jay BloomBecker.

Η πρώτη γενιά των κοινωνικών επιστημόνων που εστίασαν στο πληροφορικό έγκλημα ανέλαβαν τρία καθήκοντα ή σε μια άλλη διατύπωση, είχαν να απαντήσουν σε τρεις προκλήσεις: Αρχικά να πείσουν ότι το πληροφοριακό έγκλημα υπάρχει. Κατά δεύτερο λόγο, οι υποστηρικτές της

[30] Βλ., όπ. υπ.16,σσ. 28.29

ύπαρξης και μεγάλης σημασίας του πληροφορικού εγκλήματος έπρεπε να αναπτύξουν ένα φάσμα ορισμών και κατηγοριών που να ανταποκρίνεται με επάρκεια σε ένα τόσο ρευστό και μεταλλασσόμενο αντικείμενο και κατά τρίτο λόγο, η πρώτη αυτή γενιά εκτιμούσε ότι έπρεπε να συμβάλλει στην προώθηση κυρίως δικαιϊκών αλλά και μη - δικαιϊκών απαντήσεων στο πληροφορικό έγκλημα[31].

Πρέπει εισαγωγικά να σημειωθεί ότι το «Πληροφορικό Έγκλημα» προηγείται χρονικά και λογικά της κατηγορίας των κυβερνοεγκλημάτων. Κατά τον V. Zur Muhlen εγκληματικότητα δια μέσου των υπολογιστών «αποτελεί κάθε εγκληματική συμπεριφορά στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης».

Στην προσπάθεια αυτή έρχεται η πρώτη ολοκληρωμένη μελέτη που συνειδητά και σκόπιμα αναφερόταν στο πληροφορικό έγκλημα δημοσιεύτηκε το 1976 από τον Parker, *Crime by Computer* και η οποία έφερε το πληροφορικό έγκλημα σε μια από τις πρώτες θέσεις εγκληματολογικού, κοινωνιολογικού και νομικού ενδιαφέροντος.[32] Σύμφωνα λοιπόν με τον Parker το πληροφοριακό έγκλημα ορίζεται ως η πληροφορική προσβολή. Έτσι «ως πληροφορική προσβολή ορίζεται γενικά κάθε επεισόδιο που σχετίζεται με την πληροφορική τεχνολογία, στο οποίο το θύμα υπέστη ή θα μπορούσε να υποστεί ζημιά και ο δράστης σκόπιμα πραγματοποίησε ή θα μπορούσε να πραγματοποιήσει κέρδος. Κάθε επεισόδιο ορίζεται ως πληροφοριακή προσβολή εάν, μελετώντας ανάλογα επεισόδια, υπάρχουν πληροφορίες που μπορούν να αποκτηθούν οι οποίες θα καθιστούσαν τους υπολογιστές ασφαλέστερους στο μέλλον.»

Στην ίδια κατεύθυνση με τον Parker κινήθηκαν και οι απόψεις άλλων νομικών και κοινωνικών επιστημόνων. Για παράδειγμα ο Ingraham εκτιμά ότι εφ' όσον το πληροφορικό έγκλημα περιορίζεται στις συγκεκριμένες μορφές δράσης, οι δράσεις αυτές είτε δεν συνιστούν εγκλήματα είτε δεν

[31] Βλ., όπ., υπ..16, σελ.35
[32] Βλ., D.B.Parker, *Crime by Computer*. New York: Charles Scribner's Sons, 1976

αποτελούν κάτι το εξαιρετικό που να υποχρεώνει στο σχηματισμό ενός νέου νομοθετικού πλαισίου αντιμετώπισης του.[33]

Από την άλλη πλευρά ο Kling διατυπώνει την προειδοποίηση πως η εμμονή στον ορισμό μιας δράσης ως πληροφορικής εγκληματικής με βάση το γεγονός ότι ένας Η/Υ έχει φυσική συμμετοχή στη δράση ως μέσο ή ως αντικείμενο προσβολής, θα έχει ως αποτέλεσμα την κοινοτυποποίηση και μετάπτωση του πληροφορικού εγκλήματος σε μορφές που, έστω και με σημαντικούς περιορισμούς θα είναι δυνατό να αντιμετωπισθούν στο πλαίσιο του ήδη υπάρχοντος δικαίου.[34]

Τον Parker ακολούθησαν και άλλοι επιστήμονες προς αυτή την κατεύθυνση αλλά με διαφορετικές προτεραιότητες και εστιάσεις. Ένας σημαντικός πρωτοπόρος στο χώρο του πληροφορικού εγκλήματος είναι ο συγγραφέας και δικηγόρος August Bequai καταξιωμένος στα εγκλήματα λευκού περιλαιμίου. Ο Bequai από την μεριά του όρισε ως πληροφορικό έγκλημα «τη χρήση υπολογιστή για τη διάπραξη ενεργειών απάτης, απόκρυψης και πανουργίας που έχουν ως σκοπό την απόκτηση ιδιοκτησίας, χρήματος, υπηρεσιών και πολιτικού και επιχειρηματικού πλεονεκτήματος.»[35]

Σημαντική υπήρξε και η συνεισφορά του Jay BloomBacker σε αυτά τα πρώτα βήματα εντοπισμού και αποσαφήνισης του πληροφορικού εγκλήματος. Ως διευθυντής του National Center for Computer Crime Data, ο BloomBacker εντόπισε οκτώ τύπους κινήτρων - σκοπών που οδηγούν στη διάπραξη πληροφορικών εγκλημάτων: (1) κλοπή χρημάτων, (2) κλοπή πληροφοριών, (3) φθορά στο λογισμικό, (4) δόλια αλλοίωση δεδομένων ή προγραμμάτων, (5) αλλοίωση δεδομένων ή προγραμμάτων με σκοπό την εξαπάτηση, (6) κλοπή υπηρεσιών, (7) παρενόχληση και, (8) εκβίαση.[36]

---

[33] Βλ., D.G. Ingraham, «On charging computer crime», Computer and Law Journal, 1980,2, σ.435
[34] Βλ., R.Kling, «Computer Abuse and Computer Crime as organizational activities», *Computer and Law Journal*, 1980,2,σ.413
[35] Βλ., U.S. Congress, Senate, 1978, σσ.113-20
[36] Βλ., NCCCD, *Computer Crime, Computer Security, Computer Ethics*, Computer Crime Census 1988.

Συνολικά οι θέσεις και η στρατηγική των Donn Parker, Aygust Bequai και δευτερευόντως του Jay BloomBecker στόχευαν σε δύο σημεία: αρχικά, στη θέσπιση νόμων για το πληροφοριακό έγκλημα και, στη συνέχεια, στην ενημέρωση του κοινού σχετικά με τις επιπτώσεις του πληροφοριακού εγκλήματος στη ζωή τους.

Αποτελεί γεγονός πως την τελευταία εικοσαετία εγκληματολόγοι, νομικοί και κοινωνιολόγοι έχουν προσπαθήσει να προτείνουν ορισμούς και κατηγοριοποιήσεις που να καλύπτουν το αντικείμενο με πληρότητα χωρίς όμως να το έχουν πετύχει. Ένας λόγος είναι ότι το πληροφορικό έγκλημα άλλαξε και συνεχίζει να αλλάζει με γρήγορους ρυθμούς.

Όπως παρατηρείται (Ι. Αγγελής) δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στη διεθνή νομοθεσία, ούτε στη διεθνή νομολογία. Οι υπάρχουσες μέχρι τώρα (ελάχιστες) ποινικές αποφάσεις αφορούν εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) και όχι εγκλήματα του κυβερνοχώρου (cyber crimes)[37]. Πάνω σε αυτό το σκεπτικό και ο Barlow προτείνει την επέκταση των αρχών του Συντάγματος στον Κυβερνοχώρο.[38]

Σύμφωνα με την προσέγγιση του Ι.Αγγέλη,[39] τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς με την χρήση του διαδικτύου. Χαρακτηριστικά ο Casey[40] λέει: «Το cybercrime αναφέρεται σε κάθε έγκλημα που περιλαμβάνει υπολογιστές και υπολογιστικά δίκτυα περιλαμβάνοντας εγκλήματα που δεν στηρίζονται έντονα στους υπολογιστές». Αυτός ο γενικός όρος απαιτείται για να καλύψει καταστάσεις όπου ένα υπολογιστικό δίκτυο δεν χρησιμοποιείται για να διαπραχθεί ένα έγκλημα αλλά εξακολουθεί να περιλαμβάνει ψηφιακά δεδομένα σχετιζόμενα με το έγκλημα. Σε περίπτωση

---

[37] Βλ., Αγγέλης Ιωάννης, «Το νομικό πλαίσιο για την ασφάλεια του Κυβερνοχώρου κατά το Ελληνικό ποινικό δίκαιο», ΠοινΔικ 12/2001

[38] Στο ειδικό ζήτημα της επέκτασης του Συντάγματος του Κυβερνοχώρου βλ. και στο Κ. Αργυρόπουλος, «Το Σύνταγμα στον Κυβερνοχώρο: Η Αμερικανική Προσέγγιση». *Εφαρμογές Δημοσίου Δικαίου*, 1997, Ι, σσ. 80-93

[39] Βλ., όπ.π.

[40] Βλ., Casey E., «Digital Evidence and Computer Crime:Forensic science, Computers and the Internet», Second Edition, Academic Press, 2004

που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

Σε σχέση με τα εγκλήματα, στα οποία «εμπλέκεται» ο υπολογιστής και το δίκτυο προτείνεται από τον Carter[41] και η ακόλουθη ταξινόμηση:

1. Ο υπολογιστής ως στόχος. Εδώ κατατάσσονται τα εγκλήματα που αφορούν τη δολιοφθορά των συγκροτημάτων ηλεκτρονικών υπολογιστών ή των δικτύων υπολογιστών, τη δολιοφθορά των λειτουργικών συστημάτων και των προγραμμάτων, την κλοπή των στοιχείων πληροφοριών, τα εγκλήματα που σχετίζονται με την πνευματική ιδιοκτησία, όπως το λογισμικό υπολογιστών, τεχνο-βανδαλισμός και τεχνο-παραβίαση.

2. Ο υπολογιστής ως συμβολή του εγκλήματος. Για παράδειγμα η διαδικτυακή άπατη, απάτες πιστωτικών καρτών, απάτες που περιλαμβάνουν τις ηλεκτρονικές μεταφορές χρημάτων, απάτες τηλεπικοινωνιών και απάτες σχετικά με το ηλεκτρονικό εμπόριο και την ηλεκτρονική ανταλλαγή δεδομένων.

3. Ο υπολογιστής ως «συνεργός/πλατφόρμα» σε άλλα εγκλήματα. Για παράδειγμα διάδοση ναρκωτικών, ξέπλυμα χρήματος[42] και παράνομες τραπεζικές συναλλαγές, παιδική πορνογραφία, τζόγος Διαδικτύου κλπ. Για παράδειγμα για τα εγκλήματα του «λευκού περιλαιμίου»[43], ο Kovacich υποστηρίζει πως για να διαπραχθεί ένα τέτοιο έγκλημα πρέπει να συνυπάρχουν τρεις προυποθέσεις: Το κίνητρο (motive), η εκλογικευση της πράξης (rationalization), και η κατάλληλη ευκαιρία (opportunity).[44]

---

[41] Βλ., Carter R.A., «Computer Crime», 1983

[42] Ο όρος «ξέπλυμα» χρήματος χρησιμοποιείται για να περιγράψει τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων (βρόμικο χρήμα) υπόκεινται σε μια σειρά διαδικασιών οι οποίες καλύπτουν τις παράνομες ρίζες τους και τα κάνουν να εμφανίζονται σαν να προέρχονται από νόμιμες πηγές (καθαρό χρήμα). Βλ., στο Grabrosky, PN, και Smith, R.G., *Crime in the Digital Age*, Annandale: Transaction, 1998, σ.175

[43] Ο πρώτος που όρισε και μελέτησε τα εγκλήματα του λευκού περιλαιμίου ήταν ο Edwin Sutherland (E.H. Sutherland, «Is "White collar Cime" Crime?», 10, *American Sociological Review*, 132, 1945, και White Collar Crime, New York: Holt, Rinehart & Winston, 1949), στα μέσα της τέταρτης δεκαετίας του εικοστού αιώνα. Υποστήριξε πως υπάρχουν δυο βασικές κατηγορίες εγκλημάτων λευκού περιλαιμίου: Αυτά που αφορούν στη διαχείριση των περιουσιακών στοιχείων μιας επιχείρησης, και αυτά που έχουν να κάνουν με διαχείριση της ισχύος που παρέχει η συμμετοχή σε μια επιχείρηση.

[44] Βλ., Gerald Kovacich, «Introduction to computer fraud – Part 1», στο *Computer and Security*, July 1999, σσ. 14-15.

4. Εγκλήματα σχετικά με την εξάπλωση των υπολογιστών όπως για παράδειγμα, πειρατεία λογισμικού/ πλαστογράφηση, παραβίαση πνευματικών δικαιωμάτων των προγραμμάτων υπολογιστών, πλαστός εξοπλισμός, μαύρος εξοπλισμός υπολογιστών αγοράς και προγράμματα.

Ανεξάρτητα από τις διάφορες κατηγοριοποιήσεις και τυπολογίες εγκλήματα είναι εκείνα τα οποία ο νομοθέτης προσδιορίζει ως τέτοια, ορίζοντας μάλιστα την λεγόμενη «αντικειμενική υπόσταση» τους καθώς και τις προβλεπόμενες στο νόμο ποινές.

2.7. Ριζοσπαστικές και φιλελεύθερες απόψεις για το ηλεκτρονικό έγκλημα από τους R. J. Michalowski και E. H. Pfuhl, Dorothy E. Denning, John P. Barlow

Οι Michalowski και Pfuhl εκτιμούν ότι, μέχρι την εμφάνιση των πρώτων νόμων για το πληροφορικό έγκλημα, η απουσία σαφών νομικών ελέγχων πάνω στην ηλεκτρονική πληροφορία είχε αρχίσει να προκαλεί μιαν αποσταθεροποίηση των σχέσεων εξουσίας.

Στον καπιταλισμό, το ποιος παράγει ή δημιουργεί ένα νέο αγαθό ή μία νέα αξία έχει δευτερεύουσα σημασία. Πρωτεύουσα σημασία έχει το ποιος είναι ο ιδιοκτήτης τους, ποιος έχει το αγαθό αυτό ή την αξία κάτω από τον έλεγχό του, και είναι σε θέση να καθορίσει τους όρους -κυρίως το αν, το πότε και το αντίτιμο- της παροχής του στους άλλους. Η αμφισβήτηση ή η απώλεια του ελέγχου πάνω στην ηλεκτρονική πληροφορία αποτελεί πρόκληση στην κατεστημένη σύνθεση γνώσης και δύναμης.

Είναι για αυτούς τους λόγους που, αν και ο κύριος όγκος των πληροφορικών εγκλημάτων δεν είχε κάποια σχέση με τους hackers και το hacking, είναι ακριβώς το hacking που αναβαθμίστηκε σε έμβλημα του πληροφορικού εγκλήματος. Οι νομοθεσίες που αναπτύχθηκαν δεν απαντούσαν στο πληροφορικό έγκλημα με βάση τα πραγματικά δεδομένα που οι σχεδιαστές τους διέθεταν, αλλά με βάση τους κινδύνους που αντιπροσώπευε για τις σχέσεις ιδιοκτησίας και εξουσίας. Το να κλέψει

κάποιος τον εργοδότη του με τη χρήση της πληροφορικής τεχνολογίας λίγο-πολύ μπορεί να αντιμετωπιστεί με την ήδη υπάρχουσα νομοθεσία. Το να έχει κάποιος τη δυνατότητα πρόσβασης στα αρχεία μιας επιχείρησης ή του κράτους δημιουργεί όμως νέες δυναμικές και κινδύνους που βρίσκονται πολύ κοντά στον πυρήνα του καπιταλισμού και της ιεραρχίας. Το ουσιαστικό πρόβλημα δεν είναι η έναρξη του τρίτου παγκόσμιου πολέμου από κάποιον ανώριμο hacker ή η καταστροφή κάποιου αρχείου από κάποιο βάνδαλο hacker. Εάν δεν ρυθμιστούν με επάρκεια και σαφήνεια οι κανόνες της ιδιοκτησίας και της ιεραρχημένης εξουσίας, το ουσιαστικό πρόβλημα είναι ότι οι πολίτες θα έχουν τη δυνατότητα να δουν την εξουσία γυμνή όταν σχεδιάζει προγράμματα στρατιωτικών εξοπλισμών ή εκπαιδευτικά προγράμματα, ή ότι οι εργαζόμενοι θα είναι σε θέση να απομυθοποιήσουν το management των επιχειρήσεων και να γνωρίσουν τους τρόπους λήψης αποφάσεων. Ίσως τότε οι πολίτες-εργαζόμενοι συνειδητοποιήσουν ότι οι πολιτικές και οικονομικές εξουσίες στις οποίες υπακούουν δεν έχουν κάποιον ουσιαστικό λόγο ύπαρξης ή, έστω, ότι δεν προσφέρουν στην κοινωνία τα ανάλογα των προνομίων και των ηδονών που απολαμβάνουν. Η παρέμβαση του νομοθέτη ώστε να ποινικοποιηθεί η ελεύθερη πρόσβαση (στην πληροφορία και τη γνώση) και να μετατραπεί σε με ή χωρίς εξουσιοδότηση πρόσβαση είναι αναγκαία για τη διατήρηση της ιδιοκτησίας και της ιεραρχίας.

Όπως το διατύπωσε ο Edwards[45], η σύγχρονη κοινωνία τείνει να φθάσει στο σημείο όπου «τα πάντα θα εξαρτώνται από το λογισμικό». Για παράδειγμα, ο κύριος όγκος των πληροφοριών κάθε είδους που διακινούνται καθημερινά σε πλανητική κλίμακα, μεταβιβάζεται μέσω συστημάτων πληροφορικής και αντίστροφα. Επίσης, ο Hughes[46] διατυπώνει τη θέση ότι η τεχνολογία προωθείται σε ένα ευρύ κοινωνικό μέτωπο. Η εφεύρεση μιας καινοτομίας δε συμπίπτει αναγκαστικά με την πρακτική αποδοχή τους. Η εφεύρεση ενός νέου τρόπου οργάνωσης ή διαχείρισης ανθρώπων, πραγμάτων

[45] Βλ., Edwards. O., «Hackers from hell», *Formes*, 1995. 9, σ.182
[46] Βλ., Thomas P. Hughes, *Networks of Power: Electrification in Western Society*, 1880-1930. Baltimore: John Hopkins University Press, 1983.

και συμβόλων δεν συνιστά κάτι παραπάνω από μια πρόταση που απευθύνεται στην κοινωνία.47

Σύμφωνα με τους Michalowski και Pfuhl, η εμφάνιση νέων τεχνολογιών προκαλεί τη δημιουργία νέων νόμων48. Για παράδειγμα, η ανάπτυξη της τυπογραφίας οδήγησε τους νόμους για το αποκλειστικό δικαίωμα του δημιουργού πάνω στα προϊόντα του. Ο ατμοκίνητος σιδηρόδρομος και η βιομηχανία συνέβαλαν στη δημιουργία ενός εκτεταμένου σώματος νομοθετικών ρυθμίσεων σε εθνικές κλίμακες αλλά και διεθνώς, που συνέχισε να αναπτύσσεται μέχρι σήμερα. Ο Bigelow, σε ένα άρθρο όπου εξετάζει τους νόμους για τους υπολογιστές αναφέρει ότι «κάθε νέα τεχνολογική εξέλιξη δημιουργεί νέα νομικά προβλήματα και απαιτεί την επανεκτίμηση των παλαιών εννοιών»49. Κατά την εκτίμηση των Michalowski και Pfuhl, τα νομικά προβλήματα που δημιουργούν οι νέες τεχνολογίες εμφανίζονται επειδή απειλούν με διάσπαση τα επικρατούντα πρότυπα κοινωνικών σχέσεων. Ο πυρήνας της επιχειρηματολογίας των δύο εγκληματολόγων βρίσκεται ακριβώς σ' αυτό: κάθε νέα τεχνολογία δημιουργεί αμφιβολίες σ' ότι αφορά στα δικαιώματα και τις υποχρεώσεις τόσο αυτών που αξιώνουν τον ορισμό της ως ιδιοκτησίας τους όσο και αυτών που επηρεάζονται από την κοινωνική προώθηση και την εφαρμογή της.

Στο νέο πλαίσιο που δημιουργήθηκε από την πληροφορική τεχνολογία εμφανίστηκε μια νέα μορφή απειλής για την κοινωνία - ο πληροφορικός εγκληματίας. Ο νέος αυτός τύπος εγκληματία έχει τη δυνατότητα καταστροφής της ηλεκτρονικής υποδομής, παραβίασης της ιδιωτικότητας, και άσκησης βιομηχανικής κατασκοπίας. Από οικονομικής πλευράς, το οικονομικό κόστος που προκαλείται από ενέργειες των hackers είναι

---

[47] Κατά τον Wallerstein, μια καινοτομία ή νέα τεχνολογία – κοινωνική, οικονομική, ηθική ή ότι άλλο – θα γίνει αποδεκτή και θα αφομοιωθεί από την ιστορική κοινωνία μόνον εάν και εφόσον πληρεί επαρκώς δύο κριτήρια: Ένα συμβάλλει στη βελτίωση της απόδοσης – κυρίως της οικονομικής απόδοσης ή της απόδοσης κατανοούμενης σε οικονομικούς όρους, και εάν συμβάλλει στη βελτίωση της πολιτικής ασφάλειας, κάτι που δεν συμβαίνει σήμερα, ιδιαίτερα μετά το πλήγμα που δέχθηκε η Ελληνική κυβέρνηση στο θέμα των υποκλοπών κινητών και αρχείων του Πρωθυπουργού και ανωτάτων στελεχών της κυβέρνησης και της αντιπολίτευσης της Ελλάδος. Wallerstein, Imamanuel, *Historical Capitalism*, London: Verso, *1983, σ. 82*

[48] Βλ., R. J. Michalowski, και E. H. Pfuhl, «Technology, property and law: The case of computer crime», *Crime Law and Social Change*, 1991, 15, σ. 265.

[49] Βλ., R. P. Bigelow, «The challenges of computer law», *Western New England Law Review*, 1985, 7 (3), σ. 397.

περιορισμένο σε σύγκριση με το ανάλογο κόστος του πληροφορικού εγκλήματος από μέρους των «insiders»-υπαλλήλων και πρώην υπαλλήλων μιας επιχείρησης. Συγχρόνως, το πληροφορικό έγκλημα αποτελεί ένα δυναμικό και αναπτυσσόμενο φαινόμενο. Με αυτή τη γενική αφετηρία και στηριγμένη σε πραγματικά περιστατικά, η Dorothy E. Denning διατυπώνει μια σειρά επιφυλάξεων και φόβων για τον τρόπο δράσης των μυστικών υπηρεσιών, της ομοσπονδιακής αστυνομίας, αλλά και των εισαγγελικών αρχών στην κατεύθυνση της επίθεσης κατά των hackers κατάσχεση ηλεκτρονικών συστημάτων από επιχειρήσεις, κατάσχεση bulletin boards (που αποτελούν ηλεκτρονικούς χώρους συγκέντρωσης πολιτών και γενικότερα ατόμων με κοινά ενδιαφέροντα), υπερβολική άσκηση βίας, προσαγωγή σε δίκη με ανεπαρκή στοιχεία ως μέσο τιμωρίας και παραδειγματισμού κ.ά.. Η Denning προχώρησε στην εκτίμηση ότι οι hackers δεν είναι εύλογο να αντιμετωπίζονται αποκλειστικά με ποινικά-κατασταλτικά μέσα, συστήνει δε μια πιο ήπια ποινική αντιμετώπιση. Ειδικά σε ότι αφορά τις χωρίς εξουσιοδότηση προσβάσεις σε Η/Υ, εκτιμά ότι πρέπει να αντιμετωπίζονται κυρίως στο επίπεδο του πταίσματος. Η αυστηρότερη αντιμετώπιση που χαρακτηρίζει τις περισσότερες σύγχρονες νομοθεσίες εγκυμονεί τον κίνδυνο μετατροπής σε πληροφορικούς εγκληματίες νεαρών ατόμων που «έπαιξαν» ή «πειραματίστηκαν» για ένα διάστημα με παράνομες ενέργειες, και τις οποίες σύντομα θα ξεπερνούσαν ανώδυνα όταν θα συνειδητοποιούσαν τις ευρύτερες συνέπειες των ενεργειών τους. Κατά τη γνώμη της, η κουλτούρα των hackers πρέπει να προσεγγιστεί και να κατανοηθεί, όπως πρέπει να κατανοηθεί και η ποικιλία των κινήτρων που συμβάλλουν στην ανάπτυξη του hacking [50].

Το «Crime and Puzzlement» του John P. Barlow απευθύνεται σε δύο διαφορετικά κοινά. Σε πρώτο πρόσωπο και τόνους οικειότητας, απευθύνεται σε όσους δραστηριοποιούνται στον κυβερνοχώρο ως πλαίσιο κοινωνικής δράσης και προβληματισμού, στους «ιθαγενείς» του κυβερνοχώρου. Μια μεγάλη υποκατηγορία τους -ίσως η μεγαλύτερη- δεν έχει διαπράξει κάποια

[50] Βλ., D. Denning. «The United States vs Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking», Communications of the ACM, 1991, 34, σσ. 24-33.

παράβαση. Όχι τόσο γιατί αποτελείται από άτομα ενήμερα των νομοθετικών εξελίξεων και νομοταγή, όσο γιατί ο ειδικός τύπος δράσης τους δεν έχει ακόμα απασχολήσει το νόμο. Μία άλλη υποκατηγορία τους περιλαμβάνουν στο συνολικό τρόπο δράσης τους ενέργειες ή σκοπούς που με την εμφάνιση των πρώτων νόμων άρχισαν να αντιμετωπίζονται ποινικά ή να αποτελούν αντικείμενο συζητήσεων για το αν θα πρέπει να ποινικοποιηθούν. Τέλος, υπάρχει και μια τρίτη υποκατηγορία, μια ισχυρή μειονότητα, οι cyberpunks ή techno-hippies. Μέρος των δραστηριοτήτων τους είναι hack-ιστικές (καινοτομιστικές), ένα μικρότερο μέρος είναι επιθετικές hack-ιστικές (cracking), και, τέλος, ένα ελάχιστο μέρος τους είναι κοινωνικά επιβλαβείς. Όλοι αυτοί, των οποίων η δράση στον κυβερνοχώρο αποτελεί συστατικό στοιχείο του τρόπου ζωής και του ορισμού τους ως προσωπικοτήτων, ονομάζονται συλλήβδην hackers, εξισώνονται με τους επιθετικούς hackers και η συμπεριφορά τους ορίζεται διά νόμου ως εγκληματική. Η μεγάλη πλειονότητα των hackers με την ευρεία έννοια αρνείται να συμμορφωθεί στους όρους και τύπους δράσης που ορίζονται ως νόμιμοι. Οι άλλες δύο υποκατηγορίες προβληματίζονται για τις πιθανές μελλοντικές εξελίξεις. Συνολικά, στη μεγάλη τους πλειονότητα, οι «ιθαγενείς του κυβερνοχώρου» βλέπουν την εμφάνιση των πρώτων νόμων -των συγκεκριμένων πρώτων νόμων- σαν γνήσια αυθαιρεσία και επιβολή. Έχουν την αντίληψη ότι σε ολοένα και αυξανόμενους ρυθμούς οι μεγάλες επιχειρήσεις της πληροφορικής δηλώνουν αυθαίρετα σαν ιδιοκτησία τους ένα τμήμα του κυβερνοχώρου. Απαγορεύουν τη χρήση ή τη διέλευση ή απαιτούν από τους πολίτες να καταβάλουν τίμημα για κάτι που λίγο πριν ήταν ελεύθερο και αβίαστα κοινωνικό. Με την άρνηση των πολιτών, που ενδημούν και στον κυβερνοχώρο, να συμμορφωθούν, ύστερα από μια ηθικο-ιδεολογική επεξεργασία της κοινής γνώμης μέσω των ΜΜΕ, ο νομοθετικός και ο διωκτικός μηχανισμός του κράτους έρχονται να ορίσουν και να επιβάλουν τα συμφέροντα των επιχειρήσεων και της εξουσίας σαν συμφέροντα της κοινωνίας.

Οι προτάσεις του Barlow προς όσους πιστεύουν πως η αξιοποίηση του κυβερνοχώρου αποτελεί συστατικό της καθημερινότητάς τους είναι δύο. Η πρώτη περιλαμβάνει την προτροπή για σεβασμό και τήρηση των άτυπων συμβάσεων επικοινωνίας και κοινωνικότητας που έχουν αναπτυχθεί σταδιακά, καθώς και την προτροπή για αποφυγή των άμετρων αντιδράσεων. Η δεύτερη πρόταση του Barlow έχει ως πρόλογό της μία δήλωση και μία προειδοποίηση. Αφού δηλώνει την κοινότητα των συμφερόντων του με τους αδελφούς του στον κυβερνοχώρο («my silicon brothers»), προειδοποιεί ότι «αν έρθουμε σαν μάγισσες, θα μας κάψουν». Και αντιπροτείνει: «Αν εθελοντικά τους οδηγήσουμε με ηπιότητα σ' αυτούς τους νέους τόπους, ο Εικονικός Κόσμος θα μπορούσε να γίνει ένας πιο φιλικός χώρος για όλους μας από αυτόν που ήταν κάποτε»[51].

2.8. Τι περιλαμβάνει τελικά ο ορισμός του Πληροφορικού Εγκλήματος;

Μετά από τις θεμελιώδεις απόψεις για το ηλεκτρονικό έγκλημα και την ανακάλυψη του από τους Donn Parker, Aygust Bequai ,Jay BloomBecker, Kling, Parker, R. J. Michalowski, E. H. Pfuhl, Dorothy E. Denning και John P. Barlow αποδείχθηκε τελικά πως η ανακάλυψη του νέου αυτού κοινωνικού φαινόμενου ήταν σχετικά απλή μπροστά στο πρόβλημα που δημιουργήθηκε σχετικά με την εξεύρεση ενός κοινά αποδεκτού ορισμού και ταυτόχρονη κατηγοριοποίηση του.

Όπως αναφέρει ο Christofer Chen, η απουσία ενός κοινά αποδεκτού ορισμού του πληροφορικού εγκλήματος οδηγεί σε τρία σημαντικά επιμέρους προβλήματα:[52]

- «Πρώτο, αν δεν ξέρουμε τι είναι πληροφορικό έγκλημα, πως μπορούμε να πούμε πότε έλαβε χώρα;

[51] Βλ., Barlow, 1990, σ. 22
[52] Βλ., C. Chen, «Computer Crime and the Computer Fraud and Abuse Act of 1986», *Computer and Law Journal*, 10, σσ. 71-86.

- Δεύτερο, πώς μπορούμε να αναπτύξουμε αποτελεσματικές και συνεκτικές λύσεις στο πρόβλημα του πληροφορικού εγκλήματος αν το πληροφορικό έγκλημα παραμένει αόριστο;, και
- Τρίτο, με δοσμένη την απουσία συμφωνίας σ' ότι αφορά στο τι είναι πληροφορικό έγκλημα, οι μελέτες στο αντικείμενο θα συνεχίσουν να παράγουν μη - συνεκτικά αποτελέσματα και συμπεράσματα.»

Η σπουδαιότητα του τρόπου ορισμού σύμφωνα με τον Καθηγητή Γρ. Λάζο καθορίζει το αντικείμενο της έρευνας και της μελέτης, το τι και πως θα ερευνηθεί και θα μελετηθεί. Επίσης τονίζει πως ο τρόπος ορισμού καθορίζει τα όρια του πληροφορικού εγκλήματος, την εσωτερική του διάρθρωση και τέλος τη σχέση του με τις άλλες μορφές εγκλήματος.

Από μια άλλη επιστημονική σκοπιά ο Douglas Reimer τονίζει πως «τα πληροφοριακά εγκλήματα δεν είναι νέα εγκλήματα, είναι τα ίδια παλιά εγκλήματα που διαπράττονται με νέους και εφευρετικούς τρόπους που η υψηλή τεχνολογία των σύγχρονων υπολογιστών και τηλεπικοινωνιών καθιστά δυνατούς.»[53]

Ένα άλλο εμπόδιο στην ανάπτυξη ενός κοινά αποδεκτού ορισμού αφορά στην έμφαση που αποδίδεται σε ειδικές εκδοχές του πληροφορικού εγκλήματος. Έτσι, μια μερίδα επιστημόνων προσεγγίζει το πληροφορικό έγκλημα ως είδος οικονομικού ή επαγγελματικού εγκλήματος ή εγκλήματος του «λευκού περιλαιμίου»[54], ακολουθώντας την τυπολογία των Clinard και Quinney[55] οι οποίοι δίνουν έμφαση στο οικονομικό πληροφορικό έγκλημα.

---

[53] Βλ., Douglas M. Reimer, «Judicial and Legislative Responses to Computer Crimes», *Insurance Counsel Journal*, 1986, 53, σ.406

[54] Ο Σάδερλαντ ήταν ιδιαίτερα επιφυλακτικός απέναντι στις θεωρίες που συνέδεαν την φτώχεια με το έγκλημα, πιστεύοντας ότι τα στατιστικά της αστυνομίας στα οποία παρουσιάζονταν τα περισσότερα εγκλήματα να διαπράττονται σε φτωχογειτονιές ήταν εσφαλμένα. Για να τεκμηριώσει αυτή του την άποψη, ξεκίνησε το 1928 μία έρευνα για τις παραβιάσεις του νόμου από τις εβδομήντα μεγαλύτερες επιχειρήσεις των Ηνωμένων Πολιτειών. Μετά από 20 χρόνια κοπιαστικής δουλειάς ολοκληρώνει το βιβλίο του με τίτλο «Το Έγκλημα του Λευκού Περιλαίμιου» το οποίο αρχικά κυκλοφόρησε χωρίς να αναφέρονται τα ονόματα των επιχειρήσεων που είχαν μεν κατηγορηθεί για κάποια παραβίαση αλλά δεν είχαν καταδικαστεί, από φόβο μην ακολουθήσουν μηνύσεις. Το βιβλίο κυκλοφόρησε στην πλήρη του μορφή το 1983.

Μια άλλη μερίδα επιστημόνων όπως υποστηρίζει ο Γρ. Λάζος προσεγγίζει το πληροφορικό έγκλημα από τη σκοπιά του τρόπου διάπραξης. Ορισμένοι εκτιμούν ότι κατ' αρχήν το πληροφορικό έγκλημα αφορά σε μη εξουσιοδοτημένη πρόσβαση σε ή χρήση υπολογιστή, ενώ άλλοι περιορίζονται στην αναγωγή του πληροφορικού εγκλήματος στο hacking[56] ή επικεντρώνουν τα ενδιαφέροντα του στο hacking.

Σε μια μελέτη της British Law Commission το 1988 διαπιστώνεται πως οι διάφορες εθνικές νομοθεσίες έχουν υιοθετήσει τρεις διαφορετικές

Στα πλαίσια της έρευνάς του μελέτησε τέσσερεις τύπους εγκλημάτων που διαπράττονται από μεγάλες επιχειρήσεις: ψευδής διαφήμιση, καταχρηστικοί όροι συμβάσεων, άδικες εργοδοτικές πρακτικές και παραβιάσεις πνευματικής ιδιοκτησίας, κατατεθέντων σημάτων και πατέντων. Ανακάλυψε 980 παραβιάσεις των σχετικών με τις παραπάνω κατηγορίες νόμων (με αναλογία 14 παραβιάσεις περίπου ανά επιχείρηση). Ο Σάδερλαντ στηρίχθηκε στη θεωρία της συναναστροφής για την ερμηνεία αυτών των παραβιάσεων, θεωρώντας ότι τα νεαρά διευθυντικά στελέχη εξοικειώνονται με την παραβατική συμπεριφορά μιας και η τελευταία αποτελεί αναπόσπαστο κομμάτι της καθημερινής επιχειρηματικής πρακτικής. Κατέληξε στο συμπέρασμα ότι η κοινωνία απειλείται περισσότερο από τα εγκλήματα του λευκού περιλαίμιου παρά από την εγκληματικότητα των δρόμων, γιατί τα πρώτα προωθούν την κυνικότητα και την αμφισβήτηση βασικών κοινωνικών θεσμών της.

Στο βιβλίο ανέλυσε τις παραπάνω κατηγορίες εγκλημάτων που διαπράττονται από τις αμερικάνικες επιχειρήσεις και τα στελέχη τους, αναφέροντας παράλληλα ότι αν και συμβαίνουν, δεν υπάρχουν επίσημα στοιχεία για αυτή την κατηγορία παραβατικής συμπεριφοράς ώστε να καταγραφούν και να αναλυθούν στις στατιστικές έρευνες. Για αυτόν το λόγο υποστήριζε ότι τα εγκλήματα του λευκού περιλαίμιου θα έπρεπε να συμπεριλαμβάνονται στα δεδομένα που αναλύουν οι εγκληματολόγοι, όπως συμβαίνει και με τα εγκλήματα που διαπράττουν οι έφηβοι.

Κατά τον Σάδερλαντ, οι συνήθεις γενικεύσεις και ερμηνείες για το έγκλημα και την εγκληματικότητα δεν είναι έγκυρες. Ενδεχομένως αυτό να οφείλεται στις ελλείψεις των αναφορών και των αντίστοιχων δειγμάτων που λαμβάνονται για έλεγχο. Ο αριθμός των εγκλημάτων που γνωστοποιούνται στην αστυνομία είναι αρκετά μικρότερος από τον αριθμό των εγκλημάτων που όντως έχουν διαπραχθεί, ίσως γιατί τα θύματα πιστεύουν ότι η εγκληματική πράξη δεν αξίζει να αναφερθεί. Εκτός αυτού, η ακρίβεια του αριθμού των εγκλημάτων εξαρτάται και από την συστηματικότητα και την ακρίβεια με την οποία οι αστυνόμοι συντάσσουν τις αντίστοιχες αναφορές. Επίσης οι διαφορές του ποινικού κώδικα και κατ' επέκταση η αντίληψη του τί είναι ή δεν είναι έγκλημα από χώρα σε χώρα, είναι πιθανό να επηρεάσει τον αριθμό των αναφορών.

Μία δεύτερη αιτία πιθανής εσφαλμένης ερμηνείας των δεδομένων, αποτελεί το ίδιο το έγκλημα του λευκού περιλαίμιου. Αν και τα εγκλήματα αυτής της κατηγορίας μπορούν να είναι πιο επικίνδυνα για την κοινωνία, με την έννοια ότι επηρεάζουν τους κοινωνικούς θεσμούς και τις ιδιωτικές περιουσίες, τείνουν να μην αναφέρονται σε επίσημα ή ανεπίσημα στατιστικά εξ αιτίας της δυσκολίας εντοπισμού και τιμωρίας τους.

Από την σκοπιά της θεωρίας των εγκλημάτων του λευκού περιλαίμιου, η θεωρία η οποία συνδέει την εγκληματική συμπεριφορά είτε με την φτώχεια είτε με τις ψυχοπαθολογικές και κοινωνιοπαθολογικές συνθήκες που απορρέουν από αυτήν, εμφανίζεται ελλιπής για τρεις λόγους: Πρώτον, η γενίκευση στηρίζεται σε ένα δείγμα που παραλείπει εντελώς την συμπεριφορά των εγκληματιών του λευκού περιλαίμιου. Δεύτερον, η γενίκευση που παρουσιάζει την εγκληματικότητα να συνδέεται στενά με την φτώχεια δεν γίνεται να εφαρμοστεί στην περίπτωση των εγκληματιών του λευκού περιλαίμιου, γιατί, με λίγες εξαιρέσεις, είναι αρκετά εύποροι. Τρίτον οι συνήθεις θεωρίες δεν ερμηνεύουν επαρκώς ακόμα και την υπάρχουσα εγκληματικότητα των κατώτερων τάξεων.

Κατά τον Σάδερλαντ, στον οποίο αποδίδεται και η πατρότητα του όρου, «έγκλημα του λευκού περιλαίμιου» είναι κάθε έγκλημα που διαπράττεται από φαινομενικά ευυπόληπτα άτομα ανώτερης κοινωνικής τάξης κατά τη διάρκεια τέλεσης των καθηκόντων τους. Με αυτό τον τρόπο δίνεται ένας ταξικός ορισμός των εγκλημάτων λευκού περιλαίμιου προσανατολίζοντας το ενδιαφέρον περισσότερο στην προσωπικότητα και τις καταβολές του δράστη παρά στο έγκλημα που έχει διαπράξει.

Τέλος μία από τις κύριες θέσεις του βιβλίου, εκτός από το ότι τα άτομα ανώτερης κοινωνικοοικονομικής τάξης διαπράττουν περισσότερα εγκλήματα και με τρόπο που ακολουθεί τύπους άσκησης διευθυντικών καθηκόντων, είναι ότι σε συνήθεις ποινικές υποθέσεις, η οικονομική κατάσταση των κατηγορουμένων δεν τους εξασφαλίζει την καλύτερη υπεράσπιση, σε αντίθεση με τις μεγάλες εταιρίες που διαθέτουν οικονομική άνεση και δύναμη.

[55] Βλ., Clinard M. B. και Quinney R., Criminal Behavior Systems: A Typology, New York: Holt, Rinehart & Winston, 1967,σ.131

[56] Βλ., Κεφάλαιο 5ο.

προσεγγίσεις στο πληροφορικό έγκλημα. Την εξελικτική προσέγγιση όπως ονομάζεται η οποία εφαρμόζει τον ήδη υπάρχοντα ποινικό νόμο, η δεύτερη προσέγγιση αφορά στη θέσπιση των νόμων που αφορούν ειδικά στα πληροφορικά εγκλήματα και η τρίτη προσέγγιση της Κομισιόν έχει να κάνει με τη θέσπιση των νόμων που εστιάζουν στο πληροφορικό έγκλημα συνολικά ενώ εκτιμά πως αυτή η προσέγγιση είναι εύλογο να αποτελεί την αφετηρία εκκίνησης για την προσέγγιση του πληροφορικού εγκλήματος από το νομοθέτη.[57]

Ο Martin Wasik εντοπίζει δύο βασικές ομάδες αντιτιθέμενων απόψεων στο χώρο του πληροφορικού εγκλήματος. Η πρώτη αντίθεση απόψεων αφορά στο αν υπάρχει ή δεν υπάρχει πληροφορικό έγκλημα. Η δεύτερη αντίθεση απόψεων αφορά στο αν το ποινικό δίκαιο ως έχει, μπορεί - ίσως με κάποιες εννοιακές ερμηνευτικές προεκτάσεις - να ανταποκριθεί στο καθήκον του, δηλαδή να θέσει το πληροφορικό έγκλημα κάτω από τον κοινωνικό έλεγχο.[58] Επιπροσθέτως, ο Wasik τονίζει την ανάγκη για τη δημιουργία ενός ορισμού που θα καλύπτει όχι μόνο το πληροφορικό έγκλημα αλλά, ευρύτερα, την *κακοχρησία υπολογιστή*. Σύμφωνα με τον ποινικολόγο Mandell ως κακοχρησία υπολογιστή ορίζεται «κάθε ανήθικη ή χωρίς εξουσιοδότηση συμπεριφορά σε σχέση με τη χρήση υπολογιστών, προγραμμάτων ή δεδομένων.»[59]

Δεν θα μπορούσαμε σε αυτή τη προσπάθεια εύρεσης ενός αποδεκτού ορισμού για το πληροφορικό έγκλημα να μην αναφερθούμε στην προσπάθεια των Karen Forcht, Darhyne Thomas και Karen Wigginton οι οποίοι προτείνουν μια μη εξαντλητική κατηγοριοποίηση η οποία περιλαμβάνει το hacking, την πειρατεία λογισμικού, τις απάτες τελικού χρήστη, τη βιομηχανική κατασκοπεία, την απειλή για την ακεραιότητα των δεδομένων που αξιοποιούνται στη λήψη αποφάσεων, την τροποποίηση

[57] Βλ., British Law Commission, *Working Paper 110*, σσ. 110-122, Computer Misuse 1, 1988
[58] Βλ., M. Wasik, *Crime and the Computer*, Oxford: Clarendon Press, 1991.σσ.1-4.
[59] Βλ., S. L. Mandell, Computers, *Data Processing and the Law*, St. Paul: West Publishing, 1984, σ. 154

αρχείων, την ανάγνωση αρχείων ή ηλεκτρονικού ταχυδρομείου, τη ζημιά στον υπολογιστή και την κλοπή αρχείων ή προγραμμάτων.[60]

Ο ορισμός του Bequai που είδαμε προηγούμενα σχετικά με τη χρήση του υπολογιστή για τη διάπραξη εξαπάτησης κλπ βρίσκει υποστηρικτή τον Steve Shackelford ο οποίος έρχεται να προτείνει ένα δικό του ορισμό σύμφωνα με τον οποίο «Έγκλημα σχετιζόμενο με τους υπολογιστές αποτελεί κάθε μη-εξουσιοδοτημένη χρήση ενός υπολογιστή, περιλαμβανομένης και της υπέρβασης εξουσιοδότησης ή κάθε ανάλογης προσπάθειας.». Όπως εκτιμά ο Shackelford το σχετιζόμενο έγκλημα με τους υπολογιστές σχηματίζει δύο διακριτές κατηγορίες: «τα εγκλήματα όπου ο υπολογιστής ή τα δεδομένα που περιέχει αποτελούν το στόχο (με ενέργειες όπως) η εισαγωγή ιού ή η αλλοίωση δεδομένων και δεύτερον τα εγκλήματα στα οποία κάποιος χρησιμοποιεί έναν υπολογιστή για να προωθήσει μιαν άλλη εγκληματική πράξη, όπως η κατάχρηση. Η έννοια «ειδικά-πληροφορικό έγκλημα» υποδεικνύει εγκλήματα που δεν θα υπήρχαν αν δεν υπήρχε η πληροφορική τεχνολογία».[61]

Κατά τους Barry Herewitz και Allen Lo[62] το πληροφορικό έγκλημα μπορεί να κατηγοριοποιηθεί με κριτήριο τη θέση του υπολογιστή στη διάπραξη ενός πληροφορικού εγκλήματος. Με βάση αυτό το κριτήριο, προχωρούν στην ακόλουθη διάκριση:

Πρώτο, ο υπολογιστής μπορεί να είναι το «αντικείμενο» ενός εγκλήματος, με την έννοια ότι ο ίδιος ο υπολογιστής αποτελεί το στόχο,

Δεύτερο, ο υπολογιστής μπορεί να είναι το «υποκείμενο» ενός εγκλήματος, εννοώντας ότι ο φυσικός υπολογιστής αποτελεί το σκηνικό (site) τέλεσης μιας εγκληματικής δράσης η οποία αποτελεί πρόσβαση, (προκαλεί)

---

[60] Βλ., K. A. Forcht, D. Thomas και K. Wiggington, «Computer crime: Assesing the lawyer's perspective», Journal of Business Ethics, 1989,8, σ.244

[61] Βλ., Steve Shackelford, «Computer-related crime:an international problem in need of an internatrional solution», *Texas International Law Journal*, 1992,27, σ.483

[62] Βλ., Barry Hurewitz και Allen Lo., «Computer-related crimes», *American Criminal Law Review*, 1993, 30, σσ. 496-497

αλλοίωση, καταστροφή, διαχειρίζεται ή σαμποτάρει ηλεκτρονικά δεδομένα όπως οι «ιοί» και οι «λογικές βόμβες» και

Τρίτο ο ένας υπολογιστής μπορεί να αποτελέσει «εργαλείο» που χρησιμοποιείται ως μέσο για την τέλεση ενός άλλου πιο παραδοσιακού εγκλήματος, όπως η κλοπή, η απάτη, η κατάχρηση ή η παράνομη είσοδος».

Ο ορισμός για το πληροφορικό έγκλημα που τείνει να αποτελέσει την πρώτη ευρεία κοινή βάση επικοινωνίας και προβληματισμού μεταξύ όσων ασχολούνται με το πληροφορικό έγκλημα είναι αυτός που επεξεργάστηκε μια ομάδα επιστημόνων για λογαριασμό του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ)[63]. Σύμφωνα με αυτόν «Πληροφορικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/και τη μετάδοση δεδομένων.» Ο ορισμός του ΟΟΣΑ αποτελεί ίσως το πληρέστερο γενικό πλαίσιο ώστε οι ασχολούμενοι με το πρόβλημα του πληροφορικού εγκλήματος να διαθέτουν ένα ελάχιστο κοινό εννοιακό παρονομαστή.

Σε παράλληλη σχεδόν τροχιά με τον ορισμό του ΟΟΣΑ κινήθηκε και Ulrich Sieber ο οποίος προσεγγίζει το πληροφορικό έγκλημα με διαφορετικό κριτήριο: αντί της σκόπιμης συμπεριφοράς του δράστη ο Sieber έχει ως κριτήριο το προστατευόμενο αγαθό που προσβάλλεται ή απειλείται.[64]

Οι κατηγοριοποιήσεις του ΟΟΣΑ και του Sieber, δεν είναι αλληλοαποκλειόμενες αλλά σαφώς συμπληρωματικές μεταξύ τους. Ο μεν ορισμός του ΟΟΣΑ επιχειρεί να παράσχει μια πρώτη αποσαφήνιση των συμπεριφορών που χαρακτηρίζουν το πληροφορικό έγκλημα, ενώ ο ορισμός του Sieber επιχειρεί να αποσαφηνίσει το αγαθό στο οποίο οι συμπεριφορές αυτές εστιάζουν.

---

[63] Βλ., OECD., *Computer-related crime: Analysis of legal policy. Paris:*OECD, 1986

[64] Βλ., Ulrich Sieber. *The international handbook on computer crime*. New York: John Wiley & Sons, 1986.

Τέλος, σύμφωνα με τον Γρ. Λάζο, στη μελέτη του Crime and the Computer το 1991 ο Martin Wasik προσθέτει νέες οπτικές γωνίες στις κατηγοριοποιήσεις του ΟΟΣΑ και του Sieber, αλλά και αυξημένη συνοχή στην προσπάθεια κατηγοριοποίησης του πληροφορικού εγκλήματος.[65]

Από τη μια πλευρά, ο Wasik εστιάζοντας στη *σκόπιμη συμπεριφορά* διακρίνει μεταξύ,

Α) μη εξουσιοδοτημένης πρόσβασης ή χρήσης υπολογιστή όπως Hacking, wire-tapping και το eavesdropping

Β) απάτης και κλοπής υπηρεσιών όπως η απάτη ή κλοπή και η παράβαση του Copyright και

Γ) συνδεδεμένων παραβάσεων όπως η ζημιά σε υπολογιστές, ο εκβιασμός, διαφθορά κλπ.

Από την άλλη πλευρά, εστιάζοντας στον δράστη, ο Wasik προτείνει και τη διάκριση μεταξύ,

Α) Επιχειρηματικού πληροφορικού εγκλήματος (όταν η δράση πραγματοποιείται από άτομα που κατέχουν διευθυντική θέση στην επιχείρηση)

Β) Υπαλληλικού πληροφορικού εγκλήματος (όταν η δράση αφορά σε υπαλλήλους και στρέφεται κατά της επιχείρησης που τους απασχολεί κατά τη διάρκεια της εργασίας τους) και,

Γ) Κακοχρησίας σε βάρος υπολογιστών από τρίτους μέσω μη - εξουσιοδοτημένης πρόσβασης.

Κλείνοντας αυτό το κεφάλαιο περί Πληροφορικού Εγκλήματος και αυτά που περιέχει θα λέγαμε πως η ταχύτατη αλλαγή στο χώρο της

[65] Βλ., όπ. σημ.16, σ.53

πληροφορικής τεχνολογίας όσο και η αλλαγή στους συσχετισμούς ισχύος στο επίπεδο της κοινωνίας συνηγορούν υπέρ της θέσης του Wasik ότι οι ισχύοντες ορισμοί αποτελούν ορισμούς με ημερομηνία λήξεως.

Ακολουθεί το τρίτο κεφάλαιο στο οποίο γίνεται μια σύντομη ιστορική ανασκόπηση των υπολογιστικών εργαλείων από την προϊστορία των ηλεκτρονικών υπολογιστών μέχρι και τις γενιές που έφερε η τεχνολογική εξέλιξη τους. Στο τέλος του γίνεται μια εκτενή αναφορά στο διαδίκτυο και τις πτυχές του.

Κεφάλαιο 3ο: Ιστορική ανασκόπηση μηχανικών και υπολογιστικών εργαλείων

Α΄ Μέρος -Ο Ηλεκτρονικός Υπολογιστής (Η/Υ)

Το τρίτο κεφάλαιο της ερευνητικής αυτής μελέτης περιλαμβάνει μια σύντομη παρουσίαση των μηχανικών και υπολογιστικών εργαλείων δηλαδή της υλικής πλευράς της πληροφορικής τεχνολογίας καθώς και την εξέλιξη αυτής μέσα στο χρόνο.

1. Η προϊστορία των Η/Υ

Όταν λέμε προϊστορία των Η/Υ εννοούμε την εξιστόρηση όλων εκείνων των υπολογιστικών εργαλείων και συσκευών που κατά καιρούς χρησιμοποίησε ο άνθρωπος για να τον διευκολύνουν στους υπολογισμούς του πριν από την εμφάνιση του πρώτου υπολογιστή, του Eniac, το 1947.

Οι συσκευές αυτές είναι οι εξής :

1.1. Ο Άβακας ή Αριθμητήριο

Θεωρείται σαν η πρώτη υπολογιστική μηχανή που κατασκεύασε ο άνθρωπος και χρησιμοποιήθηκε πριν από το 4.000 π.Χ. στην κοιλάδα της Μεσοποταμίας και στη σημερινή του μορφή το 2.600 π.Χ. από τους Κινέζους. Έχει χάντρες σε δύο τμήματα με τιμές αντίστοιχα 1, 10, 100, 1000 και 5, 50, 500, 5000. Μπορεί να κάνει και τις τέσσερις αριθμητικές πράξεις και κάποιος που είναι εξοικειωμένος με τη χρήση του μπορεί να κάνει πολύ γρήγορα υπολογισμούς.

1.2. Ο Υπολογιστής των Αντικυθήρων

Βρέθηκε το 1900 κοντά στο ομώνυμο νησί από σφουγγαράδες και είναι γνωστός και σαν «*Αστρολάβος των Αντικυθήρων*». Οι αστρολάβοι ήταν όργανα που χρησιμοποιήθηκαν στην αρχαιότητα για αστρονομικές παρατηρήσεις. Ο αστρολάβος αυτός αποτελείται από πολλούς οδοντωτούς τροχούς, κίνησε το ενδιαφέρον Άγγλων κυρίως επιστημόνων και γράφτηκαν μελέτες και βιβλία

για τον τρόπο κατασκευής και λειτουργίας του. Θεωρείται σαν ένα είδος «*αρχαίου υπολογιστή*».

1.3. Η Μηχανή του Pascal

Την κατασκεύασε το 1642 σε ηλικία 19 ετών για να βοηθήσει τον πατέρα του που ήταν φοροεισπράκτορας. Η μηχανή του, που ονομάστηκε «*Πασχαλίνα*», έκανε προσθέσεις και αφαιρέσεις με συστήματα γραναζιών. Ήταν η πρώτη αθροιστική μηχανή και μπορούσε να κάνει αυτόματη μεταφορά στις δεκάδες.

1.4. Η Μηχανή του Leibniz

Τελειοποίησε τη μηχανή του Pascal το 1674 για να μπορεί να κάνει πολλαπλασιασμούς και διαιρέσεις.

1.5. Η Μηχανή του Jacquard

Την κατασκεύασε το 1820 και χρησιμοποιούσε διάτρητες καρτέλες για να μπορεί να υφαίνει αυτόματα διάφορα υφάσματα. Αλλάζοντας τις θέσεις διάτρησης των δελτίων, δημιουργούσε νέα σχέδια στο ύφασμα. Το δελτίο, δηλαδή, αποθήκευε πληροφορίες.

1.6. Η Μηχανή του Babbage

Ο Babbage ήταν Μαθηματικός στο Cambridge της Αγγλίας και κατασκεύασε το 1812 τη *διαφορική μηχανή* για να κάνει μαθηματικούς υπολογισμούς. Προσπάθησε ακόμη να φτιάξει και την *αναλυτική μηχανή*, που θεωρείται ο πρόδρομος του σημερινού Η/Υ και εκτίθεται σήμερα στο Μουσείο Επιστημών του Λονδίνου.

Η Αναλυτική Μηχανή είχε την *Αποθήκη (Μνήμη)* που αποτελείτο από τρύπες πάνω σε καρτέλες και εκεί κρατούνταν τα δεδομένα, την *Αριθμητική Μονάδα (Μύλος)*, όπου γίνονταν οι πράξεις και τον *Έλεγχο* για να γίνονται σωστά οι λειτουργίες. Ό,τι δηλαδή έχουν και οι σημερινοί Η/Υ, μόνο που η

τεχνολογία της εποχής του δεν ήταν αρκετή για να τον βοηθήσει να ολοκληρώσει τη συσκευή του.

1.7. Η Μηχανή του Hollerith

Ήταν μια μηχανή πινάκων που λειτουργούσε με διάτρητες καρτέλες και με τη βοήθειά της κατόρθωσε το 1890 να μελετήσει τα απογραφικά στοιχεία των ΗΠΑ μέσα σε τέσσερις μόλις εβδομάδες. Η βοήθεια που πρόσφερε αυτή η μηχανή ήταν τόσο μεγάλη, αρκεί να σκεφτεί κανείς ότι τα απογραφικά στοιχεία της προηγούμενης δεκαετίας δεν είχαν ακόμη μελετηθεί. Από την εταιρεία που ίδρυσε ο Hollerith προήλθε το 1924 η πολύ γνωστή στον χώρο των Η/Υ σήμερα IBM.

2. Η τεχνολογική εξέλιξη των υπολογιστών (γενιές)

Όταν λέμε Ιστορία των Ηλεκτρονικών Υπολογιστών εννοούμε την περίοδο από την κατασκευή του πρώτου υπολογιστή, στη μορφή όπως τον ξέρουμε σήμερα, δηλ. να έχει δική του μνήμη και πρόγραμμα, μέχρι και τους σημερινούς υπολογιστές.

2.1. Η Εποχή Πριν από τον Πρώτο Υπολογιστή: Ο Υπολογιστής Z3

Ο υπολογιστής αυτός κατασκευάστηκε το 1941 στη Γερμανία από τον καθηγητή *Konrad Zuse* και χρησιμοποιήθηκε αποκλειστικά στον στρατό. Χρησιμοποιούσε διάτρητη χαρτοταινία, είχε μνήμη 64 λέξεων και έκανε τις πράξεις του στο δυαδικό σύστημα. Καταστράφηκε σ' έναν βομβαρδισμό του Βερολίνου το 1944.

2.2. Ο Υπολογιστής Mark I

Κατασκευάστηκε το 1944 στο Harvard των ΗΠΑ με τη συνεργασία του επιστήμονα *Howard Aiken* και της εταιρείας IBM. Ήταν μια μεγάλη μηχανή

που έκανε πολύ θόρυβο και χάλαγε συνέχεια. Λειτούργησε μέχρι το 1959 και σήμερα εκτίθεται στο Πανεπιστήμιο του Harvard.

2.3. Ο Υπολογιστής ABC

Ο υπολογιστής αυτός ήταν ο πρώτος που χρησιμοποιήθηκε για την επίλυση μαθηματικών προβλημάτων. Χρησιμοποιούσε ηλεκτρονικές λυχνίες και το δυαδικό σύστημα. Οι κατασκευαστές του ήταν οι Atanasoff και Berry, απ' όπου πήρε και το όνομα *ABC (Atanasoff-Berry-Computer).*

3. Οι Γενιές των Η/Υ

3.1. Πρώτη Γενιά

Η γενιά αυτή κράτησε από το 1944 -1958 και το κύριο δομικό στοιχείο των υπολογιστών αυτής της γενιάς ήταν οι *ηλεκτρονικές λυχνίες.* Ο *Eniac (Electronic Numerator Integrator and Calculator)* θεωρείται σήμερα σαν ο πρώτος Η/Υ, κατασκευάστηκε το 1947 στην Πενσυλβάνια των ΗΠΑ και σχεδιάστηκε αρχικά για στρατιωτικές ανάγκες. Αποτελείτο από 19.000 λυχνίες, ζύγιζε 30 τόνους και καταλάμβανε 270 τετρ. μέτρα με κατανάλωση ηλεκτρικής ενέργειας 200 KW. Μπορούσε να κάνει 300 πολλαπλασιασμούς το δευτερόλεπτο.

Ο Eniac χάλαγε συχνά, έκανε πολλά λάθη και είχε το μεγάλο μειονέκτημα ότι κάθε φορά που ήθελαν να «τρέξουν» ένα καινούργιο πρόγραμμα, έπρεπε να ξηλώσουν και να ξανα-συνδέσουν πολλές από τις καλωδιώσεις του.

Εμφανίστηκε τότε ο Ούγγρος επιστήμονας *John Von Neumann,* ο οποίος δημιούργησε τις βάσεις ενός σύγχρονου υπολογιστή που είναι η χρήση του δυαδικού συστήματος αρίθμησης και η αποθήκευση των δεδομένων και του προγράμματος στη μνήμη του υπολογιστή. Βασισμένοι στις ιδέες του Neumann, δημιούργησαν το 1951 τον Η/Υ *Edvac* και το 1949 τον Η/Υ *Edsac* στην Αγγλία.

Στις αρχές της δεκαετίας του '50 εμφανίστηκε ο Η/Υ *Univac* που ήταν ένας μεγάλος σταθμός στην ιστορία των Η/Υ, γιατί ήταν ο πρώτος υπολογιστής που κατασκευάστηκε σε πολλά αντίτυπα και πουλήθηκε σε εταιρείες και δημόσιες υπηρεσίες. Έτσι, πολύς κόσμος άρχισε τότε να ασχολείται με τους υπολογιστές που, από μυστηριώδεις μηχανές, έγιναν ένα χρήσιμο εργαλείο για τον καθένα. Ο Univac -1 χρησιμοποιήθηκε για την απογραφή του πληθυσμού των ΗΠΑ, όπου αντικατέστησε τις μηχανές IBM, που χρησιμοποιούνταν από το 1890. Οι υπολογιστές της πρώτης γενιάς χρησιμοποιήθηκαν αποκλειστικά για στρατιωτικές και επιστημονικές εφαρμογές.

3.2. Δεύτερη Γενιά

Η γενιά αυτή κράτησε από το 1958-1964 και το κύριο χαρακτηριστικό της ήταν η αντικατάσταση των ηλεκτρονικών λυχνιών από τα *τρανζίστορς*. Αυτό είχε σαν συνέπεια τη μεγάλη μείωση του όγκου, της κατανάλωσης και του κόστους των υπολογιστών και την αύξηση της ταχύτητάς τους. Ο πρώτος Η/Υ αυτής της γενιάς ήταν ο 1401 της IBM, που πουλήθηκε σε 15.000 αντίτυπα.

Άλλοι υπολογιστές αυτής της γενιάς ήταν ο γαλλικός Honeywell-Bull και οι Control Data, General Electric και NCR. Εμφανίζονται ακόμα και οι πρώτες *γλώσσες προγραμματισμού*, που ήταν η FORTRAN και η COBOL. Η πρώτη χρησιμοποιήθηκε για μαθηματικούς υπολογισμούς, ενώ η δεύτερη για εμπορικές εφαρμογές (μισθοδοσία, λογιστικά κ.ά.) και χρησιμοποιείται πολύ ακόμα και σήμερα.

Η τεχνολογία των τρανζίστορ προχώρησε πολύ στη διάρκεια αυτής της γενιάς και άρχισε η ολοκλήρωση (συγκέντρωση) των ηλεκτρονικών στοιχείων σε μικρά κομμάτια από πυρίτιο. Μεγάλες εταιρείες στην τεχνολογία αυτή δημιουργήθηκαν στην Καλιφόρνια των ΗΠΑ, σε μια περιοχή που είναι γνωστή σαν *Κοιλάδα του Πυριτίου (Silicon Valley)*.

3.3. Τρίτη Γενιά

Η γενιά αυτή κράτησε από το 1964-1971 και το κύριο χαρακτηριστικό της ήταν η αντικατάσταση των τρανζίστορ από τα *Ολοκληρωμένα Κυκλώματα* (Ο/Κ) ή chips, τα οποία είναι πολύ μικρά κομμάτια από πυρίτιο που συγκεντρώνουν πολλές χιλιάδες ηλεκτρονικά στοιχεία.

Ο πιο χαρακτηριστικός Η/Υ αυτής της γενιάς είναι ο IBM 360, που ήταν ο πρώτος που χρησιμοποίησε *λειτουργικό σύστημα (operating system)*, δηλ. ένα ειδικό πρόγραμμα για την εύκολη επικοινωνία του χρήστη με τον υπολογιστή, και ακόμα και ο πρώτος που χρησιμοποίησε *μαγνητικούς δίσκους* για την αποθήκευση των δεδομένων.

Άλλοι υπολογιστές αυτής της γενιάς ήταν οι CDC 3600 και 6600 και ο γαλλικός CII. Εμφανίζονται ακόμα και οι μίνι υπολογιστές, που είναι μικροί, φθηνοί, γρήγοροι και κατάλληλοι για χρήση σε ιδιωτικές εταιρείες. Ο πρώτος μίνι υπολογιστής ήταν ο PDP-8 της εταιρείας DEC.

Η γενιά αυτή χαρακτηρίστηκε και από τη μεγάλη ανάπτυξη του *Λογισμικού (Software)*, που είναι όλα τα προγράμματα που χρησιμοποιεί ο υπολογιστής, είτε είναι έτοιμα από την εταιρεία ή τα έχει κάνει ο χρήστης, ενώ το *Υλικό (Hardware)* είναι όλα τα εξαρτήματα του υπολογιστή που μπορούμε να αγγίξουμε, όπως τα καλώδια, τα Ο/Κ, η οθόνη κ.ά.

Δημιουργήθηκε η γλώσσα προγραμματισμού *Basic*, που χρησιμοποιείται μέχρι και σήμερα, και είναι η πιο κατάλληλη γλώσσα για όσους είναι αρχάριοι στον προγραμματισμό. Εμφανίστηκαν ακόμη τα *συστήματα καταμερισμού χρόνου (timesharing)*, όπου πολλοί χρήστες μπορούν να δουλεύουν μαζί σ' έναν υπολογιστή, αλλά ο καθένας νομίζει ότι ο υπολογιστής είναι δικός του.

Ενώ μέχρι τότε τα προγράμματα ήταν δωρεάν και δινόταν από την εταιρεία μαζί με την αγορά του υπολογιστή, πρώτη η IBM το 1969 χρέωσε ξεχωριστά τα προγράμματα από το μηχάνημα και ακολούθησαν κι άλλες

εταιρείες αυτή την τακτική. Δημιουργήθηκαν έτσι οι *Εταιρείες Λογισμικού (Sotfware Houses)*, που αποκλειστική τους απασχόληση είναι η δημιουργία και διάθεση προγραμμάτων για υπολογιστές.

3.4. Τέταρτη Γενιά

Η γενιά αυτή κρατάει από το 1971 έως σήμερα. Κύριο χαρακτηριστικό αυτής της γενιάς είναι η εμφάνιση των Ολοκληρωμένων Κυκλωμάτων Πολύ Μεγάλης Κλίμακας (VLSI - Very Large Scale Integration), όπου εκατομμύρια ηλεκτρονικά στοιχεία χωράνε σ' ένα πολύ μικρό κομμάτι πυριτίου. Έγινε έτσι δυνατή η κατασκευή του *μικροεπεξεργαστή (microprocessor)*, δηλ. του μικροσκοπικού εκείνου εξαρτήματος που είναι η «καρδιά» κάθε σύγχρονου μικροϋπολογιστή, που κάνει όλους τους υπολογισμούς και τους ελέγχους, και οι υπολογιστές έγιναν τόσο μικροί σε όγκο και τόσο δυνατοί σε απόδοση, ώστε έγιναν απαραίτητοι σε πάρα πολλές εταιρείες και κατέκλυσαν πολλά σπίτια.

Οι πρώτοι μικροεπεξεργαστές ήταν ο 4004 και ο 8008 και ακολούθησαν ο 8080, ο 8086/8088, ο 80286, ο 80386, ο 80486 και σήμερα είναι ο πολύ δυνατός Pentium.

Στις αρχές της δεκαετίας του '80 εμφανίστηκαν οι *Προσωπικοί Υπολογιστές (PC - Personal Computer)*, που έγιναν σιγά-σιγά τόσο δυνατοί, ώστε αντικατέστησαν όλα σχεδόν τα υπολογιστικά συστήματα.

Οι πρώτοι προσωπικοί υπολογιστές ήταν ο Altair 8800, οι Apple I και II, ο TRS-80 της Radio Shack και ο IBM-PC. Στα προγράμματα πρωτοπόρησε η εταιρεία Apple, που πρώτη δημιούργησε το φιλικό περιβάλλον εργασίας για τον χρήστη με τα *παράθυρα (windows)*. Στην αγορά, όμως, κυριάρχησαν τα συμβατά με IBM συστήματα και μόλις πρόσφατα εμφανίστηκε σ' αυτά και το περιβάλλον των windows.

Τα παράθυρα (windows) λέμε ότι είναι φιλικά προς τον χρήστη (user friendly), γιατί μπορεί να τα μάθει και να τα χειριστεί πολύ εύκολα και κάποιος που είναι αρχάριος με τους υπολογιστές.[66]

3.5. Πέμπτη Γενιά

Η τεχνολογία για τη γενιά αυτή είναι ακόμα σε πειραματικό στάδιο και τα κύρια χαρακτηριστικά αυτής της γενιάς θα είναι η ακόμα ευκολότερη επικοινωνία του Η/Υ με τον άνθρωπο, η πολύ μεγάλη ταχύτητα επεξεργασίας, η εμφάνιση της Τεχνητής Νοημοσύνης, δηλ. η ικανότητα των υπολογιστών να σκέπτονται, και ακόμη να μπορούν να καταλαβαίνουν την ανθρώπινη φωνή.

Β' Μέρος – Το διαδίκτυο (Internet)

1.1. Γενικά

Όροι όπως «κυβερνοχώρος» (cyberspace), «Διαδίκτυο» (internet), «Δίκτυο» (the Net), «η Λεωφόρος των Πληροφοριών» (Information superhighway) και ο «Παγκόσμιος Ιστός» (World Wide Web) χρησιμοποιούνται εναλλακτικά για να περιγράψουν το υπάρχον κολοσσιαίο δίκτυο υπολογιστών που αλληλοσυνδέονται μέσω της τηλεπικοινωνιακής υποδομής. Ένας ορισμός του Διαδικτύου είναι ότι είναι ένα δίκτυο υπολογιστών διασυνδεδεμένο μέσω ενός παγκοσμίως μοναδικού χώρου διεύθυνσης, που βασίζεται στο πρωτόκολλο του ίντερνετ (Internet Protocol-IP), ικανό να υποστηρίζει επικοινωνίες με τη χρήση του Transmission Transfer Protocol/Internet Protocol(TCP/IP) και παρέχει υπηρεσίες σε διαδοχικά επίπεδα του, επικοινωνίες και σχετική υποδομή.[67]

---

[66] Στην οθόνη του υπολογιστή υπάρχουν εικονίδια για το κάθε αρχείο και το κάθε πρόγραμμα. Έτσι, π.χ., για να διαγράψουμε ένα αρχείο στα Windows, απλά σημαδεύουμε με το ποντίκι το εικονίδιο του αρχείου αυτού και το σύρουμε «εικονικά» σ' έναν «σκουπιδοτενεκέ». Για να το αντιγράψουμε ή να το μετακινήσουμε σε μια νέα θέση, το πιάνουμε με το ποντίκι και το αφήνουμε στη νέα του θέση.

[67] Βλ., στο (Journalism and the Internet(article). Dr Dave Nicholas, Mr. Peter Williams. Journalism information seeking Internet survey, http://www.soi.city.ac.uk/~pw/ji_lit.html)

Το Internet, όμως, δεν έχει από την αρχή τη μορφή με την οποία το γνωρίζουμε σήμερα. Στα μέσα της δεκαετίας του 1960 και κατά τη διάρκεια του Ψυχρού Πολέμου, που διεξάγεται ανάμεσα στις ΗΠΑ και στη Σοβιετική Ένωση, το αμερικανικό Πεντάγωνο επιθυμεί τη δημιουργία ενός δικτύου ελέγχου και διοίκησης ανθεκτικό σε περίπτωση πυρηνικού πολέμου, την οποία αναθέτει στη διεύθυνση ARPA (Advanced Research Projects Agency).[68] Στόχος της είναι η προώθηση τεχνολογιών με στρατιωτική χρησιμότητα. Η έρευνα έχει ως αποτέλεσμα την αποστολή δεδομένων από τον έναν υπολογιστή στον άλλο σε φέτες ή αλλιώς πακέτα, τα οποία ακολουθούν διαφορετική πορεία αλλά φθάνοντας στον προορισμό τους συναρμολογούνται ξανά στη σωστή σειρά(packet switching, διαμεταγωγή πακέτων).

Από τη χρήση του ARPANET, που αποκαλείται ο πρόδρομος του ίντερνετ, αντλούνται κάποια συμπεράσματα που οδηγούν στη δημιουργία ενός νέου μοντέλου επικοινωνίας μεταξύ των υπολογιστών, το λεγόμενο TCP/IP(Transmission Control Protocol/Internet Protocol), το οποίο δίνει ιδιαίτερη βαρύτητα στη δυνατότητα διασύνδεσης επιμέρους τοπικών δικτύων και γίνεται επίσημο πρωτόκολλο επικοινωνίας του ARPANET και των δικτύων που συνδέονται σ' αυτό την 1η Ιανουαρίου του 1983. Στη χρονιά αυτή το ARPANET διασπάται στο στρατιωτικό MILNET, στο οποίο η πρόσβαση είναι αυστηρά ελεγχόμενη και στο ακαδημαϊκό ARPANET με πρόσβαση από ένα ευρύτερο κοινό. Στη δεκαετία του 1980 τα επιμέρους δίκτυα που συναποτελούν το ARPANET, το NSFNET και άλλα δίκτυα συγκεντρώνονται σε ένα Διαδίκτυο(internetwork) και όλοι μιλούν για το Διαδίκτυο(Internet). [69]

Στη συνέχεια το δίκτυο αναπτύσσεται με σημαντικά έντονους ρυθμούς. Το 1990 το Διαδίκτυο περιέχει 3.000 δίκτυα και 200.000 υπολογιστές ενώ το 1992 συνδέεται ο πρώτος εκατομμυριοστός υπολογιστής στο δίκτυο. Το 1995 υπάρχουν πολλαπλά κεντρικά δίκτυα, εκατοντάδες γεωγραφικά δίκτυα,

[68] Βλ., Βιδάλης Τάκης, «ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΣΥΝΤΑΓΜΑ», ΝοΒ,σ.29 επ.
[69] Βλ., Manuel Castells, «THE INTERNET GALAXY», OXFORD UNIVESITY PRESS,2003, σ.9 επ.

δεκάδες τοπικά δίκτυα, δεκάδες εκατομμύρια χρήστες, οι οποίοι διπλασιάζονται περίπου κάθε χρόνο.[70]

1.2. Η Έννοια του Internet

Καταρχήν τονίζεται ότι η χρήση ηλεκτρονικού υπολογιστή οδηγεί σταδιακά στην σύνδεση με το Internet, καθόσον ένας υπολογιστής χωρίς internet καταλήγει να δίνει πολύ περιορισμένες δυνατότητες στον χρήστη.

Συνολικά, το internet, θεωρείται ως «η ίδια η πρόοδος και το μέλλον», ένας «κόσμος» που προσφέρει άπειρες δυνατότητες, οι περισσότερες γνωστές σε όλους (χρήστες και μη): αναζήτηση πληροφοριών, «εγκυκλοπαίδεια», ενημέρωση/επικαιρότητα, επικοινωνία μέσω e-mail, επικοινωνία με κρατικές υπηρεσίες, κρατήσεις εισιτηρίων, πληρωμές λογαριασμών, αλλά και ακρόαση ραδιοφώνου, downloading (κατέβασμα) τραγουδιών, παιχνίδια (κυρίως από τους νέους).

Οι ανάγκες που καλύπτει το internet είναι τόσο πρακτικές (προσωπικό και επαγγελματικό «εργαλείο»), όσο και ψυχολογικές (ατομική ικανοποίηση/ψυχαγωγία), αλλά και δυναμικά κοινωνικές (επικοινωνία, μέλος συγκεκριμένης, σύγχρονης κουλτούρας και lifestyle, «ένταξη» στο σήμερα).

Για την τυπολογία των μυημένων, το Internet φαίνεται να αποτελεί εξίσου «εργαλείο» δουλειάς όσο και ψυχαγωγία/διασκέδαση και τρόπο ζωής, ενώ για την τυπολογία των πρακτικών, αποτελεί κυρίως εργαλείο δουλειάς και τεχνολογικό επίτευγμα. Μεταξύ των μη χρηστών, οι πρόθυμοι το αντιλαμβάνονται ως εργαλείο δουλειάς και σύγχρονη ανάγκη, οι επιφυλακτικοί κυρίως ως εργαλείο δουλειάς και δευτερευόντως ως σύγχρονη ανάγκη και τεχνολογικό επίτευγμα, ενώ ακόμα και οι αρνητές αναγνωρίζουν την επαγγελματική χρησιμότητα και την σύγχρονη ανάγκη γι αυτό σε πολύ μεγαλύτερο βαθμό από τα αρνητικά του.

---

[70] Βλ., Νίκος Φώτης, *Τι είναι το Ίντερνετ:* "Το Δίκτυο", Το ΒΗΜΑ, Κυριακή 29 Οκτωβρίου 2000, σελ. 3-4

Συνολικά επομένως, το internet θεωρείται απ' όλους κάτι πολύ χρήσιμο που περισσότερο βελτιώνει, παρά χειροτερεύει τον σύγχρονο τρόπο ζωής.

1.3. Η προσφορά του Ιντερνετ

Α) Επικοινωνία:

- Chat rooms, δηλαδή ανοιχτές και κλειστές αίθουσες επικοινωνίας,
- Απευθείας επικοινωνία (IRC & WEB based chat)
- Κλειστή αίθουσα επικοινωνίας
- Ετεροχρονισμένη επικοινωνία (πίνακας ανακοινώσεων).

Β) Ηλεκτρονικό Ταχυδρομείο (E-mail)

- Αποστολή και λήψη σε επιλεγμένους παραλήπτες
- διαμορφωμένου κειμένου
- αρχείων κειμένου
- αρχείων εικόνας, βίντεο και ήχου
- ιστοσελίδες και συνδέσμους (links) ιστοσελίδων
- ηλεκτρονικές κάρτες
- Ομαδική αποστολή

Γ) Λήψη ενημερωτικών / διαφημιστικών e-mails

Δ) Διαδίκτυο & Κινητή Τηλεφωνία:

- «Κατέβασμα» λογοτύπων και ήχων κλήσης
- Chat μέσω τηλεφώνου

- Αποστολή sms (γραπτών μηνυμάτων μέσω κινητού τηλεφώνου)

Ε) Ο μαθητής και το διαδίκτυο:

- Συλλογή πληροφοριών
- Έρευνα
- Δημοσιεύσεις εργασιών στο διαδίκτυο
- Επικοινωνία με άλλους μαθητές και σχολεία
- Συνεργασίες τάξεων σε κοινές δράσεις και εργασίες
- On-line μαθήματα
- Εξ' αποστάσεως εκπαίδευση π.χ. Ανοιχτό Πανεπιστήμιο

ΣΤ) Ο καθηγητής και το διαδίκτυο:

✓ *Κατά την προετοιμασία του μαθήματος:*

- Συλλογή εκπαιδευτικού υλικού
- Αναζήτηση πηγών ενημέρωσης

✓ *Κατά τη διάρκεια του μαθήματος:*

- Περιορισμένη η χρήση – τουλάχιστον στην Ελλάδα – κυρίως στο μάθημα της πληροφορικής
- Επιμόρφωση σε θέματα χρήσης Η/Υ και διαδικτύου
- Δημοσίευση εργασιών και σχολίων σε ηλεκτρονικούς πίνακες ανακοινώσεων

✓ *Ηλεκτρονική Βιβλιοθήκη (E-library)*

- Δίκτυα βιβλιοθηκών
- Ηλεκτρονικές βάσεις δεδομένων

- Πανεπιστημίων
- Εκδοτικών οίκων
- Εφημερίδων
- Ιατρικών πληροφοριών

✓ *Τήλε – Εργασία*

- Εργασία από το σπίτι η οποία απαιτεί μόνο έναν ηλεκτρονικό υπολογιστή μόντεμ και μια σύνδεση στο διαδίκτυο.
- Απεξάρτηση του εργαζόμενου από τον χώρο εργασίας
- Κατάλληλο για επαγγέλματα όπως: δημοσιογράφοι, συγγραφείς, μεταφραστές, κ.α.

✓ *Ηλεκτρονικό Εμπόριο (E- commerce)*

Η) Πιο διαδεδομένα προϊόντα:

- Η/Υ,
- CDs
- Εξαρτήματα υπολογιστών
- Βιβλία
- Ηλεκτρονικά παιχνίδια
- Τρόφιμα
- Ενδύματα
- Υποδήματα
- Κατοικίδια ζώα

✓ *Οικονομικές συναλλαγές (E-BANKING)*

- Τραπεζικές συναλλαγές

- Εξόφληση λογαριασμών
- Κινητό
- Δάνεια,
- Πιστωτικές κ.α
- Διαχείριση λογαριασμού
- Έλεγχος υπολοίπου
- Μεταφορά υπολοίπου σε άλλο λογαριασμό κ.α.

✓ *Ψυχαγωγία*

- Κατέβασμα» ηλεκτρονικών παιχνιδιών
- On-line ατομικά παιχνίδια
- On-line διαδραστικά παιχνίδια μεταξύ τουλάχιστον δύο χρηστών
- «Κατέβασμα» αρχείων μουσικής και βίντεο
- On-line σύνδεση με ραδιοφωνικούς σταθμούς
- Σελίδες διασκέδασης (fun pages) με ανέκδοτα και αστεία σκίτσα
- Οδηγοί διασκέδασης και τουριστικοί οδηγοί με καταχωρήσεις για αξιοθέατα, κέντρα διασκέδασης, ξενοδοχεία κτλ.

1.4. Το αρνητικό πρόσωπο του Internet

Σχεδόν άμεσα, μαζί με τα θετικά, προκύπτουν και τα αρνητικά στοιχεία του internet (κυρίως από τους μη χρήστες), τα οποία εντοπίζονται τόσο σε εγγενείς αδυναμίες του, όσο και σε συγκυριακές, με βάση την σημερινή του κατάσταση στην Ελλάδα (αυτά μόνο από τους χρήστες).

Τα εγγενή αρνητικά στοιχεία τοποθετούνται σε τέσσερις βασικούς άξονες, που ενδεχομένως να καθυστερούν και τον ρυθμό ανάπτυξής του: τα ηθικά (πορνογραφία, υπόκοσμος, παιδεραστία, ναρκωτικά, αιρετική ιδεολογία), κάτι που σχετίζεται με την αίσθηση «ελευθεριότητας» που αποδίδεται στο internet η οποία προκύπτει από την αδυναμία αντίληψης ή

ελέγχου του μέσου. Τα ηθικά αυτά αρνητικά οδηγούν στην έντονη άποψη ότι το internet θεωρείται επικίνδυνο για τα παιδιά κάτω των 15 χρονών, και αυτό εκφράζεται έντονα από γονείς και κυρίως «αρνητές» και άτομα χωρίς γνώση/επαφή με το internet, αλλά και ευρύτερα περιορισμένη νοοτροπία. Όμως, η επικινδυνότητα αυτή αντιμετωπίζεται στην πράξη από έλεγχο των γονέων (φραγές, ελεγχόμενη χρήση, χρήση παρουσία άλλων κλπ.), ενώ παράλληλα αναγνωρίζεται ότι αυτό εμπίπτει στην ευρύτερη ευθύνη των γονέων για την διαπαιδαγώγηση των παιδιών τους.

Ο δεύτερος άξονας των αρνητικών είναι τα κοινωνικά, και κυρίως η πιθανότητα απομόνωσης, καθώς και η υποκατάσταση της προσωπικής επαφής/αποδυνάμωσης σχέσεων, ψυχρότητα και δημιουργία «εικονικών» σχέσεων. Όμως, αυτά ανασύρονται κυρίως από γονείς, αρνητές και μη χρήστες και συνολικά τείνουν να τοποθετούνται σε θεωρητικό και μόνο επίπεδο.

Στον τρίτο άξονα των αρνητικών, τα πρακτικά μειονεκτήματα σχετίζονται κυρίως με το κόστος, ενώ ταυτόχρονα εκφράζονται και ανασφάλεια για «υπερχρεώσεις», «αλόγιστη» χρήση κυρίως από τα παιδιά, και ελλιπή μέτρα προστασίας του καταναλωτή από τις οικονομικές συναλλαγές/ αγορές. Το κόστος αποτελεί δυναμικό προβληματισμό που απορρέουν από την σημερινή κατάσταση της αγοράς στην Ελλάδα, ενώ η ανασφάλεια απορρέει από την φύση του internet ευρύτερα και δευτερευόντως από την ελληνική αγορά.

Τέλος, ο τρίτος άξονας των αρνητικών αφορά το λειτουργικό επίπεδο, καθώς το internet γίνεται αντιληπτό ως «αχανής» χώρος πληροφοριών, και κυρίως μεταξύ των μη χρηστών και των μεγάλων ηλικιών υπάρχει άγνοια ή ασαφής γνώση των δυνατοτήτων του, καθώς επίσης και το αντιλαμβανόμενο εμπόδιο της Αγγλικής γλώσσας για όσους δεν την γνωρίζουν.

1.5. Η ανάπτυξη στο μέλλον

Η ανάπτυξη του internet στην Ελλάδα μπορεί να προέλθει από δύο πηγές: α) από την αύξηση χρήσεων/διάρκειας σύνδεσης από τους τωρινούς χρήστες και β) από την αύξηση των χρηστών/νέων συνδέσεων.

Στην πρώτη περίπτωση, η αύξηση προβλέπεται ότι μπορεί να προέλθει «αυτόματα» εάν μειωθούν τα κόστη και βελτιωθεί η λεγόμενη «προσφορά της αγοράς», αναφερόμενοι κατά κύριο λόγο στα sites και στο περιεχόμενό τους.

Στην δεύτερη περίπτωση, η ανάπτυξη της αγοράς των χρηστών/συνδέσεων μπορεί να προέλθει άμεσα από την ομάδα των «πρόθυμων» μη χρηστών, και αργότερα από εκείνη των επιφυλακτικών. Οι αρνητές δεν θεωρούνται δυνητικό κοινό, δεδομένου ότι η αρνητική τους στάση είναι αρκετά δυναμική, αλλά κυρίως επειδή δημογραφικά είναι μεγαλύτεροι και άνθρωποι μεσο-κατώτερης μόρφωσης και απασχόλησης.

Από πλευράς φορέων, το κοινό θεωρεί ότι ο ΟΤΕ αποτελεί καθοριστικό παράγοντα για το παρόν και το μέλλον του internet στην Ελλάδα, καθόσον χαρακτηρίζεται ως μονοπώλιο υπεύθυνο για τις εξελίξεις σε επίπεδο υποδομών και παροχών, ενέχοντας ταυτόχρονα το κύρος και την αξιοπιστία ενός κρατικού φορέα, και είναι οργανισμός που χαίρει μιας ευρύτερα δυνατής εικόνας.

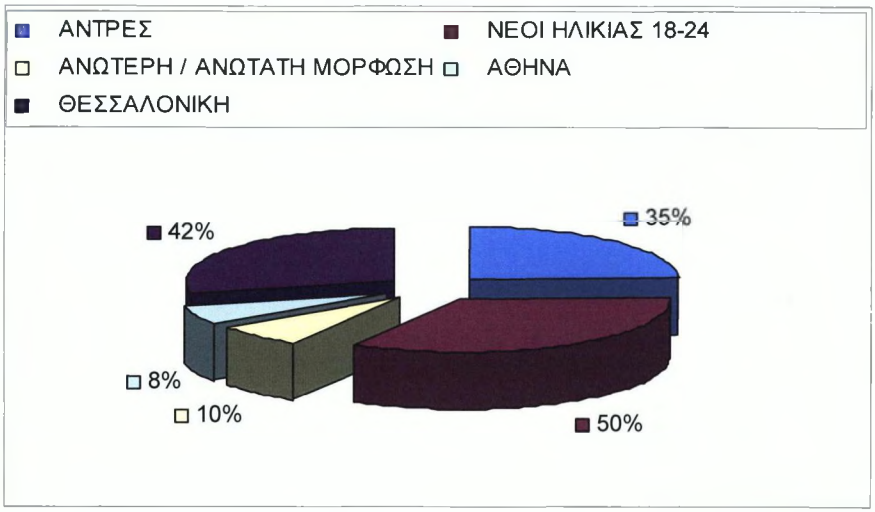
Εξ άλλου, το κοινό περιμένει και θεωρεί καταλληλότερο φορέα που θα πρέπει να δραστηριοποιηθεί πιο ενεργά για την ανάπτυξη του internet το ίδιο το Κράτος (μέσω των κατάλληλων φορέων) και τα Πανεπιστήμια, καθώς επίσης και τα Λύκεια. Αυτοί είναι οι φορείς που το κοινό δηλώνει ότι θα εμπιστευόταν και που θα το βοηθούσαν να «ξεπεράσει» τους παρόντες δισταγμούς και «φόβους» του σε σχέση με το internet.

1.6. Στατιστικά στοιχεία διαδικτύου

Από το 2001 η χρήση του internet αυξήθηκε σχεδόν κατά 10 ποσοστιαίες μονάδες, δηλαδή από 10,15% αυξήθηκε σε 19,3%.

1.6.1 Το internet το χρησιμοποιούν περισσότερο

- οι άνδρες 35%
- οι νέοι ηλικίας 18-24 50%
- όσοι έχουν ανώτερη / ανώτατη μόρφωση 50%
- Αθήνα 38%
- Θεσσαλονίκη 42%



Πίνακας 3. 1: Ποσοστιαία χρήση Internet

1.6.2 Ηλικίες.

Σε ό,τι αφορά τις ηλικίες, οι νέοι ηλικίας 15-24 ετών χρησιμοποιούν σε υψηλότερο βαθμό την τεχνολογία συγκριτικά με τις υπόλοιπες ηλικιακές ομάδες. Πιο συγκεκριμένα, ανάμεσα στους ερωτώμενους 15-24 ετών, η χρήση του Ίντερνετ φτάνει στο **54,1**%. Στους ερωτώμενους 25-34 ετών μειώνεται στο 43,2% και ακολουθούν οι ερωτώμενοι 35-44 ετών (**34,1**%), 44-54 ετών (**20,4**%) και τέλος οι ερωτώμενοι 55-64 ετών με το χαμηλότερο ποσοστό χρήσης (**5,3**%).

Η χρήση του Ίντερνετ, συνεπώς, διαφαίνεται να επηρεάζεται σε μεγάλο βαθμό από την ηλικία του ερωτώμενου.

1.6.3 Αιτίες απόστασης

Εντυπωσιακό είναι το εύρημα ότι ο κυριότερος λόγος για τον οποίο το 66,3% των ερωτώμενων δεν χρησιμοποιεί το Ίντερνετ είναι ότι δεν τους ενδιαφέρει ή ότι δεν το θεωρούν απαραίτητο (**53,6%**). Ακολουθούν με σημαντικά χαμηλότερη συχνότητα αναφοράς ότι δεν χρησιμοποιούν υπολογιστή (**28,2%**) και δεν ξέρουν να χρησιμοποιήσουν το Ίντερνετ (**14,5%**).

1.6.4 Εργαλείο ενημέρωσης

Το Ίντερνετ χρησιμοποιείται για αρκετά διαφορετικούς λόγους. Οι κυριότεροι λόγοι οι οποίοι αναφέρθηκαν είναι για πληροφορίες και ενημέρωση (**62,6%**), για email (**52,8%**), για να μαθαίνουν περισσότερα πράγματα για θέματα που τους ενδιαφέρουν (**50,4%**) και για την εργασία (**42,1%**).

1.6.5 Στο σπίτι

Το **72,1%** των ερωτώμενων δηλώνει ότι το χρησιμοποιεί στο σπίτι, το **37,7%** στη δουλειά, το **15,7%** στο σχολείο και στο πανεπιστήμιο, το **14,2%** σε Ίντερνετ cafe και το **7,7%** σε σπίτι φίλου ή γνωστού. Ωστόσο, ο χώρος χρήσης του Ίντερνετ διαφοροποιείται σημαντικά ανάλογα με την ηλικία του ερωτώμενου. Πιο συγκεκριμένα, η χρήση του Ίντερνετ στη δουλειά είναι σημαντικά υψηλότερη ανάμεσα στους ερωτώμενους άνω 35 ετών (**60,7%**) συγκριτικά με τους ερωτώμενους 15-24 ετών (**8,7%**) και τους ερωτώμενους 25-34 ετών (**47,2%**). Αντιθέτως, οι νέοι χρησιμοποιούν το Ίντερνετ πολύ πιο συχνά στο σχολείο ή στο πανεπιστήμιο (**38,9%**) και στα Ίντερνετ cafe (**28,6%**). Ανάμεσα στους χρήστες του Ίντερνετ στο σπίτι, η πλειοψηφία χρησιμοποιεί dial-up με απλή γραμμή σύνδεσης (**55,6%**). Ακολουθεί η σύνδεση ADSL (**25,9%**) και, τέλος, η dial-up ISDN σύνδεση (**16,9%**).

1.6.6 Νέοι χρήστες

Σχεδόν ο ένας στους δύο χρήστες (**45,9**%) χρησιμοποιεί το Ίντερνετ περισσότερα από τέσσερα χρόνια. Αντιθέτως, μόλις το **9,8**% έχει αρχίσει να το χρησιμοποιεί το τελευταίο έτος. Σε συνδυασμό με τη χαμηλή διείσδυση του Ίντερνετ στη χώρα μας, το ποσοστό αυτό είναι ιδιαιτέρως χαμηλό και συμβαδίζει με το γεγονός ότι η διείσδυση στη χώρα μας έχει μείνει στάσιμη.

1.6.7 Πόσες ώρες χρησιμοποιούν το internet

Η συντριπτική πλειοψηφία των χρηστών χρησιμοποιεί το internet κατά τη διάρκεια μιας τυπικής εβδομάδας (**97**%) και κατά μέσο όρο κατά τη διάρκεια μιας τυπικής εβδομάδας περνάει **8,1 ώρες** στο internet

1.6.8 Αγορά προϊόντων/υπηρεσιών μέσω internet

Οι αγορές προϊόντων/υπηρεσιών μέσω του internet είναι σε πολύ χαμηλά επίπεδα καθώς το **80,1**% των ερωτώμενων δηλώνει ότι δεν έχουν αγοράσει τίποτα μέσω του internet. Ο κυριότερος λόγος για τον οποίο οι χρήστες του internet δεν το έχουν χρησιμοποιήσει για αγορές είναι ότι δεν το θεωρούν ασφαλές (**54,1**%)

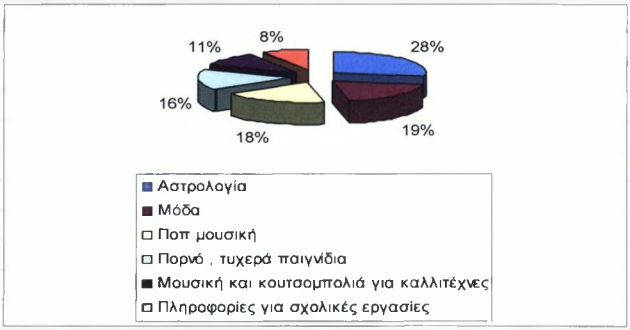
1.6.9 Ιστοσελίδες που προτιμούν τα παιδιά

Οι πρώτες επιλογές των αγοριών είναι:

- Νέα sites και εξερεύνηση καθημερινή. Εδώ εντάσσονται όλα τα πορνογραφικά, τυχερά παιγνίδια ιστοσελίδες με αίμα και τρόμο 36%
- Μουσική 20%
- Πολεμικά Διαδικτυακά παιχνίδια 20%
- Αθλητισμός γενικά - σπορ 9%
- Playstation sites 8%
- Ποδόσφαιρο 7%

Οι αντίστοιχες για τα κορίτσια είναι:

Αστρολογία	28%
Μόδα	19%
Ποπ μουσική	18%
Πορνό , τυχερά παιγνίδια	16%
Μουσική και κουτσομπολιά για καλλιτέχνες	11%
Πληροφορίες για σχολικές εργασίες	8%



Πίνακας 3. 2: Ποσοστιαία απεικόνιση ιστοσελίδων που προτιμούν τα κορίτσια

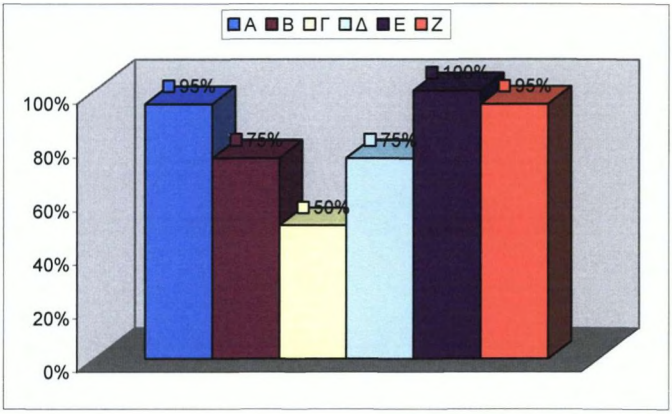
1.6.10 Συνολικά Ευρωπαϊκά αποτελέσματα

- Η χρήση της τεχνολογίας ανά ηλικιακή ομάδα.

Είναι σαφές ότι οι νέοι 15-24 ετών χρησιμοποιούν σε υψηλότερο βαθμό την τεχνολογία συγκριτικά με τις υπόλοιπες ηλικιακές ομάδες. Πιο συγκεκριμένα, ανάμεσα στους ερωτώμενους 15-24 ετών, η χρήση του internet φτάνει στο **54,1%**. Στους ερωτώμενους 25-34 ετών μειώνεται στο **43,2%**, και ακολουθούν οι ερωτώμενοι 35-44 ετών (**34,1**%), 44-54 ετών (**20,4**%) και τέλος οι ερωτώμενοι 55-64 ετών με το χαμηλότερο ποσοστό χρήσης (**5,3**%). Η χρήση του internet, συνεπώς, διαφαίνεται να επηρεάζεται σε μεγάλο βαθμό από την ηλικία του ερωτώμενου.[71]

[71] Βλ., ΔΙΚΤΥΟ ΕΛΛΗΝΙΚΩΝ ΚΑΤΑΝΑΛΩΤΙΚΩΝ ΟΡΓΑΝΩΣΕΩΝ -Ε.ΚΑΤ.Ο «Αποτελέσματα ερευνών για το Διαδίκτυο, σε Ελλάδα και Ευρώπη»Ομιλητής: Δρ. Πασχαλίδης Σωτήριος, 2007

Μετρήσεις σε ανήλικους :



Πίνακας 3. 2: Ποσοστιαία απεικόνιση ιστοσελίδων που προτιμούν ανήλικοι

A	95%
B	75%
Γ	50%
Δ	75%
E	100%
Z	95%

Όπου :

- Α : έχουν πρόσβαση σε πορνό-site και τυχερών παιχνιδιών
- Β : επηρεάζονται από διαφημίσεις στο διαδίκτυο και μπαίνουν στο πειρασμό να χρεώσουν τις πιστωτικές κάρτες των γονέων τους
- Γ : «σερφάρουν» στο διαδίκτυο για τουλάχιστον μία ώρα
- Δ : θα «σέρφαραν» περισσότερο από μία ώρα εάν κόστιζε λιγότερο
- Ε : είναι κάτω των 13 και μπαίνουν μόνο όταν οι γονείς είναι στο σπίτι
- Ζ : είναι άνω των 13 και τα οποία προτιμούν να μπαίνουν όταν απουσιάζουν οι γονείς τους, γιατί θέλουν να επικοινωνούν σε χώρους ανοιχτής επικοινωνίας, κάτι που τους το απαγορεύουν.

Κεφάλαιο 4ο:

Α΄ Μέρος – Ορισμός & Κατηγοριοποίηση Ηλεκτρονικών Εγκλημάτων

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Με τη βελτίωση όμως της ποιότητας ζωής δημιουργήθηκαν ταυτόχρονα οι ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό έγκλημα. Ηλεκτρονικό έγκλημα αποτελούν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Περικλείει όλες τις παραβάσεις με χρήση ηλεκτρονικού υπολογιστή που στρέφονται κατά οποιουδήποτε έννομου αγαθού.

Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η εν στενή έννοια ηλεκτρονική εγκληματικότητα αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων.

Αντίθετα η εν ευρεία έννοια εγκληματικότητα μέσω Η/Υ περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό μέσο.

Οι μορφές του Ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται

ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση.

4.1. Το έγκλημα στον κυβερνοχώρο (cyber crime)

Δεν υπάρχει ακόμη γενικά αποδεκτός όρος του εγκλήματος στον κυβερνοχώρο, ούτε στην διεθνή νομοθεσία, ούτε στη διεθνή νομολογία. Οι υπάρχοντες μέχρι τώρα (ελάχιστες) ποινικές αποφάσεις αφορούν εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) και όχι εγκλήματα του κυβερνοχώρου (cyber crimes).

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό» έγκλημα και η μόνη διαφορά που το διακρίνει από αυτό είναι ότι διαπράττεται σε διαφορετικό περιβάλλον (δηλαδή σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον δικτύου), δεν ανταποκρίνεται στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα κι αν υπάρχει δε χρησιμοποιείται). Μια άλλη δε κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικά σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

- Σε εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο (internet), π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με τη χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρο 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελεστή σε «περιβάλλον internet», τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με τη βοήθεια του κυβερνοχώρου (internet related crime).

- Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (χωρίς τη χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370γ & 1 του Π.Κ., π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM σε ηλεκτρονικό υπολογιστή.
- Σε «γνήσια εγκλήματα κυβερνοχώρου» (cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικά να έχει σχέση με τον κυβερνοχώρο. Μια τέτοια αξιόποινη συμπεριφορά θα μπορούσε να είναι π.χ. η μεταβίβαση κρυπτογραφικών κειμένων χωρίς σχετική άδεια ή η διάδοση πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοιες δραστηριότητες δεν αποτελούν εγκλήματα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία.

Με άλλα λόγια δηλαδή, τα «γνήσια εγκλήματα του κυβερνοχώρου» διαπράττονται αποκλειστικά με τη χρήση του διαδικτύου. Σε περίπτωση που ο υπολογιστής δεν είναι συνδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και αν διαπραχθεί, θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

Κύριες μορφές Κυβερνοεγκλημάτων που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΓΔΑΑ είναι οι ακόλουθες:

1. Απάτες μέσω Διαδικτύου
2. Παιδική πορνογραφία
3. Cracking και hacking
4. Πιστωτικές κάρτες
5. Διακίνηση ναρκωτικών
6. Διακίνηση-πειρατεία

4.2. Χαρακτηριστικά Γνωρίσματα Ηλεκτρονικού Εγκλήματος

Το Ηλεκτρονικό Έγκλημα, ανεξάρτητα από το εάν προσεγγιστεί από την στενή ή την ευρεία έννοια του, εμπεριέχει ορισμένα

χαρακτηριστικά γνωρίσματα που το διαχωρίζουν από το παραδοσιακό έγκλημα. Τέτοια σημεία είναι τα εξής[72] :

- Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε πραγματικό χρόνο, ακόμα και σε δευτερόλεπτα, και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο στη διάπραξή του για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
- Για την τέλεση του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
- Οι κυβερνο-εγκληματίες πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα, αποστέλλοντας ηλεκτρονικά μηνύματα (e-mails) με ψευδή στοιχεία.
- Μπορεί να διαπραχθεί από οποιοδήποτε μέρος, καθώς δεν απαιτείται η μετακίνηση του δράστη, και τα αποτελέσματά του να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξαρτήτου εδαφικού περιορισμού. Για αυτό, άλλωστε, και το αποκαλούν «έγκλημα χωρίς πατρίδα».
- Ο εντοπισμός ενός ψηφιακού εγκληματία, κατά κανόνα, είναι πολύ δύσκολος (αλλά όχι ακατόρθωτος) να προσδιοριστεί καθώς επίσης και ο (πραγματικός) τόπος τέλεσής του και αυτό γιατί μπορεί ο δράστης να εντοπιστεί σε ένα συγκεκριμένο τόπο, τα αποδεικτικά στοιχεία, όμως, να βρίσκονται σε διαφορετική και απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.
- Καθώς ο κίνδυνος ανακάλυψης του ηλεκτρονικού δράστη είναι μικρός, το ηλεκτρονικό έγκλημα αποδίδει μεγάλα κέρδη.
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος.

---

[72] Βλ., στο www.mopo.gr "Ηλεκτρονικό Έγκλημα – Ανθυπαστυνόμος Κωνσταντίνος Γ. Κούρος"

- Οι οικονομικές απώλειες που προξενούνται στα «ψηφιακά» εγκλήματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων.
- Καθώς για την διάπραξή του δεν απαιτείται φυσική μετακίνηση του δράστη, δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες, όπως για παράδειγμα παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται μαζί στις ίδιες ομάδες συζήτησης (π.χ. Newsgroups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (π.χ. Internet Relay Chat).
- Η καταγραφή της εγκληματικότητας στον Κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα γιατί ελάχιστες περιπτώσεις κυβερνο-εγκλημάτων καταγγέλλονται διεθνώς με άμεση συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του διαδικτύου να χαρακτηρίζεται ακόμα πιο «σκοτεινό» από ότι το έγκλημα του πραγματικού κόσμου.
- Η αστυνομική διερεύνηση του είναι πολύ δύσκολη και απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις.
- Οι οποίες εξειδικευμένες γνώσεις απαιτούνται και σε όσους, εκτός αστυνομίας, ασχολούνται με τη συγκεκριμένη μορφή εγκλήματος, όπως είναι οι εισαγγελείς, οι δικαστές, οι δικηγόροι.
- Για την διερεύνηση του απαιτείται συνεργασία τουλάχιστον δύο μηχανισμών του κράτους ώστε να γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία.[73]

[73] Βλ., στο www.elesme.gr "Κυβερνοχώρος- Το Διεθνές «Γίγνεσθαι» στο Ελληνικό «είναι» Υπαστυνόμος Α΄ Δ. Π. Αγγελοπούλου, Εξεταστού Ψηφιακών Πειστηρίων της Διεύθυνσης Εγκληματολογικών Ερευνών ΕΛ. ΑΣ.". Επίσης βλέπε. Τσουραμάνης Χρ στο www.teimes.gr_spoudastirio_yifiaki_eglimatikotita "Ψηφιακή Κοινωνία. Ψηφιακή Εγκληματικότητα και Θυματοποίηση".

4.2.1. Χαρακτηριστικά Ψηφιακού Εγκληματία

Οι δράστες των γνήσιων ψηφιακών εγκλημάτων δραστηριοποιούνται αποκλειστικά στον κυβερνοχώρο και χρησιμοποιούν αποκλειστικά και μόνο την ψηφιακή τεχνολογία για να παραβούν το νόμο.

Συγκεκριμένα, οι άνθρωποι που διαπράττουν τα εγκλήματα υπολογιστών διαφέρουν μεταξύ τους ανάλογα με τις δεξιότητες, τη γνώση, τους πόρους και τα κίνητρά τους, έχουν διαφορετικά επίπεδα ικανοτήτων που στηρίζονται στη βασική τους εκπαίδευση, τις κοινωνικές τους αλληλεπιδράσεις και στην εμπειρία τους στη χρήση των ηλεκτρονικών υπολογιστών.

Υπάρχουν τρεις κατηγορίες ψηφιακών εγκληματιών: οι κατασκευαστές εργαλείων, οι χρήστες εργαλείων και οι συγγραφείς προγραμμάτων. Τα κίνητρά τους περιλαμβάνουν την πλεονεξία, την ανάγκη (για να λύσουν τα προσωπικά τους προβλήματα), την αδυναμία να κατανοήσουν τη ζημιά που προξενούν σε άλλους, την προσωποποίηση των υπολογιστών (πολλοί τους θεωρούν ως αντιπάλους τους σε κάποιο παιχνίδι) και το σύνδρομο του Robin Hood, που τους κάνει να βλέπουν τις εταιρίες τόσο πλούσιες ώστε οι οικονομικές ζημιές που τους προκαλούν να δικαιολογούνται ηθικά.

Πολλοί ψηφιακοί εγκληματίες θεωρούν ότι η απλή εισβολή σε συστήματα, ο βανδαλισμός τους ή η προφανής παραβίαση της εμπιστευτικότητας τους είναι ένα αβλαβές και ηθικά αποδεκτό χόμπι ενώ υπάρχουν και εκείνοι που θεωρούν ότι η εισβολή σε συστήματα έχει και τη θετική της πλευρά με την έννοια ότι με αυτό τον τρόπο αυτό συμβάλλουν στη βελτίωση της ασφάλειάς τους.

Οι περισσότεροι ενεργοί ψηφιακοί εγκληματίες είναι νέοι άνθρωποι ηλικίας 12 έως 24 ετών και συνήθως η οικογένεια τους δεν έχει καμία ιδέα για το τι κάνουν.

Βεβαίως, υπάρχουν και κάποιο υποστηρικτές κυρίως των hackers που κατηγορούν τα θύματα τους για τα ανεπαρκή μέτρα ασφάλειας που έχουν λάβει και ελαχιστοποιούν τα ηθικά ζητήματα που τυχόν προκύπτουν ενώ υπάρχουν και αυτοί που περιγράφουν τις επιθέσεις τους ως δικαιολογημένες διαμαρτυρίες ή άμεση δράση ενάντια στους εχθρούς του περιβάλλοντος ή της κοινωνίας γενικά.

Η επικινδυνότητα των εισβολέων στα ηλεκτρονικά υπολογιστικά συστήματα εξαρτάται από τα κίνητρά τους. Αν τα κίνητρά τους είναι η διασκέδαση ή η επιθυμία τους να αναγνωριστούν στον κύκλο τους ως αυθεντίες στους Η/Υ ή να μάθουν τον τρόπο λειτουργίας του συστήματος μιας επιχείρησης ή ενός οργανισμού, η παράνομη πρόσβασή τους λήγει σε εκείνο το σημείο και στην πραγματικότητα, αυτό που υφίσταται βλάβη δεν είναι τίποτα άλλο από το γόητρο του συστήματος ασφαλείας της συγκεκριμένης επιχείρησης ή οργανισμού. Αν όμως το κίνητρό τους είναι το προσωπικό οικονομικό όφελος, το οποίο μπορούν να επιτύχουν βλάπτοντας με οποιοδήποτε τρόπο το σύστημα ή τα αρχεία δεδομένων των θυμάτων τους ή πουλώντας σε τρίτους τις πληροφορίες που αποκόμισαν από αυτά, τότε οι ζημιές είναι ανυπολόγιστες.[74]

4.3. Απάτες μέσω Ηλεκτρονικού Υπολογιστή

Τα περιστατικά απάτης μέσω της χρήσης ηλεκτρονικού υπολογιστή ξεπερνούν τα 30, ενώ στο διάστημα Ιανουαρίου – Μαρτίου του 2007, οι αστυνομικοί της Δίωξης Ηλεκτρονικού Εγκλήματος προχώρησαν στη σύλληψη 40 ατόμων που εμπλέκονταν σε συνολικά 22 παρόμοιες υποθέσεις. Στη συνέχεια του κεφαλαίου παρατίθενται ενδεικτικοί τύποι περιστατικών.

[74] Βλ., Τσουραμάνης Χρ. στοwww.teimes.gr_spoudastirio_yifiaki_eglimatikotita "Ψηφιακή Κοινωνία. Ψηφιακή Εγκληματικότητα και Θυματοποίηση".

4.3.1. Παρακολούθηση γραμμών επικοινωνίας χωρίς εξουσιοδότηση

Παρακολουθώντας τις επικοινωνιακές γραμμές μπορεί κανείς να αποκτήσει μη εξουσιοδοτημένη προσπέλαση σε μετακινούμενα δεδομένα, με πιθανό αποτέλεσμα να παραβιαστεί η ιδιωτικότητά τους.

4.3.2. Ανάλυση κυκλοφορίας (Traffic analysis) χωρίς εξουσιοδότηση

Για δεδομένες διευθύνσεις πηγής και προορισμού η παρακολούθηση των διακινούμενων δεδομένων μπορεί να οδηγήσει σε ανάπτυξη ενός προτύπου (pattern) κυκλοφορίας. Η στατιστική και μόνο ανάλυση της επικοινωνίας, χωρίς απαραίτητα να γίνεται ανάγνωση των ίδιων των δεδομένων, μπορεί να οδηγήσει σε χρήσιμα συμπεράσματα για κάποιον τρίτο.

4.3.3. Πλαστογράφηση διευθύνσεων δικτύου (spoofing)

Καταργείται η ιδιότητα της μονοσήμαντης αντιστοίχισης των διευθύνσεων δικτύου σε μία συγκεκριμένη θέση, με αποτέλεσμα τα διακινούμενα δεδομένα να χάνουν την ιδιότητα της αυθεντικότητας προέλευσης.

4.3.4. Υποκλοπή η απόπειρα υποκλοπής στοιχείων πρόσβαση

Στοιχεία πρόσβασης μπορούν να διαρρεύσουν σε έναν δυνητικό εισβολέα είτε από αμέλεια του χρήστη του συστήματος είτε μετά από παρακολούθηση των διακινούμενων πακέτων (sniffing) είτε με τη χρήση της μεθόδου ωμής δοκιμής (brute force attack).

4.3.5. Εκμετάλλευση κενών ασφαλείας (Security Vulnerabilities / Exploits)

Κακόβουλη εκμετάλλευση γνωστών ή άγνωστων αδυναμιών και υπηρεσιών του συστήματος που επιτρέπουν την υπέρβαση των μηχανισμών ασφάλειας για την προσπέλαση στους πόρους του συστήματος. Η ύπαρξη των αδυναμιών αυτών γίνεται γνωστή στους εισβολείς έπειτα από δοκιμαστική ανίχνευση που πραγματοποιούν στις θύρες επικοινωνίας του συστήματος (port-scanning)

4.3.6. Μη εξουσιοδοτημένη τροποποίηση (unauthorised modification)

Η τροποποίηση οποιοδήποτε στοιχείων / δεδομένων/ παραμέτρων ενός συστήματος χωρίς προηγούμενη εξουσιοδότηση από τους διαχειριστές του συστήματος.

4.3.7. Άρνηση παροχής υπηρεσίας (Denial of Service)

Η διακοπή της διαθεσιμότητας / παροχής μίας υπηρεσίας, με έμμεσο η άμεσο τρόπο από μη εξουσιοδοτημένο προσωπικό

4.3.8. Κατανεμημένη επίθεση άρνησης παροχής υπηρεσίας (Distributed Denial of Service)

Ίδια με την άρνηση παροχής υπηρεσίας - περιλαμβάνει όμως την συντονισμένη παράνομη χρήση πολλαπλών συστημάτων με στόχο την άρνηση παροχής μιας υπηρεσίας σε κάποιο άλλο σύστημα.

4.3.9. Κατάχρηση πόρων (abuse of resources)

Μία μη εξουσιοδοτημένη οντότητα είναι πιθανό να υποκλέψει πόρους ενός συστήματος, όπως κύκλους του επεξεργαστή, εύρος ζώνης δικτύου, χωρητικότητα δίσκων, είτε για να εξυπηρετηθούν διεργασίες του εισβολέα είτε για να προκληθεί άρνηση παροχής υπηρεσίας.

4.3.10. Πλαστοπροσωπία / Μεταμφίεση (masquerade)

Οποιαδήποτε ενέργεια έχει σαν σκοπό την απόκρυψη της πραγματικής ταυτότητας ενός χρήστη, μιας οντότητας, ενός συστήματος που εκτελεί η παρέχει μια υπηρεσία

4.3.11. Ιο-μορφικό λογισμικό (software virus)

Πρόκειται για κακόβουλο λογισμικό που εκτελείται ή φορτώνεται δυναμικά στο σύστημα. Συνήθως βρίσκεται ενσωματωμένο σε εκτελέσιμο κώδικα ή αυτόνομο σε μορφή δέσμης εντολών (script).

4.3.12. Καταχρηστικά μηνύματα / Ανεπιθύμητη αλληλογραφία (spam)

Αφορά κυρίως τις υπηρεσίες μηνυμάτων όπως τα νέα και η ηλεκτρονική αλληλογραφία. Πρόκειται για μηνύματα που αποστέλλονται συνήθως από πλαστές / ανύπαρκτες ηλεκτρονικές διευθύνσεις μαζικά προς

πολλαπλούς χρήστες. Περιλαμβάνουν διαφημιστικό περιεχόμενο η κακόβουλο λογισμικό (ιούς).

4.3.13. Παράνομη διακίνηση / διάθεση λογισμικού, ψηφιακού περιεχομένου (piracy)

Αφορά την διάθεση υλικού το οποίο προστατεύεται από νομοθεσία περί πνευματικών δικαιωμάτων και των οποίων η διακίνηση μπορεί να εκθέσει το ΕΔΕΤ η φορείς του ΕΔΕΤ.

4.3.14. Ηλεκτρονική απάτη / phishing

Αφορά την συλλογή η και υποκλοπή προσωπικών στοιχείων και κωδικών για την πλαστογράφηση εγγράφων ταυτοπροσωπίας με σκοπό την παράνομη πρόσβαση σε συστήματα που προσφέρουν χρηματοοικονομικές συναλλαγές η σε οργανισμούς που διαθέτουν δεδομένα προσωπικού χαρακτήρα.

4.3.15. Προγράμματα εκτροπής κλήσεων INTERNET σε γραμμές εξωτερικού με διεθνείς χρεώσεις

Η δραστηριότητα τους περνά απαρατήρητη από τον απλό χρήστη, μέχρι αυτός να λάβει τον τηλεφωνικό λογαριασμό στον οποίο εμφανίζονται οι υπέρογκες χρεώσεις. Ενεργοποιούνται αυτόματα με απλή επίσκεψη του χρήστη σε ιστοσελίδες συνήθως ερωτικού ενδιαφέροντος.

4.3.16. Πνευματικά δικαιώματα

Συγγενικά, με το δικαίωμα της πνευματικής ιδιοκτησίας, δικαιώματα είναι τα δικαιώματα των ερμηνευτών ή των εκτελεστών καλλιτεχνών, των παραγωγών υλικών φορέων και των ραδιοτηλεοπτικών οργανισμών. (αυτά ορίζονται με το νόμο 2121/1993).

Ως πνευματικό έργο νοείται κάθε πρωτότυπο πνευματικό δημιούργημα λόγου, τέχνης ή επιστήμης, που εκφράζεται με οποιαδήποτε μορφή, ιδίως τα γραπτά ή προφορικά κείμενα, οι μουσικές συνθέσεις, με κείμενο ή χωρίς, τα θεατρικά έργα, με μουσική ή χωρίς, οι χορογραφίες και οι παντομίμες, τα οπτικοακουστικά έργα, τα έργα των εικαστικών τεχνών, στα οποία περιλαμβάνονται τα σχέδια, τα έργα ζωγραφικής και γλυπτικής, τα

χαρακτικά έργα και οι λιθογραφίες, τα αρχιτεκτονικά έργα, οι φωτογραφίες, τα έργα των εφαρμοσμένων τεχνών, οι εικονογραφήσεις, οι χάρτες, τα τρισδιάστατα έργα που αναφέρονται στη γεωγραφία, την τοπογραφία, την αρχιτεκτονική ή την επιστήμη.

Νοούνται επίσης ως πνευματικά έργα οι μεταφράσεις, οι διασκευές, οι προσαρμογές και οι άλλες μετατροπές έργων ή εκφράσεων της λαϊκής παράδοσης, καθώς και οι συλλογές έργων ή συλλογές εκφράσεων της λαϊκής παράδοσης ή απλών γεγονότων και στοιχείων, όπως οι εγκυκλοπαίδειες, και οι ανθολογίες (και οι βάσεις δεδομένων), εφόσον η επιλογή ή η διευθέτηση του περιεχομένου τους είναι πρωτότυπη. Η προστασία των έργων αυτών γίνεται με την επιφύλαξη των δικαιωμάτων στα προϋπάρχοντα έργα, που χρησιμοποιήθηκαν ως αντικείμενο των μετατροπών ή των συλλογών. Ουσιαστικά τα πνευματικά έργα αποτελούν περιουσιακό στοιχείο και η τυχόν χρήση χωρίς άδεια επισύρει κυρώσεις

4.3.17. Προσβολή της προσωπικότητας - δυσφήμηση

Παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων αποτελεί η δυσφήμηση μέσω του διαδικτύου. Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο Διαδίκτυο προστατεύεται από την ελληνική νομοθεσία βάσει των σχετικών διατάξεων για την εξύβριση και τη δυσφήμηση.

4.3.18. Νέα Ηλεκτρονική απάτη

Απάτη δεκάδων εκατομμυρίων ευρώ σε βάρος ανυποψίαστων χρηστών του διαδικτύου εντόπισε η Ασφάλειας Αττικής από εταιρία παροχής υπηρεσιών διαδικτύου, η οποία, με ειδικό λογισμικό, υπερχρέωνε τους επισκέπτες μεγάλων σε επισκεψιμότητα ιστοσελίδων .

Οι χρήστες χρεώνονταν παράνομα, περισσότερα από 200 ευρώ την ώρα, όπως ανακοίνωσε η Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος. Έχει ήδη συλληφθεί ο ιδιοκτήτης της μίας εταιρίας, ενώ κατηγορίες απαγγέλθηκαν κατά του ιδιοκτήτη της δεύτερης. Εγκέφαλος της απάτης, φέρεται 57χρονος εκδότης, που συνελήφθη, ενώ οι αρχές εξετάζουν αν στην όλη υπόθεση

εμπλέκεται και ιδιωτική εταιρία παροχής υπηρεσιών τηλεφωνίας. Θύματα των επιτήδειων υπήρξαν Υπουργεία, φορείς του Δημοσίου, ανύποπτοι χρήστες αλλά και αξιωματικοί της Αστυνομίας.[75]

4.3.19. Κυβερνοσφετερισμός

Κυβερνοσφετερισμός είναι η χρησιμοποίηση από ορισμένους χρήστες για εμπορικούς σκοπούς ονομάτων χώρου (domain names) που περιέχουν την επωνυμία γνωστών επιχειρήσεων ή σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νομίμων δικαιούχων και αποκλεισμός τους από τη χρήση του Διαδικτύου με την επωνυμία τους. Ανάλογα με το αν το domain name είναι όνομα, εμπορική επωνυμία ή σήμα, παρέχεται η ανάλογη προστασία από την ελληνική νομοθεσία.

4.3.20. Αλλοίωση ή διαγραφή δεδομένων με ιούς

Οι ιοί των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος, ενώ υπάρχει και υποχρέωση αποζημίωσης κατά τις διατάξεις του Αστικού Κώδικα περί αδικοπραξίας. Παράλληλα, ο υπαίτιος υπέχει και ποινική ευθύνη για φθορά ξένης ιδιοκτησίας.

4.3.21. Δικαιοδοσία στο Internet

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος

[75] Βλ., στο www.fatsimare.net

τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος έχουν υποστηριχθεί τέσσερις θεωρίες.

Η κρατούσα θεωρία στην Ελλάδα και στην Ευρώπη είναι η θεωρία του «βαρύνοντος τόπου». Σύμφωνα με αυτή, ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

5. ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

5.1. Ορισμός

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

5.2. Δικαιώματα Πνευματική Ιδιοκτησίας

Πνευματική ιδιοκτησία είναι το δικαίωμα ιδιοκτησίας ιδεών, προϊόντων του πνεύματος καθώς και ο έλεγχος της υλικής ή εικονικής παρουσίασης αυτών των ιδεών ή προϊόντων. Το λογισμικό είναι πνευματική ιδιοκτησία, όπως είναι τα βιβλία, οι ταινίες και η μουσική. Όπως οι μουσικοί και οι συγγραφείς, οι παραγωγοί λογισμικού χρησιμοποιούν τους νόμους πνευματικής ιδιοκτησίας για να προστατέψουν την δουλειά τους και τις επενδύσεις τους σε αυτόν τον τομέα. Η κλοπή πνευματικής ιδιοκτησίας αποτελεί φραγμό στην ανάπτυξη του κλάδου, την έρευνα και ανάπτυξη νέων προϊόντων και αποθαρρύνει νέες εταιρείες να εισέλθουν σ' αυτόν.

5.3. Μορφές Πειρατείας

Υπάρχουν πέντε κοινοί τύποι πειρατείας λογισμικού. Η κατανόηση κάθε ενός εξ αυτών θα βοηθήσει τους χρήστες να αποφύγουν προβλήματα που σχετίζονται με το παράνομο λογισμικό.

Α) *Πειρατεία Τελικού Χρήστη*:

Πρόκειται για την περίπτωση κατά την οποία ο υπάλληλος μιας εταιρείας αναπαράγει αντίτυπα λογισμικού χωρίς εξουσιοδότηση. Η πειρατεία τελικού χρήστη μπορεί να λάβει τις ακόλουθες μορφές:

- Χρησιμοποίηση ενός νόμιμου αντίγραφου για την εγκατάσταση ενός προγράμματος σε πολλούς υπολογιστές
- Αντιγραφή δίσκων για εγκατάσταση και διανομή
- Εκμετάλλευση προσφορών αναβάθμισης χωρίς νόμιμο αντίγραφο της έκδοσης που πρόκειται να αναβαθμιστεί
- Απόκτηση ακαδημαϊκού ή άλλου λογισμικού περιορισμένης χρήσης που δεν κυκλοφορεί στη λιανική αγορά, χωρίς άδεια για εμπορική χρήση
- Αντιμετάθεση (ανταλλαγή) δίσκων εντός ή εκτός του χώρου εργασίας.

Β) *Κατάχρηση Πελάτη-Διακομιστή*:

Πρόκειται για την περίπτωση κατά την οποία πολλοί υπάλληλοι σε ένα δίκτυο χρησιμοποιούν ταυτοχρόνως ένα κεντρικό αντίγραφο ενός προγράμματος. Εάν διαθέτετε ένα τοπικό δίκτυο (LAN) και εγκαταστήσετε προγράμματα στον διακομιστή τα οποία μπορούν να χρησιμοποιούν πολλοί χρήστες, θα πρέπει να βεβαιωθείτε ότι η άδειά σας επιτρέπει κάτι τέτοιο. Εάν οι χρήστες υπερβαίνουν τον επιτρεπόμενο από την άδεια αριθμό, υπάρχει «κατάχρηση».

5.3.1. Πειρατεία στο Internet

Πρόκειται για την περίπτωση κατά την οποία γίνεται «φόρτωση» (download) λογισμικού από το Internet. Για την online αγορά λογισμικού θα πρέπει να ισχύουν οι ίδιοι κανόνες αγοράς με εκείνους που αφορούν την αγορά με παραδοσιακούς τρόπους. Η πειρατεία στο Internet μπορεί να λάβει τις ακόλουθες μορφές:

- Πειρατικοί δικτυακοί τόποι (websites) που διαθέτουν λογισμικό για δωρεάν φόρτωση (download) ή ως αντάλλαγμα σε χρήστες που έχουν «τοποθετήσει / ανεβάσει» προγράμματα στο συγκεκριμένο site.
- Sites δημοπρασιών που υπάρχουν στο Internet και τα οποία προσφέρουν πλαστά, εκτός καναλιού μεταπωλητών λογισμικά που υπάρχουν κατά παράβαση των πνευματικών δικαιωμάτων
- Ομότιμα δίκτυα (Peer-to-Peer networks) που δίνουν τη δυνατότητα μη εξουσιοδοτημένης μεταφοράς προγραμμάτων με κατοχυρωμένα πνευματικά δικαιώματα.

5.3.2. Εγκατάσταση στο Σκληρό Δίσκο

Πρόκειται για την περίπτωση κατά την οποία μια επιχείρηση που ασχολείται με την πώληση νέων υπολογιστών, εγκαθιστά παράνομα αντίγραφα λογισμικού στους σκληρούς δίσκους για να κάνει την αγορά των μηχανημάτων πιο ελκυστική. Οι ίδιες ανησυχίες αφορούν και στους Μεταπωλητές Προστιθέμενης Αξίας (VAR) που πωλούν ή εγκαθιστούν νέο λογισμικό στους υπολογιστές μέσα στους χώρους εργασίας.

5.3.3. Πλαστογραφία Λογισμικού

Αυτός ο τύπος πειρατείας είναι η παράνομη αντιγραφή και πώληση πνευματικά κατοχυρωμένου υλικού με πρόθεση την άμεση μίμηση του πνευματικά κατοχυρωμένου προϊόντος. Στην περίπτωση του συσκευασμένου λογισμικού, αποτελούν σύνηθες φαινόμενο τα πλαστά αντίγραφα των CD ή των δισκετών που περιλαμβάνουν προγράμματα λογισμικού, καθώς και

σχετικές συσκευασίες, εγχειρίδια, άδειες εκμεταλλεύσεως, εμπορικά σήματα, κάρτες εγγραφής και χαρακτηριστικά ασφαλείας.

5.4. Περιστατικά Πειρατείας Λογισμικού

5.4.1. Επτά χρόνια καταδίκη για πειρατεία λογισμικού

Ο ιδιοκτήτης ενός Web site, μέσω του οποίου διακινούνταν παράνομο λογισμικό, καταδικάστηκε σε πάνω από 7 χρόνια φυλάκισης. Πρόκειται για τη μεγαλύτερη ποινή που έχει επιβληθεί ποτέ στα χρονικά για ανάλογο αδίκημα. Συγκεκριμένα, ο Nathan Peterson, 27 χρονών, κάτοικος Los Angeles, πωλούσε πνευματικά προστατευόμενο software σε ιδιαίτερα χαμηλές τιμές μέσω του Web site του [του iBackups.net]. Το FBI άρχισε να ερευνά το site το 2003 και το έκλεισε τελικά το Φεβρουάριο του 2005.

Το δικαστήριο επέβαλε στον Peterson να καταβάλει αποζημιώσεις άνω των 5,4 εκατομμυρίων δολαρίων. Ο Peterson αποδέχτηκε την ενοχή του για δύο κατηγορίες (παραβίαση copyright και παράνομη αντιγραφή και μεταπώληση software αξίας μεγαλύτερης των 20 εκατομμυρίων δολαρίων). Το υπουργείο Δικαιοσύνης των ΗΠΑ και η βιομηχανία χαρακτήρισαν τη δίκη ως μια από τις μεγαλύτερες υποθέσεις πειρατείας software. Τον προηγούμενο μήνα, καταδικάστηκε για ανάλογη περίπτωση σε έξι χρόνια φυλάκισης ο Danny Ferrer.

Η πειρατεία λογισμικού προκάλεσε στις εταιρείες software απώλειες ύψους 34 δισ. δολαρίων, μια αύξηση κατά 1,6 δισ. σε σχέση με το 2004, σύμφωνα με μελέτη της Business Software Alliance.

5.5. Πειρατεία & Νόμος

5.5.1. Τι λέει ο νόμος σχετικά με την πειρατεία λογισμικού;

Οι περισσότεροι άνθρωποι δε θα σκέφτονταν ποτέ να κλέψουν κάτι που δεν τους ανήκει. Ωστόσο, όσοι αντιγράφουν λογισμικό χωρίς εξουσιοδότηση, στην ουσία, κλέβουν την ιδιοκτησία κάποιου άλλου, την πνευματική του ιδιοκτησία. Και παραβαίνουν το νόμο.

Μπορεί να μην το συνειδητοποιείτε αλλά η ανάπτυξη λογισμικού είναι μία ομαδική προσπάθεια που συνδυάζει τις δημιουργικές ιδέες και το ταλέντο προγραμματιστών, συγγραφέων και σχεδιαστών. Έτσι, όπως και με όλες τις δημιουργικές εργασίες, όπως είναι τα βιβλία, η μουσική και οι κινηματογραφικές ταινίες, το λογισμικό υπολογιστών προστατεύεται από τους ελληνικούς νόμους περί πνευματικών δικαιωμάτων.

Όταν αγοράζετε λογισμικό, δεν γίνεστε ο κάτοχος των πνευματικών δικαιωμάτων. Αγοράζετε το δικαίωμα χρήσης του λογισμικού κάτω από κάποιους περιορισμούς που θέτει ο κάτοχος των πνευματικών δικαιωμάτων, συνήθως ο εκδότης του λογισμικού. Οι ακριβείς κανονισμοί περιγράφονται στην τεκμηρίωση που συνοδεύει το λογισμικό: στην άδεια χρήσης. Είναι σημαντικό να κατανοήσετε και να τηρήσετε αυτούς τους κανονισμούς. Συνήθως, αναφέρουν ότι έχετε το δικαίωμα να φορτώσετε το λογισμικό σε έναν υπολογιστή και να κάνετε ένα αντίγραφο ασφαλείας. Εάν αντιγράψετε, διανείμετε ή εγκαταστήσετε το λογισμικό με τρόπους αντίθετους με όσα αναφέρονται στην άδεια χρήσης, δηλαδή είτε ανταλλάσσετε δίσκους με φίλους και συνάδελφους, είτε συμμετέχετε σε ευρεία αντιγραφή, παραβαίνετε την ομοσπονδιακή νομοθεσία περί πνευματικών δικαιωμάτων. Ακόμα και αν απλά βοηθήσετε κάποιον να δημιουργήσει μη εξουσιοδοτημένα αντίγραφα, είστε υπεύθυνοι σύμφωνα με την νομοθεσία περί πνευματικών δικαιωμάτων.

Πολλές επιχειρήσεις, μικρές και μεγάλες, αντιμετωπίζουν σοβαρούς νομικούς κινδύνους εξαιτίας της πειρατείας λογισμικού. Σύμφωνα με το νόμο, μία εταιρία μπορεί να θεωρηθεί υπεύθυνη για τις πράξεις των εργαζομένων της. Εάν ένας εργαζόμενος εγκαταστήσει μη εξουσιοδοτημένα αντίγραφα λογισμικού σε εταιρικούς υπολογιστές ή αγοράσει παράνομο λογισμικό μέσω του Internet, η εταιρία μπορεί να μηνυθεί για παραβίαση των πνευματικών δικαιωμάτων. Αυτό ισχύει ακόμα και αν η Διοίκηση της εταιρίας δε γνώριζε τις πράξεις των εργαζομένων.

Η δημιουργία ή λήψη (download) μη εξουσιοδοτημένων αντιγράφων λογισμικού είναι παράνομη, ανεξάρτητα από τον αριθμό των αντιγράφων. Είτε κάνετε μερικά αντίγραφα για φίλους, δανείζετε δίσκους, διανέμετε και/ή

κατεβάζετε πειρατικό λογισμικό μέσω του Internet, είτε αγοράζετε μία άδεια χρήσης ενός προϊόντος και το εγκαθιστάτε σε 100 υπολογιστές της εταιρίας, παραβιάζετε τη νομοθεσία. Δεν έχει σημασία αν θα κερδίσετε χρήματα από αυτό ή όχι, είστε εκτεθειμένοι σε σημαντικές αστικές και πιθανόν και ποινικές ποινές. Για παράδειγμα, όσοι χρησιμοποιούν το Internet για να αναφέρουν, πωλήσουν ή διανείμουν πειρατικό λογισμικό ή παράνομα αντίγραφα λογισμικού μέσα από online δημοπρασίες και τοποθεσίες "warez" μπορεί να διωχτούν ποινικά, ακόμα και αν δεν κερδίζουν χρήματα από αυτήν την παράνομη δραστηριότητα.

5.5.2.Τι προβλέπει η νομοθεσία;

Στην Ελλάδα τα προγράμματα ηλεκτρονικών υπολογιστών αποτελούν αντικείμενο προστασίας του ν. 2121/93 για την πνευματική ιδιοκτησία. (άρθρο 2 παρ. 3 εδ. α)

5.5.3. Δικαιούχοι των δικαιωμάτων επί του λογισμικού

Εταιρείες παραγωγής λογισμικού ως ειδικοί διάδοχοι των δικαιωμάτων επί των προγραμμάτων, βάσει αυτοδικαίας ή συμβατικής μεταβίβασης των πρωτογενώς αποκτημένων από τους μισθωτούς ή τους εργολήπτες δικαιωμάτων. (άρθρο 40 του ν. 2121/93) Εφαρμογή του τεκμηρίου του άρθρου 10, παρ. 2 του ν.2121/93, ότι τεκμαίρετε ως δικαιούχος της πνευματικής ιδιοκτησίας σε προγράμματα Η/Υ, το νομικό πρόσωπο, του οποίου το όνομα ή επωνυμία εμφανίζεται πάνω στον υλικό φορέα του έργου, κατά τον τρόπο, που συνήθως χρησιμοποιείται για την ένδειξη του δικαιούχου.

5.5.4. Περιουσιακά δικαιώματα των Δικαιούχων των δικαιωμάτων

Εξουσία αναπαραγωγής (εγκατάσταση προγράμματος σε Η/Υ, εγγραφή του προγράμματος σε μαγνητικά ή οπτικά αποθηκευτικά μέσα, όπως δίσκους, δισκέτες, CD, κ.λ.π) Δικαίωμα θέσης του προγράμματος ή αντιγράφων του σε κυκλοφορία (διανομή, εμπορία).

5.6. Ποιες είναι οι κυρώσεις;

5.6.1. Αστικές κυρώσεις (άρθρο 65 του ν.2121/93)

Ο δικαιούχος μπορεί να αξιώσει την αναγνώριση του δικαιώματός του, την άρση της προσβολής, την παράλειψή της στο μέλλον καθώς και αποζημίωση που δεν μπορεί να είναι κατώτερη από το διπλάσιο του οικονομικού ανταλλάγματος που ο παραβάτης θα πλήρωνε, εάν προμηθευόταν νόμιμα την άδεια για την χρήση του προγράμματος.

5.6.2. Ποινικές κυρώσεις (άρθρο 66 του ν.2121/93)

Ο παραβάτης τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή 1 έως 5 εκατομμυρίων δραχμών. Εάν η ζημία που υπέστη ο δικαιούχος είναι ιδιαίτερα μεγάλη, επιβάλλεται φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή 2 έως 10 εκατομμυρίων δραχμών.

5.6.3. Ποινικές κυρώσεις (άρθρο 66 του ν.2121/93)

Αν ο υπαίτιος τελεί τις παραπάνω πράξεις κατ' επάγγελμα ή αν οι περιστάσεις κάτω από τις οποίες έγινε η πράξη μαρτυρούν ότι ο υπαίτιος είναι ιδιαίτερα επικίνδυνος για την προστασία της πνευματικής ιδιοκτησίας ή των συγγενικών δικαιωμάτων, επιβάλλεται κάθειρξη μέχρι 10 ετών και χρηματική ποινή 5 έως 20 εκατομμυρίων δραχμών, καθώς και αφαίρεση της άδειας λειτουργίας της επιχείρησης στα πλαίσια της οποίας τελέσθηκε η πράξη. Θεωρείται ότι η πράξη έχει τελεσθεί κατ' επάγγελμα και όταν ο δράστης έχει καταδικασθεί για αδικήματα προσβολής πνευματικής ιδιοκτησίας με αμετάκλητη απόφαση σε ποινή στερητική της ελευθερίας.

5.6.4. Διοικητικές κυρώσεις (άρθρο 65Α του ν.2121/93)

Όποιος χωρίς δικαίωμα και κατά παράβαση των διατάξεων του παρόντος νόμου αναπαράγει, πωλεί ή κατ' άλλον τρόπο διανέμει στο κοινό ή κατέχει με σκοπό διανομής πρόγραμμα ηλεκτρονικού υπολογιστή, ανεξαρτήτως άλλων κυρώσεων, υπόκειται σε διοικητικό πρόστιμο ίσο με χίλια (1.000) ευρώ για κάθε παράνομο αντίτυπο προγράμματος ηλεκτρονικού υπολογιστή. Αρμόδιες για τον έλεγχο της εφαρμογής των διατάξεων του παρόντος νόμου και την επιβολή των προβλεπόμενων κυρώσεων είναι η

Υπηρεσία Ειδικών Ελέγχων (ΥΠ.Ε.Ε.), οι Αστυνομικές και Τελωνειακές Αρχές, οι οποίες μετά τη διαπίστωση της παράβασης, ενημερώνουν τους δικαιούχους μέσω του Οργανισμού Πνευματικής Ιδιοκτησίας. Σε περίπτωση υποτροπής εντός του αυτού οικονομικού έτους το διοικητικό πρόστιμο που προβλέπεται στο άρθρο 65Α διπλασιάζεται.

5.7. Ποιες είναι οι ευθύνες ενός χρήστη λογισμικού;

Η πρώτης σας ευθύνη ως χρήστης λογισμικού είναι η αγορά νόμιμων προϊόντων λογισμικού. Όταν αγοράζετε λογισμικό, να βεβαιώνεστε ότι λαμβάνετε γνήσιους δίσκους, εγχειρίδια και έγγραφα άδειας χρήσης. Αποφύγετε δίσκους με χειροποίητες ετικέτες ή λογισμικό που η τιμή του είναι «πολύ καλή για να είναι αληθινή». Προσέχετε τους αδίστακτους προμηθευτές στο Internet, οι οποίοι διαφημίζουν ελκυστικές τιμές «γνήσιου» λογισμικού το οποίο έχει μείνει στο στοκ τους ή δίνεται με έκπτωση για λόγους απογραφής. Έχετε υπόψη σας ότι ένα υψηλό ποσοστό λογισμικού που πωλείται μέσω online δημοπρασιών είναι παράνομο.

Έχετε την ευθύνη εγκατάστασης και χρήσης του λογισμικού, σύμφωνα με τους όρους της άδειας χρήσης. Αυτά τα συμφωνητικά διαφέρουν από εκδότη σε εκδότη και πρέπει να τα διαβάζετε προσεκτικά. Εάν κάποιος άλλος εγκαταστήσει το λογισμικό, βεβαιωθείτε ότι θα σας παρέχει και απόδειξη ότι το προϊόν έχει τη νόμιμη άδεια χρήσης. Εάν έχετε αναθέσει τις εργασίες σε εξωτερικό συνεργάτη, εξακολουθείτε να είστε υπεύθυνος για τη συμμόρφωση με τους όρους της άδειας χρήσης του λογισμικού.

Η πειρατεία λογισμικού δεν είναι ένα έγκλημα χωρίς θύμα. Η πειρατεία στερεί από το δημιουργό λογισμικού τα έσοδα που δικαιούται και είναι επιβλαβής για τους καταναλωτές και την αγορά συνολικά. Όλοι οι δημιουργοί λογισμικού, μικροί και μεγάλοι, ξοδεύουν χρόνο για τη δημιουργία του λογισμικού. Ένα τμήμα των χρημάτων που ξοδεύετε για την αγορά πρωτότυπου λογισμικού επιστρέφει για την έρευνα και την ανάπτυξη, έτσι ώστε να μπορεί να παραχθεί νεότερο και πιο εξελιγμένο λογισμικό. Όταν αγοράζετε παράνομα αντίγραφα, τα χρήματά σας πηγαίνουν κατευθείαν στην τσέπη των παραβατών.

5.8.Ποιες είναι οι επιπτώσεις της πειρατείας λογισμικού;

Σύμφωνα με τη Διεθνή Μελέτη για το έτος 2005 σχετικά με την πειρατεία λογισμικού παγκοσμίως, που πραγματοποιήθηκε σε 97 χώρες από την IDC (International Data Corporation), το ποσοστό πειρατείας παρέμεινε σταθερό (**35**%). Η Ελλάδα, κατατάσσεται για τρίτη συνεχή χρονιά στην πρώτη θέση ανάμεσα στις χώρες της διευρυμένης Ευρωπαϊκής Ένωσης με ποσοστό πειρατείας **64**%, σημειώνοντας οικονομικές απώλειες της τάξης των 135 εκ Ευρώ ($157 εκ.).

Ανεπτυγμένες αγορές όπως η Αμερική, η Δυτική Ευρώπη, η Ιαπωνία και ορισμένα ασιατικά κράτη εξακολουθούν να κυριαρχούν στην αγορά λογισμικού, με το μεικτό ποσοστό πειρατείας να παραμένει σχεδόν αμετάβλητο. Σε περισσότερες από τις μισές (51) η πειρατεία μειώθηκε και σε μόνο 19 χώρες παρουσιάστηκε αύξηση. Οι οικονομικές απώλειες που σημειώνονται από την πειρατεία λογισμικού σε παγκόσμιο επίπεδο είναι της τάξεως των $34 δις, παρουσιάζοντας αύξηση της τάξεως των $1,6 δις από το 2004.

Ο τομέας της πληροφορικής κατευθυνόμενος από τη βιομηχανία λογισμικού, είναι ένας από τους ταχύτατα αναπτυσσόμενους και πιο ζωτικούς τομείς της παγκόσμιας οικονομίας. Μία υγιής βιομηχανία πληροφορικής αποτελεί το θεμέλιο της εθνικής οικονομικής ευημερίας. Σύμφωνα με τη διεθνή μελέτη της IDC επενδύοντας στην προστασία της Πνευματικής Ιδιοκτησίας και μειώνοντας την πειρατεία κατά 10 ποσοστιαίες μονάδες η παγκόσμια οικονομία θα ωφεληθεί:

- εκατομμύρια θέσεις εργασίας
- $67 δις σε φορολογικά έσοδα
- $400 δις σε οικονομική ανάπτυξη

Σε διεθνή μελέτη που εκπονήθηκε από την IDC (Δεκ. 2005) ειδικά για την Ελλάδα, διαπιστώθηκε ότι ο αναπτυσσόμενος κλάδος της πληροφορικής

θα μπορούσε να παρουσιάσει αύξηση έως και 60% σε διάστημα 5 ετών, εάν η πειρατεία μειωνόταν κατά 10 ποσοστιαίες μονάδες. Η εν λόγω μελέτη που επικεντρώθηκε στις επιπτώσεις της μείωσης στην πειρατεία λογισμικού στις εθνικές οικονομίες 70 κρατών, κατέληξε στο συμπέρασμα ότι στην Ελλάδα θα μπορούσε να ενισχυθεί το ΑΕΠ της χώρας κατά 411 εκατ. δολάρια (340 εκατ. ευρώ), να αυξηθούν τα φορολογικά εισοδήματα κατά 130 εκατ. δολάρια (108 εκατ. ευρώ) και τα έσοδα της βιομηχανίας πληροφορικής τουλάχιστον κατά 261 εκατ. δολάρια (218 εκατ. ευρώ). Όσον αφορά στην αγορά εργασίας, θα μπορούσε μέσα σε μια 5ετία να δημιουργήσει 1.300 νέες θέσεις στον κλάδο της πληροφορικής.

Στη μελέτη της IDC για λογαριασμό της BSA που πραγματοποιήθηκε για το έτος 2005 και αναφέρεται στις οικονομικές επιπτώσεις της πειρατείας λογισμικού αναφέρεται ότι ο κλάδος πληροφορικής στην Ελλάδα υποστηρίζει σήμερα σχεδόν 4.500 εταιρίες τεχνολογίας, απασχολεί περίπου 28.000 εργαζόμενους ενώ εισφέρει στην οικονομία φορολογικά έσοδα της τάξεως των 1.6 δισ. ευρώ (1.9 δισ. δολάρια). Η τοπική βιομηχανία λογισμικού αποτιμάται σε 191 εκατομμύρια ευρώ (224 εκ δολάρια). Σύμφωνα με τη μελέτη μείωση 10 ποσοστιαίων μονάδων της πειρατείας λογισμικού στην Ελλάδα από το 2006 έως το 2009 θα έχει ως αποτέλεσμα:

- **1.300** νέες θέσεις εργασίας
- **351 εκ. ευρώ** (411 εκ δολάρια) στο ΑΕΠ
- **Αύξηση των φορολογικών εσόδων** κατά 111 εκ. ευρώ (130 εκ. δολάρια)

Ενίσχυση της 5ετούς ανάπτυξης του κλάδου πληροφορικής από 53% σε 60% έως το 2009, αυξάνοντας τον κύκλο εργασιών του από 1.8 δις ευρώ (2.1 δις δολάρια) που είναι σήμερα σε 2.9 δις ευρώ (3.4 δις δολάρια). Η αύξηση αυτή ισοδυναμεί με ανάπτυξη κατά 8,9% ετησίως

5.9. Ποια είναι η δέσμευση του Κράτους απέναντι στο νόμιμο λογισμικό;

Στα παραπάνω ζητήματα τόσο η Ευρωπαϊκή Ένωση όσο και τα κράτη μέλη της δεν έμειναν αδιάφορα. Έχει δημιουργηθεί και θεσμοθετηθεί ένα νομικό πλαίσιο ιδιαίτερα αυστηρό που διασφαλίζει απολύτως την προάσπιση των πνευματικών δικαιωμάτων των δημιουργών.

Η Δημόσια Διοίκηση συμβάλλοντας με τη σειρά της στην καταπολέμηση της πειρατείας εξέδωσε την εγκύκλιο ΥΑΠ/Φ.00/5273 του 1997, με θέμα «Παράνομη χρήση λογισμικού» του τότε Υπουργού Εσωτερικών κ. Αλέξανδρου Παπαδόπουλου. Με την εγκύκλιο αυτή έγιναν σημαντικά βήματα στη διασφάλιση της χρήσης νόμιμου λογισμικού στους Δημόσιους οργανισμούς αφού υπήρξαν βασικές αλλαγές στις προδιαγραφές αγορών εξοπλισμού πληροφορικής έτσι ώστε αυτές να είναι σύμφωνες με τους νόμους περί προστασίας της πνευματικής ιδιοκτησίας.

Σύνοψη

Έχει γίνει σαφές οτι η απεριόριστη χρήση των ηλεκτρονικών υπολογιστών και η λειτουργία του διαδικτύου δίνουν απεριόριστες δυνατότητες και συμβάλλουν στην οικονομική ανάπτυξη των κρατών. Μέσω, όμως της δυναμικής τους εισβολής, αναπτύσσονται τεράστιες δυνατότητες χρήσης και κατάχρησης που αφορούν την ηλεκτρονική επεξεργασία δεδομένων. Η ηλεκτρονική εγκληματικότητα συνεχώς εμπλουτίζεται και η πιθανότητα εμφάνισης νέων μορφών στο μέλλον, επιβάλλουν τη συντομότερη αντιμετώπιση του θέματος, την πραγματοποίηση συλλογικής προσπάθειας και διασυνοριακής συνεργασίας καθώς και την κατάλληλη τεχνολογική υποδομή σε συνδυασμό με την αντίστοιχη νομοθεσία ούτως ώστε να υπάρχει πραγματική απονομή δικαιοσύνης.

Β' Μέρος – Νέες μορφές ηλεκτρονικών εγκλημάτων

Τα πλέον συνηθισμένα εγκλήματα που παρουσιάζονται αυτή την στιγμή στον κυβερνοχώρο είναι: Οι απάτες (με πιστωτικές κάρτες ή μη), η διακίνηση παιδικής πορνογραφίας, εγκλήματα κατά της Εθνικής Ασφάλειας (οδηγίες για κατασκευή βομβών, εισβολή σε συστήματα ασφαλείας, που έχουν σχέση με την εθνική υποδομή), οδηγίες για παρασκευή ναρκωτικών. Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των προσωπικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον περιουσιακών αγαθών. Στη συνέχεια παρουσιάζονται ορισμένες νέες μορφές ηλεκτρονικών εγκλημάτων που η μορφή τους θα λέγαμε δανείζεται πολλά στοιχεία από τα κοινά εγκλήματα που παρουσιάζονται στην εγκληματολογική επιστήμη.

1. Αυτοκτονίες

Πολλές μελέτες έχουν αποδείξει τη στενή σχέση μεταξύ της προβολής θεμάτων σχετικών με την αυτοκτονία στα ΜΜΕ με αύξηση του ποσοστού αυτοκτονιών. Το Διαδίκτυο δεν διαφέρει σε αυτό από τα άλλα μέσα.

Το φαινόμενο, των αυτοκτονιών που έχουν οργανωθεί μέσω του Διαδικτύου και εκτελούνται στη διάρκεια του Σαββατοκύριακου, αυξάνεται με ραγδαίους ρυθμούς στην Ιαπωνία κι αποδίδεται στην επιρροή που έχει η τεχνολογία των μέσων στην ψυχολογία των σύγχρονων ανθρώπων.

Περιστατικά αυτοκτονίας μέσω chat-room έχουν αναφερθεί στην Ιαπωνία, στην Αυστραλία, τη Νορβηγία, τη Κορέα και και τις ΗΠΑ.

2. Ηλεκτρονικός Τζόγος

Πολλά παιδιά απολαμβάνουν να χρησιμοποιούν τον Ιστό για να ανακαλύπτουν δραστηριότητες ψυχαγωγίας, όπως τα Διαδικτυακά παιχνίδια. Πολλές φορές, ενώ αναζητούν μια νέα ιστοσελίδα με παιχνίδια μπορεί να βρουν ιστοσελίδες με στοιχήματα και τυχερά παιχνίδια.

Ο τζόγος, ο οποίος αφορά στα τυχερά παιχνίδια, στοιχήματα, καζίνα κ.τ.λ, γίνεται πιο σοβαρός τώρα που μπαίνει μέσα στο σπίτι μας με τη μορφή του Διαδικτυακού τζόγου. Ο τζόγος, και κυρίως ο Διαδικτυακός, οδηγεί στην εξάρτηση.

Σε κάποιες ακραίες περιπτώσεις, τα πράγματα μπορούν να φτάσουν ως γνωστών στην πτώχευση και την αυτοκτονία, ή έστω στην απόπειρα. Στις περιοχές όπου λειτουργούν καζίνο αυξάνονται κατά πολύ και τα ποσοστά εγκληματικότητας. Οι ιδιαιτερότητες του Διαδικτύου (ανωνυμία, παγκοσμιότητα κ.λ.π.), δυσχεραίνουν τόσο την πρόληψη όσο και την καταστολή του εγκλήματος που γίνεται μέσω αυτού. Μεγάλο μέρος «βρόμικου χρήματος» ξεπλένεται μέσα από τα Διαδικτυακά καζίνο.

3. Διακίνηση – Πώληση Όπλων

Η πώληση όπλων μέσω Διαδικτύου έχει αυξηθεί δραματικά και οι υπεύθυνες αρχές δεν είναι κατάλληλα εξοπλισμένες ώστε να εντοπίζουν τις χιλιάδες πωλήσεις που υπολογίζεται ότι λαμβάνουν χώρα κάθε χρόνο στο Διαδίκτυο. Σε πολλές περιπτώσεις, οι πωλήσεις είναι νόμιμες. Αυτό συμβαίνει γιατί νόμιμοι πωλητές όπλων δε πωλούν άμεσα όπλα στο Διαδίκτυο αλλά στέλνουν τους υποψήφιους αγοραστές σε κατόχους νόμιμων μαγαζιών πώλησης όπλων.

4. Διακίνηση – Πώληση Ναρκωτικών

Στροφή στο Διαδίκτυο πραγματοποίησαν και τα κυκλώματα διακίνησης ναρκωτικών. Αστυνομικοί συνέλαβαν 25χρονο, ο οποίος

χρησιμοποιώντας προγράμματα επικοινωνίας, όπως το <IRC> και το <MSN> έβρισκε πελάτες τους οποίους προμήθευε με κοκαΐνη και κάνναβη. «Ολοένα και περισσότεροι έμποροι τείνουν να χρησιμοποιούν το Διαδίκτυο για τη διακίνηση ουσιών» σχολιάζουν στην «Καθημερινή» αξιωματικοί της Αστυνομίας. «Η αγορά ναρκωτικών ουσιών και φαρμάκων είναι πολύ εύκολη μέσα από το Διαδίκτυο» τονίζουν.

Η αγορά ναρκωτικών ουσιών μέσω Διαδικτύου είναι φυσικά παράνομη. Όμως η απαγόρευση της πώλησης ναρκωτικών ουσιών δεν είναι και τόσο εύκολη υπόθεση. Αυτό γιατί υπάρχουν χώρες όπου έχουν πιο ανεκτικούς νόμους γύρω από το θέμα των ναρκωτικών (π.χ. Ολλανδία).

5. Διακίνηση - Πώληση Φαρμάκων

Τα φορτία φαρμάκων από παράνομα φαρμακεία στο Διαδίκτυο είχαν γίνει τόσο κοινά στην περιοχή των Απαλάχιων Ορέων των ΗΠΑ, που οι τοπικές ταχυδρομικές εταιρίες αναγκάσθηκαν να προσθέσουν επιπλέον φορτηγά για να καλύψουν τις ανάγκες.

Αν και η αστυνομία έχει αντιμετωπίσει σε μεγάλο βαθμό το φαινόμενο της παράνομης διακίνησης φαρμάκων στις ΗΠΑ, αδυνατεί να βρει λύση για το ευρέως διαδεδομένο φαινόμενο της αποστολής φαρμάκων από επιχειρήσεις εκτός Αμερικής.

Για όσους είναι εθισμένοι σε παράνομα παυσίπονα, όπως το κοδεϊνούχο Vicodin, που δεν πωλείται στην Ευρώπη, η λύση του Ίντερνετ είναι ιδανική, καθώς τους απαλλάσσει από την ανάγκη να πληρώνουν επίορκους ιατρούς για να εξασφαλίζουν το ελεγχόμενο φάρμακο.

Η Υπηρεσία Καταπολέμησης των Ναρκωτικών των ΗΠΑ, DEA, εκτιμά ότι ποσοστό 95% των φαρμακευτικών προϊόντων που πωλούνται μέσω Διαδικτύου είναι «δίγραμμα» (υπό καθεστώς πολύ αυστηρής συνταγογράφισης) φάρμακα. Η υπηρεσία ανακάλυψε ότι 34 παράνομα

φαρμακεία του Διαδικτύου πούλησαν το 2006 πάνω από 98,5 εκατομμύρια δόσεις Vicodin.

Οι παράνομες αυτές ιστοσελίδες προσεγγίζουν συνήθως νόμιμα μικρά φαρμακεία, τα οποία πείθουν συχνά με τη χρήση πλαστών εγγράφων να αποστείλουν ταχυδρομικά τα φάρμακα σε πελάτες.

6. Ηλεκτρονικό Εμπόριο

Εκατοντάδες είναι τα θύματα από τις απάτες που αφορούν αποστολή προϊόντων χαμηλής ποιότητας, ενώ πολλά από αυτά δεν φθάνουν ποτέ στους παραλήπτες. Δέκα περιπτώσεις αγοράς αυτοκινήτων μέσω του Διαδικτύου έχουν διαπιστώσει στο τμήμα δίωξης ηλεκτρονικού εγκλήματος. Τα θύματα είχαν καταβάλει από 5.000 ευρώ, αλλά δεν είχαν παραλάβει ποτέ αυτοκίνητο.

7. Μέθοδος Συνοικεσίου (Romance Scam)

Είναι από τις πρόσφατες μεθόδους η οποία αναπτύσσεται γρήγορα. Στην περίπτωση αυτή οι απατεώνες εκμεταλλεύονται την ανάγκη των μοναχικών ανθρώπων να γνωρίσουν τον σύντροφό τους. Αναλαμβάνουν έτσι τον ρόλο του μεσολαβητή μέσω του διαδικτύου. Στην αρχή όλα θα πηγαίνουν καλά μέχρι το κρίσιμο σημείο κατά το οποίο θα ζητήσουν αρχικά κάποιο μικρό ποσό, για να μην ρίξουν υποψίες, για κάποιας μορφής μικροέξοδα. Στην συνέχεια θα ζητήσουν τα έξοδα για το αεροπορικό εισιτήριο της νύφης ή του γαμπρού που τελικά για «κάποιο» λόγο δεν θα ταξιδεύσει.

8.Αγγελίες Δολοφόνων

Ο επικεφαλής του τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος κ. Μανώλης Σφακιανάκης υποστήριξε: «Μέσω διαδικτύου εκτελούνται συμβόλαια θανάτου», αποκαλύπτοντας μια τέτοια περίπτωση σε νοσοκομείο των ΗΠΑ, όπου εκτελέστηκε τέτοιο συμβόλαιο με έξωθεν παρέμβαση στον ηλεκτρονικό υπολογιστή και αλλαγή της φαρμακευτικής αγωγής του θύματος!

«Ζούμε το "τέλος εποχής" και τη μετάλλαξη του εγκλήματος. Πλέον όλες οι εγκληματικές δραστηριότητες, ακόμη και οι ανθρωποκτονίες, λαμβάνουν χώρα μέσω διαδικτύου και στον κυβερνοχώρο», κατέληξε ο κ. Σφακιανάκης.

9. Δημοπρασίες για αντικείμενα που άνηκαν σε διαβόητους δολοφόνους

Έμπνευση του Αμερικανού Τοντ Μποχάνον, ο οποίος δημιούργησε την ιστοσελίδα «murderauction.com», όπου δημοπρατούνται καθημερινά δεκάδες «αναμνηστικά». Για παράδειγμα, πουλήθηκαν τρίχες του Τσαρλς Μάνσον ή έργα που φιλοτέχνησε ο Τζον Γκέισι, ο οποίος τη δεκαετία του 1970 είχε δολοφονήσει 33 άτομα και εκτελέστηκε το 1994. Ο γνωστός οίκος δικτυακών δημοπρασιών eBay, πάντως, απαγόρευσε πρόσφατα την πώληση τέτοιου είδους αντικειμένων μέσα από τις δικές του σελίδες. Η λήψη επιπρόσθετων μέτρων, όμως, είναι αναγκαία, και ειδικότερα όσον αφορά στους μικρότερους χρήστες του Ίντερνετ, τα παιδιά. Η Ευρωπαϊκή Ένωση υιοθέτησε πρόγραμμα δράσης για την ασφαλέστερη χρήση του διαδικτύου από τα παιδιά, ύψους 50 εκατομμυρίων ευρώ, με διάρκεια μέχρι το 2008. Οι τέσσερις βασικοί άξονες του προγράμματος είναι: Καταπολέμηση του παράνομου περιεχομένου, αντιμετώπιση του ανεπιθύμητου και επιβλαβούς περιεχομένου, προώθηση ενός ασφαλέστερου περιβάλλοντος και ευαισθητοποίηση της κοινής γνώμης

10. Όργια με γενική είσοδο 2 (δύο) Ευρώ!

Σύμφωνα με αστυνομικές πήγες, εντοπίστηκε συγκεκριμένη αγγελία στην οποία αναφερόταν πως «στις 10 Δεκεμβρίου διοργανώνεται πάρτι οργίων με γενική είσοδο 2 Ευρώ». Για δυο ολόκληρους μήνες οι αξιωματικοί της Ασφάλειας προσπαθούσαν να βρουν το ηλεκτρονικό αποτύπωμα του δράστη. Έψαχναν δηλαδή μέσω ειδικών προγραμμάτων να εντοπίσουν τις «άστοχες» κινήσεις ανθρώπου που τοποθέτησε την αγγελία. Κι αυτό γιατί οποίος μπαίνει στο Ίντερνετ, αφήνει πίσω του ηλεκτρονικά αποτυπώματα. Όμως, όπως τονίζουν οι αστυνομικοί, ο άνθρωπος αυτός είχε πολύ μεγάλες γνώσεις ηλεκτρονικών υπολογιστών

και ήταν ιδιαίτερα δύσκολος ο εντοπισμός του, καθώς κατάφερνε να εξαφανίζει όλα τα ίχνη του. Ωστόσο οι «on line» αστυνομικοί απέδειξαν ότι είναι ανώτεροι του, αφού εκμεταλλεύτηκαν ένα αποτύπωμα του και κατάφεραν να ξετυλίξουν το κουβάρι της απίστευτης ιστορίας. Μόλις κατάφεραν να βρουν το στίγμα του, με περαιτέρω ψηφιακή έρευνα εντοπίστηκε τελικά ο άνθρωπος που κατάρτισε τη συγκεκριμένη αγγελία και την έθεσε στη διάθεση των χρηστών του Ιντερνετ.

11. Το εμπόριο Ανθρώπων

Δεν υπάρχει ένας συγκεκριμένος ορισμός για το εμπόριο ανθρώπων. Μπορούμε να πούμε ότι κύρια χαρακτηριστικά του είναι η εκμετάλλευση ανθρώπων η οποία περιλαμβάνει μεταφορά, προώθηση, πρόσληψη, υπόθαλψη ή και παράδοσή του σώματος τους, των λειτουργιών του ή και των οργάνων του με την άσκηση κάθε μορφής βίας (ψυχολογικής, σωματικής, κ.λ.π) ή κατάχρηση εξουσίας. Αποτελεί μια σύγχρονη μορφή δουλεμπορίου.

Οι μορφές που παίρνει το εμπόριο ανθρώπων είναι πολυσύνθετες, απαιτούν ιδιαίτερη οργάνωση για τη διεξαγωγή του και είναι σχεδόν πάντα, μορφές οργανωμένου εγκλήματος.

Οι ιδιαίτερες κατηγορίες του εμπορίου ανθρώπων είναι:

- Διακίνηση μεταναστών με σκοπό την οικονομική εκμετάλλευση της μεταφοράς τους. Οι δράστες εκμεταλλεύονται τις δυσκολίες μετακίνησης των μεταναστών που δημιουργούνται από την απόσταση και τα μέτρα αποτροπής που παίρνουν οι χώρες υποδοχής και αναλαμβάνουν ή διευκολύνουν τη μεταφορά εισπράττοντας μεγάλα ποσά από τους μετανάστες.
- Διακίνηση γυναικών με σκοπό τη σεξουαλική εκμετάλλευση. Οι δράστες εκμεταλλεύονται τη ζήτηση σεξουαλικών υπηρεσιών στις χώρες υποδοχής και την προσφορά εργασίας από νέες γυναίκες στις φτωχές χώρες αποστολής.

- Διακίνηση παιδιών με σκοπό τη σεξουαλική εκμετάλλευση ή ακόμη και το εμπόριο οργάνων. Οι δράστες εκμεταλλεύονται τη ζήτηση από ενήλικες για σεξουαλικές υπηρεσίες παιδιών καθώς και τη ζήτηση, συνήθως από πλούσιους ασθενείς, για ανθρώπινα όργανα προς μεταμόσχευση.
- Εκμετάλλευση αλλοδαπών στην προσπάθειά τους να βρουν δουλειά. Συχνά οι δράστες σε συνέχεια της εκμετάλλευσης της μεταφοράς μεταναστών, συνεχίζουν να τους εκμεταλλεύονται στην προσπάθειά τους να έχουν μια θέση εργασίας, παρέχοντας τους προστασία ή διαμεσολάβηση, εκμεταλλευόμενοι την άγνοια της γλώσσας, των τοπικών συνθηκών, της νομοθεσίας κ.λ.π
- Εκμετάλλευση της δουλειάς αλλοδαπών. Στην περίπτωση αυτή συχνά οι δράστες είναι «καθώς πρέπει» εργοδότες, οι οποίοι εκμεταλλεύονται την εργασία μεταναστών, στους οποίους προσφέρουν μειωμένες αμοιβές, δεν τους ασφαλίζουν ή τους αναγκάζουν να εργάζονται κάτω από απάνθρωπες και ανασφαλείς συνθήκες.

Σύμφωνα με εκτιμήσεις, το εμπόριο ανθρώπων αποφέρει παγκόσμια τα μεγαλύτερα κέρδη για τους εγκληματίες, μετά το παράνομο εμπόριο όπλων και ναρκωτικών.

Είναι αναμφίβολα ένα πολυσύνθετο πρόβλημα με πολιτικά και, κοινωνικά χαρακτηριστικά αλλά και με νομικές δικαστικές και αστυνομικές ιδιαιτερότητες. Η κυριότερη ίσως δυσκολία του έγκειται στο γεγονός ότι ως διαδικασία εμπορίου έρχεται να καλύψει μια ιδιότυπη ζήτηση των «προϊόντων» που προσφέρει, η οποία διαχέεται στην καθημερινή κοινωνική ζωή και δύσκολα χαρακτηρίζεται ως εγκληματική συμπεριφορά από το κοινωνικό σύνολο. Η ζήτηση αυτή δημιουργείται από συγκεκριμένες κοινωνικές δομές των αναπτυγμένων χωρών, από την κουλτούρα και την ιδεολογία που έχει διαμορφωθεί σ' αυτές.

12. CYBERBULLING: Η νέα τρομοκρατία που αναπτύσσεται μέσα στο σχολικό περιβάλλον

Cyber bullying είναι οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που θεσπίζεται και πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών επικοινωνίας, συγκεκριμένα του Διαδικτύου και των κινητών τηλεφώνων και η οποία επαναλαμβάνεται ανά τακτά ή άτακτα χρονικά διαστήματα. Ο όρος cyberbulling πλάσθηκε από τον Καναδό Bill Belsey και έχει τις ρίζες του στην παραδοσιακή φυσική ή ψυχολογική φοβέρα όπου ο στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του.

13. Κυβερνοτρομοκρατία

13.1. Ορισμοί

Φέρνοντας στο μυαλό μας την έννοια της τρομοκρατίας σκεπτόμαστε πάντα εικόνες βίας, καταστροφής και θανάτου. Ιστορικά η τρομοκρατία έχει χρησιμοποιηθεί από ομάδες ανθρώπων που λειτουργούσαν για την υποστήριξη ενός κοινού αγώνα ή πιστεύω, προκειμένου να αναγκάσουν ή να εκφοβίσουν ένα στόχο να προβεί σε επιθυμητή δράση. Το FBI έχει αποδώσει ένα ορισμό για την τρομοκρατία σύμφωνα με τον οποίο «Τρομοκρατία είναι η παράνομη χρήση δύναμης ή βίας εναντίον προσώπων ή περιουσίας, με σκοπό τον εκφοβισμό ή τον εξαναγκασμό μιας κυβέρνησης, του αστικού πληθυσμού ή οποιουδήποτε τμήματος του στην προώθηση πολιτικών ή κοινωνικών στόχων».[76]

Είναι πρακτικά αδύνατο για τον καθένα, που ασχολείται με τη διαχείριση και τον έλεγχο της τρομοκρατίας, να προβλέψει πότε και που θα συμβεί κάποιο χτύπημα. Το Ιντερνετ είναι το ιδανικό περιβάλλον για ότι ο Simon Garfinkel, ειδικός στην ασφάλεια συστημάτων και συγγραφέας του *Database Nation: The Death of Privacy in the 21st Century*, αποκαλεί «irrational

[76] Βλ., Furnel, Stev., «Κυβερνοέγκλημα: Καταστρέφοντας την κοινωνία της πληροφορίας», Εκδόσεις Παπαζήση, Αθήνα 2006, σ.326

terrorist» (παράλογος τρομοκράτης).[77] Αντίθετα από εκείνους που επιδιώκουν να χρησιμοποιήσουν τις πράξεις τους, για να προκαλέσουν ένα κοινό χτύπημα ή να επιφέρουν μια επιθυμητή αλλαγή, ο αποκαλούμενος «irrational terrorist» δεν ενδιαφέρεται για διαπραγμάτευση και μπορεί να δρα μόνος του. Στόχος του είναι να προκαλέσει καταστροφή.

Η Dorothy Denning καθηγήτρια πληροφορικής στο Παν/μιο της Γεωργίας, προσθέτει τα παρακάτω στον ορισμό της κυβερνοτρομοκρατίας: «Για να αξιολογήσουμε ως κυβερνοτρομοκρατία ένα χτύπημα, θα πρέπει να έχει βίαιη επίθεση εναντίον προσώπων ή κατά της περιουσίας ή τουλάχιστον, να προκαλεί αρκετό φόβο για ζημιά. Οι επιθέσεις που έχουν ως αποτέλεσμα το θάνατο ή τον τραυματισμό, εκρήξεις, αεροπορικές τραγωδίες, λειψυδρίες ή σοβαρή οικονομική απώλεια αποτελούν παραδείγματα. Σοβαρές επιθέσεις εναντίων σημαντικών μονάδων παραγωγής μπορεί να είναι πράξεις τρομοκρατίας ανάλογα με την επίδρασή τους. Επιθέσεις οι οποίες καταστρέφουν μη απαραίτητες υπηρεσίες ή που συνιστούν ανάλωση χρήματος, δεν είναι κυβερνοτρομοκρατία.»[78]

Από την άλλη πλευρά ο Emmanuel Goldstein σε ένα απόσπασμά του αναφέρει πως «όλο αυτό τον καιρό που βρίσκομαι στη σκηνή, ο οποίος καιρός είναι αρκετός, δεν έχω συναντήσει κάποιον που να τον θεωρώ *κυβερνοτρομοκράτη*, ό,τι κι αν σημαίνει αυτό. Οι περισσότεροι που μιλούν για αυτά τα πλάσματα, είτε θέλουν να πουλήσουν ή να χρεώσουν κάποιον. Δεν λέω ότι αυτό είναι απίθανο. Αλλά πιστεύω ότι οι τρέχουσες συζητήσεις δεν είναι ρεαλιστικές και ότι έχουν πολύ ύποπτα απώτερα κίνητρα».[79]

Η απειλή που προέρχεται από τους κυβερνοτρομοκράτες και τους άλλους on-line τρομοκράτες χρησιμοποιείται από κυβερνήσεις και μυστικές

---

[77] Βλ., Garfinkel, S. 2000. *Database Nation: The Death of Privacy in the 21st Century.*, O' Reilly & Associates, Inc., 211.

[78] Βλ., Denning, D.E. "Cyberterrorism." Testimony before the special Oversight Panel on Terrorism, U.S. House of Representatives, 23 Μαΐου 2000., Βλέπε επίσης στο http://www.terrorism.com/documents/denning-testimony.shtml.

[79] Βλ., "Q&A with Emmanuel Goldstein of 2600: *The Hacker's Quarterly*", CNN.com. http://www.cnn.com/TECH/specials/hackers/gandas/goldstein.html.

υπηρεσίες ως δικαιολογία για το συντονισμό και αποκλεισμό σημαντικών δυνάμεων. Για παράδειγμα, στη Μ.Βρετανία η **M15** κατασκευάζει ένα κέντρο ελέγχου ηλεκτρονικών μυνημάτων, 25 εκ. λιρών με την κυβέρνηση να απαιτεί οι πάροχοι υπηρεσιών Internet να έχουν «harwire» συνδέσεις στο σύστημα, ώστε τα μηχανήματα να μπορούν απευθείας να αποκλειστούν.[80]

13.2. Στόχοι & Σκοποί των «Κυβερνοτρομοκρατών»

Παρά το γεγονός ότι οι Denning και Goldstein είναι δύσπιστοι όσο αφορά την ύπαρξη κυβερνοτρομοκρατών, μπορεί να παρατηρηθεί με βεβαιότητα ότι οι εδραιωμένες ομάδες χρησιμοποιούν καθημερινά το Internet για διάφορους και ποικίλους σκοπούς, όπως περιγράφονται παρακάτω:

- **Προπαγάνδα - Δημοσιότητα**: Οι τρομοκράτες και οι ομάδες αντίστασης παραδοσιακά δυσκολεύονται να στηρίξουν τα πολιτικά τους μηνύματα στη κοινή γνώμη χωρίς να λογοκριθούν. Όμως, τώρα μπορούν να χρησιμοποιούν το Internet γι αυτό το σκοπό, όπως συμβαίνει στην περίπτωση της Ιρλανδικής Υπηρεσίας, Irish Republican Information Service και του κινήματος Zapatista Movement.81
- **Η αύξηση των οικονομικών πόρων**: Κάποιες τρομοκρατικές ομάδες 'η ομάδες αντίστασης, που έχουν διασυνδέσεις με τα πολιτικά κόμματα, χρησιμοποιούν το Internet για την αύξηση των οικονομικών τους πόρων. Στο μέλλον, αυτό ενδεχομένως να σημαίνει ότι μικρότερες ομάδες μπορεί να είναι ικανές να λαμβάνουν την πλειονότητα των χρηματοδοτήσεων τους με on line δωρεές μέσω πιστωτικών καρτών.
- **Η διάχυση της πληροφόρησης**: Είναι ακόμη, πιθανόν να μπορούν οι ομάδες να δημοσιεύσουν πληροφορίες για μια συγκεκριμένη χώρα. Για παράδειγμα, οι οπαδοί του Sinn Fein από το Πανεπιστήμιο του Texas έδωσαν λεπτομέρειες για τις δυνάμεις του Βρετανικού στρατού στη Βόρειο Ιρλανδία μέσω Internet.82. Επιπλέον, πληροφορίες

[80] «M15 builds new centre to read e-mails on the net», *The Sunday Times*, 30 Απριλίου 2000,1.
[81] Βλ., στο http://www.ezln.org/
[82] «Ulster security details posed on the Internet». *The Times*,25 Μαρτίου 1996.

προσφέρονται για τρομοκρατικές ενέργειες. Για παράδειγμα, το «Terrorist Handbook» (Εγχειρίδιο του Τρομοκράτη) καθοδηγεί τους αρχάριους για το πώς να φτιάχνουν εκρηκτικά και όπλα και είναι ευρέως γνωστό και προσβάσιμο μέσω Internet.[83]

- **Οι επικοινωνίες ασφάλειας**: Η χρήση από μέρους των τρομοκρατών εξελιγμένων μεθόδων αποκρυπτογράφησης ενός συστήματος, το οποίο είναι δύσκολο να σπάσει, επιτρέπει τον έλεγχο των ομάδων, όπου κι αν βρίσκονται. Αυτό προκαλεί ένα πρόβλημα στις υπηρεσίες ασφάλειας, καθώς σημαίνει ότι πρέπει να ξοδέψουν περισσότερα χρήματα και χρόνο στη προσπάθεια τους να αποκρυπτογραφήσουν τα ηλεκτρονικά μηνύματα.

Αν ληφθούν υπόψη όλα τα παραπάνω τότε αντιλαμβανόμαστε πως οι υπάρχουσες ενέργειες μπορούν να απλοποιηθούν μέσω της τεχνολογίας. Η αληθινή απειλή στο πλαίσιο του «Κυβερνοχώρου» υπάρχει όταν το Internet ή άλλες μορφές τεχνολογίας γίνονται το μέσον με το οποίο συντελείται ένα τρομοκρατικό χτύπημα.

Η χρήση των τεχνολογιών παρεμπόδισης από τις κυβερνήσεις και τους μηχανισμούς καταστολής έχει υπερτονιστεί τόσο εμπορικά όσο και πολιτικά, όπως επίσης και οι επιφυλάξεις για την ιδιωτικότητα από διάφορες πλευρές. Παρά το γεγονός ότι σε καμία περίπτωση δεν μπορούν να θεωρηθούν αυτές οι πράξεις κυβερνοέγκλημα, παρουσιάζει ενδιαφέρον να σημειώσουμε ότι η ομοιότητα των ελλοχευουσών μεθόδων σε μερικές περιπτώσεις δείχνει πάλι ότι είναι ο επιτιθέμενος και το κίνητρο που προσδιορίζουν το κυβερνοέγκλημα και όχι οι βασικές τεχνικές που χρησιμοποιούνται.

[83] Anonymous, 1994. *The Terrorist's Handbook*. Available on Internet/WW.

Κεφάλαιο 5ο: HACKERS

Εισαγωγή

«Αυτός είναι ο κόσμος μας τώρα. Ο κόσμος των ηλεκτρονίων και των διακοπτών. Κάνουμε χρήση μίας υπηρεσίας που ήδη υπάρχει χωρίς να πληρώνουμε και η οποία θα ήταν πάμφθηνη εάν δε διοικείτω από αχόρταγους κερδοσκόπους και μας αποκαλείτε εγκληματίες. Εξερευνούμε και μας αποκαλείτε εγκληματίες, αναζητούμε τη γνώση και μας αποκαλείτε εγκληματίες. Υπάρχουμε χωρίς φυλή, χωρίς εθνικότητα, χωρίς θρησκευτικές επιρροές και μας αποκαλείτε εγκληματίες. Εσείς, που φτιάχνετε ατομικές βόμβες, διεξάγετε πολέμους, δολοφονείτε, μας εμπαίζετε και μας παραπλανείτε ότι είναι για το δικό μας καλό κι όμως εμείς είμαστε οι εγκληματίες. Ναι, είμαι εγκληματίας και έγκλημά μου είναι η περιέργεια, το ότι κρίνω τους ανθρώπους από το τι λένε και τις πράξεις τους και όχι από την εμφάνιση τους. Το έγκλημά μου είναι ότι αποδείχτηκα εξυπνότερος από εσάς, κάτι που ποτέ δε θα μου συγχωρήσετε...»[84]

Ευφυείς νεαροί επαναστάτες και σύγχρονοι ταχυδακτυλουργοί ενός καινούριου εικονικού σύμπαντος ή απλά ανεύθυνοι και επικίνδυνοι εγκληματίες με εξειδίκευση στις μοντέρνες υψηλές τεχνολογίες; Εάν κάποιος ήθελε να είναι δίκαιος θα έπρεπε να συμφωνήσει και με τις δύο απόψεις. Από τον δεκατετράχρονο που εισβάλει σε ένα site με υλικό για ενηλίκους για να κλέψει μία ματιά στο απαγορευμένο, ως ένα τρομοκράτη που διεισδύει σε βάσεις δεδομένων του στρατού για να προκαλέσει την κατάρρευση συστημάτων άμυνας, έχουμε την ίδια διαδικασία. Το μόνο που διαφοροποιείται είναι το κίνητρο και το εύρος της δεξιότητας. Όπως αναφέρει και ο Γρ.Λάζος[85] το νόημα του hacking, δηλαδή μορφή μεθόδευσης στους ηλεκτρονικούς υπολογιστές[86] το οποίο αποτελεί τη χωρίς δικαίωμα διείσδυση σε συστήματα υπολογιστών διαμέσου των δικτύων επικοινωνιών τους και

[84] Βλ., Mentor - The conscience of a hacker. Phrack magazine vol.1 issue 7 Phile 3
[85] Λάζος Γρ. Επίκουρος καθηγητής τομέα Εγκληματολογίας, Παντείου Παν/μιου Αθηνών
[86] Βλ., Τσουραμάνης Χρ., «ΕΓΚΛΗΜΑΤΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΙ ΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ ΠΟΥ ΑΝΑΦΕΡΟΝΤΑΙ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ Η/Υ, ΠοινΔικ 12/2001, σ.1275

διαφοροποιείται ανάλογα με το αν η διείσδυση προκαλεί ζημίες στο σύστημα ή όχι και προσβάλει τόσο την ασφάλεια των δικτύων[87] όσο και το απόρρητο των επικοινωνιών, εκτείνεται σε τέτοιο βαθμό, ώστε να περιλαμβάνει ριζικά αντίθετες αλληλοαναιρούμενες και αλληλοαποκλειόμενες αντιλήψεις, οι οποίες αναφέρονται σε ριζικά διαφορετικές πραγματικότητες.[88]

Ίσως το κυριότερο πρόβλημα προς μία ορθή εκτίμηση της hacker κοινότητας και των πράξεών της είναι η τέλεσή τους σε ένα κόσμο ακόμη άγνωστο σε μία πλειονότητα πολιτών αλλά και κοινωνικοπολιτικών Αρχών, αυτόν του διαδικτύου. Στη σύγχρονη κοινωνία της πληροφορίας το πλήθος των hackers είναι πολύ μεγάλο και η δράση τους ξεπερνά τα όρια αντίληψης του μέσου ανθρώπου για τις λειτουργίες και τα προγράμματα που διέπουν το χώρο του Internet. Όπως εξελίχθηκαν οι δυνατότητες και οι υπηρεσίες που προσφέρει ο παγκόσμιος ιστός, έτσι και οι τρόποι και τα κίνητρα δράσης των ατόμων αυτών υπερδιπλασιάστηκαν. Αυτό βεβαίως συνέβη όπως θα δούμε κυρίως την τελευταία δεκαπενταετία καθώς παλαιότερα οι hackers είχαν πιο περιορισμένο πεδίο δράσης.

1.Hackers: Ορισμοί και είδη

Η νομοθεσία διάφορων χωρών επιχειρεί εδώ και περισσότερο από δύο δεκαετίες να ορίσει και να σημάνει το πληροφορικό έγκλημα, το νομικά επιτρεπτό και ανεπίτρεπτο. Οι αρχικές νομοθεσίες που αναπτύχθηκαν -όπως είναι αναμενόμενο- στις ΗΠΑ από τα τέλη της δεκαετίας του '70 προσέφεραν ένα γενικό πλαίσιο ορισμού τού τι είναι πληροφορικό έγκλημα. Στις αρχές του 21ου αιώνα το πλαίσιο αυτό παραμένει ισχυρό, αν και δεν έχει αναπτυχθεί στις διαστάσεις που θα του επέτρεπαν να αποδώσει και στην πράξη, τουλάχιστον τα αναμενόμενα των δημιουργών του. Επιπλέον, δέχεται μιαν αυξανόμενη κριτική από φιλελεύθερους και ριζοσπάστες εγκληματολόγους και κοινωνιολόγους ότι περιλαμβάνει μιαν εξ ορισμού

[87] Βλ., Αγγέλης Ιωάννης, «ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΤΑ ΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ», ΠοινΔικ 12/2001, σ.1293
[88] Γρ. Λάζος - Πληροφορική και έγκλημα. Σελ 95

δαιμονοποιημένη αντίληψη του hacker, επιχειρεί δε να αντιμετωπίσει το πληροφορικό έγκλημα κυρίως με ποινικές μεθόδους, ασύμβατες με τη φύση και τις σχέσεις της πληροφορικής.

Πάντως, είναι γεγονός ότι το πληροφορικό έγκλημα προκαλεί αυξανόμενες βλάβες. Με μια στενά οικονομική αντίληψη, υπολογίζεται ότι προκαλεί περί τα 20 τρισ. σε φθορές ή κλοπές ετησίως σε διεθνή κλίμακα, ενώ για την Ελλάδα το μέγεθος αυτό αγγίζει τα 100 δισ. δρχ.. Ευρύτερα ιδωμένο όμως, το ζήτημα περιλαμβάνει πολλαπλάσιες ζημιές που αφορούν βιομηχανική κατασκοπία, παραβιάσεις του copyright και του trademark, χρηματιστηριακές παρεμβάσεις κ.λπ. Βέβαια, η πληροφορική αποτελεί πλέον αναντικατάστατο εργαλείο του διεθνούς οργανωμένου εγκλήματος στη διακίνηση ναρκωτικών και όπλων, στο trafficking, στο ξέπλυμα των κερδών κ.ο.κ. Αυτά ισχύουν και για την Ελλάδα, όπως και η πρόσφατα παρατηρούμενη εκτροπή των κλήσεων με υψηλό κόστος σε πολλούς συνδρομητές τηλεφώνου, χρήστες πιστωτικών καρτών κ.λπ.

Κι όμως. Το πληροφορικό έγκλημα δεν φοβίζει μόνο, ούτε κυρίως, για τις μέχρι τώρα δράσεις και χρήσεις του. Φοβίζει κυρίως για τις απέραντες δυνατότητες που προσφέρει -για τους κινδύνους που εγκυμονεί- πέρα από τα όσα έχουν αναπτυχθεί μέχρι σήμερα. Οι κίνδυνοι αυτοί σχετίζονται με τις διεθνείς επικοινωνίες και συγκοινωνίες, με την εθνική άμυνα, με την ιδιωτική ζωή και το απόρρητο. Ή μήπως και την πιθανότητα να μείνει γυμνή η εξουσία και η αυθαιρεσία;

Η ηθική των hackers

Από την οπτική γωνία του Levy, βασική ηθική αρχή των hackers είναι η ακόλουθη:

«Η πρόσβαση στους υπολογιστές -και οτιδήποτε θα μπορούσε να σε διδάξει κάτι για τον τρόπο που ο κόσμος λειτουργεί- πρέπει να είναι

απεριόριστη και απόλυτη. Να αποδέχεσαι πάντα την προσταγή «πάνω τα χέρια»[89].

Η αρχή αυτή αναλύεται σε μια σειρά μερικών αρχών, οι κύριες από τις οποίες είναι:

- Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα[90].
- Έλλειψη εμπιστοσύνης στην εξουσία - προώθηση της αποκέντρωσης[91].
- Οι hackers πρέπει να κρίνονται με βάση την ικανότητά τους να hack-ίζουν, και όχι με βάση κίβδηλα κριτήρια, όπως τα πτυχία, η ηλικία, η φυλή ή η θέση.
- Μπορεί να δημιουργηθεί τέχνη και ομορφιά στον υπολογιστή[92].
- Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο[93].

Οι γενιές των hackers

Η πρώτη γενιά των hackers περιλαμβάνει τους επιστήμονες που είχαν συμμετοχή στην ανάπτυξη των πρώτων μεθόδων προγραμματισμού (ηλεκτρικών στην αρχή και ηλεκτρονικών στη συνέχεια) υπολογιστών. Οι

---

[89] Η έκφραση «πάνω τα χέρια» αποτελεί το αντίθετο της κτητικής-απαγορευτικής «κάτω τα χέρια».

[90] Είναι ενδιαφέρον το ότι στις πρώτες τρεις γενιές των hackers η έννοια της ελευθερίας είναι ασαφής και μάλλον κλίνει προς το να αρνείται την πολιτική-εξουσιαστική απαγόρευση («απαγορεύεται να...»). Αντίθετα, στην τέταρτη γενιά των hackers, η έννοια της ελευθερίας είναι σαφέστερη. Αφορά στην άρνηση της πολιτικής-εξουσιαστικής απαγόρευσης - την απαγόρευση που γίνεται αμέσως αντιληπτή. Αφορά όμως και την (έμμεση) οικονομική απαγόρευση. Εφόσον επιβληθεί τιμή στην πρόσβασή τους, το να είναι οι πληροφορίες πολιτικά ελεύθερες αποτελεί απλώς λειτουργικό ιδεολόγημα. Η μεγάλη πλειονότητα του πληθυσμού δεν είναι σε θέση να καταβάλλει -ή να καταβάλλει μόνιμα- το τίμημα και, συνεπώς, αποκλείεται από τις πληροφορίες. Συγχρόνως, δεν είναι σε θέση να ορίσει κάποιον υπεύθυνο και αποδίδει την πληροφοριακή στέρηση σε λαθεμένους προσωπικούς χειρισμούς ή τη μοίρα.

[91] Η αρχή διευρύνεται στην κατεύθυνση της γραφειοκρατίας: «Το τελευταίο πράγμα που χρειάζεσαι είναι μια γραφειοκρατία. Οι γραφειοκρατίες -επιχειρηματικές, κυβερνητικές, πανεπιστημιακές- είναι ελαττωματικά συστήματα, επικίνδυνα ως προς το ότι δεν είναι ικανές να φιλοξενήσουν τις ερευνητικές παρορμήσεις των αληθινών hackers. Οι γραφειοκράτες κρύβονται πίσω από αυθαίρετους κανόνες (σε αντίθεση με τους λογικούς αλγόριθμους, μέσω των οποίων οι υπολογιστές και τα προγράμματα των υπολογιστών λειτουργούν): επικαλούνται αυτούς τους κανόνες με σκοπό να σταθεροποιήσουν την εξουσία, και αντιλαμβάνονται την εποικοδομητική παρόρμηση των hackers σαν απειλή» (Levy, 1984, σ. 28).

[92] Πέρα από την τραχιά (brute) λειτουργικότητα, οι hackers οφείλουν να αποδίδουν μεγάλη σημασία στην αισθητική του προγραμματισμού και τείνουν να αξιολογούν ένα πληροφορικό πρόγραμμα και με βάση τις αισθητικές του αρετές. Υπάρχουν άσχημα και όμορφα προγράμματα (Levy, 1984, σσ. 30-32).

[93] «Και οι hackers, μέσω της γόνιμης και πλούσιας σε νοήματα συναναστροφής με τους υπολογιστές, θα είναι οι πρώτοι σε οφέλη.... Αλλά δεν θα είναι οι μόνοι ωφελημένοι. Οποιοσδήποτε θα μπορούσε να κερδίσει κάτι από τη χρήση σκεπτόμενων υπολογιστών σε έναν διανοητικά αυτοματοποιημένο κόσμο. Και δεν θα ωφεληθούν όλοι ακόμα περισσότερο προσεγγίζοντας τον κόσμο με την αυτή εξεταστική ένταση, το σκεπτικισμό προς τη γραφειοκρατία, το άνοιγμα της δημιουργικότητας, την έλλειψη εγωισμού στο μοίρασμα των επιτευγμάτων, την ώθηση για βελτιώσεις, και την επιθυμία για έργο, όπως αυτοί που ακολούθησαν την Ηθική του Hacking: (Levy, 1984, σ. 36).

πρώτοι hackers χαρακτηρίζονταν από μιαν απόλυτη προσήλωση στο έργο τους. Ζούσαν για να προγραμματίζουν. Κλεισμένοι στα εργαστήρια, κυρίως του MIT, κατά τις δεκαετίες του 1950 και του 1960, δεν είχαν κάποια συστηματική και μόνιμη επαφή με την ευρύτερη κοινωνική πραγματικότητα και τις εξελίξεις της. Ο Ψυχρός Πόλεμος τούς ήταν κάτι το μακρινό, και το γεγονός ότι εργάζονταν για λογαριασμό στρατιωτικοβιομηχανικών κύκλων και μυστικών υπηρεσιών δεν τους απασχολούσε ιδιαίτερα. Πάντως, οι ηθικές αρχές του hacking είχαν νόημα για τη μικρή ομάδα των πρώτων hackers - και μάλλον δεν προβλημάτιζαν τους εργοδότες τους. Στο πλαίσιο μιας πληροφορικής επανάστασης, περιορισμένης σε εργαστήρια υψίστης ασφαλείας, οι αρχές αυτές δεν αποτελούσαν ιδιαίτερο κίνδυνο.

Η δεύτερη γενιά περιλαμβάνει τους επιστήμονες και επιχειρηματικά προσανατολισμένους επιστήμονες που έθεσαν ως σκοπό τους τη μετάδοση της χρήσης της πληροφορικής τεχνολογίας στον ευρύτερο πληθυσμό. Πρόκειται για τους επιστήμονες που ανέπτυξαν τους πρώτους προσωπικούς υπολογιστές, συστήματα υπολογιστών που περιλάμβαναν όλες τις ουσιαστικές ιδιότητες της πληροφορικής τεχνολογίας, έστω και αν δεν διέθεταν παρά περιορισμένες δυνατότητες. Επιπλέον, η δεύτερη γενιά ασχολήθηκε συστηματικά «με τη μελέτη και τον πειραματισμό πάνω στους τρόπους βελτίωσης της επικοινωνίας μεταξύ ανθρώπων και υπολογιστών»[94].

Η τρίτη γενιά αναφέρεται στους προγραμματιστές που σχεδίασαν τις πρώτες αρχιτεκτονικές, πάνω στις οποίες θα αναπτύσσονταν στο κοντινό μέλλον τα ηλεκτρονικά παιχνίδια. Είναι φανερό ότι η τρίτη αυτή γενιά είναι πλέον σαφώς προσανατολισμένη σε μια ήδη δημιουργημένη αγορά πληροφορικής τεχνολογίας γύρω από τον προσωπικό υπολογιστή και προσπαθεί να ανταποκριθεί στη ζήτηση ή να δημιουργήσει μια ζήτηση με βάση πιθανές δυναμικές ανάγκες.

---

[94] Ενα από τα προϊόντα της προσπάθειας αυτής ήταν και το «ποντίκι» (εντολέας), που παρείχε «μία πρακτική και υπερέχουσα μέθοδο διαντίδρασης με έναν υπολογιστή, η οποία δεν καταπονούσε τις συμβολικές και συλλογιστικές δυνατότητες του χρήστη». (Ceruzzi, 1998, σ. 260.)

Οι τρεις πρώτες γενιές των hackers δεν έχουν ιδιαίτερη σχέση με το πληροφορικό έγκλημα, αν και έχουν κάποια ασταθή σχέση καταγωγής και έναν -αμφισβητούμενο ως προς το αν είναι ευρύς ή στενός- κοινό τόπο με την έννοια του hacker, όπως επικράτησε και καθιερώθηκε στις αρχές της δεκαετίας του 1980. Είναι η τέταρτη γενιά των hackers -γνωστών και ως crackers, cyberpunks κ.ο.κ.- που προσεγγίζει τους διάφορους νομικούς ορισμούς του hacking ως εγκληματικής συμπεριφοράς.

Η τέταρτη γενιά αποδέχεται τις ηθικές αρχές των προηγούμενων γενεών - όπως τουλάχιστον τις συνέθεσε ο Levy. Συγχρόνως όμως, είναι σαφώς πολυπληθέστερη, έχει γεννηθεί και κοινωνικοποιηθεί σε ένα ήδη υπάρχον πληροφορικό περιβάλλον, και αποτελείται από άτομα που ζουν σε διαφορετικές συνθήκες και έχουν διαφορετικούς στόχους και σκοπούς από τις προηγούμενες. Μεγάλο μέρος των δραστηριοτήτων, που στο πλαίσιο του εργαστηρίου πληροφορικής ή του Διαδικτύου μεταξύ ερευνητικών κέντρων και επιστημόνων θεωρούνταν ως αυτονόητες, αναπτύσσουν έναν ουσιαστικά διαφορετικό χαρακτήρα όταν μεταφέρονται στην ευρύτερη κοινωνία ή, ακριβέστερα, στον ευρύτερο κυβερνοχώρο. Στο νέο αυτό, ποιοτικά διαφορετικό, πλαίσιο, η πρόσβαση σε έναν υπολογιστή δεν θεωρείται πλέον αμέσως ελεύθερη. Απαιτεί ορισμένες ρυθμίσεις κοινωνικότητας, η κυριότερη από τις οποίες είναι η εξουσιοδότηση. Ευνόητο είναι ότι η χωρίς εξουσιοδότηση πρόσβαση σε έναν υπολογιστή αρχίζει να γίνεται αντιληπτή ως παραβίαση, μια παραβίαση που μπορεί να αξιολογείται ως ανήθικη ή ως ανήθικη και εγκληματική.

Όπως αναφέρθηκε, οι hackers βρίσκονται σε μεγάλη ποικιλία σήμερα και δραστηριοποιούνται σε πολλούς τομείς, έχοντας πληθώρα τρόπων δράσεως και κυρίως πληθώρα κινήτρων. Για το λόγο αυτό και είναι απαραίτητη μία διευκρίνιση των διαφόρων τύπων hacker, ώστε να διευκολυνθεί και η ανάλυση αλλά και η κατανόηση των διαφόρων παραμέτρων περί hacking που θα εκθέσουμε εν συνεχεία.

1.1. PHONE PHREAKS

Καθώς το τηλεφωνικό δίκτυο προϋπήρξε του δικτύου υπολογιστών, έτσι και των σύγχρονων hacker προηγήθηκαν οι phone phreaks. Αυτοί ήταν άνθρωποι που χρησιμοποιούσαν το τηλεφωνικό σύστημα κυρίως για επικοινωνία με οποιοδήποτε μέρος του κόσμου με τρόπο φθηνό, γρήγορο και φυσικά μη αντιληπτό, εκμεταλλευόμενοι κλεμμένους τηλεφωνικούς κωδικούς και κάνοντας τροποποιήσεις σε τηλεφωνικά κέντρα. Στα μέσα της δεκαετίας του '80, η δημοσιοποίηση των κωδικών αυτών για κοινή χρήση αποτελούσε μία βασική προϋπόθεση για να θεμελιωθεί μία bona fides μεταξύ του επίδοξου phreak και της phreaking κοινότητας[95].

1.2. HACKERS

Hacker είναι όποιος ενδιαφέρεται για τις μυστικές και κρυφές διεργασίες οποιουδήποτε λειτουργικού συστήματος υπολογιστή. Έχουν εκτενή γνώση λειτουργικών συστημάτων και γλωσσών προγραμματισμού. Προσπαθούν να ανακαλύψουν τα κενά και ρήγματα στα συστήματα υπολογιστών καθώς και τους λόγους ύπαρξης αυτών. Αναζητούν σταθερά πρόσθετη γνώση, τη μοιράζονται ελεύθερα και δεν καταστρέφουν ποτέ και τίποτα σκοπίμως.[96]

1.3. CRACKERS

Cracker χαρακτηρίζεται αυτός που διεισδύει ή παραβιάζει την ακεραιότητα συστημάτων (σπάει κωδικούς ασφαλείας κλπ.)με πρόθεση τη διάπραξη κακόβουλων πράξεων, όπως καταστροφή δεδομένων, στρέβλωση συστημάτων και παρεμπόδιση λειτουργιών.[97]

1.4. Hackers: Οι 4 γενιές

Ο Γρ. Λάζος βασισμένος στην εργασία του Levy (Hackers,1984), κάνει μία πλήρη αναφορά στις γενιές των hacker από την απαρχή ως τις μέρες μας.

---

[95] Βλ.. Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ. 3 -4
[96] Βλ.. Εργαστήριο εφαρμογών πληροφορικής στα ΜΜΕ - πηγή Internet
[97] Βλ.. όπ.σ.62

Η πρώτη γενιά των hackers αποτελείται από μέλη πανεπιστημιακών ομάδων των μεγάλων τεχνολογικών πανεπιστημίων MIT και Stanford.Αυτοί οι επιστήμονες, σχεδόν αποκομμένοι από την υπόλοιπη κοινωνία, ζούσαν εργαζόμενοι στα εργαστήριά τους και ανέπτυξαν τις πρώτες μεθόδους προγραμματισμού κατά το 1950 και 1960 στις υπηρεσίες κυρίως, βέβαια, της Αμερικανικής κυβέρνησης.

Η δεύτερη γενιά αποτελείται από εμπορικά προσανατολισμένους επιστήμονες που ως σκοπό είχαν την ευρεία διάδοση της πληροφορικής τεχνολογίας στις μάζες. Ήταν αυτοί που δημιούργησαν τους πρώτους προσωπικούς υπολογιστές. Επιπρόσθετος στόχος της νέας γενιάς αυτής ήταν η μελέτη και ο πειραματισμός για τη βελτίωση της αλληλεπίδρασης ανθρώπου με υπολογιστή, παραδειγματικό επίτευγμα της οποίας ήταν το γνωστό και απαραίτητο σήμερα «ποντίκι».

Η τρίτη γενιά αποτελείται από τους προγραμματιστές, οι οποίοι δημιούργησαν τις βασικές δομές στις οποίες στηρίχθηκε μετέπειτα η δημιουργία των ηλεκτρονικών παιχνιδιών. Η γενιά αυτή δείχνει πλέον να αντιλαμβάνεται πλήρως την οικονομική δυναμική του συγκεκριμένου τομέα και εργάζεται δραστικά για να ανταποκριθεί στη ζήτηση που δημιουργεί η ευρεία εξάπλωση της χρήσης προσωπικού ηλεκτρονικού υπολογιστή αλλά και για να διαμορφώσει νέες προοπτικές αγοράς και νέες ανάγκες.

Η τέταρτη όμως γενιά είναι αυτή που συγκρότησε την hacker κοινότητα όπως την ξέρουμε σήμερα. Ενώ με τις προηγούμενες γενιές υπήρχε μια προσήλωση στην επίτευξη μίας εκλαΐκευσης του νέου μέσου και κυρίως μία χρήση αυτού βασισμένη σε ανάγκες και δεδομένα της καθημερινότητας, η νέα αυτή γενιά εμφάνισε για πρώτη φορά μία αντεστραμμένη ψυχολογική συμπεριφορά, μία αναρχική τάση όχι σύνθεσης νέων δεδομένων και προγραμμάτων, αλλά αντίθετα μία αποδομητική και μία ενδοσκοπική εξερευνητική ενέργεια, που εξελίχθηκε στη μοντέρνα μορφή hacking, η οποία

προσεγγίζει την εικόνα που έχουμε στο μυαλό μας γιά τον hacker, εικόνα που άπτεται και εγκληματικών συμπεριφορών.

Η γενιά αυτή αποδέχεται γενικά τις ηθικές αρχές που εξέθεσε ο Levy και τις οποίες θα δούμε αναλυτικά παρακάτω, αλλά παράλληλα αποτελεί ένα πολυπληθές σύνολο που έχει γεννηθεί και κοινωνικοποιηθεί σε ένα ήδη υπάρχον πληροφορικό περιβάλλον, το οποίο αποτελείται από άτομα που ζουν σε διαφορετικά μήκη και πλάτη του κόσμου και έχουν αναπόφευκτα ποικίλες ιδιοσυγκρασίες και ήθη. Όπως αναφέρει και ο Kenneth Rosenblatt, εισαγγελέας στη Santa Clara, California, «η κοινωνία μας πρόκειται να βιώσει τον αντίκτυπο που θα έχει η πρώτη γενιά παιδιών γαλουχημένων στη χρήση προσωπικών υπολογιστών. Η αυξημένη εντρύφηση και η εξειδίκευση των hackers θα οδηγήσει σε αύξηση της εγκληματικότητας, καθώς μέλη της νέας γενιάς θα μπουν στον πειρασμό διάπραξης εγκληματικών πράξεων».[98] Η εκρηκτική εξέλιξη του διαδικτύου δημιούργησε ένα νέο κοινωνικό μόρφωμα, όπου αναπόφευκτα διάφορες συμπεριφορές αποκτούν μία νέα σημασία, όταν πραγματώνονται εκτός εργαστηρίων και επηρεάζουν την ανθρώπινη καθημερινότητα πλέον. Έτσι, η πρόσβαση σε έναν υπολογιστή δε θεωρείται πλέον ελεύθερη, αλλά απαιτείται μία εξουσιοδότηση. Χωρίς την εξασφάλιση αυτής, εισερχόμεθα πλέον στη νομικά ενδιαφέρουσα περίπτωση της παραβίασης, η οποία θα μπορούσε να αξιολογηθεί ως ανήθικη και εγκληματική. [99]

2. Η θετική πλευρά του hacking

Όπως είναι φανερό, αυτή ιδίως η γενιά θα αποτελέσει και το αντικείμενο της περαιτέρω ενασχόλησής μας, καθώς είναι ουσιαστικά η πρώτη γενιά που παρουσιάζει τόσο κοινωνικό όσο και αναπόφευκτα λόγω αυτού και ποινικό - εγκληματολογικό ενδιαφέρον. Φυσικά, η ανάπτυξη αυτή θα πρέπει να γίνει από δύο σκοπιές, ώστε να είναι δίκαιη απέναντι στους

[98] Βλ., Marc D. Goodman – Why the police don't care about computer crime-Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997 Σελ. 470
[99] Βλ., Γρ. Λάζος – Πληροφορική και έγκλημα. Σελ.102 - 103

hackers. Έτσι το πρώτο μέρος θα αφιερωθεί στις υγιείς εκδηλώσεις (λευκή πλευρά) και θα επακολουθήσει η αρνητική (μαύρη πλευρά) των hackers, η εγκληματική πορεία των ατόμων που έχουν ξεπεράσει τα όρια που φαίνονται θεμιτά. Αν και όπως θα δούμε, τα όρια της θεμιτότητας είναι άμεσα εξαρτημένα από την αντίληψη του ατόμου που κρίνει την πράξη.

2.1. «Λευκοί» Hackers

Οι «λευκοί» hackers είναι οι απόγονοι των επιστημονικών-ηθικών στοιχείων που αποτέλεσαν τις τρεις πρώτες γενιές. Είναι τα άτομα, τα οποία έχουν το hacking ως παιχνίδι αλλά και ως μία ευκαιρία επικοινωνίας και επανάστασης στις κατεστημένες εμπορικές και πολιτικές δυνάμεις του χώρου. Ούτως ή άλλως, η κίνηση αυτή έχει τις ρίζες της στην χίπι-αναρχική κίνηση των Yippies στα 1970, που μεταξύ άλλων σκοπό είχαν την αντίδραση ενάντια στις ιμπεριαλιστικές και διψασμένες για ισχύ πολιτικές δυνάμεις της εποχής.[100] Είναι μία ρομαντική ομάδα που συντηρεί τα υψηλά ιδανικά που κληρονόμησαν και χρησιμοποιούν τις δεξιότητες τους για πολλές δραστηριότητες πάντοτε όμως χωρίς κακόβουλο σκοπό.

Για να αντιληφθούμε όμως την ουσία αυτής της κοινότητας θα πρέπει να δούμε αναλυτικά το ψυχολογικό της προφίλ αλλά και τα κίνητρα της. Μόνο μέσα από μία τέτοια θεώρηση είναι εφικτή η ορθή εκτίμηση του φαινομένου του hacking και θα γίνει πιο γλαφυρός και ο διαχωρισμός των υποκατηγοριών της hacker κοινότητας.

Όπως γράφει και ο Levy στην εργασία του για τους hackers υπάρχουν κάποιες θεμελιώδεις αρχές ηθικής. Οι βασικές είναι ότι η πρόσβαση σε καθετί που διδάσκει κάτι για τη λειτουργία του κόσμου (και τους υπολογιστές) θα πρέπει να είναι συνολική και απεριόριστη και ότι κάθε πληροφορία πρέπει να είναι ελεύθερη. Όπως δηλώνει και ο Stallman στη συνέντευξή του στη D.Denning: «Πιστεύω πως κάθε χρήσιμη πληροφορία πρέπει να είναι ελεύθερη. Όχι ως προς την τιμή της αλλά την ελευθερία αντιγραφής και

[100] Βλ., Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ.2

προσωπικής χρήσης της. Λέγοντας χρήσιμη δεν εννοώ εμπιστευτικές πληροφορίες για άτομα ή αριθμούς πιστωτικών καρτών για παράδειγμα.»[101]

Οι αρχές αυτές όπως αναφέρει και ο Γρ.Λάζος αναλύονται σε μερικότερες αρχές:

α) Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα

β) Έλλειψη εμπιστοσύνης στην εξουσία-προώθηση αποκέντρωσης

γ) Οι hackers πρέπει να κρίνονται με βάσει την ικανότητά τους και όχι με κριτήρια όπως πτυχία, ηλικία, φυλή κλπ.

δ) Μπορεί να δημιουργηθεί τέχνη και ομορφιά στον υπολογιστή

ε) Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.[102]

Οι hackers έχοντας αυτά τα ιδανικά αποτελούν ένα σύγχρονο avant-garde πυρήνα ατόμων, τα οποία εναντιώνονται στις σύγχρονες τάσεις που θέλουν τη διαχείριση των πληροφοριών αποκλειστικά από το σύστημα και την επιβολή περιορισμών στην κυκλοφορία τους από τους απλούς πολίτες. Όλοι οι hackers είναι εμποτισμένοι με ένα ηρωικό αντιγραφειοκρατικό συναίσθημα. Επιδιώκουν την αναγνώριση σαν ένα αξιέπαινο πολιτισμικό αρχέτυπο, το μεταμοντέρνο ηλεκτρονικό αντίστοιχο του cowboy.103 Τα κίνητρα των hackers κατά τη Denning εμπεριέχουν την έμφυτη ανάγκη των ατόμων αυτών για γνώση. Επιδιώκουν πρόσβαση σε δεδομένα και δίκτυα για να μάθουν. Και ο Levy και ο Landreth διαπιστώνουν αυτή την τάση των ατόμων αυτών, τα οποία μάλιστα δραστηριοποιούνται και στον τομέα της πληροφορικής επαγγελματικά με μεγάλη συχνότητα.[104]

Στόχος τους επίσης, όπως λένε, είναι η ανακάλυψη των ρηγμάτων σε δίκτυα και υπολογιστικά προγράμματα, έτσι ώστε να εξασφαλισθεί μία

[101] Βλ., Dorothy E. Denning – Concerning hackers who break into computer systems Σελ. 4
[102] Βλ., Γρ. Λάζος – Πληροφορική και έγκλημα Σελ. 100 - 101
[103] Βλ., Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ. 7
[104] Βλ., Dorothy E. Denning – Concerning hackers who break into computer systems Σελ. 5

αυξημένη ασφάλεια στο διαδίκτυο με την βελτίωση των προγραμμάτων άμυνας των υπολογιστών και τη διόρθωση λαθών σε λειτουργικά συστήματα. Αυτό φαίνεται ξεκάθαρα στη διακήρυξη του Nomad Mobile Research Centre, ένα δίκτυο hacker που εργάζεται για την ασφάλεια των υπολογιστών, δηλαδή την αντιστροφή της εφαρμοσμένης μηχανικής: «Στόχος μας είναι να υποχρεώσουμε τις εμπορικές εταιρίες λογισμικού να διορθώνουν τα προϊόντα τους και να προσφέρουμε εναλλακτικές επιλογές. Όλα τα hacks /cracks γίνονται με σκοπό να προβληθεί η ιδέα ότι δεν μπορείς να εξασφαλίσεις ένα σύστημα για πολύ χρόνο.».[105]

Όπως λέει και η D. Denning, οι hackers έχουν στήσει ένα ιδιωτικό σύστημα εκπαίδευσης που τους δεσμεύει, τους διδάσκει και τους επιτρέπει να χρησιμοποιούν τη γνώση τους σε σκόπιμες, αν όχι πάντα νόμιμες δραστηριότητες.106 Στα πλαίσια της αθρόας διασποράς της γνώσης και των αποκτηθέντων δεδομένων, οι hackers αποτελούν μία κολεκτίβα που λειτουργεί σαν μία μυστική κοινωνία. Υπάρχουν δάσκαλοι και μαθητές, μέντορες και μαθητευόμενοι, οι οποίοι αλληλοσυνδέονται σε ένα ηλεκτρονικό πάρε-δώσε, όπου επικρατεί ο σεβασμός, η εμπιστοσύνη και η αλληλεγγύη. Η μόνη διαφορά είναι ότι ως προϋπόθεση εισόδου απαιτούν την ικανότητα και όχι κάποια αριστοκρατική καταγωγή ή οικονομική επιφάνεια. Και φυσικά δεν υπάρχει όρκος σιωπής στους hackers. Μπορεί να είναι ντροπαλοί ή και αντικοινωνικοί, αλλά όταν μιλάνε, αρέσκονται στην αυτοπροβολή και βαυκαλίζονται. Είναι ο μόνος τρόπος, ώστε να αναγνωρισθεί κάποιος από την κοινότητα και να αποκτήσει κύρος, φήμη, να θεωρηθεί άξιο μέλος και να απολαύσει και τη συνεργασία των συναδέλφων hacker.

Το κοινωνικό και ψυχολογικό υπόβαθρο της κοινότητας αυτής παρουσιάζει ιδιαίτερο ενδιαφέρον. Όπως αναφέρθηκε η ηλικία της πλειονότητας των παιδιών αυτών ξεκινά από την εφηβεία και σπάνια ξεπερνά τα 20-25 χρόνια. Αυτοί προέρχονται συνήθως από μεσοαστικές οικογένειες

[105] Βλ., Διακύρηξη Nomad Mobile Research Centre – πηγή - Internet
[106] Βλ., Dorothy E. Denning – Concerning hackers who break into computer systems Σελ.5

και είναι αντί-υλιστές ως επί το πλείστον(εκτός σε ό,τι μπορεί να αφορά τον υπολογιστή τους). Όποιος δείχνει ενδιαφέρον για χρήματα απορρίπτεται αμέσως ως διεφθαρμένος και άξιος περιφρόνησης.

Γι' αυτούς το hacking εκτός από μία πρόκληση συχνά αποτελεί και το αγαπημένο τους παιχνίδι. Όπως δηλώνει και ο Κέβιν Μίτνικ, ένας από τους θρυλικότερους hackers: «Βρίσκοντας διάφορους τρόπους να παραβιάζω τα συστήματα ασφαλείας απλώς περνούσα καλά, είχε πλάκα.».[107] Το εικονικό περιβάλλον προσφέρει μία αίσθηση ασφαλείας, καθώς ο νεαρός κατορθώνει από την ασφάλεια του δωματίου του σαν σούπερ ήρωας να υπερπηδήσει τα εμπόδια αρκετά πιο μορφωμένων και μεγαλύτερων σε ηλικία προγραμματιστών και να τους εμπαίξει.

Η πιο κοινή αντίληψη για τους hackers από το 1960 ως σήμερα είναι οτι αποτελούν μία ελίτ. Όταν είσαι ο ίδιος hacker, τότε είναι η ίδια σου η εσωτερική πεποίθηση για το ανώτερο status σου που σου επιτρέπει να υπερπηδήσεις τους κανόνες.[108] Λόγω αυτής τους της φύσης, ενός elite underground συνόλου με αναρχικές-αντικαπιταλιστικές τάσεις, πρέπει διαρκώς να διατηρούν μία μεμβράνη διαφοροποίησης. Αστεία και ξεχωριστά ρούχα και μαλλιά, ειδική διάλεκτο με διαφορετικές ορθογραφίες γραμμάτων π.χ. 0 αντί για ο, ειδικές περιοχές γκέτο στις πόλεις, διαφορετικά ωράρια ζωής. Συχνά χρησιμοποιούν παραποιήσεις ονομάτων από μεγάλες επιχειρήσεις και περιπαικτικά λογοπαίγνια ως ψευδώνυμα (Phortune 500),κυβέρνηση και αστυνομία (NASA elite) και πολλά άλλα.[109]

Η κοινωνία των hacker είναι κυριαρχούμενη από έφηβα αγόρια και γι' αυτό έχει μία ανδροκρατούμενη κουλτούρα. Μολονότι οι γυναίκες είναι σήμερα μία ανερχόμενη δύναμη στο χώρο, αντιμετωπίζουν ακόμη προκατάληψη και λοιδορία. Πολλοί άνδρες hackers, όπως οι Toxic Shock Group παραδέχονται οτι το hacking το κάνουν και για να ικανοποιήσουν μία

---

[107] *Βλ., Νέστωρ Ε. Κουράκης – Εγκληματολογικοί ορίζοντες – τεύχος Β: Πραγματολογική προσέγγιση και επιμέρους ζητήματα. Σελ. 201*

[108] Βλ., Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ. 9

[109] Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ. 19

υποσυνείδητη σεξουαλική επιθυμία κι ερωτική φόρτιση. Οι Paul Taylor και Sherry Turkle έχουν αναπτύξει θεωρίες που ξεκινούν από τον Φρόυντ (οι crackers έχουν την αρσενική επιθυμία να εισβάλουν σε ένα απρόθυμο σύστημα) και καταλήγουν στην κοινωνιολογία (οι άντρες αναζητούν σκληρή κυριαρχία σε αφηρημένα συστήματα ενώ οι γυναίκες «μαλακή» κυριαρχία σε κοινωνικές καταστάσεις).[110]

Σ' αυτό το σημείο θα πρέπει να γίνει μία ειδική μνεία σε μία όχι και τόσο διαφημισμένη πλευρά του hacking,αυτή του hacktivism (χακτιβισμού), η οποία είναι ίσως το αντιπροσωπευτικότερο δείγμα της πολιτικοποίησης που μπορεί και έχει λάβει η δραστηριότητα του hacking στις μέρες μας, καταδεικνύοντας με τον τρόπο αυτό τις βαθύτερες επαναστατικές και αντικομφορμιστικές ρίζες που επικαλεστήκαμε στην αρχή της ανάπτυξής μας.

2.2. Hacktivism (Χακτιβισμός)

Στη σύγχρονη εποχή ένας εναλλακτικός τρόπος δράσης με αμφιλεγόμενα αποτελέσματα έχει δώσει τροφή για συζητήσεις στον πολιτικό κόσμο. Η δράση αυτή είναι ο ακτιβισμός, δηλαδή η αντίδραση σε μία κατεστημένη αρνητική κατάσταση με ενέργειες όπως πορείες, καθιστικές διαμαρτυρίες, καταλήψεις, μέχρι και επιθέσεις με τούρτες και αυγά κατά οικονομικών και πολιτικών παραγόντων. Όπως λέει και η Τζ. Μαρκέτου και ο ακτιβισμός είναι ένα τέτοιο είδος πολιτικού ακτιβισμού, ένα «συστεμικό» σύνολο προτάσεων για αντίσταση και κριτικό διάλογο. Συνεπώς, ο ακτιβισμός αποτελεί μία μεταφορά του ακτιβισμού της πραγματικής ζωής σε ένα εικονικό επίπεδο έκφρασης, το διαδίκτυο, και υποδεικνύει πώς ο άνθρωπος μαθαίνει να χειρίζεται ψηφιακά πλέον τις δυνατότητες που του προσφέρονται και πώς μαθαίνει να σκέφτεται και να λειτουργεί στα πλαίσια της περιρρέουσας ηλεκτρονικής κουλτούρας.

Υπάρχουν 2 είδη χακτιβισμού: Το πρώτο επιχειρεί να γιατρέψει το Internet από κάθε κακό κώδικα και ελαττωματικό πρόγραμμα. Το δεύτερο και

[110] Συνέντευξη της Τζεννυ Μαρκέτου στην Claudia Giannetti -Hacking vs hacktivism πηγή - Internet

πιο ενδιαφέρον είδος είναι η χρησιμοποίηση του δικτύου ως όργανο για κοινωνική δικαιοσύνη, διαμέσου διαφόρων δραστηριοτήτων διαμαρτυρίας ή ως μέσο για δημοσιότητα.

Χαρακτηριστικό παράδειγμα χακτιβιστών είναι οι Electronic Disturbance Theatre, υποστηρικτές hackers των Ζαπατίστας με έδρα τη Νέα Υόρκη αλλά και οι Electrohippies. Και τα δύο αυτά γκρουπ ειδικεύονται σε virtual καθιστικές διαμαρτυρίες. Οι πρώτοι είχαν καταφέρει να κλείσουν την ιστοσελίδα του προέδρου του Μεξικό με την οργάνωση αποστολής 16000 e-mails διαμαρτυρίας για την πολιτική του, υπερφορτώνοντας το σύστημα και υποχρεώνοντάς το να καταρρεύσει. Οι δεύτεροι είναι ιδιαίτερα γνωστοί για την οργάνωση διαμαρτυρίας κατά του Παγκοσμίου Οργανισμού Εμπορίου και την πίεση που άσκησαν με e-mail σε πολλούς πολιτικούς σχετικά με τα γενετικώς τροποποιημένα προϊόντα.

Ο χακτιβισμός όμως είναι κάτι παραπάνω από μία τυπική αντίδραση, καθώς έχει περάσει και μέσα στην τέχνη ή καλύτερα έχει μετατραπεί σε μία μορφή καλλιτεχνικής έκφρασης με πολιτικά και κοινωνικά μηνύματα. Όπως δηλώνει και η Τζ. Μαρκέτου, πολλοί καλλιτέχνες πιστεύουν οτι δημιουργικότητα δεν είναι να δημιουργείς κάτι καινούριο μόνο, αλλά να χρησιμοποιείς ό,τι ήδη υπάρχει. Ο χακτιβιστής διαδικτυακός καλλιτέχνης αντί να παράγει φυσικά αντικείμενα, οργανώνει και αποδομεί το σύστημα με σκοπό την αφύπνιση του χρήστη. Στα πλαίσια της ελευθερίας δεδομένων στο δίκτυο, η τέχνη δε νοείται να είναι διαθέσιμη επί πληρωμή. Γι' αυτό και μία ομάδα χακτιβιστών καλλιτεχνών από τη Μπολόνια, η 0100101110101101.ORG εισέβαλε στην ιστοσελίδα του πιο δημοφιλούς μουσείου τέχνης στο διαδίκτυο, το hell.com και δημιούργησε ένα αντίγραφο του μουσείου με σπασμένους τους κωδικούς ασφαλείας, ώστε να είναι ελεύθερη η πρόσβαση.

Αυτοί οι καλλιτέχνες του παγκοσμίου ιστού προσπαθούν να διαπιστώσουν αν η τέχνη στο Internet μπορεί να γίνει αληθινά συμμετοχική, συνδετική και ανοιχτού κώδικα. Απ' τη μία εξερευνούν ελεύθερα τις τακτικές

του χακτιβισμού και απ' την άλλη επιτίθενται στο μηχανισμό και το μύθο του καλλιτεχνικού συστήματος, όχι μόνο αμφισβητώντας την πρωτοτυπία ή τη δημιουργία ως συλλογική διαδικασία αλλά και διαμορφώνοντας τα μοντέλα τους μέσα από τη διαδικασία αυτή.[111]

Και με την παράμετρο αυτή κλείνουμε την αναφορά μας στην υγιή πλευρά του hacking για να ασχοληθούμε με το μέρος που άπτεται της σκοτεινής πλευράς του φαινομένου, αυτή που εκδηλώνεται αντικοινωνικά, ανήθικα και φυσικά εγκληματικά.

3. Η σκοτεινή πλευρά του hacking: Οι hackers ως εγκληματικά στοιχεία

Το διαδίκτυο αποτελεί σήμερα μία νέα κοινωνική πραγματικότητα, η οποία είναι όντας ανθρώπινο δημιούργημα, δομημένη με τα προτερήματα και τα ελαττώματα που συναντά κανείς και στην πραγματική κοινωνική ζωή. Όπως δραστηριοποιούνται άνθρωποι ηθικοί και σκεπτόμενοι, που εργάζονται για την κοινωνική ευημερία λοιπόν, έτσι υπάρχουν και άνθρωποι ανήθικοι, οι οποίοι βλέπουν το νέο αυτό δημιούργημα ως μία νέα δίοδο για να ασκήσουν τις παράνομες δραστηριότητες τους με λιγότερες ενοχλήσεις και να επιδιώξουν την ικανοποίηση των φιλοδοξιών και των απωθημένων τους με τα πλεονεκτήματα της ανωνυμίας και του δύσκολου εντοπισμού από τις Αρχές. Αυτοί οι hackers είναι το διεφθαρμένο κομμάτι τους και δυστυχώς αυτοί που απολαμβάνουν τη μεγαλύτερη δημοσιότητα και προσοχή και συνεπώς αυτοί που σκιαγραφούν τη δημόσια εικόνα όλου του κινήματος. Ας δούμε λοιπόν τα χαρακτηριστικά αυτών των crackers.

3.1. Η σκοτεινή πλευρά του hacking

Όπως αναφέρεται και στη δημοσίευση του Marc D. Goodman, το προφίλ του απροσάρμοστου αθώου εφήβου μπορεί να ίσχυε για τους hackers της δεκαετίας του 1980 αλλά όχι στις μέρες μας. Πολλοί hackers σήμερα είναι

[111] Τα στοιχεία περί χακτιβισμού προέρχονται στο σύνολό τους από τη συνέντευξη της Τζεννυ Μαρκέτου στην Claudia Giannetti -Hacking vs hacktivism. πηγή - Internet

κακοήθεις και άπληστοι. Ταλαντούχοι και ικανοί hackers συχνά βρίσκουν δουλειά στη Μαφία, τα κολομβιανά καρτέλ ναρκωτικών, τα τρομοκρατικά δίκτυα και γενικά το οργανωμένο έγκλημα.[112]

Τα κίνητρα των crackers αυτών είναι ευτελή, εκτεινόμενα από το πάθος για χρήμα και δύναμη μέχρι το βανδαλισμό και την καταστροφή συστημάτων για απλή αυτοπροβολή και για την αίσθηση εξουσιασμού των λιγότερο καταρτισμένων και των αδαών. Είναι άτομα τα οποία διαθέτουν χαλαρούς ηθικούς φραγμούς λόγω ελλιπούς μόρφωσης ως προς τους ηλεκτρονικούς υπολογιστές, καθώς, όπως υποστηρίζει και ο Larry Martin, οι γονείς, ο τύπος και οι καθηγητές δεν αντιλαμβάνονται την υποχρέωσή τους να συμβάλουν στην ανάπτυξη ηθικών αρχών σχετικά με τους υπολογιστές. Είναι τεχνολογικά αναλφάβητοι και συνεπώς οι πολιτισμικές νόρμες υστερούν ως προς τις εξελίξεις της τεχνολογίας και τις εξαρτήσεις της κοινωνικής ζωής από αυτές.113 Ο Bloombecker δηλώνει σχετικά: «Ατυχώς, τόσο για την κοινωνία όσο και γι' αυτούς που χρειάζονται καθοδήγηση δεν υπάρχει κάποιο δεδομένο καθεστώς στην κοινότητα των ηλεκτρονικών υπολογιστών που να ορίζει πότε ακριβώς το παιχνίδι έχει βγει εκτός ελέγχου...».[114] Σημαντικό ρόλο στην ηθική ανεπάρκεια που εμφανίζουν οι νέοι hackers είναι κατά τον Brian Harvey το νεαρό της ηλικίας τους που δεν τους επιτρέπει μία ανεπτυγμένη αίσθηση ηθικής, ώστε να έχουν πλήρη αντίληψη για το πότε οι ενέργειές τους είναι βλαπτικές για τους συνανθρώπους τους.[115] Αλλά και μέσα από τα μάτια ενός hacker, του Chris Goggans, μέλος μίας ομάδας που στιγμάτισε τη δεκαετία του 90' με τη δράση της, τους Legion Of Doom, βλέπουμε ότι η νέα γενιά δεν του εμπνέει εμπιστοσύνη. Αναφέρει ότι με τον καιρό τα άτομα έγιναν πιο αντικοινωνικά και καθώς πέρναγαν τα χρόνια χάθηκε αυτό το αίσθημα συναδελφικότητας που επικρατούσε στους κύκλους των hackers. Οι άνθρωποι άρχισαν να μαζεύουν μανιωδώς πληροφορίες για τον εαυτό τους

[112] Βλ., Marc D. Goodman – Why the police don't care about computer crime-Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997 Σελ. 469 - 470

[113] Βλ., Dorothy E. Denning – Concerning hackers who break into computer systems Σελ 9
[114] Βλ., Paul Taylor – Hackers, distributed in Computer Underground Digest Vol.9 Issue 59 Σελ. 13
[115] Βλ., Dorothy E. Denning – Concerning hackers who break into computer systems Σελ 9

και να καταδίδουν για εκδίκηση. Το hacking έπαψε να είναι πια διασκεδαστικό. Έγινε μια διαδικασία πρωτόγονη και διψασμένη για δύναμη σε ατομικό επίπεδο. Αυτό έχει τις ρίζες του και στην αθρόα αύξηση των επίδοξων hacker που αλλοίωσαν το αίσθημα κοινότητας μεταξύ των παλαιών και λόγω πλήθους έχασε σε νόημα και η διανομή δεδομένων και πληροφοριών αλλά και η εκπαίδευση νέων από τους παλαιοτέρους.[116]

Πρόβλημα επίσης αποτελεί κατά τον Spafford η αντίληψη του υπολογιστή ως μηχάνημα με λειτουργία αδιάφορη με την κοινωνική και καθημερινή λειτουργία των ανθρώπων και τις αξίες τους. Η θέαση του ως κάτι αριθμητικό το απογυμνώνει από κάθε ηθικό προβληματισμό καθώς αποτυγχάνουμε να κατανοήσουμε ότι οι υπολογιστές είναι εργαλεία τα παράγωγα των οποίων αφορούν και επηρεάζουν τους ανθρώπους. [117]

Τα τελευταία δεδομένα συντελούν στη διαμόρφωση μίας εικόνας για το ηθικό υπόβαθρο ή μάλλον την ανυπαρξία ενός τέτοιου όσον αφορά στους crackers, ώστε να δικαιολογηθεί η πορεία που καταλήγουν να ακολουθούν. Στη συνέχεια θα εξετάσουμε τις αιτίες της εγκληματοποίησης του κοινωνικού αυτού φαινομένου αλλά και θα καταγράψουμε τις τάσεις της κοινής γνώμης απέναντι του.

3.2. Οι hackers ως εγκληματικά στοιχεία: Τα αίτια και το παρασκήνιο της εγκληματοποίησης

Είναι αναμφισβήτητο ότι πολλοί hackers επιδίδονται σε εγκληματικές συμπεριφορές. Από την εισβολή σε συστήματα τραπεζών και καταστημάτων ηλεκτρονικού εμπορίου(e-shops) για κλοπή κωδικών πιστωτικών καρτών μέχρι την εισβολή σε κρατικούς υπολογιστές για κλοπή ευαίσθητων δεδομένων και απορρήτων αρχείων ή την απελευθέρωση ιών για καταστροφή προγραμμάτων και συστημάτων, οι hackers παραβιάζουν το νόμο για να αποκομίσουν κάποιο όφελος, είτε είναι χρηματικό είτε όχι. Σήμερα όμως ακόμη και η απλή εισβολή σε ένα δίκτυο υπολογιστών χωρίς την παραμικρή

[116] Βλ.,Paul Taylor – Hackers. distributed in Computer Underground Digest Vol.9 Issue 59 Σελ. 35
[117] Βλ., όπ. π., σελ. 15-16

επίπτωση στον χειριστή ή το ίδιο το σύστημα έχει αποκτήσει ποινικό ενδιαφέρον, προξενώντας έντονες συζητήσεις σε νομικούς και όχι μόνο κύκλους για το κατά πόσο κάθε πράξη hacking πρέπει να έχει ποινικό αντίκτυπο αλλά και για τους λόγους που έχει δημιουργηθεί ένα τέτοιο κλίμα συνολικής ποινικοποίησης αυτής της δραστηριότητας. Και είναι όπως θα δούμε γεγονός είναι οτι βρίσκονται ισχυρές κοινωνικοπολιτικές δυνάμεις και τάσεις που τροφοδοτούν αυτή την κατάσταση δαιμονοποίησης των hackers, οι οποίοι χωρίς να είναι φυσικά άμοιροι ευθυνών δεν είναι αυτονόητα και πάντοτε ένοχοι.

Η δημιουργία ενός κοινωνικού ορίου μεταξύ δύο διαφοροποιημένων ομάδων-τάξεων συντελείται με μία έντονη διαδικασία, όπου κάποια ομάδα διαφοροποιείται, περιθωριοποιώντας άλλες ομάδες και θεμελιώνοντας έτσι την ταυτότητά της. Ένα τέτοιο κυνήγι μαγισσών έχουμε σε περιόδους κοινωνικής ανακατάταξης και όπως φαίνεται η κοινωνία μας βρίσκεται σε μία τέτοια περίοδο αλλαγής. Οι κύκλοι της οικονομίας επιχειρούν να επιβάλουν σχέσεις ιδιοκτησίας επί των πληροφοριών αλλά η μεταβαλλόμενη φύση της πληροφορίας υπονομεύει τις ιδιότητες της ως αγαθό.[118] Οι Dougan και Gieryn διαβλέπουν μία συγκεκριμένη λειτουργία στο μηχανισμό αυτό. Μία κοινότητα, λένε, αποκτά αίσθηση του κοινωνικού της status προσδιορίζοντας τι δεν είναι. Η αποστασιοποίηση από τους έξωθεν βοηθά τα μέλη μίας ομάδας να έχουν μία αίσθηση συνοχής. Επίσης μία κουλτούρα τείνει να περιθωριοποιεί δράσεις που πλήττουν τις αξίες της. Στην περίπτωση των hackers αυτό συνέβη, διότι με τις αντιλήψεις τους περί ελευθερίας της πληροφορίας απείλησαν ένα από τα βασικά δεκανίκια του καπιταλισμού, τα δικαιώματα ιδιοκτησίας.[119]

Βασικός επίσης παράγοντας περιθωριοποίησης και εγκληματοποίησης των hackers είναι το γεγονός ότι δημιουργείται ένας νέος τομέας επαγγελμάτων αντίθετος με τη hacking κουλτούρα και ηθική: η βιομηχανία

[118] Βλ.,Paul Taylor – Hackers, distributed in Computer Underground Digest Vol.9 Issue 59 Σελ. 4
[119] Βλ. όπ.π. Σελ. 5

ασφαλείας υπολογιστών. Μία βιομηχανία, πολύ ισχυρή σύμμαχος των καθεστώτων που θέλουν να έχουν τον απόλυτο έλεγχο των νέων τεχνολογιών για την εξυπηρέτηση των δικών τους σκοπών. Δεν ανέχονται τους ενοχλητικούς hackers, οι οποίοι αποκαλύπτουν κρατικές και εταιρικές παρασπονδίες και φυσικά εξαναγκάζουν τις εταιρίες προστασίας υπολογιστών να ξοδεύουν υπέρογκα ποσά, ώστε να αναπτύσσουν ικανά αμυντικά συστήματα σε τακτά χρονικά διαστήματα για να μπορούν να διατηρήσουν μία τυπική αμυντική γραμμή έναντι των εισβολών. Έτσι η ηθική καταδίκη αποτελεί τρόπο για αποποίηση των ευθυνών για τα ρήγματα και ελαττώματα των συστημάτων από πλευράς υπευθύνων ασφαλείας. Όπως εύγλωττα δηλώνουν στις εκκλήσεις των hackers για συνεργασία στην ανακάλυψη των συστεμικών προβλημάτων εάν οι hackers δεν υπήρχαν τότε δε θα υπήρχε και η ανάγκη για τόσα αμυντικά προγράμματα που κοστίζουν σε έσοδα και δημιουργικό χρόνο. Και πράγματι εδώ ο προβληματισμός δικαίως ευσταθεί, καθώς είναι αμφίβολο εάν δικαιολογεί την ύπαρξη της μία απειλή (οι hackers), ως προστάτης της κοινωνικής και ηλεκτρονικής ασφάλειας και ευημερίας, όταν η ύπαρξη της ιδίας της απειλής, εξωθεί στην ανάγκη για δημιουργία και διαρκή εξέλιξη αμυντικών μηχανισμών.[120]

Η αντίληψη για τους hackers τροφοδοτείται και από τη τάση να υποθέτουμε το χειρότερο δυνατό κίνητρο για τον κάθε εισβολέα, γεγονός που ενισχύεται ακόμα περισσότερο από την ανωνυμότητα αλλά και τη λαϊκή άγνοια ως προς τη διαδικασία του hacking. Η προκατάληψη βασίζεται πάνω στη δυνητική ζημία που είναι σε θέση να επιφέρει ένας hacker. Ακόμη και χωρίς καμία κακόβουλη πρόθεση από τον hacker, η υποψία και η αμφιβολία υπάρχουν. Αυτό διογκώνεται από τη δυσνόητη φύση της δράσης των ατόμων αυτών αλλά και τις δεδομένες δυσκολίες παρακολούθησης τους καθώς και από ένα αυτονόητο χάσμα γενεών που υπάρχει μεταξύ των διαχειριστών της οικονομικής και πολιτικής ζωής και των συστεμικά απορροφημένων

[120] *Βλ.,όπ.π Paul Taylor, Σελ. 7*

ενηλίκων - μαζοποιημένων μελών της καπιταλιστικής κοινωνίας έναντι των επαναστατικών νέων που αποτελούν την πλειοψηφία των hackers σήμερα.[121]

Είναι αδιαμφισβήτητο ότι σταδιακά στις μέρες μας αξίες όπως συναδελφικότητα και αλληλεγγύη έχουν αρχίσει να ατονούν με αποτέλεσμα να ασθενεί αυτό το αίσθημα κοινότητας και συντροφικότητας που επικρατούσε σε παλαιότερες εποχές και να δίνει τη θέση του στην επιδίωξη της προσωπικής ανέλιξης και τον εγωκεντρισμό. Το δημόσιο ήθος βιώνει μία παρακμή και για το λόγο αυτό επιζητά έναν αποδιοπομπαίο τράγο ώστε να δημιουργήσει ένα κλίμα αποπροσανατολισμού και να δικαιολογήσει τα ανησυχητικά δεδομένα.

Έτσι οι hackers αναλαμβάνουν αυτό το ρόλο. Όπως λέει και ο Barlow «Ο τέλειος μπαμπούλας στη σύγχρονη εποχή είναι ο cyberpunk. Είναι τόσο έξυπνος ώστε σε κάνει να νιώθεις πιο «χαζός» απ' ό,τι συνήθως. Κατανοεί την αξία πραγμάτων, τα οποία εσύ αδυνατείς να αντιληφθείς...» [122]

Μέσα σε ένα τέτοιο αρνητικά προδιατεθειμένο περιβάλλον, έρχεται να προστεθεί η καταλυτική επιρροή των ΜΜΕ, τα οποία φυσικά είναι αυτά που δίνουν μορφή σε όσα αναφέραμε ως τώρα. Ο τύπος έχει υπάρξει ιδιαίτερα ενεργός στη διαδικασία της δημιουργίας στερεοτύπων και τη διόγκωση περιστατικών hacking, μία διαδικασία που οδήγησε στην ανάπτυξη ενός περιθωριακού status για τους hackers. Οι Duff και Gardiner υποστηρίζουν ότι τα ΜΜΕ έχουν δώσει τέτοια έκταση και σημασία στο φαινόμενο hackers γιατί προσφέρονται για ηρωοποίηση ή δαιμονοποίηση. Ειδικά στις τεχνολογικά ανεπτυγμένες χώρες όπως λένε, ο λόγος για το hacking είναι πλέον μέρος της λαϊκής συνείδησης. [123] Κατά την πεποίθηση των Hollinger και Lanza-Caduce όπως τις εκθέτει ο Γρ. Λάζος στο βιβλίο του, μολονότι τα ΜΜΕ δεν υποστήριξαν την εφαρμογή του ποινικού δικαίου στον κόσμο της πληροφορικής, δημιούργησαν ένα κλίμα σοβαρού και πιθανοτά του

[121] Βλ.,όπ.π Paul Taylor. Σελ 11 - 12
[122] Βλ.,όπ.π., Paul Taylor, σελ. 33 - 34
[123] Βλ., Γρ. Λάζος – Πληροφορική και έγκλημα σελ. 104

κινδύνου στην κοινή γνώμη, με την προβολή πραγματικών ή και φανταστικών ιστοριών με hackers και συχνά προσβεβλημένες υπό ένα πρίσμα υπερβολής.[124] Γλαφυρότατη είναι η δήλωση του δημόσιου σχολιαστή Gene Spafford περί του τι είναι hacking και τι προεκτάσεις έχει: «το να δίνεις δουλειά σε ένα hacker είναι σαν να κάνεις αρχηγό της πυροσβεστικής έναν εμπρηστή, καθηγητή σχολείου έναν παιδεραστή...» Έτσι οι πράξεις των hackers τοποθετούνται εκτός διαδικτύου και επανασυστήνονται στον κανονικό κόσμο με όρους καθημερινούς και αντιληπτούς σαν αληθινές απειλητικές καταστάσεις. Εάν αυτό επιτευχθεί, τότε ο κίνδυνος και η ζημία που μπορεί να έχουν τέτοιες πράξεις γίνονται ευκολότερα κατανοητά και τρομακτικά και οι hackers παρουσιάζονται ως ηθικοί παρίες.[125] Το πρόβλημα, όπως λέει και ο Paul Taylor, έγκειται στη ρεαλιστική έκθεση και περιγραφή των περιστατικών hacking, καθώς παρουσιάζουν σύνθετη τεχνική ορολογία, η οποία πρέπει να γίνει αντιληπτή από τον τηλεθεατή αλλά παράλληλα με τρόπο ευχάριστο και διασκεδαστικό. Έτσι συνήθως η ακρίβεια και η λεπτομέρεια θυσιάζονται στο βωμό της τηλεθέασης και τα γεγονότα περιγράφονται με τρόπο διογκωμένο και τα κίνητρα των hacker παρουσιάζονται αρκετά πιο σκιώδη.[126]

Όλη αυτή η σύνθετη διαδικασία εγκληματοποίησης έχει φυσικά αντίκτυπο στην ίδια την κοινωνία και το λαϊκό αίσθημα απέναντι στους hackers αλλά και στους ίδιους όπως θα δούμε στη συνέχεια της παρουσίασης μας.

3.2.1. Συνέπειες εγκληματοποίησης σε κοινωνία και hacker κοινότητα

Αναμφισβήτητα αυτός ο πανικός που έχει δημιουργηθεί γύρω από την επικινδυνότητα του hacking έχει οδηγήσει την κοινωνία σε μία οπισθοδρομική πορεία όσον αφορά στην εμπιστοσύνη και την ενασχόληση

[124] Βλ., όπ.π.,Γρ. Λάζος, σελ. 104
[125] Βλ., Paul Taylor – Hackers, distributed in Computer Underground Digest Vol.9 Issue 59 Σελ. 4
[126] Βλ.,όπ.π., Paul Taylor, σελ. 18

του μέσου πολίτη με το διαδίκτυο και τις ποικίλες υπηρεσίες που προσφέρει. Όπως υποστηρίζει και ο Brian Harvey η μεγαλύτερη ζημία των hackers είναι η παράνοια που δημιουργείται, η οποία οδηγεί στη δικαιολόγηση αυστηρότερου ελέγχου από τις Αρχές, γεγονός που φυσικά περιορίζει τις δυνατότητες των πολιτών και μειώνει την ποιότητα ζωής που θα μπορούσαν να εξασφαλίσουν οι χρήστες.[127] Με αυτό συμφωνεί και η D.Denning, η οποία δηλώνει ότι η προβολή μίας τέτοιας εγκληματικής εικόνας των ατόμων αυτών οδηγεί σε μία τάση για κοινωνικό έλεγχο σε μία περίοδο που θα έλεγε κανείς ότι ήδη βρισκόμαστε υπό υπερβολικό έλεγχο.[128] Κι όμως, όπως φαίνεται από έρευνα του Pew Internet & American Life Project, ενώ η ανησυχία των Αμερικανών ως προς την εγκληματικότητα σε υπολογιστές είναι αυξημένη (87% ανησυχούν για κλοπή πιστωτικών καρτών on-line, 82% φοβούνται τη δυνατότητα τρομοκρατών να σπείρουν πανικό μέσω διαδικτύου, 78% πιστεύουν οτι οι hackers δύνανται να έχουν πρόσβαση σε κρατικά δίκτυα και 76% σε εμπορικά δίκτυα και ένα 70% φοβάται για φαρσέρ και εγκληματίες που στέλνουν ιούς και τροποποιούν ή σβήνουν αρχεία), τα ποσοστά των ατόμων που εμπιστεύονται τις Αρχές για έλεγχο και προστασία είναι αρκετά χαμηλότερα (54% των Αμερικανών συμφωνεί με παρακολούθηση του ηλεκτρονικού ταχυδρομείου υπόπτων από το FBI, από την αστυνομία το ποσοστό υποχωρεί κι άλλο, ενώ μόνο ένα 31% δείχνει να εμπιστεύεται τη σωστή κρίση της κυβέρνησης. Κι αυτό σε μία χώρα όπου το Internet είναι πλέον θεμελιώδες εργαλείο της κοινωνίας, αποτελεί πατρίδα των hackers και διαθέτει μία από τις αυστηρότερες πολιτικές κατά τέτοιου είδους προσβολών.[129]

Η δαιμονοποίηση όμως αυτή δημιουργεί μία κοινωνική ανισορροπία και διότι καταλήγει να πλήττει και μία νέα κοινωνική ομάδα, η οποία ενώ αποτελεί σημαντική κινητήρια δύναμη της σύγχρονης οικονομικοκοινωνικής πορείας, απειλείται με στιγματισμό. Όπως λέει και ο Bruce Sterling, υπάρχουν

[127] Βλ.,Dorothy E. Denning – Concerning hackers who break into computer systems Σελ. 10
[128] Βλ.,όπ.π., Dorothy E. Denning, σελ. 11
[129] Βλ., Susannah Fox & Oliver Lewis – Pew Internet Tracking Report – Fear of Online Crime Σελ. 2

σήμερα πολίτες, οι οποίοι εργάζονται στον τομέα της ηλεκτρονικής, λειτουργώντας στα πλαίσια του νόμου σε πολύ υψηλό επίπεδο ειδίκευσης και ικανότητας. Όταν συγκεντρώνονται σε κυβερνητικές θέσεις πανεπιστήμια και πολυεθνικές και αναγκάζονται να ακολουθούν συγκεκριμένους κανόνες, τότε τίθενται κάποιοι συμβατικοί περιορισμοί στην ελευθερία δράσης τους. Όταν όμως βρεθούν ανεξάρτητοι και ελεύθεροι να δημιουργήσουν, αυτή η επίλεκτη κατηγορία ταλαντούχων ενηλίκων είναι πολύ πιο επικίνδυνη από οποιαδήποτε ομάδα από cyberpunks. Αυτοί οι hackers διαθέτουν δύναμη, ικανότητα και επιθυμία να επιδράσουν επί της κοινωνικής διαστρωμάτωσης. Αποτελούν μία ελίτ που αν απομακρυνθεί και δράσει αποκομμένη από τις κοινωνικές αρχές και στερεότυπα, εάν αποκλεισθεί απ' αυτά, μπορεί να καταστεί επικίνδυνη. Αυτοί οι άνθρωποι γνωρίζουν ενστικτωδώς ότι μία πολιτική επίθεση στους hackers θα τους αγγίξει αναπόφευκτα. Ότι η δαιμονοποίηση του όρου hacker μοιραία θα τους επηρεάσει, θα θίξει την ισχύ και την ελευθερία που απολαμβάνουν και θα τους αφανίσει. Και φυσικό είναι να θέλουν με κάθε τρόπο να αποφευχθεί κάτι τέτοιο. [130]

Όσον αφορά τώρα στους ίδιους τους hackers, η εγκληματοποίηση της δράσης τους αλλά και η προπαγάνδα που συντελείται όπως είδαμε με την ευχή της καθεστηκυίας τάξης δημιουργώντας ένα στερεότυπο εικόνας για τα άτομα αυτά επιδρά όπως αναφέρει ο Γρ. Λάζος τόσο στην ατομική ιδιοσυγκρασία και επιλογές τους όσο και στον τρόπο που αλληλεπιδρούν με την κοινωνία και διαμορφώνουν την κοινότητά τους. Μετέτρεψε τους hackers σε μία πιό οργανωμένη για την επιβίωσή της ομάδα, ενώ η συντονισμένη επίθεση από τις διωκτικές Αρχές, τα ΜΜΕ και τους σύγχρονους ιδεολογικούς μηχανισμούς, τροφοδότησε τις αντιλήψεις τους με μία ενισχυμένη επαναστατικότητα και αντιδραστικότητα στους κατεστημένους μηχανισμούς κοινωνικού αποπροσανατολισμού και υποβολής. Σε άλλες περιπτώσεις πάλι, οι hackers παρασύρθηκαν από τη λαίλαπα μυθοποίησης του hacker-προτύπου και έτσι ακολούθησαν ένα ρόλο γραφικού εγκληματία-μορφής του

[130] Βλ.,Bruce Sterling - The hacker crackdown: Law and disorder on the electronic frontier Part 2 Σελ. 7 - 8

υποκόσμου που ήταν, όπως πίστευαν, ό,τι περίμενε η κοινωνία να δει από αυτούς.[131] Όπως λέει και η Τζ. Μαρκέτου στη συνέντευξή της, η αρνητική δημοσιότητα του hacking μέσω των ελεγχόντων την ροή και μορφή των πληροφοριών, υποβίβασε τη σημασία του hacking και του χακτιβισμού σε απλή δραστηριότητα μέσω υπολογιστή, αφαιρώντας έτσι το κοινωνικοπολιτικό περίβλημα που διαθέτει. Μετατρέποντας τους hackers σε δημοσιότητες κατάφερε να τους αποδυναμώσει και μέσω του καταναλωτισμού να απορροφήσει το δημιουργικό - ανατρεπτικό τους πνεύμα.[132]

Η τάση αυτή εγκληματοποίησης των hackers οδήγησε αναπόφευκτα στη διαμόρφωση ενός ποινικού πλαισίου νομικής αντιμετώπισης το οποίο όμως από πλευράς εγκληματολογικής θεωρίας και αποτελεσματικότητας δε φαίνεται να είναι πλήρες και να ικανοποιεί ιδιαίτερα. Αυτό το ζήτημα θα εξετάσουμε στο κεφάλαιο που ακολουθεί.

3.2.2. Ποινική αντιμετώπιση του φαινομένου και θεωρίες σχετικά με αυτή

Αναντίρρητα υφίσταται μία καθαρά εγκληματική πλευρά του hacking, την οποία προαναφέραμε (βανδαλισμοί, κλοπές πιστωτικών καρτών, παραβίαση απορρήτων αρχείων και χρήση τους), τα οποία κανείς δε θα μπορούσε να αμφισβητήσει ότι χρήζουν ποινικής αντιμετώπισης ως καθαυτά εγκλήματα που απλά εκδηλώνονται στο χώρο του διαδικτύου. Παρόλα αυτά όμως διαφαίνεται από θεωρητικούς αλλά και από τα τελικά νομοθετήματα που παράγονται, η τάση ποινικοποίησης ακόμη και της απλής χωρίς εξουσιοδότηση πρόσβασης δίχως αυτή να έχει κάποιες περαιτέρω συνέπειες. Όπως δηλώνουν για παράδειγμα οι Scott και Wasik, η πρόσβαση σε έναν υπολογιστή αποτελεί ποινικά κολάσιμη πράξη ανεξαρτήτως αν εκμεταλλεύεται αυτή για κάποιο άλλο σκοπό, εφόσον αυτή η πρόσβαση έχει εξασφαλιστεί με ακατάλληλα μέσα. Αυτή η επιλογή όπως αναφέρει και ο

[131] Βλ.,Γρ. Λάζος – Πληροφορική και έγκλημα. Σελ 105 - 106
[132] Συνέντευξη της Τζεννυ Μαρκέτου στην Claudia Giannetti -Hacking vs hacktivism πηγή-Internet

Γρ.Λάζος έχει μάλλον σαν στόχο να έρθει αντιμέτωπη με την πράξη της κακοχρησίας υπολογιστή εξαρχής δίχως να απαιτεί την εκδήλωσή της εγκληματικά με τη διάπραξη άλλων αδικημάτων μέσω αυτής. Ποινικοποιώντας όμως ο νομοθέτης, όπως μας λέει, αυτό το προκαταρκτικό στάδιο επεκτείνει το ποινικό δίκαιο σε τομείς που άπτονταν τους αστικού δικαίου κυρίως.[133]

Βέβαια κάτι τέτοιο φαίνεται λογικό εάν αναλογιστούμε το γεγονός, ότι οι hackers συχνά τιμωρούνται και καταδικάζονται όχι για εγκλήματα που διέπραξαν, αλλά για το ότι έχουν τη δυνατότητα ανά πάσα στιγμή να φέρουν εαυτόν σε θέση να διαπράξουν με ευκολία σοβαρότατα αδικήματα , αλλά και ότι ακόμη και η σύγχρονη ποινική νομοθεσία συχνά τιμωρεί κάποιες πράξεις, οι οποίες αποτελούν προκαταρκτικά στάδια άλλων σοβαρότερων αδικημάτων όπως π.χ. η κλασσική αντιστοιχία που γίνεται της χωρίς εξουσιοδότηση πρόσβασης με τη διατάραξη οικιακής ειρήνης (ως προ-στάδιο κλοπής η ληστείας), η οποία έχει δώσει τροφή για πλούσια αντιπαράθεση μεταξύ των hackers και των πολεμίων τους.[134]

Ουσιαστικά αυτή η τάση ποινικοποίησης ακόμη και της απλής πρόσβασης σε υπολογιστή είναι, όπως εύστοχα σημειώνει και η Nelson, αντιπροσωπευτική της βαθύτερης σύγκρουσης δύο ομάδων αξιών που αναφέρθηκαν και ανωτέρω: Απ' τη μία πλευρά αυτές του κοινωνικοπολιτικού κατεστημένου, τις οποίες προστατεύει το ποινικό δίκαιο και απ' την άλλη, αυτές που σχετίζονται με τις αρχές της ελευθερίας από παρεμβάσεις στην έκφραση και την πληροφορία. Κατά τη Nelson, ούτε η ανταποδοτική ούτε και η ωφελιμιστική αντίληψη είναι ικανές να προσφέρουν ικανοποιητική επιχειρηματολογία για την επιβολή ποινικής τιμωρίας στους hackers.

Η ανταποδοτική θεωρία δικαιολογεί την επιβολή ποινών από την κοινωνία σε οποιονδήποτε παραβιάζει την ηθική τάξη. Όμως είναι δεδομένο

---

[133] Βλ., Γρ. Λάζος , Πληροφορική και έγκλημα, σελ. 107

[134] Για εκτεταμένη αναφορά στο σχετικό ζήτημα βλ. Paul Taylor – Hackers, distributed in Computer Underground Digest Vol.9 Issue 59 Σελ. 23 - 24

ότι με τα νέα δεδομένα που εισάγει η κοινωνία του Internet δημιουργείται ένα χάσμα στο τι θεωρείται πλέον θεμιτό και ηθικό και τι όχι.

Και η ωφελιμιστική θεωρία πάντως, η οποία δικαιολογεί ως ορθή αντιμετώπιση ενός φαινομένου αυτή με τα καλύτερα αποτελέσματα δεν προσφέρει μία ασφαλή λύση στον προβληματισμό καθώς τα οφέλη και οι ζημίες της κοινωνίας από μία τέτοια οριακή αντιμετώπιση του hacking δεν είναι ξεκάθαρα. Η αποτροπή και η αναμόρφωση αποτελούν βάση αυτής της θεώρησης και όμως οι επικριτές της αμφιβάλλουν κατά πόσο η τιμωρία αποτρέπει το έγκλημα όπως αμφιβάλλουν και για τον αναμορφωτικό χαρακτήρα της ποινής.[135] Σε όσους μάλιστα μιλούν και για αυστηρότερα μέτρα-φυλάκιση, ώστε να σταλεί ένα ηχηρό μήνυμα στους hackers, ο John Draper, φυλακισθείς το 1970 ακόμη για τη δράση του, υποστηρίζει ότι αυτό θα χειροτερεύσει την κατάσταση, καθώς ο ίδιος εξαναγκάστηκε να διδάξει τις τεχνικές του σε άλλους έγκλειστους εγκληματίες. Η φυλάκιση των hackers θα διασπείρει την επικίνδυνη αυτή γνώση σε ευρύτερους εγκληματικούς κύκλους.[136] Και επίσης, όπως αναφέρει η D.Denning αυτό το τιμωρητικό μοντέλο που προωθεί η εγκληματοποίηση του hacking, μας οδηγεί στο να συμπεράνουμε ότι με την τιμωρία μίας ικανής μερίδας παραβατών θα είναι εφικτή η αντιμετώπιση του φαινομένου, γεγονός όμως για το οποίο η ίδια, βάσει και μίας έρευνας του Gordon Meyer στο έργο του «The social organization of the computer underground», μάλλον αμφιβάλει, καθώς θεωρεί ότι μία τέτοια πολιτική αντίθετα θα συμβάλει στη διόγκωση του αριθμού των hackers.[137]

Μέσα σε ένα τέτοιο περιβάλλον αντιπαραθέσεων έρχεται η Nelson να καταθέσει την άποψη της για τη νομική-ποινική αντιμετώπιση των hacking περιστατικών. Θεωρεί ανωμαλία την ποινική τιμωρία των hackers και υποστηρίζει ότι ο νόμος πρέπει να βασιστεί στην αρχή της αυτοσυγκράτησης,

---

[135] Βλ., Γρ. Λάζος, Πληροφορική και έγκλημα, σελ.107 - 108

[136] Βλ.,Dorothy E. Denning – Concerning hackers who break into computer systems Σελ.13

[137] Βλ., όπ.π., Dorothy E. Denning, σελ.11

ώστε να μην καταντήσει μία εκδήλωση υπερβολικής αυστηρότητας και να εξασφαλίσει όπως και χρειάζεται το κύρος και τη νομιμότητά του. [138]

Οπωσδήποτε ένα νομικό καθεστώς το οποίο θα οδηγεί σε ποινές δυσανάλογες της σοβαρότητας των περιστατικών θα καταλήξει να αποτελεί όχι μόνο κενό γράμμα αλλά ακόμη ένα λόγο αντίδρασης και δικαιολόγησης των όποιων υπερβολικών αντιδράσεων των hackers. Χαρακτηριστικό παράδειγμα οι hackers που απειλούσαν να δώσουν εμπιστευτικούς κωδικούς της Αμερικανικής κυβέρνησης στη δημοσιότητα ή σε τρομοκράτες εάν δεν απελευθερωνόταν ο Κέβιν Μίτνικ. Μάλιστα ας σημειωθεί ότι στην πλειοψηφία τους ως ανήλικοι δε διαθέτουν καν πλήρη αντίληψη της επικινδυνότητας και της σοβαρότητας των πράξεών τους.[139]

3.2.3. Αδυναμίες της νομοθεσίας

Ο Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α΄ κ. Εμμανουήλ Σφακιανάκης παρατηρεί ότι «οι νομοθετικές ρυθμίσεις που αφορούν το ηλεκτρονικό έγκλημα παρουσιάζουν εγγενείς αδυναμίες, τόσο στην Ελλάδα όσο και στις υπόλοιπες χώρες. Αυτό συμβαίνει διότι το Ηλεκτρονικό Έγκλημα αποτελεί εγκληματική δραστηριότητα αρκετά εξειδικευμένη και ανεπτυγμένη τεχνολογικά, με αποτέλεσμα να παρουσιάζονται προβλήματα στην οριοθέτηση των πράξεων που θα πρέπει να διώκονται ποινικά. Επιπλέον, οι νομοθέτες είναι αναγκασμένοι να ενημερώνονται διαρκώς για τις εξελίξεις στον τομέα της τεχνολογίας των υπολογιστών, προκειμένου να εξοικειωθούν με τον τρόπο διάπραξης αδικημάτων μέσω αυτών.» Σε ειδική έρευνα που έγινε στη Βρετανία από την Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος (Foresight Crime Prevention Panel) διαπιστώθηκε ό,τι το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια τη λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης και θα έχουν την τεχνογνωσία να υπερκεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο.

[138] Βλ., όπ.σ.101, Γρ. Λάζος, σελ 108
[139] Βλ.,Frontline - who are hackers – interview with anonymous, πηγή Internet

3.2.4. Μέτρα προστασίας

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι.

Κατά προτίμηση, ο χρήστης που εισέρχεται στο Διαδίκτυο από dial up σύνδεση θα πρέπει να κλείνει με κωδικό που θα προμηθευτεί από τον Ο.Τ.Ε τις εξερχόμενες διεθνείς κλήσεις, καθόσον υπάρχει ο κίνδυνος του dialer (κώδικας που συνδέει τον η/υ του χρήστη σε I.S.P της αλλοδαπής με αποτέλεσμα την υπερβολική τηλεφωνική χρέωση του). Επίσης, ο χρήστης θα πρέπει να έχει εγκαταστήσει προγράμματα για την προστασία από ιούς και ηλεκτρονικές επιθέσεις. Ειδικότερα:

- Να διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.
- Μην εμπιστεύεστε ότι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.
- Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου. Ένα φίλτρο είναι ένα πακέτο λογισμικού το οποίο μπορεί να αποκλείσει την προσπέλαση σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο.

Η αποτελεσματικότητα ενός φίλτρου εξαρτάται από την επινοητικότητα του λογισμικού καθώς και από το πόσο ανανεωμένες είναι οι λίστες με τους απαγορευμένους τόπους. Διαφορετικά φίλτρα είναι αποτελεσματικά στο να αποκλείουν την πρόσβαση σε τόπους με διαφορετικό

περιεχόμενο. Για παράδειγμα, κάποιο φίλτρο μπορεί να είναι πιο αποτελεσματικό στο να αποκλείει την πρόσβαση σε τόπους με πορνογραφικό περιεχόμενο, ενώ κάποιο άλλο να είναι πιο αποτελεσματικό σε περιεχόμενο με βία η ρατσισμό.

Κάποιοι από τους παροχείς υπηρεσιών Ίντερνετ έχουν ήδη εγκαταστήσει λογισμικά φίλτρα στις υπηρεσίες τους. Σε αυτή την περίπτωση δεν είναι αναγκαία

3.2.5. Η νομική αντιμετώπιση σε Ελλάδα και Ευρωπαϊκή Ένωση

Όπως προείπαμε έχουν γίνει πολλές και ποικίλης αποτελεσματικότητας προσπάθειες από τα περισσότερα κράτη, ώστε να ρυθμισθεί το ζήτημα αυτό. τη συνέχεια θα εξετάσουμε την προσπάθεια νομοθέτησης στον ελλαδικό χώρο.

Στην Ελλάδα τα ποινικά ζητήματα όσον αφορά στη χρήση υπολογιστών και διαδικτύου αντιμετωπίστηκαν κυρίως από το νόμο 1805/1988, ο οποίος βασισμένος σε γερμανικά πρότυπα θέσπισε σημαντικές διατάξεις όπως το άρθρο 370Β και 370Γ ΠΚ που αφορούν τη παράνομη αντιγραφή και παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών καθώς και το 386Α που έχει ως αντικείμενο την απάτη με υπολογιστή αλλά και δευτερευόντως από το άρθρο 4 του νόμου 2246/1994.140

Αναλυτικότερα: Ο νόμος 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα. Μολονότι ο νόμος είναι σχεδόν 20 ετών, γεγονός, που ειδικά όσον αφορά στο συγκεκριμένο τομέα φαίνεται ανησυχητικά παλαιός, αναλογιζόμενοι τους ραγδαίους ρυθμούς με τους

[140] Βλ.,Νέστωρ Ε. Κουράκης – Εγκληματολογικοί ορίζοντες – τεύχος Β: Πραγματολογική προσέγγιση και επιμέρους ζητήματα. Σελ. 188

οποίους εξελίσσεται το διαδίκτυο και οι σχετικές δραστηριότητες, είναι γραμμένος με μία μελλοντική προοπτική, ώστε να εμφανίσει μία προσαρμοστικότητα και στα νέα δεδομένα που τυχόν θα παρουσιάζονταν.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου, τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

Το άρθρο 370Β προστατεύει όπως αναφέρθηκε την προστασία του απορρήτου από τις εισβολές και των hackers. Όπως αναφέρεται στο άρθρο αυτό: Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Το άρθρο 370Γ§2 Π.Κ προβλέπει ότι: Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) Ευρώ 10.000 δρχ.].Το άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988. Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου. Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του hacker στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία

διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών hackers όπως είναι οι cracker, whacker κλπ. Ανεξάρτητα του θεωρητικού ορισμού περί hacker που δώσαμε προηγουμένως θα πρέπει να σημειωθεί ότι ο νομικός ορισμός βάσει του άρθρου 370 Γ Π.Κ. διαφέρει, καθώς ως hacker μπορεί να οριστεί το άτομο εκείνο, το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

Το άρθρο αυτό εφαρμόζεται μόνο στις περιπτώσεις που έχουμε απλά εισβολή του hacker σε ένα σύστημα υπολογιστών χωρίς εξουσιοδότηση χωρίς να έπεται κάποια άλλη ενέργεια ή βλάβη. Εάν έχουμε και προσβολή άλλων εννόμων αγαθών εφαρμόζονται και οι αντίστοιχες σχετικές διατάξεις.

Οι προϋποθέσεις για την εφαρμογή του άρθρου 370 Γ §2 Π.Κ. είναι:

α) πρόσβαση σε στοιχεία. Ως πρόσβαση θεωρείται κάθε διείσδυση του δράστη, που αποβλέπει να λάβει γνώση των στοιχείων. Αντικείμενο της πρόσβασης είναι στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

β) η πρόσβαση αυτή να πραγματοποιείται χωρίς εξουσιοδότηση ή χωρίς κάποιο δικαίωμα. Σε περίπτωση που υφίσταται συγκατάθεση δεν πληρούται η αντικειμενική υπόσταση του άρθρου 370 Γ §2 Π.Κ. και συνεπώς δεν εφαρμόζεται. Σε περίπτωση που ο δράστης είναι στην υπηρεσία του νομίμου κατόχου των στοιχείων, τότε τεκμαίρετε ότι αυτός έχει το δικαίωμα νόμιμης πρόσβασης στα στοιχεία. Αυτό συνάγεται από την §3 του ίδιου άρθρου 370 Γ Π.Κ., σύμφωνα με την οποία η πράξη της §2 τιμωρείται, μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμού ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Η έλλειψη δικαιώματος πρόσβασης τεκμαίρετε ιδίως όταν γίνεται με παραβίαση οποιασδήποτε παραμέτρου ασφαλείας που να υποδεικνύει ότι ο νόμιμος χρήστης δεν επιθυμεί την παρέμβαση από ξένους παράγοντες στο σύστημά του. Μέθοδοι εξασφάλισης τέτοιας μορφής είναι τα συνθηματικά και οι κωδικοί αριθμοί χρήστη ή τα τείχη προστασίας(firewall) για παράδειγμα. Η διατύπωση του άρθρου 370 Γ§2 Π.Κ. είναι "αρκούντως ευρεία", ώστε να περιλαμβάνει κάθε πρόσβαση σε δεδομένα και αρχεία. Στην ευρεία αυτή διατύπωση του, οφείλεται και το γεγονός ότι, μπορεί να υπαχθούν στο άρθρο αυτό οι hackers και τα σχετικά περιστατικά hacking. Άλλωστε, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα. Το έγκλημα του άρθρου 370 Γ§2 Π.Κ. είναι έγκλημα διακινδύνευσης και όχι έγκλημα βλάβης.[141]

Όσον αφορά στο νόμο 2246/1994 άρθρο 4 αυτός αναφέρεται συμπληρωματικά σε παραβάσεις σχετικές με την άσκηση τηλεπικοινωνιακών δραστηριοτήτων. Όπως αναφέρει και το ίδιο το άρθρο: Στη διάταξη αυτή υπάγονται όλες οι περιπτώσεις παράνομης λειτουργίας ραδιοηλεκτρικών συστημάτων μετάδοσης μηνυμάτων και δεδομένων. Όποιος με οποιονδήποτε τρόπο παραβαίνει τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής, τήρησης του απορρήτου και διαφύλαξης της πνευματικής ιδιοκτησίας του περιεχομένου των μηνυμάτων και δεδομένων, που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων, που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματικές ποινές. Υφίστανται και άλλες παράμετροι όπως δήμευση του χρησιμοποιηθέντος εξοπλισμού καθώς και διατάξεις που κυρίως αφορούν στην παροχή υπηρεσιών χωρίς τις νόμιμες προϋποθέσεις που αφορούν κυρίως θέματα παροχής διαδικτυακών υπηρεσιών.[142]

[141] Βλ.,Διαδίκτυο και ποινική νομοθεσία – πηγή Internet
[142] Βλ., Τράπεζα νομικών πληροφοριών – πηγή Internet.

Επίσης το ζήτημα έχει εξεταστεί και από την Ευρωπαϊκή Ένωση. Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα:

α) Η Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime β) Η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology). Η σπουδαιότητα της σύστασης αυτής είναι πολύ μεγάλη, διότι καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο, οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων. Στη συνέχεια καταρτίσθηκε Διεθνής Σύμβαση (Ν. 185, Βουδαπέστη, 23.11.2001)για την αντιμετώπιση του διαδικτυακού εγκλήματος. Στην κατάρτιση της Σύμβαση αυτής έλαβε μέρος και η Ελλάδα. Σκοπός της Σύμβασης είναι η αποτελεσματική προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο θεσπίζοντας νομοθεσία, η οποία να ανταποκρίνεται στις ιδιαιτερότητες και αυξημένες απαιτήσεις του συγκεκριμένου κλάδου αλλά παράλληλα, όπως κατέδειξε και η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology), με μία διάθεση για ενιαίο και εναρμονισμένο ρυθμιστικό πλαίσιο, τουλάχιστον στις περισσότερες χώρες.

Η συζήτηση της Σύμβασης άρχισε τον Απρίλιο του 1997 με αρχικό χρονοδιάγραμμα περάτωσης το τέλος του έτους 1999. Λόγω όμως των ιδιαιτέρων προβλημάτων (η εξέλιξη της τεχνολογίας και η παρουσία νέων μορφών συμπεριφορών που θα μπορούσαν να θεωρηθούν ως αξιόποινες έτρεχαν ταχύτερα από τις εργασίες της Σύμβασης), η προθεσμία περάτωσης παρατάθηκε μέχρι το τέλος του έτους 2000. Η Σύμβαση περατώθηκε και έχει

ήδη υπογραφεί από αρκετά κράτη.[143] Η ανάλυση των επιμέρους παραμέτρων της σύμβασης αυτής απαιτεί ιδιαίτερη μνεία, η οποία θα υπερέβαινε τα όρια της συγκεκριμένης εργασίας.

Παρόλο όμως που υπάρχει ένα νομικό πλαίσιο το οποίο δείχνει να συντονίζει σιγά αλλά σταθερά τις προσπάθειες δίωξης των hackers είναι γεγονός ότι η εφαρμογή των νόμων και η καταστολή των hacking περιστατικών συναντά αρκετά προβλήματα για λόγους που θα αναλύσουμε στο ακόλουθο κεφάλαιο.

3.2.6. Προβλήματα δίωξης και καταστολής των hackers

Αρχικά, ιδιαίτερη μνεία θα πρέπει να κάνουμε στις διωκτικές Αρχές οι οποίες δυστυχώς ακόμη δε βρίσκονται ούτε στο κατάλληλο επίπεδο κατάρτισης για την αντιμετώπιση των πολύπλοκων τεχνικά ηλεκτρονικών εγκλημάτων, ούτε την κατάλληλη ψυχολογία και ευαισθητοποίηση διαθέτουν, ώστε να προσδώσουν τη βαρύτητα που απαιτείται στα τέτοιου τύπου εγκλήματα, ούτε βέβαια ο εξοπλισμός τους, πλην ελαχίστων εξαιρέσεων ανταποκρίνεται στις απαιτήσεις της δίωξης και ηλεκτρονικής σήμανσης. Όπως σημειώνεται στην έκθεση του Marc D. Goodman, το έγκλημα σχετικό με υπολογιστές έχει προβληματίσει τις Αρχές για αρκετό καιρό όμως η πλειοψηφία της αστυνομικής δύναμης παραμένει αδιάφορη απέναντι σε αυτό το φαινόμενο. Παρά τη ραγδαία αύξηση του ηλεκτρονικού εγκλήματος ένα 72% των αστυνομικών τμημάτων δεν διαθέτουν εξειδικευμένο προσωπικό για τη δίωξή του.[144]

Αξίζει να σημειωθεί ότι σε έρευνα του FBI σε ιστοσελίδες κυβερνητικών οργανισμών σε 428 χώρες διαπιστώθηκε ότι το 40% είχε παραβιαστεί, ενώ σύμφωνα με έκθεση που δημοσιεύει ο αμερικανικός όμιλος Science Applications International Corp. κάθε χρόνο 40 μεγάλες εταιρίες αναφέρουν

[143] Βλ.,Ιωάννης Εμμ. Αγγελής – Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη. πηγή Internet
[144] Βλ.,Marc D. Goodman – Why the police don't care about computer crime-Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997 Σελ. 478

ζημίες από hackers γύρω στα 800 εκατ. δολάρια. Όμοια στην Αγγλία το κόστος των επιθέσεων ανέρχεται στα 200 εκατ. λίρες.145 Η αστυνομία έχει ως στόχο την καταπολέμηση του εγκλήματος και τη διατήρηση της κοινωνικής ειρήνης. Εφόσον λοιπόν το έγκλημα του δρόμου παραμένει μία κύρια και προπάντων μία εμφανής απειλή με αντίκτυπο στην κοινή γνώμη φυσικό και λογικό είναι οι πόροι αλλά και το ενδιαφέρον της πλειονότητας των αστυνομικών οργάνων και των πολιτών να απευθύνονται σε πιο «απτές» μορφές εγκληματικότητας.146

Ειδικότερα, σημαντικότατο πρόβλημα είναι φυσικά και η έλλειψη κατάρτισης των ενασχολούμενων με τέτοιου τύπου εγκλήματα, καθώς ελάχιστοι σήμερα διαθέτουν την απαραίτητη γνώση σχετικά με την πληροφορική τεχνολογία και με τα τεχνικά χαρακτηριστικά και ιδιαιτερότητες του πληροφορικού εγκλήματος. Η έλλειψη κατάρτισης δεν πλήττει μόνο τις αστυνομικές αλλά και τις δικαστικές Αρχές και τους συνηγόρους των θυμάτων και θυτών. Οι γοργοί ρυθμοί της πληροφορικής τεχνολογίας είναι φυσικό να δυσκολεύουν ιδιαίτερα τους εφαρμοστές του δικαίου, καθώς μάλιστα αυτή τη στιγμή στην πλειοψηφία τους είναι άτομα, τα οποία έχουν μεγαλώσει χωρίς επαφή με ηλεκτρονικούς υπολογιστές. Έτσι παρουσιάζουν δυσκολίες στον προσδιορισμό, στην περιγραφή και τον τρόπο δίωξης των hacking περιστατικών. Επίσης σε συνδυασμό με την όχι σπάνια ανεπάρκεια στη νομοθεσία ή και σε ιδιαίτερες περιπτώσεις, όπως στις ΗΠΑ, επικαλυπτόμενη πολιτειακή και ομοσπονδιακή νομοθέτηση, η πλειονότητα των δικαστικών λειτουργών τείνει εκ φύσεως να ερμηνεύει τις σχετικές διατάξεις με βάση παραδοσιακά δεδομένα που συχνά όπως είναι εύκολα αντιληπτό, δεν ανταποκρίνονται και δεν αντιστοιχούν στα δεδομένα του πληροφορικού εγκλήματος.147 Και όπως οι νέες μορφές εγκληματικότητας δημιουργούν νέες τεχνικές και λειτουργικές ανάγκες και απαιτήσεις, έτσι

---

145 Βλ.,Εργαστήριο εφαρμογών πληροφορικής στα ΜΜΕ - πηγή Internet

146 Βλ.,Marc D. Goodman – Why the police don't care about computer crime-Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997, σελ. 477

147 Βλ., Γρ. Λάζος ,Πληροφορική και έγκλημα., σελ 216

«επαναδομούν» και τους ποινικούς νόμους και όρους αλλά και τις παραδοσιακές αντιλήψεις περί σήμανσης και πειστηρίων. Η μεταπήδηση από ένα περιβάλλον αστυνομικής έρευνας με υλικά, απτά στοιχεία σε ένα σύμπαν με αόρατα ηλεκτρονικά στοιχεία θα μπορούσε να δημιουργήσει ιδιαίτερα προβλήματα σε άτομα συνηθισμένα να εργάζονται με στοιχεία γραμμένα σε χαρτί, όπως υποστηρίζει ο Dan Duncan, εκπαιδευτής στο Federal Law Enforcement Training Centre.[148]

Ο χαρακτήρας του διαδικτύου που παρουσιάζει μία παγκοσμιότητα αλλά παράλληλα αποτελεί ένα νοητό επίπεδο της κοινωνίας, δημιουργεί πολλά προβλήματα και νομικά ζητήματα κατά την προσπάθεια αντιμετώπισης των hackers. Κι αυτό διότι τα άτομα αυτά χρησιμοποιώντας διάφορες μεθόδους (weaving, looping), είναι σε θέση να κρύβουν τα ίχνη τους αλλά και να διατρέχουν το διαδίκτυο μέσα από πολλά διαφορετικά συστήματα, τα οποία μπορεί να ελέγχουν παροδικά, ώστε να δημιουργούν εκτός από μία αυτονόητη δυσκολία εντοπισμού της πραγματικής τους τοποθεσίας, πολύ σημαντικά ζητήματα δικαιοδοσίας και έκδοσης, καθώς η νομοθεσία ποικίλει από χώρα σε χώρα.[149] Είναι πραγματικά άξιο προβληματισμού το ζήτημα επιλογής νομικού πλαισίου αντιμετώπισης ενός hacker που μπορεί να βρίσκεται σε μία χώρα, να επικοινωνεί με έναν παροχέα σε δεύτερη χώρα και να επιτίθεται κατά ενός θύματος του σε μία τρίτη χώρα. Τα ζητήματα του forum εδώ, κάθε άλλο παρά απλά είναι όπως εκτενώς παρουσιάζεται στα πονήματα «Against Cyberanarchy» και «Against Against Cyberanarchy» των Jack L.Goldsmith και David G. Post αντίστοιχα.

Μεγάλο ποσοστό της δραστηριότητας των hackers δε γνωστοποιείται ποτέ και αυτό φυσικά έχει να κάνει με λόγους κύρους ευθιξίας και επαγγελματικής φήμης μεγάλων οργανισμών αλλά και με το πολύ απλό ζήτημα ότι δε γίνονται πάντοτε αντιληπτές οι επιθέσεις. Συνεπώς το

[148] Βλ.,Marc D. Goodman – Why the police don't care about computer crime - Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997, σελ. 482
[149] Βλ., όπ.π., Marc D. Goodman, σελ. 483

πληροφορικό έγκλημα γίνεται ακόμη πιο δύσκολα αντιμετωπίσιμο καθώς τα θύματα δεν το αναφέρουν στην πλειοψηφία των περιπτώσεων. Ειδικά για τις μεγάλες εταιρίες, συχνά η ζημία του hacker είναι πολύ μικρότερη από τις απώλειες που θα υποστεί από την αρνητική δημοσιότητα και τη δυνητική απώλεια πελατών εξ αυτού του λόγου. Δεν έχουν εμπιστοσύνη στη αστυνομία για την ορθή αντιμετώπιση του προβλήματος και συχνά θεωρούν τη συμβολή τους αναποτελεσματική. Ένα **65%** του δείγματος έρευνας που διεξήχθη από το Computer Security Institute σε εταιρίες, ανέφερε οτι ο φόβος αρνητικής δημοσιότητας αποθάρρυνε από το να αναφέρει την εισβολή, ενώ ένα εντυπωσιακό **83%** ανέφεραν ότι δεν απευθύνθηκαν καν στην αστυνομία, όταν έπεσαν θύματα πληροφορικού εγκλήματος. Με τόσο ελλιπή ενημέρωση λοιπόν, είναι φυσικό να μην είναι δυνατή η αποτελεσματική αντιμετώπιση του φαινομένου, ενώ πολλές φορές οι πολυεθνικές φτάνουν αφού αποκρύψουν την εισβολή να επικοινωνούν με τον hacker και να τον στρατολογούν στις τάξεις τους, ώστε να έχουν το προβάδισμα στον ανταγωνισμό και την εμπορική κατασκοπεία.[150]

Συνοψίζοντας θα μπορούσαμε να κάνουμε μία αναφορά και σε επιμέρους στοιχεία που ενισχύουν τη δυσκολία ανακάλυψης και καταπολέμησης των hackers, όπως για παράδειγμα η ευκολία με την οποία είναι εφικτή η καταστροφή και εξαφάνιση κάθε στοιχείου του εγκλήματος ή η πραγματοποίηση του εγκλήματος μετά από ικανό χρονικό διάστημα ώστε να χαθούν τα όποια ίχνη[151] και φυσικά για τις νέες μεθόδους κρυπτογράφησης και κωδικοποίησης όπου η ψηφιακή πληροφορία μετατρέπεται σε άλλη μορφή μέσω ψηφιακού αλγορίθμου, ο οποίος δεν είναι αποκωδικοποιήσιμος χωρίς το συνθηματικό.

Συμπληρώνοντας και αυτό το κεφάλαιο ουσιαστικά κλείνουμε και με τα θεωρητικά ζητήματα που θα αποτελέσουν αντικείμενο αυτής της εργασίας. Κρίνεται σκόπιμο όμως να εξεταστούν τόσο τα μέσα και οι τρόποι που

[150] Βλ. ,όπ.π.,Marc D. Goodman. σελ. 486 - 487

[151] Βλ., Γρ. Λάζος, Πληροφορική και έγκλημα., σελ. 218 - 219

χρησιμοποιούνται από τους hackers για την επιτέλεση των σκοπών τους, όσο και μερικά περιστατικά στην πορεία του hacking που αποτέλεσαν σημαντικά γεγονότα και στιγμάτισαν τη δράση τους.

4. Είδη, μεθοδολογία και περιπτώσεις επιθέσεων

4.1. Είδη επιθέσεων

Αρχικά θα κάνουμε μία επιγραμματική αναφορά στους κυριότερους τρόπους με τους οποίους εκδηλώνεται παρανόμως η δράση των hackers και με πιο σκοπό.

1)Απόκτηση πρόσβασης σε ένα σύστημα υπολογιστή/ών με το «σπάσιμο» του κωδικού χρήσης

2)Καταστροφή - διαγραφή στοιχείων και κλοπή εμπιστευτικών αρχείων και πληροφοριών

3)Απόκτηση ελέγχου συστήματος και μεταβολή δεδομένων πρόσβασης με σκοπό τον αποκλεισμό χρηστών

4)Χρησιμοποίηση - διαχείριση ενός συστήματος υπολογιστή/ών για αποστολή δεδομένων σε τρίτο σύστημα

5)Παρεμπόδιση ομαλής λειτουργίας συστήματος με την επιβολή πρόσθετων εργασιών ή με την υπερφόρτωση με υπερβολικές ποσότητες δεδομένων.

Μετά από αυτή την απαρίθμηση σκόπιμο θα ήταν να διερευνήσουμε και τους τρόπους και τα μέσα που χρησιμοποιούν οι hackers για να επιτύχουν αυτούς τους στόχους.

4.2. Hacker: εργαλεία του επαγγέλματος

Denial of service (DoS attack):

Οι hackers τρέχουν πολλαπλά προγράμματα με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών τα οποία βομβαρδίζουν το δίκτυο με δεδομένα και έτσι το υπερφορτώνουν ώστε να αδυνατεί να ανταποκριθεί.

Distributed denial of service (DDoS attack):

Οι hackers με τη χρήση δουρείων ίππων αποκτούν τον έλεγχο πολλών υπολογιστών ανυποψίαστων χρηστών. Σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο και φυσικά μετά από την υπερβολική ζήτηση που αντιμετωπίζει, καταρρέει.

DNS Spoofing:

Στην περίπτωση αυτή ο hacker τροποποιεί το Domain Name Code το οποίο είναι η αριθμητική, δυαδικά ψηφιοποιημένη διεύθυνση του site, έτσι ώστε να την αντιλαμβάνεται και ο υπολογιστής και να ανταποκρίνεται στην εντολή. Οπότε οι χρήστες ζητώντας μία ιστοσελίδα με αλλοιωμένη την αριθμητική της διεύθυνση (numerical address), θα βρεθούν σε άλλη ιστοσελίδα αυτόματα. Αυτό μπορεί να σημαίνει απώλεια εσόδων για την ιστοσελίδα που δεν κατόρθωσε να επισκεφθεί ο χρήστης τελικά αλλά και με τη δημιουργία ενός ακριβούς αντιγράφου κάποιας ιστοσελίδας (mirror site) να εκμαιεύσει ο hacker ευαίσθητα προσωπικά δεδομένα που ο χρήστης πιστεύει ότι δίνει στην αληθινή ιστοσελίδα που ζήτησε.

Packet Sniffers:

Στην ουσία είναι προγράμματα που επιτρέπουν στο χρήστη να προσλαμβάνει και να ερμηνεύει πακέτα πληροφοριών που διακινούνται στο

διαδίκτυο. Κάθε πληροφορία που κοινοποιείται σε ένα δίκτυο υπολογιστών (όνομα χρήστη, κωδικός εισόδου, e-mail κλπ.) μεταφράζεται σε πακέτα, τα οποία στέλνονται στο δίκτυο. Το Internet λειτουργεί κυρίως με το Ethernet πρωτόκολλο μετάδοσης. Όταν λοιπόν κάποιος στείλει ένα πακέτο στο Ethernet, κάθε μηχάνημα στο δίκτυο βλέπει το πακέτο. Κάθε πακέτο που αποστέλλεται μέσω διαδικτύου έχει μία Ethernet κεφαλή-μία αριθμητική διεύθυνση, ώστε να είναι βέβαιο ότι η σωστή μηχανή παίρνει τη σωστή πληροφορία. Κάθε μηχάνημα υποτίθεται ότι εντοπίζει τα πακέτα δεδομένων με τη δική της διεύθυνση. Όμως το Ethernet packet sniffer είναι λογισμικό που επιτρέπει στο hacker ή το διαχειριστή του δικτύου κανονικά να υποκλέπτει πληροφορίες, οι οποίες δεν προορίζονται για τη διεύθυνσή του.

Δούρειοι Ίπποι:

Τα προγράμματα αυτά είναι «κερκόπορτες» σε ένα σύστημα υπολογιστή. Ο hacker μεταμφιέζει τον ίππο σε ένα άλλο πρόγραμμα, όπως για παράδειγμα παιχνίδι, ώστε να ξεγελαστεί ο χρήστης και να κατεβάσει και να εγκαταστήσει το πρόγραμμα. Μόλις ο ίππος εγκατασταθεί στον υπολογιστή του θύματος, ο hacker αποκτά πρόσβαση στο σκληρό δίσκο ή στο e-mail του χρήστη. Κρύβοντας προγράμματα ώστε να τρέξουν αργότερα ο hacker μπορεί να αποκτήσει πρόσβαση και σε άλλα συστήματα ή και να πραγματοποιήσει DDoS επιθέσεις. Ο απλούστερος ίππος αντικαθιστά τα μηνύματα που εμφανίζονται όταν ζητείται ένα συνθηματικό από τον χρήστη. Οι χρήστες παρέχουν τα ονόματα χρήστη και κωδικούς πρόσβασης θεωρώντας ότι συνδέονται στο σύστημα, ενώ στην ουσία αυτά καταγράφονται από τον ίππο προς χρήση του hacker. Ο διασημότερος ίππος είναι ο Black Orifice που δημιουργήθηκε από το hacker group: Cult of the Dead Cow και που προσφέρει πρόσβαση και έλεγχο σε κάθε προσωπικό υπολογιστή που λειτουργεί με το λειτουργικό σύστημα Windows 95/98 και επόμενα, εκμεταλλευόμενο ένα ελάττωμα σε ένα πρόγραμμα για αποστολή e-mail.

Ιοί και σκουλήκια:

Τα σκουλήκια και οι ιοί είναι αυτοαναπαραγόμενα προγράμματα, τα οποία μπορούν να εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο. Συνήθως οδηγούν στην καταστροφή και δυσλειτουργία συστημάτων και αρχείων. Τα σκουλήκια αντιγράφονται από υπολογιστή σε υπολογιστή χωρίς να απαιτούν τη συμβολή κανενός άλλου προγράμματος ή αρχείου. Το διασημότερο σκουλήκι «I LOVE YOU» υπολογίζεται ότι επηρέασε περίπου 45 εκατ. υπολογιστές.

4.3. Τα πιο σημαντικά περιστατικά hacking

Οι περιπτώσεις εδώ έχουν κάτι κοινό. Καθεμία από αυτές σηματοδοτεί και μία σημαντική εξέλιξη στην πορεία του hacking.

- Το 1988, ένας 23χρονος απόφοιτος του Κορνέλ, δημιούργησε το πρώτο *«σκουλήκι»*. Έγραψε 99 γραμμές κώδικα και το ελευθέρωσε στο δίκτυο πειραματικά. Πολλοί υπολογιστές κατέρρευσαν. Για να περιοριστεί η διάδοση της επιδημίας, πολλά δίκτυα αναγκάστηκαν να αποσυνδεθούν από το διαδίκτυο. Το 1990, Ο Μόρρις καταδικάστηκε σε 400 ώρες κοινωνικής υπηρεσίας και 10,000 δολάρια πρόστιμο. Μολονότι ο Morris επέμεινε οτι δεν είχε πρόθεση να προξενήσει ζημίες σε δίκτυα, παραδέχτηκε ότι επεδίωκε να αποκτήσει πρόσβαση στα «μολυσμένα συστήματα» και έτσι βρέθηκε ένοχος υπό το νόμο Computer Fraud & Abuse Act του 1986, για μη εγκεκριμένη πρόσβαση σε υπολογιστή κυβερνητικού ενδιαφέροντος, δηλαδή υπολογιστές που χειρίζεται αποκλειστικά η ομοσπονδιακή κυβέρνηση ή οικονομικά ιδρύματα.
- *Ένα διεθνές δίκτυο*, οι "Phonemasters", εισέβαλαν στα δίκτυα των εταιριών MCI WorldCom, Sprint, AT&T,και Equifax. Το FBI εκτιμά ότι η συμμορία προξένησε απώλειες του ποσού του 1.85 εκατ. δολαρίων. Οι Phonemasters αναφέρεται ότι προώθησαν μία γραμμή του FBI σε μία sex-chat γραμμή, δημιουργώντας λογαριασμούς γύρω στα 200,000

δολάρια. Εισέβαλαν σε αρχεία του FBI για να ανακαλύψουν ποιών τα τηλέφωνα παρακολουθούνταν από τη Δίωξη Ναρκωτικών. Εισέβαλαν στα συστήματα διαφόρων εταιριών και «κατέβασαν» νούμερα από τηλεκάρτες και προσωπικά δεδομένα πελατών και δημιούργησαν τηλεφωνικούς αριθμούς για δική τους χρήση. Το Σεπτέμβρη του 1999 μέλη του δικτύου αυτού καταδικάστηκαν για κλοπή, κατοχή συσκευών για μη εξουσιοδοτημένη είσοδο σε δίκτυα και σε κυβερνητικούς υπολογιστές. Ο υποτιθέμενος εγκέφαλος Lindsly καταδικάστηκε σε 41 μήνες φυλάκιση, μία από τις πιο αυστηρές ποινές για hacker στην Αμερική. Η υπόθεση των Phonemasters είναι η πρώτη όπου ο τίτλος III της Omnibus Crime Control and Safe Streets Act του 1968, αρχικά προορισμένος να επιτρέπει στις Αρχές να παρακολουθούν καλωδιακές και προφορικές επικοινωνίες, ερμηνεύθηκε έτσι, ώστε να επιτρέπει την τοποθέτηση «κοριού δεδομένων» σε ένα δίκτυο υπολογιστών.

- Η υπόθεση *Citibank* στιγμάτισε την κοινότητα των hackers. Το 1994, ο Ρώσος hacker Vladimir Levin οργάνωσε μία κλοπή, κάνοντας τους υπολογιστές της εταιρίας να διανείμουν περίπου 10 εκατ. δολάρια στον ίδιο και τους συνεργούς του σε 7 διαφορετικές χώρες. Όταν ο Levin δήλωσε ένοχος το Γενάρη του 1998, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς από πελάτες της Citibank για να μεταφέρει χρήματα στους λογαριασμούς του. Ενώ οι εκπρόσωποι της Citibank υποστήριξαν ότι ο Levin απέκτησε πρόσβαση στο σύστημα διαχείρισης ρευστού της εταιρίας μέσω έγκυρων λογαριασμών που δεν ήταν κωδικοποιημένοι, υπάρχει η φήμη ότι κάποιος μέσα από την εταιρία ήταν συνεργός του. Η Citibank όμως το αρνείται. Η Citibank κατάφερε να ανακτήσει τα περισσότερα χρήματα. Ο Levin δήλωσε ένοχος σε κατηγορίες συνομωσίας για τραπεζική απάτη και απάτη με υπολογιστές. Το Φεβρουάριο του 1998 ο Levin καταδικάστηκε σε 3 έτη φυλάκιση και υποχρέωση αποζημίωσης της Citibank 240,000 δολαρίων.
- *Το Μάιο του 2000,ο Timothy Lloyd* καταδικάστηκε ότι έγραψε 6 γραμμές κωδικού, στην ουσία μία βόμβα κωδικό, η οποία αφάνισε τα

προγράμματα σχεδιασμού και παραγωγής της Omega Engineering Corporation. Η βόμβα ήταν προορισμένη να πυροδοτηθεί στις 31 Ιουλίου του 1996. Με την είσοδό του στο σύστημα, ο υπάλληλος αυτός απελευθέρωσε τον κωδικό που έδωσε εντολή να σβηστούν τα προγράμματα παραγωγής της Omega. Η μυστική υπηρεσία δήλωσε ότι ο Lloyd είχε διαπράξει τη μεγαλύτερη πράξη computer sabotage, προξενώντας στην Omega σχεδόν 10 εκατ. δολάρια σε απώλειες πωλήσεων.

- Μετά το *«σκουλήκι» Morris* το σημαντικότερο αντίστοιχο φαινόμενο των επομένων ετών υπήρξε ο Melissa. Οι ζημίες υπολογίζονται περί τα 400 εκατ. δολάρια. Αποτέλεσε επίσης σημαντικό γεγονός και διότι ο Melissa ήταν το πρώτο περιστατικό τέτοιου τύπου που έπληξε το εμπορικό Internet. Τα πρώτα στοιχεία του Melissa βρέθηκαν σε μία δημοσίευση στο alt.sex newsgroup από ένα AOL e-mail. Ένας AOL server υπήρξε αγωγός για τον ιό, ο οποίος εμπεριέχετο σε ένα αρχείο ονόματι "list.zip." Τα θύματα που περίμεναν το list.zip να περιέχει μία λίστα από ιστοσελίδες σεξουαλικού περιεχομένου μαζί με τα ονόματα χρήστη και τους κωδικούς, κατέβαζαν και έτρεχαν το πρόγραμμα. Με τον τρόπο αυτό γίνονταν και οι ίδιοι κοινωνοί του ιού. Το Δεκέμβρη του 1999, ο δημιουργός δήλωσε ένοχος για δημιουργία και κυκλοφορία καταστροφικού και ζημιογόνου ιού και συμφώνησε ότι προκάλεσε περίπου 80 εκατ. δολάρια ζημίες. Εξέτισε και 5 χρόνια φυλάκισης.
- *Το Φεβρουάριο του 2000,* μερικά από τα πιο αξιόπιστα sites έγιναν σχεδόν μη προσβάσιμα από μία συντονισμένη επίθεση άρνησης εξυπηρέτησης [distributed denial-of-service (DDoS) attacks]. Το Yahoo δέχθηκε το πρώτο χτύπημα το Φεβρουάριο του 2000. Μερικές ημέρες αργότερα τοι ιστοσελίδες , Buy.com, eBay, CNN, Amazon.com, ZDNet.com, E*Trade, και Excite κατέρρευσαν από DDoS επιθέσεις. Οι εκτιμήσεις ζημιών ποικίλουν με το FBI να υπολογίζει ότι οι εταιρίες είχαν απώλειες της τάξης των 1.7 δις. Δολαρίων. Στις 18 Απριλίου του 2000 ένας νεαρός από τον Καναδά, γνωστός στο διαδίκτυο με το

ψευδώνυμο "mafiaboy," συνελήφθη ως σχετιζόμενος με τις εν λόγω επιθέσεις. Οι Αρχές ισχυρίστηκαν ότι εισέβαλε σε πολλούς υπολογιστές, κυρίως αμερικανικών πανεπιστημίων και χρησιμοποίησε τα δίκτυα αυτά για να εξαπολύσει τις επιθέσεις του στα sites αυτά. Σύμφωνα με την αστυνομία ο mafiaboy υπερηφανευόταν για την επίτευξη των επιθέσεων σε διάφορα Chat rooms και έτσι εντοπίστηκε. Τον Ιανουάριο του 2001 ο 16χρονος hacker ομολόγησε ένοχος σε 56 κατηγορίες, όπως απάτη και παράνομη χρήση δικτύου υπολογιστών.

4.4. Computer Forensics Science

Η Forensic Science είναι η επιστήμη που ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Ο έλεγχος του DNA και των δακτυλικών αποτυπωμάτων είναι ένα μικρό δείγμα από τις τεράστιες δυνατότητες της επιστήμης αυτής.

Η Computer Forensics Science είναι η εφαρμογή μεθόδων και τεχνικών έρευνας και ανάλυσης, με στόχο την εξακρίβωση των ενεργειών που έγιναν σε έναν υπολογιστή ή σε ένα δίκτυο, αλλά και την νομική τεκμηρίωση των στοιχείων που βρέθηκαν.

Όταν γίνει μια αξιόποινη πράξη, συχνά αφήνει πίσω της φυσικές αποδείξεις, όπως αποτυπώματα, υγρά, αίμα κλπ. Το όπλο με τα δακτυλικά αποτυπώματα είναι ένα σαφές, χειροπιαστό αποδεικτικό στοιχείο. Υπάρχουν διαδικασίες δοκιμασμένες και ασφαλείς που τις αποδέχεται κάθε δικαστήριο.

Όλο και πιο συχνά όμως οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή. Τα προβλήματα που προκύπτουν τότε είναι πολλά. Είναι αρκετά δύσκολο όχι μόνο να ανακαλύψουμε τα ψηφιακά ίχνη, αλλά και να τα συγκεντρώσουμε με τέτοιο τρόπο που να είναι αποδεκτά σε ένα δικαστήριο, αν χρειαστεί. Πρέπει να κάνουμε κάθε δυνατή πράξη ώστε να

αποκαλυφθεί η αλήθεια, και να αποφύγουμε κάθε παράλειψη που δημιουργεί ερωτηματικά.

Οι ψηφιακές αποδείξεις αποτελούνται από μαγνητικά πεδία και ηλεκτρικά ρεύματα. Είναι εύκολο να αλλοιωθούν, να διαγραφούν, να καλυφθούν από άχρηστα δεδομένα. Πριν από λίγα χρόνια δεν ήταν δυνατή η έρευνα, η εξαγωγή και η τεκμηρίωση των ψηφιακών αποδεικτικών στοιχείων. Σήμερα τα αποτελέσματα όλο και περισσότερων δικών εξαρτώνται από την νομική αλλά ταυτόχρονα και την τεχνική ικανότητα των εμπλεκομένων μερών να κατανοήσουν τι ακριβώς έγινε αλλά και τι θα έπρεπε να έχει γίνει.

Σύνοψη

Καταλήγοντας στο τέλος αυτού του κεφαλαίου για τους hackers θα λέγαμε ότι δεν είναι εφικτό να γίνει ένας διαχωρισμός εύκολα ως προς το κατά πόσο οι hackers είναι πληγή του κοινωνικού γίγνεσθαι, μία καταστροφική, ασυνείδητη κολλεκτίβα ή μία νέα ανερχόμενη δύναμη, ένας επαναστατικός άνεμος που μέσα από ένα νεοσυσταθέν σχετικά επικοινωνιακό μέσο και εργαλείο κοινωνικής αλληλεπίδρασης προσπαθεί να σταθεί εμπόδιο στις σύγχρονες αυταρχικές τάσεις που ζώνουν την ανθρώπινη καθημερινότητα. Η ουσία είναι ότι το hacking είναι σαν το μαχαίρι: μπορεί να μας βοηθήσει να τραφούμε, να επιβιώσουμε και να εξελιχθούμε ή να σκοτώσουμε και να σκοτωθούμε. Τη διαφορά θα την κάνει η επιλογή μας και όχι το εργαλείο. Αυτό υπάρχει και δεν είναι δυνατό να πάψει να υφίσταται. Και ας μην ξεχνάμε ότι η επανάσταση είναι μία οριακή κατάσταση και πολλές φορές τα όρια, είτε λόγω ζήλου, είτε από σκοπιμότητα καταπατούνται μέσα στην πραγματοποίησή της. Σκοπός δεν πρέπει να είναι η καταδίκη της επανάστασης, λόγω των φανατικών μελών της και των πράξεών τους, αλλά η συλλογική εκατέρωθεν προσπάθεια για αποπομπή των εγκληματικών και ανήθικων στοιχείων και η συνειδητοποίηση, διατύπωση και θεμελίωση των αποκτημάτων αυτής της αντίδρασης.

Κεφάλαιο 6ο: ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ

Εισαγωγή

Το Διαδίκτυο προάγει την επικοινωνία και τον τρόπο με τον οποίο οι άνθρωποι δουλεύουν και κινούνται μέσα στην σύγχρονη ψηφιακή κοινωνία καθώς έχει μειώσει τις αποστάσεις μεταξύ απομακρυσμένων χρηστών και προσφέροντας ένα απίστευτο αριθμό πληροφοριών συμβάλλει σημαντικά στην εκπαιδευτική διαδικασία.

Παρ' όλα αυτά, το κυριότερο πρόβλημα είναι η μη ασφάλεια αυτών των πληροφοριών καθώς απειλούνται από αλλοιώσεις και καταστροφές που μπορεί να προέρχονται από μη εξουσιοδοτημένη χρήση των πόρων του με άμεσο αποτέλεσμα την εμφάνιση διαφόρων τύπων ηλεκτρονικών εγκλημάτων, όπως η διανομή Παιδικού Πορνογραφικού υλικού. Για να κατανοήσουμε καλύτερα αυτή τη μάστιγα της σύγχρονης κοινωνίας, που πλέον βρίσκεται σε παγκόσμιο επίπεδο, θα δούμε πρώτα το φαινόμενο αυτό διαχρονικά.

1. Ιστορικές διαστάσεις της παιδικής πορνογραφίας

Όσο πιο προς τα πίσω πηγαίνει η ιστορία όλο και πιο ογκώδη βρίσκει κανείς την παραμέληση και τη σκληρότητα και όλο και περισσότερα παιδιά έχουν σκοτωθεί, απορριφθεί, χτυπηθεί, τρομοκρατηθεί και σεξουαλικά κακοποιηθεί από τους υπεύθυνους για την φροντίδα τους.

Ο ψυχοϊστορικός Lloyd deMause έχει γράψει εκτενώς για την κακοποίηση παιδιών. Στην «Ιστορία της Παιδικής Ηλικίας», απαριθμεί την εμπειρία παιδιών στην Ινδία και την Κίνα ως ιδιαίτερα καταχρηστική. Στην Ινδία, τα παιδιά αυνανίζονταν από τις μητέρες τους και οι ενήλικοι τα χρησιμοποιούσαν σεξουαλικά πολύ πριν φθάσουν στην ηλικία των δέκα. Το να μεγαλώνει κανείς στην Κίνα ήταν εξίσου σκληρό. Και στα αρσενικά και

στα θηλυκά παιδιά είχαν επιτεθεί σεξουαλικά και τα είχαν αναγκάσει να βγουν στη πορνεία. Τα αρχαία ελληνικά και ρωμαϊκά κορίτσια βιάζονταν συχνά, και ηλικιωμένοι χρησιμοποιούσαν συχνά μικρά αγόρια για την ικανοποίηση των σεξουαλικών τους ορέξεων. Μέχρι πρόσφατα, από τις αρχές μέχρι και τα μέσα του 20ου αιώνα, στις δυτικές χώρες τα παιδιά θεωρούνταν μικροί ενήλικοι καθώς εργάζονταν από πολύ μικρά σε ιδιαίτερα βαριές δουλειές.[152]

Η παιδική εκμετάλλευση υπήρξε πολύ πριν από το Διαδίκτυο, και τα δίκτυα των παραβατών που επικοινωνούσαν πριν από την ανακάλυψη των προσωπικών υπολογιστών ήταν μέρος της καθημερινής ζωής αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης παιδιών.

Η αυξανόμενη χρήση του Διαδικτύου από τους έφηβους και από τα πιο μικρά παιδιά δημιούργησαν την πιθανότητα δίωξης τους από τους ενήλικους παραβάτες. Καθώς όλο και περισσότερα παιδιά συγκεντρώθηκαν στο Διαδίκτυο στη δεκαετία του '90, οι ενήλικες που επιθυμούσαν να τους δελεάσουν για σεξουαλικές σχέσεις τους υποδέχθηκαν με χαρά. Τι συνέβαινε πριν από την ευρεία χρήση του Διαδικτύου;

Εάν ένας ενήλικος ενδιαφερόταν να έρθει σε σεξουαλική επαφή με ένα παιδί, θα επιδίωκε την επαφή με την εύρεση της απασχόλησης όπου θα υπήρχε έκθεση στα παιδιά, ή θα προσφερόταν εθελοντικά να συνεργαστεί με παιδιά, ή αποκτώντας με τον ένα ή τον άλλο τρόπο δικά του ή γίνονταν φιλικός με τα παιδιά γειτονιάς.

Φανταστείτε την απέραντη διαφορά στην τεχνολογία επικοινωνιών που έχει εμφανιστεί κατά τη διάρκεια του προηγούμενου τετάρτου του αιώνα.

---

[152] Βλ., Ενότητα 1.2, Κεφάλαιο 1, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

Η παιδική εκμετάλλευση υπήρξε από τα αρχαία, ακόμα, χρόνια ενώ τα δίκτυα παραβατών που επικοινωνούσαν πριν την ανακάλυψη των προσωπικών υπολογιστών και του Διαδικτύου ήταν μέρος της καθημερινής ζωής αν και χρειαζόταν μεγαλύτερη προσπάθεια να βρει κανείς και να εισάγει ένα δίκτυο εκμετάλλευσης των ανηλίκων.

Οποτεδήποτε πριν το 1995, ένα πρόσωπο που επιδίωκε τη σεξουαλική επαφή με ένα παιδί, είτε θα γινόταν ιερέας, δάσκαλος, κλόουν, πατέρας, θείος, οδηγός λεωφορείων ή θα κρυβόταν γύρω από τη παιδική χαρά της γειτονιάς.

Το 1996 στη Στοκχόλμη, το Παγκόσμιο Συνέδριο κατά της Σεξουαλικής Εκμετάλλευσης Παιδιών για Εμπορικούς Σκοπούς, είχε αναγνωρίσει ότι άτομα που επιδιώκουν σεξουαλική εκμετάλλευση και πορνογράφοι χρησιμοποιούν καταχρηστικά το Διαδίκτυο και ότι το πρόβλημα αυτό επιδεινώνεται συνεχώς. Για να δοθεί απάντηση σε αυτή την απειλή δημιουργήθηκαν δύο πρωτοβουλίες, η Internet Action (πρόγραμμα δράσης για τη βελτίωση της ασφάλειας του Διαδικτύου) και η πρωτοβουλία Internet Hotline Providers in Europe (INHOPE) Forum (το ευρωπαϊκό φόρουμ των προμηθευτών «κόκκινων γραμμών» του Διαδικτύου στην Ευρώπη).

Η πρωτοβουλία Internet Action, διοργάνωσαν σεμινάρια για άτομα που διαδραματίζουν κοινωνικούς ρόλους καθοριστικής σημασίας, στα οποία περιλαμβάνονταν εκπαιδευτικοί, κοινωνικοί λειτουργοί και αστυνομικοί καθώς και δημιούργησαν νέο υλικό και μετέφρασαν τις υφιστάμενες οδηγίες NetSmart για να τις διανείμουν σε επαγγελματίες που εργάζονται με παιδιά.

Η πρωτοβουλία INHOPE Forum έφερε σε επαφή τις τηλεφωνικές «κόκκινες γραμμές» που υπάρχουν στη Γερμανία, στις Κάτω Χώρες, στη Νορβηγία καθώς επίσης και εταιρείες που θα μπορούσαν να παρέχουν «κόκκινες γραμμές» στο Βέλγιο, τη Γαλλία, την Ιρλανδία και την Ισπανία.

1.1. Παιδική πορνογραφία - Ορισμός

Ο όρος «πορνογραφία» καθορίστηκε αρχικά το 1857 στο αγγλικό λεξικό της Οξφόρδης και παραπέμφθηκε νωρίτερα στο γαλλικό γράψιμο για να αναφερθεί στην πορνεία, στην αισχρολογία, και στις άσεμνες εικόνες.

Η πορνογραφία που επιδεικνύει τα παιδιά είναι το αποτέλεσμα της σεξουαλικής εκμετάλλευσης ή η σεξουαλική κακοποίηση ενός παιδιού.

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Ο κοινός παρανομαστής είναι οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή ή και καρτούν.

Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις.

Επιπλέον υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα. Σε ορισμένες χώρες για παράδειγμα, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας είναι έγκλημα (όπως στην Ισπανία).

Σύμφωνα με τη Σύμβαση για τα διαδικτυακά εγκλήματα του Συμβουλίου της Ευρώπης η παιδική πορνογραφία έχει τις εξής μορφές:

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

Γενικά θα μπορούσαμε να αναφέρουμε ότι :

Παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς.[153]

Κυρίως πρόκειται για μορφή σεξουαλικής εκμετάλλευσης με σκοπό το κέρδος. Υπό την επήρεια ναρκωτικών ουσιών ή με τη χρήση βίας, ανήλικα αγόρια και κορίτσια υποχρεούνται να συμμετέχουν σε σεξουαλικές πράξεις μεταξύ τους, με ενήλικες, ακόμη και με ζώα. Τα παιδιά (κάποιες φορές βρέφη, ηλικίας μικρότερης των 2 ετών), βασανίζονται, υφίστανται κάθε μορφή σωματικής και ψυχολογικής βίας και συχνά δολοφονούνται.

Οι παιδόφιλοι δράστες - πολύ συχνά - φωτογραφίζουν ή βιντεοσκοπούν τις σεξουαλικές τους εμπειρίες με ανήλικους, καθώς και σκληρές σκηνές κακοποίησης αυτών και προωθούν έπειτα το υλικό αυτό μέσω του διαδικτύου.

Τη δράση αυτή των συγκεκριμένων χρηστών του διαδικτύου εκμεταλλεύονται οι επιχειρήσεις παραγωγής πορνογραφικού υλικού, οι οποίες τροφοδοτούνται με «ανθρώπινο υλικό» από το ***trafficking*** παιδιών.

Πορνογραφικό υλικό συνιστά κάθε περιγραφή είτε πραγματική είτε εικονική, σε οποιοδήποτε υλικό φορέα, του σώματος ανηλίκου που αποσκοπεί στη γενετήσια διέγερση, καθώς και η καταγραφή ή αποτύπωση σε οποιοδήποτε υλικό φορέα, πραγματικής, προσποιητής ή εικονικής ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο.[154]

Ο αριθμός των παιδιών (ανήλικων) που υποχρεούνται σε σεξουαλικές επαφές on-line μέσω του διαδικτύου αυξάνεται δραματικά. Στα τέλη του 1997 βρίσκονταν σε «ζωντανή σύνδεση» 10 εκ. παιδιά παγκόσμια, έναντι του 1.1 εκ. το έτος 1995.

---

[153] Σύμφωνα με τον Προϊστάμενος Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος Διεύθυνσης Αττικής, Αστυνόμος Α΄ Εμμανουήλ Σφακιανάκης

[154] Βλ., όπ.π. υπ. 133

Ανήλικος, σύμφωνα με τις διατάξεις του άρθρου 121 Π.Κ., νοείται κάθε πρόσωπο ηλικίας από 8 έως 18 ετών, ενώ οι μικρότερες ηλικίες υπάγονται στην έννοια του παιδιού.

1.2. Πρώιμη τεχνολογία και παιδική πορνογραφία

Από τη στιγμή που οι άνθρωποι ξεκίνησαν να γράφουν, να σχεδιάζουν, να ζωγραφίζουν και να ασχολούνται με την γλυπτική και τη φωτογραφία, η ανθρώπινη μορφή και η σεξουαλική δραστηριότητα αποτελούσαν το κυρίως αντικείμενο ενός μεγάλου μέρους από αυτά, χαρακτηρίζοντας τα «δημιουργική διαδικασία».

Πριν από την ευρεία χρήση του Διαδικτύου, η ταχυδρομική υπηρεσία ήταν ο αρχικός τρόπος διανομής του υλικού της παιδικής πορνογραφίας ενώ το κόστος και ο κίνδυνος ήταν συνυφασμένος με αυτή αφού το παράνομο υλικό διατίθεντο σε περιορισμένη ποσότητα και πωλούταν σε ιδιαίτερη υψηλή τιμή.[155]

1.3. Τρόπος προσέγγισης ανηλίκων προ διαδικτύου

Προ Διαδικτύου, οι παιδόφιλοι επικοινωνούσαν είτε μέσω του ερασιτεχνικού ραδιοφώνου είτε μέσω οργανώσεων που επικοινωνούσαν μεταξύ τους και προσέφεραν διάφορες υπηρεσίες στα μέλη τους, π.χ. ενίσχυση για τους παιδόφιλους και μια σταθερή πηγή για νέες φιλίες και ανεφοδιασμό νέων θυμάτων. Μια τέτοια οργάνωση ήταν και η Childhood Sensuality Circle - CSC.

2. Διαδίκτυο & παιδική σεξουαλική επίθεση

Το Διαδίκτυο, παρέχει ένα νέο τόπο συναντήσεως για την εκμετάλλευση παιδιών, μειώνει τα αντικίνητρα με την παροχή ανωνυμίας και διευκολύνει την ανάπτυξη της φαντασίας δίνοντας στους θύτες ευκολότερη

[155] Βλ., Ενότητα 1.4, Κεφάλαιο 1, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

πρόσβαση σε ομάδες ομοϊδεατών περιορίζοντας την αίσθηση της περιθωριοποίησης.

2.1. WORLD WIDE WEB (W.W.W)

Ένας Ιστοχώρος είναι ένα σύνολο αρχείων, αποκαλούμενο «ιστοσελίδες» που είναι προσιτό μέσω του Διαδικτύου. Τα αρχεία αυτά περιλαμβάνουν εικόνες, ήχο, κείμενο, βίντεο και κάθε πιθανό συνδυασμό. Κάθε ιστοχώρος έχει μια διεύθυνση, τον Ομοιόμορφο Εντοπιστή Πόρων (URL) ενώ κάθε ιστοσελίδα αποτελείται από **HTML** «ετικέτες» ή σύνολα οδηγιών που λένε στον browser πώς να επιδείξει την κάθε ιστοσελίδα.

Δημιουργήθηκε το 1989 από την εφεύρεση της γλώσσας σήμανσης υπερκειμένων (**HTML**) και επέτρεψε την πρόσβαση των υπολογιστών στο Διαδίκτυο για να επικοινωνήσουν ο ένας με τον άλλο ακόμα και αν χρησιμοποιούν διαφορετικά λειτουργικά συστήματα.

2.2. Τρόποι επικοινωνίας μέσω διαδικτύου & η χρήση τους στη διανομή παιδικού πορνογραφικού υλικού

1. Δωμάτιο Συνομιλίας
2. Στιγμιαίο Μήνυμα (**IM**)
3. Ηλεκτρονικό ταχυδρομείο (**e-mail**)
4. Ηλεκτρονικές ομάδες (**e-groups**)
5. Κατάλογοι ηλεκτρονικών διευθύνσεων
6. Ομάδες πληροφόρησης
7. Πίνακας δελτίων (**BBS**)

2.3. Λογισμικές εφαρμογές που χρησιμοποιούνται για τη διανομή παιδικού πορνογραφικού υλικού

Οι έμποροι παιδικής πορνογραφίας, χρησιμοποιούν λογισμικές εφαρμογές για να διανείμουν το παράνομο υλικό. Ευρέως χρησιμοποιείται το Πρωτόκολλο Μεταφοράς Αρχείων (FTP) ενώ οι εφαρμογές Peer-to-Peer έχουν

αναπτυχθεί πρόσφατα. Διάφορες P2P εφαρμογές που χρησιμοποιούνται για την διακίνηση παιδικού πορνογραφικού υλικού είναι :

1. **KaZaA**
2. **Morpheus**
3. **Gnutella**
4. **WinMX**
5. **FreeNet**
6. **iMesh**

3. Παιδόφιλοι

Παιδόφιλος είναι εκείνος ο ενήλικας που σεξουαλικά προσελκύεται από παιδιά. Τα διαγνωστικά κριτήρια για ένα παιδόφιλο περιλαμβάνουν :

- **Επαναλαμβανόμενες** και **έντονες** σεξουαλικά φαντασίες, ωθήσεις ή συμπεριφορές που αφορούν σεξουαλικές πράξεις με ένα προεφηβικό παιδί.
- **Το άτομο** έχει δράσει με τέτοιες σεξουαλικές ωθήσεις ή αυτές οι σεξουαλικές ωθήσεις και φαντασίες είναι τα αίτια **μιας διαπροσωπικής δυσκολίας.**
- **Το άτομο είναι 16 ετών** ή μεγαλύτερο και έχει τουλάχιστον 5 χρονών ηλικιακή διαφορά από το παιδί.

Οι παιδικοί σεξουαλικοί κακοποιοί μπορούν να υποδιαιρεθούν σε 4 κριτήρια :

1. Η ηλικία του δράστη
2. Το φύλο του παραβάτη
3. Ο σεξουαλικός προσανατολισμός ή η προτίμηση
4. Ο τύπος των θυμάτων

Οι παραβάτες διακρίνονται σε δυο κατηγορίες :

5. Προνομιακό
6. Περιστασιακό

Ενώ με τη σειρά του, ο **περιστασιακός** παραβάτης, διακρίνεται :

1. στον Παλινδρομικό
2. στον Ηθικά άνευ Διακρίσεως
3. στον Σεξουαλικά άνευ Διακρίσεως και
4. στον Ανεπαρκή

Αυτοί που προτιμούν να κακοποιούν σεξουαλικά τα παιδιά, εκθέτουν τρία γενικά πρότυπα :

1. Προκλητικό
2. Εσωστρεφείς
3. Σαδιστές

Τέλος, το διάστημα *Οκτ. 2005- Μάιο 2006* διαπιστώθηκαν **692** αναφορές στο διαδίκτυο. Το **25.4%** αφορούσαν παραβατική συμπεριφορά, ενώ από τις παραβατικές αυτές αναφορές το **21.2%** αφορούσε την **παιδεραστία** και την **πορνογραφία**.[156]

3.1. Χρήσιμες πληροφορίες για τους παραβάτες

Υπάρχουν δύο προσεγγίσεις στη λήψη πληροφοριών για τους παραβάτες :

1. «Επαγωγική Σκιαγράφηση». Είναι η αναθεώρηση προηγούμενων ερευνών και παραβατών για να εξακριβωθούν οι τάσεις ή οι ομοιότητες μεταξύ αυτών,

[156] Βλ., εφημερίδες ΚΑΘΗΜΕΡΙΝΗ και ΒΗΜΑ. Έρευνα Ανδράς Χρήστος. παρουσίαση σε διεθνές συνέδριο 9/2006.

2. «Παραγωγική Σκιαγράφηση», σύμφωνα με την οποία συμπεραίνονται τα χαρακτηριστικά ενός παραβάτη από τα στοιχεία που είναι διαθέσιμα σε ένα συγκεκριμένο έγκλημα ή σε μια σειρά υπό έρευνα συνδεδεμένων εγκλημάτων.

3.2. Φτιάχνοντας το προφίλ του παραβάτη

Τα στατιστικά προφίλ των παραβατών προσφέρουν ελάχιστη βοήθεια σε μια έρευνα καθώς μπορούν να προσφέρουν μια εικόνα ενός χαρακτηριστικού παραβάτη, οι πληροφορίες όμως χάνουν την εξεταστική τους χρησιμότητα στον πραγματικό κόσμο. Το κυριότερο πρόβλημα είναι ότι μπορεί κάποιος να έχει ένα ή περισσότερα χαρακτηριστικά που να συνδέονται με την ύπαρξη παραβατών αλλά να μην είναι παραβάτης

Εάν θέτουμε πολύ ευρέα χαρακτηριστικά, υπάρχει κίνδυνος να χαρακτηριστούν πολλοί άνθρωποι παραβάτες («λάθος θετικότητα») ενώ αν θέσουμε τα χαρακτηριστικά με πολύ λεπτομέρεια υπάρχει ο κίνδυνος ο πραγματικός παραβάτης να ξεφύγει («λάθος αρνητικότητα»).

Συχνά, παρατηρείται ότι άτομα υπεράνω πάσης υποψίας, ακόμη και παντρεμένοι με παιδιά, εμπλέκονται στο κερδοφόρο «εμπόριο» φωτογραφιών με γυμνά παιδιά. Οκτώ στους δέκα κατηγορουμένους υποστηρίζουν ότι το κάνουν από το πάθος που έχουν για το γυμνό παιδικό κορμί. Ωστόσο δεν είναι λίγοι και εκείνοι που έχουν ως αποκλειστικό σκοπό την κερδοσκοπία, αδιαφορώντας για το περιεχόμενο των αρχείων ή αν πρόκειται για μικρά παιδιά.

Το ποσό που αγγίζει ο τζίρος από την παράνομη δραστηριότητα αποτελεί δέλεαρ για παιδόφιλους αλλά και επιχειρηματίες που διαθέτουν έναντι τιμήματος τους αποθηκευτικούς χώρους που διαθέτουν για να αναπτυχθούν οι ιστοσελίδες με την παιδική πορνογραφία. Βίντεο και φωτογραφίες με γυμνά παιδικά κορμιά κάνουν τον γύρο του κόσμου μέσω του Internet.

Σύμφωνα με στοιχεία που έχουν προκύψει από τις εξιχνιάσεις υποθέσεων σε όλον τον κόσμο, οι παιδόφιλοι προσεγγίζουν για να ικανοποιήσουν το πάθος τους συνήθως παιδιά και εφήβους από 12 ως 17 ετών. Παράλληλα οι διαχειριστές ιστοσελίδων με υλικό παιδικής πορνογραφίας χρησιμοποιούν ονομασίες ηρώων κινουμένων σχεδίων για να παραπλανούν τους επισκέπτες και να εισέρχονται στα site τους.

Η προώθηση των συγκεκριμένων site γίνεται ως επί το πλείστον μέσω chat rooms, ηλεκτρονικού ταχυδρομείου και ομάδων συζήτησης (newsgroup). Σχεδόν ποτέ δεν καταχωρούνται οι ιστοσελίδες στις μηχανές αναζήτησης (search engines). Στη συνέχεια ο διαχειριστής της ιστοσελίδας με το παράνομο υλικό στέλνει μέσω e-mail την ηλεκτρονική διεύθυνση, που σπανίως περιλαμβάνει λέξη σχετικά με παιδική πορνογραφία. Επίσης έχει διαπιστωθεί ότι μικρά παιδιά τη στιγμή που συμμετέχουν σε συζητήσεις στα δωμάτια επικοινωνίας ή στο e-mail τους δέχονται διαφημιστικά μηνύματα τέτοιων ιστοσελίδων.

Οι επισκέψεις που δέχονται καθημερινά οι ιστοσελίδες με υλικό παιδικής πορνογραφίας είναι χιλιάδες. Ανάμεσα στους επισκέπτες και μικρά παιδιά που οδηγούνται από την περιέργεια να ανακαλύψουν την ιστοσελίδα που τους έχει προτείνει ένας άγνωστος. Είναι χαρακτηριστικό ότι πολλά από τα παιδιά αυτά μόλις αντιλαμβάνονται το περιεχόμενο των ιστοσελίδων δεν αλλάζουν αμέσως σελίδα αλλά από περιέργεια την εξερευνούν. Στην αρχική σελίδα ο επισκέπτης βλέπει φωτογραφίες που αποτελούν «μαγνήτη» για τους παιδόφιλους.

Όποιος ενδιαφέρεται να μπει πιο βαθιά και να ανακαλύψει τον ηλεκτρονικό παράδεισο των παιδόφιλων πρέπει να καταβάλει διάφορα χρηματικά ποσά που ξεκινούν από 50 ως 60 ευρώ. Η καταβολή γίνεται αφού δώσουν τον αριθμό της πιστωτικής κάρτας τους. Όταν γίνει αυτόματα η πίστωση των χρημάτων στον διαχειριστή της ιστοσελίδας, παρέχεται ένας κωδικός πρόσβασης, το «κλειδί» για τα αρχεία. Επίσης για να επισπεύδουν

τον χρόνο αναπαραγωγής και καταχώρισης των αρχείων στα site, οι παιδόφιλοι χρησιμοποιούν πλέον τις κάμερες υπολογιστών.

3.3. Πως δρουν οι on line παραβάτες

Ο online σεξουαλικά κακοποιός, εκτός από τις υπολογιστικές αντιλήψεις, στηρίζεται σε δεξιότητες που έχουν χρησιμοποιηθεί από ομοϊδεάτες του και συχνάζει σε περιοχές, όπως τα δωμάτια συνομιλίας, όπου είναι πιθανό να υπάρχουν ανήλικα άτομα. Από τη στιγμή που θα ξεκινήσει η επικοινωνία με το θύμα, ο παραβάτης θα φροντίσει να του εμπνεύσει την εμπιστοσύνη, να του δείξει ότι το νοιάζεται και να δημιουργήσει μια σχέση εξάρτησης και αγάπης.

3.4. Τι είναι τα κυκλώματα παιδοφιλίας

Ένα κύκλωμα παιδοφιλίας είναι μια ομάδα ανθρώπων που εργάζονται μαζί μέσω Διαδικτύου σε διαφορετικές χώρες και υπό διαφορετικά νομοθετικά πλαίσια, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση.

Μπορεί επίσης να γίνεται και ανταλλαγή εμπειριών και γνώσεων ως προς την αποφυγή ανίχνευσης και το σχεδιασμό εγκληματικών ενεργειών εις βάρος παιδιών.

3.5. Πως τα κυκλώματα παιδοφιλίας χρησιμοποιούν το διαδίκτυο;

Υπάρχει μια ισχυρή εντύπωση ότι το Διαδίκτυο έχει γίνει ένας ισχυρός παράγων στην εξέλιξη των παιδοφιλικών κυκλωμάτων παγκοσμίως. Πολλές πρόσφατες καταδίκες στις Ηνωμένες Πολιτείες Αμερικής και στο Ηνωμένο Βασίλειο απέδειξαν ότι το Διαδίκτυο χρησιμοποιείται ευρέως από τα μέλη τέτοιων κυκλωμάτων, τόσο για να την ανταλλαγή εμπειριών όσο και για την διακίνηση φωτογραφιών παιδικής πορνογραφίας.

Η διάδοση της παιδικής πορνογραφίας προκαλεί μεγάλη ανησυχία στους διεθνείς φορείς που ασχολούνται με την προστασία των ανηλίκων.

Ανεξάρτητα από τους τρόπους που χρησιμοποιούνται για την διακίνηση φωτογραφιών παιδικής πορνογραφίας στο Διαδίκτυο, το πρόβλημα εξακολουθεί να είναι σοβαρό στη δυτική Ευρώπη, όπου αποκαλυφτήκαν σημαντικά κυκλώματα παιδικής πορνογραφίας στη Δανία, την Ισπανία, τη Γερμανία, την Ιταλία, την Ολλανδία, τη Σουηδία και το Ηνωμένο Βασίλειο. Καθώς αυτά τα δίκτυα χρησιμοποιούν εξελιγμένες τεχνολογίες τηλεπικοινωνιών , κάνοντας χρήση κρυπτογράφησης και κωδικών ονομασιών, γίνεται συνεχώς δυσκολότερη η ανακάλυψή τους από τις αρχές.

3.6. Τι σημαίνει ο όρος grooming ;

Το *grooming* είναι η διαδικασία κατά την οποία, παιδόφιλοι, προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα chat rooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν.

Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Μέσα από την σχέση αυτή προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή.

Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

3.7. Δελεασμός Ανηλίκου

Ο όρος «δελεασμός» αναφέρεται στους τρόπους με τους οποίους ένας σεξουαλικός παραβάτης αποκτά έλεγχο πάνω στα θύματα, εκμεταλλεύεται τις αδυναμίες τους για να κερδίσει την εμπιστοσύνη ή να τους ενσταλάξει το φόβο. Ο δελεασμός, συνήθως, περιλαμβάνει την εκμετάλλευση των αναγκών ενός θύματος όπως η μοναξιά, ο αυτοσεβασμός, η σεξουαλική περιέργεια ή απειρία, η έλλειψη χρημάτων και μέσα από αυτά να αναπτυχθεί ένας δεσμός ανάμεσα στον θύτη και στο θύμα. Τα στοιχεία δελεασμού δεν αποτελούν στοιχεία και αποδείξεις ενός εγκλήματος, αλλά μπορούν να χρησιμοποιηθούν για να παρουσιαστεί η κύρια πρόθεση του υπόπτου.[157]

3.8. Στατιστικά στοιχεία παιδικής πορνογραφίας

Πριν από πέντε χρόνια, οι καταγγελίες που δεχόταν η Αστυνομία για το κυβερνοέγκλημα ήταν περίπου μία κάθε μήνα. Σήμερα, όμως ανέρχονται σε **30** την ημέρα. Το **45-50%** αυτών των καταγγελιών αφορούν την παιδική πορνογραφία. Υπάρχουν περίπου **100.000 ιστοσελίδες** διακίνησης παιδικού πορνογραφικού υλικού, ο **ετήσιος τζίρος** ανέρχεται στο **1.000.000.000 €** ενώ τα έσοδα από τη γενικότερη διαδικτυακή πορνογραφία ανέρχονται στα **2,6.000.000.000 €** ετησίως. Τα στατιστικά στοιχεία που διαθέτει η Ε.ΚΑΤ.Ο. από έρευνα της Ευρωπαϊκής Επιτροπής είναι σοκαριστικά:[158]

---

[157] Βλ., Ενότητα 9.4 και 9.5, Κεφάλαιο 9, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

[158] Ενότητα 4.3, Κεφάλαιο 4, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

- *Τα μισά από τα παιδιά που χρησιμοποιούν το Διαδίκτυο δεν επιβλέπονται κατά τη διάρκεια της πλοήγησης*
- *Το **1/3** των γονέων που έχουν στο σπίτι υπολογιστή, έχουν εγκαταστήσει κάποιο φίλτρο προστασίας σε αυτόν.*
- *Ένας στους πέντε ανηλίκους έχει δεχθεί σεξουαλική προσέγγιση ή υποκίνηση στο Διαδίκτυο.*
- *Ένας στους 33 ανηλίκους έχει δεχθεί επιθετική σεξουαλική προσέγγιση, δηλαδή του ζητήθηκε από παιδόφιλο να συναντηθούν κάπου, ο παιδόφιλος επικοινώνησε τηλεφωνικά μαζί του ή έστειλε επιστολή, χρήματα ή δώρα για να τον παρακινήσει στη συνάντηση.*
- *Ένας στους τέσσερις ανηλίκους έχει εκτεθεί χωρίς να το επιθυμεί σε φωτογραφικό υλικό γυμνών ανθρώπων ή σεξουαλικών περιπτύξεων*
- *Μόνο το **17%** των νέων και το **11%** των γονέων γνωρίζουν έστω και έναν φορέα στον οποίο μπορούν να αναφέρουν ένα τέτοιο περιστατικό.*
- *Περίπου το **25%** των νέων που έχουν δεχθεί σεξουαλική προσέγγιση ή παρενόχληση το είπαν στους γονείς τους.*
- *Το **40%** αυτών που εκτέθηκαν σε ανεπιθύμητου περιεχομένου ιστοσελίδες το ανέφεραν στους γονείς τους.*

Οι Διαδικτυακοί τόποι που «φιλοξενούν» παιδικό πορνογραφικό υλικό αυξάνονται ραγδαία από το 2001. Συγκεκριμένα, παρατηρείται αύξηση έως και **345%** ενώ σταδιακά, εμφανίζονται **67** με **82** νέα sites μηνιαία και **8** με **21** καθημερινά.

Σύμφωνα με μια έρευνα που πραγματοποιήθηκε από το πανεπιστήμιο του New Hampshire σε παιδιά ηλικίας 10-17 ετών που χρησιμοποιούν το Διαδίκτυο:[159]

[159] Βλ., στο www.neodynamiko.gr. Επίσης βλ., στο www.politis.com.cy/cgibin/hweb?-A=635684&-V=archive και στο www.eportal.gr

- *Περίπου το ένα στα πέντε έλαβε κάποια μορφή σεξουαλικής παράκλησης πέρα του Διαδικτύου*
- *Το ένα στα τριάντα τρία έλαβε μια επιθετική σεξουαλική παράκληση (αίτημα να συναντηθεί, να συζητήσει τηλεφωνικώς, κ.λπ.)*
- *Το ένα στα τέσσερα εκτέθηκε σε ανεπιθύμητες εικόνες που περιείχαν γυμνό ή σεξουαλική δραστηριότητα*
- *Το ένα στα δεκαεπτά αισθάνθηκε απειλημένο ή παρενοχλημένο (σχετικά με κάποια σεξουαλικό περιεχόμενο)*
- *Τα κορίτσια στοχεύτηκαν ως σεξουαλικά θύματα δύο φορές περισσότερο από ότι τα αγόρια*
- *Το **77%** της νεολαίας που στοχεύτηκε ως πιθανά σεξουαλικά θύματα ήταν άνω των **14 ετών**.*
- *Αν και το **22%** της νεολαίας που θεωρήθηκε πιθανό θύμα ήταν ηλικίες **10** έως **13**, αυτή η ηλικιακή ομάδα ενοχλήθηκε δυσανάλογα από το γεγονός*
- *Οι ενήλικοι (οι περισσότεροι μεταξύ των ηλικιών 18 και 25) αποτέλεσαν το **24%** των σεξουαλικών παρακλήσεων*
- *Οι νεαροί αποτέλεσαν το **48%** των επιθετικών παρακλήσεων*
- *Η ηλικία ήταν άγνωστη για **27%** των προαγωγών*
- *Ελαφρώς περισσότερο από τα **2/3** των παρακλήσεων και των σε απευθείας σύνδεση προσεγγίσεων προήλθαν από αρσενικό φύλο*
- ***1/4** των επιθετικών προσεγγίσεων προερχόταν από θηλυκό φύλο*

3.9. Περιπτώσεις παιδικής πορνογραφίας

3.9.1. Πέδρο Λοπέζ: Το «Τέρας των Άνδεων»

Ο Πέδρο Λοπέζ, γνωστός και ως «Τέρας των Άνδεων», θεωρείται ο μεγαλύτερος εγκληματίας όσον αφορά στην παιδοφιλία. Κατηγορήθηκε για το βιασμό και τη δολοφονία 300 μικρών κοριτσιών 5-12 ετών, αν και - σύμφωνα με τον ίδιο και την αστυνομία της Κολομβίας- ο πραγματικός

αριθμός είναι κατά πολύ ψηλότερος. Ο ίδιος ισχυρίζεται ότι ο «άντρας του αιώνα», όπως αποκαλούσε τον εαυτό του, δολοφόνησε πέραν των 1.000 κοριτσιών.

Γεννημένος το 1949 στην Κολομβία από μητέρα ιερόδουλη, ο Λόπεζ από ηλικία 8 ετών έφυγε από το σπίτι, γιατί τον βίαζε ο φίλος της μητέρας του. Ζούσε στους δρόμους, όπου βιαζόταν επανειλημμένως από σοδομιστή. Αργότερα, μια αμερικανική οικογένεια τον πήρε στο σπίτι της και τον έστειλε σε σχολείο για ορφανά. Εκεί δέχτηκε ξανά επίθεση και βιασμό από το δάσκαλό του. Όταν συνελήφθη επειδή έκλεψε φαγητό σε ηλικία 18 ετών, φυλακίστηκε για ένα χρόνο. Εκεί τον βίασαν ξανά τρία μέλη μιας συμμορίας, τα οποία δολοφόνησε αργότερα.

Αφού αποφυλακίστηκε, ο ψυχολογικά διαταραγμένος νεαρός ξεκίνησε τα αποτρόπαια εγκλήματά του. Τριγυρνώντας σε φτωχά χωριά σε Κολομβία, Εκουαδόρ και Περού, αποπλανούσε νεαρά κορίτσια, τα βίαζε και στη συνέχεια τα στραγγάλιζε. Όπως ομολόγησε αργότερα, όταν δεν έβρισκε κοριτσάκια, ξέθαβε τα προηγούμενα θύματά του και προέβαινε σε νεκροφιλία. Το 1978, έχοντας δολοφονήσει ήδη 100 παιδιά, μια φυλή στο Περού τον τσάκωσε επ' αυτοφώρω. Καθώς ετοιμάζονταν να τον εκτελέσουν, μια Αμερικανίδα ιεραπόστολος επενέβη και τον παρέδωσε στην αστυνομία της χώρας. Αφού η αστυνομία δεν ενδιαφέρθηκε για τη δολοφονία φτωχών κοριτσιών, τον άφησε να φύγει με την προϋπόθεση να εγκαταλείψει τη χώρα.

Ο Λόπεζ αρκέστηκε σε Εκουαδόρ και Κολομβία. Μετά από εκατοντάδες δολοφονίες, ο αποτρόπαιος εγκληματίας έκανε ένα τραγικό λάθος. Δολοφόνησε ένα πλουσιοκόριτσο από την Κολομβία το 1980. Τότε οι Αρχές συγκινήθηκαν και αποφάσισαν να τον συλλάβουν. Λίγο αργότερα το πέτυχαν. Η ομολογία του αρχικά δεν έγινε πιστευτή, λόγω του αριθμού των θυμάτων. Η αστυνομία, όμως, πείστηκε όταν, μετά από μια πλημμύρα, αποκαλύφθηκε μαζικός χώρος ταφής 200 περίπου κοριτσιών στην Κολομβία.

Ολόκληρη η χώρα ξεχείλισε από οργή. Οι Αρχές λέγεται ότι τον μετακινούσαν συνεχώς στη χώρα με ελλιπή προστασία, για να μπορέσουν οι γονείς των θυμάτων να τον δολοφονήσουν. Κανείς, όμως, δεν έκανε τίποτα. Ο Λόπεζ καταδικάστηκε σε ισόβια φυλάκιση. Παραδόξως αποφυλακίστηκε το 1998 και έκτοτε χάθηκαν τα ίχνη του.

3.9.2. Επιχείρηση «PURITY»

Σύμφωνα με τον Προϊστάμενο του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος, Αστυνόμο Α', κ. Εμμανουήλ Σφακιανάκη, στη χώρα μας η διακίνηση παιδικής πορνογραφίας μέσω του Διαδικτύου δεν έχει λάβει ακόμη τα χαρακτηριστικά οργανωμένου εγκλήματος, καθώς οι δράστες λειτουργούν στη συντριπτική τους πλειοψηφία μεμονωμένα. Η επιχείρηση PURITY, είναι μία από τις μεγαλύτερες επιχειρήσεις που εκτέλεσε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Ασφάλειας Αττικής καθώς ύστερα από κατάλληλη ψηφιακή επεξεργασία ηλεκτρονικών ιχνών, προέκυψε η εμπλοκή ογδόντα (80) Ελλήνων χρηστών internet σε διεθνές κύκλωμα on-line εμπορίας υλικού παιδικής πορνογραφίας. Στα μέσα του Φεβρουαρίου το 2005, κλιμάκια Αστυνομικών της Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος, μετέβησαν και διενήργησαν έρευνες στις οικίες και σε λοιπούς χώρους των κατηγορουμένων στην Αθήνα, την Θεσσαλονίκη, τα Χανιά, την Μύκονο, την Λάρισα και την Δράμα. «Το ότι εξιχνιάζουμε περισσότερες υποθέσεις, σημαίνει ότι αυξάνεται συνεχώς και ο αριθμός των εμπλεκομένων», καταλήγει. Παράλληλα, εκφράζει την ανησυχία του, διότι μέσω του Διαδικτύου πολλοί παιδόφιλοι καταφέρνουν πλέον να προσεγγίζουν παιδιά, να συνομιλούν μαζί τους, ακόμη και να τα πείθουν να φωτογραφηθούν γυμνά.[160]

3.10. Ελληνική & Ευρωπαική Νομοθεσία

Οι έρευνες γύρω από την παιδική πορνογραφία διεξάγονται μετ' εμποδίων καθώς οι εταιρείες του Internet δεν κρατούν πάντα αρχεία που θα

[160] Βλ., www.kathimerini.gr-10/4/2005.gr

βοηθούσαν τους ανακριτές να εντοπίσουν ποια άτομα διακινούν παράνομο υλικό. Στην ελληνική έννομη τάξη δεν υπάρχει ειδική νομοθεσία σχετική με την παιδική πορνογραφία καθώς επίσης δεν υπάρχουν και εξειδικευμένα δικαστικά όργανα. Το θέμα καλύπτεται από το άρθρο 29 του ν.5060/1931, νόμου περί τύπου, προσβολών της τιμής εν γένει και άλλων σχετικών διατάξεων.

Το Δεκέμβριο του 2004, με απόφαση του Υπουργού Δικαιοσύνης κ. Αναστάση Παπαληγούρα, συστάθηκε Ειδική Νομοπαρασκευαστική Επιτροπή με σκοπό να επεξεργαστεί ένα σχέδιο νόμου το οποίο θα ενσωματώνεται στο εσωτερικό δίκαιο, το Προαιρετικό Πρωτόκολλο για την Εμπορία Παιδιών, την Παιδική Πορνεία και την Παιδική Πορνογραφία, που με τη σειρά του προσαρτάται στη Διεθνή Σύμβαση για τα Δικαιώματα του Παιδιού, στα πλαίσια του Ο.Η.Ε.

Το νομοσχέδιο προβλέπει τις εξής ρυθμίσεις:

- Αποσαφηνίζεται ο ορισμός της παιδικής πορνογραφίας και της ασελγούς πράξης
- Αποσυνδέεται ο σκοπός της κερδοσκοπίας από την αντικειμενική υπόσταση του εγκλήματος της διακίνησης πορνογραφικού υλικού, και αντικαθίσταται από την «πρόθεση».
- Προβλέπεται φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή από 10.000 έως 100.000 ευρώ για τη διακίνηση πορνογραφικού υλικού .
- Τιμωρείται αυστηρότερα (με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή από 50.000 έως 300.000 ευρώ) η ίδια πράξη, όταν τελείται μέσω Ηλεκτρονικού Υπολογιστή.
- Προβλέπονται επιβαρυντικές περιπτώσεις παιδικής πορνογραφίας, όπως πορνογραφία ανηλίκου κατ' επάγγελμα και κατά συνήθεια, που επισύρει ποινή κάθειρξης έως 10 έτη και χρηματική ποινή από 5.000 έως 100.000 ευρώ.

- Επιβάλλεται ποινή κάθειρξης τουλάχιστον 10 ετών και χρηματική ποινή από 100.000 έως 500.000 ευρώ, αν από την τέλεση της αξιόποινης πράξης της παιδικής πορνογραφίας προκληθεί βαριά σωματική βλάβη.

Παράλληλα, στο νομοσχέδιο περιέχονται ρυθμίσεις που εκσυγχρονίζουν το νομικό οπλοστάσιο της Ελλάδας και επεκτείνουν την προστασία των ανήλικων θυμάτων. Μεταξύ άλλων προβλέπονται :

- Αυτεπάγγελτος διορισμός συνηγόρου για τα θύματα παιδικής πορνείας και πορνογραφίας.
- Σύμπραξη παιδοψυχολόγου ή παιδοψυχιάτρου κατά την ανάκριση.
- Ψυχοδιαγνωστική εξέταση και θεραπεία και του θύματος και του δράστη.
- Αναστολή της παραγραφής καθ' όλη τη διάρκεια της ανηλικότητας του θύματος.
- Απαγορεύεται η δημοσιοποίηση περιστατικών τα οποία μπορεί να αποκαλύπτουν την ταυτότητα του ανήλικου θύματος.
- Δεν απαιτείται η αυτοπρόσωπη εμφάνιση του θύματος στο ακροατήριο, καθώς υποκαθίσταται από τη χρήση ηλεκτρονικού οπτικοακουστικού μέσου (μαγνητοταινία ή βίντεο).

Σύμφωνα με τις αποφάσεις του Ευρωπαϊκού Κοινοβουλίου όλα τα κράτη-μέλη υποχρεούνται να λάβουν τα κατάλληλα μέτρα ώστε να εξασφαλιστεί ότι σε ένα πρόσωπο που καταδικάστηκε για αδίκημα σχετικά με ανήλικο είναι δυνατόν να απαγορευθεί, προσωρινά ή μόνιμα, η άσκηση επαγγελματικών δραστηριοτήτων που σχετίζονται με συναλλαγές με ανηλίκους. Με τις προτεινόμενες αποφάσεις της Ευρωπαϊκής Ένωσης, ορίζεται ότι τόσο οι ποινικές καταδίκες όσο και οι σχετικές με την εργασία απαγορεύσεις θα πρέπει να εγγράφονται στο ποινικό μητρώο.

4. Οι επιδράσεις της παιδικής πορνογραφίας στον ψυχισμό των παιδιών

Σύμφωνα με τον κ. Χρήστο ΖΕΡΒΗ υπεύθυνο του τμήματος ψυχιατρικής εφήβων και νέων του ΓΝΑ «Γ. Γεννηματάς», η σεξουαλική παραβίαση ενός παιδιού, έτσι όπως λαμβάνει χώρα σε σκηνές που μεταδίδονται μέσω του Διαδικτύου, μπορεί να προκαλέσει ανεπανόρθωτη ζημιά στον ψυχισμό του, εξαιτίας τόσο της φύσης της σεξουαλικής πράξης όσο και της ανωριμότητας του ψυχισμού του νεαρού ατόμου που την υφίσταται.

Είναι μόνο κατά τη διάρκεια της εφηβείας και με προοδευτικό τρόπο που ο έφηβος οριστικοποιεί τη σεξουαλική του ταυτότητα και τις σεξουαλικές του προτιμήσεις, που μπορεί να διαχειριστεί, νοητικά, συναισθηματικά και σωματικά, τα σεξουαλικά μηνύματα και νοήματα και που θα επιχειρήσει τη σεξουαλική πράξη.

Κάθε εξωτερική ενέργεια που θα εισαγάγει το ανώριμο ακόμη σεξουαλικά παιδί ή τον έφηβο πρόωρα, βίαια και απότομα στη σεξουαλικότητα μπορεί να διαταράξει τις λεπτές αυτές διαδικασίες, που έχουν έναν εσωτερικό ρυθμό εκτύλιξης, και να καταστήσει το σεξουαλικό αντί για παράγοντα ωρίμανσης τραυματικό παράγοντα. Αν αυτό συμβεί, θα επηρεαστεί αρνητικά η σεξουαλική ή η γενικότερη ταυτότητα του ατόμου, ενώ μπορεί να προκληθούν και σημαντικά ψυχικά ή ψυχοσωματικά συμπτώματα.

5. Ο χάρτης του εγκλήματος

Τα δύο σημαντικότερα κέντρα διακίνησης πορνογραφικού υλικού είναι οι **Ηνωμένες Πολιτείες Αμερικής** (ΗΠΑ) και η **Ρωσία**. Είναι χαρακτηριστικό ότι περισσότερες από τις μισές παράνομες ιστοσελίδες φιλοξενούνται σε παροχείς Internet οι οποίοι εδρεύουν στις ΗΠΑ. Το φαινόμενο όμως παρουσιάζει έξαρση και στην Ανατολική Ευρώπη, στη Βρετανία και στη Λατινική Αμερική. Τα στοιχεία των Οργανώσεων Αυτορρύθμισης του Internet ανά τον κόσμο είναι ανατριχιαστικά και δεν αφήνουν περιθώρια παρερμηνειών σχετικά με το εύρος της παιδικής

πορνογραφίας στο Διαδίκτυο. Κάθε εβδομάδα προωθούνται **20.000** φωτογραφίες παιδιών. Σε ορισμένες περιπτώσεις, όπως π.χ. στις ΗΠΑ το 2005, σε μόλις έξι εβδομάδες προωθήθηκαν στο Internet **140.000** φωτογραφίες παιδιών.

Η ηλικία των παιδιών που απεικονίζονται κυμαίνεται μεταξύ 6 και 12 ετών, αλλά οι ειδικοί επισημαίνουν ότι σταδιακά ο μέσος όρος μειώνεται. Στον Καναδά οι αστυνομικές αρχές τα τελευταία τρία χρόνια έχουν εντοπίσει φωτογραφίες και βίντεο παιδιών ηλικίας από 2 ως 4 ετών.

Σύμφωνα με στοιχεία δικτύων για την καταπολέμηση της παιδοφιλίας στην Ευρώπη, 20 νέα παιδιά εμφανίζονται σε πορνογραφικές ιστοσελίδες κάθε μήνα, πολλά εκ των οποίων στη συνέχεια εκδίδονται στην αγορά λευκής σαρκός. Οι αμερικανικές υπηρεσίες υπολογίζουν ότι περισσότερες από **100.000** ιστοσελίδες προσφέρουν έναντι χρηματικού αντιτίμου υλικό παιδικής πορνογραφίας. Ο ετήσιος τζίρος υπολογίζεται από **200 εκατ. ευρώ ως και 1 δισ. ευρώ**. Οι ενδιαφερόμενοι πληρώνουν μέσω πιστωτικών καρτών μηνιαία συνδρομή 30-50 ευρώ και αποκτούν το δικαίωμα να «κατεβάσουν» φωτογραφίες ή βίντεο.

Οι παγκόσμιες διαστάσεις της παιδικής πορνογραφίας γίνονται φανερές και από τα ποσοστά που καταλαμβάνει διεθνώς στην κλίμακα του ηλεκτρονικού εγκλήματος. Το **45%-50%** των ηλεκτρονικών αδικημάτων αφορά παιδική πορνογραφία. Οι συλλήψεις και οι καταδίκες έχουν τετραπλασιαστεί τα τελευταία δύο χρόνια. Σύμφωνα με τα νέα στοιχεία μόνο στην *Αγγλία* και στην *Ουαλία το 2003* κατηγορήθηκαν για αδικήματα που σχετίζονται με την παιδική πορνογραφία **2.234 άτομα**. Στις ίδιες περιοχές της *Βρετανίας το 2001* είχαν κατηγορηθεί μόλις **549** άτομα. Πρόκειται για αύξηση των συλλήψεων κατά **307%** σε μόλις δύο χρόνια.

Παρά τις σημαντικές επιτυχίες των διωκτικών αρχών σε διεθνές επίπεδο, η παιδική πορνογραφία εξακολουθεί να έχει τεράστιες διαστάσεις. Μάλιστα, η διαρκής πρόοδος της τεχνολογίας προβληματίζει, καθώς το

Internet πλέον είναι προσβάσιμο σε ικανοποιητικές ταχύτητες και στους χρήστες των κινητών τηλεφώνων τρίτης γενιάς, μεταξύ των οποίων περιλαμβάνεται ένας ολοένα αυξανόμενος αριθμός μικρών παιδιών.

5.1. Πρόσφατα αποτελέσματα ερευνών

Παγκόσμια αύξηση στην παιδική πορνογραφία στο Διαδίκτυο αναφέρει ο Σύνδεσμος Ανοιχτών Γραμμών Ίντερνετ Παγκοσμίως, **INHOPE**, στην πρόσφατη δημοσίευσή του «Global Internet Trend Report». Οι επιβεβαιωμένες καταγγελίες για παιδική πορνογραφία που δέχεται το INHOPE κάθε μήνα φτάνουν τις **9.600.**

Το INHOPE που αποτελεί τον Σύνδεσμο Ανοιχτών Γραμμών Ίντερνετ Παγκοσμίως, αντιπροσωπεύει και συντονίζει ένα παγκόσμιο δίκτυο ανοιχτών γραμμών για αναφορές και καταγγελίες παράνομου, επιβλαβούς ή ύποπτου υλικού στο Διαδίκτυο.

Η στατιστική ανάλυση των αναφορών που δέχθηκε το δίκτυο για περίοδο 28 μηνών οδήγησε στην πρώτη λεπτομερή ανάλυση παράνομης διαδικτυακής δραστηριότητας.

Τα στατιστικά στοιχεία για την περίοδο Σεπτεμβρίου 2001 - Δεκεμβρίου 2006 μας δείχνουν ότι:

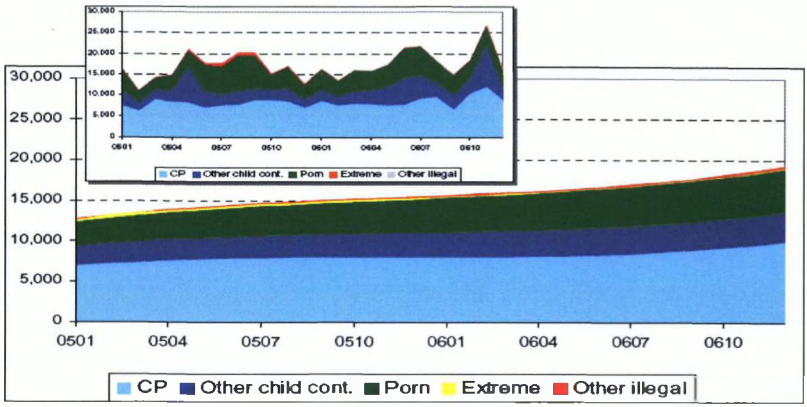
- Το δίκτυο INHOPE δέχτηκε **900.000** καταγγελίες από το ευρύ κοινό.
- Συνολικά το INHOPE επεξεργάστηκε **1.9** εκατομμύρια καταγγελίες.
- **160.000** καταγγελίες προωθήθηκαν στις διωκτικές αρχές - **5.800** καταγγελίες το μήνα κατά μέσο όρο.
- **21%** των καταγγελιών αφορούσαν παράνομο ή επιβλαβές περιεχόμενο (20.000/μήνα)
- **50%** αυτών αφορούσαν παιδική πορνογραφία.
- **19%** αφορούσαν άλλου είδους υλικό όπου εμπλέκονται παιδιά.
- **28%** αυτών αφορούσε πορνογραφία ενηλίκων.

Οι μηνιαίες τάσεις που προκύπτουν από τις αναφορές δείχνουν ότι:

- Η παιδική πορνογραφία *αυξήθηκε* κατά **15%.**
- Η πορνογραφία ενηλίκων *αυξήθηκε* κατά **24%.**
- Ο *ρατσισμός* και η *ξενοφοβία* αυξήθηκαν κατά **33%.**

5.2. Αναφορά INHOPE 2007

Αναφορές για παράνομο ή επικίνδυνο περιεχόμενο ,συγκεντρώθηκαν στατιστικά που κατά μέσο όρο είναι παράνομα σε τουλάχιστον μια χώρα που συνεργάζεται με το INHOPE. Ο παρακάτω πίνακας (1), συγκρίνει όλες τις αναφορές που θεωρήθηκαν παράνομες και που προήλθαν από μέλη του «κοινού», με τον όρο παράνομες όπως αυτός ορίζεται από το δίκτυο INHOPE.



© INHOPE 2007

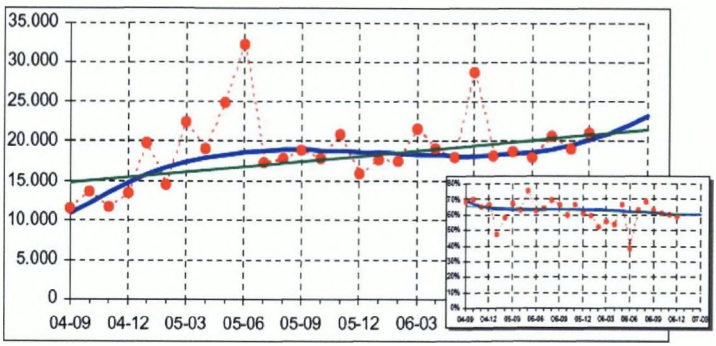
Πίνακας 6. 1: Αναφορές σε παράνομο περιεχόμενο

- Παιδική πορνογραφία
- Άλλο παιδικό περιεχόμενο
- Πορνογραφικό υλικό
- Ιδιαίτερα ακραίο υλικό
- Άλλο παράνομο υλικό

Ενδεχόμενο παράνομο ή επιβλαβές περιεχόμενο, περιλαμβάνει αναφορές για θέματα όπως: παιδική πορνογραφία, παιδικό trafficking, παιδικός τουρισμός για sex, παιδικό γυμνισμό, παιδικές ερωτικές/σε απρεπείς στάσεις φωτογραφίες παιδιών, ενήλικη πορνογραφία με πρόσβαση

σε παιδιά, ακραίο ενήλικο υλικό, ενήλικη πορνογραφία, ρατσιστικό περιεχόμενο, υλικό που προωθεί τη βία, τρομοκρατικό περιεχόμενο και περιεχόμενο με ναρκωτικά. (Τα παραπάνω δεν αποτελούν για όλες τις χώρες παράνομο υλικό).

Ο αριθμός των αναφορών για παράνομο ή επιβλαβές υλικό, ανέρχεται σε περίπου 19.000 αναφορές τον μήνα, το τελευταίο τρίμηνο του 2006. Η μεγαλύτερη επεξεργασία παράνομου υλικού ανέρχεται στις 32.000 αναφορές σε ένα μήνα. Ο μέσος όρος αύξησης του ποσοστού, μεταξύ του Σεπτεμβρίου 2004 και Δεκεμβρίου 2006, ήταν επιπλέον 200 αναφορές τον μήνα (περίπου +12% το χρόνο). Αναμένεται για την αρχή του 2007 130-270 επιπλέον αναφορές.



Πίνακας 6. 2: Γραφική αναπαράσταση της επικρατούσας τάσης.

- Οι ακριβείς μετρήσεις αναπαριστώνται στον πίνακα με τις ενωμένες **κόκκινες** κουκίδες .
- Η **μπλε** καμπύλη αναπαριστά την ακριβή αντίληψη για την τάση που επικρατεί .
- Η **πράσινη** γραμμή αναπαριστά τη γραμμική τάση της κλίσης του μέσου μηνιαίου ποσοστού μεταβολής .[161]

[161] Μετάφραση από την αναφορά του INHOPE 2007.

6. Το νομοθετικό πλαίσιο που υπάρχει στην Ελλάδα

Δημοσιεύθηκε (08.01.2008) ο Νόμος για την καταπολέμηση της σεξουαλικής εκμετάλλευσης, της παιδικής πορνογραφίας, τα νέα όρια των προσωπικών δεδομένων και τη χρήση καμερών κατά τη διάρκεια εκνόμων πράξεων.

Σε δύο φάσεις θα πραγματοποιηθεί η εφαρμογή του συνόλου των διατάξεων που περιλαμβάνονται στο νόμο 3625/2007, που ψηφίστηκε από τη Βουλή και περιλαμβάνει τρεις μεγάλες θεματικές ενότητες: [162]

Την κύρωση και εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία, που ενσωματώνεται στο εσωτερικό μας Δίκαιο και προσαρτάται στη Διεθνή Σύμβαση για τα Δικαιώματα του Παιδιού, στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών (άρθρα 17).

Σειρά νέων διατάξεων, οι οποίες εναρμονίζουν την Ελληνική νομοθεσία προς το περιεχόμενο του παραπάνω πρωτοκόλλου και άλλα διεθνή νομοθετήματα, για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών και της παιδικής πορνογραφίας, σε ένα σύνολο κατηγοριών (σεξουαλικός τουρισμός, ασέλγεια μεταξύ συγγενών, παιδική πορνογραφία στο διαδίκτυο, διανομή και χρήση υλικού παιδικής πορνογραφίας μέσω συστήματος Η/Υ ή με τη χρήση Διαδικτύου, προστασία της ιδιωτικής ζωής του ανηλίκου κλπ.).

Νέες ρυθμίσεις για τα προσωπικά δεδομένα, στην περίπτωση εγκλημάτων κατά της κοινωνίας και τη λειτουργία των καμερών κατά τη

---

[162] Βλ., στο www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=90 "Ηλεκτρονικό Έγκλημα" www.lawnet.gr "Η προς Ψήφιση Σύμβαση του Συμβουλίου της Ευρώπης για το Έγκλημα στο Κυβερνοχώρο : Η Σχέση της με την Ελληνική Έννομη Τάξη – Ιωάννης Εμμ. Αγγελής, Εισαγγελέας Πρωτοδικών"

διάρκεια συγκεντρώσεων, εφόσον επίκειται σοβαρός κίνδυνος για τη δημόσια ασφάλεια και μόνον κατόπιν εντολής εκπροσώπου της εισαγγελικής αρχής.

Η εφαρμογή των παραπάνω διατάξεων άρχισε από τις 24/12/2007, με τη δημοσίευση του νόμου 3625/2007 στην Εφημερίδα της Κυβερνήσεως (Τεύχος Ά, Αρ. φύλλου 290, 24/12/07).

Σύμφωνα με το Άρθρο 14 του Προαιρετικού Πρωτοκόλλου, η εφαρμογή του θα αρχίσει ένα μήνα αργότερα, δηλαδή στις 24/01/2008. Με τις παραπάνω ρυθμίσεις, διαμορφώνεται ένα νέο, αποτελεσματικό και ισχυρό οπλοστάσιο της Ελληνικής κοινωνίας και της νέας γενιάς απέναντι στα απειλητικά φαινόμενα της εκμετάλλευσης της εργασίας και της εμπορίας ανθρωπίνων οργάνων με θύματα παιδιά, της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της πορνογραφίας με πρωταγωνιστές παιδιά - φαινομένων που τείνουν να προσλάβουν διαστάσεις σύγχρονης μάστιγας και εμφανίζουν χαρακτηριστικά οργανωμένου εγκλήματος.

Βασικά σημεία των ρυθμίσεων του σχεδίου νόμου - μεταξύ άλλων αποτελούν:

Η αναμόρφωση του αδικήματος της παιδικής πορνογραφίας ώστε να κολάζεται ο δράστης και όταν ο σκοπός του δεν είναι η αποκόμιση κέρδους, σκοπός που παραμένει ως ιδιαίτερα επιβαρυντική περίσταση. Συγχρόνως προσδιορίζεται ως τιμωρητέο υλικό παιδικής πορνογραφίας η αναπαράσταση, ή πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο φορέα:

α) του σώματος ή μέρος του σώματος ανηλίκου με τρόπο που προδήλως προκαλεί γενετήσια διέγερση, β) πραγματικής ή εικονικής ασελγούς πράξης.

- Ο αυτεπάγγελτος διορισμός συνηγόρου σε ανήλικα θύματα.

- Η σύμπραξη κατά την ανάκριση παιδοψυχολόγου ή παιδοψυχιάτρου, που λειτουργεί με εχέγγυα πραγματογνώμονα.
- Η καταχώριση της κατάθεσης ανηλίκου θύματος σε ηλεκτρονικό μέσο.
- Η αποφυγή εμφάνισης του ανηλίκου θύματος σε ακροατήριο.
- Η ψυχοδιαγνωστική εξέταση και θεραπεία ανηλίκου θύματος και του δράστη των συγκεκριμένων εγκλημάτων.
- Η απαγόρευση δημοσίευσης περιστατικών, που μπορεί να οδηγήσουν στην εξακρίβωση της ταυτότητας του ανηλίκου θύματος με την απειλή ανάλογων ποινικών κυρώσεων.
- Η αναστολή της παραγραφής καθ' όλη τη διάρκεια της ανηλικότητας και μετά την ενηλικίωση του θύματος επί τρία έτη για τα κακουργήματα και επί ένα έτος για τα πλημμελήματα.
- Η εφαρμογή των ελληνικών ποινικών νόμων για τα εγκλήματα παιδικής πορνογραφίας και της διενέργειας ταξιδιών για την τέλεση συνουσίας ή άλλων ασελγών πράξεων σε βάρος ανηλίκου, που διαπράττονται από ημεδαπούς ή αλλοδαπούς -φαινόμενο γνωστό και διαδεδομένο ευρύτατα ως «σεξουαλικός τουρισμός».
- Η καθιέρωση ευθύνης νομικών προσώπων με βαρύτατες διοικητικές κυρώσεις.
- Η σύντομη εκδίκαση υποθέσεων σε όλους τους βαθμούς δικαιοδοσίας για τις συγκεκριμένες πράξεις που δεν μπορεί να υπερβεί τη διετία από την τέλεση ή διαπίστωσή τους.

Σύμφωνα με τις ανακοινώσεις στο Συνέδριο της Ελληνικής Καταναλωτικής Οργάνωσης (ΕΚΑΤΟ), στη Θεσσαλονίκη, για την ασφαλή πλοήγηση στο διαδίκτυο, ο πρόεδρος της Safeline, Νίκος Φρυδάς, ανακοίνωσε τα εξής:

Μέσα στο 2005, στα γραφεία της Safeline έφτασαν **288** καταγγελίες για ύποπτες ιστοσελίδες.

- **153** αφορούσαν κάποιο έγκλημα με θύμα ανηλίκους.
- Το **90%** αυτών των καταγγελιών οδηγούσαν σε ιστοσελίδες παιδικής πορνογραφίας .
- Το **28%** προερχόταν από την Ευρωπαϊκή Ένωση και το **10%** από χώρες της πρώην Σοβιετικής Ένωσης. το 5% ανήκε στην Ελλάδα. Το μεγαλύτερο ποσοστό ανήκε στις Η.Π.Α.[163]

6.1. Βαριές ποινές για την παιδική πορνογραφία

Σύμφωνα με άρθρο που δημοσιεύτηκε στην εφημερίδα Ελευθεροτυπία *στις* 16/11/2007 βαριές ποινές θεσπίζει, μεταξύ άλλων, το νομοσχέδιο για τους δράστες που διακινούν, ακόμη και μέσω ηλεκτρονικών υπολογιστών, πορνογραφικό υλικό με πρωταγωνιστές παιδιά, ενώ προβλέπει ότι το αδίκημα της παιδικής πορνογραφίας θα αποτελεί λόγο άρσης του απορρήτου των επικοινωνιών.

Θα τιμωρείται πλέον σε βαθμό κακουργήματος με ποινές από 5 έως 10 χρόνια όποιος παράγει, προσφέρει, πωλεί με οποιονδήποτε τρόπο, διαθέτει, αγοράζει, προμηθεύεται και κατέχει υλικό παιδικής πορνογραφίας, ανεξαρτήτως αν γίνεται μέσω ηλεκτρονικού υπολογιστή ή έχει σκοπό την κερδοσκοπία. Επίσης, θα υπάρχει ποινική ευθύνη και για τα νομικά πρόσωπα που εμπλέκονται στη διάπραξη των συγκεκριμένων αδικημάτων και θα προβλέπεται η προσωρινή ή οριστική διακοπή της λειτουργίας τους.

Σύμφωνα με τα αναλυτικά στοιχεία που μας παραχώρησε το τμήμα δίωξης Ηλεκτρονικού Εγκλήματος της ΓΑΔΑ και συγκεκριμένα ο επικεφαλής του κ. Σφακιανάκης Μανώλης σε συνεργασία με το Υπουργείο Δημόσιας Τάξης παρατηρούνται τα ακόλουθα:

---

[163] Βλ.. στο neodynamiko.gr/forum/viewtopic.php?t=1186 - 34k. *Δημοσίευση 23 Σεπ 2006 "Αρχονταρίκι"*

ΥΠΟΘΕΣΕΙΣ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΤΗΣ ΓΑΔΑ

Α/Α	ΗΜΕΡΟΜ.	ΠΕΡΙΓΡΑΦΗ	ΑΠΟΤ.ΠΟΙΝ.ΔΙΑΔΙΚ.	ΤΟΠΟΣ ΤΕΛΕΣΗΣ
1	21/4/2002	ΜΕΣΩ ΙΣΤΟΣΕΛΙΔΟΣ ΠΟΥ ΕΙΧΕ ΚΑΤΑΣΚΕΑΣΕΙ ΔΙΑΚΙΝΟΥΣΕ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ(ΑΓΟΡΙΑ 6-16 ΕΤΩΝ)-ΔΡΑΣΤΗΣ ΣΥΝΕΛΗΦΘΗ ΣΤΗΝ ΚΑΛΛΟΝΗ ΛΕΣΒΟΥ	ΑΥΤΟΦΩΡΟ ΤΡ. 8-ΜΗΝΕΣ	ΜΥΤΙΛΗΝΗ ΜΥΤΙΛΗΝΗ
2	13/6/2002	ΜΕΣΩ ΙΣΤΟΣΕΛΙΔΑΣ ΠΟΥ ΕΙΧΕ ΚΑΤΑΣΚΕΥΑΣΕΙ ΔΙΑΚΙΝΟΥΣΕ ΥΛΙΚΟ ΠΑΙΔ. ΠΟΡΝΟΓΡΑΦΙΑΣ (ΑΓΟΡΙΑ-ΚΟΡΙΤΣΙΑ 5-15 ΕΤΩΝ)-ΔΡΑΣΤΗΣ ΣΥΝΕΛΗΦΘΗ ΣΤΗΝ ΣΠΑΡΤΗ ΛΑΚΩΝΙΑΣ	ΑΥΤΟΦΩΡΟ 7-ΜΗΝΕΣ	ΣΠΑΡΤΗ
3	28/6/2002 ΔΥΟ ΚΑΤ.	2 ΑΔΕΡΦΙΑ ΑΠΟ ΑΘΗΝΑ, ΜΕΣΩ ΙΣΤΟΣΕΛΙΔΑΣ ΠΟΥ ΕΙΧΑΝ ΚΑΤΑΣΚΕΥΑΣΕΙ ΔΙΑΚΙΝΟΥΣΑΝ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔ. ΠΟΡΝΟΓΡΑΦΙΑΣ ΚΑΘΩΣ ΚΑΙ ΣΤΙΓΜΕΣ ΙΔΙΩΤΩΝ ΠΟΥ ΕΙΧΑΝ ΑΝΑΠΑΡΑΓΕΙ ΜΕ ΚΡΥΦΗ ΚΑΜΕΡΑ ΣΕ ΔΙΑΦΟΡΟΥΣ ΧΩΡΟΥΣ ΤΗΣ ΕΛΛΑΔΑΣ	ΦΥΛΑΚΙΣΗ 2 ΕΤΩΝ ΚΑΙ ΧΡΗΜΑΤΙΚΗ ΠΟΙΝΗ 10.000€ ΕΚΑΣΤΟΣ	ΑΘΗΝΑ
4	23/9/2002	ΕΠΙΛΟΧΙΑΣ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΣΤΡΑΤΟΥ ΔΙΑΚΙΝΟΥΣΕ ΑΠΟ ΚΟΙΝΟΥ ΜΕ ΣΥΝΕΡΓΟ ΣΤΗΝ ΚΥΠΡΟ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ.ΣΥΝΕΛΗΦΘΗ ΣΤΗΝ ΑΛΕΞΑΝΔΡΟΥΠΟΛΗ ΚΑΙ ΑΠΕΤΑΧΘΗ ΑΠΟ ΤΟ ΣΤΡΑΤΕΥΜΑ	ΣΤΡΑΤΟΔΙΚΕΙΟ	ΑΛΕΞ/ΠΟΛΗ
5	1/11/2002	ΔΙΑΚΙΝΟΥΣΕ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΚΑΙ ΣΥΝΕΛΗΦΘΗ ΣΤΗΝ ΔΡΑΜΑ	ΑΥΤΟΦΩΡΟ 9-ΜΗΝΕΣ	ΔΡΑΜΑ

6	20/12/2002 ΕΞΙ ΚΑΤ.	2 ΕΚΠΑΙΔΕΥΤΙΚΟΙ ΑΠΌ ΑΘΗΝΑ ΚΑΙ ΛΑΡΙΣΑ ΑΠΌ ΚΟΙΝΟΥ ΜΕ 4 ΣΥΝΕΡΓΟΥΣ ΔΙΑΚΙΝΟΥΣΑΝ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΚΑΙ ΣΥΝΕΛΗΦΘΗΣΑΝ ΣΤΙΣ ΑΝΩΤΕΡΟ ΠΟΛΕΙΣ ΚΑΙ ΣΤΟ ΑΚΡΑΙΦΝΙΟ ΘΗΒΩΝ. Η ΥΠΟΘΕΣΗ ΠΑΡΑΠΕΜΦΘΗΚΕ ΣΕ ΑΝΑΚΡΙΣΗ	ΕΚΚΡΕΜΕΙ ΔΙΚΗ ΑΝΑΚΡΙΤΗ 45,98,348,348Α,187Π.Κ. 3054/2002 2472/97 348Α,187,295 Π.Κ.	ΛΑΡΙΣΑ ΑΘΗΝΑ ΑΚΡΑΙΦΝΙΟ
7	31/1/2003 ΔΥΟ ΚΑΤ	ΜΕΣΩ ΚΑΤΑΣΚΕΥΑΣΜΕΝΗΣ ΙΣΤΟΣΕΛΙΔΑΣ ΔΙΚΑΙΝΟΥΣΑΝ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ. ΣΥΝΕΛΗΦΘΗΣΑΝ ΣΤΗ ΛΑΡΙΣΑ ΚΑΙ Υ ΥΠΟΘΕΣΗ ΠΑΡΑΠΕΜΦΘΗΚΕ ΣΕ ΤΑΚΤΙΚΗ ΑΝΑΚΡΙΣΗ	ΑΝΑΚΡΙΤΗ ΕΚΚΡΕΜΕΙ ΔΙΚΗ 98,42,348Α,5060/31	ΛΑΡΙΣΑ
8	22/2/2003 12 ΚΑΤΗΓ.	ΔΡΑΣΤΕΣ ΜΕΣΩ ΙΚΑΤΑΣΚΕΥΑΣΜΕΝΗΣ ΙΣΤΟΣΕΛΙΔΑΣ ΑΛΙΕΥΑΝ ΑΝΗΛΙΚΑ ΘΥΜΑΤΑ ΚΑΙ ΕΔΙΝΑΝ ΕΡΩΤΙΚΑ ΡΑΝΤΕΒΟΥ ΣΕ ΑΥΤΑ ΣΕ ΜΠΑΡ ΤΩΝ ΑΘΗΝΩΝ. ΔΡΑΣΤΕΣ ΣΥΝΕΛΗΦΘΗΣΑΝ ΚΑΙ Η ΥΠΟΘΕΣΗ ΠΑΡΑΠΕΜΦΘΗΚΕ ΣΕ ΤΑΚΤΙΚΗ ΑΝΑΚΡΙΣΗ	ΑΝΑΚΡΙΤΗ ΕΚΚΡΕΜΕΙ ΔΙΚΗ 348,353,98,45,348Α Π.Κ Ν.1729/87 Ν.5060/31	ΑΘΗΝΑ
9	10/3/2003	ΔΙΑΚΙΝΗΣΗ ΣΚΛΗΡΟΥ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΑΠΌ ΑΘΗΝΑ. ΔΕΝ ΣΥΝΕΛΗΦΘΗ ΕΛΛΕΙΨΕΙ ΑΥΤΟΦΩΡΟΥ	ΕΚΚΡΕΜΕΙ ΔΙΚΗ 348Α,361 Π.Κ.	ΑΘΗΝΑ
10	14/7/2003 2-ΚΑΤΗΓ	ΑΠΌ ΤΟΝ ΒΟΛΟ ΜΑΓΝΗΣΙΑΣ ΔΡΑΣΤΕΣ ΔΙΑΚΙΝΟΥΣΑΝ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΜΕΡΟΣ ΤΟΥ ΟΠΟΙΟΥ ΕΙΧΕ ΑΝΑΠΑΡΑΧΘΕΙ ΣΤΗΝ ΧΩΡΑ Μας. Ο 1ος ΤΩΝ ΚΑΤΗΓΟΡΟΥΜΕΝΩΝ ΠΡΟΦΥΛΑΚΙΣΤΗΚΕ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ 45,348Α,Ν.2472/97 Ν.5060/31	ΒΟΛΟΣ
11	17/9/2003 3-ΚΑΤ	ΜΕΣΩ ΒΙΝΤΕΟΚΛΑΜΠ ΚΑΙ ΑΓΓΕΛΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ	ΑΝΑΚΡΙΤΗΣ 2 ΕΤΗ ΦΥΛΑΚΙΣΗ	ΑΘΗΝΑ

		ΔΙΕΘΕΤΑΝ ΠΡΟΣ ΠΩΛΗΣΗ ΕΡΩΤΙΚΕΣ ΒΙΝΤΕΟΚΑΣΕΤΕΣ ΜΕ ΑΝΗΛΙΚΑ.ΤΟΥΣ ΕΠΕΒΛΗΘΗ ΠΟΙΝΗ ΦΥΛΑΚΙΣΗΣ 2 ΕΤΩΝ	45,98,348Α,Ν.5060/31	
12	26/9/2003	ΔΙΑΚΙΝΟΥΣΕ ΔΙΕΘΝΩΣ ΣΚΛΗΡΟΤΑΤΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΑΠΕΙΚΟΝΙΖΟΝ **ΒΡΕΦΗ ΣΕ ΑΣΕΜΝΕΣ ΣΤΑΣΕΙΣ.** ΣΥΝΕΛΗΦΘΗ ΚΑΙ ΠΡΟΦΥΛΑΚΙΣΤΗΚΕ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ 98,348Α Π.Κ.,Ν.5060/31	ΑΘΗΝΑ
13	6/11/2003	ΑΠΌ ΤΑ ΓΙΑΝΝΙΤΣΑ ΚΑΙ ΣΕ ΦΡΟΝΤΙΣΤΗΡΙΟ ΠΟΥ ΔΙΑΤΗΡΟΥΣΕ ΔΙΑΚΙΝΟΥΣΕ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΜΕ ΑΝΗΛΙΚΑ ΚΟΡΙΤΣΙΑ, ΕΠΙ ΤΟ ΠΛΕΙΣΤΟΝ ΜΑΘΗΤΡΙΕΣ ΤΟΥ. ΣΥΝΕΛΗΦΘΗ ΚΑΙ ΠΡΟΦΥΛΑΚΙΣΤΗΚΕ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ 98,348Α,Ν.5060/31	ΓΙΑΝΝΙΤΣΑ
14	16/12/2003 6-ΚΑΤΗΓ	ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ ΔΙΑΚΙΝΟΥΣΑΝ ΣΑΤΑΝΙΣΤΙΚΟ ΥΛΙΚΟ-ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ.ΣΥΝΕΛΗΦΘΗΣΑΝ ΣΕ ΑΘΗΝΑ-ΛΑΡΙΣΑ-ΘΕΣΣΑΛΟΝΙΚΗ. Η ΥΠΟΘΕΣΗ ΣΕ ΚΥΡΙΑ ΑΝΑΚΡΙΣΗ	ΑΝΑΚΡΙΤΗΣ 45,98,348ΑΠ.Κ.,Ν 5060/31 Ν.1363/38	ΘΕΣ/ΝΙΚΗ ΑΘΗΝΑ ΠΥΡΓΟΣ ΛΑΡΙΣΑ
15	28/1/2004	ΑΠΌ ΘΕΣΣΑΛΟΝΙΚΗ ΚΑΙ ΜΕΣΩ ΚΑΤΑΣΚΕΥΑΣΜΕΝΗΣ ΙΣΤΟΣΕΛΙΔΑΣ ΔΙΑΚΙΝΟΥΣΕ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ. ΣΥΝΕΛΗΦΘΗ ΚΑΙ Η ΥΠΟΘΕΣΗ ΣΕ ΚΥΡΙΑ ΑΝΑΚΡΙΣΗ	ΑΝΑΚΡΙΤΗΣ 98,348Α,Ν.5060/31	ΘΕΣ/ΝΙΚΗ

16	11/2/2004	ΔΙΑΚΙΝΟΥΣΕ ΣΚΛΗΡΟΤΑΤΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΤΟ ΟΠΟΙΟ ΑΠΕΙΚΟΝΙΖΕ ΑΚΟΜΗ ΚΑΙ ΒΡΕΦΗ ΣΕ ΠΕΟΘΗΛΑΣΜΟΥΣ. Η ΔΙΑΚΙΝΗΣΗ ΓΙΝΟΤΑΝ ΜΕΣΩ ΔΗΜΟΣΙΑΣ ΥΠΗΡΕΣΙΑΣ ΟΠΟΥ ΕΡΓΑΖΟΤΑΝ. ΔΡΑΣΤΗΣ ΠΡΟΦΥΛΑΚΙΣΤΗΚΕ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ 98,348Α,Ν.5060/31	ΑΘΗΝΑ
17	13/2/2004 2-ΚΑΤΗΓ.		ΑΝΑΚΡΙΤΗΣ 45,98,348,348Α,Ν.5060/31 Ν.2472/97	
18	12/3/2004	ΑΠΟ ΤΗΝ ΧΙΟ ΔΙΑΚΙΝΟΥΣΕ ΣΚΛΗΡΟΤΑΤΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ. ΣΥΝΕΛΗΦΘΗ-ΥΠΟΘΕΣΗ ΣΕ ΤΑΚΤΙΚΗ ΑΝΑΚΡΙΣΗ	ΑΝΑΚΡΙΤΗΣ 348Α-Ν.5060/1931	ΧΙΟΣ
19	27/5/2004	ΜΕΣΩ ΜΠΟΥΚΕΤΟΥ ΙΣΤΟΣΕΛΙΔΩΝ ΠΟΥ ΕΙΧΑΝ ΚΑΤΑΣΚΕΥΑΣΕΙ ΚΕΡΔΟΣΚΟΠΟΥΣΑΝ ΜΕ ΤΗΝ ΠΩΛΗΣΗ DVD ΟΠΟΥ ΠΡΩΤΑΓΩΝΙΣΤΟΥΣΑΝ ΑΝΗΛΙΚΑ ΠΡΟΣΩΠΑ. ΑΠΕΔΕΙΧΘΗ Η ΒΙΝΤΕΟΣΚΟΠΗΣΗ 16ΧΡΟΝΗΣ ΑΝΗΛΙΚΗΣ ΚΑΙ ΟΙ 3 ΠΡΩΤΟΙ ΠΡΟΦΥΛΑΚΙΣΤΗΚΑΝ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ 45,98,187,348Α Ν.2331/95 Ν.2472/97 Ν.2331/95 Ν.3028/2002	ΑΘΗΝΑ
20	15/7/2004	ΔΙΑΚΙΝΟΥΣΑΝ ΣΚΛΗΡΟ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ-ΥΠΟΘΕΣΗ ΣΕ ΚΥΡΙΑ ΑΝΑΚΡΙΣΗ-ΑΝΑΜΕΣΑ ΣΤΟΥΣ ΔΡΑΣΤΕΣ ΚΑΙ ΚΑΘΗΓΗΤΗΣ ΠΑΝΕΠΙΣΤΗΜΙΟΥ	ΑΝΑΚΡΙΤΗΣ 45,98,348Α Π.Κ.Ν.5060/1931 ΠΕΡΙΟΡΙΣΤΙΚΟΙ ΟΡΟΙ	ΑΘΗΝΑ ΘΕΣ/ΝΙΚΗ
21	23/7/2004	ΔΙΑΚΙΝΗΣΗ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΜΕΣΩ ΙΝΤΕΡΝΕΤ	348Α,45,Ν.5060/31 ΑΝΑΚΡΙΤΗΣ ΑΘΗΝΑ	ΠΕΡΙΟΡΙΣΤΙΚΟΙ ΟΡΟΙ
22	13/9/2004	ΔΙΑΚΙΝΗΣΗ ΥΛΙΚΟΥ ΠΑΙΔΙΚΗΣ	98,348Α Π.Κ	

	7519/3/47-Α	ΠΟΡΝΟΓΡΑΦΙΑΣ ΜΕΣΩ ΙΝΤΕΡΝΕΤ-ΦΩΤΟΓΡΑΦΙΣΗ ΓΥΜΝΩΝ ΑΝΗΛΙΚΩΝ-ΠΡΟΦΥΛΑΚΙΣΗ	ΑΝΑΚΡΙΤΗΣ ΠΡΟΦΥΛΑΚΙΣΗ	ΑΘΗΝΑ
23	7/7/2004	ΔΙΕΘΕΤΑΝ ΠΑΡΑΝΟΜΑ ΣΕ ΚΥΚΛΟΦΟΡΙΑ ΜΕΣΩ ΙΝΤΕΡΝΕΤ ΚΙΝΗΜΑΤΟΓΡΑΦΙΚΕΣ ΤΑΙΝΙΕΣ ΣΕ DVD-ΚΥΡΙΑ ΑΝΑΚΡΙΣΗ	45,98,394 2121/31	ΑΘΗΝΑ
24		ΔΡΑΣΤΕΣ ΕΙΧΑΝ ΚΑΤΑΣΚΕΥΑΣΕΙ ΙΣΤΟΣΕΛΙΔΑ ΑΠΟ ΟΠΟΥ ΕΠΙ ΠΛΗΡΩΜΗ ΔΙΑΚΙΝΟΥΣΑΝ ΥΛΙΚΟ ΠΑΙΔΙΚΗΣ ΠΟΡΝΟΓΡΑΦΙΑΣ ΚΑΙ ΠΡΟΣΩΠΙΚΕΣ ΣΤΙΓΜΕΣ ΑΝΥΠΟΠΤΩΝ ΠΟΛΙΤΩΝ ΜΕ ΧΡΗΣΗ ΚΡΥΦΩΝ ΚΑΜΕΡΩΝ ΚΑΙ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ ΜΕ ΚΑΜΕΡΑ. Ο 1ος ΤΩΝ ΔΡΑΣΤΩΝ ΠΡΟΦΥΛΑΚΙΣΤΗΚΕ	348Α, 98 Π.Κ. Ν.5060/31	ΑΘΗΝΑ ΣΕΡΡΕΣ

Πίνακας 6. 3: Υποθέσεις παιδικής πορνογραφίας σύμφωνα με τη ΓΑΔΑ

Επίσης, από τις **01/07/2004** μέχρι τις **20/01/2008** έχουν εξιχνιασθεί ηλεκτρονικά **130** υποθέσεις διακίνησης υλικού παιδικής πορνογραφίας. Από τις 130 υποθέσεις έχουν εκδικαστεί **32**, λόγω άρσης του απορρήτου[164], από τις οποίες συνελήφθησαν **41** άτομα και κατηγορούνται **110**.[165]

[164] Σύμφωνα με το Υπ. Δημόσιας τάξεως επιβεβαιώνονται τα ακόλουθα:«1. Η παράγραφος 2 του άρθρου 3 του ν.2472/1997 (ΦΕΚ 50Α) Σε ότι αφορά τα όρια προστασίας των προσωπικών δεδομένων. ο νέος νόμος επιτρέπει τη δημοσίευσή τους, **μετά από άδεια των εισαγγελικών ή δικαστικών αρχών**. από τη φάση της προανάκρισης έως εκείνη της δίκης για τις εξής περιπτώσεις, σύμφωνα με το άρθρο όγδοο. του νέου νόμου αντικαθίσταται ως εξής:

Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων η οποία πραγματοποιείται: α) από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών, β) από τις δικαστικές-εισαγγελικές αρχές και τις υπηρεσίες που ενεργούν υπό την άμεση εποπτεία τους στο πλαίσιο της απονομής της δικαιοσύνης ή για την εξυπηρέτηση των αναγκών της λειτουργίας τους με σκοπό τη βεβαίωση εγκλημάτων. που τιμωρούνται ως κακουργήματα ή πλημμελήματα με δόλο και ιδίως εγκλημάτων κατά της ζωής, κατά της γενετήσιας ζωής, κατά της προσωπικής ελευθερίας, κατά της ιδιοκτησίας, κατά των περιουσιακών δικαιωμάτων, παραβάσεων της νομοθεσίας περί ναρκωτικών, επιβουλής της δημόσιας τάξης, ως και τελουμένων σε βάρος ανηλίκων θυμάτων.

Ως προς τα ανωτέρω εφαρμόζονται οι ισχύουσες ουσιαστικές και δικονομικές ποινικές διατάξεις. Ειδικά για τα σχετικά με ποινικές διώξεις ή καταδίκες δύναται να επιτραπεί η δημοσιοποίηση μόνον από την εισαγγελική αρχή για τα αδικήματα που αναφέρονται στο εδάφιο β' της παραγράφου 2 του άρθρου 3 με διάταξη του αρμόδιου

6.2. Ασφάλεια και τρόποι προστασίας ανηλίκων

Οι κίνδυνοι για τα παιδιά που ελλοχεύουν από τη χρήση του Διαδικτύου μπορούν να είναι:[166]

- να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο
- να έρθουν σε επαφή με αγνώστους που μπορεί να τα βλάψουν
- να υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο
- ή ακόμα και να εθιστούν τόσο πολύ στη χρήση του που να κινδυνέψουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις ή τα παιχνίδια με τους φίλους τους.

Πώς θα αντιληφθούν οι γονείς ότι κάτι περίεργο συμβαίνει :[167]

- το παιδί λαμβάνει ανεξήγητα ή ύποπτα δώρα, από ανθρώπους που δεν γνωρίζουν ή δεν έχουν ακούσει ποτέ,
- το παιδί λαμβάνει τηλεφωνήματα από ενήλικους ή από μεγαλύτερους εφήβους που δεν γνωρίζουν,
- το παιδί ξοδεύει ιδιαίτερα μεγάλο χρονικό διάστημα στο Διαδίκτυο,

---

Εισαγγελέα Πρωτοδικών ή του Εισαγγελέα Εφετών, εάν η υπόθεση εκκρεμεί στο Εφετείο. Η δημοσιοποίηση αυτή αποσκοπεί στην προστασία του κοινωνικού συνόλου, των ανηλίκων, των ευάλωτων ή ανίσχυρων πληθυσμιακών ομάδων και προς ευχερέστερη πραγμάτωση της αξίωσης της Πολιτείας για τον κολασμό των παραπάνω αδικημάτων».

165 Βλ. στο www.kathimerini.gr/4dcgi/_w_articles_ell_156325_10/04/2005_139979 - 51k

[166] Βλ., στο Ενότητα 3.2, Κεφάλαιο 3, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

[167] Βλ., Ανθυπαστυνόμος Κωνσταντίνος Γ. Κούρος στο www.mopo.gr "Ηλεκτρονικό Έγκλημα ", Επίσης βλ., Σφακιανάκης Εμμανουήλ, Αστυνόμος Α', Προϊστάμενος Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος Διεύθυνσης Αττικής, και στο www.saferinternet.gr

- το παιδί γρήγορα αλλάζει το παράθυρο που έχει ανοιχτό στην οθόνη του υπολογιστή του ή τον κλείνει τελείως καθώς μπαίνει ο γονιός στο δωμάτιο του,
- το παιδί λαμβάνει ανεξήγητα και ύποπτα δώρα, ιδιαίτερα ψηφιακά, όπως φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεφωνικές κάρτες, υπολογιστές ή λεφτά,
- το παιδί γίνεται επιθετικό, τρέχει μακριά από το σπίτι ή ξεκινάει κάποια εγκληματική δραστηριότητα
- οι συνήθειες καλλωπισμού του παιδιού ή οι συνήθειες υγιεινής αλλάζουν. Αλλαγές στο ντύσιμο έτσι ώστε να κρύβουν το παιδικό του σώμα ή να το κάνουν να εμφανίζεται μη ελκυστικό θα πρέπει να προσεχθούν.

7. Θυματοποίηση

Τα θύματα των παραβατών μέσω Διαδικτύου δεν διαφέρουν σημαντικά από τα θύματα του φυσικού κόσμου εκτός από το γεγονός ότι το Διαδικτυακό θύμα είναι αρκετά μεγάλο σε ηλικία για να ξέρει πως να χρησιμοποιήσει έναν υπολογιστή και αρκετά εγγράμματος για να αλληλεπιδράσει Διαδικτυακά. Τέτοια παιδιά γενικά τείνουν να έχουν χαμηλό αυτοσεβασμό, έλλειψη επίβλεψης στη χρήση του Διαδικτύου, δυσλειτουργικές οικογένειες, κ.λ.π. Ενώ όλα αυτά τα γνωρίσματα μπορούν να είναι κοινά για το Διαδικτυακό θύμα, παρόλα αυτά δεν είναι απαιτούμενα γνωρίσματα τους.

Ένας άριστος σπουδαστής με μεγάλη αυτοπεποίθηση και μία θαυμάσια οικογενειακή ζωή δεν αποτελεί εξαίρεση από μια σεξουαλική παρενόχληση. Για παράδειγμα, μια δεκατριάχρονη μαθήτρια από τη Μινεσότα γνώρισε ένα άτομο που νόμιζε ότι ήταν 18 σε ένα δωμάτιο συνομιλίας AOL πριν από τα Χριστούγεννα. Μίλησαν στο τηλέφωνο πριν από την παραμονή του νέου έτους και συμφώνησαν να συναντηθούν κοντά στο σπίτι της. Αντί για τον δεκαοχτάχρονο, συνάντησε ένα σαρανταενός ετών άτομο που την πήγε σε ένα μοτέλ της έδωσε βίντεο-παιχνίδια για να παίξουν και κρασί για να πιει. Ο

άντρας στη συνέχεια βίασε το κορίτσι όταν αντιστάθηκε στις ορέξεις του, ενώ ένα δεκαπεντάχρονο κορίτσι βρέθηκε σε ένα κρατικό πάρκο της Νέας Υόρκης με ένα σαραντατριάχρονο καθηγητή ψυχολογίας να έχει σεξουαλική επαφή στο αυτοκίνητο του. Ο καθηγητής και το θύμα είχαν γνωριστεί στο Διαδίκτυο.[168]

Το θύμα ενός σεξουαλικού παραβάτη μπορεί να έχει συνεργαστεί με τον παραβάτη με κάποιο τρόπο με αποτέλεσμα να μην συνεργαστεί με το νόμο. Το θύμα μπορεί να αισθανθεί μια αίσθηση της πίστης στον παραβάτη, μπορεί έχει συμμετάσχει σε εγκλήματα (για παράδειγμα, στη μεταφορτωμένη ή εμπορική παιδική πορνογραφία), ή μπορεί απλά να θεωρεί τον εαυτό του επαναστατική φύση και να μην έχει συνειδητοποιήσει ότι στην ουσία έχει χρησιμοποιηθεί. Είναι δύσκολο για τους ανακριτές και τους κατηγόρους να ανακρίνουν ή να πάρουν οποιαδήποτε πληροφορία από ένα τέτοιο θύμα καθώς θεωρείται ο λιγότερο βέλτιστος μάρτυρας.

Είναι σημαντικό για το προσωπικό επιβολής του νόμου να καταλάβει ότι το να είναι επικριτικοί και αυστηροί με το θύμα δεν θα τους ωφελήσει και να δεχτούν το γεγονός ότι το κέρδος της συνεργασίας του θύματος μπορεί να πάρει έναν ιδιαίτερα μεγάλο χρονικό διάστημα. Παραδείγματος χάριν, σε μια έρευνα που έγινε σε δέκα παιδιά που βρεθήκανε μέσω συλλήψεων, κανένα από τα δέκα δεν εξέθεσε ότι είχε υποστεί οποιαδήποτε μορφής κακοποίηση.

Τα θύματα των παραβατών που αναφέρθηκαν παραπάνω μπορούν να διαφέρουν κάπως από τα θύματα της παιδικής πορνογραφίας, των οποίων οι εικόνες διανέμονται από το Διαδίκτυο. Τα θύματα που περιγράφονται παραπάνω είναι πιθανόν ακόμα να διαμένουν στο σπίτι, αν και αυτό δεν εγγυάται την ασφάλεια τους.

---

[168] Βλ., Ενότητα "Cyber Victims", Κεφάλαιο 3, Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP, Eoghan Casey MS, Michael Mc Grath MD Contributor, Elsevier Academic Press

Τα θύματα παιδικής πορνογραφίας είναι διαφόρων τύπων : παιδιά και έφηβοι που είναι υπό εκμετάλλευση από τους κηδεμόνες τους, θύματα στα οποία προσφέρονται οινόπνευμα ή/και ναρκωτικά και βιντεοσκοπούνται σε σεξουαλικές πράξεις είτε εν αγνοία τους είτε επειδή απειλούνται ή εκβιάζονται. Η ηθική κατάρρευση εκείνων που επιθυμούν να εκμεταλλευτούν δεν έχει κανένα όριο. Ακόμα, υπάρχουν λέσχες που αποτελούνται από γονείς που ανταλλάσσουν πορνογραφικό υλικό των ίδιων των παιδιών τους με άλλους ομοϊδεάτες. Έχει αναφερθεί ότι υπάρχει ακόμα και ζωντανό σόου με σεξουαλικές πράξεις όπου λαμβάνουν μέρος παιδιά το οποίο στέλνεται μέσω του Διαδικτύου σε κάθε ενδιαφερόμενο, διαβιβάζοντας παράλληλα οδηγίες στους ενήλικους συμμετέχοντες όσον αφορά αυτό που θα επιθυμούσαν να δουν να συμβαίνει με τους ενήλικους.

Εκείνοι που υλοποιούν παιδικό πορνογραφικό υλικό συχνά επιθυμούν να απεικονίσουν την πράξη τους ως ένα έγκλημα χωρίς θύματα. Αλλά αυτό σαφώς και δεν είναι έτσι σε πολλά επίπεδα. Σε ένα επίπεδο τίθεται απλά το θέμα της χρησιμοποίησης από εκείνους που έχουν μια πιστωτική σχέση προς ένα παιδί που μεγαλώνουν. Ακριβώς όπως ένας γονέας δεν πρέπει να πουλήσει το παιδί του για τη διάπραξη σεξουαλικής πράξης, δεν θα πρέπει και να το φωτογραφίσει για σεξουαλικό όφελος άλλων. Με το να ταχυδρομήσει ακόμη και τις πιο "αθώες" φωτογραφίες ή να τις καταστήσει διαθέσιμες σε άλλους με οποιοδήποτε τρόπο, γνωρίζοντας ότι ο στόχος είναι η σεξουαλική διέγερση, ο γονέας ή ο κηδεμόνας ουσιαστικά έχει καταδείξει μία πλήρη έλλειψη κατανόησης του ρόλου του. Σε ένα άλλο επίπεδο, εκείνος που έχει αναγκάσει τα παιδιά να συμμετέχουν σε σεξουαλικές σχέσεις με άλλα παιδιά ή με ενηλίκους τους τοποθετεί σε μια θέση που δεν είναι ψυχολογικά (ούτε και φυσικά) προετοιμασμένα και θα προκαλέσει σημαντική ζημιά στην ψυχοσεξουαλική ανάπτυξή τους όπως και στις μελλοντικές σχέσεις τους με άλλους γενικότερα. Ίσως το χειρότερο από όλα είναι εκείνες οι καταστάσεις στις οποίες τα παιδιά αναγκάζονται σε σεξουαλική δραστηριότητα με άλλους.

Μια κοινή τακτική των παιδόφιλων και των παιδικών προαγωγών είναι να παρουσιάσουν τη πορνογραφία (συμπεριλαμβανομένης της παιδικής πορνογραφίας) στα παιδιά ως ένα τρόπο που μειώνει τους όποιους δισταγμούς τους, κάνοντας το να φανεί ότι αυτός ο τύπος δραστηριότητας είναι αποδεκτός.

Υπάρχει μια ολόκληρη κουλτούρα στους παιδόφιλους που κυνηγούν κυρίως παιδιά τριτοκοσμικών χωρών, υποθέτοντας ότι είτε η κυβέρνηση είτε η οικογένεια, είτε και οι δύο μαζί δεν θα τα φροντίσουν. Η Ασία, η κεντρική και νότια Αμερική, είναι ο κύριος στόχος. Τα θύματα τείνουν να είναι φτωχά, ακαλλιέργητα και εύκολα παρασυρμένα από χρήματα ή άλλα δώρα. Περιπτώσεις όπως αυτήν του Marvin Hersh, ενός καθηγητή από τη Φλώριδα, συμβαίνει συχνότερα από ότι θα επιθυμούσαμε να πιστέψουμε ότι συμβαίνει. Ο Hersh ταξίδεψε στην Ασία και στην Κεντρική Αμερική για να έρθει σε σεξουαλική επαφή με ανηλίκους, δίνοντας σε αυτούς και στις οικογένειές τους χρήματα, ενδύματα, κ.λ.π.. Στόχευε τα θύματά του διαλέγοντας φτωχά παιδιά των οποίων οι γονείς ήταν ακαλλιέργητοι και τους έπειθε ότι τα βοηθούσε.

Δεν υπάρχει κανένας αξιόπιστος αριθμός για την εμπορική συμμετοχή παιδιών σε σεξουαλική εκμετάλλευση. Οι επίσημοι κυβερνητικοί αριθμοί δεν είναι αξιόπιστοι επειδή είναι πολύ χαμηλοί και οι αριθμοί που αναφέρονται από τις ομάδες υπεράσπισης είναι πιθανώς πάρα πολύ υψηλές.[169]

Συμπεράσματα

Η δραματική αύξηση του φαινομένου της παιδικής πορνογραφίας μέσω διαδικτύου αναγκάζει την Ευρωπαϊκή Ένωση να αντιμετωπίσει κατάματα το πρόβλημα και να ενώσει τις δυνάμεις της για την πάταξη αυτού του εγκλήματος.

[169] Βλ., Ενότητα 3.1. Κεφάλαιο 3. Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science by Monique Mattei Ferraro JD CISSP. Eoghan Casey MS. Michael Mc Grath MD Contributor. Elsevier Academic Press

Βίντεο που σοκάρουν αλλά και φωτογραφίες που ξεπερνούν ακόμα και την πιο διεστραμμένη φαντασία με παιδιά να κακοποιούνται σεξουαλικά κυκλοφορούν στις ιστοσελίδες του διαδικτύου ικανοποιώντας νοσηρές φαντασιώσεις και αρρωστημένα μυαλά.

Η παιδική πορνογραφία αποτελεί την ταχύτερα αναπτυσσόμενη επιχείρηση στο διαδίκτυο με έσοδα που ανέρχονται σε δισεκατομμύρια. Είναι λοιπόν κατανοητό γιατί χιλιάδες άνθρωποι ανά τον κόσμο εκπροσωπούν τη σκοτεινή πλευρά του κυβερνοχώρου χωρίς τύψεις, χωρίς ανθρωπιά, χωρίς συναίσθημα.

Αυτή την επιχείρηση όμως μπορούμε να την κλείσουμε αν συνεργαστούμε όλοι. Με πρώτη από όλους την αρμόδια αρχή, η οποία θα πρέπει να επιστήσει την προσοχή και να ενημερώσει την κοινή γνώμη για τη σοβαρότητα του προβλήματος, να παράσχει μια σφαιρική επισκόπηση της κατάστασης με τη κινητοποίηση όλων των ενδιαφερομένων φορέων (κυβερνήσεων, ειδικών οργανισμών του ΟΗΕ, ΜΚΟ, αστυνομικών υπαλλήλων, επιστημόνων κλπ.), και να εγκρίνει μια διακήρυξη και, κυρίως, ένα πρόγραμμα δράσης.

Χρειάζεται να ληφθούν ειδικά μέτρα προστασίας του παιδιού, κατά τη διεξαγωγή της ανάκρισης και της ακροαματικής διαδικασίας: Σε πολλές περιπτώσεις λείπει η γνώση για τα δικαιώματα του παιδιού. Σημαντικό θέμα είναι και η παροχή προστασίας στο παιδί-θύμα, μετά την διεξαγωγή της δίκης. Σύμφωνα με την επιταγή της Σύμβασης για τα Δικαιώματα του Παιδιού του ΟΗΕ, απαιτείται να δημιουργηθούν αποτελεσματικές διαδικασίες και καθιέρωση κοινωνικών προγραμμάτων που θα προσφέρουν την απαιτούμενη ψυχολογική και συμβουλευτική βοήθεια στο παιδί και σε όσους έχουν την επιμέλεια του. Τα κράτη πρέπει να εξασφαλίζουν ότι οι ανακριτικές και οι δικονομικές διαδικασίες δεν προκαλούν επιπρόσθετη ζημία στο θύμα (π.χ. επιτρέπεται η μαγνητοσκόπηση της κατάθεσης των παιδιών).

Σίγουρα, η προώθηση νομοθετικών ρυθμίσεων δεν αποτελεί τη μοναδική λύση στην όλη προσπάθεια. Απαιτείται να δοθεί έμφαση στις αιτίες που συνηγορούν στην ύπαρξη και διάδοση του φαινομένου.

Η φτώχεια, η εξαθλίωση, η ανεπάρκεια δομών προστασίας των παιδιών, η ανυπαρξία των μηχανισμών ελέγχου και πρόληψης, η έλλειψη παιδείας, η χαλάρωση του κοινωνικού ιστού τόσο σε οικογενειακό, όσο και σε διαπροσωπικό επίπεδο, η άγνοια και η ελλιπής ενημέρωση για το φαινόμενο του εγκλήματος και κυρίως η ύπαρξη σχετικής αγοράς προσφοράς και ζήτησης, που λειτουργεί μέσα στους κόλπους της Ευρωπαϊκής Ένωσης ευνοούν τη δημιουργία οργανωμένων ομάδων και εγκληματικών δικτύων που δεν διστάζουν στο βωμό του κέρδους να μετατρέψουν σε εμπόρευμα ακόμη και παιδικά σώματα και ψυχές.

Σίγουρα απαιτείται αφύπνιση, ευαισθητοποίηση και κινητοποίηση του συνόλου της κοινωνίας για την αποτελεσματική καταπολέμηση της εκμετάλλευσης των παιδιών και την προστασία της παιδικής ηλικίας.

Η παιδική πορνογραφία δεν είναι γόρδιος δεσμός, είναι θηλιά που λύνεται αλλά θέλει πρώτα να δοθεί γροθιά στο στομάχι της ίδιας της κοινωνίας.

Κεφάλαιο 7ο

Α' Μέρος - ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΔΙΚΑΙΟ

1.Εισαγωγή

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (internet). Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στον πεδίο του εγκλήματος στον κυβερνοχώρο (cyber crime), όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί «τον σταυρό του μαρτυρίου» για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

Ένα εξ ίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με την νομική πλευρά του θέματος από ποινική άποψη, είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων. Είναι ευνόητο ότι, η έλλειψη αυτή οφείλεται στο γεγονός ότι, το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος. Αποτελεί κοινή διαπίστωση ότι, η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση, από ότι η αντίστοιχη ποινική πλευρά. Αυτό οφείλεται στην μεγάλη επιρροή του κυβερνοχώρου, τόσο στο αστικό (σύναψη συμβάσεων εξ αποστάσεως δια του κυβερνοχώρου κλπ), όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο, νέα οικονομία κλπ).

Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του ημερήσιου Τύπου. Άλλωστε και το ίδιο το διαδίκτυο αποτελεί πηγή αντλήσεως πληροφοριών (ίσως την σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες - θέσεις (Sites).

2. Το γενικότερο πρόβλημα της νομικής ορολογίας

Πρέπει ιδιαιτέρως να τονιστεί ότι, η διαφορετική κατανόηση - αντίληψη των ίδιων εννοιών από τον τεχνικό και νομικό αποτελεί ένα από τα σημαντικότερα προβλήματα του υπό εξέταση θέματος. Έτσι, π.χ. διαφορετικά αντιλαμβάνεται την έννοια του όρου «κυβερνοχώρος», «ασφάλεια», «χάκερ» κλπ ο τεχνικός και διαφορετικά ο νομικός. Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος. Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ανατρέχει ο νομικός στη νομολογία, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει «φθάσει» η υπόθεση ή άλλη παρόμοια στο δικαστήριο. Σε περίπτωση που, ούτε νομολογία υπάρχει, ο νομικός ανατρέχει στη νομική επιστήμη, προς αναζήτηση θεωρητικής τουλάχιστον λύσης του θέματος. Αυτό βέβαια δεν σημαίνει ότι, η νομική θεωρία, όπως αυτή έχει αναπτυχθεί ή αναπτύσσεται από τη (νομική) επιστήμη, γίνεται υποχρεωτικώς δεκτή στην νομική πρακτική, δηλαδή στην διερεύνηση ή την εκδίκαση των σχετικών εγκλημάτων.

Στο υπό εξέταση λοιπόν θέμα, είναι απαραίτητο να προσδιοριστεί η νομική έννοια των όρων «ασφάλεια», «κυβερνοχώρος – διαδίκτυο», «χάκερ». Πριν απ' αυτό όμως κρίνεται απαραίτητο να οριοθετηθεί η έννοια του εγκλήματος στον κυβερνοχώρο, να προσδιοριστούν τα χαρακτηριστικά του (εγκλήματος στον κυβερνοχώρο), να καθοριστεί η σχέση μεταξύ εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή και να δοθεί το «προφίλ» του εγκληματία στον κυβερνοχώρο.

3. Το πρόβλημα της Ελληνικής νομικής ορολογίας

Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη - κατά κανόνα - στην Αγγλική γλώσσα. Η αντίστοιχη μεταφορά των όρων αυτών στα Ελληνικά, δεν είναι ούτε εύκολη, ούτε δόκιμη. Βέβαια κατά την καθημερινή πρακτική πολλοί όροι χρησιμοποιούνται στην ξενόγλωσση διάστασή των, κατά τρόπο που τείνουν να ενσωματωθούν και στο Ελληνικό νομικό λεξιλόγιο. Έτσι π. χ. αντί του Ελληνικού όρου "διαδικτυακό «έγκλημα» ή «έγκλημα στο διαδίκτυο» ή «έγκλημα στον κυβερνοχώρο» πολλές φορές χρησιμοποιείται αυτούσιος ο όρος Cyber crime ή Internet crime . Σχετικοί με το θέμα ξενόγλωσσοι όροι είναι: *Cyber crime, Internet, crime, Crime in cyberspace, On line crime, On line computer crime, communication crime, digital crime, electronic crime, electronic evidence, Computer crimes* (υπολογιστικά εγκλήματα), *Computer related crime*. Σχετικοί με τον δράστη όροι είναι: *hacker, Cracker, Internet freak, Cyber crook, Cyber freak, Internet freak.*

Το πρόβλημα αυτό της Ελληνικής νομικής ορολογίας παρουσιάζεται όχι μόνον στο πεδίο του ουσιαστικού ποινικού δικαίου, αλλά και στο αντίστοιχο του ποινικού δικονομικού .

Διευκρινίζεται ότι, στην παρούσα μελέτη γίνεται προσπάθεια χρησιμοποιήσεως των σχετικών όρων στην Ελληνική γλώσσα, για την πληρέστερη όμως κατανόηση των, χρησιμοποιείται σε παρένθεση και ο Αγγλικός όρος, όπου αυτό απαιτείται. Η ανάγκη παραθέσεως και των ξενόγλωσσων όρων προκύπτει από το γεγονός ότι, οι όροι αυτοί δεν έχουν ακόμα «δοκιμαστεί» στην Ελληνική νομική πρακτική. Έτσι για έννοιες με το ίδιο νομικό περιεχόμενο χρησιμοποιούνται στην Ελληνική γλώσσα διαφορετικοί όροι.

Σημειώνεται επίσης ότι, εκ των πραγμάτων είναι αδύνατο να αναφερθούμε στο διαδίκτυο και τη σχέση του με το ποινικό Δίκαιο, χωρίς

παραπομπές στην τεχνική πλευρά των ηλεκτρονικών υπολογιστών και στην τεχνολογία γενικότερα.

4. Η νομική έννοια του διαδικτύου και του κυβερνοχώρου

Η Ελληνική νομοθεσία δεν προσδιορίζει την έννοια του διαδικτύου ή του κυβερνοχώρου. Κατά συνέπεια οι έννοιες αυτές λαμβάνονται από την τεχνολογία. Έτσι λοιπόν, ως διαδίκτυο (internet) μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ των, ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το internet, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών, όπου δηλαδή η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση. Στο άρθρο 2 του Ν 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών προσδιορίζονται οι έννοιες «δίκτυο καλωδιακής τηλεόρασης», «ιδιωτικό δίκτυο», «παροχή ανοικτού δικτύου» και «τηλεπικοινωνιακό δίκτυο». Δεν προσδιορίζεται όμως η έννοια του διαδικτύου ή του κυβερνοχώρου.

Πρέπει να λεχθεί ότι, στη συνείδηση του μέσου νομικού, δεν γίνεται διάκριση μεταξύ διαδικτύου και κυβερνοχώρου και κατά κανόνα οι έννοιες αυτές θεωρούνται ως ταυτόσημες και χρησιμοποιούνται πάντα με το ίδιο περιεχόμενο.

5. Προσδιορισμός της εννοίας του εγκλήματος στον κυβερνοχώρο

Δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στην διεθνή νομοθεσία, ούτε στην διεθνή νομολογία ή βιβλιογραφία . Ομοίως ούτε στην Ελληνική βιβλιογραφία υπάρχει ορισμός του εγκλήματος στον κυβερνοχώρο.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό έγκλημα» και η μόνη

διαφορά που το διακρίνει απ' αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον, (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται πλήρως στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μια άλλη κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικά σε περιβάλλον του κυβερνοχώρου. Σύμφωνα με τον Ι.Αγγέλη,[170] τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

α) Σε εγκλήματα που διαπράττονται τόσο σε «κοινό» περιβάλλον, όσο και στο διαδίκτυο (internet) π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελείται σε «περιβάλλον internet» (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

β) Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς την χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παράγρ. 1 του Π.Κ. π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM ή σε ηλεκτρονικό υπολογιστή.

γ) Σε «γνήσια εγκλήματα κυβερνοχώρου» (Cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο. Μια τέτοια αξιόποινη συμπεριφορά μπορεί να θεωρηθεί η

[170] Βλ., όπ. υπ. 37

παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία. Δηλαδή τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικά σε περιβάλλον διαδικτύου. Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

6. Εξέλιξη ποινικού δικαίου της Κοινωνίας της Πληροφορίας

Η εξέλιξη του ποινικού δικαίου του κυβερνοχώρου χαρακτηρίζεται από τέσσερα στάδια:

α) Στη δεκαετία του 70 και του 80 το πρώτο κύμα νομοθεσίας αφορούσε την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων.

β) Στη δεκαετία του '80 ένα δεύτερο κύμα τροποποιήσεων των νόμων αφορούσε την καταστολή του οικονομικού ηλεκτρονικού εγκλήματος

γ) Η τρίτη σειρά στη διάρκεια της δεκαετίας του '80 αφορούσε την προστασία της πνευματικής ιδιοκτησίας

δ) Μετά τα μέσα του'90 σημειώνεται ένα τέταρτο κύμα νομοθετικών τροποποιήσεων που αφορά το παράνομο και αθέμιτο περιεχόμενο.

7. Προστασία της ιδιωτικότητας

Οι νόμοι για την προστασία προσωπικών δεδομένων περιέχουν ποινικές διατάξεις που αφορούσαν κατά πρώτο λόγο τα ηλεκτρονικά αρχεία αλλά που βαθμιαία επεκτάθηκαν και στα χειρόγραφα αρχεία. Υπάρχουν ωστόσο διαφοροποιήσεις ως προς τις συμπεριφορές που ποινικοποιούνται. Στη νομοθεσία των ΗΠΑ, Καναδά και Ιαπωνίας συναντάται περιορισμένος αριθμός τέτοιων εγκλημάτων. Αντίθετα στις ευρωπαϊκές χώρες ο σχετικός κατάλογος είναι σαφώς μακρύτερος και αφορά :

α) προσβολή ουσιαστικών δικαιωμάτων (παράνομη διάδοση, διαβίβαση προσωπικών δεδομένων, παράνομη καταχώριση, τροποποίηση, παραποίηση αλλά και χρήση προσωπικών δεδομένων,

β) παραβάσεις υποχρεώσεων εκ του νόμου π.χ. ο ιταλικός νόμος για την προστασία δεδομένων προβλέπει ως ποινικό αδίκημα τη μη συμμόρφωση σε αποφάσεις της αρχής ελέγχου ή την άρνηση επίδειξης εγγράφων ή παροχής πληροφοριών.

γ) προσβολή δικαιωμάτων πρόσβασης του υποκειμένου στα δεδομένα που το αφορούν. (π.χ. νόμοι Λουξεμβούργου, Δανίας, Σουηδίας)

δ) μη τήρηση των υποχρεώσεων ασφαλείας (data security measures) που επιβάλλει ο νόμος (π.χ. νόμοι Δανίας, Ιταλίας)

8. Χαρακτηριστικά γνωρίσματα του εγκλήματος στον κυβερνοχώρο

Το έγκλημα στον κυβερνοχώρο είναι γρήγορο (quick), διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

Είναι εύκολο (easy) στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα).

Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις, αυτή τη στιγμή είναι πιο προηγμένο «ανεβασμένο» και από το έγκλημα του «λευκού περιλαιμίου».

Μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.

Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σε όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδια ομάδες συζητήσεως (News groups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC- Internet Relay Chat).

Οι «εγκληματίες του κυβερνοχώρου» πολλές φορές δεν εμφανίζονται με την πραγματική των ταυτότητα π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές (e-mail) ανωνύμως ή και με ψευδή στοιχεία.

Είναι έγκλημα «χωρίς πατρίδα», παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους.

Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεως του. Ακόμα όμως και αν προσδιοριστεί αυτός, είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης.

Η εξωτερίκευσή του μπορεί να εντοπίζεται στην Α χώρα πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται στο άλλο άκρο της γης ή και να βρίσκονται ταυτόχρονα σε πολλούς τόπους.

Για την διερεύνησή του απαιτείται κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (δηλ. του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος, και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Περιπτώσεις που το έγκλημα στον κυβερνοχώρο (cyber-crime) περιορίζεται στα όρια ενός μόνον κράτους είναι (θεωρητικώς τουλάχιστον) ελάχιστες και σπάνιες.

Οι παραδοσιακές (κοινές) Συμβάσεις για αμοιβαία Δικαστική Συνδρομή δεν επαρκούν, λόγω της φύσεως του αποδεικτικού ολικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί

και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενεργείας των διωκτικών Αρχών.

Δεν υπάρχουν επαρκή στατιστικά στοιχεία, όχι μόνο στον Ελληνικό, αλλά και στον διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια ο «σκοτεινός αριθμός» της εγκληματικότητας στον χώρο του διαδικτύου είναι «ακόμα πιο σκοτεινός», από ότι στον κοινό εγκληματικό χώρο.

Η Αστυνομική διερεύνησή γενικότερα, αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

Εξειδικευμένες γνώσεις επίσης απαιτούνται και για όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (Εισαγγελείς, Δικαστές, Δικηγόρους).

9. Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή

Το έγκλημα στον κυβερνοχώρο (Cyber Crime) είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος (Computer Crime), το οποίο με τη σειρά του είναι μία ειδικότερη μορφή του «κοινού» εγκλήματος, όπως αυτό προσδιορίζεται στο άρθρο 14 Π.Κ.

Ως ηλεκτρονικό έγκλημα μπορεί να οριστεί αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών

Ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων .

Σημειώνεται ότι, ο ορισμός αυτός διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΑΣΑ, που συνεστήθη ειδικώς για να εξετάσει το θέμα της ηλεκτρονικής εγκληματικότητας. Ο ορισμός αυτός βέβαια είναι πολύ ευρύς και είναι ευνόητο ότι, μόνον ως «οδηγός» μπορεί να χρησιμοποιηθεί. Η οριστικοποίησή του επαφίεται στον Εθνικό Νομοθέτη και στη νομολογία των Δικαστηρίων.

10. Σκιαγράφηση (προφίλ) εγκληματία του Κυβερνοχώρου

Ο «εγκληματίας του κυβερνοχώρου» διαφέρει ουσιωδώς από τον «κοινό εγκληματία». Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. Ο δράστης πρέπει να διαθέτει ειδικές γνώσεις, τεχνική επιδεξιότητα, τεχνικά μέσα. Χαρακτηριστικώς αναφέρεται ότι, στο έγκλημα στον κυβερνοχώρο (cyber-crime) δεν υπάρχει «Γιάννης - Αγιάννης». Υπάρχουν μόνο «άθλιοι». Τι σημαίνει αυτό; Ο εγκληματίας του κυβερνοχώρου, (cyber-crook), δεν μπορεί να υποστηρίξει ότι ενήργησε «από ανάγκη» δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Τους «εγκληματίες του κυβερνοχώρου» μπορούμε να τους διακρίνουμε σε δύο κατηγορίες :

α) Σε αυτούς που «επιτίθενται» (εισβάλουν) στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη «εισβάλουν» σε υπολογιστή δια της χρήσεως του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία,

β) Σε αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη ανήκουν αυτοί που δεν «εισβάλουν» απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμό τους.

Σε ειδική έρευνα που έγινε στη Βρετανία, από την «*Επιτροπή Πρόβλεψης και Πρόληψης Εγκλήματος*» (Foresight Crime Prevention Panel), για το «ποιόν» (who is who) του μελλοντικού εγκληματία διαπιστώθηκε ότι: Το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμα δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον «ξεγελούν» με την ανάλογη κατασκευή φακών επαφής.

11. Σχέση «εγκληματία του κυβερνοχώρου» (cyber - criminal) και του «εγκληματία του λευκού περιλαιμίου» (white - collar criminal)

Μπορεί να υποστηριχθεί ότι το έγκλημα στον κυβερνοχώρο (cyber-crime) είναι μια ειδικότερη μορφή του εγκλήματος του «λευκού περιλαιμίου». Και αυτό γιατί ο εγκληματίας του κυβερνοχώρου πρέπει να διαθέτει:

α) *Εξειδικευμένη επιδεξιότητα*: Ο εγκληματίας του κυβερνοχώρου πρέπει να είναι επιδέξιος, να έχει γνώσεις του όλου συστήματος πληροφορικής, να είναι κοινωνικός και να μπορεί να αντιληφθεί που θα «πετύχει» το θύμα του.

β) *Γνώση*: Ο εγκληματίας του κυβερνοχώρου δεν έχει απλώς γνώση του όλου συστήματος πληροφορικής και του διαδικτύου (internet). Γνωρίζει πολύ καλά το επιμέρους «περιβάλλον», καθώς και τα μυστικά του χώρου που θα παραβιάσει. Όπως ακριβώς ο «κοινός εγκληματίας» συλλέγει πληροφορίες, κατοπτεύει το χώρο κλπ. που πρόκειται να κλέψει ή να ληστέψει, κατ' ανάλογο τρόπο και ο εγκληματίας του κυβερνοχώρου (cyber-criminal)

κατοπτεύει και παρακολουθεί το ηλεκτρονικό περιβάλλον (site), στο οποίο πρόκειται να ενεργήσει την παράνομη πράξη του.

γ) *Απαραίτητα τεχνικά και οικονομικά μέσα*: Ο εγκληματίας του κυβερνοχώρου πρέπει, εκτός από τη γνώση, να κατέχει και τα κατάλληλα τεχνικά μέσα. Χωρίς την οικονομική δυνατότητα για αγορά του εξοπλισμού (computer - software κλπ.) και χωρίς την κατοχή των τεχνικών μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Συμπερασματικά λοιπόν μπορεί να λεχθεί ότι, το έγκλημα του κυβερνοχώρου, είναι πιο προηγμένα «ανεβασμένο» και από το έγκλημα του «λευκού περιλαιμίου».

Β' Μέρος - ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΠΟΙΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

1. Γενικές παρατηρήσεις

Το ερώτημα που προκύπτει από την σχέση διαδικτύου και ποινικής νομοθεσίας είναι, αν η συμπεριφορά των χρηστών του διαδικτύου μπορεί να ρυθμιστεί με ποινικούς κανόνες δικαίου και εάν στην συνέχεια οι ποινικοί αυτοί κανόνες μπορούν να εφαρμοστούν στην πράξη. Το πρώτο αποτελεί ερώτημα του ουσιαστικού ποινικού δικαίου και το δεύτερο ερώτημα του ποινικού δικονομικού δικαίου.

Η απάντηση είναι: Πάρα πολύ δύσκολα και σε πολύ περιορισμένο τομέα. Και αυτό γιατί, η τεχνολογία εξελίσσεται τόσο γρήγορα, που η νομοθεσία όσο και αν προσπαθεί «ασθμαίνουσα», αδυνατεί να την προφτάσει. Επιπλέον για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο απαιτούνται εξειδικευμένες γνώσεις, τόσο σε τεχνικό, όσο και σε νομικό επίπεδο. Η απόκτηση των γνώσεων αυτών από νομικούς, που έχουν σχέση με την έρευνα, δίωξη και εκδίκαση των σχετικών υποθέσεων, αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε πολιτείας.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικώς τις καταστάσεις, πιεζόμενες από τα πράγματα. Κλασσικό παράδειγμα στον τομέα της τεχνολογίας αποτελεί η εμφάνιση των εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes). Πριν από δυο δεκαετίες περίπου η «συμβατική νομοθεσία» δεν επαρκούσε για την αντιμετώπισή τους. Σήμερα όλες οι προηγμένες (τουλάχιστον) χώρες έχουν καταρτίσει σχετική νομοθεσία, που προσπαθούν να αντιμετωπίσουν τα εγκλήματα που διαπράττονται με τη χρήση υπολογιστών. Στην Ελληνική έννομη τάξη ισχύει ο Ν. 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes).

Στο ίδιο σημείο με αυτό της προ δεκαπενταετίας, νομοθετικής ελλείψεως βρίσκονται σήμερα οι έννομες τάξεις, όσον αφορά το θέμα του εγκλήματος στον κυβερνοχώρο (cyber crime). Πολλά από τα εγκλήματα που έχουν παρουσιαστεί στο διαδίκτυο, δεν μπορούν να αντιμετωπιστούν με την συμβατική νομοθεσία, στο χώρο τουλάχιστο του ποινικού δικαίου. Σημειώνεται ότι ελάχιστα κράτη έχουν θεσπίσει μέχρι σήμερα ειδική νομοθεσία, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Στο σημείο αυτό πρέπει να τονιστεί ότι, η κατάρτιση νομοθεσίας για την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο δεν αποτελεί «εσωτερική υπόθεση» κάθε κράτους χωριστά. Λόγω των ιδιαιτέρων χαρακτηριστικών των εγκλημάτων του κυβερνοχώρου απαιτείται κατάρτιση συμβάσεων στα πλαίσια διεθνών οργανισμών, με ιδιαίτερη έμφαση στη δικαστική και αστυνομική συνεργασία.

Από μη νομικούς έχει υποστηριχθεί η άποψη ότι, δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομικό κενό στο διαδίκτυο, διότι αναλογικά το «κοινό δίκαιο» μπορεί να εφαρμοστεί και στον χώρο του

διαδικτύου. Η άποψη βέβαια αυτή είναι εμφανώς εσφαλμένη, καθότι στον ποινικό τουλάχιστο χώρο, δεν ισχύει η αρχή της αναλογίας.

2. Διαδίκτυο και Γενικό Ποινικό Δίκαιο

Στην Ελληνική έννομη τάξη δεν υπάρχει γενικός νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου.

Ο Ν. 1805/88, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα. Όταν καταρτιζόταν ο νόμος αυτός το διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη καταρτίσεως ειδικότερης νομοθεσίας. Η διατύπωση όμως του νόμου αυτού έχει γίνει με τέτοιο τρόπο (συνδυασμός τεχνικών και νομικών εννοιών), που είναι εμφανής η επιθυμία του συντάκτη, να περιλάβει στο μέλλον και κάθε μορφή συμπεριφοράς, που θα δημιουργήσει η εξέλιξη της τεχνολογίας.

Ανεξάρτητα όμως από το εάν ο παραπάνω Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής , το βέβαιο είναι ότι, δεν επαρκεί να "καλύψει" τα εγκλήματα που έχουν παρουσιαστεί από την χρήση του διαδικτύου.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

3. Προσπάθεια νομικής αντιμετώπισης του θέματος στον Ευρωπαϊκό νομικό χώρο.

Η πρωτοπορία και στη νομική αντιμετώπιση το εγκλήματος στον κυβερνοχώρο ανήκει, όπως και η τεχνική, στις Η.Π.Α. Η Ελλάδα

συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων Διεθνών Οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Στον Ευρωπαϊκό χώρο γίνεται προσπάθεια να ρυθμιστεί το θέμα, η δε προσπάθεια αυτή βρίσκεται σε ακόμα σε εξέλιξη. Σχετικές προσπάθειες πάντως έχουν γίνει τόσο στα πλαίσια του Συμβουλίου της Ευρώπης, όσο και στα πλαίσια της Ευρωπαϊκής Ένωσης.

3.1. Συμβούλιο Ευρώπης και έγκλημα στον κυβερνοχώρο.

Το Συμβούλιο της Ευρώπης έχει ασχοληθεί τόσο με το ηλεκτρονικό έγκλημα, όσο και με το έγκλημα στον κυβερνοχώρο. Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα :

α) Η Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer - related crime).

β) Η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology).

Στο Συμβούλιο της Ευρώπης καταρτίζεται από το έτος 1997, η Διεθνής Σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στο Κυβερνοχώρο. Στην κατάρτιση της Σύμβαση αυτής συμμετέχει και η Ελλάδα. Σκοπός της Συμβάσεως είναι η προστασία της Κοινωνίας από το έγκλημα στον κυβερνοχώρο, με την θέσπιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα Δικαστικής Συνεργασίας μεταξύ των κρατών, που θα υπογράψουν την Σύμβαση. Αρχικά ως χρονοδιάγραμμα για την περαίωση των εργασιών, είχε τεθεί το τέλος του έτους 1999. Επειδή όμως τα προβλήματα (νομικά και τεχνικά) που προέκυψαν κατά την συζήτηση ήταν τόσα πολλά και τόσο περίπλοκα, ζητήθηκε (και χορηγήθηκε) παράταση

της προθεσμίας περαιώσεως μέχρι το τέλος του 2000. Ήδη η Σύμβαση έχει περαιωθεί και υπεγράφει σε ειδική τελετή που έγινε στις 22 και 23 Νοεμβρίου 2001 στην Βουδαπέστη.

Η συγκεκριμένη σύμβαση καθιερώνει την υποχρέωση εναρμονίσεως των Εθνικών νομοθεσιών σε θέματα εγκλημάτων στον κυβερνοχώρο (internet crimes) τόσο σε θέματα ποινικού, όσο και Αστικού Δικαίου.

Κύριο χαρακτηριστικό της Διεθνούς αυτής Συμβάσεως είναι η υποχρέωση που αναλαμβάνουν τα κράτη-μέλη, να ποινικοποιήσουν ορισμένη συμπεριφορά στο διαδίκτυο.

3.1.1. Η Παράνομη πρόσβαση (illegal Access).

Σύμφωνα με το άρθρο 2 της Συμβάσεως κάθε μέλος θα θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα. Το μέρος μπορεί να απαιτεί ότι, το αδίκημα θα διαπράττεται ή με παραβίαση των μέτρων ασφαλείας ή με το σκοπό αποκτήσεως ηλεκτρονικών δεδομένων ή για άλλο παράνομο σκοπό ή σε σχέση με ένα σύστημα ηλεκτρονικών υπολογιστών, που συνδέεται με άλλο σύστημα ηλεκτρονικών υπολογιστών.

Το άρθρο αυτό έχει ως σκοπό να ποινικοποιήσει αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «hacking». Ο όρος στα Ελληνικά μπορεί να αποδοθεί ως «εισβολή». Ως εισβολή μπορεί να οριστεί η ενέργεια το εισβολέα hacker να εισέλθει (διεισδύσει - αποκτήσει πρόσβαση), με διάφορους τεχνικούς τρόπους, σε ξένα συστήματα υπολογιστών. Προστατευόμενο έννομο αγαθό είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα στο σύστημα. Αποτελεί δηλαδή το άρθρο αυτό, το ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο της διατάραξης οικιακής ειρήνης

(άρθρο 334 Π.Κ.). Όπως δηλαδή ο δικαιούχος της κατοικίας έχει το δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται και να παραμένει σε αυτήν, έτσι και ο «δικαιούχος» του ηλεκτρονικού υπολογιστή δικαιούται να ορίζει ποιος θα τον χρησιμοποιεί και ποιος θα «εισέρχεται» σε αυτόν.

Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι, ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος, τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή ή του συστήματος υπολογιστή.

Ο όρος «πρόσβαση» περιλαμβάνει την «χωρίς εξουσιοδότηση είσοδο» σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή μέρος αυτού (π.χ. σε επιμέρους φακέλους). Δεν περιλαμβάνει όμως την χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων.

Για την θεμελίωση της υποκειμενικής υποστάσεως απαιτείται πρόθεση , όπως αυτός προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε μέλους κράτους. Οι περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή.

3.1.2. Η αθέμιτη παγίδευση - υποκλοπή (illegal interception)

Σύμφωνα με το άρθρο 3 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η παγίδευση - υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία. Ένα μέλος μπορεί να απαιτήσει ότι το αδίκημα

διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών, το οποίο συνδέεται με άλλο σύστημα.

Η διάταξη αυτή μπορεί να εφαρμοστεί σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων, είτε αυτά διακινούνται δια του κυβερνοχώρου με μεταφορά φακέλων (file transfer), είτε με e-mail, είτε με FAX.

Προστατευόμενο έννομο αγαθό είναι «το δικαίωμα στην ιδιωτική ζωή και της ασφάλειας των τηλεπικοινωνιών στον κυβερνοχώρο» Αποτελεί δηλαδή το άρθρο αυτό, το «ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο» της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας (υποκλοπή).

Στην Ελληνική έννομη τάξη η συμπεριφορά αυτή προβλέπεται στην στο άρθρο 370 Α §§1 και 2 Π.Κ. Σύμφωνα με αυτό όποιος αθέμιτα παγιδεύει ή με οποιαδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση. Επίσης, όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων, που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων τιμωρείται με φυλάκιση.

3.1.3. Επέμβαση σε δεδομένα (Data interference)

Σύμφωνα με το άρθρο 4 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττονται εκ προθέσεως η καταστροφή (damaging), η διαγραφή (deletion), η χειροτέρευση (deterioration), η μεταβολή (alteration), ή η απόκρυψη (suppression) δεδομένων χωρίς δικαίωμα. Σκοπός του άρθρου

αυτού είναι να προστατεύσει τα δεδομένα (data) και τα προγράμματα των ηλεκτρονικών υπολογιστών ως «υλικές υποστάσεις» από οποιαδήποτε επέμβαση (παρεμβολή), που γίνεται με πρόθεση πρόκλησης ζημιάς σ' αυτά. Προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

Ως εγγύτερο άρθρο στην Ελληνική έννομη τάξη μπορεί να θεωρηθεί αυτό της φοράς ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.).

3.1.4. Επέμβαση σε σύστημα (System Interference)

Σύστημα ηλεκτρονικού υπολογιστή (Computer system) σημαίνει κάθε συσκευή ή ομάδα συσκευών που είναι εσωτερικώς συνδεδεμένες μεταξύ των ή με άλλες σχετικές συσκευές, μια ή περισσότερες από τις οποίες επεξεργάζονται αυτομάτως δεδομένα (data), σύμφωνα με κάποιο πρόγραμμα.

Δεδομένα υπολογιστή (computer data) είναι κάθε αναπαράσταση (representation) γεγονότων (facts), πληροφοριών ή εννοιών (concepts) σε μορφή κατάλληλη για επεξεργασία σε σύστημα υπολογιστή, συμπεριλαμβανομένου προγράμματος κατάλληλο να προκαλέσει σε ένα σύστημα υπολογιστή την εκτέλεση μιας λειτουργίας.

Σύμφωνα με το άρθρο 5 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττεται εκ προθέσεως η σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση (Inputting), μεταφορά (transmitting), καταστροφή (damaging), διαγραφή (deleting), χειροτέρευση (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression) δεδομένων υπολογιστών.

Το προστατευόμενο έννομο αγαθό στο άρθρο αυτό είναι το δικαίωμα του χρήστη να έχει μια «κανονική» λειτουργία του υπολογιστή του. Η διάταξη αυτή ποινικοποιεί, αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «computer sabotage» (δολιοφθορά ηλεκτρονικού υπολογιστή).

3.1.5. Κακή χρήση συσκευών (misuse of devices)

Σύμφωνα με το άρθρο 6 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα προκειμένου να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα η παραγωγή, πώληση, η προετοιμασία για χρήση εισαγωγή, διανομή ή με οποιοδήποτε άλλο τρόπο διάθεση μιας συσκευής συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα αδικήματα που θεμελιώνονται στα άρθρα 2-5 της Συμβάσεως.

Στην Ελληνική έννομη τάξη το άρθρο αυτό αντιστοιχεί με το 370 Α §7 Π.Κ. Σύμφωνα με αυτό, όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση τεχνικά μέσα ειδικά μόνο για την τέλεση των πράξεων των §§ 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση και με χρηματική ποινή.

3.2. Η θέση της Ευρωπαϊκής Ένωσης απέναντι στο διαδίκτυο

Η Ευρωπαϊκή Ένωση δεν έμεινε αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα γενικότερα και στον κυβερνοχώρο (Internet) ειδικότερα. Έτσι στις 17.2.1997 εκδίδεται το Νο 97/C 70/01 ψήφισμα του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών, που συνήλθαν στα πλαίσια του Συμβουλίου της Ευρωπαϊκής Ένωσης.

Κύριο χαρακτηριστικό του ψηφίσματος αυτού είναι ότι η Ευρωπαϊκή Ένωση αναγνωρίζει τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητες στους πολίτες, μειώνοντας τα εμπόδια ως προς τη δημιουργία και τη διανομή περιεχομένου και προσφέροντας ευρεία πρόσβαση σε όλο και πλουσιότερες πηγές ψηφιακών πληροφοριών. Αναγνωρίζει επίσης το παραπάνω ψήφισμα την ανάγκη καταπολέμησης της παράνομης χρήσης των τεχνικών δυνατοτήτων του κυβερνοχώρου, ιδιαίτερα για αξιόποινες πράξεις κατά των παιδιών. Πριν από την έκδοση του ψηφίσματος αυτού είχαν γίνει για το θέμα διάφορες επίσημες ή ανεπίσημες για το θέμα συναντήσεις .

Χαρακτηριστικό επίσης του ψηφίσματος αυτού είναι ότι, η Ευρωπαϊκή Ένωση διαχωρίζει το περιεχόμενο (content) του διαδικτύου, δηλαδή τα δεδομένα - στοιχεία (data), που διακινούνται, σε παράνομο και επιβλαβές.

3.2.1. Παράνομο περιεχόμενο του Internet

Το σχετικό ψήφισμα (97/C 70/01/17-2-1997) του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών της Ευρωπαϊκής Ένωσης για το παράνομο και επιβλαβές περιεχόμενο του διαδικτύου (Internet), δεν καθορίζει τι είναι παράνομο και τι είναι επιβλαβές περιεχόμενο.

Κατά συνέπεια λοιπόν οι έννοιες αυτές θα προσδιοριστούν από το νομοθέτη σε περίπτωση που ψηφιστεί σχετικός νόμος που θα ρυθμίζει την συμπεριφορά, όσων «κινούνται» στον χώρο του διαδικτύου. Και λέγοντας εδώ «νομοθέτη» εννοούμε τον εθνικό νομοθέτη κάθε επιμέρους χώρας.

Στο σημείο όμως αυτό προκύπτει το ερώτημα , εάν οι «εσωτερικές νομοθεσίες» μπορούν αυτοτελώς, να αντιμετωπίσουν αποτελεσματικά τις παρανομίες στο κυβερνοχώρο, λόγω της φύσεως του εγκλήματος και του ιδιαίτερου τρόπου τελέσεώς των. Κατά την άποψή μου, οι εσωτερικές

νομοθεσίες από μόνες τους δεν επαρκούν. Απαιτούνται πολυμερείς Διεθνείς Συμβάσεις.

Προς το παρόν ως παράνομο περιεχόμενο μπορεί να θεωρηθεί καθετί που, είναι μεν παράνομο (και) εκτός δικτύου, μπορεί δε (τεχνικώς) να κινηθεί και εντός κυβερνοχώρου (π.χ. συκοφαντική δυσφήμηση).

3.2.2. Επιβλαβές περιεχόμενο του Internet

Το «επιβλαβές περιεχόμενο» αποτελεί ευρύτερη έννοια από αυτή του «παρανόμου περιεχομένου». Εννοείται ότι, οτιδήποτε είναι επιβλαβές, δεν είναι οπωσδήποτε και παράνομο. Η έννοια του «επιβλαβούς περιεχομένου» ενέχει σε μεγάλο βαθμό και το υποκειμενικό στοιχείο.

Είναι ευνόητο βέβαια ότι, η έννοια του επιβλαβούς περιεχομένου έχει διαφορετική βαρύτητα, όταν πρόκειται για χρήση του διαδικτύου (Internet) από ανηλίκους . Παράδειγμα: Στο Internet υπάρχουν εκατοντάδες θέσεις (sites) που αναφέρονται στο Σατανισμό και στη λατρεία του Σατανά . Για πολλούς το περιεχόμενο των sites αυτών αποτελεί κλασσική μορφή «επιβλαβούς περιεχομένου». Για άλλους όμως αποτελεί μια μορφή ελεύθερης έκφρασης της προσωπικότητας ή ακόμα και μια μορφή ανεξιθρησκίας.

Γενικώς ως επιβλαβές περιεχόμενο μπορεί να θεωρηθεί, ότι αναφέρεται σε ρατσιστικές διακρίσεις ή σε παραπλανητική διαφήμιση. Ως χαρακτηριστικό (κατά την άποψή μου) παράδειγμα επιβλαβούς περιεχομένου υλικό του διαδικτύου, μπορεί να θεωρηθεί και η περίπτωση (κατά τον Οκτώβριο του 1999) πλειοδοσίας κατά την πώληση ωαρίων εμφανίσιμων γυναικών («μανεκέν» σε ειδική τοποθεσία (site)). Ομοίως η περίπτωση της «ερωτικής συνεύρεσης για πρώτη φορά» (τον Αύγουστο 1998) μεταξύ δύο «παρθένων νέων», που όμως τελικά δεν έγινε. Είναι ευνόητο βέβαια ότι, πριν από την ματαίωση της «παράστασης» εκατομμύρια χρήστες από όλον τον κόσμο είχαν «επισκεφθεί» την αντίστοιχη τοποθεσία (site), με τεράστια οικονομικά κέρδη για τους «διοργανωτές». Η περίπτωση αυτή μπορεί να θεωρηθεί και ως

απάτη, που διαπράττεται στο διαδίκτυο. Είναι ευνόητο όμως ότι, ουδείς βλαπτόμενος (ιδιώτης) ενδιαφέρθηκε για την υποβολή εγκλήσεως προς άσκηση ποινικής διώξεως, λαμβάνοντας υπόψη την μικρή οικονομική ζημία που υπέστη ως άτομο ή την «διαπόμπευσή» του για τις «διαδικτυακές του προτιμήσεις», σε σχέση και με τα τεράστια δικαστικά έξοδα που απαιτούνται, για την κίνηση ενός τέτοιου δικαστικού αγώνα.

Σημειωτέων ότι, για την αντιμετώπιση του παρανόμου και επιβλαβούς περιεχομένου του κυβερνοχώρου έχει προταθεί -μεταξύ των άλλων- και η δημιουργία «οργάνου αυτορύθμισης» στο πλαίσιο λειτουργίας των παροχέων υπηρεσιών, καθώς και λειτουργία «θερμής γραμμής», όπου θα μπορούν να γίνονται σχετικές (επώνυμες ή και ανώνυμες) καταγγελίες .

3.2.3. Η νομική αντιμετώπιση του "Χάκερ" κατά το γενικό ποινικό δίκαιο.

Σύμφωνα με το άρθρο 370Γ§2 Π.Κ., όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών , εφ' όσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις του κράτους ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. Η πράξη αυτή διώκεται μόνον ύστερα από έγκληση του παθόντα. Διευκρινίζεται δε ότι, το άρθρο 148 Π.Κ., το οποίο στην §2 αποτελεί κακούργημα, αναφέρεται στην κατασκοπεία, που διαπράττεται από πολίτη, παραπέμπει δε (το άρθρο 148 Π.Κ.) και στο άρθρο 146, το οποίο αναφέρεται στην παραβίαση των μυστικών της πολιτείας, όταν διαπράττεται βέβαια από πολίτη και όχι από στρατιωτικό. Το τελευταίο αυτό σημαίνει ότι, εάν ο χάκερ, ο οποίος εισήλθε παράνομα στα ηλεκτρονικά δεδομένα του Υπουργείου Εθνικής Αμύνης, έλαβε στην κατοχή του ή στη γνώση του αντικείμενα ή ειδήσεις, που τα συμφέροντα της πολιτείας ή των

συμμάχων της επιβάλουν να τηρηθούν απόρρητα απέναντι σε ξένη κυβέρνηση τιμωρείται με φυλάκιση μέχρι ενός έτους. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει τα ανωτέρω αντικείμενα ή ειδήσεις για να τα διαβιβάσει σε άλλον ή να τα ανακοινώσει έτσι ώστε να μπορούν να εκθέσουν σε κίνδυνο το συμφέρον του κράτους και ιδίως την ασφάλειά του ή κάποιου από τους συμμάχους του, τιμωρείται με ποινή κάθειρξης.

Αξιοσημείωτο είναι επίσης ότι, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα.

Διευκρινίζεται ότι, το παραπάνω άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988. Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου. Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του "χάκερ" στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών "χάκερς", όπως είναι οι cracker, whacker κλπ .

Λέγοντας απόρρητο εννοούμε το δικαίωμα του κατόχου των δεδομένων να αποκλείει άλλους από την πρόσβαση σε αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου από ουσιαστική έννοια. Στο άρθρο 370 Β §1 ορίζεται ότι, ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Είναι ευνόητο βέβαια ότι, ή παραπάνω διάταξη του άρθρου 370 Γ §2 Π.Κ. θα εφαρμοστεί κατά την περίπτωση εκείνη που ο δράστης απλώς θα έχει εισέλθει χωρίς δικαίωμα σε σύστημα υπολογιστών, χωρίς να προκαλέσει οποιαδήποτε άλλη βλάβη. Σε περίπτωση δε, που από την χωρίς δικαίωμα

διείσδυσή του έχει επέλθει και παραβίαση άλλων εννόμων αγαθών, η νομική αντιμετώπιση είναι κάθε φορά ανάλογη. Έτσι π.χ. στην πλέον γνωστή υπόθεση «χάκιγκ», που απασχόλησε την Ελληνική νομική πράξη τον Ιούλιο του 2000, εναντίον του Έλληνα «χάκερ» γνωστού ως *cyberia* ασκήθηκε ποινική δίωξη και για παράβαση του άρθρου 386 Α Π.Κ. σε βαθμό κακουργήματος. Το άρθρο αυτό, το οποίο περιλαμβάνεται στα εγκλήματα κατά των περιουσιακών δικαιωμάτων, προστατεύει την περιουσία.

3.2.4. Νομικός ορισμός του χάκερ.

Σύμφωνα λοιπόν με όσα αναφέρθηκαν παραπάνω για το άρθρο 370 Γ Π.Κ., ως Χάκερ, μπορεί να οριστεί το άτομο εκείνο, το οποίο, χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών. Οι χάκερς εμφανίστηκαν για πρώτη φορά κατά την δεκαετία του 1970 στις ΗΠΑ, ως δράστες κατά των τηλεπικοινωνιακών συστημάτων. Σήμερα εμφανίζονται με δύο μορφές: α)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, χωρίς την πρόκληση βλάβης και β)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, με πρόκληση βλάβης. Το είδος της βλάβης που θα προκαλέσει εξαρτάται από τις συγκεκριμένες περιπτώσεις. Στην δεύτερη αυτή περίπτωση έχει επικρατήσει ο όρος «κράκερ», ο οποίος όμως είναι και αυτός όρος τεχνικής φύσεως και όχι νομική έννοια.

Από άποψη νομικής επιστήμης, η εξέταση της προσωπικότητας του χάκερ αποτελεί αντικείμενο της επιστήμης της εγκληματολογίας .

3.2.5. Νομικές προϋποθέσεις για την ύπαρξη χάκιγκ κατά το Ελληνικό Δίκαιο

Για την ουσιαστική εφαρμογή του άρθρου 370 Γ §2 Π.Κ. πρέπει να συντρέχουν οι παρακάτω προϋποθέσεις:

α) πρόσβαση σε στοιχεία. Ως πρόσβαση θεωρείται κάθε διείσδυση του δράστη, που αποβλέπει να λάβει γνώση των στοιχείων. Αντικείμενο της πρόσβασης είναι στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

β) η πρόσβαση αυτή να γίνεται χωρίς δικαίωμα, δηλαδή χωρίς την συγκατάθεση του κατόχου των στοιχείων. Σε περίπτωση που υφίσταται η συγκατάθεση αυτή, είναι ευνόητο ότι, δεν θεμελειούται η αντικειμενική υπόσταση του εγκλήματος του άρθρου 370 Γ §2 Π.Κ. Σε περίπτωση που ο δράστης είναι στην υπηρεσία του νομίμου κατόχου των στοιχείων, τότε τεκμαίρεται ότι, αυτός έχει το δικαίωμα νόμιμης πρόσβασης στα στοιχεία. Αυτό συνάγεται από την §3 του ίδιου άρθρου 370 Γ §2 Π.Κ., σύμφωνα με την οποία η πράξη της §2 τιμωρείται, μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμού ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Η έλλειψη δικαιώματος πρόσβασης τεκμαίρεται ιδίως όταν, γίνεται (η πρόσβαση) με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους. Ως τέτοια μέτρα ασφαλείας θεωρούνται οι κωδικοί λέξεων (passwords) οι κωδικοί αριθμοί χρηστών, μαγνητικές κάρτες κλπ. Η διατύπωση του άρθρου 370 Γ§2 Π.Κ. είναι «αρκούντως ευρεία», ώστε να περιλαμβάνει κάθε πρόσβαση σε δεδομένα και αρχεία. Στην ευρεία αυτή διατύπωση του, οφείλεται και το γεγονός ότι, μπορεί να υπαχθεί στο άρθρο αυτό η ενέργεια του *χάκερ*, δηλαδή το *χάκιγκ*. Άλλωστε, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα. Το έγκλημα του άρθρου 370 Γ§2 Π.Κ. είναι έγκλημα διακινδύνευσης και όχι έγκλημα βλάβης.

3.2.6. Ο δεκάλογος των δικαιωμάτων του χρήστη του διαδικτύου

Ο κ. Γιώργος Επιτήδειος, Πρόεδρος της ΕΕΤΤ[171], μας αναφέρει ποιος πρέπει να είναι ο τρόπος χρήσης του διαδικτύου από τον πολίτη για να αισθάνεται και να είναι ασφαλείς κατά την πλοήγησή του σε αυτό :

1. **Προσωπικό απόρρητο**: Κάθε χρήστης έχει δικαίωμα να γνωρίζει ποια από τα προσωπικά του στοιχεία καταγράφονται και για ποιο σκοπό, ενώ έχει δικαίωμα να αποφασίζει για την διαγραφή όσων από αυτά δεν είναι υποχρεωτικά από το νόμο.

2. **Εμπιστοσύνη του νομοθέτη**: Κάθε χρήστης πρέπει να θεωρείται ένοχος μόνο όταν διαπράξει μια αξιόποινη πράξη και όχι όταν διαθέτει απλώς την τεχνική δυνατότητα για μια τέτοια ενέργεια.

3. **Ισοτιμία των πράξεων εντός και εκτός δικτύου**: Οτιδήποτε επιτρέπεται στον «φυσικό» κόσμο δεν μπορεί να απαγορεύεται στον δικτυακό.

4. **Ισορροπημένη προάσπιση δικαιωμάτων**: Η κρατική προστασία των ιδιωτικών επιχειρηματικών συμφερόντων δεν μπορεί να είναι ισχυρότερη από την προστασία των ατομικών δικαιωμάτων του χρήστη όταν απειλούνται από αυτά ιδιωτικά συμφέροντα.

5. **Ασφάλεια και αξιοπιστία προϊόντων και υπηρεσιών**: Η σε βάθος χρόνου συντήρηση και επισκευή όσων εργαλείων χρησιμοποιεί ο χρήστης αποτελεί θεμελιώδες δικαίωμά του. Ειδικά για τα προϊόντα λογισμικού οποιαδήποτε εγκατάλειψη υποστήριξης θα πρέπει να συνοδεύεται από δημοσίευση του πηγαίου κώδικα ώστε να καθίσταται δυνατή η ανάληψη της εργασίας αυτής από τους ίδιους του χρήστες εάν το επιθυμούν.

---

[171] Βλ., στο dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html "ΚΕΝΤΡΟ ΠΛΗ. ΝΕ. Τ. Ν. ΦΛΩΡΙΝΑΣ – Δίκαιο και Internet"

6. **Ελεύθερη χρήση ιδεών:** Κάθε χρήστης έχει το δικαίωμα να χρησιμοποιεί (ή ακόμα και να δημιουργεί) προϊόντα λογισμικού ή υπηρεσίες χωρίς να δεσμεύεται από γενικής διατύπωσης άδειες πνευματικών δικαιωμάτων που εμποδίζουν αντί να προάγουν την τεχνολογική ανάπτυξη.

7. **Ελεύθερη πρόσβαση**: Το περιεχόμενο του Διαδικτύου δεν μπορεί να αποτελεί αντικείμενο λογοκρισίας. Οποιοσδήποτε νομικός περιορισμός πρόσβασης πρέπει να είναι σαφώς καθορισμένος και να υπάρχει η δυνατότητα ελέγχου για αποτροπή της καταχρηστικής εφαρμογής του.

8. **Ανωνυμία**: Κάθε χρήστης πρέπει να έχει το δικαίωμα πλήρους ανώνυμης επικοινωνίας μέσω Διαδικτύου αν το επιθυμεί. Οι προμηθευτές υπηρεσιών ανώνυμης πρόσβασης πρέπει να «δηλώνουν» τον ανώνυμο χαρακτήρα αυτής της επικοινωνίας (π.χ. των μηνυμάτων) ώστε οι άλλοι χρήστες του δικτύου αλλά και οι αρμόδιες υπηρεσίες (π.χ. διωκτικές αρχές) να γνωρίζουν το γεγονός και να κρίνουν ανάλογα για την αξία του σχετικού περιεχομένου.

9. **Δυνατότητα δειγματοληψίας** (fair use): Κάθε χρήστης μπορεί να χρησιμοποιεί κατά την επικοινωνία του με άλλους χρήστες ή τις δημοσιεύσεις του μικρά αποσπάσματα έργων προστατευμένων με συγγραφικά δικαιώματα κατά τρόπο όχι διαφορετικό από την επικρατούσα πρακτική στον Τύπο («φυσικό» και διαδικτυακό).

10. **Νομική προστασία από απαράδεκτη πρόσβαση και χρήση πόρων**: Ο χρήστης έχει δικαίωμα να ζητήσει μέσω της νομίμου οδού αποζημίωση για κάθε αδικαιολόγητη απασχόληση του εξοπλισμού και του χρόνου του (πρόσβαση χωρίς εξουσιοδότηση στο μηχάνημά του, spamming στο mailbox του κ.λ.π.).

Κεφάλαιο 8ο: Α΄ Μέρος - Η ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1. Γενικές παρατηρήσεις

Στην καθομιλουμένη γλώσσα ασφάλεια είναι η κατάσταση εκείνη, στην οποία δεν υπάρχει κίνδυνος, όπου αισθάνεται κάποιος ότι, δεν απειλείται. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας. Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του. Ετσι π.χ. για τον στρατιωτικό η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο απ΄ ότι για τον αστυνομικό, ο οποίος επίσης αντιλαμβάνεται την ίδια έννοια εντελώς διαφορετικά απ΄ ότι ο εργαζόμενος σε οικοδομικές εργασίες κλπ. Αλλά και στον ίδιο ευρύτερο επαγγελματικό κλάδο η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο, ανάλογα με την επιμέρους ενασχόληση του κάθε προσώπου. Ετσι π.χ. για τον στρατιωτικό που ασχολείται με τα όπλα η έννοια της ασφάλειας, δεν ταυτίζεται με αυτή που αντιλαμβάνεται ο ασχολούμενος με τους ηλεκτρονικούς υπολογιστές του ίδιου κλάδου. Ακόμα όμως και στον ίδιο στενότερο - επιμέρους κλάδο, η οπτική γωνία θεωρήσεως του όρου ασφάλεια είναι εντελώς διαφορετική. Ετσι, π.χ. διαφορετικά αντιλαμβάνεται τον όρο "ασφάλεια" ο τεχνικός ασφαλείας δικτύων υπολογιστικών συστημάτων και διαφορετικά ο τεχνικός ασφάλειας τραπεζικών πληροφοριακών συστημάτων.

Σε κάθε περίπτωση όμως όλοι, όσοι ασχολούνται με θέματα ασφαλείας «συναντώνται» στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου αισθάνονται ασφαλείς, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν την σιγουριά και την βεβαιότητα κατά την ενάσκηση του έργου των. Είναι ευνόητο βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες.

2. Η νομική έννοια της ασφάλειας στον κυβερνοχώρο

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρονται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο «τον κίνδυνο να επέλθει κάποια βλάβη», θα πρέπει να ορίσει ταυτόχρονα και τους όρους «κίνδυνο» και «βλάβη».

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα έλεγα, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό.

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

Συμπερασματικά μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

3. Βασικές αρχές του όρου «ασφάλεια» στο Διαδίκτυο

Στο διαδίκτυο *διακινούνται* πληροφορίες - δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα «αδιάκριτα βλέμματα». Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. Η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από τις βασικότερες Αρχές του δικαίου. Είναι ευνόητο ότι, οι θεμελιώδεις αυτές Αρχές πρέπει να εφαρμόζονται και στον κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω Αρχές. Δεν μπορούμε να ομιλούμε για κρατικό έλεγχο, καθότι η έννοια του κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο διαδίκτυο.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται) από ένα άλλο τρόπο «αντι-ασφάλειας» Από νομική άποψη διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογικές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειες των, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν «σταθεροποιηθεί» κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο, σε ουσιαστικό ή δικονομικό επίπεδο.

4. Η τεχνική διάσταση του όρου ασφάλεια στο διαδίκτυο

Από τεχνική άποψη, ασφάλεια (security) είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα . Κλασσικό παράδειγμα ασφαλείας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με την χρήση πιστωτικής κάρτας. Σ' αυτήν την περίπτωση πρέπει να εξασφαλιστεί ότι, δεν είναι δυνατόν να «συλλάβει» (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αντιγράψει από τον διακομιστή, που είναι αποθηκευμένος. Επίσης πρέπει να επαληθευτεί ότι, ο αριθμός της πιστωτικής κάρτας αποστέλλεται πράγματι, από το πρόσωπο, που ισχυρίζεται ότι τον στέλνει.

Η ασφάλεια δηλαδή των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιεί την *εμπιστευτικότητα*,[172] την *ακεραιότητα*[173] και την *διαθεσιμότητα*[174] των δεδομένων.

5. Σχέση ασφάλειας και μυστικότητας στο διαδίκτυο

Μυστικότητα είναι το δικαίωμα που έχει κάποιος να μην μοιράζεται τις πληροφορίες (π.χ. ηλικία, θρήσκευμα, αριθμούς πιστωτικής κάρτας κλπ) που αφορούν το άτομό του με άλλους. Οι πληροφορίες αυτές είναι καταγεγραμμένες στο διαδίκτυο. Η ασφάλεια και η μυστικότητα στο χώρο του διαδικτύου είναι (ουσιαστικά) θεωρητικές έννοιες. Στην πράξη, ότι κινείται στον χώρο του διαδικτύου μπορεί να γίνει γνωστό, ουσιαστικά δηλαδή να υποκλαπεί. Έχει χαρακτηριστικά λεχθεί ότι, «κανένα κινούμενο ηλεκτρόνιο του πλανήτη δεν μπορεί να τρέφει σοβαρές ελπίδες ότι θα ξεφύγει από τον ιστό της παρακολούθησης». Κατά συνέπεια η ασφάλεια και η μυστικότητα του διαδικτύου δεν είναι μόνο νομικές, αλλά και τεχνικές έννοιες . Μπορεί όμως να λεχθεί ότι, η ασφάλεια είναι πρωτίστως τεχνική και

---

[172] Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος

[173] Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητά των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή των να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας

[174] Διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος

δευτερευόντως νομική έννοια, ενώ αντίθετα η μυστικότητα είναι πρωτίστως νομική και δευτερευόντως τεχνική έννοια. Σε κάθε περίπτωση όμως, με την χρήση της τεχνολογίας και ιδιαίτερα του διαδικτύου, η προσωπική ζωή του ατόμου έχει γίνει «διαφανής».

Συμπερασματικά, μυστικότητα και η ασφάλεια είναι εντελώς διαφορετικά πράγματα, δεν είναι όμως υπερβολικό να λεχθεί ότι, ασφάλεια και μυστικότητα στο διαδίκτυο αποτελούν τις δυο διαφορετικές όψεις, ενός και του ίδιου νομίσματος.

6. Σχέση ασφάλειας και κρυπτογραφίας στο διαδίκτυο

Κρυπτογραφία (cryptography) είναι η χρήση κωδίκων για την μετατροπή δεδομένων, κατά τέτοιο τρόπο, ώστε να μπορούν να διαβαστούν μόνο από συγκεκριμένο παραλήπτη με τη χρήση ενός κλειδιού . Σκοπός της κρυπτογραφίας είναι να αποτραπεί η πρόσβαση στα δεδομένα, σε μη εξουσιοδοτημένα άτομα ιδιαίτερα κατά την διάρκεια μετάδοσής των. Σχετικοί είναι οι όροι «διαχείριση κινδύνων» (risk management) και ανάλυση κινδύνων (risk analysis). Είναι χαρακτηριστικό ότι οι μεγάλες εταιρείες προσλαμβάνουν ειδικώς εκπαιδευμένο προσωπικό (security administration), που καταστρώνει ειδικά σχέδια προστασίας του δικτύου της εταιρείας (system administration).

Μέχρι προσφάτως ο όρος «κρυπτογραφία» περιοριζόταν μόνο στον στρατιωτικό και τον διπλωματικό χώρο. Σήμερα όμως που η επικοινωνία με το ηλεκτρονικό ταχυδρομείο (e-mail) έχει αυξηθεί αλματωδώς, η κρυπτογραφία αποτελεί σημαντικό παράγοντα του κυβερνοχώρου. Με την χρήση της κρυπτογραφίας δεν διακινούνται βέβαια μόνον νόμιμα, αλλά και παράνομα δεδομένα στον κυβερνοχώρο, όπως π.χ. ανταλλαγή πορνογραφικού υλικού, ανταλλαγή παρανόμων μηνυμάτων από οργανωμένους ή μη εγκληματίες κλπ.

Η διαδικασία της κωδικοποίησης των δεδομένων λέγεται κρυπτογράφηση (enscryption). Η κρυπτογράφηση στηρίζεται σε κλειδί (key) που πρέπει να κατέχει τόσο αυτός που στέλνει τα δεδομένα, όσο και αυτός που τα παραλαμβάνει. Αν ο παραλήπτης δεν κατέχει το κλειδί, υπάρχει κίνδυνος να γίνει υποκλοπή του κατά την μεταβίβαση (διαδρομή). Γενικώς η κρυπτογράφηση - αποκρυπτογράφηση γίνεται με την βοήθεια μιας μαθηματικής διαδικασίας.

Η διαδικασία της αποκατάστασης των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή λέγεται αποκρυπτογράφηση.

Είναι ευνόητο ότι, με την χρήση της κρυπτογραφίας αποκρύπτεται, όχι μόνον το περιεχόμενο του παράνομου υλικού που διακινείται, αλλά αποφεύγεται επιπλέον και ο εντοπισμός του δράστη. Βέβαια ο εντοπισμός του δράστη μπορεί να αποφευχθεί και με την λεγομένη «ανωνυμία στον κυβερνοχώρο».

Από νομικής απόψεως ενδιαφέρον παρουσιάζει το ερώτημα, εάν είναι σύμφωνα με τις βασικές Αρχές του Δικαίου, η απαγόρευση χρήσεως της κρυπτογραφίας ή ο περιορισμός αυτής σε άτομα ή φορείς (π.χ. κρατικούς), που έχουν ειδική προς τούτο άδεια.

7. Σχέση ασφάλειας και δικαιώματος ανωνυμίας στο διαδίκτυο

Είναι γνωστό ότι κάθε χρήστης του διαδικτύου (Internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητά του. Με κατάλληλες όμως τεχνικές παρεμβάσεις μπορεί να έχει κάποιος πρόσβαση στο διαδίκτυο ως ανώνυμος ή ακόμα και με ψευδή στοιχεία που αναφέρονται σε άλλο άτομο. Η παρουσίαση βέβαια με ψευδή στοιχεία μπορεί να γίνει και στο «κοινό» εγκληματικό περιβάλλον. Εκεί όμως ο εντοπισμός του δράστη είναι ευκολότερος. Μπορεί ακόμα ο χρήστης του διαδικτύου να έχει ως στοιχείο ταυτότητος το όνομα «ανώνυμος», οπότε τυπικά φαίνεται ότι έχει όνομα. Η δυνατότητα αυτής της ανωνυμίας στο διαδίκτυο (Internet) διευκολύνει την

διάπραξη παρανομιών και κάνει δύσκολο, αν όχι και αδύνατο τον εντοπισμό του δράστη. Επιπλέον η ανωνυμία, σε συνδυασμό με την ανυπαρξία ή την δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους «ηλεκτρονικούς δράστες» να αισθάνονται ασφαλείς κατά την διάπραξη των εγκλημάτων των.

Το ερώτημα που προκύπτει στο σημείο αυτό είναι, μήπως σε περίπτωση ψήφισης σχετικού νόμου για το διαδίκτυο, πρέπει να ποινικοποιηθεί η ανώνυμη χρήση του, ή ακόμα και η παρουσία με ψευδή στοιχεία. Κάτι τέτοιο βέβαια επαφίεται στην βούληση του νομοθέτη. Αξίζει όμως να σημειωθεί, σχετικός νόμος που ψηφίστηκε στις Η.Π.Α και τιμωρούσε ποινικά την ανώνυμη χρήση ή την χρήση με ψεύτικο όνομα στο διαδίκτυο , κηρύχθηκε αντισυνταγματικός από τα Δικαστήρια των ΗΠΑ . Και αυτό γιατί, η ανωνυμία δεν χρησιμοποιείται στο διαδίκτυο μόνον από τους παράνομους, αλλά και από όσους θέλουν να αποκρύψουν αυστηρώς προσωπικά των (νόμιμα) στοιχεία.

Β' Μέρος - ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΑΠΟ ΤΙΣ ΔΙΩΚΤΙΚΕΣ ΑΡΧΕΣ

1. Γενικές παρατηρήσεις

Ο «παραδοσιακός» τρόπος προσεγγίσεως του εγκλήματος, δηλ. της περιγραφής του δράστη με την κατάθεση του θύματος, της συλλογής πληροφοριών από πληροφοριοδότες της διεξαγωγής έρευνας, κατάσχεσης κλπ. δεν ισχύει στον κυβερνοχώρο. Ο "ηλεκτρονικός δράστης» ή « ηλεκτρονικός εγκληματίας» δεν θα πάρει το όπλο, ούτε θα φορέσει τα γάντια και θα εισέλθει στη Τράπεζα για να τη ληστέψει ή σε ένα σπίτι για να κλέψει. Αντίθετα με τους κατάλληλους κωδικούς αριθμούς, που κατά κανόνα παράνομα έχει αποκτήσει (πάλι διαπράττοντας ένα ηλεκτρονικό έγκλημα) θα δώσει εντολή για μεταφορά ενός χρηματικού ποσού από τον λογαριασμό του «ηλεκτρονικού θύματος» σε ένα άλλο στο εξωτερικό. Και όταν το θύμα πάρει

είδηση την εναντίον του ενέργεια ο δράστης ή θα έχει μεταφέρει τα χρήματα σε διάφορους άλλους λογαριασμούς για να χαθούν τα ίχνη του, ή θα τα έχει «σηκώσει» και θα έχει εξαφανισθεί. Στο μέλλον οι κλέφτες δεν θα κυκλοφορούν με την κουκούλα και το περίστροφο στο χέρι, ούτε θα τους περιμένει ο συνεργός τους με την μηχανή αναμμένη για να διαφύγουν. Οι μελλοντικοί κλέφτες θα είναι σκυμμένοι πάνω σε ένα πληκτρολόγιο, μέσω του οποίου θα δίνουν εντολές σε μικρούς, αλλά πανίσχυρους ηλεκτρονικούς υπολογιστές και οι κλοπές τους θα απαιτούν από τους Αστυνομικούς, όλο και πιο εξειδικευμένες γνώσεις.

Αλλά και στην περίπτωση εκείνη που ο παθών αντιλαμβάνεται εγκαίρως ότι έπεσε θύμα ηλεκτρονικού εγκλήματος, ερωτάται: Σε ποια Αρχή θα καταγγείλει το έγκλημα αυτό; Έχει η Αρχή αυτή τις απαιτούμενες γνώσεις να ερευνήσει την αξιόποινη πράξη που της καταγγέλθηκε;

2. Αρμόδιες υπηρεσίες για την έρευνα του εγκλήματος στον κυβερνοχώρο

Στα λεγόμενα τεχνολογικώς αναπτυγμένα κράτη, όπου το έγκλημα στον κυβερνοχώρο «ανθεί», έχουν συσταθεί ειδικές υπηρεσίες για την έρευνα και καταπολέμηση του νέου αυτού εγκλήματος. Ενδεικτικώς αναφέρεται ότι στις Η.Π.Α. το F.B.I. έχει συστήσει το National Infrastructure Protection Center (NIPC), με παραρτήματα σε διάφορες πολιτείες για την έρευνα των σχετικών εγκλημάτων. Στα πλαίσια μάλιστα της «Ηλεκτρονικής Αστυνομίας» έχει συσταθεί ειδική μονάδα, που έχει ως αντικείμενο το «σπάσιμο» των κωδικών των ηλεκτρονικών επιστολών (e-mails), που χρησιμοποιούν οι έμποροι ναρκωτικών και τα δίκτυα παιδεραστίας. Ομοίως έχει συσταθεί ειδικό σώμα Εισαγγελέων, οι οποίοι ύστερα από κατάλληλη εκπαίδευση, ασχολούνται με το έγκλημα στον κυβερνοχώρο. Παρόμοια εκπαίδευση έχει γίνει και στους Δικαστές. Στην Scotland Yard έχει συσταθεί το Computer Fraud Squad. Στον Καναδά έχει συσταθεί το the Royal Canadian Mounted Police Computer Crime Unit.

Δεκάδες συναντήσεις, συνέδρια κλπ γίνονται κάθε χρόνο από τις παραπάνω υπηρεσίες για θέματα σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Επίσης έχουν εκδοθεί δεκάδες γραπτές οδηγίες (guide lines) και Κώδικες Πρακτικής (Code of Practice), που απευθύνονται στους δημόσιους εκείνους λειτουργούς, οι οποίοι είναι επιφορτισμένοι με την έρευνα και την καταπολέμηση των σχετικών εγκλημάτων. Ενδεικτικώς αναφέρεται ο Κώδικας Πρακτικής του Τμήματος Εμπορίου και Βιομηχανίας (DTI) της Βρετανίας (The British Code of Practice - Department of Industry).

3. Γενικά για τις έρευνες που έχουν σχέση με το έγκλημα στον κυβερνοχώρο

Οι δικαστικές-αστυνομικές έρευνες που γίνονται προς διακρίβωση εγκλημάτων του κυβερνοχώρου, ουδεμία σχέση έχει με τις έρευνες, που μέχρι τώρα γνωρίζουμε. Στις μέχρι τώρα «παραδοσιακές» έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κλπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα έχει να ψάξει files , note pads , botes, dada, κρυπτογραφημένα στοιχεία κλπ. Μπορεί το προς έρευνα αντικείμενο να βρίσκεται μπροστά στα μάτια του ερευνητή και να μην μπορεί να το εντοπίσει, εάν δεν έχει τις απαραίτητες τεχνικές γνώσεις. Ερωτάται λοιπόν, πως θα διεξαχθεί σε μια τέτοια περίπτωση η αστυνομική έρευνα; Ο «παραδοσιακός Εισαγγελέας» και η «παραδοσιακή αστυνομία» δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων.

Ένα άλλο πρόβλημα είναι ότι στην κοινή έρευνα το αντικείμενο βρίσκεται σε ένα σημείο. Αντίθετα στο έγκλημα του κυβερνοχώρου το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές οι οποίοι μάλιστα μπορεί να βρίσκονται σε διάφορες χώρες. Το πρόβλημα του τόπου τελέσεως είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζεται κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι, η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή και χιλιάδες τόπους τελέσεως. Γενικώς ο αριθμός των τόπων τελέσεως

εξαρτάται από την συγκεκριμένη λειτουργία του διαδικτύου (αποστολή e-mails, new groups, internet relay chat, κλπ). Ακόμα και σε δορυφόρους (Satellite-technology) είναι δυνατό να βρίσκονται τα αποδεικτικά στοιχεία, δεδομένου ότι, οι επικοινωνίες (κινητά τηλέφωνα κλπ.) γίνονται πλέον δορυφορικώς.

Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας, αλλά και σε θέματα κατά τόπον αρμοδιότητος ως προς την εκδίκαση της πράξεως. Η έννοια επίσης των γεωγραφικών συνόρων είναι άγνωστη στα εγκλήματα του κυβερνοχώρου. Ειδικότερα, όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ των ολόκληρος ο πλανήτης αποτελεί «μία χώρα». Κατά συνέπεια οι μέχρι τώρα Διεθνείς Συμβάσεις περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασίας, είναι "παραχωρημένες" στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη.

4. Η Ελληνική Αστυνομική Πραγματικότητα

Στην Ελληνική Αστυνομία από το 2003 λειτουργεί τμήμα, που ερευνά αποκλειστικά το έγκλημα στον κυβερνοχώρο. Πρόκειται για το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος υπο την εποπτεία του Αστυνόμου Α' και προϊσταμένου του τμήματος, κ. Εμμανουήλ Σφακιανάκη.

Σε κάθε περίπτωση όμως την σχετική έρευνα συνδράμει με τις ειδικές της γνώσεις η Διεύθυνση Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) και ειδικότερα το εργαστήριο γραφολογίας, στο οποίο υπάγεται και λειτουργεί ο Τομέας Ανάλυσης Ψηφιακών δεδομένων. Ο Τομέας αυτός δημιουργήθηκε το 1992, στελεχώνεται δε από ειδικά εκπαιδευμένους αστυνομικούς, με τεχνογνωσία στην εξέταση λογισμικού κατασχεθέντων ηλεκτρονικών υπολογιστών, στο «σπάσιμο» κωδίκων κλπ.

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΕΞΙΧΝΙΑΣΘΕΝΤΩΝ ΥΠΟΘΕΣΕΩΝ ΤΗΣ ΓΑΔΑ
ΑΠΟ 1-1-2004 ΕΩΣ ΚΑΙ 25-7-2004[175]

ΑΔΙΚΗΜΑ	ΥΠΟΘΕΣΕΙΣ	ΣΥΛΛΗΦΘΕΝΤΕΣ	ΚΑΤΗΓΟΡΟΥΜΕΝΟΙ
348 Α Π.Κ. & Ν. 5060/1931 «ΠΟΡΝΟΓΡΑΦΙΑ ΑΝΗΛΙΚΩΝ» ΚΑΙ «ΠΕΡΙ ΑΣΕΜΝΩΝ ΔΗΜΟΣΙΕΥΜΑΤΩΝ»	10	36	36
386 Α Π.Κ. «ΑΠΑΤΗ ΜΕ ΥΠΟΛΟΓΙΣΤΗ» HACKING	3	0	3
370 Β Π.Κ. «ΠΑΡΑΒΙΑΣΗ ΑΠΟΡΡΗΤΩΝ ΣΕ ΥΠΟΛΟΓΙΣΤΗ»	3	0	8
«ΔΙΑΡΡΟΗ ΔΙΑΒΑΘΜΙΣΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΜΕΣΩ INTERNET»	1	0	1
Αρ. 66 Ν. 2121/93 «ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ» & 394 Π.Κ. «ΑΠΟΔΟΧΗ ΚΑΙ ΔΙΑΘΕΣΗ ΠΡΟΪΟΝΤΩΝ ΕΓΚΛΗΜΑΤΟΣ ΜΕΣΩ INTERNET» & 386 Π.Κ. «ΑΠΑΤΗ ΜΕ ΥΠΟΛΟΓΙΣΤΗ»	2	3	3
«ΣΥΚΟΦΑΝΤΙΚΗ ΔΥΣΦΗΜΗΣΗ ΜΕΣΩ INTERNET»	1	0	2
361 Π.Κ. «ΕΡΓΟ ΕΞΥΒΡΙΣΗ ΜΕΣΩ INTERNET»	1	0	1
ΣΥΝΟΛΙΚΑ	**21**	**39**	**54**

Πίνακας 4-1

5. Συλλογή και διατήρηση των αποδεικτικών στοιχείων

Η ανακριτική τεχνική, όπως είναι η συλλογή των αποδεικτικών στοιχείων, η λήψη των μαρτυρικών καταθέσεων, η διενέργεια των ερευνών κλπ, απαιτεί διαφορετική τεχνική από εκείνη των «κοινών» εγκλημάτων. Κύριο χαρακτηριστικό της συλλογής και εκτίμησης των αποδεικτικών στοιχείων είναι ότι, οι νομικές γνώσεις του (προ) ανακριτικού υπαλλήλου δεν επαρκούν για την έρευνα της υποθέσεως. Οι κατάλληλες και επαρκείς ειδικές τεχνικές γνώσεις είναι εξ ίσου σημαντικές -αν όχι και σημαντικότερες- από τις νομικές. Π.χ. η εσφαλμένη αποσύνδεση των καλωδίων του ηλεκτρονικού υπολογιστή, στον οποίο είναι *αποθηκευμένα* τα αποδεικτικά στοιχεία. Μπορεί να οδηγήσει στην εξαφάνισή «χάσιμο» των. Η παρατηρητικότητα επίσης του (προ)ανακριτικού υπαλλήλου είναι σημαντική, π.χ. ο συνδυασμός αριθμών, που μπορεί μεν να εμφανίζονται (εξωτερικώς) ως αριθμοί τηλεφώνων,

[175] Πηγή ΓΑΔΑ. Γραφείο Ηλεκτρονικού Εγκλήματος

ενδεχομένως να αποτελούν τα «κλειδιά» (passwords) πρόσβασης στο σύστημα ή ακόμα και τους κωδικούς αποκρυπτογράφησης, σε περίπτωση που τα στοιχεία (data) τηρούνται κρυπτογραφημένα. Μετά την συλλογή των αποδεικτικών στοιχείων σημαντική είναι η γνώση του (προ)ανακριτικού υπαλλήλου για την διατήρησή των. Η έκθεσή των π.χ. σε ήλιο, υγρασία, σκόνη κλπ, ενδεχομένως να οδηγήσει στην καταστροφή των.

6. Ηλεκτρονική απόδειξη

Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα «παραδοσιακά» αποδεικτικά μέσα. Τα τελευταία αυτά είναι «χειροπιαστά», έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα τα ηλεκτρονικά αποδεικτικά μέσα είναι κατά κανόνα «μη χειροπιαστά» μπορεί να τα κατευθύνει ή και να τα διαχειρίζεται κάποιος από μακριά, να αλλάζει την μορφή και το περιεχόμενό των ή ακόμα και να τα εξαφανίζει με το πάτημα ενός πλήκτρου.

Για παράδειγμα, ο εγκληματίας Α αποστέλλει με το ηλεκτρονικό ταχυδρομείο (e-mail) κρυπτογραφημένη επιστολή από την χώρα Χ, στον επίσης εγκληματία Β, ο οποίος διαμένει στην χώρα Ψ, αναφέροντάς του λεπτομέρειες σχετικά με την ελεγχόμενη παράδοση (άρθρο 9 Ν. 1990/91) μεγάλης ποσότητος ναρκωτικών ουσιών. Η Αστυνομική Αρχή της χώρας που παρακολουθεί την περίπτωση διαπιστώνει ότι ο Β, δεν παραλαμβάνει αμέσως το «γράμμα» (e-mail), γιατί κατά την ώρα αποστολής - λήψεως έχει κλειστό τον ηλεκτρονικό υπολογιστή του.

Ερωτάται: Σε ποιες νόμιμες ενέργειες μπορεί να προβεί η Αστυνομία προκειμένου να αποκτήσει και στη συνέχεια να χρησιμοποιήσει το «κλειδί» του κρυπτογραφημένου μηνύματος; Θεωρείται το *e-mail* επιστολή τηλεγράφημα ή τηλεομοιοτυπικό έγγραφο (fax) ; Σε περίπτωση που αυτό (e-mail) θεωρείται ως επιστολή, πρέπει να εφαρμοστούν οι σχετικές διατάξεις περί ανοικτών επιστολών (Συνταγματική προστασία κλπ.) ή περί κλειστών

επιστολών (ευκολότερη κατάσχεση κλπ.) Δικαιούται η Αστυνομία να κατάσχει το «γράμμα» (e-mail) στις εγκαταστάσεις του παροχέα; Σε θετική περίπτωση δικαιούται να ανοίξει το e-mail και να το διαβάσει; Όταν το e-mail βρίσκεται στις εγκαταστάσεις του παροχέα αποτελεί κλειστή ή ανοικτή επιστολή; Μπορεί η Αστυνομική Αρχή να υποχρεώσει τον παροχέα να της παραδώσει όλη την ηλεκτρονική αλληλογραφία μεταξύ Α και Β; Μπορεί να υποχρεωθεί ο παροχέας να φυλάττει για ορισμένο χρονικό διάστημα (και για πόσο) τα «στοιχεία – δεδομένα» (data) που «περνούν» από τις εγκαταστάσεις του; Και μόνο το παραπάνω απλό (για το διαδίκτυο) παράδειγμα αρκεί για να δώσει το μέγεθος των σημαντικών προβλημάτων που αντιμετωπίζει, αυτός που ασχολείται με την έρευνα του εγκλήματος στο διαδίκτυο.

7. Ηλεκτρονική Υπογραφή (digital Signature)

Χαρακτηριστική περίπτωση ηλεκτρονικής αποδείξεως αποτελεί η αξιολόγηση της ηλεκτρονικής ή ψηφιακής υπογραφής (digital Signature). Ψηφιακή υπογραφή είναι η υπογραφή εκείνη που τίθεται στα (ηλεκτρονικά) έγγραφα, τα οποία διακινούνται δια μέσου του διαδικτύου (ή και των computers γενικότερο) από τον εκδότη του εγγράφου. Έχει σχέση δηλ. η ψηφιακή υπογραφή με την γνησιότητα του εγγράφου και αποτελεί το αντίστοιχο της ιδιόχειρης (φυσικής) υπογραφής. Η ψηφιακή υπογραφή τίθεται σε συμφωνίες που γίνονται «εξ αποστάσεως» δηλ. οι αντισυμβαλλόμενοι βρίσκονται σε διαφορετικό τόπο. Η ψηφιακή υπογραφή είναι συνυφασμένη με την κρυπτογραφία. Βρίσκει πρακτική εφαρμογή στις Τράπεζες, στο ηλεκτρονικό εμπόριο, στις ηλεκτρονικές συναλλαγές και ειδικότερα στις συναλλαγές που γίνονται εξ αποστάσεως. Λέγοντας ηλεκτρονικό εμπόριο (electronic commerce ή απλώς e- commerce) εννοούμε την εμπορική εκείνη δραστηριότητα που αναπτύσσεται δια μέσου συνδεδεμένων ηλεκτρονικών υπολογιστών (internet).

Στο Ποινικό Δίκαιο ο Νομοθέτης προσδιορίζει την έννοια του ηλεκτρονικού εγγράφου στο άρθρο 13γ του Π.Κ., όπως αυτό τροπ. με άρθρο 2

Ν.1805/88. Σύμφωνα λοιπόν με το άρθρο αυτό έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβιβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.

Σχετική με την έννοια του ηλεκτρονικού εγγράφου είναι και η διάταξη του άρθρου 444 περ. 3 Κ.Πολ.Δικ. σύμφωνα με την οποία ιδιωτικά έγγραφα θεωρούνται και οι φωτογραφικές ή κινηματογραφικές αναπαραστάσεις φωνοληψίες και κάθε άλλη μηχανική απεικόνιση. Σκοπός της ηλεκτρονικής υπογραφής είναι να εξασφαλίσει την γνησιότητα του ηλεκτρονικού εγγράφου, τόσο ως προς τον εκδότη του, όσο και ως προς το περιεχόμενό του. Δηλαδή με άλλα λόγια με την ψηφιακή υπογραφή, το ηλεκτρονικό έγγραφο αποκτά ανάλογη αποδεικτική δύναμη με το «φυσικό» έγγραφο, που φέρει ιδιόχειρη υπογραφή. Η ψηφιακή υπογραφή, όπως και όλο το περιεχόμενο ενός ηλεκτρονικού εγγράφου, μπορεί να πλαστογραφηθεί, και μάλιστα χωρίς να αφήσει καθόλου (ορατά) ίχνη.

8. Συμπεράσματα και Προτάσεις

8.1. Συμπεράσματα

Η τεχνολογία, οι ηλεκτρονικοί υπολογιστές και ο κυβερνοχώρος έχουν εισέλθει για καλά στη ζωή μας. Ακόμα και στην επαγγελματική ζωή του Νομικού, η γραπτή - έντυπη δομή του Δικαίου τείνει να αντικατασταθεί από την *ηλεκτρονική εποχή του Δικαίου*. Όποιος αρνείται να ασχοληθεί με την σύγχρονη τεχνολογία ομοιάζει με αυτόν που, όταν ανακαλύφθηκε το

αυτοκίνητο αρνιόταν να ανέβει σε αυτό και προτιμούσε να πηγαίνει με το γαϊδουράκι ή στην καλύτερη περίπτωση με το άλογο.

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computer) και διαδικτύου (internet). Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στον πεδίο του εγκλήματος στον κυβερνοχώρο, χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, για την κατανόηση των νομικών θεμάτων του διαδυκτίου, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις.

Το ήδη υπάρχον «νομικό οπλοστάσιο» δεν επαρκεί για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Γι' αυτό απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών υποστάσεων εγκλημάτων, που να θέτουν όρια στην συμπεριφορά όσων χρησιμοποιούν το διαδίκτυο. Κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθεί υπόψη η ελεύθερη διακίνηση των ιδεών και οι λοιπές Συνταγματικές Αρχές, που ισχύουν στον κοινό «Δικαιϊκό χώρο».

Οι εισαγγελικές, δικαστικές, αστυνομικές αρχές κλπ, δεν έχουν μέχρι στιγμής τις απαιτούμενες γνώσεις, για την αντιμετώπισή του εγκλήματος στον κυβερνοχώρο. Και αυτό είναι πολύ λογικό, αφού ουδεμία εκπαίδευση έχουν υποστεί μέχρι τώρα. Είναι βέβαιον δε ότι, εάν η πολιτεία δεν φροντίσει για την εκπαίδευσή των στα αντίστοιχα θέματα, θα υπάρξει (στο πολύ σύντομο μέλλον) αδυναμία απονομής ορθής δικαιοσύνης σε θέματα εγκληματικότητας του κυβερνοχώρου και ηλεκτρονικής εγκληματικότητας γενικότερα. Απαραίτητη επομένως καθίσταται η άμεση εκπαίδευση, όσων Αρχών (Εισαγγελικών, Δικαστικών, Αστυνομικών) ασχολούνται με θέματα διαδικτύου και ηλεκτρονικής εγκληματικότητας γενικότερα.

8.2. Προτάσεις

Απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών υποστάσεων εγκλημάτων, που να θέτουν όρια στην συμπεριφορά όσων χρησιμοποιούν το διαδίκτυο. Κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθεί υπόψη η ελεύθερη διακίνηση των ιδεών και οι λοιπές Συνταγματικές Αρχές, που ισχύουν στον κοινό «Δικαιϊκό χώρο». Απαραίτητη καθίσταται η εκπαίδευση όσων Αρχών (Εισαγγελικών, Δικαστικών, Αστυνομικών) σε θέματα διαδικτύου και ηλεκτρονικής εγκληματικότητας γενικότερα.[176]

[176] Βλ., στο http://www.diaplous.org/library/nomothesia.php

Κεφάλαιο 9ο – Έρευνες, Μελέτες & Περιστατικά για το Ηλεκτρονικό Έγκλημα

9.1. - Έρευνα 1η: Έρευνα Ηλεκτρονικού Εγκλήματος & Ασφάλειας του CSI/FBI/2003[177]

CSI

ΙΝΣΤΙΤΟΥΤΟ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

[177] Του Robert Richardson

Η Έρευνα Ηλεκτρονικού Εγκλήματος και ασφαλείας καθοδηγείται από το Ινστιτούτο Ηεκτρονικής Ασφάλειας (CSI) με την συμμετοχή της ομάδας δίωξης ηλεκτρονικής διείσδυσης του Ομοσπονδιακού Γραφείου Ερευνών του Σαν Φρανσίσκο. Η έρευνα που τώρα βρίσκεται στο όγδοο έτος της, έχει χαρακτηριστεί ως η πιο μακροχρόνια έρευνα στο πεδίο της ασφάλειας πληροφοριών. Όπως και τις προηγούμενες χρονιές, η επισκόπηση σκιαγραφεί ένα πορτρέτο για το πόσο συχνά λαμβάνει χώρα ένα έγκλημα στο διαδίκτυο και πόσο δαπανηρό μπορεί να είναι ένα τέτοιου είδους έγκλημα.

Βασισμένη στις ανταποκρίσεις 530 επαγγελματιών ηλεκτρονικής ασφάλειας στις Ηνωμένες Πολιτείες σε οργανισμούς, κυβερνητικές υπηρεσίες, οικονομικά ιδρύματα, ιατρικά ιδρύματα και πανεπιστήμια, τα ευρήματα του 2003 για άλλη μια φορά δείχνουν ότι δεν υπάρχει μείωση επιθέσεων αλλά υποδηλώνουν ότι φέτος η δριμύτητα και το κόστος αυτών των επιθέσεων έχει πτωτική τάση για πρώτη φορά από 1999.

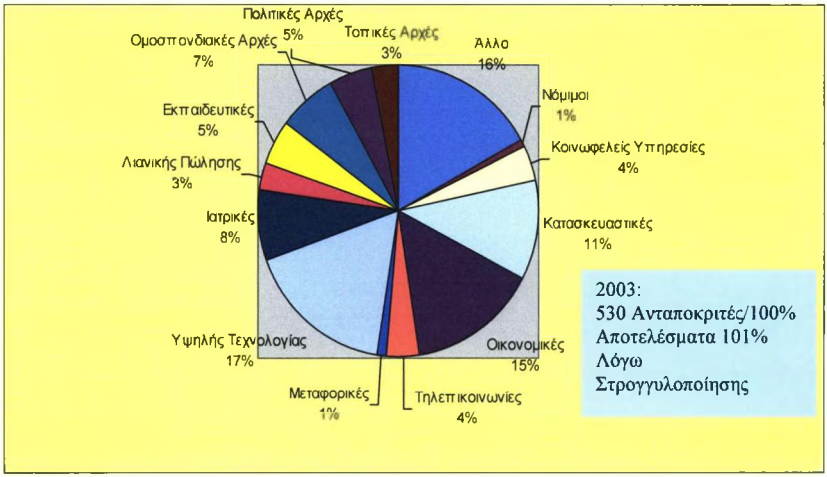
Παρά τον χαμηλότερο αριθμό για συνολικές οικονομικές απώλειες ανάμεσα σε ανταποκριτές της επισκόπησης, το πιο σημαντικό συμπέρασμα που κάποιος πρέπει να κρατήσει από την έρευνα παραμένει ότι το ρίσκο των διαδικτυακών επιθέσεων συνεχίζει να είναι υψηλό. Ακόμα και οργανισμοί που έχουν αναπτύξει και έχουν διευρύνει τεχνολογίες ασφαλείας μπορούν να πέσουν θύματα με σημαντικές απώλειες. Επιπλέον, το ποσοστό των περιστατικών αυτών που αναφέρονται στις αρχές παραμένει χαμηλό. Έτσι οι επιδρομείς μπορούν λογικά να συμπεράνουν ότι οι πιθανότητες να στο να πιαστούν και να μην καταδικαστούν παραμένουν ισχυρά με το μέρος τους.

ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΑΝΤΑΠΟΚΡΙΤΕΣ

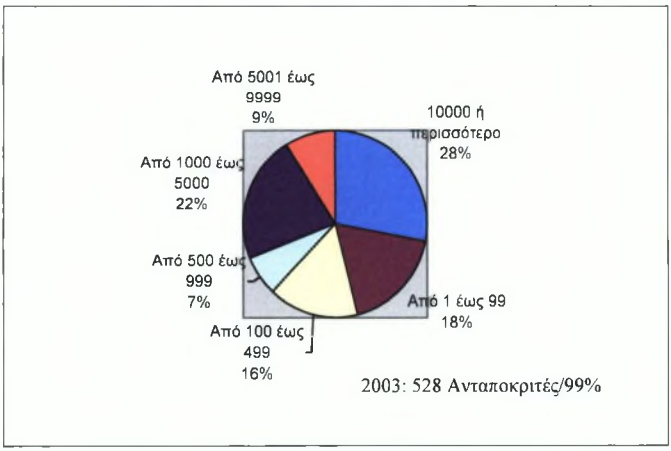
Αυτοί που απαντούν στην έρευνα αντιπροσωπεύουν εταιρείες και οργανισμούς δια μέσω της μοντέρνας ζωής. Ένα 17 τοις εκατό προέρχεται από εταιρείες υψηλής τεχνολογίας, και ένα επιπρόσθετο 15 τοις εκατό προέρχεται από τον οικονομικό τομέα. Οι κυβερνητικές υπηρεσίες συγκεντρώνουν

συνολικά περίπου το 15 τοις εκατό των ανταποκριτών της έρευνας. Έτσι, περίπου οι μισές από τις ανταποκρίσεις προέρχονται από αρχηγεία όπου είναι μόλις απίθανο η ηλεκτρονική ασφάλεια να ήταν σημαντική ανησυχία. Αυτό προσεγγίζει αρκετά τις προηγούμενες χρονιές, παρ' όλο που αυτοί που απαντούν άλλο αυξήθηκαν στο 17 τα εκατό από μόλις 5 τα εκατό στην έρευνα του 2002.

Ανταποκριτές ανά Βιομηχανικό Τομέα



Ανταποκριτές ανά Αριθμό Εργαζομένων



Περισσότεροι από τους μισούς οργανισμούς που αντιπροσωπεύονται στην έρευνα απασχολούν περισσότερους από 1000 εργαζομένους, με περίπου το ¼ των ανταποκριτών (28 τα εκατό) να αναφέρουν περισσότερους απο 10000 εργαζομένους. Αυτό πάνω - κάτω αντιστοιχεί σε εισοδήματα : το 34 τα εκατό αναφέρει περισσότερα από 1 δισεκατομμύριο δολάρια στα ετήσια

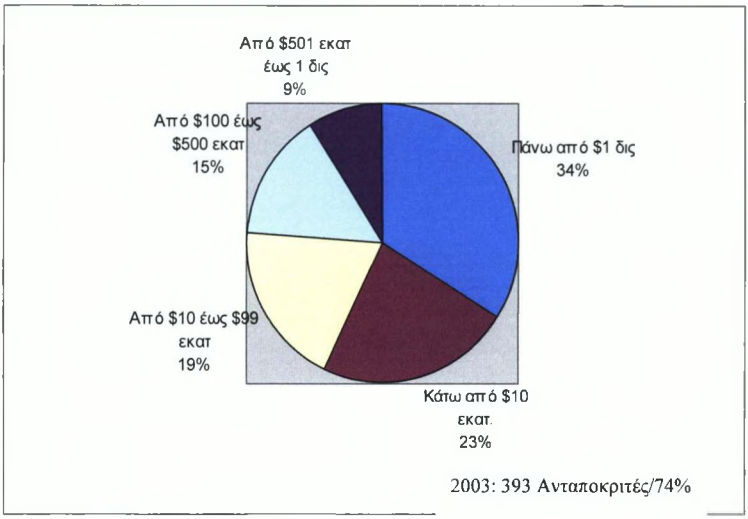
εισοδήματα. Ενώ αυτό ξεκάθαρα δείχνει ότι η μεγάλη σε κλίμακα σωματείων Αμερική εκπροσωπείται επάξια ανάμεσα στο σύνολο των μελών του CSI και ανάμεσα στους ανταποκριτές της έρευνας, δεν είναι το θέμα ότι οι εμπειρίες μικρών επιχειρήσεων δεν έχουν θέση στην έρευνα. Στην πραγματικότητα, το 18% των ανταποκριτών εργάζονται σε οργανισμούς με 99 ή λιγότερους υπαλλήλους και το 23% εργάζονται σε οργανισμούς με ετήσια αναφορά εισοδήματος λιγότερο από 10 εκατομμύρια δολάρια.

Αυτοί που πραγματικά απαντούν τις ερωτήσεις της έρευνας είναι, χωρίς να μας ξαφνιάζει, επαγγελματίες ασφαλείας. Επιπλέον είναι αυτοεπιλεγόμενοι και υποτίθεται πως είναι περισσότερο ευαίσθητοι σε θέματα ασφαλείας απ' ότι είναι αυτοί που δεν συνεργάζονται με επαγγελματικούς οργανισμούς όπως το CSI. Αυτοί είναι άνθρωποι που δίνουν περισσότερη σημασία στο ηλεκτρονικό έγκλημα και που είχαν άμεσο ενδιαφέρον στο να το αποτρέψουν.

ΤΑ ΕΠΙΚΕΝΤΡΑ ΤΗΣ ΕΡΕΥΝΑΣ

Ενώ το ποσοστό των ανταποκριτών που αναφέρουν κάποια μορφή απαγορευμένης χρήσης ηλεκτρονικού υπολογιστή παρέμεινε περίπου το ίδιο με προηγούμενες χρονιές, οι οικονομικές απώλειες αυτού του είδους που αναφέρθηκαν έχουν μειωθεί. Το 56 τα εκατό των ανταποκριτών ανέφεραν απαγορευμένη χρήση σε σχέση με πέρυσι που ήταν 60% (και σε σύγκριση με ένα μέσο όρο του 59% τα τελευταία 7 χρόνια της επισκόπησης). Οι συνολικές ετήσιες απώλειες που αναφέρθηκαν στην επισκόπηση του 2003 ήταν

$201,797,340 ένας αριθμός που μειώθηκε κατά 56 τα εκατό από το υψηλότερο σημείο των 445 εκατομμυρίων που αναφέρθηκαν πέρυσι. Θα έπρεπε να σημειωθεί παρ' όλα αυτά ότι αυτός ο αριθμός σχετίζεται με προγενέστερους αριθμούς του 2001 που αναφέρθηκαν. Συγκεκριμένα είναι σημαντικό να θυμόμαστε ότι αυτός ο αριθμός είναι απλά οι συνολικές απώλειες που αναφέρθηκαν από έναν συγκεκριμένο αριθμό οργανισμών (251 από αυτούς) και δεν είναι κάποιου είδους βασικότερο σύνολο.



Ανταποκριτές ανά Συνολικό Εισόδημα

ΑΛΛΑ ΣΗΜΑΝΤΙΚΑ ΕΥΡΗΜΑΤΑ

- Ο συνολικός αριθμός των σημαντικών περιστατικών παρέμεινε πάνω - κάτω ο ίδιος όπως πέρυσι παρά την μείωση των οικονομικών απωλειών.
- Όπως και τα προηγούμενα χρόνια η κλοπή ιδιωτικών πληροφοριών προκάλεσε τις μεγαλύτερες οικονομικές απώλειες (χάθηκαν $70,195,900 με τον μέσο όρο απωλειών που αναφέρθηκαν να αγγίζει περίπου τα 2,7 εκατομμύρια δολάρια).

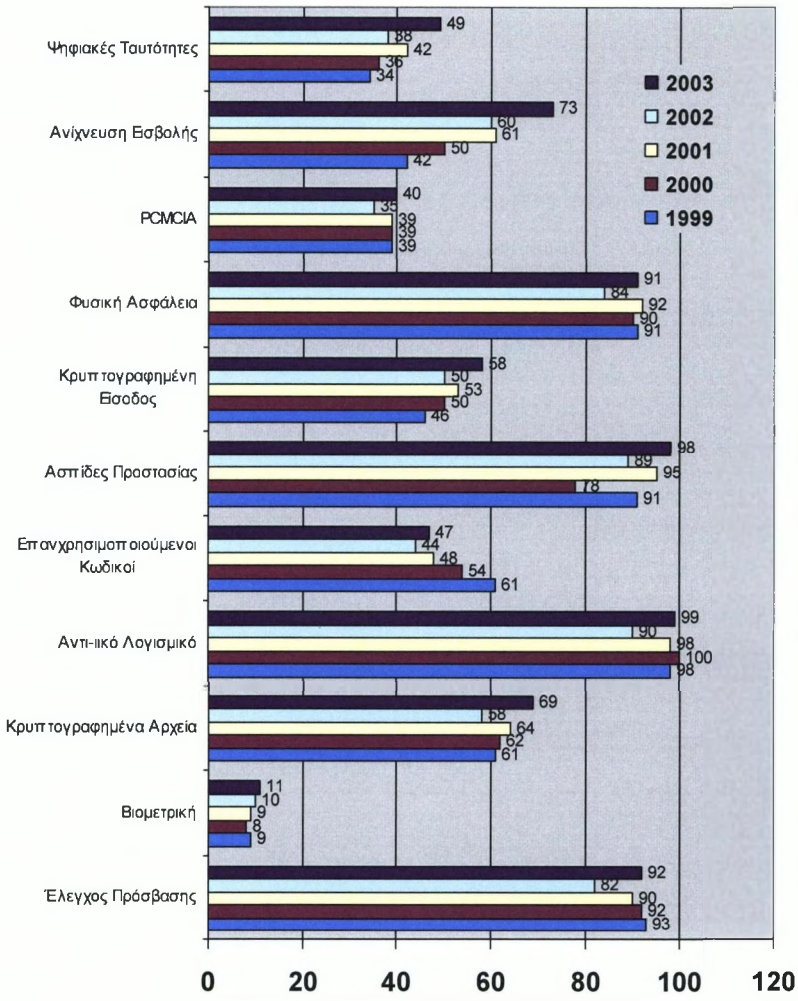
- Σε μία μετατόπιση από τα προηγούμενα χρόνια το δεύτερο πιο δαπανηρό ηλεκτρονικό έγκλημα ανάμεσα στους ανταποκριτές της έρευνας ήταν η άρνηση υπηρεσιών με κόστος που έφτασε τα $65,643,300.
- Οι απώλειες που αναφέρθηκαν για οικονομική εξαπάτηση μειώθηκαν δραστικά στα $10,186,400. Αυτό σε σύγκριση με πέρυσι όπου αναφέρθηκαν απώλειες περίπου 116 εκατομμυρίων δολαρίων.
- Όπως και σε προηγούμενες χρονιές τα περιστατικά ιών (82%) και οι εσωτερικές προσβολές της διαδικτυακής πρόσβασης (80%) ήταν οι πιο αξιομνημόνευτες μορφές επίθεσης ή προσβολής.
- Για ακόμη μια φορά οι ανταποκριτές εναντιώθηκαν αυστηρά στην ιδέα του να προσλάβουν πρώην χάκερς (68% ήταν εναντίον).
- Το ποσοστό αυτών που ανέφεραν ότι έπεσαν θύματα περιστατικών την περασμένη χρονιά, και που είπαν πως ανέφεραν πως ανέφεραν τα περιστατικά αυτά στις αρχές, παρέμειναν χαμηλά (30%).

Η ΧΡΗΣΙΜΟΠΟΙΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΑΣΦΑΛΕΙΑΣ

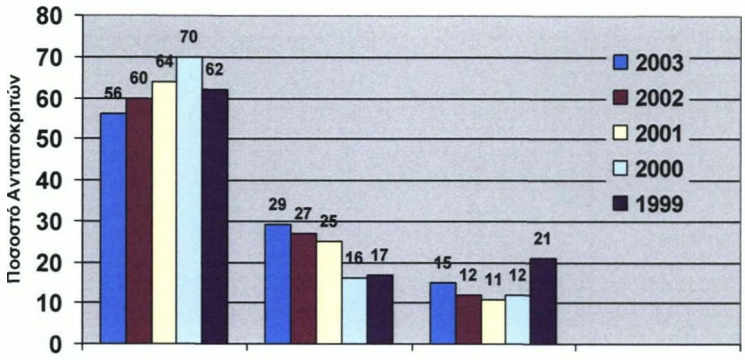
Για έκτη συνεχόμενη χρονιά οι ανταποκριτές ερωτήθηκαν για το τι είδους τεχνολογίες ασφαλείας είχαν εφαρμόσει για να προστατέψουν τους οργανισμούς τους. Παρ' όλο που στην επισκόπηση δεν απαντήθηκαν όλες οι ερωτήσεις από όλους τους ανταποκριτές, η ερώτηση για την χρήση διαφόρων ειδών τεχνολογίας απαντάται από το 99% (525 από τους 530) των ανταποκριτών.

Ουσιαστικά όλοι οι οργανισμοί χρησιμοποιούν λογισμικό ασφαλείας ενάντια στους ιούς (92%) και ασπίδες προστασίας (98%). Όπως θα περίμενε κανείς οι περισσότεροι (91%) εφαρμόζουν κάποιου είδους φυσικής ασφάλειας για να προστατέψουν τον υπολογιστή τους και περιουσιακά στοιχεία πληροφοριών και οι περισσότεροι εφαρμόζουν κάποιο μέτρο ελέγχου πρόσβασης (92%).

Τεχνολογίες ασφαλείας που χρησιμοποιήθηκαν



Μη εξουσιοδοτημένη χρήση υπολογιστικών συστημάτων μέσα στους τελευταίους 12 μήνες



2003: 524 Ανταποκρτές/99%
2002: 481 Ανταποκρτές/96%
2001: 532 Ανταποκρτές/99.6%
2000: 585 Ανταποκρτές/91%
1999: 512 Ανταποκρτές/98%

Αυτές οι δύο κατηγορίες είναι ίσως η κατάλληλη στιγμή να πούμε κάτι για την φύση αυτού του είδους των ανταποκρίσεων. Η έρευνα η ίδια, επιφυλακτικά, παραμένει χαμηλά και έχει παραμείνει κατά ένα μεγάλο ποσοστό η ίδια με το πέρασμα της οχτάχρονης ζωής της (αυτό όσο αναφορά το ενδιαφέρον της διατήρησης των τάσεων των πληροφοριών). Έτσι οι ανταποκριτές ερωτώνται να ερμηνεύσουν διάφορες πιθανές απαντήσεις στην έρευνα σύμφωνα με τη δική τους κατανόηση για την βιομηχανία ασφαλείας και την ορολογία της. Για τους περισσότερους, αυτή είναι μια ευαίσθητη προσέγγιση – το μεγαλύτερο μέρος της ορολογίας εντός της βιομηχανίας είναι επαρκώς διευθετημένη ότι δεν υπάρχει μεγάλη απορία για το τι σημαίνει όταν η έρευνα ρωτά για παράδειγμα αν χρησιμοποιούνται ασπίδες ασφαλείας. Δεν υπάρχει μεγάλη αμφιβολία για το τι είναι η ασπίδα προστασίας. Στην περίπτωση της φυσικής ασφάλειας παρ' όλα αυτά ο όρος είναι αποδεδειγμένα βασικός. Μερικοί ανταποκριτές μπορεί να ερμηνεύσουν ότι αυτή η ερώτηση απλά ρωτά αν το γραφείο είναι κλειδωμένο όταν είναι κλειστό. Άλλοι μπορεί δικαιολογημένα ως ένα βαθμό να ερμηνεύσουν ότι η ερώτηση ρωτά αν υπάρχουν συγκεκριμένα μέτρα (ειδικοί συναγερμοί ή

κλειδωμένες περιοχές) σχεδιασμένα να προστατέψουν ηλεκτρονικά και διαδικτυακά περιουσιακά στοιχεία.

Η πιο ενδιαφέρουσα άποψη ίσως αυτού του ιδιαίτερου ευρήματος, είναι ότι ένας στους δέκα οργανισμούς δεν χρησιμοποιεί κάποιες επιπλέον φυσικές προφυλάξεις για να προστατέψουν τα ηλεκτρονικά τους περιουσιακά στοιχεία. Με άλλα λόγια, είναι πολύ πιθανό να μην έχουν εξοπλισμό server εντός ειδικά κλειδωμένων δωματίων ή ότι δεν εξοπλίζονται φορητό εξοπλισμό όπως φορητούς υπολογιστές με καλώδια ασφαλείας.

Ενώ ο έλεγχος ασφαλείας σαν κατηγορία είναι εύκολα κατανοητός, υπάρχει ένα βασικό ερώτημα. Θα προσδοκούσαμε πως κάθε οργανισμός που χρειαζόταν οι χρήστες να δώσουν κωδικούς για να έχουν πρόσβαση.

Πόσα περιστατικά; Πόσα εξωτερικά; Πόσα εσωτερικά;

Περιστατικά (%)

Έτη	Από 1-5	Από 6-10	Από 11-30	Από 31- 60	> 60	Άγνωστα
2003	38	20	> 16	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29

Εξωτερικά (%)

2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	42
1999	43	8	5	1	3	39

Εσωτερικά (%)

2003	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35

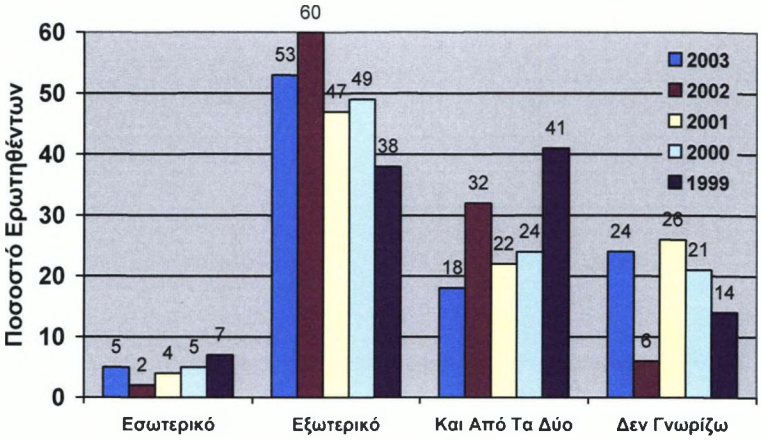
***Συνολικά 101% λόγω στρογγυλοποίησης**

Έτσι επιπλέον είναι ενδιαφέρον ότι το 8% των ανταποκριτών που λένε όχι, δεν χρησιμοποιούν έλεγχο πρόσβασης. Από τους 48 ανταποκριτές που είπαν πως δεν χρησιμοποιούσαν έλεγχο πρόσβασης μόνο 6 είπαν ότι παρήγαγαν εισόδημα με πλεόνασμα 1 δισεκατομμυρίου, με τους δύο από αυτούς να απαντούν ότι χρησιμοποίησαν επαναχρησιμοποιημένους κωδικούς. Αντιθέτως, 23 (δηλαδή περίπου οι μισοί) από τους ανταποκριτές που δεν χρησιμοποιούσαν έλεγχο πρόσβασης φανήκαν σε οργανισμούς με εισόδημα λιγότερο των $100 εκατομμυρίων.

Προφανώς αυτοί που δεν χρησιμοποιούσαν έλεγχο πρόσβασης έχουν πάρει τις αποφάσεις τους όσο αναφορά την ασφάλεια με προφανής διορατικότητα: δεν βρίσκονται ανάμεσα στους ανταποκριτές που αναφέρουν υψηλές οικονομικές απώλειες. Πράγματι, κανένας από τους 48 ανταποκριτές δεν αναφέρει σημαντικές οικονομικές απώλειες από ιδιωτικές πληροφορίες.

Ανάμεσα στα περασμένα χρόνια της παγκόσμιας έκρηξης της τεχνολογίας, τα συστήματα εντοπισμού εισβολέων (IDSs) αναπτύχθηκαν ευρέως (73%) σε αντίθεση με την βιομετρική (11%). Χωρίς να μας εκπλήσσει παρ' όλα αυτά, οι οργανισμοί που ανέπτυξαν την βιομετρική ήταν πιθανόν περισσότερες από τον μέσο οργανισμό στο δείγμα για την ανάπτυξη άλλων πρωτοποριακών τεχνολογιών. Ένα 83% των οργανισμών που χρησιμοποιούν την βιομετρική ανέφεραν πως χρησιμοποίησαν κρυπτογραφημένους λογάριθμους, το 72% χρησιμοποίησαν ψηφιακές ταυτότητες ή πιστοποιητικά, και το 87% ανέφεραν πως χρησιμοποίησαν κρυπτογράφηση αρχείων. Αυτοί οι αριθμοί συγκρίνονται με τις συνολικές μέσες τιμές του 58% που χρησιμοποίησαν κρυπτογραφημένους λογάριθμους, το 49% που χρησιμοποίησε ψηφιακές ταυτότητες ή πιστοποιητικά, και το 69% που χρησιμοποίησε κρυπτογράφηση αρχείων.

WWW Περιστατικά Ιστοσελίδων: Οι επιθέσεις προήλθαν από το εσωτερικό ή από το εξωτερικό;



2003: 181 Ερωτηθέντες/34%
2002: 209 Ερωτηθέντες/42%
2001: 163 Ερωτηθέντες/31%
2000: 153 Ερωτηθέντες/23%
1999: 125 Ερωτηθέντες/24%

Ωστόσο, αυτό που πραγματικά ξαφνιάζει σχετικά με τα νούμερα της οικονομικής απάτης αυτή τη χρονιά, είναι οι αναφερόμενες οικονομικές απώλειες, οι οποίες χοντρικά είναι στο 1/10 από τη περσινή τους κατάσταση. Πιθανώς, δεν είναι λογικό να θεωρήσουμε ως δεδομένο τίποτα απολύτως σχετικά με τη πλατύτερη κατάσταση στο κόσμο των επιχειρήσεων των Ηνωμένων Πολιτειών, αλλά πράγματι μπορεί να είναι η περίπτωση κατά την οποία η ομάδα δείγματος στην έρευνα απόλαυσε τη περασμένη χρονιά μια εμπειρία καλύτερη από το μέσο όρο. Ενώ το 15 τοις εκατό των ερωτηθέντων ανάφερε οικονομική απώλεια - λίγο περισσότερη από τα προηγούμενα χρόνια - υπάρχει επίσης και η περίπτωση που η ακριβότερη απώλεια που αναφέρθηκε ήταν 4 εκατομμύρια δολάρια. Αυτό είναι ένα κλάσμα της υψηλότερης αναφερόμενης απώλειας της περσινής χρονιάς, η οποία ήταν 50 εκατομμύρια δολάρια. Εκείνο το μοναδικό αναφερόμενο παράδειγμα τη

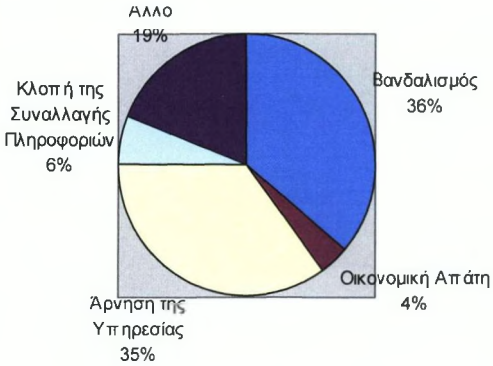
περσινή χρονιά ήταν σχεδόν πέντε φορές υψηλότερο από όλες τις αναφερόμενες απώλειες εξαιτίας της οικονομικής απάτης τη φετινή χρονιά.

Όπως θα περίμενε κανείς, ο μέσος όρος της απώλειας εξαιτίας της οικονομικής απάτης αυτή τη χρονιά, ήταν αντιστοίχως χαμηλότερη από τα προηγούμενα χρόνια. Ο μέσος όρος των 328.594 δολαρίων αυτής της χρονιάς ήταν κυριολεκτικά κατά εκατομμύρια λιγότερος από τα προηγούμενα τρία χρόνια, όπου οι μέσοι όροι ήταν 4.632.000 δολάρια το 2002, 4.420.738 δολάρια το 2001 και 1.646.941 δολάρια το 2002.

Που να βρούμε την πείρα;

Μία από τις επερχόμενες δημόσιες συζητήσεις στη βιομηχανία πληροφόρησης και ασφάλειας αφορά την αποτελεσματικότητα της πρόσληψης χάκερ οι οποίοι ισχυρίζονται ότι έχουν βελτιωθεί. Το 2002 ήταν μια ενδιαφέρουσα χρονιά από αυτή την άποψη διότι αντικρίσαμε την επιστροφή, στο δραστήριο (αλλά νόμιμο) καθήκον, ενός από τους πιο γνωστούς χάκερ της κοινωνίας, του Κέβιν Μίτνικ. Μετά από μία σύλληψη το 1995 και μία καταδίκη για αρκετά κεφάλαια κατηγορίας ηλεκτρονικού εγκλήματος τον επόμενο χρόνο, ο Μίτνικ αφέθηκε ελεύθερος από τη φυλακή το 2000. Πολλοί και διάφοροι περιορισμοί σχετικά με τους όρους της απευλεθέρωσης του τον ανάγκασαν να αποσυρθεί για λίγο, αλλά το 2002 δημοσίευσε ένα βιβλίο σχετικά με τη κοινωνική μηχανική, με τίτλο, «Η τέχνη της απάτης», και έβαλε εμπρός μια εταιρία συμβούλων, την «Αμυντική Σκέψη». Ωστόσο ο συλλογισμός μεταξύ των περισσότερων ερωτηθέντων της έρευνας, δίνει την εντύπωση πως η καλύτερη άμυνα είναι η αποφυγή των χάκερ που έχουν βελτιωθεί.

WWW Περιστατικά Ιστοσελίδων: Ποια τα είδη της παράνομης πρόσβασης ή της κατάχρησης;



2003: 185 Ερωτηθέντες/35%

Ο συλλογισμός ανάμεσα στους επαγγελματίες ασφάλειας δίνει την εντύπωση πως οι χάκερ πιθανόν να βελτιώσουν τους εαυτούς τους, αλλά δεν υπάρχει υποχρεωτική αιτία να βασιστούν σε εκείνο το γεγονός, δεδομένου ότι υπάρχουν πολλοί ειδικευμένοι επαγγελματίες οι οποίοι δεν έχουν προϊστορία ως χάκερ. Ναι, πιθανόν να θολώσει τα νερά το γεγονός ότι μερικοί χάκερ είναι καταδικασμένοι, ενώ πολλοί άλλοι διαπράττουν τα ίδια εγκλήματα ασύλληπτοι και έτσι μπορούν να παρουσιάσουν καθαρά διαπιστευτήρια. Και ναι, μπορεί να είναι πιθανή η πρόσληψη πρώην χάκερ σε ρόλους όπου δεν έχουν το δικαίωμα πρόσβασης σε απόρρητα συστήματα παραγωγής. Όμως οι περισσότεροι ερωτηθέντες δεν φαίνονται διατεθειμένοι να χάσουν τον ύπνο τους με αυτές τις διακρίσεις.

Στην έρευνα υπάρχει το ερώτημα εάν οι ερωτηθέντες θα σκέπτονταν να προσλάβουν έναν βελτιωμένο χάκερ και οι απαντήσεις είναι κατηγορηματικές. Οι ερωτηθέντες έχουν τη συνήθεια να απαντάνε σε αυτή την ερώτηση κατηγορηματικά, με σημεία αναφώνησης και σημειώσεις κακογραμμένες στο περιθώριο για να υποστηρίξουν τη θέση τους (αυτό δεν συμβαίνει κάπου αλλού στο έντυπο της έρευνας).

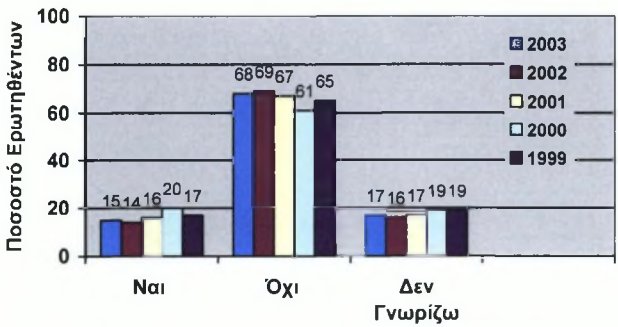
Μόνο το 15% λέει ότι θα προσλάμβανε πρώην χάκερ. Αντίθετα, το 68% αναφέρει πως δεν θα το έκανε, με το 17% να είναι αβέβαιο για τη θέση του στο θέμα.

Ωστόσο θα μπορούσαμε γενικά να δηλώσουμε πως το να έχεις συλληφθεί και να έχεις συνεχίσει με επιτυχία ως ηλεκτρονικός εγκληματίας δεν είναι ένα σίγουρο εισιτήριο στη μετέπειτα επιτυχία στη βιομηχανία ασφάλειας, καθώς τα τρία-τέταρτα της αγοράς δεν θα σε προσελάμβαναν.

Δεν έχουν αναφερθεί ακόμη

Ο σκοπός της ετήσιας έρευνας του CSI/FBI σχετικά με το Ηλεκτρονικό Έγκλημα και την Ασφάλεια, δεν είναι μόνο να συγκεντρώσει δεδομένα σχετικά με τη σκοτεινή πλευρά του διαδικτυακού τόπου, αλλά και να καλλιεργήσει μεγαλύτερη συνεργασία ανάμεσα στην εφαρμογή του νόμου και στον ιδιωτικό τομέα έτσι ώστε να υπάρχει ένα βιώσιμο αποτρεπτικό στο διαδικτυακό έγκλημα.

Θα σκεφτόταν ο Οργανισμός σας την πρόσληψη βελτιωμένων Χάκερ ως Συμβούλους;



2003: 513 Ερωτηθέντες/97%
2002: 442 Ερωτηθέντες/88%
2001: 524 Ερωτηθέντες/98%
2000: 620 Ερωτηθέντες/96%
1999: 506 Ερωτηθέντες/97%

Τα τρία πρώτα χρόνια της έρευνας, μόνο το 17% από αυτούς που είχαν υποστεί σοβαρές επιθέσεις τις ανάφεραν με σκοπό την εφαρμογή του νόμου.

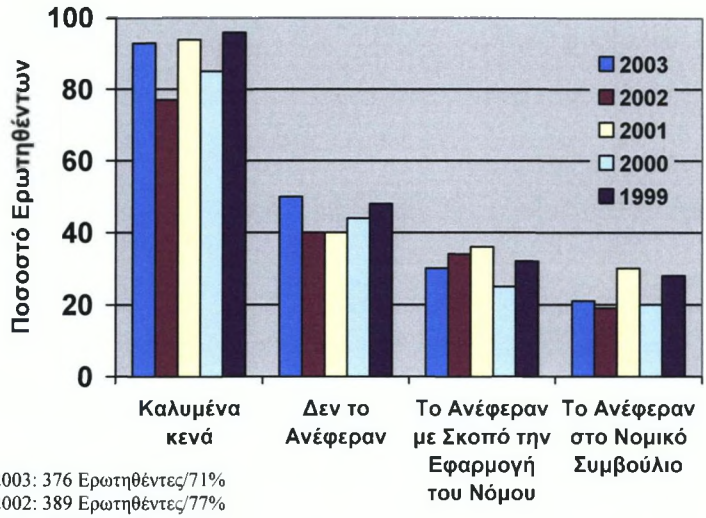
Τα επόμενα χρόνια, εκείνος ο αριθμός διπλασιάστηκε. Τα τωρινά νούμερα της χρονιάς παραμένουν χοντρικά σ' αυτό το διπλασιασμένο επίπεδο, με το 30% να λέει ότι ανάφερε τα περιστατικά του με σκοπό την εφαρμογή του νόμου.

Γιατί δεν είναι αυτός ο αριθμός μεγαλύτερος; Μόνο το 45% του συνόλου των ερωτηθέντων της έρευνας απάντησε για ποιο λόγω δεν ανάφεραν περιστατικά με σκοπό την εφαρμογή του νόμου, αλλά από αυτούς πλήρως το 53% είπε πως δεν αντιλαμβανόταν ότι θα μπορούσαν να αναφέρουν τα περιστατικά. Ενώ αυτό μπορεί να φαίνεται περίεργο, δεδομένου ότι αρκετές περιπτώσεις χάκερ προβάλλονται πολύ από τα μαζικά μέσα ενημέρωσης (προφανώς και οι αρχές εμπλέκονται πολύ σ' αυτά) κάνει περισσότερο αίσθηση πως δεν είναι πάντα ολοφάνερο σε ποιόν να απευθυνθεί κανείς όταν είναι χάκερ, όπως αναφέρουν τα δεδομένα πελατών του διαδικτύου. Θα απευθυνόσασταν στη τοπική αστυνομία; Γενικώς, δεν θα λάβετε βοήθεια εκεί. Θα έπρεπε να απευθυνθείτε στο FBI; Σε μερικές περιπτώσεις μπορούν να σας βοηθήσουν και σε άλλες δεν μπορούν (όμως σίγουρα δεν βλάπτει να τηλεφωνήσετε).

Μια ενδιαφέρουσα ιστορία που έκανε το γύρο στις αρχές του 2002 ξεκαθαρίζει τις δυσκολίες που μερικές φορές παρουσιάζονται όταν έχουμε σχέσεις με το διαδικτυακό έγκλημα. Ο Τζέισον Έρικ Σμίθ πούλησε το φορητό του υπολογιστή μέσω της ιστοσελίδας του eBay, παραδίδοντας το c.o.d. και λαμβάνοντας απόδειξη πως ήταν ένας πλαστός ταμειακός έλεγχος. Τώρα, ομολογουμένως αυτή δεν είναι μία περίπτωση ομαδικού ηλεκτρονικού κλεψίματος υψηλής τεχνολογίας και δεν είναι ούτε καν αμέσως μία περίπτωση κλοπής πάνω από το καλώδιο. Από την άλλη πλευρά, είναι μία

απλή συνδεδεμένη ηλεκτρονικά με κεντρικό υπολογιστή περίπτωση απάτης όπου ένα έγκλημα διαπράχθηκε ολοφάνερα - ο έλεγχος ήταν πλαστός.

Αν ο Οργανισμός σας μέσα στους τελευταίους 12 μήνες είχε την εμπειρία της αυθαίρετης εισόδου στους Υπολογιστές, ποιες από τις παρακάτω πράξεις θα κάνατε?



2003: 376 Ερωτηθέντες/71%
2002: 389 Ερωτηθέντες/77%
2001: 345 Ερωτηθέντες/64%
2000: 407 Ερωτηθέντες/63%
1999: 295 Ερωτηθέντες/57%

Ωστόσο, ακόμη και όταν ο Σμίθ μπήκε στο κόπο να ανακαλύψει το πλαστογράφο μόνος του, δεν μπορούσε να κάνει τις αρχές να διακόψουν εν ώρα εργασίας από μεγαλύτερες περιπτώσεις για να τον διώξουν και να κάνουν τη σύλληψη. Η κλοπή ήταν κάτω από τα αρχικά 5.000 δολάρια του FBI και παρόμοια δεν ήταν μία επαρκώς σημαντική ψεύτικη περίπτωση για να καταδιώξει η Μυστική Υπηρεσία. Τελικά, παρ' όλα αυτά ο Σμίθ τα έβγαλε πέρα δουλεύοντας με ένα τμήμα τοπικής αστυνομίας. Ο Σμίθ σε μία κριτική επαινετικής της καταδίωξης του αναφέρει (στην ιστοσελίδα www.remodern.com/caught.html):

Αφού μίλησα σε δύο ντέτεκτιβ στο Σικάγο, σε ένα κτηματομεσίτη του FBI, σε έναν αντιπρόσωπο στο κτηματομεσιτικό γραφείο της Μυστικής Υπηρεσίας στη Νέα Ορλεάννη, σε έναν αντιπρόσωπο της Μυστικής Υπηρεσίας του Λος Άντζελες, και αφού είχα μία τηλεφωνική σύσκεψη με μία μεγάλη ομάδα αντιπροσώπων από τη Μυστική Υπηρεσία του Σικάγο, τελικά τα κατάφερα.

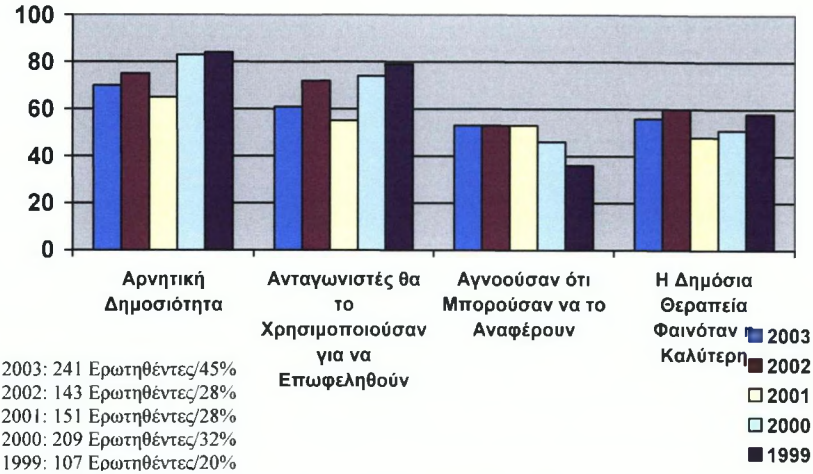
Σχετικά με την έρευνα

Η έρευνα του CSI/FBI σχετικά με το Ηλεκτρονικό Έγκλημα και την Ασφάλεια είναι ιστορικά μία εντελώς ανεπίσημη δουλειά, ανεξαιρέτως και αυτή τη χρονιά. Σκοπός της είναι να επιτείνει τη συναίσθηση ασφάλειας, να προωθήσει τη προστασία πληροφοριών και να παρακινήσει συνεργασία ανάμεσα στην εφαρμογή του νόμου και στον ιδιωτικό τομέα.

Παρά την ανεπισημότητα, υπάρχουν λόγοι να έχουμε ένα σωστό βαθμό εμπιστοσύνης στη στατιστική αυστηρότητα των πορισμάτων της έρευνας. Πρώτον, η ίδια έρευνα απονέμεται για οχτώ συνεχόμενα χρόνια και τα αποτελέσματα τη φετινή χρονιά είναι σίγουρα αρκετά αληθοφανή όταν εγκρίνονται με τους μέσους όρους και τις τάσεις των περασμένων χρόνων.

Ένα δεύτερο σημείο έχει να κάνει με το είδος του δείγματος που ελήφθη σ' αυτή την έρευνα.

Οι λόγοι για τους οποίους οι οργανισμοί δεν ανέφεραν τις αυθαίρετες εισόδους με σκοπό την εφαρμογή του Νόμου



2003: 241 Ερωτηθέντες/45%
2002: 143 Ερωτηθέντες/28%
2001: 151 Ερωτηθέντες/28%
2000: 209 Ερωτηθέντες/32%
1999: 107 Ερωτηθέντες/20%

Είναι σίγουρα αλήθεια ότι οι αποδέκτες της έρευνας δεν είναι τυχαία επιλεγμένοι. Προέρχονται από μία ομάδα επαγγελματιών ασφάλειας, και μεταξύ αυτής της μεγάλης ομάδας, είναι αυτοεπίλεκτοι.

Παρ' όλα αυτά, εάν ρωτήσουμε ποιο μπορεί να είναι το αποτέλεσμα αυτής της αυτοεπιλογής, είναι πιθανό ότι αυτό δεν φθείρει την εγκυρότητα όσων αναφέρθηκαν. Αυτοί είναι άνθρωποι που δίνουν πολύ προσοχή στις θέσεις ασφαλείας και στις εμπειρίες των οργανισμών τους. Με άλλα λόγια, αυτοί είναι επιχειρηματολογικά σε μία καλύτερη θέση από τους περισσότερους, να γνωρίζουν από τι επεισόδια υπέφεραν το περασμένο χρόνο. Δεν είναι πάντα φανερό πότε επιτίθενται σε ένα σύστημα υπολογιστή - και αυτό το αποδεικνύει το γεγονός ότι το 22 τοις εκατό των ερωτηθέντων δεν γνωρίζει εάν οι ιστοσελίδες του κλάπηκαν από χάκερ τη περασμένη χρονιά - έτσι είναι αυτονόητο ότι άνθρωποι που δίνουν αυστηρή προσοχή, ίσως να παρέχουν καλύτερα ενημερωμένες απαντήσεις από αυτούς που δεν δίνουν ιδιαίτερη προσοχή.

Φυσικά, είναι πιθανό ότι αυτή η ομάδα ίσως να έχει λόγο να μεγαλοποιεί τις απώλειες της, σαν τρόπο εξοπλισμού των εαυτών της με τρομερές στατιστικές μελέτες τις οποίες θα αποφέρει στα αφεντικά της όταν η προϋπολογιστική εποχή περάσει. Ενώ αυτό μπορεί να φαινόταν πιθανό για αρκετά χρόνια όταν όλες οι οικονομικές απώλειες μετακινήθηκαν ανένδοτα προς τα πάνω, είναι πιο δύσκολο να υποστηρίξουμε αυτή τη θεωρία όπου παρατηρείται η σημαντική πτώση των αναφερόμενων απωλειών στην έρευνα της φετινής χρονιάς. Ωστόσο, πέρα από εκείνο, η θεωρία «προσωπικού συμφέροντος» (αν μπορεί κανείς να τη πει έτσι) στηρίζεται στην αντίληψη ότι οι ερωτηθέντες είναι για κάποιο λόγο ενήμεροι για την ικανότητα μερικών από την ομάδα να παραποιούν τα νούμερα και ενεργούν σύμφωνα με αυτή την αντίληψη.

Το Κόστος Του Ηλεκτρονικού Εγκλήματος
Ο ακόλουθος πίνακας δείχνει το συνολικό κόστος των ηλεκτρονικών εγκλημάτων και την παραβίαση της ασφάλειας για μία περίοδο άνω των 48 μηνών.

Πώς χάθηκαν τα χρήματα

	Τα χαμηλότερα που αναφέρθηκαν				**Τα υψηλότερα που αναφέρθηκαν**			
	00	01	02	03	00	01	02	03
Κλοπή των ιδιωτικών πληροφοριών	$1K	$100	$1K	$2K	$25M	$50M	$50M	$35M
Σαμποτάζ δεδομένων δικτύων	1K	100	1K	500	15M	3M	10M	2M
Κλέψιμο της τηλεπικοινωνίας	200	1K	5K	1K	5OOK	5OOK	5M	50K
Διείσδυση στο σύστημα από ξένο	1K	100	1K	100	5M	10M	5M	1M
Κατάχρηση της πρόσβασης του Net από γνώστη	240	100	1K	100	15M	10M	10M	6M
Οικονομική απάτη	500	500	1K	1K	21M	40M	40M	4M
Άρνηση υπηρεσίας	1K	100	1K	500	5M	2M	50M	60M
Ιός	100	100	1K	40	10M	20M	9M	6M
Πρόσβαση γνώστη χωρίς έγκριση	1K	1K	2K	100	20M	5M	1.5M	100K
Απάτη της τηλεπικοινωνίας	1K	500	1K	100	3M	8M	100K	250K
Ενεργές υποκλοπές τηλεφωνημάτων	5M	0	0	5K	5M	0	0	700K
Κλοπή φορητού υπολογιστή	500	1K	1K	2400	1.2M	2M	5M	2M

Το 2003, το 75% των ερωτηθέντων της έρευνας μας παραδέχτηκε οικονομικές απώλειες, αλλά μόνο το 47% μπορούσε να προσδιορίσει τις απώλειες.

Πώς χάθηκαν τα χρήματα

	Ο μέσος όρος των απωλειών				Συνολικές ετήσιες απώλειες			
	00	01	02	03	00	01	02	03
Κλοπή των ιδιωτικών πληροφοριών	$3,032,818	$4,447,900	$6,571,000	$2,699,842	$66,708,000	$4,447,900	$6,571,000	$2,699,842
Σαμποτάζ δεδομένων δικτύων	969,577	199,350	541,000	241,521	27,148,000	5,183,1000	15,134,000	5,148,500
Κλέψιμο της τηλεπικοινωνίας	66,080	55,375	1,205,000	15,200	991,200	886,000	346,0000	76,000
Διείσδυση στο σύστημα από ξένο	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Κατάχρηση της πρόσβασης του Net απο γνώστη	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Οικονομική απάτη	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Άρνηση υπηρεσίας	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Ιός	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Πρόσβαση γνώστη χωρίς έγκριση	1,124,725	275,636	300,00	31,254	22,554,500	6,064,000	4,503,000	406,300
Απάτη της τηλεπικοινωνίας	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,00	701,500
Ενεργές υποκλοπές τηλεφωνημάτων	5M	0	0	352,500	5,000,000	0	0	705,000
Κλοπή φορητού υπολογιστή	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
					265,337,990	**377,828,700**	**455,848,000**	
	Συνολικές Ετήσιες Απώλειες				**201,797,340**			

Αν εκείνη ήταν η περίπτωση, θα περίμενε κανείς να βρει τους ερωτηθέντες να αναφέρουν απώλειες στις περισσότερες κατηγορίες (μετά από όλα αυτά γιατί να μην ανεβάσουμε όλες τις απώλειες;). Όμως, δεν είναι για το πόσο ξεχωριστές φαίνονται οι απαντήσεις - οι περισσότεροι ερωτηθέντες αναφέρουν μόνο τρεις ή τέσσερις κατηγορίες απώλειας. Επιπλέον, σημαντικό είναι ότι περισσότεροι ερωτηθέντες ισχυρίζονται διάφορα είδη επιθέσεων από το να αναφέρουν απώλειες για εκείνες τις επιθέσεις. Ίσως να περίμενε κανείς κάθε επίθεση να έχει μία τιμή εάν το συνολικό συμφέρον έσπρωχνε τα νούμερα.

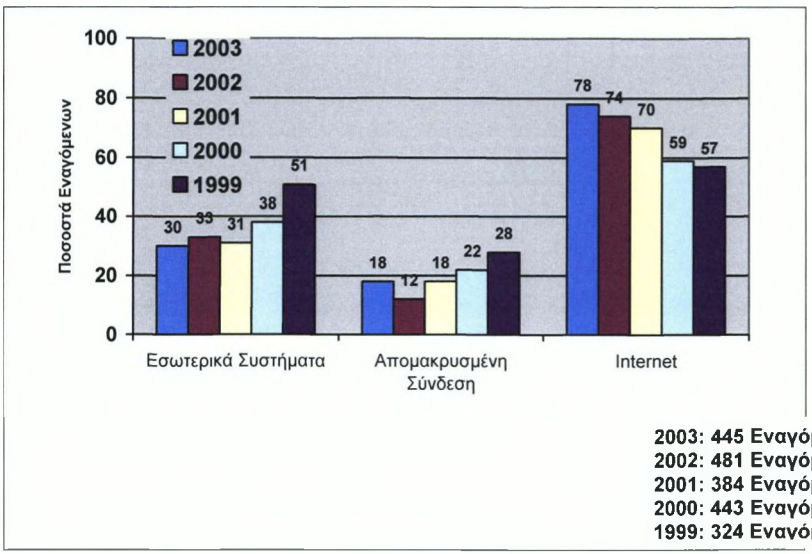
Θεωρώντας ως δεδομένο το γεγονός ότι οι ερωτηθέντες είναι ειλικρινείς και τα νούμερα νόμιμα, υπάρχει ακόμη το βασικό πρόβλημα των ερευνών - δεν είναι ποτέ τόσο απρόσβλητες όσο θα ήθελες να είναι. Αυτή η έρευνα, όπως οι περισσότερες, είναι στη καλύτερη περίπτωση μία σειρά από

στιγμιότυπα που απεικονίζουν πως άνθρωποι στα χαρακώματα αντίκρισαν τη κατάσταση τους σε μία δεδομένη στιγμή.

Το CSI παρέχει τα αποτελέσματα της έρευνας σαν μία δημόσια υπηρεσία. Η αναφορά είναι ελεύθερη στην ιστοσελίδα του CSI (www.gocsi.com) όπου μία αντιγραμμένη έκδοση επίσης μπορεί να ζητηθεί σαν τεκμήριο επί τη εμφανίσει. (αυτή παρέχεται προς πώληση).

Η συμμετοχή του γραφείου του FBI του Σαν Φραντζίσκο είναι ανεκτίμητη. Παρείχαν δεδομένα στην ανάπτυξη της έρευνας και έδρασαν σαν συνέταιροι μας στη προσπάθεια να ενθαρρύνουμε ανταπόκριση. Όμως δεν έχουμε συμβατική ή οικονομική σχέση με το FBI. Απλά είναι μία μεγάλη και εκπαιδευτική προσπάθεια από τη μεριά και των δύο οργανισμών. Το CSI χρηματοδοτεί το πρόγραμμα και είναι αποκλειστικά υπεύθυνο για τα αποτελέσματα.

Η σύνδεση στο Internet αναφέρεται όλο και πιο πολύ ως ένα συχνό σημείο επίθεσης



2003: 445 Εναγόμενοι/84%
2002: 481 Εναγόμενοι/96%
2001: 384 Εναγόμενοι/72%
2000: 443 Εναγόμενοι/68%
1999: 324 Εναγόμενοι/62%

Αυτή η τελευταία στατιστική- όπου το 69% των εναγόμενων που χρησιμοποιούν κρυπτογράφηση φακέλων- μπορούν να δείξουν μία ήπια αυξανόμενη τάση. Αυτό είναι πάνω από το 58% του προηγούμενου χρόνου, το οποίο θα ήταν μία στατιστικά σημαντική άνοδος. Ο μέσος όρος των 5 χρόνων γι' αυτή την ερώτηση είναι 59%, το οποίο δίνει βάση στην αντίληψη ότι η χρήση κρυπτογραφημένων φακέλων αυξάνεται.

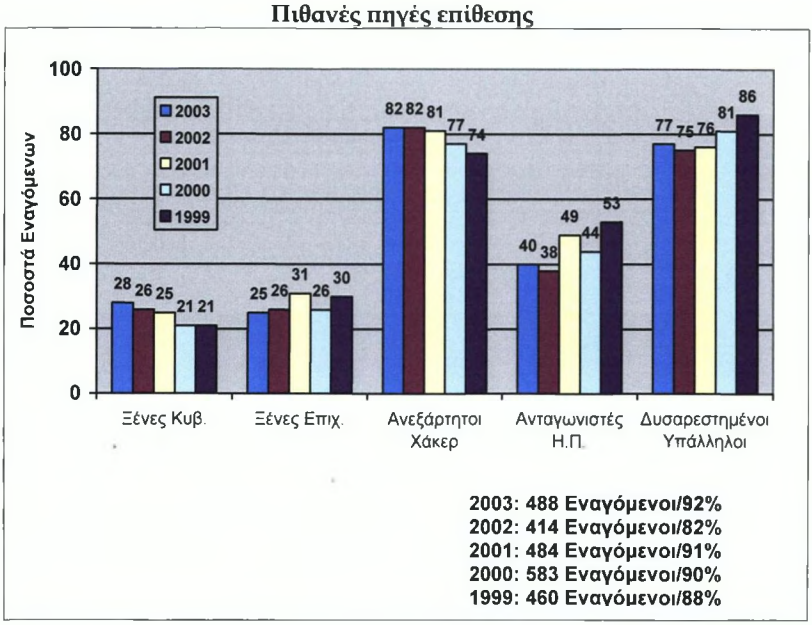
Ανεξάρτητα από τα εργαλεία που χρησιμοποιούνται, υπάρχει ακόμα η υπόθεση ότι πολλοί εναγόμενοι απλώς δεν ξέρουν τι συμβαίνει μέσα στα δίκτυά τους. 15% των εναγόμενων λένε ότι δεν γνωρίζουν αν υπήρχε κάποια μη εξουσιοδοτημένη χρήση των υπολογιστικών συστημάτων τον τελευταίο χρόνο. Αυτό είναι ενοχλητικό, θα μπορούσε να υποστηρίξει κανείς. Την ίδια στιγμή, παρόλα αυτά, είναι περίπου το ίδιο ποσοστό όπως πάντα ˙ ο μέσος όρος για τα προηγούμενα 7 χρόνια της έρευνας ήταν ότι το 16,3% δεν γνώριζαν.

ΠΡΟΣΩΠΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Μέσα από την ιστορία της έρευνας, η κλοπή των πληροφοριών ιδιοκτησίας έχει γίνει μία από ακριβοπληρωμένες μορφές ηλεκτρονικού εγκλήματος. Πράγματι, από το 1999 έχει ξεπεράσει σταθερά τις καταγραφές των αναφερόμενων οικονομικών απωλειών. Αυτό δε θα έπρεπε να προκαλεί έκπληξη σε μία οικονομία όπου ένα μεγάλο μέρος της συνολικής παραγωγικότητας περιστρέφεται γύρω από την πληροφορία και την υψηλή τεχνογνωσία.

Μέσα στον κόσμο του διαδικτύου, θέματα που αφορούν την πνευματική ιδιοκτησία ήταν στο επίκεντρο το 2002. Τα αντικείμενα νέων υψηλού προφίλ δεν ήταν απαραίτητα για την κλοπή εμπορικών μυστικών, η οποία είναι και η μεγαλύτερη απειλή για τις περισσότερες επιχειρήσεις, αλλά ακόμα η συγκέντρωση στην παράβαση πνευματικών δικαιωμάτων δημιούργησε ένα κλίμα στο οποίο το ενδιαφέρον για τον έλεγχο που

βασίζεται σε κρυπτογράφηση όπως ο νέος διακομιστής Διαχείρισης Ψηφιακών Δικαιωμάτων της Microsoft έχει αυξηθεί σταθερά.



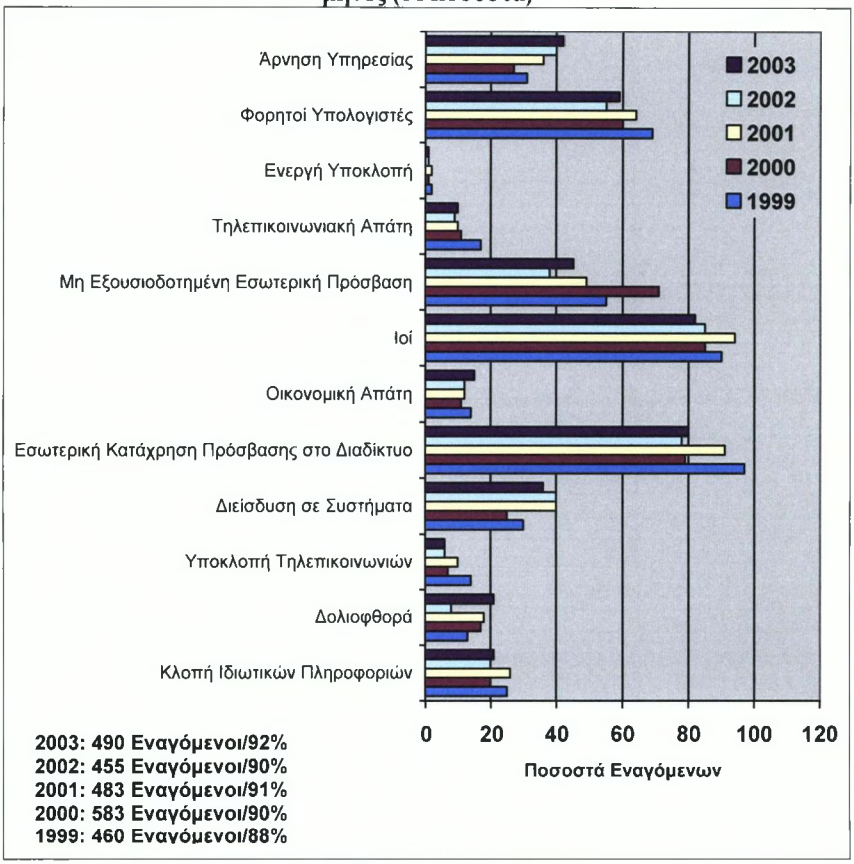
Το ενδιαφέρον του Ανώτατου Δικαστηρίου για την επέκταση των όρων πνευματικών δικαιωμάτων των Ηνωμένων Πολιτειών που πάρθηκαν από το Κογκρέσο το 1998 ήταν ένα από τα σημαντικότερα θέματα πνευματικής ιδιοκτησίας του προηγούμενου χρόνου. Αυτό που οι κριτικοί όρισαν ως νομοσχέδιο Ντίσνεϋ επειδή επεκτάθηκε (ανάμεσα σε πολλά άλλα πράγματα) στον έλεγχο της εταιρείας πάνω στο χαρακτήρα της Μίκυ Μάους, ήταν η 11η προσθήκη όρων πνευματικών δικαιωμάτων σε 40 χρόνια. Η απόφαση του Ανώτατου Δικαστηρίου δεν παραδόθηκε μέχρι τον Ιανουάριο του 2003, αλλά το γραπτό ήταν ήδη στον τοίχο το δεύτερο μισό του 2002 · το Κογκρέσο μπορούσε να κάνει ότι ήθελε με τους όρους πνευματικής ιδιοκτησίας.

Το ότι το Κογκρέσο θα ήθελε να κάνει τους όρους μακρύτερους είναι μία ξεκάθαρη έκφραση σε μία γενική αλλαγή στις επιχειρησιακές και κυβερνητικές

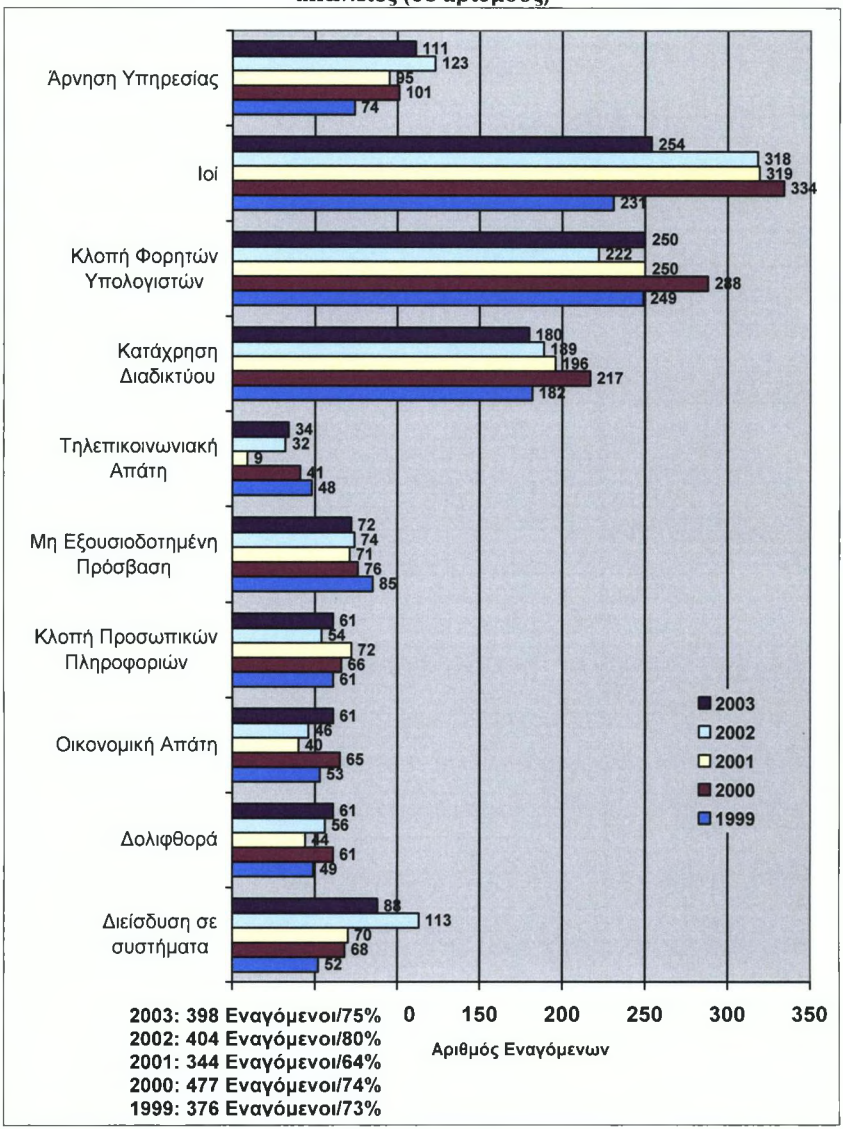
ευαισθησίες προς πιο ξεκάθαρη και αδιαμφισβήτητη κυριότητα πνευματικής ιδιοκτησίας. Μέσα σε αυτό το πλαίσιο το RIAA συγκεκριμένα ήταν ιδιαίτερα δραστήριο τον προηγούμενο χρόνο. Τον Απρίλιο ο οργανισμός κέρδισε 1 εκατομμύριο δολάρια με διακανονισμό εκτός δικαστηρίων σε μια αγωγή ενάντια στα Συστήματα Οργανωμένης Πληροφόρησης (IIS), η οποία είχε τρέξει έναν εσωτερικό διακομιστή όπου οι εργαζόμενοι αντάλλασαν φακέλους MP3 για τους οποίους η RIAA ισχυρίστηκε ότι ήταν παράνομα χιλιάδες πνευματικά δικαιώματα. Άλλος ένας διακανονισμός με την Audiogalaxy.com ανάγκασε αυτό που ήταν μία υπηρεσία ανταλλαγής μουσικής τύπου Napster να τεθεί σε ένα σεβασμό σε νέα βάση, τέτοια ώστε η υπηρεσία τώρα να είναι με βάση τη συνδρομή και να χρεώνει τους χρήστες ανά κομμάτι για το δικαίωμα να αντιγράψουν τραγούδια στα δικά τους CD. Τον Σεπτέμβριο η ομάδα πήρε μία κλήτευση να αποκτήσει πληροφορίες συνδρομητών από το Verizon προκειμένου να ανιχνεύσει την ταυτότητα ενός υποτιθέμενου παραβάτη πνευματικών δικαιωμάτων - μία κίνηση χωρίς προηγούμενο ενάντια στο άτομο αντί για μία επιχείρηση. Και παρόλο που δεν έλεγαν πολλά γι' αυτό η RIAA δούλεψε αρκετά επιμελώς στο προσκήνιο τον τελευταίο χρόνο για να "δηλητηριάσει το πηγάδι" για του εμπόρους μουσικής, δημιουργώντας και διανέμοντας ψεύτικους φακέλους που φαίνεται ότι είναι πραγματικοί φάκελοι τραγουδιών αλλά οι οποίοι στην πραγματικότητα περιέχουν θόρυβο ή, σε μία περίπτωση το 2003, τη Madonna να καταριέται του οπαδούς της.

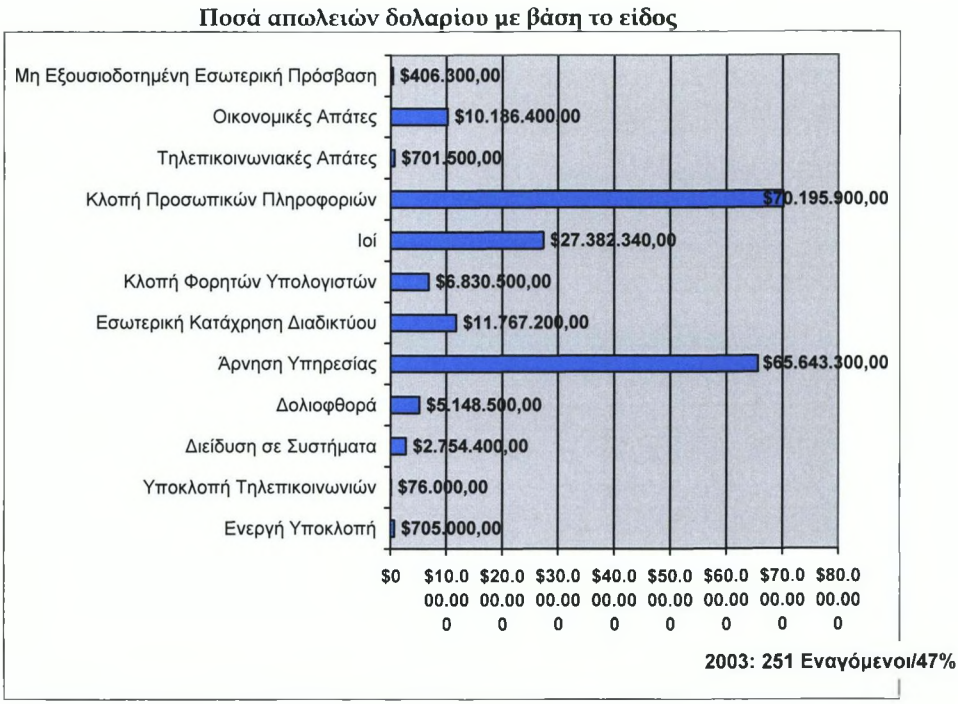
Αυτό δε σημαίνει ότι δεν υπήρχε αρκετή «συμβατική» κλοπή επιχειρησιακών πληροφοριών. Σκεφτείτε την περίπτωση του Richard Glenn Dopps, ο οποίος κρίθηκε ένοχος για ένα κακούργημα για «απόκτηση πληροφοριών από έναν προστατευμένο υπολογιστή». Αυτή είναι η περίληψη από την ιστοσελίδα του τμήματος δικαιοσύνης σε περιπτώσεις ηλεκτρονικού εγκλήματος.

Είδη επιθέσεων ή καταχρήσεων που εντοπίστηκαν τους τελευταίους 12 μήνες (σε ποσοστά)



Είδη επίθεσης ή κατάχρησης σε Οργανισμούς που ανέφεραν οικονομικές απώλειες (σε αριθμούς)





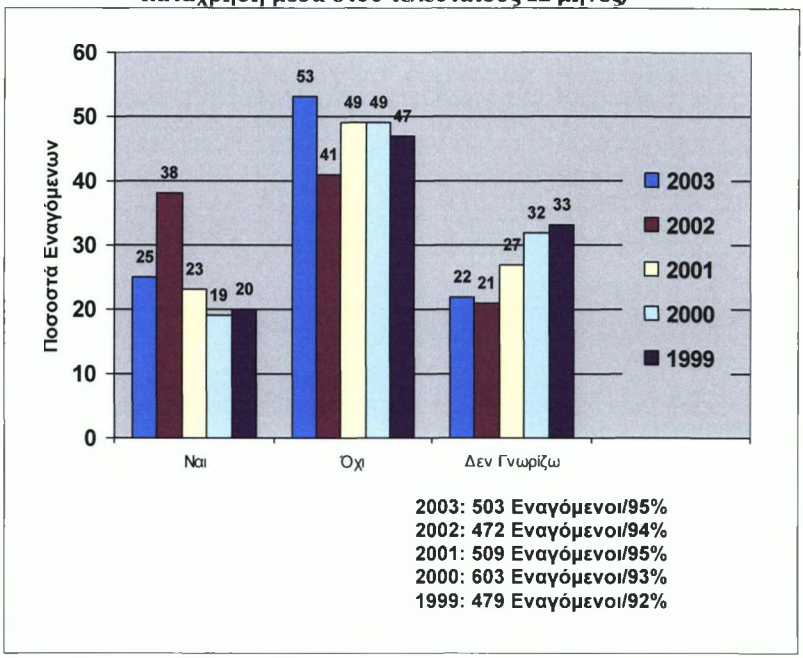
Από τον Φεβρουάριο του 2001, ο Dopps προσελήφθηκε από τις επιχειρήσεις Bergman (TBC), μία εργολαβική φίρμα βασισμένη στην Chino. Αφού έφυγε από την TBC για να δουλέψει σε έναν ανταγωνιστή, ο Dopps χρησιμοποίησε τη σύνδεσή του στο Internet για να αποκτήσει πρόσβαση στα υπολογιστικά συστήματα της TBC σε περισσότερες από 20 περιπτώσεις.

Όταν ο Dopps έμπαινε στα συστήματα της TBC, διάβαζε μηνύματα e-mail των στελεχών της TBC για να μείνει ενημερωμένος για τις τρέχουσες δουλειές της TBC και για να αποκτήσει διαφημιστικό πλεονέκτημα για το νέο του εργοδότη.

Η παράνομη είσοδος του Dopps στα ηλεκτρονικά συστήματα της TBC προκάλεσε περίπου 21.636 δολάρια σε ζημιές και κόστη στο TBC.

Υπάρχουν πολλά περισσότερα εκεί απ' όπου ήρθε αυτό. Πράγματι, ψάχνοντας μέσα ψάχνοντας μέσα στη λίστα υποθέσεων της DOJ (στο www.usdoj.gov/criminal/cybercrime/cccases.html) είναι λίγο διδακτική, ιδιαίτερα αν κάποιος έχει κάποια ρομαντική αντίληψη για τους τυπικούς καταδικασμένους κυβερνο-εγκληματίες που είναι εγκέφαλοι χάκερ.

Έχει η Ιστοσελίδα σας υποστεί μη εξουσιοδοτημένη είσοδο ή κατάχρηση μέσα στου τελευταίους 12 μήνες;



Σημαντικό από άποψη λύσεων για την κλοπή προσωπικών δεδομένων, ίσως, είναι ότι η αντίληψη των έμπιστων υπολογιστικών συστημάτων επανήλθε το 2002. Ένας τρόπος σκέψης σχετικά με αυτή τη γενική τάση είναι ότι αυτή επικεντρώνεται στην αύξηση ασφάλειας στον υπολογιστή του τελικού χρήστη (αν και, φυσικά, τα ίδια εργαλεία αναμφίβολα θα

υιοθετηθούν στον εξοπλισμό του server). Στον υπολογιστή γραφείου, δεν υπάρχει προς το παρόν κανένας αποτελεσματικός τρόπος να πεις από απόσταση (από την άποψη του server εφαρμογής, για παράδειγμα) αν κάποιος ή κάποια πονηρή διεργασία έχει βάλει χέρι στο λογισμικό ή στα δεδομένα που τρέχουν στον υπολογιστή γραφείου.

Το 2002, παρόλα αυτά, δημιουργοί τσιπ και η Microsoft άρχισαν να αντιμετωπίζουν το πρόβλημα και στο λειτουργικό και στα επίπεδα διαχείρισης συστήματος. Η βασική ιδέα είναι να καθιερώσει ένα ανθεκτικό στους εισβολείς τσιπ ασφαλείας στα υπολογιστικά συστήματα, παρέχοντας μία τοποθεσία για να αποθηκεύονται πληροφορίες σχετικά με το πώς υποτίθεται ότι πρέπει να μοιάζει το λογισμικό στο σύστημα. Οι τυπικές διαδικασίες χαμηλού επιπέδου στο σύστημα διαχείρισης μετά χρησιμοποιούν αυτές τις πληροφορίες για να επαληθεύσουν την αξιοπιστία του συστήματος πριν του επιτραπεί να τρέξει λογισμικό.

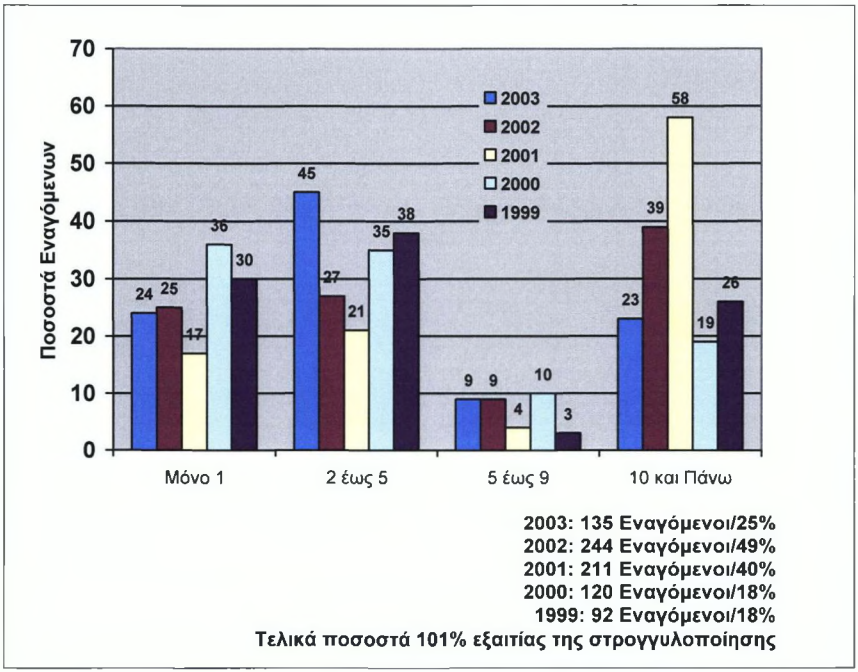
Αυτή η ιδέα έμπιστων συστημάτων δεν είναι καινούρια- υπήρχε σημαντικό ενδιαφέρον στην ιδέα στη δεκαετία του 80- αλλά είναι καινούρια στους υπολογιστές γραφείου. Μέχρι τώρα, η πρώτη παραγωγή του τσιπ ασφαλείας τα πάει καλά. Ήδη το 2002 η IBM είχε έναν εμπορικά διαθέσιμο υπολογιστή τύπου notebook που περιείχε ένα έμπιστο λειτουργικό τσιπ. Στις αρχές του 2003, η Microsoft άρχισε να δείχνει πρωτότυπες παραλλαγές του συστήματος διαχείρισης Windows που θα υποστήριζε έμφυτα αυτό το λειτουργικό.

Παρόλο που η Microsoft και η Intel έχουν και οι δύο προσπαθήσει να συγκεντρωθούν σε αυτές τις προσπάθειες στην πορεία προστατεύουν το λογισμικό από το να παραβιαστεί, πολλοί παρατηρητές έχουν επισημάνει ότι οι ίδιοι μηχανισμοί είναι ακριβώς ότι χρειάζεται για συστήματα που διευθύνουν την πρόσβαση και την χρήση των δεδομένων- Συστήματα Διαχείρισης Ψηφιακών Δικαιωμάτων. Πράγματι, οι κριτικοί αυτών των πρωτοβουλιών έμπιστης υπολογιστικής υποστηρίζουν ότι αυτό που

πραγματικά κάνουν είναι να προστατεύουν παροχείς περιεχομένου από πιθανούς παραβάτες πνευματικών δικαιωμάτων (και επιχειρήσεις από παρατηρητές οι οποίοι κατά πάσα πιθανότητα δε θα είναι πλέον σε θέση να στέλνουν αντίγραφα ενοχοποιητικών εγγράφων στον τύπο ή σε κυβερνητικές υπηρεσίες, αντί να εξασφαλίζουν τους χρήστες από εξωτερικές επιθέσεις.

Οι επιπτώσεις όλων αυτών στην ασφάλεια υπολογιστών στον πραγματικό κόσμο, αδιαμφισβήτητα θα πάρει κάποιο χρόνο να αξιολογηθεί, ίσως 5 με 10 χρόνια.

Περιπτώσεις που αφορούν Ιστοσελίδες: Αν ναι, πόσες περιπτώσεις;



2003: 135 Εναγόμενοι/25%
2002: 244 Εναγόμενοι/49%
2001: 211 Εναγόμενοι/40%
2000: 120 Εναγόμενοι/18%
1999: 92 Εναγόμενοι/18%
Τελικά ποσοστά 101% εξαιτίας της στρογγυλοποίησης

ΟΙΚΟΝΟΜΙΚΗ ΑΠΑΤΗ

Αυτή η έρευνα πρώτα μελέτησε τις απώλειες εξαιτίας οικονομικής απάτης το 1997, οπότε το 12% των εναγόμενων βεβαίωσαν εντοπισμό οικονομικής απάτης. Φέτος το 15% που ανέφεραν οικονομική απάτη είναι το υψηλότερο ποσοστό που έχει υπάρξει στην ιστορία της έρευνας, αλλά είναι μόνο 1% πάνω από το προηγούμενο ρεκόρ, που καταγράφηκε το 1999. Έτσι ενώ είναι πιθανό ότι η αύξηση σηματοδοτεί την απαρχή μιας αυξανόμενης τάσης, φαίνεται κάπως πιο πιθανό ότι ο ρυθμός απωλειών από οικονομική απάτη έχει μείνει πάνω κάτω σταθερός, κυμαινόμενος γύρω στο 13% με 14%.

9.2. - Έρευνα 2η – Έρευνες που διεξήχθησαν στις Ηνωμένες Πολιτείες της Αμερικής για την εγκληματικότητα μέσω υπολογιστή: Η επιρροή της γνώσης από το παρελθόν διευθύνει το μέλλον

9.2.1. Εισαγωγή

Οι εγκληματικές έρευνες είναι το θέμα συζήτησης για ακαδημαϊκούς και ελεύθερους επαγγελματίες ομοίως, και ορίζεται σαν «τη διαδικασία της συγκέντρωσης νόμιμων αποδείξεων του εγκλήματος το οποίο είχε συμβεί ή επρόκειτο να διαπραχθεί»[178]. Γυρεύει να αναγνωρίσει τις αλήθειες που συνδέονται με το πώς και γιατί λαμβάνει χώρα ένα έγκλημα, και λειτουργεί για το σκοπό της οικοδόμησης μιας υπόθεσης η οποία ενδέχεται να έχει επιρροή στην επιτυχή δίωξη παραβατών. Αρκετές μελέτες προσπάθησαν να προσδιορίσουν τον καλύτερο τρόπο με τον οποίο η ερευνητική διαδικασία μπορεί να διεξαχθεί και να διαχειριστεί. Ο σκοπός αυτός ο οποίος καλύπτει ευρύ μέρος ερευνών δίνει τη δυνατότητα στα αστυνομικά τμήματα να παραθέσουν τις συνήθειές τους ενάντια στα πορίσματα, και ύστερα να θέσουν σε εφαρμογή κατηγορηματικές αλλαγές οι οποίες επρόκειτο να βελτιώσουν τις καθημερινές λειτουργίες της οργάνωσής τους. Η άσκηση της έρευνας έχει τροποποιηθεί και εξευγενιστεί με την πάροδο των χρόνων, λαμβάνοντας υπόψη τις αλλαγές στην κοινωνική, την πολιτική και την επιστημονική επικράτεια. Αυτές οι ασκήσεις έχουν χαρακτηριστεί «επιστήμες» μια ιδιότητα που βασικά θεωρείται «τέχνη»[179], και επομένως επαυξάνει την ερευνητική διαδικασία.

Σε αυτό το νόμο καταχώρησης, ο Gabriel Tarde (1890 - 1903) υποστηρίζει ότι οι νέες μορφές εγκληματικής συμπεριφοράς καλλιεργούνται μέσω της αύξησης των νέων πρακτικών πάνω σε παραδοσιακές πρακτικές, συχνά μέσω των τεχνολογικών προόδων και της καινοτομίας. Χάρη στην ερμηνευτική ανάπτυξη της πληροφοριακής τεχνολογίας στην υψηλή

[178] Βλ., Brown. 2001:3
[179] Βλ., Beveridge. 1957

κοινωνία, πολλά παραδοσιακά εγκλήματα συνεργούν στη χρήση των ηλεκτρονικών υπολογιστών και του Διαδικτύου, και η εγκληματικότητα μέχρι τώρα είναι επιφανειακή εξαιτίας των απίστευτων ικανοτήτων των πληροφοριακών συστημάτων. Η εγκληματικότητα μέσω ηλεκτρονικού υπολογιστή[180] θα χρειαστεί γενικώς νομική εφαρμογή τμημάτων, και συγκεκριμένα εγκληματικούς ερευνητές να δημιουργήσουν μια αυξανόμενη ποσότητα της προσπάθειάς τους ενάντια στην επιτυχή αναγνώριση, τη σύλληψη και τη βοήθεια στην αποτελεσματική δίωξη δραστών.

Για να αναπτύξουμε μια στρατηγική ήχου, είναι κρίσιμο να γνωρίζουμε από προηγούμενες έρευνες, και να ενσωματώσουμε τις νομικές οργανώσεις με τις τακτικές οι οποίες θεωρούνται πιο καρποφόρες. Στο κείμενο που ακολουθεί, μια περίληψη από τις δύο πιο σημαντικές μελέτες όσον αφορά τις παραδοσιακές έρευνες στην Αμερική παρουσιάζεται με σκοπό να εξασφαλίσει μια ιστορική και συγκριτική στάση. Επιπροσθέτως, προέκυψαν ομοιότητες και οι διαφορές σχετικά με τις έρευνες που διεξήχθησαν μεταξύ εγκληματικότητας μέσω ηλεκτρονικού υπολογιστή και παραδοσιακής εγκληματικότητας, και η σημασία τους συζητήθηκε από την άποψη ότι: ο ρόλος του πρώτου ανταποκριτή αστυφύλακα και οι πληροφορίες του ερευνητή, η οργάνωση και οι συνεντεύξεις η συλλογή αποδείξεων και η επεξεργασία τους· τα θέματα δικαιοδοσίας οι αντιδραστικές και υπερδραστήριες στρατηγικές και τέλος η χρησιμότητα συμβολικών ερευνών.

[180] Τα πιο σημαντικά σημεία αυτού του άρθρου είναι οι έρευνες για: 1) παραδοσιακά εγκλήματα στα οποία ένας ηλεκτρονικός υπολογιστής χρησιμοποιείται ως βοηθητικό στοιχείο, και 2) υψηλής τεχνολογίας ή μη παραδοσιακά εγκλήματα στα οποία ένας ηλεκτρονικός υπολογιστής είναι πρωταρχικός στόχος, συμβάλλει, κάτι που αποδεικνύει πως σχετίζεται με ένα έγκλημα.

9.2.2. Η μελέτη της εταιρείας RAND για την εγκληματική έρευνα

Τη δεκαετία του 1970, η εταιρεία RAND των Ηνωμένων Πολιτειών (Η.Π.Α) διεξήγαγε μια πανεθνική μελέτη εγκληματικών ερευνών από τη νομική εφαρμογή των τμημάτων με πάνω από 150 άσπονδους υπαλλήλους και κοινοποιώντας έναν πληθυσμό πάνω από 100.000. Με τη βοήθεια της ανάλυσης διαφόρων οργανισμών με διαφορετικές ερευνητικές φιλοσοφίες, συγκριτικά με τις εγκληματικές στατιστικές για τον καθορισμό της ερευνητικής δραστικότητας, και μια ανασκόπηση λεπτομερών υποθέσεων που πρόκειται να μελετηθούν, βγήκε στην επιφάνεια ένας τρόπος με τον οποίο οι οργανισμοί διαχειρίζονταν και οργάνωναν τις έρευνες τους. Τέσσερα σημαντικά συμπεράσματα εκτίθενται:

Απόδοση λύσης: Ο πιο καθοριστικός τρόπος απόδοσης λύσης είναι οι πληροφορίες υπό τον όρο ανταπόκρισης του θύματος[181]. Επίσης ανακαλύφθηκε πως η εκμετάλλευση των ερευνών δεν χρησίμευε. Συγκεκριμένα, εάν το θύμα δεν ήταν ικανό να εξασφαλίσει αναγνωρισμένες πληροφορίες από το δράστη, είναι πιθανό η σύλληψη να μην είχε αποτέλεσμα. Η σπουδαιότητα του υπευθύνου αστυφύλακα αποκορύφωσε την ανάγκη για οργανωμένη περίπολο με ευρύτερο ανακριτικό ρόλο, που είναι εξαιρετικά ικανή εξιχνιάζοντας πολλές υποθέσεις παρά παραπέμποντας αυτές σε κάποιο άλλο πρόσωπο[182]. Σαν συνέπεια, πρόκειται να παρέχει ειδικευόμενες ερευνητικές δυνάμεις οι οποίες θα απευθύνονται μόνο σε εκείνα τα συμβάντα που θα χρειάζονται ειδικές ικανότητες, και θα διατηρούν τα θύματά τους σε καλή ψυχολογική κατάσταση.

Ερευνητική αποτελεσματικότητα: Διαφορές στην ερευνητική οργάνωση, εκπαίδευση, επάνδρωση, φόρτο εργασίας, και διαδικασίες δεν θα

[181] Βλ., Greenwood, Chaiken, & Petersilia, 1977
[182] Βλ., Block & Weidman, 1975, Greenberg, Elliot, Kraft, & Proctor, 1977

επηρεάσουν αναλογικά τους ρυθμούς εγκληματικότητας, σύλληψης, ή εκτελωνισμού.

Η διαδικασία της φυσικής μαρτυρίας: Ενώ η εκτέλεση νομικών τμημάτων συμφωνεί με τη μαρτυρία, πολλά από αυτά δεν επεξεργάστηκαν με αποτελεσματικό τρόπο. Επιπλέον, η προτεινόμενη πολιτική περιέπλεξε τη διάθεση περισσότερων διεξόδων για τα πρακτικά της περισυλλεγμένης μαρτυρίας, η οποία με αυτόν τον τρόπο πρόκειται να έχει θετική επιρροή για την επίλυση των εγκλημάτων.

Ερευνητική διεξοδικότητα: Οι ερευνητές γενικότερα παρέλειπαν να ολοκληρώνουν σημαντικά έγγραφα φανερών γεγονότων τα οποία θα ενίσχυαν την ικανότητα των μηνυτών να εξασφαλίζουν τις πιο κατάλληλες πεποιθήσεις. Επιχειρηματολογώντας, το να είναι ημιτελή μια τεκμηρίωση ίσως να συμβάλλει σε μια αύξηση και σε μια εξασθένιση μιας δήθεν συμφωνίας των μηνυτών[183]. Αυτή η ανεπάρκεια σε περιεκτική καταγραφή απαιτεί άμεση προσοχή.

9.2.3. Η μελέτη της PERF όσον αφορά τη διάρρηξη και τη ληστεία

Σε μια άλλη σημαντική έρευνα με ηγέτη τον John Eck υπό την αιγίδα της μελέτης των αστυνομικών στελεχών στον τόπο συζήτησης δημοσίων θεμάτων (PERF), περισσότερες από 3.360 διαρρήξεις και 320 ληστείες σε διάστημα δύο χρόνων αναλύθηκαν από τη δικαιοσύνη: DeKalb County, Georgia, St. Petersburg, Florida, και Wichita, Kansas. Η έρευνα της PERF διαφέρει από την πρόωρη έρευνα της RAND, η οποία επικεντρώθηκε σε ολόκληρη την ερευνητική διαδικασία, όχι μόνο στα περιστατικά σύλληψης. Ο Eck ήταν ικανός να προσδιορίσει τον αντίκτυπο του ασταθούς πλήθους το οποίο επηρεάζει το αποτέλεσμα σε δυσανάλογες βαθμίδες.

[183] Βλ., όπ. υπ.125

Πρωταρχικό αποτέλεσμα ήταν πως τόσο οι μυστικοί αστυνόμοι όσο και οι αστυφύλακες συνέβαλλαν εξίσου στην επίλυση των υποθέσεων. Θα ήταν άσχημο λοιπόν να τονίσουμε τον έναν περισσότερο από τον άλλο[184]. Η έρευνα έδειξε επίσης ότι τα άτομα και στις δυο περιπτώσεις δεν χρειάζεται να εξαρτώνται από τις πληροφορίες που παρέχονται από το θύμα και πως πρέπει να είναι πιο υπερδραστήρια στην εξερεύνηση πληροφοριών εφόσον έχουν κάποια σχέση με το συμβάν. Η εξάσκηση στην έρευνα της γειτονιάς και η χρήση των πληροφοριών θεωρούνται σημαντικές τεχνικές για την αύξηση της αποτελεσματικότητας των ερευνών. Φαίνεται ότι ενώ οι περισσότερες πληροφορίες παρήχθησαν από τα θύματα των εγκλημάτων κατά τη διάρκεια της ανάκρισης της αστυνομίας, πολλές από αυτές δεν ήταν καρποφόρες. Ωστόσο, ενώ είχαν ληφθεί υπόψη άλλες πηγές, ανακαλύφθηκαν περισσότερες πληροφορίες.

Ο Eck υπογραμμίζει την ανάγκη της ευαισθησίας των θυμάτων και ισχυρίζεται πως δεν είναι χρήσιμη η επανάληψη συνεντεύξεων των θυμάτων κατά τη διάρκεια εκμετάλλευσης των ερευνών. Οι φυσικές αποδείξεις βρέθηκαν να είναι πιο χρήσιμες για την επιβεβαίωση της προϋπαρξης ταύτισης παρά οι τρόποι αναγνώρισης γεγονότων που προηγουμένως ήταν άγνωστα[185]. Η συνεργασία, η περισυλλογή και η διαχείριση πληροφοριών μεταξύ αστυνομικών τμημάτων είναι σημαντικοί παράγοντες για τις επιτυχημένες έρευνες [186].

Μια από τις πιο χρήσιμες υποδείξεις που προέρχεται από την έρευνα του Eck αφορά την κατηγοριοποίηση των υποθέσεων σε τρεις ομάδες - εκείνες που πρόκειται να επιλυθούν, εκείνες που έχουν επιλυθεί και εκείνες που ίσως επιλυθούν με λίγη προσπάθεια[187]. Αυτό το σύστημα «τρίγωνο» επινοήθηκε για τη βοήθεια νομικής εφαρμογής παίρνοντας αντικειμενικές αποφάσεις για το ποιες υποθέσεις ήταν πιο δαπανηρές ως προς την εφευρετικότητα τους.

---

[184] Βλ., Eck, 1983
[185] Βλ., Sanders, 1977, Wilson, 1976
[186] Βλ., όπ., υπ. 128
[187] Βλ., όπ. υπ. 123

Μέσω αυτού του τρόπου εξέτασης των υποθέσεων, οι έρευνες συνεχίζονται με έναν στοχευόμενο και πληροφοριακό τρόπο αφού πρώτα καθοριστεί η παρουσία των παραγόντων που μπορούν να δώσουν λύση, κάτι που ενδεχομένως να οδηγήσει στην εξιχνίαση των υποθέσεων. Επιπροσθέτως, αυτός ο τρόπος επιτρέπει στα νομικά τμήματα να ενεργούν ενάντια στις μικρές ομάδες των παραβατών ή των «καριεριστών εγκληματιών» που διαπράττουν την πλειοψηφία σοβαρών εγκλημάτων[188]. Ο Eck αισθάνθηκε πως αυτές οι συστηνόμενες αλλαγές θα κρατήσουν πολύ για τον εκλεπτυσμό της διαδικασίας και τη βελτίωση της χρησιμότητας και του ρυθμού επιτυχίας.

Από αυτές τις δυο εντατικές προσπάθειες έρευνας στις Ηνωμένες Πολιτείες, προκύπτουν μερικά σημαντικά μαθήματα. Πρώτον, ο ρόλος του αστυνομικού ανταποκριτή είναι κρίσιμος στις έρευνες, και τις περισσότερες φορές οι πληροφορίες που προμηθεύονται είναι ο αποφασιστικός παράγοντας επίλυσης μιας υπόθεσης. Επιπροσθέτως, φαίνεται ότι επεκτείνοντας το πλάτος των ερευνών διερευνώντας άλλες οδούς απόκτησης πληροφοριών ίσως αποδειχθεί πολύτιμο, όπως και τα ενημερωτικά στοιχεία που μπορούν να αποκτηθούν με αυτό τον τρόπο. Τέλος, η τελειότητα σε προβολή τεκμηρίωσης είναι φαινομενικά κρίσιμη στη δομή μιας ισχυρής υπόθεσης και αυξάνει την πιθανότητα μιας επιτυχημένης ομάδας δίωξης.

9.2.4. Καθοριστικές διαφορές

Όπως αναφέρεται, οι ερευνητικές πράξεις και οι τρόποι ενέργειας τόσο για τα παραδοσιακά εγκλήματα όσο και για την ανεπτυγμένη μορφή των εγκλημάτων μέσω υπολογιστή είναι όμοιες από πολλές απόψεις εξαιτίας της έμφυτης μεθόδου επανάληψης της τροποποίησης των παραδοσιακών εγκλημάτων μέσω νεωτερισμού ή τεχνολογικής ανάπτυξης[189]. Παρ' όλα αυτά, οι ζωτικές διαφορές υπάρχουν στην ερευνητική μέθοδο, και πρέπει να προσαρμοστούνε για την αντιμετώπιση των εγκλημάτων μέσω υπολογιστών.

[188] Βλ., Wolfgang, Figlio, & Sellin, 1972
[189] Βλ., Tarde, [1890] 1903

Αυτές οι διαφορές αποκαλύφτηκαν κυρίως από τις σημασιολογικές του διακρίσεις.

Τα παραδοσιακά εγκλήματα γενικότερα αφορούν προσωπικά ή περιουσιακά αδικήματα για τα οποία οι νομικοί αγωνίζονται εδώ και αιώνες, όπως το παράπτωμα του Τύπου Ι της εγκληματικής αναφοράς του FBI στις Ηνωμένες Πολιτείες.

Τα μη παραδοσιακά εγκλήματα, με σκοπό τη ροή εργασίας, περικλείουν εκείνους που εμπλέκονται σε έναν υπολογιστή. Αυτά ιστορικά δεν έχουν λάβει μια ανάλογη ποσότητα προσοχής σε σύγκριση με τα παραδοσιακά εγκλήματα, παρά τη σοβαρότητά τους και την ουσιαστική ζημιά που συχνά προκαλούν[190]. Επιπλέον, δεν εκμαιεύουν την ίδια ουσία και συναισθηματική αντίδραση από το Αμερικανικό κοινό και το πολιτικό σύστημα όπως κάνει ένα συνηθισμένο άτομο[191]. Αυτές οι οντότητες είχαν σημαντική επιρροή στην τακτική και τις ενέργειες συστήματος εγκλήματος και δικαιοσύνης των Ηνωμένων Πολιτειών, με αποτέλεσμα μια συγκριτικά μικρή ποσότητα προσπάθειας και διεξόδων που κατανέμονται για τα εγκλήματα μέσω υπολογιστή.

Η εγκληματικότητα μέσω υπολογιστή ορίζεται ως «παράνομες πράξεις οι οποίες τροφοδοτούνται ή διευκολύνονται από έναν υπολογιστή, είτε ο υπολογιστής είναι αντικείμενο εγκληματικής πράξης, είτε είναι ένα όργανο που χρησιμοποιείται για τη διάπραξη ενός εγκλήματος, είτε αποδεικνύει τη συσχέτισή του με ένα έγκλημα»[192]. Μερικά από τα πιο διακεκριμένα είδη συμπεριλαμβανομένου της εμπορικής απάτης, είναι αυτό της παιδικής πορνογραφίας, της πειρατείας και της παράβασης της ασφάλειας του διαδικτύου. Οι ερευνητικές δυσκολίες εισάγονται στην απόπειρα αντιμετώπισης εγκλημάτων μέσω υπολογιστή εξαιτίας των τεχνολογικών επιπέδων της φύσης, γεγονός που μπορεί να προκύψει σχεδόν ακαριαία, και

[190] Βλ., Braithwaite, 1985, Hinduja, 2004, Newman & Clarke, 2003, Parker, 1976, Rosoff, Pontell, & Tillman, 2002, Webster, 1980
[191] Βλ., Benson, Cullen, & Maakestad, 1990, Cullen, Link, & Polanzi, 1982
[192] Βλ., Royal Canadian Mounted Police, 2000

επειδή είναι δύσκολο να τα παρατηρήσεις, να τα διακρίνεις ή να τα παρακολουθήσεις[193]. Αυτά τα προβλήματα αναμειγνύονται με τη συγκριτική ανωνυμία η οποία παρέχεται από το διαδίκτυο καθώς και η υπερβατικότητα των γεωγραφικών και φυσικών περιορισμών στο χώρο του διαδικτύου, δύο απ' τα οποία καθιστούν δύσκολη την ανίχνευση των εγκληματιών που είναι ικανοί να θέσουν σε ανεπάρκεια τα θύματά τους.

9.3. - Έρευνα 3η: Έρευνα για τη Σχέση Παιδιών - Διαδικτύου από τη εταιρία λογισμικού Symantec και τη Διεθνή Ένωση για την Εξακρίβωση Εγκλημάτων

Η Symantec και η Διεθνής Ένωση για την Εξακρίβωση Εγκλημάτων (International Crime Analysis Association - ICAA) πραγματοποίησαν μια έρευνα για το έγκλημα στο Διαδίκτυο και τους πιθανούς κινδύνους που προκύπτουν κατά τη χρήση του Διαδικτύου από τα παιδιά. Η έρευνα βασίστηκε σε ψυχολογικές μελέτες, που πραγματοποιήθηκαν αναφορικά με τους πιθανούς κινδύνους που γεννιούνται για τα παιδιά κατά τη διάρκεια πλοήγησης τους στο Διαδίκτυο, επισημαίνοντας την σοβαρότητα τους. Η έρευνα διεξήχθη σε δείγμα παιδιών ηλικίας 8 έως 13 ετών, ενώ πραγματοποιήθηκε με την υποστήριξη του Υπουργείου Επικοινωνιών της Ιταλίας, της Αστυνομίας Διαδικτύου (Internet Police), της Κοινότητας Lazio και της διεθνούς οργάνωσης UNICEF.

Η παραπάνω έρευνα κατέγραψε την συμπεριφορά των ανήλικων παιδιών απέναντι σε υπαρκτούς κινδύνους, που υπάρχουν στο Διαδίκτυο αλλά και τη συνολική τους στάση κατά τη διάρκεια χρήσης του Διαδικτύου. Κατέγραψε επίσης στοιχεία σχετικά με τις αντιλήψεις και τη στάση ενηλίκων, που έχουν υπό την ευθύνη τους παιδιά – όπως οι κηδεμόνες και οι δάσκαλοι- απέναντι σε αυτούς τους κινδύνους.

Τα αποτελέσματα της έρευνας έδειξαν ότι:

[193] Βλ., Leibowitz, 1999, United Nations, 1994

• Η πλειοψηφία των παιδιών επισκέπτεται κυρίως chat-rooms και άλλες διαδραστικές υπηρεσίες γιατί τους επιτρέπει να επικοινωνούν ζωντανά με άτομα που δεν γνώριζαν προηγουμένως.

• Τα παιδιά που συμμετείχαν στην έρευνα απάντησαν ότι ενδιαφέρονται για θέματα που σχετίζονται με το sex

• Το **47%** των ενηλίκων που συμμετείχαν δήλωσαν ότι σπάνια επιβλέπουν τα παιδιά κατά την πλοήγηση τους στο Διαδίκτυο

• **27%** των παιδιών που συμμετείχαν στην έρευνα δήλωσαν ότι δεν είναι ποτέ κάτω από επίβλεψη

• **34%** των παιδιών που συμμετείχαν στην έρευνα δήλωσαν ότι δεν δέχτηκαν πότε συμβουλές από τους γονείς τους για θέματα πλοήγησης στο Internet

• Η πλειοψηφία των δασκάλων ή καθηγητών που συμμετείχαν δήλωσε ότι δεν γνωρίζει πώς να προσεγγίσει το θέμα του Διαδικτύου και ότι η διδασκαλία που αφορά τη χρήση υπολογιστών, Internet και νέων τεχνολογιών πρέπει να βελτιωθεί.

«Όταν η επικοινωνία με τους γονείς είναι ελλιπής, τα παιδιά αντιμετωπίζουν την εμπειρία τους στο Internet σαν μία ιδιωτική στιγμή της ζωής τους», δηλώνει η Francesca Guidice, Αντιπρόεδρος και Διευθύνουσα Σύμβουλος της Symantec στη Νότια Ευρώπη, Μέση Ανατολή και Αφρική. «Η κατάλληλη εκπαίδευση, σε παιδιά, γονείς και δασκάλους κρίνεται απαραίτητη ώστε να μπορούν οι νέοι να χρησιμοποιούν το Internet με υπεύθυνο και ενημερωμένο τρόπο. Έχοντας αυτό σαν βάση, η υιοθέτηση παραμέτρων ασφαλείας που επιτρέπει στους ενήλικες να ρυθμίζουν εκ των προτέρων τα όρια της πλοήγησης και περιεχομένου στα οποία θα μπορούν τα παιδιά να έχουν πρόσβαση, είναι πολύ σημαντική».

Τα στοιχεία της έρευνας συγκεντρώθηκαν από ένα πλήθος ερωτηματολογίων που διανεμήθηκαν σε σχολεία σε δείγμα 5.000 παιδιών, ηλικίας μεταξύ 8 και 13 ετών σε ολόκληρη την Ιταλία (Βόρεια Ιταλία: 1000, Κεντρική/ Βόρεια Ιταλία: 1000, Κεντρική Ιταλία: 1000, Κεντρική / Νότια Ιταλία: 1000, Νότια Ιταλία: 1000), καθώς και από σύντομες συνεντεύξεις, που πραγματοποιήθηκαν σε ένα δείγμα γονέων και καθηγητών.

Μια αρχική έρευνα πραγματοποιήθηκε σε δείγμα 500 παιδιών που χρησιμοποιούσαν ήδη το Internet και τα οποία φοιτούν σε σχολεία της Ρώμης, της Καμπανίας και της Σικελίας. Το τελικό ερωτηματολόγιο διανεμήθηκε σε 5000 μαθητές από επιλεγμένες Ιταλικές πόλεις, μεταξύ των οποίων ήταν το Τορίνο, η Γένοβα, το Τέρνι, η Ρώμη, η Νάπολη, η Ρέντζιο, η Καλαβρία και το Παλέρμο. Οι ερωτήσεις αφορούσαν τέσσερα βασικά θέματα: χρήση του Διαδικτύου, προεπιλεγμένοι τρόποι επικοινωνίας, γενικές γνώσεις των παιδιών για το Διαδίκτυο και προθυμία των νέων να συζητούν για τις εμπειρίες που αποκομίζουν στο Διαδίκτυο.

«Το σχέδιο για την καταγραφή του βαθμού αντίληψης των παιδιών για τους κινδύνους στο Διαδίκτυο (Child Internet Risk Perception - CIRP) συμβαδίζει με το σκοπό της Διεθνούς Ένωσης για την Εξακρίβωση Εγκλημάτων - ICAA, η οποία εργάζεται σκληρά για τη διενέργεια εγκληματολογικών και επιστημονικών ερευνών, με στόχο την πρόληψη της εγκληματικής συμπεριφοράς και την προστασία των ανηλίκων», δήλωσε ο Marco Strano, Πρόεδρος της ICAA. «Στόχος μας είναι η μελέτη της ενδεχόμενης επικίνδυνης συμπεριφοράς των παιδιών και του βαθμού αντίληψης τους για τους κινδύνους που προκύπτουν στο Διαδίκτυο. Θέλουμε επίσης να καταλάβουμε πως οι ενήλικες που είναι νομικά υπεύθυνοι για την επίβλεψη και την εκπαίδευση των παιδιών (τόσο οι γονείς όσο και οι δάσκαλοι) αντιλαμβάνονται τους κινδύνους του Διαδικτύου. Το πρόγραμμα «Παιδική Αντίληψη για τους Κινδύνους στο Διαδίκτυο» συμπεριλαμβάνει ενημερωτικές καμπάνιες και εκπαιδευτικές εκδηλώσεις, στις οποίες ο καθένας παίζει τον ανάλογο ρόλο (παιδί, γονείς και δάσκαλοι), αξιοποιώντας

αποτελεσματικά εκπαιδευτικά εργαλεία (μικρά τμήματα, focus groups, έντυπα κ.α.) καθώς και εξειδικευμένες τεχνολογίες, που αναπτύχθηκαν από την Symantec σε συνεργασία με την ICAA.

Τα αποτελέσματα αυτής της μελέτης επιβεβαιώνουν την ανάγκη ενημέρωσης και εκπαίδευσης βασικών κοινωνικών ομάδων (οικογένειες και σχολεία). Οι συγκεκριμένες ενέργειες θα έχουν ως στόχο να αποτρέψουν και να ελαχιστοποιήσουν τις πιθανότητες επικίνδυνων συναλλαγών ή δραστηριοτήτων στο Διαδίκτυο. Μέσα από αυτή την εκπαίδευση θα ενισχυθεί η προστασία που παρέχεται στους νέους για ασφαλή χρήση του Διαδικτύου δημιουργώντας τις προϋποθέσεις για την γρήγορη τους ανάπτυξη. Ένα πρώτο βήμα για την ασφαλή πλοήγηση τω νέων στο Διαδίκτυο είναι η ύπαρξη εργαλείων τα οποία θα επιτρέπουν στους κηδεμόνες να επιβλέπουν τις κινήσεις των παιδιών στο Διαδίκτυο και θα θέτουν περιορισμούς ως προς το περιεχόμενο στο οποίο τους δίνεται πρόσβαση. Αυτά τα εργαλεία για την προστασία και την ασφάλεια κατά τη διάρκεια της πλοήγησης συμπληρώνονται με εξειδικευμένα εργαλεία, που μπορούν να ενισχύσουν ακόμη και το πιο απλό λογισμικό anti-virus με ισχυρές λύσεις firewall, επιτρέποντας με αυτόν τον τρόπο στους γονείς να επιβλέπουν την πρόσβαση των παιδιών στο Internet.

Η *Διεθνής Ένωση για την Εξακρίβωση Εγκλημάτων* είναι ένα μη κερδοσκοπικό ερευνητικό και επαγγελματικό ινστιτούτο εκπαίδευσης με έδρα την Ρώμη, που διεξάγει έρευνες σε βασικές θεματικές περιοχές της ψυχολογίας και της εγκληματολογίας. Η I.C.A.A συγκεντρώνει ερευνητές, ακαδημαϊκούς και στελέχη, που εργάζονται στον τομέα της εγκληματολογίας. Η I.C.A.A έχει δημιουργήσει μία επαγγελματική ομάδα 80 ερευνητών (από διαφορετικές ειδικότητες: ψυχολογία, ιατρική, εγκληματολογία, κοινωνιολογία) με σημαντική δραστηριότητα και μελέτες, τα αποτελέσματα των οποίων

παρέχονται στο ερευνητικό τμήμα της κρατικής αστυνομίας της Ιταλίας αλλά και σε επιχειρήσεις που ενδιαφέρονται για την πρόληψη του εγκλήματος[194].

9.4. Περιστατικά Ηλεκτρονικού Εγκλήματος

9.4.1. Παγίδες με παιχνίδια σε παιδιά

Έμποροι παιδικής πορνογραφίας παραπλανούν μικρά παιδιά εμφανιζόμενοι σε παιχνίδια ως συνομήλικοί τους για να παίξουν!

Η εικόνα του Μίκυ Μάους στο Ιντερνετ δεν είναι πάντα ακίνδυνη, ειδικά όταν χρησιμοποιείται ως προκάλυμμα από τους εμπόρους της παιδικής πορνογραφίας μέσω διαδικτύου. Πρόκειται για ένα φαινόμενο που πλέον παρουσιάζει αλματώδη αύξηση και στη χώρα μας. Είναι ενδεικτικό ότι συνδρομητικά sites (δικτυακοί τόποι) με φωτογραφίες παιδικής πορνογραφίας έχουν εντοπιστεί από τις αστυνομικές αρχές σε όλη την Ελλάδα (κυρίως σε Αθήνα, Βόλο, Μυτιλήνη, Ηράκλειο Κρήτης κ.α.). Σε όλο αυτό το σκηνικό, το οποίο είναι παγίδα για τους ανήλικους χρήστες του Ιντερνετ, συνηγορεί η νομιμοφάνεια των πορνογραφικών sites -με πρόσβαση χαμηλού κόστους- καθώς και η ανωνυμία του διαδικτυακού εμπόρου που ξέρει τρόπους να παραπλανά έναν ανήλικο εμφανιζόμενος ως... συνομήλικός του.

Παιδεραστές

Η επικινδυνότητα των παιδεραστών μέσω του Ιντερνετ με σκοπό το κέρδος είναι ανάλογη με τον φρενήρη ρυθμό αύξησης των ανήλικων χρηστών (στις ιστοσελίδες παιδικού ενδιαφέροντος), που ηλικιακά -σε παγκόσμια κλίμακα- κυμαίνονται από 2 μέχρι 17 ετών. Οι τρόποι με τους οποίους οι έμποροι του πορνογραφικού υλικού ξέρουν να «εισχωρούν» ακόμη και στα παιδικά παιχνίδια του διαδικτύου, καθώς και όλα τα στοιχεία της παρούσας

[194] Βλ., στο www.icaa-italia.org

έρευνας αποτελούν μελέτη, καταγραφή και επεξεργασία του κ. Αναστάσιου Παρθένη.[195]

ΠΡΟΣΤΑΣΙΑ: Σημαντικός ο ρόλος των γονιών

Όπως προτείνει ο ειδικός επί του θέματος κ. Παρθένης[196], «είναι καιρός να σταματήσει αυτό το κυνήγι μαγισσών και να καταλάβει η ελληνική κοινωνία και η ανθρωπότητα συνολικά ότι το Ιντερνετ είναι όπως και ένα νυστέρι: μπορεί να θεραπεύσει αλλά και να σκοτώσει». Σημαντικός θεωρείται, κατά τον ίδιο, ο ρόλος των γονιών, που «εξαιτίας της απροθυμίας τους να μάθουν πώς λειτουργεί το Ιντερνετ, γίνονται άμεσοι συνεργοί στα εγκλήματα με θύματα τα παιδιά τους, επειδή δεν κατάφεραν, πολύ δε περισσότερο δεν προσπάθησαν, να τα βοηθήσουν στη χρήση αυτού του επικίνδυνου εργαλείου, που συνάμα αποτελεί το μεγαλύτερο δώρο γνώσης από την τεχνολογία στην κοινωνία».

Τέλος στο ερώτημα «αν είναι δυνατός ο έλεγχος του περιεχομένου (εν προκειμένω του πορνογραφικού υλικού) στο Ιντερνετ, ο κ. Παρθένης[197] απαντά ότι κατά τη γνώμη του «η καλύτερη διαχείριση συστημάτων διαδικτυακής δημοσίευσης θα επιτευχθεί με την αύξηση του στοιχείου της ανθρώπινης επιτήρησης και της επιβεβαίωσης της ταυτότητας των συμμετασχόντων μελών, οι οποίες θα μειώσουν μεν τα κέρδη των επιχειρήσεων, αλλά θα έχουν ως αποτέλεσμα ένα πιο υγιεινό και ασφαλές Ιντερνετ».

---

[195] Ο Αναστάσιος Παρθένης είναι δικηγόρος, εγκληματολόγος και υποψήφιος διδάκτορας Δικαίου Internet στο ΕΚΠ Αθηνών. Επίσης βλ., στο (info@parthenis.gr και http://parthenis.gr).

[196] Βλ., ο.π. σ.147
[197] Βλ., ο.π.π.

ΤΟ ΠΑΙΔΙΚΟ ΠΑΙΧΝΙΔΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΡΥΒΕΙ ΚΙΝΔΥΝΟΥΣ

Όπως εξηγεί ο κ. Παρθένης στην εφημερίδα το «Εθνος», οι μεγαλύτεροι «σύμμαχοι» των εμπόρων της παιδικής πορνογραφίας είναι:

- Η νομιμοφάνεια που υπάρχει σε πλήθος πορνογραφικά sites, στα οποία η πρόσβαση γίνεται με πολύ χαμηλό κόστος. Υπάρχει π.χ υπηρεσία στις ΗΠΑ (και δεν είναι η μόνη), που αριθμεί 11.000.000 αρχεία με παιδικό πορνογραφικό περιεχόμενο και λειτουργεί... νόμιμα, έχοντας μάλιστα στην υπηρεσία της 110 υπαλλήλους και έχοντας τον ψευδεπίγραφο τίτλο «υπηρεσία ψυχαγωγίας ενηλίκων» (!). Μέσω της υπηρεσίας αυτής, παρέχεται στον χρήστη ένας κωδικός (password), που του δίνει πρόσβαση σε άνω των 200.000 sites, τα οποία περιέχουν φωτογραφίες ή βίντεο αντί χαμηλού τιμήματος.
- Η «ανωνυμία» που μπορούν να έχουν στο διαδίκτυο οι έμποροι της πορνογραφίας (και της παιδικής), τους βοηθά ώστε να παραπλανούν έναν ανήλικο χρήστη, ο οποίος θεωρεί ότι έχει να κάνει με έναν συνομήλικό του και «ανοίγει» μαζί του διαδικτυακή συνομιλία.

Αυτοματοποίηση

Η αυτοματοποίηση του web (παγκόσμιου ιστού), είναι ένα νόμισμα με δύο όψεις. Οπως τονίζει ο κ. Παρθένης, με τον ίδιο εύκολο τρόπο που αυτόματα δημοσιεύεται το μήνυμα κλήσης για βοήθεια από χρήστη ασθενή του AIDS, έτσι δημοσιεύεται και το μήνυμα του παιδεραστή στο διαδίκτυο, ο οποίος μιμούμενος τον ανήλικο, καλεί «συνομηλίκους» του «να κάνουν παρέα».

Διακίνηση πορνογραφικού περιεχομένου γίνεται ακόμη α) μέσω ομάδων συζητήσεων είτε, β) μέσω peer-to-peer προγραμμάτων (ανταλλαγή αρχείων). Τα προγράμματα αυτά είναι δημοφιλή στις νέες ηλικίες για την ανταλλαγή αρχείων μουσικής, πλην όμως διακινείται και πορνογραφικό υλικό. «Η συγκεκριμένη συμπεριφορά, εξηγεί ο κ. Παρθένης, δεν έχει

κερδοσκοπικό χαρακτήρα με την έννοια ότι ουδείς πληρώνει ή εισπράττει τίμημα για την ανταλλαγή αρχείων. Γι' αυτόν τον λόγο, τα προγράμματα αυτά έχουν αποτελέσει το κεντρικό μέτωπο επίθεσης των δισκογραφικών εταιρειών, δεδομένου ότι αυτές πλήττονται περισσότερο από την παράνομη ανταλλαγή των αρχείων μουσικής». Όπως διευκρινίζει ο ειδικός, «η απλή "περιήγηση' στο Ιντερνετ έστω και σε sites με πορνογραφικό περιεχόμενο δεν στοιχειοθετεί το αδίκημα της πορνογραφίας ανηλίκων, καθώς σύμφωνα με το άρθρο 348 Α του Ποινικού Κώδικα, απαιτείται να υπάρχει η πρόθεση του κέρδους».

ΔΙΚΑΙΟΣΥΝΗ: Επιτακτική η επιμόρφωση των δικαστικών σε ζητήματα τεχνολογίας

Επειδή το διαδικτυακό έγκλημα έχει πάρει διαστάσεις και στη χώρα μας, οι ειδικοί συμφωνούν ότι η Δικαιοσύνη δεν πρέπει να είναι μόνο τυφλή, αλλά... να έχει και γνώσεις Ιντερνετ (έστω και στοιχειώδεις) όταν δικάζει τέτοιου είδους υποθέσεις. Ο κ. Παρθένης θεωρεί «ως πρώτιστο στοιχείο για την ορθή απονομή της δικαιοσύνης (σχετικά με υποθέσεις Ιντερνετ) την επιμόρφωση των δικαστικών λειτουργών σχετικά με το γίγνεσθαι της τεχνολογίας».

Ως χαρακτηριστικό παράδειγμα ο ίδιος αναφέρει ότι «αν και έχουν δαπανηθεί χρήματα για την αγορά φορητών υπολογιστών με προορισμό δικαστικούς λειτουργούς, παρ' όλα αυτά, η καθημερινή πρακτική δείχνει ότι παραδίδονται δικαστικές αποφάσεις σε... χειρόγραφες σημειώσεις και μάλιστα σε κόλλες μεγέθους μισής σελίδας Α4, ώστε να είναι δυνατή η αντικατάστασή τους κατά την επεξεργασία των κειμένων». «Αυτή η νοοτροπία δεν είναι δυνατό να βοηθήσει στην εκδίκαση αδικημάτων που τελούνται με ή μέσω του Ινερνετ» προσθέτει ο κ. Παρθένης.

Αντιμετώπιση

Το πρόβλημα όμως αυτό φαίνεται ότι απασχολεί σε παγκόσμιο επίπεδο με στόχο την αντιμετώπιση του «κοινού εχθρού». Με αφορμή τη προειδοποίηση για παραπομπή στο Ευρωπαϊκό Δικαστήριο οκτώ χωρών αν δεν λάβουν μέτρα για την προστασία της ιδιωτικής ζωής μέσω ανεπίκλητων ηλεκτρονικών μηνυμάτων, η διευθύντρια των νομικών υπηρεσιών της Microsoft στην Ευρώπη κ. Μπεατρίς Μπελμάς δήλωσε χαρακτηριστικά: «... Προσφεύγουμε κάποιες φορές στα δικαστήρια, για να ανακαλύψουμε ότι οι δικαστές δεν έχουν καν χρησιμοποιήσει το Διαδίκτυο». Όπως τονίζουν οι ειδικοί, είναι αναγκαίο ένα σύγχρονο νομοθετικό «οπλοστάσιο» στελεχωμένο από λειτουργούς που να γνωρίζουν καλά το αντικείμενο αυτό.

Επιπροσθέτως ο κ. Παρθένης επικαλείται τον νόμο 2121/1993 «περί πνευματικής ιδιοκτησίας», σύμφωνα με τον οποίο, προβλέπεται λειτουργία ειδικού τμήματος στα δικαστήρια για την εκδίκαση ειδικών υποθέσεων». «Παρ' όλα, συμπληρώνει, δέκα χρόνια μετά, ουδέποτε δημιουργήθηκε τέτοιο τμήμα». Επίσης, όπως επισημαίνει, «είναι κατανοητή μεν η προδιάθεση των δικαστικών λειτουργών και ανακριτών να καταδικάσουν τον φερόμενο ως κατηγορούμενο για αδίκημα παιδικής πορνογραφίας, ωστόσο από την άλλη, αποτελεί κακή δίκη' να προφυλακίζεται κάποιος επειδή απλώς συνελήφθη να ανταλλάσσει ή να κατέχει φωτογραφίες πορνογραφικού περιεχομένου στο Ιντερνετ χωρίς κέρδος». [198]

9.4.2. Απετράπη δημοπρασία γυναικών στο διαδίκτυο

Αγγελία που προσέφερε σε δημοπρασία τρεις νεαρές Βιετναμέζες απέσυρε η ιστοσελίδα ηλεκτρονικού εμπορίου eBay Inc . και ανακοίνωσε ότι θα καταγγείλει στις αρχές το άτομο που την δημοσίευσε. Η αγγελία, που ανέφερε ότι οι γυναίκες μπορούσαν να παραδοθούν μόνο στην Ταϊβάν, ''είναι μια στυγερή παραβίαση όχι μόνο της πολιτικής του eBay, αλλά και του

---

[198] Βλ., στο http://www.edra.ipet.gr 13/4/04

νόμου'', δήλωσε ο εκπρόσωπος της εταιρείας, Χάνι Ντάρζι. ''Την αποσύραμε μόλις την αντιληφθήκαμε. Η οποιαδήποτε παρανομία αντίκειται στην πολιτική μας. Δεν υπάρχει κανένα περιθώριο για εμπόριο ανθρώπων στην ιστοσελίδα", πρόσθεσε.

Επικρίσεις κατά Ταϊβάν

Ο Ντάρζι είπε ότι δεν είναι σίγουρος για το **πότε** δημοσιεύτηκε η αγγελία. Το άτομο που την ανάρτησε χρησιμοποίησε το **ταϊβανέζικο eBay** .

Σύμφωνα με το Εθνικό Συμβούλιο Αμερικανών Βιετναμέζων, η αγγελία πρωτοδημοσιεύτηκε στις 2 Μαρτίου.

Ο Χουνγ Νγκουέν, ο πρόεδρος του Συμβουλίου, είπε ότι έγραψε στο eBay ζητώντας να αποσυρθεί η προσφορά μόλις το αντιλήφθηκε, τρεις ημέρες αργότερα. Τέτοιες ενέργειες "πραγματικά μας **ανησυχούν**", πρόσθεσε ο Νγκουέν, εγκωμιάζοντας το eBay για τη **γρήγορη αντίδρασή** του.

Το Στέιτ Ντιπάρτμεντ υποστηρίζει ότι η **Ταϊβάν** είναι η **χώρα προέλευσης** ή **προορισμού** ατόμων που μεταφέρονται για **σεξουαλική εκμετάλλευση** ή **καταναγκαστική εργασία** .

Συχνά τα θύματα μεταφέρονται στην Ταϊβάν από την Κίνα, την Ταϊλάνδη, την Καμπότζη, το Βιετνάμ, την Ινδονησία και τις Φιλιππίνες.199

9.4.3. «Ασυδοσία» στα chat rooms

Σιάτλ: Τα chat rooms του δικτύου MSN κλείνουν στις περισσότερες αγορές, καθώς έχουν πια γεμίσει με διαφημιστικά μηνύματα (spam), συχνά

---

[199] Βλ., στο http://www.ert.gr/eidiseis/index_news.asp?id=35290

πορνογραφικού περιεχομένου, και έχουν μετατραπεί σε χώρο δράσης παιδόφιλων, ανακοίνωσε την Τετάρτη η Microsoft.

Σύμφωνα με την εταιρεία, οι χρήστες των chat rooms είχαν ούτως ή άλλως μειωθεί, στα 8,6 εκατομμύρια, καθώς όλο και περισσότεροι προτιμούν να συζητούν μέσω υπηρεσιών στιγμιαίας ανταλλαγής μηνυμάτων, όπως το Messenger της ίδιας της Microsoft.

Τα chat rooms του MSN κλείνουν στις 14 Οκτωβρίου σε περισσότερες από 32 χώρες στην Ευρώπη, τη Λατινική Αμερική και την Ασία. Στις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Βραζιλία τα δωμάτια συζήτησης θα παραμείνουν ανοιχτά, ωστόσο θα δέχονται μόνο τους χρήστες που έχουν πληρώσει συνδρομή για τουλάχιστον μία άλλη υπηρεσία του MSN.

Η Microsoft εκτιμά ότι οι επώνυμοι συνδρομητές είναι λιγότερο πιθανό να εκδηλώσουν παράνομη ή ανήθικη συμπεριφορά στα chat rooms, από ό,τι οι ανώνυμοι επισκέπτες που δεν έχουν πληρώσει για την υπηρεσία.

Αρκετές περιπτώσεις σεξουαλικής παρενόχλησης ανηλίκων σε chat rooms έχουν παραπεμφθεί στη Δικαιοσύνη στις ΗΠΑ και άλλες χώρες.

Ωστόσο η απόφαση της Microsoft ήδη προκαλεί αντιδράσεις, τόσο από υποστηρικτές της ελευθερίας του λόγου όσο και από αναλυτές της αγοράς, που εκτιμούν ότι η κατάργηση της υπηρεσίας είναι στην πραγματικότητα μέσο προώθησης του MSN Messenger.[200]

9.4.4. Ενοικιάζονται «φίλοι» ανηλίκων...

Θέλετε συντροφιά για το ανήλικο παιδί σας ούτως ώστε να μην νιώθει μόνο του; Τη λύση σε αυτό έρχεται να δώσει μια νέα ομάδα που έκανε την

---

[200] Βλ., στο http://tech.pathfinder.gr/tech/9350.html - Associated Press

εμφάνισή της στη Μελβούρνη η οποία ενοικιάζει φίλους και φιλενάδες για ανήλικα παιδιά με το αζημίωτο.

Η Μαίρη Μπόουμαν, κάτοικος Μελβούρνης αποτελεί ένα χαρακτηριστικό παράδειγμα του παραπάνω καθώς πληρώνει σε γειτονόπουλα πέντε δολάρια την ώρα για να παίξουν με τον Ντάμιεν που πάσχει από το σύνδρομο Down και νιώθει μόνος, μια και δεν έχει αδέλφια ούτε και φίλους. Ο Ντάμιεν είναι 20 χρόνων, αλλά έχει την πνευματική ανάπτυξη νεαρού έφηβου.

Εν τω μεταξύ, ο διευθυντής του Συνδέσμου Υπεράσπισης των Ατόμων με Ειδικές Ανάγκες, Κέβιν Στόουν, εκτιμά ότι η πληρωμή για φιλία με άτομα με ειδικές ανάγκες είναι κάτι σπάνιο και, οπωσδήποτε, κάτι για το οποίο ο ίδιος νιώθει πάρα πολύ άβολα, προσθέτοντας, εντούτοις, ότι καταλαβαίνει και τη δύσκολη θέση των γονιών.

Μια άλλη συναφής είδηση που είδε το φως της δημοσιότητας, είναι ότι εννιάχρονο κοριτσάκι πουλά τη συντροφιά της σε μοναχικά παιδιά. Η ίδια μοίρασε μπροσούρες με τη διαφήμιση "νοικιάστε με να παίξουμε".

Η νεαρή επιχειρηματίας, χρεώνει πέντε δολάρια την ώρα και δηλώνει χαρούμενη που βοηθάει μαμάδες και μπαμπάδες με το να κρατά συντροφιά στα παιδιά τους. Εκπρόσωπος, ωστόσο, του οργανισμού προστασίας παιδιών Childwise, προειδοποιεί ότι η μικρή διατρέχει μεγάλο κίνδυνο από παιδεραστές.[201]

9.4.5. Εξαρθώθηκε κύκλωμα διακίνησης πορνό μέσω Internet

Υπόθεση διακίνησης σκληρού πορνό μέσω Ιντερνετ αποκαλύφθηκε όταν ένας 30χρονος υπάλληλος μεγάλης εταιρίας που μπήκε στη

---

[201] Βλ., στο http://woman.flash.gr//pregnancy/2004/2/6/3002id/print_version.htm

συγκεκριμένη σελίδα είδε σε βίντεο τη γυναίκα του 25 χρόνων σε σκηνές σκληρού σέξ με τον εραστή της.

Το περιστατικό αποτέλεσε τον κρίκο μέσω του οποίου εξιχνιάστηκε η υπόθεση από το ειδικό τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής. Όπως έγινε γνωστό από την αστυνομία δημιουργός της σελίδας είναι ένας 22χρονος άριστος χρήστης ηλεκτρονικού υπολογιστή και του Ιντερνετ ο οποίος συνελήφθη και ομολόγησε. Ο 22χρονος πρόβαλε φωτογραφίες και βίντεο μέσω του ιδιότυπου ερωτικου κλάμπ που παρουσίαζαν ερωτικές διαστροφές μελών. Οι περισσότερες εικόνες είχαν ληφθεί από άντρες εν αγνοία των παρτενέρ τους αλλά μεγάλο μέρος του υλικού είχε δοθεί από τα ίδια τα ζευγάρια και έδειχναν τις ερωτικές τους συνευρέσεις. Η επίσκεψη της ιστοσελίδας ήταν δωρεάν γι' αυτό υπολογίζεται από τους αστυνομικούς ότι οι επισκέπτες ήταν πολλές χιλιάδες καθημερινά. Ο ιδρυτής της σελίδας ωστόσο έβγαζε αρκετά χρήματα από διαφημίσεις που δημοσιεύονταν μέσα από αυτή. Σε βάρος του 22χρονου σχηματίστηκε δικογραφία η οποία υποβλήθηκε στον εισαγγελέα. Μια ακόμα υπόθεση διακίνησης πορνογραφικού υλικού και ειδικότερα παιδικής πορνογραφίας εξαρθρώθηκε από το τμήμα Προστασίας Ανηλίκων της Ασφάλειας Αττικής. Ειδικότερα, μετά από πληροφορίες που έδωσαν οι νορβηγικές αρχές εντοπίστηκε από τους ειδικούς του τμήματος Προστασίας Ανηλίκων το ηλεκτρονικό αποτύπωμα του Έλληνα χρήστη που διακινούσε το υλικό και ο οποίος συνελλήφθη και ομολόγησε.

Ο δράστης ηλικίας 33 ετών είχε εγκαταστήσει τη μονάδα του ηλεκτρονικού υπολογιστή στο χώρο εργασίας του έχοντας υποκλέψει μια τηλεφωνική γραμμή από τον κεντρικό κατανεμητή την οποία μέσα από ένα ψευδοπάτωμα την είχε μεταφέρει στο γραφείο του απ' όπου έκανε την εκπομπή μέσω του Ιντερνετ ή έκανε εκτροπή της σύνδεσης που είχε στην εργασία του σε ροζ γραμμές του εξωτερικού, ζημιώνοντας έτσι την επιχείρηση. Στο γραφείο βρέθηκε και κατασχέθηκε ο υπολογιστής, βιντεοκάμερες και Cd-Rom καθώς και δισκέτες και βιντεοκασέτες που

περιείχαν 12.000 αρχεία σκληρού παιδικού πορνό το οποίο απεικόνιζε ακόμα και βρέφη σε σεξουαλική δραστηριότητα. Ο 33χρονος οδηγήθηκε στον εισαγγελέα και όπως είπε διακινούσε το υλικό για κερδοσκοπία αλλά και για να ικανοποιεί το πάθος του.[202]

9.4.6. «Τρομοκρατία» στο διαδίκτυο

Ο ιός Blaster προκάλεσε χάος σε μισό εκατομμύριο ηλεκτρονικούς υπολογιστές σε ολόκληρο τον κόσμο. Θεωρείται όμως ασήμαντος μπροστά στο τι θα μπορούσε να κάνει μια πραγματική τρομοκρατική επίθεση στον κυβερνοχώρο, όπως υποστηρίζουν Αμερικανοί αξιωματούχοι του υπουργείου Εσωτερικής Ασφάλειας.

Οι επιθέσεις που έχουν εξαπολυθεί μέχρι σήμερα ήταν σχετικά απλές και μη καταστροφικές, είπε ο Αμίτ Γιόραν, διευθυντής του τμήματος εθνικής Κυβερνητικής Ασφάλειας, σε μια σύσκεψη κυβερνητικών αξιωματούχων με στελέχη εταιρειών υψηλής τεχνολογίας. «Όμως δεν μπορούμε να βασιστούμε σε αυτό επ' άπειρον», πρόσθεσε.

Ο υπουργός Τομ Ριτζ τόνισε από την πλευρά του ότι το Ιντερνετ και τα δίκτυα από τα οποία εξαρτάται η σύγχρονη αμερικανική βιομηχανία αποτελούν ελκυστικό στόχο για τρομοκράτες.

Μια άσκηση προσομοίωσης επίθεσης σε τράπεζες, εταιρείες κοινής ωφέλειας και άλλες υπηρεσίες, που έγινε τον Οκτώβριο, έδειξε ότι υπάρχουν προβλήματα στην επικοινωνία μεταξύ εταιρειών και κυβέρνησης που θα πρέπει να αντιμετωπιστούν γρήγορα, είπε.

Ο Γιόραν χαρακτήρισε την άσκηση αυτή σαν ένα τεστ για να δοκιμαστεί πόσο γρήγορα θα μπορούσαν να αντιδράσουν οι εταιρείες και οι

---

[202] Βλ., στο http://tech.flash.gr/news/greece/2004/2/24/10523id/

κυβερνητικές υπηρεσίες σε μια ενδεχόμενη κυβερνοεπίθεση. Το επίπεδο προστασίας των κυβερνητικών δικτύων είναι απαράδεκτο, τόνισε.

Η κυβέρνηση ανησυχεί ότι τέτοιου είδους επιθέσεις μπορεί να σπείρουν το χάος στα συστήματα τηλεπικοινωνιών, στα τραπεζικά και εμπορικά δίκτυα και σε άλλες υπηρεσίες. Οι δράστες θα μπορούσαν να χρησιμοποιήσουν κάποιον ιό ή να μπουν στα δίκτυα μέσω κενών ασφαλείας στο λογισμικό ή με κάποια άλλη μέθοδο. [203]

9.4.7. Ιός εξαπατά όσους έχουν πιστωτικές κάρτες

Ο Mimail.J είναι ένας καινούργιος ιός, που προσπαθεί να εξαπατήσει τους χρήστες που κάνουν αγορές μέσω του Διαδικτύου. Η εμφάνισή του έγινε την προηγούμενη Δευτέρα και πιστεύεται πως προέρχεται από τη Γαλλία, αν και τα περισσότερα μηνύματα στέλνονται από τις ΗΠΑ. Η εξάπλωση του ιού αυτού γίνεται μέσω της ηλεκτρονικής αλληλογραφίας. Συγκεκριμένα, ο ιός επισυνάπτεται σε ηλεκτρονικό μήνυμα και, όταν ανοιχθεί, αντιγράφεται σε νέες ηλεκτρονικές διευθύνσεις.

Χρησιμοποιεί ψεύτικη ιστοσελίδα

Ο συγκεκριμένος ιός υποτίθεται πως είναι από την εταιρία **Paypal** και το θέμα του ηλεκτρονικού μηνύματος αναγράφει τη λέξη "**επείγον**". Στο μήνυμα **επισυνάπτονται** κυρίως δύο αρχεία, με τα ονόματα **InfoUpdate.exe** ή **www.paypal.com.pif**.

Πώς όμως **εξαπατά** τους χρήστες; Διαβάζοντας το αρχείο που επισυνάπτεται, ο χρήστης "ενημερώνεται" πως, ο τραπεζικός του **λογαριασμός** ή η πιστωτική του κάρτα **πλησιάζουν** στην **ημερομηνία λήξης** και για αυτό καλείται να **ανανεώσει** τα στοιχεία του λογαριασμού του. Φυσικά, αν ο χρήστης στείλει τα στοιχεία, οι επιτήδειοι μπορούν να τα

[203] Βλ.. στο http://news.antenna.gr/articleDetail/0,3091,76233,00.html

χρησιμοποιήσουν για να κάνουν αγορές μέσω του Διαδικτύου ή να βγάλουν πλαστές πιστωτικές κάρτες.

Οικονομική απάτη

Όπως παρατηρούν οι ειδικοί, ο ιός αυτός δεν αποσκοπεί στο να μπλοκάρει κάποιο πρόγραμμα των Windows, αλλά να **εξαπατήσει οικονομικά** τους χρήστες του Internet και να τους αποσπάσει χρηματικά ποσά. Ο Μάρκ Σάνερ, επικεφαλής συστημάτων ασφαλείας της εταιρία MessageLabs, τονίζει πως, ο ιός αυτός αποδεικνύει ότι "στόχος των εγκληματιών του Διαδικτύου είναι να γεμίσουν τις τσέπες τους".

Ο κ. Σάνερ, επισημαίνει πως, οι **χρήστες** του Διαδικτύου γίνονται ολοένα και πιο **ευάλωτοι** σε κάθε λογής ιό, αν και ο Mimail.J έχει ρυθμιστεί να έχει σύντομη διάρκεια ζωής. Ωστόσο, τονίζει πως οι επιτήδειοι θα "χτυπήσουν" και πάλι, με μια **νέα παραλλαγή** του ιού. Για το λόγο αυτό, οι χρήστες του Διαδικτύου πρέπει να είναι **επιφυλακτικοί** και να μην ανοίγουν κάθε ηλεκτρονικό μήνυμα που λαμβάνουν, ιδιαίτερα όταν αυτό προέρχεται από έναν άγνωστο αποστολέα ή έχει "περίεργες" επισυνάψεις. [204]

9.4.8. «Ιδιαίτερα μαθήματα» μέσω INTERNET. www... Έμπορος ναρκωτικών

Αμερικανικό παιχνίδι στρατηγικής στηρίζεται στην ικανότητα του παίκτη να πλουτίζει από το εμπόριο του «λευκού θανάτου»

Ένα παιχνίδι εξοικειώνει τους χρήστες του Ιντερνετ με τον κόσμο των ναρκωτικών και έρχεται να προστεθεί στα παιχνίδια βίας και παρανομίας που κυκλοφορούν εν αφθονία στο διαδίκτυο. Το «DOPE WARS», ένα παιχνίδι στρατηγικής της αμερικανικής εταιρείας Beermat Software Ltd, βασίζεται στην ικανότητα του παίκτη να πλουτίσει από το εμπόριο

---

[204] Βλ., στο http://www.ert.gr/site/news/newsbody_eu.asp?ID=88626

ναρκωτικών. Ο παίκτης είναι ο έμπορος ναρκωτικών που επιδιώκει μέσα σε 30 ημέρες να θησαυρίσει μέσω της αγοραπωλησίας παράνομων ψυχοτρόπων ουσιών. Ταυτόχρονα, θα πρέπει να αποφύγει κίνδυνους όπως τη σύλληψή του από την αστυνομία ή τη χρεοκοπία ακόμη και τον θάνατο.

Στην πρώτη οθόνη του παιχνιδιού, ο παίκτης καλείται να επιλέξει την πόλη στην οποία θα αναπτύξει τη δράση του. Μπορεί να διακινήσει ναρκωτικά στη Νέα Υόρκη, στο Λονδίνο, στο Λος Αντζελες, στο Σικάγο, στο Γιοχάνεσμπουργκ και σε άλλες μεγάλες πόλεις του κόσμου. Στη συνέχεια, βλέπει μια οθόνη όπου δίνεται μια λίστα με τα είδη των ναρκωτικών που είναι πιο δημοφιλή στην πόλη που επέλεξε. Στη Νέα Υόρκη, για παράδειγμα, μπορεί να αγοράσει και να πουλήσει κοκαΐνη, κρακ, έκσταση, χασίς, «μανιτάρια» και άλλες ουσίες. Παράλληλα βλέπει μια μπάρα που απεικονίζει την κατάσταση της υγείας του κατά τη διάρκεια του παιχνιδιού. Ο δείκτης της υγείας του μειώνεται όταν κάποιος τον πυροβολεί και αν φτάσει στο μηδέν πριν εξαντληθεί το διαθέσιμο χρονικό διάστημα ο φιλόδοξος έμπορος ναρκωτικών πεθαίνει και χάνει το παιχνίδι.

Όταν ξεκινά, έχει στη διάθεσή του κάποιο χρηματικό ποσό για να κινηθεί, ενώ ταυτόχρονα καλείται να ξεπληρώσει τα χρέη του. Κατά τη διάρκεια του παιχνιδιού, πρέπει να αναζητήσει την καλύτερη τιμή, προκειμένου να διακινήσει ναρκωτικά, σε διάφορες περιοχές της πόλης. Στη Νέα Υόρκη μπορεί να αγοράσει «έκσταση» για 33 δολάρια, ενώ συμφέρει να πουλήσει στο Μπρονξ για 53! Ο παίκτης μπορεί να συναναστραφεί με άτομα του υποκόσμου και να δανειστεί χρήματα με υψηλούς τόκους. Επίσης έχει τη δυνατότητα να αγοράσει όπλα. Στο μεταξύ, σε τακτά χρονικά διαστήματα δέχεται πληροφόρηση σχετικά με την τύχη κακοποιών ή άλλων προσώπων που συνδέονται με το λαθρεμπόριο. Συχνά τοκογλύφοι τον απειλούν αν δεν τους επιστρέψει τα δανεικά.

Η εταιρεία προειδοποιεί πριν από την έναρξη του παιχνιδιού: «Μην ξεχνάτε, είναι απλώς ένα παιχνίδι, μην το δοκιμάσετε στην πραγματικότητα

και μην κλέβετε». Παράλληλα, καλεί τα άτομα κάτω των 18 ετών να μην προχωρήσουν στο παιχνίδι. Ενήμερη για την ύπαρξη του συγκεκριμένου ηλεκτρονικού παιχνιδιού είναι η αστυνομία. Σύμφωνα με αξιωματικό της Ασφάλειας που ασχολείται με το ηλεκτρονικό έγκλημα, δεν υπάρχει τίποτα παράνομο στο παιχνίδι που να τους υποχρεώνει να επέμβουν. Σύμφωνα με τους νόμους της χώρας μας, αφού δεν πρόκειται για πραγματικό εμπόριο ναρκωτικών αλλά για παιχνίδι, από το οποίο δεν απειλείται η έννομη τάξη, δεν είναι δυνατή η αστυνομική παρέμβαση.

Σύμφωνα με τη Λάουρα Μαράτου, διδάκτορα κοινωνιολογίας και ερευνήτρια στο Εθνικό Κέντρο Κοινωνικών Ερευνών (ΕΚΚΕ), οι συνθήκες που διαμορφώνονται στη σύγχρονη κοινωνία της πληροφορίας, είναι τέτοιες που κάνουν τη στάση μας απέναντι στα υλικά αγαθά να αλλάζει με ραγδαίους ρυθμούς, ενώ γεννάνε συνέχεια νέες ανάγκες. «Αποτέλεσμα των τάσεων που επικρατούν, στο πλαίσιο του ευδαιμονισμού και τη μαζικότητα της επικοινωνίας, είναι η παραγωγή τέτοιων παιχνιδιών», λέει η κα Μαράτου και προσθέτει: «Ζούμε στην εποχή που ισοπεδώνονται καθημερινά οι παραδοσιακές αξίες. Η δημιουργία ενός τέτοιου παιχνιδιού δεν μας εκπλήσσει. Βλέπουμε όλο και πιο συχνά να μπαίνουν στη ζωή μας παιχνίδια που πριν μερικά χρόνια δεν θα μπορούσαμε να φανταστούμε την ύπαρξή τους».

Όσον αφορά στη δυνατότητα αρνητικής επιρροής ενός τέτοιου παιχνιδιού στην προσωπικότητα η κα Μαράτου λέει: «Είναι ένα παιχνίδι που μεταδίδει μηνύματα εξοικείωσης με τα ναρκωτικά και τον υπόκοσμο. Είναι ανησυχητικό. Ίσως να μην μπορεί να επηρεάσει άτομα που έχουν ήδη μια ολοκληρωμένη προσωπικότητα, αλλά οι νέοι ή κάποια άτομα που έχουν ανάλογους προβληματισμούς είναι πιο επιρρεπείς σε τέτοια μηνύματα. Άλλωστε είναι γεγονός ότι σήμερα οι νέοι αργούν περισσότερο από ό,τι παλιότερα να ενηλικιωθούν. Η διαμονή στο πατρικό σπίτι που παρατείνεται εξαιτίας των σπουδών ή της έλλειψης εργασίας καθυστερεί τη διαδικασία της ωρίμανσης».

Τέλος επισημαίνει ότι αφού είναι πρακτικά αδύνατο να υπάρξει δεοντολογικός ή άλλος έλεγχος σε παιχνίδια του Ιντερνετ, η μόνη λύση για να αποφεύγουν οι νέοι ανάλογες επιρροές και τέτοιου είδους ενδιαφέροντα είναι ο θετικός αντίκτυπος από τους ενήλικες. «Ούτε μπορεί να κλειδώσει κανείς τον υπολογιστή ούτε να ελέγχει το διαδίκτυο. Έγκειται στην ικανότητα του κάθε γονέα ή εκπαιδευτικού να πείθει τους νέους να αποφεύγουν τέτοιες προκλήσεις». [205]

9.4.9. Ο χάρτης του ελληνικού Internet

Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα αποτελέσματα έρευνας - μια από τις ελάχιστες έρευνες, που έχουν γίνει για την καταγραφή με συγκεκριμένα στοιχεία της χρήση του Internet στην Ελλάδα. Η έρευνα έγινε από την GfK Market Analysis, μέσω τηλεφωνικών συνεντεύξεων, από τις 11 έως τις 24 Νοεμβρίου 2003 σε αντιπροσωπευτικό πανελλαδικό δείγμα - συμπεριλαμβανομένων και των ημι-αστικών και αγροτικών περιοχών - 1.250 ατόμων (ανδρών και γυναικών ηλικίας από 18 έως 64 ετών).

Βάσει των στοιχείων που ανακοινώθηκαν η διάδοση του Internet παρουσίασε έντονους ρυθμούς αύξησης το 2002, σε σύγκριση με το 2001 στην Αθήνα, τη Θεσσαλονίκη και τις αστικές περιοχές, ενώ το 2003, φαίνεται να επικρατούν σταθεροποιητικές τάσεις.
Οι χρήστες του διαδικτύου νέοι ηλικίας **18-24** χρονών (50%), έχουν ανώτερη/ανώτατη μόρφωση (50%) και ανήκουν στα ανώτερα κοινωνικά στρώματα (53%). Αθήνα (38%) και Θεσσαλονίκη (42%) έχουν υψηλότερα ποσοστά χρήσης σε σύγκριση με την υπόλοιπη Ελλάδα.
Όσον αφορά τον τόπο χρήσης του Ιντερνετ, το 59% των χρηστών έχει πρόσβαση από το σπίτι του, το 30% από τον εργασιακό του χώρο, ενώ ακολουθούν τα Internet cafe και τα πανεπιστήμια με ποσοστά 5% και 7%

[205] Βλ.. στο http://www.ethnos.gr/pages/2002/feb/21/p020103.htm

αντίστοιχα. Ένα πολύ μικρό ποσοστό (2%) σερφάρει από συγγενικά ή φιλικά σπίτια.

Οι νέοι ηλικίας **18-24** και **25-29** χρονών προτιμούν το σπίτι σε ποσοστό 69% και 62% αντίστοιχα, όσοι έχουν ανώτερη/ανώτατη και μέση εκπαίδευση το χρησιμοποιούν περισσότερο στο σπίτι σε ποσοστό 60% και 62%, ενώ τα μεγαλύτερα ποσοστά χρήσης στα Internet cafe και τα πανεπιστήμια έχουν οι νέοι ηλικίας 18-24 χρονών, με 7% και 16% αντίστοιχα. Τέλος, στις αγροτικές περιοχές 6% των χρηστών επισκέπτεται το Ιντερνετ από συγγενικά ή φιλικά σπίτια.

Το 86% των χρηστών απάντησε ότι ο πιο σημαντικός λόγος που χρησιμοποιούν το Ιντερνετ είναι η ενημέρωση και η πλειάδα πληροφοριών που μπορεί κανείς να εντοπίσει για οποιοδήποτε θέμα χρειαστεί. Ο δεύτερος πιο σημαντικός λόγος (40%) είναι η ψυχαγωγία, ιδιαίτερα για τους νέους ηλικίας 18-24 χρονών, όπου το ποσοστό φτάνει το 55%. Ακολουθεί το ηλεκτρονικό ταχυδρομείο (e-mail) με ποσοστό 34%, ενώ φαίνεται ότι ο λόγος αυτός αφορά περισσότερο τους νέους ηλικίας 25-29 χρονών, αφού το ποσοστό φτάνει το 40%. Σε χαμηλότερα επίπεδα κυμαίνονται οι επαγγελματικοί λόγοι σύνδεσης (2%), η αναζήτηση προϊόντων (10%), καθώς και το downloading (5%). Όσον αφορά το ηλεκτρονικό εμπόριο (e-commerce), η πιο ενεργητική ομάδα είναι άτομα ηλικίας 45-54 χρονών με ποσοστό 16%.

Σύμφωνα με την έρευνα της *GfK Market Analysis*, 8% του δείγματος δήλωσε ότι προτίθεται να κάνει σύνδεση με το Ιντερνετ μέσα στον επόμενο χρόνο. Υψηλότερη τάση σύνδεσης έχουν οι νέοι ηλικίας 18-24 και 25-29 χρονών με ποσοστό 16% για κάθε ηλικιακή ομάδα, καθώς και όσοι ανήκουν στην ανώτερη και μεσαία κοινωνική τάξη, με ίδιο ποσοστό 9% ή έχουν μεσαία και ανώτερη/ανώτατη μόρφωση, με ποσοστό 11% για κάθε περίπτωση.[206]

206 Βλ., στο http://greece.flash.gr//soon/2004/2/4/25332id/

9.4.10. Οι πωλήσεις ναρκωτικών ουσιών μέσω του διαδικτύου θα είναι ο πονοκέφαλος τα επόμενα χρόνια για τις διωκτικές αρχές

Οι πωλήσεις ναρκωτικών ουσιών και ψυχοτρόπων φαρμάκων μέσω του διαδικτύου θα είναι ο πονοκέφαλος τα επόμενα χρόνια για τις διωκτικές αρχές, επισημαίνεται σε ετήσια έκθεση του Οργανισμού Ηνωμένων Εθνών για το 2003, η οποία παρουσιάστηκε σήμερα από το Κέντρο Θεραπείας Εξαρτημένων Ατόμων το οποίο είναι σύμβουλος του Οργανισμού για θέματα ναρκωτικών στη χώρα μας.

Οπως τονίστηκε, ορισμένες πρόσφατες κατασχέσεις φαρμακείων του διαδικτύου στις Ηνωμένες Πολιτείες απέδειξαν ότι το 90% των φαρμάκων που παραγγέλλονταν ήταν ουσίες, οι οποίες υπόκεινται σε διεθνή έλεγχο, καθώς οι περισσότερες από αυτές ήταν διεγερτικές ή κατασταλτικές.

Στην έκθεση τονίζεται ότι η διακίνηση των ουσιών αυτών μέσω του δικτύου είναι δύσκολο να ελεγχθεί καθώς ισχύουν διαφορετικές νομοθεσίες σε αρκετές χώρες του κόσμου για το θέμα, ενώ αναφερόμενη η έκθεση στα στοιχεία εγκληματικότητας που σχετίζονται με τη χρήση ναρκωτικών διεθνώς τονίζει ότι μόνο στη Βραζιλία έχουν χάσει τη ζωή τους 30.000 άνθρωποι σε δολοφονίες, που σχετίζονται με διακίνηση ναρκωτικών και το πιο θλιβερό είναι ότι πολλοί από αυτούς ήταν παιδιά.

Οι εκπρόσωποι του Κέντρου Εξαρτημένων Ατόμων τόνισαν ότι είναι καλό να συνεχιστούν τα προγράμματα απεξάρτησης αλλά και χορήγησης υποκατάστατων. [207]

9.4.11. Παραμονεύουν στο e-mail σας!

Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να βλάψουν την τσέπη, τον υπολογιστή ή απλά τα νεύρα σας!

---

[207] Βλ., στο http://news.pathfinder.gr/health/33765.html

Το ηλεκτρονικό ταχυδρομείο είναι ένα κυβερνό- «προνόμιο», ένας γρήγορος, οικονομικός και πρακτικός τρόπος επικοινωνίας. Όμως δεν είναι λίγες οι φορές που γίνεται από εκνευριστικό έως επικίνδυνο!

Το πιο πιθανό είναι ότι έχετε δει έστω μια από τις παρακάτω φράσεις σε μηνύματα ηλεκτρονικού ταχυδρομείου που λάβατε πρόσφατα -αν δεν βλέπετε μια από αυτές κάθε μέρα.

«Αποκτήστε αυτό το πρόγραμμα και πλοηγηθείτε στο διαδίκτυο με μεγαλύτερη ταχύτητα», «Αμυνθείτε απέναντι στα ζημιογόνα προγράμματα που μεταφέρονται με το ηλεκτρονικό ταχυδρομείο», «Υπάρχει κάποιο πρόβλημα με το λογαριασμό σας», «Αγαπητέ κύριε, είμαι πρώην πρόξενος μιας χώρας του εξωτερικού και χρειάζομαι τη βοήθειά σας για να μεταφέρω χρήματα στη χώρα για να μπορέσω να ζήσω».

Συνήθως τα μηνύματα αυτά φαίνονται ενδιαφέροντα, αλλά αν πάρετε τη ριψοκίνδυνη απόφαση να ακολουθήσετε τις συμβουλές που σας δίνουν εσείς ή (και) ο υπολογιστής σας πρέπει να είστε έτοιμοι να πληρώσετε το τίμημα.

Ένα μήνυμα με την πρώτη πρόταση στο θέμα του, θα σας δώσει κάποια ηλεκτρονική διεύθυνση από την οποία θα ανακτήσετε ένα διόλου χρήσιμο πρόγραμμα, το οποίο πιθανότατα θα επιβραδύνει την απόδοση του υπολογιστή σας, θα καταγράφει τις κινήσεις σας στο διαδίκτυο, ενώ θα μπορούσε να σας προκαλέσει και σημαντικά κενά ασφαλείας ή να σας προσφέρει απλόχερα ηλεκτρονικές διαφημίσεις.

Εγκαταστήστε το πρόγραμμα που σας προτείνει ένα μήνυμα με τίτλο τη δεύτερη φράση και θα καταλήξετε με μια ακόμα αποφώλια εφαρμογή. Θα μπορούσε να στέλνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου μέσω του δικού σας υπολογιστή. Θα μπορούσε να καταγράψει τους κωδικούς πρόσβασής σας σε υπηρεσίες ή τις πληροφορίες της πιστωτικής σας κάρτας. Ή απλά θα μπορούσε να παρακολουθεί τις κινήσεις σας στο διαδίκτυο.

Ένα μήνυμα με θέμα την τρίτη φράση είναι κλασικό παράδειγμα «ηλεκτρονικού μηνύματος απάτης» (phishing e-mail). Μοιάζει με ένα καθ' όλα νόμιμο μήνυμα από την τράπεζά σας, ή από την εταιρία που σας παρέχει την πιστωτική σας κάρτα, όμως ο ηλεκτρονικός σύνδεσμος που σας παραθέτει οδηγεί σε ένα δικτυακό τόπο που έχει κατασκευαστεί από κάποιον που θέλει να σας εξαπατήσει. Σκοπός είναι, εισερχόμενοι στον ιστοχώρο να πληκτρολογήσετε τον αριθμό της πιστωτικής σας κάρτας ή του τραπεζικού λογαριασμού, έτσι ώστε οι άνθρωποι πίσω από αυτή την ηλεκτρονική σελίδα να μπορέσουν να εκμεταλλευτούν τις πληροφορίες που τους δίνετε άθελά σας.

Όσο για τα χρήματα που μεταφέρονται από τη μια χώρα στην άλλη; Υπάρχουν εκατομμύρια παραλλαγές αυτού που ονομάζεται «Νιγηριανή απάτη 419». Το μόνο που θέλουν από σας είναι πληροφορίες για τον τραπεζικό σας λογαριασμό και θα σας δώσουν το 10% των χρημάτων, έτσι; Όχι. Θα αδειάσουν το λογαριασμό σας, ενώ έχουν καταγραφεί και περιπτώσεις απαγωγής εκείνων που πήραν την απόφαση να συναντήσουν πρόσωπο με πρόσωπο τον ηλεκτρονικό τους «συνέταιρο». Μπορεί να ακούγεται ανόητο, ή παρατραβηγμένο, όμως τα θύματα αυτής της απάτης απασχολούν μεγάλο μέρος των Αμερικανικών Μυστικών Υπηρεσιών, σύμφωνα με δημοσίευμα του PC Magazine.

Υπάρχει μόνο ένας τρόπος να ησυχάσετε μια και καλή από αυτού του είδους τα μηνύματα ηλεκτρονικού ταχυδρομείου: Να σταματήσετε να χρησιμοποιείτε το ηλεκτρονικό ταχυδρομείο! Για τους περισσότερους όμως μια τέτοια λύση δεν είναι μόνο ανέφικτη, είναι και ανεπιθύμητη.

Το επόμενο «στάδιο» είναι να εφαρμόσετε πρακτικές που θα μειώσουν τον αριθμό των ανεπιθύμητων ή και επικίνδυνων μηνυμάτων ηλεκτρονικού ταχυδρομείου που λαμβάνετε.

Μια εύκολη λύση είναι να χρησιμοποιείτε δύο ηλεκτρονικές διευθύνσεις: μία για να επικοινωνείτε με γνωστούς, φίλους και συγγενείς και μια δεύτερη την οποία θα χρησιμοποιείτε για να αποκτήσετε πρόσβαση σε

ιστοχώρους, για να γίνετε μέλη ηλεκτρονικών κοινοτήτων ή σε όποια άλλη περίπτωση ένα site που θεωρείτε «ύποπτο» σας το ζητήσει.

Το πιο πιθανό είναι ότι ο πρώτος λογαριασμός σας θα είναι αξιοσημείωτα πιο «καθαρός.

Πάντως, αν έχετε τον ίδιο λογαριασμό για χρόνια, ο πιο σίγουρος τρόπος για να σωθείτε από τον όγκο των ανεπιθύμητων μηνυμάτων που λαμβάνετε καθημερινά είναι να τον εγκαταλείψετε και να δημιουργήσετε ένα καινούργιο.

Σε δεύτερο στάδιο καλό θα ήταν να αποκτήσετε ένα σύστημα προστασίας από τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (anti-spam system). Το PC Magazine προτείνει το Cloudmark SafetyBar 4.0 και το Qube –το οποίο λειτουργεί μόνο με το πρόγραμμα διαχείρισης ηλεκτρονικού ταχυδρομείου Outlook.

Ηλεκτρονικές ...απάτες!

Πέρα όμως από τα ανεπιθύμητα ηλεκτρονικά μηνύματα, υπάρχουν και εκείνα που στόχο έχουν την πρόσβαση στον τραπεζικό σας λογαριασμό ή την πιστωτική σας κάρτα.

Τα μηνύματα αυτά –που, όπως και τα spam στέλνονται σε εκατομμύρια ημερησίως- στο θέμα τους συνήθως έχουν μια πρόταση όπως «Υπάρχει ένα πρόβλημα με το λογαριασμό σας», ενώ χρησιμοποιούν μεγάλα ονόματα, όπως CitiBank, Visa, PayPal και άλλα.

Μπορεί να δημιουργείται η εντύπωση ότι πολύ δύσκολα κάποιος θα «την πατούσε» από ένα τέτοιο μήνυμα. Και όμως: σύμφωνα με την Επιτροπή Ενάντια στην Ηλεκτρονική Απάτη, 5% των ανθρώπων που λαμβάνουν τέτοια μηνύματα ανταποκρίνεται.

Ο καλύτερος τρόπος για να αποφύγετε να συμπεριληφθείτε και εσείς σε αυτό το 5% είναι να ενημερωθείτε, να διαβάζετε προσεκτικά τα μηνύματα που αναφέρονται στα οικονομικά σας και να αποφεύγετε να δίνεται πληροφορίες για τον τραπεζικό σας λογαριασμό ή την πιστωτική σας κάρτα αν δεν εξακριβώσετε σε ποιο ηλεκτρονικό τόπο βρίσκεστε. Επίσης, όσο νόμιμο και αν δείχνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, αποφύγετε να κάνετε «κλικ» στον ηλεκτρονικό σύνδεσμο που περιέχει. Κάντε «αντιγραφή- επικόλληση» σε ένα φυλλομετρητή μόνοι σας.

Αν θέλετε να καταφύγετε σε ειδικά προγράμματα που θα σας βοηθήσουν να αναγνωρίζετε τα ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μπορείτε να ακολουθήσετε τις υποδείξεις τους PC Magazine. Ανάμεσα στα προγράμματα που προτείνει, το Cloudmark's SafetyBar 4.0, το SpamNet 3.0, το EarthLink, Netcraft Toolbar και το Webroot.

«Μας παρακολουθούν!»

Αν δεν έχετε λογισμικό προστασίας από τα προγράμματα που παρακολουθούν τις κινήσεις σας στο διαδίκτυο (spyware) και περνάτε χρόνο συνδεμένοι με τον παγκόσμιο ιστό, το πιο πιθανό είναι ότι ο υπολογιστής σας ασφυκτιά από το πλήθος των spyware!

Η επικινδυνότητα αυτών των προγραμμάτων έχει διαβαθμίσεις: μπορεί απλά να καταγράφουν τις ηλεκτρονικές σας προτιμήσεις, μπορεί να αποθηκεύουν κωδικούς ή άλλες πληροφορίες που πληκτρολογείτε, μπορεί να σας «σερβίρουν» διαφημίσεις (pop-ups) ή ακόμα και να «ψαχουλεύουν» το σύστημά σας για προσωπικές πληροφορίες.

Η απόκτηση λογισμικού για την προστασίας σας από αυτού του είδους των προγραμμάτων θεωρείται απαραίτητη. Οι προτάσεις Pc Magazine για

τον τομέα αυτό είναι το Spybot Search and Destroy, το Ad-Aware SE Plus 1.02 και το Sweeper 2.2.[208]

9.4.12. Ποινή φυλάκισης σε κυβερνόσφετεριστή

Ποινή φυλάκισης 30 μηνών επέβαλε ομοσπονδιακό δικαστήριο του Μανχάταν σε κυβερνοσφετεριστή ο οποίος παραποιούσε τα Domain names γνωστών ιστοσελίδων και οδηγούσε ανηλίκους ιστοσελίδες μα πορνογραφικό περιεχόμενο.

Συγκεκριμένα το δικαστήριο έκρινε ένοχο τον John Zuccarini, ο οποίος κατηγορούταν ότι παραποιούσε τα Domain names ιστοσελίδων όπως της Disneyland, της Britney Spears και των Teletubbies και οδηγούσε ανήλικους σε πορνογραφικές ιστοσελίδες.

Σύμφωνα με τον δικαστή ο Zuccarini με αυτό τον τρόπο κέρδισε περισσότερα από 1 εκατομμύριο δολάρια ετησίως.

Αξίζει να σημειωθεί πως κατά το παρελθόν ο εν λόγω κύριος έχει κατηγορηθεί περισσότερες από 100φορές από διάφορους οργανισμούς όπως ο Dow Jones και ο The National Association of Professional Baseball Leagues για παρόμοιες υποθέσεις.[209]

9.4.13. Τζόγος στον κυβερνοχώρο

Δυόμισι δις δολάρια άλλαξαν χέρια μέσα σε δύο βδομάδες κατά την διάρκεια του Εθνικού πρωταθλήματος μπάσκετ στις ΗΠΑ. Από αυτά μόνο 50 εκατ. δολ. ήταν νόμιμα στοιχήματα -- τα υπόλοιπα παράνομος τζόγος.

---

[208] Βλ., στο http://news.pathfinder.gr/periscopio/dangerous_inbox.html

[209] Βλ., στο http://tech.pathfinder.gr/tech/law/3873.html

Η βιομηχανία της τύχης είναι πολύ χρυσοφόρα επένδυση για να παραμείνει έξω από τον κυβερνοχώρο. Μια σειρά υπηρεσιών αναπτύχθηκαν στο Internet, έτσι ώστε κάθε άνθρωπος του πλανήτη να μπορεί να ... «επενδύσει» τα λεφτά του στον μαγικό άσο ή την μπίλια της ρουλέτας από το σπίτι του. Τα μόνα προαπαιτούμενα είναι ένα κομπιούτερ με μόντεμ και μια καλή πιστωτική κάρτα. Δεκάδες sites ξεπήδησαν τον τελευταίο χρόνο -- WEB σελίδες που υπόσχονται κέρδη, βιβλία με τεχνικές για να σαγηνεύσετε την τύχη, ή απλές σελίδες με τουριστικές πληροφορίες για τα πραγματικά καζίνο. Ο τζόγος διεθνοποιείται και γίνεται πολύ ... οικεία υπόθεση.

Εδώ όμως αρχίζουν τα προβλήματα. Ο online τζόγος είναι ημιπαράνομος. Σε μερικά μέρη του κόσμου (όπως στην Χαβάη) το κάθε μορφής τυχερά παίγνια -- ακόμη και τα κρατικά λαχεία -- απαγορεύονται. Τι γίνεται με τους κατοίκους αυτής της πολιτείας οι οποίοι ποντάρουν ηλεκτρονικά σε ρουλέτα που βρίσκεται στο Λας Βέγκας; Αν κάποιος προσαχθεί στο δικαστήριο ποιας πολιτείας το δίκαιο θα ισχύσει; Ο εισαγγελέας θα υποστηρίξει ότι αφού το υποκείμενο του νόμου βρίσκεται στην Χαβάη το έγκλημα τελέσθηκε εκεί και πρέπει να τιμωρηθεί. Η υπεράσπιση από την μεριά της θα ζητήσει αθώωση αφού η πράξη τελέσθηκε θεωρητικά στο Λας Βέγκας όπου επιτρέπεται ο τζόγος. Κατά συνέπεια δεν υπάρχει αδίκημα. Μύλος!

Υπόθεση τέτοια βεβαίως δεν υπάρχει ακόμη στα δικαστικά χρονικά οποιουδήποτε κράτους. Είναι όμως βέβαιο ότι πολύ σύντομα η "τυφλή θεά" θα κληθεί να λύσει αυτό το πρόβλημα.

Υπάρχει μετά και το ζήτημα της φορολογίας των κερδών. Αν κάποιος Έλληνας κερδίσει στο Ατλάντικ Σίτι ένα ποσό -- παίζοντας από το σπίτι του -- πρέπει να φορολογηθεί από την κυβέρνηση των ΗΠΑ, ή τον ημέτερο Αλέκο Παπαδόπουλο;

Το τρίτο και σημαντικότερο πρόβλημα αφορά τους ανήλικους. Αν και υπάρχουν διάφορες δικλείδες ασφαλείας, ο γκρουπιέρης του "οιονεί καζίνο"

δεν μπορεί ποτέ να είναι σίγουρος για το ποιος βρίσκεται στην άλλη άκρη της τηλεφωνικής γραμμής.

Νέοι καιροί λοιπόν, νέα προβλήματα. Αυτά όμως πρέπει να τα αντιμετωπίσει μια νέου είδους νομοθεσία που αυτή τη φορά δεν πρέπει να είναι τοπική. Αν π.χ. κάποιος (κατά την προσφιλή μέθοδο των Ελληνικών κυβερνήσεων) εκδώσει ένα διάταγμα που απαγορεύει τον online τζόγο, το μόνο που θα καταφέρει είναι να θεωρηθεί ηλίθιος στην παγκόσμια κοινότητα. Δεν υπάρχει τρόπος να ελεγχθεί τοπικά το πρόβλημα. Το Παγκόσμιο Χωρίο απαιτεί παγκοσμιότητα και στον τρόπο θεώρησης των προβλημάτων.[210]

9.4.14. Φοβούνται χάκερς και αντιγραφή

Τη **διαρροή** στο Διαδίκτυο μέρους του κώδικα των Windows γνωστοποίησε η εταιρία υπολογιστών Microsoft. Ωστόσο, παραμένει **άγνωστο** πόσο **μέρος** του κώδικα έχει διαρρεύσει και πόσοι απέκτησαν **πρόσβαση** σε αυτόν, όπως δήλωσε ο εκπρόσωπος της εταιρείας, Τομ Πίλα. Μάλιστα, ο κώδικας που διέρρευσε, προέρχεται από τα **Windows 2000** και τα **Windows NT**, δύο από τις εκδόσεις του συστήματος, που χρησιμοποιούνται από εκατομμύρια ανθρώπους σε όλο τον κόσμο. Η διαρροή αυτή είναι το **δεύτερο πλήγμα**, που δέχεται η αξιοπιστία της Microsoft. Την Τετάρτη, η εταιρία ανακοίνωσε "σοβαρό **ελάττωμα**" στις τελευταίες εκδόσεις του λειτουργικού συστήματος, Windows, που καθιστά το πρόγραμμα ευάλωτο στους χάκερς, οι οποίοι μπορούν να έχουν πρόσβαση στους υπολογιστές των χρηστών.

Η νέα διαρροή του λειτουργικού συστήματος της Microsoft προκαλεί ανησυχία για την **ασφάλεια** των υπολογιστών. Όπως υποστηρίζουν οι ειδικοί, **χάκερς** θα μπορούσαν να εκμεταλλευθούν τον κώδικα και να αποκτήσουν πρόσβαση σε εκατοντάδες εκατομμύρια ηλεκτρονικούς υπολογιστές σε όλο τον κόσμο, που χρησιμοποιούν τα Windows.

---

[210] Δημοσιεύτηκε στην εφημερίδα "Έθνος" στις 20.11.1995

Επίσης, ελλοχεύει ο κίνδυνος της **αντιγραφής**, αφού ορισμένες εταιρείες μπορούν να χρησιμοποιήσουν μέρη του κώδικα των Windows και να τα χρησιμοποιήσουν σε **παρόμοια προγράμματα**.

Πάντως, η εταιρεία δεν έχει εντοπίσει την πηγή της διαρροής, η οποία, σύμφωνα με τον κ. Πίλα, δεν οφείλεται στο δίκτυο της Microsoft, ενώ έρευνα διενεργούν οι αρμόδιες αρχές.

9.4.15. Τηλεχειρισμός των smam

"Δεν μπορεί να είσαι ένας αποτελεσματικός spamer αν δεν ελέγχεις εν αγνοία των χρηστών ένα εκτεταμένο δίκτυο υπολογιστών".[211]

Υπολογίζεται ότι τουλάχιστον **το ένα τρίτο όλων των spams** διαδίδονται μέσω των υπολογιστών, που χρησιμοποιούμε στο σπίτι μας. Το φαινόμενο είναι άκρως **ανησυχητικό** αν αναλογισθούμε ότι ο "ταπεινός" υπολογιστής, που έχουμε στο δωμάτιό μας μπορεί να μετατραπεί σ' ένα **σταθμό αναμετάδοσης spams** από ένα ή περισσότερους διαδικτυακούς ιούς. Οι **hackers**, έναντι αδράς αμοιβής, επινοούν ιούς, που **εντοπίζουν "ευπρόσβλητους" ηλεκτρονικούς υπολογιστές**, στους οποίους προσθέτουν σ' ένα δίκτυο PC, που μπορεί να ενεργοποιηθεί οποιαδήποτε στιγμή για την **εξάπλωση των spams**.

Η **επιστράτευση** των «αθώων» κατά άλλα ηλεκτρονικών υπολογιστών «οικιακής χρήσεως» άρχισε με τον **ιό Sobig**, που για πρώτη φορά εμφανίσθηκε τον Ιανουάριο του 2003 ενώ η τάση ενισχύθηκε με την εμφάνιση ιών όπως ο **Sinit**, ο **Fizzer** και ο **MyDoom**. Ειδικά ο τελευταίος καταφθάνει ως συνημμένο αρχείο και εάν ανοιχτεί στέλνει μηνύματα, που τον **πολλαπλασιάζουν** προς κάθε κατεύθυνση, επιτρέποντας παράλληλα την

---

[211] Τζόε Στίουαρτ, ερευνητής της εταιρείας Lurhq.

πρόσβαση στον υπολογιστή, που τον φιλοξενεί αφού **εγκαθίσταται** στο μηχάνημα και επιτρέπει τον **εξ αποστάσεως έλεγχο** του.

"Δεν μπορεί να είσαι **ένας αποτελεσματικός spamer** αν δεν **ελέγχεις** εν αγνοία των χρηστών ένα **εκτεταμένο δίκτυο υπολογιστών** ", υποστηρίζει στο BBC ο Τζόε Στίουαρτ, ερευνητής της εταιρείας Lurhq.

Safer Internet plus

Το πρόγραμμα της Κομισιόν, το οποίο θα υλοποιηθεί το διάστημα 2005 - 2008, θα βασιστεί στις δράσεις, που υλοποιούνται ήδη σε επίπεδο Ε.Ε, από το 1996, για την καταπολέμηση του παράνομου και επιβλαβούς περιεχομένου του Διαδικτύου. Το πρόγραμμα, που ονομάζεται **"Safer Internet plus"** περιλαμβάνει τέσσερις βασικούς άξονες:

Καταπολέμηση του παράνομου περιεχομένου: οι ανοικτές γραμμές επικοινωνίας αποτελούν μηχανισμούς αναφοράς, οι οποίες παρέχουν τη δυνατότητα στο κοινό να καταγγέλλει την ύπαρξη παράνομου περιεχόμενου. Στη συνέχεια μεταβιβάζουν τις καταγγελίες αυτές στον κατάλληλο οργανισμό για ανάληψη δράσης. Η Κομισιόν προτείνει τη χρηματοδότηση του συντονισμού του δικτύου καθώς και μεμονωμένων ανοικτών γραμμών επικοινωνίας .

Αντιμετώπιση ανεπιθύμητου και επιβλαβούς περιεχομένου: το πρόγραμμα θα εξασφαλίσει χρηματοδότηση για τεχνολογικά μέτρα, που αφενός παρέχουν στους χρήστες τη δυνατότητα να περιορίζουν το ανεπιθύμητο και επιβλαβές περιεχόμενο, που λαμβάνουν και αφετέρου αξιολογούν την αποτελεσματικότητα της διαθέσιμης τεχνολογίας φιλτραρίσματος. Θα διατεθεί επίσης χρηματοδότηση για την υποστήριξη της περαιτέρω ανάπτυξης αποτελεσματικής σχετικής τεχνολογίας καθώς και μέτρων για τη διευκόλυνση και τον συντονισμό ανταλλαγής πληροφοριών και βέλτιστης πρακτικής όσον αφορά αποτελεσματική επιβολή μέτρων κατά του φαινομένου "spam".

Προαγωγή ασφαλέστερου περιβάλλοντος: η Ε.Ε έχει υπογραμμίσει την υποστήριξή της υπέρ μιας προσέγγισης αυτορρύθμισης, που παρέχει ευελιξία και κατανοεί τις ανάγκες του εκάστοτε μέσου επικοινωνίας σε ένα πεδίο, που συνδυάζει την υψηλή τεχνολογία, την ταχεία μεταβολή και τη διασυνοριακή δραστηριότητα. Η Ευρωπαϊκή Επιτροπή θα συγκροτήσει πλατφόρμα για την ανταλλαγή απόψεων μεταξύ των εθνικών φορέων από κοινού ρύθμισης ή αυτορρύθμισης, ένα forum για το ασφαλέστερο Διαδίκτυο.

Ευαισθητοποίηση: η Κομισιόν προτείνει την υποστήριξη της συστηματικής ενημέρωσης σχετικά με την ασφαλέστερη χρήση του Διαδικτύου, ιδίως όσον αφορά εξατομικευμένες, διαλογικές και κινητές εφαρμογές, οι οποίες συνδέονται με άλλες κοινοτικές δράσεις αναφορικά με την εκπαίδευση στα μέσα επικοινωνίας και την εκμάθηση του Διαδικτύου. Η Επιτροπή θα επικεντρώσει τις προσπάθειές της στην ενίσχυση των χρηματοδοτικών μέσων, στην ενθάρρυνση των πολλαπλασιαστικών αποτελεσμάτων και στην ανταλλαγή βέλτιστης πρακτικής μέσω δικτύου[212].

9.4.16. Στη Βραζιλία διογκώνεται το διαδικτυακό έγκλημα

Σε παγκόσμιο κέντρο του διαδικτυακού εγκλήματος τείνει να εξελιχθεί η Βραζιλία, σύμφωνα με εκτιμήσεις ειδικών. Τον περασμένο χρόνο, οι δέκα πιο δραστήριες ομάδες βανδάλων του Ιντερνετ είχαν ως έδρα τους τη Βραζιλία, διαφημίζοντας τις ικανότητές τους με ονόματα όπως «Σπάμε την Ασφάλειά σας», «Εικονική Κόλαση» και «Καταστρέφοντας το Σύστημά σας». Μέσα στο 2003, πάνω από 96.000 επιθέσεις προήλθαν από τη Βραζιλία. Τα κενά στη νομοθεσία της Βραζιλίας σε ό,τι αφορά τα εγκλήματα του Διαδικτύου, καθώς και η κυβερνητική προτεραιότητα στην αντιμετώπιση της βίαιης εγκληματικότητας, που ταλανίζει τις μεγαλουπόλεις, έχουν αφήσει ουσιαστικά ατιμώρητους τους Βραζιλιάνους πειρατές του Ιντερνετ.

---

[212] Βλ., στο http://www.ert.gr/eidiseis/index_news.asp?id=35931

Πρωτοπόρος υπήρξε, ωστόσο, η αστυνομία του Σάο Πάολο, που ίδρυσε πρόσφατα Τμήμα Αντιμετώπισης Ηλεκτρονικού Εγκλήματος. Οι 20 αξιωματικοί που απασχολούνται στο τμήμα, οδήγησαν στη σύλληψη 40 απατεώνων τον τελευταίο μήνα. Οι προσπάθειες της ειδικής μονάδας, όμως, δυσχεραίνονται από την ξεπερασμένη νομοθεσία της χώρας. Σύμφωνα με νόμο του 1988, η αστυνομία δεν μπορεί να συλλάβει χάκερ για εισβολή σε ξένο δικτυακό χώρο ή για τη διάδοση ιού υπολογιστών, εάν δεν αποδείξουν ότι οι πράξεις του οδήγησαν στην τέλεση εγκλήματος. Ειδικοί του Ιντερνετ εκτιμούν ότι οι τράπεζες και οι μεγάλοι χρηματιστηριακοί οργανισμοί της Βραζιλίας φέρουν μέρος της ευθύνης, καθώς άργησαν χαρακτηριστικά να αντιληφθούν τους κινδύνους που παρουσιάζει η σύγχρονη δικτυωμένη και παγκόσμια οικονομία. Οι τολμηροί Βραζιλιάνοι χάκερ, μην έχοντας ουσιαστικά τίποτε να φοβηθούν από τον νόμο, προβαίνουν σε εντυπωσιακές και παράτολμες ενέργειες πειρατείας και κλοπής δεδομένων από το Διαδίκτυο, ενώ διακρίνονται για το πνεύμα συνεργασίας τους, προωθώντας μυστικούς κωδικούς και άλλες πληροφορίες στην κοινότητα των παρανόμων του Ιντερνετ[213].

9.4.17. Η Ευρωπαϊκή Επιτροπή υποστηρίζει ένθερμα τη δημιουργία μιας «Ευρωπαϊκής Συμμαχίας εναντία στην εμπορία της σεξουαλικής εκμετάλλευσης παιδιών μέσα από το Διαδίκτυο»

Ο Αντιπρόεδρος της Επιτροπής Μπαρό, αρμόδιος Επίτροπος για την Δικαιοσύνη, Ελευθερία και Ασφάλεια, εξέφρασε την ένθερμη υποστήριξή του για τα προχωρημένα σχέδια που αφορούν στη δημιουργία μιας τέτοιας Ευρωπαϊκής Συμμαχίας αρμοδίων φορέων, που παρουσίασαν η Ευρωπαϊκή ομοσπονδία για εξαφανισμένα και σεξουαλικώς κακοποιημένα παιδιά «Missing Children Europe» μαζί με άλλους φορείς σε συνέντευξη Τύπου που παραχώρησαν στις 6 Μαΐου, στις Βρυξέλλες.

Το 2007 σημειώθηκε 16,4% αύξηση στις καταγγελίες που δέχτηκε η Αγγλική ανοιχτή γραμμή καταγγελιών «Internet Watch Foundation» για

[213] Βλ., στο http://news.kathimerini.gr/4dcgi/_w_articles_world_1_28/10/2003_82139

εικόνες παιδικής κακοποίησης σε σχέση με την αντίστοιχη περίοδο του 2006. «Η εμπορία της σεξουαλικής εκμετάλλευσης παιδιών μέσα από το Διαδίκτυο είναι μια ταχέως αναπτυσσόμενη, χαμηλού ρίσκου και επικερδής δραστηριότητα. Η Συμμαχία θα διευκολύνει τη διεξαγωγή ορθώς συντονισμένων επιχειρήσεων των αστυνομικών αρχών και άλλου είδους συμπληρωματικές εξαρθρωτικές δράσεις εναντίον όσων επωφελούνται από τέτοιου είδους αποτρόπαια εγκλήματα. Θα συμβάλλει ιδιαίτερα στην προστασία των πιο ευάλωτων ανάμεσά μας, των παιδιών, στη δίωξη των θυτών καθώς και στην κατάσχεση εγκληματικού υλικού», δήλωσε ο Αντιπρόεδρος Μπαρό.

Η συμμαχία θα φέρει κοντά όλους τους φορείς που δραστηριοποιούνται στην καταπολέμηση την εμπορικής διανομής εικόνων παιδικής σεξουαλικής κακοποίησης στο Διαδίκτυο, ειδικότερα τις αρχές επιβολής του νόμου, τις μη κυβερνητικές οργανώσεις, τις τράπεζες, τις εταιρίες πιστωτικών καρτών και on-line πληρωμών, τους παρόχους υπηρεσιών Διαδικτύου και άλλους ιδιωτικούς φορείς που δραστηριοποιούνται στο Διαδίκτυο.

Σε αυτόν τον τομέα, η Επιτροπή συμβάλλει στη δημιουργία ενός μηχανισμού που θα εντοπίζει τις πληρωμές που πραγματοποιούνται μέσω πιστωτικής κάρτας ή ηλεκτρονικές πληρωμές για την αγορά εικόνων σεξουαλικής κακοποίησης παιδιών στο Διαδίκτυο, προσβλέποντας σε διακοπές συμβολαίων και πάγωμα κεφαλαίων, καθώς και στον εντοπισμό και τη δίωξη των εγκληματιών. Έχουν πραγματοποιηθεί αρκετές προπαρασκευαστικές συναντήσεις μεταξύ των βασικών εμπλεκόμενων φορέων και έχει συνταχθεί ένα προσχέδιο έγγραφο που ανακινεί το ζήτημα μιας πλατφόρμας για όλους τους εμπλεκόμενους (τράπεζες, εταιρίες

πιστωτικών καρτών και online πληρωμών, παρόχους υπηρεσιών Διαδικτύου και εθνικές αρχές).[214]

9.4.18. Πονοκέφαλος για τις ΗΠΑ η «κυβερνοτρομοκρατία»

Το FBI ανακοίνωσε ότι κατάφερε την παραμονή της Πρωτοχρονιάς να εμποδίσει όσους χάκερ προσπάθησαν να δημιουργήσουν "εορταστικά" προβλήματα παρεισφρέοντας σε διάφορα υπολογιστικά συστήματα και ηλεκτρονικά δίκτυα. Την Παρασκευή, ο Μπιλ Κλίντον αναμενόταν να ανακοινώσει μια σειρά μέτρων για την ενίσχυση των ειδικών υπηρεσιών αντιμετώπισης του ηλεκτρονικού εγκλήματος.

Ο Μάικλ Βέιτις, υπεύθυνος της σχετικής υπηρεσίας του FBI, δήλωσε ότι η πολυήμερη επιφυλακή απέδωσε καρπούς. Τα μέλη της υπηρεσίας κατάφεραν να αποτρέψουν 20 συνολικά τρομοκρατικές ενέργειες που είχαν προγραμματιστεί για την κρίσιμη στιγμή της αλλαγής του έτους. Από αυτές, οι έξι ήταν τυπικές περιπτώσεις ηλεκτρονικής παραβίασης υπολογιστικών συστημάτων και δικτύων εκ μέρους των λεγόμενων "χάκερ".

Σχετική είναι λοιπόν η πληροφορία που θέλει τον Πρόεδρο Κλίντον να ανακοινώνει την Παρασκευή το βράδυ την πρόθεσή του να εκχωρήσει από τον προϋπολογισμό του κράτους το ποσό των 2,03 δισεκατομμυρίων δολαρίων για την ενίσχυση των σχετικών υπηρεσιών, τη βελτίωση του τεχνολογικού τους εξοπλισμού και την επιμόρφωση των μελών τους.

Στο Λευκό Οίκο γνωρίζουν ότι η ενδεχόμενη επιτυχία ενός ηλεκτρονικού τρομοκρατικού χτυπήματος θα μπορούσε να προκαλέσει σημαντική ζημιά στην οικονομία της χώρας.

---

[214] Βλ., στο http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/696&format=HTML&aged=0&language=EN&guiLanguage=en

Οπως δήλωσε χαρακτηριστικά αξιωματούχος της κυβέρνησης που κράτησε την ανωνυμία του, "αφού ξεπεράσαμε το πρόβλημα του 2000, καιρός είναι να ξεπεράσουμε και την απειλή της κυβερνοτρομοκρατίας".[215]

[215] Βλ., στο http://www.in.gr/NEWS/article.asp?lngEntityID=314985

Κεφάλαιο 10ο - Προτάσεις & Συμπεράσματα

10.1. Πληροφορική παρέκκλιση ή πληροφορική άγνοια; Μερικές συμπερασματικές προτάσεις.

Λίγο πριν το τέλος αυτής της έρευνας, θα ήταν σίγουρα δύσκολο να πούμε πως καταφέραμε να εξαντλήσουμε τις προεκτάσεις ενός νέου κοινωνικά φαινομένου. Θα μπορούσαμε όμως να πούμε πως καταφέραμε να παρουσιάσουμε τις ολοένα και αυξανόμενες παρεκκλίνουσες πτυχές μέχρι σήμερα ώστε να μπορούμε να μιλάμε πραγματικά για ένα νέο κοινωνικό φαινόμενο.

Κατά μέσο όρο στον κόσμο διακινούνται ηλεκτρονικά πάνω από 3,5 δισεκατομμύρια δολάρια το λεπτό. Οι χρήστες είναι «εν δυνάμει» θύματα. Η θυματοποίηση των ανηλίκων από την έκθεση σε πορνογραφικό και παράνομο υλικό, είναι ευρεία, σύμφωνα με τις έρευνες παγκοσμίως Τα ποιοτικά χαρακτηριστικά αυτών των εγκλημάτων αυξάνουν τον κίνδυνο θυματοποίησης και μειώνουν τις πιθανότητες αποτελεσματικής πρόληψης και αντιμετώπισης. Οι δράστες αποκκλίνουν από το «παραδοσιακό» προφίλ των εγκληματιών, άρα δύσκολα εντοπίζονται και συλλαμβάνονται (σκοτεινός αριθμός).

Στην προσπάθεια μας να προτείνουμε μερικούς τρόπους αντιμετώπισης ενός κοινωνικού φαινομένου όπως αυτό της πληροφορικής παρέκκλισης θα λέγαμε πως οι ευθύνες αρχικά είναι πολλαπλές και ο κοινωνικός «ρόλος» του κάθε πολίτη ιδιαίτερα σημαντικός και χρήσιμος. Ένας ρόλος που θα μπορούσε να στηριχθεί αρχικά σε δύο επίπεδα:

Πρώτο, στη σωστή *χρήση της τεχνολογίας* ώστε να είναι ένα όπλο για τον εντοπισμό και εξουδετέρωση αυτού του προβλήματος όπου είναι τεχνικά δυνατό, και

Δεύτερο, *ενημέρωση και επιμόρφωση* των γονέων, εκπαιδευτικών και παιδιών τόσο όσο αφορά τη χρήση των νέων τεχνολογιών, του διαδικτύου, την καταπολέμηση φαινομένων σχετικά με την «άγνοια του νόμου»[216] αλλά επίσης και στην ανάπτυξη της σωστής διαδικτυακής κουλτούρας.

Η *ενημέρωση και επιμόρφωση* των εκπαιδευτικών θα μπορούσε να είναι αρχικά σε ένα γενικό επίπεδο με κάποια σεμινάρια διάρκειας για απόκτηση βασικών δεξιοτήτων πληροφορικής καθώς και εξειδικευμένα σεμινάρια που αφορούν την κάθε ειδικότητα ξεχωριστά με σκοπό την εφαρμογή της τεχνολογίας της πληροφορικής στη διαδικασία της μάθησης.

Η ενημέρωση των μαθητών θα περιελάμβανε στην πρώτη τάξη του γυμνασίου θέματα που να αφορούν:

- Προστασία από ιούς, spyware / adware
- Πνευματική ιδιοκτησία και παράνομη χρήση περιεχομένου και προγραμμάτων
- Προστασία Προσωπικών δεδομένων
- Συνομιλίες πραγματικού χρόνου (chat) και οι κίνδυνοι που περιέχουν.

Στην δεύτερη τάξη θα μπορούσαν να διδάσκονται θέματα για τη χρήση του ηλεκτρονικού ταχυδρομείου με αναφορά σε θέματα

- spam mail και viruses

Επίσης η χρήση του διαδικτύου θα πρέπει να γίνεται σε όλα τα μαθήματα πληροφορικής που διδάσκονται τόσο στο γυμνάσιο όσο και στο Λύκειο είτε σαν μέρος του αναλυτικού προγράμματος είτε σε μορφή εργασιών. Παράλληλα ιδιαίτερη έμφαση θα πρέπει να δίνεται στην αξιολόγηση της πληροφορίας ώστε ο μαθητής να μην παίρνει σαν δεδομένο

[216] Βλ., A. Manganas, *L' erreur de droit comme defense en droit penal Canadien. Quebec:* Universite Laval, 1982 στο Μαγγανά Δ. Αντώνη – Λάζου Γρηγόρη «Ο ποινικός Κώδικας για τον Πολίτη: Μια επιλογή παραδειγμάτων», 1998 Αθήνα. Εκδόσεις Παπαζήση

ότι υπάρχει καταγραμμένο στο διαδίκτυο αλλά να είναι σε θέση να αξιολογεί τις πηγές και την αξιοπιστία της πληροφορίας. Τέλος η εργασία στο διαδίκτυο του σχολείου θα πρέπει να γίνεται κάτω από την επίβλεψη του εκπαιδευτικού ακολουθώντας συγκεκριμένες οδηγίες.

Από την άλλη πλευρά η απαγόρευση χρήσης για αποφυγή των προβλημάτων δεν είναι λύση. Γι αυτό το λόγο οι γονείς θα πρέπει να επιμορφωθούν ώστε να κατανοήσουν τόσο τις δυνατότητες όσο και τους κινδύνους του διαδικτύου δημιουργώντας έτσι καλύτερες συνθήκες επικοινωνίας με τα παιδιά.

Το θεσμικό πλαίσιο προστασίας ανηλίκων φαίνεται να έχει πλούσια δράση σε διεθνές, ευρωπαϊκό και εθνικό πλαίσιο για την αναγκαιότητα και τις πρακτικές της προστασίας των ανηλίκων. Ένα καλό παραδείγματα καλών πρακτικών σε παιδαγωγικό-κοινωνικό επίπεδο είναι για παράδειγμα η Σουηδία. Στα σχολεία τους προστέθηκε για το εκπαιδευτικό έτος 2006 βιβλίο σχετικά με την ασφάλεια του internet. Επίσης καθιερώθηκε ημέρα ασφαλούς περιήγησης στο internet και δημιουργήθηκε *comic book* σχετικά με την ασφάλεια για χρήση από τους δασκάλους στα σχολεία. Τέλος διεξήχθεισαν σεμινάρια σε εκπαιδευτικούς με επίδειξη χρήσης από τα παιδιά.

Μερικά από τα βήματα που μπορεί η πολιτεία να πραγματοποιήσει για την καταπολέμηση του πληροφορικού εγκλήματος είναι η ενημέρωση των χρηστών του γενικού πληθυσμού, η ανάπτυξη τεχνολογικής προστασίας αξιοποιήσιμη από όλους, η δημιουργία εκπαιδευτικών προγραμμάτων ενημέρωσης και ευαισθητοποίησης της οικογένειας, των σχολικών συμβούλων κ.α. για τους κινδύνους των ανηλίκων χρηστών, η. ενδυνάμωση και επέκταση όλων των σχετικών δράσεων των μη κυβερνητικών οργανώσεων (π.χ. Web Police) καθώς και η συνεργασία, συνέργεια, συντονισμός όλων των φορέων που εμπλέκονται αντίστοιχα. Τέλος η συνεχής ενημέρωση κοινού, γονέων, διδασκάλων, χρηστών διαδικτύου, η παρακολούθηση των τεχνολογικών εξελίξεων, ο εκσυγχρονισμός της νομοθεσίας σε συνεργασία με τον συνεχή

εκσυγχρονισμό των διωκτικών αρχών, η αξιοποίηση της διεθνούς εμπειρίας και εθνικής τεχνογνωσίας και η συνεργασία των τοπικών φορέων θα δημιουργήσουν νέες προϋποθέσεις για την μείωση της πληροφορικής εγκληματικότητας.

Συνοψίζοντας θα λέγαμε πως οι νέες μορφές θυματοποίησης ανηλίκων και μη, απαιτούν νέες παρεμβάσεις πρόληψης, πέραν των παραδοσιακών ποινικών μέτρων[217]. Στόχος είναι η μείωση του κινδύνου θυματοποίησης, η εναρμόνιση της ποινικής νομοθεσίας σε διεθνές επίπεδο ενώ η γενική πρόληψη και ευαισθητοποίηση είναι πιο αποτελεσματικές στρατηγικές από τις όποιες αντίστοιχες κατασταλτικές.

Προσβλέπουμε λοιπόν σε ένα ασφαλέστερο διαδίκτυο, το οποίο θα αποτελέσει το νέο περιβάλλον μέσα στο οποίο οι γονείς, τα παιδιά και η κοινωνία εν γένει, θα μαθαίνουν, θα ψυχαγωγούνται και θα επικοινωνούν με ασφάλεια.

Ακολουθούν κάποιες προτάσεις – σκέψεις για την προστασία των πολιτών από την αυξημένη εγκληματικότητα στο διαδίκτυο. Έτσι στις επόμενες παραγράφους θα δούμε συγκεκριμένα τρόπους προστασίας από παρενοχλήσεις δίνοντας κάποιες συμβουλές στους γονείς και τους νέους, προστασία από κακόβουλο λογισμικό, προστασία από το Spam, συμβουλές για τους χρήστες Αυτόματων Τραπεζικών Μηχανών (Α.Τ.Μ.), συμβουλές για ασφαλείς οικονομικές συναλλαγές και τρόπους προστασίας κατά την περιήγηση στο Διαδίκτυο.

[217] Βλ., ΑΡΤΙΝΟΠΟΥΛΟΥ ΒΑΣΩ. Αν. Καθηγήτρια Παντείου Πανεπιστημίου. Ημερίδα ICT Forum: «Ηλεκτρονικό Έγκλημα και Θυματοποίηση», Αθήνα 29/10/2007

10.2. Προστασία κατά την περιήγηση στο Διαδίκτυο

Α) <u>Συμβουλές για τους Γονείς</u>

- Προτιμήστε να τοποθετήσετε τον Η/Υ σας σε χώρους, όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.
- Κάντε την πλοήγηση στο Διαδίκτυο μία οικογενειακή δραστηριότητα. Χρησιμοποιείστε τον Η/Υ μαζί με τα παιδιά σας.
- Ενημερώστε τα παιδιά σας για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chatrooms.
- Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.
- Διδάξτε τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ακόμα και ωράρια σχολείου ονόματα φίλων κ.λπ.) και να μην χρησιμοποιούν την κάρτα σας.
- Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου.
- Διδάξτε τα επίσης, να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν, μπορεί να είναι επικίνδυνοι.
- Χρησιμοποιείστε τα λεγόμενα «φίλτρα» που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητές σελίδες (βία, πορνογραφία).
- Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.α., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.

- Ενημερωθείτε σχετικά με τις αρμόδιες αρχές, που θα πρέπει να επικοινωνήσετε σε περίπτωση που συναντήσετε βλαβερό ή παράνομο περιεχόμενο στο Internet.

Β) <u>Για νέους</u>

- Μη δίνετε σε κανέναν, ακόμα και στον καλύτερό σας φίλο, τον κωδικό πρόσβασης στο Διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τον κωδικό είναι οι γονείς σας.
- Μην απαντάτε σε ηλεκτρονικά μηνύματα που σας κάνουν να αισθάνεστε «άβολα». Σε περίπτωση που λάβετε ένα τέτοιο μήνυμα, μη διστάσετε να το πείτε στους γονείς σας ή σε κάποιο πρόσωπο που εμπιστεύεστε.
- Αν αισθανθείτε άβολα την ώρα που συνομιλείτε μέσω chatroom, διακόψτε αμέσως τη συνομιλία.
- Αποφύγετε να στέλνετε τη φωτογραφία σας και τα προσωπικά στοιχεία σας μέσω Διαδικτύου σε άγνωστο.
- Σκεφτείτε πολύ καλά πριν αποφασίσετε να συναντηθείτε με κάποιο άτομο που γνωρίσατε στο Διαδίκτυο. Ζητείστε την άποψη των γονιών σας σχετικά με αυτό το θέμα.
- Σε περίπτωση που αποφασίσετε να συναντηθείτε με το «διαδικτυακό σας φίλο», ενημερώστε τους γονείς σας ή κάποιο άτομο που εμπιστεύεστε και φροντίστε αυτή η συνάντηση να γίνει σε δημόσιο χώρο.
- Αναπτύξτε κριτική διάθεση σε ό,τι διαβάζετε στο Διαδίκτυο. Μην εμπιστεύεστε αμέσως ότι δείτε.
- Μιλήστε στους γονείς σας για τα όσα βλέπετε και ζείτε όταν «σερφάρετε» στο Internet.

10.3. Συμβουλές για ασφαλείς οικονομικές συναλλαγές

Α) <u>Βασικές Οδηγίες</u>

1. Αποφεύγετε να πραγματοποιείτε οικονομικές συναλλαγές μέσω Διαδικτύου από Internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές . Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας.
2. Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείτε για τις διαδικτυακές συναλλαγές:

- Αλλάζετε συχνά τους κωδικούς πρόσβασης και πάντα στην περίπτωση που υποψιάζεστε ότι έχουν εκτεθεί.
- Αποφεύγετε να χρησιμοποιείτε ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να βρεθούν και από άλλα έγγραφα
- Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες. Σε περίπτωση απώλειας ή κλοπής τους θα διευκολύνετε πολύ τους δράστες.
- Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια κάρτες σας.
- Μην δίνετε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.

3. Επικοινωνήστε με την τράπεζά σας αν νομίζετε ότι κάποιος γνωρίζει τον κωδικό σας πρόσβασης στην υπηρεσία Internet banking.

4. Απενεργοποιήστε τη λειτουργία «Αυτόματης Καταχώρησης» του προγράμματος περιήγησης. Η λειτουργία αυτή αποθηκεύει τους κωδικούς σας στον υπολογιστή, γεγονός που τους καθιστά έκθετους.

5. Κάνετε αγορές μόνο από γνωστές εταιρείες που σας παρέχουν εγγυήσεις ασφάλειας. Αν κάνετε συχνά αγορές από το Διαδίκτυο, χρησιμοποιείτε μια κάρτα, αποκλειστικά για αυτή τη χρήση. Έτσι, αν πέσετε θύμα απάτης δεν θα χρειαστεί να ακυρώσετε όλες τις κάρτες σας.

6. Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας.

Ειδικότερα:

- Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιήστε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοση του.
- Εγκαταστήστε ένα πρόγραμμα προστασίας από τους ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχτείτε κατά τις περιηγήσεις σας στο διαδίκτυο.
- Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

7. Αν είστε χρήστες ηλεκτρονικού ταχυδρομείου (e-mails):

- Μην ανοίγετε τα ηλεκτρονικά μηνύματα (e-mails) για την προέλευση ή τον αποστολέα των οποίων δεν είστε βέβαιοι. Ιδιαίτερα επικίνδυνα είναι τα ηλεκτρονικά μηνύματα άγνωστης προέλευσης που περιέχουν συνημμένα αρχεία με κατάληξη .exe, .pif, ή .vbs. Επίσης, θα πρέπει να

γνωρίζετε ότι ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές που υπάρχουν στο βιβλίο διευθύνσεων του υπολογιστή. Αυτό σημαίνει ότι το ηλεκτρονικό μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό σας.

- Μην απαντάτε σε ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά σας στοιχεία. Επίσης, μην στέλνετε ποτέ προσωπικά σας στοιχεία ή στοιχεία των συναλλαγών σας μέσω μίας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail). Είναι εύκολη η υποκλοπή των στοιχείων από τρίτα, μη εξουσιοδοτημένα άτομα.

8. Να ενημερώνεστε για τους λογαριασμούς σας και να φροντίζετε για την ασφάλεια των προσωπικών σας στοιχείων και εγγράφων.

Ειδικότερα:

- Ελέγχετε τακτικά τους τραπεζικούς σας λογαριασμούς και τους λογαριασμούς των πιστωτικών καρτών σας για οποιαδήποτε ασυνήθιστη συναλλαγή ή ανάληψη και ειδοποιήστε αμέσως την τράπεζα σε περίπτωση που διαπιστώσετε οποιαδήποτε διαφορά.
- Φροντίστε να καταστρέφετε όσα έγγραφα δεν σας χρειάζονται πλέον, όπως οι πιστωτικές και τραπεζικές κάρτες που ακυρώνετε, τα αντίγραφα των λογαριασμών σας ακόμα και τις αποδείξεις που λαμβάνετε από τα Α.Τ.Μ.

10.4. Συμβουλές για τους χρήστες Αυτόματων Τραπεζικών Μηχανών (Α.Τ.Μ.)

Α) <u>Ως προς τον τρόπο χρήσης των Α.Τ.Μ.</u>

- Πριν ξεκινήσετε τη συναλλαγή ελέγξτε προσεκτικά το χώρο γύρω σας για τυχόν ύποπτες κινήσεις.
- Βεβαιωθείτε ότι στο χώρο που βρίσκεται το Α.Τ.Μ. δεν υπάρχει κάποιο πρόσθετο εξάρτημα, του οποίου η παρουσία δεν δικαιολογείται.

- Εάν εντοπίσετε οποιοδήποτε ύποπτο αντικείμενο, αλλοιώσεις ή σημάδια στη σχισμή υποδοχής της κάρτας, όπως στρεβλωμένο πλαίσιο, εκδορές, επιπλέον εξαρτήματα, τρύπες κ.λ.π. αποφύγετε να χρησιμοποιήσετε το συγκεκριμένο Α.Τ.Μ. Ειδοποιήστε αμέσως την Τράπεζα.
- Σε περίπτωση που το Α.Τ.Μ. κρατήσει την κάρτα ή αντιμετωπίσετε οποιοδήποτε προβλήματος κατά τη συναλλαγή, επικοινωνήστε μόνο με την Τράπεζα που σας χορήγησε την κάρτα.
- Μην εμπιστεύεστε αγνώστους που προθυμοποιούνται να σας βοηθήσουν στο χειρισμό του Α.Τ.Μ. ή ζητούν το PIN της κάρτας σας.
- Σε περίπτωση που το μηχάνημα παρουσιάσει οποιαδήποτε βλάβη, επικοινωνήστε μόνο με τα τηλέφωνα της Τράπεζας.
- Όταν πληκτρολογείτε τον κωδικό σας PIN «προστατέψτε» το πληκτρολόγιο, ώστε κανείς γύρω σας να μην αντιληφθεί τον τετραψήφιο αριθμό.
- Μετά την ολοκλήρωση της ανάληψης χρημάτων μετρήστε τα χρήματα με διακριτικότητα και όσο πιο σύντομα μπορείτε.
- Φροντίστε να μην είστε μόνοι σας, αν χρειαστεί να χρησιμοποιήστε Α.Τ.Μ. κατά τη διάρκεια της νύχτας και σε μη πολυσύχναστες περιοχές.
- Εάν χρησιμοποιείτε Α.Τ.Μ. που βρίσκεται σε ειδικό θάλαμο, μην επιτρέπετε σε άτομα που δεν γνωρίζετε να εισέλθουν στο χώρο, κατά τη διάρκεια της συναλλαγής.
- Μην αφήνετε τα κλειδιά σας ή πολύτιμα αντικείμενα στο αυτοκίνητό σας, ενώ χρησιμοποιείτε Α.Τ.Μ. και μην αφήνετε τη μηχανή του αυτοκινήτου σας αναμμένη.

Β) Για την προστασία του λογαριασμού σας

- Αποφεύγετε να χρησιμοποιείτε ως κωδικό (PIN) την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία που μπορεί να γίνουν εύκολα αντιληπτά από επιτήδειους.
- Αποφεύγετε να γράφετε το PIN οπουδήποτε.
- Αποφεύγετε να χρησιμοποιείτε το ίδιο PIN σε περισσότερες από μια κάρτες σας.
- Επιλέξτε και απομνημονεύστε τον κωδικό PIN που μόνο εσείς θα γνωρίζετε και που δεν θα μπορεί να προσδιορισθεί από προσωπικά σας αντικείμενα που υπάρχουν στο πορτοφόλι ή στη τσάντα σας.
- Μην δίνετε τον κωδικό σας PIN σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεσθεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό του PIN για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.
- Μην αφήνετε ποτέ την απόδειξη συναλλαγής που έχει εκδώσει το Α.Τ.Μ.
- Συγκρίνετε τις αποδείξεις ανάληψης χρημάτων του Α.Τ.Μ. με το μηνιαίο ενημερωτικό δελτίο κίνησης του λογαριασμού σας. Εάν παρατηρήσετε οποιαδήποτε συναλλαγή που δεν έχετε πραγματοποιήσει ενημερώστε αμέσως την Τράπεζα.
- Να υπογράφετε την κάρτα σας. Αυτό εμποδίζει τον οποιοδήποτε να παραποιήσει το όνομά σας πάνω σε αυτήν.
- Μη δίνετε και μη δανείζετε ποτέ και σε κανέναν την κάρτα σας.
- Όταν κυκλοφορείτε έχετε μαζί σας μόνο τις κάρτες που προτίθεστε να χρησιμοποιήσετε.

- Αναφέρατε αμέσως την κλοπή ή την απώλεια κάρτας στην Τράπεζα και στην Αστυνομία.[218]

10.5. Προστασία από το Spam

- Να μην απαντάτε ποτέ σ' ένα spam e-mail και να μην κάνετε πουθενά κλικ, γιατί απλούστατα η απάντησή σας ή και η άρνησή σας θα επιβεβαιώσει την εγκυρότητα του δικού σας e-mail και έτσι το e-mail σας θα γίνει μια πολύτιμη πληροφορία για πολλούς spammers.
- Να έχετε μια πρόχειρη και μη συχνά χρησιμοποιούμενη ηλεκτρονική διεύθυνση, εκτός φυσικά από την κανονική, και να την δίνετε σε πρώτη ζήτηση έτσι ώστε να πηγαίνουν εκεί όλα τα ανεπιθύμητα e-mails.
- Αναζητήστε και εγκαταστήστε ειδικά προγράμματα και φίλτρα που μπλοκάρουν τα spam e-mails. Να ελέγχετε πάντα αν αυτά τα προγράμματα-φίλτρα κάνουν σωστά το μπλοκάρισμα των spam e-mails.
- Να μην κάνετε ποτέ προώθηση (forward) των spam e-mails σε φίλους ή και τρίτους, γιατί κι αυτοί θα προστεθούν στην λίστα αποδοχής.
- Να μην παρασύρεστε ποτέ από δελεαστικούς τίτλους, όπως a very special message for you, earn money easily, urgent and confidential κ.ά.
- Να μην δημοσιεύεται την διεύθυνση του ηλεκτρονικού ταχυδρομείου (e-mail). Η ύπαρξη της ηλεκτρονικής διεύθυνσης σε μια ιστοσελίδα, είναι σχεδόν σίγουρο ότι σύντομα θα φέρει πολλά μηνύματα spam στο γραμματοκιβώτιο σας.
- Να μην δίνετε εύκολα την διεύθυνση του ηλεκτρονικού ταχυδρομείου (e-mail). Πρέπει να είστε προσεκτικοί όταν επισκεπτόσαστε διάφορους δικτυακούς τόπους και ζητείται η συμπλήρωση προσωπικών στοιχείων

[218] Βλ., στο www.vdt.gr

και στοιχείων επικοινωνίας, όπως είναι το e-mail. Θα πρέπει να διαβάσετε προσεκτικά τους όρους χρήσης και την πολιτική εχεμύθειας για την οποία δεσμεύεται ο δημιουργός της ιστοσελίδας.

- Να μην απαντάμε ποτέ στα spam e-mails ακόμα και στην υποτιθέμενη ένδειξη διαγραφής, γιατί έτσι διαπιστώνεται η εγκυρότητα της ηλεκτρονικής μας διεύθυνσης και επομένως θα αποτελούμε πολύτιμο στόχο για τους spammers.
- Να χρησιμοποιείται ειδικά προγράμματα-φίλτρα.219

10.6. Προστασία από κακόβουλο λογισμικό

- Επιλογή ενός καλού antivirus προγράμματος
- Συνεχής ανανέωση (update) του antivirus και τακτική ανίχνευση όλου του δίσκου
- Έλεγχος κάθε δισκέτας/cd με το antivirus πριν την ανοίξετε
- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε cd ή δισκέτα
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας.
- Αν χρησιμοποιείτε IRC chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
- Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.

---

[219] Βλ., στο http://dide.flo.sch.gr/Plinet/plinet.html

- Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
- Διατήρηση της ανωνυμίας σας με την ενημέρωση του φυλλομετρητή που χρησιμοποιείτε. Προτιμήστε πάντα την πιο πρόσφατη έκδοση και φυσικά φροντίστε να την ενημερώνετε τακτικά. Στον Internet Explorer, για να απενεργοποιήσετε τα «third party cookies» (τα cookies που «φυτεύονται» στο σύστημα όχι από τα sites που επισκέπτεστε αλλά από τριτογενείς φορείς)
- Σωστή ρύθμιση των δικτυακών εφαρμογών. Οι περισσότεροι φυλλομετρητές διαθέτουν ρυθμίσεις ασφαλείας που καθορίζουν ποια πρόσθετα μπορούν να «εκτελεστούν», ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies.
- Αν χρησιμοποιείτε instant messengers, να αποφεύγετε να συνομιλείτε με ξένους[220].

10.7. Προστασία από παρενοχλήσεις

- Επιλέξτε ένα ουδέτερο όνομα χρήστη, e-mail κλπ. Αποφύγετε οτιδήποτε χαριτωμένο, σεξουαλικό, ή γυναικείο.
- Διατηρείστε τη βασική σας διεύθυνση ηλεκτρονικού ταχυδρομείου μυστική. Να την χρησιμοποιείται μόνο με ανθρώπους που γνωρίζετε και εμπιστεύεστε.
- Δημιουργείστε ένα ελεύθερο λογαριασμό ηλεκτρονικής αλληλογραφίας τον οποίο να χρησιμοποιείται στις on-line δραστηριότητές σας.
- Μην δίνεται προσωπικές σας πληροφορίες απλά επειδή τις ζητάνε. Πολλοί δικτυακοί τόποι ζητάνε να δώσετε το πλήρες όνομά σας,

[220] Βλ., στο www.kathimerini.gr

ημερομηνία γέννησης, διεύθυνση, αριθμό τηλεφώνου, e-mail, κ.α. Δώστε όσο το δυνατόν λιγότερες πληροφορίες.

- Όταν συνομιλείτε σε ένα chat room, να αποκλείεται χρήστες που σας ενοχλούν ρυθμίζοντας τους παραμέτρους του προγράμματος συνομιλίας που χρησιμοποιείται.
- Μην επιτρέπεται στους άλλους να δημιουργούν συγκρούσεις μαζί σας. Είναι προτιμότερο να μην ανοίγετε διάλογο με κάποιον που σας επιτίθεται και να τον αγνοείται. Όταν αντιληφθεί ότι δεν αντιδράτε θα αναζητήσει άλλο στόχο.
- Πριν συμμετάσχετε σε οποιαδήποτε on-line δραστηριότητα, παρακολοθείστε για αρκετό χρονικό διάστημα το περιεχόμενο των συζητήσεων.
- Εάν χρειαστεί να αλλάξετε το όνομα χρήστη για να αποφύγετε κάποιον που σας παρενοχλεί, να φροντίσετε ώστε το νέο όνομα που θα διαλέξετε να μην έχει καμιά σχέση με αυτό που χρησιμοποιούσατε.
- Ποτέ μην χρησιμοποιείτε τα στοιχεία της εταιρείας που εργάζεστε (διεύθυνση, τηλέφωνο κλπ.) σε μια δημόσια συζήτηση στο διαδίκτυο.
- Ποτέ μην δίνετε το κωδικό πρόσβασης σε κανέναν.[221]

Σύνοψη

Όπως είδαμε, το Διαδίκτυο όσες ευκολίες και ευκαιρίες μπορεί να παρουσιάζει για την ζωή και την επικοινωνία των ανθρώπων, όσο πιο εύχρηστη μπορεί να κάνει τη ζωή μας, οι κίνδυνοι που ελλοχεύουν από μια απρόσεχτη ή και απερίσκεπτη κίνηση από εμάς τους ίδιους μπορεί να οδηγήσει σε ανεπιθύμητα αποτελέσματα. Η πρόληψη της εγκληματικής δράσης μπορεί να επιτευχθεί καλύτερα από τους ίδιους τους χρήστες κυρίως

---

[221] Βλ., στο http://www.haltabuse.org/resources/online.shtml

με την προσοχή που πρέπει να δείχνουν για την κάθε κίνηση τους στο χώρο του Διαδικτύου ώστε να μη δώσουν δικαιώματα να προσβάλλουν τις ατομικές τους ελευθερίες αλλά και να μη δώσουν το χώρο να προσβληθεί μία αθώα παιδική ψυχή.

Η ενημέρωση των γονιών αλλά και όλων των ανθρώπων που ζουν και κινούνται με γνώμονα τη χρήση των υπολογιστών και του Ιστοχώρου, ίσως τελικά να είναι και η μόνη λύση για την αντιμετώπιση της νέας μάστιγας που έχει ήδη εμφανιστεί στα κοινωνικά δρώμενα καθώς όλο και πιο συχνά, θα μπορούσαμε να πούμε καθημερινά, υπάρχουν καταγγελίες για φαινόμενα παιδικής πορνογραφίας στο Διαδίκτυο.

Επίλογος

Στην «Πολιτεία» ο Πλάτωνας θέτει ένα θεμελιώδες ερώτημα για την ηθική των μελών μιας ευνομούμενης κοινωνίας: «Έστω ότι έχετε ένα δαχτυλίδι που, όταν γυρνάτε μια πέτρα του, σας καθιστά αόρατους. Για ποιο σκοπό τότε θα έπρεπε να πράττετε δίκαια;». Στους καιρούς μας, στην εποχή της παγκοσμιοποίησης και της Κοινωνίας της Πληροφορίας, το ίδιο διαχρονικό ζήτημα ηθικής καθίσταται ιδιαίτερα επίκαιρο. Ποιες είναι άραγε οι δεοντολογικές αρχές του σύγχρονου ανθρώπου που, με τη βοήθεια των μέσων των Τεχνολογιών της Πληροφορίας και Επικοινωνίας (ΤΠΕ), θεωρεί ότι καθίσταται «αόρατος», αποκτά ελευθερίες να κινείται ανεξέλεγκτα στο Διαδίκτυο (Internet) και νομίζοντας ότι διατηρεί τη ανωνυμία του περιηγείται στις «λεωφόρους» του κυβερνοχώρου (cyberspace), έχοντας πρόσβαση στις ανεξάντλητες πηγές πληροφοριών του Παγκόσμιου Ιστού (World Wide Web-WWW); Το Διαδίκτυο αποτελεί το μεγαλύτερο υπολογιστικό σύστημα στον κόσμο, η δομή του είναι πλήρως ανοικτή σε κάθε χρήστη Ηλεκτρονικού Υπολογιστή (Η/Υ), είναι απόλυτα αποκεντρωμένο και αυτοδιαχειριζόμενο, καθώς δεν είναι ιδιοκτησία κανενός και δεν ελέγχεται από κανέναν. Οι υπηρεσίες του Internet (ο παγκόσμιος ιστός, το ηλεκτρονικό ταχυδρομείο, οι τηλε-συνδιασκέψεις, οι συνομιλίες σε ομάδες συζητήσεων κα) παρέχουν στους χρήστες Η/Υ μια πληθώρα ωφελειών που σχετίζονται με την επίλυση απλών ή σύνθετων προβλημάτων, την αύξηση της παραγωγικότητας, την πρόσβαση σε ένα απεριόριστο πλούτο πληροφοριών, την εκπαίδευση και κατάρτιση από απόσταση, την ανάπτυξη νέων τύπων εργασίας (τηλε-εργασία) και εμπορίου (ηλεκτρονικό εμπόριο), την ψυχαγωγία και, πάνω από όλα, την επικοινωνία. Ο χρήστης του Διαδικτύου είναι σε θέση, αν αξιοποιήσει θετικά όλα αυτά τα τεχνολογικά αγαθά, να γίνει κοινωνός πρωτόγνωρων δυνατοτήτων και εμπειριών σε ό,τι αφορά στην ανάπτυξη της ελευθερίας της σκέψης, της έκφρασης, της μάθησης και της επικοινωνίας, στην ενίσχυση της ισοτιμίας του έναντι των άλλων μελών της ψηφιακής κοινότητας (e-citizens), στη

διαφύλαξη της ιδιωτικότητας και στην ενίσχυση της ακεραιότητας της προσωπικότητάς του.

Όπως όμως για κάθε τεχνολογικό επίτευγμα έτσι και για το Διαδίκτυο, θα ήταν λάθος αν κανείς προσπαθούσε να του προσδώσει το χαρακτηρισμό του «ηθικού» ή του «ανήθικου». Οι απόψεις αυτές ανήκουν σε άλλες εποχές και υποστηρίζονται ακόμη από εκείνους τους λίγους που άκριτα αποδέχονται ή με πάθος αντιστέκονται σε κάθε τεχνολογική εξέλιξη. Η δεοντολογική χρήση του Διαδικτύου (e-χρήση) και η αξιοποίηση των μέσων των Τεχνολογιών της Πληροφορίας και Επικοινωνίας εξαρτάται σχεδόν αποκλειστικά από την ηθική των χρηστών, ηθική που διαμορφώνεται, εκτός Διαδικτύου, από το οικογενειακό περιβάλλον, το σχολείο, το σύστημα εκπαίδευσης, την παιδεία, και γενικότερα, το κοινωνικοοικονομικό περιβάλλον και τις επιδράσεις του στην προσωπικότητα του καθενός. Έτσι εκτός από «φωτεινή» πλευρά του Διαδικτύου, υπάρχει και μια άλλη «σκοτεινή» πλευρά, η γνωριμία με την οποία εξαρτάται, κατά κύριο λόγο, από τη στάση ζωής του καθενός. Το πρόβλημα έχει παγκόσμιες διαστάσεις. Η σκοτεινή (και διόλου αθέατη) πλευρά του «πλανητικού χωριού» περιλαμβάνει κυρίως την ανεξέλεγκτη έκθεση άσεμνου, πορνογραφικού υλικού, με πολλές φορές διαστροφικό περιεχόμενο, σε ένα ανεξάντλητο πλήθος δικτυακών τόπων (web sites) και ιστοσελίδων (web pages). Εξίσου επικίνδυνη είναι η πλοήγηση σε sites βίαιας, ρατσιστικής και τρομοκρατικής θεματολογίας, η συμμετοχή σε παράνομο τζόγο, η πρόσβαση σε ιστοσελίδες σατανιστικών και παραθρησκευτικών οργανώσεων. Στο σκοτεινό τοπίο περιλαμβάνεται η λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου με ακατάλληλο περιεχόμενο (χωρίς να είναι τις περισσότερες φορές γνωστά τα στοιχεία του αποστολέα), η διακίνηση αρχείων με προσωπικά - ευαίσθητα δεδομένα, η παραβίαση του ιδιωτικού απορρήτου, το οικονομικό έγκλημα σε on-line συναλλαγές, η αποστολή ιών (computer viruses) και προγραμμάτων με σκοπό την πρόκληση καταστροφών στους Η/Υ των αποδεκτών, η προώθηση προπαγανδιστικού υλικού, η διάδοση μηνυμάτων με σκοπό τον προσηλυτισμό ή ακόμη και την παρότρυνση σε αυτοκαταστροφικές ενέργειες. Τον μακρύ κατάλογο συμπληρώνουν οι

τηλεσυνομιλίες με άτομα αμφιβόλου ηθικής και προθέσεων που εκμεταλλεύονται τις τεχνολογικές τους δεξιότητες για να αντλήσουν δεδομένα προσωπικού χαρακτήρα, ή ακόμη να ασκήσουν δράσεις διακίνησης ναρκωτικών και προϊόντων εγκλήματος.

Ανακεφαλαιώνοντας σκέψεις, προτάσεις και λύσεις θα λέγαμε πως για όλα τα προαναφερθέντα και με δεδομένες τις διαπιστωμένες αδυναμίες του νομοθετικού πλαισίου να αντιμετωπίσει το θέμα του πληροφορικού εγκλήματος, κρίνεται αναγκαία η εντατικοποίηση της διωκτικής προσπάθειας σε ποινική βάση. Θεωρείται απαραίτητη η εφαρμογή σκληρότερης ποινικής νομοθεσίας, η ευθυγράμμιση των δικαίων μεταξύ των κρατών ώστε να μπορούν να αντιμετωπιστούν διακρατικά εγκλήματα, όπως επίσης και η παράλληλη προστασία των δικαιωμάτων των υπόπτων και κατηγορουμένων. Τα σύγχρονα και πληροφορικώς ανεπτυγμένα κράτη οφείλουν να κινηθούν αποφασιστικά προς αυτή την πάταξη του ηλεκτρονικού εγκλήματος το οποίο αναμένεται να πάρει ακόμα μεγαλύτερες διαστάσεις στο μέλλον. Επίσης από την πλευρά των υποψηφίων θυμάτων (τόσο των ιδιωτών όσο και των επιχειρήσεων), είναι αναγκαίος ο εκσυγχρονισμός των υπολογιστικών τους συστημάτων με σύγχρονες μεθόδους ασφάλειας και προστασίας.

Βιβλιογραφία

Ελληνική

- Αγγέλης Ιωάννης, «Το νομικό πλαίσιο για την ασφάλεια του Κυβερνοχώρου κατά το Ελληνικό ποινικό δίκαιο», ΠοινΔικ 12/2001, σ.1293
- Αλεξιάδης, Σ., Εγκληματολογία, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα, 1989
- Αργυρόπουλος Κ., «Το Σύνταγμα στον Κυβερνοχώρο: Η Αμερικανική Προσέγγιση», *Εφαρμογές Δημοσίου Δικαίου*,1997
- Αρτινοπούλου Βάσω, Αν. Καθηγήτρια Παντείου Πανεπιστημίου Αθηνών, Ημερίδα ICT Forum: «Ηλεκτρονικό Έγκλημα και Θυματοποίηση», Αθήνα, 29/10/2007
- Αφεντάκης, Α, Η εξέλιξη της παιδαγωγικής και διδακτικής σκέψης (17ος - 20ος αι.), Αθήνα, Χ.Ε. , 1993
- Αφεντάκης, Α., Θεματική της παιδαγωγικής επιστήμης. Παιδαγωγική ανθρωπολογία - Παιδαγωγική ηθική, Αθήνα, Χ.Ε., 1992
- Βιδάλης Τάκης, «Κοινωνία της Πληροφορίας και Σύνταγμα», ΝοΒ,σ.29 επ.
- Βινσέντι, Λ., Αγωγή και ελευθερία. Καντ και Φίχτε (μτφρ. Γ. Πρελορέτζος), Αθήνα, εκδόσεις Πατάκη., 1997
- Γρηγοροπούλου, Β., «Οι εξομολογήσεις του Ζ-Ζ. Ρουσσώ ή η κρυφή αιτιότητα των συναισθημάτων», Ο Πολίτης, τεύχος 51, Απρίλιος 1998.
- Δασκαλάκης, Η., Η εγκληματολογία της κοινωνικής αντίδρασης, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα, 1985
- Εργαστήριο εφαρμογών πληροφορικής στα ΜΜΕ - πηγή Internet
- ΕΛΛΗΝΙΚΗ ΕΤΑΡΕΙΑ ΜΕΛΕΤΗΣ & ΠΡΟΛΗΨΗΣ ΤΗΣ ΣΕΞΟΥΑΛΙΚΗΣ ΚΑΚΟΠΟΙΗΣΗΣ, "Παιδική σεξουαλική κακοποίηση», 25/11/2007

- Ζαραφωνίτου Χριστίνα, «Εμπειρική Εγκληματολογία», Νομική Βιβλιοθήκη, Αθήνα, 1995
- Ιωάννης Εμμ. Αγγελής, «Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη», πηγή Internet
- Κουράκης, Ν., Εγκληματολογικοί ορίζοντες, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα,1991
- ΚΕΝΤΡΟ ΠΛΗ. ΝΕ. Τ. Ν. ΦΛΩΡΙΝΑΣ - "Δίκαιο και Internet" στο dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html
- Λάζος Γρ., «Πληροφορική και Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2001.
- Λαμπροπούλου Έφη, «Κοινωνικός Έλεγχος του Εγκλήματος», Εκδόσεις Παπαζήση, Αθήνα 1994.
- Λεξικό κοινωνικών επιστημών υπό την αιγίδα της Unesco, εκδόσεις Ελληνική Παιδεία Α.Ε., Αθήνα, 1972.
- Μαγγανά Δ. Αντώνη - Λάζου Γρηγόρη, «Ο ποινικός Κώδικας για τον Πολίτη: Μια επιλογή παραδειγμάτων», 1998 Αθήνα, Εκδόσεις Παπαζήση
- Μάριος Δ. Δικαιάκος, ''Παράνομο Περιεχόμενο στο Διαδίκτυο: Η Κυπριακή Εμπειρία στην Αντιμετώπισή του'', Διδακτορική έρευνα, 12/01/2008
- Μετοχιανάκης, Η., Παιδαγωγικές θεωρίες. Φιλοσοφική προσέγγιση, Ηράκλειο Κρήτης, Χ.Ε., 1994
- Μπογδής Ιωάννης, «Παιδική Πορνογραφία στο διαδίκτυο και η καταγραφή τους στα ΜΜΕ», Άρθρο, 25/11/2007
- Νέστωρ Ε. Κουράκης - Εγκληματολογικοί ορίζοντες - τεύχος Β: Πραγματολογική προσέγγιση και επιμέρους ζητήματα.
- Πανούσης, Γ., Θεμελειώδη ζητήματα της εγκληματολογίας, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα., 1987
- Πανούσης, Γ., Οι κοινωνικές σχέσεις ως αναγκαίοι όροι της εγκληματογένεσης, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα, 1985

- Ρουσσώ, Z.Z., Αιμίλιος ή για την εκπαίδευση (μτφρ. Ι. Λ. Σκόκκο), Αθήνα, εκδόσεις Γερ. Αναγνωστίδη.
- Ρουσσώ, Z.Z., Οι εξομολογήσεις του Ζαν Ζακ Ρουσσώ (μτφρ. Α. Παπαθανασοπούλου), Αθήνα, εκδόσεις Ιδεόγραμμα, 1997
- Σπινέλλη, Κ. Δ., Εγκληματολογία, Αθήνα - Κομοτηνή, εκδόσεις Σάκκουλα, 1985
- Τσουραμάνης.Χρ., "Ψηφιακή Κοινωνία, Ψηφιακή Εγκληματικότητα και Θυματοποίηση " στο www.teimes.gr_spoudastirio_yifiaki_eglimatikotita,
- Τσουραμάνης Χρ., «Εγκλήματα του κυβερνοχώρου και δικτυακοι τόποι που αναφέρονται στην ασφάλεια των Η/Υ», ΠοινΔικ 12/2001, σ.1275
- Χρυσαφίδης, Κ., Σημειώσεις για το μάθημα: Προγραμματισμός και διδασκαλία, Αθήνα, 1998

Ξενόγλωσση

- Barry Hurewitz και Allen Lo., «Computer-related crimes», American Criminal Law Review, 1993.
- British Law Commission, Working Paper 110, Computer Misuse 1, 1988
- Bruce Sterling, «The Hacker Crackdown Law and Disorder on the Electronic Frontier», 1992
- Casey E., «Digital Evidence and Computer Crime:Forensic science, Computers and the Internet», Second Edition, Academic Press, 2004
- Carter R.A., «Computer Crime», 1983
- Ceruzzi Paul A., "A history of modern computing", MIT Press, 1998
- Chen C., «Computer Crime and the Computer Fraud and Abuse Act of 1986», Computer and Law Journal.
- Clinard M. B. και Quinney R., Crriminal Behavior Systems: A Typology, New York: Holt, Rinehart & Winston, 1967.

- D. Hopper, Destructive ILOVEYOU Computer Virus Strikes WorldWide, στο http://archives.cnn.com/2000/TECH/computing/05/04/iloveyou/.
- D.B.Parker, Crime by Computer, New York: Charles Scribner's Sons, 1976
- D.G. Ingraham, «On charging computer crime», Computer and Law Journal, 1980.
- Denning, D.E. "Cyberterrorism," Testimony before the special Oversight Panel on Terrorism, U.S. House of Representatives, 23/05/ 2000
- Dorothy E. Denning, «The United States vs Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking», Communications of the ACM, 1991.
- Douglas M. Reimer, «Judicial and Legislative Responses to Computer Crimes», Insurance Counsel Journal.
- Dr Dave Nicholas, Mr. Peter Williams, *Journalism and the Internet*, , στο http://www.soi.city.ac.uk/~pw/ji_lit.html
- Edwards. O., «Hackers from hell», Formes, 1995.
- Friday, P., (1996), Comparing nations and cultures. Readings in a cross - disciplinary perspective, New Jersey, Prentice Hall.
- Furnel, Stev., «Κυβερνοέγκλημα: Καταστρέφοντας την κοινωνία της πληροφορίας», Εκδόσεις Παπαζήση, Αθήνα 2006.
- Grabrosky, PN, και Smith, R.G., *Crime in the Digital Age*, Annandale: Transaction, 1998
- Garfinkel, S. 2000. «Database Nation: The Death of Privacy in the 21st Century.», O' Reilly & Associates, Inc., 211
- Garlad . D., «The Limits of the sovereign State: Strategies of Crime Control in Contemporary Society», British Journal of Criminology, 1996, 36/4.
- Garlad . D., «The Culture of High Crime Societies: Some Preconditions of Recent "Law and Order" Policies», British Journal of Criminology, 2000, 40/3
- Gerald Kovacich, «Introduction to computer fraud – Part 1», στο *Computer and Security*, July 1999

- Casey E., «Digital Evidence and Computer Crime:Forensic science, Computers and the Internet», Second Edition, Academic Press, 2004
- Giddens, A., «Sociology», X.T., Polity Press, 1989
- J. Leyden, LoveBug Threatens στο http://www.vnunet.com/news/1100661 .
- James A. Fagin., «Computer Crime: A Technology Gap», International Journal of Comparative and Applied Criminal Justice, 1991, τ. 15 2
- K. A. Forcht, D. Thomas και K. Wiggington, «Computer crime: Assesing the lawyer's perspective», Journal of Business Ethics, 1989.
- M. D. Goodman and S. Brenner, «The Emerging Consensus on Criminal Conduct in Cyberspace», *Oxford, International Journal of Law and Information Technology*, [200] Vol. 10, n. 2 p. 3.
- A. Manganas, L' erreur de droit comme defense en droit penal Canadien, Quebec: Universite Laval, 1982
- Manuel Castells, "THE INTERNET GALAXY, OXFORD UNIVESITY PRESS",2003, σ.9 επ.
- M. Dodge, «Mapping Cyberspace», *N.Y, Routeldge*, 2001.
- M. Lyman and G. Potter, Organized Crime (New Jersey, Prenhall); U. SIEBER, Legal Aspects of Computer Related Crime (European Commission), 1998
- M. Wasik, «Crime and the Computer», Oxford: Clarendon Press, 1991.
- M.R. Volgyes, "The investigation, prosecution and prevention of computer crime: A State-of-the-art review», Computer and Law Journal, 1980.
- Marc D. Goodman, "Why the police don't care about computer crime», Harvard Journal of Law and Technology Vol. 10 N.3 Summer 1997.
- Mcconnell International, Cybercrime...and Punishment? Archaic Laws Threaten Global Information Dec., 2000.
- Monique Mattei Ferraro JD CISSP, Eoghan Casey MS,. Michael Mc Grath MD., «Investigating Child Exploitation And Pornography: The Internet, The Law And Forensic Science», Contributor: Elsevier Academic Press

- NCCCD, Computer Crime, Computer Security, Computer Ethics, Computer Crime Census 1988.
- Nomad Mobile Research Centre, πηγή - Internet
- OECD., Computer-related crime: Analysis of legal policy, Paris: OECD, 1986
- P. Festa and J. Wilcox, "Experts Estimate Damages in the Billions for Bug" στο http://news.com.com/2100-1001-240112.html?legacy=cnet.
- Parker, Computer Related Crime, στο *Journal of Forensic Sciences*, 1974, 296 επ.
- Paul Taylor, «Hackers, distributed in Computer Underground Digest», Vol.9 Issue 59.
- C. REED, Computer Law (U.K, John Angel), 2004.
- R. Hollinger και L.lanza-Kaduse, «The process of criminalization: The case of computer crime laws», Criminology, 1988.
- R. J. Michalowski, και E. H. Pfuhl, «Technology, property and law: The case of computer crime», Crime Law and Social Change, 1991..
- R. P. Bigelow, «The challenges of computer law», Western New England Law Review, 1985, 7 (3).
- R.Kling, «Computer Abuse and Computer Crime as organizational activities», Computer and Law Journal, 1980.
- S. L. Mandell, Computers, Data Processing and the Law, St. Paul: West Publishing, 1984.
- Steve Shackelford, «Computer-related crime:an international problem in need of an internatrional solution», Texas International Law Journal, 1992.
- Susannah Fox & Oliver Lewis, *Pew Internet Tracking Report:* Fear of Online Crime.
- Thomas P. Hughes, Networks of Power: Electrification in Western Society, 1880-1930, Baltimore: John Hopkins University Press, 1983.
- U.S. Congress, Senate, 1978.
- Ulrich Sieber, The international handbook on computer crime, New York: John Wiley & Sons, 1986.

- W. Gibson, "Neuromancer", New York, Grafton, 1984;
- Wallerstein, Imamanuel., "Historical Capitalism", London: Verso, 1983.
- Mentor, "The conscience of a hacker". *Phrack magazine*, vol.1 issue 7 Phile 3
- "Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly", CNN.com., στο (http://www.cnn.com/TECH/specials/hackers/gandas/goldstein.html.)

Διαδικτυακή

- Βέργου Ντανί, "Τελευταίοι στο Διαδίκτυο, Πρώτοι στο Πορνό", Αρθρο ΕΛΕΥΘΕΡΟΤΥΠΙΑ, 03/02/2007, στο http://www.enet.gr/online/online_obj?pid=127&tp=T&id=530828
- Χριστιάνα Χατζηιορδανόγλου, "Προστασία ανηλίκων από τις παγίδες του διαδικτύου", Άρθρο, Ο ΚΟΣΜΟΣ ΤΟΥ ΕΠΕΝΔΥΤΗ, 10/12/2006, στο http://dide.kil.sch.gr/draseis/epimorfosi2006/Internettraps.doc
- Σωτήρχου Ιωάν. - Μώρου Αρ., "Μια σύγχρονη Μάστιγα", Άρθρο, ΕΛΕΥΘΕΡΟΤΥΠΙΑ, 11/08/2007, στο http://ddikeoma.eu/news/wp-content/uploads/2007/08/%
- ΕΡΕΥΝΑ ΤΗΛΕΟΠΤΙΚΟΥ ΣΤΑΘΜΟΥ ΣΚΑΙ, "Παιδική Πορνογραφία και Internet", 21/02/2007, στο www.skai.gr/master_story.php?id=40272
- www.news.pathfinder.gr : «Συνέντευξη Μιχάλη Σαμιωτάκη, σύμβουλος Ασφαλείας Πληροφοριακών και Τηλεπικοινωνιακών Συστημάτων της εταιρίας MD5 Α.Ε. στην Ζέτα Καρφίδου», 27/10/2005.
- www.ydt.gr
- www.broadboard.gr : «Οι εφηβικές ασθένειες του Διαδικτύου», Λαμπρίνης Υ. Θωμάς, 2007.
- www.simerini.gr : «παιδεραστές προκαλούν και καιροφυλαχτούν στο διαδίκτυο», 28/08/2006.
- www.tovima.gr : «Η μαφία του Διαδικτύου», Κ. Τσαρούχας, 21/02/2002, Αρ. Φύλλου 13617, σελ. Α34.
- www.topontiki.gr : «Παγκόσμια υπερδύναμη το οργανομένο έγκλημα», ποντίκι, 27/04/2006.
- www.e-go.gr : «Συνελήφθησαν δολοφόνοι που σχεδίασαν απαγωγή μέσω Διαδικτύου», 17/08/2007.
- www.police.gov.cy.doc : «Απάτες μέσω Διαδικτύου», Χριστόφορος Μαυρομάτης, ανώτερος υπαστυνόμος, γραφείο διερεύνησης οικονομικού εγκλήματος, αρχηγείο αστυνομίας, Ιανουάριος 2007.
- www.medata.gr : «Παράνομη διακίνηση φαρμάκων», 26/08/2007.
- www.e-pcmag.gr : «7 χρόνια καταδίκη για πειρατεία λογισμικού», πηγή : News.com, 11/04/2006.

- www.bsa.org/hellas/antipiracy : «Πειρατεία λογισμικού Business Software Alliance, 2007.
- www.athos.cti.gr : «Απειλές περιεχομένου από το internet», Σπηλιοπούλου Θεοδώρα.
- www.kathimerini.gr : «Συμβόλαια θανάτου μέσω internet», Ζώγια Κουταλιανού, 12/10/2007.
- www.disabled.gr : «Το προφίλ των δραστών», Κώστα Κυριακοπούλου, πηγή : Ελευθεροτυπία, 26/09/2005.
- www.ydt.gr : «Ηλεκτρονικά εγκλήματα», Περιοδικό Αστυνομίας, Σεπτέμβριος - Οκτώβριος, Τεύχος 233 (Επετειακό).
- www.sdtv.gr : «Ο αστυνόμος Εμμανουήλ Σφακιανάκης μιλά για τη μετάλλαξη του εγκλήματος στη Μιράντα Λυσάνδρου, 05/06/2006.
- www.lawnet.gr : «Ηλακτρονικό έγκλημα», Μπαλωμένου Χριστίνα, 2004.
- www.apodikos.gr : «Κυβερνοχώρος το διεθνές γίγνεσθαι στο Ελληνικό είναι», Υπαστυνόμος Α' Δ.Π. Αγγελόπουλος, Εξεταστής ψηφιακών πιεστηρίων της Διεύθυνσης Εγκληματολογικών ερευνών ΕΛ.Α.Σ. .
- www.pathfinder.gr : «Ανησυχία για την αύξηση της σεξουαλικής κακοποίησης σταδίων στο διαδίκτυο», Οκτώβριος 2006.
- www.provataslaw.gr : «Internet και νομική προστασία», 2006.
- www.enet.gr : «Οι διαδικτυακές κοινωνίες υποκαθιστούν τις πραγματικές», 2006.
- www.enet.gr : «Ορισμός ηλεκτρονικού εγκλήματος», Θεμιστοκλής Ι. Σοφός, Διδάκτωε. Ποινικού δικαίου του Πανεπιστημίου της Βόνης, 2001.
- www.enet.gr : «Το δίκτυο των παρανόμων», Γ. Μαρνέλος, Κ. Κυραικόπουλος, 27/11/2001.
- www.enet.gr : «Stop, στη παιδεραστία τους», Βάλιας-Φωτοπούλου, 2007.
- www.connection.gr : «Απάτες μέσω ATM», Υποστράτηγος ΕΛ.Α.Σ. Π. Λαγγάρη, 23/09/2007.
- www.nuked.com : «Η μαφία του διαδικτύου», 2006.
- www.pc4all.com : «Ηλεκτρικτρονική απάτη», 06/01/2007.
- http://www.greek-language.gr
- D. HOPPER, Destructive ILOVEYOU Computer Virus Strikes WorldWide , διαθέσιμο στο http://archives.cnn.com/2000/TECH/computing/05/04/iloveyou/.
- J. LEYDEN, LoveBug Threatens Email Servers στο http://www.vnunet.com/news/1100661.
- P. FESTA and J. WILCOX, Experts Estimate Damages in the Billions for Bug, στο http://news.com.com/2100-1001-240112.html?legacy=cnet>
- http://www.diaplous.org/library/nomothesia.php
- www.icaa-italia.org
- http://www.edra.ipet.gr

- http://www.ert.gr/eidiseis/index_news.asp?id=35290
- http://tech.pathfinder.gr/tech/9350.html - Associated Press
- http://inhope.com
- http://woman.flash.gr//pregnancy/2004/2/6/3002id/print_version.htm
- http://tech.flash.gr/news/greece/2004/2/24/10523id/
- http://news.antenna.gr/articleDetail/0,3091,76233,00.html
- http://www.ert.gr/site/news/newsbody_eu.asp?ID=88626
- http://www.ethnos.gr/pages/2002/feb/21/p020103.htm
- http://greece.flash.gr//soon/2004/2/4/25332id/
- http://news.pathfinder.gr/periscopio/dangerous_inbox.html
- http://news.kathimerini.gr/4dcgi/_w_articles_world_1_28/10/2003_82139
- http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/696&format=HTML&aged=0&language=EN&guiLanguage=en
- http://dide.flo.sch.gr/Plinet/plinet.html
- http://www.haltabuse.org/resources/online.shtml
- Frontline - who are hackers – interview with anonymous, πηγή Internet
- Διαδίκτυο και ποινική νομοθεσία – πηγή Internet
- Τράπεζα νομικών πληροφοριών – πηγή Internet.
- Ιωάννης Εμμ. Αγγελής – Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη, πηγή Internet
- .Εργαστήριο εφαρμογών πληροφορικής στα ΜΜΕ - πηγή Internet
- Διακύρηξη Nomad Mobile Research Centre – πηγή - Internet
- Εργαστήριο εφαρμογών πληροφορικής στα ΜΜΕ - πηγή Internet
- Νίκος Φώτης, Τι είναι το Ίντερνετ: "Το Δίκτυο", Το ΒΗΜΑ, 2000.
- ΔΙΚΤΥΟ ΕΛΛΗΝΙΚΩΝ ΚΑΤΑΝΑΛΩΤΙΚΩΝ ΟΡΓΑΝΩΣΕΩΝ δ-Ε.ΚΑΤ.Ο «Αποτελέσματα ερευνών για το Διαδίκτυο, σε Ελλάδα και Ευρώπη»,. Ομιλητής: Δρ. Πασχαλίδης Σωτήριος, 2007 στο www.fatsimare.net
- www.politikokafeneio.com
- www.saferinternet.gr
- www.fititis.gr
- www.pacific.jour.anth.gr

- www.portal.boutsikas.gr
- www.ekato.org/gr
- www.nouskalis.gr
- www.theatrocrime.gr
- www.go-online.gr
- www.elwikipedia.org

Λεξικό Όρων Πληροφορικής

A

ActiveX: Σύνολο τεχνολογιών που επιτρέπει σε στοιχεία λογισμικού να αλληλεπιδρούν μέσα σε περιβάλλον δικτύου, άσχετα από την γλώσσα με την οποία δημιουργήθηκαν.

ADSL: ADSL (Asymmetric Digital Subscriber Line) Είναι μια τεχνολογία για τη μετάδοση ψηφιακών πληροφοριών σε πολύ υψηλές ταχύτητες, μέσα από τις υπάρχουσες τηλεφωνικές γραμμές. Το ADSL παρέχει συνδέσεις που είναι πάντα "ανοικτές" - δεν χρειάζεται, δηλαδή, η πραγματοποίηση κλήσης για σύνδεση. Οι ταχύτητες μεταφοράς δεδομένων που μπορούν να επιτευχθούν, κυμαίνονται από τα 512Kbps έως τα 10Mbps.

Algorithm: Μία διαδοχή βημάτων που χρησιμοποιείται στην επίλυση ενός προβλήματος ή στην εκτέλεση μιας εργασίας.

Anonymous FTP: Η δυνατότητα πρόσβασης σε απομακρυσμένο σύστημα υπολογιστή, από κάποιον που δεν έχει εκεί λογαριασμό, μέσω του Πρωτοκόλλου Μεταφοράς Αρχείων του Διαδικτύου. Με το ανώνυμο FTP, οι χρήστες έχουν περιορισμένα δικαιώματα πρόσβασης και συνήθως έχουν το δικαίωμα μόνο να αντιγράφουν αρχεία προς και από ένα δημόσιο κατάλογο του απομακρυσμένου συστήματος.

Antivirus programm: Πρόγραμμα το οποίο σαρώνει την μνήμη του υπολογιστή και τα μέσα μαζικής αποθήκευσης για να εντοπίσει, να απομονώσει και να εξαλείψει τους ιούς, ενώ εξετάζει επίσης τα εισερχόμενα αρχεία για ιούς τη στιγμή που τα παραλαμβάνει ο υπολογιστής.

Applet: Μια μικρή εφαρμογή-πρόγραμμα, όπως, για παράδειγμα, τα προγράμματα σχεδιασμού των Windows. Γράφονται στην Γλώσσα προγραμματισμού Java και εκτελούνται στο φυλλομετρητή. Χρησιμοποιούνται για την προσθήκη δυνατοτήτων αλληλεπίδρασης σε ιστοσελίδες.

ARPANET: Μεγάλο δίκτυο ευρείας περιοχής που δημιουργήθηκε την δεκαετία του 1960 από την Υπηρεσία Προηγμένων Ερευνητικών Έργων του Υπουργείου Άμυνας των Η.Π.Α.

Artificial Intelligence: (Τεχνητή Νοημοσύνη) Κλάδος της πληροφορικής που επιδιώκει να μπορέσουν οι υπολογιστές να προσομοιώσουν διάφορες πτυχές της ανθρώπινης νοημοσύνης.

ASCII: (American Standard Code for Infor) (American Standard Code for Infor) Η πιο συνηθισμένη μορφή απλών αρχείων κειμένου, όπου κάθε χαρακτήρας αντιπροσωπεύεται από ένα δυαδικό αριθμό 7-bit (δηλαδή μια σειρά 7 χαρακτήρων που μπορούν να είναι 0 ή 1). Στο πρότυπο αυτό καθορίζονται συνολικά 128 χαρακτήρες.

B

Backup: (Εφεδρικό αντίγραφο, αντίγραφο ασφαλείας.) Ακριβές αντίγραφο προγράμματος, δίσκου, ή δεδομένων, που δημιουργείται είτε για λόγους αρχειοθέτησης είτε για την αποτροπή της απώλειας

πολύτιμων αρχείων σε περίπτωση φθοράς καταστροφής του ενεργού αντιγράφου. Ορισμένες εφαρμογές δημιουργούν αυτόματα εφεδρικά αντίγραφα των αρχείων δεδομένων, διατηρώντας στο δίσκο τόσο των τρέχουσα όσο και την προηγούμενη εκδοχή του αρχείου. Ονομάζεται επίσης: backup copy, backup file

Bad sector: Κάθε δίσκος διαιρείται σε sectors - τομείς (η μικρότερη δυνατή μονάδα), clusters (συστοιχίες) και tracks (ίχνη). Αν ένας τομέας είναι κατεστραμμένος, δεν μπορεί να αποθηκεύσει δεδομένα αξιόπιστα. Αν αποθηκεύσετε ένα αρχείο και μέρος του αρχείου αποθηκευτεί σε έναν καταστραμμένο τομέα, δεν θα είναι εφικτό το άνοιγμα του αρχείου αυτού.

Backbone: Ο δίαυλος επικοινωνιών από όπου περνάει το μεγάλο ποσοστό της κίνησης ενός δικτύου. Χρησιμοποιείται και για την σύνδεση δικτύων που βρίσκονται σε τεράστιες αποστάσεις μεταξύ τους (π.χ. το Internet).

Bandwidth: (εύρος ζώνης): Η ποσότητα των δεδομένων που μπορεί να μεταδοθεί σε συγκεκριμένο χρόνο. Σε ψηφιακές συσκευές το bandwidth μετριέται σε bits ανά δευτερόλεπτο (bps) ή bytes ανά δευτερόλεπτο. Σε αναλογικές συσκευές το bandwidth μετριέται σε κύκλους ανά δευτερόλεπτο (Hertz - Hz). Το bandwidth είναι ιδιαίτερα σημαντικό σε συσκευές εισόδου εξόδου (I/O). Για παράδειγμα, ένας ταχύτατος σκληρός δίσκος μπορεί να εμποδίζεται στη λειτουργία του από ένα bus με μικρό bandwidth. Αυτός είναι και ο βασικός λόγος, για τον οποίο συνεχώς σχεδιάζονται και υλοποιούνται νέα buses για τους υπολογιστές, όπως το AGP και το USB.

Banner: Τμήμα ιστοσελίδας με μια διαφήμιση που συνήθως έχει ύψος μια ίντσα ή λιγότερο και καταλαμβάνει όλο το πλάτος της ιστοσελίδας.

BASIC: (Beginner´s All-Purpose Symbolic Instruction Code). Είναι μια γλώσσα προγραμματισμού που συμπεριλαμβανόταν παλιά στο πακέτο του MS-DOS. Η BASIC θεωρείται από πολλούς ευκολότερη από όλες τις άλλες γλώσσες προγραμματισμού και είναι εύκολη στην εκμάθησή της.

Beta: Νέο προϊόν λογισμικού ή υλικού, ή προϊον που υφίσταται ενημέρωση, το οποίο είναι έτοιμο να παραδοθεί σε χρήστες για δοκιμή. Συνήθως τα προϊόντα beta έχουν όλες, ή έστω τις περισσότερες, δυνατότητες και λειτουργίες που πρόκειται να έχει το ολοκληρωμένο προϊόν.

BIOS: (Basic Input/ Output System) Ένα σύνολο εντολών ενσωματωμένων μέσα στον υπολογιστή που ελέγχει το πώς οι πληροφορίες και τα δεδομένα ρέουν προς και από τον υπολογιστή.

Bit: (Binary Digit.Δυαδικό ψηφίο (0 ή 1). Χρησιμοποιείται για την έκφραση μιας από δυο δυνατές καταστάσεις ή τιμές. Στο δυαδικό 0 δεν υπάρχει ροή ή τάση από ηλεκτρικό ρεύμα, ενώ στο 1 υπάρχει.

Bluetooth: Πρότυπο ασύρματης διασύνδεσης που χρησιμοποιεί κι αυτό την μπάντα των μικροκυμάτων στη συχνότητα των 2,4GHz, αλλά προσανατολίζεται στην επικοινωνία μεταξύ μικρών φορητών συσκευών, όπως τα κινητά τηλέφωνα, τα PDAs και τα notebooks, με εμβέλεια 10 μέτρα.

Boot Sector: (Τομέας Εκκίνησης) Σε έναν υπολογιστή ο όρος Boot αναφέρεται στη διαδικασία εκκίνησης του λειτουργικού συστήματος και μεταφοράς του στην κύρια μνήμη. Το boot sector είναι η περιοχή στην επιφάνεια ενός δίσκου, όπου είναι αποθηκευμένες οι πληροφορίες του λειτουργικού συστήματος που θα χρειαστούν κατά την εκκίνηση.

Bridge: (Γέφυρα) Συσκευή δικτύου που συνδέει δύο Τοπικά Δίκτυα και επιτρέπει την μετάδοση μηνυμάτων από το ένα στο άλλο.

Broadband: (Ευροζωνικός, ευρείας ζώνης) Επίθετο που αναφέρεται ή χαρακτηρίζει συστήματα επικοινωνιών στα οποία το μέσο μετάδοσης (π.χ., ένα καλώδιο οπτικών ινών) μεταφέρει πολλά μηνύματα ταυτόχρονα. Κάθε μήνυμα διαμορφώνεται στη δική του συχνότητα φέροντος σήματος μέσω μόντεμ. Οι επικοινωνίες ευρείας ζώνης συναντώνται στα δίκτυα ευρείας περιοχής.

Browser (Φυλλομετρητής) : Συντομία του Web browser. Ένα πρόγραμμα, το οποίο χρησιμοποιείται για τον εντοπισμό και την απεικόνιση σελίδων του Web. Δύο από τους δημοφιλέστερους browsers είναι ο Netscape Navigator και ο Microsoft Internet Explorer. Και οι δύο είναι "graphical browsers", δηλαδή μπορούν να απεικονίσουν, εκτός από κείμενο, και γραφικά. Οι πρώτοι browsers δεν είχαν τη δυνατότητα απεικόνισης γραφικών, αφού και η δομή του Internet ήταν διαφορετική και δεν υπήρχε ο multimedia χαρακτήρας που έχει λάβει. Σήμερα, η εικόνα, ο ήχος και το video είναι συνήθη και πολλές φορές αναπόσπαστα μέρη των sites

Buffer: Τμήμα της μνήμης του υπολογιστή που χρησιμοποιείται ως χώρος προσωρινής τοποθέτησης δεδομένων που μεταφέρονται από ένα μέρος (ή μια συσκευή) σε ένα άλλο.

Byte: Ο όρος αφορά τον συνδυασμό δυαδικών ψηφίων που αποτελεί ενιαία και αυτοτελή μονάδα για τον ηλεκτρονικό υπολογιστή. Ο συνδυασμός αυτός μπορεί να έχει την τιμή χαρακτήρα μέσα στις υπολογιστικές διατάξεις. Μια ψηφιολέξη αποτελείται από 8 bits και μπορεί να εκφράζει είτε ένα χαρακτήρα, είτε δυο ψηφία

C

C: Γλώσσα προγραμματισμού που αναπτύχθηκε με αρχικό στόχο την υλοποίηση του λειτουργικού συστήματος UNIX, αλλά χρησιμοποιείται πλέον σε ευρύτερη κλίμακα από τους προγραμματιστές. Η γλώσσα C συνδυάζει την δομή μιας γλώσσας υψηλού επιπέδου με την ικανότητα πρόσβασης στο υλικό της μηχανής.

Cache: Πρόκειται για τη μνήμη που παρεμβάλλεται μεταξύ κύριας μνήμης και επεξεργαστή, με σκοπό την ταχύτερη τροφοδοσία του τελευταίου με δεδομένα και την ταχύτερη ανάκληση εντολών και λειτουργιών από προηγούμενες επεξεργασίες. Η cache είναι μνήμη υψηλής ποιότητας και ταχύτητας, άρα και κόστους. Όσο περισσότερη διαθέτει ένα σύστημα, τόσο ανεβαίνει κατακόρυφα η απόδοσή του.

Chat: Συνδιάλεξη σε πραγματικό χρόνο μέσω υπολογιστή. Όταν κάποιος πληκτρολογήσει μια γραμμή κειμένου και μετά πατήσει το πλήκτρο Enter, οι λέξεις που εμφανίζονται στις οθόνες όλων των άλλων

που συμμετέχουν επίσης, οι οποίοι μπορούν να απαντήσουν ανάλογα. Οι περισσότερες ηλεκτρονικές υπηρεσίες άμεσης επικοινωνίας υποστηρίζουν συνομιλία στο Διαδίκτυο.

Chat room: (δωμάτιο συζητήσεων) Ο ανεπίσημος όρος για το κανάλι επικοινωνίας δεδομένων που συνδέει υπολογιστές επιτρέποντας σε χρήστες να συνομιλούν στέλνοντας μηνύματα κειμένου σε πραγματικό χρόνο.

Client/Server network: Τοπικό δίκτυο δομημένο με βάση το διαχωρισμό των κόμβων σε μηχανήματα πελάτες (χρήστες) και υπολογιστές-διακομιστές, οι οποίοι κάνουν μέρος της επεξεργασίας (που λέγεται παρασκηνιακή επεξεργασία) για τα μηχανήματα πελάτες, για παράδειγμα την ταξινόμηση των εγγραφών μιας βάσης δεδομένων ώστε να παραδοθούν μόνο οι εγγραφές που ζήτησε ο πελάτης.

Codec: Σύντμηση των λέξεων compressor/decompressor. Είναι ένας μαθηματικός αλγόριθμος που δηλώνει τον τύπο της συμπίεσης που χρησιμοποιείται κατά την εγγραφή video. Γνωστοί codecs είναι οι MPEG, M-JPEG και Indeo.

Cookies: Μερικές πληροφορίες που αποστέλλονται από έναν Web server σε κάποιον Web browser Οι πληροφορίες αυτές αποθηκεύονται με τη μορφή ενός text file. Κάθε φορά που ο browser ζητήσει μια ιστοσελίδα από τον Web server, αυτές οι πληροφορίες αποστέλλονται πίσω σε αυτόν.

Crack: (σπάζω) Αποκτώ μη εξουσιοδοτημένη πρόσβαση σε κάποιο δίκτυο παραβιάζοντας τα μέτρα ασφαλείας. Επίσης αποκρυπτογραφώ κρυπτογραφημένες πληροφορίες.

Cryptography: (κρυπτογραφία) Η κωδικοποίηση πληροφοριών με τρόπο ώστε να μην είναι κατανοητές από κανέναν άλλο εκτός από τα άτομα που διαθέτουν το κλειδί του κώδικα.

Cyberspace: (κυβερνοχώρος) Το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδύκτιο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη απο την υλική υπόσταση.

D

Debug: (αποσφαλματώνω). Ψάχνω, εντοπίζω, και διορθώνω τα λογικά ή συντακτικά λάθη ενός προγράμματος ή τις δυολειτουργίες ενός στοιχείου του υλικού. Σε σχέση με το υλικό, χρησιμοποιείται συχνότερα ο όρος troubleshooting (αντιμετώπιση προβλημάτων), ιδίως όταν το πρόβλημα είναι σημαντικό.

Decompiler: (απομεταγλωτιστής). Πρόγραμμα που επιχειρεί να παράγει πηγαίο κώδικα γλώσσας υψηλού επιπέδου, έχοντας ως αφετηρία κώδικα γλώσσας assembly ή κώδικα μηχανής. Το εγχείρημα αυτό συνήθως είναι δύσκολο, επειδή ο κώδικας γλώσσας assembly δεν αντιστοιχεί πάντοτε σε πηγαίο κώδικα υψηλού επιπέδου.

Defragmentation: (αποκατάτμιση, ανασυγκρότηση, αποκατακερματισμός). Η διαδικασία της επανεγγραφής τμημάτων κάθε αρχείου σε συνεχόμενα τμήματα του σκληρού δίσκου, προκειμένου να αυξηθεί η ταχύτητα πρόσβασης και ανάκτησης. Όταν ένα αρχείο τροποποιείται, ο υπολογιστής συνήθως αποθηκεύει τα τροποποιούμενα τμήματά του στο μεγαλύτερο διατιθέμενο χώρο του δίσκου, δηλ. συχνά σε διαφορετικό τομέα από τα άλλα τμήματα του αρχείου. Έτσι, τα αρχεία κατακερματίζονται και, όταν γίνεται πρόσβαση σε αυτά, ο υπολογιστής πρέπει να αναζητήσει τα τμήματά τους σε ολόκληρο το σκληρό δίσκο, κάτι που επιβραδύνει το χρόνο απόκρισης.

Dial-up: Επίθετο που αναφέρεται σε ή χαρακτηρίζει μια σύνδεση η οποία χρησιμοποιεί το δημόσιο τηλεφωνικό δίκτυο.

Digital Signature: (Ψηφιακή Υπογραφή) Μηχανισμός ασφαλείας που χρησιμοποιείται στο Internet και βασίζεται σε δύο κλειδιά, ένα κοινόχρηστο και ένα ιδιωτικό, τα οποία χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων πριν τη μετάδοση και αποκρυπτογράφησή τους κατά τη λήψη.

DNS: Ακρωνύμιο του Domain Name System του ιεραρχικού συστήματος που χρησιμοποιείται για την ονομασία τοποθεσιών στο Internet.

Driver: (οδηγός) Ένα πρόγραμμα που παρεμβάλλεται ανάμεσα σε μια συσκευή και ένα πρόγραμμα ή το λειτουργικό, επιτρέποντας στα δεύτερα την επικοινωνία και το χειρισμό της πρώτης.

E

Encryption: Η κωδικοποίηση πληροφοριών με τέτοιο τρόπο ώστε να είναι ακατανόητες σε οποιονδήποτε εκτός αυτούς που έχουν το κλειδί, δηλαδή των κώδικα που απαιτείται για να γίνουν πάλι κατανοητές.

Ethernet: Ένα πολύ διαδεδομένο δίκτυο που αποτέλεσε τη βάση του προτύπου IEEE 802.3. για τα δίκτυα διαύλου. Είναι δυνατή η μετάδοση δεδομένων με ταχύτητες 10, 100 και 1000 Mbps.

Extranet: Επέκταση του ενδοδικτύου μιας επιχείρησης στην οποία χρησιμοποιείται η τεχνολογία του Παγκόσμιου Ιστού ώστε να διευκολύνεται η επικοινωνία με τους πελάτες και τους προμηθευτές της επιχείρησης.

F

FAT file system: Το σύστημα που χρησιμοποιείται απ το MS-DOS για την οργάνωση και την διαχείριση αρχείων. Ο FAT είναι μια δομή δεδομένων στην οποία δημιουργεί το MS-DOS στο δίσκο όταν ο δίσκος διαμορφώνεται. Όταν το MS-DOS αποθηκεύει ένα αρχείο σε ένα φορμαρισμένο δίσκο, το λειτουργικό σύστημα τοποθετεί πληροφορίες για το αποθηκευμένο αρχείο στον πίνακα FAT, ώστε να μπορεί αργότερα να ανακτήσει το αρχείο όταν του ζητηθεί.

File recovery: Η διαδικασία της ανασυγκρότησης χαμένων ή μη αναγνωρίσιμων αρχείων στο δίσκο. Η αποκατάσταση αρχείων γίνεται με την χρήση βοηθητικών προγραμμάτων που επιχειρούν να

ανασυγκροτήσουν τις πληροφορίες του δίσκου σχετικά με τις θέσεις αποθήκευσης των διαγραμμένων αρχείων.

File Server: Ένας υπολογιστής, που του έχουν ανατεθεί καθήκοντα κεντρικής αποθήκευσης αρχείων. Σε απαιτητικά εργασιακά περιβάλλοντα, δεν είναι ένα τυπικό μηχάνημα, αλλά συνήθως διαθέτει ισχυρά χαρακτηριστικά απομακρυσμένης διαχείρισης.

File sharing: Η χρήση αρχείων υπολογιστή σε δίκτυα, όπου τα αρχεία είναι αποθηκευμένα σε ένα κεντρικό υπολογιστή ή ένα διακομιστή και περισσότεροι από ένας χρήστες τα ανακτούν, τα εξετάζουν και τα τροποποιούν.

Firewall: Το firewall είναι ένα λογισμικό ή μια συσκευή που προστατεύει τους πόρους του δικτύου από τους χρήστες άλλων δικτύων.

Format: Η διαδικασία μορφοποίησης ενός αποθηκευτικού μέσου (δισκέτα, σκληρός δίσκος, μαγνητική ταινία) από το λειτουργικό σύστημα, έτσι ώστε το μέσο αυτό να είναι έτοιμο να δεχτεί δεδομένα προς εγγραφή.

Freeware: Μια κατηγορία προγραμμάτων, τα οποία διατίθενται δωρεάν από τους δημιουργούς τους. Πολλές φορές, τέτοιου είδους προγράμματα έχουν τις ίδιες δυνατότητες με τα αντίστοιχα εμπορικά που αγοράζουμε.

FTP: (Πρωτόκολλο μεταφοράς αρχείων) Τα αρχικά σημαίνουν File Transfer Protocol. Πρόκειται για το πρωτόκολλο που χρησιμοποιείται για τη μεταφορά αρχείων μέσα από το Internet.

G

Gateway (πύλη): Συνδυασμός υλικού και λογισμικού, που συνδέει δύο διαφορετικούς τύπους δικτύων. Για παράδειγμα, οι πύλες μεταξύ συστημάτων ηλεκτρονικής αλληλογραφίας επιτρέπουν στους χρήστες που δουλεύουν σε συστήματα ηλεκτρονικής αλληλογραφίας διαφορετικής αρχιτεκτονικής, να ανταλλάσσουν μηνύματα μεταξύ τους.

H

Hardware: Τα υλικά μέρη ενός συστήματος υπολογιστή, μεταξύ των οποίων και οι τυχόν περιφερειακές συσκευές.

Hexdecimal: (δεκαεξαδικός) Αυτός που χρησιμοποιεί το 16 ως βάση του αριθμητικού συστήματος αντί του 10. Το δεκαεξαδικό σύστημα χρησιμοποιεί τα ψηφία από το 0 έως το 9 και τα λατινικά γράμματα από το A έως και το F (κεφαλαία ή πεζά) για να αναπαραστήσει τους αριθμούς του δεκαδικού συστήματος από το 10 έως και το 15. Ένα δεκαεξαδικό ψηφίο είναι ισοδύναμο με 4 δυαδικά, ενώ ένα byte μπορεί να εκφραστεί με 2 δεκαεξαδικά ψηφία. Για παράδειγμα, το δυαδικό 0101 0011 αντιστοιχεί στο δεκαεξαδικό 53. Για να αποφευχθεί η σύγχυση με τους αριθμούς του δεκαδικού συστήματος, οι

δεκαεξαδικοί αριθμοί στα προγράμματα ή στην τεκμηρίωση συνήθως ακολουθούνται από ένα Η ή προτάσσεται κάποιο από τα σύμβολα &, $ ή 0x.

Host : Λέγοντας host εννοούμε έναν υπολογιστή, στον οποίο μπορεί να γίνει πρόσβαση από ένα χρήστη από μια απομακρυσμένη τοποθεσία. Συνήθως αυτό γίνεται με τη βοήθεια κάποιου modem μέσω της τηλεφωνικής γραμμής. Ο υπολογιστής, στον οποίο υπάρχουν τα δεδομένα, ονομάζεται host, ενώ ο υπολογιστής, τον οποίο χρησιμοποιεί ο χρήστης για να συνδεθεί, ονομάζεται terminal.

HTML: (HyperText Markup Language) Γλώσσα προσδιορισμού ιδιοτήτων υπερκειμένου με εφαρμογή στα κείμενα που αναρτώνται σε Web sites. Καθορίζει το είδος γραμματοσειράς, θέση, μέγεθος, διάφορα εφέ, animation κ.ά. των απεικονιζόμενων χαρακτήρων και γραφικών.

HTTP: (HyperText Transfer Protocol) Είναι το πρωτόκολλο επιπέδου εφαρμογών, το οποίο χρησιμοποιείται από το World Wide Web. Το HTTP καθορίζει μια σειρά από παραμέτρους επικοινωνίας και μετάδοσης. Μεταξύ αυτών, καθορίζει τον τρόπο μορφοποίησης και μετάδοσης των μηνυμάτων (e-mail), καθώς και τις ενέργειες που θα κάνουν οι Web servers και οι browsers σε μια σειρά εντολών που θα λάβουν. Στο HTTP κάθε εντολή εκτελείται ξεχωριστά, χωρίς να λαμβάνονται υπ' όψιν οι εντολές που προηγήθηκαν. Βασικό του πλεονέκτημα είναι η δυνατότητα που έχει για τη μεταφορά πολλαπλών αρχείων μέσω της ίδιας σύνδεσης.

HUB: (ομφαλός) Υλική συσκευή στην οποία συνδέονται οι κόμβοι στα αστεροειδή δίκτυα.

Hypertext: (υπερκείμενο). Κείμενο που διαθέτει συνδέσμους ώστε να αποτελεί ένα πολύπλοκο, μη σειριακό ιστό από συνδέσεις, τον οποίο ο χρήστης μπορεί να διατρέξει μετακινούμενος από το ένα θέμα σε άλλο συναφές.

ICQ: Πρόγραμμα λογισμικού που ειδοποιεί τους χρήστες του Διαδικτύου όταν φίλοι τους, συγγενείς, ή άλλοι χρήστες της επιλογής τους βρίσκονται επίσης συνδεδεμένοι με το Διαδίκτυο και τους επιτρέπει να επικοινωνούν μεταξύ τους σε πραγματικό χρόνο.

I

Intranet: (ενδοδίκτυο) Ιδιωτικό δίκτυο βασισμένο στις τεχνολογίες του Internet, αλλά περιορισμένο για χρήση μέσα σε ένα οργανισμό, όπως είναι μια εταιρεία.

IP Address: Είναι το μέσο της αναγνώρισης ενός υπολογιστή σε ένα δίκτυο TCP/IP. Τα δίκτυα που κάνουν χρήση του πρωτοκόλλου TCP/IP, κατευθύνουν τα μηνύματα βασιζόμενα στη διεύθυνση IP του υπολογιστή. Η μορφή μιας διεύθυνσης IP είναι τέσσερις αριθμοί, οι οποίοι διαχωρίζονται με τελείες (000.111.222.333) και μπορεί να έχουν τιμή από 0 έως 255. Σε ένα τοπικό, αυτόνομο δίκτυο μπορεί να αποδοθούν διευθύνσεις IP σε οποιαδήποτε τυχαία μορφή. Όταν, όμως, συνδέεται ένα ιδιωτικό δίκτυο στο Internet, απαιτείται να γίνεται χρήση συγκεκριμένων, προκαθορισμένων αριθμών για την αποφυγή διπλοεγγραφών.

IRC: Ακρωνύμιο του Internet Relay Chat, μιας υπηρεσίας τους Internet που δίνει τη δυνατότητα στους συμμετέχοντες να συνομιλούν σε πραγματικό χρόνο.

ISDN: (Integrated Services Digital Network). Διεθνές τηλεπικοινωνιακό πρότυπο για τη μεταφορά φωνής, δεδομένων και video μέσω ψηφιακών τηλεφωνικών γραμμών. Το ISDN απαιτεί ειδικές καλωδιώσεις και υποστηρίζει ρυθμούς μεταφοράς δεδομένων της τάξης των 64kbps.

ISP: (Internet Service Provider). Μια εταιρεία που παρέχει στους συνδρομητές της πρόσβαση στο Internet (παροχέας). Με κάποιο προκαθορισμένο, συνήθως μηνιαίο αντίτιμο, ο παροχέας παραχωρεί στο χρήστη ένα κωδικό όνομα και ένα συνθηματικό (password) πρόσβασης, μέσω των οποίων ο τελευταίος πιστοποιεί την ταυτότητά του και έχει τη δυνατότητα να χρησιμοποιήσει τις τηλεπικοινωνιακές γραμμές. Η πρόσβαση του χρήστη μπορεί να γίνει είτε με τηλεφωνική κλήση είτε με μόνιμη σύνδεση με τον παροχέα.

J

Java: Αντικειμενοστρεφής γλώσσα προγραμματισμού που αναπτύχθηκε από τη Sun Microsystems,inc. Η Java είναι παρόμοια με τη C++, αλλά είναι μικρότερη και πιο εύχρηστη από τη C++, επειδή είναι πιο ανθεκτική και διαχειρίζεται τη μνήμη μόνη της. Επίσης, η Java είναι σχεδιασμένη έτσι ώστε να είναι ασφαλής και ανεξάρτητη από σύστημα (δηλ. μπορεί να εκτελεστεί σε οποιοδήποτε σύστημα υλικού), αυτό οφείλεται στο γεγονός ότι τα προγράμματα της Java μεταγλωττίζονται σε κώδικες byte, που δεν είναι τόσο εξειδικευμένοι ώστε να επιδέχονται εντολές ειδικές για κάποιο συγκεκριμένο σύστημα, ενώ εκτελούνται στον υπολογιστή σε ένα ειδικό περιβάλλον λογισμικού που είναι γνωστό ως εικονική μνήμη. Το χαρακτηριστικό αυτό κάνει τη Java γλώσσα χρήσιμη για προγραμματισμό εφαρμογών του Ιστού αφού η πρόσβαση των χρηστών στον Ιστό γίνεται από μεγάλη ποικιλία υπολογιστών. Η Java χρησιμοποιείται στον προγραμματισμό μικροεφαρμογών για τον Παγκόσμιο Ιστό, καθώς και για τη δημιουργία κατανεμημένων εφαρμογών δικτύου.

Javascript: Η Javascript συνδέεται με την Java αλλά δεν είναι αντικειμενοστραφής γλώσσα και είναι περιορισμένης απόδοσης σε σχέση με την Java επειδή δε μεταγλωττίζεται. Με την Javascript μπορούν να προστεθούν σε ιστοσελίδες βασικές εφαρμογές και λειτουργίες ηλεκτρονικής άμεσης επικοινωνίας, αλλά οι διαθέσιμες διασυνδέσεις προγραμματισμού εφαρμογών είναι λιγότερες και απλούστερες από εκείνες που είναι διαθέσιμες με την Java.

L

LAN: (Local Area Network). Τοπικό δίκτυο που εκτείνεται σε εσωτερικό χώρο (γραφείο, όροφος ή κτίριο) χωρίς εξωτερικές καλωδιώσεις, μέσω του οποίου συνδέονται υπολογιστές και περιφερειακά που βρίσκονται στο χώρο αυτό. Υπάρχουν διάφορα είδη τοπικού δικτύου LAN και διαφοροποιούνται ανάλογα με το λειτουργικό σύστημα, στο οποίο βασίζονται, τα είδη καλωδίωσης, τα λειτουργικά συστήματα των συνδεδεμένων υπολογιστών κ.λπ.

Linux: Έκδοση του Unix που διατίθεται ελεύθερα και μπορεί να εγκατασταθεί σε διάφορες πλατφόρμες. Ο πυρήνας του λειτουργικού (kernel) αναπτύχθηκε κυρίως από τον Linus Torvald. Εξαιτίας της σταθερότητας που προσφέρει, του γεγονότος ότι είναι δωρεάν και του ότι μπορεί να τρέξει σε διάφορες πλατφόρμες από -PC μέχρι MAC- έχει γίνει ένα αρκετά δημοφιλές εναλλακτικό λειτουργικό σύστημα.

M

Macro Virus: Ιός γραμμένος σε γλώσσα μακροεντολών και συνδεδεμένος με μια εφαρμογή. Βρίσκεται μέσα σε ένα αρχείο εγγράφου, χρησιμοποιείται με την εφαρμογή και εκτελείται όταν ανοίξει το έγγραφο.

MP3: Το MP3 είναι ένας τύπος συμπιεσμένων αρχείων, στα οποία αποθηκεύονται μουσικές πληροφορίες. Η ονομασία του προήλθε από τον ενιαίο τρόπο ονομασίας των συμπιεσμένων αρχείων multimedia, τα οποία είναι γνωστά και ως MPEG. Αναλόγως με τον τύπο του συμπιεσμένου αρχείου - δηλαδή αν είναι εικόνα ή ήχος- και με τη μέθοδο συμπίεσης που χρησιμοποιείται, δίδεται η ανάλογη ονομασία, η οποία αντιστοιχεί στην προέκταση του αρχείου. Τα MP3 είναι αρχεία MPEG-Layer 3, προδιαγραφή που αντιστοιχεί σε συμπίεση ήχου.

Multitasking: Η ιδιότητα ενός λειτουργικού να εκτελεί ταυτόχρονα περισσότερες από μία εργασίες Στην πραγματικότητα, δεν γίνεται ταυτόχρονη εκτέλεση εργασιών αλλά ταχύτατη εναλλαγή μεταξύ τους.

N

NTFS: (Ακρώνυμο του NT file system - σύστημα αρχείων NT). Προηγμένο σύστημα αρχείων, σχεδιασμένο για χρήση ειδικά με το λειτουργικό σύστημα Windows NT. Υποστηρίζει μεγάλα ονόματα αρχείων, πλήρως ασφαλή έλεγχο πρόσβασης, αποκατάσταση συστήματος αρχείων, εξαιρετικά μεγάλα μέσα αποθήκευσης, και διάφορα άλλα χαρακτηριστικά.

O

Overflow: Γενικά η κατάσταση που δημιουργείται όταν τα δεδομένα που προκύπτουν από την είσοδο ή την επεξεργασία απαιτούν περισσότερα δυαδικά ψηφία από όσα έχει προβλεφθεί από το υλικό ή το λογισμικό για την αποθήκευση τους.

P

Packet: Η μονάδα δεδομένων που δρομολογείται μεταξύ ενός αποστολέα και ενός αποδέκτη συστήματος στο Internet ή οποιουδήποτε άλλου δικτύου μεταφοράς πακέτων. Κάθε αρχείο που αποστέλλεται μέσω του δικτύου τεμαχίζεται σε πακέτα, ώστε να είναι ταχύτερη και πιο ευέλικτη η μεταφορά του. Καθένα από τα πακέτα διατηρεί πληροφορίες διεύθυνσης IP για την πηγή και τον αποδέκτη.

Peer-to-Peer: Μοντέλο δικτύωσης υπολογιστικών συστημάτων, όπου κάθε μέλος του δικτύου είναι ισότιμο με τα υπόλοιπα. Αυτή είναι η ειδοποιός διαφορά της δικτύωσης Peer-to-Peer από τη δικτύωση Client-Server. Στην τελευταία, ένας υπολογιστής, ο οποίος αποκαλείται Server, έχει μεγαλύτερη υπολογιστική ισχύ και πόρους. Ο Server αναλαμβάνει να εξυπηρετεί τους υπόλοιπους υπολογιστές του δικτύου, οι οποίοι συνήθως έχουν μέτρια ισχύ και αποκαλούνται Clients.

PHP: Γλώσσα δημιουργίας δυναμικών σελίδων Web.

Plug And Play: Η ικανότητα ενός συστήματος υπολογιστή, να εγκαθιστά και να ρυθμίζει αυτόματα μια συσκευή που προστίθεται στο σύστημα.

Port: (θύρα) Δίαυλος ή σημείο επαφής μέσω του οποίου διακινούνται πληροφορίες μεταξύ ενός υπολογιστή και κάποιας συνδεμένης συσκευής εισόδου – εξόδου.

Proxy Server: (Διακομιστής μεσολάβησης) Υπολογιστής, μέσω του οποίου είναι δυνατή η ταυτόχρονη πρόσβαση μιας ομάδας χρηστών στο Internet, χωρίς την ανάγκη ύπαρξης ξεχωριστού λογαριασμού (account) για τον καθένα.

R

RAID: Μέθοδος αποθήκευσης δεδομένων στην οποία τα δεδομένα κατανέμονται σε μια ομάδα μονάδων σκληρού δίσκου οι οποίες λειτουργούν σαν μια ενιαία μονάδα αποθήκευσης.

RAM: - Random Access Memory Μνήμη ημιαγωγών στην οποία η κεντρική μονάδα επεξεργασίας ή άλλες συσκευές του υλικού μέρους μπορούν εκτελέσουν ανάγνωση και εγγραφή. Η πρόσβαση στις μονάδες αποθήκευσης μπορεί να γίνει με οποιαδήποτε σειρά. Τα δεδομένα της μνήμης RAM χάνονται όταν κλείσει ο υπολογιστής.

RAM Cache: Κρυφή μνήμη που χρησιμοποιείτε από το σύστημα για αποθήκευση και ανάκτηση δεδομένων από την RAM.Η μνήμη RAM Cache (κρυφή μνήμη) είναι ταχύτερη από την μνήμη RAM.

Router Ενδιάμεση συσκευή σε δίκτυο επικοινωνιών η οποία διεκπεραιώνει την παράδοση μηνυμάτων. Ο δρομολογητής δέχεται τα μεταδιδόμενα μηνύματα και τα προωθεί στον εκάστοτε σωστό προορισμό.

S

Safe Mode: Ένας τρόπος εκκίνησης του υπολογιστή στον οποίο τα βασικά αρχεία εκκίνησης παρακάμπτονται και φορτώνονται μόνο οι πιο βασικοί οδηγοί. Η κατάσταση ασφαλούς λειτουργίας επιτρέπει στο χρήστη να διορθώσει ορισμένα προβλήματα του συστήματος.

Script: (Σενάριο). Είναι ένα σύνολο εντολών που μπορούν να εκτελεστούν χωρίς την παρέμβαση του χρήστη. Μια γλώσσα script" (script language) είναι μια απλή γλώσσα προγραμματισμού, στην οποία μπορούν να γραφτούν scripts.

Sector: (Τομέας). Ο όρος αφορά, κυρίως, τους μαγνητικούς δίσκους. Κάθε επιφάνεια δίσκου έχει ομόκεντρους κύκλους ή αυλάκια, όπου γράφονται τα στοιχεία (δεδομένα) με τη μορφή μαγνητικών στιγμάτων. Κάθε αυλάκι είναι χωρισμένο σε τομείς -sectors-, καθένας από τους οποίους έχει τη δική του διεύθυνση.

Server: (Διακομιστής): Αποτελεί το κεντρικό, υψηλής δυναμικότητας σύστημα ενός τοπικού ή απομακρυσμένου δικτύου, το οποίο προσφέρει είτε υπηρεσίες είτε τους πόρους του στους χρήστες του δικτύου.

Source code (πηγαίος κώδικας): Προτάσεις προγράμματος αναγνώσιμες από ανθρώπους, γραμμένες από προγραμματιστή ή υπεύθυνο ανάπτυξης λογισμικού σε γλώσσα υψηλού επιπέδου ή σε συμβολική γλώσσα. Ο πηγαίος κώδικας δεν είναι απευθείας αναγνώσιμος από τον υπολογιστή. Για να μπορέσει να εκτελεστεί από υπολογιστή, πρέπει προηγουμένως να μεταγλωττιστεί σε αντικειμενικό κώδικα.

Spoofing (εξαπάτηση): Ένας τρόπος μεταμφίεσης, όπου μια μετάδοση σε ένα δίκτυο εμφανίζεται να προέρχεται από έναν εξουσιοδοτημένο υπολογιστή.

Subnet (υποδίκτυο): Ένα δίκτυο που αποτελεί τμήμα ενός μεγαλύτερου δικτύου

T

TCP/IP (Transmission Control Protocol over Internet Protocol).: Μια ομάδα πρωτοκόλλων που έχει σχεδιαστεί για να κάνει εφικτή την επικοινωνία μέσω διασυνδεμένων και πολλές φορές ανόμοιων δικτύων. Το TCP/IP υποστηρίζεται από όλα σχεδόν τα δίκτυα. Βρίσκεται στην καρδιά των επικοινωνιών του Internet.

Telnet: Πρωτόκολλο της σουίτας TCP/IP που επιτρέπει σε άτομα να συνδέονται με έναν απομακρυσμένο υπολογιστή και να τον χρησιμοποιούν σαν να χρησιμοποιούσαν τερματικό απευθείας συνδεδεμένο με το μηχάνημα.

U

UNIX: Λειτουργικό Σύστημα πολυδιεργασίας και πολλών χρηστών, το οποίο επειδή είναι γραμμένο σε γλώσσα C, είναι περισσότερο φορητό από πολλά άλλα λειτουργικά συστήματα. Σε ορισμένες παραλλαγές του unix διατίθενται δωρεάν και ο πηγαίος κώδικας κάτι που έχει αναγάγει το unix σε καθοριστικό παράγοντα κινήματος του ανοικτού πηγαίου κώδικα.

Update: Νέα κυκλοφορία ενός υπάρχοντος προϊόντος λογισμικού. Η ενημέρωση λογισμικού συνήθως προσθέτει νέες δυνατότητες σε ένα πρόγραμμα ή διορθώνει σφάλματα που διαπιστώθηκαν μετά την προηγούμενη κυκλοφορία του.

Upgrade: Η νέα βελτιωμένη έκδοση ενός προϊόντος.

Upload Η μεταφορά του αντιγράφου ενός αρχείου από ένα τοπικό υπολογιστή σε ένα απομακρυσμένο.

URL: (Uniform Resource Locator) Μια διεύθυνση πόρου στο Διαδίκτυο. Τα URL χρησιμοποιούνται από τους φυλλομετρητές του Ιστού για τον εντοπισμό πόρων στο Διαδίκτυο.

User Interface: (Διεπαφή χρήστη) Το τμήμα ενός προγράμματος με το οποίο αλληλεπιδρά ένας χρήστης.

V

Virus (Ιός): Μικρό πρόγραμμα που μπορεί να εξαπλώνεται από ένα υπολογιστικό σύστημα σε ένα άλλο. Οι ιοί μπορούν να γραφτούν σε διάφορες γλώσσες προγραμματισμού ακόμα και σε γλώσσα μηχανής και συνήθως προκαλούν ανεπιθύμητες συνέπειες στα συστήματα που εγκαθίστανται.

Visual Basic: Εμπορική ονομασία, που αποτελεί ιδιοκτησία της Microsoft Corporation, μιας υψηλού επιπέδου παραλλαγής της γλώσσας προγραμματισμού Basic κατάλληλης για οπτικό προγραμματισμό. Η Visual Basic σχεδιάστηκε για τη δημιουργία εφαρμογών Windows.

W

Wireless communication (ασύρματη επικοινωνία): Επικοινωνία μεταξύ ενός υπολογιστή και άλλου υπολογιστή ή άλλης συσκευής χωρίς σύρματα. Η μορφή ασύρματης επικοινωνίας που παρέχεται ως τμήμα του λειτουργικού συστήματος Windows χρησιμοποιεί το υπέρυθρο φως για τη μετάδοση αρχείων. Μια άλλη μορφή ασύρματης επικοινωνίας είναι οι ραδιοσυχνότητες, που χρησιμοποιούνται από τα κινητά και τα ασύρματα τηλέφωνα.