

ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ  
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ  
ΤΜΗΜΑ ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ

ΘΕΜΑ:

***«Hackers: Κουλτούρα και Ηθική ».***

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΦΟΙΤΗΤΡΙΑ:

Κατερίνα Φραντζέσκου 188/03

ΚΑΘΗΓΗΤΗΣ:

Αικατερίνη Γιαννουκάκου

ΘΕΣΣΑΛΟΝΙΚΗ - 2009

## ΕΠΙΤΟΜΗ

Το θέμα των hackers έχει συζητηθεί ευρέως τα τελευταία χρόνια από τα ΜΜΕ, τους νομικούς, τις κυβερνήσεις και τους υπεύθυνους ασφαλείας υπολογιστών. Όλοι καταβάλουν τη μέγιστη προσπάθεια να προσελκύσουν την προσοχή μας. Παρόλο που τα τελευταία χρόνια παρατηρείται μια έκρηξη ενδιαφέροντος για το θέμα, η κουλτούρα των hackers δεν εμφανίστηκε πρόσφατα, υπάρχει στο προσκήνιο από το 1960 και γεννήθηκε μέσα από τα εργαστήρια του Πανεπιστημίου MIT (Massachusetts Institute of Technology).

Ο όρος hacker μέσα από την πορεία της εξέλιξης του έχει διευρυνθεί πολύ με αποτέλεσμα να παρεξηγηθεί, να διαστρεβλωθεί και να χάσει την ακριβή έννοια του. Σε αυτό συνέβαλαν και τα ΜΜΕ, η προκατάληψη της κοινωνίας στις καινοτομίες και ο κινηματογράφος. Ο όρος γεννήθηκε μέσα από τα εργαστήρια του MIT και προσδίδονταν τιμητικά σε άτομα ευφυή που είχαν ταλέντο στους ηλεκτρονικούς υπολογιστές και τον προγραμματισμό, άτομα με ανήσυχο πνεύμα και αντιεξουσιαστική διάθεση. Ιστορικά το hacking ξεκίνησε το 1960, εξελίχτηκε και μεταλλάχτηκε με το πέρασμα των χρόνων.

Η κοινωνία των hackers χωρίζεται και κατηγοριοποιείται σε τρεις κατηγορίες με κριτήριο την ηθική —όπως οι hackers την αντιλαμβάνονται— τους λευκούς, τους μαύρους και τους γκριζούς hackers. Χωρίζεται επίσης σε επίπεδα με δείκτη διάκρισης τις ικανότητες, τους elite hacker, script kiddies, cracker, spammer.

Αντίθετα με την κοινή γνώμη οι hackers δεν είναι μοναχικοί. Συχνά οι hackers είναι μέλη ομάδων, με δημοσιεύσεις και κοινές δραστηριότητες αφιερωμένες στα ενδιαφέροντα τους. Η κουλτούρα των hackers είναι φιλελεύθερη προοδευτική, ανεξάρτητη, μαχητική. Οι απόψεις των hackers είναι συχνά πολύ διαφορετικές από αυτές τις οποίες έχουμε εμείς που παρατηρούμε τις πράξεις τους. Σκοπός των hackers είναι η τεχνολογική καινοτομική ανάπτυξη. Στοχεύουν στην απελευθέρωση της πληροφορίας και στην εξασφάλιση της ελεύθερης και εύκολης πρόσβασης του κοινού σε αυτήν. Στόχος τους είναι η συλλογή πληροφοριών και η παραγωγή γνώσης καθώς και η διάδοση της.

Συσχετίζοντας τους hackers και τις βιβλιοθήκες παρατηρούνται κοινοί στόχοι. Οι βιβλιοθήκες ως ιδρύματα που προάγουν την γνώση και την διαθέτουν δωρεάν είναι ενεργά μέλη στην διαχείριση των πληροφοριών. Επιπλέον πολλά προϊόντα που

προήλθαν από τους hackers, όπως το λογισμικό Linux και οι άδειες Creative Commons χρησιμοποιούνται από βιβλιοθήκες.

Η κοινωνία της πληροφόρησης επηρεάζεται άμεσα από την τεχνολογία της πληροφόρησης την οποία διαχειρίζονται εν μέρη οι hacker, ως εκ τούτου οι hackers επηρεάζουν την κοινωνία της πληροφορίας. Από κοινωνιολογικής απόψεως το hacking προσφέρει πολλά θετικά τεχνολογικά επιτεύγματα στη κοινωνία αλλά δυστυχώς με την λανθασμένη διάσταση που έχει πάρει το θέμα προκαλεί πανικό και προκατάληψη για την ασφάλεια του Διαδικτύου και της τεχνολογίας. Ως εκ τούτου, οι νέες λειτουργίες που εμφανίζονται, όπως το ηλεκτρονικό εμπόριο, μπορεί να καταπνίγονται ως αποτέλεσμα των ανησυχιών για την ασφάλεια του Διαδικτύου.

## ΠΕΡΙΕΧΟΜΕΝΑ

	σελ.
<b>Επιτομή</b>	<b>i</b>
<b>Πίνακας συντομογραφιών</b>	<b>vi</b>
<b>Πρόλογος</b>	<b>x</b>
<b>Μεθοδολογία</b>	<b>xiii</b>
<b>Βιβλιογραφική ανασκόπηση</b>	<b>xvii</b>
<b>Κεφάλαιο 1: Ιστορική αναδρομή</b>	<b>1</b>
1.1 Κοινωνία της Πληροφορίας	1
1.2 Συνοπτική ιστορία του Διαδικτύου	3
1.2.1 Δεκαετία 1960: ένα ενδιαφέρον πείραμα ξεκινά	4
1.2.2 Δεκαετία 1970: οι πρώτες συνδέσεις	4
1.2.3 Δεκαετία 1980: ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα	5
1.2.4 Δεκαετία 1990: ένα παγκόσμιο δίκτυο για όλους	6
1.3 Ορισμοί	7
1.4 Συνοπτική ιστορία του hacking	10
1.4.1 Επίπεδο 1	15
1.4.2 Επίπεδο 2	16
1.4.3 Επίπεδο 3	16
1.5 Κίνητρα πίσω από τις πράξεις των hackers	17
1.6 Χαρακτηριστικά των hackers	20
<b>Κεφάλαιο 2: Διάσημοι και δημοφιλείς hackers</b>	<b>28</b>
2.1 John Draper – Captain Crunch	28

2.2 Kevin David Mitnick	30
2.3 Kevin Poulsen	34
2.4 Robert Tappan Morris	35
2.5 Vladimir Levin	37
2.6 Mark Abene	38
2.7 Andrew Miffleton – Daphtpunk	39
2.8 David Smith	40
2.9 Timothy Lloyd (Computer Sabotage)	41
2.10 Michael Calce – Mafiaboy	42
2.11 Patrick W. Gregory – MostHateD	43
2.12 Adrian Lamo	44
2.13 Stephen Wozniak	45
2.14 Tim Berners-Lee	47
2.15 Linus Benedict Torvalds	49
2.16 Richard Stallman	51
2.17 Tsutomu Shimomura	53
2.18 Raven Alder	54
<b>Κεφάλαιο 3: Η κουλτούρα και η ιδεολογία των hackers</b>	<b>58</b>
3.1 Κουλτούρα και πολιτισμός	58
3.2 Υπόγεια κοινότητα και ομάδες hacker	60
3.2.1 Legion of Doom	60

3.2.2 Masters of Deception	62
3.2.3 Cult of the Dead Cow	64
3.2.4 L0pht Heavy Industries	67
3.2.5 Chaos Computer Club (CCC)	68
3.2.6 Infonomicon Computer Club	70
3.3 Η ηθική των hackers	71
<b>Κεφάλαιο 4: Η απελευθέρωση της πληροφορίας και η προώθηση του ελεύθερου λογισμικού: μια μαρξιστική προσέγγιση</b>	<b>74</b>
<b>Κεφάλαιο 5: Πνευματικά δικαιώματα, οι άδειες creative commons και το ελεύθερο λογισμικό στα ακαδημαϊκά ιδρύματα και τις βιβλιοθήκες</b>	<b>85</b>
5.1 Οι επιδράσεις του hacking στην κοινωνία	87
<b>Συμπεράσματα</b>	<b>96</b>
<b>Λεξικό όρων</b>	<b>101</b>
<b>Βιβλιογραφία</b>	<b>104</b>
<b>Ευρετήριο</b>	<b>123</b>

## ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Ελληνόγλωσσες	
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
Η/Υ	ηλεκτρονικός υπολογιστής
κ.α.	και άλλα
κλπ	και τα λοιπά
κ.ο.κ	και ούτω καθεξής
ΜΜΕ	Μέσα Μαζικής Ενημέρωσης
π.χ.	παραδείγματος χάριν
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Ξενόγλωσσες	
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
AT&T	American Telecommunications Company
CC	Creative Commons
CCC	Chaos Computer Club

cd	compact disc
cd-rom	Compact Disc – Read Only Memory
cDc	Cult of the Dead Cow
CERN	Conseil Européen pour la Recherche Nucléaire (European Organization for Nuclear Research)
CSAIL	Computer Science and Artificial Intelligence Laboratory
DDoS	Distributed Denial of Service
EHAP	Ethical Hackers Against Paedophilia
FBI	Federal Bureau of Investigation
FM	Frequency Modulation
FTP	File Transfer Protocol
GPL	General Public License
IBM	International Business Machines Corporation
INTP	Introversion, iNtuition, Thinking, Perception
IP	Internet Protocol
ISPs	Internet Service Providers
L0pht	L0pht Heavy Industries



LGPL	Lesser General Public License
LOD	Legion of Doom
MILNET	Military Net
MIT	Massachusetts Institute of Technology
MLP	Mozilla Localization Project
NASA	National Aeronautics and Space Administration
NINJA	Ninja Strike Force
NSA	National Security Agency
NSFnet	National Science Foundation NetWare
OSI	Open Source Institute
Pdf	Portable Document Format
PDP-1	Programmed Data Processor-1
PIN	Personal Identification Number
POCSAG	Post Office Code Standardization Advisory Group
RBOC	Regional Bell Operating Company
RSS	Rich Site Summary

SQL	Structured Query Language
TCP	Transmission Control Protocol
TRW	Thompson Ramo Wooldridge Inc.
UNIX	Προκύπτει από το “UNInplexed Information & Computing System”
WSRI	Web Science Research Initiative
WWW	World Wide Web

## ΠΡΟΛΟΓΟΣ

Η πτυχιακή εργασία "Η κουλτούρα και η ηθική των hacker" έγινε για το Τμήμα Βιβλιοθηκονομίας του Ανώτατου Τεχνολογικού Εκπαιδευτικού Ιδρύματος Θεσσαλονίκης (ΑΤΕΙ-Θ). Επιλέχθηκε το συγκεκριμένο θέμα μετά από προσωπική μου εισήγηση στην κυρία Κατερίνα Γιαννουκάκου

Η μελέτη αυτή αποσκοπεί να στέψει την προσοχή του αναγνώστη στο hacking και να αποτελέσει μια εισαγωγή στον κόσμο των hacker και να προσφέρει κάποιες σκέψεις για την σημασία και την προσφορά των hacker στην κοινωνία. Δεν αποσκοπεί στην κριτική του hacking, στόχος είναι να παρουσιαστεί η αντικειμενική διάσταση του θέματος εξιλεωμένη από μύθους και υπερβολές. Μέσα από την παράθεση του έργου των σημαντικότερων hacker στην ιστορία και την ιστορική αναδρομή και εξέλιξη της κοινωνίας των hacker γνωρίζει ο αναγνώστης ένα αθέατο κόσμο ο οποίος είναι απρόσιτος στους πολλούς, ίσος και αυτός είναι ο λόγος που παραμένει σκοτεινός και μυστήριος.

Προσεγγίζοντας το θέμα των hackers θα εστιάζουμε στην υποκουλτούρα και τα κοινωνικά χαρακτηριστικά τους. Θα εξετάσουμε σε βάθος και θα αναλύσουμε την μορφή αυτής της κοινωνικής ομάδας, τις τάξεις και τις υποομάδες της. Αναλύοντας τις δομές παρατηρούμε την κοσμοθεωρία και την ηθική αυτών των ατόμων τόσο σε ομαδικό όσο και σε ατομικό επίπεδο. Όλη προσπάθεια έχει σκοπό να προσεγγίσει το θέμα με προσοχή και σοβαρότητα και να προβάλει πληροφορίες, οι οποίες δεν είναι γνωστές στο ευρύ κοινό. Η προσέγγιση θα είναι σε βαθύ και τεκμηριωμένο επίπεδο, προσπαθώντας να προσεγγιστεί το θέμα ρεαλιστικά ξεφεύγοντας από τις μέχρι τώρα αντιλήψεις τους. Στόχος είναι να δούμε που σταματά η αλήθεια και που ξεκινά ο μύθος και η παραπληροφόρηση.

Η προσπάθεια αυτή είχε μια βασική δυσκολία, την προσέγγιση του θέματος. Το θέμα μπορεί να προσεγγισθεί και να υποστηριχθεί από δύο όψεις. Η πρώτη θεώρηση είναι οι απόψεις επί του θέματος των ίδιων των hackers, ενώ η δεύτερη από την πλευρά των υπεύθυνων ασφάλεια καθώς και των επίδοξων θυμάτων των hackers. Θέλοντας να παρουσιάσουμε το θέμα πιο αντικειμενικά πρέπει να αντλήσουμε στοιχεία και από τις δύο πλευρές.

Η άλλη δυσκολία είναι ο θεματικός προσανατολισμός του θέματος. Οι hackers είναι ένα διακλαδικό θέμα το οποίο αφορά πολλούς τομείς όπως την οικονομία, την κοινωνία, την τεχνολογία κ.ο.κ. Υπάρχει μια ποικιλία θεμάτων, η οποία αυξάνει τον

πήχη δυσκολίας της προσέγγισης του θέματος. Αν και δεν είναι εφικτό να εξετάσεις το θέμα μόνο προς μια κατεύθυνση προσπάθησα να δώσω βαρύτητα στην κοινωνική προσέγγιση του θέματος χωρίς βέβαια να αφήσω εντελώς ανέπαφους τους άλλους τομείς –οικονομία, πολιτική, τεχνολογία, νομικό προσανατολισμό.

Οι βιβλιοθήκες και τα ακαδημαϊκά ιδρύματα είναι οργανισμοί υπεύθυνοι για την προαγωγή και την διάθεση της πληροφορίας και της γνώσης. Μια βιβλιοθήκη είναι ένας ναός από πολύτιμες πληροφορίες, όπως και το Διαδίκτυο με την διαφορά ότι το πρώτο είναι σε αναλογική μορφή και το δεύτερο σε ψηφιακή. Σήμερα όμως το Διαδίκτυο έχει γίνει αναπόσπαστο εργαλείο μιας βιβλιοθήκης, έχει συγχωνευθεί με αυτή. Ο πιο πάνω παραλληλισμός έγινε με σκοπό να επισημανθεί η ανάγκη για αλλαγή των παραδοσιακών υπηρεσιών μιας βιβλιοθήκης καθώς και το γνωστικό πλαίσιο των εργαζομένων σε αυτή.

Η τεχνολογία έχει επηρεάσει κατά κόρον τη γνώση. Τα ηλεκτρονικά περιοδικά, οι βάσεις δεδομένων, οι ηλεκτρονικοί θεματικοί κατάλογοι είναι τα νέα προϊόντα μιας σύγχρονης βιβλιοθήκης καθώς και η ψηφιακή αναζήτηση υλικού για έρευνα, η ηλεκτρονική επικοινωνία μεταξύ βιβλιοθηκών, η ψηφιοποίηση τεκμηρίων είναι καθημερινές εργασίες μία επίσης σύγχρονης και εξελιγμένης βιβλιοθήκης. Η τάση να ψηφιοποιείται η γνώση και οι νέες τεχνολογικές δυνατότητες επιτάσσουν μια άμεση ανανέωση στον χώρο των πνευματικών δικαιωμάτων και την προσαρμογή τους στα νέα δεδομένα. Οι hackers διαδραματίζουν σημαντικό ρόλο στις συζητήσεις για τα πνευματικά δικαιώματα. Είναι οι πρωτοπόροι που δημιούργησαν το copyleft και τις άδειες των Creative Commons.

Πώς όμως οι στόχοι μιας βιβλιοθήκης και ενός hacker συμπίπτουν; Οι βιβλιοθήκες έχουν ως κυρίαρχο στόχο τη διάδοση πληροφοριών και τη συλλογή ύλης για την δημιουργία της γνώσης καθώς και την ελεύθερη πρόσβαση του κοινού σε αυτή. Οι hacker θεωρούν ότι η πρόσβαση στη γνώση πρέπει να είναι ελεύθερη και είναι αναφαίρετο δικαίωμα του κάθε ατόμου να έχει πρόσβαση σε αυτή. Ως εκ τούτου και οι δύο υπερασπίζονται και υπηρετούν το ανθρώπινο δικαίωμα της ελεύθερης πρόσβασης στην πληροφορία.

Οι βιβλιοθήκες έχουν πολλά να πάρουν αλλά και να διδαχτούν από τον ελεύθερο χαρακτήρα των hackers και το αγωνιστικό τους πνεύμα. Τα προϊόντα που παράγουν όπως το ελεύθερο / ανοικτό λογισμικό μπορούν να ωφελήσουν και απευθύνονται σε κάθε οργανισμό όχι μόνο σε μια βιβλιοθήκη. Η ελεύθερη σκέψη και οι συντονισμένες προσπάθειες για απελευθέρωση της γνώσης και εύκολη πρόσβαση σε αυτή, η

διάδοση των πληροφοριών και της γνώσης είναι στόχοι για τους οποίους μάχεται και μια βιβλιοθήκη.

Ελεύθερο λογισμικό, ελεύθερη κουλτούρα, copyleft αντί copyright. Οι βιβλιοθήκες λόγω του λειτουργικού τους πυρήνα (οίκος της γνώσης) οφείλουν να υποστηρίζουν αυτή την νέα κουλτούρα ελευθερίας που γεννήθηκε μέσα από την κοινότητα των hackers. Σκοπός και τον δύο είναι η εύκολη πρόσβαση στη γνώση και η ελεύθερη ροή των πληροφοριών.

Η μελέτη του φαινομένου του που ονομάζεται hacking αποσκοπεί στην ανάλυση του ώστε να γνωρίσουμε καλύτερα από που προήλθαν οι ριζοσπαστικές αλλαγές στην τεχνολογία όπως για παράδειγμα το ελεύθερο λογισμικό αλλά και οι ριζοσπαστικές φιλελεύθερες απόψεις για την διακίνηση της πληροφορίας. Γνωρίζοντας εμπειριστατωμένα και σωστά το θέμα θα αποφανθούμε για το πόσο αυτές οι ιδέες είναι ορθές και αν πρέπει να υποστηριχθούν από ένα οργανισμό όπως είναι η βιβλιοθήκη.

Θέμα της παρούσας έρευνας είναι η παρουσίαση της ιστορική ανάπτυξη του hacking, των εκπρόσωπων του, των ιδεών και του τρόπου σκέψης των hackers και κατά πόσο η ιδεολογία τους και οι στόχοι τους συμπίπτουν με την βασική λειτουργία της βιβλιοθήκης, δηλαδή στην διάδοση των πληροφοριών και στην παραγωγή της γνώσης υπέρ του οικουμενικού καλού.

Στα κείμενα υπάρχουν πολλοί τεχνικοί και τεχνολογικοί όροι, για τους οποίους δίνεται ένας σύντομος ορισμός στο «Γλωσσάρι» για την καλύτερη κατανόηση των κειμένων.

## **ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ**

Στο κεφάλαιο μεθοδολογία έρευνας καταγράφονται όλα τα στάδια που πραγματοποιήθηκαν για την ολοκλήρωση της εργασίας αυτής. Ο σκοπός και οι στόχοι που τέθηκαν και καθόρισαν το πλαίσιο στο οποίο έχει κινηθεί η μελέτη αυτή. Παράλληλα δίνεται μια περίληψη για την βιβλιογραφική έρευνα και την βιβλιογραφική ανασκόπηση που έγινε για τη συγγραφή της έρευνας αυτής. Καταγράφονται τα προβλήματα που παρουσιάστηκαν κατά την διάρκεια της διεξαγωγής της μελέτης και τέλος παρουσιάζονται τα συμπεράσματα που προέκυψαν από το κεφάλαιο αυτό.

### **Σκοπός**

Σκοπός της μελέτης είναι η έρευνα και η συλλογή πληροφοριών για την κοινότητα των hackers. Μια μελέτη για την ηθική της υποκουλτούρας των hackers και της προσφοράς τους στην Κοινωνία της Πληροφορίας. Μια επιτομή στο κόσμο των hackers και της ελεύθερης κουλτούρας.

### **Στόχοι**

Οι στόχοι της μελέτης είναι οι ακόλουθοι:

- Η βιβλιογραφική μελέτη των είδη υπαρχόντων εργασιών με θέμα την κοινότητα των hackers
- Η ιστορική αναδρομή στην εξέλιξη του hacking
- Η συλλογή και καταγραφή βιογραφικών σημαντικών hackers στον χώρο του hacking
- Η έρευνα ως και παρουσίαση της κουλτούρας των hackers
- Η παρουσίαση του κοινού κώδικα ηθικής των hackers
- Η έρευνα και η κριτική του έργου των hackers και η προσφορά τους στην κοινωνία.

### **Περιορισμοί της έρευνας**

Η συγκεκριμένη έρευνα διεξήχθη να παρουσιάσει την κοινωνία των hackers και να εισάγει των αναγνώστη στη φιλοσοφία του hacking. Η επιλογή αυτή έγινε μετά έρευνα στο Διαδίκτυο και την διαπίστωση του ενδιαφέροντος που παρουσιάζει το

θέμα καθώς και του γεγονότος ότι η ηθική των hackers ενδιαφέρει άμεσα ακαδημαϊκά ιδρύματα όπως είναι η βιβλιοθήκες.

Αρχική σκέψη ήταν να πραγματοποιηθεί η έρευνα σε όλο το φάσμα του θέματος του hacking, κατά την διεξαγωγή όμως της έρευνας κατάλαβα ότι αυτό δεν ήταν εφικτό πρώτον γιατί είναι αδύνατο να καλύψω ένα τέτοιο μεγάλο θέμα επαρκώς και δεύτερον δεν είχα τις τεχνολογικές γνώσεις ώστε να κατανοώ πλήρως το τεχνολογικό κομμάτι του hacking. Αργότερα αποφάσισα να εστιάσω στην φιλοσοφία, την ηθική και την κοινωνία των hackers προσεγγίζοντας το θέμα κοινωνιολογικά.

Αφού συνέλεξα αρκετά στοιχεία, ώστε να μπορέσω να έχω μια ολοκληρωμένη εικόνα για την κοινότητα των hackers, μελέτησα την προσφορά της στην κοινωνία και το κατά πόως επηρεάζει και επηρεάζεται από αυτήν.

### **Ανασκόπηση της βιβλιογραφίας**

Η ανασκόπηση και η μελέτη της βιβλιογραφίας είναι ένα πολύ σημαντικό κομμάτι της εργασίας. Το μεγαλύτερο μέρος της ανασκόπησης γίνεται στην αρχή της έρευνας. Συνεχίζει και στα επόμενα στάδια και τελειώνει, όταν ολοκληρωθεί η συγγραφή της μελέτης.

Στην αρχή της εργασίας αυτής ερευνήσα σε πληροφορικά λεξικά ώστε να βρω ορισμούς για τους όρους hacking, hacker, κυβερνοέγκλημα και ηλεκτρονικό έγκλημα. Στην συνέχεια διεξήγα έρευνα για να εντοπίσω και να συλλέξω όλα τα στοιχεία και τις πηγές που αφορούν το θέμα μου. Βρήκα πληροφορίες από διάφορα είδη έντυπων πηγών (βιβλία, περιοδικά, εγκυκλοπαίδειες, πρακτικά συνεδρίων, εγχειρίδια, ηλεκτρονικά έγγραφα) και τα κατέγραψα έτσι ώστε να έχω μια πληρέστερη εικόνα γύρω από το θέμα μου.

Η αναζήτηση έγινε επί το πλείστον σε πηγές του Διαδικτύου όσον αφορά τη συγκέντρωση στοιχείων και πληροφοριών από πρόσφατες έρευνες που αφορούν το hacking. Καθώς η ελληνική βιβλιογραφία, δεν είναι ιδιαίτερα εκτεταμένη σε αυτό το θέμα, οι χρήσιμες πληροφορίες αντλήθηκαν κυρίως από ξένες πηγές.

### **Διεξαγωγή έρευνας**

Αρχικά αναζήτησα τον όρο hacking σε εξειδικευμένα λεξικά πληροφορικής. Αφού ολοκλήρωσα την έρευνα μου αναζήτησα ελληνική έντυπη βιβλιογραφία. Μετά από μελέτη αυτών των έργων αποφάσισα να εστιάσω την μελέτη μου στην φιλοσοφία και την κουλτούρα των hackers και να αφήσω έξω από το πεδίο μελέτης μου το

τεχνολογικό κομμάτι του hacking. Αναζήτησα ελληνική ηλεκτρονική βιβλιογραφία χωρίς μεγάλο βαθμό ανάκτησης. Έτσι στράφηκα στην ξένη ηλεκτρονική βιβλιογραφία, κυρίως αγγλόφωνη, όπου υπήρχε αρκετό υλικό για μελέτη. Κυρίως αναζήτησα πληροφορίες μέσα από άρθρα σε διαθέτες βάσεων όπως οι ProQuest, Emerald, The ACM Portal και αγγλόφωνες εφημερίδες όπως οι New York Times και New York Daily News, καθώς και ψηφιακές βιβλιοθήκες όπως η ACM Digital Library. Επίσης σημαντικό εργαλείο στην έρευνα μου ήταν το Google Scholar μέσα από το οποίο ανακτούσα επιστημονικά άρθρα.

## **Προβλήματα**

Η κάθε έρευνα ή μελέτη που διεξάγεται παρουσιάζει δυσκολίες και προβλήματα. Έτσι, και στην παρούσα έρευνα παρουσιάστηκαν αρκετά προβλήματα. Ευτυχώς ξεπεράστηκαν τα εμπόδια και η έρευνα ολοκληρώθηκε.

Το πρώτο εμπόδιο ήταν η δυσκολία μετάφρασης των ξενόγλωσσων πηγών. Με τη βοήθεια λεξικών και μηχανών μετάφρασης όπως η Google Translation και η Altavista Translation και με εξάσκηση συνέλεξα τις πληροφορίες που χρειαζόμουν.

Πολλές πληροφορίες βρίσκονταν σε ιστολόγια και ιστοσελίδες που ανήκουν στην κοινότητα των hackers και έτσι έπρεπε να εκλεχθεί προσεχτικά το περιεχόμενο της πηγής, ώστε να κρίνω αν οι πληροφορίες αυτές ήταν έγκυρες.

Επίσης, ένα μεγάλο πρόβλημα που αντιμετώπισα ήταν η προσέγγιση του θέματος και η επαρκής κάλυψη του. Αφενός το θέμα hacking εφάπτεται σε πολλαπλά τεχνολογικά θέματα κι αφετέρου –αν και ασχολούμαι με ηλεκτρονικούς υπολογιστές— δεν γνώριζα τόσο εξειδικευμένα θέματα και ήταν πολύ δύσκολο να τα κατανοήσω. Μελετώντας το θέμα κατάλαβα ότι αυτό το κομμάτι του hacking δεν με αφορούσε και δεν επηρέαζε άμεσα το αντικείμενο που ήθελα να προσεγγίσω, δηλαδή την κουλτούρα των hackers. Αρχικά αποφάσισα να το περιγράψω επιφανειακά, ενώ αργότερα το απέκλεισα εντελώς από την εργασία μου.

Το τελευταίο μου πρόβλημα ήταν αν θα κρατούσα τους αγγλικούς όρους όπως hacker, hacking, internet κ.α. Τελικός αποφάσισα να χρησιμοποιήσω τους αγγλικούς όρους για όσους δεν έχουν ελληνική απόδοση (hacking) και να χρησιμοποιήσω σε ελληνική ορολογία για όσους έχουν ελληνική απόδοση (π.χ. Διαδίκτυο). Ειδικά για τον όρο “hacker”, επειδή στην ελληνική βιβλιογραφία τον συνάντησα πολλές φορές μεταγραμματισμένο στα ελληνικά ως «hacker» αποφάσισα να τον διατηρήσω έτσι σε όλη την εργασία.



Για την σύνταξη της βιβλιογραφίας και των παραπομπών χρησιμοποίησα το βιβλιογραφικό πρότυπο Harvard που βασίστηκε στην 6<sup>η</sup> έκδοση της Australian Government Publishing Service (AGPS).

## **Συμπεράσματα**

Στο κεφάλαιο Μεθοδολογία παρουσιάζεται ο τρόπος με τον οποίο διεξήχθη η έρευνα. Καταρχάς, δίνεται ο σκοπός και οι στόχοι που προκαθορίστηκαν για την συγκεκριμένη έρευνα. Μέσα από αυτούς δίνεται η δυνατότητα να κατανοήσουμε καλύτερα το θέμα που θα πραγματευθεί η μελέτη.

Μετά από επαρκή συλλογή πληροφοριών και μελέτη κατέληξα στο συμπέρασμα ότι τα πράγματα δεν είναι μονοδιάστατα και δεν μπορούν να χαρακτηριστούν ούτε μαύρα ούτε και άσπρα. Οι hackers είναι επιστήμονες αφοσιωμένοι στην ανάπτυξη της τεχνολογίας και με στόχο την αποδέσμευση της πληροφορίας και του Διαδικτύου τόσο από τα τέλη της όσο και από τη λογοκρισία που υφίσταται. Οι hackers είναι ευφυείς άνθρωποι, επαναστάτες. Πιστεύω ότι το hacking εκφράζει μια βαθιά εσωτερική ανάγκη που δεν έχει σχέση με την τεχνολογία. Είναι η ανάγκη για γνώση, για περιπέτεια, για εξερεύνηση και ανακαλύψεις. Οι hackers μοιάζουν πολύ με τους δημοσιογράφους που διψούν για αποκλειστικότητα και μυστικά..

Η ανασκόπηση της βιβλιογραφίας είναι από τα σημαντικότερα κεφάλαια της εργασίας. Στο κεφάλαιο αυτό εντοπίστηκαν και συγκεντρώθηκαν όλες οι διάσπαρτες πληροφορίες σχετικά με το συγκεκριμένο θέμα. Αυτό βοήθησε στην εξοικείωση του ερευνητή με το θέμα και τους ερωτώμενους. Επίσης, έγινε προσπάθεια να εκπληρωθούν οι στόχοι που προκαθορίστηκαν και να επιτευχθεί όσο το δυνατό καλύτερο αποτέλεσμα.

## ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Η βιβλιογραφική ανασκόπηση είναι η έρευνα για εντοπισμό και η μελέτη προηγούμενων τεκμηρίων για το θέμα της hacker κουλτούρας και ιδεολογίας. Η βιβλιογραφική αυτή έρευνα γίνεται με σκοπό να επιβεβαιώσει, να αμφισβητήσει ή να εμπλουτίσει προηγούμενα ευρήματα.

Η παρούσα πτυχιακή εργασία μελετά την κοινωνία των hackers προσεγγίζοντας το θέμα από κοινωνική απόψεως και εστιάζοντας σε σημεία όπως ηθική, η ιδεολογία και το παραγόμενο έργο. Η βιβλιογραφική ανασκόπηση ανέδειξε μικρό αριθμό παρόμοιων εργασιών στο χώρο των ελληνικών εκδόσεων και της ελληνικής τριτοβάθμιας εκπαίδευσης.

### Εννοιολόγηση και προέλευση του όρου

Το Jargon Lexicon<sup>1</sup> (γνωστό και ως New Hackers Dictionary) αναλύει τον όρο hacker ως εξής:

hacker: [κυριολεκτικά αυτός που φτιάχνει έπιπλα πελεκώντας το ξύλο με τσεκούρι]

1. Το άτομο που αρέσκεται να εξερευνά τις λεπτομέρειες προγραμματιζόμενων συστημάτων και τους τρόπους με τους οποίους μπορεί να επεκτείνει τις δυνατότητές τους, σε αντιδιαστολή με την πλειοψηφία των χρηστών, που προτιμούν να μαθαίνουν το ελάχιστο δυνατό.
2. Το άτομο που γράφει (μανιωδώς πολλές φορές) προγράμματα ή που απολαμβάνει περισσότερο την πρακτική παρά τη θεωρητική πλευρά του προγραμματισμού.
3. Ένα άτομο ικανό να εκτιμήσει την αξία της πειρατείας πληροφοριών.
4. Ένα άτομο ικανό να γράφει προγράμματα σε ελάχιστο χρόνο.
5. Κάποιος ειδικός στη χρήση ενός συγκεκριμένου προγράμματος ή κάποιος που δουλεύει συχνά με αυτό ή σε αυτό όπως π.χ. “Unix hacker”.
6. Ένας ειδικός ή ένας ενθουσιώδης οποιουδήποτε είδους. Μπορεί κάποιος να είναι hacker αστρονομίας, παραδείγματος χάριν.
7. Ένας που απολαμβάνει τη διανοητική πρόκληση να υπερνικήσει δημιουργικά ή να παρακάμψει τους περιορισμούς.

---

<sup>1</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

8. (Υποτιμητικά) Ένας κακόβουλος παρείσακτος που προσπαθεί να ξεθάψει πληροφορίες ψαχουλεύοντας εδώ κι εκεί. Εξού και οι όροι “password hacker”, “network hacker”. Ο σωστός όρος είναι cracker (=σπάστης).
9. Υποδηλώνει επίσης ότι το συγκεκριμένο άτομο προσυπογράφει κάποιες έστω από τις αρχές ηθικής των hacker.

Ο όρος hacker παραπέμπει στη συμμετοχή στην παγκόσμια κοινότητα που ορίζεται από το Διαδίκτυο. Αυτός ο όρος υιοθετείται αρχικά ως διακριτικό στη δεκαετία του 1960 από τους hackers που περιβάλλουν το TMRC (Tech Model Railroad Club) και το Artificial Intelligence Laboratory MIT (εργαστήριο Τεχνητής Νοημοσύνης του MIT).

### **Άλλες έννοιες σχετικές με τους hacker**

Το **hacking** θα μπορούσε να χαρακτηριστεί ως «η κατάλληλη εφαρμογή της ευφυΐας»<sup>2</sup>.

**Η ηθική των hackers (hacker ethics)** θεσπίζει ότι η ανταλλαγή πληροφοριών είναι ένα ισχυρό εφικτό καλό, και είναι μια ηθική υποχρέωση των hacker για να μοιραστούν την εμπειρία τους από το ελεύθερο λογισμικό να διευκολύνουν την πρόσβαση στις πληροφορίες και στους υπολογιστικούς πόρους, όπου αυτό είναι δυνατόν<sup>3</sup>.

Το “**freeware**” (**Free Software**), ή **ελληνιστί ελεύθερο λογισμικό**, είναι προγράμματα συχνά γραμμένα από τους λάτρεις του προγραμματισμού που διανέμονται από τους χρήστες και τις ομάδες καταναλωτών, ή μέσω ηλεκτρονικού ταχυδρομείου, των τοπικοί πήνακες ανακοινώσεων, Usenet ή μέσω άλλων ηλεκτρονικών μέσων<sup>4</sup>.

Σύμφωνα και με τον ορισμό που δίνει η επίσημη ιστοσελίδα του ελεύθερου λογισμικού, «το ελεύθερο λογισμικό είναι λογισμικό που σας δίνει στο χρήστη την ελευθερία να μοιραστούν, να σπουδάζουν και να το τροποποιήσετε. Ονομάζεται ελεύθερο γιατί η χρήση του είναι ελεύθερη»<sup>5</sup>. Αναπτύχθηκε αρχικά από τον Richard M. Stallman.

---

<sup>2</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

<sup>3</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

<sup>4</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

<sup>5</sup> *About Free Software Foundation and the GNU operating system* 2008, Free Software Foundation Inc. Διαθέσιμο στο: <<http://www.fsf.org/about>> [28 Δεκεμβρίου 2008].

Το “worm” (σκουλήκι στα ελληνικά) είναι ένα πρόγραμμα που αναπαράγει τον εαυτό του μέσω του δικτύου, πολλαπλασιάζεται και αυτοαποστέλλεται. Σήμερα ο όρος αυτός έχει αρνητική χροιά, καθώς είναι δεδομένο ότι μόνο crackers γράφουν σκουλήκια. Ίσως το πιο γνωστό παράδειγμα ήταν ο Robert T. Morris που δημιούργησε το “Internet Worm” το 1988<sup>6</sup>.

Ο **ιός υπολογιστή** είναι ένα συγκεκριμένο είδος κακόβουλου κώδικα, που αντιγράφει τον εαυτό του. Εισάγει αντίγραφα ή νέες εκδόσεις του εαυτού σε άλλα προγράμματα. Αντικαθιστά μια εντολή στο πρόγραμμα με στόχο την εντολή για την μεταβίβαση του ελέγχου για τον ιό που είναι αποθηκευμένα στη μνήμη. Κάθε φορά που το πρόγραμμα εκτελεί εντολή μεταφοράς, ευσυνείδητα μεταβιβάζει τον έλεγχο στο πρόγραμμα του ιού, το οποίο στη συνέχεια εκτελεί τις εντολές αντικαθίστανται και εκτελεί τις εργασίες της ίδιας του της ενσωμάτωσης σε άλλα προγράμματα. Υπάρχουν σήμερα πάνω από 10.000 ιοί που επηρεάζουν τους υπολογιστές και τα λειτουργικά συστήματα της Apple. Επιπλέον, λίγοι είναι οι ιοί που επηρεάζουν άλλα λειτουργικά συστήματα όπως το UNIX<sup>7</sup>.

## **Ο κόσμος των hacker**

Ελληνική βιβλιογραφία

Από τους πρώτους έλληνες συγγραφείς που ασχολήθηκαν με το θέμα των hackers είναι ο Γρηγόρης Λάζος με το έργο του «Πληροφορική και Έγκλημα». Το θέμα των hackers σήμερα είναι μπερδεμένο και εξαιτίας της προπαγάνδας των ΜΜΕ και τις προκατάληψης της κοινωνίας για τις νέες τεχνολογίες και τις τεχνολογικές καινοτομίες. «Μολονότι τα ΜΜΕ δεν υποστήριξαν την εφαρμογή του ποινικού δικαίου στον κόσμο της πληροφορικής, δημιούργησαν ένα κλίμα σοβαρού και πιθανότατου κινδύνου στην κοινή γνώμη, με την προβολή πραγματικών ή και φανταστικών ιστοριών με hackers και συχνά προσβλημένες υπό ένα πρίσμα υπερβολής»<sup>8</sup>.

Τα ΜΜΕ ίσως παρακινούμενα από άλλους υποθάλποντες οργανισμούς ή είτε για την θεαματικότητα μεγαλοποιούν γεγονότα και υπερβάλουν σε θέματα που αφορούν hackers με αποτέλεσμα να πανικοβάλλουν την μέση κοινή γνώμη. Ως εκ τούτου σε

---

<sup>6</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

<sup>7</sup> Chawki, M 2005, *A critical look at the regulation of cybercrime*, Computer Crime Research Center. Διαθέσιμο στο: <<http://www.crime-research.org/articles/Critical/>> [28 Δεκεμβρίου 2008].

<sup>8</sup> Λάζος, Γ 2001, *Πληροφορική και έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα.

συνδυασμό με την ελλιπή τεχνολογική εκπαίδευση και γνώση η κοινωνία μας δεν είναι έτοιμη να δεχθεί ένα τόσο επαναστατικό κίνημα όπως οι hackers<sup>9</sup>.

Η ανάπτυξη της πληροφορικής, πέρα από την αναμφισβήτητα θετική επίδραση στην καθημερινή μας ζωή και κυρίως ως επαγγελματικό εργαλείο, επέτρεψε και τη δημιουργία νέων μορφών εγκληματικής δράσης. Η νέα αυτή κατάσταση πραγμάτων δημιουργεί προβληματισμό και διχασμό. Οι hackers θεωρούνται εγκληματίες ή ο σύγχρονος Robin των Δασών.

“Hacker” είναι ένας τιμητικός τίτλος που χρησιμοποιούσαν οι επιστήμονες του MIT το 1960 και αναφερόταν σε άτομα ιδιοφυή που είχαν διαπρέψει στον τομέα της τεχνολογίας. Σήμερα ο τίτλος έχει γίνει πολύ ευτελής. Ο λόγος κυρίως αυτής της παρακμής είναι η κακή χρήση του όρου αυτού από τα ΜΜΕ και η παραπληροφόρηση του κοινού. Οι hackers πλασάρονται ως εγκληματίες και συγχέονται με τους crackers.

Λίγοι γνωρίζουν ότι πολλοί hackers εργάζονται για την παγκόσμια ασφάλεια και για την απελευθέρωση των πληροφοριών. Δημιουργήματα τους είναι το γνωστό σε όλους WWW (World Wide Web), το ελεύθερο λογισμικό, η εταιρία Apple και πολλά άλλα τεχνολογικά επιτεύγματα του αιώνα μας. «Με τα παιχνίδια τους, άλλωστε, οι hackers έχτισαν το Διαδίκτυο, έφτιαξαν το λειτουργικό πρόγραμμα ανοιχτού κώδικα Linux και βρήκαν την προστασία από τους ιούς»<sup>10</sup>.

«Ο πειραματισμός, το αστείο, η κακεντρεχής χαρά τού να γράφεις κώδικα λίγο πιο έξυπνο από των συναδέλφων σου, να καταστρατηγείς τα αντίμετρά τους, ήταν πάντα ακέραιο μέρος της κουλτούρας μέσα από την οποία ξεπήδησε το Διαδίκτυο. Οι hackers με τις κακές φάρσες τους βοηθούν με το να βασανίζουν και να τελειοποιούν το ανοσοποιητικό μας σύστημα»<sup>11</sup>.

«Αλλά και η κοινωνία ως σύνολο είναι ανέτοιμη ακόμη στην πλειονότητά της να κατανοήσει τις δυναμικές του μοντέρνου αυτού φαινομένου. Η έλλειψη κατάρτισης των φορέων παιδείας, γονείς – καθηγητές – σχολείο, δημιουργεί ένα κενό στη δημιουργία ενός ήθους ως προς τη χρήση υπολογιστών και φυσικά η νέα γενιά δεν διαπαιδαγωγείται με τις απαραίτητες αξίες για μια ορθή χρήση του μέσου αυτού. Εάν σε αυτό προσθέσουμε τόσο τη δικαιολογημένη επιφυλακτικότητα που κάθε ριζοσπαστικό φαινόμενο αντιμετωπίζει από την κοινωνία όσο και την επίδραση των

<sup>9</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ;: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

<sup>10</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ;: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

<sup>11</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ;: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

ΜΜΕ στον ευρύ πληθυσμό με τις συχνά υπερβολικές και ασαφείς εξιστορήσεις περιστατικών hacking, δεν είναι δύσκολο να ανακαλύψουμε γιατί η λέξη hacker ηχεί σχεδόν πάντα αρνητικά στα αυτιά μας. Εισερχόμαστε λοιπόν σε ένα φαύλο κύκλο, όπου οι κακοπροαίρετοι hackers βρίσκουν δικαιολογία για τις πράξεις τους στην αρνητικά προδιατεθειμένη κοινωνία, η οποία με τη σειρά της δαιμονοποιεί κάθε μέλος αυτής της κοινότητας ανεξαρτήτως κινήτρων, οδηγώντας συχνά ακόμη και τους πιο υγιείς ηθικά hackers στην υιοθέτηση ενός περιθωριακού έστω προτύπου συμπεριφοράς»<sup>12</sup>.

Η εργασία του Βασίλη Καραγιαννόπουλου, φοιτητή Νομικής Σχολής, είναι από τις αρτιότερες εργασίες στην Ελλάδα με θέμα τους hackers. Εμβαθύνει στην έρευνα του και αναλύει θέματα όπως η hacker κουλτούρα, η ηθική, η εγκληματικότητα, η προσφορά.

Οι παράνομες χακιστικές δραστηριότητες συμπεριλαμβάνονται στο ηλεκτρονικό έγκλημα. «Οι hackers συχνά λαμβάνουν περισσότερης προσοχής από τις κοινές και επικίνδυνες απειλές. Το Αμερικανικό Υπουργείο Δικαιοσύνης προτείνει τρεις λόγους για αυτό. Πρώτον η απειλή των hackers είναι πιο πρόσφατη, δεύτερον οι οργανισμοί δεν γνωρίζουν τις προθέσεις των hackers, τρίτον οι επιθέσεις των hackers κάνουν τους ανθρώπους να νιώθουν αδύναμους γιατί είναι ανώνυμες»<sup>13</sup>.

Φοβόμαστε τους hackers γιατί είναι κάτι άγνωστο σε εμάς, υπάρχει ημιμάθεια. Που όμως σταματά ο μύθος και που αρχίζει η πραγματικότητα. Ποίοι είναι πραγματικοί hackers και ποιοί απλά μανιακοί με του υπολογιστές. Σε μια συνέντευξη του ο Stallman όταν ρωτήθηκε αν είναι hacker δήλωσε «έτσι λένε οι άλλοι»<sup>14</sup>.

«Τις περισσότερες φορές η απάντηση ενός πραγματικού hacker είναι ότι δεν ανήκει σε αυτή την ομάδα ή ότι ξέρει μόνο κάποια απλά κόλπα»<sup>15</sup>.

Είναι καλύτερα να περιγράφεται κανείς σαν hacker από άλλους παρά να συστήνεται σαν τέτοιος. Οι hackers θεωρούν τον εαυτό τους μέλη μίας ελίτ (μιας αξιοκρατικής ομάδας που διακρίνεται για τις ικανότητες της), η οποία ωστόσο είναι πάντα ανοιχτή σε νέα μέλη. Υπάρχει λοιπόν μία ικανοποίηση όταν παρουσιάζεται κανείς σαν hacker αλλά αν ισχυρίζεσαι ότι είσαι και δεν είσαι, σύντομα θα ονομαστείς bogus/wannabee.

<sup>12</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: <[www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc)> [28 Δεκεμβρίου 2008].

<sup>13</sup> Λάζος, Γ 2001, *Πληροφορική και έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα.

<sup>14</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: <[www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc)> [28 Δεκεμβρίου 2008].

<sup>15</sup> Σαραφάς, Κ 2008, *Hackers: μύθος ή πραγματικότητα?*, Προπομπός, Αθήνα.

Σίγουρα τα πράγματα δεν είναι τόσο γαλήνια στην κοινότητα των hackers. Φυσικά και είναι δημιουργοί τεχνολογικών επιτευγμάτων είναι όμως και δημιουργοί κακόβουλων λογισμικών και υπαίτιοι διαδικτυακών βανδαλισμών. Όχι όμως όλοι. Όπως και σε κάθε κοινωνία και κοινότητα υπάρχουν επίπεδα και ποιότητες ανθρώπων. Οι hackers είναι ευφυή άτομα με πάθος την τεχνολογία. Η κοινωνία τους χωρίζονται σε κατηγορίες και τάξεις με βάση κριτήρια ικανοτήτων και με δείκτη ηθικής. Οι crackers είναι συνήθως υπαίτιοι τις για καταστροφές. Ένας hacker χτίζει δεν καταστρέφει. Στην πυραμίδα της ταξικής κατάταξης των hackers υπάρχουν πολλά επίπεδα με βάση την ηθική. Οι κακόβουλες συμπεριφορές καταδικάζονται από τους hackers και θεωρούνται κατώτερες και φθηνές.

«Πολλοί συγγραφείς κακόβουλου λογισμικού, χρησιμοποιούν έτοιμα εργαλεία που χρησιμοποιούν στο Διαδίκτυο για να εξαπολύσουν επιθέσεις, για αυτό ονομάζονται υποτιμητικά script kitties από τους πιο εξελιγμένους hacker» (Βλάχος, 2007).

Υπάρχουν και άλλες εκδόσεις ελληνικές με θέμα το hacking μεταφράσεις ξένων έργων στα οποία θα αναφερθώ πιο κάτω.

Η ελληνική αρθρογραφία ασχολείται με το θέμα hacker, συνήθως όμως ασχολούνται περισσότερο με επίκαιρα θέματα όπως η εκάστοτε επίθεση κάποιου hacker. Υπάρχει η έλλειψη μιας βαθύτερης έρευνας και πιο εμπειριστατωμένης μελέτης του θέματος.

Το περιοδικό Ram στο τεύχος 129 αναφέρεται στους hackers, αναλύει τον κόσμο τους, τα κατορθώματα τους προσεγγίζοντας το θέμα ιστορικά και κοινωνιολογικά. Είναι ένα πολύ ενδιαφέρον άρθρο.

«Οι hackers ζουν μόνο για να εισβάλλουν σε συστήματα υπολογιστών. Μετά την επίτευξη της εισβολής, προσπαθούν να μη δημιουργήσουν πρόβλημα στο σύστημα και συνήθως τις πληροφορίες που βρίσκουν εκεί τις κρατούν μόνο για τον εαυτό τους. Για αυτούς το σημαντικό είναι να φτάσουν στην Ιθάκη και όχι το τι θα κάνουν, όταν φτάσουν. Μια υποκατηγορία των hacker είναι οι Phone hackers»<sup>16</sup>.

Στα ηλεκτρονικά περιοδικά IC e-zine, Reverse Engineering, InterBIZ αναφέρονται κάποια θέματα για τους hackers αλλά εστιάζουν περισσότερο σε περιστατικά επιθέσεων των hackers.

---

<sup>16</sup> Τσουραμάνης, Χ 2005, *Ψηφιακή εγκληματικότητα : η (αν)ασφαλής όψη του διαδικτύου*, Εκδόσεις Βασ. Ν. Κατσαρού, Αθήνα.

## Διεθνή βιβλιογραφία

Στην διεθνή βιβλιογραφία παρατηρείται μία πληθώρα υλικού πολλαπλής και πολυδιάστατης προσέγγισης του θέματος. Τόσο στον χώρο των εκδόσεων βιβλίων, όσο και στην αρθρογραφία και στις επιστημονικές αναλύσεις, το θέμα έχει μελετηθεί αρκετά.

Αρχικά η πρώτη συντεταγμένη θεώρηση για τους hackers έγινε από τον Levy Steven το 1984 στο έργο του “Hackers: Heroes of the Computer Revolution”. Ήταν η πρώτη φορά που η ηθική των hackers και οι άγραφοι νόμοι τους αποτυπώνονται γραπτά, σε αυτό το αξιόλογο έργο. Όπως χαρακτηριστικά γράφει στο έργο του «Access to computers and anything which might teach you something about the way the world works should be unlimited and total. Always yield to the Hands-On Imperative!»<sup>17</sup>.

Πάνω σε αυτή την σκέψη στηρίζεται όλη η φιλοσοφία και η δράση των hackers. Η πληροφορία είναι ένα παγκόσμιο αγαθό και πρέπει να έχουμε απεριόριστη πρόσβαση σε αυτή. Οι hackers ως αγωνιστές υπέρ της ελεύθερης διακίνησης της πληροφορίας θεωρούν ότι είναι χρέος τους η απελευθέρωση της, τόσο για την πρόσβαση σε αυτή, όσο και για την τιμή της.

Μέσω της ελεύθερης ανταλλαγής αρχείων και πληροφοριών δημιουργήθηκαν μεγάλα έργα. Αυτοί οι νέοι άνθρωποι έγραφαν συναρπαστικά νέα προγράμματα ακριβώς σαν τους προκατόχους τους, αλλά κάτι νέο θα ερχόταν μαζί τους: τα προγράμματα στην οθόνη εμφανίζονταν μαζί με σημειώσεις πνευματικής ιδιοκτησίας. Για τον Stallman, που ακόμα πίστευε ότι όλη η πληροφορία έπρεπε να ρέει ελεύθερα, αυτό ήταν βλασφημία. «...δεν πιστεύω ότι το λογισμικό θα έπρεπε να ανήκει σε κάποιον, γιατί η πρακτική αυτή σαμποτάρει την ανθρωπότητα σαν σύνολο. Εμποδίζει τους ανθρώπους να λάβουν το μέγιστο όφελος από την ύπαρξη του προγράμματος»<sup>18</sup>.

Οι πρώτοι hackers (φοιτητές του MIT στα τέλη της δεκαετίας του 1960) εξειδικεύτηκαν στο να κατασκευάζουν λεπτομερή σχέδια τηλεφωνικών κυκλωμάτων και στο να ανιχνεύουν τα κυκλώματα και τους διακόπτες ρύθμισης του συστήματος μετάδοσης του δικτύου του MIT.

Αξίζει να σημειωθεί η γλωσσική εξέλιξη της έννοιας "hacker". Ο όρος έχει χρησιμοποιηθεί για να εκφράσει το σεβασμό και το θαυμασμό για την ανώτερη εμπειρία προγραμματισμού υπολογιστών. Τα τελευταία δέκα χρόνια –ιδίως μεταξύ

<sup>17</sup> Levy, S 1984, *Hackers: heroes of the computer revolution*, Penguin Books, New York.

<sup>18</sup> Levy, S 1984, *Hackers: heroes of the computer revolution*, Penguin Books, New York.



των μελών των οργάνων επιβολής του νόμου— ωστόσο, η έννοια έχει αναλάβει μια εξαιρετικά αρνητική σημασία και χρησιμοποιείται για βάνδαλους ηλεκτρονικών υπολογιστών. Οι hackers δεν είναι εγκληματίες. Είναι άτομα που προσπαθούν να απαλλάξουν το μαζικό προϊόν από τις μεγιστοκερδικές αντιλήψεις και να το φέρουν πιο κοντά στις συγκεκριμένες ανάγκες των χρηστών που το χρησιμοποιούν. Γίνεται μια συλλογική προσπάθεια να απεγκλωβιστεί το υλικό από τις εμπορευματικές του ιδιότητες. Για αυτό τον λόγο σαμποτάρονται από τις κερδοσκοπείς εταιρίες που προσπαθούν να αλυσοδέσουν την πληροφορία<sup>19</sup>.

## Η hacker κουλτούρα και πολιτισμός

Ο πολιτισμός των hackers είναι ένας φιλελεύθερος πολιτισμός που αντιστέκεται στον κυβερνητικό έλεγχο, το μυστικισμό και εναντιώνεται στους κολοσσούς του βρόμικου κέρδους που εκμεταλλεύονται το Διαδίκτυο. Αξιόλογο είναι το έργο του Thomas Douglas με τίτλο “Hacker culture”. Ο Douglas εστιάζει εύστοχα στον πολιτισμό των hackers και δημιουργεί μια μελέτη με θέμα την υποκουλτούρα των hackers. Το hacking επισημαίνει ο συγγραφέας δεν ήταν ποτέ μια αποκλειστική τεχνική διαδικασία. Είναι ένα σύμπλεγμα πολιτικοοικονομικών και τεχνολογικών παραγόντων.

Η εικόνα των hackers διακυμαίνεται από την εικόνα ενός hi-tech επιστήμονα μέχρι το προφίλ ενός στυγνού εγκληματία. Οι hackers δεν βλέπουν τον εαυτό τους σαν εγκληματία αλλά σαν ένα σύγχρονο επαναστάτη. Λύνουν προβλήματα και χτίζουν πράγματα. Πιστεύουν στην ελευθερία και στην εθελοντική αμοιβαία βοήθεια. Η κουλτούρα των hackers βασίζεται σε δύο βασικά χαρακτηριστικά της ιδεολογία τους, στην απόλαυση της λύσης προβλημάτων και στη πεποίθηση ότι η ελευθερία είναι αγαθή. «Ναι, είμαι εγκληματίας. Το έγκλημά μου είναι αυτό της περιέργειας. Το έγκλημά μου είναι αυτό της κρίσης των ανθρώπων από αυτά που λένε και σκέφτονται, όχι από αυτό που μοιάζουν. Το έγκλημά μου δεν θα μου συγχωρήσετε ποτέ το ξέρω. Είμαι hacker, και αυτό είναι το μανιφέστο μου. Μπορείτε να σταματήσετε αυτό το άτομο, αλλά όχι τους επόμενους».<sup>20</sup>

Η «υπόγεια» κοινότητα των hackers (underground groups) αποτελείται από κάποιες ομάδες που καταργούν το μύθο ότι οι hackers δεν είναι κοινωνικά άτομα. Οι

---

<sup>19</sup> Chiesa, R, Ciappi, S & Ducci, S 2008, *Profiling hackers: the science of criminal profiling as applied to the world of hacking*, CRC Press, Boca Raton.

<sup>20</sup> Douglas, T. 2003, *Hacker Culture*, Minnesota Press, Minneapolis

ομάδες hackers αποτελούνται από άτομα που οργανώνονται με σκοπό την ανταλλαγή πληροφοριών και την προώθηση και θέσπιση των δικαιωμάτων και των συμφερόντων τους. Οι ομάδες hackers είναι ένα μέσο προώθησης των πληροφοριών σε άλλα μέλη και στο κοινό. Μέσα από αυτές οι hackers αποκτούν αξιοπιστία.

Στο έργο του Richard Gissel “Digital underworld: computer crime and resulting Issues” γίνεται μια αξιότιμη αναφορά στις ομάδες hackers και στην ιστορία της δημιουργίας τους. Κάποιες από τις ομάδες αυτές είχαν κηρύξει πόλεμο μεταξύ τους. Κάποιες είχαν υψηλό προφίλ και κοινωνικούς/ πολιτικούς στόχους, μάχονταν για ιδανικά όπως η ελευθερία του λόγου και της έκφρασης, άλλες ήταν κατωτέρου επιπέδου. Πολλές γίνονταν γνωστές μετά από κάποιο χτύπημα τους και την ενασχόληση των ΜΜΕ μαζί τους, όπως για παράδειγμα η ομάδα Chos Computer Club (CCC). «...η CCC έγινε διάσημη όταν χάραξαν το γερμανικό BILDSCHIRMTEXT (videotex διαδραστικό σύστημα) δίκτυο υπολογιστών και πέτυχαν να πάρουν μια χρέωση τραπεζών σε απευθείας online λογισμός για 134.000 δολάρια στο όνομα της ομάδας»<sup>21</sup>.

Ο Gissel αναφέρει επίσης συνοπτικά την βιογραφία πολλών ένδοξων hackers, οι οποίοι πέρασαν από το σκοτεινό παρασκήνιο του hacking στο νόμιμο.

Οι hacker διαχωρίζονται σε τρεις κατηγορίες, τους λευκούς hacker (white hacker) που εργάζονται για το καλό της παγκόσμιας ασφάλειας, τους γκριζούς που κυμαίνονται ανάμεσα στις άλλες δύο κατηγορίες και τους μαύρους hacker που λειτουργούν για προσωπικά συμφέροντα και προκαλούν βανδαλισμούς, συνήθως αυτοί ονομάζονται crackers.

Ο καθένας κάνει τις επιλογές του σύμφωνα με τα πιστεύω του και τα κίνητρα του. Ο Steven Furnell κάνει μια έρευνα για τα κίνητρα της κάθε κατηγορίας και τα παρουσιάζει στο έργο του “Cybercrime: vandalizing the information society”. «...το κίνητρο για τους περισσότερους είναι απλώς η διασκέδαση και η πρόκληση που μπορεί να αποφέρει ένα παιχνίδι με το σύστημα. Υπάρχουν πολλά να μάθει κανείς και όταν κάποιος καταφέρνει να υποτάξει την πολυπλοκότητα, τότε η αίσθηση του κατορθώματος είναι μεγάλη»<sup>22</sup>.

Οι hackers έχουν κοινά πιστεύω και αντιλήψεις. Οι ίδιοι βλέπουν τον εαυτό τους σαν τον σύγχρονο cowboy του εικονικού κόσμου, ή σαν τον Robin των Δασών.

---

<sup>21</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο : Google Books Search [29 Δεκεμβρίου 2008].

<sup>22</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

Σκοπός τους είναι να απελευθερώσουν τη γνώση και να λειτουργούν υπέρ του κοινού καλού. Συχνά όμως παράνομες πράξεις υποστηρίζονται από τέτοιου είδους ιδεαλιστικά υπόβαθρα. Η παρανομία και οι κακόβουλες πράξεις δεν είναι κάτι που υποστηρίζεται από την κοινότητα των hackers, απόδειξη ότι οι καινοτόμοι και ηθικοί hacker χαρακτηρίζονται ως elit, ενώ οι παράνομοι που χρησιμοποιούν έτοιμα εργαλεία για την δράση τους υποβαθμίζονται στον τίτλο των kiddies.

Παρόλο που υπάρχουν σοβαρές κυρώσεις επιβολής του νόμου από τις παράνομες δραστηριότητες hacking, οι hackers συνεχίζουν την δράση τους. Η μελέτη των Randall Young, Lixuan Zhang και Victor R. Prybutok “Hacking into the minds of hackers” παρουσιάζει τα αποτελέσματα μιας έρευνας για τους hackers σχετική με τις αντιλήψεις τους όσο αφορά στην παράνομη δραστηριότητα του hacking. Τα αποτελέσματα δείχνουν ότι οι hackers συνεχίζουν να επιδίδονται σε παράνομες δραστηριότητες hacking παρά τις ποινικές διώξεις. Μια πιο προσεκτική ματιά δείχνει ότι hackers αντιλαμβάνονται την υψηλή αξία της γνώσης που αποχτούν από το hacking, η οποία είναι πολύτιμη και πολύ μικρές οι κυρώσεις, καθώς θεωρούν ότι υπάρχει μια πολύ χαμηλή πιθανότητα τιμωρίας. Αυτές οι αντιλήψεις σε συνδυασμό με ένα υψηλό επίπεδο ηθικής απεμπλοκής εξηγούν την παράνομη συμπεριφορά του hacker. «...υπάρχουν ποινές για την διάπραξη των εγκλημάτων hacking και είναι αρκετά σοβαρές. Οι hackers δεν τις λαμβάνουν υπόψη τους, επειδή διακατέχονται από ένα αίσθημα αλαζονείας, της πεποίθησης ότι υπερέχουν του νόμου και των υπόλοιπων ανθρώπων»<sup>23</sup>.

Οι hackers προκαλούν αναστάτωση στο χώρο της γνώσης και η κοινή γνώμη διχάζεται. Το ερώτημα που δημιουργείται είναι αν πρέπει η γνώση να διαχέεται ελεύθερα στο κοινό ή πρέπει να υπάρχει κάποιος φραγμός. Στο άρθρο του Tom Cross “Academic freedom and the hacker ethic” (2007) αναπτύσσονται ενδιαφέρουσες απόψεις. Η ακαδημαϊκή κοινότητα τάσσεται υπέρ της άποψης ότι η γνώση που αποχτούν οι hackers δεν πρέπει να διαχέεται στο κοινό. Οι hackers από την πλευρά τους υποστηρίζουν ότι καμία πληροφορία δεν πρέπει να δεσμεύεται. «...οι hackers υποστηρίζουν την ελεύθερη άσκηση και την κοινή χρήση των γνώσεων, χωρίς περιορισμό, αν και αναγνωρίζουν ότι η εφαρμογή είναι κάτι άλλο» .

---

<sup>23</sup> Young, R, Zhang, L & Prybutok, V 2007, ‘Hacking into the minds of hackers’, *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

Ο Wark McKenzie είναι υποστηρικτής της δράσης των hackers και στο βιβλίο του «Ένα Μανιφέστο των Hacker» διευρύνει τον όρο και θεωρεί hacker όλους όσους τάσσονται υπέρ της ελεύθερης διακίνησης της πληροφορίας. Επίσης ως hackers χαρακτηρίζονται όσοι δημιουργούν γνώση την οποία προσπαθούν να μονοπωλήσουν οι μεγάλες εμπορευματικές εταιρίες. «...αυτό το περιμάχητο έδαφος, η σφαίρα της αποκαλούμενης «πνευματικής ιδιοκτησίας», προκαλεί ένα τελείως νέο είδος ταξικής πάλης, που φέρνει αντιμέτωπους τους δημιουργούς της πληροφορίας –την τάξη των hackers, που απαρτίζουν ερευνητές και συγγραφείς, καλλιτέχνες και βιολόγοι, χημικοί και μουσικοί, φιλόσοφοι και προγραμματιστές— με μια τάξη ιδιοκτητών, οι οποίοι θέλουν να μονοπωλήσουν ό,τι ο hacker παράγει»<sup>24</sup>.

---

<sup>24</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα.

# ΚΕΦΑΛΑΙΟ 1: ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

## 1.1 Κοινωνία της Πληροφορίας

Κοινωνία της πληροφορίας είναι η δική μας κοινωνία, ο τρόπος ζωής μας, η καθημερινότητα μας. Πολλές φορές έχουμε ακούσει ότι οι φλέβες της κοινωνίας μας είναι οι πληροφορίες –οι ηλεκτρονικές κατά κύριο λόγο— και ότι ολόκληρο το σύστημα αυτής της κοινωνίας στηρίζεται στους ηλεκτρονικούς υπολογιστές. Οι φλέβες όμως και οι αρτηρίες αυτού του συστήματος αιμορραγούν. Τι σημαίνει αυτό; Σημαίνει ότι πρέπει να επανεξετάσουμε τα θεμέλια αυτής της κοινωνίας και να επιστημόνουμε τα τρωτά της σημεία.<sup>25</sup>

Η τεχνολογία της πληροφόρησης επηρεάζει και στηρίζει κοινωνία της πληροφορίας. Δεν θα ήταν καθόλου υπερβολή αν λέγαμε ότι η δεύτερη βασίζεται και λειτουργεί χάρη στις άπειρες δυνατότητες που χαρίζει η πρώτη. Είναι απόλυτα εξαρτώμενη από αυτήν. Η ταχύτητα ανάπτυξης και εκτέλεση των εφαρμογών της πληροφορικής προσφέρει τόσα πλεονεκτήματα και σε τέτοιο βαθμό που επηρεάζει καταλυτικά την παιδεία, το κράτος την οικονομία, τις ανθρώπινες σχέσεις σε βαθμό άμεσης εξάρτησης.

Προσεγγίζοντας ιστορικά το θέμα βλέπουμε αρχικά μια αγροτική κοινωνία βασισμένη αποκλειστικά σε αγροτικές εργασίες όπως η κτηνοτροφία και η καλλιέργεια της γης που για πολλούς αιώνες αποτελούσαν τη βασική μορφή της κοινωνίας. Την αγροτική κοινωνία ακολούθησε η βιομηχανική επανάσταση (1750-1850) που άλλαξε ριζικά τη ζωή των ανθρώπων. Διαμόρφωσε μια νέα κοινωνία που δεν βασίζεται πια αποκλειστικά στην εκμετάλλευση της γης, αλλά χαρακτηριστικό της είναι η εκμετάλλευση των υγρών καυσίμων και ανάπτυξη μεγάλων εργοστασίων, καθώς και η οικονομία στηριζόταν στην επεξεργασία των φυσικών αγαθών. Όταν κατά τη δεκαετία του 1940 κάνουν την εμφάνιση τους οι ηλεκτρονικοί υπολογιστές δίνουν νέα ώθηση στη βιομηχανία και η μορφή της κοινωνίας αλλάζει ριζικά για ακόμα μια φορά. Η ανταλλαγή και η διακίνηση των πληροφοριών είναι το επίκεντρο των δραστηριοτήτων της νέας αυτής κοινωνίας που ορθώς ονομάστηκε κοινωνία της πληροφόρησης. Γίνεται λόγος εδώ για δυο αλληλοεπιδρώμενες έννοιες, την κοινωνία

---

<sup>25</sup> Furnell, S 2006, *Κυβερνοέγκλημα : καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

της πληροφορίας η οποία επηρεάζει και επηρεάζεται από την τεχνολογία της πληροφορίας και οι δύο μαζί επηρεάζουν την ζωή του ανθρώπου.<sup>26</sup>

Η πληροφοριακή επανάσταση με όλο τεχνολογικό εξοπλισμό (hardware), αλλά και τον άυλο (software) ήρθε για να αλλάξει την ζωή μας καθοριστικά υπηρετώντας τον άνθρωπο να καλυτερέψει τις συνθήκες ζωής του ή εκμηδενίζοντας τον, αντικαθιστώντας αυτόν. Οι ηλεκτρονικοί υπολογιστές εισέβαλαν στην ζωή μας και την άλλαξαν άρδην μετά την μείωση του κόστους τους. Σήμερα ο μέσος άνθρωπος μπορεί να έχει στην κατοχή του έναν προσωπικό υπολογιστή (personal computer). Επανάσταση στον χώρο της τεχνολογίας αλλά αποτέλεσε η ανάπτυξη του Παγκόσμιου Ιστού (World Wide Web – WWW), το οποίο έχει πλέον γίνει κομμάτι της καθημερινότητας μας. Όταν όμως αναπτύχθηκε και άρχισε την λειτουργία του ARPANET, ο πρόδρομος του σημερινού Διαδικτύου, αναπτύχθηκε στη φιλελεύθερη φιλοσοφία της ελεύθερης ανταλλαγής πληροφοριών και δεδομένων. Πολλά ήταν τα ιδρύματα που δημιούργησαν τα υπολογιστικά τους συστήματα χωρίς καμία προστασία. Επειδή όμως το Διαδίκτυο ήταν και είναι ένας χώρος που διακινούνται πολλά χρήματα λόγω του ηλεκτρονικού εμπορίου, καθώς και πολύτιμες πληροφορίες υπήρξε ένα εύκρατο κλίμα και ιδανικό περιβάλλον για την ανάπτυξη του πληροφοριακού εγκλήματος. Έτσι η πληροφορική τεχνολογία, το εγχείρημα της επανάληψης του κοινωνικού συστήματος σε εικονική μορφή, κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων που εκτείνονται από ανήθικο μέχρι και το εγκληματικό<sup>27</sup>. Ίσως είναι το πλέον αρνητικό στοιχείο της πληροφοριακής τεχνολογίας.

Ως «ηλεκτρονικό έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την νομοθεσία<sup>28</sup>. Ο νόμος έρχεται να επιβάλλει τα όρια της ηθικής και της ανηθικότητας στα πλαίσια της νομιμότητας. Να ορίσει δηλαδή τι είναι ηλεκτρονικό έγκλημα και πληροφοριακή κακοχρηστία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση ηλεκτρονικών υπολογιστών (computer crime) και σε κυβερνοεγκλήματα (cyber crime), αν τελέσθηκε μέσω του Διαδικτύου.

---

<sup>26</sup> Kellerman A.2000, “Phases in the rise of the information society”, *Info - The journal of policy, regulation and strategy for telecommunications*, vol. 2, no.6, pp. 537-541. Διαθέσιμο στο: Emerald [15 Νοεμβρίου 2008].

<sup>27</sup> Λάζος, Γ 2001, *Πληροφορική και έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα.

<sup>28</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

Μέχρι τα μέσα της δεκαετίας του 1970 το ηλεκτρονικό έγκλημα ως έννοια και αντικείμενο δεν διαφοροποιούταν από την ευρύτερη έννοια του εγκλήματος. Μέσα σε λίγα χρόνια η προσοχή των ειδικών εστιάστηκε περισσότερο στις ιδιαιτερότητες αυτής της μορφής της εγκληματικότητας και αντιμετωπίζεται πλέον ως χωριστό αντικείμενο. Είναι μία μορφή εγκλήματος που αποτελείται από τους δικούς του δράστες και δράσεις που εξελίσσονται σε άλλο επίπεδο και επιβάλουν μια άλλη και πιο προσεγμένη αντιμετώπιση. Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Μια συνοπτική κατηγοριοποίηση των μορφών του ηλεκτρονικού εγκλήματος έγινε από το “Convention on Cybercrime” (του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην συνθήκη που υπογράφει στην Βουδαπέστη στις 23.11.2001)<sup>29</sup>, τα οποία είναι:

1. Τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών (hacking).
2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη μέσω ηλεκτρονικών υπολογιστών και πλαστογραφία.
3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας.
4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

## 1.2 Συνοπτική ιστορία του Διαδικτύου

Επειδή οι ηλεκτρονικοί υπολογιστές και η δικτύωση τους συντελέστηκαν στον δυτικό (κυρίως) κόσμο δεν δόθηκε μεγάλη σημασία στην ασφάλεια τους. Ο πρόδρομος του Διαδικτύου, το ARPANET, είχε σχεδιαστεί από το Υπουργείο Άμυνας των ΗΠΑ ως μια μέθοδος ανταλλαγής πληροφοριών μεταξύ της κυβέρνησης, των ερευνητικών κέντρων και των εκπαιδευτικών οργανισμών. Έτσι πολλά τεχνολογικά ιδρύματα έστησαν υπολογιστικά συστήματα σχεδόν χωρίς κανένα μέτρο ασφάλειας.

---

<sup>29</sup> *Convention on Cybercrime* 2001, Council of Europe, Budapest. Διαθέσιμο στο: <<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>> [15 Νοεμβρίου 2008].

Το Διαδίκτυο είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές που εκτείνεται σχεδόν σε κάθε γωνιά του πλανήτη και παρέχει τις υπηρεσίες του σε εκατομμύρια χρήστες. Αποτελεί ένα «παγκόσμιο ηλεκτρονικό χωριό», οι κάτοικοι του οποίου μοιράζονται πληροφορίες και ανταλλάσσουν ελεύθερα απόψεις πέρα από γεωγραφικά και κοινωνικά σύνορα ανεξάρτητα από υπηκοότητα, ηλικία, θρήσκευμα και χρώμα.

### 1.2.1 Δεκαετία 1960: ένα ενδιαφέρον πείραμα ξεκινά

Στα πανεπιστήμια των ΗΠΑ οι ερευνητές ξεκινούν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο ARPANET γεννιέται το 1969 με πόρους του προγράμματος ARPA (Advanced Research Project Agency) του Υπουργείου Άμυνας, με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή.<sup>30</sup>

Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας, ακόμα και σε περίπτωση πυρηνικού πολέμου καθώς ήταν η εποχή του Ψυχρού Πολέμου. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνθεσή του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης. Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.<sup>31</sup>

### 1.2.2 Δεκαετία 1970: οι πρώτες συνδέσεις

Το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται “Internetting Project” (Πρόγραμμα Διαδικτύωσης) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η

---

<sup>30</sup> Marson, S.M. 1997, “A selective history of Internet technology and social work”, *Computers in Human Services*, vol. 14, no. 2, pp. 35 – 49. Διαθέσιμο στο: ACM portal. [15 Νοεμβρίου 2008].

<sup>31</sup> Dreyfus, H.L. 2003, *Το διαδίκτυο*, Κριτική, Αθήνα.



διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται μια νέα τεχνολογία, το Διαδίκτυο Protocol (IP) (Πρωτόκολλο Διαδικτύωσης) από την οποία θα πάρει αργότερα το όνομά του το Διαδίκτυο. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε τελικά οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με οποιονδήποτε άλλον.<sup>32</sup>

Επίσης, σχεδιάζεται μια άλλη τεχνολογία για τον έλεγχο της μετάδοσης των δεδομένων το Transmission Control Protocol (TCP – Πρωτόκολλο Ελέγχου Μετάδοσης). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (File Transfer Protocol -- FTP) και για το ηλεκτρονικό ταχυδρομείο (Electronic Mail - e-mail). Σταδιακά συνδέονται με το ARPANET ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Μεγάλη Βρετανία) και το Royal Radar Establishment (Νορβηγία).<sup>33</sup>

### 1.2.3 Δεκαετία 1980: ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα

Το 1983, το πρωτόκολλο TCP/IP (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος Berkeley UNIX, το οποίο περιλαμβάνει το TCP/IP συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών. Εκατοντάδες πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983, χωρίζεται σε δύο τμήματα: στο MILNET για στρατιωτικές επικοινωνίες, και στο νέο ARPANET για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση.<sup>34</sup>

Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το NSFnet χρησιμοποιώντας το πρωτόκολλο TCP/IP προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του 1980, όλο και περισσότερες χώρες συνδέονται στο NSFnet όπως ο Καναδάς, η Γαλλία, η Σουηδία, η Αυστραλία, η Γερμανία, η Ιταλία, κ. ά. Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει

<sup>32</sup> Λεάνδρος, Ν. 2005, *Το διαδίκτυο : ανάπτυξη και αλλαγή*, Καστανιώτης, Αθήνα.

<sup>33</sup> Dreyfus, H.L. 2003, *Το διαδίκτυο*, Κριτική, Αθήνα

<sup>34</sup> Marson, S.M. 1997, "A selective history of Internet technology and social work", *Computers in Human Services*, vol. 14, no. 2, pp. 35 – 49. Διαθέσιμο στο: ACM portal. [15 Νοεμβρίου 2008].

να γίνεται γνωστό σαν «ΔΙΑΔΙΚΤΥΟ» και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Το 1990, το ARPANET πλέον καταργείται επίσημα.<sup>35</sup>

#### 1.2.4 Δεκαετία 1990: ένα παγκόσμιο δίκτυο για όλους

Όλο και περισσότερες χώρες συνδέονται στο NSFnet, μεταξύ των οποίων και η Ελλάδα το 1990.

Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (WWW – Παγκόσμιος Ιστός) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Διαδίκτυο σε ολόκληρο τον κόσμο και παρουσιάσής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας την απλουστευμένη τεχνική του διπλού κλικ.

Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Διαδίκτυο προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Διαδίκτυο διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Διαδίκτυο (Internet Service Providers - ISPs) και προσφέρουν πρόσβαση για όλους. Οποιοσδήποτε διαθέτει ηλεκτρονικό υπολογιστή και modem μπορεί να συνδεθεί με το Διαδίκτυο σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFnet καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα.<sup>36</sup>

Η ανακάλυψη του Παγκόσμιου Ιστού σε συνδυασμό με την ευκολία απόκτησης πρόσβασης στο Διαδίκτυο προσέελκυσε έναν μεγάλο αριθμό καινούργιων χρηστών επιφέροντας την «έκρηξη» της τελευταίας δεκαετίας. Σήμερα, το μεγαλύτερο μέρος του πληθυσμού της Γης ζει σε χώρες που είναι συνδεδεμένες στο Διαδίκτυο. Καθημερινά περιοδικά και εφημερίδες εκδίδονται «on-line» και μας παραπέμπουν στις διευθύνσεις τους, ενώ για τις επιχειρήσεις η διαδικτυακή παρουσία κρίνεται σχεδόν απαραίτητη και ολοένα περισσότεροι ιδιώτες δημιουργούν τις δικές τους ιστοσελίδες. Είναι προφανές ότι το Διαδίκτυο δεν αποτελεί πλέον ένα δίκτυο των φοιτητών και των ερευνητών, αλλά ότι επεκτείνεται και επιδρά στις καθημερινές πρακτικές όλων. Το ηλεκτρονικό εμπόριο, η τηλε-εργασία, η τηλε-εκπαίδευση είναι πια μέρος της καθημερινότητας πολλών ανθρώπων.

---

<sup>35</sup> Λεάνδρος, Ν. 2005, Το διαδίκτυο : ανάπτυξη και αλλαγή, Καστανιώτης, Αθήνα.

<sup>36</sup> Παπαδημητρίου, Χ. (2004) Ισόβια στους χάκερ; : απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα. Αθήνα, Καστανιώτης

### 1.3 Ορισμοί

Αν και η χρήση και η σημασία του όρου μπορεί να ποικίλει, Για να κατανοήσουμε τον όρο hacker θα παραθέσω πιο κάτω διάφορους ορισμούς όπως αυτοί εμφανίζονται σε διάφορα λεξικά πληροφορικής.

Ένας πρώτος ορισμός οριοθετεί τον hacker ως «ένα φανατικό των υπολογιστών ειδικά κάποιος που μέσω ενός προσωπικού υπολογιστή εισβάλλει σε ένα σύστημα υπολογιστών μιας εταιρίας, κυβέρνησης, κλπ.»<sup>37</sup>.

Ένας πιο απλός ορισμός περιγράφει τον hacker ως «ένα πρόσωπο που χρησιμοποιεί υπολογιστές προκειμένου να αποκτήσει πρόσβαση δίχως άδεια σε δεδομένα»<sup>38</sup>.

Οι δύο ορισμοί δεν αποκλίνουν ιδιαίτερα αναμεταξύ τους αναγνωρίζοντας ως απαραίτητο χαρακτηριστικό την άριστη γνώση και χειρισμό της τεχνολογίας των υπολογιστών και μάλιστα σε επίπεδο που ξεπερνάει αυτό του μέσου χρήστη.

Για να κατανοηθεί ο κόσμος των hackers και η λειτουργία του κρίνεται αναγκαίο να παρατεθεί μια σύντομη ιστορική αναδρομή ώστε να διαπιστωθούν οι αλλαγές που υπέστη με το πέρασμα του χρόνου, να μελετηθούν τα χαρακτηριστικά της κουλτούρα τους, τις δραστηριότητες τους και γενικότερα την κοσμοθεωρία τους.

Ο όρος προέρχεται από το ρήμα “hack” που σημαίνει «σπάζω, κομματιάζω»<sup>39</sup>, ενώ ο όρος “hacker” στην κυριολεξία σημαίνει «αυτός που κόβει κάτι σε κομματάκια». Η λέξη hacker είναι μια παρομοίωση αφού μπορεί να σημαίνει ότι καταστρέφει κάτι, μπορεί όμως και να σημαίνει ότι απλά αναλύει κάτι. Στις αρχές της δεκαετίας του 1970 η λέξη άλλαξε νόημα και αναφερόταν σε κάποιον που ήταν πάρα πολύ καλός στον προγραμματισμό των ηλεκτρονικών υπολογιστών και πολύ πρόθυμος να κάνει αυτή τη δουλειά.

Ο όρος hacking είναι πολύ πιθανό να προέρχεται από τα μικρά προγράμματα, που ονομάστηκαν hackers (εργαλεία κοπής) και που ήταν πολύ συνηθισμένα τον πρώτο καιρό των υπολογιστών, όταν ο προγραμματισμός ήταν μια πολύ δύσκολη και επίπονη εργασία και μόνο για πολύ λίγους και φυσικά μόνο σε γλώσσα μηχανής. Οι

---

<sup>37</sup> ‘Hacker’, *Collins English dictionary*, 1994, HarperCollins, Glasgow.

<sup>38</sup> ‘Hacker’, *The new oxford dictionary of English*, 1998, Oxford University Press, New York.

<sup>39</sup> Sdictionary community, 2009, *Greek etymological dictionary*, AXMA Soft. Διαθέσιμο στο: <[http://sdict.com/cgi-bin/sdict.cgi/browse?dicname=ilhs\\_mel.dct&letter=&word=&offset=](http://sdict.com/cgi-bin/sdict.cgi/browse?dicname=ilhs_mel.dct&letter=&word=&offset=) Greek Etymological Dictionary> [18 Νοεμβρίου 2008].

προγραμματιστές που δημιουργούσαν τέτοιες εντολές για να διευκολύνονται στη δουλειά τους ονομάστηκαν hackers.<sup>40</sup>

Το hacking είναι φιλοσοφία ζωής που δεν αφορά μόνο τους υπολογιστές αλλά και άλλα πολλά πράγματα. Είναι μάθηση υπολογιστών, δικτύων, κρυπτογράφησης, τηλεφωνικών συστημάτων, συστήματα κατασκοπείας, τα μυστικά που κρύβει η κυβέρνηση. Θα μπορούσε ακόμα να ονομαστεί το τρίτο μάτι που βλέπει στα παρασκήνια<sup>41</sup>.

Ο όρος πρωτοεμφανίστηκε όταν μια ομάδα ατόμων εργαζόταν για το πρώτο ψηφιακό πείραμα του ARPANET γύρω στο 1950, και ήταν ένας τιμητικός τίτλος για τους πρωτοπόρους στον τομέα των υπολογιστών που αποδόθηκε σε αυτούς ως ένδειξη σεβασμού για τις θαυμαστές ικανότητες τους στους υπολογιστές. Συγκεκριμένα ο όρος αποδιδόταν σε άτομα μεγαλοφυή, γκουρού των προγραμμάτων και των υπολογιστών, άτομα ικανά να βρίσκουν λύσεις σε περίπλοκα τεχνικά προβλήματα. Δεν είχε καμία σχέση με εγκληματικότητα και παρανομία (στοιχεία που εμπερικλείει ο σημερινός ορισμός του hacker). Οι χαρισματικοί αυτοί προγραμματιστές θεωρούσαν την τεχνολογία ως μέσο ελευθερίας και όχι ως εργαλείο πρόκλησης ζημιάς σε τρίτους. Σήμερα ο όρος αποδίδεται σε άτομα που αποκτούν παράνομα πρόσβαση σε δεδομένα μέσω υπολογιστή και συχνά συγχύζεται ο όρος «hacker» με τον όρο «cracker».<sup>42</sup>

Σήμερα για τον πολύ κόσμο, ο όρος hacker σημαίνει λανθασμένα τον ταλαντούχο φανατικό των ηλεκτρονικών υπολογιστών που σκορπά την καταστροφή. Οι ίδιοι οι hackers ενοχλούνται απ' αυτόν τον χαρακτηρισμό και ξεχωρίζουν τους εαυτούς τους από τους κακόβουλους hackers ή crackers (criminal hackers), οι οποίοι έχουν ως στόχο την πρόκληση ζημιών σε μεγάλα δίκτυα υπολογιστών, την δημιουργία ή/και την εξάπλωση ιών και την κυβερνοτρομοκρατία.

Ο συνδυασμός εξουσίας, τεχνογνωσίας και εξασφαλισμένης ανωνυμίας, που υπήρχε στον κοινότητα των hackers, επέδρασε σαν ακαταμάχητος πειρασμός στα νεαρά αγόρια των δεκαετιών του 1980 και του 1990. Καταλυτικό ρόλο στην εξέλιξη του hacking έπαιξε η προβολή της ταινίας (War Games – Παιχνίδια Πολέμου) στις

---

<sup>40</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: <[www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc)> [8 Δεκεμβρίου 2008].

<sup>41</sup> Duvel, 2007, 'A brief history of the underground scene', *Phrack Magazine*, 64. Διαθέσιμο στο: <<http://www.phrack.com/issues.html?issue=64&id=4#article>> [20 Νοεμβρίου 2008].

<sup>42</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: <[www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc)> [8 Δεκεμβρίου 2008].

αρχές της δεκαετίας του 1980, η οποία ταινία στηρίχθηκε σ' ένα πραγματικό γεγονός.<sup>43</sup>

Υπάρχει μια λανθασμένη εντύπωση για τους hackers και αυτό οφείλεται σε μεγάλο βαθμό από την προβολή που δίνουν στο θέμα τα ΜΜΕ, θέλοντας να δημιουργήσουν ένα αίσθημα μυστηρίου γύρω από τους hackers επηρέασαν την κοινή γνώμη με αποτέλεσμα να ομαδοποιηθούν οι hackers με τους crackers. Στην παρανόηση αυτή συνέβαλε και το Hollywood δημιουργώντας ταινίες με κεντρικό θέμα το hacking. Οι παραγωγοί ταινιών έχουν καταλάβει ότι πρόκειται για ένα ενδιαφέρον και πλούσιο θέμα που αφορά και συναρπάζει πολλοί κοινό.

Το πρόβλημα όμως ήταν ότι ενώ το hacking είναι ενδιαφέρον στην ταινία ήταν κάπως βαρετό να αναπαραστήσει όλη αυτή τη διαδικασία, ένα τύπο δηλαδή που μπροστά από την οθόνη του υπολογιστή του σπάει κωδικούς και εισβάλλει σε δίκτυα. Έτσι επιβαλλόταν η πρόσθεση δράσης και αγωνιάς, που ως αποτέλεσμα είχε να παρουσιάζονται οι hackers επιθετικοί, μανιασμένοι και εγκληματικοί. Εικόνα που είναι πολύ μακράν από την πραγματική εικόνα του hacker. Ποία άτομα όμως θα χαρακτηρίζαμε hackers;

Σύμφωνα με το κείμενο “The Jargon File” hacker είναι «ένα άτομο περίεργο που του αρέσει να ασχολείται με τους υπολογιστές και να δοκιμάζει τις δυνατότητες του σε περίπλοκα τεχνολογικά προβλήματα. Άτομα που απολαμβάνουν τον προγραμματισμό και τον θεωρούν ως διασκέδαση και μπορούν να προγραμματίζουν με πολύ γρήγορους ρυθμούς. Ένα άτομο ικανό να εκτιμήσει την αξία της διείσδυσης. Κάποιος που απολαμβάνει την πνευματική κόπωση και είναι φίλος των προκλήσεων και της παράβασης των κανονισμών»<sup>44</sup>.

Κάποιο κακόβουλο άτομο που ψάχνει και ανακαλύπτει ευαίσθητες πληροφορίες, οι λεγόμενοι hackers κωδικών πρόσβασης, αυτά τα άτομα δεν ανήκουν κατεξοχήν στους hackers αλλά περνούν σε άλλη κατηγορία, τους crackers. Σε αντίθεση με τον hacker, ως cracker θεωρείται κάποιος που παραβιάζει την ασφάλεια ενός συστήματος. Ο cracker είναι άτομο (ή ομάδα ατόμων) που αποπειράται να αποκτήσει πρόσβαση σε υπολογιστικό σύστημα για την οποία όχι μόνο δε διαθέτει εξουσιοδότηση, αλλά με

---

<sup>43</sup> Furnell, S. 2006, *Κυβερνοέγκλημα : καταστρέφοντας την κοινωνία της πληροφορίας*, Αθήνα, Παπαζήσης

<sup>44</sup> Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <<http://catb.org/jargon>> [28 Δεκεμβρίου 2008].

στόχο να το βλάψει με οποιοδήποτε τρόπο<sup>45</sup>. Είναι οι προγραμματιστές που σπάνε παράνομα τους κωδικούς προστασίας εφαρμογών που ίσως να αποτελεί μια τεχνολογική πρόκληση για τους ειδήμονες των υπολογιστών, όμως σε καμιά περίπτωση δεν δικαιολογείται ειδικά αν δημοσιευτούν τα σπασμένα προγράμματα! Ο όρος αυτός επινοήθηκε από τους hackers το 1985 για να διαχωρίσουν την θέση τους από τα άτομα αυτά που τα θεωρούν υποδεέστερα. Ενώ οι crackers συχνά αυτοαποκαλούνται hackers ή και τα ΜΜΕ τους αποκαλούν έτσι. Οι αυθεντικοί hackers δεν τους αποδέχονται αφού είναι αντίθετοι με την ηθική τους. Οι crackers δεν είναι μαύροι (black hat) hacker αλλά ανήκουν στο ηλεκτρονικό έγκλημα και συχνά συνεργάζονται αναμεταξύ τους.<sup>46</sup>

Οι crackers είναι εξ' ορισμού κακόβουλοι. Ο όρος hacker είναι ένδειξη σεβασμού και αποδίδεται σε άτομα μεγαλοφυή και όχι σε κακόβουλους εισβολείς υπολογιστικών συστημάτων. Κύρια διαφορά ανάμεσα hackers και crackers είναι ότι οι πρώτοι συνέφεραν στην οικοδόμηση του σημερινού Διαδικτύου, ενώ οι crackers στην αλλοίωση του.

#### 1.4 Συνοπτική ιστορία του hacking

Ο όρος hacker δεν έχει την ίδια σημασία την οποία είχε το 1950 δεν έχει όμως ξεπέσει στο επίπεδο των crackers. Οι πρώτοι hackers ονομάζονταν πραγματικοί προγραμματιστές. Ήταν μηχανικοί με γνωστικό υπόβαθρο στη φυσική. Το σημερινό τους προσωνύμιο θα ήταν "geeks" (σπασίκλης)<sup>47</sup>.

Οι hackers εμφανίστηκαν μετά το τέλος του 2<sup>ου</sup> Παγκοσμίου Πολέμου, όταν οι φοιτητές του MIT (Massachusetts Institute of Technology) υιοθέτησαν το PDP-1<sup>48</sup> και έγινε το πρώτο εκπαιδευτικό ίδρυμα το οποίο έδωσε ιδιαίτερη σημασία στην τεχνολογία των υπολογιστών ανοίγοντας νέους ορίζοντες στην τεχνολογία των υπολογιστών. Ήταν το κυρίαρχο κέντρο το οποίο επηρέασε την ανάπτυξη του ARPANET. Για πρώτη φορά χρησιμοποιείται ο όρος hacker. Το ARPANET ένωσε όλους τους hackers των ΗΠΑ και έγινε η πρώτη κύρια πηγή για hacking. Οι πιο

---

<sup>45</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: [www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc) [8 Δεκεμβρίου 2008].

<sup>46</sup> Μαύρος hacker είναι ο hacker που είναι ταγμένος με την εγκληματική πλευρά του hacking.

<sup>47</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

<sup>48</sup> Το PDP-1 (Programmed Data Processor-1) ήταν ο πρώτος υπολογιστής της Digital Equipment Corporation's PDP και κατασκευάστηκε το 1960. Ήταν πολύ ξακουστός και ήταν ο σημαντικότερος και καλύτερος υπολογιστής στην κουλτούρα των hackers. Το PDP-1 ήταν επίσης το μηχάνημα στο οποίο παίχτηκε το πρώτο ηλεκτρονικό παιχνίδι, το Steve Russell's Spacewar.

πολλοί hackers ήταν φοιτητές και όχι άτομα που κατείχαν κυβερνητικές θέσεις. Οι φοιτητές ήταν μέρος της κουλτούρας των hackers και βοήθησαν σημαντικά στην προώθηση του Παγκόσμιου Ιστού. Συνέχισαν να χρησιμοποιούν τα νέα προγράμματα δικτύου όπως το UNIX μέχρι την αρχή της δεκαετίας του 1970. Το UNIX λόγω της χρηστικότητας του σε σύγκριση με το ARPANET έγινε το κυρίαρχο εργαλείο δικτύωσης των hackers σε όλα τα πανεπιστήμια της Αμερικής<sup>49</sup>.

Έτσι δημιουργήθηκε μια άλλη ομάδα έχοντας ως κεντρικό σημείο της κουλτούρας της το λειτουργικό σύστημα UNIX. Η φιλοσοφία των hackers παρέμεινε πιστή, δηλαδή στη βελτίωση της χρήσης του λογισμικού. Στα τέλη του 1970 αναπτύχθηκαν νέες τεχνολογίες και για τους hackers. Οι προσωπικοί υπολογιστές και οι ομάδες του δικτύου Usenet βοήθησαν στην δημιουργία ενός «παράδεισου» για τους hackers. Όταν το 1990 οι προσωπικοί υπολογιστές έγιναν πιο δημοφιλείς και σε πιο προσιτή τιμή, ο κάθε hacker μπορούσε να έχει το χώρο εργασίας του σπίτι του παρά σε κάποιο εργαστήριο.

Οι hackers είναι ενάντια στη λογοκρισία και στην επιβολή των νόμων. Είναι από την φύση τους ανατρεπτικοί και έχουν αναρχικό πνεύμα. Ο αναρχικός τους χαρακτήρας σε συνδυασμό με την ευφυΐα τους είναι ο λόγος που κινούν την προσοχή των κυβερνήσεων. Οι hackers έχουν επικηρυχθεί από την κυβέρνηση και παρακολουθούνται από πράκτορες διαφόρων κυβερνητικών υπηρεσιών των ΗΠΑ. Συχνά οι συναντήσεις των hackers παρακολουθούνται από πράκτορες, που δεν έχουν σκοπό να προβούν σε συλλήψεις αλλά σκοπός τους είναι η κατασκοπία των νέων τεχνολογικών επιτευγμάτων και των ιδεών που προέρχονται από τα συνέδρια αυτά όπως το συνέδριο της DEFCON<sup>50</sup>. Οι πράκτορες μπορούν να δουν από πρώτο χέρι τα εργαλεία και να παρακολουθούν τις εξελίξεις στον χώρο των hackers, να έχουν τα μάτια τους ανοικτά για νέες απειλές ή για κάποιο λαμπρό νέο, ο οποίος μπορεί να ξεχωρίζει για τις ικανότητες του!!!<sup>51</sup>

Το 1980 εμφανίστηκε ο πρώτος ιός υπολογιστών από ένα ατύχημα και προκάλεσε κατάρρευση του δικτύου ARPANET. Το 1983 η προβολή της ταινίας “War Games” (Παιχνίδια Πολέμου) επηρέασε σημαντικά πολλά νέα παιδιά, ώστε αποφάσισαν να μιμηθούν τον πρωταγωνιστή της ταινίας και να γίνουν οι πρώτοι hackers. Η ταινία

---

<sup>49</sup> Turgeman, G.O. 2005, “Hackers' Accounts Hacking as a Social Entertainment”, *Social Science Computer Review*, vol. 23, no. 1, pp. 8-23. Διαθέσιμο στο: Sage Publignation. [20 Νοεμβρίου 2008].

<sup>50</sup> DEFCON είναι το ετήσιο διεθνές συνέδριο των hackers.

<sup>51</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την Κοινωνία της Πληροφορίας*, Παπαζήσης, Αθήνα.

αυτή –που αποτέλεσε σταθμό στην ιστορία του hacking— και σύμφωνα με το σενάριό της ένα νεαρό παιδί είχε εμπλακεί παίζοντας κατά λάθος με τον υπολογιστή του σε μια ψηφιακή σύρραξη μεταξύ των τότε υπερδυνάμεων ΗΠΑ και Σοβιετικής Ένωσης. Η ταινία προσέδωσε στο hacking μια νέα διάσταση καθώς έφερε στο προσκήνιο τα ψηφιακά παιχνίδια και τον υπόκοσμο της πληροφορικής.<sup>52</sup>

Το 1988 έκανε την εμφάνισή του ένας ιός, το γνωστό σκουλήκι (worm) του Διαδίκτυου, το οποίο αναπαράχθηκε με πολύ γρήγορους ρυθμούς σε χιλιάδες υπολογιστές που ήταν συνδεδεμένοι στο Διαδίκτυο. Ο φοιτητής που το δημιούργησε συνελήφθη και καταδικάστηκε. Το 1989 συνελήφθη και καταδικάστηκε ο πιο γνωστός απ’ όλους τους hackers, ο Αμερικανός Kevin Mitnick, για κλοπή προγραμμάτων λογισμικού και για εξαπάτηση τηλεφωνικής εταιρείας. Την εποχή εκείνη έκαναν την εμφάνισή τους και οι πρώτοι νόμοι για την καταδίκη των hackers.

Τα επόμενα χρόνια θα πολλαπλασιαστούν οι επιθέσεις σε υπολογιστικά συστήματα στρατιωτικών, κυβερνητικών, τραπεζικών και πανεπιστημιακών εγκαταστάσεων αλλά και στις ιστοσελίδες πολλών οργανισμών και υπηρεσιών.

Το 1999 έκανε την εμφάνισή του ο ιός Melissa, ο οποίος διαδιδόμενος παγκοσμίως μέσω του Διαδίκτυου κατάφερε να κάνει ζημιά σε χιλιάδες υπολογιστές. Ο δημιουργός του ιού συνελήφθη από τις αρχές των ΗΠΑ. Το 2000 έκανε την εμφάνισή του ένας νέος τρόπος επίθεσης, ο γνωστός με τον όρο DDoS (Distributed Denial of Service), που είχε ως αποτέλεσμα την κατάρρευση των εξυπηρετητών ιστού (web servers) πολλών μεγάλων εταιρειών στον χώρο του Διαδίκτυου από την προγραμματισμένη αποστολή χιλιάδων αιτήσεων για δεδομένα.

Την ίδια χρονιά έκανε την εμφάνισή του και ένας άλλος ιός που άφησε εποχή, ο γνωστός ως “I Love You”, ο οποίος κατάφερε και πάλι μέσω του Διαδίκτυου να προξενήσει ζημιά σε χιλιάδες υπολογιστές ανά τον κόσμο. Η διάδοσή του γινόταν αυτόματα μέσα από το βιβλίο διευθύνσεων (address book) των ανυποψίαστων χρηστών του Διαδικτύου.

Ο όρος “hacker” καλύπτει ένα μεγάλο εύρος χρηστών υπολογιστών, ενώ οι ίδιοι οι hackers διαχωρίζονται σε εξειδικευμένες κατηγορίες ανάλογα με τις προθέσεις των

---

<sup>52</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.



προσπαθειών τους, ορισμένες από τις οποίες ανήκουν στη «σκοτεινή» πλευρά. Γενικά υπάρχουν 3 κατηγορίες hackers<sup>53</sup>:

- 1. Λευκοί– Hackers (White Hat):** είναι οι hackers με το άσπρο καπέλο. Το χρώμα είναι συμβολικό και περιγράφει την «αγνότητα» των προθέσεων αυτού του είδους των hackers. Χαρακτηρίζονται ως οι «ηθικοί» hacker. Στόχος τους είναι να καταπολεμήσουν το ηλεκτρονικό έγκλημα και τους μαύρους (black hat) hackers . Συνήθως είναι οι ειδικοί ασφαλείας και οι διαχειριστές συστημάτων. Πολλοί τέτοιοι hacker δουλεύουν για μεγάλες εταιρίες λογισμικών και λειτουργικών συστημάτων και εργάζονται για το καλό των συστημάτων ασφαλείας.
- 2. Μαύροι– Hackers (Black Hat):** είναι αυτοί που εμπλέκονται στο ηλεκτρονικό έγκλημα. Αποκτούν πρόσβαση σε συστήματα χωρίς να έχουν άδεια και συχνά με σκοπό να υποκλέψουν πληροφορίες προκαλώντας ζημία στο σύστημα. Χρησιμοποιούν τις γνώσεις τους σε οργανωμένες ομάδες φτιάχνοντας παράνομα προγράμματα, όπως ηλεκτρονικούς ιούς και κατασκοπευτικά προγράμματα. Διεισδύουν σε δίκτυα και τα κατασκοπεύουν, σπάνε κωδικούς από ιστοσελίδες και τις καταστρέφουν ή αλλάζουν την αρχική σελίδα (διαδικασία που ονομάζεται “deface”). Το κίνητρο τους είναι χρηματικό στις περισσότερες περιπτώσεις και όχι ιδεολογικό. Όταν μιλάμε για το οργανωμένο ηλεκτρονικό έγκλημα, πίσω του κρύβονται συνήθως εταιρίες και οργανωμένες ομάδες από έμπειρους προγραμματιστές και όχι μεμονωμένα άτομα. Τα άτομα αυτά αποτελούν τους hackers της σκοτεινής πλευράς. Αν και ο ορισμός του μαύρου-Hacker μοιάζει με αυτόν του cracker, δεν πρέπει να γίνεται σύγχυση γιατί οι crackers δεν δημιουργούν προγράμματα, χρησιμοποιούν έτοιμα εργαλεία που έχουν κατασκευάσει οι hackers.
- 3. Γκρίζοι– Hackers (Grey Hat):** είναι μια ενδιάμεση κατηγορία στην οποία ανήκουν τα άτομα που τα κίνητρα τους δεν είναι ξεκάθαρα ή αλλάζουν στην πορεία. Μιλάμε για hackers που παραβιάζουν το νόμο χωρίς κακόβουλους στόχους. Κίνητρο τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Μπορεί να ανακαλύψουν κενά ασφαλείας ξένων δικτύων ή προγραμμάτων και να τα σπάσουν για να αποδείξουν την αδυναμία τους.

---

<sup>53</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την Κοινωνία της Πληροφορίας*, Παπαζήσης, Αθήνα

Για να διακριθεί όμως καλύτερα η διαφορά ανάμεσα στο άσπρο και στο μαύρο – δηλαδή το καλό και το κακό— θα πρέπει να γίνει μια πιο λεπτομερή κατηγοριοποίηση που να βασίζεται στα κίνητρα και τους σκοπούς κάθε υποκατηγορίας<sup>54</sup>:

- **Κυβερνοτρομοκράτες (Cyberterrorists)**: τρομοκράτες που χρησιμοποιούν τεχνικές των hackers για να απειλήσουν ή να βλάψουν υπολογιστικά συστήματα. Η δράση των ατόμων αυτών γίνεται με βάση κάποιο πολιτικό, κυβερνητικό ή κοινωνικό σκοπό. Για παράδειγμα στόχος τους είναι να πλήξουν κάποια άλλη κυβέρνηση
- **Κυβερνοπολεμιστές (Cyber-fighters)**: η δράση των ατόμων αυτών σχετίζεται με στρατιωτικά θέματα. Χρησιμοποιούν τεχνικές των hackers και επιτίθενται σε συστήματα ζωτικής σημασίας π.χ. οικονομικές συναλλαγές, επείγουσες υπηρεσίες
- **Χακτιβιστές (Hacktivists)**: παραλλαγή της λέξης ακτιβιστής (άτομο ενεργητικό, δραστήριο, διαμαρτυρόμενο) συχνά διαδηλώνουν με τον τρόπο τους παραποιώντας ιστοσελίδες. Εισβάλλουν σε συστήματα για να υποστηρίξουν ακτιβιστικές απόψεις
- **Δημιουργοί επιβλαβών προγραμμάτων (Creators of harmful programs)**: είναι τα άτομα που είναι υπεύθυνα για την δημιουργία επιβλαβών προγραμμάτων όπως οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι
- **Φρίκερ (Phone hackers ή phreakers)**: είναι οι hackers των τηλεφώνων. Μαζεύουν πληροφορίες –συνήθως από τους κάδους απορριμμάτων των τηλεφωνικών εταιρειών— τις οποίες χρησιμοποιούν για να πραγματοποιούν δωρεάν αλλά και μη ανιχνεύσιμες τηλεφωνικές κλήσεις. Όπλα τους επίσης είναι τα λεγόμενα «κουτιά» διαφόρων χρωμάτων (κόκκινο, μπλε κ.λπ.), ιδιότυπες ηλεκτρονικές ιδιοκατασκευές, τις οποίες χρησιμοποιούν για να ξεγελούν τα τηλεφωνικά δίκτυα. Η δράση τους μπορεί να ποικίλει από την απλή εξερεύνηση του δικτύου μέχρι και την εκμετάλλευση στοιχείων. Στο σημείο αυτό μπορεί να ειπωθεί ότι σχεδόν όλοι οι hackers είναι και Phone hackers λόγω ανάγκης να έχουν μη ανιχνεύσιμη τηλεφωνική πρόσβαση, ώστε να μπορούν να πραγματοποιούν τις επιθέσεις τους

---

<sup>54</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

- **Σαμουράι (Samurai):** γνωστοί και ως sneakers, άτομα που προσλαμβάνονται για να διεξάγουν νόμιμες δραστηριότητες cracking σχετικές με υπολογιστικά συστήματα
- **Κλέφτες προγραμμάτων (pocket monkeys ή code kiddies):** άτομα με περιορισμένες ικανότητες hacking που βασίζονται σε προγράμματα γραμμένα από άλλους και συχνά προκαλούν ζημιές και βανδαλισμούς για διασκέδαση
- **Πειρατές λογισμικού (Ware d00dz):** ειδικοί στη διακίνηση κλεμμένου λογισμικού. Μόλις κυκλοφορήσει το καινούριο πακέτο λογισμικού μιας εταιρίας, αμέσως αυτό βρίσκεται στις βάσεις δεδομένων των Ware d00dz και στη διάθεση οποιουδήποτε έχει πρόσβαση σε αυτές. Μια καλή επίδοση είναι η λεγόμενη «0 day», όταν δηλαδή το κλεψίτυπο κυκλοφορεί στις βάσεις των Ware d00dz ταυτοχρόνως με την κυκλοφορία του αυθεντικού προγράμματος στα ράφια των καταστημάτων. Όμως οι πραγματικά καλές ομάδες Ware d00dz διαθέτουν στις βάσεις τους τα προγράμματα πολύ πριν αυτά κυκλοφορήσουν στο εμπόριο.

Μια άλλη κατηγοριοποίηση είναι αυτή που παρουσιάζει ο Duvel στο άρθρό του στο Phrack magazine “A brief history of the Underground scene”<sup>55</sup>. Το σημερινό σκηνικό του hacking απαρτίζεται από τρεις κατηγορίες που μπορούν να απεικονιστούν με την μορφή μιας πυραμίδας. Ο συγγραφέας αποφεύγει να δώσει όνομα σε κάθε κατηγορία, αλλά αντιθέτως αρκείται μόνο να τις ονομάσει Επίπεδο 1, Επίπεδο 2 και Επίπεδο 3.

#### 1.4.1 Επίπεδο 1

Σύμφωνα με τον συγγραφέα πριν πέντε χρόνια –περίπου γύρω στο 2002— υπήρχαν κάποιες αξιόλογες ομάδες με ταλαντούχα παιδιά που πρόσφεραν πολλά στην παγκόσμια διαδικτυακή ασφάλεια. Το επίπεδο αυτό χωρίζεται σε δύο κατηγορίες τους “Front-end groups” και “Back-end groups”. Στη κατηγορία των front-end κατατάσσονται οι ομάδες:

- Η ομάδα TESO (typo, edi, stanly, oxigen), οι οποίοι είναι προγραμματιστές υπολογιστών εξειδικευμένοι στη διαδικτυακή ασφάλεια και έρευνα

<sup>55</sup> Duvel, 2007, ‘A brief history of the underground scene’, *Phrack Magazine*, 64. Διαθέσιμο στο: <<http://www.phrack.com/issues.html?issue=64&id=4#article>> [20 Νοεμβρίου 2008].

- Η ομάδα THC (The Hacker Choice) μια μη-εμπορική ομάδα ειδικών προγραμματιστών υπολογιστών οι οποίοι ασχολούνται με τη θεωρητική και τεχνική ασφάλεια των υπολογιστών και των δικτύων
- Η ομάδα W00W00 είναι ο μεγαλύτερος μη-κερδοσκοπικός οργανισμός ασφάλειας υπολογιστών στον κόσμο.

Στους back-end ανήκουν οι ομάδες:

- Η ομάδα AMD (Advanced Micro Devices) είναι κερδοσκοπική εταιρία παροχής ασφάλειας υπολογιστών
- Η ομάδα SYNERGY εμπορική επιχείρηση που παρέχει προγράμματα ασφαλείας υπολογιστών.

#### 1.4.2 Επίπεδο 2

Πρόκειται για ομάδες χαμηλότερης κλίμακας επιδόσεων και ποιότητας από το Επίπεδο 1, οι οποίες όμως διατηρούν επικοινωνία με το Επίπεδο 1. Τέτοιες ομάδες είναι οι Τέτοιες ομάδες είναι οι TOXYN (Toxyn Technologies), NETRIC (Netric Security Team), FELINEMENACE (μια από τις τελευταίες ομάδες phrack που ασχολούνται με την αποκρυπτογράφηση).

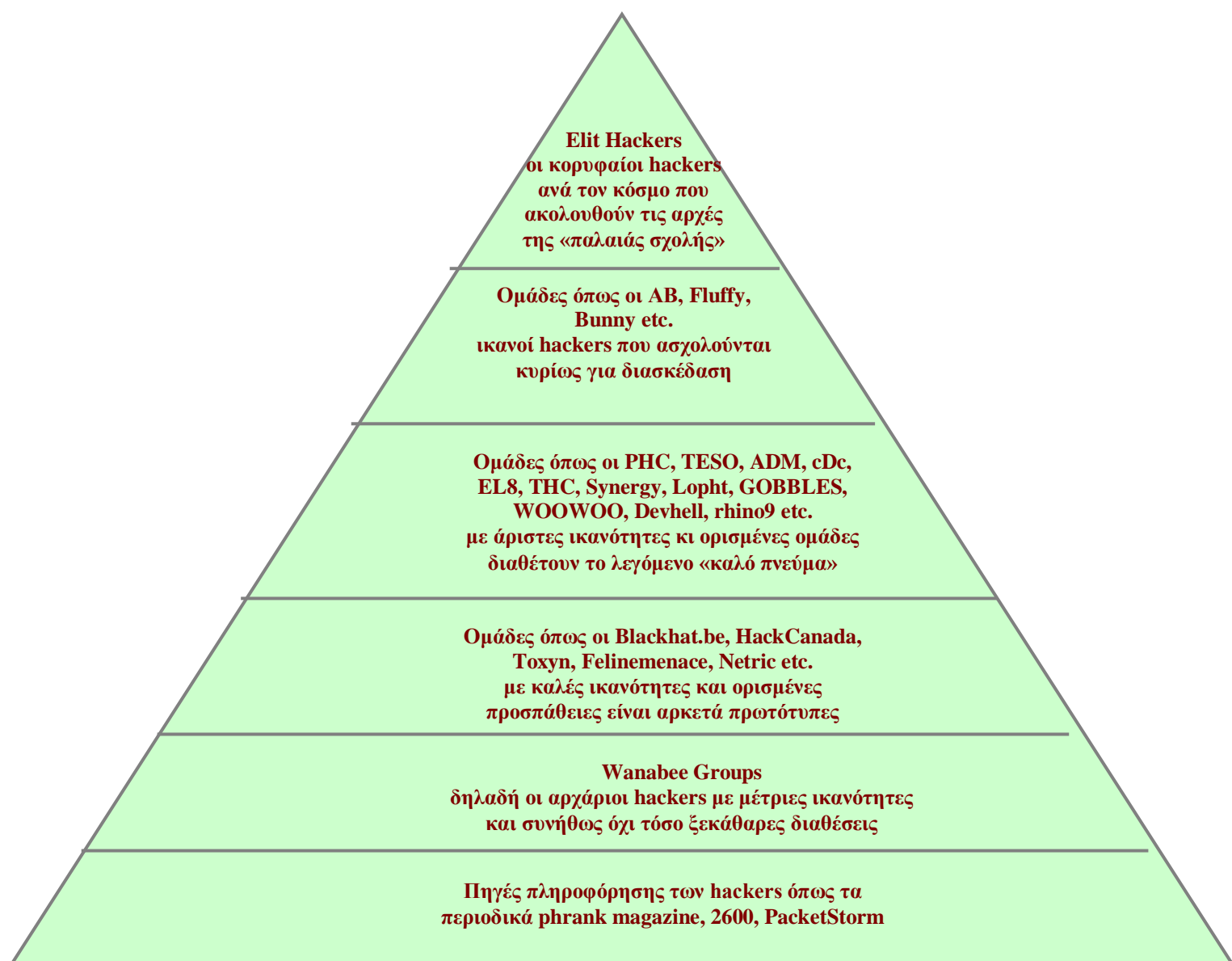
#### 1.4.3 Επίπεδο 3

Εδώ κατατάσσονται κάποιες «αισιόδοξες» ομάδες που αποτελούνται από την νέα γενιά των hackers. Μερικές από αυτές τις ομάδες έχουν πολλές δυνατότητες αλλά τα περισσότερα από αυτά τα παιδιά έμαθαν hacking σε κάποιο σχολείο ή από περιοδικά για hacking. Οι hackers που συχνά συλλαμβάνονται τις περισσότερες φορές ανήκουν σε αυτή την κατηγορία.

Τα τρία βασικά στοιχεία της πυραμίδας είναι αυτά. Στην κορυφή ωστόσο βρίσκονται κάποιες εκλεκτές ομάδες, η elit θα λέγαμε, όπως για παράδειγμα η ομάδα AB. Σε κατώτερη βαθμίδα βρίσκονται οι πηγές πληροφόρησης για hackers όπως το phrack magazine, 2600, PacketStorm κ.ά.

Η κατηγοριοποίηση αυτή γίνεται με βάση τις ικανότητες των hackers και όχι με την ηθική τους ή την ιδεολογία τους. Όλοι αυτοί οι hackers συνθέτουν το σημερινό σκηνικό του hacking, που στην πραγματικότητα πρόκειται για ένα μείγμα από άσπρους, μαύρους και γκριζούς hackers.

## THE UNDERGROUND PYRAMID<sup>56</sup>



Εικόνα 1: Πυραμίδα κατηγοριοποίησης των hackers

### 1.5 Κίνητρα πίσω από τις πράξεις των hackers

Οι λόγοι που οδηγούν κάποια άτομα να εκτελούν επιθέσεις βασίζονται σε κίνητρα που διαφέρουν για τον καθένα και έχουν να κάνουν τόσο με την προσωπικότητα του κάθε επιτιθέμενου όσο και με το κέρδος που προκύπτει από αυτές τις ενέργειες. Από καταθέσεις όσων συνελήφθησαν, οι λόγοι που ωθούν αυτούς τους νέους ανθρώπους να πειραματίζονται με τα δίκτυα είναι συνήθως η απλή προσωπική ευχαρίστηση, η διασκέδαση ακόμη και η περιέργεια. Κάποιοι από αυτούς δείχνουν ιδιαίτερο

<sup>56</sup> Duvel 2007, A brief history of the Underground scene. *Phrack Magazine*, 64. Διαθέσιμο στο Διαδίκτυο: <<http://www.phrack.com/issues.html?issue=64&id=4#article>> [20 Νοεμβρίου 2008].

ενδιαφέρον σε ειδικότερα θέματα, όπως είναι τα ανθρώπινα δικαιώματα, η αυτοδιάθεση των λαών, η προστασία των ζώων και μια σειρά από άλλα κοινωνικού περιεχομένου θέματα. Όμως τις περισσότερες φορές είναι η διασκέδαση και η περιέργεια, η ευχαρίστηση της κατάρρευσης ενός στόχου και της τόνωσης του εγώ. Η ευχαρίστηση της κόπωσης και της πρόκλησης.<sup>57</sup>

Μέσα σε ένα χώρο όπως το Διαδίκτυο ο καθένας μπορεί να κινηθεί ελεύθερα και να πάρει όποιο ρόλο θέλει, πράγμα που δεν συμβαίνει στον συμβατό κόσμο. Κρυμμένος πίσω από μια οθόνη μπορεί κανείς να φανερώσει τον πραγματικό του εαυτό ή το alter ego του. Χαρακτηριστικά όπως το φύλλο, η σεξουαλική ταυτότητα, τα πιστεύω ή εθνικότητα κ.ο.κ. δεν αποτελούν στοιχεία διάκρισης –πράγμα που συμβαίνει στον πραγματικό κόσμο— όταν είναι κάποιος συνδεδεμένος με το δίκτυο. Μπορεί κανείς να κρατήσει την ανωνυμία του και να εμφανίζεται σαν κάποιος άλλος που στην πραγματικότητα θα ήθελε να ήταν.

Πολλοί από τους hackers είναι εθισμένοι στο Διαδίκτυο και η έλλειψη του τους προκαλεί δυσάρεστα συναισθήματα. Από έρευνες που έχουν γίνει φαίνεται ότι το πρόβλημα του εθισμού στο Διαδίκτυο αυξάνεται συνεχώς. Στην Ελλάδα 1 στα 6 παιδιά έχει προβλήματα από την υπερβολική χρήση Διαδικτύου και 1 στα 100 είναι πλέον εθισμένο και έχει άμεση ανάγκη απεξάρτησης. Πάνω από το 18% των Ελληνόπουλων παρουσιάζουν περιοδικά ή συχνά προβλήματα σχετικά με την κατάχρηση του Διαδικτύου<sup>58</sup>. Όπως αναφέρει ο Κωνσταντίνος Σ. Ναλμπάντης σε ένα άρθρο του σύμφωνα με έρευνες στη Γερμανία έχει διαπιστωθεί ότι ο εγκέφαλος χρηστών υπολογιστών και του Διαδικτύου ενεργοποιείται με παρόμοιο τρόπο όπως των αλκοολικών για παράδειγμα. Σε μανιώδεις χρήστες του Διαδικτύου έδειξαν φωτογραφίες από υπολογιστές, μπύρα και οινόπνευματώδη ποτά και τα αποτελέσματα ήταν ότι οι αλκοολικοί και μανιώδεις χρήστες έδειξαν ορμές του εγκεφάλου παρόμοιων μοντέλων που αρχικά ενεργοποιούν τον εγκέφαλο<sup>59</sup>.

---

<sup>57</sup> Lakhani, K. & Wolf, B 2005, “Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects”, *Perspectives on Free and Open Source Software*. Διαθέσιμο στο: <<http://freesoftware.mit.edu/papers/lakhaniwolf.pdf>> [20 Νοεμβρίου 2008].

<sup>58</sup> Σπυρόπουλου, Λ 2008, ‘Η κατάχρηση του Ίντερνετ φέρνει εθισμό’, *Ελευθεροτυπία*, 18 Ιανουαρίου. Διαθέσιμο στο: <[http://www.enet.gr/online/online\\_text/c=112,dt=18.01.2008,id=62418256](http://www.enet.gr/online/online_text/c=112,dt=18.01.2008,id=62418256)> [20 Δεκεμβρίου 2008].

<sup>59</sup> Ναλμπάντης, ΚΣ 2008, ‘Η υπερβολική χρήση του Internet’, *Τετράδιο.gr*, 21 Μαΐου. Διαθέσιμο στο: <[http://www.tetradio.gr/html/modules/pico2/index.php?content\\_id=2](http://www.tetradio.gr/html/modules/pico2/index.php?content_id=2)> [20 Νοεμβρίου 2008].

Το hacking για πολλούς είναι ο συνδυασμός δύναμης και ανωνυμίας, η ηδονή της απόκτησης της μυστικής γνώσης<sup>60</sup>. Ίσως να μπορεί να ειπωθεί ότι οι hackers ότι είναι περίεργοι εξερευνητές του Διαδικτύου, που αναζητούν κρυμμένα μυστικά χωρίς να προκαλούν κακό. Αυτή θα ήταν μια πολύ ωραιοποιημένη εικόνα της κατάστασης και μη ρεαλιστική. Σε ορισμένες περιπτώσεις μπορεί και να ισχύει αλλά παράλληλα το hacking μπορεί να χρησιμοποιηθεί για να επιτευχθούν σκοποί όχι και τόσο νόμιμοι. Συνοψίζοντας ορισμένα από τα κίνητρα που ωθούν κάποιους σε αυτή την τεχνική είναι τα ακόλουθα<sup>61</sup>:

- **Από κακία ή εκδίκηση:** σε αυτήν την περίπτωση ο επιτιθέμενος νιώθει μίσος για τον στόχο του και θέλει να προκαλέσει ζημιά σε αυτόν, συνήθως παίρνοντας με αυτόν τον τρόπο εκδίκηση για κάποιο γεγονός που συνέβη στο παρελθόν και για το οποίο νιώθει ότι αδικήθηκε. Ένα τέτοιο παράδειγμα θα μπορούσε να είναι ένας υπάλληλος μίας εταιρίας που απολύθηκε και θέλει να πάρει εκδίκηση
- **Για το γόητρο:** διεισδύοντας σε υποτιθέμενα γνωστά καλά ασφαλισμένα δίκτυα, προσπαθούν να εντυπωσιάσουν τους ομοϊδεάτες τους και να διευρύνουν την φήμη τους. Κάτι τέτοιο θα μπορούσε να τους βοηθήσει και στη μετέπειτα επαγγελματική τους καριέρα
- **Για το κέρδος:** υπάρχουν εταιρίες που στα πλαίσια του ανταγωνισμού με τους αντίπαλούς τους προσλαμβάνουν επαγγελματίες μαύρους- hackers ή crackers με σκοπό να εισβάλουν στα συστήματα του ανταγωνιστή και να κατασκοπεύσουν τα σχέδιά του, ή ακόμα και να του προκαλέσουν προβλήματα και καταστροφές
- **Από περιέργεια ή χόμπι:** Είναι αρκετοί που πραγματοποιούν τέτοιου είδους ενέργειες είτε γιατί δεν έχουν κάτι καλύτερο να κάνουν και θέλουν να ξεφύγουν από την ανία τους είτε γιατί διακατέχονται από αυξημένη περιέργεια και τους αρέσει να «ψάχνουν τα ξένα πράγματα». Τέτοιου είδους άτομα συνήθως δεν γνωρίζουν αρκετά για αυτό που κάνουν και αγνοούν τους κινδύνους που προκύπτουν από αυτήν την δραστηριότητά τους, καθώς θεωρείται παράνομη και μπορεί να οδηγήσει στην νομική δίωξή τους
- **Για πολιτικούς λόγους:** τέτοιου είδους δραστηριότητα έχει στόχο κυρίως κυβερνητικούς οργανισμούς και σχετίζεται με ιδεολογικά κίνητρα, που οδηγούν

---

<sup>60</sup> Mitnick, KD & Simon, WL 2003, *Η τέχνη της απάτης: ο ανθρώπινος παράγοντας στην ασφάλεια*, Ωκεανίδα, Αθήνα.

<sup>61</sup> Furnell, S 2006, *Κυβερνοέγκλημα : καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

σε εκδηλώσεις διαμαρτυρίας ή περαιτέρω σε ενέργειες κατασκοπίας και τρομοκρατίας.

Μια πληρέστερη μελέτη των κινήτρων της κάθε υποκατηγορίας παρατίθεται στον ακόλουθο πίνακα όπως υπάρχει στο βιβλίο του Steven Fyrnell «Κυβερνοέγλημα: καταστρέφοντας την κοινωνία της πληροφορίας». Η κατηγορία των hackers παλιάς σχολής αναφέρεται στους hackers της παλιάς σχολής, δηλαδή σε αυτούς που αναφέρει ο Steven Levy στο βιβλίο του “Hackers: the heroes of the computer revolution”.

	Κυβερνο-τρομοκράτες	Κυβερνο-πολιτικοί	Χακτεβιστές	Δημιουργοί κακόβουλων προγραμμάτων	Χάκερ παλιάς σχολής	Φρίκερ	Σαμουράι	Κλέφτες προγραμμάτων
Εμπειρία				#	#	#	#	
Εγώ				#	#	#		#
Κατασκοπία		#	#	#				
Ιδεολογία	#	#			#			
Παρανόηση				#		#		#
Χρήματα		#		#		#	#	
Εκδίκηση	#		#	#				#

Πίνακας 1: Κίνητρα ανά ομάδα hacker

Το κίνητρο του χρήματος είναι διαφορετικό για κάποιες ομάδες, όπως για παράδειγμα στους Phone hackers είναι η αποφυγή να πληρώνουν τέλη κλήσεων και συνδρομή δικτύου, ενώ στην περίπτωση των Σαμουράι και των Κυβερνοπολεμιστών είναι η χρηματική αμοιβή για τις υπηρεσίες τους. Στους Warer doodz είναι τα έσοδα από την πώληση των πειρατικών τους προγραμμάτων. Μπορεί ορισμένα κίνητρα να είναι επιφανειακά όπως στους χακτεβιστές.

Πολλές φορές το «εγώ» παίζει σημαντικό ρόλο, είναι στην φύση του hacker να γράφει κώδικες λίγο πιο έξυπνους από τους συναδέλφους του και να καταστρατηγεί την άμυνα των συστημάτων τους. Πολλοί hackers παρακολουθούν το Διαδίκτυο και ψάχνουν μια ευκαιρία για να ικανοποιήσουν την ματαιοδοξία τους. Όπως λύνοντας ένα περίπλοκο σταυρόλεξο, το να μαντεύεις κωδικούς (passwords) και να επινοείς τρόπους παράκαμψης της προστασίας των αρχείων, παρουσιάζει ενδιαφέροντα προβλήματα που μερικά άτομα θα αφιέρωναν μεγάλα χρονικά διαστήματα για να τα λύσουν<sup>62</sup>.

<sup>62</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.



Για άλλους, το hacking αντιπροσωπεύει ένα τρόπο ζωής που στηρίζεται πάνω στην κοινωνική ανεπάρκεια ανάμεσα σε διάφορα διανοητικώς ικανά άτομα το επονομαζόμενο σύνδρομο των “computer nerd”<sup>63</sup>.

## 1.6 Χαρακτηριστικά των hackers

Το hacking εκφράζει μια βαθιά εσωτερική ανάγκη που δεν έχει σχέση με την τεχνολογία. Είναι η ανάγκη για γνώση, για περιπέτεια, για εξερεύνηση και ανακαλύψεις. Οι hackers μοιάζουν πολύ με τους δημοσιογράφους που διγούν για αποκλειστικότητα και μυστικά. Η τεχνολογία είναι μόνο η αφορμή για την αναζήτηση αυτού που ούτε οι hackers μπορούν να ορίσουν<sup>64</sup>.

Ποια είναι η πραγματική εικόνα ενός hacker και πια εικόνα έχει υιοθέτηση η κοινή γνώμη επηρεαζόμενη από τα ΜΜΕ και τον χολιγουντιανό κινηματογράφο; Ένας τυπικός hacker συγκεντρώνει ένα σύνολο χαρακτηριστικών. Πρόκειται κυρίως για νεαρά άτομα, ως επί το πλείστον άνδρες ηλικίας 16 έως 30 ετών χωρίς ιδιαίτερες κοινωνικές δεξιότητες αλλά ιδιαίτερα ευφυείς και πολύ καλοί γνώστες της πληροφορικής.<sup>65</sup>

Οι μεγαλύτεροι σε ηλικία εργάζονται ή έχουν εργαστεί σε εταιρείες ηλεκτρονικών υπολογιστών ή στις ένοπλες δυνάμεις, όπου είχαν την ευκαιρία να ασχοληθούν ουσιαστικά με την ανάπτυξη και την εξέλιξη των υπολογιστών, όπως και προγραμμάτων για υπολογιστές. Συνήθως πάσχουν από το επονομαζόμενο σύνδρομο των “computer nerd”, το οποίο επηρεάζει κυρίως τους αρσενικούς εφήβους μεταξύ των ηλικιών δεκατέσσερα και δεκαέξι. Αυτά τα άτομα είναι συνήθως αυτοδίδακτα, απολαμβάνουν διανοητικά παιχνίδια, δεν είναι σεξουαλικά ενεργά και πιθανώς ακόμη και να παραμελούν την προσωπική τους υγιεινή. Μάλιστα, μια περίπτωση ψύχωσης με τον υπολογιστή έχει ήδη αναφερθεί στην Κοπεγχάγη της Δανίας. Προφανώς, ο αναφερόμενος νεαρός γοητεύτηκε από τον υπολογιστή του τόσο πολύ ώστε του ήταν αδύνατο να ξεχωρίσει τον πραγματικό κόσμο από τα υπολογιστικά προγράμματα

---

<sup>63</sup> φανατικός / μανιώδης / πωρωμένος κομπιουτεράς, κομπιουτερόβιος

<sup>64</sup> Saleem, S 2006, ‘Ethical hacking as a risk management technique’ *Proceeding from the third annual conference on information security curriculum development*, pp. 201–203. Διαθέσιμο στο: ACM Portal [15 Δεκεμβρίου 2008].

<sup>65</sup> Young, R, Zhang, L & Prybutok, V 2007, ‘Hacking into the minds of hackers’, *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

μιλούσε σε γλώσσα προγραμματισμού όταν εκτελούσε συνηθισμένες καθημερινές δουλειές<sup>66</sup>.

Η συμπεριφορά των hackers έχει τα χαρακτηριστικά του τύπου INTP (Introversion, iNtuition, Thinking, Perceiving) του διάσημου τεστ προσωπικότητας<sup>67</sup> Myers-Brigg, το οποίο είναι βασισμένο στην τυπολογία Γιούνγκ<sup>68</sup>. Φυσικά κάθε κατηγορία hacker έχει τη δική της προσωπικότητα. Με κίνητρό τους τη γνώση αλλά και την ανάγκη για δημιουργία προσπαθούν να ανακαλύψουν τα μυστικά πολύπλοκων συστημάτων. Συνήθως το σχολείο δεν τους δίνει τα κατάλληλα ερεθίσματα για να ικανοποιήσουν τη δίψα τους για μάθηση και στρέφονται σε πιο ενδιαφέροντα πράγματα, όπως η τεχνολογία.<sup>69</sup>

Κάθε μυστήριο τους ελκύει, κάθε πρόβλημα που φαίνεται αδύνατο να λυθεί. Οι ηλεκτρονικοί υπολογιστές είναι γεμάτοι τέτοιες προκλήσεις και αποτελούν το ιδανικό παζλ ή σταυρόλεξο για τέτοια άτομα. Σύντομα το ενδιαφέρον τους για την τεχνολογία αυξάνεται και αφιερώνουν όλο και περισσότερο χρόνο στη διαδικασία επίλυσης των μικρών και μεγάλων προβλημάτων που αντιμετωπίζουν, καθώς χειρίζονται τους ηλεκτρονικούς υπολογιστές και το Διαδίκτυο.<sup>70</sup>

Το γεγονός όμως ότι κάποιος μπορεί να συγκεντρώσει αυτά τα χαρακτηριστικά δεν τον καθιστά hacker. Είναι όμως αυτή η πραγματική εικόνα του hacker ή είναι μια εικόνα την προβάλλουν τα ΜΜΕ και ο κινηματογράφος; Πού βρίσκεται ο μύθος και που η αλήθεια; Το μόνο σίγουρο είναι ότι η εικόνα του μανιακού έφηβου με γυαλιά που κάθετε απομονωμένος σε ένα δωμάτιο με τον υπολογιστή του πρέπει να διαγραφεί ως μη ισχύουσα.

Γεγονός είναι ότι οι hackers συγκεντρώνουν κάποια από αυτά τα χαρακτηριστικά —αν όχι όλα— και ο λόγος είναι πασιφανές. Η εξερεύνηση του ηλεκτρονικού κόσμου απαιτεί αφοσίωση και συγκέντρωση στο αντικείμενο. Οι ώρες που πρέπει να διαθέσει κανείς είναι πάρα πολλές με αποτέλεσμα να κάνει την εμφάνισή του ο εθισμός. Η γραμμή μεταξύ του εθισμού, της εμμονής και της αφοσίωσης στους υπολογιστές είναι

---

<sup>66</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

<sup>67</sup> *Personality test based on Jung-Myers-Briggs typology* 2008, HumanMetrics.com. Διαθέσιμο στο: <<http://www.humanmetrics.com/cgi-win/JTypes1.htm>> [20 Δεκεμβρίου 2008].

<sup>69</sup> Saleem, S 2006, 'Ethical hacking as a risk management technique' *Proceeding from the 3rd annual conference on information security curriculum development*, pp. 201 – 203. Διαθέσιμο στο: ACM Portal [15 Δεκεμβρίου 2008].

<sup>70</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

πολύ λεπτή. Ο υπερβολικός ζήλος μετατρέπεται πολύ εύκολα σε εθισμό. Όταν αρχίσει κανείς το hacking και μετά από τις πρώτες επιτυχίες εισβολές σε συστήματα, είναι πολύ δύσκολο να σταματήσει. Το αίσθημα που έχει ο hacker είναι μιας βαθιάς ικανοποίησης και αποδεικνύει την ανωτερότητά του και τις γνώσεις που έχει. Ίσως τελικά το hacking να είναι απλά ένα θέμα εγωισμού γι' αυτό και μερικοί hackers υποσυνείδητα ως και συνειδητά θέλουν να συλληφθούν για να μάθει το ευρύ κοινό τα κατορθώματά τους. Αυτή είναι μια από τις αυτοκαταστροφικές τάσεις που έχουν.<sup>71</sup>

Υπάρχουν όμως και hackers που δεν είναι τόσο επιφανειακοί. Σαν INTP δεν τους αφορά να είναι κοινωνικά αποδεκτοί –ακόμα και με την αρνητική φήμη— αλλά να μπορούν να χτίζουν και να δημιουργούν νέες τεχνολογικές προσεγγίσεις και πραγματικότητες. Η ικανοποίηση που νιώθουν με την εισβολή τους σε ξένα συστήματα προέρχεται από το αίσθημα επιτυχίας σαν μια επιβράβευση. Μέσα από αυτές τις εμπειρίες μαθαίνουν όλο και περισσότερα. Το γεγονός ότι ο απλός υπολογιστής που έχουν στο σπίτι τους έχει τη δυνατότητα να συνδεθεί με όλα τα μεγάλα δίκτυα τους συναρπάζει<sup>72</sup>. Είναι κάτι που στη φαντασία των hackers, που ξέρουν να θαυμάζουν το αυτονόητο, φαίνεται μαγικό. Οι τεχνολογικές προκλήσεις γίνονται όλο και μεγαλύτερες και πάντα υπάρχουν προβλήματα να λύσουν. Το hacking τους δίνει ένα σκοπό και νόημα ύπαρξης.<sup>73</sup>

Το δίκτυο και οι υπολογιστές γενικότερα είναι ένα ψυχρό μέσο και ως εκ τούτου μπορεί να υπάρχει μια αναλογία με τους συστηματικούς χρήστες του. Γιατί είναι πιο εύκολο να επικοινωνεί κανείς με άλλα άτομα από το δίκτυο από ότι σε πραγματικό χρόνο και τόπο. Ο λόγος που η πλειοψηφία δεν έχει πολλές κοινωνικές επαφές είναι απλά ότι οι άνθρωποι που συναντούν δεν τους ερεθίζουν πνευματικά και θεωρούν χάσιμο πολύτιμου χρόνου την επικοινωνία με άτομα που δεν εκτιμούν τη γνώση.

Μέσα στον εικονικό κόσμο που δημιούργησε το δίκτυο μπορεί κανείς να κινηθεί απελευθερωμένος και αδέσμευτος. Ο χώρος αυτός προσφέρει τόση ελευθερία που μπορεί εύκολα κανείς να βγει εκτός ορίων. Οι hackers ποτέ δεν χρησιμοποιούν τα πραγματικά τους ονόματα, γεγονός που συμβαίνει για πρακτικούς λόγους. Βέβαια η επιλογή του εκάστοτε παράνομου προδίδει την προσωπικότητα του hacker. Πολλοί χρησιμοποιούν αστεία ψευδώνυμα π.χ. «Tweety Fish» δηλώνοντας την αίσθηση του

<sup>71</sup> Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

<sup>72</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα.

<sup>73</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα

χιούμορ που έχουν αυτά τα άτομα, ενώ άλλοι επιλέγουν κάποιο παράνομο με κύρος που να φανερώνει δύναμη όπως για παράδειγμα «Mafiaboy». Τα ψευδώνυμα τους αποκαλύπτουν το alter ego τους, όχι το ποιοι είναι αλλά πως αυτοί βλέπουν τον εαυτό τους και πως θα ήθελαν οι υπόλοιποι να τους αντιμετωπίζουν. Φορώντας λοιπόν την δικτυακή μάσκα, που προσδίδει το εκάστοτε ψευδώνυμο, είναι δύσκολο να ελέγξει τα όρια μεταξύ ηθικού και ανήθικου<sup>74</sup>.

Το ερώτημα είναι πως βλέπουν και πως δικαιολογούν τις δραστηριότητες τους οι ίδιοι οι hackers. Μια δημοφιλής εικόνα που έχουν οι ίδιοι για τον εαυτό τους είναι ότι πρόκειται για ταλαντούχα άτομα που χαρακτηρίζονται ως σκαπανείς του κυβερνοχώρου. Οι hackers θεσπίζουν και υποστηρίζουν έντονα ότι υπάρχει διαχωρισμός μεταξύ των elit hackers και των kiddies. Οι elit hackers χαρακτηρίζονται ως καινοτόμοι, έχουν την ηθική των παλιών hackers και βρίσκονται στη κορυφή της κοινωνικής ταξικής πυραμίδας των hackers. Σε αντίθεση οι kiddies είναι άτομα χωρίς ιδιαίτερες ικανότητες που χρησιμοποιούν έτοιμα εργαλεία και υλικό –αυτά που κατασκευάζουν οι elit hackers.<sup>75</sup>

Ζουν σε ένα εικονικό κόσμο όπου οι κυβερνητικές αρχές και η ιδιοκτησία των πληροφοριών δεν υπάρχουν. Συχνά θεωρείται ότι οι hackers έχουν μία αντί-αυταρχική πολιτική συνείδηση και ένα αναρχικό πνεύμα απέναντι στους νόμους που περιορίζουν την ελευθερία της πληροφορίας. Από κοινωνιολογικής απόψεως ίσως να μπορούν να παρομοιαστούν με επαναστάτες της εποχής. Κατ' αντιστοιχία στην αγροτική κοινωνία θα ήταν τα άτομα που ζητούσαν αναδάσμο της γης, στην βιομηχανική εποχή θα ήταν το επαναστατικό εργατικό που ζητά καλύτερες συνθήκες εργασίας. Σήμερα το κίνημα των hackers αποτελεί συνέχεια του εργατικού αγώνα<sup>76</sup>.

Στην σύγχρονη κοινωνία της πληροφόρησης είναι τα άτομα που ζητούν την από-ιδιωτικοποίηση των πληροφοριών και ελεύθερο λογισμικό. Προσπαθούν να απελευθερώσουν την τεχνολογία από τα επιχειρησιακά μονοπώλια –μια καλή προσπάθεια είναι η δημιουργία του ανοικτού λειτουργικού συστήματος LINUX που

---

<sup>74</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

<sup>75</sup> Clive, T. 2005, “Meet the life hackers”, *New York Times*, 16 Οκτωβρίου. Διαθέσιμο στο: <http://www.nytimes.com/2005/10/16/magazine/16guru.html?scp=1&sq=Meet%20the%20Life%20Hackers%20&st=cse> [13 Δεκεμβρίου 2008].

<sup>76</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα.

έρχεται να χτυπήσει το μονοπώλιο της Microsoft και έγινε η απαρχή για τη ραγδαία ανάπτυξη και εξάπλωση του μοντέλου λογισμικών ανοικτού κώδικα παγκοσμίως.<sup>77</sup>

Το ηλεκτρονικό περιβάλλον τους βοηθά να δικαιολογήσουν τις πράξεις τους, καθώς όταν οι παράνομες πράξεις υποστηρίζονται από ένα ηθικό απελευθερωμένο υπόβαθρο και συχνά επαναστατικά ιδεώδη, τότε μπορούν να δικαιολογηθούν ηθικά. Οι ίδιοι οι hackers δηλώνουν ότι με το να διεισδύουν σε ξένα υπολογιστικά συστήματα βοηθούν τις εταιρίες να δουν τα τρωτά τους σημεία. Θεσπίζουν και καλούνται μιας αποστολής να είναι το τρίτο μάτι που παρακολουθεί τις μη δεοντολογικές και συχνά ανήθικη συμπεριφορά των κυβερνήσεων και των επιχειρήσεων, υποστηρίζουν ότι λειτουργούν και δρουν για το κοινό καλό. Αντιπροσωπεύουν ένα σύγχρονο Robbin Hood<sup>78</sup>.

Σύμφωνα με τον Schwartau στο άρθρο του Cyber-vigilantes hunt down hackers (1999) «...η χωρίς εξουσιοδότηση είσοδος σε έναν υπολογιστή δεν πρέπει να είναι ένα έγκλημα, αλλά να βλάψει τους ανθρώπους με τα στοιχεία ή να βλάψει τον υπολογιστή πρέπει να είναι παράνομο. Να ασκήσει αρνητική επίδραση πρέπει να είναι παράνομο. Έχετε πολλούς καλοκάγαθους ανθρώπους που πηγαίνουν να φυλακίσετε... Δεν είναι πραγματικοί εγκληματίες. Είναι εξερευνητές που διώκονται για τη σκέψη»<sup>79</sup>. Παραδεκτό είναι ότι από μίας απόψεως οι ισχυρισμοί τους υφίστανται, αλλά ωραιοποιώντας και ηρωοποιώντας τις πράξεις τους, τις καθιστούν εκούσια τυφλές και αγνοούν τυχόν αρνητικές επιπτώσεις των πράξεων τους. Η πολύ-ειπωμένη ατάκα «δεν κάνουμε κακό» θα ήταν καλύτερα να εκφραζότανε ως «δεν σκοπεύουμε να κάνουμε κακό» --αναφερόμενοι πάντα στην κατηγορία elit hacker— καθώς άθελα τους μπορούν να προκαλέσουν βλάβη για παράδειγμα την νόμιμη είσοδο ενός αλλού χρήστη στο σύστημα.<sup>80</sup>

Μπορεί ένας hacker να δεχτεί την ευθύνη για τις παράνομες δραστηριότητες του, αλλά θα επιμένει στο γεγονός ότι δεν είναι και τόσο επιβλαβείς ειδικά εφόσον έχει ήδη γνωστοποιήσει τις αδυναμίες και τα τρωτά του συστήματος στον εκάστοτε οργανισμό που πλήττει, κι αυτός με τη σειρά του τα λάβει υπόψη ως προς την

---

<sup>77</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

<sup>78</sup> Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

<sup>79</sup> Schwartau, W. 1999, "Cyber-vigilantes hunt down hackers", *CCN*, 12 Ιανουαρίου. Διαθέσιμο στο: <<http://edition.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/>> .[13 Δεκεμβρίου 2008].

<sup>80</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα

βελτιστοποίηση της ασφάλειας του συστήματός του. Θεωρούν ότι οι πράξεις τους όχι μόνο δεν είναι ντροπή ούτε και εγκληματικές, αλλά αντιθέτως αξίζουν επαίνου από τους υπόλοιπους hackers. Όταν έρχονται αντιμέτωποι με την ποινή των πράξεων τους συνηθίζουν να κατηγορούν το θύμα, όπως λόγου χάριν «αν είναι τόσο χαζοί (οι διαχειριστές του συστήματος) ώστε να με αφήσουν να μπω (στο σύστημα) κι δεν υπάρχει απολύτως κανένας λόγος να το κάνω, τότε δεν έχουν κανένα δικαίωμα να κρατούν τις πληροφορίες για τον εαυτό τους»<sup>81</sup>.

Μέσα από τη σκιαγράφηση του χαρακτήρα των hackers είναι φανερό και διακρίνεται με πάσα σαφήνεια ότι τα άτομα αυτά διακατέχονται από ισχυρό αίσθημα αλαζονείας, το οποίο πηγάζει από την αυτόβουλη πεποίθησή τους ότι είναι πάνω από τους νόμους και υπεράνω των νοητικών ικανοτήτων των υπολοίπων ανθρώπων. Αυτός είναι και ο λόγος που συνεχώς οι δραστηριότητες hacking αυξάνονται, παρόλο που υπάρχουν ποινές για την πραγματοποίηση τέτοιων δραστηριοτήτων. Βέβαια ο λόγος που οι hackers δεν υπολογίζουν τις ποινές για κυβερνο-έγκλημα, εκτός από την πεποίθησή ότι δεν πρόκειται ποτέ να τους συλλάβουν, είναι επίσης ότι οι νόμοι για το ηλεκτρονικό έγκλημα δεν είναι εύκολο να εφαρμοστούν και να οριοθετηθούν.<sup>82</sup>

Παράλληλα, δράττονται της προκαταλήψεως που υπάρχει και πιστεύουν ότι μια πλήττουσα εταιρία δεν θα δημοσιεύσει και πολλές φορές δεν θα καταγγείλει την παραβίαση που δέχτηκε γιατί αυτό θα έχει μεγάλο αντίκτυπο στην εικόνα της. Οι hackers κερδίζουν πολλά περισσότερα από το hacking τόσο σε χρήματα όσο και σε εμπειρίες, γι' αυτό ρισκάρουν και τολμούν να διαπράξουν τις παράνομες εισόδους σε ξένα υπολογιστικά συστήματα. Τέλος, οφείλουμε να παραδεχτούμε ότι η ευφυΐα και οι απίστευτες ικανότητες τους βοηθούν να αποφύγουν τη σύλληψη. Το γεγονός ότι η συμπεριφορά τους θεωρείται ηθικά σωστή και αποδεκτή από τους υπόλοιπους hackers αλλά και από το οικογενειακό τους περιβάλλον σε συνδυασμό με την πεποίθησή ότι υπάρχει μία πολύ μικρή πιθανότητα να συλληφθεί τους επιτρέπει να παίρνουν ρίσκα και να ξεπερνούν τα όρια του Διαδίκτυου.

Υπάρχουν πολλοί προικισμένοι hackers, οι οποίοι με τις ικανότητές τους και με την προβολή που είχαν από τα MME έγιναν διάσημοι στο ευρύ κοινό. Εκμεταλλεύτηκαν την εμπειρία τους και συνεργάστηκαν με συγγραφείς, σκηνοθέτες

---

<sup>81</sup> Murphy, C 2004, 'Inside the mind of the hacker', *Accountancy Ireland Journal*, vol. 36, no. 3, pp.12-13. Διαθέσιμο στο: British Library Direct [15 Δεκεμβρίου 2008].

<sup>82</sup> Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

και ηθοποιούς, έγιναν επίσημοι καλεσμένοι σε συνεδρία «ασφάλειας υπολογιστών». Χαρακτηριστικό παράδειγμα ο Mark Abene, ο οποίος μετά την αποφυλάκιση του – είχε καταδικαστεί για 1 χρόνο φυλάκισης για παράνομες δραστηριότητες hacking— ψηφίστηκε από το New York Magazine το 1994, ως ένας από τους 100 εξυπνότερους ανθρώπους στην Νέα Υόρκη.<sup>83</sup>

---

<sup>83</sup> Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

## ΚΕΦΑΛΑΙΟ 2: ΔΙΑΣΗΜΟΙ ΚΑΙ ΔΗΜΟΦΙΛΕΙΣ HACKERS

Διαχρονικά μέσα από την κοινότητα των hackers ξεχώρισαν ορισμένα άτομα. Μερικοί από αυτούς είναι διάσημοι για την συνεισφορά τους στην παγκόσμια ηλεκτρονική ασφάλεια, ενώ οι άλλοι είναι διάσημοι επειδή τους κυνηγούσε το FBI (Federal Bureau of Investigation). Το σίγουρο είναι ότι όλοι ξεχώρισαν για τις ικανότητες τους και την ευφυΐα τους. Η εικόνα των hacker στα μέσα μαζικής ενημέρωσης κυμαίνεται από την εικόνα ενός high-tech υπερκατασκόπου μέχρι την εικόνα του μοναχικού, αντικοινωνικού έφηβου που απλά αναζητά διασκέδαση.

Ακολουθεί μια λίστα από τους διασημότερους hacker όλου του κόσμου. Ο καθένας από αυτούς θα μας βοηθήσει να διαμορφώσουμε μια άποψη για την προσωπικότητα ενός hacker, τον τρόπο σκέψης και δράσης του, αλλά και γενικότερα θα σχηματίσουμε μια άποψη για τη διαφορά του ηλεκτρονικού εγκλήματος από την προσφορά στην παγκόσμια ασφάλεια υπολογιστών.

### 2.1 John Draper – Captain Crunch

Ο John T. Draper, Captain Crunch είναι γνωστός και ως ο παππούς των hacker. Το 1969 ο John Draper είχε μόλις έναν χρόνο που είχε αποχωρήσει τιμητικά από την αμερικανική αεροπορία. Στα 26 του, ζούσε στο Σαν Χοσέ όπου δούλευε ως μηχανικός στη National Semiconductor και φοιτούσε στο Κολέγιο.

Για την ακρίβεια ο John Draper ήταν phreaker τηλεφώνων. Εφόσον όλοι οι phreaker είχαν ένα ψευδώνυμο για λόγους ασφαλείας, αλλά και ακολουθώντας το εθνικό δίκαιο της κάθε λογής υποκουλτούρας, έπρεπε και ο Τζον να αποκτήσει ένα. Έτσι λόγω της ανακάλυψης που έκανε, να χρησιμοποιήσει με ένα ιδιαίτερο τρόπο μια παιδική σφυρίχτρα που ήταν δώρο σε κάποια πακέτα δημητριακών πρωινού γεύματος (με το ίδιο όνομα) πήρε και το ανάλογο ψευδώνυμο “Captain Crunch”.

Ο Captain Crunch διαπίστωσε το 1971 ότι με την χρήση αυτής της σφυρίχτρας που μπορούσε να παράγει έναν τόνο ταυτόσημο με αυτόν που χρησιμοποιούσε το τηλεφωνικό δίκτυο των Ηνωμένων Πολιτειών και έτσι μπορούσε να παρακάμψει το σύστημα χρέωσης τηλεφωνικών συνδιαλέξεων των Η.Π.Α. Οι δυνατότητες του μικρού αυτού παιχνιδιού λέγεται ότι αποκαλύφθηκαν τυχαία (αν και φημολογείται ότι πρώτος που το ανακάλυψε ήταν ένας νεαρός τυφλός phreaker). Το παιχνίδι αυτό, αν καλυφθεί μια από τις τρύπες έβγαζε τον ήχο μιας ψιλής νότας ΛΑ, που βρισκόταν πολύ κοντά στον τόνο των 2600 κύκλων που χρησιμοποιούσε η Bell για τις



υπεραστικές της γραμμές. Πιτσιρίκια που έκαναν επίδειξη του νέου τους παιχνιδιού στη γιαγιά, στην άλλη άκρη της γραμμής ανακάλυπταν συχνά ότι το τηλέφωνο έκλεινε. Η Bell χρειάστηκε πολύ καιρό για να ανακαλύψει την αιτία ή το πρόβλημα. Ο Draper επεξεργάστηκε αυτό το παιχνίδι και ανέπτυξε τα μπλε κουτιά (blue boxes), δηλαδή γεννήτριες ηλεκτρονικών τόνων που θα μπορούσαν να αναπαράγουν ολόκληρη την σειρά τόνων που χρησιμοποιούσε το τηλεφωνικό δίκτυο των Ηνωμένων Πολιτειών στο σύστημα δρομολόγησης τηλεφωνημάτων του. Με τέτοιες συσκευές, ήταν δυνατό να τηλεφωνήσεις οπουδήποτε στον κόσμο δωρεάν. Με την ανακάλυψη του ο Draper και την κατασκευή των μπλε κουτιών (blue box) έκανε το phreaking πολύ πιο εύκολο<sup>84</sup>.

Σύμφωνα με την Bell Telephone η πρώτη περίπτωση κλοπής σε υπεραστικό τηλεφώνημα με τη χρήση ηλεκτρονικής συσκευής εντοπίστηκε στα 1971, αφού ένας διευθυντής σε κάποιο τοπικό γραφείο στο νοτιοδυτικό υποκατάστημα της εταιρίας παρατήρησε κάποιες ασυνήθιστα μεγάλες σε διάρκεια κλήσεις σε κάποιον εκτός περιοχής αριθμό. Τα τηλεφωνήματα γίνονταν από ένα στούντιο στο Washington State College. Όταν οι τεχνικοί της Bell πήγαν για να ελέγξουν, βρήκαν εκεί αυτό που αργότερα περιέγραψαν σαν μια περίεργη συσκευή πάνω σε ένα μπλε μεταλλικό κουτί συνδεδεμένο με το τηλέφωνο. Του έδωσαν άμεσα το παρατσούκλι bluebox («μπλε κουτί»). Το χρώμα της συσκευής ήταν τυχαίο, αλλά το όνομα κόλλησε. Ο σκοπός της περιέργης αυτής συσκευής ήταν να επιτρέπει στους χρήστες να κάνουν υπεραστικά τηλεφωνήματα χωρίς χρέωση<sup>85</sup>.

Ο Draper δημοσίευσε το θέμα ευρέως τον Οκτώβρη του 1971 στο αμερικάνικο περιοδικό Esquire. Μετά την δημοσίευση αυτού του άρθρου δεν θεωρείται περίεργο γεγονός της σύλληψη του. Συνελήφθηκε και κατηγορήθηκε για απάτη τον Μάιο του 1972 και καταδικάστηκε σε 5 χρόνια φυλάκισης στις φυλακές ασφαλείας του Lompoc. Ο ίδιος υποστηρίζει ότι αυτό θα χειροτερεύσει την κατάσταση, καθώς ο ίδιος εξαναγκάστηκε να διδάξει τις τεχνικές του σε άλλους έγκλειστους εγκληματίες<sup>86</sup>. Έτσι για λόγους επιβίωσης και ασφάλειας παίζει το ρόλο του δασκάλου και μεταφέρει τις γνώσεις του σε άλλους κρατούμενους. Το αποτέλεσμα

---

<sup>84</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [9 Σεπτεμβρίου 2008].

<sup>85</sup> Forester, T & Morrison, P 1994, *Computer ethics: cautionary tales and ethical dilemmas in computing*, MIT Press, Cambridge, Mass. Διαθέσιμο στο: Google Books Search [10 Σεπτεμβρίου 2008].

<sup>86</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: [www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc) [10 Σεπτεμβρίου 2008].

αυτής της διδασκαλίας ήταν να αποκτήσουν γνώσεις hacking, κακόβουλα άτομα και έτσι το phone hacking να πάρει ένα πιο εγκληματικό και σκοτεινό χαρακτήρα.

Τη δεκαετία του 1970 ο John Draper δούλεψε για λίγο στην Apple και κατασκεύασε ένα τηλεφωνικό πίνακα αναγνώρισης για το PC Apple II. Ο πίνακας αυτός όμως δεν προωθήθηκε γιατί πολλοί ανησυχούσαν για την κακόβουλη χρήση αυτής της κάρτας. Το 1977 καταδικάζεται πάλι, αυτή τη φορά για κλοπή 50.000 δολλαρίων με τηλεφωνικές κλήσεις<sup>87</sup>. Όταν ήταν στις φυλακές έγραψε το πρώτο πρόγραμμα “word processing” (επεξεργαστή κειμένων) για την Apple II, το οποίο υπερίσχυσε του Bill Gates σε ένα συμβόλαιο για το πρόγραμμα της IBM.

Ο Draper ξεκίνησε τη δική του επιχείρηση το 2002 με το όνομα Shop IP, μία εταιρεία που παρέχει λύσεις σε προβλήματα ασφάλειας, η οποία κατασκεύασε ένα σύστημα ασφάλειας το οποίο σταματά την εξάπλωση των ιών στους ηλεκτρονικούς υπολογιστές<sup>88</sup>. Ο Draper συνεχίζει να διευθύνει τη συγκεκριμένη εταιρεία.

Προσωπική ιστοσελίδα <<http://www.webcrunchers.com/crunch>>.

## 2.2 Kevin David Mitnick

Ένας από τους διασημότερους και πολυσυζητημένους hacker στον κόσμο. Θεωρείται ένα από τα πιο αξιόλογα πρόσωπα στην σκηνή των hacker. Γύρω από το πρόσωπο του δημιουργήθηκε ένας μύθος κυρίως από την δημοσιότητα που απέκτησε. Ιστοσελίδες, ντοκιμαντέρ και ταινίες έχουν γυριστεί για τη ζωή του Mitnick κάνοντας τον έναν ζωντανό θρύλο για κάποιους, σύμβολο του ανήσυχου πνεύματος των hacker.

Γεννήθηκε στις 6 Αυγούστου το 1963. Παιδί χωρισμένων γονιών μεγάλωσε στο Σαν Φραντσίσκο της Καλιφόρνιας. Ο νεαρός Mitnick ξεκίνησε την «καριέρα» του ως hacker κατορθώνοντας να εισχωρήσει στο ηλεκτρονικό σύστημα εισιτηρίων των λεωφορείων του Λος Άντζελες για να ταξιδεύει με αυτά δωρεάν. Όταν ήταν έφηβος δεν είχε την οικονομική δυνατότητα να πάρει δικό του υπολογιστή, έτσι σύχναζε σε τοπικά καταστήματα ηλεκτρονικών και χρησιμοποιούσε μικρά μοντέλα υπολογιστών και modem για να συνδέεται με άλλους υπολογιστές. Ανέπτυξε πολλά χόμπι, εκ των οποίων ο ραδιοερασιτεχνισμός, που αργότερα τον οδήγησε στο phreaking του τηλεφωνικού δικτύου. Η πρώτη φορά που κατηγορήθηκε ο Mitnick ήταν όταν,

---

<sup>87</sup> Wayner, P. 1997, ‘Who's hacking whom?: hope springs in Manhattan’, *The New York Times*, 11 Αυγούστου. Διαθέσιμο στο: <<http://partners.nytimes.com/library/cyber/hackstock/081197hope.html?scp=5&sq=John%20Draper%20hacker&st=cse>> [10 Σεπτεμβρίου 2008].

<sup>88</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [9 Σεπτεμβρίου 2008].

έφηβος ακόμα, διείσδυσε στον υπολογιστή του σχολείου του και προσπάθησε να αλλάξει τους βαθμούς του<sup>89</sup>.

Οι περισσότεροι φίλοι του ήταν phnefric και έτσι κατάφερε να εισχωρήσει μέσα σε μια από αυτές τις ομάδες. Ως μέλος της κοινότητας των phreakers, ο Mitnick έμαθε τις αρχές της κοινωνικής μηχανικής<sup>90</sup>, τις οποίες αργότερα ανέπτυξε και εφάρμοσε σε τέτοιο σημείο ώστε πλέον ο όρος κοινωνική μηχανική να είναι εφάμιλλος του ονόματος του Mitnick. Μέσα σε αυτές τις ομάδες ο Mitnick μαθαίνει περισσότερα για τους προσωπικούς υπολογιστές, τα δίκτυα και το phnefricing. Αυτές οι ομάδες μπορούσαν να διοικήσουν ένα τηλεπικοινωνιακό σταθμό με ελάχιστες αλλαγές στο υπολογιστικό σύστημα του. Παράλληλα μπορούσαν να παίρνουν δωρεάν κλήσεις, να κρυφακούν και να κάνουν φάρσες.

Τη δεκαετία του 1980, ο νεαρός τότε Mitnick συνδυάζει την ικανότητα του στο phreaking με τις δυνατότητες των υπολογιστών και αρχίζει να ασχολείται με την ιδέα της πρόσβασης σε απομακρυσμένους υπολογιστές. Οι φίλοι του και αυτός περνούσαν τον χρόνο τους ψάχνοντας στα παλιά αρχεία των εταιρειών τηλεπικοινωνίας για παλιά εγχειρίδια που θα μπορούσαν να τους δώσουν πληροφορίες για τους ηλεκτρονικούς υπολογιστές της εταιρείας. Το 1981 όταν ήταν μόλις 17 χρονών αναμειγνύεται στην διάρρηξη του τηλεφωνικού κέντρου COSMOS της εταιρείας Pacific Bell για κλοπή λειτουργικών εγχειριδίων. Εκεί πήραν λίστες κωδικών, στις οποίες υπήρχαν και passwords για 9 κεντρικά γραφεία της Packard Bell και κάποια εγχειρίδια χρήσης του συστήματος COSMOS. Για να αχρηστεύσουν τους μηχανισμούς άφησαν τα ψευδώνυμα και τους τηλεφωνικούς τους αριθμούς σε κάποιο αρχείο. Οι αριθμοί τηλεφώνου χτυπούσαν σε έναν τηλεφωνικό θάλαμο μιας καφετέριας στο Van Nuys. Καταδικάζεται σε τρεις μήνες φυλάκισης στις φυλακές ανηλίκων του Λος Άντζελες και ακολούθησε επιτήρηση ενός χρόνου. Μετά από αυτό ακολουθεί μια πορεία γεμάτη παραβιάσεις και συλλήψεις<sup>91</sup>.

Τα πρώτα χρόνια της ενασχόλησης του Mitnick με τους υπολογιστές, το ψευδώνυμο του ήταν «Κόνδορας» από την ταινία «Οι τρεις μέρες του Κόνδορα». Το 1983 συλλαμβάνεται από την αστυνομία του Πανεπιστημίου της Καλιφόρνιας για χρήση του υπολογιστή του Πανεπιστημίου με σκοπό παράνομης πρόσβασης στους

---

<sup>89</sup> Mitnick, KD & Simon, WL 2005, *The art of intrusion: the real stories behind the exploits of hackers, Intruders and Deceivers*, Wiley, Indianapolis.

<sup>90</sup> Ως κοινωνική μηχανική αναφέρεται η τακτική που ακολουθείται για την παράνομη απόκτηση δεδομένων μέσω της εξαπάτησης.

<sup>91</sup> Mitnick, KD 2003, *Η τέχνη της απάτης ο άνθρωπος παράγοντας στην ασφάλεια*, Ωκεανίδα, Αθήνα.

υπολογιστές του Πενταγώνου διαμέσω από το ARPANET. Καταδικάστηκε σε 6 μήνες φυλάκισης στις φυλακές νέων της Καλιφόρνιας. Το 1984 κατηγορείται για διενέργεια παράνομων ελέγχων TRW (Thompson Ramo Wooldridge) σε πιστωτικά αρχεία. Εκείνο το διάστημα εργαζόταν στην Great American Merchandising. Το Δεκέμβριο του 1987 καταδικάζεται για την κλοπή λογισμικού από την εταιρία Santa Cruz της Καλιφόρνιας, μια εταιρεία παραγωγής λογισμικού στην Καλιφόρνια και καταδικάστηκε σε 36 μήνες επιτήρηση<sup>92</sup>.

Ένοχος κρίθηκε το 1988, για εισβολή σε σύστημα κλέβοντας πηγαίο κώδικα της Digital Equipment Corporation. Ο Mitnick και ένας φίλος του, ο Lenny DiCicco, άνοιξαν ηλεκτρονικό πόλεμο με τους ερευνητές του Palo Alto. Σύντομα τα τηλεφωνήματα ανακαλύφθηκαν, όμως το FBI δεν μπόρεσε να βρει την πηγή τους, καθώς ο Mitnick πείραζε τη συνδεσμολογία των τηλεφώνων της εταιρίας για να καλύπτει τα ίχνη του. Ο DiCicco ομολόγησε τα πάντα στον εργοδότη του και ο Mitnick κατέληξε στο Ομοσπονδιακό Δικαστήριο του Λος Άντζελες. Ο Mitnick καταδικάστηκε για απάτη μέσω υπολογιστή και την απόκτηση υπεραστικών κωδικών πρόσβασης σε ένα 1 χρόνο φυλάκισης και έξι μήνες παρακολούθησης προγράμματος για απεξάρτηση από τους υπολογιστές. Το 1992 κατηγορείται ότι έκλεψε λογισμικό από τις DEC, Motorola, Nec, Nokia, Sun Microsystems, Fujitsu Siemens, Apple, παραβιάζοντας με τον τρόπο αυτό τους όρους της επιτήρησης<sup>93</sup>.

Το Δεκέμβριο του 1994 ο Mitnick αναμειγνύεται σε μια υπόθεση κλοπής λογισμικού, παραβίασης προσωπικού ηλεκτρονικού ταχυδρομείου και παραβίασης αρχείων ιδιοκτησίας του Tsutomu Shimomura, ειδικού σε θέματα ασφαλείας υπολογιστών στο κέντρο υπολογιστών του San Diego. Ο Shimomura συνεργάστηκε με το FBI για την καταδίωξη του Mitnick. Τέλος το 1995 συλλαμβάνεται στην Καλιφόρνια μετά από 2 χρόνια καταδίωξης και καταδικάστηκε σε 5 χρόνια φυλάκισης. Με τη δράση του έγινε το επίκεντρο των μέσων μαζικής ενημέρωσης αλλά και του FBI. Το κόστος από τις χακιστικές δραστηριότητες του Mitnick υπολογίζεται γύρω στα 291.8 εκατομμύρια δολάρια<sup>94</sup>.

---

<sup>92</sup> Mitnick, KD & Simon, WL 2005, *The art of intrusion: the real stories behind the exploits of hackers, Intruders and Deceivers*, Wiley, Indianapolis.

<sup>93</sup> Markoff, J 1988, 'Californian held in computer case', *The New York Times*, 26 Δεκεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=940DE3D71E3CF935A15751C1A96E948260&scp=1&sq=1988%20Digital%20Equipment%20Corporation%20mitnick&st=cse>> [9 Σεπτεμβρίου 2008].

<sup>94</sup> Fallows, J 1996, 'An outlaw in cyberspace', *The New York Times*, 4 Φεβρουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9B00E3D71739F937A35751C0A960958260&sec>>

Όταν αποφυλακίστηκε, το 2000, του απαγόρευσαν της χρήση συσκευών με πληκτρολόγιο για χρόνια. Μετά από αυτό το πολυβόητο βιογραφικό ο Mitnick θεωρείτο πολύ επικίνδυνος για να του επιτραπεί έστω και να ακουμπήσει ένα τηλέφωνο. Παρόλο που θα περίμενε κανείς ότι δεν θα είχε ευμενή αντιμετώπιση από τον τύπο και το κοινό, εντούτοις με τις δραστηριότητες του αλλά και την φυλάκιση του, ξεσήκωσε κίνημα που υποστήριζε στην απελευθέρωση του, το “Free Kevin”<sup>95</sup>.

Ένας από τους ένθερμους υποστηρικτές του Mitnick ήταν το αμερικανικό περιοδικό σχετικά με το hacking το ‘2600 Magazine’, το οποίο φιλοξένησε συνέντευξη του Mitnick, άρθρα και γενικά ασχολήθηκε με διάφορες εκδηλώσεις διαμαρτυρίας για την υπερβολική τιμωρία του Mitnick καθώς και την αποφυλάκιση του. Ένδειξη διαμαρτυρίας για την φυλάκιση του Mitnick ήταν και ο ιστοτόπος <<http://www.freekevin.org>>. Ο Mitnick απέκτησε πολλούς υποστηρικτές που πίστευαν ότι η τιμωρία του ήταν υπερβολική και τον θεώρησαν σαν τον μεγαλύτερο hacker της εποχής μας καθώς επίσης και ως τον καλύτερο κοινωνικό μηχανικό (social engineer).

Σήμερα ο Mitnick έχει γράψει 2 βιβλία γύρω από την κοινωνική μηχανική και τα κενά ασφαλείας σε συστήματα. Έχει ιδρύσει την δικιά του εταιρία που ασχολείται με θέματα ασφαλείας σε δίκτυα, την Mitnick Security Consulting. Επίσης κάνει σεμινάρια ασφαλείας σε μεγάλες εταιρίες του χώρου. Όλα δείχνουν ότι απέβαλε τον μανδύα του «κακού» hacker.

Για τον Mitnick έχουν γραφτεί αρκετά βιβλία όπως το “Cyberpunk: outlaws and hackers on the computer frontier” του John Markoff (αρθρογράφος της εφημερίδας New York Time), το “Takedown: the pursuit and capture of Kevin Mitnick, America's most wanted computer outlaw-by the man who did it” των John Markoff και του Tsutomu Shimomura. Μια εναλλακτική θεώρηση του θέματος βρίσκεται στο βιβλίο του Jonathan Littman “The fugitive game: online with Kevin Mitnick”. Το βιβλίο προσφέρει μια άλλη οπτική γωνία και την ανάλυση των δεδομένων από τον ίδιο το Mitnick. Το 2000 παρουσιάστηκε η ταινία “Takedown,” βασισμένη στο βιβλίο, που δίχασε την κοινότητα για το πόσο αληθή είναι κάποια στοιχεία που περιέχει, και σκηνοθετημένη από τον Joe Chappelle. Η ταινία δεν κυκλοφόρησε λόγω της φήμης

---

=&spon=&&scp=1&sq=Tsutomu%20Shimomura%20mitnick%20%201994&st=cse> [9 Σεπτεμβρίου 2008].

<sup>95</sup> Thompson, C 2003, ‘The way we live now: 1-12-03: questions for Kevin Mitnick: connected again’, *The New York Times*, 12 Ιανουαρίου. Διαθέσιμο στο : <<http://query.nytimes.com/gst/fullpage.html?res=9A0DE3DA133EF931A25752C0A9659C8B63&scp=4&sq=Free%20Kevin&st=cse>> [9 Σεπτεμβρίου 2008].

ότι ο Mitnick κινήθηκε νομικά για συκοφαντική δυσφήμιση και διαστρέβλωση της πραγματικότητας.

Το 1999 ο Mitnick συμπεριλήφθηκε στο ρεκόρ Γκίνες με τον τίτλο «η πιο αξιοσημείωτη περίπτωση hacker», για τον οποίο υπήρξαν πολλές αντιδράσεις για το λόγο ότι ένας τέτοιος τίτλος δεν μπορεί να ευσταθεί λογικά. Το περιοδικό '2600' υποστηρίζει ότι «...θα ήταν πιο σωστό αν του δινόταν ο τίτλος της πιο ευρέως αναφερόμενης περίπτωσης hacker»<sup>96</sup>. Επίσης ένα γνωστό ντοκιμαντέρ σχετικά με τον Mitnick είναι και το Freedom Downtime<sup>97</sup>.

Ο ίδιος ο Mitnick χαρακτηρίζει τον εαυτό του «...βλέπω τον εαυτό μου σαν ηλεκτρονικό καβαλάρη... ήμουν σαν τον James Bond πίσω από τον υπολογιστή. Απλώς ανατίναξα... Ήμουν ολοκληρωμένος εισβολέας. Δεν θεωρώ τον εαυτό μου κλέφτη»<sup>98</sup>.

Ιστοσελίδα Mitnick Security Consulting <<http://www.kevinmitnick.com>>.

### 2.3 Kevin Poulsen

Γνωστός και ως «Dark Dante». Γεννήθηκε στην Pasadena της Καλιφόρνιας το 1965. Λέγεται ότι ήταν 17 χρονών όταν χρησιμοποίησε το Radio shack TRS- 80 (μικρουπολογιστής) για να επιτεθεί στο ARPANET. Για αυτή του την πράξη ο Poulsen δεν καταδικάστηκε, παρόλο που ήταν καταζητούμενος για παράβαση του νόμου. Δούλεψε σαν προγραμματιστής στο Stanford Research Institute (SRI) and Sun Microsystems και σαν σύμβουλος δοκιμών στην υπηρεσία ασφάλειας του Πενταγώνου. Το 1988 οι αρχές υποψιάστηκαν ότι διείσδυσε στα απόρρητα κυβερνητικά αρχεία. Όταν κατάλαβε ότι το FBI τον καταζητούσε, εξαφανίστηκε. Όντας καταζητούμενος διείσδυσε σε κυβερνητικούς υπολογιστές και απορρέοντας πληροφορίες από τα αρχεία του FBI και βοηθούσε παραβάτες ακόμα και το αμερικανικό κίνημα απελευθερωτικού αγώνα παρέχοντας τους πληροφορίες από τα απόρρητα αρχεία του FBI<sup>99</sup>.

---

<sup>96</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

<sup>97</sup> *Freedom downtime: the story of Kevin Mitnick* 2003, (video recording), 2600 Films. Διαθέσιμο στο: <<http://video.google.ca/videoplay?docid=-6746139755329108302>> [11 Σεπτεμβρίου 2008].

<sup>98</sup> 'Mitnick gets out of Lompoc' 2000, *Wired magazine*, 21 Ιανουαρίου. Διαθέσιμο στο: <<http://www.wired.com/news/politics/0,1283,33823,00.html>> [11 Σεπτεμβρίου 2008].

<sup>99</sup> Biersdorfer, JD 1997, 'Books in brief: nonfiction', *The New York Times*, 30 Μαρτίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9504E5D7173BF933A05750C0A961958260&n=Top/Features/Books/Book%20Reviews&scp=1&sq=Kevin%20Poulsen%20fbi&st=cse>> [11 Σεπτεμβρίου 2008].

Κυρίως όμως ο λόγος που έγινε γνωστός ήταν για την υποκλοπή στις τηλεφωνικές γραμμές του ραδιοσταθμού Kiss στο Λος Άντζελες, η οποία του απέφερε, μεταξύ των υπόλοιπων «δώρων» και μία ολοκαίνουργια Porsche. Οι αρχές τον αποκάλεσαν «ο Hannibal Lecter του ηλεκτρονικού εγκλήματος»<sup>100</sup>.

Ο Poulsen τελικά συνελήφθη σε ένα σούπερ-μάρκετ και καταδικάστηκε για 5 χρόνια φυλάκισης. Τον Ιούνιο του 1994 κρίνεται ένοχος για απάτες υπολογιστών και κλοπή χρημάτων καθώς και για αποφυγή δικαιοσύνης. Καταδικάζεται για 51 μήνες φυλάκισης και πρόστιμο 56.000 δολάρια. Ήταν η μεγαλύτερη ποινή που δόθηκε σε hacker. Αργότερα βέβαια βρέθηκε ένοχος για παράνομη εισβολή σε υπολογιστές και απόσπαση απόρρητων πληροφοριών. Όταν εκτέλεσε την ποινή του αφέθηκε ελεύθερος με τον όρο να μην ακουμπήσει υπολογιστή για 3 χρόνια<sup>101</sup>.

Σήμερα εργάζεται ως δημοσιογράφος και αρχισυντάκτης του Wired News. Το πλέον εξέχον άρθρο του αφορά την ανακάλυψη 744 σεξουαλικών παραβάσεων μέσω του MySpace. Καθώς επίσης εργάζεται και σαν συντάκτης του ιστοτόπου “Security Website” της Security Focus.

Η ιστορία της ζωής του γράφτηκε σε βιβλίο με τον τίτλο «The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen» με συγγραφέα τον Jonathan Littman.

Η προσωπική ιστοσελίδα του Kevin Poulsen <<http://www.kevinpoulsen.com>>.

## 2.4 Robert Tappan Morris

Ο Robert Morris γεννήθηκε το 1965, ενώ ο πατέρας του ήταν πρώην επιστήμονας του Κέντρου Εθνικής Ασφάλειας Ηλεκτρονικών Υπολογιστών, το οποίο ήταν τμήμα της National Security Agency (NSA – Υπηρεσίας Εθνικής Ασφάλειας). Ο Robert Morris, είναι γνωστός ως ο δημιουργός του “Morris Worm” –του πρώτου σκουληκιού (είδος ιού)— που κυκλοφόρησε στο Διαδίκτυο το 1988. Το σκουλήκι αυτό του επέτρεπε να σερφάρει στο Διαδίκτυο δωρεάν. Όταν ο Morris δημιούργησε το σκουλήκι ήταν 23 ετών και έγραψε αυτό το πειραματικό πρόγραμμα –αποτελούμενο από έναν κώδικα μεγέθους 99 γραμμών— ως απόφοιτος του Πανεπιστημίου Cornell και το κυκλοφόρησε στο Διαδίκτυο. Ο ίδιος ο Morris στην απολογία του στο δικαστήριο δήλωσε ότι το έκανε με σκοπό να ανακαλύψει πόσο ευρύ είναι το

<sup>100</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

<sup>101</sup> Garfinkel, S 2002, ‘The FBI's cybercrime crackdown’, *Technology Review*. Διαθέσιμο στο: <<http://jrichardstevens.com/articles/garfinkle-FBI.pdf>> [11 Σεπτεμβρίου 2008].

Διαδίκτυο. Έτσι απελευθέρωσε το σκουλήκι από το MIT ελπίζοντας να πετύχει αυτό του το στόχο<sup>102</sup>.

Το σκουλήκι, ωστόσο, πολλαπλασιάστηκε τρομακτικά, με αποτέλεσμα να μειώνει τόσο πολύ τις ταχύτητες των υπολογιστών ώστε να καθίστανται τελικά άχρηστοι. Οι ειδικοί υπολογίζουν ότι το σκουλήκι προσέβαλλε περί τους 6.000 υπολογιστές. Εκτός ότι μόλυνε τους υπολογιστές είχε και την ιδιότητα να ξαναστέλνεται στα πρώτα πέντε άτομα του καταλόγου ηλεκτρονικού ταχυδρομείου (email list) του κάθε υπολογιστή. Όταν αντιλήφθηκε το μέγεθος της ζημιάς που δημιούργησε τηλεφώνησε σε ένα φίλο του στο Harvard για να βρουν μια λύση. Έτσι προσπάθησαν να στείλουν ένα ανώνυμο μήνυμα σε όλο το δίκτυο με κατευθυντήριες γραμμές και υποδείξεις για τους προγραμματιστές για το πως να σταματήσουν το σκουλήκι. Επειδή όμως το δίκτυο ήταν φραγμένο, το μήνυμα δεν κατόρθωσε να σταλεί. Το αποτέλεσμα ήταν να μολυνθούν πολλοί υπολογιστές και το υπολογιζόμενο κόστος αντιμετώπισης του σκουληκιού για κάθε εγκατάσταση κυμάνθηκε από 200 μέχρι 53.000 δολάρια. Για να περιοριστεί η διάδοση της επιδημίας, πολλά δίκτυα αναγκάστηκαν να αποσυνδεθούν από το Διαδίκτυο<sup>103</sup>.

Ο Morris καταδικάστηκε σε 3 χρόνια αστυνομικής επιτήρησης, τετρακόσιες ώρες κοινωνικής εργασίας και πρόστιμο 10.500 δολαρίων. Κρίθηκε ένοχος για απάτη μέσω υπολογιστή και κακόβουλη πράξη. Ο Morris επέμενε ότι δεν είχε πρόθεση να προξενήσει ζημιές σε δίκτυα, παραδέχτηκε ότι επεδίωκε να αποκτήσει πρόσβαση στα «μολυσμένα συστήματα» και έτσι βρέθηκε ένοχος για μη εγκεκριμένη πρόσβαση σε υπολογιστή κυβερνητικού ενδιαφέροντος, δηλαδή υπολογιστές που χειρίζεται αποκλειστικά η ομοσπονδιακή κυβέρνηση ή οικονομικά ιδρύματα σύμφωνα με το Νόμο Computer Fraud & Abuse Act του 1986.

Μετά το σκουλήκι του Morris, ιδρύεται η CERT (Computer Emergency Response Team) για να εξετάσει τις ανησυχίες που προκλήθηκαν από το επεισόδιο αυτό. Σήμερα ο Robert Tappan Morris είναι βοηθός διευθυντής στο Massachusetts Institute of Technology και το 2005 βοήθησε στην ίδρυση της επενδυτικής εταιρείας Y Combinator.

Η προσωπική ιστοσελίδα του Robert Tappan Morris<<http://pdos.csail.mit.edu/~rtm/>>.

---

<sup>102</sup> Berk, V, Bakos, G & Morris, R 2003, 'Designing a framework for active worm detection on global networks', *Proceedings of the IEEE International Workshop on Information Assurance*, pp. 13-23. Διαθέσιμο στο: IEEE Xplore [11 Σεπτεμβρίου 2008].

<sup>103</sup> Chen, T M & Robert, J M 2004, 'Worm epidemics in high-speed networks', *Computer*, vol. 37, no. 6, pp. 48-53. Διαθέσιμο στο: IEEE Computer Society Digital Library [11 Σεπτεμβρίου 2008].



## 2.5 Vladimir Levin

Ο Ρώσος Vladimir Levin ήταν βιοχημικός απόφοιτος του Πανεπιστημίου Τεχνολογίας του St. Petersburg στην Ρωσία. Βοήθησε στο να γίνει η πρώτη διάρρηξη της διεθνούς τράπεζας στο Διαδίκτυο.

Η υπόθεση Citibank στιγματίσε την κοινότητα των hackers. Το Ιούλιο του 1994, ο Levin οργάνωσε μία κλοπή κάνοντας τους υπολογιστές της εταιρίας να διανείμουν περίπου 10 εκατομμύρια δολάρια στον ίδιο και τους συνεργούς του σε 7 διαφορετικές χώρες. Διείσδυσε στο σύστημα διαχείρισης μετρητών, το οποίο επέτρεπε στους πελάτες να κάνουν τις δικές τους συναλλαγές με άλλες τράπεζες. Δούλενε αργά τη νύχτα από το διαμέρισμα του στη Ρωσία κρατώντας τις εργασιακές ώρες της Νέας Υόρκης, ώστε να αποφύγει την ασφάλεια της Citibank. Για να αποφύγει τον περαιτέρω έλεγχο χρησιμοποιούσε έγκυρες ταυτότητες και κώδικες άλλων τραπεζών. Ο τρόπος με τον οποίο ο Levin πήρε αυτούς τους κωδικούς παραμένει μέχρι σήμερα ανεξιχνίαστο. Αν και η Citibank δηλώνει ότι μάλλον ήταν δουλειά εκ των έσω. Μέσα σε μερικές βδομάδες οι συναλλαγές γίνονταν στην τράπεζα Bank America και φυλάγονταν από τις εταιρίες Primorye και Shore, που και οι δύο βρίσκονταν στο San Francisco και ανήκαν στον Jevgenij Korolkov, φίλο του Levin. Σύμφωνα με την Citibank τα συστήματα ασφαλείας κατέγραψαν δύο παράξενες συναλλαγές τον Αύγουστο του 1994. Η μια 26.800 δολάρια και η άλλη 304.000 δολάρια. Τότε η Citibank άρχισε τις έρευνες, ενώ ο Korolkov και ο Levin στρατολόγησαν νέους συνεργάτες. Τον Οκτώβριο του 1994 ακόμα 40 συναλλαγές στην Καλιφόρνια, στο Ισραήλ, στη Γερμανία, στην Ελβετία και Ολλανδία. Τότε το FBI ξεκίνησε τις έρευνες με τη συνεργασία της Citibank και τη βοήθεια των τηλεπικοινωνιακών εταιριών στην Ρωσία. Έτσι εντοπίστηκαν οι παράνομες συναλλαγές και η Interpol συνέλαβε τον Levin και την ομάδα του στο αεροδρόμιο Heathrow του Λονδίνου. Επίσης συνελήφθησαν και πέντε συνεργάτες του σε άλλες χώρες (Ισραήλ, Ολλανδία, ΗΠΑ)<sup>104</sup>.

Ο Levin δήλωσε ένοχος και το Γενάρη του 1998 παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς από πελάτες της Citibank για να μεταφέρει χρήματα στους λογαριασμούς του. Δήλωσε ένοχος σε κατηγορίες συνομοσίας για τραπεζική απάτη και απάτη με υπολογιστές. Το Φεβρουάριο του 1998 καταδικάστηκε σε τρία έτη φυλάκισης και σε υποχρέωση αποζημίωσης της Citibank 240.015 δολαρίων. Η

<sup>104</sup> Gissel R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press Διαθέσιμο στο: Google Books Search [12 Σεπτεμβρίου 2008].

τράπεζα πήρε πίσω το μεγαλύτερο μέρος των χρημάτων της και κατάφερε να ανακτήσει τα περισσότερα χρήματα.

## 2.6 Mark Abene

Γεννήθηκε το 1972 στην Νέα Υόρκη όπου έζησε και έδρασε. Χρησιμοποιούσε το ψευδώνυμο του Phiber Optik αλλά και επίσης γνωστός ως Il Duce. Ο Mark Abene υπήρξε αρχηγός των MOD (Masters Of Deception ) μετά την εκδίωξη του από τους LOD και τη διαμάχη του με τον Erik Bloodaxe. Το 1990 ξέσπασε ανάμεσα στις δύο ομάδες ο διετής «Μεγάλος Πόλεμος των Hackers» πάντα σε δικτυακό επίπεδο. Υπήρξε ένας υψηλού προφίλ hacker στη δεκαετία του 1990. Είχε γίνει γνωστός σε όλη την Αμερική καθώς συνεντεύξεις του είχαν δημοσιευτεί σε διάφορα περιοδικά.

Όταν το εθνικό τηλεφωνικό σύστημα της AT&T καταστράφηκε, τότε μυστικές υπηρεσίες της Αμερικής μπήκαν στο σπίτι του Mark Abene στις 24 Ιανουαρίου 1990. Σύμφωνα με πληροφορίες ο Abene και η ομάδα του ήταν υπαίτιοι για την κατάρρευση του συστήματος. Παρόλα αυτά η AT&T αρνήθηκε ότι είχαν χτύπημα από hacker και δήλωσε ότι το πρόβλημα οφειλόταν σε λογισμικό λάθος<sup>105</sup>.

Το Φεβρουάριο του 1991 ο Mark Abene κατηγορήθηκε από την Πολιτεία της Νέας Υόρκης για παράνομη πρόσβαση σε υπολογιστή, υποκλοπή πληροφοριών και για δολιοφθορά στην τηλεφωνική υπηρεσία 900. Βρέθηκε ένοχος και καταδικάστηκε σε 35 ώρες κοινωνικής εργασίας. Επίσης το Δεκέμβριο του 1991 ο Mark Abene και άλλα 4 μέλη των MOD συνελήφθησαν και κατηγορήθηκαν για παραβάσεις, όπως συνομωσία και παράνομη πρόσβαση σε υπολογιστικά κυβερνητικά συστήματα<sup>106</sup>.

Το 1994 ο Mark Abene καταδικάστηκε σε 1 χρόνο φυλάκιση, 3 χρόνια επιτήρηση και 600 ώρες κοινωνικής εργασίας. Οι κατηγορίες που του προσάπτονταν ήταν παράνομη πρόσβαση σε υπολογιστές και τηλεφωνικά συστήματα. Όταν μαθεύτηκε ότι επρόκειτο να φυλακιστεί, πολλοί ήταν εκείνοι που τον υποστήριζαν. Μέσα στο δίκτυο κυκλοφόρησαν αρκετές προκηρύξεις διαμαρτυρίας. Στην απολογία του Mark Abene δήλωσε ότι δεν είχε πρόθεση να κάνει κακό σε κανένα σύστημα. Χαρακτηριστική όμως ήταν και η δήλωση του δικαστή, ο οποίος τον καταδίκασε:

---

<sup>105</sup> Timothy, S U 1996, 'Cyberspace sovereignty: the Internet and the international system', *Harvard Journal of Law & Technology*, vol. 10, no. 3. Διαθέσιμο στο: <<http://scholar.google.gr/scholar?q=info:nUhCDdzpP8J:scholar.google.com/&hl=en&lr=&output=viewport&shm=1>> [12 Σεπτεμβρίου 2008].

<sup>106</sup> Ramirez, A 1992, 'Are indicted in computer credit theft', *The New York Times*, 9 Ιουλίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9E0CE7D6133DF93AA35754C0A964958260&sec=&spon=&&scp=1&sq=%20Phiber%20Optik%201991%20&st=cse>> [12 Σεπτεμβρίου 2008].

«Μπορεί να έχετε δίκιο, μα πρέπει να σταλεί επιτέλους ένα μήνυμα σε όλους τους επίδοξους ηλεκτρονικούς εγκληματίες»<sup>107</sup>.

Το Σεπτέμβριο του 2000 ο Mark Abene προκάλεσε αναστάτωση στην υπηρεσία ασφαλείας υπολογιστών μετά την απόρριψη της αίτησης του για να εργαστεί εκεί λόγω του παρελθόντος του. Αυτό το γεγονός όξινε την διαμάχη μεταξύ hackers και υπεύθυνων ασφαλείας, καθώς και τις συζητήσεις για το ρόλο των hackers και την εργοδότησή τους στις υπηρεσίες ασφαλείας υπολογιστών. Τώρα ο Abene κάνει μια φιλήσυχη ζωή ως ανεξάρτητος ασφαλιστής υπολογιστών, ενώ έχει λάβει μέρος και στην κινηματογραφική παραγωγή *Urchin* το 2007.

## 2.7 Andrew Miffleton – Daphtpunk

Καταγόταν από το Arlington του Τέξας και σχετιζόταν με την γνωστή ομάδα “the darkside Hackers”, μια ομάδα με υψηλό επίπεδο γνώσεων που σκοπό είχε την παράνομη διείσδυση σε υπολογιστικά συστήματα. Από το Μάιο του 1998 μέχρι τον Φεβρουάριο του 1999 ο Miffleton χρησιμοποιούσε το ψευδώνυμο Daphtpunk. Δημιούργησε την ιστοσελίδα των «the darkside Hackers».

Το Φεβρουάριο του 1999 εξασφάλισε μια λίστα από κωδικούς της Εθνικής Υπηρεσίας Διαδικτύου. Αυτοί οι κωδικοί επέτρεπαν στο χρήστη να έχει τον πλήρη έλεγχο του συστήματος (root – level password). Ο Miffleton διάδωσε αυτούς τους κωδικούς μέσα στη ομάδα και έτσι οι «the darkside Hackers» διείσδυσαν σε πολλούς υπολογιστές σε όλη την χώρα δημιουργώντας έτσι ζημιά 90.000 δολαρίων στην Verio (μηχανή αναζήτησης ιστοσελίδων στο Διαδίκτυο)<sup>108</sup>.

Στις 24 Ιουλίου το 2000 ο Andrew Miffleton σε ηλικία 25 ετών καταδικάστηκε από το ομοσπονδιακό δικαστήριο σε 21 μήνες φυλάκισης και 3.000 δολάρια πρόστιμο καθώς και 89.480 δολάρια αποζημίωση. Οι κατηγορίες που αντιμετώπισε ήταν η παράνομη πρόσβαση σε υπολογιστή, η κακόβουλη πράξη, η κατοχή παράνομων συσκευών πρόσβασης και η δόλια χρήση κινητών τηλεφώνων.

Σήμερα εργάζεται στο Learning and Teaching Institute at Sheffield, Centre for Learning & Performance Technologies<sup>109</sup>.

<sup>107</sup> Σπυράκης. Π 1997, 'Εγκλημα στον κυβερνοχώρο', *Το Βήμαonline*, 13 Ιανουαρίου. Διαθέσιμο στο: <[http://tovima.dolnet.gr/print\\_article.php?e=B&f=12461&m=I20&aa=1](http://tovima.dolnet.gr/print_article.php?e=B&f=12461&m=I20&aa=1)> [12 Σεπτεμβρίου 2008].

<sup>108</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο : Google Books Search [12 Σεπτεμβρίου 2008].

<sup>109</sup> Poulsen, K 2001, 'Max vision begins 18-month term', *Security Focus*. Διαθέσιμο στο <<http://www.securityfocus.com/news/221>> [12 Σεπτεμβρίου 2008].

## 2.8 David Smith

Ο David Smith είναι ο δημιουργός του ιού “Melissa” που χάριν σε αυτόν έγινε παγκοσμίως γνωστός. Το 1999, όταν ήταν 31 χρονών εξάπλωσε τον ιό στο Διαδίκτυο. Ο “Melissa”, είναι ένας «μακρο-ιός» που εμφανίστηκε τον Απρίλιο του 1999 θέτοντας εκτός λειτουργίας τα υπολογιστικά συστήματα 300 εταιριών και επηρεάζοντας συνολικά πάνω από 100.000 χρήστες μέσα σε μερικές μόνο ώρες από την κυκλοφορία του. Αυτός ο ιός αναπαραγόταν μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και προκαλούσε ζημιές στα αρχεία του χρήστη. Ο εντοπισμός του Smith έγινε μέσω ενός άγνωστου στον πολύ κόσμο αλλά και στον Smith— κωδικού που χαρακτηρίζει τον υπολογιστή, στον οποίο γράφεται ένα αρχείο Word. Ο ιός κυκλοφόρησε σε διαφημιστικούς, στρατιωτικούς και κυβερνητικούς υπολογιστές δημιουργώντας ζημιά γύρω στα 80 εκατομμύρια δολάρια<sup>110</sup>.

Συνελήφθηκε από τις κυβερνητικές αρχές στο New Jersey ως υπεύθυνος για τη δημιουργία και τη διανομή μέσω του Διαδικτύου του ηλεκτρονικού ιού “Melissa”, ενώ ομολόγησε την ενοχή του ενώπιον του δικαστηρίου. Ο ίδιος δήλωσε ότι δεν γνώριζε το πόσο επικίνδυνο ήταν αυτό που έφτιαξε ούτε το πόσο κακό μπορούσε να προξενήσει.

Λίγες μέρες μετά την σύλληψη του, ένας πανομοιότυπος τύπος ιού εξαπλώθηκε στο Διαδίκτυο. Ο καινούριος κλώνος του “Melissa” λεγόταν “Papa”. Ο “Papa” ήταν ένας ιός του Excel ο οποίος αποστέλλόταν με τον ίδιο τρόπο όπως ο “Melissa”, δηλαδή μέσω ηλεκτρονικού ταχυδρομείου. Ύστερα από διαπραγματεύσεις μεταξύ των συνηγόρων του και των αμερικανικών Αρχών, ο Smith είχε μια προσφορά. Θα μπορούσε να μειώσει τα χρόνια φυλάκισης του από 10 χρόνια φυλάκισης και πρόστιμο 50.000 δολάρια σε ποινή 20 μηνών κράτησης, 3.000 δολάρια πρόστιμο και 3 χρόνια παρακολούθησης μετά την αποφυλάκιση του. Αυτά με την προϋπόθεση να βοηθήσει και να συνεργαστεί με τις αρχές άλλων δημιουργών ιών παρόμοιων με τον “Melissa”. Έτσι από το Μάιο του 2001 ο David Smith εκτίει την προσυμφωνημένη καταδίκη του. Επίσης του απαγορεύτηκε η πρόσβαση σε δίκτυα εκτός και αν έχει άδεια δικαστηρίου<sup>111</sup>.

---

<sup>110</sup> Becker, M 2002, ‘Fed. pen for e-mail virus guy’, *NY Daily News*, 2 Μαΐου. Διαθέσιμο στο: <[http://www.nydailynews.com/archives/news/2002/05/02/2002-05-02\\_fed\\_pen\\_for\\_email\\_virus\\_guy.html](http://www.nydailynews.com/archives/news/2002/05/02/2002-05-02_fed_pen_for_email_virus_guy.html)> [12 Σεπτεμβρίου 2008].

<sup>111</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο : Google Books Search [12 Σεπτεμβρίου 2008].

## 2.9 Timothy Lloyd (Computer Sabotage)

Ο Timothy Lloyd ήταν προγραμματιστής υπολογιστών στην κατασκευαστική εταιρεία Omega Engineering στο Bridgeport του New Jersey. Η εταιρία αυτή κατασκεύαζε συσκευές μέτρησης για το ναυτικό. Ο Timothy Lloyd είναι μια χαρακτηριστική περίπτωση οργισμένου απολυμένου που παίρνει εκδίκηση. Όταν απολύθηκε για λόγους μειωμένης απόδοσης, εξαπέλυσε μέσα στο υπολογιστικό σύστημα της εταιρίας μια λογική βόμβα.

Δούλευε για την Omega 11 χρόνια και είχε μία διευθυντική θέση στο τμήμα που ήταν υπεύθυνο για το δίκτυο. Μια τέτοια θέση τον έκανε ειδήμονα στους ηλεκτρονικούς υπολογιστές και τα δίκτυα. Η βόμβα είχε ως σκοπό να σβήσει το πρόγραμμα σχεδιασμού και παραγωγής της Omega Engineering Corporation ένα από τα σημαντικότερα συστήματα της εταιρίας<sup>112</sup>.

Μετά από έρευνα των μυστικών υπηρεσιών, το Μάιο του 2000, ο Timothy Lloyd κρίθηκε ένοχος για το μεγαλύτερο σαμποτάζ σε υπολογιστές. Μετά την σύλληψη του ομολόγησε ότι έγραψε 6 γραμμές κώδικα και δημιούργησε ένα πρόγραμμα-βόμβα που 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 δολιοφθοράς υπολογιστών (computer sabotage), προξενώντας στην Omega σχεδόν 10 εκατομμύρια δολάρια σε απώλειες πωλήσεων. Ο Lloyd θεωρήθηκε υπεύθυνος και για το σκουλήκι με την ονομασία “Love Letter”. Το σκουλήκι αυτό εξαπλωνόταν μέσω ηλεκτρονικού ταχυδρομείου και το κόστος των μηχανημάτων που είχαν μολυνθεί παγκοσμίως πιθανολογείται ότι έφτασε τα 45 εκατομμύρια ευρώ<sup>113</sup>.

---

<sup>112</sup> Tahmincioglu, E.2001, ‘Management: vigilance in the face of layoff rage: employer miscues can breed retaliation’, *The New York Times*, 1 Αυγούστου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9C04EFDB1F3DF932A3575BC0A9679C8B63&sc=&spon=&&scp=4&sq=Timothy%20Lloyd%20Omega%20Engineering%20Corporation&st=cse>> [12 Σεπτεμβρίου 2008].

<sup>113</sup> Strunsky, S 2002, ‘Metro briefing | New Jersey: Newark: prison sentence in computer case’, *The New York Times*, 27 Φεβρουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9C07EFD91431F934A15751C0A9649C8B63&scp=3&sq=Timothy%20Lloyd%20Omega%20Engineering%20Corporation&st=cse>> [12 Σεπτεμβρίου 2008].

## 2.10 Michael Calce – Mafiaboy

Το ψευδώνυμο Mafiaboy ανήκε στο δεκαεξάχρονο μαθητή που κατοικούσε στο Μόντρεαλ του Καναδά<sup>114</sup>. Στις 18 Απριλίου 2000, μετά από ανθρωποκυνηγητό που εξαπέλυσε το FBI, ο Mafiaboy συλλαμβάνεται και κρίνεται ένοχος ενώπιον δικαστηρίου του Μόντρεαλ, για κατηγορίες επιθέσεων σε 64 δημοφιλείς δικτυακούς τόπους όπως το CNN.com, Yahoo.com, το EBay.com, Dell.com και το Amazon.com. Σύμφωνα με την αστυνομία ο Mafiaboy υπερηφανευόταν για την επίτευξη των επιθέσεων σε διάφορα δωμάτια δημοσίων συζητήσεων (chatrooms) και έτσι εντοπίστηκε<sup>115</sup>.

Οι καναδικές Αρχές αποδίδουν στο Mafiaboy 64 συνολικά επιθέσεις σε δικτυακούς τόπους, που είχαν αποτέλεσμα να τεθούν οι δικτυακοί τόποι εκτός λειτουργίας για αρκετές ώρες (internet blackout). Οι Αρχές ισχυρίστηκαν ότι εισέβαλε σε πολλούς υπολογιστές, κυρίως αμερικανικών πανεπιστημίων και χρησιμοποίησε τα δίκτυα αυτά για να εξαπολύσει τις επιθέσεις του στους δικτυακούς αυτούς τόπους. Παρά το γεγονός ότι δήλωσε αθώος, οι Αρχές είχαν συγκεντρώσει αρκετά στοιχεία, ικανά να αποδείξουν την ενοχή του και να τον καταδικάσουν σε δύο χρόνια φυλάκισης. Αφέθηκε ελεύθερος με εγγύηση και με την προϋπόθεση να χρησιμοποιεί τους υπολογιστές μόνο στο σχολείο και υπό την επίβλεψη καθηγητή. Το όνομα του νεαρού απαγορευόταν, σύμφωνα με τον καναδικό νόμο, να αποκαλυφθεί, επειδή είναι ανήλικος<sup>116</sup>.

Ο Mafiaboy συλλαμβάνεται και πάλι επειδή παρεμβαίνει τους περιοριστικούς όρους που του είχαν επιβληθεί όταν συνελήφθη. Οι Αρχές τού είχαν επιτρέψει να ζει στο σπίτι του επιβάλλοντάς του όμως όρους όπως να παραμένει μακριά από υπολογιστές, να παρακολουθεί καθημερινά τα σχολικά μαθήματα και να μένει εν γένει ήσυχος. Ο Mafiaboy συνελήφθη εκ νέου, επειδή απουσίαζε από το σχολείο και δεν πειθαρχούσε στους καθηγητές του.

---

<sup>114</sup> Richtel, M 2000, 'Canada arrests 15-year-old in web attack', *The New York Times*, 20 Απριλίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9F04E0DC1131F933A15757C0A9669C8B63&sec=&spon=&scp=2&sq=Mafiaboy&st=cse>> [12 Σεπτεμβρίου 2008].

<sup>115</sup> Beale, L 2000, 'Seven days the last word on last week', *NY Daily News*, 23 Απριλίου. Διαθέσιμο στο: <[http://www.nydailynews.com/archives/news/2000/04/23/2000-04-23\\_seven\\_days\\_the\\_last\\_word\\_on\\_.html](http://www.nydailynews.com/archives/news/2000/04/23/2000-04-23_seven_days_the_last_word_on_.html)> [12 Σεπτεμβρίου 2008].

<sup>116</sup> 'Canada broadens its case against suspected hacker' 2000, *The New York Times*, 4 Αυγούστου. Διαθέσιμο στο: <<http://partners.nytimes.com/library/tech/00/08/biztech/articles/04hacker.html?scp=1&sq=Mafiaboy%2064&st=cse>> [12 Σεπτεμβρίου 2008].

Στην απολογία του έχει δηλώσει αθώος για περισσότερες από 60 περιπτώσεις «επιθέσεων» σε υπολογιστικά συστήματα. Αρχικά αρνήθηκε την ευθύνη, αλλά αργότερα κρίθηκε ένοχος για τις περισσότερες από τις κατηγορίες που του προσήψαν. Ο δικηγόρος του νεαρού επέμενε το παιδί δεν είχε σκοπό να βλάψει, αλλά έκανε μόνο δοκιμές για να βοηθήσει στο σχεδιασμό ενός βελτιωμένου τείχους ασφαλείας. Οι έρευνες όμως έδειξαν ότι ο Mafiaboy δεν έδειξε μεταμέλεια και εξέφρασε την επιθυμία να κινηθεί προς την Ιταλία, καθώς διατηρεί πιο χαλαρή νομοθεσία όσον αφορά στην εγκληματικότητα<sup>117</sup>.

Κατά το 2005, ο Mafiaboy γράφει ως αρθρογράφος για θέματα ασφαλείας υπολογιστών για τη γαλλόφωνη εφημερίδα “Le Journal de Montréal”. Αργότερα το φθινόπωρο του 2008, στα 23 του χρόνια ο Mafiaboy μαζί με το δημοσιογράφο Craig Silverman, εκδίδουν ένα βιβλίο σχετικά με την επίθεση που εξαπέλησε ο Mafiaboy το 2000 στο Διαδίκτυο. Ο τίτλος του βιβλίου είναι “Mafiaboy: how I cracked the Internet and why it’s still broken”. Μετά την έκδοση του βιβλίου αποκαλύφθηκε το όνομα του, Michael Calce. Ο 23χρονος hacker εξηγεί στο βιβλίο του ότι δεν ήταν από τους ανθρώπους που περνούσε όλη τη ζωή του μπροστά από έναν υπολογιστή. Απλά έμαθε πολύ γρήγορα να τους χειρίζεται και διεύρυνε τις γνώσεις του κάνοντας παρέα με άλλους hackers. «...αισθάνθηκα πολύ οικεία ανάμεσα σε όλους αυτούς του ανώνυμους προγραμματιστές και αντάρτες του Διαδικτύου», λέει σε ένα απόσπασμα του βιβλίου και συμπληρώνει «...για μένα αυτά τα άτομα ήταν τα πιο ενδιαφέροντα στον κυβερνοχώρο. Ήθελα να βγαίνω έξω μαζί τους. Ήθελα να γίνω κι εγώ hacker» Στις 26 Οκτωβρίου 2008 εμφανίστηκε στη γαλλοκαναδική τηλεόραση στην τηλεοπτική εκπομπή “Tout le Monde en Parle” για να μιλήσει για το βιβλίο.

## 2.11 Patrick W. Gregory – MostHateD

Ο Patrick W. Gregory στα 19 του χρόνια ήταν μέλος της οργάνωσης globalHell, ενός διαδικτυακού οργανισμού των hackers. Ο Patrick W. Gregory –πιο γνωστός ως με το ψευδώνυμο MostHateD— μετά την σύλληψη του παραδέχτηκε ότι αυτός και η ομάδα του ήταν υπεύθυνοι για σημαντικές υποθέσεις hacking με ζημιές σε διάφορες αμερικανικές εταιρείες και κρατικές υπηρεσίες –όπως ο Λευκός Οίκος και ο Αμερικανικός Στρατός— που ξεπερνούν το 1.5 εκατομμύριο δολάρια. Ο Gregory παραδέχτηκε ότι χρησιμοποιούσε κλεμμένους τηλεφωνικούς αριθμούς, αριθμούς

<sup>117</sup> ‘Prison urged for Mafiaboy’ 2007, *Wired magazine*, 20 Μαΐου. Διαθέσιμο στο: <<http://www.wired.com/politics/law/news/2001/06/44673>> [12 Σεπτεμβρίου 2008].

κλεμμένων ταυτοτήτων και αριθμούς πιστωτικών καρτών, ενώ υπέκλεπτε τις υπηρεσίες τηλεφωνικών διασκέψεων από την AT&T, την MCI και τη Latitude Communications για να συνομιλεί με άλλους hackers σε όλη τη χώρα<sup>118</sup>.

Το 1998 χρησιμοποιώντας ένα κλεμμένο PIN (Personal Identification Number – Προσωπικός Αριθμός Ταυτοποίησης), που ανήκε στην AT&T, μετέφερε με τηνβοήθεια της ομάδας του 4200.00 δολάρια σε τρίτο πρόσωπο. Επίσης, ο ίδιος ευθύνεται και για μία σειρά παραβιάσεων των υπολογιστών διάφορων ISPs (Internet Service Provider – Παροχέας Υπηρεσιών Διαδικτύου) της Αμερικής<sup>119</sup>.

Το 1999 παραβιάζει το υπολογιστικό σύστημα της 1688.com κλέβοντας τραπεζικές πληροφορίες μηνύματα ηλεκτρονικού ταχυδρομείου και τα προώθησε στο Διαδίκτυο. Κρίθηκε ένοχος για όλα αυτά και καταδικάστηκε σε 26 μήνες φυλάκιση, αποζημίωση ύψους 154.529,86 δολαρίων και 3 χρόνια επιτήρηση. Μετά την αποφυλάκιση του, προσπάθησε να ανοίξει δική του εταιρεία που θα ασχολείται με την ασφάλεια υποκλοπής τηλεφωνικών συσκευών.

## 2.12 Adrian Lamo

Ο Adrian Lamo, γεννημένος το 1981, είναι πρώην γκρίζος hacker και νυν δημοσιογράφος. Γεννήθηκε στη Βοστώνη της Μασαχουσέτη, ενώ αργότερα μετακομίζει με την οικογένειά του στο Σαν Φρανσίσκο, όπου θα ζήσει και θα δράσει. Η φήμη του κυρίως προέρχεται από τις «εισβολές» του σε γιγαντιαίους οργανισμούς όπως οι New York Times και η Microsoft. Επίσης είναι γνωστός και για την προσπάθειά του να εντοπίσει τα κενά ασφάλειας στα δίκτυα υπολογιστών της εταιρίας Fortune 500<sup>120</sup>.

Παρά το υψηλό προφίλ της δουλειάς του ο Adrian Lamo ποτέ δεν δέχθηκε να πληρωθεί για την δουλειά του. Η κοινότητα των hackers τον αποκαλούσε «homeless hacker», επειδή χρησιμοποιούσε το Διαδίκτυο από διάφορα μέρη όπως βιβλιοθήκες ή καφετέριες. Όπως είπε κάποτε και ο ίδιος: «...έχω ένα laptop στο Pittsburgh και μια αλλαξιά ρούχα στο D.C.»<sup>121</sup>.

---

<sup>118</sup> Poulsen, K 2001, 'Hackers face life imprisonment under 'Anti-Terrorism' Act', *Security Focus*, 24 Σεπτεμβρίου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/257>> [12 Σεπτεμβρίου 2008].

<sup>119</sup> Poulsen, K 2000, MostHateD to Plead Guilty Wednesday, *Security Focus*, 29 Μαρτίου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/11>> [12 Σεπτεμβρίου 2008].

<sup>120</sup> Poulsen, K 2003, 'Adrian Lamo charged with computer crimes', *Security Focus*. 9 Μαΐου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/6888>> [12 Σεπτεμβρίου 2008].

<sup>121</sup> Weiser, B 2003, 'Computer use limited for accused hacker free on bond', *The New York Times*, 13 Σεπτεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9804E6D7113BF930A2575AC0A9659C8B63>> [12 Σεπτεμβρίου 2008].



Αυτό που έκανε ο Lamo ήταν να ανακαλύπτει τα σφάλματα στην ασφάλεια λειτουργικών συστημάτων διαφόρων εταιρειών και να τους ενημερώνει έπειτα για την ανεπάρκειά τους. Η «διάρρηξή» του στους New York Times, ωστόσο, αποκαλύφθηκε και, πέραν των περιοριστικών μέτρων, τιμωρήθηκε με τη χρηματική ποινή των 65.000 δολαρίων ως αποζημίωση. Σήμερα ο Lamo εργάζεται ως βραβευμένος δημοσιογράφος και δημόσιος ομιλητής<sup>122</sup>.

### 2.13 Stephen Wozniak

Ο Stephen Wozniak είναι ο άνθρωπος που κρύβεται πίσω από την δημιουργία του πρώτου MAC, είναι αυτός που έκανε τον υπολογιστή, είναι ο μηχανικός, είναι ο σχεδιαστής, είναι η μεγαλοφυΐα. Ο Stephen Wozniak είναι διάσημος ως ο άλλος Steve της Apple<sup>123</sup>.

Ο Stephen Wozniak μαζί με τον φίλο του Steve Jobs ίδρυσαν το 1977 την κορυφαία εταιρεία υπολογιστών την Apple Computer Corporation. Φέρνουν την επανάσταση, αφού καταφέρνουν με τη δημιουργία των πρώτων υπολογιστών Apple και στη συνέχεια του θρυλικού Mac να κάνουν προσιτή και αποδεκτή τη νέα τεχνολογία στην αγορά και στις επιχειρήσεις<sup>124</sup>. Το τρομερό εμπορικό δαιμόνιο αλλά και το επικοινωνιακό χάρισμα που διέθετε ο Jobs σε συνδυασμό με την ιδιοφυΐα και τις απίστευτες ικανότητες του Wozniak οδηγούν την Apple στην κορυφή και τους δύο φίλους στη λίστα των πολυεκατομμυριούχων προτού καν συμπληρώσουν τα 30 τους χρόνια. Ο Wozniak έχει βραβευθεί με το Εθνικό Μετάλλιο Τεχνολογίας και διάφορα διδακτορικά πανεπιστημίων, ενώ το 2000 καταχωρήθηκε στο Hall of Fame των Εθνικών Εφευρετών<sup>125</sup>.

Τον Wozniak από πολύ μικρό τον ενδιέφερε πολύ η ενασχόληση με τη δημιουργία ηλεκτρονικών μηχανών και συσκευών παντός είδους. Όλη την ημέρα την περνούσε παρέα με τα εργαλεία και τα ηλεκτρονικά του κυκλώματα. Δεν τον ενδιέφερε καν να εκμεταλλευτεί τις ικανότητές του και αυτά που έφτιαχνε. Τον

---

<sup>122</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο : Google Books Search [12 Σεπτεμβρίου 2008].

<sup>123</sup> Thompson, N 2004, 'For hackers, shop talk, a warning and advice', *The New York Time*, 12 Ιουλίου. Διαθέσιμο στο: <<http://www.nytimes.com/2004/07/12/technology/12hack.html?ex=1231995600&en=dbbcaeb039042d20&ei=5070>> [15 Σεπτεμβρίου 2008].

<sup>124</sup> Λαϊνάς Θ 2000, 'Οι θεοί της τεχνολογίας'. *To Βήμαonline*, 16 Ιουλίου. Διαθέσιμο στο: <[http://www.tovima.gr/print\\_article.php?e=B&f=12993&m=C09&aa=1](http://www.tovima.gr/print_article.php?e=B&f=12993&m=C09&aa=1)> [15 Σεπτεμβρίου 2008].

<sup>125</sup> Markoff, J 2003, 'Technology; Apple co-founder creates electronic ID tags', *The New York Times*, 21 Ιουλίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9507E0DC1F3CF932A15754C0A9659C8B63&scp=3&sq=Stephen%20Wozniak%20apple&st=cse>> [15 Σεπτεμβρίου 2008].

ικανοποιούσε από μόνη της η πρόκληση για τη δημιουργία και την εξέλιξη και μεγαλύτερη πληρωμή από την επιτυχία της κάθε προσπάθειάς του δεν μπορούσε να φανταστεί. Ξεκίνησε ως hacker τηλεφωνικών υποκλοπών δημιουργώντας μαζί με τον φίλο του τα λεγόμενα μπλε κουτιά (blue box) που χάρη στην έρευνά τους στις συχνότητες, τους βοηθούσαν να κάνουν υπερατλαντικά τηλεφωνήματα στον οποιονδήποτε –π.χ. με ένα μπλε κουτί (blue box) κάλεσε και τον Πάπα, προσποιούμενος πως ήταν ο Henry Kissinger<sup>126</sup>.

Όταν παράτησε το κολέγιο, είχε τη φαινή ιδέα, μαζί με τον Jobs, να κατασκευάζει ολοκληρωμένους υπολογιστές με ενσωματωμένα λειτουργικά συστήματα. Ιδρύουν, στο γκαράζ των γονιών του Steve Jobs στην Καλιφόρνια, την εταιρία Apple. Σε λίγες εβδομάδες κατασκευάζουν και παρουσιάζουν στο Homebrew Computer Club του Palo Alto τον υπολογιστή Apple I, ο πρώτος πραγματικά ολοκληρωμένος προσωπικός υπολογιστής αποτελούμενος από έναν κεντρικό επεξεργαστή, πληκτρολόγιο και έγχρωμη οθόνη, ο οποίος σύντομα βγαίνει στην αγορά στην τιμή των 666,66 δολαρίων και γνώρισε τεράστια εμπορική επιτυχία. Ένα χρόνο αργότερα κατασκευάζουν τον Apple II. Χρήση της τηλεοπτικής συσκευής ως οθόνη, χρωματιστά γραφικά και προγράμματα που αποθηκεύονται και «τρέχουν» με τη βοήθεια ενός κοινού κασετόφωνου είναι τα χαρακτηριστικά που κάνουν τον Apple II να αξίζει τα 1.298 δολάρια που κοστίζει<sup>127</sup>.

Ο Wozniak το 1985 εγκατέλειψε την Apple, σταμάτησε κάθε επιχειρηματική δραστηριότητα και άρχισε να ασχολείται με φιλανθρωπίες και δωρεές σχετικές φυσικά με το αντικείμενό του. Αφιερώνει τον χρόνο του σε φιλανθρωπίες, προσφέροντας κυρίως τη γνώση του πάνω στους υπολογιστές σε υποβιβασμένα σχολεία της Αμερικής. Ο πατέρας του Apple II επικεντρώνει τώρα την ενέργειά του βοηθώντας παιδιά να μάθουν τους υπολογιστές. «...πιστεύω ολοένα και περισσότερο ότι θα πρέπει να υποστηρίξουμε τους ανθρώπους που δεν είναι ειδικοί στους υπολογιστές». Όχι μόνο ξοδεύει εκατοντάδες ώρες διδάσκοντας αλλά επίσης πληρώνει ο ίδιος προσωπικά το κόστος της America Online για περίπου 100 παιδιά.<sup>128</sup> «...το χειρότερο πρόβλημα δεν είναι οι μαθητές, αλλά οι καθηγητές που

<sup>126</sup> Arlene, H 2001, 'A dramaturgical analysis of charismatic leader discourse', *Journal of Organizational Change Management*, vol. 14, no 3, pp. 253-265. Διαθέσιμο στο: Emerald [15 Σεπτεμβρίου].

<sup>127</sup> Donald, B 2006, *Steve Jobs, Steve Wozniak and the personal computer*, Capstone Press, New York.

<sup>128</sup> Krauss, A 2001, 'Technology briefing', *The New York Times*, 5 Δεκεμβρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2001/12/05/technology/05TBRF.html?ex=1232686800&en=b7fa92486de87109&ei=5070>> [15 Σεπτεμβρίου 2008].

πραγματικά χρειάζονται εκπαίδευση. Αυτό κοστίζει. Οι επικεφαλής του σχολείου θα πρέπει να κάτσουν και να βάλουν σε μια σειρά το τι πρέπει να διδαχθεί»<sup>129</sup>.

Ο Wozniak βρίσκεται για χρόνια σε μια ιδιόμορφη σχέση με την εταιρεία που ίδρυσε. Μια σχέση αγάπης αλλά και συνεχούς παραγωγικής κριτικής. Σε μια πρόσφατη συνέντευξή του σε ένα φοιτητή του Πανεπιστημίου του Stanford, ο Wozniak δεν φείδεται εκδηλώσεων αγάπης προς την Apple αλλά ούτε κριτικής. Ιδιαίτερα όταν μιλάει για το λογισμικό επισημαίνει στοιχεία που όχι μόνο τα έχουν ξεχάσει μεγαθήρια όπως η Microsoft, αλλά που τείνει να τα χάσει και η αγαπημένη του Apple. Σε ετέρα συνέντευξη του, ο ιδρυτής της Apple, δήλωσε ότι οι hackers δεν μπορούν να θεωρούνται «τρομοκράτες» και να επιπλήττονται με σοβαρές ποινές. Άλλωστε, αυτοί οι άνθρωποι κρύβονται πίσω από τόσες τεχνολογίες που έχουν αναπτυχθεί<sup>130</sup>.

#### 2.14 Tim Berners-Lee

Γεννήθηκε στις 8 Ιουνίου 1955 στο Λονδίνο. Ο Berners-Lee, γνωστός ως ο δημιουργός του Παγκόσμιου Ιστού (World Wide Web), αποφοίτησε από το Queen's College του Πανεπιστημίου της Οξφόρδης το 1976. Κατά τη διάρκεια της φοίτησής του εκεί κατασκεύασε μόνος του τον πρώτο του υπολογιστή με ένα ηλεκτρικό κολλητήριο, πύλες λογικής (TTL gates), έναν M6800 επεξεργαστή και μια παλιά τηλεόραση. Στο Πανεπιστήμιο της Οξφόρδης, όπου σπούδασε Φυσική, πιάστηκε στα πράσα να κάνει hacking με συνέπεια να αποκλειστεί από τη χρήση του πανεπιστημιακού υπολογιστή. Έχει δεχθεί αναρίθμητες βραβεύσεις με αποκορύφωμα το Millenium Technology Prize<sup>131</sup>.

Εργάστηκε σε επιχειρήσεις σύγχρονης τεχνολογίας και τηλεπικοινωνιών ως προγραμματιστής και σύμβουλος. Το 1980 άρχισε τη συνεργασία του με το περίφημο CERN ως σύμβουλος Μηχανικός Προγραμματισμού. Εκεί επινόησε και το πρόγραμμα Enquire, τον πρόδρομο του Παγκόσμιου Ιστού, που αφορούσε την αποθήκευση πληροφοριών και τον βοηθούσε να παρακολουθεί τον τεράστιο αριθμό

---

<sup>129</sup> Biersdorfer, J D 2006, 'Desktop icon', *The New York Times*, 1 Οκτωβρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2006/10/01/books/review/Biersdorfer.t.html?scp=1&sq=Stephen%20Wozniak%20hacker%201985&st=cse>> [16 Σεπτεμβρίου 2008].

<sup>130</sup> *An evening with Steve Wozniak* 2006, (video recording). Διαθέσιμο στο: <<http://video.google.com/videosearch?q=Steve+Wozniak+&emb=0#>> [16 Σεπτεμβρίου 2008].

<sup>131</sup> Shannon, V 2004, 'Pioneer who kept the web free honored with a technology prize', *The New York Times*, 14 Ιουνίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9801EED61330F937A25755C0A9629C8B63&scp=1&sq=Tim%20Berners-Lee%20Millenium%20Technology%20Prize&st=cse>> [16 Σεπτεμβρίου 2008].

ερευνητών και προγραμμάτων. Αυτό το πρόγραμμα ποτέ δε δόθηκε για χρήση στο κοινό, δεν κυκλοφόρησε ποτέ εκτός του γραφείου του Lee. Ολοκλήρωσε την πρώτη μορφή διαδικτύωσης (server—client / διακομιστή—πελάτη) σε παγκόσμιο επίπεδο, τον μετέπειτα Παγκόσμιο Ιστό<sup>132</sup>.

Η δημιουργία του προγράμματος ξεκίνησε το φθινόπωρο του 1990 και το καλοκαίρι του 1991 δόθηκε από το CERN προς γενική χρήση στο Διαδίκτυο. Ο Lee ως το 1993 συνέχισε να εργάζεται πάνω στη βελτίωση του προγράμματος με τη βοήθεια των παρατηρήσεων και των προτάσεων που ζητούσε να του κάνουν διάφοροι χρήστες του Διαδικτύου. Η επόμενη κίνησή του ήταν να δημιουργήσει τον ορισμό και την καθιέρωση των τεχνολογιών URL (Uniform Resource Locator – Ομοιόμορφος Εντοπιστής Πόρων), HTTP (HyperText Transmission Protocol – Πρωτόκολλο Μεταφοράς Υπερκειμένου) και HTML (Hypertext Markup Language – Γλώσσα Σήμανσης Υπερκειμένου).

Αν και εφευρέτης του Παγκόσμιου Ιστού, δηλώνει πως η δημιουργία του WWW, που προέκυψε ενώ εργαζόταν σε ένα ευρωπαϊκό πυρηνικό ερευνητικό πρόγραμμα ήταν για αυτόν παιχνίδι. Το μόνο που είχε να κάνει ήταν να φτιάξει ένα πρωτότυπο σύστημα υπερκειμένου που θα βοηθά τους ερευνητές να μοιράζονται και να ανανεώνουν πληροφορίες με ευκολία.

Από το 1994 συνεργάζεται με το MIT ως κάτοχος της έδρας 3Com στο CSAIL (Computer Science & Artificial Intelligence Laboratory – Εργαστήριο Πληροφορικής και Τεχνητής Νοημοσύνης) του MIT, ενώ είναι επίτιμος καθηγητής στο Πανεπιστήμιο του Southampton στο School of Electronics από το 2004. Επίσης είναι διευθυντής του World Wide Web Consortium (Επιτροπή Ελέγχου & Εξέλιξης του Κυβερνοχώρου), η οποία επιτηρεί τη συνεχή ανάπτυξή του. Είναι, επίσης, συνδιευθυντής του φορέα Web Science Research Initiative (WSRI – Πρωτοβουλία Επιστημονικής Έρευνας στον Ιστό) που δημιουργήθηκε το 2006.

Έχει πολλές τιμητικές διακρίσεις, μεταξύ πολλών άλλων και Ιππότης της Βρετανικής Αυτοκρατορίας (2004) από την Βασίλισσα της Αγγλίας και παράσημο Order of Merit από την ίδια το 2007. Έχει πάρει πολλά βραβεία ευρεσιτεχνίας και

---

<sup>132</sup> Lewis, P 1994, 'Companies rush to set up shop in cyberspace', *The New York Times*, 2 Νοεμβρίου. Διαθέσιμο στο: <http://query.nytimes.com/gst/fullpage.html?res=9A04EEDF163EF931A35752C1A962958260&sec=&spon=&scp=5&sq=Tim%20Berners-Lee%20biography&st=cse> [16 Σεπτεμβρίου 2008].

επιστήμης, ενώ έχει γράψει και ένα βιβλίο σχετικά με το παρελθόν και το μέλλον του κυβερνοχώρου με τίτλο “Weaving the Web”<sup>133</sup>.

Το περιοδικό Time τον κατέταξε ανάμεσα σε ένα από τα 100 λαμπρότερα πνεύματα του αιώνα<sup>134</sup>. Η επινόηση του Tim Berners-Lee μεταμόρφωσε τον κόσμο, αφού άλλαξε τα στάνταρ όχι μόνο στην ανταλλαγή πληροφοριών, αλλά και σε θέματα της καθημερινότητας, όπως διακίνηση και εμπόριο αγαθών, εκπαίδευση, ταξίδια, ενημέρωση, χρηματοοικονομικές συναλλαγές. Είναι αυτή που πραγματικά άνοιξε το Διαδίκτυο σε πολύ ευρεία μάζα χρηστών σε ολόκληρο τον πλανήτη. Στόχος του Berners-Lee είναι να καταφέρει να κρατήσει ουδέτερο το Διαδίκτυο. Όπως είπε χαρακτηριστικά ο ίδιος «...το θέμα δεν είναι από πού θα πληροφορηθώ για το τι παπούτσια θα αγοράσω. Το θέμα είναι πώς θα επιλέξω ενημέρωση για την ψήφο μου στις εκλογές, πώς θα διαλέξω πιστεύω, πώς θα αποφασίσω αν ανήκω κάπου ή όχι, το πώς θα αποφασίσω αν κάτι ανήκει στην σφαίρα της επιστημονικής αλήθειας. Το θέμα είναι τι ισχύει πραγματικά και τι είναι απλώς ανοησίες».<sup>135</sup>

## 2.15 Linus Benedict Torvalds

Ο Linus Benedict Torvalds γεννήθηκε στις 28 Δεκεμβρίου του 1969 στο Ελσίνκι της Φινλανδίας. Ο Φιλανδός επιστήμονας ηλεκτρονικών υπολογιστών έγινε γνωστός για την δημιουργία του Linux (λειτουργικό σύστημα ανοικτού κώδικα). Αποκαλεί τον εαυτό του «μηχανικό» λέγοντας «...θέλω μόνο να περνάω καλά και να δημιουργώ όσο το δυνατό καλύτερα λειτουργικά συστήματα»<sup>136</sup>.

Το 1991 Linus Torvalds εφευρίσκει τον λειτουργικό πυρήνα αυτού που αργότερα εξελίχθηκε στο Linux. Το 1992 ο Torvalds εκδίδει το Linux υπό την άδεια χρήσης GPL (General Public License – Γενική Άδεια Δημόσιας Χρήσης). Το Linux είναι ένα λειτουργικό σύστημα που βασίζεται στο σύστημα Unix<sup>137</sup>. Το λειτουργικό που

---

<sup>133</sup> Λαϊνός Θ 2000, ‘Οι θεοί της τεχνολογίας’, *To Βήμαonline*, 16 Ιουλίου. Διαθέσιμο στο: <[http://www.tovima.gr/print\\_article.php?e=B&f=12993&m=C09&aa=.1](http://www.tovima.gr/print_article.php?e=B&f=12993&m=C09&aa=.1)> [16 Σεπτεμβρίου 2008].

<sup>134</sup> Quittner, J 1999, ‘Tim Berners-Lee: from the thousands of interconnected threads of the Internet, he wove the World Wide Web and created a mass medium for the 21st century’, *Time*, 29 Μαρτίου. Διαθέσιμο στο: <<http://www.time.com/time/time100/scientist/profile/bernerslee.html>> [17 Σεπτεμβρίου 2008].

<sup>135</sup> Berners, L.T. 1999, *Weaving the Web*, Harper, San Francisco.

<sup>136</sup> Hafner, K 1998, ‘Mac, windows and now, linux’, *The New York Times*, 8 Οκτωβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=950CE3DB143BF93BA35753C1A96E958260&n=Top/Reference/Times%20Topics/People/H/Hafner,%20Katie&scp=1&sq=Linus%20Torvalds%20engineering&st=cse>> [18 Σεπτεμβρίου 2008].

<sup>137</sup> Ghosh, R A 1998, ‘Interviews with Linus Torvalds: what motivates free software developers?’, *First Monday Journal*, vol. 3, no 3. Διαθέσιμο στο:

δημιούργησε είναι μια σύμπραξη, καθώς ζήτησε και τη βοήθεια των άλλων συμφοιτητών του στο Πανεπιστήμιο που σπούδαζε. Προσπάθησε να φέρει την επανάσταση στον χώρο του λογισμικού σπάζοντας την παντοκρατορία των Windows και δημιουργώντας ένα νέο λειτουργικό σύστημα, το Linux, που σε αντίθεση με τον «αντίπαλό» (windows) του βασιζόταν στη λογική του ανοικτού κώδικα. Αυτό σήμαινε ότι όποιος ήθελε μπορούσε να επέμβει και να διαμορφώσει ή και να εξελίξει το πρόγραμμα όπως εκείνος επιθυμούσε. Ο Linus Torvalds αποδέχεται τις συμπληρώσεις και τροποποιήσεις του πυρήνα από τον καθένα. Κάτι τέτοιο θα αποτελούσε αφορμή για αναρχία αλλά ασκείται αυστηρός έλεγχος της. Η θεωρία του Torvalds ήταν να δημιουργήσει ένα λειτουργικό σύστημα στο οποίο θα μπορούσε να παρέμβει ο κάθε χρήστης και προγραμματιστής και να επεκτείνει τις δυνατότητές του. Ήταν τότε που τέθηκε η θεωρία του λογισμικού ανοικτού κώδικα. Εκατομμύρια απλοί χρήστες αλλά και πολλές εταιρίες ήδη ασχολούνται με το Linux προσπαθώντας να το προωθήσουν και να το εξελίσσουν έτσι ώστε να γίνει ένας ικανός ανταγωνιστής των Windows. Η ονομασία του, Linux, είναι ένα όνομα που συνδυάζει το όνομα του δημιουργού και το σύστημα Unix. Ένα νέο σύστημα είχε δημιουργηθεί για να ανταχθεί στα Windows της Microsoft, με τη διαφορά ότι ήταν ένα σύστημα δημιουργημένο από την αγάπη για τη διάδοση της πληροφορικής, από φοιτητές που αγαπούσαν αυτό που έκαναν χωρίς να έχουν ως σκοπό το κέρδος<sup>138</sup>.

Ο Linus Torvalds στη συνέχεια κλείστηκε στα εργαστήρια της εταιρίας Transmeta συμμετέχοντας στη δημιουργία ενός ακόμη επαναστατικού προϊόντος, του επεξεργαστή Crusoe, ο οποίος, σύμφωνα με τους δημιουργούς του, θα αλλάξει τον κόσμο των μικροεπεξεργαστών αφού θα κοστίζει λιγότερο από τους «κλασικούς», θα έχει μικρότερη κατανάλωση ενέργειας και θα προσφέρει καλύτερες υπηρεσίες<sup>139</sup>.

Σήμερα ο Linus Torvalds παραμένει ο αρχηγός της Linux, συντάσσοντας τον ομώνυμο κώδικα στον πυρήνα του οποίου συνεισφέρουν εθελοντές προγραμματιστές. Έχει δώσει το όνομά του σε έναν αστεροειδή και έχει λάβει τιμητικά διδακτορικά διπλώματα για την προσφορά του στην τεχνολογία. Αποτελεί, άλλωστε και χαρακτηριστική φυσιογνωμία στο άρθρο του περιοδικού Time «60 Years of Heroes».

---

<<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/583/504>> [15 Σεπτεμβρίου 2008].

<sup>138</sup> Rusling DA 1998, *The Linux kernel*. Διαθέσιμο στο: <[http://kos.enix.org/pub/linux\\_kernel.pdf](http://kos.enix.org/pub/linux_kernel.pdf)> [17 Σεπτεμβρίου 2008].

<sup>139</sup> Schoolman, J 2000, 'Computer chip maker set for powerful IPO', *NY Daily News*, 7 Νοεμβρίου. Διαθέσιμο στο: <[http://www.nydailynews.com/archives/money/2000/11/07/2000-11-07\\_computer\\_chip\\_maker\\_set\\_for\\_.html](http://www.nydailynews.com/archives/money/2000/11/07/2000-11-07_computer_chip_maker_set_for_.html)> [20 Σεπτεμβρίου 2008].

Προσωπική ιστοσελίδα <<http://www.cs.helsinki.fi/u/torvalds>>.

## 2.16 Richard Stallman

Ο Richard Matthew Stallman (RMS) γεννήθηκε στις 16 Μαρτίου 1953 στο Μανχάταν της Νέας Υόρκης. Είναι ο ιδρυτής του κινήματος ελεύθερου λογισμικού, του εγχειρήματος GNU, του Free Software Foundation (FSF – Ίδρυμα Ελεύθερου Λογισμικού), και της League for Programming Freedom (LPF -- Ένωση για την Ελευθερία του Προγραμματισμού). Εφηύρε την έννοια του “copyleft” για να προστατεύσει τα ιδανικά αυτού του κινήματος, και διαφύλαξε αυτή την έννοια στην ευρέως χρησιμοποιούμενη GPL (General Public License) για το λογισμικό<sup>140</sup>.

Ήρθε για πρώτη φορά σε επαφή με ηλεκτρονικό υπολογιστή κατά τη διάρκεια του τελευταίου έτους του γυμνασίου, το 1969. Μετά την αποφοίτησή του, εργάστηκε για λογαριασμό της IBM, πάνω στη δημιουργία ενός προεπεξεργαστή για την γλώσσα προγραμματισμού PL/I. Παράλληλα, υπήρξε εθελοντής βοηθός εργαστηρίου, στο τμήμα Βιολογίας του Πανεπιστημίου Rockefeller. Άνηκε στην γενιά των πρώτων hackers, που έμαθαν hacking στα τεράστια IBM μηχανήματα στα πανεπιστήμια<sup>141</sup>.

Τον Ιούνιο του 1971, ως πρωτοετής φοιτητής του Πανεπιστημίου Χάρβαρντ, ξεκίνησε να εργάζεται ως προγραμματιστής στο MIT, αποτελώντας κεντρική φυσιογνωμία στην κοινότητα των hackers. Την ίδια εποχή, σε μια επίσκεψη στο Εργαστήριο Τεχνητής Νοημοσύνης του Πανεπιστημίου Stanford εντυπωσιάστηκε από τον επεξεργαστή κειμένου "E", κάτι που είχε σαν αποτέλεσμα να ξεκινήσει την ανάπτυξη του επεξεργαστή κειμένου GNU Emacs, ο οποίος αναπτύσσεται συνεχώς από τότε και παραμένει ακόμα πολύ δημοφιλής ανάμεσα στους προγραμματιστές<sup>142</sup>.

Το 1974, αποφοίτησε από το Χάρβαρντ με βασικό πτυχίο στη Φυσική και συνέχισε τις μεταπτυχιακές του σπουδές στο Εργαστήριο Τεχνητής Νοημοσύνης του MIT. Όταν η ομάδα των hackers στο MIT διαλύθηκε, ο Stallman συνέχισε να αναπτύσσει την γλώσσα LISP, στην οποία ήταν γραμμένος ο Emacs, γράφοντας

---

<sup>140</sup> Rothstein, E 2004, ‘Connections; liberty, technology, duty: where peace overlaps war’, *The New York Times*, 8 Μαΐου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9C05E2D8173CF93BA35756C0A9629C8B63&sc=&spn=&scp=9&sq=Richard%20Stallman%20hacker&st=cse>>. [27 Σεπτεμβρίου 2008].

<sup>141</sup> Wusteman, J 2004, ‘Patently ridiculous’, *Library Hi Tech*, vol. 22, no. 2, pp. 231–237. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

<sup>142</sup> Wusteman, J 2004, ‘Patently ridiculous’, *Library Hi Tech*, vol. 22, no. 2, pp. 231–237. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

λογισμικό για την εταιρία Lisp Machines Inc., τελευταίο προπύργιο των hackers, βοηθώντας την στον ανταγωνισμό της με την αντίπαλη Symbolics<sup>143</sup>.

Ο Stallman είχε μάθει στο υπολογιστικό κέντρο του MIT ότι ένας αναρχικός οργανισμός ήταν εφικτός. Αλλά υπήρχε έλλειψη μαχητών λόγω της αποκέντρωσης των hackers χάρη στο σπιτικό υπολογιστή. Στην αρχή της δεκαετίας του 1980 ο Stallman αισθανόταν ως ο τελευταίος υποστηρικτής ενός νεκρού κινήματος με αναρχικές αρχές. Αυτό το κίνημα ήθελε να αναζωογονήσει. Με το κίνημα ελεύθερου λογισμικού η hacker κουλτούρα αναγεννήθηκε και ο Stallman άρχισε να ελευθερώνει τον πηγαίο κώδικα από ιδιόκτητες άδειες<sup>144</sup>.

Το 1984 ο Stallman πήρε την πολιτική απόφαση να ξεκινήσει τη δημιουργία ενός ελεύθερου λειτουργικού συστήματος, που ο καθένας θα μπορούσε να χρησιμοποιήσει, να τροποποιήσει και να αναδιανείμει ελεύθερα. Έτσι ίδρυσε το Project GNU και ξεκίνησε τη δημιουργία του ελεύθερου λειτουργικού συστήματος GNU, το οποίο θα ήταν συμβατό με το UNIX. Το 1985 ο Stallman δημοσιεύει το GNU Μανιφέστο, στο οποίο διακηρύττει την πρόθεσή του να εκδώσει το GNU ως ελεύθερο λογισμικό και ιδρύει το Free Software Foundation<sup>145</sup>. Απασχολείται με την προώθηση του ελεύθερου λογισμικού και κατά των ευρεσιτεχνιών λογισμικού και επέκτασης του νόμου για τα πνευματικά δικαιώματα στο λογισμικό.

Ταυτόχρονα με αυτές τις εξελίξεις διαμορφωνόταν μέσα στις κοινότητες των hackers η ιδέα του copyleft, ως αντιστροφή και αναποδογύρισμα των κανόνων του copyright. Το copyleft είναι ο όρος που περιγράφει κάθε άδεια χρήσης πνευματικού έργου, με την οποία ο δημιουργός επιτρέπει την ελεύθερη χρήση, αναπαραγωγή, τροποποίηση και βελτίωση του έργου, υπό τον όρο ότι κάθε νέα τροποποιημένη/βελτιωμένη έκδοση αυτού θα εκδίδεται με την ίδια άδεια. Η ιδέα του copyleft αποτέλεσε το νομικό όχημα πάνω στο οποίο χτίστηκε όλο το κίνημα του ελεύθερου λογισμικού και κατέστη δυνατή η απελευθέρωση της δημιουργίας από τα δεσμά της ιδιοκτησίας και το συνεργατικό χτίσιμο τεράστιων συγκεντρώσεων κώδικα από τις κοινότητες<sup>146</sup>.

---

<sup>143</sup> Mateas, M 2005, 'Procedural literacy: educating the new media practitioner', *On the Horizon*, vol. 3, no. 2, pp. 101–111, Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

<sup>144</sup> Elliot, M S & Scacchi, M 2008, 'Mobilization of software developers: the free software movement', *Information Technology & People*, vol. 21, no. 1, pp. 4–33. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

<sup>145</sup> Bynum, T W & Rogerson, S 2004, *Computer ethics and professional responsibility*, Blackwell, New York.

<sup>146</sup> Wusteman, J. 2004, 'Patently ridiculous', *Library Hi Tech*, vol. 22, no. 2, pp. 231–237. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].



Το 1989 ο Stallman συγγράφει την πιο σημαντική copyleft άδεια, την General Public Licence (GPL), η οποία εκτός των άλλων υποχρεώνει τους δημιουργούς να δημοσιεύουν τον πηγαίο κώδικα των λογισμικών τους, απαραίτητο στοιχείο για να είναι δυνατή η τροποποίησή του από τρίτους. Πολύ γρήγορα στο κομμάτι της διαμόρφωσης της άδειας, νομικής κατοχύρωσης και νομικής προστασίας στα δικαστήρια του κινήματος εμπλέκεται ο Eben Moglen, καθηγητής Ιστορίας του Δικαίου στο Πανεπιστήμιο Columbia. Σήμερα υπολογίζεται ότι 70% των έργων ελεύθερου λογισμικού έχουν εκδοθεί υπό την GPL<sup>147</sup>.

Στις αρχές του 1990, μαζί με άλλα μέλη της κοινότητας GNU, συμμετείχε στην προσπάθεια δημιουργίας του GNU Hurd, του λειτουργικού συστήματος που είχε περιγραφεί στο GNU Μανιφέστο<sup>148</sup>. Αν και η ανάπτυξη του GNU Hurd προχώρησε με γρήγορα βήματα στην αρχή, στη συνέχεια τελματώθηκε καθώς ο μικροπυρήνας που επιλέχτηκε, ο Mach, παρουσίασε προβλήματα τα οποία ακόμη δεν έχουν λυθεί εντελώς. Η επιλογή του Mach ήταν προσωπική απόφαση του Stallman, την οποία αργότερα χαρακτήρισε λαθεμένη. Τώρα πια ζει γυρνώντας όλον τον κόσμο ως καλεσμένος σε ομιλίες και διαλέξεις σε πανεπιστήμια, συνέδρια και ιδρύματα.

## 2.17 Tsutomu Shimomura

Ο Tsutomu Shimomura γεννήθηκε στην Ιαπωνία το 1964. Είναι ένας επιστήμονας, ειδικός ασφαλείας υπολογιστών, με έδρα τις Ηνωμένες Πολιτείες. Πατέρας του είναι ο Osamu Shimomura νικητής του Νόμπελ χημείας το 2008. Μεγάλωσε στο Princeton του New Jersey και πήγε σχολείο στο Princeton High School. Αργότερα εργάστηκε στο Εθνικό Εργαστήριο Los Alamos, όπου συνέχισε την πρακτική τους εκπαίδευση στη θέση του φυσικού μαζί με τον Brosl Hasslacher. Το 1987 γίνεται ερευνητής στο Τμήμα Φυσικής του Πανεπιστημίου της Καλιφόρνια στο Σαν Ντιέγκο, και ανώτερος ερευνητής στο San Diego Supercomputer Center. Το 1992 έκανε διάλεξη στο Αμερικανικό Κογκρέσο και μίλησε για προβλήματα που

---

<sup>147</sup> Jones, R & Andrew, T 2005, 'Open access, open source and e-theses: the development of the Edinburgh Research Archive', *Program: Electronic Library and Information Systems*, vol. 39, no. 3, pp. 198–212. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

<sup>148</sup> Elliot, M S & Scacchi, M 2008, 'Mobilization of software developers: the free software movement', *Information Technology & People*, vol. 21, no. 1, pp. 4–33. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

υπήρχαν στην ιδιωτική χρήση και ασφάλεια των κινητών τηλεφώνων και εργάστηκε για την Sun Microsystems κατά το τέλος της δεκαετίας του 1990<sup>149</sup>.

Ανήμερα Χριστουγέννων του 1994 δέχεται επίθεση από τον Kevin Mitnick και από τη στιγμή αυτή γίνεται διάσημος. Ο Kevin Mitnick υπέκλεψε το ηλεκτρονικό ταχυδρομείο του Shimomura και άλλα προσωπικά αρχεία. Μετά από αυτή την προσωπική επίθεση έκανε στόχο ζωής να βοηθήσει το FBI να τον συλλάβει. Το κατάφερε υποκλέπτοντας κατά κάποιο τρόπο τα τηλεφωνήματά του με βοήθεια του FBI. Χρησιμοποίησε για αυτό μία κυτταρική συχνότητα και μία κεραία ενός laptop πού τον οδήγησε στο να εντοπίσει το διαμέρισμα από το οποίο δρούσε ο Mitnick. Μετά το «κυνηγητό» ο Shimomura και δημοσιογράφος John Markoff έγραψαν το βιβλίο με τον τίτλο “Takedown”, το οποίο πραγματευόταν τη σύλληψη και τη φυλάκιση του Mitnick, το οποίο αργότερα γυρίστηκε σε ταινία.

Τώρα εργάζεται σαν καθηγητής στο Integrated Center for Educational Research University στο San Diego.

## 2.18 Raven Alder

Γεννήθηκε το 1976 στο Μισισιπή των Ηνωμένων Πολιτειών. Είναι σύμβουλος ασφάλειας, hacker και συγγραφέας. Είναι μια από λίγες γυναίκες hackers και γνωστή για DoS Attacks (Denial of Service Attacks)<sup>150</sup>.

Χαρακτηρίστηκε παιδί-θαύμα αφού στα 14 της μόλις χρόνια αποφοίτησε από το Λύκειο και τελείωσε το κολλέγιο στα 18. Η πρώτη φορά που ασχολήθηκε με ηλεκτρονικούς υπολογιστές ήταν το 1985<sup>151</sup>.

Η Raven Alder είναι ανώτερος μηχανικός ασφαλείας της IOActive, μιας εταιρίας συμβούλων που ειδικεύεται στην ασφάλεια των δικτύων, στο σχεδιασμό και την υλοποίηση. Είναι ειδικευμένη στην ασφάλεια των δικτύων και στους τρόπους ελέγχου για το LinuxChix.org, κρυπτογραφική και εντοπισμός τρωτών σημείων για την Open Source Vulnerability Database. Η Raven ζει στο Σιάτλ της Ουάσινγκτον. Είναι ένας από τους σημαντικότερους χρηματοδότες του Nessus Network Auditing. Έχει στο ιστορικό της βελτίωση πολύπλοκων συστημάτων. Είναι από τις λίγες

---

<sup>149</sup> Cranor, LF 2000, ‘Ten years of computers, freedom and privacy: a personal retrospective, computers, freedom and privacy’, *Proceedings of the tenth conference on computers, freedom and privacy*, pp. 11–15. Διαθέσιμο στο: <<http://www.cfp2000.org/papers/2cranor.pdf>> [28η Σεπτεμβρίου 2008].

<sup>150</sup> Πρόκειται για έναν τρόπο επίθεσης σε ένα δίκτυο με σκοπό να «ρίξει» το δίκτυο πλημμυρίζοντάς το με άχρηστη κίνηση.

<sup>151</sup> Long, J 2007, *Stealing the network: how to own a shadow*, Syngress, Cambera.

γυναίκες που μίλησαν ποτέ στα συνέδρια της DefCon, στα συνέδρια του Open Source (Linux World Expo) και αποτελεί μέλος της κοινότητας LinuxChix. Εργάστηκε ως ανώτερος αρχιτέκτονας της Senior Consultant στο IT Security ασφαλείας. Το ενδιαφέρον για την εξασφάλιση δικτύων από άκρο σε άκρο την οδήγησε να εξετάσει πρότυπα και έγινε πρωτοπόρος σε θέματα ασφαλείας των υποδομών δικτύου<sup>152</sup>.

Συνοψίζοντας όλες αυτές τις βιογραφίες παρατηρούμε ότι πολλοί μαύροι (black hat) hackers μετατρέπονται σε άσπρους (white hat) hackers. Μεταφέρονται από την εγκληματική πλευρά του hacking στην ηθική και χρησιμοποιούν τις ικανότητες τους για την προστασία των δικτύων και την παγκόσμια ασφάλεια. Οι περισσότεροι λευκοί hackers έχουν αμαυρωμένο παρελθόν. Φυσικά δεν είναι κανόνας ότι όλοι οι λευκοί hackers είναι πρώην μαύροι hackers. Πολλοί hackers ποτέ δεν ανακατεύτηκαν με την σκοτεινή πλευρά του hacking.

Οι λόγοι αυτής της μετάλλαξης είναι πολλοί. Αρχικά το χρήμα. Εκτός κάποιων εξαιρούμενων περιπτώσεων το να είναι κάποιος μαύρος hacker δεν έχει και πολλά έσοδα. Υπάρχουν βέβαια οι ιστορίες για hackers, οι οποίοι υπέκλεψαν μεγάλα χρηματικά ποσά από εταιρίες, πληρώθηκαν αδρά για να κλέψουν πληροφορίες, και άλλες πολλές ιστορίες. Όπως είδαμε αρκετές από αυτές είναι αλήθεια, αλήθεια όμως είναι ότι αργά ή γρήγορα τα άτομα αυτά συνελήφθησαν. Αυτές οι περιπτώσεις και τα περιστατικά σπανίζουν. Η πλειοψηφία των μαύρων hackers λειτουργεί με οικονομική ζημιά δεδομένου ότι ξοδεύουν πολλά χρήματα για την αγορά εξοπλισμού υλικού και τα έσοδα από το εγκληματικό (black hat) hacking συνήθως δεν είναι τόσο μεγάλα. Σε μακροπρόθεσμο επίπεδο, είναι πολύ καλύτερο να λειτουργεί κανείς ως λευκός hacker. Για παράδειγμα να εργάζεται ως σύμβουλος ασφαλείας για επιχειρήσεις και παίρνει ένα σταθερό και καλό εισόδημα κάθε εβδομάδα<sup>153</sup>.

Η εξάντληση και η κούραση είναι ένας ανασταλτικός παράγοντας για να συνεχίσει κάποιος να είναι στο στρατόπεδο των μαύρων hackers. Ζουν μια πολλή έντονη ζωή με τον φόβο ότι κάποια στιγμή θα αποκαλυφθούν και θα καταδικαστούν. Φυσικά μπροστά στη γνώση που αποκτούν από τις παράνομες δραστηριότητες τους δεν υπολογίζουν το νόμο, παρόλα αυτά μια απρόσμενη σύλληψη πάντα караδοκεί. Οι hackers είναι ευφυή άτομα δεν είναι εγκληματίες ούτε ψυχικά άρρωστοι. Μπορούν

---

<sup>152</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο : Google Books Search [28 Σεπτεμβρίου 2008].

<sup>153</sup> Edwards, J 2007, 'Why black-hat hackers become white-hat heroes', *Network Security Journal*, 11 Σεπτεμβρίου. Διαθέσιμο στο: <<http://www.networksecurityjournal.com/features/black-hats-become-white-hats-091107/>> [30 Σεπτεμβρίου 2008].

να καταλάβουν ότι αυτό που κάνουν είναι επικίνδυνο και σε μια πιο ώριμη ηλικία ίσως μετά από κάποιο πάθημα –π.χ. μια σύλληψη ή φυλάκιση— βρίσκουν τρόπο να κάνουν αυτό που τους αρέσει νόμιμα, δουλεύοντας ως λευκοί hackers<sup>154</sup>.

Πολλοί hackers προτιμούν να γραφτούν στην ιστορία του hacking ως λαμπροί επιστήμονες και «καλοί» hackers. Είναι προτιμότερο αυτός ο τίτλος από τον τίτλο του «κακού» hacker που εκμεταλλεύτηκε τις αδυναμίες ενός συστήματος για να γίνει γνωστός. Καλύτερα να αναγνωρίζεται κανείς για την προσφορά του στην παγκόσμια ηλεκτρονική ασφάλεια. Για παράδειγμα πολλοί hackers θαυμάζουν τη δόξα των Richard Stallman, Linus Torvalds, Tim Berners-Lee και πολλών άλλων γιγάντων στο χώρο των δικτύων και των υπολογιστών.

Πολλοί λίγοι είναι οι μαύροι hackers που είναι άνω των 30 ετών. Τα περισσότερα από τα άτομα που επιδίδονταν σε πράγματα όπως η δημιουργία κακόβουλου λογισμικού, η διείσδυση σε δίκτυα, η ανατίναξη servers, αργότερα στα χρόνια της ωριμότητας άλλαξαν τρόπο ζωής. Είναι παρόμοιο με το πόσο πιο βίαιοι και αντιδραστικοί είμαστε όταν βρισκόμαστε στην εφηβεία. Ίσως η ωριμότητα και η ηθική δράση να έχει σχέση με τα φθίνοντα επίπεδα τεστοστερόνης. Όσο μεγαλώνουμε τόσο λιγότερη τεστοστερόνη παράγουμε<sup>155</sup>.

Παρατηρείται ότι οι λευκοί hackers είναι πιο ευφυείς από τους αντιπρόσωπους του εγκληματικού hacking. Ο καθένας μπορεί να ρίξει μια πέτρα από το παράθυρο και να δημιουργήσει αναστάτωση, αλλά χρειάζεται ένας εξειδικευμένος εμπειρογνώμονας για να φτιάξει την ζημιά. Ίσως, αφού έμαθαν όλα αυτά από τις επιθέσεις τους και τις παράνομες διεισδύσεις, οι μαύροι hackers να είναι έτοιμοι να προχωρήσουν προς άλλους δρόμους πιο δημιουργικούς<sup>156</sup>.

Ο Richard Stallman αναφέρει σε μια συνέντευξη του ότι πολλοί μαύροι hackers μετατρέπονται σε μαχητές της ελευθερίας και αντιπρόσωποι του ακτιβισμού. Το 1983 όταν άρχισε η κίνηση ελεύθερου λογισμικού, πολλοί hackers τότε κατάλαβαν ότι το ελεύθερο λογισμικό είναι ο μόνος τρόπος να γίνει ελεύθερος ένας χρήστης

---

<sup>154</sup> Erickson, K & Howard, NP 2007, 'A case of mistaken identity?: news accounts of hacker, consumer, and organizational responsibility for compromised digital records' *Journal of Computer-Mediated Communication*, vol. 12, no. 4, pp. 1229–1247. Διαθέσιμο στο: Wiley Interscience [30 Σεπτεμβρίου 2008].

<sup>155</sup> Edwards, J 2007, 'Why black-hat hackers become white-hat heroes', *Network Security Journal*, 11 Σεπτεμβρίου. Διαθέσιμο στο: <<http://www.networksecurityjournal.com/features/black-hats-become-white-hats-091107/>> [30 Σεπτεμβρίου 2008].

<sup>156</sup> Ambrosek, R 2006, *Shawn fanning: the founder of Napster*, The Rosen Publishing Group, New York.

υπολογιστή. Βρήκαν έναν τρόπο να διοχετεύσουν την ενέργεια τους και την αντίδραση τους στο κατεστημένο<sup>157</sup>.

Οι αρχικοί hackers είχαν συνείδηση και ηθική. Αυτό το πνεύμα του hacking μπορεί να έχει φθαρεί με το πέρασμα του χρόνου, όμως ακόμα υπάρχει. Όποιος έχει έστω και λίγο ίχνος ηθικής τελικά θα απομακρυνθεί από το εγκληματικό (black hat) hacking. Ο hacker είναι άτομο που χτίζει, δεν καταστρέφει. Ίσως στην αρχή να είναι μαγεμένος από την δύναμη των ικανοτήτων του, αργότερα όμως δεν γοητεύεται από τα ηλεκτρονικά μακελειά. Αυτός που γοητεύεται από την καταστροφή είναι ο cracker.

---

<sup>157</sup> Harmon, A 2002, 'Technology: free software, at least to a certain point', *The New York Times*, 23 Σεπτεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9403E7DD1739F930A1575AC0A9649C8B63&scp=1&sq=Richard%20Stallman%20freedom%20fighter&st=cse>> [30 Σεπτεμβρίου 2008].

## ΚΕΦΑΛΑΙΟ 3: Η ΚΟΥΛΤΟΥΡΑ ΚΑΙ ΙΔΕΟΛΟΓΙΑ ΤΩΝ HACKERS

Στο προηγούμενο κεφάλαιο εξετάστηκε και αναλύθηκε ο ατομικός τύπος των hackers. Αυτό το κεφάλαιο είναι μια τομή στον πολιτισμό των hackers, επικεντρώνεται δηλαδή στην ανάλυση της συμπεριφοράς τους μέσα σε ομάδες και την προώθηση ιδεών και συμφερόντων. Τα κοινά νοήματα, τις σημασίες, τις αξίες, τις πρακτικές και τους θεσμούς αυτής κοινωνίας (των hacker). Θα αναφερθούν στοιχεία τις ιδεολογίας τους πάνω στα οποία έχει αναπτυχθεί ο πολιτισμός τους.

Βασική πηγή που μπορούμε να αντλήσουμε πληροφορίες είναι ένα πολύ γνωστό και δημοφιλές έγγραφο γνωστό ως « Το Μανιφέστο του hacker»<sup>158</sup>, το οποίο γράφτηκε το 1969 από ένα hacker με το ψευδώνυμο Μέντορας. Επίσης πολλά περιοδικά που εκδίδονται από την κοινότητα των hackers είναι πολύτιμες πηγές πληροφοριών, όπως το περιοδικό “Phrack Magazine”<sup>159</sup>, το “2600: the hacker quarterly”<sup>160</sup>, το “H Datenschleuder”<sup>161</sup> του Chaos Computer Club (CCC).

### 3.1 Κουλτούρα και πολιτισμός

Ο πολιτισμός των hackers είναι ένας φιλελεύθερος πολιτισμός που αντιστέκεται στον κυβερνητικό έλεγχο, το μυστικισμό και εναντιώνεται στους κολοσσούς του βρόμικου κέρδους που εκμεταλλεύονται το Διαδίκτυο. Σύμφωνα με το Μέντορα οι hackers δε βλέπουν τον εαυτό τους σαν εγκληματία αλλά σαν ένα σύγχρονο επαναστάτη. Λύνουν προβλήματα και χτίζουν πράγματα. Πιστεύουν στην ελευθερία και στην εθελοντική αμοιβαία βοήθεια. Η κουλτούρα των hackers βασίζεται σε δύο βασικά χαρακτηριστικά της ιδεολογία τους στην απόλαυση λύσης προβλημάτων και στη πεποίθηση τους ότι η ελευθερία είναι αγαθό. Οι hackers έχουν εκ φύσης τους ένα ενθουσιασμό στο να λύνουν προβλήματα, να δοκιμάζουν την ευφυΐα τους. Κινηγούν την γνώση και την πληροφορία. Θεωρούν ότι όλη η πληροφορία πρέπει να είναι ανοιχτή και να είναι προσβάσιμη από τον καθένα. Η πληροφορία για έναν hacker είναι κάποιο πρόγραμμα, ο κώδικας αυτού του προγράμματος, αλλά ακόμα και

---

<sup>158</sup> The Mentor 1986, ‘The conscience of a hacker’, *Phrack Magazine*, vol. 7, no. 3. Διαθέσιμο στο: <<http://www.phrack.org/issues.html?issue=7&id=3>> [2 Νοεμβρίου 2008].

<sup>159</sup> *Phrack Magazine* 2008, *Phrack Magazine*. Διαθέσιμο στο: <<http://www.phrack.org>> [4 Νοεμβρίου 2008].

<sup>160</sup> *2600: the hacker quarterly* 2008, *2600 Magazine*. Διαθέσιμο στο: <[www.2600.com](http://www.2600.com)> [4 Νοεμβρίου 2008].

<sup>161</sup> *Chaos Computer Club e.V* 2008, *Chaos Computer Club*. Διαθέσιμο στο: <<http://www.ccc.de>> [4 Νοεμβρίου 2008].

οποιοδήποτε αρχείο υπάρχει σε οποιονδήποτε υπολογιστή βρίσκεται συνδεδεμένος στο δίκτυο<sup>162</sup>.

Ο Douglas Thomas επισημαίνει ότι το hacking δεν ήταν ποτέ μια αποκλειστική τεχνική διαδικασία. Είναι ένα σύμπλεγμα πολιτικοοικονομικών και τεχνολογικών παραγόντων<sup>163</sup>.

Οι hackers λατρεύουν να λύνουν γρίφους και να χρησιμοποιούν την τεχνολογία με ένα τρόπο που δεν έχει ειπωθεί για το πως θα μπορούσε να χρησιμοποιηθεί. Απολαμβάνουν να σπάζουν τον κώδικα και να παίρνουν τον έλεγχο του λογισμικού και του υπολογιστή στα χέρια τους<sup>164</sup>. Λατρεύουν το έργο τους και ποτέ δεν θεωρούν μια εργασία που έχει σχέση με την τεχνολογία ως αγγαρεία ή βαρετή. Η κουλτούρα των hackers είναι μια μη οικονομικά δραστηριοποιούμενη κουλτούρα. Στον κόσμο του hacking μετράει η φήμη και η αναγνωρισιμότητα, οι ήδη καταξιωμένοι hackers θα κρίνουν το έργο σου. Για αυτό το λόγο δεν είσαι hacker μέχρι άλλοι hackers να σε καλέσουν έτσι. Συγκεκριμένα, ο κόσμος του hacking είναι αυτό που οι κοινωνιολόγοι ονομάζουν «κουλτούρα δώρων». Σύμφωνα με αυτή δεν γίνεται αναγνωρίσιμος με το να κατακτάς άλλους ανθρώπους, ούτε με το να είσαι όμορφος, ούτε με το να έχεις πράγματα που θέλουν οι άλλοι, αλλά με το να δίνεις πράγματα. Συγκεκριμένα με το να δίνεις τον χρόνο σου, τη δημιουργικότητά σου, και τα αποτελέσματα των ικανοτήτων σου<sup>165</sup>.

Βάση αυτής της ιδεολογίας έχει αναπτυχθεί η κουλτούρα των hackers. Όπως κάθε υποκουλτούρα που είναι αυτοδημιούργητη και αυτοργανωμένη προωθούν μαζί τα κοινά τους συμφέροντα<sup>166</sup>. Η «υπόγεια» κοινότητα των hackers (underground groups) αποτελείται από κάποιες ομάδες που καταργούν το μύθο ότι οι hacker δεν είναι κοινωνικά άτομα.

---

<sup>162</sup> Granger, S 1994, 'The hacker ethic', *Proceedings of the conference on ethics in the computer age*, pp. 7-9. Διαθέσιμο στο: ACM Portal [15 Νοεμβρίου 2008].

<sup>163</sup> Douglas, T 2003, *Hacker culture*, Minnesota Press, Minneapolis.

<sup>164</sup> Poulsen, K 2001, 'Ethics challenge softens hacker con: cyber ethics contest will join hacker jeopardy and spot the fed at DefCon', *Security Focus*, 31 Μαΐου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/211>> [15 Νοεμβρίου 2008].

<sup>165</sup> Raymond, ES 2001, *How to be a hacker*. Διαθέσιμο στο: <<http://www.catb.org/~esr/faqs/hacker-howto.html>> [23 Αυγούστου 2008].

<sup>166</sup> Murphy, C 2004, 'Inside the mind of the hacker', *Accountancy Ireland Journal*, vol. 36, no. 3, pp. 12-13. Διαθέσιμο στο: British Library Direct [15 Δεκεμβρίου 2008].

## 3.2 Υπόγεια κοινότητα και ομάδες hackers

Οι ομάδες hackers αποτελούνται από hackers, οι οποίοι οργανώνονται με σκοπό την ανταλλαγή πληροφοριών, την προώθηση και θέσπιση των δικαιωμάτων και των συμφερόντων τους. Σε αυτή τη ενότητα θα γίνει αναφορά στις πιο γνωστές ομάδες, αν και πολλές από αυτές έχουν διαλυθεί, αλλά άφησαν πίσω τους αξιόλογο έργο και σημαντική ιστορία στο χώρο του hacking.

Οι ομάδες hackers άρχισαν να δημιουργούνται στις αρχές της δεκαετίας του 1980, με την έλευση του προσωπικού υπολογιστή. Οι ομάδες αυτές κέντριζαν τον Τύπο και συχνά προκαλούσαν τα ΜΜΕ να ασχοληθούν μαζί τους. Οι ομάδες άκμασαν μια εποχή που ακόμα δεν υπήρχε νομικό πλαίσιο για παραβάσεις υπολογιστών. Μέσα από τις ομάδες αυτές η πληροφορία γίνεται πιο εύκολα προσβάσιμη. Τα ονόματα ομάδων είναι μια παρωδία των μεγάλων εταιρειών, κυβερνήσεων, αστυνομίας και εγκληματιών. Συχνά χρησιμοποιείται εξειδικευμένη ορθογραφία.

### 3.2.1 Legion of Doom

Ο όρος "Legion of Doom" προέρχεται από τα κόμικς. Οι πρώτοι Legion of Doom που σύχναζαν στην Plovernet τη βάση του Quasi Moto, ήταν phreaks των τηλεφώνων. Μια παρέα ενθουσιωδών νέων με ενδιαφέρον στους υπολογιστές και στην αναζήτηση της γνώσης δημιουργήθηκαν πάνω στα συντρίμια ενός πιο παλιού γκρουπ phreaks, τους The Knights of Shadow. Αρχικά δηλαδή ξεκίνησαν από την εξερεύνηση των τηλεφωνικών γραμμών<sup>167</sup>.

Το 1984 ιδρύθηκε από τον επονομαζόμενο Lex Luthor (ψευδώνυμο), η ομάδα Legion of Doom με έδρα το Σικάγο. Μέλη της Ομάδας ήταν οι Lex Luthor, Karl Marx, Mark Tabas, Agrajag the ProlongedKing, Blotto Blue, Archer, EBA, The Dragyn Unknown Soldier<sup>168</sup>. Η Legion of Doom είχε την φήμη ότι συγκέντρωνε τους καλύτερους hackers. Η ομάδα αρχικά αποτελούνταν από δύο μέρη: τη Legion of Doom και τη Legion of Doom Hackers. Η τελευταία ήταν υποομάδα της πρώτης και απαρτιζόταν από ανθρώπους που ασχολούνταν με υπολογιστές και δίκτυα. Αργότερα,

---

<sup>167</sup> Leeson, PT & Coyne, CJ 2006, 'The economics of computer hacking', *Journal of Law, Economics and Policy*, vol. 1, no. 2, pp.511–532. Διαθέσιμο στο: <<http://scholar.google.gr/scholar?hl=en&lr=&q=info:hp7GBEQVx-oJ:scholar.google.com/&output=viewport&pg=1>> [15 Δεκεμβρίου 2008].

<sup>168</sup> 'The history of the Legion of Doom' 1990, *Phrack Magazine*, vol. 3, no. 31. Διαθέσιμο στο: <<http://www.phrack.org/issues.html?issue=31&id=5#article>> [15 Δεκεμβρίου 2008].



δεδομένου ότι όλα τα μέλη ασχολούνταν πια με υπολογιστές κρατήθηκε μόνο η μια ονομασία<sup>169</sup>.

Ο "Lex Luthor" (ο οποίος ήταν κάτω των 18 όταν σχημάτισε τους Legion) ήταν ένας εξπέρ του COSMOS, (Central System for Mainframe Operations) ένα εσωτερικό δίκτυο κομπιούτερ των τηλεφωνικών εταιριών. Ο Lex ήταν αρκετά καλός στο να παραβιάζει τα IBM mainframes. Για μερικά χρόνια η ομάδα αυτή μάζευε ότι καλύτερο υπήρχε στον χώρο του hacking. Μέχρι τη στιγμή που ένα από τα μέλη της, ο Phiber Optik (επίσης ψευδώνυμο) μαζί με μερικούς ακόμη, αποχώρησαν και σχημάτισαν την ανταγωνιστική ομάδα "Masters of Deception". Από το 1990 έως το 1992, οι δύο ομάδες επιδόθηκαν σ' έναν πραγματικό αγώνα αλληλοεξόντωσης, που είχε ως θύματα μια σειρά από υπολογιστικά συστήματα σε ολόκληρο τον πλανήτη, που «υπέφεραν» από τις παρενέργειες του δικτυακού πολέμου των ενθουσιωδών νεαρών<sup>170</sup>.

Οι περισσότεροι εξ' αυτών (από την πλευρά των MOD, τουλάχιστον) κατέληξαν στη φυλακή, όταν το FBI κατόρθωσε να τους εντοπίσει. Από τα πιο γνωστά περιστατικά αυτής της ομάδας ήταν η κλοπή ενός αρχείου της Bellsouth που περιέγραφε τη λειτουργία ενός συστήματος συναγεμίου<sup>171</sup>.

Η Legion of Doom συνέβαλε σημαντικά στη γενική στην πορεία του hacking και στην απελευθέρωση της πληροφορίας και παρήγαγε πολύτιμη γνώση σχετικά με την εξ' αποστάσεως διείσδυση σε υπολογιστικά συστήματα<sup>172</sup>. Στο έργο των LOD συμπεριλαμβάνεται και μια σειρά τευχών που κυκλοφόρησαν με το όνομα LOD/H με περιεχόμενο διάφορες πληροφορίες για την κοινότητα των hacker "Electronic Magazines: The Legion of Doom/Hackers Technical Journal<sup>173</sup>".

Στην underground κοινότητα, η Legion of Doom θεωρείται ως καινοτόμος και πρωτοποριακή δύναμη, που βελτίωσε με συνέπεια το συλλογικό επίπεδο γνώσης και έδωσε πολλές απαντήσεις στις ερωτήσεις που κυμαίνονται από τα έργα του τηλεφωνικού συστήματος ως τη δομή των λειτουργικών συστημάτων υπολογιστών.

---

<sup>169</sup> Coutorie, LE 1995, 'The future of high-technology crime: a parallel celphi study', *Journal of Criminal Justice*, vol. 23, no. 1, pp. 13-27. Διαθέσιμο στο: Elsevier [15 Δεκεμβρίου 2008].

<sup>170</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [9 Σεπτεμβρίου 2008].

<sup>171</sup> Sterling, B 1994, *The hacker crackdown: law and disorder on the electronic frontier*, Bantam Books, New York. Διαθέσιμο στο: <<http://www.mit.edu/hacker/hacker.html>> [15 Νοεμβρίου 2008].

<sup>172</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [9 Σεπτεμβρίου 2008].

<sup>173</sup> *The Legion of Doom: hackers technical journal*, The Legion of Doom. Διαθέσιμο στο: <<http://www.textfiles.com/magazines/LOD>> [15 Νοεμβρίου 2008].

Καμία άλλη ομάδα δεν αφιερώθηκε αποκλειστικά στην αναζήτηση του υπολογιστή και στη γνώση των τηλεπικοινωνιών.

Η λειτουργία της ομάδας έπαψε το 1990 λόγω της δίωξης των hackers από τη κυβέρνηση των ΗΠΑ. Πολλά από τα μέλη της ομάδας συνελήφθησαν μετά την επιχείρηση Sundevil (αντι-hacker δραστηριότητα του 1990, η «Επιχείρηση Sundevil» με σαρωτικές, πανεθνικές κατασχέσεις υπολογιστών της 8ης Μαΐου 1990)<sup>174</sup>. Σήμερα υπάρχουν κάποια μέλη της ομάδας και έχουν δημιουργήσει την μια εταιρία ασφαλείας με ονομασία LOD Communication Inc <<http://www.lod.com>>.

### 3.2.2 Masters of Deception

Η Masters of Deception (MOD) ήταν μια ομάδα hackers με έδρα της τη Νέα Υόρκη. Οι ιδρυτές των MOD ήταν οι Mark Abene ("Phiber Optik"), Paul Stira ("Scorpion"), Eli Ladopoulos ("Acid Phreak"), HAC, John Lee ("Corrupt," a.k.a. "Netw1z"), and Julio Fernandez ("Outlaw"). Το όνομα τους είναι μια παρωδία του LOD καθώς το M είναι ένα γράμμα πιο πάνω από το L. Η μοναδική ειρωνεία και το καυστικό μαύρο χιούμορ των MOD θα προκαλέσει το ενδιαφέρον των MME<sup>175</sup>.

Ο Mark Abene, ο οποίος ήταν μέλος των LOD, εκδιώχθηκε από την ομάδα εξαιτίας της σύγκρουσης του με τα άλλα μέλη. Έτσι λόγω της προελεύσεως των MOD δεν είναι καθόλου παράξενο το γεγονός ότι η δύο ομάδες κατέληξαν ανταγωνιστικές μεταξύ τους. Από το 1990 και για δύο χρόνια, οι δύο ομάδες πολέμησαν μεταξύ τους. Οι μάχες τους έγιναν θρύλος για πολλά χρόνια μέχρι που οι περισσότεροι συνελήφθησαν το 1993 από το FBI.

Το κοινό πρωτάκουσε για την ομάδα στις 28 Νοεμβρίου 1989, όταν οι hackers εξαφάνισαν τις πληροφορίες από τους υπολογιστές της Learning Link της επιχείρησης WNET, Channel 13, στη Νέα Υόρκη, η οποία εξυπηρετούσε εκατοντάδες σχολεία. Οι καθηγητές και οι βιβλιοθηκονόμοι που ήταν συνδεδεμένοι με στο σύστημα διάβασαν το μήνυμα, "Happy Thanksgiving you turkeys, from all of us at MOD<sup>176</sup>".

<sup>174</sup> Halbert, D 1997, 'Discourses of danger and the computer hacker', *Information Society*, vol. 13, no. 4, pp. 361–374. Διαθέσιμο στο: InformaWorld [15 Νοεμβρίου 2008].

<sup>175</sup> Carpenter, T 1995, Hijacking on the infobahn', *The New York Times*, 22 Ιανουαρίου. Διαθέσιμο στο: <[http://query.nytimes.com/gst/fullpage.html?res=990CE4DA1238F931A15752C0A963958260&sec=&spon=&scp=1&sq=Masters%20of%20Deception%20\(MOD\)&st=cse](http://query.nytimes.com/gst/fullpage.html?res=990CE4DA1238F931A15752C0A963958260&sec=&spon=&scp=1&sq=Masters%20of%20Deception%20(MOD)&st=cse)> [22 Νοεμβρίου 2008].

<sup>176</sup> Gabriele, T 1995, 'Reprogramming a convicted hacker: to his on-line friends, Phiber Optik is a virtual hero', *The New York Times*, 14 Ιανουαρίου. Διαθέσιμο στο:

Αρχικά οι MOD ασχολούνταν με το phone phreaking, δηλαδή ήταν άτομα που έκαναν χτυπήματα με διαφόρους τρόπους μέσω τηλεφωνικού δικτύου. Είχαν καταφέρει φυσικά να μην πληρώνουν υπεραστικά τηλεφωνήματα και να ακούν συνδιαλέξεις άλλων χρηστών, ενώ είχαν ένα σύστημα για να μιλούν πολλά άτομα ταυτόχρονα. Αυτό που τους έκανε όμως διάσημους ήταν όταν κατάφεραν να μπουν στα υπολογιστικά συστήματα κάποιων βάσεων δεδομένων, οι οποίες άνηκαν σε οργανισμούς όπως NSA (National Security Agency/Central Security Service), η AT&T (American Telecommunications Company), η Bank of America και της TRW (Thompson Ramo Wooldridge Inc.). Από την τελευταία κατάφεραν να έχουν πρόσβαση σε τραπεζικές αναφορές για περιουσιακή κατάσταση ορισμένων από τους πιο πλούσιους ανθρώπους των ΗΠΑ όπως εκείνες του Geraldo Rivera, Richard Gere και Tony Randall. Μερικές από αυτές τις πληροφορίες πουλήθηκαν κιόλας<sup>177</sup>.

Οι Masters of Deception ελέγχουν με επιτυχία τα τηλεφωνικά δίκτυα της RBOC (Regional Bell Operating Company) και της X.25 (ένα ITV – T πρωτότυπο πρωτόκολλο επιπέδων δικτύου για μεταγωγή πακέτων επικοινωνίας για δίκτυα ευρείας περιοχής (WAN)) αλλά και μεγάλου τμήματος του Διαδικτύου. Μερικές από τις μεθόδους που χρησιμοποιούσαν οι MOD είναι η εσφαλμένη κατεύθυνση, οι πίσω πόρτες, οι ιοί, οι Δούρειοι ίπποι (trojan horses), η κοινωνική μηχανική και το ψάξιμο στα απορρίμματα των εταιριών. Παραδείγματος χάριν, οι MOD ήταν σε θέση να εισβάλουν και να ελέγχουν το σύστημα τηλεπικοινωνιών μόνο μετά από έρευνα και συλλογή πληροφοριών που βρέθηκαν στα απορρίμματα της τηλεφωνικής εταιρείας της Νέας Υόρκης<sup>178</sup>.

Οι MOD λειτουργούσαν διαφορετικά από πολλές απόψεις από τις άλλες ομάδες hackers. Αν και μοιράζονταν μεταξύ τους τις πληροφορίες αμφισβητείται εάν αντάλλασσαν αυτές τις πληροφορίες με άλλους hackers εκτός της ομάδας τους (αν και είναι κάτι αντίθετα στο πνεύμα του hacking). Θεωρούσαν ότι κάποιες πληροφορίες θα ήταν επικίνδυνο αν διατίθεντο σε άλλα άτομα εκτός ομάδας. Για να

---

<<http://query.nytimes.com/gst/fullpage.html?res=990CEED71F39F937A25752C0A963958260>> [22 Νοεμβρίου 2008].

<sup>177</sup> Tabor, BW & Ramirez, A 1992, 'Computer savvy with an attitude: young working-class hackers accused of high-tech crime', *The New York Times*, 23 Ιουλίου. Διαθέσιμο στο: <[http://query.nytimes.com/gst/fullpage.html?res=9E0CE0DD123EF930A15754C0A964958260&sec=technology&spon=&&scp=3&sq=Masters%20of%20Deception%20\(MOD\)&st=cse](http://query.nytimes.com/gst/fullpage.html?res=9E0CE0DD123EF930A15754C0A964958260&sec=technology&spon=&&scp=3&sq=Masters%20of%20Deception%20(MOD)&st=cse)> [22 Νοεμβρίου 2008].

<sup>178</sup> Winkler, I & Dealy, B 1995, 'Information security technology?: don't rely on it.: a case study in social engineering', *Proceedings of the fifth Usenix Unix Security Symposium*, The usenix Association. Διαθέσιμο στο <[http://www.usenix.org/publications/library/proceedings/security95/full\\_papers/winkler.pdf](http://www.usenix.org/publications/library/proceedings/security95/full_papers/winkler.pdf)> [22 Νοεμβρίου 2008].

έχει κάποιος πρόσβαση στη γνώση των MOD θα έπρεπε να επιδείξει σοβαρότητα, υπευθυνότητα και σεβασμό στους ανώτερους της ιεραρχίας. Για την ακρίβεια αυτός ο τρόπος προστασίας των πληροφοριών ήταν επινόηση των LOD<sup>179</sup>.

Το 1984 η αμερικάνικη κυβέρνηση για να πατάξει την αύξηση των hackers θεωρεί τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα έγκλημα και αυτό αποτέλεσε την αρχή του μεγάλου πολέμου κατά των hackers. Το 1992 πέντε μέλη από την ομάδα κατηγορούνται για ηλεκτρονικές απάτες. Ο Phiber Optik κλήθηκε ένοχος το 1993 για την χωρίς έγκριση είσοδο του στους υπολογιστές της Southwestern Bell, εγκαθιστώντας το πρόγραμμα "back door" για να του επιτρέψει να εισέλθει εκ νέου και να κάνει άλλες αλλαγές, που κοστίζουν στην εταιρεία περίπου 370.000 δολάρια για τη διόρθωση του προβλήματος που δημιούργησε<sup>180</sup>. Μετά την σύλληψη του ο Phiber Optik δήλωσε «...επειδή συλλήφθηκα δεν θα το ξανάκανα αυτό...δεν λέω στους υπόλοιπους ανθρώπους να μην κάνουν αυτά που έκανα. Πάντα θα υπάρχουν άνθρωποι που θα χακεύουν. Αυτό που κάνουμε εμείς είναι να τους προειδοποιούμε ότι πρέπει να προσέχουν»<sup>181</sup>. Υποστηρίζει επίσης ότι έσπασε στους υπολογιστές για να κερδίσει μόνο μια κατανόηση για το πώς λειτούργησαν οι φίλοι του χρησιμοποίησαν τη γνώση για να κάνουν τα χρήματα. Ήταν κάτι που βγήκε εκτός ελέγχου. Ο «Phiber Optik» μετά από μια έρευνα του New York Magazine ως ένας από τους 100 εξυπνότερους ανθρώπους της χώρας<sup>182</sup>.

### 3.2.3 Cult of the Dead Cow

Μια από τις μεγαλύτερες και πιο γνωστές ομάδες ακτιβιστών του Διαδικτύου, η "Cult of the Dead Cow", γνωστή και ως cDc ή cDc Communications, ιδρύθηκε τον Ιούνιο του 1984 στο Lubbock του Τέξας από τον Grandmaster Ratte (γνωστός και ως wamp Ratte), τον Franken Gibe και τον Sid Vicious. Χαρακτηρίστηκε ως η ισχυρότερη πολιτική ομάδα των hackers στο Διαδίκτυο. Η cDc είναι αφιερωμένη στην προστασία της online ιδιωτικής ζωής και στα δικαιώματα όλων των χρηστών του Διαδικτύου. Η αποστολή της είναι να εξαλειφθεί η κατάχρηση του Διαδικτύου

---

<sup>179</sup> Quittner, J & Slatalla, M 1995, *Masters of Deception: the gang that ruled cyberspace*, Vintage, London.

<sup>180</sup> Macz, M 2002, *Internet underground: the way of the hacker*, PageFree Publishing, Galaxy.

<sup>181</sup> Gabriele, T 1995, 'Reprogramming a convicted hacker; to his on-line friends, Phiber Optik is a virtual hero', *The New York Times*, 14 Ιανουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=990CEED71F39F937A25752C0A963958260>> [22 Νοεμβρίου 2008].

<sup>182</sup> Leeson PT & Coyne, CJ 2006, 'The economics of computer hacking', *Journal of Law, Economics and Policy*. Διαθέσιμο στο: <<http://www.peterleeson.com/hackers.pdf>> [22 Νοεμβρίου 2008].

και η καταπάτηση της ιδιωτικής ζωής που μαστίζει της Ηνωμένες Πολιτείες και όλο τον κόσμο<sup>183</sup>.

Η ομάδα διατηρεί ένα ιστολόγιο (weblog), στο Διαδίκτυο με τίτλο "Cult of the Dead Cow", όπου δημοσιεύονται θέματα hacking, τις σκέψεις και τις απόψεις των μελών της διεκδικώντας με αξιώσεις τον τίτλο του πρώτου διαδικτυακού περιοδικού στον κόσμο, με επίσημη online έκδοση το 1984<sup>184</sup>. Περισσότερα από είκοσι χρόνια μετά, το διαδικτυακό περιοδικό συνεχίζει να εκδίδεται (αν και πλέον έχει μια εντελώς blog εικόνα)<sup>185</sup>. Η ιστοσελίδα αυτή χαρακτηρίζεται από το ειρωνικό και καυστικό ύφος <<http://www.cultdeadcow.com>>.

Η CDC Communications είναι η μητρική οργάνωση της Cult of the Dead Cow, ωστόσο η Cult of the Dead Cow είναι μόνο μία από τις τρεις ομάδες που εμπίπτουν στην CDC Communications. Τα άλλα δύο είναι το "Ninja Strike Force" και "Hacktivismο" <<http://www.hacktivismο.com>>.

Το 1996, το CDC ανακοίνωσε τη γέννηση του Ninja Strike Force, μια ομάδα "NINJA" αφιερωμένη στην επίτευξη των στόχων του CDC, τόσο online και offline. Στα τέλη του 1999, το CDC δημιουργεί την ομάδα Hacktivismο. Σύμφωνα με την CDC Communications πρόκειται για μια ανεξάρτητη ομάδα, αφιερωμένη στη δημιουργία τεχνολογίας αντι-λογοκρισίας για την προαγωγή των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο<sup>186</sup>.

Η μεγαλύτερη συνεισφορά της ομάδας στη σκηνή του hacking είναι το εργαλείο Back Orifice 2000 που εμφανίστηκε στις 3 Αυγούστου 1998 στην ετήσια συγκέντρωση των hackers, την DEF CON. Ουσιαστικά πρόκειται για ένα πρόγραμμα, το οποίο επιτρέπει σχεδόν σε οποιονδήποτε να επέμβει στον υπολογιστή μέσω του Διαδικτύου, δηλαδή ένα εργαλείο τηλεχειριζόμενης διεύθυνσης. Το πρόγραμμα αποτελείται από δύο τμήματα: τον διακομιστή (server) και τον πελάτη (client). Το πρώτο τμήμα το χρησιμοποιεί ο ανεπιθύμητος εισβολέας και στέλνοντας το άλλο τμήμα στο υποψήφιο θύμα αποκτά αυτόματα τον έλεγχο του υπολογιστή του. Το θύμα μπορεί να λάβει το Back Orifice 2000 μέσω ενός ηλεκτρονικού μηνύματος, μιας

---

<sup>183</sup> Ruffin, O 2002, 'Waging peace on the internet', *The Register*. Διαθέσιμο στο: <<http://thehacktivist.com/archive/news/2002/WagingPeace-TheReg-2002.pdf>> [28 Νοεμβρίου 2008].

<sup>184</sup> *Cult of the Dead Cow*, 2008, cDc communications. Διαθέσιμο στο: <<http://www.cultdeadcow.com>> [29 Νοεμβρίου 2008].

<sup>185</sup> Νταραδήμου, Α 2008, 'E-zines, τα περιοδικά της hi-tech εποχής', *Ελεύθερος Τύπος*, 9 Ιανουαρίου. Διαθέσιμο στο: <<http://www.e-tipos.com/newsitem?id=21504>> [29 Νοεμβρίου 2008].

<sup>186</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [29 Σεπτεμβρίου 2008].

ανταλλαγής αρχείων ή ακόμη σερφάροντας απλώς στο Διαδίκτυο. Το πρόγραμμα δεν γίνεται καθόλου αντιληπτό, αφού, όταν φτάνει στον υπολογιστή μας εγκαθίσταται κρυφά, χωρίς να καταλάβουμε τίποτα. Από τη στιγμή που θα εγκατασταθεί, ο εισβολέας μπορεί να δει τους κωδικούς μας, να διαβάσει το ηλεκτρονικό ταχυδρομείο μας, να παρακολουθήσει τις εντολές μας, να ξεκινήσει κάποιο άλλο πρόγραμμα, όπως κάποιον ιό ή ακόμη χειρότερα να χρησιμοποιήσει τον υπολογιστή μας προκειμένου να εισχωρήσει κάπου αλλού<sup>187</sup>.

Ένα άλλο χαρακτηριστικό του είναι ότι είναι πολύ απλό στη χρήση και δεν απαιτεί ούτε ιδιαίτερες γνώσεις, αλλά ούτε και προηγούμενη εμπειρία σε τέτοιου είδους προγράμματα. Από τότε έχει διαπιστωθεί ότι τουλάχιστον 100.000 άνθρωποι έχουν πέσει θύματά του. Και αυτό ήταν μόνο η αρχή. Σκοπός της ομάδας αυτής δεν ήταν, σύμφωνα με την ίδια, να βλάψουν τους χρήστες του Διαδικτύου, αλλά να δείξουν στη Microsoft πόσο ευάλωτο είναι το λειτουργικό της σύστημα σε τέτοιες απειλές<sup>188</sup>.

Η δράση της ξεκίνησε από τη δεκαετία του 1980 αλλά μόλις πρόσφατα έχει προσανατολιστεί αποκλειστικά σε πολιτικούς στόχους και δράσεις. Η εν λόγω ομάδα έχει δημιουργήσει και έναν δικτυακό τόπο συνάντησης και πληροφόρησης όλων των ηλεκτρονικών ακτιβιστών –το [hactivism.org](http://hactivism.org)– στον οποίο οι ενδιαφερόμενοι μπορούν να συμμετέχουν σε δικτυακά workshops, να παρακολουθήσουν επιδείξεις και να κατεβάσουν εργαλεία λογισμικού για ηλεκτρονικό ακτιβισμό. Η ίδια ομάδα επίσης συνεργάζεται με την ηλεκτρονική ομάδα Κινέζων αντιφρονούντων, τους Hong Kong Blondes, οι οποίοι εισβάλλουν σε τακτά διαστήματα στα αρχεία της Αστυνομίας και της κρατικής Ασφάλειας της Κίνας, συλλέγουν πληροφορίες και προειδοποιούν «πολιτικούς στόχους» για επικείμενες συλλήψεις<sup>189</sup>.

Στις αρχές του το CDC προώθησε το «Goolag» μια εκστρατεία ως απάντηση στην απόφαση της Google να συμμορφωθεί με την Κινέζικη διαδικτυακή πολιτική λογοκρισίας και τα ελεγχόμενα αποτελέσματα αναζήτησης στην ηπειρωτική-κινεζική έκδοση της μηχανής αναζήτησης. Η εκστρατεία κατά κύριο λόγο είναι μια παρωδία

---

<sup>187</sup> Zeltser, L 2000, 'The evolution of malicious agents', *Web Report*, Απρίλιος. Διαθέσιμο στο: <<http://www.securitytechnet.com/resource/security/virus/agents.pdf>> [19 Ιανουαρίου 2008].

<sup>188</sup> Schwartz, J 2001, 'Fighting crime online: who is in harm's way?', *The New York Times*, 8 Φεβρουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9B0DE2D91631F93BA35751C0A9679C8B63&sec=&spon=&scp=1&sq=Back%20Orifice%2000%20&st=cse>> [19 Ιανουαρίου 2008].

<sup>189</sup> Gissel, R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [29 Ιανουαρίου 2008].

της Google. Η ομάδα ενθάρρυνε τους αναγνώστες να κάνουν μπλουζάκια και άλλα εμπορεύματα και δώρισε τα έσοδα από τις πωλήσεις τους για τα ανθρώπινα δικαιώματα στην Κίνα. Η CDC στη συνέχεια εξέδωσε δελτίο τύπου για την εκστρατεία, στο οποίο περιγράφεται η Microsoft, η Yahoo, η Google και η Cisco, όπως η «συμμορία των τεσσάρων» λόγω των αντίστοιχης πολιτικής συμμόρφωσης με την κυβερνητική πολιτική του Διαδικτύου του Πεκίνου. Ουσιαστικά το Goolag είναι ένα εργαλείο, το οποίο επιτρέπει να χρησιμοποιούν το Google για να εξετάσει κάθε ιστοτόπο και να βρει τα τρωτά σημεία του<sup>190</sup>.

### 3.2.4 L0pht Heavy Industries

Η “L0pht Heavy Industries” αποτελεί μια από τις πλέον διαβόητες ομάδες hackers, η οποία έχει κατά καιρούς απασχολήσει το χώρο των MME και του hacking είτε με τη δράση της είτε με τα προγράμματα που έχει φέρει στο φως της δημοσιότητας. Η L0pht Heavy Industries, πάντως, είναι μία μόνο από τις πολλές ομάδες hackers που παρέχουν και υπηρεσίες anti-hacking. Η ομάδα αυτή δραστηριοποιήθηκε μεταξύ του 1992 και του 2000 με έδρα της τη Βοστώνη της Μασαχουσέτη. Τα μέλη της ομάδας ήταν οι Brian Oblivion, Count Zero, Dildog, Golgo 13, John Tan, Kingpin, Mudge, Silicosis, Space Rogue, Stefan Von Neuman, Weld Pond, White Knight<sup>191</sup>.

Ο δεύτερος χαρακτήρας στο όνομά της ήταν αρχικά ένα μηδενικό (0), ένα σύμβολο που χρησιμοποιούνταν σε παλαιά τηλέτυπα. Το σύγχρονο όνομά της είναι "l0pht". Η αρχική ιδέα για το όνομα ήταν απλά "L0pht", αλλά ένα μέλος της πρότεινε το '0' να αντικαταστήσει το «ο», και η ιδέα υιοθετήθηκε γρήγορα. Η προέλευση του ονόματος μπορεί να επισημανθεί στο γεγονός ότι μερικά από τα ιδρυτικά μέλη L0pht μοιράστηκαν ένα κοινό διώροφο διαμέρισμα (loft apartment) στη Βοστώνη, από όπου πειραματιζόνταν σε χακιστικές δραστηριότητες με προσωπικούς ηλεκτρονικούς υπολογιστές<sup>192</sup>.

---

<sup>190</sup> Cult of the Dead Cow 2006, cDc launches global campaign against Google. 12 Φεβρουαρίου 2006. *Cult of the Dead Cow: Blog*. Διαθέσιμο στο: <<http://w3.cultdeadcow.com/cms/2006/02/cdc-launches-gl.html>> [29 Ιανουαρίου 2008].

<sup>191</sup> Hafner, K 2000, ‘In world of hackers, good guys and bad guys are often a blur’, *The New York Times*, 12 Φεβρουαρίου. Διαθέσιμο στο <<http://query.nytimes.com/gst/fullpage.html?res=9B03E5DA1F3EF931A25751C0A9669C8B63&sec=&spon=&scp=5&sq=L0pht&st=cse>> [29 Ιανουαρίου 2008].

<sup>192</sup> Spangler, R 2003, *Packet Sniffer Detection with AntiSniff*, Department of Computer and Network Administration, University of Wisconsin. Διαθέσιμο στο: <<http://www.linux-sec.com/Sniffer.Detectors/snifferdetection.pdf>> [29 Ιανουαρίου 2008].

Δημιούργησαν μια επιχείρηση με όνομα L0pht Heavy Industries, ένα ινστιτούτο μελετών και απόψεων για τους hackers. Μέσα από αυτή την ομάδα κυκλοφορούν αρκετές συμβουλές ασφαλείας και παράγονται ευρέως διαδεδομένα εργαλεία λογισμικού όπως το L0phtCrack, έναν κωδικό πρόσβασης για τα Windows NT. Στις 19 Μαΐου 1998, τα επτά μέλη του L0pht κατέθεσαν ενώπιον του Κογκρέσου των Ηνωμένων Πολιτειών ότι θα μπορούσαν να κλείσουν ολόκληρο το Διαδίκτυο σε 30 λεπτά. Τον Ιανουάριο του 2000, η L0pht Heavy Industries συγχωνεύθηκε με την @stake (Computer Security Professional Services Company) και έτσι ολοκληρώθηκε η αργή μετάβαση της L0pht από μια underground οργάνωση σε μια "whitehat" εταιρεία ασφάλειας υπολογιστών. Στις 14 Μαρτίου 2008, αρκετά μέλη της L0pht δημιούργησαν μια επιτροπή με ονομασία INFOSEC, InfoSec Professionals<sup>193</sup>.

### 3.2.5 Chaos Computer Club (CCC)

Η CCC ιδρύθηκε στο Βερολίνο στις 12 Σεπτεμβρίου 1981. Η Chaos Computer Club (CCC) είναι μία από τις μεγαλύτερες και πιο σημαντικές οργανώσεις hackers. Η CCC έχει ως έδρα της την Γερμανία αλλά επεκτάθηκε και σε άλλες γερμανόφωνες χώρες και σήμερα έχει περισσότερα από 4.000 μέλη. Περιγράφει τον εαυτό της ως «ένα γαλαξία ζωής» της κοινότητας των ανθρώπων, ανεξάρτητα από ηλικία, φύλο, τη φυλή ή κοινωνικό προσανατολισμό, η οποία αγωνίζεται εκτός συνόρων για την ελευθερία της πληροφόρησης. Σε γενικές γραμμές, η CCC αγωνίζεται για μεγαλύτερη διαφάνεια στις κυβερνήσεις, την ελευθερία της πληροφόρησης και το ανθρώπινο δικαίωμα στην επικοινωνία. Στηρίζει τις αρχές ηθικής των hackers και τους αγώνες για ελεύθερη πρόσβαση σε υπολογιστές και τεχνολογική υποδομή για όλους. Μια ομάδα hacker, με τρωκτική δράση και αξιοζήλευτες διεισδυτικές επιδόσεις στον χώρο του Διαδικτύου με στόχο, όπως τονίζουν οι εκπρόσωποί του, να αποδείξουν πόσο εύαλωτος είναι ο τομέας ασφαλείας στον ψηφιακό κόσμο<sup>194</sup>.

Η CCC έγινε παγκοσμίως γνωστή όταν επέστησε την προσοχή του κοινού στην ανασφάλεια του γερμανικού Bildschirmtext δίκτυο υπολογιστών. Το 1984 η CCC ανακάλυψε μια «τρύπα» στο σύστημα των γερμανικών ταχυδρομείων και κατάφερε να μεταβιβάσει μέσα σε μια νύκτα από το ταμειυτήριο του Αμβούργου 135.000 μάρκα στον τραπεζικό λογαριασμό της CCC. Τα χρήματα επέστρεψαν την επόμενη

<sup>193</sup> Gissel R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [29 Ιανουαρίου 2008].

<sup>194</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.



μέρα μπροστά στον Τύπο. Πριν από το περιστατικό, το σύστημα παροχής είχε δημοσίως παραλείψει να αντιδράσει ως απόδειξη της ανασφάλειας όπως ισχυρίζονται οι CCC<sup>195</sup>.

Έχοντας αναλάβει τον ρόλο του υπέρτατου προστάτη των προσωπικών δεδομένων στον κυβερνοχώρο δεν διστάζουν να διεισδύουν στα κεντρικά δικτυακά συστήματα διαφόρων φορέων, υπηρεσιών ή εταιρειών, προκαλώντας κάθε είδους και μεγέθους «βλάβη», φροντίζοντας ωστόσο πάντα αυτή να είναι αναστρέψιμη, και εν συνεχεία δίνουν στη δημοσιότητα τα ευρήματά τους. Η CCC μπαίνει στο σύστημα βλέπει αφήνει το αποτύπωμα της και φεύγει, δεν δημιουργεί ανεπανόρθωτες βλάβες. Αφήνοντας το μήνυμα ότι πρέπει επιτέλους να αποκτήσουμε ασφάλεια.

Τρία χρόνια αργότερα μετά την υπόθεση με το ταμειυτήριο του Αμβούργου, διείσδυσαν στα ηλεκτρονικά συστήματα της NASA, της Ευρωπαϊκής Διαστημικής Υπηρεσίας, της Philips και της Γαλλικής Υπηρεσίας Ατομικής Ενέργειας. «Δεν εργαζόμαστε καταστροφικά, δεν λεηλατούμε ή πουλάμε δεδομένα και δεν φυτεύουμε ιούς στον κόσμο», τονίζουν οι εκπρόσωποι του CCC περικλείοντας τη φιλοσοφία του συλλόγου σε τρεις προτάσεις<sup>196</sup>.

Χαρακτηριστικό είναι ότι μέλη του CCC κατάφεραν τον Μάρτιο του 2008 να αποσπάσουν και να δημιουργήσουν ένα πιστό αντίγραφο του δακτυλικού αποτυπώματος του Βόλφγκανγκ Σόιμπλε (Υπουργού Εσωτερικών της Γερμανίας) εν συνεχεία να παραγάγουν χιλιάδες αντίτυπά του, τυπωμένα σε ειδικές διαφάνειες και να τα διανεμούν στον κόσμο<sup>197</sup>. Οποιοσδήποτε μπορεί πλέον να προσαρμόσει τη μικρή διαφάνεια με το υπουργικό αποτύπωμα στον δείκτη του χεριού του και να ξεγελάσει κατ' αυτό τον τρόπο το ηλεκτρονικό σύστημα πρόσβασης εισόδου στο γραφείο, για παράδειγμα, του Γερμανού υπουργού, καθώς ο αισθητήρας λέιζερ θα αναγνώριζε το αποτύπωμα ως αυθεντικό, επιτρέποντας την είσοδο στον ψεύτικο Σόιμπλε. Οι εκπρόσωποι της CCC, δηλώνουν ότι το συγκεκριμένο παράδειγμα αποδεικνύει ότι όσο πιστό είναι το αντίγραφο του αποτυπώματος στη διαφάνεια τόσο χαζή είναι η ηλεκτρονική συσκευή. Επίσης απειλούσαν να δημοσιεύσουν στο

---

<sup>195</sup> Gissel R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press. Διαθέσιμο στο: Google Books Search [29 Ιανουαρίου 2008].

<sup>196</sup> Schmemmann, S 1987, 'Computer buffs tapped NASA files', *The New York Times*, 16 Σεπτεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9B0DE1DA1530F935A2575AC0A961948260&scp=1&sq=nasa%20%20hackers%20%20Chaos%20Computer%20Club%201987&st=cse>> [19 Ιανουαρίου 2008]

<sup>197</sup> Βενιού, Ε 2008, 'Τι κρύβουν τα νέα βιομετρικά διαβατήρια', *Το Βήμαonline*, 30 Νοεμβρίου. Διαθέσιμο στο: <<http://www.tovima.gr/default.asp?pid=2&ct=33&artId=244778>> [19 Ιανουαρίου 2008].

Διαδίκτυο τα δαχτυλικά αποτυπώματα της Γερμανίδας καγκελαρίου Άγκελα Μέρκελ. Οι γερμανοί hackers διαμαρτύρονται με τον τρόπο αυτό για τη συλλογή βιομετρικών δεδομένων Γερμανών πολιτών από τις διοικητικές αρχές της χώρας<sup>198</sup>.

Πολλά μέλη της CCC καλούνται συχνά να δώσουν τα φώτα τους σε μέλη του Συνταγματικού Δικαστηρίου, ενώ έχουν παρευρεθεί σε ακροάσεις ερευνητικών επιτροπών στο γερμανικό Κοινοβούλιο. Ένα από τα πιο χαρακτηριστικά παραδείγματα της αποτελεσματικής και όπως αποδείχτηκε καθοριστικής δράσης τους αποτελεί η απομυθοποίηση της αξιοπιστίας της ηλεκτρονικής εκλογικής διαδικασίας που είχε αποφασιστεί να ακολουθηθεί τον περασμένο Μάρτιο στις δημοτικές εκλογές στο Αμβούργο. Οι εκπρόσωποι της CCC ζήτησαν από την αρμόδια αρχή να τους παραχωρήσουν μία από τις ειδικές συσκευές προκειμένου να διαπιστώσουν εάν και κατά πόσο είναι ασφαλές το σύστημα καταμέτρησης των ψήφων, αυτή αρνήθηκε. Έτσι οι hackers αγόρασαν μια παρεμφερή συσκευή, την άνοιξαν και άρχισαν να εξετάζουν ενδελεχώς το εσωτερικό της, τη μικροκάμερα, το λογισμικό, το σύστημα μεταφοράς των δεδομένων, και έτσι κατάφεραν να αποκωδικοποιήσουν το σύστημα. Η έρευνά τους απέδειξε ότι θα μπορούσε κάποιος να επέμβει στα ψηφοδέλτια κατά τέτοιο τρόπο, ώστε ανεξαρτήτως της προτίμησης των εκλογέων, η ψήφος τους να κατέληγε σε συγκεκριμένο ή συγκεκριμένους υποψηφίους. Μετά την παρουσίαση των ευρημάτων του εκπροσώπου της CCC Φρανκ Ρίγκερ στη δημοτική αρχή του Αμβούργου, απεσύρθη η πρόταση διεξαγωγής των εκλογών με ηλεκτρονικά ψηφοδέλτια<sup>199</sup>.

### 3.2.6 Infonomicon Computer Club

Η Infonomicon Computer Club είναι μια οργάνωση hackers που αποτελείται πάνω από 12 μέλη από όλη την Αμερική. Μέλη της ομάδας είναι οι Droops, Obfuscated, Phizone, Irongeek, Lowtek\_Mystik, Enigma, p0trillo23, kn1ghtl0rd, Ponyboy, Livinded, Kotrin, Downer, Dosman, Zach, Electroman<sup>200</sup>.

Η Infonomicon ξεκίνησε τον Ιούνιο του 2004 μια σειρά εκπομπών στο ραδιοφωνικό σταθμών με την επωνυμία Droops Radio, που αργότερα άλλαξε σε

---

<sup>198</sup> Σωνίδου, Μ 2008, 'Δικαιοσύνη των hacker', *Η Καθημερινή*, 1 Απριλίου. Διαθέσιμο στο: <[http://news.kathimerini.gr/4dcgi/\\_w\\_articles\\_world\\_2\\_01/04/2008\\_264705](http://news.kathimerini.gr/4dcgi/_w_articles_world_2_01/04/2008_264705)> [19 Ιανουαρίου 2008].

<sup>199</sup> Κατσουλής, Α 2007, 'Οι φύλακες... χάκερ των προσωπικών δεδομένων', *Το Έθνος*, 24 Μαΐου. Διαθέσιμο στο: <<http://www.ethnos.gr/article.asp?catid=11429&subid=2&pubid=1020438>> [19 Ιανουαρίου 2008].

<sup>200</sup> *Infonomicon Computer Club: the least constructive guys on the interwebs* 2008, Infonomicon Computer Club. Διαθέσιμο στο: <<http://nomicon.info/members.php>> [19 Ιανουαρίου 2008].

Infonomicon Radio. Τα επεισόδια επικεντρώθηκαν σε μια ποικιλία θεμάτων, από hardware hacking, lockpicking, πομπών FM. Η σειρά διήρκεσε μέχρι τις 25 Δεκεμβρίου του 2005 είχε 53 επεισόδια. Τον Αύγουστο του 2005, ο Phizone, εντάχθηκε στην ομάδα και βοήθησε την έναρξη ενός νέου δικτυακού τόπου καλείται PodcastIncubator.com, η οποία παρέχεται δωρεάν φιλοξενία σε άλλα άτομα που ενδιαφέρονται να ξεκινήσουν τη δική τους εκπομπή.

Η Infonomicon προσφέρει πολλά στην χακιστική κοινότητα διότι περιέχει πολύ καλές ηχογραφήσεις από ομιλίες hacker από τις οποίες μπορεί κανείς να αντλήσει πολύτιμο υλικό. Το Infonomicon TV είναι τμήμα του δικτυακού κόμβου τους που περιέχει λίγα επεισόδια για δει κανείς σχετικά με το hacking. Το twatech.org όπου υπάρχει μια καθημερινή ραδιοφωνική εκπομπή με περιεχόμενο θέματα σκληροπυρηνικής τεχνολογίας των hackers. Επίσης το hackermedia.org για να μπορεί το κοινό να δημοσιεύει ότι νέο υπάρχει.

Η ιστοσελίδα της Infonomicon Computer Club <<http://nomicon.info/index.php>>.

### 3.3 Η ηθική των hackers

Η ηθική των hackers αφορά τους δεοντολογικούς κανόνες, ή αλλιώς τον κώδικα των hackers. Κάθε κοινότητα έχει τους δικούς της κανόνες τους οποίους τα υπόλοιπα μέλη ασπάζονται, πιστεύουν και θεσπίζουν. Ίσως να φαίνεται ειρωνικό να μιλάμε για ηθική όταν το θέμα μας στη προκειμένη περίπτωση είναι οι hackers.

Η ηθική των hackers προέκυψε από τους αρχικούς αυθεντικούς hackers της δεκαετίας του 1950, τους επιστήμονες του MIT και αποτυπώθηκαν γραπτά για πρώτη φορά στο έργο του Steven Levy με τον τίτλο "Hackers: heroes of the computer revolution". Από την οπτική γωνία του Levy, η βασική ηθική αρχή των hackers θεσπίζει ότι 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». Η αρχή αυτή αναλύεται σε μια σειρά μερικών αρχών, οι κύριες από τις οποίες είναι<sup>201</sup>:

1. Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα.
2. Έλλειψη εμπιστοσύνης στην εξουσία και στις αρχές - προώθηση της αποκέντρωσης.
3. Οι hackers πρέπει να κρίνονται με βάση τις ικανότητες και τις επιδόσεις τους, και όχι με βάση κριτήρια, όπως τα πτυχία, η ηλικία, η φυλή ή η θέση.

<sup>201</sup> Levy, S 1984, *Hackers: heroes of the computer revolution*, Penguin Books, New York.

4. Μπορεί να δημιουργηθεί τέχνη και ομορφιά στον υπολογιστή.
5. Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

Οι θεμελιώδεις αυτές αρχές προέρχονται από αυθεντικούς και οραματιστές hackers και όχι από κυβερνοεγκληματίες<sup>202</sup>.

Η ηθική στην προκειμένη περίπτωση δεν ταυτίζεται απόλυτα με την κλασική έννοια του όρου. Η ηθική για τους hackers είναι το σπάσιμο κωδικών, η εισβολή σε υπολογιστικά συστήματα, η αναζήτηση της απαγορευμένης πληροφορίας, η προώθηση του ελεύθερου λογισμικού, τα μέσα δηλαδή, με τα οποία μπορούν να υπερασπιστούν τα πιστεύω τους και να υποτριξουν την δράση τους. Για παράδειγμα η παραβίαση του υπολογιστικού συστήματος ενός οργανισμού είναι μια πράξη αντίστασης στην πολιτική του οργανισμού αυτού στο να κρατά την πληροφορία και να μην την διαθέτει στο κοινό ή στη χρέωση πρόσβασης προς την πληροφορία.<sup>203</sup>

Η ηθική σχετίζεται περισσότερο με τους λευκούς hackers, αυτούς δηλαδή που ακόμα αντιπροσωπεύουν τους αυθεντικούς hackers. Ο κώδικας ηθικής υφίσταται ακόμα μέχρι σήμερα στον μοντέρνο hacker, για αυτό και η δράση των μαύρων hackers, των cracker ή των script kiddies θεωρείται κατώτερη και υποτιμάται από την κοινότητα των elite hackers.

Οι hackers διακατέχονται από περιέργεια και επαναστατικό πνεύμα, άλλοι το εκφράζουν πιο βίαια, ενώ άλλοι έχουν την ωριμότητα να διαχειριστούν τη δύναμη τους για το ηλεκτρονικό οικουμενικό καλό. Χρειάζονται κάποιες κατευθυντήριες γραμμές που να ενώνουν όλη την κοινότητα. 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<sup>204</sup>.

Ο κώδικας ηθικής των hackers θα μπορούσε να παραλληλισθεί με τον όρκο του Ιπποκράτη που δίνουν οι γιατροί. Μπορεί να μην είναι αυστηρός, να είναι γενικός, σε ορισμένες κατηγορίες να μην υφίσταται τόσο πολύ αλλά ακόμα υπάρχει στο προσκήνιο. Όπως δηλώνει και ο Stallman στη συνέντευξή του στη D. Denning: «...πιστεύω πως κάθε χρήσιμη πληροφορία πρέπει να είναι ελεύθερη. Όχι ως προς

---

<sup>202</sup> Λάζος, Γ 2001, *Πληροφορική και έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα.

<sup>203</sup> Furnell, S 2006, *Κυβερνοέγκλημα : καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα.

<sup>204</sup> Cross, T 2006, 'Academic freedom and the hacker ethic', *Communications of the ACM*, vol. 49, no. 6. Διαθέσιμο στο: ACM Portal [21 Αυγούστου 2008].

την τιμή της αλλά την ελευθερία αντιγραφής και προσωπικής χρήσης της. Λέγοντας χρήσιμη δεν εννοώ εμπιστευτικές πληροφορίες για άτομα ή αριθμούς πιστωτικών καρτών για παράδειγμα<sup>205</sup>». Βάση αυτής της ιδεολογίας και με καθήκον να θεσπίσουν τα πιστεύω τους οι hacker δρουν και δημιουργούν.

---

<sup>205</sup> Denning, D 1990. 'Concerning hackers who break into computer systems' *Proceedings of the thirteen national computer security conference*. Διαθέσιμο στο: <<http://cyber.eserver.org/hackers.txt>> [21 Αυγούστου 2008].

## ΚΕΦΑΛΑΙΟ 4:

### Η ΑΠΕΛΕΥΘΕΡΩΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ Η ΠΡΩΘΗΣΗ ΤΟΥ ΕΛΕΥΘΕΡΟΥ ΛΟΓΙΣΜΙΚΟΥ: ΜΙΑ ΜΑΡΞΙΣΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Ο hacker είναι υπέρμαχος της ελευθερίας και ως εκ τούτου υποστηρίζει την ελεύθερη αναζήτηση και ανταλλαγή της γνώσης χωρίς περιορισμούς. Την δεκαετία του 1980 οι hackers υποστήριζαν ότι η πληροφορία πρέπει να είναι ελεύθερη. Η πληροφορία στη προκειμένη περίπτωση είναι τα πάντα, οτιδήποτε ψηφιακό είναι δεδομένα, δηλαδή πληροφορίες. Το Διαδίκτυο είναι ένας χώρος όπου διαμοιράζονται και διακινούνται τεράστιες ποσότητες πληροφοριών.

Η διεθνής κοινότητα των hackers πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοικτού κώδικα όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό. Το «προλεταριάτο» των hackers τάσσεται και υπερασπίζεται την ελεύθερη ροή της πληροφορίας. Υποστηρίζουν κάθετα ότι η πληροφορία και η γνώση δεν ανήκουν σε ιδρύματα, δεν ανήκουν σε κράτη, δεν ανήκουν στις αυθεντίες και στους ειδικούς κι ότι είναι μέγα λάθος να προσφέρεται επεξεργασμένη και έτοιμη για κατανάλωση. Την πληροφορία οφείλουμε να τη φιλτράρουμε, να την επεξεργαστούμε, να την ανασυνθέσουμε μέσα μας. Έτσι δημιουργούμε την δική μας γνώση, έχει τα χαρακτηριστικά μας και είναι μοναδική γιατί πηγάζει μέσα από τον εαυτό μας<sup>206</sup>.

Η γνώση όμως δεν είναι μια στατική αξία που έχεις ή δεν έχεις. Δεν είναι τα βιβλία που διάβασες και που λένε ότι γνωρίζεις αυτό ή εκείνο. Η γνώση είναι διαρκής εξέλιξη, διαρκής εξερεύνηση, διαρκής ερμηνεία και διαρκής αμφιβολία. Είναι ένας τρόπος να ζεις και ένα μέσο ανάπτυξης και επιβίωσης μέσα στη κοινωνία, όχι μια ταμπέλα. Η γνώση όταν παραμένει στατική χάνει την αξία της. Ο κόσμος μας θα είχε μείνει πολλά χρόνια πίσω αν δεν ανταλλάζονταν οι πληροφορίες και αν δεν προσπαθούσαμε συλλογικά για κάτι καλύτερο<sup>207</sup>.

---

<sup>206</sup> Cross, T. 2006, 'Academic freedom and the hacker ethic', *Communications of the ACM*, vol. 49, no. 6. Διαθέσιμο στο: ACM Digital Library [4 Αυγούστου 2008].

<sup>207</sup> Μπουντουρίδης, Μ 2006, Κριτική της εργασίας στην κοινωνία της πληροφορίας. 21 Αυγούστου 2006. *Κοινωνικά Κινήματα & Δίκτυα: Blog*. Διαθέσιμο στο: <<http://thrymmata.blogspot.com/2006/08/blog-post.html>> [4 Αυγούστου 2008].

Στη συνείδηση της κοινής γνώμης, οι hackers είναι οι εγκληματίες των υπολογιστών, οι επικίνδυνοι πειρατές των συστημάτων ασφαλείας. Τα ΜΜΕ, ίσως παρακινούμενα από υποθάλπτοντα συμφέροντα προάγουν μια αρνητική και δαιμονοποιημένη εικόνα για τους hackers. Συγγέουν τους λαμπρούς επιστήμονες, ανθρώπους ευφυείς, που εργάζονται για την τεχνολογική πρόοδο και το οικουμενικό πληροφοριακό καλό, με νεαρούς που με την επιμονή τους σπάνε κωδικούς και δημιουργούν ψηφιακά μακελειά με έτοιμα προγράμματα. Η αλήθεια όμως βρίσκεται πολύ μακριά από αυτή την εικόνα.

Στο Μανιφέστο τους το 1986, οι ίδιοι οι hackers αυτοπροσδιορίζονται ως εξερευνητές και κυνηγοί της γνώσης, οπαδοί της πολυπολιτισμικότητας και της διαφοράς και πολέμοι του κέρδους, που το μόνο έγκλημά τους είναι η περιέργεια<sup>208</sup>. Ο Αμερικανός καθηγητής Μακένζι Γουάρκ, στο βιβλίο του «Μανιφέστο των hackers», διευρύνει ακόμα περισσότερο την έννοια του όρου ορίζοντας ότι «...οι hackers είναι οι παραγωγοί και διακινητές της πληροφορίας, ο επιστήμονας και ο καλλιτέχνης, ο φιλόσοφος και προγραμματιστής, όλοι όσοι πιστεύουν στην ανθρώπινη εφευρετικότητα, η οποία δεν μπορεί να υπάρξει εκτός της συνεργασίας και της αλληλεγγύης. Hackers είναι όλοι όσοι προασπίζουν την ελεύθερη ροή της πληροφορίας. Διότι η πληροφορία θέλει να είναι ελεύθερη, αλλά είναι παντού αλυσοδομένη»<sup>209</sup>.

Η μαρξιστική θεωρία επιβεβαιώνεται από την πραγματικότητα του ελεύθερου λογισμικού και η σύμπτωση μεταξύ τους είναι εντυπωσιακή. Αρχικά θα ήθελα να κάνω μερικές παρατηρήσεις σε ότι αφορά το νόημα των εννοιών που θα μας απασχολήσουν (ελεύθερο λογισμικό και μαρξισμός). Ο όρος ελεύθερο λογισμικό εμπερικλείει μία «ηθική» με συγκεκριμένη στάση απέναντι στο λογισμικό. Χαρακτηριστικό του είναι ότι δεν υπόκειται σε σχέσεις εμπορικές όπως αγοραστή/πωλητή, δεν έχει πατρίδα, η συνεργασία αποτελεί τη βάση της δραστηριότητας/ανάπτυξης του και η ικανοποίηση της προσφοράς προς την κοινότητα αποτελεί στόχο της παραγωγής.

Ο Μαρξισμός είναι η θεωρία η οποία, μεταξύ άλλων, ισχυρίζεται ότι η εξέλιξη του καπιταλισμού οδηγεί στην δημιουργία μίας νέας μετά-καπιταλιστικής κοινωνίας, η οποία δεν θα διέπεται από εμπορικές σχέσεις και πρώτα απ' όλα χωρίς μισθωτή

---

<sup>208</sup> The Mentor, 1986, 'The conscience of a hacker', *Phrack Magazine*, vol. 1, no. 7. Διαθέσιμο στο: <<http://www.phrack.org/issues.html?issue=7&id=3>>. [4 Αυγούστου 2008].

<sup>209</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα.

εργασία, χωρίς πατρίδες, βασισμένη στην ελεύθερη συνεργασία των παραγωγών χωρίς τάξεις, όπου η ελεύθερη ανάπτυξη του κάθε ένα αποτελεί όρο για την ελεύθερη ανάπτυξη όλων.<sup>210</sup>

Προσεγγίζοντας λοιπόν μαρξιστικά το θέμα, οι hackers είναι οι δημιουργοί και οι χρήστες της πληροφορίας. Στο αντίπαλο στρατόπεδο οι ανυσματοκράτες, αυτοί που παρεμποδίζουν την ελεύθερη και συνεργατική αξιοποίησή της<sup>211</sup>. Σύμφωνα λοιπόν μ' αυτή τη προσέγγιση, τους ανυσματοκράτες —όπως οι ανυσματοκράτες καπιταλιστές που περιγράφηκαν από τον Mackenzie Wark που αποκομίζουν τη δύναμή τους από τον έλεγχο των ανυσμάτων επικοινωνίας— αντιπροσωπεύουν οι σύγχρονοι υπερεθνικοί καπιταλιστές, οι διάφοροι κολοσσοί της αισχροκέρδειας με ηγέτη τον Bill Gates, ιδιοκτήτη της Microsoft Corporation. Στόχος τους είναι να δεσμεύσουν και να εμπορευματοποιήσουν την πληροφορία, παραβιάζοντας τον εθιμικό και άγραφο κώδικα της δωρεάς και του μοιράσματος στον οποίο στηρίχτηκε η ανάπτυξη του Διαδικτύου και τον οποίο ασπάζονται και θεσπίζουν οι hackers. Προσπαθούν να εφαρμόσουν το παλαιό βιομηχανικό καπιταλιστικό σύστημα της ιδιοκτησίας και της υπεραξίας στον χώρο της πληροφορίας επιβάλλοντας την πνευματική ιδιοκτησία<sup>212</sup>.

Αυτή τη στιγμή η κοινωνία του δυτικού κόσμου δικαιολογημένα χαρακτηρίζεται ως Κοινωνία της Πληροφορίας, καθώς το Διαδίκτυο ωθεί την ελεύθερη και μαζική κυκλοφορία της πληροφορίας και αυτός είναι ο λόγος που, παγκοσμίως, οι κυβερνήσεις και οι πολυεθνικές εταιρίες απελπισμένα μάχονται να «σκλαβώσουν» τη πληροφορία με τις πατέντες και τα copyrights<sup>213</sup>. Έτσι σήμερα αναδύεται μια τρίτη μορφή του καπιταλισμού, ο λεγόμενος «γνωστικός καπιταλισμός», ο οποίος προωθείται από αυτούς που ελέγχουν και εκμεταλλεύονται τη πληροφορία και τη γνώση. Όσο και αν μάχονται θα βρίσκουν πάντα απέναντι τους κυβερνοαντάρτες της ελεύθερης έκφρασης<sup>214</sup>.

---

<sup>210</sup> Molyneux, J. 1983, *What is the Real Marxist Tradition?*, Bookmarks, London

<sup>211</sup> Coleman, EG & Golub A 2008, 'Hacker practice: moral genres and the cultural articulation of liberalism', *Anthropological Theory*, vol. 8, no. 3, pp. 255-277. Διαθέσιμο στο: <[http://ciilibrary.org:8000/ciil/Fulltext/Anthropological\\_Theory/Vol\\_8\\_3\\_2008/Article\\_3.pdf](http://ciilibrary.org:8000/ciil/Fulltext/Anthropological_Theory/Vol_8_3_2008/Article_3.pdf)> [26 Αυγούστου 2008].

<sup>212</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα.

<sup>213</sup> Berry, DM & Moss, G 2005, 'The libre culture manifesto: a manifesto for free/libre culture', *Free Software Magazine*, no. 2, Μάρτιος Διαθέσιμο στο: <[http://tinrp.free.fr/empty/pages/things/libre\\_manifesto.pdf](http://tinrp.free.fr/empty/pages/things/libre_manifesto.pdf)> [10 Αυγούστου 2008].

<sup>214</sup> Soderberg, J 2002, 'Copyleft vs. copyright: a marxist critique', *First Monday Journal*, vol. 7, no. 3, 4 Μαρτίου. Διαθέσιμο στο: <[http://firstmonday.org/issues/issue7\\_3/soderberg/index.html](http://firstmonday.org/issues/issue7_3/soderberg/index.html)> [10 Αυγούστου 2008].



Ο Richard Stallman δηλώνει «...δεν πιστεύω ότι το λογισμικό θα έπρεπε να ανήκει σε κάποιον, γιατί η πρακτική αυτή σαμποτάρει την ανθρωπότητα σαν σύνολο. Εμποδίζει τους ανθρώπους να λάβουν το μέγιστο όφελος από την ύπαρξη του προγράμματος»<sup>215</sup>. Οι hackers αγωνίζονται για έναν νέο τρόπο κοινωνικής οργάνωσης που να διαμορφώνεται και να επεκτείνεται μέσα από τη μαζική εμπλοκή, τη συνεργασία, τη συλλογική δημιουργία και την άμεση συμμετοχή στη λήψη αποφάσεων πετυχαίνοντας επίσης τη συνεχή απελευθέρωση της πληροφορίας που θα μετασχηματίζεται σε γνώση και η γνώση σε ερέθισμα για επικοινωνία, συνεργασία και δημιουργία. Η απελευθέρωση της πληροφορίας είναι δεν είναι ανάγκη, είναι επιβολή του νέου τρόπου κοινωνικής οργάνωσης<sup>216</sup>.

Βλέποντας το θέμα λιγότερο θεωρητικά και περισσότερο πρακτικά και εμπειρισταωμένα θα γίνει αναφορά στην εξέλιξη του ελεύθερου λογισμικού. Το ελεύθερο λογισμικό, όπως ορίζεται από το Free Software Foundation, είναι λογισμικό που μπορεί να χρησιμοποιηθεί, αντιγραφεί, μελετηθεί, τροποποιηθεί και αναδιανεμηθεί χωρίς περιορισμό<sup>217</sup>. Το ελεύθερο λογισμικό πρεσβεύει τέσσερις θεμελιώδεις αρχές<sup>218</sup>:

- α) την ελευθερία να τρέξεις ένα πρόγραμμα χωρίς περιορισμούς στη χρήση του
- β) την ελευθερία να μελετήσεις τις εσωτερικές λειτουργίες ενός προγράμματος και να το προσαρμόσεις στις ανάγκες σου (για αυτό, η πρόσβαση στον πηγαίο κώδικα είναι προαπαιτούμενο στοιχείο)
- γ) την ελευθερία να διανέμεις αντίγραφα
- δ) την ελευθερία να βελτιώνεις το πρόγραμμα και να εκδίδεις τις βελτιώσεις του, έτσι ώστε να ωφελείται ολόκληρη η κοινότητα από αυτό.

Η ιστορία του ελεύθερου λογισμικού αποτελεί στην ουσία της την ιστορία της πάλης των τάξεων στην Κοινωνία της Πληροφορίας. Σήμερα το κίνημα των hackers αποτελεί συνέχεια του εργατικού αγώνα. Οι κεφαλαιοκράτες της ψηφιακής εποχής με την υποστήριξη του δικαίου της πνευματικής ιδιοκτησίας μοιράζονται τη γνώση, την πληροφορία που παράγεται στον ψηφιακό κόσμο. Η τάξη των hackers, που

---

<sup>215</sup> Levy, S 1984, *Hackers: heroes of the computer revolution*, Penguin Books, New York.

<sup>216</sup> Lakhani, K και Wolf, R G 2003, 'Why hackers do what they do: understanding motivation and effort in free/open source software projects', *MIT Sloan Working Paper No. 4425-03*. Διαθέσιμο στο: <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=443040](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=443040)> [10 Αυγούστου 2008].

<sup>217</sup> *FSF to host free software licensing seminars and discussions on SCO v. IBM in New York* 2004, Free Software Foundation. Διαθέσιμο στο: <<http://www.gnu.org/press/2004-01-02-nyc-seminars.html>> [12 Αυγούστου 2008].

<sup>218</sup> *Free Software Foundation and the GNU operation system* 2008, Free Software Foundation. Διαθέσιμο στο: <<http://www.fsf.org/about>> [12 Αυγούστου 2008].

δημιουργεί την παραγόμενη γνώση, είναι αναγκασμένη να προσφέρει την εργασία της και επομένως να εκχωρεί τα δικαιώματα πάνω στη δημιουργικότητά της στους κεφαλαιοκράτες για λόγους επιβίωσης<sup>219</sup>.

Στα τέλη της δεκαετίας του 1970 είναι η εποχή που οι εταιρείες διεισδύουν στην οικονομία του λογισμικού, πολλοί hackers διαπιστώνουν ότι είναι δέσμοι των αφεντικών. Πρώτος ο Stallman αποχωρεί από το MIT για να προστατεύσει την εκμετάλλευση της ιδέα του, το GNU Project. Οι hackers προς απάντηση σε αυτή την αισχροκέρδεια φτιάχνουν το δικό τους κόσμο, τα ελεύθερα λογισμικά, και επαναστατούν έναντι του υπάρχον άδικου συστήματος. Χτίζουν τεράστιες συνεργατικές μη-εμπορευματικές δημιουργίες, τις οποίες αποδίδουν απελευθερωμένες από ιδιοκτησία στο κοινωνικό σύνολο. Είναι η εξέγερση των νέων παραγωγικών δυνάμεων απέναντι στις παλαιές κεφαλαιοκρατικές σχέσεις παραγωγής. Το ελεύθερο λογισμικό είναι η επιβεβαίωση της μαρξιστικής άποψης ότι η μετακαπιταλιστική κοινωνία μπορεί να είναι μία παγκόσμια μη-εμπορική κοινωνία, και όχι μία γραφειοκρατική κοινωνία μισθωτής σκλαβιάς. Είναι μια πράξη αλτρουισμού και εθελοντισμού που χαίρει χειροκροτήματος<sup>220</sup>.

Αν και το ελεύθερο λογισμικό προέκυψε μέσα από την ανάπτυξη των τεχνολογιών που δημιουργήθηκαν μέσα στην καπιταλιστική παραγωγική λογική είναι ένα ανθρώπινο αγαθό που φτιάχτηκε για να δωριστεί. Το ελεύθερο λογισμικό μπορεί να αποτελεί μέσο παραγωγής και έχει τη νέα και ξεχωριστή ιδιότητα να αναπαράγεται με ελάχιστο κόστος. Πολλοί hackers δρουν χωρίς να το γνωρίζουν, με βάση κάποιες βασικές αρχές του Μαρξισμού<sup>221</sup>.

Δεν είναι τυχαίο ότι η ιστορία του ελεύθερου λογισμικού συμβαδίζει με την ιστορία του Διαδικτύου<sup>222</sup>. Το Διαδίκτυο είναι χτισμένο σε Unix τεχνολογία δικτύωσης σε μεγάλο βαθμό<sup>223</sup>. Η εμφάνιση του ελεύθερου λογισμικού συμπίπτει με τις απαρχές της εμπορευματοποίησης του λογισμικού. Στη δεκαετία του 1970, για πολλούς και ιδίως προσέλκυσαν τα λειτουργικά συστήματα των σπουδαστών hackers

---

<sup>219</sup> McKenzie, W 2006, *Ένα μανιφέστο των hacker*, Scripta, Αθήνα/

<sup>220</sup> Keltly, CM 2004, 'Culture's open sources: software, copyright, and cultural critique', *Anthropological Quarterly*, vol. 77, no. 3, pp. 499-506. Διαθέσιμο στο: Project Muse [14 Αυγούστου 2008].

<sup>221</sup> Harold F & Tipton, MK 2007, *Information security management handbook*, 6<sup>th</sup> ed. CRC Press, Boca Raton.

<sup>223</sup> Cramer, F 2000, *Free software as collaborative text*. Διαθέσιμο στο: <[http://java.khm.de/content/pdf/free\\_software\\_as\\_text.pdf](http://java.khm.de/content/pdf/free_software_as_text.pdf)> [14 Αυγούστου 2008].

κοινοτήτων στο MIT και του Πανεπιστημίου Berkeley της Καλιφόρνια<sup>224</sup>. Οι έννοιες της ανοικτής, αποκεντρωμένης και της ελεύθερης λειτουργίας πολλών δικτύων υπολογιστών έχουν την καταγωγή τους στην επιστήμη των υπολογιστών που αναπτύχθηκε στα εργαστήρια των ιδρυμάτων αυτών<sup>225</sup>. Μέχρι τέλη 1970 η ελεύθερη ανταλλαγή, σπουδή και βελτίωση των λογισμικών θεωρούταν σχεδόν αυτονόητη.

Από τις αρχές του 1980 οι εταιρείες προχωρούν στην εμπορευματοποίηση των λογισμικών, δρουν πίσω από την μάσκα του δικαίου πνευματικής ιδιοκτησίας και δημιουργούν τη νέα αγορά λογισμικού. Η πρακτική αυτή ανατρέπει την προγενέστερη, αυτή δηλαδή της συνεργασίας και της ελεύθερης ανταλλαγής υλικού. Στις αρχές της δεκαετίας του 1980, ο Richard Stallman αποφασίζει να αντιδράσει στο νέο κατεστημένο και να μοιραστεί τη γνώση του με τον υπόλοιπο κόσμο. Δημιούργησε την αρχή του “free software” (ελεύθερου λογισμικού), ενώ το 1985 ο Stallman δημοσιεύει το «GNU Μανιφέστο», στο οποίο διακηρύττει την πρόθεσή του να εκδώσει το GNU ως ελεύθερο λογισμικό και ιδρύει το Free Software Foundation.

Μέσα στην κοινότητα των hackers αρχίζει να δημιουργείται η ιδέα του η copyleft, ως απάντηση στο copyright (all rights reversed)<sup>226</sup>. Το copyleft είναι ο όρος που περιγράφει κάθε άδεια χρήσης πνευματικού έργου, με την οποία ο δημιουργός επιτρέπει την ελεύθερη χρήση, αναπαραγωγή, τροποποίηση και βελτίωση του έργου, υπό τον όρο ότι κάθε νέα τροποποιημένη και βελτιωμένη έκδοση αυτού θα εκδίδεται με την ίδια άδεια.

Ακόμα ένα επίτευγμα και μία απάντηση στην καταπίεση της πνευματικής ιδιοκτησίας και της εμπορευματοποίησης της γνώσης δίνει ο Φιλανδός Linus Torvalds το 1991 δημιουργώντας τον πρόγονο του Linux και το 1992 υπό την άδεια χρήσης GPL δημοσιεύει το πρόγραμμα. Απελευθέρωσε αρχικά το Linux με άδεια που επέτρεπε την ανακατανομή, με την προϋπόθεση ότι ο κωδικός πηγής να παρέχεται

---

<sup>224</sup> Hars, A & Ou, S. 2002, ‘Working for free? motivations of participating in open source projects’, *International Journal of Electronic Commerce*, vol. 6, no. 3, pp. 25-39. Διαθέσιμο στο: <<http://mesharpe.metapress.com/app/home/contribution.asp?referrer=parent&backto=searcharticles&results,1,1;>> [14 Αυγούστου 2008].

<sup>225</sup> Cramer, F 2000, *Free software as collaborative text*, CodeKit. Διαθέσιμο στο: <[http://java.khm.de/content/pdf/free\\_software\\_as\\_text.pdf](http://java.khm.de/content/pdf/free_software_as_text.pdf)> [14 Αυγούστου 2008].

<sup>226</sup> Soderberg, J 2002, ‘Copyleft vs. copyright: a marxist critique’, *First Monday Journal*, vol. 7, no. 3, 4 Μαρτίου. Διαθέσιμο στο: <[http://firstmonday.org/issues/issue7\\_3/soderberg/index.html](http://firstmonday.org/issues/issue7_3/soderberg/index.html)> [10 Αυγούστου 2008].

χωρίς κόστος<sup>227</sup>. Το 1999 εκδίδεται για πρώτη φορά το βασικό γραφικό περιβάλλον του Linux, το Gnome.

Στις 23 Μάιου 1995 κάνει τη εμφάνιση του για πρώτη φορά το πιο δημοφιλές ελεύθερο λογισμικό για τη δημιουργία βάσεων δεδομένων, το λογισμικό MySQL, με 11 εκατομμύρια εγκαταστάσεις σήμερα. Η MySQL είναι ένα πολύ γρήγορο και δυνατό, σύστημα διαχείρισης βάσεων δεδομένων<sup>228</sup>. Στις 26 Φεβρουαρίου 2008 η MySQL αγοράζεται από τη Sun Microsystems για 1 δισεκατομμύριο δολάρια<sup>229</sup>. Ταυτόχρονα, εμφανίζεται η γλώσσα προγραμματισμού JAVA που χρησιμοποιείται σε περισσότερες από 20 εκατομμύρια δυναμικές ιστοσελίδες.

Το 1998 ιδρύεται το Open Source Initiative που αντιπροσωπεύει μια πιο εμπορική εκδοχή και τάση του κινήματος του ελεύθερου λογισμικού. Το OSI υποστηρίζει ότι η διαθεσιμότητα του κώδικα ενός προγράμματος προωθεί την εξέλιξή του. Αυτός είναι κι ο λόγος που δεν πρέπει να συγχέεται το Open Source & Free Software με το "freeware". Ο όρος freeware χρησιμοποιείται συνήθως για προγράμματα που δίνονται δωρεάν μόνο σε εκτελέσιμη μορφή χωρίς πρόσβαση στον κώδικα του προγράμματος.

Ο Stanford Lawrence Lessig βασισμένος στην ιδέα του copyleft, ιδρύει το 2001 το ίδρυμα Creative Commons<sup>230</sup>. Δημιουργεί άδειες χρήσης για κάθε είδος πνευματικής δημιουργίας. Το ίδρυμα Creative Commons (CC), που δημιουργήθηκε στις Η.Π.Α, ανέπτυξε νομικά και τεχνολογικά την ιδέα των αδειών χρήσης και άλλων προϊόντων και συγγενικών δικαιωμάτων πνευματικής ιδιοκτησίας και είναι μια μη κερδοσκοπική οργάνωση αφιερωμένη στην επέκταση του εύρους των πνευματικών έργων που είναι διαθέσιμα για να βασιστούν σε αυτά και άλλα έργα και να μοιραστούν νόμιμα. Η οργάνωση έχει εκδώσει διάφορες άδειες πνευματικών δικαιωμάτων γνωστές ως άδειες Creative Commons. Αυτές οι άδειες επιτρέπουν στους δημιουργούς να δηλώσουν εύκολα ποια δικαιώματα διατηρούν και ποια

---

<sup>227</sup> O' Sullivan, M 2002, 'Making copyright ambidextrous: an expose of copyleft', *The Journal of Information, Law and Technology*, no. 3. Διαθέσιμο στο: <[http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002\\_3/osullivan](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_3/osullivan)> [16 Αυγούστου 2008].

<sup>228</sup> *MySQL* 2009, MySQL AB Sun Microsystems. Διαθέσιμο στο: <<http://www.mysql.com>> [16 Αυγούστου 2008].

<sup>229</sup> O' Brien, KJ 2008, 'Sun buying swedish software firm for \$1 billion', *The New York Times*, 16 Ιανουαρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2008/01/17/technology/17sun.html?scp=4&sq=MySQL%20Sun%20Microsystems%20&st=cse>> [16 Αυγούστου 2008].

<sup>230</sup> Conhaim, WW 2002, 'Creative commons nurtures the public domain' *Information Today*, 3 Ιουνίου. Διαθέσιμο στο: <<http://newsbreaks.infotoday.com/nbreader.asp?ArticleID=17167>> [19 Αυγούστου 2008].

δικαιώματα παραμερίζουν προς όφελος άλλων δημιουργών<sup>231</sup>. Η δημιουργία και τα βασικά δομικά χαρακτηριστικά των αδειών Creative Commons οιστρηλατήθηκαν από την General Public License.

Ως πηγή έμπνευσης για τη δημιουργία των Creative Commons αποτέλεσε το περιεχόμενο επιστολής του τρίτου Προέδρου των Ηνωμένων Πολιτειών Thomas Jefferson προς τον Isaac McPherson τον Αύγουστο του 1813 όπου αναφέρεται «...αυτός που λαμβάνει μια ιδέα από εμένα, εμπνέεται χωρίς εγώ να χάνω την ιδέα. Αυτός που ανάβει το κερί του από το δικό μου, φωτίζεται χωρίς να με συσκοτίζει»<sup>232</sup>. Ο Stanford Lawrence Lessig θεωρεί ότι «...ένας πολιτισμός στον οποίο οι δημιουργοί μπορούν να δημιουργήσουν μόνο με την άδεια του ισχυρού είναι παρελθόν»<sup>233</sup>. Υποστηρίζει ότι ο σύγχρονος πολιτισμός εξουσιάζεται από τους παραδοσιακούς διανομείς προκειμένου να διατηρηθούν και να ενισχυθούν τα μονοπώλιά τους στα πολιτιστικά προϊόντα, όπως η μουσική και ο κινηματογράφος, και ότι η Creative Commons μπορεί να παρέχει εναλλακτικές λύσεις σε αυτούς τους περιορισμούς<sup>234</sup>.

Τον Ιανουάριο του 2006 η κυβέρνηση της Βενεζουέλας προχωράει ταχύτατα προς την υιοθέτηση του ελεύθερου λογισμικού. Ψηφίζει νόμο σύμφωνα με τον οποίο όλες οι δημόσιες υπηρεσίες της χώρας θα πρέπει εντός δύο χρόνων να μεταφέρουν τις υποδομές τους σε ελεύθερα λογισμικά. Ο Hugo Chaves, Πρόεδρος της χώρας, δήλωσε ότι η επιλογή αυτή ακολουθεί την αρχή της εθνικής επιστημονικής ανεξαρτησίας και την απεξάρτηση από λογισμικά που ανήκουν σε ιδιωτικά συμφέροντα<sup>235</sup>.

Σε αντίθεση με τα διεθνή παραδείγματα μεταστροφής προς τη χρήση του ελεύθερου κι ανοικτού λογισμικού, η ελληνική πολιτεία έχει υπογράψει μνημόνιο αποκλειστικής συνεργασίας με την Microsoft για όλο το δημόσιο τομέα δυσχεραίνοντας την αποδέσμευσή της από μονοπωλιακές πρακτικές, ενώ παράλληλα

---

<sup>231</sup> Seadle, M 2005, 'Copyright in the networked world: author's rights', *Library Hi Tech*, vol. 23, no. 1, pp. 130–136. Διαθέσιμο στο: Emerald [19 Αυγούστου 2008].

<sup>232</sup> Walterscheid, EC 1998, 'Thomas Jefferson and the patent act of 1793', *Essays in History*, vol. 40, Corcoran Department of History, University of Virginia. Διαθέσιμο στο: <<http://etext.virginia.edu/journals/EH/EH40/walter40.html>> [19 Αυγούστου 2008].

<sup>233</sup> Lessig, L 2001, *The future of ideas*, Random House, New York.

<sup>234</sup> Lawrence, L 2004, *Free culture: how big media uses technology and the law to lock down culture and control creativity*, The Penguin Press, New York. Διαθέσιμο στο: <<http://www.free-culture.cc/freeculture.pdf>> [26 Αυγούστου 2008].

<sup>235</sup> Cleto AS 2004, 'Venezuela embraces linux and open source software, but faces challenges', *Venezuelanalysis.com*, 8 Δεκεμβρίου. Διαθέσιμο στο: <<http://www.venezuelanalysis.com/news/827>> [26 Αυγούστου 2008].

απομονώνεται από τη διεθνοποιημένη τάση της συμπόρευσης προς την ελεύθερη διακίνηση.

Το 2007 η Sun εκδίδει την πλατφόρμα Java υπό τη GPL. Ταυτόχρονα, η Microsoft μπαίνει και αυτή στο παιχνίδι σημειώνοντας στροφή στη στρατηγική της απέναντι στο κίνημα περνώντας από την ολότελα εχθρική στάση σε μία ιδιότυπη προσπάθεια διάσπασης των κοινοτήτων, π.χ. συνεργασία με Novell.

Η ανάπτυξη του ελευθέρου και ανοικτού λογισμικού δεν είναι η τέλεια, επειδή, προφανώς, έχουν τις ελλείψεις τους και σφάλματα τους. Ωστόσο η ως τώρα ιστορία του ελεύθερου λογισμικού έχει εισαγάγει έννοιες που είναι δυνητικά χρήσιμες για την ενίσχυση των μεγάλων έργων λογισμικού, που αποτελείται εκατομμύρια γραμμές κώδικα να εξελίσσονται και αναπτύσσονται με υγιή τρόπο<sup>236</sup>. Σήμερα το ελεύθερο λογισμικό αποτελεί ένα παγκόσμιο φαινόμενο, που αλλάζει τα δεδομένα στον ψηφιακό κόσμο. Ελεύθερα και δωρεάν για όλους. Η χρήση του τόσο στον ιδιωτικό εμπορικό τομέα όσο και στο δημόσιο κρατικό επεκτείνεται με την προοπτική να υπερκεράσει τα εμπορευματικά λογισμικά. Αρχίζει μία εποχή όπου το «δωρεάν» και το «ελεύθερο» δεν θεωρούνται απλώς αναγκαία, αλλά αυτονόητα. Μετά το ελεύθερο λογισμικό ήρθε η ελεύθερη πρόσβαση στη γνώση που, έστω ερασιτεχνικά ακόμα, τρανταχτό παράδειγμα η Wikipedia<sup>237</sup>.

Στον κόσμο είναι εγκατεστημένοι και λειτουργούν περίπου ένα δισεκατομμύριο υπολογιστές. Το 90% από αυτούς λειτουργεί με Windows, ένα ποσοστό τρία με τέσσερα τοις εκατό με Macintosh και το υπόλοιπο με Linux. Μελλοντικά, στην επόμενη πενταετία οι υπολογιστές προβλέπεται να διπλασιαστούν με τις εκτιμήσεις να υποδεικνύουν ότι η σημερινή κατάσταση θα αντιστραφεί. Το 90% θα λειτουργεί με ελεύθερο λογισμικό και αυτό θα συμβεί για καθαρά τεχνικούς και επιχειρηματικούς λόγους<sup>238</sup>.

Το παραγωγικό μοντέλο του ελεύθερου λογισμικού ήδη χρησιμοποιείται σε άλλους τομείς της άυλης οικονομίας με επιτυχία και με την προοπτική να επεκταθεί στο σύνολό της. Ο Stallman και οι GNU άνθρωποι του κινήματος ελεύθερου

---

<sup>236</sup> Bauer, A & Pizka, M 2003, 'The contribution of free software to software evolution', *Proceedings of the international workshop on principles of software evolution*, pp 1-10. Διαθέσιμο στο: <<http://www4.informatik.tu-muenchen.de/publ/papers/mp03f.pdf>> [26 Αυγούστου 2008].

<sup>237</sup> Coleman, EG & Golub A 2008, 'Hacker practice: moral genres and the cultural articulation of liberalism', *Anthropological Theory*, vol. 8, no. 3, pp. 255-277. Διαθέσιμο στο: <[http://ciillibrary.org:8000/ciil/Fulltext/Anthropological\\_Theory/Vol\\_8\\_3\\_2008/Article\\_3.pdf](http://ciillibrary.org:8000/ciil/Fulltext/Anthropological_Theory/Vol_8_3_2008/Article_3.pdf)> [26 Αυγούστου].

<sup>238</sup> Νταραδήμου, Α 2008, 'Ελεύθερο λογισμικό', *Ελεύθερος Τύπος*, 2 Μαΐου. Διαθέσιμο στο: <<http://www.e-tipos.com/newsitem?id=34547>> [6 Αυγούστου 2008].

λογισμικού θέλουν να απελευθερώσουν όχι μόνο το λογισμικό, αλλά και τη μουσική και τα βιβλία από ιδιόκτητες άδειες. Σε μια συνέντευξη στο Spiegel Online ο Stallman εξηγεί ότι «...τείνω προς την αριστερής κατεύθυνσης αναρχική ιδέα ότι θα πρέπει εθελοντικά να βρεθούμε μαζί και να σκεφτούμε πως μπορούμε μέσω της συνεργασίας να φροντίσουμε για όλους»<sup>239</sup>.

Η ελεύθερη διακίνηση της πληροφορίας στο Διαδίκτυο, το κίνημα του ελεύθερου λογισμικού, η συλλογική εργασία για δημιουργία και η δωρεάν ανταλλαγή αρχείων έχουν δημιουργήσει έντονες συζητήσεις και διχασμούς. Η απόλυτη ελευθερία και η άνθηση της δημιουργικότητας επηρέασε κι άλλους τομείς της δημιουργίας, όχι μόνο την κοινότητα των ηλεκτρονικών υπολογιστών. Ο Ντενί Ολιβέν, γάλλος συγγραφέας, σε ένα δοκίμιό του υποστηρίζει ευθαρσώς ότι «κλοπή είναι το δωρεάν» παραφράζοντας την πρόταση «η ιδιοκτησία είναι κλοπή». Σύμφωνα με τον Ντενί Ολιβέν, η δωρεάν διάθεση του άυλου πολιτισμικού προϊόντος αντισταθμίζει απλώς την εμπορική διάθεση του υλικού τεχνολογικού προϊόντος. Κλέβει, δηλαδή, από τους δημιουργούς και ενισχύει τις εταιρείες. Ή μήπως απλώς αφαιρεί κέρδη από τις εταιρείες πολιτισμικής παραγωγής και διακίνησης προς όφελος των εταιρειών τεχνολογίας; Και η ανταμοιβή του δημιουργού είναι το τελευταίο ζητούμενο;<sup>240</sup>

Η αντιπαράθεση αυτή εντάσσεται στη γενικότερη διαμάχη των οπαδών της ελεύθερης διακίνησης της πληροφορίας στο Διαδίκτυο, δηλαδή των hackers και των υποστηρικτών της εμπορευματοποίησής των πληροφοριών, δηλαδή των μεγάλων εταιριών, τους εκδότες, τους υπεράκτιους οργανισμούς. Η μια πλευρά προσπαθεί και μάχεται για ανανέωση και επανάσταση θεσπίζοντας την ελεύθερη ανταλλαγή πληροφοριών και προσπαθώντας με συλλογική δουλειά να φτάσουν στο ζενίθ της τεχνολογίας και της γνώσης. Η άλλη πλευρά προσπαθεί να δαμάσει την τεχνολογία και να την προσαρμόσει δεσποτικά στα παλαιά σχήματα<sup>241</sup>. Η συζήτηση για τα πνευματικά δικαιώματα είναι μακροσκελής και θα μπορούσε να αποτελέσει αντικείμενο ξεχωριστής έρευνας. Ο σκοπός που θίγω αυτό το θέμα ήταν για να αναφερθώ στο βιβλίο και κατά πόσο αυτό επηρεάζεται από την νέα τάξη πραγμάτων.

---

<sup>239</sup> Imhorst, C 2005, *Anarchy and source code: what does the free software movement have to do with anarchism?*, Free/Open Source Research Community. Διαθέσιμο στο: <<http://freesoftware.mit.edu/papers/imhorst.pdf>> [26 Αυγούστου 2008].

<sup>240</sup> Olivennes, D 2007, *La gratuité, c'est le vol: quand le piratage tue la culture*, Grasset & Fasquelle, Paris.

<sup>241</sup> Bauer, A & Pizka, M 2003, 'The contribution of free software to software evolution', *Proceedings of the international workshop on principles of software evolution*, pp 1-10. Διαθέσιμο στο: <<http://www4.informatik.tu-muenchen.de/publ/papers/mp03f.pdf>> [26 Αυγούστου 2008].

Το βιβλίο παραμένει ανεπηρέαστο μέχρι στιγμής σε αυτή την μάχη των πνευματικών δικαιωμάτων και της απελευθέρωσης της πληροφορίας. Ίσως λόγω της μοναδικότητας του, το βιβλίο δεν δέχεται τις επιδράσεις αυτής της διαμάχης σε αντίθεση βέβαια με την μουσική βιομηχανία. Το αξιοσημείωτο είναι ότι ο λογοτεχνικός θεσμός δεν μοιάζει να μετασχηματίζεται με τους ίδιους ρυθμούς όπως η μουσική ή η κινηματογραφική βιομηχανία.

Το βιβλίο με την πάροδο της τεχνολογίας εξελίσσεται και από χαρτί και κόλλα μετατρέπεται σε ασύρματη συσκευή ανάγνωσης. Φυσικά χωρίς το δεύτερο να καταργεί το πρώτο. Ο νέος e-book reader ακούει στο όνομα Amazon, ενώ φαίνεται ότι το τρίτης γενιάς ηλεκτρονικό βιβλίο επαναφέρει στο προσκήνιο το βιβλίο ως αρχείο με νέες προοπτικές. Φυσικά η εποχή όμως όπου οι συγγραφείς θα διαθέτουν οι ίδιοι το βιβλίο τους μόνο μέσω Διαδικτύου είναι ακόμα σχεδόν ουτοπική.

Πολλοί hackers μπορεί να αγνοούν τον μαρξισμό ή ίσως τον συχέουν με τον σταλισμό. Αυτό που έχει συμασία είναι ότι σε κάποιο βαθμό, δουλεύουν με μαρξιστικό τρόπο όταν αναπτύσσουν ελεύθερο λογισμικό, πιθανόν χωρίς οι ίδιοι να το γνωρίζουν. Το πιο σημαντικό είναι ότο το επιδιόκουν, αρέσκονται στην ομαδική εργασία, την αλληλοβοήθεια, την ελεύθερη ανταλλαγή ιδεών για την επίτευξη ενός κοινού στόχου.<sup>242</sup> Το ελεύθερο λογισμικό μεγαλώνει την παρουσία του στην κοινωνική ζωή και το ερώτημα είναι αν η κοινωνία είναι ενημερομένη και έτημη να το δεκτεί.

Σίγουρο είναι ότι νησίδες ελευθερίας δεν υπάρχουν μέσα στο καπιταλιστικό σύστημα χωρίς τάσεις εκφυλισμού. Υπάρχει όμως ένα εχέγγυο, λόγω του οποίου το φαινόμενο του ελεύθερου λογισμικού θα έχει τη δυνατότητα να ανθίσταται, όσο και αν παρουσιάζει τάσεις εκφυλισμού προς την εμπορευματοποίηση. Αυτό το εχέγγυο είναι η αρχή της συνεργατικής δημιουργίας, πάνω στην οποία όλο το οικοδόμημα του ελεύθερου λογισμικού βασίζεται. Τα μέλη της κοινότητας του ελεύθερου λογισμικού αλλάζουν τον κόσμο και η κοινωνία έχει πολλά οφέλει από αυτή την ριζική αλλαγή.<sup>243</sup>

---

<sup>242</sup> Cross, T. 2006, 'Academic freedom and the hacker ethic', *Communications of the ACM*, vol. 49, no. 6. Διαθέσιμο στο: ACM Digital Library [27 Αυγούστου 2008].

<sup>243</sup> Μπουντουρίδης, Μ 2006, Κριτική της εργασίας στην κοινωνία της πληροφορίας. 21 Αυγούστου 2006. *Κοινωνικά Κινήματα & Δίκτυα: Blog*. Διαθέσιμο στο: <<http://thrymmata.blogspot.com/2006/08/blog-post.html>> [27 Αυγούστου 2008].



## **ΚΕΦΑΛΑΙΟ 5:**

### **ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ, ΟΙ ΑΔΕΙΕΣ CREATIVE COMMONS ΚΑΙ ΤΟ ΕΛΕΥΘΕΡΟ ΛΟΓΙΣΜΙΚΟ ΣΤΑ ΑΚΑΔΗΜΑΪΚΑ ΙΔΡΥΜΑΤΑ ΚΑΙ ΤΙΣ ΒΙΒΛΙΟΘΗΚΕΣ**

Υπάρχει μια επιθυμία εκ μέρους των ακαδημαϊκών να αλλάξουν την ισορροπία των δικαιωμάτων μέσα στα πνευματικά δικαιώματα μεταξύ των συντακτών και των εκδοτών στα επιστημονικά περιοδικά επικοινωνίας. Οι βιβλιοθήκες και τα ακαδημαϊκά ιδρύματα συμμετέχουν ήδη στην επιστημονική συζήτηση πνευματικών δικαιωμάτων επικοινωνίας και θα μπορούσαν να χρησιμοποιήσουν αυτά τα αποτελέσματα για να ευθυγραμμίσουν τις θέσεις τους με τις απόψεις των ακαδημαϊκών

Τα ακαδημαϊκά ιδρύματα και οι βιβλιοθήκες έχουν ως κυρίαρχο στόχο τη διάδοση πληροφοριών και τη συλλογή ύλης για την δημιουργία της γνώσης. Με τους φραγμούς των πνευματικών δικαιωμάτων η λειτουργία αυτών των ιδρυμάτων δυσχεραίνεται.

Οι βιβλιοθήκες και οι άδειες Creative Commons έχουν ταύτιση στόχων. Στοχεύουν και οι δύο στη διατήρηση, ανανέωση και διάδοση του υλικού τους. Τα χαρακτηριστικά των αδειών Creative Commons υποστηρίζουν αυτού του είδους τις χρήσεις. Έτσι οι βιβλιοθήκες και τα αρχεία έχουν δείξει ιδιαίτερο ενδιαφέρον για τη διάδοση έργων με άδειες των Creative Commons.

Οι νέες τεχνολογίες έχουν επηρεάσει τη λειτουργία των βιβλιοθηκών που εκτός από βιβλία και έντυπο υλικό, παρέχουν στο κοινό μία πληθώρα γνωστικών μέσων και σύγχρονων τρόπων πρόσβασης στην πληροφορία όπως ηλεκτρονικές εκδόσεις, φωτογραφίες, χάρτες, χειρόγραφα, επιστολές, βιντεοταινίες, φωνογραφήματα, slides, cd-rom, εκπαιδευτικό λογισμικό, βάσεις δεδομένων, οπτικοακουστικά μέσα, online συνδέσεις σε δίκτυα. Η τάση να ψηφιοποιείται η γνώση και οι νέες τεχνολογικές δυνατότητες επιτάσσουν μια άμεση ανανέωση στον χώρο των πνευματικών δικαιωμάτων και την προσαρμογή τους στα νέα δεδομένα. Το ψηφιακό δίλημμα και η τεχνολογική πρόκληση οδήγησαν σε πρωτοποριακές αναζητήσεις και προτάσεις με στόχο τον επαναπροσδιορισμό της πνευματικής ιδιοκτησίας. Οι βιβλιοθήκες και τα αρχεία που επιτελούν ένα ρόλο κυρίως εκπαιδευτικό και πολιτιστικό αντιμετωπίζουν πολλές φορές δυσκολίες σε θέματα που έχουν σχέση με τα πνευματικά δικαιώματα,

τόσο στον αναλογικό όσο και στον ψηφιακό τομέα. Οι Creative Commons φαίνεται να είναι μια λυτρωτική λύση και η νέα θεώρηση της πνευματικής ιδιοκτησίας<sup>244</sup>.

Με την χρήση των Creative Commons οι βιβλιοθήκες και τα ακαδημαϊκά ιδρύματα μπορούν να διεξάγουν το έργο τους πληρέστερα, και η πρόσβαση στην επιστημονική έρευνα να γίνεται καλύτερα με τη διανομή των πνευματικών δικαιωμάτων στην επαναχρησιμοποίηση των επιστημονικών πληροφοριών για εκπαιδευτικούς και επιστημονικούς λόγους. Στον ελεύθερο αυτό κόσμο, η έννοια της ιδιοκτησίας δεν είναι στη διαδικασία του αποκλεισμού αλλά της διάθεσης.

Οι βιβλιοθήκες λόγω του λειτουργικού τους πυρήνα (οίκος της γνώσης) οφείλουν να υποστηρίζουν αυτή την νέα κουλτούρα ελευθερίας που γεννήθηκε μέσα από την κοινότητα των hackers. Σκοπός και των δύο είναι η εύκολη πρόσβαση στη γνώση και η ελεύθερη ροή των πληροφοριών.

Η μεταφορά των αδειών Creative Commons όσο και η εφαρμογή των αδειών Ελευθέρου Λογισμικού / Ανοικτού Κώδικα –π.χ. GNU General Public License & Lesser General Public License (GPL & LGPL— στην ελληνική έννομη τάξη κρίνεται απαραίτητη<sup>245</sup>. Στον ελληνικό χώρο ο πρώτος συγγραφέας που χρησιμοποίησε της άδειες Creative Commons είναι ο Μίμης Ανδρουλάκης στο έργο του «Το χαμένο μπλουζ και don't look back»<sup>246</sup>.

Το ελεύθερο λογισμικό άρχισε να χρησιμοποιείται ευρέως στον δημόσιο τομέα κατά συνέπεια και στις βιβλιοθήκες. Εξαιτίας των χαρακτηριστικών του είναι ένα εναλλακτικό μοντέλο ανάπτυξης και χρήσης λογισμικού. Παρέχει τη δυνατότητα αλλαγών ή βελτιώσεων ώστε να καλύπτονται οι ανάγκες αυτού που το χρησιμοποιεί. Η λειτουργική του διαφάνεια δίνει τη δυνατότητα για διορθώσεις του κώδικα μέχρι και την τελειοποίηση του, ώστε να καλύψει τις ανάγκες του εκάστοτε οργανισμού. Με βάση αυτή τη φιλοσοφία δημιουργήθηκε μια μεγάλη κοινότητα χρηστών και προγραμματιστών, οι οποίοι συνεργάζονται για τη συνεχή βελτίωση του λογισμικού, παρέχοντας γνώσεις και εργασία. Σήμερα λειτουργεί ένα παγκόσμιο ανοικτό δίκτυο προγραμματιστών, οι οποίοι παράλληλα αναπτύσσουν και διορθώνουν τον κώδικα

---

<sup>244</sup> Fitzgerald, B (ed.) 2007, *Open content licensing: cultivating the creative commons*, Sydney University Press, Sydney.

<sup>245</sup> Καλλινίκου, Δ, Καρούνος, Θ & Παπαδόπουλος, Μ 2007, 'Οι ελληνοποιημένες άδειες creative commons', *Πρακτικά από το δέκατο έκτο πανελλήνιο συνέδριο ακαδημαϊκών βιβλιοθηκών*. Διαθέσιμο στο: <<http://www.marinos.com.gr/bbpdf/pdfs/msg63.pdf>> [13 Αυγούστου 2008].

<sup>246</sup> *Ο Μίμης Ανδρουλάκης διαθέτει ελεύθερα το βιβλίο του "Χαμένο Μπλουζ" με άδεια Creative Commons* 2008, Creative Commons. Διαθέσιμο στο : <[http://www.creativecommons.gr/news/newsvieeach/index.php?ctn=7&context\\_url=0P7UnewsvieeachCSFall&page=0&language=el](http://www.creativecommons.gr/news/newsvieeach/index.php?ctn=7&context_url=0P7UnewsvieeachCSFall&page=0&language=el)> [13 Αυγούστου 2008].

των προγραμμάτων, κυκλοφορώντας ταχύτατα νέες βελτιωμένες εκδόσεις λογισμικού. Με αυτό τον τρόπο συμβάλλουν καθημερινά στη δημιουργία νέων κοινών αγαθών<sup>247</sup>.

Το λογισμικό ανοικτού κώδικα με τις συνεχείς βελτιώσεις και την αυξημένη πλέον φιλικότητα προς το χρήστη χρησιμοποιείται όλο και από περισσότερους ανθρώπους. Στην εκπαίδευση, στη δημόσια διοίκηση και στις επιχειρήσεις, οι ενδιαφερόμενοι ενημερώνονται και αποκτούν λογισμικό απαλλαγμένο από τα σημαντικά κόστη αγοράς και συνεχούς αναβάθμισης που απαιτούν τα κλειστά λογισμικά. Πολλές βιβλιοθήκες σήμερα χρησιμοποιούν το ανοικτό λογισμικό όπως για παράδειγμα το Greenstone για τη δημιουργία ψηφιακής βιβλιοθήκης ή το πρόγραμμα αυτοματοποίησης βιβλιοθηκών Koha.

### 5.1 Οι επιδράσεις του hacking στην κοινωνία

Οι υγιείς εκδηλώσεις του hacking επηρεάζουν άμεσα την κοινωνία καθώς και τους ίδιους τους hackers. Σε αυτή την περίπτωση το θετικό και το αρνητικό δεν είναι απόλυτα διακριτά. Και γι' αυτό η τοποθέτηση πάνω στο θέμα δεν μπορεί να είναι απόλυτη. Το θεμιτό και το αθέμιτο είναι δύο υποκειμενικοί όροι και επηρεάζονται άμεσα από την σκοπιά που βλέπει κανείς το πρόβλημα. Τα όρια της θεμιτότητας είναι άμεσα επενεργούντα από την αντίληψη του ατόμου που κρίνει την πράξη. Το ενδιαφέρον θα εστιαστεί κυρίως στους άσπρους hackers (white hat hackers) και τους γκριζούς hackers (grey hat hackers) γιατί παρουσιάζουν ιδιαίτερο κοινωνικοπολιτικό ενδιαφέρον<sup>248</sup>.

Οι hackers έχουν συνεισφέρει πολλά στην παγκόσμια ηλεκτρονική ασφάλεια. Ανακαλύπτοντας τα κενά ασφάλειας των συστημάτων, τα τρωτά σημεία και τις αδυναμίες ενός συστήματος ασφάλειας βοηθούν τις εταιρείες ασφάλειας υπολογιστών. Δημοσιεύουν αυτές τις πληροφορίες πριν αυτές εκμεταλλευτούν από συγγραφείς ιών και μαύρους hackers (black hat hackers). Ενημερώνουν τους διαχειριστές και το κοινό για αυτά τα κενά και ευαισθητοποιούν τον κόσμο σχετικά με την ασφάλεια. Διευκολύνουν τους διαχειριστές ασφάλειας υπολογιστών απαλλάσσοντας τους από τον κόπο να ανακαλύψουν μόνοι τους τις αδυναμίες του

---

<sup>247</sup> Ανδρέου, ΑΚ 2008, Ελεύθερο Λογισμικό / Λογισμικό Ανοικτού Κώδικα (ΕΛ/ΛΑΚ). 14 Μαρτίου 2008. *Η βιβλιοθηκονομία στην Κύπρο σήμερα: Blog*. Διαθέσιμο στο: <[http://kebep.blogspot.com/2008/03/blog-post\\_14.html](http://kebep.blogspot.com/2008/03/blog-post_14.html)> [13 Αυγούστου 2008].

<sup>248</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

συστήματος. Αποδεικνύουν ότι με την έρευνα και τις γνώσεις μπορούμε να βελτιώσουμε την τεχνολογία σε βαθμό που παλιά θεωρείτο αδύνατος και με ταχύτατους ρυθμούς. Έτσι οι εταιρείες υποχρεώνονται να διορθώνουν και να βελτιώνουν τα λογισμικά τους. Πολλές φορές το κυνήγι αυτής της γνώσης θεωρείται παράνομο<sup>249</sup>. Ένα δίκτυο hackers που εργάζεται για την ασφάλεια των υπολογιστών είναι το Nomad Mobile Research Center (NMRC)<sup>250</sup>.

Οι hacker απορρίπτουν την ιδέα ότι η άγνοια σε κάνει ασφαλέστερο. Στη δεκαετία του 1980, όταν τα δίκτυα υπολογιστών μεγάλωσαν, τα προβλήματα ασφάλειας υπολογιστών μεγάλωσαν μαζί τους. Οι πωλητές, οι δημόσιοι οργανισμοί και τα πανεπιστημιακά εργαστήρια λογισμικού κρατούν μυστικές τις ευπάθειες του λογισμικού τους από το ευρύ κοινό. Οι πρώτοι άνθρωποι που συζήτησαν ανοιχτά τις ευπάθειες των υπολογιστών άνηκαν στην κοινότητα των hackers. Αντιμετωπίζοντας όμως το θέμα από διαφορετική σκοπιά θα μπορούσαμε να πούμε ότι αν δεν υπήρχαν οι hackers, τότε δε θα υπήρχε και η ανάγκη για ανάπτυξη αμυντικών προγραμμάτων που κοστίζουν σε έσοδα και δημιουργικό χρόνο. Χωρίς απειλή δεν υπάρχει λόγος για άμυνα, αλλά και για βελτίωση.

Το hacking βασίζεται κυρίως στην εξερεύνηση ξένων συστημάτων χωρίς εξουσιοδοτημένη πρόσβαση και συχνά γίνονται συλλήψεις ευφυών ανθρώπων, οι οποίοι δικάζονται ως κοινοί εγκληματίες. Οι κανόνες των hackers λένε ότι αφού δεν προξενούν κακό στο σύστημα τότε η πράξη αυτή δεν πρέπει να είναι κατακριτέα. Αν όμως αυτή η πράξη μεταφερθεί στον πραγματικό κόσμο –δηλαδή η έρευνα σε ένα ιδιωτικό χώρο (π.χ. το σπίτι μας) με την παραβίαση της εισόδου— είναι κατανοητό ότι πρόκειται για μια παράνομη και ποινικά διωκόμενη πράξη, έστω αν και αυτή η πράξη δεν είχε σκοπό να βλάψει κανένα, αλλά ο μόνος λόγος ήταν ο κορεσμός της περιέργειας του εισβολέα, κανένας δεν θα ήταν τόσο ελαστικός ώστε να αποδεχθεί την έρευνα του σπιτιού του<sup>251</sup>.

Οι hackers είναι υπέρμαχοι της ελευθερίας. Υποστηρίζουν την ελεύθερη ανταλλαγή γνώσης χωρίς περιορισμούς<sup>252</sup>. Πολλές φορές όμως καταδιώκονται

---

<sup>249</sup> Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: [21 Αυγούστου 2008]

<sup>250</sup> *About NMRC* 2008, Nomad Mobile Research Center. Διαθέσιμο στο: <<http://www.nmrc.org/about/index.html>> [21 Αυγούστου 2008].

<sup>251</sup> Ludlow, P 1996, *High noon on the electronic frontier: conceptual issues in cyberspace*, MIT Press, Cambridge, Mass.

<sup>252</sup> Murphy, C 2004, 'Inside the mind of the hacker', *Accoutacy Ireland Journal*, vol. 36, no. 3, pp.12-13. Διαθέσιμο στο: British Library Direct [21 Αυγούστου 2008].

ποινικά διότι με τις αντιλήψεις τους περί ελευθερίας της πληροφορίας απείλησαν ένα από τα βασικά δεκανίκια του καπιταλισμού, τα δικαιώματα ιδιοκτησίας. Σύμφωνα με το άρθρο “Academic Freedom and Hacker Ethic”<sup>253</sup> υπάρχει μια παγκόσμια υποκουλτούρα όπου σύμφωνα με αυτή οι hackers θεσπίζουν ότι οι πληροφορίες πρέπει να είναι ελεύθερες και η αναζήτηση της γνώσης είναι ουσιαστικό ανθρώπινο δικαίωμα. Το ερώτημα όμως είναι κατά πόσο η απαγορευμένη γνώση μπορεί να διατίθεται στο κοινό. Σύμφωνα πάντα με το άρθρο η ακαδημαϊκή κοινότητα τάσσεται υπέρ της απόψεως ότι οι hackers δεν πρέπει να έχουν πρόσβαση σε μυστικές πληροφορίες και πολύ περισσότερο να τις δημοσιοποιούν. Η γνώση που αποκτούν από την παραβίαση ξένων συστημάτων δεν πρέπει να ρέει προς τα έξω. Είναι γεγονός ότι ορισμένες πληροφορίες θα ήταν πολύ επικίνδυνο να περάσουν στα χέρια του κοινού, όπως π.χ. οι μυστικές στρατιωτικές πληροφορίες. Αν και οι ιστοσελίδες της Πολεμικής Αεροπορίας και του Στρατού είναι αγαπημένος στόχος των hackers, τις περισσότερες φορές από απλή περιέργεια αλλά και πνευματική ικανοποίηση ότι μπόρεσαν να προσπελάσουν ένα τόσο καλά οργανωμένο και δυνατό σύστημα ασφαλείας. Με βάση την κουλτούρα των hackers και την ηθική τους, κανένας ηθικός hacker δεν θα χρησιμοποιούσε τις πληροφορίες αυτές για προσωπικό όφελος. Παραμένει όμως ο κίνδυνος να διαρρεύσουν αυτές οι πληροφορίες και να πέσουν σε κακόβουλα χέρια.

Οι hackers να υποστηρίζουν ότι δεν κάνουν κακό, αλλά ορθότερα θα έπρεπε να υποστηρίζουν ότι δεν προτίθενται να κάνουν κακό. Για παράδειγμα, με την παράνομη είσοδο τους μπορεί να εμποδίσουν κάποια άλλη εξουσιοδοτημένη και νόμιμη είσοδο κάποιου άλλου χρήστη. Εδώ μπορεί παρατεθεί ένα σχετικό παράδειγμα, το 1997 κινδύνευσαν αστροναύτες των ΗΠΑ όταν ένας hacker εισέβαλε σε ένα υπολογιστή της NASA και τον υπερφόρτωσε τόσο ώστε η ιατρική επικοινωνία ανάμεσα στους αστροναύτες και το κέντρο των επιχειρήσεων να καταστεί προβληματική<sup>254</sup>.

Αυτή είναι η μια όψη του νομίσματος, η άλλη άποψη υποστηρίζει ότι η γνώση πρέπει να μοιράζεται αφιλόκερδος ώστε όλοι να έχουν λόγο στα τεκταινόμενα. Θεωρούν ότι οι πολύτιμες νέες ιδέες δεν προέρχονται πάντα από τα καθιερωμένα όργανα. Όταν οι κυβερνήσεις αναμιγνύονται ώστε να ρυθμίσουν τη γνώση, συχνά δημιουργούν εμπόδια στους ερασιτέχνες. Παραδείγματος χάριν, ο νόμος πνευματικών

<sup>253</sup> Cross, T 2006, ‘Academic freedom and the hacker ethic’, *Communications of the ACM*, vol. 49, no. 6, pp. 37-40. Διαθέσιμο στο Διαδίκτυο: ACM Portal [21 Αυγούστου 2008].

<sup>254</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

ψηφιακών δικαιωμάτων της Αμερικής του 1998 που απαγόρευσε την έρευνα σε ορισμένες κατηγορίες ευπαθών ασφάλειας υπολογιστών εκτός αν το πρόσωπο συμμετέχει σε νόμιμες σπουδές, απασχολείται ή εκπαιδεύεται κατάλληλα ή ασχολείται με τον τομέα της τεχνολογίας κρυπτογράφησης.

Αυτοί οι περιορισμοί φαίνονται να στοχεύουν συγκεκριμένα στους hackers. Αυτός ο περιορισμός έχει επιπτώσεις σε ολόκληρη κοινότητα πληροφορικής. Είναι ευρέως παραδεκτό ότι οι κρίσιμες εξελίξεις στην επιστήμη των υπολογιστών έχουν προέλθει από τα εργαστήρια και τις λέσχες (κυρίως του Homebrew Computer Club). Αν περιορίσουμε σκόπιμα την επιστήμη μόνο σε μερικά επίλεκτα εργαστήρια και ερευνητικά όργανα, θα ήταν ένα μεγάλο πλήγμα για την κοινωνία. Αυτός είναι ο αγώνας που κάνουν οι hackers για την απελευθέρωση της γνώσης, όχι τόσο για την τιμή της αλλά για τη χρήση της. Η επιδίωξη της γνώσης είναι ένα αναφαίρετο δικαίωμα, δεμένο άμεσα με την ελευθερία του λόγου. Αν οι κυβερνητικές ρυθμιστικές αρχές έχουν την νομική εξουσία να αποφασίζουν ποια θέματα μπορούν να τεθούν και να απαντηθούν, θα έχουν τη δύναμη να μας εμποδίσουν να ανακαλύψουμε τις αλήθειες που είναι κρίσιμες για τα συμφέροντα μας. Χωρίς την έρευνα και τη συνεχή εξέλιξη θα συνεχίσουμε να ήμαστε εξαρτημένοι από ιδιωτικά λογισμικά και κερδοσκοπικούς οργανισμούς που εμπορευματοποιούν την γνώση<sup>255</sup>.

Η Microsoft και η κοινότητα των hackers βρίσκονται εδώ και κάποια χρόνια σε εμπόλεμη κατάσταση. Φήμες υποστηρίζουν πως ο ίδιος ο Bill Gates ως ιδιοκτήτης της Microsoft αποδείχτηκε καλός μαθητής των hackers βελτιώνοντας αφενός μεν συνεχώς τα συστήματα ασφαλείας των προϊόντων του –βέβαια όχι υπέρ της ασφαλείας δεδομένων των καταναλωτών αλλά με στόχο την απόλυτη ασφάλεια ενάντια στην πειρατεία λογισμικού— κι αφετέρου δημιουργώντας συστήματα συλλογής δεδομένων, τα οποία δεν είναι διάφανα στους κοινούς χρήστες. Αν και η ίδια η Microsoft χρωστάει την παγκόσμια της επιτυχία στην αρχική διάδοση των προϊόντων της στους hackers και έχει αντιμετωπίσει η ίδια πολλές μηνύσεις για παράνομη ενσωμάτωση λογισμικού στα προϊόντα της, επίσημα δηλώνει ότι είναι πρώτη στην καταπολέμηση των hackers. Δεν νοείται η ύπαρξη του σημερινού μονοπωλίου της Microsoft χωρίς την «ελεύθερη» αντιγραφή του λογισμικού στις αρχές της δεκαετίας του 1980. Για πολλά χρόνια η Microsoft μονοπωλούσε τα λειτουργικά συστήματα, ενώ κρατάει το copyright του λειτουργικού συστήματος

---

<sup>255</sup> Bynum, TW & Rogerson, S 2004, *Computer ethics and professional responsibility: introductory text and readings*, Blackwell, New York.

Windows για εκατό χρόνια, χωρίς να επιτρέπει σε άλλους να προχωρήσουν και να το βελτιώσουν καταδικάζοντας τον κόσμο σε μια αργή τεχνολογική εξέλιξη<sup>256</sup>.

Αχτίδα φωτός αποτελεί το λειτουργικό σύστημα LINUX, το οποίο είναι ένα ανώτερα τεχνολογικό και ουσιαστικά δωρεάν σύστημα (ελεύθερο λογισμικό) που αναπτύχθηκε από τη δημόσια διαδικασία ανοικτού κώδικα από πολλούς προικισμένους προγραμματιστές που εργάστηκαν για τη δόξα, για να δουν τον κώδικα τους να υιοθετείται και να χρησιμοποιείται<sup>257</sup>. Οι «ημίθεοι» στον κόσμο του hacking είναι άνθρωποι που έχουν γράψει μεγάλα, χρήσιμα προγράμματα, τα οποία έχουν διαδώσει ευρέως και έτσι τώρα όλοι τα χρησιμοποιούν. Η ανάπτυξή του ελεύθερου λογισμικού αυξήθηκε απίστευτα γρήγορα χάρη στις συνεισφορές τις κοινότητας των hackers. Σε έναν κόσμο ψηφιακών ήχων, εικόνων και λέξεων, το ελεύθερο λογισμικό αυξάνεται ώστε να εξισορροπηθεί με την ελευθερία γενικότερα<sup>258</sup>.

Μέσα από τα εργαστήρια των hackers γεννήθηκαν τα μεγαλύτερα τεχνολογικά επιτεύγματα του αιώνα μας. Η ελεύθερη ανταλλαγή δεδομένων και πληροφοριών βοηθούν τους hackers να δημιουργούν δυναμικά και ελευθέρως λογισμικά όπως τα free software, τα open source, το Linux, τη Java τα οποία μας δίνουν την δυνατότητα ανεξάρτησης από τα ιδιωτικά λογισμικά.

Οι hackers ως επαναστάτες εναντιώνονται στους κολοσσούς του κέρδους που εκμεταλλεύονται το Διαδίκτυο και μονοπωλούν τις τηλεφωνικές υπηρεσίες. Ουσιαστικά οι hackers που ζουν μέσα από το Διαδίκτυο το χρησιμοποιούν εντελώς δωρεάν καθώς επίσης και τις τηλεφωνικές γραμμές. Οι εταιρίες εκμεταλλεζόμενες το μονοπώλιο τους προσφέρουν αυτές τις υπηρεσίες πολύ ακριβά. Μήπως όμως οι hackers δεν προσπαθούν να μειώσουν την τιμή των υπηρεσιών, οι οποίες αν δεν διαχειρίζονταν από αυτές τις εταιρείες θα ήταν εξευτελίστηκα φθηνές, αλλά προτιμούν να τις χρησιμοποιούν εντελώς δωρεάν. Εφόσον κάτι μπορούμε να το έχουμε εντελώς δωρεάν τότε τι χρειαζόμαστε την μείωση των τιμών. Εδώ κάνουμε λόγο για βρόμικη φθηνία<sup>259</sup>.

---

<sup>256</sup> Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

<sup>257</sup> Για περισσότερες πληροφορίες για το ελεύθερο λογισμικό LINUX στη ιστοσελίδα <<http://manual.zenwalk.org/el/ch01s02.html>>, καθώς και στην επίσημη ιστοσελίδα του LINUX <<http://www.linux.org>>.

<sup>258</sup> Raymond, ES 2001, *How to be a hacker*. Διαθέσιμο στο: <<http://www.catb.org/~esr/faqs/hacker-howto.html>> [23 Αυγούστου 2008].

<sup>259</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

Μιλώντας για τα θετικά του hacking επιβάλλεται η αναφορά σε ένα νέο είδος πολιτιστικού ακτιβισμού, το “hacktivism” (χακτιβισμός). Ο ακτιβισμός είναι ένα είδος αντίδρασης στο κατεστημένο που γίνεται με πορείες, διαδηλώσεις και διαμαρτυρίες. Μεταφέροντας αυτή την κατάσταση στον εικονικό κόσμο του Διαδικτύου, ο ακτιβισμός μετατρέπεται σε χακτιβισμό. Ο χακτιβισμός είναι μία διαδικασία που περιλαμβάνει ένα συνδυασμό διάδοσης πληροφοριών, άμεση δράση και δημιουργικές λύσεις. Είναι μία συνεχώς εξελισσόμενη ανοικτή διαδικασία. Οι τακτικές και η μεθοδολογία του δεν είναι στατικές. Υπό αυτή την έννοια, ο χακτιβισμός δεν ανήκει σε κανένα - δεν έχει προφήτη, ευαγγέλιο ή επίσημη λίστα αναγνωσμάτων. Ο χακτιβισμός είναι ένα ριζοσπαστικό φαινόμενο με ανοικτό κώδικα<sup>260</sup>.

Σύμφωνα με τον ορισμό που δίνει ο Thomas στο άρθρο του “Ethics of Hacktivism”, ο χακτιβισμός είναι η πολιτική του hacking, phreaking ή η δημιουργία τεχνολογίας για την επίτευξη ενός πολιτικού ή κοινωνικού στόχου<sup>261</sup>. Στην πολιτική του χακτιβισμού χρησιμοποιείται ο ηλεκτρονικός υπολογιστής και το hacking για κοινωνική αλλαγή. Θα μπορούσαμε να πούμε ότι το hacking σε αυτή την περίπτωση γίνεται για ηθικούς και πολιτικούς λόγους. Σύμφωνα με τον ορισμό που δίνει Still Brian στο άρθρο του “Hacking For A Cause” «...οι χακτιβιστικές δραστηριότητες εκτείνονται σε πολλά πολιτικά ιδεώδη θέματα. Ο χακτιβισμός είναι μια απόρροια που προήλθε κύριως από την ομάδα Cult of the Dead Cow. Θεσπίζει την πρόσβαση στην πληροφόρηση ως βασικό ανθρώπινο δικαίωμα και την ελευθερίας του λόγου»<sup>262</sup>. “Το μέλλον του ακτιβισμού είναι στο Διαδίκτυο» είπε ο διευθυντής προγράμματος του Electronic Frontier Foundation<sup>263</sup>.

Ουσιαστικά οι χακτιβιστές παραμορφώνουν ιστοσελίδες γράφοντας τα δικά τους μηνύματα αυτά δηλαδή που θέλουν να περάσουν στο κόσμο. Στο συμβατικό κόσμο είναι μια πράξη παρόμοια με το να γράφει κανείς τις ιδέες τους στον τοίχο. Ποιους πλήττει αυτή η πράξη; Σίγουρα την εταιρία στην οποία ανήκει η ιστοσελίδα που παραμορφώθηκε, γιατί έτσι προσβάλλεται η εικόνα ασφάλειας της εταιρίας. Αν και οι

---

<sup>260</sup> Ronfeldt, D & Arquilla, J 2001, ‘Networks, netwars and the fight for the future’, *First Monday Magazine*, vol. 6, no. 10. Διαθέσιμο στο: <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889>> [24 Αυγούστου 2001].

<sup>261</sup> Thomas, JLC 2001, *Ethics of hacktivism*, Hacker Culture. Διαθέσιμο στο: <[http://www.dvara.net/HK/Julie\\_Thomas\\_GSEC.pdf](http://www.dvara.net/HK/Julie_Thomas_GSEC.pdf)> [24 Αυγούστου 2008].

<sup>262</sup> Still, B 2005, ‘Hacking for a cause’, *First Monday Journal*, vol. 10, no. 9. Διαθέσιμο στο: <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1274>> [24 Αυγούστου 2008].

<sup>263</sup> Fuchs, C 2006, ‘The self-organization of cyberprotest’, in *The Internet Society II*, eds K Morgan, CA Brebbia & JM Spector, WITPress, Boston, pp 275-295. Διαθέσιμο στο: <<http://igw.tuwien.ac.at:16080/christian/SM3.pdf>> [24η Αυγούστου 2008].



χακτιβιστές απλά παραμορφώνουν τις ιστοσελίδες χωρίς να παίρνουν προσωπικά στοιχεία πελατών ή να κλέβουν απόρρητες προσωπικές πληροφορίες και αρχεία ούτε καταστραφούν δεδομένα (όπως αριθμοί πιστωτικών καρτών) αυτό δεν είναι και τόσο γνωστό στο κοινό με αποτέλεσμα οι πελάτες της εκάστοτε πληγείσας εταιρίας να πανικοβάλλονται. Υπάρχει μια ιδεολογία και κάποια κριτήρια για την επιλογή του εκάστοτε στόχου όπως ότι δεν προσβάλλονται ιστοσελίδες μικρών εταιριών και προτιμούνται οι πολυσύχναστες σελίδες. Η φαινομενική αύξηση των χακτιβιστών μπορεί να οφείλεται εν μέρει στην αυξανόμενη σημασία του Διαδικτύου ως μέσου επικοινωνίας. Αποδεικνύει επίσης ότι πολλοί κυβερνητικοί ιστότοποι είναι αρκετά εύκολο να προσπελαστούν<sup>264</sup>.

Αναγνωρισμένη είναι και η συμβολή των hackers στην καταπολέμηση της παιδικής πορνογραφίας. Με τις εξειδικευμένες γνώσεις τους στους ηλεκτρονικούς υπολογιστές βοηθούν στον εντοπισμό τέτοιου υλικού. Έχουν συγκροτηθεί πολλοί οργανισμοί με σκοπό τους την εξολοθρεύσει της παιδική πορνογραφίας μέσω του Διαδικτύου όπως ο Anti-Child Porn.org (<<http://www.antichildporn.org>>) και ο Ethical Hackers Against Pedophilia (EHAP), των hackers που δραστηριοποιούνται ενάντια στην παιδεραστία μέσω του Διαδικτύου.

Χωρίς να ωραιοποιείται εκούσια η πραγματικότητα πρέπει να γίνει αναφορά και στην κατηγορία των κακοηθών και άπληστων hackers, οι οποίοι εκμεταλλεύονται το ταλέντο τους μπορούν να βγάλουν αρκετά χρήματα συμμετέχοντας στο οργανωμένο έγκλημα, όπως η τρομοκρατία, η μαφία, η κατάχρηση μεγάλων ποσών από εταιρίες. Σε αυτές τις περιπτώσεις μιλάμε για μαύρους hackers. Σε ένα πρόσφατο συμπόσιο σημάτων, ένας ανώτατος αξιωματικός του αμερικάνικου Στρατού έδειξε ότι ο έφηβος hacker είναι ισότιμα θανάσιμα ανταγωνιστικός όπως ένας ισχυρός στρατιώτης που αγωνίζεται στη πρώτη θέση<sup>265</sup>. Ο ρόλος του υπολογιστή ως όπλο αλληλοεξαρτώμενος με την επαναστατικότητα του έφηβου ή κάποιου αδικημένου ατόμου το hacking μπορεί να γίνει πολύ επικίνδυνο. Στον πόλεμο των πληροφοριών, οι «κακώς εξοπλισμένοι» δράστες μπορούν να παραμείνουν ανώνυμοι και να δημιουργήσουν τη

---

<sup>264</sup> Auty, C 2004, 'Political hacktivism: tool of the underdog or scourge of cyberspace', *Aslib Proceedings*, vol. 56, no. 4, pp. 212–221. Διαθέσιμο στο: Emerald [24 Αυγούστου 2008].

<sup>265</sup> Jim T 2005, 'The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age of hacking'', *New Media & Society*, vol. 7, no. 5, pp. 599–624. Διαθέσιμο στο: Sage Journals Online [24 Αυγούστου 2008].

μεγάλη ζημιά<sup>266</sup>. Το να προκαλέσει κάποιος hacker ζημιά δεν είναι πάντα για προσωπικό όφελος, αντιθέτως σε πολλές περιπτώσεις ίσως να οφείλεται στην άγνοια ή και για λόγους εκδίκησης.

Ποιο είναι το αντίκτυπο του hacking; Ο πανικός που έχει δημιουργηθεί γύρω από το θέμα δεν επηρεάζει μόνο την κοινωνία αλλά και τους ίδιους τους hackers. Τα ΜΜΕ δημιούργησαν ένα υστερικό αλάφιασμα για το θέμα των hackers με αποτέλεσμα η κοινή γνώμη να πανικοβληθεί. Λόγω της φύσης των hackers και της μυστικότητας των ενεργειών τους, έχουν δημιουργηθεί πολλοί μύθοι γύρω από αυτούς. Στην παραμόρφωση της πραγματικότητας συνέβαλλαν τόσο τα ΜΜΕ, που διογκώνουν ένα θέμα χάριν της τηλεθέασης αλλά και ο κινηματογράφος που δημιούργησε ήρωες hackers που δεν ανταποκρίνονται στη πραγματικότητα. Η κοινωνία λόγω της έλλειψης σωστής πληροφόρησης και επηρεαζόμενη από της επιρροές των μέσων είναι δύσπιστη στη χρήση του Διαδικτύου. Η κατάσταση αυτή οδήγησε την κοινωνία σε μια οπισθοδρομική και συντηρητική παρία όσο αφορά τη χρήση του Διαδικτύου και των υπηρεσιών του, με αποτέλεσμα να μειώνεται η ποιότητα ζωής μας και δημιουργείται η εντύπωση ότι το Διαδίκτυο είναι εμπόλεμη ζώνη<sup>267</sup>.

Όσο αφορά τη μεγαλύτερη ζημιά του hacking μάλλον ότι είναι η υστερία και ο πανικός που δημιουργείται γύρω από αυτό. Σε αυτό συμβάλει η τάση και η προκατάληψη των ατόμων να σκέφτονται το χειρότερο και να δαιμονοποιούν καταστάσεις. Έτσι ένας hacker θεωρείται ότι είναι επικίνδυνος λόγω των εξειδικευμένων γνώσεων του και της ευφυΐας του και ότι είναι ικανός για το χειρότερο, το πιο εγκληματικό. Αυτή η δαιμονοποιημένη εικόνα των hackers που πλασάρεται από τα ΜΜΕ και τον κινηματογράφο δεν φοβίζει μόνο τους πολίτες αλλά επηρεάζει και τους μελλοντικούς hacker. Νεαρά άτομα με ικανότητες στους ηλεκτρονικούς υπολογιστές και τη τεχνολογία παρασύρονται από αυτό το λανθασμένα μυθοποιημένο πρότυπο και το ακολουθούν<sup>268</sup>.

---

<sup>266</sup> Nitzberg, S 1998, 'Conflict and the computer: information warfare and related ethical issues', *Proceedings of the twenty-first national information systems security conference*. Διαθέσιμο στο: <<http://csrc.nist.gov/nissc/1998/proceedings/paperD7.pdf>> [24 Αυγούστου 2008].

<sup>267</sup> Rogers, MK 2001, *A social learning theory and moral disengagement analysis of criminal computer behavior*, PhD thesis, University of Manitoba, Winnipeg. Διαθέσιμο στο: <[https://www.cerias.purdue.edu/assets/pdf/bibtex\\_archive/rogers\\_01.pdf](https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf)> [28 Αυγούστου 2008].

<sup>268</sup> Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης Αθήνα.

Έτσι υποβαθμίζεται η υψηλή δραστηριότητα του hacking, αφού η κοινότητα των hackers αποκτά άτομα με χαμηλή ηθική και αποπροσανατολισμένους στόχους με αποτέλεσμα να εξευτελίζεται η σημασία του hacking και να αποκτά έναν ύποπτο και εγκληματικό χαρακτήρα αφού την αντιπροσωπεύουν διεφθαρμένες προσωπικότητες. Το hacking τείνει να χάσει τον κοινωνικοπολιτικό ανατρεπτικό του χαρακτήρα και να περάσει στην ζώνη της εγκληματικότητας και της παρανομίας χωρίς αξίες και ιδανικά. Ίσως αυτό τον αποπροσανατολισμό του hacking να τον προωθούν εν μέρει οι εταιρίες ασφάλειας ηλεκτρονικών υπολογιστών, να είναι ένας υπόγειος πόλεμος. Προσπαθούν να υποθάλψουν το hacking και έμμεσα για να το εξαφανίσουν πίσω από το προσωπείο του νόμου. Φυσικά οι ίδιοι οι hackers υποστηρίζουν ότι υπάρχουν δύο τρόποι για να τους ξεφορτωθούν οι κυβερνήσεις. Ο πρώτος είναι η κατάργηση των υπολογιστών και των τηλεφωνικών συσκευών, πράγμα ανέφικτο, και ο δεύτερος τρόπος είναι η κατάργηση της ιδιοκτησίας της πληροφορίας.

Πολλοί hackers μπορεί να αγνοούν τον μαρξισμό ή ίσως τον συγχέουν με τον σταλινισμό. Αυτό που έχει σημασία είναι ότι σε κάποιο βαθμό, δουλεύουν με μαρξιστικό τρόπο όταν αναπτύσσουν ελεύθερο λογισμικό, πιθανόν χωρίς οι ίδιοι να το γνωρίζουν. Το πιο σημαντικό είναι ότι το επιδιώκουν, αρέσκονται στην ομαδική εργασία, την αλληλοβοήθεια, την ελεύθερη ανταλλαγή ιδεών για την επίτευξη ενός κοινού στόχου. το ελεύθερο λογισμικό μεγαλώνει την παρουσία του στην κοινωνική ζωή και το ερώτημα είναι αν η κοινωνία είναι ενημερωμένη και έτοιμη να το δεχτεί.

Σίγουρο είναι ότι νησίδες ελευθερίας δεν υπάρχουν μέσα στο καπιταλιστικό σύστημα χωρίς τάσεις εκφυλισμού. Υπάρχει όμως ένα εχέγγυο, λόγω του οποίου το φαινόμενο του ελεύθερου λογισμικού θα έχει τη δυνατότητα να ανθίσει, όσο και αν παρουσιάζει τάσεις εκφυλισμού προς την εμπορευματοποίηση. Αυτό το εχέγγυο είναι η αρχή της συνεργατικής δημιουργίας, πάνω στην οποία όλο το οικοδόμημα του ελεύθερου λογισμικού βασίζεται. Τα μέλη της κοινότητας του ελεύθερου λογισμικού αλλάζουν τον κόσμο και η κοινωνία έχει πολλά οφέλη από αυτή την ριζική αλλαγή.

## ΣΥΜΠΕΡΑΣΜΑΤΑ

Καταλήγοντας στο τέλος αυτού του πονήματος για τους hackers θα έλεγα 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. Η διάκριση του καλού και του κακού, του ηθικού και του ανήθικου είναι πολύ δύσκολη και πολλές φορές ακατόρθωτη. Δεν είναι εφικτό να γίνει ένας απολύτως διαχωρισμός εύκολα, ως προς το κατά πόσο οι hackers είναι πληγή του κοινωνικού γίνεσθαι, ένα καρκίνωμα του Διαδικτύου, όπως παρουσιάζεται από τα ΜΜΕ και τις εταιρίες ασφάλειας υπολογιστών, 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 συζήτηση έδειξε ότι οι hackers δεν είναι εθισμένοι έφηβοι που περνούν την ώρα τους μπροστά σε ένα ηλεκτρονικό υπολογιστή ούτε οργισμένοι κακοποιοί που θέλουν να ανατινάξουν το δίκτυο, όπως επί το πλείστον θεωρεί η κοινή γνώμη. Είναι επιστήμονες αφιερωμένοι στην ανάπτυξη της τεχνολογίας και με στόχο την αποδέσμευση της πληροφορίας και του Διαδικτύου τόσο από τα τέλη της όσο και από τη λογοκρισία που υφίσταται. Οι hackers είναι ευφυείς άνθρωποι, επαναστάτες και σύγχρονοι ταχυδακτυλουργοί ενός καινούριου εικονικού σύμπαντος.

Χωρίς να εθελουφλώ και να ωραιοποιώ καταστάσεις, δεν κλείνω τα μάτια στο ηλεκτρονικό έγκλημα και στο εγκληματικό hacking. Αυτό που πρέπει να σημειωθεί είναι ότι ο όρος hacker έχει μια ευρεία έννοια και πολλές φορές κακώς χρησιμοποιείται ευρέως και γενικώς καθώς τα άτομα που έχουν αυτή την ετικέτα δεν είναι όλα ίδια μεταξύ τους. Από τον δεκατετράχρονο που εισβάλλει σε έναν ιστοτόπο 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 και τον λευκό hacker που ψάχνει κενά ασφαλείας για να ενισχύσει το πρόγραμμα ασφαλείας υπάρχει μια αγεφύρωτη διαφορά.

Υπάρχει η αντίληψη ότι οι hackers είναι απλά ανεύθυνοι και επικίνδυνοι εγκληματίες με εξειδίκευση στις μοντέρνες υψηλές τεχνολογίες. Θέλοντας να είναι κανείς δίκαιος θα έπρεπε να συμφωνήσει και με αυτή την άποψη. Αυτό που πρέπει να γίνει κατανοητό είναι ότι είναι εντελώς λάθος να χρησιμοποιείται ο όρος τόσο ευρύν.

Υπάρχουν διακρίσεις ηθικής και επιπέδων δεξιοτήτων που αυτά κάνουν την διαφοροποίηση. Όπως αναφέρει και ο Λάζος το νόημα του hacking εκτείνεται σε τέτοιο βαθμό, ώστε να περιλαμβάνει ριζικά αντίθετες, αλληλοαναιρούμενες και αλληλοαποκλειόμενες αντιλήψεις, οι οποίες αναφέρονται σε ριζικά διαφορετικές πραγματικότητες<sup>269</sup>.

Ίσως το κυριότερο πρόβλημα προς μία ορθή εκτίμηση της hacker κοινότητας και των πράξεών της είναι η τέλεσή τους στον εικονικό κόσμο που οι νόμοι δεν είναι τόσο σαφείς και τα όρια όχι τόσο καλά οριοθετημένα. 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 Διαδικτύου. Όπως εξελίχθηκαν οι δυνατότητες και οι υπηρεσίες που προσφέρει ο παγκόσμιος ιστός, έτσι και οι τρόποι και τα κίνητρα δράσης των ατόμων αυτών υπερδιπλασιάστηκαν.

Η ορθότητα του hacking κρίνεται από την συνεισφορά του στην κοινωνία και τη τεχνολογία και από εκεί κρίνεται ορθότερα η χρηστικότητα του καθώς και από την συνεισφορά των hackers στην παγκόσμια ηλεκτρονική ασφάλεια. Οι hackers, έχουν συνεισφέρει πολλά στην παγκόσμια ηλεκτρονική ασφάλεια. Ανακαλύπτουν κενά ασφαλείας και τα δημοσιεύουν πριν αυτά τα εκμεταλλευτούν οι συγγραφείς ιών και οι μαύροι hackers. Ενημερώνουν τους διαχειριστές και το κοινό για αυτά τα κενά και ευαισθητοποιούν τον κόσμο σχετικά με την ασφάλεια. Αποδεικνύουν ότι με την έρευνα και τις γνώσεις μπορούμε να βελτιώσουμε την τεχνολογία σε βαθμό που παλιά θεωρούταν αδύνατος και με ταχύτατους ρυθμούς. Η παλιά φιλοσοφία ασφαλείας που βασίζεται στην ασάφεια «Security through obscurity<sup>270</sup>» δεν είναι αποτελεσματική τακτική την εποχή του Διαδικτύου και της παγκοσμιοποίησης. Το να κρύβει κανείς τις αδυναμίες ενός συστήματος για να αποτρέπει επίδοξους εισβολείς είναι σαν να κλείνει τα μάτια για να μη τον δουν. Ο μόνος πρακτικά αποτελεσματικός τρόπος αντιμετώπισης είναι η έγκαιρη ανακάλυψη των προβλημάτων και η ενημέρωση τους μέσω update και patches. Η ιστορία αποδεικνύει ότι αντί να εκτιμηθεί η συνεισφορά των εκάστοτε hackers στην παγκόσμια ασφάλεια και την εξέλιξη της τεχνολογίας είχαμε συλλήψεις και άδικες ποινές φυλάκισης. Εδώ τίθεται

---

<sup>269</sup> Λάζος, Γ 2001, *Πληροφορική και έγκλημα*, Νομική Βιβλιοθήκη, Αθήνα.

<sup>270</sup> Security through obscurity : “ασφάλεια μέσω αφάνειας” είναι η γνώμη και η άποψη ότι ένα σύστημα είναι τόσο ασφαλές που κανένας δεν γνωρίζει και δεν μπορεί να μπει μέσα στους εσωτερικούς του μηχανισμούς όπως κωδικούς" Πολλοί οργανισμοί όπως τράπεζες και μεγάλες εταιρείες δουλεύουν πάνω σε αυτή την βάση και άποψη.

ένα τεράστιο ηθικό θέμα για το αν η δημοσιοποίηση κενών ασφάλειας, ακόμα και αν περιλαμβάνει μη εξουσιοδοτημένη εισχώρηση σε ξένα συστήματα, πρέπει να τιμωρείται ή όχι.

Επιπλέον προσφέρουν καινοτομικά προϊόντα τα οποία μας αποδεσμεύουν από τις ιδιωτικές εταιρίες λογισμικού και αναπτύσσουν κλίμα αλτρουισμού και συνεισφοράς. Οι hackers ως επαναστάτες εναντιώνονται στους κολοσσούς του κέρδους που εκμεταλλεύονται το Διαδίκτυο και μονοπωλούν τις τηλεφωνικές υπηρεσίες. Ουσιαστικά οι hackers που ζουν μέσα από το Διαδίκτυο το οποίο και χρησιμοποιούν εντελώς δωρεάν καθώς επίσης και τις τηλεφωνικές γραμμές. Οι εταιρίες εκμεταλλεόμενες το μονοπώλιο τους προσφέρουν αυτές τις υπηρεσίες πολύ ακριβά.

Μέσα από το hacking γεννήθηκε ένα νέο είδος πολιτιστικού ακτιβισμού το Hacktivism (Χακτιβισμός). Πρόκειται για μια ηλεκτρονική διαμαρτυρία και ένας τρόπος έκφρασης για τα όσα μας ενοχλούν και δεν ταιριάζουν με τα πιστεύω μας.

Αναγνωρισμένη είναι και η συμβολή των hackers στην καταπολέμηση της παιδικής πορνογραφίας. Με τις εξειδικευμένες γνώσεις τους στους ηλεκτρονικούς υπολογιστές βοηθούν στον εντοπισμό τέτοιου υλικού. Έχουν συσταθεί πολλοί οργανισμοί με σκοπό τους την εξολόθρευση της παιδική πορνογραφίας μέσω του Διαδικτύου όπως ο Anti-Child Porn.org.

Φυσικά υπάρχει το ηλεκτρονικό έγκλημα που βασανίζει το Διαδίκτυο και ως εκ τούτου ο πανικός που έχει δημιουργηθεί γύρω από αυτό το θέμα δεν επηρεάζει μόνο την κοινωνία αλλά και τους ίδιους τους hackers. Για αυτό όμως θα ήταν άδικο να κρίνουμε αποκλειστικά τους hackers. Η δράση των hackers φαίνεται να συναρπάζει μια ευρεία ομάδα ανθρώπων, εκ των οποίων και τα MME, κάτι που οδηγεί στην ανάδειξη των hackers σε διασημότητες επί το πλείστον φανταστικές και διαστρεβλωμένες. Το θέμα απολαμβάνεται από τα MME και η πλειονότητα των ανθρώπων μπορεί να θυμηθεί τον φρικτό ιό που ταλαιπώρησε χιλιάδες χρήστες του Διαδικτύου, πόσοι όμως από εμάς γνωρίζουν ότι ο ιδρυτής της εταιρίας Apple είναι ένας hacker όπως και ο δημιουργός του προγράμματος Linux, που αποτελούν μια πνοή και μια ηλιαχτίδα φωτός για την αποδέσμευση μας από τις ιδιωτικές εταιρίες λογισμικού.

Ο όρος hacker είναι τόσο ευρύς όσο και η λέξη άνθρωπος. Όλοι μας ήμαστε άνθρωποι, οι οποίοι κρινόμαστε από τις πράξεις μας και τις δεξιότητες μας. Στον κόσμο των hackers τα πράγματα είναι ακόμα πιο απλά, η μόνη διάκριση είναι με

βάση τις ικανότητες και την ηθική και όχι το χρώμα, το φύλο, τη φυλή ή το χρήμα. Υπάρχουν προφανείς ενδείξεις –π.χ. το «Μανιφέστο των hackers»-- ότι για πολλούς ανθρώπους το hacking δεν είναι απλά κάτι που κάνουν, αλλά ένας τρόπος σκέψης για την τεχνολογία και την κοινωνία γενικότερα. Το να είναι κανείς hacker αποτελεί τρόπο ζωής.

Η «υπόγεια» κοινότητα των hackers ήταν πολύ πιο ανοιχτή στα πρώτα χρόνια του Διαδικτύου. Σήμερα είναι πολύ πιο δύσκολο να βρεθεί κανείς ανάμεσα σε αυθεντικούς hackers. Αυτό οφείλεται σε ένα μεγάλο βαθμό στην αυξημένη δημοτικότητα του Διαδικτύου, στην εμπορευματοποίηση του μύθου των hackers και κυρίως στους νομικούς κινδύνους. Το να είναι κανείς hacker προϋποθέτει πολλές ώρες απομόνωσης, μάθησης και προσωπικής έρευνας χωρίς να είναι σημαντική η επικοινωνία. Όταν υπάρχει επικοινωνία γίνεται μόνο σε τεχνικό επίπεδο πάνω σε συγκεκριμένα θέματα. Στην αρχή μπορεί να νομίζει κανείς ότι οι άνθρωποι που ασχολούνται σε βάθος με τους υπολογιστές και το Διαδίκτυο είναι απότομοι και αντικοινωνικοί. Η πραγματικότητα όμως είναι ότι ενδιαφέρονται περισσότερο για την ουσία παρά την εμφάνιση των πραγμάτων. Hacker θα βρει κανείς σε φόρουμ σχετικά με την ασφάλεια, οι λιτές αλλά ουσιαστικές απαντήσεις τους προδίδουν τις γνώσεις τους. Δυστυχώς όμως, ίσως η μεγαλύτερη μερίδα των hackers δεν ασχολούνται με δημόσιες συζητήσεις και κατά κανόνα δεν ενδιαφέρονται για επικοινωνία σε προσωπικό επίπεδο. Οι σημερινοί hackers είναι πολύ προσεκτικοί, μεθοδικοί και δεν αποκαλύπτουν τις δραστηριότητες τους ούτε σε φίλους.

Το hacking που βασίζεται στην εξερεύνηση ξένων συστημάτων χωρίς να βλάπτεται με οποιοδήποτε τρόπο το σύστημα δεν θα έπρεπε να είναι σοβαρό αδίκημα. Οι περισσότεροι hackers έχουν μοναδικό κίνητρό τους τη μάθηση. Πρόκειται για άτομα με υψηλό δείκτη νοημοσύνης που για κοινωνικούς και ψυχολογικούς λόγους καταφεύγουν στο hacking. Είναι πραγματικά τραγικό να δικάζονται ως κοινοί εγκληματίες και να τους τοποθετούν σε φυλακές δίπλα σε δολοφόνους και βιαστές.

Πιστεύω ότι το hacking εκφράζει μια βαθιά εσωτερική ανάγκη που δεν έχει σχέση με την τεχνολογία. Είναι η ανάγκη για γνώση, για περιπέτεια, για εξερεύνηση και ανακαλύψεις. Οι hackers μοιάζουν πολύ με τους δημοσιογράφους που διψούν για αποκλειστικότητα και μυστικά. Η τεχνολογία είναι μόνο η αφορμή για την αναζήτηση αυτού που ούτε οι hackers μπορούν να ορίσουν. Αν αυτά τα ταλαντούχα και ανήσυχα πνεύματα καταφέρουν να διοχετεύσουν την ενέργειά τους σε άλλους

τομείς, έχουν όλες τις δυνατότητες να διαπρέψουν. Αν τελικά καταφέρουν να καταπολεμήσουν τον κυνισμό και την απαισιοδοξία που πολλές φορές τους διακατέχει. Οι hackers ξεκίνησαν εδώ και μερικά χρόνια μια επανάσταση για ένα πιο ελεύθερο δίκτυο 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. Αυτό που πρέπει να κατανοήσουμε είναι ότι δεν υπάρχουν μόνο δύο χρώματα, άσπρο και μαύρο, υπάρχουν πολλοί χρωματισμοί ανάμεσα τους. Ακόμη και ο hacker που κρίνεται κακόβουλος ίσως να έχει κάτι χρήσιμο να προσφέρει.



## ΛΕΞΙΚΟ ΟΡΩΝ

ARPANET (Advanced Research Project Agency Network): Ένα διαδικτυακό πρόγραμμα το οποίο άρχισε στα τέλη του 1960 από το Advanced Research Project Agency των ΗΠΑ και το οποίο αργότερα αναπτύχθηκε και μεταλλάχθηκε σε Διαδίκτυο.

BLACK HAT (Μαύρο καπέλο): Ένας όρος που αναφέρεται στους κακόβουλους και καταστροφικούς hackers, των οποίων η δράση κατευθύνεται προς την καταστροφή των συστημάτων ασφαλείας.

BLUE BOX (Μπλε κουτί): Ένα πολύ συνηθισμένο μηχάνημα τονικής προέλευσης που δημιουργήθηκε και χρησιμοποιήθηκε από τους πρώτους Phone hackers για να διαπεράσουν την συνηθισμένη τηλεφωνική κλήση και να την χρεώσουν στο Διαδίκτυο, γνωστό και ως μπλε κουτί.

CRACKER: Όρος για μια μορφή hacker. Η διάκριση μεταξύ των όρων hacker και cracker είναι πολύ δύσκολη.

ETHICAL HACKER (Ηθικός hacker): Hacker με κίνητρο η αμυντική ασφάλεια.

FIREWALL (Τείχος προστασίας): Firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

FTP (File Transfer Protocol): Είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet) και χρησιμοποιείται για την μεταφορά αρχείων μεταξύ των συστημάτων μέσω Διαδικτύου.

**HACKER:** Κάποιος ο οποίος καταφέρνει ή κερδίζει τη μη μόνιμη πρόσβαση σε ένα σύστημα ηλεκτρονικών υπολογιστών.

**HACTIVISM (Χακτιβισμός):** Όταν κάνεις hacking σε κάτι που πάει αντίθετα με το πιστεύω σου.

**GREY HAT (Γκρίζο καπέλο):** Άτομα τα οποία βρίσκονται μεταξύ των δύο κατηγοριών (White Hat και Black Hat), των οποίων τα κίνητρα είναι αδιευκρίνιστα και έχουν την τάση να αλλάζουν.

**PHONE HACKER ή PHREAK:** είναι κάποιος ο οποίος καταχράζεται 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.

**SECURITY VULNERABILITIES: (τρύπες/σφάλματα ασφαλείας)** Τα τρωτά σημεία είναι λάθη, ελαττώματα ή λάθη προγραμματισμού. Χρησιμοποιούνται από μη εξουσιοδοτημένους χρήστες για να αποκτήσουν πρόσβαση σε δίκτυα υπολογιστών ή διακομιστές web από το Internet. Όταν διαπιστωθούν αυτές οι ευπάθειες, οι εταιρείες λογισμικού σχεδιάζουν «επιδιορθώσεις» (fixes), «προσθήκες» (patches) ή «ενημερώσεις» (updates) που μπορείτε να κατεβάσετε για να επιδιορθώσετε τα προβλήματα.

**SNIFFER:** Ένα εργαλείο, το οποίο κινητοποιεί και καταγράφει τη δράση του Διαδικτύου.

**TROJAN HORSE (Δούρειοι ίπποι):** Φαινομενικά αξιόπιστο λογισμικό που μεταφέρει ανεπιθύμητο επιζήμιο φορτίο. Συνήθως, το φορτίο είναι ιός που χρησιμοποιείται για να αποκτήσει κανείς μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφορικής.

URL (Uniform Resource Locator): Δηλώνει μια διεύθυνση ενός πόρου του Παγκόσμιου Ιστού και επιτρέπει τον εντοπισμό της πηγής στον Παγκόσμιο Ιστό.

VIRUS (Ιός): Πρόγραμμα που δημιουργεί αντίγραφα του εαυτού του σε άλλα προγράμματα που είναι αποθηκευμένα σε έναν υπολογιστή. Μπορεί να είναι ακίνδυνος, αλλά συνήθως έχει επιζήμιες παρενέργειες, όπως επιβράδυνση του υπολογιστή ή καταστροφή της μνήμης και των αρχείων του υπολογιστή.

WHITE HAT (Άσπρο καπέλο): Όρος που χρησιμοποιείται για τους ηθικούς hackers, των οποίων οι δράση είναι προς όφελος των συστημάτων ασφαλείας. Τα ίδια άτομα ονομάζονται και ethical hacker.

WWW (World Wide Web): Το συλλογικό όνομα για το παγκόσμιο δίκτυο της πληροφορίας το οποίο είναι προσβάσιμο μέσο.

WORM (Σκουλήκι): Επιβλαβές πρόγραμμα που δημιουργεί αντίγραφα του εαυτού του μέχρι να γεμίσει όλο το χώρο αποθήκευσης ενός δίσκου ή δικτύου. Τα σκουλήκια, δημιουργώντας αντίγραφα, καταναλώνουν το χρόνο, το χώρο και την ταχύτητα του υπολογιστή, με σκοπό να επιβραδύνουν ή να προκαλέσουν την κατάρρευση ολόκληρων διακομιστών web και την αποσύνδεση από το Διαδίκτυο.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

### Ξένη έντυπη

Ambrosek, R 2006, *Shawn fanning: the founder of Napster*, The Rosen Publishing Group, New York.

Berners, L.T. 1999, *Weaving the Web*, Harper, San Francisco.

Bynum, T W & Rogerson, S 2004, *Computer ethics and professional responsibility*, Blacwell, New York

Chiesa, R, Ciappi, S & Ducci, S 2008, *Profiling hackers: the science of criminal profiling as applied to the world of hacking*, CRC Press, Boca Raton.

Donald, B 2006, *Steve Jobs, Steve Wozniak and the personal computer*, Capstone Press, New York.

Douglas, T 2003, *Hacker culture*, Minnesota Press, Minneapolis.

Fitzgerald, B (ed.) 2007, *Open content licensing: cultivating the creative commons*, Sydney University Press, Sydney

“Hacker”, *The new oxford dictionary of English*, 1998, Oxford University Press, New York.

“Hacker”, *Collins English dictionary*, 1994, HarperCollins, Glasgow.

Harold F & Tipton, MK 2007, *Information security management handbook*, 6<sup>th</sup> ed. CRC Press, Boca Raton.

Lessig, L 2001, *The future of ideas*, Random House, New York.

Levy, S 1984, *Hackers: heroes of the computer revolution*, Penguin Books, New York.

Long, J 2007, *Stealing the network: how to own a shadow*, Syngress, Cambera.

Ludlow, P 1996, *High noon on the electronic frontier: conceptual issues in cyberspace*, MIT Press, Cambridge, Mass

Macz, M 2002, *Internet underground: the way of the hacker*, PageFree Publishing, Galaxy.

Mitnick, KD & Simon, WL 2005, *The art of intrusion: the real stories behind the exploits of hackers, Intruders and Deceivers*, Wiley, Indianapolis

Molyneux, J. 1983, *What is the Real Marxist Tradition?*, Bookmarks, London

Olivennes, D 2007, *La gratuité, c'est le vol: quand le piratage tue la culture*, Grasset & Fasquelle, Paris.

Quittner, J & Slatalla, M 1995, *Masters of Deception: the gang that ruled cyberspace*, Vintage, London.

### **Ξένες Ιστοσελίδες**

*2600: the hacker quarterly* 2008, 2600 Magazine. Διαθέσιμο στο: <[www.2600.com](http://www.2600.com)> [4 Νοεμβρίου 2008].

*About NMRC* 2008, Nomad Mobile Research Center. Διαθέσιμο στο: <<http://www.nmrc.org/about/index.html>> [21 Αυγούστου 2008].

*An evening with Steve Wozniak* 2006, (video recording). Διαθέσιμο στο: <<http://video.google.com/videosearch?q=Steve+Wozniak+&emb=0#>> [16 Σεπτεμβρίου 2008].

Arlene, H 2001, 'A dramaturgical analysis of charismatic leader discourse', *Journal of Organizational Change Management*, vol. 14, no 3, pp. 253-265. Διαθέσιμο στο: Emerald [15 Σεπτεμβρίου].

Auty, C 2004, 'Political hacktivism: tool of the underdog or scourge of cyberspace', *Aslib Proceedings*, vol. 56, no. 4, pp. 212–221. Διαθέσιμο στο: Emerald [24 Αυγούστου 2008].

Bauer, A & Pizka, M 2003, 'The contribution of free software to software evolution', *Proceedings of the international workshop on principles of software evolution*, pp 1-

10. Διαθέσιμο στο: <<http://www4.informatik.tu-muenchen.de/publ/papers/mp03f.pdf>> [26 Αυγούστου 2008].

Beale, L 2000, 'Seven days the last word on last week', *NY Daily News*, 23 Απριλίου. Διαθέσιμο στο:<[http://www.nydailynews.com/archives/news/2000/04/23/2000-04-23\\_seven\\_days\\_the\\_last\\_word\\_on\\_.html](http://www.nydailynews.com/archives/news/2000/04/23/2000-04-23_seven_days_the_last_word_on_.html)> [12 Σεπτεμβρίου 2008].

Becker, M 2002, 'Fed. pen for e-mail virus guy', *NY Daily News*, 2 Μαΐου. Διαθέσιμο στο: <[http://www.nydailynews.com/archives/news/2002/05/02/2002-05-02\\_fed\\_pen\\_for\\_e-mail\\_virus\\_guy.html](http://www.nydailynews.com/archives/news/2002/05/02/2002-05-02_fed_pen_for_e-mail_virus_guy.html)> [12 Σεπτεμβρίου 2008].

Berk, V, Bakos, G & Morris, R 2003, 'Designing a framework for active worm detection on global networks', *Proceedings of the IEEE International Workshop on Information Assurance*, pp. 13-23. Διαθέσιμο στο: IEEE Xplore [11 Σεπτεμβρίου 2008].

Berry, DM & Moss, G 2005, 'The libre culture manifesto: a manifesto for free/libre culture', *Free Software Magazine*, no. 2, Μάρτιος Διαθέσιμο στο: <[http://tinrp.free.fr/empty/pages/things/libre\\_manifesto.pdf](http://tinrp.free.fr/empty/pages/things/libre_manifesto.pdf)> [10 Αυγούστου 2008].

Biersdorfer, J.D. 1997, 'Books in brief: nonfiction', *The New York Times*, 30 Μαρτίου. Διαθέσιμο στο:<<http://query.nytimes.com/gst/fullpage.html?res=9504E5D7173BF933A05750C0A961958260&n=Top/Features/Books/Book%20Reviews&scp=1&sq=Kevin%20Poulsen%20fbi&st=cse>> [11 Σεπτεμβρίου 2008].

Biersdorfer, J.D. 2006, 'Desktop icon', *The New York Times*, 1 Οκτωβρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2006/10/01/books/review/Biersdorfer.t.html?scp=1&sq=Stephen%20Wozniak%20hacker%201985&st=cse>> [16 Σεπτεμβρίου 2008].

"Canada broadens its case against suspected hacker 2000", *The New York Times*, 4 Αυγούστου. Διαθέσιμο στο: <<http://partners.nytimes.com/library/tech/00/08/biztech/articles/04hacker.html?scp=1&sq=Mafiaboy%2064&st=cse>> [12 Σεπτεμβρίου 2008].

Carpenter, T 1995, Hijacking on the infobahn', *The New York Times*, 22 Ιανουαρίου. Διαθέσιμο στο: <[http://query.nytimes.com/gst/fullpage.html?res=990CE4DA1238F931A15752C0A963958260&sec=&spon=&scp=1&sq=Masters%20of%20Deception%20\(MOD\)&st=cse](http://query.nytimes.com/gst/fullpage.html?res=990CE4DA1238F931A15752C0A963958260&sec=&spon=&scp=1&sq=Masters%20of%20Deception%20(MOD)&st=cse)> [22 Νοεμβρίου 2008].

*Chaos Computer Club e.V* 2008, Chaos Computer Club. Διαθέσιμο στο: <<http://www.ccc.de>> [4 Νοεμβρίου 2008].

Chawki, M 2005, *A critical look at the regulation of cybercrime*, Computer Crime Research Center. Διαθέσιμο στο: <<http://www.crime-research.org/articles/Critical/>> [28 Δεκεμβρίου 2008].

Chen, T M & Robert, J M 2004, 'Worm epidemics in high-speed networks', *Computer*, vol. 37, no. 6, pp. 48-53. Διαθέσιμο στο: IEEE Computer Society Digital Library [11 Σεπτεμβρίου 2008].

Cleto AS 2004, 'Venezuela embraces linux and open source software, but faces challenges', *Venezuelanalysis.com*, 8 Δεκεμβρίου. Διαθέσιμο στο: <<http://www.venezuelanalysis.com/news/827>> [26 Αυγούστου 2008].

Clive, T. 2005, "Meet the life hackers", *New York Times*, 16 Οκτωβρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2005/10/16/magazine/16guru.html?scp=1&sq=Meet%20the%20Life%20Hackers%20&st=cse>> [13 Δεκεμβρίου 2008].

Coleman, EG & Golub A 2008, 'Hacker practice: moral genres and the cultural articulation of liberalism', *Anthropological Theory*, vol. 8, no. 3, pp. 255-277. Διαθέσιμο στο: <[http://ciilibrary.org:8000/ciil/Fulltext/Anthropological\\_Theory/Vol\\_8\\_3\\_2008/Article\\_3.pdf](http://ciilibrary.org:8000/ciil/Fulltext/Anthropological_Theory/Vol_8_3_2008/Article_3.pdf)> [26 Αυγούστου 2008].

Conhaim, WW 2002, 'Creative commons nurtures the public domain' *Information Today*, 3 Ιουνίου. Διαθέσιμο στο: <<http://newsbreaks.infotoday.com/nbreader.asp?ArticleID=17167>> [19 Αυγούστου 2008].

*Convention on Cybercrime* 2001, Council of Europe, Budapest. Διαθέσιμο στο: <<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>> [15 Νοεμβρίου 2008].

Couturie, LE 1995, 'The future of high-technology crime: a parallel celphi study', *Journal of Criminal Justice*, vol. 23, no. 1, pp. 13-27. Διαθέσιμο στο: Elsevier [15 Δεκεμβρίου 2008].

Cramer, F 2000, *Free software as collaborative text*, CodeKit. Διαθέσιμο στο: <[http://java.khm.de/content/pdf/free\\_software\\_as\\_text.pdf](http://java.khm.de/content/pdf/free_software_as_text.pdf)> [14 Αυγούστου 2008].

Cramer, F 2000, *Free software as collaborative text*. Διαθέσιμο στο: <[http://java.khm.de/content/pdf/free\\_software\\_as\\_text.pdf](http://java.khm.de/content/pdf/free_software_as_text.pdf)> [14 Αυγούστου 2008].

Cranor, LF 2000, 'Ten years of computers, freedom and privacy: a personal retrospective, computers, freedom and privacy', *Proceedings of the tenth conference on computers, freedom and privacy*, pp. 11–15. Διαθέσιμο στο: <<http://www.cfp2000.org/papers/2cranor.pdf>> [28η Σεπτεμβρίου 2008].

Cross, T 2006, 'Academic freedom and the hacker ethic', *Communications of the ACM*, vol. 49, no. 6. Διαθέσιμο στο: ACM Portal [21 Αυγούστου 2008].

Cult of the Dead Cow 2006, cDc launches global campaign against Google. 12 Φεβρουαρίου 2006. *Cult of the Dead Cow: Blog*. Διαθέσιμο στο: <<http://w3.cultdeadcow.com/cms/2006/02/cdc-launches-gl.html>> [29 Ιανουαρίου 2008].

*Cult of the Dead Cow*, 2008, cDc communications. Διαθέσιμο στο: <<http://www.cultdeadcow.com>> [29 Νοεμβρίου 2008].

Denning, D 1990. 'Concerning hackers who break into computer systems' *Proceedings of the thirteen national computer security conference*. Διαθέσιμο στο: <<http://cyber.eserver.org/hackers.txt>> [21 Αυγούστου 2008].

Duvel, 2007, 'A brief history of the underground scene', *Phrack Magazine*, 64. Διαθέσιμο στο: <<http://www.phrack.com/issues.html?issue=64&id=4#article>> [20 Νοεμβρίου 2008].



Edwards, J 2007, 'Why black-hat hackers become white-hat heroes', *Network Security Journal*, 11 Σεπτεμβρίου. Διαθέσιμο στο: <<http://www.networksecurityjournal.com/features/black-hats-become-white-hats-091107/>> [30 Σεπτεμβρίου 2008].

Elliot, M S & Scacchi, M 2008, 'Mobilization of software developers: the free software movement', *Information Technology & People*, vol. 21, no. 1, pp. 4–33. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

Erickson, K & Howard, NP 2007, 'A case of mistaken identity?: news accounts of hacker, consumer, and organizational responsibility for compromised digital records' *Journal of Computer-Mediated Communication*, vol. 12, no. 4, pp. 1229–1247. Διαθέσιμο στο: Wiley Interscience [30 Σεπτεμβρίου 2008].

Fallows, J 1996, 'An outlaw in cyberspace', *The New York Times*, 4 Φεβρουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9B00E3D71739F937A35751C0A960958260&sec=&spon=&scp=1&sq=Tsutomu%20Shimomura%20mitnick%20%201994&st=cse>>

Forester, T & Morrison, P 1994, *Computer ethics: cautionary tales and ethical dilemmas in computing*, MIT Press, Cambridge, Mass. Διαθέσιμο στο: Google Books Search [10 Σεπτεμβρίου 2008].

*Free Software Foundation and the GNU operation system* 2008, Free Software Foundation. Διαθέσιμο στο: <<http://www.fsf.org/about>> [12 Αυγούστου 2008].

*Freedom downtime: the story of Kevin Mitnick* 2003, (video recording), 2600 Films. Διαθέσιμο στο: <<http://video.google.ca/videoplay?docid=-6746139755329108302>> [11 Σεπτεμβρίου 2008].

*FSF to host free software licensing seminars and discussions on SCO v. IBM in New York* 2004, Free Software Foundation. Διαθέσιμο στο: <<http://www.gnu.org/press/2004-01-02-nyc-seminars.html>> [12 Αυγούστου 2008].

Fuchs, C 2006, 'The self-organization of cyberprotest', in *The Internet Society II*, eds K Morgan, CA Brebbia & JM Spector, WITPress, Boston, pp 275-295. Διαθέσιμο στο: <<http://igw.tuwien.ac.at:16080/christian/SM3.pdf>> [24η Αυγούστου 2008].

Gabrie, T 1995, 'Reprogramming a convicted hacker: to his on-line friends, Phiber Optik is a virtual hero', *The New York Times*, 14 Ιανουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=990CEED71F39F937A25752C0A963958260>> [22 Νοεμβρίου 2008].

Gabrie, T 1995, 'Reprogramming a convicted hacker; to his on-line friends, Phiber Optik is a virtual hero', *The New York Times*, 14 Ιανουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=990CEED71F39F937A25752C0A963958260>> [22 Νοεμβρίου 2008].

Garfinkel, S 2002, 'The FBI's cybercrime crackdown', *Technology Review*. Διαθέσιμο στο: <<http://jrichardstevens.com/articles/garfinkle-FBI.pdf>> [11 Σεπτεμβρίου 2008].

Ghosh, R A 1998, 'Interviews with Linus Torvalds: what motivates free software developers?', *First Monday Journal*, vol. 3, no 3. Διαθέσιμο στο: <<http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/583/504>> [15 Σεπτεμβρίου 2008].

Gissel R 2005, *Digital underworld: computer crime and resulting issues*, MacroTech Press Διαθέσιμο στο: Google Books Search [28 Δεκεμβρίου 2008].

Granger, S 1994, 'The hacker ethic', *Proceedings of the conference on ethics in the computer age*, pp. 7-9. Διαθέσιμο στο: ACM Portal [15 Νοεμβρίου 2008].

Hafner, K 1998, 'Mac, windows and now, linux', *The New York Times*, 8 Οκτωβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=950CE3DB143BF93BA35753C1A96E958260&n=Top/Reference/Times%20Topics/People/H/Hafner,%20Katie&scp=1&sq=Linus%20Torvalds%20engineering&st=cse>> [18 Σεπτεμβρίου 2008].

Hafner, K 2000, 'In world of hackers, good guys and bad guys are often a blur', *The New York Times*, 12 Φεβρουαρίου. Διαθέσιμο στο

<<http://query.nytimes.com/gst/fullpage.html?res=9B03E5DA1F3EF931A25751C0A9669C8B63&sec=&spon=&scp=5&sq=L0pht&st=cse>> [29 Ιανουαρίου 2008].

Halbert, D 1997, 'Discourses of danger and the computer hacker', *Information Society*, vol. 13, no. 4, pp. 361–374. Διαθέσιμο στο: InformaWorld [15 Νοεμβρίου 2008].

Harmon, A 2002, 'Technology: free software, at least to a certain point', *The New York Times*, 23 Σεπτεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9403E7DD1739F930A1575AC0A9649C8B63&scp=1&sq=Richard%20Stallman%20freedom%20fighter&st=cse>> [30 Σεπτεμβρίου 2008].

Hars, A & Ou, S. 2002, 'Working for free? motivations of participating in open source projects', *International Journal of Electronic Commerce*, vol. 6, no. 3, pp. 25-39. Διαθέσιμο στο: <<http://mesharpe.metapress.com/app/home/contribution.asp?referrer=parent&backto=searcharticlesresults,1,1;>> [14 Αυγούστου 2008].

Imhorst, C 2005, *Anarchy and source code: what does the free software movement have to do with anarchism?*, Free/Open Source Research Community. Διαθέσιμο στο: <<http://freesoftware.mit.edu/papers/imhorst.pdf>> [26 Αυγούστου 2008].

*Infonomicon Computer Club: the least constructive guys on the interwebs* 2008, Infonomicon Computer Club. Διαθέσιμο στο: <<http://nomicon.info/members.php>> [19 Ιανουαρίου 2008].

Jim T 2005, 'The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age of hacking'', *New Media & Society*, vol. 7, no. 5, pp. 599-624. Διαθέσιμο στο: Sage Journals Online [24 Αυγούστου 2008].

Jones, R & Andrew, T 2005, 'Open access, open source and e-theses: the development of the Edinburgh Research Archive', *Program: Electronic Library and Information Systems*, vol. 39, no. 3, pp. 198–212. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

Kellerman A.2000, "Phases in the rise of the information society", *Info - The journal of policy, regulation and strategy for telecommunications*, vol. 2, no.6, pp. 537-541. Διαθέσιμο στο: Emerald [15 Νοεμβρίου 2008].

Kelty, CM 2004, 'Culture's open sources: software, copyright, and cultural critique', *Anthropological Quarterly*, vol. 77, no. 3, pp. 499-506. Διαθέσιμο στο: Project Muse [14 Αυγούστου 2008].

Krauss, A 2001, 'Technology briefing', *The New York Times*, 5 Δεκεμβρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2001/12/05/technology/05TBRF.html?ex=1232686800&en=b7fa92486de87109&ei=5070>> [15 Σεπτεμβρίου 2008].

Lakhani, K και Wolf, R G 2003, 'Why hackers do what they do: understanding motivation and effort in free/open source software projects', *MIT Sloan Working Paper* No. 4425-03. Διαθέσιμο στο: <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=443040](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=443040)> [10 Αυγούστου 2008].

Lawrence, L 2004, *Free culture: how big media uses technology and the law to lock down culture and control creativity*, The Penguin Press, New York. Διαθέσιμο στο: <<http://www.free-culture.cc/freeculture.pdf>> [26 Αυγούστου 2008].

Leeson, PT & Coyne, CJ 2006, 'The economics of computer hacking', *Journal of Law, Economics and Policy*, vol. 1, no. 2, pp.511-532. Διαθέσιμο στο: <<http://scholar.google.gr/scholar?hl=en&lr=&q=info:hp7GBEQVx-oJ:scholar.google.com/&output=viewport&pg=1>> [15 Δεκεμβρίου 2008].

Lewis, P 1994, 'Companies rush to set up shop in cyberspace', *The New York Times*, 2 Νοεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9A04EEDF163EF931A35752C1A962958260&sec=&spon=&scp=5&sq=Tim%20Berners-Lee%20biography&st=cse>> [16 Σεπτεμβρίου 2008].

Markoff, J 1988, 'Californian held in computer case', *The New York Times*, 26 Δεκεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res>

=940DE3D71E3CF935A15751C1A96E948260&scp=1&sq=1988%20Digital%20Equipment%20Corporation%20mitnick&st=cse> [9 Σεπτεμβρίου 2008].

Markoff, J 2003, 'Technology; Apple co-founder creates electronic ID tags', *The New York Times*, 21 Ιουλίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9507E0DC1F3CF932A15754C0A9659C8B63&scp=3&sq=Stephen%20Wozniak%20apple&st=cse>> [15 Σεπτεμβρίου 2008].

Marson, S.M. 1997, "A selective history of Internet technology and social work", *Computers in Human Services*, vol. 14, no. 2, pp. 35 – 49. Διαθέσιμο στο: ACM portal. [15 Νοεμβρίου 2008].

Mateas, M 2005, 'Procedural literacy: educating the new media practitioner', *On the Horizon*, vol. 3, no. 2, pp. 101–111, Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

"Mitnick gets out of Lompoc" 2000, *Wired magazine*, 21 Ιανουαρίου. Διαθέσιμο στο: <<http://www.wired.com/news/politics/0,1283,33823,00.html>> [11 Σεπτεμβρίου 2008].

Murphy, C 2004, 'Inside the mind of the hacker', *Accountancy Ireland Journal*, vol. 36, no. 3, pp.12-13. Διαθέσιμο στο: British Library Direct [15 Δεκεμβρίου 2008].

MySQL 2009, MySQL AB Sun Microsystems. Διαθέσιμο στο: <<http://www.mysql.com>> [16 Αυγούστου 2008].

Nitzberg, S 1998, 'Conflict and the computer: information warfare and related ethical issues', *Proceedings of the twenty-first national information systems security conference*. Διαθέσιμο στο: <<http://csrc.nist.gov/nissc/1998/proceedings/paperD7.pdf>> [24 Αυγούστου 2008].

O' Brien, KJ 2008, 'Sun buying swedish software firm for \$1 billion', *The New York Times*, 16 Ιανουαρίου. Διαθέσιμο στο: <<http://www.nytimes.com/2008/01/17/technology/17sun.html?scp=4&sq=MySQL%20Sun%20Microsystems%20&st=cse>> [16 Αυγούστου 2008].

O' Sullivan, M 2002, 'Making copyright ambidextrous: an expose of copyleft', *The Journal of Information, Law and Technology*, no. 3. Διαθέσιμο στο: <[http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002\\_3/osullivan](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_3/osullivan)> [16 Αυγούστου 2008].

*Personality test based on Jung-Myers-Briggs typology* 2008, HumanMetrics.com. Διαθέσιμο στο: <<http://www.humanmetrics.com/cgi-win/JTypes1.htm>> [20 Δεκεμβρίου 2008].

*Phrack Magazine* 2008, Phrack Magazine. Διαθέσιμο στο: <<http://www.phrack.org>> [4 Νοεμβρίου 2008].

Poulsen, K 2000, MostHateD to Plead Guilty Wednesday, *Security Focus*, 29 Μαρτίου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/11>> [12 Σεπτεμβρίου 2008].

Poulsen, K 2001, 'Ethics challenge softens hacker con: cyber ethics contest will join hacker jeopardy and spot the fed at DefCon', *Security Focus*, 31 Μαΐου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/211>> [15 Νοεμβρίου 2008].

Poulsen, K 2001, 'Hackers face life imprisonment under 'Anti-Terrorism' Act', *Security Focus*, 24 Σεπτεμβρίου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/257>> [12 Σεπτεμβρίου 2008].

Poulsen, K 2001, 'Max vision begins 18-month term', *Security Focus*. Διαθέσιμο στο <<http://www.securityfocus.com/news/221>> [12 Σεπτεμβρίου 2008].

Poulsen, K 2003, 'Adrian Lamo charged with computer crimes', *Security Focus*. 9 Μαΐου. Διαθέσιμο στο: <<http://www.securityfocus.com/news/6888>> [12 Σεπτεμβρίου 2008].

"Prison urged for Mafiaboy 2007", *Wired magazine*, 20 Μαΐου. Διαθέσιμο στο: <<http://www.wired.com/politics/law/news/2001/06/44673>> [12 Σεπτεμβρίου 2008].

Quittner, J 1999, 'Tim Berners-Lee: from the thousands of interconnected threads of the Internet, he wove the World Wide Web and created a mass medium for the 21st

century', *Time*, 29 Μαρτίου. Διαθέσιμο στο: <http://www.time.com/time/time100/scientist/profile/bernerslee.html> [17 Σεπτεμβρίου 2008].

Ramirez, A 1992, 'Are indicted in computer credit theft', *The New York Times*, 9 Ιουλίου. Διαθέσιμο στο: <http://query.nytimes.com/gst/fullpage.html?res=9E0CE7D6133DF93AA35754C0A964958260&sec=&spon=&scp=1&sq=%20Phiber%20Optik%201991%20&st=cse> [12 Σεπτεμβρίου 2008].

Raymond, ES 2001, *How to be a hacker*. Διαθέσιμο στο: <http://www.catb.org/~esr/faqs/hacker-howto.html> [23 Αυγούστου 2008].

Raymond, ES 2003, *The Jargon File*. Διαθέσιμο στο: <http://catb.org/jargon> [28 Δεκεμβρίου 2008].

Richtel, M 2000, 'Canada arrests 15-year-old in web attack', *The New York Times*, 20 Απριλίου. Διαθέσιμο στο: <http://query.nytimes.com/gst/fullpage.html?res=9F04E0DC1131F933A15757C0A9669C8B63&sec=&spon=&scp=2&sq=Mafiaboy&st=cse> [12 Σεπτεμβρίου 2008].

Rogers, MK 2001, *A social learning theory and moral disengagement analysis of criminal computer behavior*, PhD thesis, University of Manitoba, Winnipeg. Διαθέσιμο στο: [https://www.cerias.purdue.edu/assets/pdf/bibtex\\_archive/rogers\\_01.pdf](https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf) [28 Αυγούστου 2008].

Ronfeldt, D & Arquilla, J 2001, 'Networks, netwars and the fight for the future', *First Monday Magazine*, vol. 6, no. 10. Διαθέσιμο στο: <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889> [24 Αυγούστου 2001].

Rothstein, E 2004, 'Connections; liberty, technology, duty: where peace overlaps war', *The New York Times*, 8 Μαΐου. Διαθέσιμο στο: <http://query.nytimes.com/gst/fullpage.html?res=9C05E2D8173CF93BA35756C0A9>

629C8B63&sec=&spon=&&scp=9&sq=Richard%20Stallman%20hacker&st=cse>.

[27 Σεπτεμβρίου 2008].

Ruffin, O 2002, 'Waging peace on the internet', *The Register*. Διαθέσιμο στο:

<<http://thehacktivist.com/archive/news/2002/WagingPeace-TheReg-2002.pdf>> [28

Νοεμβρίου 2008].

Rusling DA 1998, *The Linux kernel*. Διαθέσιμο στο:

<[http://kos.enix.org/pub/linux\\_kernel.pdf](http://kos.enix.org/pub/linux_kernel.pdf)> [17 Σεπτεμβρίου 2008].

Saleem, S 2006, 'Ethical hacking as a risk management technique' *Proceeding from*

*the third annual conference on information security curriculum development*, pp.

201–203. Διαθέσιμο στο: ACM Portal [15 Δεκεμβρίου 2008].

Schmemann, S 1987, 'Computer buffs tapped NASA files', *The New York Times*, 16

Σεπτεμβρίου.

Διαθέσιμο

στο:

<<http://query.nytimes.com/gst/fullpage.html?res=9B0DE1DA1530F935A2575AC0A>

961948260&scp=1&sq=nasa%20%20hackers%20%20Chaos%20Computer%20Club

%201987&st=cse> [19 Ιανουαρίου 2008]

Schoolman, J 2000, 'Computer chip maker set for powerful IPO', *NY Daily News*, 7

Νοεμβρίου.

Διαθέσιμο

στο:

<<http://www.nydailynews.com/archives/money/2000/11/07/2000-11->

07\_computer\_chip\_maker\_set\_for\_.html> [20 Σεπτεμβρίου 2008].

Schwartau, W. 1999, "Cyber-vigilantes hunt down hackers", *CCN*, 12 Ιανουαρίου.

Διαθέσιμο

στο:

<<http://edition.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/>>

. [13

Δεκεμβρίου 2008].

Schwartz, J 2001, 'Fighting crime online: who is in harm's way?', *The New York*

*Times*,

8

Φεβρουαρίου.

Διαθέσιμο

στο:

<<http://query.nytimes.com/gst/fullpage.html?res=9B0DE2D91631F93BA35751C0A9>

679C8B63&sec=&spon=&&scp=1&sq=Back%20Orifice%202000%20&st=cse> [19

Ιανουαρίου 2008].



Sdictionary community, 2009, *Greek etymological dictionary*, AXMA Soft. Διαθέσιμο στο: <[http://sdict.com/cgi-bin/sdict.cgi/browse?dicname=ilhs\\_mel.dct&letter=&word=&offset=&](http://sdict.com/cgi-bin/sdict.cgi/browse?dicname=ilhs_mel.dct&letter=&word=&offset=&) Greek Etymological Dictionary> [18 Νοεμβρίου 2008].

Seadle, M 2005, 'Copyright in the networked world: author's rights', *Library Hi Tech*, vol. 23, no. 1, pp. 130–136. Διαθέσιμο στο: Emerald [19 Αυγούστου 2008].

Shannon, V 2004, 'Pioneer who kept the web free honored with a technology prize', *The New York Times*, 14 Ιουνίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9801EED61330F937A25755C0A9629C8B63&scp=1&sq=Tim%20Berners-Lee%20Millenium%20Technology%20Prize&st=cse>> [16 Σεπτεμβρίου 2008].

Soderberg, J 2002, 'Copyleft vs. copyright: a marxist critique', *First Monday Journal*, vol. 7, no. 3, 4 Μαρτίου. Διαθέσιμο στο: <[http://firstmonday.org/issues/issue7\\_3/soderberg/index.html](http://firstmonday.org/issues/issue7_3/soderberg/index.html)> [10 Αυγούστου 2008].

Spangler, R 2003, *Packet Sniffer Detection with AntiSniff*, Department of Computer and Network Administration, University of Wisconsin. Διαθέσιμο στο: <<http://www.linux-sec.com/Sniffer.Detectors/snifferdetection.pdf>> [29 Ιανουαρίου 2008].

Sterling, B 1994, *The hacker crackdown: law and disorder on the electronic frontier*, Bantam Books, New York. Διαθέσιμο στο: <<http://www.mit.edu/hacker/hacker.html>> [15 Νοεμβρίου 2008].

Still, B 2005, 'Hacking for a cause', *First Monday Journal*, vol. 10, no. 9. Διαθέσιμο στο: <<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1274>> [24 Αυγούστου 2008].

Strunsky, S 2002, 'Metro briefing New Jersey: Newark: prison sentence in computer case', *The New York Times*, 27 Φεβρουαρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9C07EFD91431F934A15751C0A9649C8B63&scp=3&sq=Timothy%20Lloyd%20Omega%20Engineering%20Corporation&st=cse>> [12 Σεπτεμβρίου 2008].

Tabor, BW & Ramirez, A 1992, 'Computer savvy with an attitude: young working-class hackers accused of high-tech crime', *The New York Times*, 23 Ιουλίου. Διαθέσιμο στο: <[http://query.nytimes.com/gst/fullpage.html?res=9E0CE0DD123EF930A15754C0A964958260&sec=technology&spon=&&scp=3&sq=Masters%20of%20Deception%20\(MOD\)&st=cse](http://query.nytimes.com/gst/fullpage.html?res=9E0CE0DD123EF930A15754C0A964958260&sec=technology&spon=&&scp=3&sq=Masters%20of%20Deception%20(MOD)&st=cse)> [22 Νοεμβρίου 2008].

Tahmincioglu, E.2001, 'Management: vigilance in the face of layoff rage: employer miscues can breed retaliation', *The New York Times*, 1 Αυγούστου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9C04EFDB1F3DF932A3575BC0A9679C8B63&sec=&spon=&&scp=4&sq=Timothy%20Lloyd%20Omega%20Engineering%20Corporation&st=cse>> [12 Σεπτεμβρίου 2008].

"The history of the Legion of Doom" 1990, *Phrack Magazine*, vol. 3, no. 31. Διαθέσιμο στο: <<http://www.phrack.org/issues.html?issue=31&id=5#article>> [15 Δεκεμβρίου 2008].

*The Legion of Doom: hackers technical journal*, The Legion of Doom. Διαθέσιμο στο: <<http://www.textfiles.com/magazines/LOD>> [15 Νοεμβρίου 2008].

The Mentor 1986, 'The conscience of a hacker', *Phrack Magazine*, vol. 7, no. 3. Διαθέσιμο στο: <<http://www.phrack.org/issues.html?issue=7&id=3>> [2 Νοεμβρίου 2008].

Thomas, JLC 2001, *Ethics of hacktivism*, Hacker Kulture. Διαθέσιμο στο: <[http://www.dvara.net/HK/Julie\\_Thomas\\_GSEC.pdf](http://www.dvara.net/HK/Julie_Thomas_GSEC.pdf)> [24 Αυγούστου 2008].

Thompson, C 2003, 'The way we live now: 1-12-03: questions for Kevin Mitnick: connected again', *The New York Times*, 12 Ιανουαρίου. Διαθέσιμο στο : <<http://query.nytimes.com/gst/fullpage.html?res=9A0DE3DA133EF931A25752C0A9659C8B63&scp=4&sq=Free%20Kevin&st=cse>> [9 Σεπτεμβρίου 2008]

Thompson, N 2004, 'For hackers, shop talk, a warning and advice', *The New York Time*, 12 Ιουλίου. Διαθέσιμο στο: <<http://www.nytimes.com/2004/07/12/technology/12hack.html?ex=1231995600&en=dbbcaeb039042d20&ei=5070>> [15 Σεπτεμβρίου 2008].

Timothy, S U 1996, 'Cyberspace sovereignty: the Internet and the international system', *Harvard Journal of Law & Technology*, vol. 10, no. 3. Διαθέσιμο στο: <<http://scholar.google.gr/scholar?q=info:nUhCDdzpP8J:scholar.google.com/&hl=en&lr=&output=viewport&shm=1>> [12 Σεπτεμβρίου 2008].

Turgeman, G.O. 2005, "Hackers' Accounts Hacking as a Social Entertainment", *Social Science Computer Review*, vol. 23, no. 1, pp. 8-23. Διαθέσιμο στο: Sage Publication. [20 Νοεμβρίου 2008].

Walterscheid, EC 1998, 'Thomas Jefferson and the patent act of 1793', *Essays in History*, vol. 40, Corcoran Department of History, University of Virginia. Διαθέσιμο στο: <<http://etext.virginia.edu/journals/EH/EH40/walter40.html>> [19 Αυγούστου 2008].

Wayner, P. 1997, 'Who's hacking whom?: hope springs in Manhattan', *The New York Times*, 11 Αυγούστου. Διαθέσιμο στο: <<http://partners.nytimes.com/library/cyber/hackstock/081197hope.html?scp=5&sq=John%20Draper%20hacker&st=cse>> [10 Σεπτεμβρίου 2008].

Weiser, B 2003, 'Computer use limited for accused hacker free on bond', *The New York Times*, 13 Σεπτεμβρίου. Διαθέσιμο στο: <<http://query.nytimes.com/gst/fullpage.html?res=9804E6D7113BF930A2575AC0A9659C8B63>> [12 Σεπτεμβρίου 2008].

Winkler, I & Dealy, B 1995, 'Information security technology?: don't rely on it.: a case study in social engineering', *Proceedings of the fifth Usenix Unix Security Symposium*, The usenix Association. Διαθέσιμο στο <[http://www.usenix.org/publications/library/proceedings/security95/full\\_papers/winkler.pdf](http://www.usenix.org/publications/library/proceedings/security95/full_papers/winkler.pdf)> [22 Νοεμβρίου 2008].

Wusteman, J 2004, 'Patently ridiculous', *Library Hi Tech*, vol. 22, no. 2, pp. 231–237. Διαθέσιμο στο: Emerald [28 Σεπτεμβρίου 2008].

Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

Young, R, Zhang, L & Prybutok, V 2007, 'Hacking into the minds of hackers', *Information Systems Management Journal*, vol. 24, no. 4, pp. 281-283. Διαθέσιμο στο: Informaworld [13 Δεκεμβρίου 2008].

Zeltser, L 2000, 'The evolution of malicious agents', *Web Report*, Απρίλιος. Διαθέσιμο στο: <<http://www.securitytechnet.com/resource/security/virus/agents.pdf>> [19 Ιανουαρίου 2008].

### **Ελληνική έντυπη**

Dreyfus, H.L. 2003, *Το διαδίκτυο*, Κριτική, Αθήνα.

Furnell, S 2006, *Κυβερνοέγκλημα: καταστρέφοντας την κοινωνία της πληροφορίας*, Παπαζήσης, Αθήνα

McKenzie, W 2006, *Ένα μανιφέστο των χάκερ*, Scripta, Αθήνα.

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

Λέανδρος, Ν. 2005, *Το διαδίκτυο : ανάπτυξη και αλλαγή*, Καστανιώτης, Αθήνα.

Σαραφάς, Κ 2008, *Hackers: μύθος ή πραγματικότητα?*, Προπομπός, Αθήνα. Τσουραμάνης, Χ 2005, *Ψηφιακή εγκληματικότητα : η (αν)ασφαλής όψη του διαδικτύου*, Εκδόσεις Βασ. Ν. Κατσαρού, Αθήνα.

Παπαδημητρίου, Χ 2004, *Ισόβια στους χάκερ: απόψεις για το Ίντερνετ, την επιστήμη και όλα τα υπόλοιπα*, Καστανιώτης, Αθήνα.

## Ελληνικές ιστοσελίδες

Ανδρέου , ΑΚ. 2008, Ελεύθερο Λογισμικό / Λογισμικό Ανοικτού Κώδικα (ΕΛ/ΛΑΚ). 14 Μαρτίου 2008. *Η βιβλιοθηκονομία στην Κύπρο σήμερα: Blog*. Διαθέσιμο στο: <[http://keber.blogspot.com/2008/03/blog-post\\_14.html](http://keber.blogspot.com/2008/03/blog-post_14.html)> [13 Αυγούστου 2008].

Βενιού, Ε 2008, 'Τι κρύβουν τα νέα βιομετρικά διαβατήρια', *Το Βήμαonline*, 30 Νοεμβρίου. Διαθέσιμο στο: <<http://www.tovima.gr/default.asp?pid=2&ct=33&artId=244778>> [19 Ιανουαρίου 2008].

Καλλινίκου, Δ, Καρούνος, Θ & Παπαδόπουλος, Μ 2007, 'Οι ελληνοποιημένες άδειες creative commons', *Πρακτικά από το δέκατο έκτο πανελλήνιο συνέδριο ακαδημαϊκών βιβλιοθηκών*. Διαθέσιμο στο: <<http://www.marinos.com.gr/bbpdf/pdfs/msg63.pdf>> [13 Αυγούστου 2008].

Καραγιαννόπουλος, Β 2005, *Hackers*, Εργαστήριο Ποινικών και Εγκληματολογικών Ερευνών. Διαθέσιμο στο: <[www.theartofcrime.gr/artofcrime/assets/hackers.doc](http://www.theartofcrime.gr/artofcrime/assets/hackers.doc)> [28 Δεκεμβρίου 2008].

Κατσουλης, Α 2007, 'Οι φύλακες... χάκερ των προσωπικών δεδομένων', *Το Έθνος*, 24 Μαΐου. Διαθέσιμο στο: <<http://www.ethnos.gr/article.asp?catid=11429&subid=2&pubid=1020438>> [19 Ιανουαρίου 2008]

Λαϊνός Θ 2000, 'Οι θεοί της τεχνολογίας', *Το Βήμαonline*, 16 Ιουλίου. Διαθέσιμο στο: <[http://www.tovima.gr/print\\_article.php?e=B&f=12993&m=C09&aa=.1](http://www.tovima.gr/print_article.php?e=B&f=12993&m=C09&aa=.1)> [16 Σεπτεμβρίου 2008].

Μπουντουρίδης, Μ 2006, Κριτική της εργασίας στην κοινωνία της πληροφορίας. 21 Αυγούστου 2006. *Κοινωνικά Κινήματα & Δίκτυα: Blog*. Διαθέσιμο στο: <<http://thrymmata.blogspot.com/2006/08/blog-post.html>> [4 Αυγούστου 2008].

Ναλμπάντης, ΚΣ 2008, 'Η υπερβολική χρήση του Internet', *Τετράδιο.gr*, 21 Μαΐου. Διαθέσιμο στο:

<[http://www.tetradio.gr/html/modules/pico2/index.php?content\\_id=2](http://www.tetradio.gr/html/modules/pico2/index.php?content_id=2)> [20 Νοεμβρίου 2008].

Νταραδήμου, Α 2008, 'Ελεύθερο λογισμικό', *Ελεύθερος Τύπος*, 2 Μαΐου. Διαθέσιμο στο: <<http://www.e-tipos.com/newsitem?id=34547>> [6 Αυγούστου 2008].

Νταραδήμου, Α 2008, 'E-zines, τα περιοδικά της hi-tech εποχής', *Ελεύθερος Τύπος*, 9 Ιανουαρίου. Διαθέσιμο στο: <<http://www.e-tipos.com/newsitem?id=21504>> [29 Νοεμβρίου 2008].

Ο Μίμης Ανδρουλάκης διαθέτει ελεύθερα το βιβλίο του "Χαμένο Μπλουζ" με άδεια Creative Commons 2008, Creative Commons. Διαθέσιμο στο : <[http://www.creativecommons.gr/news/newsvieeach/index.php?ctn=7&context\\_url=0P7UnewsvieeachCSFall&page=0&language=el](http://www.creativecommons.gr/news/newsvieeach/index.php?ctn=7&context_url=0P7UnewsvieeachCSFall&page=0&language=el)> [13 Αυγούστου 2008].

Σπυράκης. Π 1997, "Έγκλημα στον κυβερνοχώρο", *Το Βήμαonline*, 13 Ιανουαρίου. Διαθέσιμο στο: <[http://tovima.dolnet.gr/print\\_article.php?e=B&f=12461&m=I20&aa=1](http://tovima.dolnet.gr/print_article.php?e=B&f=12461&m=I20&aa=1)> [12 Σεπτεμβρίου 2008].

Σπυρόπουλου, Λ 2008, 'Η κατάχρηση του Ίντερνετ φέρνει εθισμό', *Ελευθεροτυπία*, 18 Ιανουαρίου. Διαθέσιμο στο: <[http://www.enet.gr/online/online\\_text/c=112,dt=18.01.2008,id=62418256](http://www.enet.gr/online/online_text/c=112,dt=18.01.2008,id=62418256)> [20 Δεκεμβρίου 2008].

Σωνίδου, Μ 2008, 'Δικαιοσύνη των hacker', *Η Καθημερινή*, 1 Απριλίου. Διαθέσιμο στο: <[http://news.kathimerini.gr/4dcgi/\\_w\\_articles\\_world\\_2\\_01/04/2008\\_264705](http://news.kathimerini.gr/4dcgi/_w_articles_world_2_01/04/2008_264705)> [19 Ιανουαρίου 2008].

## ΕΥΡΕΤΗΡΙΟ

(Αγγλικοί όροι)

### A

Abene, 28, 41, 42, 66, 67  
Alder, 58  
Apple, 32, 35, 48, 49, 50, 106,  
ARPANET, 2, 3, 4, 5, 6, 8, 11, 12, 34, 37, 108

### B

Bell Telephone, 31

### C

Captain Crunch. *Βλέπε* John  
Chaos Computer Club, 62, 73  
Computer Emergency Response Team, 39  
Computer Sabotage. *Βλέπε* Timothy Lloyd  
Copyleft, 55, 56, 57, 84, 85, 86,  
Cracker, 8, 10, 14, 61, 78,  
Creative Commons, 86, 91, 92  
Cult of the Dead Cow, 69, 70, 72, 99

### D

Daphtpunk. *Βλέπε* Miffleton

### F

Free Software, 54, 56, 81, 82, 84, 85, 114

### G

GNU, 54, 55, 56, 57, 82, 83, 84, 88, 92  
GPL, 53, 55, 57, 85, 87, 92  
Gregory, 47

### H

Hacker  
Ηθική, 76  
Χαρακτηριστικά, 22, 23, 24, 25, 27, 28, 29  
Κίνητρα, 14, 15, 16, 17, 18, 19, 20, 21,  
Γκρίζοι, 15, 59, 60, 61  
Μαύρος, hacker 10, 14, 59, 60, 61  
Λευκοί, 14, 59, 60, 61  
Ορισμός, 7, 8, 9  
Hacking  
ιστορία hacking, 11, 12, 13  
επιδράσεις στη κοινωνία, 93, 94, 95, 96, 97, 98,  
99, 100, 101, 102,  
HTTP, 52

### I

IBM, 32, 55, 82  
Infonomicon Computer Club, 75, 76

### J

Jargon File, 10  
John Draper, 30, 32

### K

Kiddies, 16, 26, 78

### L

L0pht Heavy Industries, 72  
Lamo, 48, 123  
Legion of Doom, v, viii, 64, 65, 66  
Levin, 39, 40  
Linux, ii, xxi, 53, 54, 59, 85, 88, 98, 106  
Lloyd, 44

### M

Mafiaboy, 25, 45, 46  
*Βλέπε* Michael Calce  
Masters of Deception, 65, 66, 68  
Miffleton, 42  
MIT, 31, 52, 55, 56, 76, 82, 83, 84, 95  
Mitnick, 13, 32, 33, 34, 35, 36, 37, 58,  
Morris, 38, 39,  
MostHateD. *Βλέπε* Patrick W. Gregory

### N

National Science Foundation, 5  
National Security Agency, viii, 38, 67

### P

Phiber Optik. *Βλέπε* Mark Abene  
Phone hackers, 15, 21  
phreakers. *Βλέπε* phone hacker  
Poulsen, 37, 38,

### S

Shimomura 35, 36, 57, 58  
Smith, 43  
Stallman, 54, 55, 56, 57, 60, 61, 78, 82, 83, 84, 88

### T

TCP/IP, 5, 6  
THE UNDERGROUND PYRAMID, 18  
Tim Berners-Lee, 6, 51, 52, 60  
Torvalds, 53, 54, 60, 85

### U

Unix, 53, 68, 84,

UNIX, 5, 11, 56

## **W**

War Games, 9, 12

windows, 53

Wozniak, 48, 49, 50, 51



## ΕΥΡΕΤΗΡΙΟ

(Ελληνικοί όροι)

### **A**

Αγροτική κοινωνία, 1, 26

### **B**

Βιβλιοθήκες, 48, 91, 92, 93

### **Δ**

Διαδίκτυο,  
Ιστορία διαδικτύου, 3, 4, 5, 6 1

### **H**

Ηλεκτρονικό έγκλημα, 2, 3, 10, 14, 28, 103, 106  
Ηλεκτρονικό περιβάλλον, 26  
ΗΠΑ, 4, 5, 11, 12, 13, 40, 66, 67, 96

### **I**

Ιός  
I Love You, 13  
Melissa, 12, 13, 43

Para, 43

### **K**

Κοινωνία της πληροφορίας, 1,, 2, 3, 101, 103, 104,  
Κυβερνοπολεμιστές, 15  
Κυβερνοτρομοκράτες, 15

### **M**

MME, 9, 10, 22, 24, 28, 64, 67, 72, 80, 101, 103,  
106  
Μπλε κουτί, 31, 49, 109

### **Π**

Πειρατές λογισμικού, 16  
Πληροφοριακή επανάσταση, 2  
Πνευματικά δικαιώματα, xi, 56, 89, 91, 92

### **Σ**

Σαμουράι, 16, 22  
Σκουλήκι  
Morris worm, 13, 38, 39, 44

### **X**

Χακτιβιστές, 15, 98, 99