ΠΕΡΙΛΗΨΗ

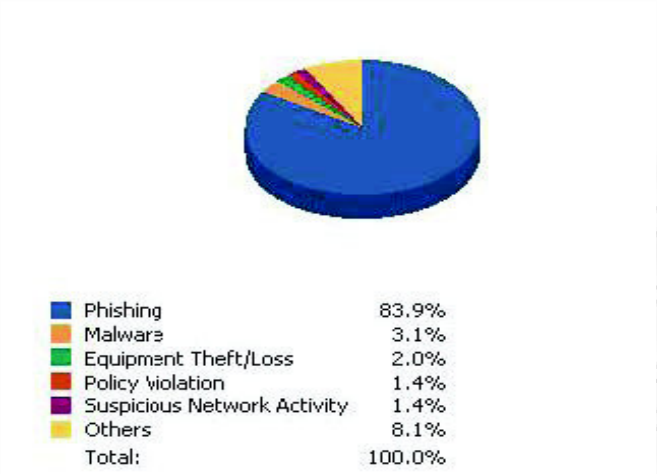
Η παρακάτω εργασία περιγράφει τις δυνατότητες που μας δίνει η σημερινή τεχνολογία στην αντιμετώπιση της Κυβερνο-τρομοκρατίας (cyber terrorism) με τη χρήση μεθόδων ηλεκτρονικής παραπλάνησης. Ο κυβερνοχώρος αποτελεί σήμερα ένα «πεδίο μάχης» αναρίθμητων επιθέσεων και «ενοχλήσεων», οι οποίες ξεκινούν από τον τομέα της Εθνικής Ασφάλειας και Άμυνας και επεκτείνονται σε όλες τις φάσεις τις καθημερινής μας ζωής. Πιθανόν να είναι απλά ζήτημα χρόνου τρομοκρατικές και εξτρεμιστικές ομάδες να κάνουν χρήση των παραπάνω δυνατοτήτων. Ερευνούμε λοιπόν ορισμένα ερωτήματα τα οποία έχουν προκύψει όσον αφορά τη συνιστάμενη απειλή της Κυβερνο-τρομοκρατίας εξετάζοντας διαφορετικά γεγονότα, κίνητρα, ενέργειες, στόχους και πως αυτοί σχετίζονται προκειμένου να καταλήξουμε σε ορισμένα συμπεράσματα. Ένας τρόπος είναι να εξάγουμε συμπεράσματα από τις περιπτώσεις παραπλάνησης και να τις εφαρμόσουμε ενάντια σε cyber-επιθέσεις. Όπως ακριβώς χρησιμοποιείται η τεχνική της παραπλάνησης στις στρατιωτικές εφαρμογές και το φυσικό περιβάλλον, έτσι μπορεί να χρησιμοποιηθεί και στον κυβερνοχώρο. Από τις διαφορετικές κατηγορίες επιτιθέμενων μπορούμε να διακρίνουμε τρόπους με τους οποίους μπορούν να εξαπατηθούν. Πολλές εξάλλου από τις τεχνικές που οι Κυβερνο-τρομοκράτες χρησιμοποιούν είναι παραπλήσιες με αυτές λιγότερο «κακόβουλων» hacker, με αποτέλεσμα να υπάρχει η δυνατότητα για ακριβή προσδιορισμό του τρόπου αντιμετώπισης τους.

ΕΙΣΑΓΩΓΗ

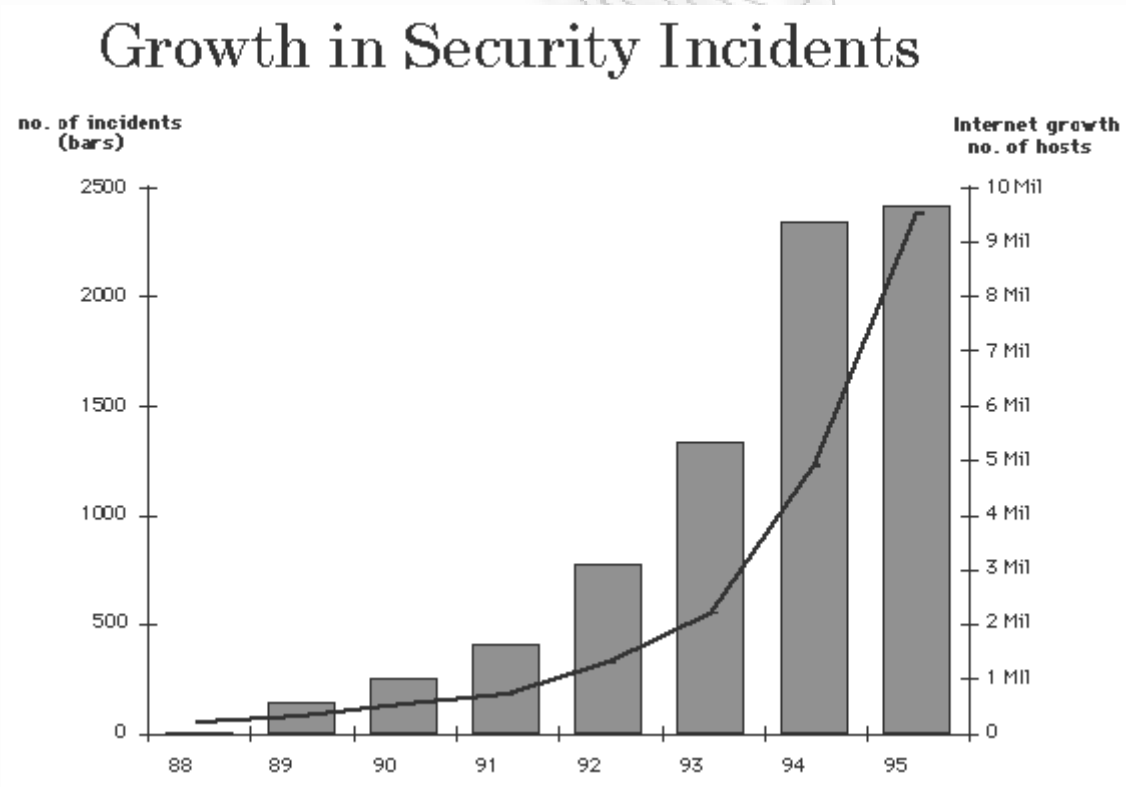
Τα τελευταία χρόνια μία σειρά από "καθημερινές" εργασίες έχουν ως απαραίτητο δομικό στοιχείο ένα δίκτυο Η/Υ καθώς και το Διαδίκτυο όπως ο προγραμματισμός των πτήσεων στο Ελευθέριος Βενιζέλος και η παραλαβή μιας βεβαίωσης από ένα Κ.Ε.Π. (Κέντρο Εξυπηρέτησης Πολιτών). Αυτή η ραγδαία διάδοση της τεχνολογίας ελλοχεύει και αρκετούς κινδύνους. Ένας από αυτούς είναι η χρήση της από Τρομοκρατικές Ομάδες με σκοπό τη δημιουργία συνθηκών αποσυντονισμού της κρατικής μηχανής, αναστάτωσης στο κοινωνικό σύνολο, οικονομικής ζημιάς σε εταιρείες και κράτη, παραπληροφόρησης και προπαγάνδας.

Πολλοί λοιπόν είναι εκείνοι που μιλούν τα τελευταία για την πιθανότητα ενός "Ηλεκτρονικού Περλ-Χάρμπορ", ιδιαίτερα μετά τις τρομοκρατικές επιθέσεις της 11^{ης} Σεπτεμβρίου σε Νέα Υόρκη και Ουάσιγκτον. Ως συνέπεια των επιθέσεων αυτών μία σειρά από ερωτήματα έχουν προκύψει για την πιθανότητα πραγματοποίησης ηλεκτρονικών επιθέσεων. Σύμφωνα με το Carnegie-Mellon Computer Emergency Response Team Coordination Center (CERT/CC) των ΗΠΑ από το 1988 και μετά έχουν καταγραφεί 300.000 "επεισόδια ασφαλείας" στο Διαδίκτυο στην χώρα αυτή (για την χώρα μας δεν υπάρχουν διαθέσιμα επίσημα καταγεγραμμένα στοιχεία). Οι περισσότερες από αυτές τις επιθέσεις καταγράφονται ανάμεσα στο 2002 και το 2006 (εικόνα 2 και 3).

Παράλληλα σύμφωνα με τις τελευταίες αναφορές το 84% των επιθέσεων αφορούν το λεγόμενο "phising", δηλαδή την εγκληματική δραστηριότητα κατά την οποία προσπαθεί ο hacker να αποκτήσει στοιχεία όπως αριθμός pin πιστωτικών καρτών και άλλες λεπτομέρειες των υποψήφιων θυμάτων του. Επίσης μόλις το 3% των καταγεγραμμένων περιπτώσεων αφορούν επιθέσεις με Trojan όπως φαίνεται στο παρακάτω διάγραμμα :



ΕΙΚΟΝΑ 1:Ποσόστωση συμβάντων ασφαλείας στο Διαδίκτυο(Πηγή:CERT/CC)



ΕΙΚΟΝΑ 2:Περιστατικά ασφαλείας 1988-1995 (Πηγή:CERT/CC)

Οι ένοχοι αυτών των επιθέσεων αν και είναι εξαιρετικά δύσκολο να ανακαλυφθούν και να επιβεβαιωθούν, συνήθως είναι hackers οι οποίοι μπορεί να ενεργούν αυτοβούλως είτε κάτω από τις εντολές κάποιου ατόμου ή οργανισμού. Για παράδειγμα σύμφωνα με διεθνή δημοσιεύματα ο Λαϊκός Στρατός της Κίνας έχει από το 1992 συστήσει μονάδες Hacking, όπως θα μπορούσαμε να τις ονομάσουμε, οι οποίες ασχολούνται αποκλειστικά στην εκπόνηση σχεδίων, τακτικών και μεθόδων Η/Ν επιθέσεων εναντίον εχθρικών προς τα Κινεζικά συμφέροντα κρατών π.χ. εναντίον των ΗΠΑ.

Το Νοέμβριο του 2006 καταγράφηκε επίθεση από ομάδα Κινέζων hacker στο δίκτυο το Αμερικανικού Naval War College με αποτέλεσμα για αρκετές εβδομάδες οι Η/Υ του τοπικού δικτύου να παραμείνουν κλειστοί. Η ειρωνεία όμως του Ιστορικού Περλ-Χάρμπορ που αναφέραμε παραπάνω είναι το γεγονός ότι παρά το ότι η συγκεκριμένη επιχείρηση αποτελεί πρότυπο στρατηγικής σύλληψης, συνεργασίας μεταξύ διαφορετικών όπλων, παραπλάνησης και εκτέλεσης το Αυτοκρατορικό Ιαπωνικό Ναυτικό τα χρόνια που ακολούθησαν ουσιαστικά αποδεκατίστηκε.

Η επιτυχία του ήταν πολύ σύντομη χωρίς ανάλογη συνέχεια στον θέατρο επιχειρήσεων του Ειρηνικού Ωκεανού. Έτσι αρκετοί είναι εκείνοι που θεωρούν πως ένα "Ηλεκτρονικό Περλ-Χάρμπορ" είναι πολύ πιο πιθανό από ένα "Ηλεκτρονικού Βατερλό", το οποίο θα προκαλέσει ριζική και ολοκληρωτική αλλαγή-καταστροφή στις οικονομικές, κρατικές και στρατιωτικές δομές, αλλάζοντας παράλληλα την διεθνή πολιτική κατάσταση.

Στην περίπτωση αυτή οι επίδοξοι επιτιθέμενοι θα εκτελέσουν συστηματική αναγνώριση για μήνες ή ακόμα και χρόνια, προκειμένου να αποκομίσουν κρίσιμες πληροφορίες, τις οποίες θα εκμεταλλευθούν στην περίπτωση των πραγματικών επιθέσεων. Από την άλλη, η συνεχώς αυξανόμενη καταγραφή περιστατικών ασφαλείας στο Διαδίκτυο μπορεί εύκολα να αντικρουσθεί από κάποιους ως αποτέλεσμα της διάδοσης του τα τελευταία χρόνια. Παράλληλα η αυξανόμενη πολυπλοκότητα των software των operating systems και των web browsers αυξάνει την τρωτότητά τους.

Την ίδια χρονική στιγμή οι μέθοδοι hacking γίνονται με την πάροδο του χρόνου πιο πολύπλοκοι αλλά και πιο διαθέσιμοι στο ευρύ κοινό δηλαδή πιο άμεσα εκμεταλλεύσιμοι από τον οποιοδήποτε .Σύμφωνα με τα επίσημα στοιχεία του US Department of Defense (Υπουργείο Άμυνας των ΗΠΑ) ο αριθμός των παράνομων επιθέσεων έχει αυξηθεί τα

τελευταία χρόνια τόσο σε ποσότητα όσο και σε ποιότητα ως λογικό αποτέλεσμα της συνεχούς εξέλιξης της τεχνολογίας και της προσβασιμότητας σε μεγαλύτερο μέρος του πληθυσμού. Προκειμένου να προστατευθούν οι "καθαροί" χρήστες του Διαδικτύου από άλλους, απαιτείται μία σειρά από ποικιλία μέτρων όπως νομικά μέτρα, μέτρα αποτροπής, μηχανισμοί προστασίας, μηχανισμοί αυτοπροστασίας, εκπαίδευση του καταναλωτή-χρήστη και φυσικά η εγρήγορση των Υπηρεσιών Ασφαλείας. Στην παρούσα πτυχιακή εργασία εξετάζεται αναλυτικά ένα συγκεκριμένο μέτρο προστασίας αυτό του software deception.

Στη συνέχεια θα αναφερθούμε εν συντομία στα κυριότερα σημεία κάθε κεφαλαίου και τον τρόπο με τον οποίο αυτά συνδέονται μεταξύ τους. Ουσιαστικά όλα αυτά μπορούν να συμπεριληφθούν στην έννοια των Information Operations (IO). Παρά το γεγονός πως υπάρχουν διάφοροι ορισμοί για αυτή την έννοια, εδώ θα χρησιμοποιήσουμε αυτόν που επίσημα δίνει το US Department of Defense ως αντιπροσωπευτικό: *«Information warfare(Πληροφοριακός Πόλεμος) είναι κάθε ενέργεια για την προστασία των πληροφοριακών μας δυνατοτήτων ανεξάρτητα από τα μέσα που χρησιμοποιούνται».*

Αναλυτικότερα, το "Information warfare" (Πληροφοριακός Πόλεμος) περιλαμβάνει όλες τις λαμβανόμενες ενέργειες για την προστασία της ακεραιότητας των πληροφοριακών μας συστημάτων από πιθανή εκμετάλλευση, διάρρηξη και αποσύνθεση, ενώ παράλληλα προσπαθεί να επιτύχει τα ανωτέρω εναντίον των εχθρικών πληροφοριακών συστημάτων με σκοπό την απόκτηση πληροφοριακού πλεονεκτήματος πριν την εφαρμογή οποιασδήποτε μορφής δύναμης π.χ. στρατιωτικής.

Στον παραπάνω ορισμό ένα μέρος αναφέρεται στην επιθετική πλευρά του I.W.. Στον κυβερνοχώρο, αυτό περιλαμβάνει επιθέσεις σε βάσεις δεδομένων, σε πληροφοριακά συστήματα και δίκτυα Η/Υ. Παραδείγματα τέτοια περιλαμβάνουν τοποθέτηση "μοχθηρών" κωδικών τύπου Trojan, ιών ή worm σε servers, Η/Υ και δίκτυα για την απόκτηση μη προστατευμένων βάσεων δεδομένων και την παράλυση συγκεκριμένων λειτουργιών π.χ. ενός κρίσιμου Υπουργείου. Όλα τα παραπάνω αποτελούν τις λεγόμενες ηλεκτρονικές επιθέσεις (cyber attacks). Πολλές από τις τεχνικές και τα μέσα που χρησιμοποιούνται σε αυτές εμφανίζονται και στην Κυβερνοτρομοκρατία, εμπίπτοντας στην κατηγορία του επιθετικού I.W..

Το άλλο μέρος αναφέρεται στον αμυντικό I.W.. Για τον κυβερνοχώρο αυτό περιλαμβάνει την προστασία της εμπιστευτικότητας και της ακεραιότητας των data (δεδομένων), καθώς και την απρόσκοπτη λειτουργία υπηρεσιών και δικτύων. Έτσι γίνεται χρήση κρυπτογράφησης για την προστασία δεδομένων, τοποθέτηση firewalls και χρήση συστημάτων εντοπισμού ανεπιθύμητων "επισκεπτών". Η αμυντική μορφή του I.W. περιλαμβάνει επίσης την ηλεκτρονική εξαπάτηση, την χρήση παραπλανητικών μεθόδων για την ματαίωση ή και την εξαπάτηση cyber επιθέσεων. Επομένως η χρήση του cyber deception ανήκει στην κατηγορία του αμυντικού I.W.. *(Denning 1999)*

Στο Κεφάλαιο Ι εξετάζεται η Τρομοκρατία, ως πηγή της Κυβερνοτρομοκρατίας. Αυτό που γίνεται κατανοητό από την αρχή είναι ότι η δυσκολία διατύπωσης ενός κοινά αποδεκτού ορισμού για την έννοια της τρομοκρατίας επηρεάζει άμεσα το διακριτό ορισμό της Κυβερνο-τρομοκρατίας. Θα ερευνηθούν αναλυτικά τα αίτια και οι μορφές της τρομοκρατίας, το ιστορικό της παρελθόν και ο τρόπος με τον οποίο οδηγεί στην Κυβερνοτρομοκρατία στις μέρες μας.

Κατά την ανάλυση της τελευταίας διαφορετικές αντιλήψεις, ιδεολογίες και θρησκευτικά πιστεύω οδηγούν σε τελείως διαφορετική αξιολόγηση του κινδύνου της συγκεκριμένης απειλής. Παράλληλα γίνεται ανάλυση των κινήτρων, των τεχνικών και των "στόχων" της Κυβερνο –τρομοκρατίας. Τέλος αναφέρονται τα μέτρα τα οποία εφαρμόζονται μέχρι σήμερα για την αντιμετώπιση της.

Στο Κεφάλαιο ΙΙ αναλύεται η παραπλάνηση (deception) στην ιστορία του ανθρώπου καθώς και στον Κυβερνοχώρο. Επίσης εξετάζονται διάφορες πλευρές-μορφές της παραπλάνησης, η δομή, η αξία της αλλά και το ρίσκο που υπάρχει κατά την εφαρμογή της. Παράλληλα εξερευνώνται το intelligence και counter deception, οι μορφές της παραπλάνησης που σχετίζονται περισσότερο με την τρομοκρατία .

Το Κεφάλαιο ΙΙΙ ασχολείται με την χρήση του deception για την παραπλάνηση των τρομοκρατών στον Κυβερνοχώρο. Παράλληλα εξετάζονται οι διάφορες θεωρίες cyber deception που υπάρχουν και ο τρόπος που χρησιμοποιούνται για την άμυνα των πληροφοριακών συστημάτων.

Τέλος, το Κεφάλαιο IV περιλαμβάνει συμπεράσματα από την συγκεκριμένη εργασία, τα κυριότερα σημεία αυτής και πεδία προβληματισμού για επόμενους μελετητές.

ΚΕΦΑΛΑΙΟ Ι: ΚΥΒΕΡΝΟΤΡΟΜΑΚΡΑΤΙΑ (CYBER TERRORISM)

Είναι προφανές ότι για να υπάρξει επαρκής ορισμός και κατανόηση της έννοιας της Κυβερνοτρομοκρατίας θα πρέπει κάποιος να ξεκινήσει πρώτα την ανάλυση του από την "κλασική" τρομοκρατία.

1.1 Προέλευση της τρομοκρατίας

Ιστορική ανασκόπηση

1.1.1 Αρχαία χρόνια

Παρά το γεγονός ότι σήμερα η παραπάνω έννοια ακούγεται και γράφεται σχεδόν καθημερινά στα ΜΜΕ, σε πλήθος εντύπων, βιβλίων και επίσημων κειμένων, ελάχιστοι είναι εκείνοι οι οποίοι συμφωνούν στο τι ακριβώς είναι η τρομοκρατία. Μία στερεότυπη φράση είναι ότι: αυτός που για κάποιους θεωρείται τρομοκράτης, για κάποιους άλλους θεωρείται μαχητής της ελευθερίας και απελευθερωτής με αποτέλεσμα η συμφωνία για κοινή αντίληψη της έννοιας να είναι αδύνατη. Άλλωστε καμία τέτοιου είδους εξτρεμιστική ομάδα δεν αυτοαποκαλείται τρομοκρατική αλλά προβάλλει την εθνική ή τη θρησκευτική της πλευρά π.χ. η Hezbollah στο Λίβανο, η οποία αυτοπροβάλλεται ως θρησκευτική και κοινωνική Σιιτική οργάνωση.

Όμως παρότι μετά την 11^{η} Σεπτεμβρίου οι ΗΠΑ κυρίως και οι σύμμαχοι τους ανακαλύπτουν παντού "εχθρούς", το φαινόμενο της τρομοκρατίας δεν είναι κάτι το καινούργιο. Αντιθέτως συναντάται σε όλες σχεδόν τις ιστορικές περιόδους ξεκινώντας ακόμα από τα Αρχαία χρόνια. Μία τρομοκρατική ομάδα με σύγχρονα χαρακτηριστικά ήταν αυτοί των Ζηλωτών στην Ιουδαία, οι οποίοι διέπρατταν δολοφονίες Ρωμαίων και Ιουδαίων που θεωρούσαν συνεργάτες τους.

Το κίνητρο τους ήταν η ασυμβίβαστη αντίληψη μη υποταγής στους Ιουδαίους τυράννους τους οποίους θεωρούσαν ανδρείκελα της Ρωμαϊκής Διοίκησης.*(5)* Οι Ασσασσίνοι (Assassins) ήταν άλλη μία ομάδα η οποία χαρακτηρίστηκε τρομοκρατική (Η λέξη αυτή ήρθε στην Ευρώπη από τους ναυτικούς, λόγω της φήμης που υπήρχε ότι οι Σιίτες αυτοί μουσουλμάνοι έκαναν χρήση χασίς (hashish) προκειμένου να αποκτούν θάρρος για τις παράτολμες ενέργειες τους.

Αυτοί αποτελούσαν μία ακραία Σιιτική οργάνωση, η οποία ονομάζονταν Nizari Ismalis και η οποία χρησιμοποιούσε τις δολοφονίες εχθρικών ηγετών ως μέθοδο για την αντιμετώπιση των εχθρών της, επειδή δεν μπορούσε να τους αντιμετωπίσει σε ανοιχτή μάχη. Αρχηγός τους ήταν ο Hassam-I Sabbah με κρησφύγετο τα βουνά του βόρειου Ιράν. Η τακτική που ακολουθούσαν ήταν εξαιρετικά απλή. Στρατολογούσαν νεαρούς άνδρες, πιστούς Σιίτες τους οποίους εκπαίδευαν για αρκετά χρόνια εθίζοντας τους παράλληλα στην συστηματική χρήση οπίου. Η αποστολή που τους ανέθεταν ήταν η δολοφονία κάποιου αξιωματούχου εχθρικής φατρίας και εκτελείτο πάντα από ένα μόνο άτομο χωρίς την οποιαδήποτε υποστήριξη. Η φήμη αυτής της οργάνωσης ήταν τόση μεγάλη που μόνο στο άκουσμα της δημιουργούσε πανικό ενώ το όνομα της έχει περάσει στο σύγχρονο λεξιλόγιο ως συνώνυμο του δολοφόνου.*(6)*

Οι δύο παραπάνω ομάδες έδρασαν στα Αρχαία και Μεσαιωνικά χρόνια, τα κίνητρα τους όμως, οι μέθοδοι τους, η οργάνωση τους, οι σκοποί τους και οι στόχοι τους είναι σχεδόν κοινές με αυτές των σύγχρονων τρομοκρατικών ομάδων. Παράλληλα τα αποτελέσματα – ιδιαίτερα τα ψυχολογικά – της δράσης τους είναι ιδιαίτερα έντονα και τώρα και τότε.

1.1.2 14ος -18ος αιώνας: Η γέννηση της σύγχρονης τρομοκρατίας

Από την εποχή των Ασσασίνων (τέλος 13ου αιώνα) ως τον 18ο αιώνα βαρβαρότητες και τρομοκρατικές μέθοδοι ήταν κάτι το πολύ συνηθισμένο στις συγκρούσεις μεταξύ κρατών. Μετά την συνθήκη της Βεστφαλίας το 1648 και τη γέννηση του σύγχρονου δυτικού έθνους – κράτους, αίτια τα οποία μπορούν να καταλήξουν στην τρομοκρατία (θρησκευτικά σχίσματα, επαναστάσεις, εθνικές διαμάχες) οδηγούσαν τελικά σε ανοιχτή πολεμική αναμέτρηση. Επίσης με την πάροδο του χρόνου τα "βασίλεια" μετασχηματίζονταν σε κρατικούς οργανισμούς έχοντας την δυνατότητα επιβολής της εξουσίας τους και περιορισμού-εξάλειψης τρομοκρατικών φαινομένων.

Η πρώτη χρήση των λέξεων "τρομοκράτης" και "τρομοκρατία" έγινε κατά την διάρκεια της Γαλλικής Επανάστασης το 1795 από την επαναστατική κυβέρνηση, καθιερώνοντας το "Βασίλειο του τρόμου". Τα μέλη της Επιτροπής δημόσιας ασφάλειας και του Εθνικού Συμβουλίου ονομάζονταν "τρομοκράτες" και εφάρμοσαν τεχνικές καταπίεσης του γαλλικού πληθυσμού, οι οποίες αποτέλεσαν παράδειγμα προς μίμηση στο μέλλον και από άλλα κράτη. Όμως οι πρακτικές αυτές των επαναστατών προκάλεσαν την ανάλογη αντίδραση

των φιλομοναρχικών οι οποίοι εφάρμοσαν τρομοκρατικές μεθόδους εναντίον των πρώτων όπως πολιτικές δολοφονίες και εκφοβισμούς.

Παράλληλα ο Παρισινός όχλος διαδραμάτισε καθοριστικό ρόλο για τις παραπάνω πρακτικές πριν, κατά τη διάρκεια και μετά τη Γαλλική Επανάσταση. Πολύ πριν τις περίφημες γκιλοτίνες οι δολοφονίες αριστοκρατών, εκκλησιαστικών αξιωματούχων και εύπορων φιλοβασιλικών οικογενειών ήταν συχνό φαινόμενο στους στενούς δρόμους του Παρισιού και τη γαλλική ύπαιθρο.

1.1.3 19ος αιώνας-Είσοδος στη σύγχρονη εποχή

Κατά τη διάρκεια του 19^{ου} αιώνα η εμφάνιση πρωτότυπων πολιτικών θεωριών, σε συνδυασμό με τη ραγδαία ανάπτυξη της τεχνολογίας των όπλων, ώθησε καθοριστικά την δημιουργία μικρών επαναστατικών ομάδων οι οποίοι επιτίθεντο στους κρατικούς θεσμούς με μεγάλη επιτυχία. Κυρίως οι "αναρχικοί" ήταν εκείνοι που υιοθέτησαν και πίστεψαν στην θεωρία της "προπαγάνδας των νεκρών" δολοφονώντας τους επικεφαλής κρατικών θεσμών της Ρωσίας, της Ιταλίας, της Γαλλίας, της Ισπανίας και των ΗΠΑ.

Σύμφωνα με την παραπάνω θεωρία στις πλατιές λαϊκές μάζες υπάρχει έμφυτη επαναστατικότητα η οποία όμως παραμένει "εν υπνώσει". Έτσι προκειμένου ο λαός να ξεσηκωθεί και να ζητήσει τα δικαιώματα του πρέπει να πραγματοποιηθούν πράξεις επαναστατικές, βίας, αντίστασης και να "υπάρχουν νεκροί στους δρόμους" σύμφωνα με την προσφιλή έκφραση των θιασωτών αυτής της άποψης.

Όμως η έλλειψη οργάνωσης και η άρνηση αυτών των αναρχικών ομάδων να συνεργαστούν και με άλλες κοινωνικές και πολιτικές δυνάμεις τους κατέστησε αναποτελεσματικούς ως πολιτική κίνηση. Αντίθετα ο Κομουνισμός αν και ως βάση για την ανάπτυξη τρομοκρατικών πρακτικών βρισκόταν τον 19^{ο} αιώνα σε αρχικό στάδιο, τα επόμενα χρόνια και κυρίως τον 20^{ο} αιώνα η δράση του αυτή θα ήταν καθοριστική στην μεταβολή του πολιτικού σκηνικού των Δυτικών κυρίως κρατών.

Παράλληλα τον 19^{ο} αιώνα αναπτύσσεται ραγδαία ο εθνικισμός στα πλαίσια κυρίως της δημιουργίας του κράτους – έθνους. Πληθυσμοί οι οποίοι βρίσκονται ως μειονότητα σε μία χώρα και οι οποίοι αισθάνονται ως πολίτες ΄β κατηγορίας καταφεύγουν σε εξτρεμιστικές πράξεις ανάλογες με αυτές των ζηλωτών στην Ιουδαία την Ρωμαϊκή εποχή. Χαρακτηριστικό

παράδειγμα αποτελεί η Βόρεια Ιρλανδία, με την πάλη μεταξύ Ιρλανδών καθολικών και της προτεσταντικής Αγγλικής Διοίκησης να ξεκινάει από τον 19ο αιώνα και να παραμένει ως τις μέρες μας.

Ένα άλλο παράδειγμα αποτελεί η Ρωσική τρομοκρατική οργάνωση Narodnya Volya (Η θέληση του λαού), η οποία παρουσιάζει χαρακτηριστικά που συναντάμε και στις σύγχρονες εξτρεμιστικές ομάδες: μυστικότητα, "κυτταρική" δομή, αλλά και ανυπομονησία και πολλές φορές αποτυχία επίτευξης των στόχων που έχουν θέσει με την χρήση τυφλής βίας. Η παραπάνω οργάνωση, όπως και αρκετές σημερινές επιδίωκαν όσον τον δυνατόν πιο βίαια, πολύνεκρα και θεαματικά χτυπήματα με σκοπό την απόκτηση φήμης και την πρόκληση της προσοχής των Μέσων Ενημέρωσης, αδιαφορώντας για τυχόν παράπλευρες απώλειες αθώων πολιτών.

1.1.4 20ος αιώνας-σύγχρονη εποχή

Κατά τη διάρκεια του πρώτου μισού του 20ου αιώνα δύο ήταν τα κυριότερα γεγονότα τα οποία επηρέασαν καθοριστικά την εξέλιξη και τελική μορφή του Δικαίου του Πολέμου, ο Ά και ο Ί Παγκόσμιος Πόλεμος. Αυτοί αναθέρμαναν πάθη, μίση μεταξύ εθνών και εθνοτικών ομάδων, θρησκειών, ιδεολογιών και αναπτέρωσαν τους εθνικούς πόθους ανά την υφήλιο καταστρέφοντας όμως την Διεθνή νομιμότητα.

1.1.5 Καταργώντας κάθε έννοια νομιμότητας

Οι μέθοδοι ολοκληρωτικού πολέμου που χρησιμοποιήθηκαν κατά την διάρκεια του Ί Παγκοσμίου Πολέμου δημιούργησαν την πεποίθηση σε ορισμένους ότι η ανεξέλεγκτη χρήση τρομοκρατικών μεθόδων είναι επιτρεπτή, αν όχι ακόμα και δικαιολογημένη προκειμένου να νικηθεί ο αντίπαλος. Η αντίληψη αυτή ξεκίνησε κατά τον Ά Παγκόσμιο Πόλεμο και εδραιώθηκε κατά τη διάρκεια του Ί, όπου εχθροί θεωρούνταν ακόμα και οι άμαχοι πολίτες, ενώ η καταστροφή της οικονομικής δυνατότητας του αντιπάλου ήταν κάτι κοινό και συνηθισμένο. Παράλληλα οι "Μεγάλες Δυνάμεις" της εποχής υποστήριζαν με υλικά και όπλα τις αντιστασιακές οργανώσεις, στην Ευρώπη κυρίως των οποίων οι τακτικές θα μπορούσαν να χαρακτηριστούν και ως τρομοκρατικές.

1.1.6 Η ραγδαία άνοδος του Εθνικισμού

Από τα μέσα ως το τέλος του 20ου αιώνα ο εθνικισμός παρουσιάζει ραγδαία άνοδο, ιδιαίτερα μετά τον Ά Παγκόσμιο Πόλεμο. Αποτέλεσε μία κυρίαρχη ιδεολογική φόρμουλα εναντίον των αποικιακών δυνάμεων της εποχής (Βρετανία, Γαλλία, Βέλγιο κ.α.), παρά το γεγονός της αποτίναξης του αποικιακού ζυγού και μέσω της πολιτικής της "μη βίας" όπως αυτή ξεκάθαρα εφαρμόσθηκε στην Ινδία από τον Μαχάτμα Γκάντι και μάλιστα με επιτυχία.

Πολλές λοιπόν εθνικές ομάδες, οι οποίες παρέμεναν υπό την κυριαρχία κράτους που δεν επιθυμούσαν ή που δεν είδαν τα όνειρα της εθνικής τους ανεξαρτησίας και αυτοδιάθεσης να πραγματοποιούνται κατέφυγαν στον εξτρεμισμό με σκοπό να γίνουν συμπαθείς στις μεγάλες δυνάμεις και τη διεθνή κοινότητα. Στην Ευρωπαϊκή ήπειρο είναι βασικό το παράδειγμα των Ιρλανδών κατοίκων της Βόρειας Ιρλανδίας με τον IRA να χρησιμοποιεί τρομοκρατικές μεθόδους για την αυτονομία της περιοχής.

1.1.7 Εποχή του Ψυχρού Πολέμου

Η εποχή του Ψυχρού Πολέμου άλλαξε τα μέχρι εκείνη την εποχή δεδομένα των διακρατικών συγκρούσεων. Οι δύο μεγάλοι στρατιωτικοί και πολιτικοί σχηματισμοί που υπήρχαν ήταν από την μία πλευρά το ΝΑΤΟ (Βορειοατλαντική Συμμαχία με κυρίαρχη δύναμη τις ΗΠΑ) η οποία αντιπροσώπευε το καπιταλιστικό μοντέλο οικονομικής και κοινωνικής οργάνωσης και από την άλλη το Σύμφωνο της Βαρσοβίας (με κυρίαρχη δύναμη την ΕΣΣΔ)το οποίο αντιπροσώπευε το κομουνιστικό μοντέλο. Η συγκέντρωση τόσο συμβατικών όπλων (Π/Β, τανκ, Α/ΦΗ, Π πλοία), όσο και πυρηνικών κεφαλών υπήρξε πρωτοφανής στην ανθρώπινη ιστορία.

Ο κίνδυνος λοιπόν κλιμάκωσης της έντασης και η κατάληξη σε έναν πυρηνικό όλεθρο ήταν ένα αρκετά πιθανό σενάριο το οποίο και οι δύο αντίπαλοι μάλλον προσπαθούσαν να αποφύγουν. Έτσι καταλήξαμε στους λεγόμενους "πληρεξούσιους πολέμους" σε περιοχές κατά κύριο λόγο περιφερειακές όπως η Αφρική και η Ασία. Εδώ η χρήση τρομοκρατικών μεθόδων δράσης τόσο από τα διάφορα επαναστατικά κινήματα όσο και από τις κυβερνητικές δυνάμεις ήταν κάτι απόλυτα συνηθισμένο.

Κυρίως όμως η ΕΣΣΔ ήταν αυτή που κατά τη διάρκεια του Ψυχρού Πολέμου εξόπλισε και εκπαίδευσε τέτοιες ομάδες οι οποίες αποσκοπούσαν στην απελευθέρωση από τις Δυτικές

αποικιακές δυνάμεις. Παράλληλα με υλική υποστήριξη υπήρξε και υποστήριξη στον ιδεολογικό τομέα (πόλεμοι της εθνικής ανεξαρτησίας) αλλά και στους διάφορους Διεθνείς οργανισμούς πράγμα το οποίο τους προσέφερε κάποιας μορφής νομιμοποίηση στις ενέργειες τους.

1.1.8 Η Διεθνοποίηση της τρομοκρατίας

Πολλοί είναι οι μελετητές του φαινόμενου τρομοκρατίας οι οποίοι θεωρούν το έτος 1968 ως το έτος έναρξης των σύγχρονων μορφών τρομοκρατικής δράσης, με την αεροπειρατεία από μέλη του Λαϊκού Μετώπου για την Απελευθέρωση της Παλαιστίνης, ενός αεροσκάφους της EL.AL (Ισραηλινές Αερογραμμές) εν πτήση από το Τελ-Αβίβ προς τη Ρώμη. Η συμβολική σημασία της πράξης αυτής θεωρείται κορυφαία με Άραβες τρομοκράτες να καταλαμβάνουν Ισραηλινό αεροσκάφος χρησιμοποιώντας τους επιβάτες ως ανθρώπινη ασπίδα και με στόχο να κάνουν τα αιτήματα τους γνωστά στην παγκόσμια κοινή γνώμη καθώς και την αντίσταση τους στην Ισραηλινή κυβέρνηση, κυρίως μέσω της Τηλεόρασης.

Μάλιστα σύμφωνα με τον Γιασέρ Αραφάτ ηγέτη και από τους ιδρυτές της οργάνωσης, η δημοσιότητα και ο σάλος που προκλήθηκε από την συγκεκριμένη πράξη ήταν πολύ μεγαλύτερος από τις συγκρούσεις μεταξύ Παλαιστινίων και Ισραηλινών στρατιωτών όλα τα προηγούμενα χρόνια *(11)*. Φυσικά η πιο "διάσημη" τρομοκρατική πράξη της οργάνωσης, υπήρξε η δολοφονία των Ισραηλινών αθλητών στους Ολυμπιακούς του Μονάχου το 1972 από Παλαιστίνιους τρομοκράτες.*(12)*

1.2 Ορισμός της Τρομοκρατίας

Όπως αναφέραμε και παραπάνω παρά τη συχνή χρήση του όρου τρομοκρατία τόσο από επίσημα όσο και από ανεπίσημα χείλη, ο ορισμός του απαιτεί την προσεκτική μελέτη των σύγχρονων κοινωνικών και πολιτικών συνθηκών που επικρατούν. Σύμφωνα λοιπόν με τον Brian Jenkins –ειδικό σε θέματα τρομοκρατίας – "η τρομοκρατία είναι ένα θέατρο".*(13)*

Έτσι όπως μία θεατρική παράσταση παρακολουθείτε από μεγάλο κοινό, περνάει το μήνυμα της και προσελκύει τα φώτα της δημοσιότητας το ίδιο γίνεται και από μία τρομοκρατική πράξη. Οι στόχοι μίας τέτοιας πράξης τις περισσότερες φορές έχουν δυσάρεστα αποτελέσματα στις τοπικές κοινωνίες αλλά και την παγκόσμια κοινότητα.

Τα σύγχρονα Μ.Μ.Ε. εξασφαλίζουν τη "σκηνή" και το "κοινό" και όπως στις θεατρικές παραστάσεις, το "κλειδί" είναι τα συναισθήματα που θα προκληθούν στους θεατές και όχι στους ηθοποιούς. Όμως αν και από την ιστορική αναδρομή της τρομοκρατίας διαπιστώνουμε ότι το φαινόμενο δεν είναι καινούριο και μάλιστα καταγράφεται πολύ πριν από της δημιουργία των σύγχρονων εθνών –κρατών, υπάρχουν πολλά διλήμματα τα οποία προκύπτουν από την ανάλυση αυτού του περίπλοκου φαινομένου. Για παράδειγμα ένας ιρακινός βομβιστής αυτοκτονίας είναι τρομοκράτης ή επαναστάτης για την ελευθερία της πατρίδας του.

Η δράση του ως μεμονωμένο άτομο μπορεί να συγκριθεί με το ευρύτερο κύμα τρομοκρατίας κατά την διάρκεια της Γαλλικής Επανάστασης το 1790 ή με τις πρακτικές της "τρομοκρατίας του προλεταριάτου" από τους Μπολσεβίκους στη Ρωσία Επιπλέον η δράση όλων των παραπάνω ποια σχέση έχει (αν έχει) με την οργάνωση Baader-Meinhof της Δυτικής Γερμανίας ή τη Weather Underground στις ΗΠΑ. Παράλληλα η αξιοσημείωτη τα τελευταία χρόνια αύξηση των αιτιών και των προϋποθέσεων για πράξεις τρομοκρατίας σε συνδυασμό με την προσαρμοστικότητα του φαινομένου στις εκάστοτε ανά εποχή συνθήκες έχουν συμβάλλει στη σύγχυση για την ακριβή σημασία του όρου.

Μία προσπάθεια ορισμού της τρομοκρατίας μπορεί να είναι αυτή που έχει δοθεί από το Αμερικανικό Υπουργείο Άμυνας και η οποία μπορεί να κριθεί ως η πιο απλή και πλήρης όσον αφορά την περιγραφή του φαινομένου: "*The calculated use of unlawful violence or threat of unlawful violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideologicalal".*

«Τρομοκρατία είναι η εκ προθέσεως χρήση παράνομης βίας ή απειλής χρήσης βίας με σκοπό την πρόκληση φόβου και τον εξαναγκασμό κυβερνήσεων και κοινωνιών για την επίτευξη στόχων πολιτικών, θρησκευτικών ή ιδεολογικών». (14)

Ενδεικτικά να αναφέρουμε ότι σύμφωνα με τον Bruce Hoffman υπάρχουν 109 διαφορετικοί ορισμοί για την τρομοκρατία. *(15)* Παρακάτω θα παραθέσουμε μερικούς για την όσο δυνατόν καλύτερα κάλυψη του φαινομένου. Έτσι σύμφωνα με το FBI:

"Terrorism is the unlawful use of force and violence against persons or property to Intimidate or coerce a government, the civilian population, or any segment there of, in furtherance of political or social objectives".

«Τρομοκρατία είναι η παράνομη χρήση δύναμης και βίας εναντίον προσώπων ή περιουσιών με σκοπό τον εξαναγκασμό κυβερνήσεων, του άμαχου πληθυσμού ή μέρους αυτού για την προώθηση πολιτικών ή κοινωνικών στόχων». (16)

Ενώ σύμφωνα με το U.S Department of State και στον ορισμό που δίδεται στο 22 U.S.C. Section 2656f(d)(Εγχειρίδιο της Αμερικανικής Σχολής Πολέμου) έχουμε :

"Terrorism" means "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience". (17)

«Τρομοκρατία σημαίνει την προμελετημένη και πολιτικά υποκινούμενη βία εναντίον μη μάχιμων στόχων από μικρές εθνικές ομάδες ή μυστικούς πράκτορες άλλων κρατών, συνήθως με σκοπό την τον επηρεασμό του κοινού».

Από τους παραπάνω ορισμούς διαπιστώνει κανείς ότι ακόμα και από τους Οργανισμούς Ασφαλείας του ίδιου κράτους (στην προκειμένη περίπτωση οι ΗΠΑ) δε χρησιμοποιείται ο ίδιος ορισμός. Έτσι το FBI επιμένει περισσότερο στον παράνομο χαρακτήρα των τρομοκρατικών πράξεων δεδομένου του αστυνομικού του χαρακτήρα ως υπηρεσία ενώ το U.S. Department of State περισσότερο επικεντρώνεται στα πολιτικά κίνητρα και την δράση εχθρικών χωρών λόγω της αποστολής του σχετικά με την διπλωματία και τις διεθνείς σχέσεις .

Παράλληλα σύμφωνα με τα Ηνωμένα Έθνη τρομοκρατία είναι :

"An anxiety inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination - the direct targets of violence are not the main targets".

«Μία αγωνιώδης μέθοδος επαναλαμβανόμενης βίαιης δράσης από μυστικούς ή ημιμυστικούς μεμονωμένους δράστες, ομάδες ή κρατικούς υπαλλήλους για ιδιοσυγκρασιακούς, εγκληματικούς ή πολιτικούς λόγους, οι κύριοι στόχοι της οποίας – σε αντίθεση με αυτόν της πολιτικής δολοφονίας - δεν είναι η βία αυτή καθαυτή». (18)

Ενώ σύμφωνα με το U.S Department of State και στον ορισμό που δίδεται στο 22

Τέλος η Βρετανική κυβέρνηση χρησιμοποιεί ένα πιο συνοπτικό ορισμό της τρομοκρατίας:

"…the use of violence for political ends, and includes any use of violence for the purpose of putting the public, or any section of the public, in fear."(19)

«είναι η χρήση βίας για πολιτικούς λόγους και περιλαμβάνει κάθε χρήση βίας με στόχο να εκφοβίσει την κοινή γνώμη ή κάθε μέρος της».

Διαπιστώνουμε λοιπόν ότι υπάρχει μία τεράστια γκάμα ορισμών που μπορεί κάποιος να χρησιμοποιήσει. Από τη μελέτη αυτών καταλήγουμε στην συγκέντρωση κοινών στοιχείων τα οποία συναντάμε σε αυτούς και με βάση τους οποίους η τρομοκρατία χαρακτηρίζεται ως δράση :

- Πολιτική
- Ψυχολογική
- Βίαιη
- Δυναμική
- Καλά προετοιμασμένη

Πολιτική

Είναι προφανές ότι κάθε τρομοκρατική πράξη είναι πολιτική πράξη ή σκοπό έχει να προκαλέσει πολιτικό αποτέλεσμα. Χαρακτηριστικό είναι το παράδειγμα της 17^{ης} Νοέμβρη στην χώρα μας, αλλά και το πρόσφατο τρομοκρατικό χτύπημα στην Ισπανία κατά την προεκλογική περίοδο, το οποίο προκάλεσε απώλεια της κυβέρνησης από την Δεξιά παράταξη και νίκη του Σοσιαλιστικού Κόμματος. Η κυβερνητική αυτή αλλαγή είχε ως άμεσο αποτέλεσμα την αποχώρηση των Ισπανικών στρατευμάτων από το Ιράκ, όπως επιθυμούσε η τρομοκρατική οργάνωση Αλ-Κάιντα η οποία εκτέλεσε τις πολύνεκρες επιθέσεις. Άλλωστε για τους τρομοκράτες, το γνωστό ρητό του θεωρητικού του πολέμου Clausewitz ότι "ο πόλεμος είναι η συνέχιση της πολιτικής με άλλα μέσα" *(20)* αποτελεί δεδομένο. Φυσικά οι τελευταίοι απαλείφουν εσκεμμένα τις έννοιες των στρατιωτικών δυνάμεων, των παραδοσιακών μορφών πολέμου και εφαρμόζουν την βία κατευθείαν στον πολιτικό τους στόχο. Όπως αναφέρει και το U.S. Department of State "οι τελικοί στόχοι των τρομοκρατών είναι πολιτικοί. Πολιτικά δικαιολογούμενη τρομοκρατία πάντοτε περιλαμβάνει ένα βαθύ αίσθημα αδικίας, αυτή η

αδικία μπορεί να είναι κοινωνική ή οικονομική αλλά πάντοτε αποδίδεται σε μία συγκεκριμένη εξουσία". *(21)*

Ψυχολογική

Τα αποτελέσματα μίας πράξης τρομοκρατίας είναι κυρίως ψυχολογικά- κυρίως ο φόβος πέρα από τα θύματα που μπορεί αυτή να προκαλέσει. Οι τρομοκρατικές ομάδες έχουν ουσιαστικά διπλό κάθε φορά στόχο. Από την μία πλευρά αυτούς των οποίων τη φυσική εξόντωση επιθυμούν και από την άλλη την ομάδα του πληθυσμού που προσπαθούν να εκφοβίσούν. Έτσι "πολεμούν" ολόκληρη την κοινωνία ή μία συγκεκριμένη εθνική (βλ. Κοσσοβάροι εξτρεμιστές εναντίον Σέρβων) ή θρησκευτική (βλ. βομβιστικές επιθέσεις μεταξύ Σιιτών και Σουνιτών στο Ιράκ) ή πολιτική ομάδα.

Βίαιη

Η δράση όλων των τρομοκρατικών οργανώσεων χαρακτηρίζεται από τη βία ή την απειλή χρήσης βίας, τόσο κατά μεμονωμένων στόχων (π.χ. δολοφονίες) όσο και κατά ομάδων ανθρώπων. Στις περισσότερες των περιπτώσεων ακόμα και μόνο η απειλή χρήσης βίας προκαλεί καταλυτικά αποτελέσματα. Έτσι στην περίπτωση που ο φόβος για χρήση βίας δεν είναι πιστευτός η δύναμη των τρομοκρατών τίθεται υπό αμφισβήτηση.

ΕΙΚΟΝΑ 3:Οι τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου

Δυναμική

Η βασική επιδίωξη του εξτρεμισμού είναι κυρίως η αντίσταση η αντίδραση σε μία δεδομένη κατάσταση και δευτερευόντως η πολιτική αλλαγή. Αν λοιπόν και η τρομοκρατική δράση είναι κυρίως αντιδραστική από την φύση της, πολλές φορές επιδιώκει να "γυρίσει το ρολόι της ιστορίας πίσω" σε θεσμούς και αξίες που στην εποχή μας δεν υπάρχουν. Χαρακτηριστικό είναι το παράδειγμα της Αλ-Κάιντα η οποία επιθυμεί να επιβάλλει την Σαρία, τον Ιερό Ισλαμικό Νόμο, παράλληλα με την επανίδρυση του Χαλιφάτου στην Μέση Ανατολή διώχνοντας από την περιοχή τους "άπιστους Δυτικούς" και τα καθεστώτα που τους ανέχονται π.χ. τη βασιλική οικογένεια της Σαουδικής Αραβίας.

Καλά προετοιμασμένη

Η τρομοκρατία είναι μία πράξη πολύ καλά σχεδιασμένη η οποία έχει συγκεκριμένους στόχους. Η τακτική σχεδίαση στηρίζεται στη "μαθηματική" λογική, απαιτεί ποικίλο οπλισμό και εξοπλισμό και σίγουρα δεν πρόκειται για τυχαία δράση. *(22)* Εκτός των περιπτώσεων που τα θύματα είναι προσεκτικά επιλεγμένα συνήθως από την "εχθρική ελίτ" οι τρομοκράτες δεν ενδιαφέρονται για την αξία των θυμάτων αλλά την ποσότητα τους. Όσο πιο μαζικό είναι ένα χτύπημα τόσο περισσότερο θόρυβο θα προκαλέσει. Χαρακτηριστικό είναι το παράδειγμα των Δίδυμων Πύργων της 11^{ης} Σεπτεμβρίου και των συνεπειών που προκάλεσε. Παράλληλα η σωστή προετοιμασία συμβαδίζει με την συμβολική αξία του ενδεχόμενου στόχου. Στις περιπτώσεις χτυπημάτων μεγάλης "ειδικής αξίας" ο χρόνος προετοιμασίας μπορεί να υπερβαίνει τους 12 μήνες.

Στις 18 Απριλίου του 1983 χτυπήθηκε η Αμερικανική Πρεσβεία στην Βηρυτό, ο συνολικός αριθμός θυμάτων ήταν 63. Η CIA ανακάλυψε 15 χρόνια περίπου μετά ότι η συγκεκριμένη επίθεση προετοιμάζονταν από Ιρανούς πράκτορες για 14 μήνες υπό πλήρη μυστικότητα. *(23)* Το αποτέλεσμα της επίθεσης αυτής ήταν οι Αμερικανικές Δυνάμεις να κλειστούν στους στρατώνες τους και 8 μήνες αργότερα να αποχωρήσουν οριστικά από το Λίβανο. Επιπλέον το ψυχολογικό αποτέλεσμα της συγκεκριμένης επιθέσεως αλλά και όλων των υπολοίπων ήταν τεράστιο. Αυτό έχει σκοπό να δημιουργήσει μία περιραίουσα ατμόσφαιρα φόβου και ψυχικού καταναγκασμού με στόχο να υποκύψει το κοινωνικό σύνολο στις απαιτήσεις των τρομοκρατών.

1.3 Τα κίνητρα της τρομοκρατίας

Τα κίνητρα της τρομοκρατίας είναι τόσα πολλά όσοι πιθανόν είναι και οι ορισμοί της. Όμως τα τρία βασικότερα θεωρούνται τα πολιτικά, θρησκευτικά και ιδεολογικά. Από τα παραπάνω τα πολιτικά κίνητρα είναι αυτά που συναντώνται στους περισσότερους ορισμούς της τρομοκρατίας μια και γεγονότα όπως η μεροληψία, η κατάφωρη κοινωνική αδικία, η έλλειψη δυνατότητας πολιτικής εκπροσώπησης και δράσης και ο κοινωνικός αποκλεισμός μπορεί να οδηγήσουν σε εξτρεμιστικού χαρακτήρα αντιδράσεις. *(24)*

Η έντονη δυσφορία εθνικών και πολιτικών ομάδων του πληθυσμού όπως για παράδειγμα μία εθνική μειονότητα, οι διακρίσεις εις βάρος της ή η επιθυμία της για ξεχωριστή εθνική-πολιτική εκπροσώπηση πιθανόν να καταλήξουν σε ακραίες αντιδράσεις. Φυσικά αυτό δεν σημαίνει ότι κάθε φορά που υπάρχει ένα παράπονο απέναντι στην πολιτεία θα πρέπει να καταλήγει σε τρομοκρατικές πράξεις. Όμως σε καθεστώτα που η καταπίεση εθνικών και πολιτικών ομάδων είναι συνηθισμένη πρακτική και η χρήση κατασταλτικής βίας εκτεταμένη μόνη διέξοδος φαντάζει η επαναστατική τρομοκρατία.

Παράλληλα τρομοκρατικά φαινόμενα μπορούν να εμφανιστούν στην περίπτωση της νεολαίας που θεωρεί τον εαυτό της περιττό και παραγκωνισμένο, σε μια κοινωνία η οποία αντιμετωπίζει τα σύγχρονα προβλήματα με απάθεια. Αν στα παραπάνω προστεθεί και η βίαιη καταστολή των διαμαρτυριών από την πλευρά του κράτους δημιουργείτε ένα εκρηκτικό μείγμα. Χαρακτηριστικό παράδειγμα αστικής τρομοκρατίας είναι οργανώσεις, όπως ο IRA (Irish Republican Army) και η οργάνωση RAF (Red Army Faction) στην Δυτική Γερμανία.

Οι επιθέσεις της 11^{ης} Σεπτεμβρίου αν και περιορίστηκαν στην Νέα Υόρκη και την Ουάσιγκτον προκάλεσαν άμεσα αύξηση των μέτρων ασφαλείας στα Αμερικάνικά –και όχι μόνο –αεροδρόμια και δημόσιους χώρους. Η συγκεκριμένη πράξη ως μία καθαρόαιμη πράξη πολιτικής βίας, δημιουργεί παρακλάδια και σε χώρους πέρα από τον άμεσο στόχο της επηρεάζοντας μεγαλύτερη μερίδα του πληθυσμού, πέρα από την τοπική κοινωνία. Στις περισσότερες περιπτώσεις και με την βοήθεια των ΜΜΕ ξεπερνάει τα εθνικά σύνορα προκαλώντας αντιδράσεις σε παγκόσμιο επίπεδο.

Το γεγονός αυτό καθαυτό-της παγκόσμιας προσοχής που τυγχάνει ένα τρομοκρατικό χτύπημα σε μία "ξεχασμένη" γωνιά του πλανήτη, αποτελεί ένα πολύ ισχυρό κίνητρο για όλες

τις τρομοκρατικές ομάδες. *(25)* Παράλληλα κίνητρο της τρομοκρατίας μπορεί να θεωρηθεί η ίδια η βίαιη πράξη αφού μόνο μέσω αυτής επιβεβαιώνουν το ρόλο τους.

Επιπλέον σύμφωνα με τον Whittaker *(26)*: τρεις ακόμα παράγοντες μπορούν να θεωρηθούν ως κίνητρα του φαινομένου της τρομοκρατίας ορθολογικοί, ψυχολογικοί και πολιτισμικοί. Με την έννοια ορθολογικοί περιγράφουμε μία αντίληψη καθαρά τεχνοκρατική, αυτή συνίσταται στη μελέτη της σχέσης κέρδους –κόστους, της ανάλυσης ρίσκου όπως ακριβώς στην περίπτωση μίας εταιρίας από την εξτρεμιστική ομάδα.

Φυσικά εμπεριέχεται ο κίνδυνος ο υπολογισμός αυτός να είναι λανθασμένος οδηγώντας στον αφανισμό ή τη σύλληψη των μελών της οργάνωσης. Τα ψυχολογικά κίνητρα αφορούν άτομα ή ομάδες ατόμων που έχουν ανάγκη να ανήκουν σε μία ομάδα-οργάνωση και να πιστεύουν σε μία αλήθεια – ιδεολογία ανεξάρτητα από το πόσο ακραία μπορεί να είναι αυτή. Τόσο η οργάνωση αυτή όσο και η ιδεολογία δίνουν έμφαση στην θεωρία "εμείς (οι καλοί) ενάντια στους κακούς". Κακοί θεωρούνται όσοι δεν ενστερνίζονται τις ίδιες αντιλήψεις και αρχές, έτσι δικαιολογείται η βίαιη δράση της οργάνωσης.

Με την έννοια των πολιτισμικών κινήτρων περιλαμβάνουμε το σύνολο των δομών που συνιστούν απειλή ενάντια στην ύπαρξη μας. Αν ένα ανθρώπινο σύνολο θεωρεί ότι ο εθνικός του χαρακτήρας, η θρησκεία του, ο πολιτισμός του, η γλώσσα και ο τρόπος ζωής του απειλείται από εξωτερικές επιρροές πολύ πιθανόν να οδηγηθεί σε πράξεις βίας και τρομοκρατίας με στόχο την επιβίωση του. Αυτό είναι πιθανότερο αν διαπιστωθεί ότι η ένοπλη δράση θα αναγκάσει σε συνθηκολόγηση τις ομάδες που το πιέζουν. Έτσι μέσω της ένοπλης δράσης θα προσπαθήσει να επιτύχει την ανάσχεση όλων των δυνητικών κινδύνων και απειλών.

1.4 Τρομοκρατία και Κυβερνοχώρος (cyberspace)

Οι τρομοκρατικές οργανώσεις πάντα προσπαθούν να εντοπίσουν τα αδύνατα σημεία και τους τρόπους πρόσβασης προς το στόχου που έχουν επιλέξει. Όμως μετά τις επιθέσεις της 11Σεπτεμβρίου και τον πόλεμο εναντίον των Ταλιμπάν στο Αφγανιστάν, τα αυστηρότερα μέτρα ασφαλείας παγκοσμίως, έχουν μειώσει τις "ευκαιρίες" για επιθέσεις στο φυσικό πεδίο. Υπάρχουν σοβαρές ενδείξεις ότι πιθανόν δίαφορες εξτρεμιστικές ομάδες προσπαθούν να αυξήσουν τις δυνατότητες τους στην πληροφορική παράλληλα με τον προσηλυτισμό ατόμων του ηλεκτρονικού εγκλήματος με σκοπό να αποκτήσουν πρόσβαση σε υψηλού επιπέδου

τεχνικές στον τομέα των Η/Υ. Παράλληλα στην σημερινή ανοιχτή κοινωνία της γνώσης και επικοινωνίας οι τρωτότητες των υπολογιστικών συστημάτων και δικτύων εύκολα ανακαλύπτονται. Το γεγονός αυτό ενδεχομένως να προσελκύσει τις διάφορες εξτρεμιστικές ομάδες προκειμένου να εκτελέσουν επιθέσεις σε κρίσιμες κρατικές δομές. Ο Gabriel Weiman, καθηγητής στο Πανεπιστήμιο της Χάιφα του Ισραήλ, ερευνά συστηματικά web-site τα οποία σχετίζονται με διάφορες τρομοκρατικές ομάδες ανά τον κόσμο. Το 1998 ο αριθμός αυτών των site ήταν μόλις 8 ενώ σήμερα 4500. Ο μεγαλύτερος αριθμός σχετίζεται με οργανώσεις του ακραίου Ισλάμ και με παρακλάδια της Αλ-Κάιντα. *(27)*

Σύμφωνα με το FBI, σε επίσημη αναφορά που δημοσιεύθηκε το 2004, οι cyber attacks στο Διαδίκτυο έχουν περιοριστεί στο e-mail bombing και την καταστροφή ή αμαύρωση ενός site. *(28)* Παράλληλα όμως αναπτύσσουν συνεχώς τις ικανότητες τους σε επιθέσεις εναντίον κρατικών δικτύων Η/Υ συνδυαζόμενες με συμβατικές επιθέσεις. Η εταιρία IBM έχει αναφέρει ότι το πρώτο μισό του 2005, οι cyber attacks έχουν αυξηθεί κατά τουλάχιστον 50% κυρίως εναντίον κυβερνητικών υπηρεσιών και οργανισμών των ΗΠΑ.

Επιπλέον το ηλεκτρονικό έγκλημα στις μέρες μας αναπτύσσεται ραγδαία ως εγκληματική δραστηριότητα. Με την πάροδο των χρόνων –σύμφωνα με εκτιμήσεις του FBI- ο συνδυασμός cyber attacks και ηλεκτρονικού εγκλήματος θα είναι τέτοιος που η διάκριση θα είναι σχεδόν αδύνατη. Παραδείγματος χάρη πρόσφατα σύμφωνα με το House Homeland Security Committee των Η.Π.Α. ομάδες της Αλ-Κάιντα χρησιμοποίησαν κλεμμένες ταυτότητες και πιστωτικές κάρτες για την υποστήριξη των τρομοκρατικών τους δραστηριοτήτων.*(29)* Επιπλέον οι επιθέσεις στο Μπαλί της Ινδονησίας το 2002, χρηματοδοτήθηκαν από ένα δίκτυο πλαστών πιστωτικών καρτών. *(30)*

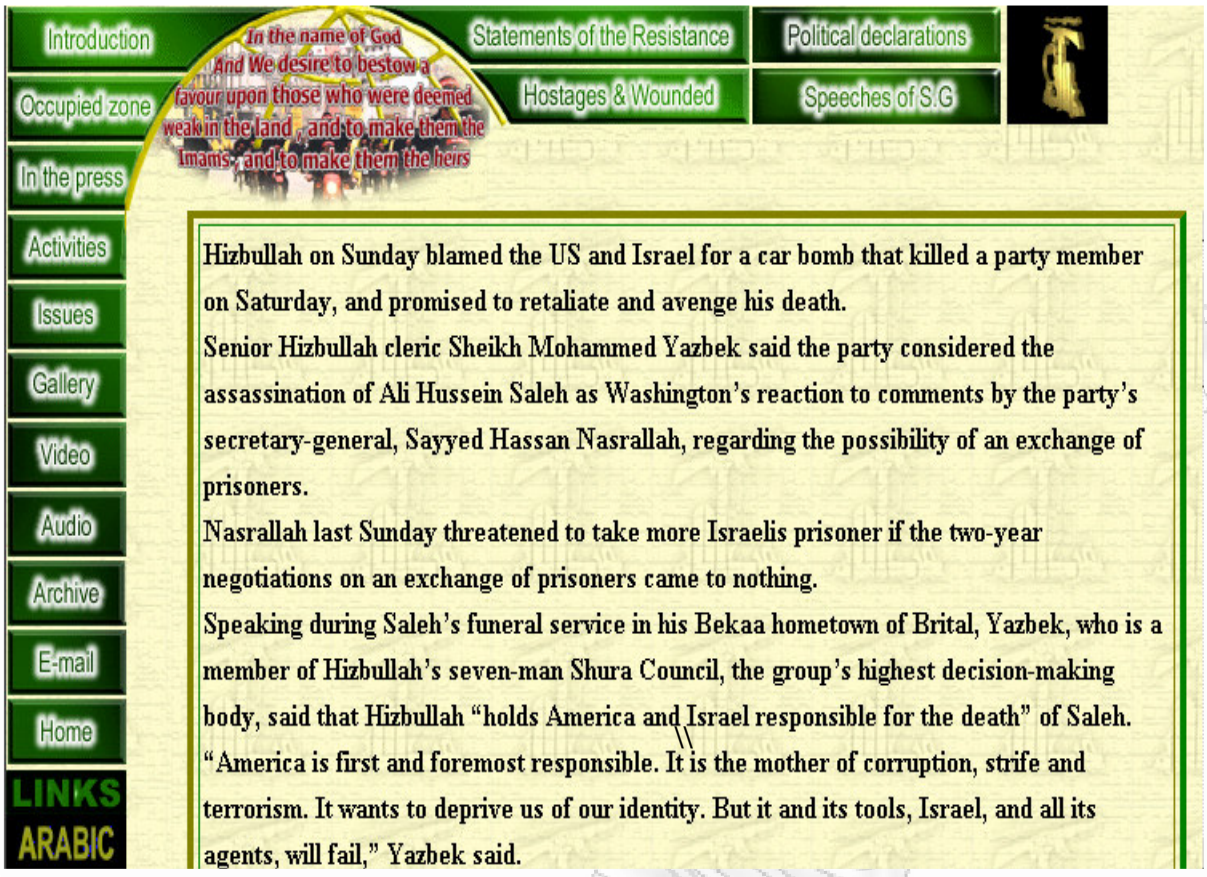
Παράλληλα στον πόλεμο του Ιράκ ο Κυβερνοχώρος αποτελεί έναν "αγαπημένο" τόπο των ανταρτών, οι οποίοι έχουν δημιουργήσει πολλά αραβικά web-site. *(31)* Σε αυτά περιέχονται διάφορες πληροφορίες όπως: πώς να φτιάξει κάποιος μία αυτοσχέδια βόμβα, τακτικές ελεύθερων σκοπευτών, τρόπους να περάσει κάποιος παράνομα υλικά από τα check-points (σημεία ελέγχου) του Αμερικανικού Στρατού, αποσπάσματα από το Κοράνι κ.α. *(32)*

1.5 Ο κυβερνοχώρος στην υπηρεσία της τρομοκρατίας

Παρακάτω αναλύονται ορισμένοι τρόποι χρήσης του Διαδικτύου (Internet) από τις εξτρεμιστικές ομάδες.

(1) **Σχεδιασμός χτυπημάτων**: η επικοινωνία μεταξύ των μελών μιας οργάνωσης, η οργάνωση σχεδίων δράσεως, οι επόμενοι στόχοι είναι αντικείμενα που διεκπεραιώνονται μέσω του internet πολύ συχνά. Η ασφάλεια των επικοινωνιών εξασφαλίζεται με τη χρήση κωδικών και μεθόδων κωδικοποίησης που υπάρχουν "ελεύθερα" στο διαδίκτυο. Παράλληλα με τη χρήση στενογραφίας αποκρύπτουν μηνύματα, εικόνες, σχέδια και σχόλια που κάνουν στα διάφορα chat rooms. Οι οδηγίες και οι εικόνες μπορούν να αναγνωσθούν μόνο από αυτόν που έχει στην κατοχή του το "ιδιωτικό κλειδί" (private key) ή κώδικα. *(33)*

(2) **Στρατολόγηση νέων μελών**: αποτελεί θεμελιώδη διαδικασία για την επιβίωση κάθε τρομοκρατικής ομάδας. Έτσι παράλληλα με τις κλασικές μεθόδους όπως δημοσιεύσεις, εκδόσεις βιβλίων και CDs, χρησιμοποιούν τα sites τους για να προσελκύσουν νέα μέλη. Σε αυτά προβάλλεται συνήθως η ιστορία της οργάνωσης, οι επιτυχίες της, ο αριθμός των μελών της, η ιδεολογία της, οι στόχοι της ενώ ενθαρρύνονται νέοι κυρίως να γίνουν μέλη της. Χαρακτηριστικά είναι τα παραδείγματα των παρακάτω site: της οργάνωσης Χαμάς, http://www.hamasonline.com, της Hizbullah, http://www.hizbollah.org και του Απελευθερωτικού Στρατού της Κολομβίας Revolutionary Armed Forces of Colombia (F.A.R.C.), http://www.farcep.org/pagina_ingles .



ΕΙΚΟΝΑ 4:Web-site της οργάνωσης Hizbullah

(3)**Έρευνα – αναζήτηση πληροφοριών**: με τη χρήση του Internet οι τρομοκράτες έχουν την δυνατότητα να χρησιμοποιήσουν μία τεράστια γκάμα από database, ηλεκτρονικές βιβλιοθήκες, δημοσιεύματα για να αντλήσουν πληροφορίες για το θέμα που επιθυμούν. Αυτές μπορεί να είναι κείμενα, φωτογραφίες, χάρτες, δορυφορικές εικόνες ακόμα και αρχεία video. Δεν απαιτούνται ιδιαίτερες γνώσεις Η/Υ αλλά μόνο η χρήση της μηχανής αναζήτησης του Google. Για παράδειγμα πληκτρολογώντας τη λέξη "βόμβα" στο Google σε 0,17 sec εμφανίζονται 2.870.000 σχετικά αρχεία. Για να μειώσουμε την παραπάνω λίστα πληκτρολογούμε το "αυτοσχέδια βόμβα" και εμφανίζονται 47200 σχετικά σε 0,08 sec. Παρά το γεγονός ότι τα περισσότερα από τα αρχεία στα προηγούμενα παραδείγματα είναι απλές αναφορές στη συγκεκριμένη λέξη υπάρχουν και ακριβείς πληροφορίες για το πώς να κατασκευάσει κάποιος μια βόμβα. Παράλληλα οι τρομοκράτες μπορούν να χρησιμοποιήσουν το διαδίκτυο για να αποκτήσουν πληροφορίες κρίσιμων κρατικών φορέων. Μάλιστα το 2001 το FBI ανακάλυψε ένα εκτεταμένο δίκτυο ηλεκτρονικής παρακολούθησης μίας σειράς κρατικών υπηρεσιών των ΗΠΑ. Η παρακολούθηση γίνονταν μέσω τηλεφωνικών συνδέσεων και με χρήση άγνωστων browsers στη Μέση Ανατολή και Ανατολική Ασία και κυρίως από χώρες όπως το Πακιστάν, τη Σαουδική Αραβία και την Ινδονησία. Η παρακολούθηση αυτή

είχε εστιασθεί σε κρίσιμους τομείς όπως: τηλεφωνικά συστήματα ανάγκης, εργοστάσια παραγωγής ηλεκτρικής ενέργειας, μεταφορικές και αεροπορικές εταιρείες, νοσοκομεία, συστήματα κατανομής ηλεκτρικής ενέργειας, νερού και φυσικού αερίου, διυλιστήρια, αεροδρόμια, λιμάνια και λιμενικές εγκαταστάσεις και πυρηνικά εργοστάσια. *(34)*

(4)**Προπαγάνδα**: σύμφωνα με τον Christopher Harmon και το βιβλίο του, *Terrorism Today*, η προπαγάνδα αποτελεί κορυφαία προτεραιότητα όλων των εξτρεμιστικών ομάδων. Η χρήση της έχει διπλό ρόλο. Από την μία πλευρά να κάνει γνωστή την δική της θεώρηση των πραγμάτων, να προβάλει τα χτυπήματα και την ιδεολογία της και από την άλλη να δυσφημίσει τους εχθρούς της. Παλαιότερα, αλλά και στις μέρες μας αυτό γίνονταν με προκηρύξεις και δημοσιεύσεις στις εφημερίδες. Σήμερα η χρήση των sites είναι πολύ διαδεδομένη, ιδιαίτερα από το εξτρεμιστικό ισλάμ όπως είδαμε και στην παραπάνω φωτογραφία από το site της οργάνωσης Hezbollah.

1.6 Το παράδειγμα της τρομοκρατικής οργάνωσης Αλ-Κάιντα

Το Νοέμβριο του 2001 ξεκίνησε η επίθεση των ΗΠΑ εναντίον του καθεστώτος των Ταλιμπάν στο Αφγανιστάν. Αυτό στέρησε από τον Osama Bin Laden το βασικότερο του καταφύγιο στην περιοχή της Κεντρικής Ασίας. Σύμφωνα με τον Hamid Mir, βιογράφο του ηγέτη της οργάνωσης "κάθε μέλος της οργάνωσης έφερε πλέον μαζί με το Καλάσνικοφ και από ένα laptop". Με τη χρήση αυτών διασώθηκαν οι επικοινωνίες, η εκπαίδευση και ο σχεδιασμός της, ενώ οι εγκαταστάσεις που καταστράφηκαν από τους μαζικούς βομβαρδισμούς αντικαταστάθηκαν από διαδικτυακούς τόπους. Οι μαχητές της Αλ-Κάιντα στο Ιράκ καθώς και οι βομβιστές αυτοκτονίας χρησιμοποιούν ευρέως το internet ως μέσο εκπαίδευσης και τεχνικής υποστήριξης βασιζόμενοι στην ανωνυμία, την ευελιξία και την ασυλία που τους δίνει η σύγχρονη τεχνολογία. Στην Αίγυπτο, το Κατάρ και την Ευρώπη ομάδες σχετιζόμενες με την Αλ-Καίντα σχεδίαζαν βομβιστικές επιθέσεις με κύριο μέσω επικοινωνίας το internet. Παράλληλα τα τελευταία χρόνια στη γενέτειρα του Οσάμα Μπιν Λάντεν τη Σαουδική Αραβία αλλά και σε χώρες όπως το Πακιστάν, οι διωκτικές αρχές έχουν σημειώσει επιτυχία στη σύλληψη μελών της οργάνωσης. Αυτό ανάγκασε την τελευταία να καταφύγει στο διαδίκτυο για τη στρατολόγηση νέων μελών. Εξάλλου τα ιδεολογικά χαρακτηριστικά της κινούνται περισσότερο προς μία παγκόσμια θρησκευτική θεώρηση των πραγμάτων παρά προς μία στενά εθνική σκοπιά. Στις τάξεις υπηρετούν μέλη από όλο τον

μουσουλμανικό κόσμο, οι οποίοι πιστεύουν στην ίδια ερμηνεία του Κορανίου. Το γεγονός αυτό την κάνει αρχικά θετικά διακείμενη προς αυτής της μορφής παγκοσμιοποίηση και των εργαλείων που αυτή προσφέρει ένα από τα οποία είναι και το internet. Με τη χρήση του η Αλ-Καίντα αντικαθιστά τα στρατόπεδα εκπαίδευσης με την εικονική πραγματικότητα του Η/Υ, η οποία εντοπίζεται και καταστρέφεται δυσκολότερα. Επιπλέον χρησιμοποιείται κατά κόρον ως εργαλείο προπαγάνδας, προσηλυτισμού νέων μελών, διασποράς απειλών, οικονομικής ενίσχυσης και εξαπάτησης χρηστών του διαδικτύου με την κλοπή δεδομένων και ψηφιακών αρχείων. *(34)*

1.7 Τι είναι η Κυβερνοτρομοκρατία (cyber terrorism)

Cyber terrorism is the convergence of cyberspace and terrorism. (Κυβερνοτρομοκρατία είναι η σύγκλιση κυβερνοχώρου και τρομοκρατίας). *Dorothy E. Denning (2000)*

Τον Οκτώβριο του 2002 πραγματοποιήθηκε η πιο "εξελιγμένη και εκτεταμένη επίθεση εναντίον κρίσιμων Η/Υ συστημάτων στην ιστορία του internet", εννέα από τους 13 βασικούς κρατικούς servers των ΗΠΑ δέχθηκαν ηλεκτρονική επίθεση για μία ώρα περίπου, με αποτέλεσμα τελικά να καταρρεύσουν. *(35)* Μετά από το γεγονός αυτό, ορισμένοι ειδικοί προειδοποίησαν ότι αναμένονταν μεγαλύτερης έκτασης επιθέσεις και τέθηκε άμεσα το ερώτημα αν η δομή του διαδικτύου είναι αρκετά "δεμένη" για να αντέξει παρόμοιες ή ακόμα χειρότερες επιθέσεις.

Παράλληλα τον Απρίλιο του 2002 η Κεντρική Υπηρεσία Πληροφοριών (CIA) σε αναφορά προς την αρμόδια επιτροπή του Αμερικανικού Κογκρέσου είχε αναφέρει ότι ηλεκτρονικές επιθέσεις εναντίον κρίσιμων κρατικών υποδομών αποτελεί ευχέρεια των τρομοκρατικών οργανώσεων μιας και τα μέλη τους εξοικειώνονται όλο και περισσότερο με την υψηλή τεχνολογία των δικτύων Η/Υ. *(36)*

Επιβεβαίωση της παραπάνω αναφοράς αποτέλεσαν και διάφορα έγγραφα, αρχεία, laptop και λοιπός εξοπλισμός που οι μαχητές της Αλ-Κάιντα άφησαν πίσω τους στο Αφγανιστάν κατά τη διάρκεια των Αμερικανικών επιθέσεων μετά το Νοέμβριο του 2001. Από την ανάλυση αυτών των ευρημάτων διαπιστώνεται η ύπαρξη στελεχών στις τάξεις της οργάνωσης με ιδιαίτερα υψηλού επιπέδου γνώσεις στον τομέα των Η/Υ και τεχνικά εγχειρίδια στα Αραβικά, Αγγλικά, Τουρκικά, Κουρδικά και Ρωσικά. *(37)*

Το Σεπτέμβριο του 2003 στο web-site Αλ-Φαρούκ (το οποίο θεωρείτε άμεσα συνδεδεμένο στο δίκτυο της Αλ-Κάιντα) δημοσιεύθηκε ένα βιβλίο με τον τίτλο *"Οι 39 αρχές του Jihad"*ή για την ακρίβεια οι 39 αρχές του Jihad με βάση την θεωρία της Αλ-Κάιντα. Η έννοια του Jihad κατά λέξη σημαίνει τον αγώνα στο όνομα του Θεού και είναι άμεσα συνδεδεμένο με την έννοια του Ιερού Πολέμου. Στο κείμενο αυτό τα μέλη της οργάνωσης καλούνται να κάνουν χρήση των δυνατοτήτων που τους παρέχει η σύγχρονη τεχνολογία για την διάδοση του κηρύγματος της με τη δημιουργία forums, web sites και χρήση ως εργαλείου επικοινωνιών των sms. Επίσης οι οπαδοί της οργάνωσης καλούνται να "εφαρμόσουν το ηλεκτρονικό Jihad" και με τις ικανότητες τους να "καταστρέψουν Αμερικανικά, Ισραηλινά και κοσμικά web site". *(38)*

Τα παραπάνω παραδείγματα δίνουν μια γεύση των προβλημάτων που σχετίζονται με την Κυβερνοτρομοκρατία. Στο πρώτο παράδειγμα οι στόχοι και τα κίνητρα αυτών που εκτέλεσαν την επίθεση παραμένουν άγνωστα. Μπορεί να ήταν έργο ενός αριθμού "παιδιών – θαύμα" που προσπαθούσαν να διερευνήσουν τις ικανότητες τους στο hacking ή έργο μιας ομάδας τρομοκρατών οι οποίοι προσπαθούσαν να βρουν "ανοιχτές πόρτες" στους κρατικούς servers.

Επίσης δεν έχει ξεκαθαριστεί γιατί ξαφνικά μέσα στη μισή ώρα οι επιθέσεις διακόπηκαν για λίγο, για να συνεχιστούν αργότερα καλύπτοντας το διάστημα των 60 min. Ορισμένοι θεώρησαν το γεγονός ως προμήνυμα μίας μεγαλύτερης κλίμακας επίθεσης, ενώ άλλοι ότι οι δράστες σταμάτησαν όταν διαπίστωσαν ότι οι προσπάθειες τους δεν έφεραν το επιθυμητό αποτέλεσμα.

Στο δεύτερο παράδειγμα μία από τις διαβόητες τρομοκρατικές ομάδες των ημερών μας, είναι θιασώτης της χρήσης του διαδικτύου όπως αναφέραμε και σε προηγούμενη παράγραφο αλλά και των web-site προς το χειρότερο. Ουσιαστικά περνάει τα μηνύματα καταστροφής, βίας και το σχεδιασμό αυτών μέσω του διαδικτύου.

1.7.1 Ορισμός της Κυβερνοτρομοκρατίας (cyber terrorism)

Όπως ο ορισμός της τρομοκρατίας έχει πολλές και διαφορετικές διατυπώσεις έτσι και ο ορισμός της Κυβερνοτρομοκρατίας παρουσιάζει διάφορες παραλλαγές. Παρακάτω θα αναφέρουμε τους σημαντικότερους και τους – κατά το δυνατόν – πληρέστερους. Σύμφωνα με την Dorothy E.Denning και κατά την διάρκεια του Special Oversight Panel on Terrorism *(39)*:

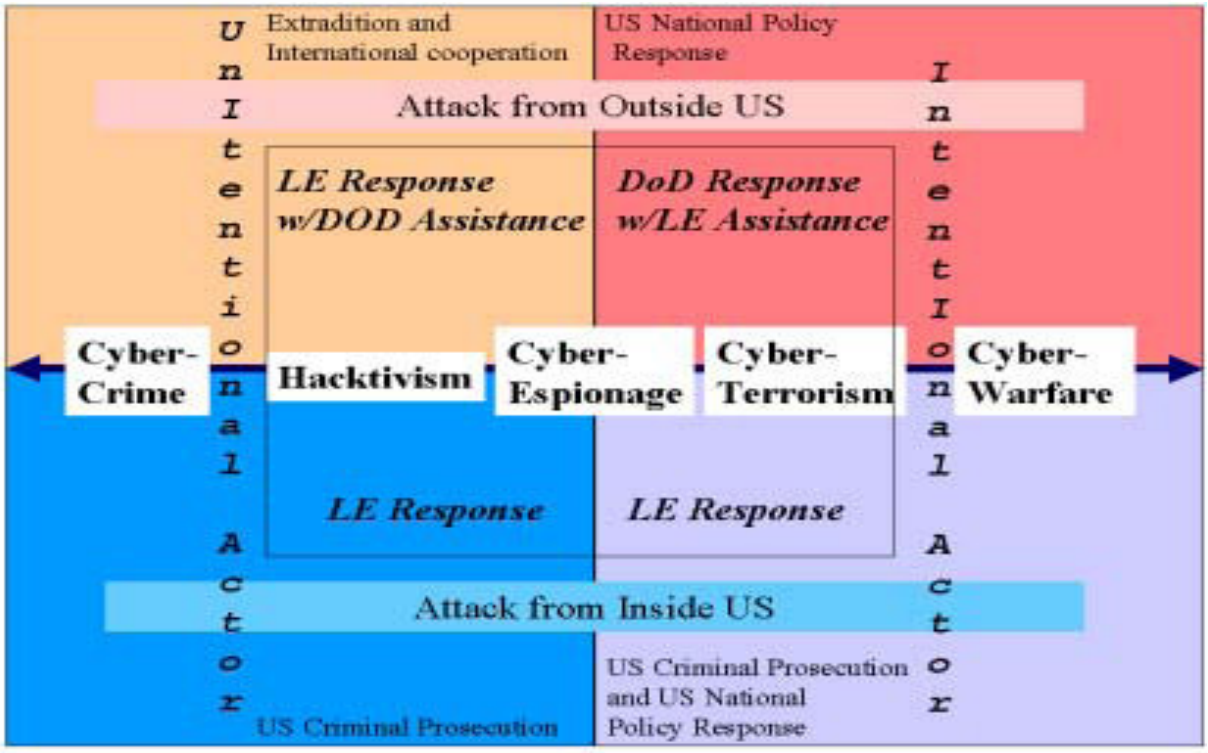
"Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives".

«Κυβερνοτρομοκρατία είναι η σύγκλιση τρομοκρατίας και κυβερνοχώρου. Γενικά γίνεται κατανοητή ως οι παράνομες επιθέσεις και απειλές επιθέσεων εναντίον Η/Υ, δικτύων και των αποθηκευμένων πληροφοριών και όταν πραγματοποιείται έχει σκοπό να πανικοβάλλει ή να πειθαναγκάσει μία κυβέρνηση ή τους ανθρώπους της στην ενίσχυση ενός πολιτικού ή κοινωνικού σκοπού».

Ένας άλλος ορισμός είναι από τον J.T. Caruso του U.S. FBI, ο οποίος δόθηκε κατά την κατάθεση του στην επιτροπή House Subcommittee on National Security, Veterans Affairs and International Relations τον Μάρτιο του 2002:

"Cyber terrorism – meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population".

«Κυβερνοτρομοκρατία – σημαίνει την χρήση ηλεκτρονικών εργαλείων για να κλείσουν κρίσιμες εθνικές υποδομές (όπως ενέργεια , μεταφορές ή κυβερνητικές υπηρεσίες) με σκοπό τον εξαναγκασμό ή την πρόκληση πανικού στην κυβέρνηση ή τον άμαχο πληθυσμό».



ΕΙΚΟΝΑ 5: Το φάσμα του Cyber Conflict στο οποίο εντάσσεται και η Κυβερνοτρομοκρατία

Με βάση τους παραπάνω ορισμούς, μπορούμε από μία σύντομη ιστορική ανασκόπηση να εντοπίσουμε παραδείγματα κυβερνοτρομοκρατίας τα οποία έγιναν ευρύτερα γνωστά μέσω των ΜΜΕ. Έτσι έχουμε *(40)*:

- Τον Απρίλιο του 2001 ένα Κινεζικό μαχητικό αεροσκάφος και ένα Αμερικανικό αναγνωριστικό συγκρούσθηκαν στον αέρα. Μετά από το συμβάν αυτό παρατηρήθηκε παραμόρφωση σε διάφορα Αμερικανικά web-sites.
- Κατά την διάρκεια του πολέμου στον Κόλπο (1990-1991) Γερμανοί hackers έκλεψαν πληροφορίες για την κίνηση των Αμερικανικών στρατευμάτων από τους Η/Υ του Υπουργείου Αμύνης. Μάλιστα προσπάθησαν να τις πουλήσουν στους Ιρακινούς, αλλά οι τελευταίοι θεώρησαν ότι πρόκειται για μπλόφα.
- Διείσδυση από ένα έφηβο Κροάτη στο δίκτυο Η/Υ της Αμερικανικής Αεροπορικής Βάσης Guam.

Ένας άλλος πιο πρακτικός ίσος ορισμός της έννοιας που εξετάζουμε είναι αυτός που δίδεται από τον Αμερικανικό Στρατό στο DCSINT Handbook .1.02 ως εξής :

"Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves".

«Κυβερνοτρομοκρατία είναι η ανάπτυξη ικανοτήτων τρομοκρατίας στηριζόμενη στις νέες τεχνολογίες και διαδικτυακούς οργανισμούς, τα οποία επιτρέπουν στους τρομοκράτες να πραγματοποιούν τις επιχειρήσεις τους με μικρό ή καθόλου φυσικό ρίσκο για τον εαυτό τους».

Από την ανάλυση των διαφόρων ορισμών της κυβερνοτρομοκρατίας διαπιστώνουμε ότι υπάρχουν θεμελιώδεις διαφορές όσον αφορά την απειλή που αυτή συνιστά τη χρησιμότητα που προσφέρει στους εξτρεμιστές, τους αντικειμενικούς σκοπούς της, τους στόχους της και τα αποτελέσματα της εν τέλει. Κάθε ένας από τους παραπάνω δίνει και διαφορετική όψη στην έννοια της για αυτό και θα αναλύσουμε παρακάτω ορισμένες βασικές κατηγορίες εκτιμήσεων, οι οποίες αποτελούν τα λεγόμενα cyber terrorist "camps".

1.7.2 Cyber terrorist "Camps"

Στη πρώτη κατηγορία ανήκουν οι περισσότερο απαισιόδοξοι, όσοι δηλαδή πιστεύουν ότι απλά είναι θέμα χρόνου να πραγματοποιηθεί μία μεγάλης κλίμακας επίθεση στα υπολογιστικά συστήματα και δίκτυα των Δυτικών κρατών και κυρίως των ΗΠΑ.

Τα τελευταία χρόνια και κυρίως μετά την λήξη του Ψυχρού Πολέμου η κυριαρχία των ΗΠΑ στον στρατιωτικό και τεχνολογικό τομέα είναι δεδομένη. Τόσο τα υπόλοιπα κράτη της Δύσης (π.χ. Γαλλία, Γερμανία κ.α.) όσο και της Ανατολής (Ιαπωνία, Κίνα ,Ινδία) δε μπορούν να τις συναγωνιστούν σε ισχύ πυρός ιδιαίτερα στο συμβατικό τομέα. Έτσι ο τομέας του cyber warfare αποτελεί μία εναλλακτική μορφή πολέμου με πιθανότητες επιτυχίας απέναντι στη μονοκρατορία των ΗΠΑ.

Αυτό ενισχύεται και από το γεγονός ότι με την πάροδο του χρόνου όλο και μεγαλύτερος αριθμός από τα πιο κρίσιμα και πολύτιμα "περιουσιακά στοιχεία" των κρατών δε βρίσκονται πια σε θησαυροφυλάκια αλλά σε ψηφιακές βάσεις δεδομένων, με αποτέλεσμα να αποτελούν στόχο. Με την επανάσταση τα τελευταία χρόνια στον τομέα των Η/Υ είναι ευκολότερο "φτωχά" κράτη και διάφορες ομάδες να αποκτήσουν ικανότητες για την

διεξαγωγή επιχειρήσεων I.W. (Information Warfare) χρησιμοποιώντας ευρύτερα διαδεδομένο software και hardware από τον εμπορικό τομέα.

Παράλληλα η διάδοση της χρήσης του διαδικτύου σε όλο σχεδόν τον πλανήτη, ανεξαρτήτως εθνικών, γεωγραφικών, πολιτικών και κοινωνικών περιορισμών το έχει μετατρέψει σε ένα εύκολο στη χρήση και διαδεδομένο εργαλείο hactivismv(ο όρος προέρχεται από την συνένωση της λέξης hacking και activism =ακτιβιστής) καθώς και για άλλες δραστηριότητες σχετικές με το hacking.

Επιπλέον οι ειδικοί του I.W. πιστεύουν ότι δεν απαιτείται ένα ποσό πάνω από 10 εκατομμύρια δολάρια για εξοπλισμό και μέσα, από μία καλά προετοιμασμένη και συντονισμένη επίθεση από λιγότερο από 30 computer hackers οι οποίοι θα βρίσκονται τοποθετημένοι σε στρατηγικά σημεία ανά την υφήλιο για να "γονατίσουν" κρίσιμες υπηρεσίες όπως η παραγωγή ενέργειας, ο έλεγχος της εναέριας κυκλοφορίας, η λειτουργία των μέσων μαζικής μεταφοράς κ.ά. .

Το συμπέρασμα αυτό στηρίζεται κυρίως στα αποτελέσματα των ασκήσεων με την επωνυμία ELIGIBLE RECEIVER που ξεκίνησαν το 1997 και επαναλαμβάνονται ανά δύο χρόνια. Στην πρώτη από αυτές, μία Red Team αναπαριστούσε την Βόρεια Κορέα η οποία εκτελούσε ηλεκτρονικές επιθέσεις σε μία μεγάλη γκάμα από κυβερνητικά site χρησιμοποιώντας όμως εργαλεία hacking τα οποία κυκλοφορούν ελεύθερα στο internet. Τα αποτελέσματα της ασκήσεως είναι άξια προσοχής: ένας μεγάλος αριθμός στρατηγικών συστημάτων command and control κατέρρευσε, μόλις το 4% των "στόχων" βρισκόταν σε εγρήγορση για την αντιμετώπιση απροειδοποίητης επιθέσεως και από αυτά μόνο 1 στα 150 ανέφερε την διείσδυση στους ανωτέρους του. *(41)*

Επίσης το 2003 ο ηλεκτρονικός slammer worm κατάφερε να σταματήσει τις δραστηριότητες του Χρηματιστηρίου της Νότιας Κορέας για αρκετές ώρες. *(42)* Η αποστολή ενός τέτοιου ιού προς άλλες σημαντικές κρατικές υποδομές από τη Βόρεια Κορέα, πριν από μια στρατιωτική εισβολή ίσως να είναι μοιραία για το Νότιο κομμάτι της Κορεατικής χερσονήσου.

Η δεύτερη κατηγορία περιλαμβάνει αυτούς που θεωρούν απίθανη μια ηλεκτρονική επίθεση και πιστεύουν ότι οι εξτρεμιστικές οργανώσεις ενδιαφέρονται περισσότερο για την φυσική βία και καταστροφή, ενώ δεν έχουν τις τεχνικές γνώσεις και ικανότητες για να

πραγματοποιήσουν σύγχρονες cyber επιθέσεις. Οι βομβιστικές επιθέσεις, οι δολοφονίες και οι υπόλοιπες πράξεις βίας εξακολουθούν να προσελκύουν τα φώτα της δημοσιότητας, να προκαλούν φόβο και ανησυχία όπως άλλωστε είναι ο στόχος τους. Επομένως δεν υπάρχει λόγος για αλλαγή "πολιτικής" από την πλευρά των τρομοκρατών. Οι προσδοκίες από τη χρήση του cyber terror εξαρτώνται από την επιθυμία της οργάνωσης και από τη διαθεσιμότητα ή όχι των μέσων να το πραγματοποιήσει.

Από την ιστορική διαδρομή της παγκόσμιας τρομοκρατίας διαπιστώνουμε την επιμονή των περισσότερων οργανώσεων στην "παραδοσιακή εξτρεμιστική βία". Άλλωστε απαιτείται ουσιαστικά μία απότομη στροφή προς την τεχνολογία για τις ομάδες αυτές, η οποία μπορεί να διαρκέσει και χρόνια ολόκληρα για να αναπτύξουν ικανοποιητικές δυνατότητες αποτελεσματικής δράσης στο διαδίκτυο. Ο συνδυασμός των δύο αυτών στοιχείων που προαναφέραμε, μειώνει δραματικά σύμφωνα με τους υποστηρικτές αυτού του "camp" τις πιθανότητες cyber επιθέσεων από ελάχιστες τρομοκρατικές οργανώσεις. Παράλληλα θεωρούν το internet ως μέσο σχεδιασμού και εκπαίδευσης, παρά ως "όπλο" επιθέσεως.*(43)*

Στην τρίτη κατηγορία ανήκουν όσοι ισχυρίζονται ότι η κυβερνοτρομοκρατία δεν είναι τίποτα διαφορετικό από την εφαρμογή της "παραδοσιακής τρομοκρατίας" σε άλλο όμως τομέα. Δεν υπάρχει αμφιβολία ότι μία τεχνολογικά ανεπτυγμένη τρομοκρατία αποτελεί κίνδυνο για ολόκληρο το κοινωνικό σύνολο αυτό όμως δεν σημαίνει, σύμφωνα με τους υποστηριχτές αυτής της θεωρίας ότι η διαφορά από την "κλασική" της μορφή είναι αξιοπρόσεκτη. Φυσικά τα μέτρα προστασίας που εφαρμόζονται πρέπει να είναι ισοδύναμα και αντίστοιχα με τη φύση και τη μορφή της απειλής. Έτσι πρέπει να γίνεται χρήση συστημάτων ασφάλειας δικτύων, εντοπισμού παράνομης διείσδυσης, κρυπτογραφίας και αντιμετώπισης ηλεκτρονικών επιθέσεων.

Παράλληλα θεωρούν ότι με την εξέλιξη της τεχνολογίας αναδύονται κίνδυνοι οι οποίοι αν και έχουν τα συμπτώματα τρομοκρατικής δράσης, στην ουσία πρόκειται για άλλου είδους γεγονότα τα οποία όμως έχουν την ίδια σοβαρότητα. Χαρακτηριστικό είναι το παράδειγμα της Solar Sunrise το Φεβρουάριο του 1998, όπου δύο έφηβοι από την Καλιφόρνια των ΗΠΑ και ένας από το Ισραήλ προκάλεσαν σοβαρά προβλήματα στη μεταφορά και ανάπτυξη στρατευμάτων στον Περσικό Κόλπο, όταν επιτέθηκαν στα υπολογιστικά συστήματα του Αμερικανικού Πενταγώνου.*(44)* Αν και οι τρεις αυτοί νεαροί δεν είχαν ως

στόχο την τρομοκρατική δράση, τα αποτελέσματα της δράσης τους ήταν ισάξια με αυτά μιας τέτοιου είδους δραστηριότητας. Η καθυστέρηση στην ανάπτυξη των στρατευμάτων στη Μέση Ανατολή εξαιτίας του παραπάνω γεγονότος διήρκεσε μία εβδομάδα περίπου.

Η τέταρτη κατηγορία "camp" έχει ως βασική θέση ότι ο κίνδυνος της κυβερνοτρομοκρατίας συνεχώς μεγαλοποιείται, μιας και δεν υπάρχουν γεγονότα αυστηρά καταγεγραμμένα όπως π.χ. μια βομβιστική επίθεση ή μια δολοφονία και σίγουρα όχι στο μέγεθος της 11 Σεπτεμβρίου. Χρησιμοποιείται ως επιχείρημα η αναφορά Symantec Internet Security Threat Report όπου δίνονται λεπτομερείς πληροφορίες για malicious code, win32 ιούς, worms τύπου slammer and blaster, spam activity αλλά δεν γίνεται καμία αναφορά στην κυβερνοτρομοκρατία.*(45)*

Επιπλέον θεωρούν ως κινητήρια δύναμη για την εμφάνιση του φαινομένου τα οικονομικά κίνητρα. Ουσιαστικά οι έννοιες ηλεκτρονική απάτη και τρομοκρατική δράση είναι άμεσα συνδεδεμένες. Επιπλέον πιστεύουν ότι οι κύριες μορφές επιθέσεων στο διαδίκτυο όπως η παραμόρφωση web-site, οι επιθέσεις τύπου denial-of-service, οι διαδικτυακές απάτες δε σκοτώνουν ανθρώπους ούτε καταστρέφουν περιουσίες, όπως οι πραγματικές τρομοκρατικές επιθέσεις και συνεπώς δεν αποτελούν τόσο μεγάλο κίνδυνο.

Την τελευταία κατηγορία αποτελούν οι λεγόμενοι "ρεαλιστές" οι οποίοι υποστηρίζουν ότι η πραγματική απειλή δεν προέρχεται από τρομοκράτες αλλά από ανθρώπους του υποκόσμου που επιδίδονται στο λεγόμενο cyber crime (ηλεκτρονικό έγκλημα). Ο όρος «Ηλεκτρονικό Έγκλημα» διακρίνεται σε δύο έννοιες: τη στενή και την ευρεία. Η στενή έννοια, αναφέρεται σε εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί το κύριο μέσο για την τέλεση τους, όπως για παράδειγμα οικονομικά εγκλήματα (ηλεκτρονική απάτη, κατασκοπεία, πειρατεία, παραποίηση δεδομένων κ.α.) ενώ η ευρεία έννοια αναφέρεται σε εκείνα τα εγκλήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής αποτελεί βοηθητικό μέσο, όπως για παράδειγμα τα εγκλήματα που έχουν σχέση με το Κυβερνοχώρο, τα λεγόμενα Κυβερνοεγκλήματα, η διάδοση πορνογραφικών εικόνων, ρατσιστικών διακηρύξεων, πληροφοριών που παροτρύνουν σε βία, δεδομένων προσωπικού χαρακτήρα κ.α.

Η θεώρηση των ρεαλιστών για την πραγματική απειλή της τρομοκρατίας στηρίζεται στα στατιστικά στοιχεία των τελευταίων ετών, τα οποία παρουσιάζουν μια αλματώδη ανάπτυξη των παράνομων δραστηριοτήτων που σχετίζονται με το διαδίκτυο και κυρίως τον

οικονομικό τομέα. Ένα γνωστό παράδειγμα είναι αυτό που δημοσιεύθηκε στου Times του Λονδίνου το Νοέμβριο του 2003, σύμφωνα με την οποία hackers εκμεταλλευτήκαν τις αδυναμίες των Η/Υ προκειμένου να εκβιάσουν εταιρίες on line για την απόσπαση χρημάτων. Οι τελευταίοι εφάρμοσαν μία κατηγορία επιθέσεων, τη denial of service, με την οποία "έριχναν" τα sites των εταιρειών του που ήταν εισηγμένες στο Βρετανικό Χρηματιστήριο και απειλούσαν για ακόμα μεγαλύτερες επιθέσεις αν δεν τους καταβάλλονταν τα χρήματα που απαιτούσαν.

Παράλληλα, σήμερα ο ρυθμός κατασκευής νέων web-sites –περισσότερα από ένα κάθε 4 δευτερόλεπτα - κάνει την επιβολή του νόμου στο διαδίκτυο μία υπόθεση τόσο δαπανηρή όσο χρονοβόρα. Αυτό επιδεινώνεται από την προτίμηση στελεχών με την κατάλληλη εκπαίδευση να εργασθούν στον ιδιωτικό τομέα, παρά στις αντίστοιχες κρατικές υπηρεσίες (π.χ. Δίωξη Ηλεκτρονικού Εγκλήματος, Ε.Υ.Π. κ.α.) όπου οι οικονομικές απολαβές είναι σαφώς μικρότερες. *(46)*

Από την παραπάνω ανάλυση των διάφορων camps καταλήγουμε ότι όλοι σχεδόν αναγνωρίζουν το φαινόμενο της κυβερνοτρομοκρατίας και ότι υπάρχουν κίνδυνοι υπαρκτοί . Επιπλέον συμφωνούν ότι οι ενδεχόμενοι "στόχοι" είναι και ελκυστικοί αλλά και πολυάριθμοι. Από την άλλη πλευρά δε συμφωνούν με τη σημασία και το μέγεθος του κινδύνου. Επομένως η ερώτηση που πρέπει να απαντηθεί με σαφήνεια είναι όχι πιο είναι το ύψος της απειλής αλλά τι έχει ή απαιτείται να γίνει για να καταπολεμηθεί αυτός ο "εχθρός".

1.8 Η απειλή της Κυβερνοτρομοκρατίας (cyber terrorism)

1.8.1 Κίνητρα-Πλεονεκτήματα-Μειονεκτήματα του κυβερνοχώρου

Σε προηγούμενο κεφάλαιο αναλύσαμε τα κίνητρα της τρομοκρατίας καθώς και το ιστορικό της υπόβαθρο. Η κυβερνοτρομοκρατία σε γενικές γραμμές μπορεί και να θεωρηθεί η χρήση του κυβερνοχώρου από τους εξτρεμιστές για να πετύχουν το σκοπό τους. Ως εκ τούτου τα κίνητρα της "κλασικής" τρομοκρατίας είναι αυτά που οδηγούν και στην κυβερνοτρομοκρατία και είναι πολιτικά, θρησκευτικά, ιδεολογικά και κοινωνικά.

Πράγματι ο κυβερνοχώρος παρουσιάζει αρκετά πλεονεκτήματα σε σύγκριση με το φυσικό επίπεδο, τα οποία από πολύ νωρίς έγιναν αντιληπτά και τα οποία φαίνονται καθαρά από την προσεκτική μελέτη των κυβερνοεπιθέσεων. Αυτά είναι:

- η ανωνυμία των δραστών
- η μη απαίτηση φυσικής παρουσίας , μία επίθεση μπορεί να πραγματοποιηθεί από πολύ απομακρυσμένη περιοχή
- δεν απαιτείται η χρήση οποιασδήποτε μορφής όπλου ή εκρηκτικού για να γίνει μια επίθεση
- δεν υπάρχει ο κίνδυνος λάθους όπως για παράδειγμα με μία "κλασική" βομβιστική επίθεση όπου ο εκρηκτικός οργανισμός πιθανόν να εκραγεί νωρίτερα από τον καθορισμένο χρόνο ή σε λάθος σημείο
- η δημοσιότητα μίας cyber attack φθάνει ή ακόμα και ξεπερνάει αυτό μίας "κλασική" τρομοκρατικής επίθεσης
- μικρές σε αριθμό μελών ομάδες μπορούν να προκαλέσουν μαζικές απώλειες και καταστροφές, όπως για παράδειγμα οι δημιουργοί του ιού nimda και blaster worm

Όμως υπάρχουν και ορισμένα μειονεκτήματα στις επιθέσεις μέσω του κυβερνοχώρου, τα οποία θα πρέπει να λαμβάνονται συνεχώς υπόψιν. Αυτά είναι:

- πολλές φορές ο έλεγχος μιας κυβερνοεπίθεσης είναι πολύ δύσκολός έως και αδύνατος με αποτέλεσμα να μην μπορεί να επιτευχθεί ακριβώς το επιθυμητό επίπεδο καταστροφής και τελικά τα αποτελέσματα να είναι διαφορετικά από τα επιθυμητά
- οι cyber attacks (κυβερνοεπιθέσεις) είναι λιγότερο εκτεθειμένες στις ιδιοτροπίες των αρχηγών των τρομοκρατικών οργανώσεων μια και οι τελευταίοι τις περισσότερες φορές δεν έχουν εξειδικευμένες γνώσεις Η/Υ
- ο σάλος που προκαλείται από μια τρομοκρατική επίθεση στο επίπεδο του κυβερνοχώρου είναι πολλές φορές μικρός γιατί αρκετές φορές οι υπηρεσίες, οι οργανισμοί που έχουν δεχτεί την επίθεση αποφεύγουν να την ανακοινώνουν στο ευρύ κοινό για την αποφυγή πανικού και δημιουργίας κλίματος στο κοινωνικό σύνολο. Εξάλλου πολλοί λιγότεροι σε αριθμό πολίτες θα καταλάβουν ότι μια δυσλειτουργία π.χ. σε μια υπηρεσία προέρχεται από ηλεκτρονική επίθεση παρά μια βομβιστική επίθεση ή μια δολοφονία.

Παρά όμως τα μειονεκτήματα που παρουσιάστηκαν παραπάνω, τα τελευταία χρόνια με τη συνεχή ανάπτυξη της τεχνολογίας έχει καταγραφεί μεγάλος αριθμός cyber attack. Παρακάτω θα αναλύσουμε τα είδη αυτών και τον τρόπο με τον οποίο σχεδιάζονται αυτές.

1.8.2 Είδη επιθέσεων εναντίον Η/Υ

Σύμφωνα με τους Janet J. Prichard και Laurie E. MacDonald Bryant University, Smithfield, R.I., U.S.A. τα είδη των επιθέσεων εναντίον Η/Υ μπορούν να κατηγοριοποιηθούν αρχικά σε τρεις βασικές κατηγορίες: (*52)*

1. φυσικές επιθέσεις ή αλλιώς επιθέσεις στο φυσικό επίπεδο
2. συντακτικές επιθέσεις (ακριβής όρος στα αγγλικά syntactic)
3. σημασιολογικές (ακριβής όρος στα αγγλικά semantic)

Με την έννοια της φυσικής επιθέσεως περιγράφουμε την επίθεση που γίνεται εναντίον ενός υπολογιστικού συστήματος ή δικτύου με την χρήση συμβατικών όπλων όπως μία βόμβα ή ένα περίστροφο π.χ. και σκοπό έχει την καταστροφή του ή την αδρανοποίηση του.

Από την άλλη πλευρά συντακτική είναι η επίθεση που χρήση software τύπου ενός ιού με στόχο την πρόκληση ζημιών σε έναν Η/Υ ή δίκτυο. Εδώ χρησιμοποιείται αρκετές φορές και ο όρος “malicious software” ή “malware” που περιλαμβάνει virus, worms και Trojan horses τα οποία διαδίδονται κυρίως μέσω internet. Επιπλέον στη δεύτερη κατηγορία περιλαμβάνονται επιθέσεις του τύπου denial of service (dos) και distributed denial of service (ddos) τα οποία θα αναλυθούν παρακάτω σε μεγαλύτερη έκταση.

Η τρίτη κατηγορία περιλαμβάνει τις σημασιολογικές επιθέσεις οι οποίες περιλαμβάνουν την τροποποίηση-παραμόρφωση πληροφοριών –παραπληροφόρηση- καθώς και τη διασπορά λανθασμένων δεδομένων και μηνυμάτων. *(53)* Φυσικά η παραπληροφόρηση και η διασπορά ψευδών ειδήσεων δεν είναι κάτι πρωτόγνωρο στην ανθρώπινη ιστορία, απλά σήμερα μέσω του διαδικτύου και των Ή/Υ γίνεται ευκολότερα σε μικρότερο χρόνο και πιθανόν αποτελεσματικότερα μέσω των web-site, email και sms.

Επιπλέον μία άλλη κατηγοριοποίηση των ηλεκτρονικών επιθέσεων είναι ανάλογα με τον βαθμό πρόσβασης του επιτιθέμενου στο "στόχο". Έτσι μια τέτοια πράξη μπορεί να πραγματοποιηθεί:

a.΄΄από μέσα΄΄ δηλαδή από άτομο που έχει φυσική πρόσβαση σε Η/Υ

b.΄΄εξωτερικά΄΄ δηλαδή από άτομο που στοχεύει σε συγκεκριμένο ευπρόσβλητο Η/Υ ή δίκτυο σε κάποιο intranet ή συνδεδεμένο στο διαδίκτυο

c. ΄΄εξωτερικά΄΄ μέσω εισόδου σε Η/Υ ή δίκτυο με την μέθοδο ΄΄βήμα-βήμα ΄΄ δηλαδή από Η/Υ σε Η/Υ

Σύμφωνα με το Australian Government Institute of Criminology σε έρευνα που πραγματοποιήθηκε το 2004 σε δημόσιες υπηρεσίες και μεγάλες εταιρίες , το 67% ανέφερε τη καταγραφή τουλάχιστον μίας ηλεκτρονικής επίθεσης στο έτος έρευνας, η οποία επηρέασε καθοριστικά τη διαθεσιμότητα των Η/Υ και των βάσεων δεδομένων. Επίσης από το σύνολο των επιθέσεων, το 88% προέρχονταν από εξωτερική πηγή ενώ το 36% από "εσωτερική πηγή".

1.8.3 Σχεδιασμός και εκτέλεση των Cyber attacks

Πολλές φορές η cyber attack ονομάζεται και Computer Network Attack (CNA) επειδή για την πραγματοποίηση τέτοιου είδους επιθέσεων απαιτείται η διασύνδεση μέσω κάποιου δικτύου (network) και με τον όρο αυτό συναντάτε στην διεθνή βιβλιογραφία.

Μία CNA επίθεση έχει ως στόχο να εμποδίσει την αποτελεσματική χρήση των υπολογιστικών και δικτυακών λειτουργιών από τον αντίπαλο. Με άλλα λόγια η διαδικασία CNA αρνείται στον εχθρό την εκτέλεση λειτουργιών που στηρίζονται σε υπολογιστικές και δικτυακές ευκολίες και καλύπτει μία σειρά από τομείς της κρατικής δομής από τις Ένοπλες Δυνάμεις ως τις μεταφορές και την Δημόσια Παιδεία.

Οι computer hackers παραδοσιακά χρησιμοποιούν πέντε βασικά βήματα προκειμένου να επιτύχουν την πρόσβαση σε μη εξουσιοδοτημένα "μέρη". Αυτά τα βήματα χρησιμοποιούνται και στην "κλασική" τρομοκρατία πολύ συχνά. Η αυτοματοποίηση τους στο χώρο του διαδικτύου γίνεται με τη χρήση αλγορίθμων και προγραμμάτων που κυκλοφορούν ελεύθερα στο internet.*(47)* Παράλληλα υψηλής τεχνολογίας εργαλεία hacking

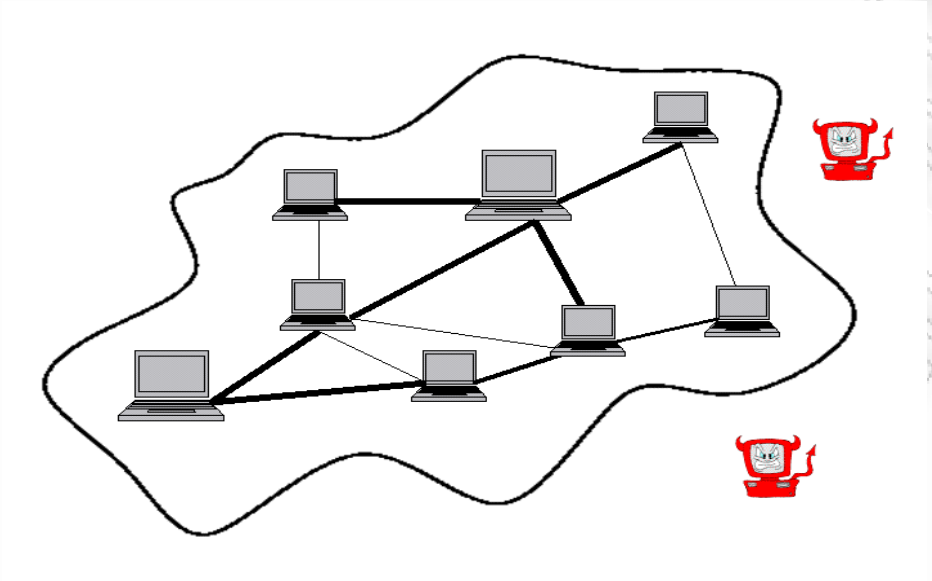
χρησιμοποιούνται από ιδιαίτερων ικανοτήτων hackers, τα οποία είναι πολύ δύσκολο για τους μηχανισμούς εντοπισμού και άμυνας να τα ανιχνεύσουν και να αντιμετωπίσουν.*(48)*

Τα βήματα που προαναφέραμε είναι τα ακόλουθα :

1. **Βήμα 1ο. Αναγνώριση και επιτήρηση του χώρου**

   Σε αυτό το πρώτο βήμα οι hackers εγκαθιστούν μια πολύ προσεκτική και λεπτομερή αναγνώριση με στόχο να ανακαλύψουν λεπτομερείς πληροφορίες για τον οργανισμό-επιχείρηση την οποία στοχεύουν ,προκειμένου αργότερα να επιτύχουν μη εξουσιοδοτημένη πρόσβαση σε αρχεία και βάσεις δεδομένων του ΄΄στόχου΄΄. Η πιο συνηθισμένη μέθοδος είναι η εξαπάτηση ενός υπαλλήλου της εταιρίας με την υποκλοπή ευαίσθητων πληροφοριών του όπως ένας προσωπικός τηλεφωνικός αριθμός ή το password, το εταιρικό email και το pin των πιστωτικών του καρτών. Μία άλλη μέθοδος είναι το λεγόμενο dumpster diving ή αλλιώς το ψάξιμο στα σκουπίδια μιας εταιρίας για την ανεύρεση ευαίσθητων πληροφοριών όπως π.χ. ένα floppy disk ή σπουδαία έγγραφα τα οποία δεν έχουν τεμαχιστεί στο κατάλληλο μηχάνημα. Αυτό το βήμα φυσικά μπορεί να αυτοματοποιηθεί αν ο επιτιθέμενος καταφέρει να τοποθετήσει ένα ιό (virus),worm ή ΄΄spy ware΄΄ πρόγραμμα το οποίο προσφέρει επιτήρηση και στη συνέχεια αποστολή χρήσιμων πληροφοριών (π.χ. Passwords) πίσω στον επιτιθέμενο. Το΄΄spy ware΄΄ ανήκει στην κατηγορία του malicious code ο οποίος πολύ εύκολα και γρήγορα εγκαθίσταται σε ένα υπολογιστή, χωρίς ο χρήστης να το αντιλαμβάνεται όταν ο τελευταίος επισκέπτεται διάφορα malicious web-site.*(49)* Μπορεί να παραμείνει ανεντόπιστο από τα firewalls και τα διάφορα anti-virus προϊόντα στέλνοντας σε ένα τρίτο πρόσωπο snapshots της οθόνης και άλλες απαγορευμένες πληροφορίες

όπως τα web-site που ο χρήστης επισκέπτεται και τα προγράμματα που χρησιμοποιεί.



ΕΙΚΟΝΑ 6: Δίκτυο Η/Υ υπό εχθρική επιτήρηση

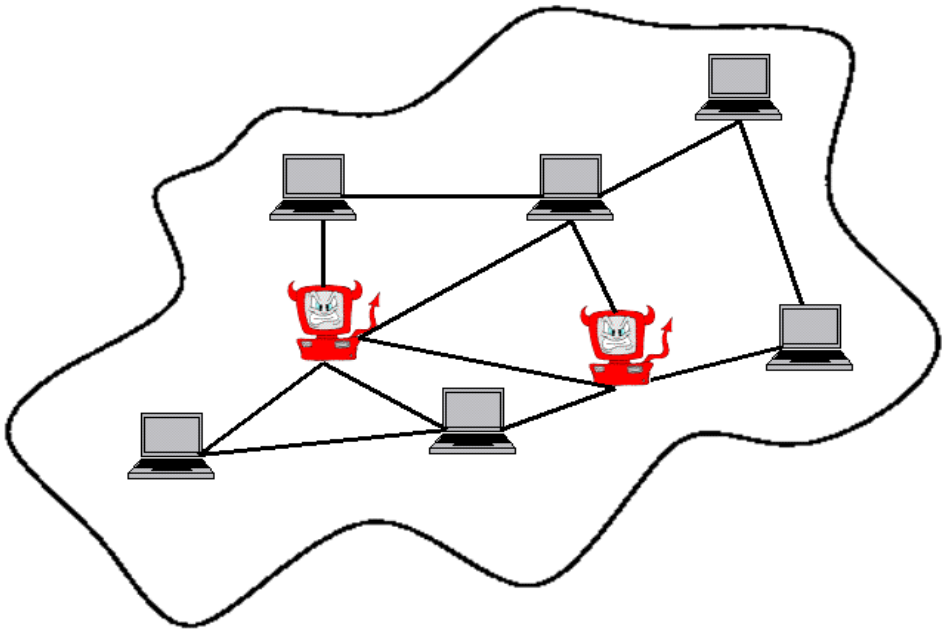
2. Βήμα 2ο. Scanning

Κατά τη διαδικασία του δεύτερου βήματος ο επιτιθέμενος προσπαθεί να αντλήσει πιο λεπτομερείς πληροφορίες για το software των Η/Υ του ΄΄στόχου΄΄ καθώς και τη διαμόρφωση του τοπικού του δικτύου. Στόχος του είναι να εντοπίσει αδυναμίες και παραλείψεις των ανωτέρω και πιθανά σημεία εισόδου στα συστήματα του. Όλη αυτή η προσπάθεια διαρκεί από μήνες έως και χρόνια και είναι αργή. Σε αρκετές περιπτώσεις γίνεται χρήση του λογισμικού "War Dailing" το οποίο σαρώνει χιλιάδες τηλεφωνικά νούμερα ψάχνοντας για modems που είναι συνδεδεμένα σε Η/Υ. Αν το computer modem απαντήσει όταν το War dialer καλέσει, τότε ο επιτιθέμενος θα έχει βρει το κατάλληλο "μονοπάτι" για να εισχωρήσει στο δίκτυο του οργανισμού- επιχείρησης που στοχεύει, έχοντας διαπεράσει το firewall της ασφάλειας. Ένα άλλο λογισμικό που

χρησιμοποιείται για scanning είναι το λεγόμενο “War Diving”. Η χρήση του γίνεται ως εξής: μία ομάδα hackers περνάει από τυχαία επιλεγμένες γειτονιές με σκοπό να εντοπίσει ασύρματα δίκτυα τόσο εταιρειών όσο και ιδιωτών, όταν το “ελεύθερο” δίκτυο εντοπιστεί ο hacker σταματάει σε κοντινό σημείο και πετυχαίνει μη εξουσιοδοτημένη πρόσβαση στο εκάστοτε δίκτυο.*(50)*

3. **Βήμα 3ο. Πρόσβαση**

Ο επιτιθέμενος έχει πετύχει την πλήρη καταγραφή του Software και των αδυναμιών της διαμόρφωσης του δικτύου του στόχου. Επομένως σιωπηλά πλέον διεισδύει στο δίκτυο με την χρήση κάποιου κλεμμένου κώδικα. Τοποθετεί ένα Trojan Horse ή κάποιο ανάλογο λογισμικό μέσω του οποίου θα δίνει εντολές από το διαδίκτυο.



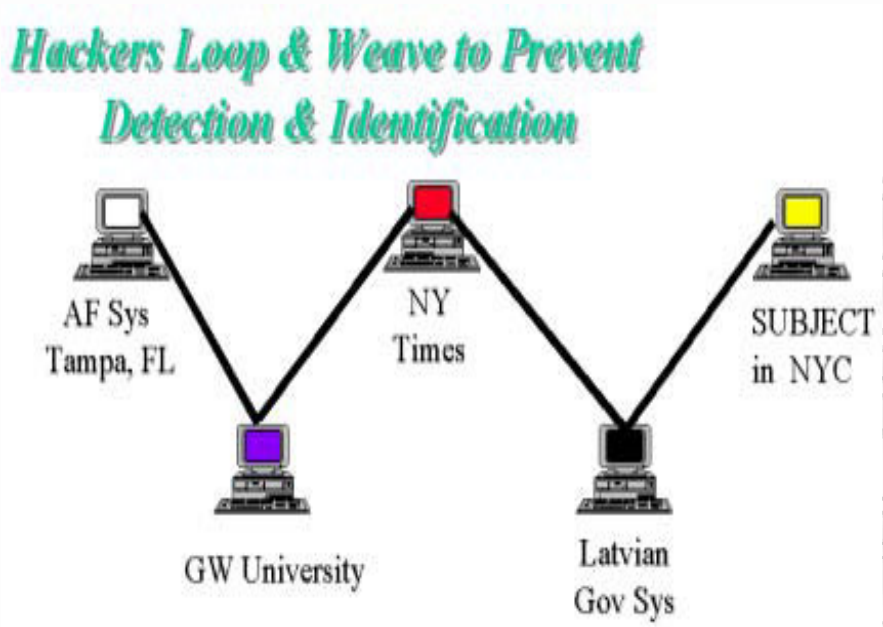
ΕΙΚΟΝΑ 7:Ο επιτιθέμενος έχει αποκτήσει πρόσβαση στο Δίκτυο

4. **Βήμα 4ο. Διατηρώντας την πρόσβαση**

"Οι πύλες είναι πλέον ανοιχτές" ο hacker έχει διεισδύσει στο δίκτυο το στόχου ενώ παράλληλα έχει τοποθετήσει και άλλα malicious codes-programs που του επιτρέπουν να επαναλαμβάνει την είσοδο κάθε φορά που το επιθυμεί. Προγράμματα που χρησιμοποιούνται πολύ συχνά είναι τα "Root Kits" ή "Back Doors". Σε μερικές περιπτώσεις ο επιτιθέμενος μπορεί να αποκτήσει όλα τα "προνόμια" ενός system administrator και τότε ο Η/Υ ή το δίκτυο έρχεται κυριολεκτικά στον πλήρη έλεγχο του. Μάλιστα σε κάποιες περιπτώσεις έχει παρατηρηθεί το εξής παράδοξο φαινόμενο: hacker ο οποίος έχει διεισδύσει σε δίκτυο παράνομα τοποθετεί διάφορα software patches προκειμένου να μειώσει τα τρωτά σημεία και να κρατήσει άλλους επίδοξους hackers μακριά.

5. **Βήμα 5^{ο}. Καλύπτοντας τα ίχνη**

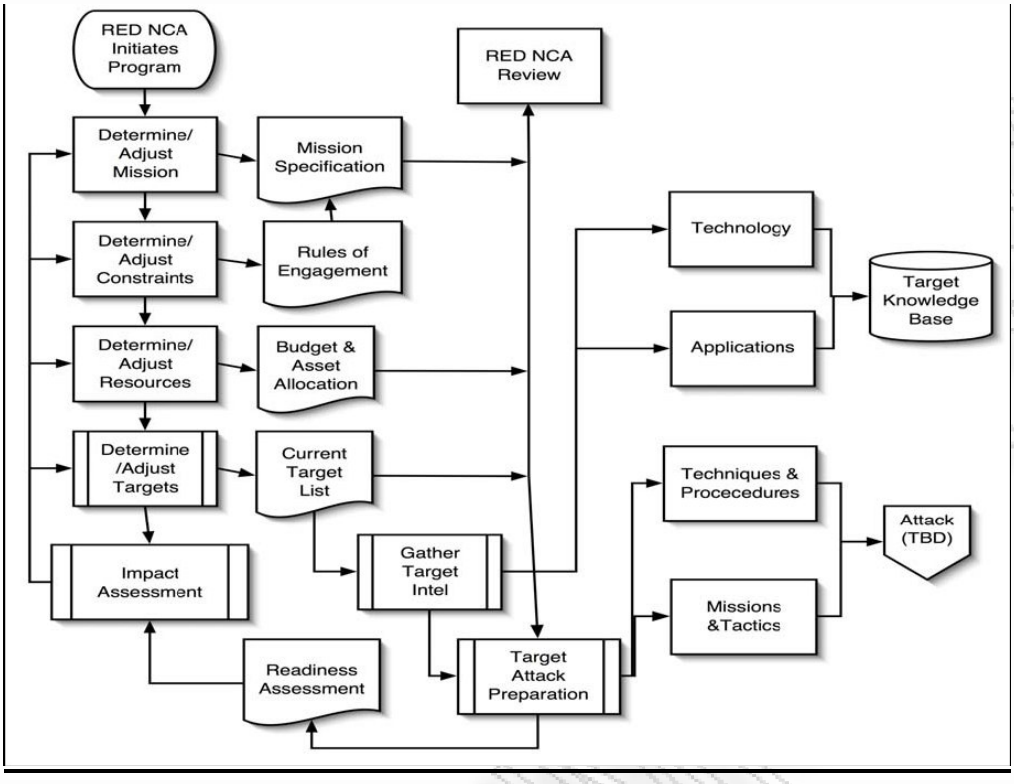
Ένας σοβαρός hacker προσπαθεί να πετύχει σιωπηλή και διακριτική διείσδυση σε ένα δίκτυο προκειμένου να καταφέρει να υποκλέψει τα δεδομένα που επιθυμεί χωρίς να αφήσει τα παραμικρό ίχνος. Παράλληλα προσπαθεί να παραμείνει για όσον το δυνατόν κρυμμένος προκειμένου να διατηρήσει τον έλεγχο του δικτύου ή του Η/Υ για μεγαλύτερο χρονικό διάστημα να πραγματοποιήσει όσο το δυνατόν μεγαλύτερη υποκλοπή στοιχείων και δεδομένων και να βελτιώσει την προεργασία του για να προκαλέσει όσο γίνεται μεγαλύτερη ζημία. Λογισμικά όπως τα Trojan Horse και Root Kit δίνουν τη δυνατότητα στον επιτιθέμενο να δημιουργήσει κρυφούς φακέλους για να αποφύγει τον εντοπισμό από τα διάφορα αμυντικά συστήματα. Τα τελευταία μπορεί να μη μπορέσουν να εντοπίσουν προσπάθεια μη εγκεκριμένης εισόδου στα συστήματα κάποιου από ένα εισβολέα για μεγάλο χρονικό διάστημα. *(51)*



ΕΙΚΟΝΑ 8: Προσπάθεια αποφυγής εντοπισμού HACKER

Με την πάροδο του χρόνου και τη συνεχή εξέλιξη της τεχνολογίας τα βήματα που προαναφέραμε εκτελούνται αυτομάτως από προγράμματα που ονομάζονται “bots”, τα οποία είναι ιδιαιτέρως αυτόνομα, πολύπλοκα και δύσκολο να εντοπιστούν και να αντιμετωπισθούν. Επιπλέον ελέγχονται από μακριά με εντολές που στέλνονται μέσω internet με αποτέλεσμα την ενεργοποίηση τέτοιων προγραμμάτων σε χιλιάδες Η/Υ ανά την υφήλιο ταυτόχρονα. Με την ενεργοποίηση τους Η/Υ που βρίσκονται υπό τον έλεγχο εισβολέα μπορούν ταυτόχρονα να εκτελέσουν ηλεκτρονική επίθεση μέσω διαδικτύου η οποία περιγράφεται με τον όρο “swarm” (σμήνος).

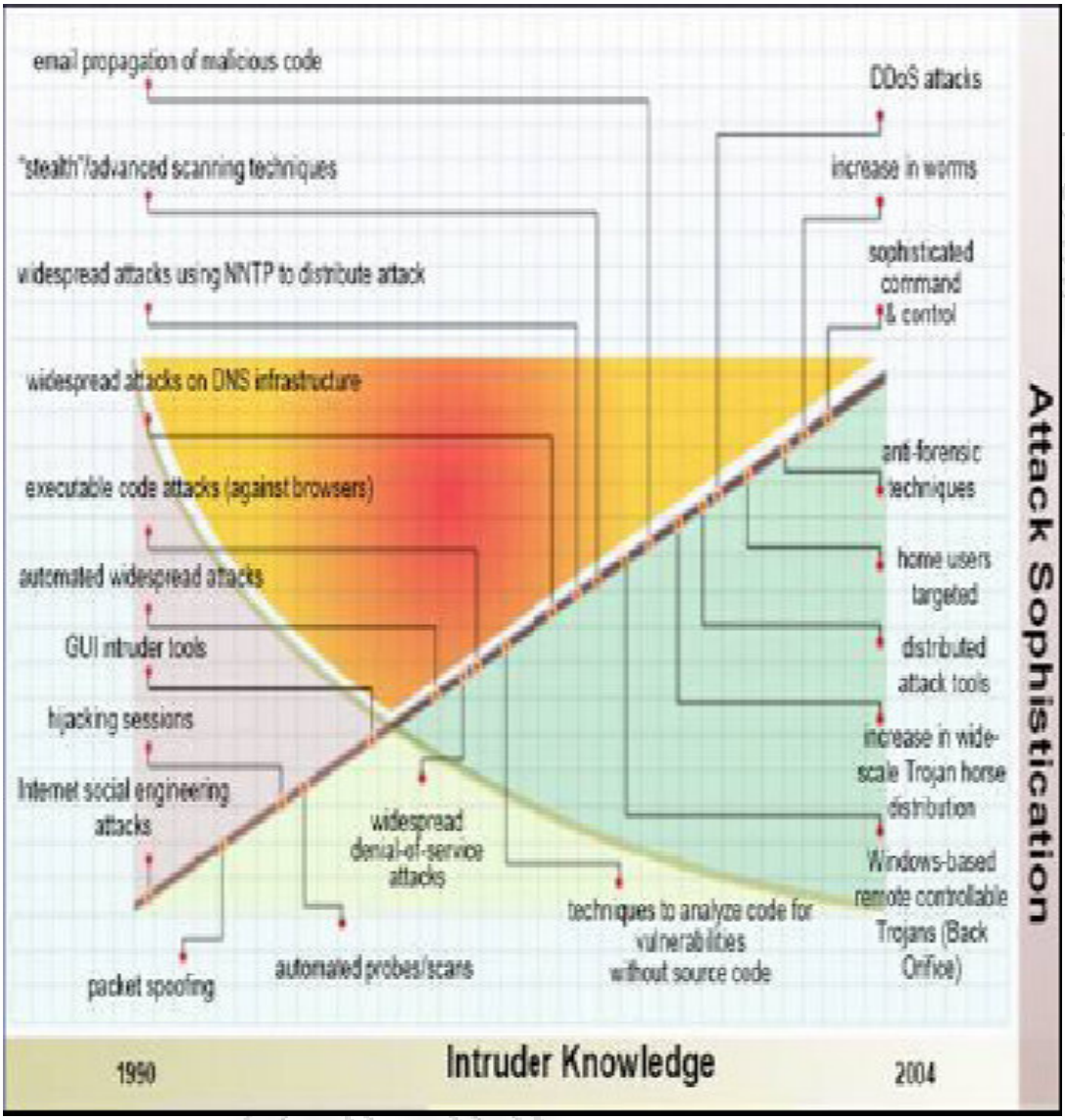
Στο παρακάτω διάγραμμα γίνεται θεωρητική ανάλυση σε blocs μιας CNA η οποία όμως προέρχεται από κάποιο κρατικό οργανισμό π.χ. το Ιράν, την Κίνα κ.α. Σε μικρότερης κλίμακας επιθέσεις το παρακάτω μοντέλο πραγματοποιείται επιτόπου και σε πολύ πιο σύντομο χρονικό διάστημα. Όμως αποτελεί ένα πολύ καλό παράδειγμα της προετοιμασίας και της προσοχής που απαιτεί μία cyber attack για να είναι επιτυχής.



ΕΙΚΟΝΑ 9: Βήματα μιας CNA εκτελεσθείσας από κρατική υπηρεσία

1.8.4 Κατηγοριοποίηση των Cyber Attacks

Στο παρακάτω διάγραμμα φαίνεται η εξελικτική διαδικασία όσον αφορά τις εκτελούμενες επιθέσεις εναντίον οργανισμών, εταιρειών και ιδιωτών στο χώρο του διαδικτύου. Στη συνέχεια αναφέρουμε αναλυτικά αυτές τις κατηγορίες των Cyber Attacks. Έτσι έχουμε:



ΕΙΚΟΝΑ 10: Διάγραμμα εξελικτικής πορείας των cyber επιθέσεων από το 1990 - 2004

1.8.4.1 Denial of Service attack (Επίθεση άρνησης υπηρεσίας)

Σε αυτή την κατηγορία επιθέσεων σκοπός του επιτιθέμενου δεν είναι η καταστροφή, με την κλασική έννοια του όρου του Η/Υ ή ενός δικτύου αλλά να τα καταστήσει τόσο απασχολημένα με αποτέλεσμα την αδυναμία εξυπηρέτησης των νόμιμων χρηστών. Υπάρχουν διάφοροι τρόποι για να επιτύχουμε μια επίθεση τύπου DoS όπως π.χ. με την αλλαγή των επίσημων χαρακτηριστικών ενός Η/Υ, με τη προσβόλη των διαφόρων εφαρμογών του κ.α.

Η ταξινόμηση αυτών των επιθέσεων γίνεται με βάση τον server που χρησιμοποιείται από τον επιτιθέμενο ώστε να καταστεί αδύνατη η χρήση του από τους επίσημους χρήστες, όπως φαίνονται και στον παρακάτω πίνακα.

ΕΙΔΟΣ ΕΠΙΘΕΣΗΣ	SERVICE	ΑΠΟΤΕΛΕΣΜΑ ΤΗΣ ΕΠΙΘΕΣΗΣ
Apache 2	HTTP	ΚΑΤΑΡΡΕΥΣΗ
Back	HTTP	Η ΑΝΤΙΔΡΑΣΤΙΚΗ ΙΚΑΝΟΤΗΤΑ ΤΟΥ SERVER ΜΕΙΩΝΕΤΑΙ
Land	HTTP	ΚΑΤΑΡΡΕΥΣΗ
Mail Bomb	N/A	ΠΡΟΒΛΗΜΑΤΑ ΣΤΗ ΛΕΙΤΟΥΡΓΙΑ
SYN Flood	TCP	ΑΔΥΝΑΜΙΑ ΕΞΥΠΗΡΕΤΗΣΗΣ ΕΝΟΣ Ή ΠΕΡΙΣΣΟΤΕΡΩΝ PORTS
Ping of Death	LCMP	ΚΑΝΕΝΑ ΑΠΟΤΕΛΕΣΜΑ
Process Table	TCP	ΑΔΥΝΑΜΙΑ ΝΕΩΝ ΣΥΝΔΕΣΕΩΝ
Smurf	LCMP	ΜΕΙΩΣΗ ΤΗΣ ΤΑΧΥΤΗΤΑΣ ΤΟΥ ΔΙΚΤΥΟΥ
Syslog	SYSLOG	ΚΑΤΑΡΡΕΥΣΗ
Teardrop	N/A	ΕΠΑΝΕΚΚΙΝΗΣΗ ΤΗΣ ΜΗΧΑΝΗΣ

Upstrom	ECHO/CHARGEN	ΜΕΙΩΣΗ ΤΗΣ ΤΑΧΥΤΗΤΑΣ ΤΟΥ ΔΙΚΤΥΟΥ

Πίνακας 1:Εείδη επιθέσεων, server και αποτελέσματα επιθέσεως

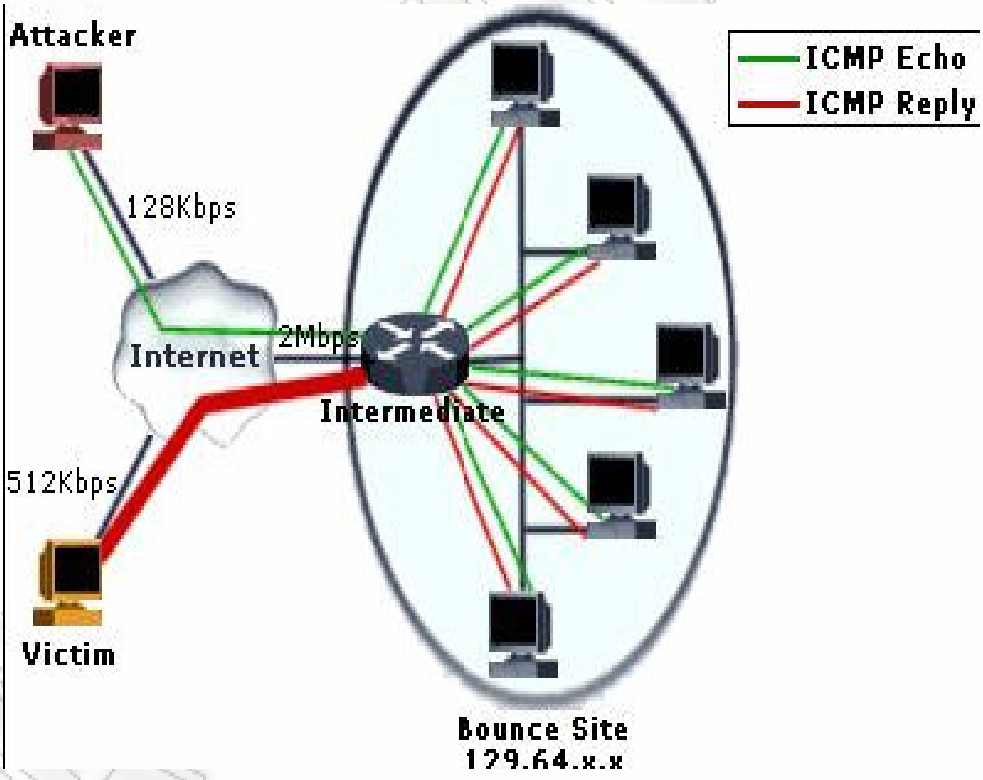
- Apache 2. Στη συγκεκριμένη περίπτωση χρησιμοποιείται το web server Apache 2. Το τελευταίο δέχεται υπερβολικά μεγάλο αριθμό αιτήσεων εξυπηρέτησης με αποτέλεσμα να μειώνεται η διαθεσιμότητα του και τελικά να καταρρέει. Η επαναλειτουργία του server γίνεται με την παρέμβαση του system administrator.
- Back. Αντίστοιχο με το παραπάνω και με ανάλογα αποτελέσματα.
- Land. Επιθέσεις εναντίον TCP/IP εφαρμογών όταν ο "εχθρός" στέλνει spoofed SYN πακέτα με τη source και destination address να είναι οι ίδιες. Φυσικά το γεγονός αυτό θεωρητικά δεν είναι και τόσο συνηθισμένο. Ο επιτιθέμενος στοχεύει στα δίκτυα που δεν είναι τόσο καλά μορφοποιημένα και χρησιμοποιεί "αθώους" Η/Υ ως zombie προκειμένου να εκτελεσθούν οι DoS επιθέσεις. Αυτού του τύπου οι επιθέσεις μπορούν να αντιμετωπισθούν μόνο με την καλή και λειτουργική σχεδίαση και κατασκευή των δικτύων.
- Mail Bomb. Σε αυτή την περίπτωση ο επιτιθέμενος προσπαθεί να στείλει χιλιάδες e-mail σε ένα μόνο user. Αποτέλεσμα της επίθεσης αυτής είναι η απώλεια του server μόνιμα. Αντιμετώπιση μια τέτοιας δυσάρεστης κατάστασης γίνεται με την επέμβαση του system administrator.
- SYN Flood (Neptune). Ανήκει στην κατηγορία των DoS επιθέσεων εναντίον κάθε TCP/IP εφαρμογής όπου ο επιτιθέμενος κάνει χρήση των μισών διαθέσιμων TCP συνδέσεων, προκειμένου να παραφορτώσει ένα δίκτυο δεδομένων. Με τον τρόπο αυτό οι επίσημοι χρήστες του δικτύου δεν έχουν πρόσβαση σε αυτό ενώ η βλάβη μπορεί να είναι μόνιμη. Η αναμονή αριθμού ταυτόχρονων πακέτων προερχόμενα από τον ίδιο host σε δεδομένη σύντομη χρονική περίοδο μπορεί να αποτρέψει τέτοιου είδους επιθέσεις.

- Ping of Death (PoD). Τέτοιου είδους επιθέσεις πραγματοποιούνται κυρίως εναντίον παλαιότερων εκδόσεων operating systems, όπου ο "εχθρός" προσπαθεί να αποστείλει ένα υπερμέγεθες IP πακέτο. Η αντίδραση του συστήματος είναι συχνά απρόβλεπτη προκαλώντας crashing και rebooting στον Η/Υ. Η τεχνική που χρησιμοποιείτε για την αντιμετώπιση τέτοιων περιστατικών είναι ο αποκλεισμός ICMP (Internet Control Message Protocol) πακέτων μεγαλύτερων των 64000 bytes.

- Process Table. Αυτής της κατηγορίας οι επιθέσεις πραγματοποιούνται εναντίον μιας πληθώρας συστημάτων Unix. Ο επιτιθέμενος προσπαθεί να διαθέσει νέα και διαφορετική διαδικασία κάθε φορά για κάθε TCP/IP σύνδεση. Έτσι όταν το system process table είναι γεμάτο οι διάφορες εντολές δε μπορούν να πραγματοποιηθούν. Η αδυναμία παροχής υπηρεσιών συνήθως σε αυτές τις περιπτώσεις είναι προσωρινή.

- Smurf. Οι επιθέσεις αυτές αποτελούν ουσιαστικά παράδειγμα των ενισχυμένων "*reflector attack"* ή διαφορετικά "αντιδραστικών επιθέσεων". Σε γενικότερο πλαίσιο αυτής της ομάδας οι επιθέσεις περιλαμβάνουν τα εξής: πακέτα τα οποία περιέχουν την IP διεύθυνση του θύματος στο μέρος του source address, τα οποία μεταδίδονται από τον επιτιθέμενο σε ένα μεγάλο αριθμό servers και routers του διαδικτύου. Οι τελευταίοι αντιλαμβάνονται αυτά τα πακέτα ως αίτηση υπηρεσίας (request of service) και αποστέλλουν ("*αντιδρούν"*) απαντήσεις απευθείας στην source address του πακέτου, δηλαδή απευθείας στο θύμα. Αποτέλεσμα είναι το θύμα να κατακλύζεται από ένα τεράστιο αριθμό πακέτων των οποίων τα ίχνη είναι δύσκολο να εντοπισθούν μιας και προέρχονται από τελείως διαφορετικές διευθύνσεις και μηχανές. Παράδειγμα Smurf IP Denial of Service Attack: Η επίθεση αυτή βασίζεται στην ικανότητα του "εχθρού" να νοθεύει τις IP source addresses. Ο τελευταίος στέλνει request για return packet σε ορισμένα ενδιάμεσα δίκτυα, το οποίο αυτομάτως καταλήγει σε request σε όλα τα μηχανήματα που είναι συνδεδεμένα στο διαδίκτυο. Αυτά απαντούν στην παραπάνω πρόσκληση με ένα return packet. Παράλληλα ο επιτιθέμενος αντικαθιστά την αληθινή source address (δηλαδή τη διεύθυνση στην οποία

όλα τα μηχανήματα θα απαντήσουν) με τη διεύθυνση του υποψήφιου θύματος. Έτσι τελικά το θύμα κατακλύζεται από απαντήσεις από όλα τα μηχανήματα που είναι συνδεδεμένα στο ενδιάμεσο δίκτυο. Αυτό έχει ως αποτέλεσμα να φαίνεται το ενδιάμεσο δίκτυο ως θύμα, χωρίς να είναι στην πραγματικότητα. Με τον τρόπο αυτό ο επιτιθέμενος μπορεί να στείλει παρόμοια νοθευμένα πακέτα και σε άλλα ενδιάμεσα δίκτυα ταυτόχρονα για την καλύτερη εκτέλεση της επίθεσης δημιουργώντας τόσο μεγάλο συνωστισμό στο site του θύματος που θα είναι εξαιρετικά απίθανο να μπορέσει να εκτελέσει οποιαδήποτε εργασία ή να παρέχει την οποιαδήποτε υπηρεσία.*(72)*



ΕΙΚΟΝΑ 11: Smurf IP Denial of Service Επίθεση

Οι τρόποι αντίδρασης του θύματος σε μια τέτοια κατάσταση είναι εξαιρετικά περιορισμένοι ειδικά αν η επίθεση είναι σε εξέλιξη. Όμως τα τελευταία χρόνια έχει διαπιστωθεί ότι η καλύτερη μέθοδος άμυνας είναι το

φιλτράρισμα και η απόρριψη εξερχόμενων πακέτων που περιέχουν source addresses και οι οποίες δεν είναι μέρος των IP διευθύνσεων του δικτύου τους και συνεπώς δεν μπορεί να αποτελούν επίσημα πακέτα αυτού. Παράλληλα πρέπει να ακολουθείται η ίδια διαδικασία για τους network administrators για πακέτα εισερχόμενα εκτός της "επικράτειας" τους. Με αυτούς τους δύο τρόπους προστατεύεται ένα δίκτυο, από όλους εκείνους που κάνουν χρήση επιθετικών πακέτων με σκοπό την δυσλειτουργία του δικτύου.

- Syslog. Αυτού του είδους οι DoS επιθέσεις εκτελούνται εναντίον Solaris servers με σκοπό την καταστροφή του Syslog service. Η βλάβη που μπορεί να προκληθεί είναι πάγια και αντιμετωπίζεται όπως και αρκετές παραπάνω με την επέμβαση του administrator του συστήματος.
- Teardrop. Στην περίπτωση αυτή το θύμα είναι παλαιότερες εκδόσεις του TCP/IP. Ο επιτιθέμενος αξιοποιεί τα χαρακτηριστικά της διαδικασίας αναμόρφωσης του IP. Η βλάβη που προκαλείται είναι προσωρινή.
- Udpstrom. Επιθέσεις τύπου DoS όπου ο επιτιθέμενος χρησιμοποιεί τα χαρακτηριστικά του UDP για να προκαλέσει συμφόρηση και μείωση της ταχύτητας του δικτύου. Ο εντοπισμός μιας τέτοιας επίθεσης απαιτεί την έρευνα για spoofed πακέτα και τον έλεγχο του traffic του δικτύου. Παρά το γεγονός ότι η βλάβη που προκαλείται είναι μόνιμη, αντιμετωπίζεται με την βοήθεια του system administrator.

Ένα πρόσφατο σχετικά παράδειγμα αυτής της κατηγορίας επιθέσεων είναι εναντίον του Yahoo, του CNN και του eBay και άλλων εμπορικών web-sites το Φεβρουάριο του 2000, οι οποίες προκάλεσαν ζημιές δισεκατομμυρίων δολαρίων. Επίσης πιο εξειδικευμένα δίκτυα Η/Υ όπως αυτά του NATO έχουν δεχτεί DoS επιθέσεις. Συγκεκριμένα το 1999 από hackers, οι οποίοι διαμαρτύρονταν για τους Νατοϊκούς βομβαρδισμούς στο Κοσσυφοπέδιο.

1.8.4.2 Distributed Denial of Service Επίθεση (Κατανεμημένη Επίθεση άρνησης υπηρεσίας)

Αποτελεί τη δεύτερη κατηγορία cyber attack, παραδείγματα της οποίας έχουν κατά καιρούς δει το φως της δημοσιότητας. Στη περίπτωση αυτή πρόκειται για Denial of Service επίθεση όπου χρησιμοποιούνται πολλαπλά συστήματα για να επιτεθούν σε ένα ή περισσότερα

θύματα, με στόχο την αδυναμία εξυπηρέτησης των νόμιμων χρηστών αυτών των συστημάτων και την υποκλοπή πληροφοριών μεγάλης αξίας, παρά την καταστροφή Η/Υ και δικτύων. Συνηθισμένοι στόχοι τέτοιου είδους επιθέσεων είναι συνδέσεις DSL και πανεπιστημιακά address blocks. Σε μια τυπική DDoS επίθεση το θύμα τίθεται εκτός μέσω μιας πλημμυρίδας από malicious attack packets, με καταγωγή ένα τεράστιο αριθμό από μηχανές zombie, οι οποίες προηγουμένως έχουν διαφθαρεί από τον επιτιθέμενο. *(Με τον όρο zombie εννοούμε ένα μη ασφαλή server ελεγχόμενο από hacker, ο οποίος όταν διαταχθεί θα εξαπολύσει ένα τεράστιο αριθμό επιθέσεων ενός web-site, συνήθως σε συνεργασία με άλλες zombie machines για τον συγχρονισμό και την αύξηση της αποτελεσματικότητας των επιθέσεων. Με τον όρο πακέτο –packet- νοείται μια ομάδα δεδομένων η οποία κινείται μεταξύ σημείου και σημείου προορισμού στο Διαδίκτυο).*

Το destination address θα περιλαμβάνει και την IP διεύθυνση του θύματος, όμως η IP κάθε πακέτου έχει διαφθαρεί. Στις σύγχρονες DDoS επιθέσεις η "πειραγμένη" source address επιλέγεται τυχαία. Έτσι όλα τα attack packets περιέχουν ψεύτικη source IP διεύθυνση με αποτέλεσμα να μην είναι δυνατός ο εντοπισμός των πραγματικών διευθύνσεων, αυτών που εκτελούν μια τέτοιου είδους επίθεση.

Επιπλέον αρκετές φορές τα attack packets περιλαμβάνουν μη αρτιμελής source address η οποία δεν ανταποκρίνεται σε κανένα Η/Υ συνδεδεμένο στο διαδίκτυο. Επιθέσεις αυτής της κατηγορίας έχουν παρουσιαστεί κατά καιρούς όπως αυτή του on line casino BetCRIS .com. Ο επιτιθέμενος αφού εκτέλεσε επίθεση στο συγκεκριμένο δικτυακό τόπο, απαίτησε το πόσο των 500$ για να σταματήσει να το παρενοχλεί. Όταν του καταβλήθηκε το ποσό επανήλθε απαιτώντας αυτή τη φορά 40.000$. Τελικά οι δημιουργοί του συγκεκριμένου web-site αποφάσισαν να μην ενδώσουν και απευθύνθηκαν στις αρμόδιες αρχές με αποτέλεσμα τη σύλληψη μιας ομάδας φοιτητών οι οποίοι ήταν υπεύθυνοι για τον εκβιασμό.

1.8.4.3 Domain Name Service (DNS) Επίθεση

Το Domain Name Service είναι κρίσιμης σημασίας για την αρτιότητα του Διαδικτύου μιας και αντιστοιχεί ένα όνομα σε μια IP διεύθυνση. Οι χρήστες του internet το εμπιστεύονται και μέσω αυτού γίνεται η εύρεση του site που επιθυμούν με την χρήση απλά ενός ονόματος, π.χ. όταν πληκτρολογούν www.cnn.com για να βρουν το δικτυακό τόπο του καναλιού CNN

επιθυμούν να βρεθούν άμεσα σχεδόν στο συγκεκριμένο web-site. Φυσικά αυτό αντιστοιχεί σε κάποια συγκεκριμένη αριθμητική διεύθυνση, στην παραπάνω περίπτωση 64.12.50.153.

Αν όμως ο DNS Server εκτελέσει λανθασμένη αντιστοίχηση ονόματος – αριθμητικής διεύθυνσης τότε ο χρήστης του Διαδικτύου θα συνδεθεί σε λανθασμένο server. Εκτός όμως αυτού, αν μια επίθεση στο DNS είναι καλά οργανωμένη το θύμα δεν πρόκειται να αντιληφθεί το παραμικρό. Παράλληλα θα έχει την εντύπωση ότι βρίσκεται στον web server του CNN, ενώ στην πραγματικότητα θα βρίσκεται στον server του επιτιθέμενου. Επιπλέον ο επιτιθέμενος μέσω μιας επίθεσης αυτής της κατηγορίας μπορεί να διασπείρει ψευδείς πληροφορίες τόσο μέσω ενός server ή ομάδας server και μπορεί να εμποδίσει την πρόσβαση στο πραγματικό web-site παραπλανώντας τους χρήστες του Διαδικτύου.

Η δομή των DNS server είναι ιεραρχική. Τα local DNS server ανανεώνουν τις πληροφορίες που έχουν μόνο για την δική τους ζώνη και επικοινωνούν με τα άλλα DNS server για πληροφορίες στις υπόλοιπες ζώνες. Στην κορυφή της ιεραρχίας είναι ο root name server ο οποίος διατηρεί συνεχώς πληροφόρηση για το ποιος server είναι υπεύθυνος για κάθε τοπική ζώνη. Η μέχρι τώρα εμπειρία έχει δείξει ότι επιτυχημένες επιθέσεις αυτού του τύπου έχουν προετοιμασθεί εναντίον local DNS server, προκαλώντας συμφόρηση σε επιλεγμένα web-sites και τελικά κατάρρευση τους.

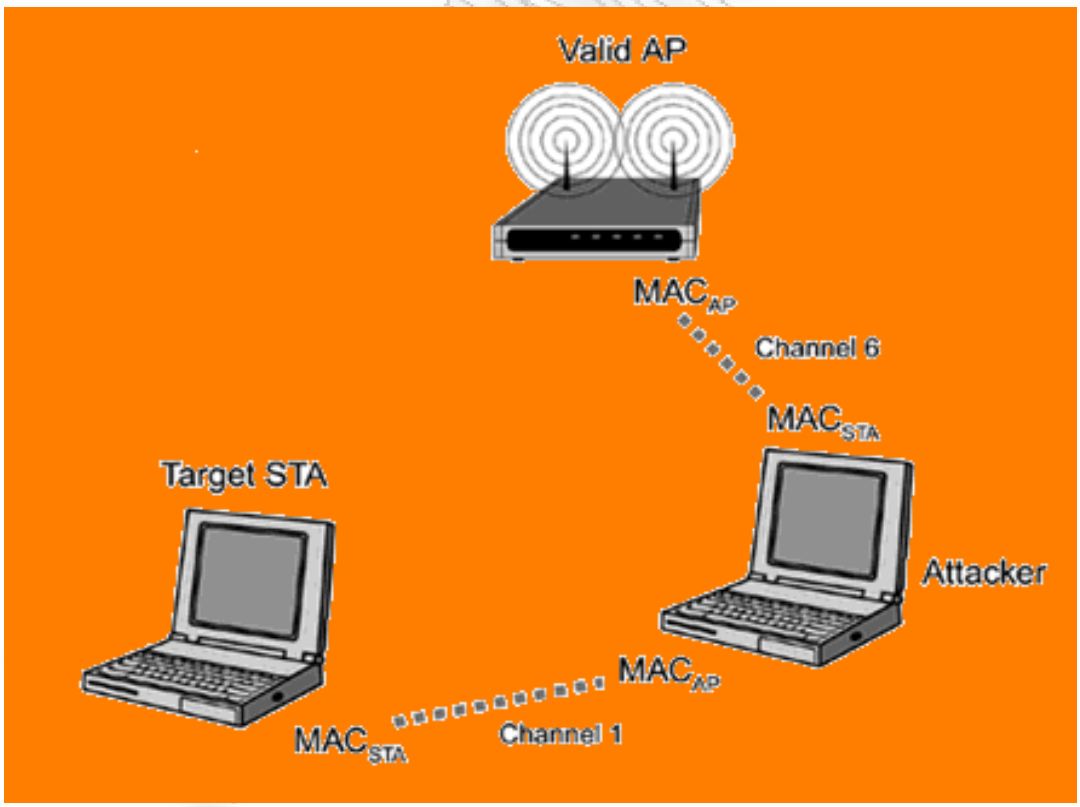
1.8.4.4 Επιθέσεις τροποποίησης

Οι τροποποιήσεις στα δεδομένα μπορούν να επιτευχθούν με μερικούς μη ορατούς τρόπους. Όταν σκεφτόμαστε τις επιθέσεις τροποποίησης οι περισσότεροι σκέφτονται έναν επιτιθέμενο που τροποποιεί το ηλεκτρονικό ταχυδρομείο με κακόβουλο περιεχόμενο ή που αλλάζει τους αριθμούς σε μια ηλεκτρονική τραπεζική μεταφορά. Ενώ τέτοιες υψηλού επιπέδου τροποποιήσεις έχουν ολοκληρωθεί, υπάρχουν και άλλοι τρόποι να τροποποιηθούν τα δεδομένα. Παραδείγματος χάριν, εάν κάποιος μπορεί να παρεμποδίσει μια ασύρματη μετάδοση και να αλλάξει τον τομέα διεύθυνσης προορισμού (διεύθυνση IP) σε ένα μήνυμα, θα μπορούσε να διαβιβάσει το μήνυμα στον εαυτό του διαμέσου του Διαδικτύου, αντί το μήνυμα να διαβιβαστεί στον προοριζόμενο παραλήπτη. Αυτό θα το έκανε γιατί το μήνυμα στην ασύρματη σύνδεση κρυπτογραφείται και δε μπορεί να διαβαστεί το περιεχόμενο αλλά, εάν μπορεί ο επιτιθέμενος να το πάρει διαβιβασμένο από το Διαδίκτυο θα λάβει την αποκρυπτογραφημένη έκδοση. Η επιγραφή IP είναι ευκολότερο να δεχτεί επίθεση γιατί είναι

μια γνωστή μορφή. Μια επίθεση τροποποίησης είναι η man-in-the-middle επίθεση (άτομο στην μέση).

1.8.4.5 Man-in-the-middle επιθέσεις

Υπάρχουν δύο διαφορετικές μέθοδοι για να καθιερωθεί μια Man-in-the-middle επίθεση (MiM) σε ένα ασύρματο δίκτυο. Ο πρώτος χρησιμοποιεί τα πλαίσια διαχείρισης και είναι συγκεκριμένος για την ασύρματη δικτύωση και ο δεύτερος είναι ARP spoofing, η οποία είναι επίσης ένα πρόβλημα για τα συνδεμένα με καλώδιο δίκτυα. Στις επιθέσεις αυτές ο δράστης διεισδύει μεταξύ δύο σημείων ασύρματης πρόσβασης (AP) ενός δικτύου εξαναγκάζοντας καθένα από αυτά να εξουσιοδοτήσει και πιστοποιηθεί με το σημείο ή συσκευή ασύρματης πρόσβασης του δράστη. Έτσι, το περιεχόμενο της επικοινωνίας των δύο σημείων ασύρματης πρόσβασης στο δίκτυο κατευθύνεται από τον αποστολέα στον λήπτη μέσω του ασύρματου σημείου ή συσκευής πρόσβασης του δράστη, ο οποίος φυσικά υποκλέπτει πλήρως το περιεχόμενο της επικοινωνίας.



EIKONA12: Man in the Middle Επίθεση

1.8.4.6 Επιθέσεις Μεταμφίεσης

Η μεταμφίεση είναι ο όρος που χρησιμοποιείται όταν μια επιτιθέμενη συσκευή δικτύων παίζει τον ρόλο μιας έγκυρης συσκευής. Είναι η ιδανική προσέγγιση εάν ένας επιτιθέμενος θέλει να παραμείνει μη ανιχνευθείς. Εάν η συσκευή μπορεί επιτυχώς να ξεγελάσει το δίκτυο στόχο με την επικύρωση του ως εξουσιοδοτημένη συσκευή, ο επιτιθέμενος παίρνει όλα τα δικαιώματα πρόσβασης που η εξουσιοδοτημένη συσκευή καθιέρωσε κατά τη διάρκεια της σύνδεσης. Επιπλέον, δε θα υπάρξει καμία προειδοποίηση ασφάλειας. Ούτε ένας διευθυντής I.T. που ανιχνεύει τα αρχεία κυκλοφορίας δε θα δει τίποτα ύποπτο, εκτός εάν ο επιτιθέμενος κάνει τα πράγματα που ένας κανονικός χρήστης δε θα έκανε, όπως η προσπάθεια να προσεγγιστούν οι περιοχές συστημάτων. Υπάρχουν φυσικά, μη ηλεκτρονικές επιθέσεις βασισμένες στη μεταμφίεση που είναι εξίσου αποτελεσματικές εάν κάποιος αφήνει το τερματικό του συνδεμένο και απομακρύνεται από την θέση εργασίας του, καθένας μπορεί να καθίσει και να πάρει τα δικαιώματα πρόσβασής του.

1.8.5 Τεχνικές Hacking-"εργαλεία" επιθέσεων

Πριν αναλύσουμε τις σύγχρονες τεχνικές hacking είναι ορθό να δώσουμε στοιχεία για την έννοια του hacker, δηλαδή του ατόμου που προβαίνει σε τέτοιου είδους ενέργειες ανεξάρτητα από τα βαθύτερα αίτια της πράξης του .

Με τον όρο hackers χαρακτηρίζονται εκείνα τα άτομα που έχουν εξειδικευμένες τεχνικές γνώσεις υπολογιστών γενικότερα, προχωρημένες γνώσεις προγραμματισμού και μπορούν να εντοπίσουν αδυναμίες σε συστήματα υπολογιστών. Αρχικά οι ίδιοι θεωρούσαν ότι προσφέρουν κοινωνικό έργο καθώς η παράνομη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε υπολογιστικά συστήματα δεν γίνονταν με σκοπό την δολιοφθορά ή την καταστροφή, την υποκλοπή ή την κατασκοπεία αλλά κυρίως την προσωπική τους ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ και την επιβεβαίωση της έννοιας της ελευθερίας στον ψηφιακό χώρο με την δημιουργία και την διάδοση ελεύθερου software.

Οι hackers εμφανίστηκαν για πρώτη φορά στα τηλεπικοινωνιακά δρώμενα τη δεκαετία του 1970 στις Η.Π.Α. . Συγκεκριμένα το 1972 ο John Draper ή αλλιώς Captain Crunch χρησιμοποιούσε μια απλή παιδική σφυρίχτρα για να πραγματοποιεί δωρεάν τηλεφωνήματα οπουδήποτε επιθυμούσε στις Η.Π.Α. . Αυτός υπήρξε και ο πρώτος επίσημα καταγεγραμμένος

hacker. Το 1984 ο Fred Cohen δημιουργεί τον πρώτο virus και το 1989 ο Kevin Mitnic καταδικάζεται για την κλοπή software από ηλεκτρονικό εξοπλισμό, ενώ το 1995 συλλαμβάνεται για δεύτερη φορά για την κλοπή 20.000 αριθμών πιστωτικών καρτών.

Οι crackers από την άλλη μεριά, είναι εκείνα τα άτομα τα οποία χαρακτηρίζονται ως κακόβουλους hackers αφού η παράνομη εισβολή τους στα υπολογιστικά συστήματα γίνεται με στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την άρση της προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους και ενέργειες που θα τους αποκομίσουν οικονομικά οφέλη όπως για παράδειγμα μεταφορά σε προσωπικό λογαριασμό τραπέζης μεγάλων χρηματικών ποσών από υποκλοπή αριθμού πιστωτικής/ων κάρτας/ων. Τα τελευταία χρόνια οι δύο παραπάνω έννοιες συγχωνεύτηκαν με επικράτηση του όρου hacking και hacker αντίστοιχα.

Τα "εργαλεία" που χρησιμοποιούνται για την εκτέλεση των στόχων ενός hacker, είναι πολλά και κάθε μέρα ανανεώνονται και εξελίσσονται. Επιπλέον στις περισσότερες περιπτώσεις γίνεται όπου αυτό είναι δυνατόν συνδυασμένη χρήση τους. Παρακάτω περιγράφουμε τα κυριότερα από αυτά:

1. **IP Address Spoofing.** Πρόκειται για μία μέθοδο με την οποία δημιουργούνται Transmission Control Protocol/Internet Protocol (TCP/IP) πακέτα με την χρήση της IP κάποιου άλλου. Οι routers χρησιμοποιούν την destination address για την προώθηση των πακέτων στο διαδίκτυο και αγνοούν την source address. Έτσι ο hacker χρησιμοποιεί μία σειρά από τεχνικές για να εντοπίσει την IP address ενός external H/Y ο οποίος έχει πρόσβαση στο "δίκτυο-στόχος" ή προσπαθεί να υποκλέψει IP address από τις IP που χρησιμοποιούν οι H/Y σε αυτό το δίκτυο. Οι παράνομοι IP address εν συνεχεία χρησιμοποιούνται για τη διαμόρφωση των πακέτων που ο hacker πλέον στέλνει μέσω διαδικτύου. Έτσι η ταυτότητα του επιτιθέμενου αποκρύπτεται πολύ εύκολα. Η παραπάνω μέθοδος χρησιμοποιείται πολύ συχνά στις επιθέσεις τύπου DDOS (Distributed Denial of Service Attacks) και κυρίως εναντίον καλά προστατευμένων δικτύων.
2. **Keylogger.** Υπάρχουν διάφορα προγράμματα software και διάφορα μηχανήματα τα χρησιμοποιούνται για τον έλεγχο και την επεξεργασία καθενός από τα κλειδιά τα οποία ο χρήστης πληκτρολογεί στο keyboard ενός H/Y. Επομένως εκείνος που

φόρτωσε το software ή το μηχάνημα που προαναφέραμε έχει στην συνέχεια πρόσβαση σε όλα τα κλειδιά που δημιουργούνται από αυτό τον χρήστη. Με τον τρόπο αυτό μπορούν εύκολα να υποκλαπούν password και άλλες κρίσιμες πληροφορίες που computer operator θέλει να κρατάει μυστικές και μέσω αυτών να διεισδύσει ο επιτιθέμενος στο δίκτυο ή στον Η/Υ μιας εταιρίας -οργανισμού ή ενός ιδιώτη.

3. **Φυσική επίθεση.** Όπως αναφερθήκαμε και προηγουμένως μία κατηγορία επιθέσεων εναντίον Η/Υ και δικτύων είναι και η φυσική επίθεση με την χρήση διαφόρων μέσων βίας. Αυτή περιλαμβάνει τόσο την καταστροφή των δικτύων όσο και τον εξοπλισμό των τερματικών.

4. **Sniffer.** Πρόκειται για προγράμματα που ελέγχουν την μεταφορά δεδομένων που γίνεται εντός ενός δικτύου Η/Υ. Αυτά χρησιμοποιούνται κυρίως στη διαχείριση δικτύων και τον έλεγχο των μεταβλητών που έχουν τεθεί για την εύρυθμη λειτουργία τους. Όμως κατά τη διάρκεια των cyber attacks ο ρόλος τους είναι η κλοπή πληροφοριών, βάσεων δεδομένων και password από ένα δίκτυο. Ο εντοπισμός και η καταστροφή τους είναι πάρα πολύ δύσκολή, ενώ διασπείρονται σε όλους τους Η/Υ του στόχου με πολύ μεγάλη ταχύτητα.

5. **Cookies.** Τα cookies είναι ένα είδος αρχείων τα οποία δημιουργούνται και αποθηκεύονται στον σκληρό δίσκο του υπολογιστή από τα Web sites που επισκέπτονται οι χρήστες στο internet με απώτερο σκοπό την αναγνώριση τους από τα ίδια τα Web sites την επόμενη φορά που θα τα επισκεφθούν. Υποτίθεται ότι εξυπηρετούν χρήσιμους σκοπούς για τους χρήστες του διαδικτύου, καθώς συγκεντρώνουν πληροφορίες σχετικά με τις καταναλωτικές τους συνήθειες, τις οποίες μπορούν να αξιοποιήσουν sites μεγάλων εταιρειών για να εξειδικεύσουν έτσι ή και να βελτιώσουν τα προϊόντα ή τις υπηρεσίες τους. Παρόλα αυτά, η σημαντικότερη χρήση των cookies είναι η παρακολούθηση και η καταγραφή των κινήσεων των χρηστών στο internet, συνήθως τις καταναλωτικές, τις προτιμήσεις στα site που επισκέπτονται, το χρόνο που μένουν σε αυτά, τις φορές που τα επισκέπτονται κ.τ.λ. Τα cookies αποτελούν ένα από τα πιο αμφιλεγόμενα θέματα του διαδικτύου καθώς έχουν να κάνουν με τα προσωπικά δεδομένα και το προσωπικό απόρρητο των χρηστών του. Για

το λόγο αυτό και αναφέρονται στην κατηγορία των "εργαλείων" με συγκρατημένη επιφύλαξη.

6. **Trojan Horse.** Ονομάζεται διαφορετικά και Remote Administration Tool ή RAT και πρόκειται για μέρος software το οποίο αρχικά δημιουργήθηκε για τον έλεγχο της ορθής λειτουργίας του Η/Υ. Κυρίως όμως χρησιμοποιείται για κακό σκοπό, όπως την κλοπή ευαίσθητων πληροφοριών, password, μη εξουσιοδοτημένη επισκόπηση ενός συστήματος, διαγραφή αρχείων και ακόμα και καταγραφή ατόμων μέσω webcams χωρίς άδεια. Οι Trojan Horse αποτελούνται από τρία μέρη: client, build/edit server, server. Ο client είναι το μέρος του Trojan που έρχεται όταν γίνεται download από το internet. Χρησιμοποιείται για τη σύνδεση των προσβλημένων Η/Υ και την ανταλλαγή πληροφοριών. Ο build/edit server είναι ένα πρόγραμμα που χρησιμοποιείται για τον καθορισμό των παραμέτρων ενός Trojan server, όπως η notification information (δηλαδή πως ο server στέλνει IP address στον hacker), start up μεθόδους (πως ο Trojan θα τρέξει κατά την εκκίνηση ενός συστήματος), stealth options (παράκαμψη του firewall) κ.ά. .*(54)* Τελευταίο μέρος είναι ο server, ο οποίος αποτελεί τον πραγματικό ιό που ο επιτιθέμενος προσπαθεί να εμφυτεύσει στον "στόχο". Ένας τέτοιος malicious code δημιουργεί συνεχώς αντίγραφα του εαυτού του στα Windows του Η/Υ που θα τοποθετηθεί και στη συνέχεια τροποποιεί την registry του συστήματος. Παρακάτω παρατίθενται ορισμένα γνωστά Trojans όπως το NET-DEVIL 1.5 και το Optix Pro. Για την αντιμετώπιση τους το Naval Post Graduated School αναπτύσσει ένα νέο εργαλείο ασφάλειας δικτύου το οποίο ονομάζεται "Terminator" και είναι σχεδιασμένο να εντοπίζει πιθανές ηλεκτρονικές επιθέσεις με προσεκτική ανάλυση και παρακολούθηση της κυκλοφορίας δικτύου (network traffic). *(55)*

EIKONA 13: Το Trojan Horse Net-Devil 1.5

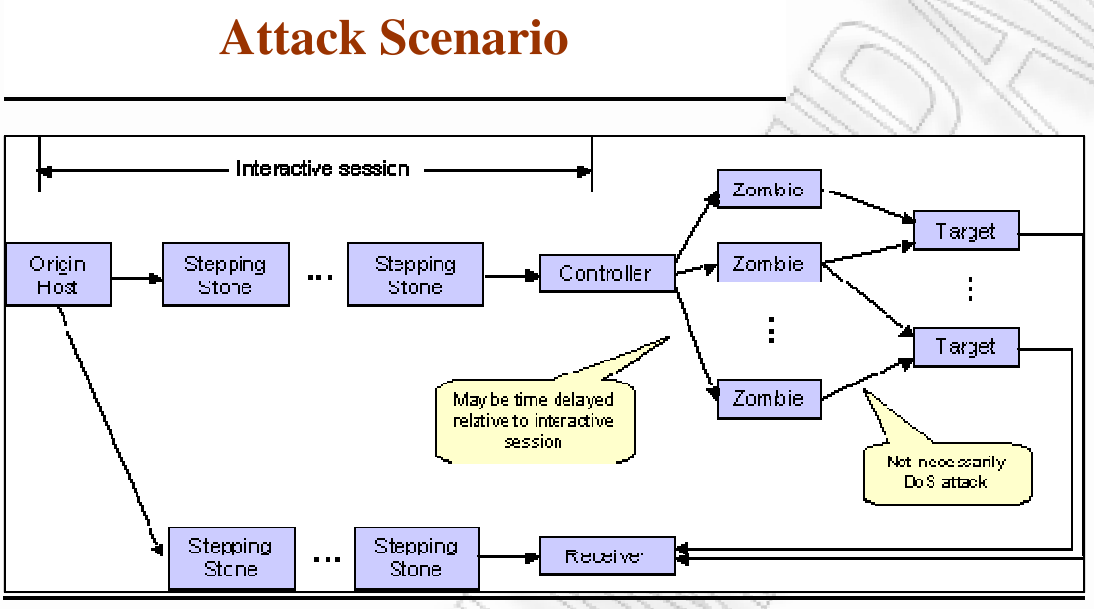
EIKONA 14: Το Trojan Horse Optix Pro v1.33 Client

7. **Worms.** Τα σκουλήκια (worms), είναι προγράμματα Η/Υ που χρησιμοποιούνται σαν ένα μηχανισμός μεταφοράς άλλων προγραμμάτων. Ανήκουν και αυτά στην κατηγορία των malicious code όπως και τα Trojan horse και δίνουν τη δυνατότητα παράνομης εισόδου σε δίκτυα Η/Υ επιτρέποντας τη διαγραφή και τη παραμόρφωση δεδομένων. Αυτό-αντιγράφουν τον εαυτό τους ταχύτατα και διασπείρονται χωρίς να είναι απαραίτητη η ανθρώπινη παρουσία κυρίως σε non-patched Η/Υ και παρά το γεγονός ότι ο στόχος δεν έχει κάνει την οποιαδήποτε κίνηση. Επιπλέον σχετίζονται κατά κύριο λόγο με της τύπου "Bbuffer overflow" επιθέσεις που επιτρέπουν την υποκλοπή γνήσιων προγραμμάτων για χρήση τους σε παράνομες ενέργειες. Το Bbuffer overflow είναι η διαδικασία κατά την οποία υπερβολικός αριθμός data τοποθετείται σε ένα buffer, δηλαδή σε ένα computer data holding area, πολύ μεγαλύτερος από αυτόν που μπορεί να αντέξει. Αυτό είναι αποτέλεσμα της μη ορθής σύνδεσης μεταξύ της παραγωγικής και καταναλωτικής – διεκπεραιωτικής διαδικασίας και μπορεί να οδηγήσει σε κατάρρευση του συστήματος ή στη δημιουργία backdoor, καταλήγοντας σε μη εξουσιοδοτημένη είσοδο σε ένα δίκτυο ή Η/Υ. Τα τελευταία πέντε χρόνια τέτοιες επιθέσεις ήταν κάτι ευρύτερα διαδεδομένο στην κοινότητα των hackers στο διαδίκτυο. Το 2001 μια εταιρεία ασφαλείας δικτύων και Η/Υ διαπίστωσε αδυναμία σε ένα γνωστό web-server και η οποία μπορούσε να οδηγήσει σε φαινόμενο Bbuffer overflow. Πριν προλάβει να διορθώσει την παραπάνω δυσλειτουργία έκανε την εμφάνιση του το Code Red worm, μετά από μερικές εβδομάδες το Code Red worm II και το Nimda worm, τα οποία διαδίδονται αυτομάτως μέσω διαδικτύου από τον παραπάνω server. Το 2007, ο Witty worm κατάφερε να διεισδύσει και να καταστρέψει παγκοσμίως περί τις 12000 "εκτεθειμένες" Η/Υ μηχανές εντός μόλις 45 λεπτών από την είσοδο του στο διαδίκτυο και σε συνολικό χρόνο περί τις 36 ώρες. Ένας άλλος worm, ονομαζόμενος "Blaster" επιτέθηκε σε 500.000 Η/Υ παγκοσμίως σε μία εβδομάδα. Μεταξύ των δικτύων που προσέλαβε ήταν και αυτό του Σιδηροδρόμου του Jacksonville Florida προκαλώντας πραγματικό χάος στη λειτουργία της υπηρεσίας. *(56)* Η επίθεση από τον "Blaster" είχε ως συνέχεια την επόμενη εβδομάδα την επίθεση από τον worm "Welchia" παγκοσμίως, ο οποίος χρησιμοποιούσε την ίδια μέθοδο για να εισέρχεται παράνομα στους Η/Υ. Στον τελευταίο αποδίδεται και η πρώτη επίσημα καταγεγραμμένη επίθεση σε στρατιωτικό δίκτυο η οποία "χτύπησε" το υψηλής

ασφάλειας Navy Marine Corps Intranet (NMCI) του Αμερικανικού Ναυτικού φορτώνοντας το με ανεπιθύμητο traffic. *(57)* Τα νέα είδη worm περιλαμβάνουν μία "εν υπνώσει" περίοδο κατά την οποία σιωπηλώς διεισδύουν σε όσο τον δυνατόν μεγαλύτερο αριθμό host, πριν ενεργοποιήσουν την καταστροφική τους δράση ρυθμιζόμενα ώστε η δράση αυτή να είναι ταυτόχρονη. Παράλληλα υπάρχουν οι πιο εξελιγμένοι τύποι worm (Warhol worm, flash worm) οι οποίοι διαδίδονται σε μερικά λεπτά ή ακόμα και δευτερόλεπτα αφήνοντας ελάχιστο ή καθόλου περιθώριο στα system administrators να αντιδράσουν. Η τάση των hacker όσον αφορά αυτή την κατηγορία malicious code, είναι η δημιουργία και χρήση υβριδικών (hybrid) worm οι οποίοι αφενός θα διατηρούν τα παραδοσιακά χαρακτηριστικά του κώδικα και αφετέρου θα προσφέρουν καινούριες δυνατότητες. Σκοπός τους είναι να περιλαμβάνουν ακόμα υπό-worm τα οποία θα επιτίθενται στους πιο εύκολους στόχους ελκύοντας την προσοχή των μηχανισμών προστασίας, επιτρέποντας στους πιο sophisticated να κάνουν ανενόχλητοι τη ζημιά τους σε κρίσιμες υποδομές. Παράλληλα, στο στάδιο της ανάπτυξης είναι οι web-based worms. Ένα διάσημο παράδειγμα αποτελεί ο Santy A, ο οποίος με τη βοήθεια της μηχανής αναζήτησης Google εντοπίζει και προσβάλλει εκτεθειμένους στόχους οι οποίοι χρησιμοποιούν την web εφαρμογή phpBB. Από τη στιγμή που θα εντοπισθεί ο τρωτός Η/Υ επωφελείται από τη "ρωγμή" αυτή και διασπείρει τον εαυτό του μέσω αυτού στο διαδίκτυο. *(58)* Ένα άλλο παράδειγμα τέτοιου τύπου worm είναι οι XSS worm. Οι τελευταίοι χρησιμοποιούν την παρακάτω μέθοδο διάδοσης. Τοποθετούνται σε ένα συγκεκριμένο web-site και περιμένουν το υποψήφιο θύμα να το επισκεφθεί, όπου και εφαρμόζουν τον κώδικα που φέρουν στην πλευρά του client. Όταν κάτι τέτοιο πραγματοποιείται δίνει τη δυνατότητα στο worm να μεταφέρεται και σε άλλα websites μέσω διαδικτύου. Περιμένει πλέον και άλλους client να επισκεφθούν τα web-sites που έχουν προσβληθεί. Με τον τρόπο αυτό μπορεί να προσβληθεί ως και ένα εκατομμύριο profiles στη web community του My Space για παράδειγμα, προκαλώντας πραγματικό χάος σε ένα δίκτυο Η/Υ. *(59),(60)* .

8. **Zombie.** Αν ένας server ή Η/Υ έχει δεχτεί επίθεση και ο επιτιθέμενος έχει καταφέρει να τον διαβάλλει με κάποιου είδους malicious code, τότε μπορεί να χρησιμοποιηθεί για να πραγματοποιηθεί επίθεση από τον hacker σε άλλο στόχο. Όπως φαίνεται και

στο παρακάτω σχεδιάγραμμα ο hacker χρησιμοποιεί διάφορους Zombie για να πετύχει επίθεση προς τον target.



ΕΙΚΟΝΑ 15: Σενάριο ηλεκτρονικής επίθεσης με ΄΄Zombie΄΄

9. **Spy ware.** Ανήκει και αυτό στην κατηγορία του malicious code με περισσότερες όμως ικανότητες στην επιτήρηση, παρακολούθηση και κατασκόπευση δικτύων και PCs. Επιπλέον έχει τη δυνατότητα αυτόματης καταγραφής και μετάδοσης keystrokes, passwords και άλλων ευαίσθητων πληροφοριών ενός δικτύου στον επιτιθέμενο. Ένα τέτοιο software ανακαλύφθηκε από το FBI το 2003 και είχε ως στόχο την οικονομική απάτη εναντίον πολυεθνικών εταιρειών όπως J.P.Morgan, American Express Co, Wachovia Corp, Bank of America Corp και τη Citibank N.A. Το όνομα του Spy ware είναι Bugbear και διαθέτει ικανότητες mass-mailing και keystroke – logging ενώ μπορεί να καταστρέφει μια μεγάλη γκάμα antivirus και firewall συστήματα. Παράλληλα το software που διαθέτει είναι προγραμματισμένο να εντοπίζει πότε το "θύμα" χρησιμοποίησε e-mail address η οποία ανήκει σε ένα από τους 1300 χρήστες που είναι καταχωρημένοι στις λίστες του. Όταν ο επιτιθέμενος επιτύχει σύνδεση προσπαθεί να υποκλέψει password και άλλες πληροφορίες που θα επιτρέψουν στο

hacker να επιτύχει πρόσβαση στο τραπεζικό δίκτυο. Στη συνέχεια μεταδίδει τα κλεμμένα password σε 10 e-mail address, όπου επίσης περιλαμβάνονται στις λίστες του μέσω διαδικτύου. Φυσικά αυτό δε σημαίνει ότι με την αντίστροφη διαδικασία μπορεί να εντοπιστεί αυτός που πραγματοποιεί την επίθεση αφού ο οποιοσδήποτε μπορεί να δημιουργήσει ένα λογαριασμό e-mail με χρήση ψεύτικων και παραπλανητικών στοιχείων. Επομένως ο εντοπισμός του φυσικού προσώπου που εκτελεί την επίθεση είναι σχεδόν αδύνατος. *(61)*

10. **E-mail bombs.** Αυτή η κατηγορία hacking tool (εργαλείου hacking) είναι μια από τις πιο σύγχρονες και σημαντικές. Η βασική σχεδιαστική απαίτηση ενός συστήματος αποστολής μηνυμάτων είναι κανένα mail να μη χάνεται. Το ίδιο ισχύει και για το e-mail (ηλεκτρονικό ταχυδρομείο), του οποίου ο αλγόριθμος είναι τόσο ισχυρός που σε περίπτωση που η παράδοση ενός μηνύματος δε μπορεί να επιβεβαιωθεί, η διαδικασία επαναλαμβάνεται από την αρχή. Το πρωτόκολλο που χρησιμοποιείται είναι το SMTP. Οι servers και τα προγράμματα που χρησιμοποιούνται για την αποθήκευση και την προώθηση των e-mail στο διαδίκτυο ονομάζονται MTA (Mail Transfer Agent). Παρά το γεγονός αυτό η πολυπλοκότητα του δίνει μικρά περιθώρια άμυνας σε επιθέσεις με e-mail bombs, ιδιαίτερα στην περίπτωση της μετάδοσης e-mail σε εκτεταμένη περιοχή μεταξύ TCP/IP hosts και servers. Στόχος των e-mail bombs να πλημμυρίσουν το δίκτυο ή/και τον Η/Υ με άχρηστα δεδομένα καθώς και να τοποθετήσουν κρυφά κάποιο ιό ή Trojan horse ώστε ο server να καταστεί μη διαθέσιμος. Συνήθως η είσοδός του στο δίκτυο γίνεται μέσω internet, κάνοντας downloading σε επίσημα προγράμματα στα οποία έχουν προσκολληθεί. Υπάρχουν δύο βασικές κατηγορίες e-mail bombs, το chain bombs και το error message bombs, τα οποία χρησιμοποιούν διαφορετικές τεχνικές για να διασπείρονται επιτυγχάνοντας όμως τα ίδια σχεδόν αποτελέσματα.

11. **E-mail spoofing.** Συχνά ένα email εμφανίζεται να προέρχεται από συγκεκριμένη πηγή αλλά αντίθετα έρχεται από κάποια τελείως διαφορετική. Αυτό σε γενικές γραμμές μπορεί να περιγράψει το E-mail spoofing. Χρησιμοποιείται πολύ συχνά από τους hackers για την απόκρυψη της ταυτότητας τους και για να κατηγορήσουν κάποιον άλλο για τις παράνομες πράξεις τους, όπως π.χ. η κλοπή password και άλλων προσωπικών δεδομένων. Τελευταία είδε το φως της δημοσιότητας περίπτωση 12χρονου Βρετανού ο οποίος κατάφερε να στέλνει e-mail από τον προσωπικό Η/Υ του

Βρετανού Πρωθυπουργού. *(62)* Η μεθοδολογία που χρησιμοποιείται στην αποστολή spoof email είναι αρκετά απλή. Τα περισσότερα email software displays έχουν ως πεδία το "from subject" και το "date received", ενώ πιο εξειδικευμένες πληροφορίες όπως την πορεία του mail κ.ά. είναι κρυμμένες –δεν εμφανίζονται στην οθόνη - για να μην μπερδεύουν το χρήστη και να δημιουργούν σύγχυση. Επομένως πολύ απλά αλλάζοντας το πεδίο "from" αλλάζουμε τον αποστολέα θέτοντας διαφορετικό από τον πραγματικό.

12. **Ιοί (virus).** Οι ηλεκτρονικοί ιοί ανήκουν στην κατηγορία των malicious code αλλά λειτουργούν διαφορετικά από τα άλλα είδη, όπως π.χ. το Trojan Horse. Πρόκειται για software το οποίο έχει σχεδιασθεί για να διεισδύει, καταστρέφει, μεταμορφώνει και να δημιουργεί και άλλου είδους προβλήματα σε προγράμματα, Η/Υ και δίκτυα. Επιπλέον στην περίπτωση που ο Η/Υ που έχει προσβληθεί είναι συνδεδεμένος στο διαδίκτυο, γίνεται διασπορά του ιού και μεταφορά του σε όλους όσους βρίσκονται στη λίστα των ηλεκτρονικών διευθύνσεων του χρήστη. Ένα χαρακτηριστικό παράδειγμα email virus θεωρείται ο Melissa virus, ο πιο ταχέα διαδιδόμενος ιός που φτιάχτηκε μέχρι τώρα. Ο τελευταίος προσβάλλει έναν Η/Υ όταν αυτός μπει στο διαδίκτυο, αυτομάτως στέλνει τον εαυτό του στις 50 πρώτες διευθύνσεις email που έχει χρησιμοποιήσει ο χρήστης. Οι δυνατότητες του συγκεκριμένου malicious code είναι τόσο μεγάλες που θεωρείται ότι έχει προκαλέσει ζημιά 80 εκατομμυρίων δολαρίων σε υποδομές και συστήματα των Η.Π.Α. τα τελευταία δύο χρόνια. *(63)* Παράλληλα και άλλοι ιοί έχουν προκαλέσει οικονομικού επιπέδου, ζημιά συγκρίσιμη με αυτή του τυφώνα Andrew. Ο τυφώνας αυτός προκάλεσε καταστροφές ύψους 25 δισεκατομμυρίων δολαρίων στις Η.Π.Α., ενώ ο ιός Love Bug (δημιούργημα ενός φοιτητή πανεπιστημίου στις Φιλιππίνες), *(64)* εκτιμάται ότι έχει προκαλέσει παγκοσμίως στους χρήστες των Η/Υ απώλειες της τάξης των 15 δισεκατομμυρίων δολαρίων.

Οι βασικοί τύποι ιών είναι οι παρακάτω:

- **Boot sector virus:** Κάθε φορά που ανοίγουμε τον Η/Υ πραγματοποιείται η διαδικασία boot (bootάρισμα). Ο σκληρός δίσκος περιλαμβάνει στο πρώτο του επίπεδο ένα πρόγραμμα που ονομάζεται Master Boot Sector (M.B.R.), το οποίο ψάχνει για την

τοποθεσία του operating system - OS (λειτουργικού συστήματος) στο σκληρό δίσκο έτσι ώστε να μπορεί να φορτωθεί στη μνήμη RAM του Η/Υ. Το πρόγραμμα MBR πραγματοποιεί αυτή τη διαδικασία με τη βοήθεια ενός πίνακα partition, ο οποίος περιλαμβάνει τις διευθύνσεις όλων των μερών (partitions) του σκληρού δίσκου. Οι ιοί τύπου Boot sector virus δεν επιτρέπουν στον Η/Υ να πραγματοποιήσει τη διαδικασία εκκίνησης. Ο ιός επιτίθεται είτε στον boot sector είτε στο πρόγραμμα MBR του Η/Υ αντικαθιστώντας τον παραπάνω κώδικα με τον κώδικα του ιού. Υπάρχουν δύο κύριες μέθοδοι τις οποίες χρησιμοποιούν αυτού του είδους οι ιοί για να αντικαταστήσουν τον MBR κώδικα. Στην πρώτη μέθοδο ο ιός αντιγράφει το MBR σε διαφορετικό file ή γράφει πάνω στο MBR το πρόγραμμα του ιού. Στην πρώτη περίπτωση ο ιός εξαπλώνεται σε όλα τα partitions που διαβάζει ο MBR προκειμένου να βρει το OS. Τελικά, ο ιός επηρεάζει και τη λειτουργία της μνήμης RAM. Στη δεύτερη μέθοδο γίνεται χρήση ενός Repair disk, δηλαδή ενός floppy disk που χρησιμοποιείται για να διορθώσει και να κάνει επανεκκίνηση των Windows, όταν το OS έχει υποστεί κάποιου είδους ζημιά. Αυτό το floppy disk περιλαμβάνει ένα αντίγραφο από όλα τα start-up files που απαιτούνται για τη διαδικασία boot του Η/Υ. Έτσι όταν τρέχει ο Repair disk περνάει στον Η/Υ το M.B.R. που έχει προσβληθεί από τον ιό και τελικά στη μνήμη RAM όπως και με την πρώτη μέθοδο. *(65)*

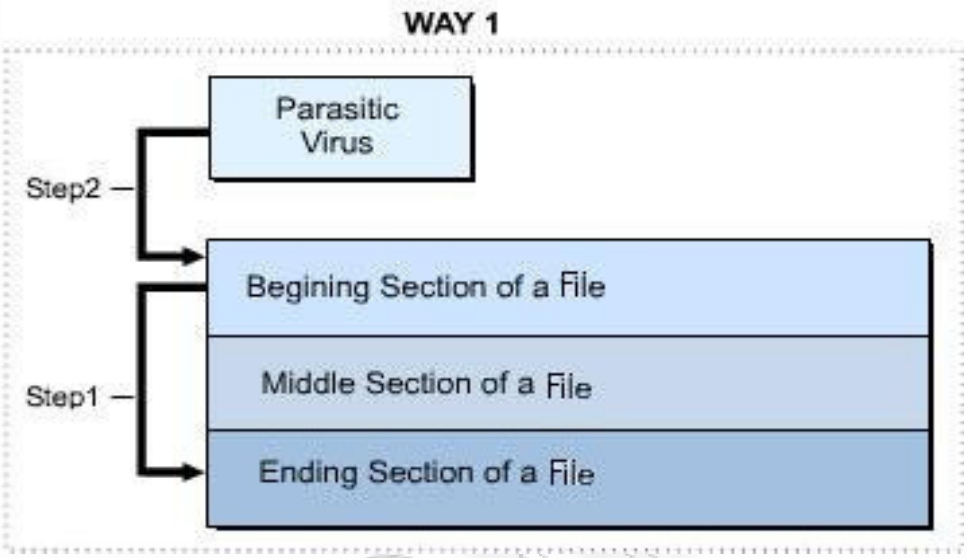
- **File virus:** Στην κατηγορία αυτή, ανήκουν εκείνοι οι ιοί που συνοδεύουν εκτελέσιμα files σε διάφορες μορφές και διαφθείρουν το file όταν αυτό ανοίγεται. Συνήθως επιτίθενται σε αρχεία που τελειώνουν σε .com, .exe, .dll, .ovr, .ovl και αντικαθιστούν τον κώδικα του αρχείου με τον κώδικα του ιού. Αυτοί οι File virus δεν είναι πολύ επιτυχημένοι, διότι συχνά εμφανίζουν προβλήματα στη λειτουργία τους με αποτέλεσμα τη σχεδόν άμεση ανακάλυψη του ιού. *(66)* Οι πιο εξελιγμένοι ιοί αυτής της κατηγορίας δεν αντικαθιστούν, αλλά διατηρούν το κανονικό πρόγραμμα του αρχείου. Αυτό έχει ως αποτέλεσμα μετά το τρέξιμο του ιού να λειτουργεί το πρόγραμμα χωρίς προβλήματα και όλα να φαίνονται κανονικά. Οι File virus κατηγοριοποιούνται με βάση τον τρόπο με τον οποίο επιδρούν στο file, στο οποίο επιτίθενται και αριθμούν μερικές χιλιάδες αν και δε θεωρούνται η πιο μεγάλη κατηγορία ιών. Παράλληλα δημιουργούν προβλήματα κυρίως σε

LAN δίκτυα, τα οποία τρέχουν διάφορες εφαρμογές μοιρασμένες στους χρήστες του δικτύου. Μπορούν να μεταφερθούν μέσω ενός δικτύου ως ένα email-attachment. Συνήθως η αντιμετώπιση τους γίνεται με gate-way antivirus τα οποία αναχαιτίζουν τη διάδοση των ιών αυτών στην "περίμετρο" του δικτύου. Έτσι έχουμε τις παρακάτω περιπτώσεις:

1.overwriting virus. Στην κατηγορία αυτή ο ιός overwrites το αρχείο στο οποίο έχει επιτεθεί. Τα περιεχόμενα του αρχείου αντικαθίστανται από τον κώδικα του ιού και όταν το αρχείο αυτό χρησιμοποιείτε ο ιός εξαπλώνεται και στα άλλα προγράμματα που πιθανόν λειτουργούν στον Η/Υ εκείνη τη χρονική στιγμή. Εξάλλου ένα εκτελέσιμο αρχείο αποτελείται από δύο μέρη, το EXE-Header και το EXE-body. Το πρώτο είναι τοποθετημένο στην αρχή του αρχείου και περιλαμβάνει διάφορες πληροφορίες όπως την κατάσταση των registers, ενώ το EXE-body περιλαμβάνει τον κώδικα του αρχείου. Αν ο ιός επιτεθεί στο EXE-Header το αρχείο λειτουργεί χωρίς προβλήματα αλλά το header καταστρέφεται. Αντίθετα αν ιός επιτεθεί στο EXE-body ο κώδικας του αρχείου παραμορφώνεται και η λειτουργία του είναι προβληματική.

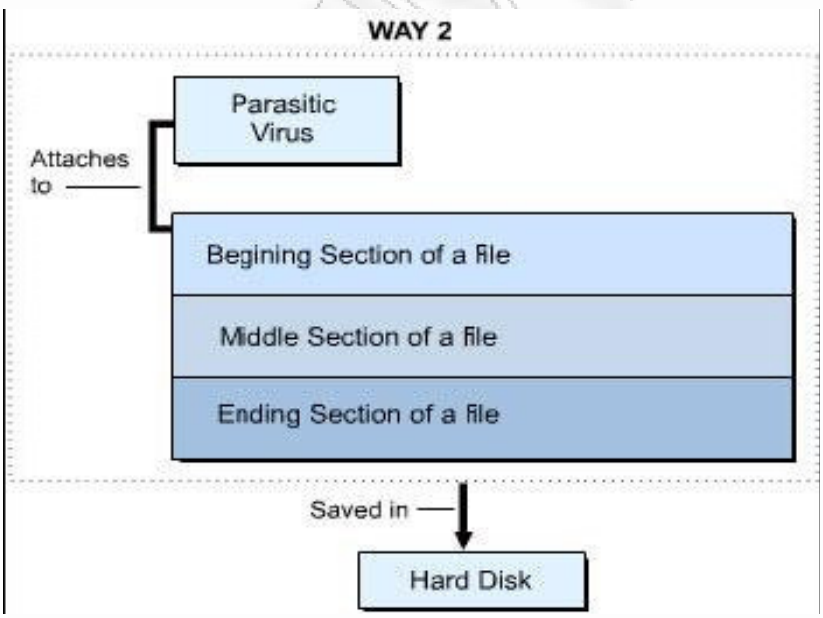
2.parasitic virus: Η κατηγορία αυτή, file virus αντικαθιστά τμήματα του αρχείου από τον κώδικα του ιού με διάφορους τρόπους. Οι ιοί αυτής της ομάδας έχουν ως στόχο αρχεία τύπου .com και .exe και χρησιμοποιούν τις παρακάτω μεθόδους.

- ***Ά μέθοδος:*** ο ιός τοποθετείται στην αρχή του συγκεκριμένου file. Σε αυτή την περίπτωση ο parasitic virus μεταφέρει τα περιεχόμενα του αρχείου από την αρχή στο τέλος. Στο παρακάτω διάγραμμα φαίνεται καθαρά ο τρόπος με τον οποίο λειτουργεί.



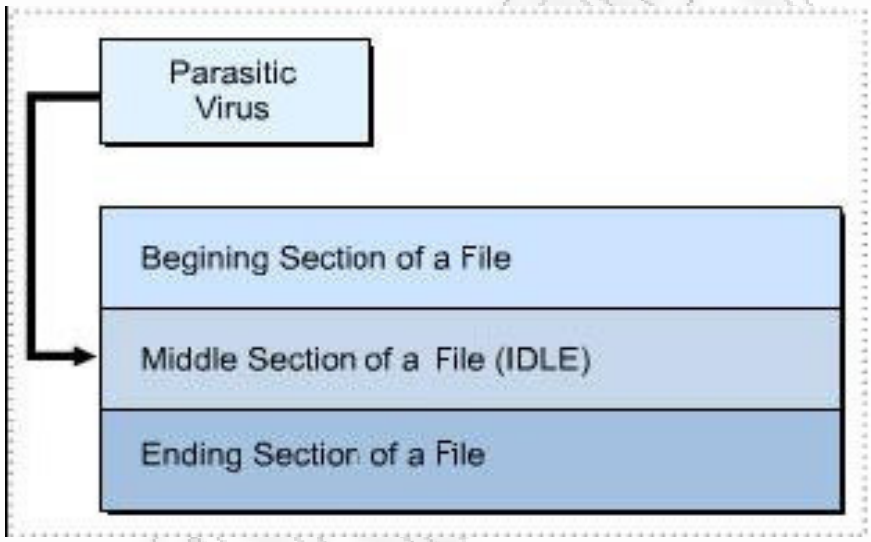
ΕΙΚΟΝΑ 16: Ά μέθοδος λειτουργίας του parasitic virus

- ***Έβ μέθοδος:*** Ο παρασιτικός ιός δημιουργεί αντίγραφο του εαυτού του στην κύρια μνήμη του Η/Υ και στην συνέχεια προσκολείται στο file όπως φαίνεται στο παρακάτω διάγραμμα:



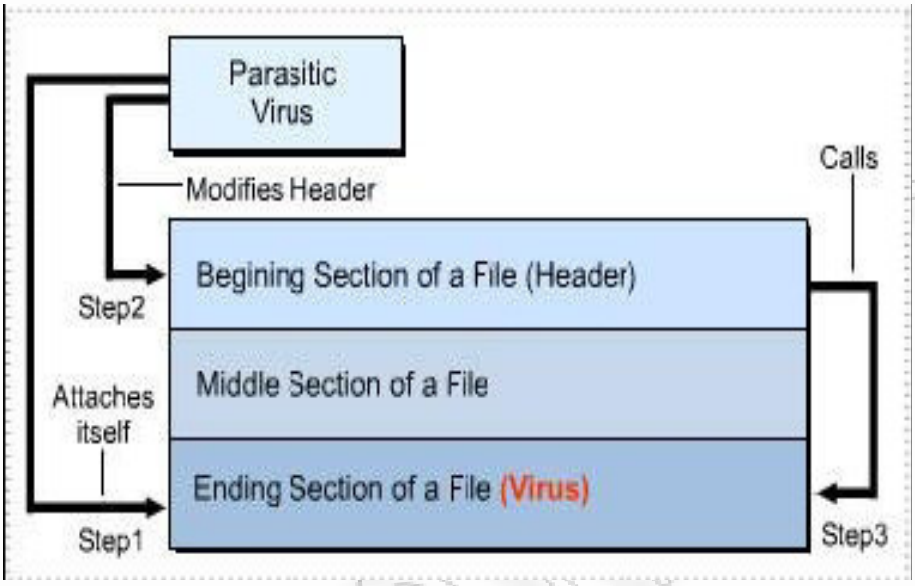
ΕΙΚΟΝΑ 17: Έβ μέθοδος λειτουργίας του parasitic virus

- ***Γ μέθοδος :*** Ο ιός τοποθετείται στο μέσον του file. Σε αυτή την περίπτωση ο παρασιτικός ιός προσβάλει το συγκεκριμένο αρχείο τοποθετούμενος στον αποδεσμευμένο χώρο, στο μέσον του file, όπως φαίνεται και παρακάτω:



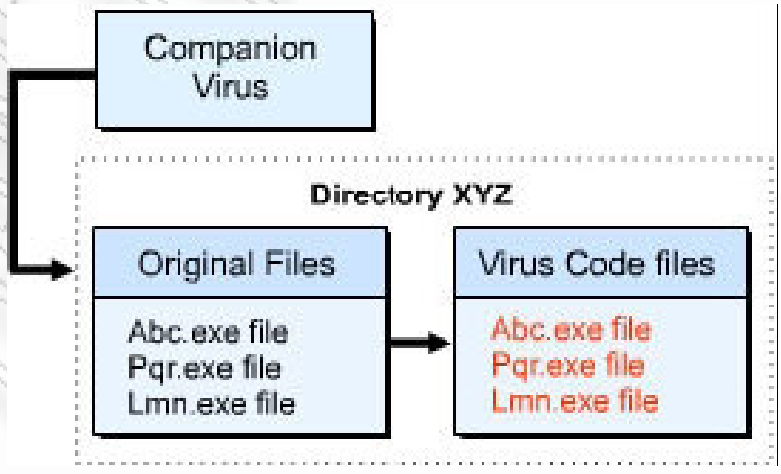
ΕΙΚΟΝΑ 18: Γ μέθοδος λειτουργίας του parasitic virus

- ***Δ μέθοδος:*** Η τέταρτη μέθοδος που χρησιμοποιείται από τους παρασιτικούς ιούς είναι με τη βοήθεια του relocation table. Ο ιός ανακαλύπτει τα κενά μέρη του αρχείου και πηγαίνει και τα καλύπτει με τον κώδικα του.
- ***Ε μέθοδος :*** Η πέμπτη και τελευταία μέθοδος που χρησιμοποιείται είναι με την επίθεση του ιού στο τέλος του αρχείου. Ο παρασιτικός ιός αλλάζει μερικά bytes από τον header του file προκειμένου να αναγκαστεί το τελευταίο να χρησιμοποιήσει κώδικα του ιού σε αντιδιαστολή με τα άλλα μέρη του αρχείου.



ΕΙΚΟΝΑ 19: Ε μέθοδος λειτουργίας του parasitic virus

3.companion virus: Αυτής της κατηγορίας οι ιοί λειτουργούν με τέτοιο τρόπο ώστε το αρχείο να μην επηρεάζεται ή να ενοχλείται με οποιονδήποτε τρόπο. Δημιουργούν πιστό αντίγραφο του αυθεντικού αρχείου και το σώζουν μαζί με διαφορετική προέκταση στο ίδιο σημείο όπως και το αυθεντικό αρχείο. Το αντίγραφο αυτό περιέχει πλέον και το κώδικα του ιού. Στην παρακάτω εικόνα φαίνεται ο τρόπος λειτουργίας.

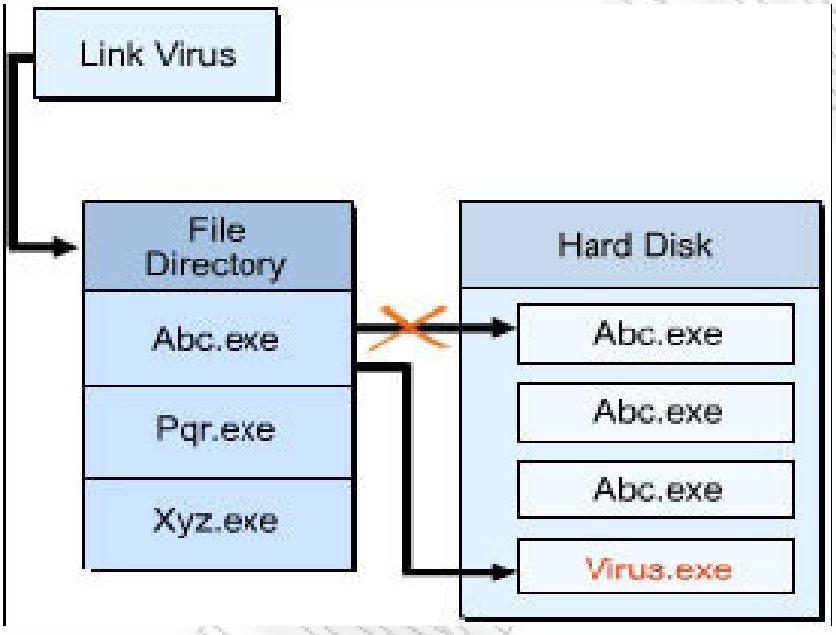


ΕΙΚΟΝΑ 20:Η μέθοδος λειτουργίας του companion virus

Παράλληλα οι companion virus χρησιμοποιούν μέρη του operating system για να προσβάλουν τα διάφορα αρχεία. Για παράδειγμα χρησιμοποιείτε η διαδικασία χρήσης των batch files αντί των .com και .exe files. Στην περίπτωση αυτή κάθε φορά που θα γίνεται προσπάθεια εκτέλεσης ενός .com και .exe file το MS-DOS θα εκτελεί το αντίστοιχο batch file το οποίο όμως περιέχει τον ιό. Διαπιστώνουμε λοιπόν, ότι οι companion virus δεν αλλάζουν ένα ήδη υπάρχον αρχείο αλλά δημιουργούν ένα πρόγραμμα το οποίο εκτελείται στη θέση του προηγούμενου. Με τον τρόπο αυτό όλα εμφανίζονται να λειτουργούν κανονικά. Στους Η/Υ, επίθεση από τέτοιου είδους ιούς πραγματοποιείται με τη δημιουργία ενός .com file (που περιέχει τον ιό) στη θέση ενός ήδη υπάρχοντος .exe file με το ίδιο όνομα. Για να γίνει πιο κατανοητός ο τρόπος λειτουργίας θα αναφέρουμε το εξής σύντομο παράδειγμα. Ας υποθέσουμε ότι στον Η/Υ υπάρχει ένας τέτοιος ιός και αποφασίζει να επιτεθεί σε ένα συγκεκριμένο αρχείο. Εντοπίζει ένα αρχείο με την ονομασία PGM.EXE, δημιουργεί ένα δεύτερο αρχείο που ονομάζεται PGM.COM και το οποίο περιέχει τον ιό. Αυτό το αρχείο συνήθως τοποθετείται από τον ιό στο ίδιο directory όπως και το .exe file. Έτσι αν πληκτρολογήσουμε PGM και πατήσουμε enter, DOS θα εκτελέσει το αρχείο PGM.COM αντί του PGM.EXE. Αυτό γίνεται, γιατί το DOS εκτελεί τα .com files πριν τα .exe files και έτσι ο ιός εισέρχεται πρώτος στη μνήμη. Ο χρήστης όμως του αρχείου δεν θα καταλάβει το παραμικρό θεωρώντας ότι όλα γίνονται κανονικά.

4.link virus (γνωστοί και ως cluster virus): Σκοπός αυτών των ιών είναι να αλλάξουν το directory με αποτέλεσμα όταν προσπαθούμε να τρέξουμε ένα πρόγραμμα πρώτα να τρέχει ο ιός. Δημιουργούν πολύ σοβαρό πρόβλημα όταν ο χρήστης του Η/Υ δεν γνωρίζει την ύπαρξη του. Για όσο χρονικό διάστημα βρίσκεται στη μνήμη ελέγχει την πρόσβαση στο directory. Έτσι αν η εκκίνηση γίνει από ένα καθαρό floppy disk και στη συνέχεια τρέξουμε την εφαρμογή SCANDISK, θα εμφανίσει σοβαρό πρόβλημα με τα cross-linked αρχεία του Η/Υ. Θα εμφανιστεί η επιλογή

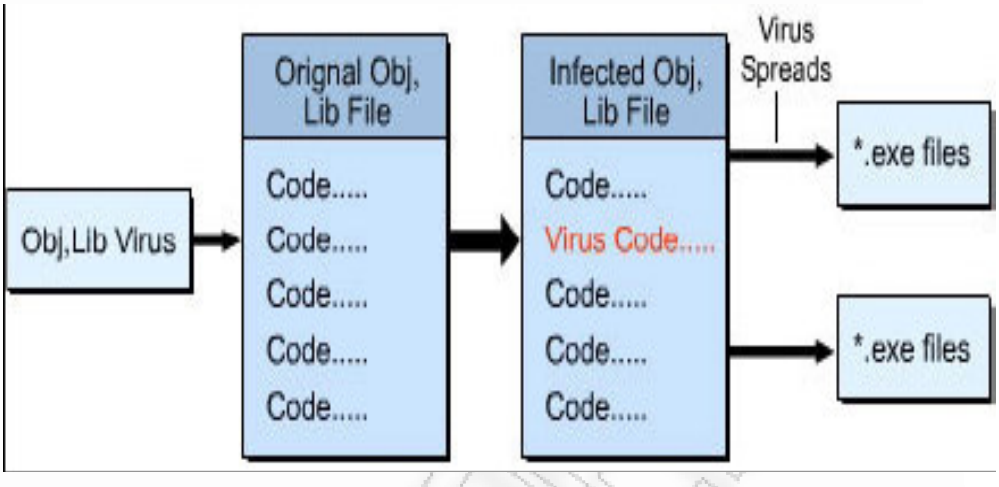
για διόρθωση των προβλημάτων και αν επιλεχθεί τότε όλα τα original αρχεία θα χαθούν.



ΕΙΚΟΝΑ 21:Η μέθοδος λειτουργίας του Link virus

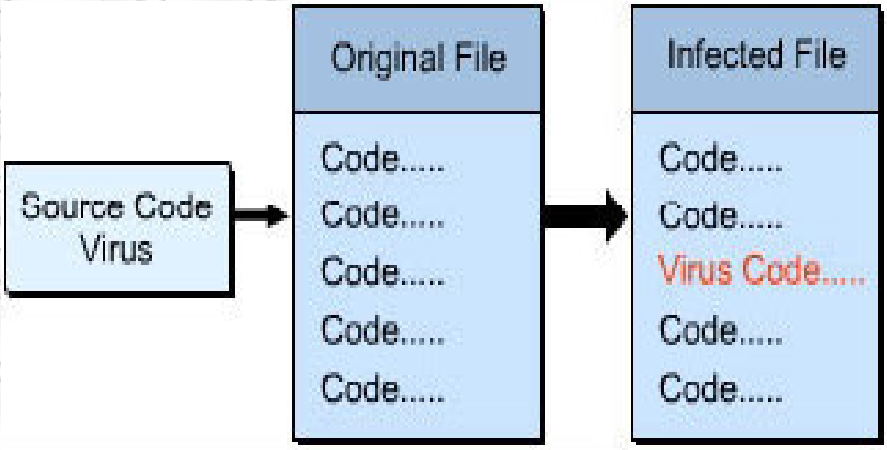
Για την αντιμετώπιση αυτής της κατηγορίας ιών χρησιμοποιούνται antivirus software αλλά και η παρακάτω απλή μέθοδος. Αλλάζουμε όλα τα extension των .exe files σε κάτι διαφορετικό. Στη συνέχεια κάνουμε επανεκκίνηση στον Η/Υ και τρέχουμε την επιλογή CHKDSK. Μετονομάζουμε όλα τα εκτελέσιμα αρχεία στα πραγματικά τους ονόματα και τρέχουμε ξανά την επιλογή CHKDSK. *(65)*

5.OBJ/LIB virus: Οι OBJ/LIB virus τροποποιούν τα object module files και τα complier library files αντίστοιχα με την εισαγωγή κώδικα του ιού στα αυθεντικά files. Όταν αυτό πραγματοποιηθεί ο ιός δεν διασπείρεται άμεσα. Η διασπορά και ενεργοποίηση του γίνεται όταν τα αρχεία .com ή .exe files έχουν επικοινωνία (link) με τα προσβεβλημένα αρχεία, όπως φαίνεται και στο παρακάτω διάγραμμα. *(65)*



ΕΙΚΟΝΑ 22:Η μέθοδος λειτουργίας του OBJ/LIB virus

6.source code virus: Ανήκουν και αυτοί στην κατηγορία των file virus αν και είναι σχετικά σπάνιοι λόγω του διαφορετικού τρόπου και γλώσσας που χρησιμοποιεί ο καθένας για να γράψει κώδικα. Ο ιός Die Hard αποτελεί ένα παράδειγμα αυτής της κατηγορίας και εξαπλώνεται προσβάλλοντας COM και EXE files. Γενικότερα σε αυτή την ομάδα οι ιοί αλλάζουν τον source code ενός file με την εισαγωγή του κώδικα του ιού σε αυτό. Παρατηρούμε από το παρακάτω διάγραμμα, ότι ο ιός θα γίνει αντιληπτός μόνο όταν το file που έχει προσβληθεί εκτελεσθεί.



ΕΙΚΟΝΑ 23:Η μέθοδος λειτουργίας του source code virus

- Macro virus: Η κατηγορία αυτή αντιπροσωπεύει την δεύτερη γενιά απειλής και διαδίδεται με τη χρήση μέσων που συναντάμε σε εφαρμογές office όπως Microsoft Word και Excel. Οι macro virus είναι τις περισσότερες φορές μέρος ενός αρχείου και μπορεί να μεταφερθεί ως attachment μέσω ενός e-mail. Ειδικά για τα αρχεία τύπου Microsoft Word υπάρχουν τρεις ιοί αυτής της κατηγορίας που μπορούν να τα αλλοιώσουν:

  1.Aauto-Execute Macro. Αποτελεί ένα αυτοεκτελέσιμο macro το οποίο βρίσκεται στο start-up directory του Word και εκτελείται σε οποιαδήποτε περίπτωση γίνεται έναρξη του αρχείου.

  2. Auto Macro. Πρόκειται για macro virus που λειτουργούν στις παρακάτω περιπτώσεις: άνοιγμα, κλείσιμο ενός αρχείου Word και δημιουργία ενός νέου αρχείου.

  3. Macros with command names. Αποτελούν τον πιο επικίνδυνο τύπο για αρχεία Microsoft Word μια έχουν το ίδιο όνομα με τις υπάρχουσες εντολές του Word. Παραδείγματος χάριν υπάρχει ιός αυτής της κατηγορίας με το όνομα File Close και οποίος αντικαθιστά την αυθεντική εντολή του Word. Έτσι όταν γίνει επιλογή από τον χρήστη της εντολής File -> Close θα εκτελεσθεί ο ιός και όχι η γνωστή εντολή του Word.

  Η οποιαδήποτε εφαρμογή που υποστηρίζει αυτομάτως εκτελέσιμα macros είναι και δυνητικός "κομιστής" macro virus και με δεδομένη τη συνεχή εξάπλωση του διαδικτύου αποτελούν ένα πολύ σημαντικό "εχθρό". Στην περίπτωση που ένα file περιέχει ιό της κατηγορίας αυτής και χρησιμοποιείται, ο ιός αναπαράγεται και σε άλλες εφαρμογές από όπου θα μολυνθούν και άλλα Word και Excel αρχεία. Αυτοί οι ιοί δε μπορούν να εντοπισθούν και να αντιμετωπισθούν με τα "κλασικά" antivirus software αλλά απαιτούν πιο ευρηματικές μεθόδους. *(67)*

- Script virus: Πρόκειται για ιούς που κατασκευάζονται με τη χρήση γλώσσας προγραμματισμού όπως JavaScript και VBScript (Visual Basic Script). Η προσβολή ενός Η/Υ ή ενός δικτύου γίνεται μέσω e-mail μηνύματος όσο και μέσω email attachment. Επίσης η διασπορά του ιού μπορεί να γίνει και μέσω ιστοσελίδων HTML, οι οποίες μπορεί να περιέχουν κώδικα του ιού στον κώδικα τους. Ο ιός δεν προσβάλει μόνο ένα συγκεκριμένο Η/Υ αλλά μεταφέρεται και σε όλες τις ηλεκτρονικές διευθύνσεις που είναι καταχωρημένες στο address book. Στην περίπτωση που έχουμε προεπιλέξει να γίνεται αυτόματα άνοιγμα Word και Excel files από το email program, τότε ο ιός αυτόματα θα ενεργοποιηθεί προκαλώντας βλάβη στο PC.

Μία διαφορετικού είδους κατηγοριοποίηση των ιών γίνεται με βάση τον τρόπο με τον οποίον ενεργούν στους Η/Υ και τα δίκτυα και οφείλουμε να την περιγράψουμε για την πληρότητα της ανάλυσης. Διακρίνουμε λοιπόν τους παρακάτω ιούς:

- Πολυμορφικοί ιοί: Οι πολυμορφικοί ιοί αποτελούν κρυπτογραφημένους ιούς που σε κάθε μετάδοση τους αλλάζουν μορφή. Ο εντοπισμός και η αντιμετώπιση από τα antivirus software είναι δύσκολος εξαιτίας ακριβώς της συνεχούς μεταμόρφωσης τους. Διακρίνονται σε δύο βασικές κατηγορίες :

  1.Πολυμορφικοί ιοί οι οποίοι μπορούν και αλλάζουν τον κώδικα τους κάθε φορά επιτίθενται σε ένα αρχείο. Σε ορισμένες περιπτώσεις η αλλαγή του κώδικα γίνεται απλά με την προσθήκη μη λειτουργικού κώδικα στο file του ιού. Έτσι, το file αυτό αλλάζει και εμφανίζεται ως κάτι τελείως διαφορετικό με αποτέλεσμα ο εντοπισμός του ιού από το antivirus software να είναι σχεδόν αδύνατος.

  2. Πολυμορφικοί ιοί οι οποίοι μπορούν και κρυπτογραφούν τον κώδικα τους ενώ και το κλειδί τους είναι μη μόνιμο. Η διαδικασία αποκρυπτογράφησης σε κάθε αντίγραφο είναι διαφορετική όπως και το κάθε αντίγραφο είναι διαφορετικό από το άλλο.

Η δημιουργία των πολυμορφικών ιών στηρίζεται στην χρήση Μηχανών Μετάλλαξης (Mutation Engine) με τις οποίες γίνεται τόσο δημιουργία νέου εξολοκλήρου ιού όσο και η μετάλλαξη ενός ήδη υπάρχοντος. Ένα τέτοιο "εργαλείο" είναι το γνωστό Dark Avenger's Mutation Engine (γνωστό και ως MTE ή DAME). *(65)*

- Stealth virus: Σκοπός της χρήσης ενός ηλεκτρονικού ιού είναι η αλλαγή ή η καταστροφή κάποιων πραγμάτων, π.χ. δεδομένων. Αν όμως οι αλλαγές αυτές είναι σε μεγάλη έκταση ή εύκολα αντιληπτές ο ιός θα εντοπισθεί από τα antivirus software και θα καταστραφεί. Ο stealth virus προσπαθεί αυτό να αποφύγει κρύβοντας τις αλλαγές που εκτελεί, τόσο από τους χρήστες όσο από τα antivirus software. Οι μετατροπές αυτές είναι στο μέγεθος του file, στη δομή του directory και/ή στην μορφή του operating system. Διακρίνονται σε δύο κατηγορίες :

  1.File stealth virus. Προσβάλουν τα αρχεία .com, .exe αλλάζοντας το μέγεθος του αυθεντικού file. Αν χρησιμοποιήσουμε την επιλογή CHKDSK τότε το μολυσμένο αρχείο καταστρέφεται ολοσχερώς.

  2.Full stealth virus. Οι ιοί αυτοί όταν προσβάλουν ένα αρχείο, προσωρινά αποθηκεύουν τα περιεχόμενα του με αποτέλεσμα αυτό να εμφανίζεται ως απόλυτα φυσιολογικό, χωρίς να έχει προσβληθεί από ιούς. Αν πάλι χρησιμοποιήσουμε την ανωτέρω επιλογή το file καταστρέφεται τελείως.

  Οι ιοί αυτής της κατηγορίας υπάρχουν εδώ και δύο δεκαετίες περίπου. Με την εμφάνιση των Microsoft Windows 95 θεωρήθηκε ότι, δε θα αντιμετωπίζαμε ξανά τέτοιας κατηγορίας malicious code. Όμως μερικά χρόνια αργότερα το φαινόμενο επανήλθε. *(68)* Επιπλέον σύμφωνα με τον Timothy L.Thomas *(69)* οι Ρωσικές Ένοπλες Δυνάμεις έχουν αναπτύξει τα τελευταία χρόνια γκάμα από stealth virus. Οι τελευταίοι δε μπορούν να αντιμετωπισθούν με τις γνωστές μεθόδους, ενώ μπορούν να διεισδύσουν

ακόμα και σε δίκτυα υψηλής ασφαλείας όπως των Δυνάμεων Στρατηγικών Πυραύλων των Η.Π.Α. .*(70)*

- Fast and slow infectors: Η χρήση του όρου fast (ταχύς) and slow (αργός) έχει να κάνει με το πόσο συχνά και κάτω από ποιες συνθήκες οι ιοί αυτοί διασπείρουν την μόλυνση τους. Έτσι ο fast infector μολύνει κάθε file με το οποίο έρχεται σε επαφή ενώ ο slow infector μόνο αρχεία κατά την δημιουργία ή μετατροπή τους. Η τυπική διαδικασία εξάπλωσης που ακολουθεί ένας ιός είναι η εξής: ο ιός φορτώνει τον εαυτό του στη μνήμη, όταν το μολυσμένο πρόγραμμα τρέχει. Παραμένει εκεί για όσο χρόνο χρειασθεί ώσπου να τρέξουν και άλλα προγράμματα τα οποία στην συνέχεια προσβάλλει. Ο fast infector επιτίθεται σε προγράμματα όχι μόνο όταν αυτά τρέχουν αλλά απλά και όταν απλά έχει πρόσβαση σε αυτά .Ο σκοπός αυτής της διαδικασίας διασποράς είναι να παρακαμφθεί το antivirus software καθώς αυτό θα κάνει τον προβλεπόμενο έλεγχο για τον εντοπισμό πιθανών ιών. Ο slow infector όπως αναφέραμε και προηγουμένως κάνει ακριβώς το αντίθετο. Σκοπός αυτής της διαδικασίας είναι η προσπάθεια υπερνίκησης της μεθόδου ελέγχου ακεραιότητας του file. Έτσι στην περίπτωση της τροποποίησης του κώδικα ενός file είναι πολύ πιθανόν ο χρήστης να μην υποψιασθεί μόλυνση αυτού του file. Εκ φύσεως λοιπόν και επειδή ο εκτελέσιμος κώδικας δεν αλλάζει πολύ συχνά η ανωτέρω διαδικασία είναι πιο αργή. Για την αντιμετώπιση τέτοιων ιών συνήθως χρησιμοποιείτε ένας καθαρός floppy disk για εκτέλεση boot στον Η/Υ.
- Sparse infectors: Με το όνομα αυτό περιγράφονται μια σειρά από cyber virus οι οποίοι χρησιμοποιούν σπάνιες τεχνικές για την αποφυγή εντοπισμού τους. Χαρακτηριστικά παραδείγματα αυτών είναι π.χ. η επίθεση σε ένα file την $20^{η}$ φορά που θα χρησιμοποιείται, η επίθεση σε files το οποίο το μέγεθος είναι συγκεκριμένο, η επίθεση σε file που το όνομα τους ξεκινάει από συγκεκριμένο ή συγκεκριμένη ομάδα γραμμάτων του αλφαβήτου κ.ά. .
- Multipartite virus: Οι ιοί αυτής της κατηγορίας επιτίθενται τόσο σε boot sectors όσο και σε εκτελέσιμα files ανάλογα με τις εκάστοτε ανάγκες. Έχουν

την ικανότητα να συνδυάζουν μερικές ή όλες τις τεχνικές stealth σε συνδυασμό με τον πολυμορφισμό (polymorphism), προκειμένου να αποφύγουν τον εντοπισμό.

- Cavity virus: Οι περισσότεροι cyber virus χρησιμοποιούν τον πιο εύκολο δρόμο προκειμένου να προσβάλλουν ένα file, κάνοντας attach τον εαυτό τους στο τέλος του file και στη συνέχεια αλλάζουν την αρχή του προγράμματος με αποτέλεσμα αυτό αρχικά να περιέχει κώδικα του ιού και στη συνέχεια το πραγματικό program code. Παράλληλα χρησιμοποιούν τεχνικές stealth ώστε να αποκρύψουν την αύξηση στο μέγεθος του μολυσμένου file, όταν ιός είναι ενεργός στη μνήμη του Η/Υ. Από την άλλη πλευρά οι cavity virus λειτουργούν λίγο πιο έξυπνα. Μερικά program files για μια σειρά από λόγους έχουν κενά σημεία τα οποία χρησιμοποιούν οι ιοί αυτού του είδους για να κρυφτούν. Με τη μέθοδο αυτή δεν αυξάνεται η έκταση του file και δεν απαιτείται η χρήση τεχνικών stealth. Εξαιτίας όμως της δυσκολίας δημιουργίας τέτοιας κατηγορίας ιών και του περιορισμένου αριθμού πιθανών host σπάνια αντιμετωπίζουμε cavity virus. *(66)*

1.8.6 Actors –Πρόσωπα που εκτελούν Cyber Attacks – περιστατικά

Ένα βασικό ερώτημα που απασχολεί όλους όσους ασχολούνται με την τρομοκρατία στο Διαδίκτυο είναι ποιοι είναι τελικά αυτοί που εκτελούν τέτοιου είδους επιθέσεις και τι πρεσβεύουν. Με βάση τη θεώρηση που κάναμε παραπάνω, ότι η τρομοκρατία είναι σαν μια "θεατρική παράσταση", ονομάσαμε actors (ηθοποιούς) αυτούς που την εφαρμόζουν.

Είναι επίσης ξεκάθαρο ότι κάθε χρήστης του internet και της τεχνολογίας της πληροφορικής που πιθανόν να παρενοχλεί ένα ανταγωνιστή του, δεν είναι cyber terrorist. Σαφέστατα είναι πολύ δύσκολό τις περισσότερες φορές να αντιληφθούμε αν η επίθεση προέρχεται από κάποια συγκεκριμένη ομάδα- οργάνωση ή από κάποιους φοιτητές με ιδιαίτερες ικανότητες για παράδειγμα, με αποτέλεσμα και τα όρια ανάμεσα στο απλό hacking και την κυβερνοτρομοκρατία να είναι θολά. Παρακάτω θα προσπαθήσουμε να κατηγοριοποιήσουμε τους πιθανούς "εχθρούς" που κάποιος μπορεί να συναντήσει στο Διαδίκτυο και που μπορούν ανά πάσα στιγμή να μετατραπούν σε cyber terrorist.

1.8.6.1 Κατάσκοποι -Spies

Οι κατάσκοποι είναι τα άτομα τα οποία επιδιώκουν την παράνομη απόκτηση πληροφοριών με απώτερο στόχο το πολιτικό όφελος. Συνήθως τα άτομα αυτά είναι μέλη κυβερνητικών υπηρεσιών, οι στόχοι τους όπως είναι λογικό είναι τα υπολογιστικά συστήματα των ξένων και συνήθως εχθρικών χωρών, ακόμα και οι πληροφορίες που επιδιώκουν να αποκτήσουν έχουν να κάνουν με ταξιδιωτικά σχέδια ανώτερων αξιωματούχων, σχέδια εκτάκτου ανάγκης και πολιτικής άμυνας, δορυφορικά δεδομένα, δεδομένα επιβολής νόμου, ανακρίσεων, αρχείων ασφαλείας κ.α. Χαρακτηριστικό είναι το παρακάτω παράδειγμα: μεταξύ 1986 και 1989, σύμφωνα με τον Clifford Stohl (στο βιβλίο του The Cuckoo's egg, Information Warfare and Security p205-206), μία ομάδα Δυτικογερμανών hackers παρακολουθούσαν και κατέγραφαν εκπαιδευτικά, στρατιωτικά και εταιρικά δίκτυα σε Η.Π.Α., Ιαπωνία και σε άλλες χώρες της Δύσης. Τις πληροφορίες που συνέλεξαν τις παρέδωσαν έναντι αμοιβής σε πράκτορες της KGB (Υπηρεσία Κατασκοπείας της Σοβιετικής Ένωσης).

1.8.6.2 Corporate Raiders – Βιομηχανικοί κατάσκοποι

Οι corporate raiders είναι ένα είδος κατασκόπων που ειδικεύονται στη βιομηχανική κατασκοπεία. Φυσικά ο όρος δεν είναι καινούριος στην ανθρώπινη ιστορία. Χαρακτηριστικά παραδείγματα υπάρχουν στην Αρχαία Ελλάδα αλλά και στα Μεσαιωνικά χρόνια. Τα άτομα που ασχολούνται με αυτή είναι ικανά να συλλέξουν ιδιοκτησιακά δεδομένα από εταιρείες που αποσκοπούν στην αρωγή άλλων εταιρειών. Τους corporate raiders μπορούν να τους χρησιμοποιήσουν είτε εταιρείες που αποσκοπούν στην βελτίωση των συγκριτικών πλεονεκτημάτων τους είτε κυβερνήσεις που επιδιώκουν να βοηθήσουν τις εγχώριες βιομηχανίες τους. Η κατασκοπεία που διαπράττουν τα άτομα αυτά όταν έχουν προσληφθεί από κάποια κυβέρνηση ονομάζεται οικονομική κατασκοπεία. Σήμερα η βιομηχανική κατασκοπεία είναι σε άνθηση. Μια έρευνα υποστήριξε ότι το 58 τις εκατό των "κλοπών" διαπράχθησαν από νυν ή πρώην υπαλλήλους. Οι τρεις πιο καταστροφικές κατηγορίες κλεμμένων πληροφοριών ήταν πληροφορίες τιμολόγησης, πληροφορίες βιομηχανικής διαδικασίας και πληροφορίες ανάπτυξης και προδιαγραφών προϊόντων.

1.8.6.3 Insiders –Εσωτερικοί εχθροί

Οι ειδικοί της ασφάλειας των πληροφοριών προσπαθούν συνεχώς να εξασφαλίσουν στα συστήματα τους τη μη πρόσβαση από ανεπιθύμητους επισκέπτες. Όμως σε αρκετές

περιπτώσεις η επίθεση προέρχεται "από μέσα", δηλαδή από κάποιον που έχει ήδη άδεια πρόσβασης σε ένα δίκτυο. Ένα τέτοιο παράδειγμα είναι υπάλληλοι εταιριών και οργανισμών που εργάζονται μεμονωμένα π.χ. από το σπίτι τους. Το 1997 στις ΗΠΑ υπάλληλος της Ακτοφυλακής κατάφερε χρησιμοποιώντας το password συναδέλφου του και έχοντας πρόσβαση στα συστήματα του Σώματος να προκαλέσει ζημιά που θα ζήλευε και ο κάθε τρομοκράτης, διαγράφοντας μεγάλο μέρος από την επίσημη Data Base. Για την αποκατάσταση της ζημιάς και την ανάκτηση μέρους μόνο αυτών των δεδομένων χρειάσθηκε να εργασθούν 115 υπάλληλοι και για 18.000 εργατοώρες. Ένα άλλο παράδειγμα εσωτερικού εχθρού είναι οι "σύμβουλοι"-κατασκευαστές. Η σημασία του ρόλου τους, φαίνεται ξεκάθαρα στο ακόλουθο συμβάν: το Μάρτιο του 2000, η Μητροπολιτική Αστυνομία του Τόκυο ανέφερε τη χρήση ενός software system για την παρακολούθηση συνεχώς της θέσης των περιπολικών της, το οποίο είχε κατασκευασθεί από μέλη της αίρεσης Aum Shinryko. Μετά από έρευνες ανακαλύφθηκε ότι τα μέλη της οργάνωσης είχαν αποκτήσει πρόσβαση σε διαβαθμισμένες πληροφορίες για την κίνηση των οχημάτων της Αστυνομίας. Παράλληλα είχαν εγκαταστήσει ένα Trojan Horse τόσο στο παραπάνω software system όσο και σε άλλα που είχαν κατασκευάσει για διάφορες εταιρείες και οργανισμούς, προκειμένου να πραγματοποιήσουν τρομοκρατική επίθεση σε μελλοντικό χρόνο.

1.8.6.4 Επαγγελματίες εγκληματίες

Αυτοί στοχεύουν στην ικανοποίηση κυρίως προσωπικών οικονομικών οφελών μέσω της παράνομης απόκτησης πληροφοριών ή παραποίησης τους. Ειδικότερα αυτά τα άτομα έχουν εξειδικευτεί στις απάτες χρησιμοποιώντας τα υπολογιστικά συστήματα. Με τα υπολογιστικά συστήματα είναι δυνατή η εκμετάλλευσή τους για απάτες και για κλοπή. Για παράδειγμα, άτομα μπορούν να χρησιμοποιήσουν ένα υπολογιστή για να καταχραστούν μικρά ποσά από ένα μεγάλο αριθμό λογαριασμών, υποθέτοντας ότι τα μικρά αυτά ποσά ποτέ δεν θα γίνουν αντιληπτά ότι καταχράστηκαν. Τα οικονομικά συστήματα δεν είναι τα μόνα που ριψοκινδυνεύουν. Συστήματα τα οποία ελέγχουν την πρόσβαση σε οποιουσδήποτε πόρους είναι και αυτά στόχοι (π.χ. συστήματα απογραφών, συστήματα που κρατούν την βαθμολογία στα σχολεία, μεγάλων αποστάσεων τηλεφωνικά συστήματα κ.α.). Η ηλεκτρονική απάτη μπορεί να γίνει και από άτομα που έχουν σχέση με το σύστημα και από αυτά που δεν έχουν. Τα άτομα που έχουν κάποια σχέση είναι αυτά που ευθύνονται για το μεγαλύτερο ποσοστό απάτης. Αφού τα άτομα αυτά έχουν πρόσβαση και γνωρίζουν καλύτερα το θύμα-υπολογιστικό

σύστημα, είναι σε καλύτερη θέση να προκαλέσουν ζημιά. Τα άτομα που έχουν σχέση με το υπολογιστικό σύστημα μπορεί να είναι είτε χρήστες είτε τεχνικό προσωπικό. Ένας πρώην υπάλληλος του οργανισμού με γνώσεις για τις λειτουργίες του οργανισμού μπορεί επίσης να είναι μια απειλή ιδιαίτερα αν η συνεργασία του με τον οργανισμό δεν έχει τερματιστεί με τον καλύτερο τρόπο. Παραδείγματα δράσεως τέτοιων εγκληματιών έχουν καταγραφεί αρκετά, όπως: ο μεγιστάνας των MME Michael Bloomberg. Τα συστήματα της εταιρείας του πριν μερικά χρόνια είχαν παραβιασθεί από δύο hackers οι οποίοι του ζητούσαν για να μη διαδώσουν πως το κατάφεραν 200.000$. Ένα άλλο παράδειγμα αφορά τη πρόσβαση σε διαβαθμισμένα κυβερνητικά δίκτυα και την απόκτηση πληροφοριών με σκοπό το οικονομικό κέρδος. Το Σεπτέμβριο 2003 ανακαλύφθηκε η ύπαρξη συνωμοσίας στις ΗΠΑ από ιδιώτη ο οποίος ήταν πρόεδρος σε εταιρία computer security. Σκοπός του τελευταίου, ήταν η είσοδος σε στρατιωτικά και κυβερνητικά δίκτυα, η αντιγραφή files και data base και η δημοσιοποίηση αυτών στα MME ως διαφήμιση για την εταιρεία του. Με τον τρόπο αυτό θα προσέγγιζε νέους πελάτες και θα αύξανε τα κέρδη του. Είχε καταφέρει να αποκτήσει αρχεία από τη NASA, τον Αμερικανικό Στρατό, το Αμερικανικό Ναυτικό, το Υπουργείο Ενέργειας και το Υπουργείο Υγείας.*(73)*

1.8.6.5 Βάνδαλοι -Vandals

Αυτή η κατηγορία ατόμων είναι από τις πιο επικίνδυνες για την ασφάλεια των υπολογιστικών συστημάτων. Τα άτομα αυτά έχουν ως μόνο στόχο την πρόκληση ζημιάς με οποιονδήποτε τρόπο και χωρίς κανένα συγκεκριμένο προσωπικό όφελος. Τα παραπάνω είναι και ο λόγος που κάνουν αυτά τα άτομα αρκετά επικίνδυνα διότι δεν υπάρχουν ούτε οι ηθικοί φραγμοί ούτε και ο λόγος που θα τους κάνει να σταματήσουν την επίθεση, ακριβώς επειδή δεν υπάρχει κανένα προσωπικό όφελος. Ακόμα είναι αρκετά δύσκολος ο προσδιορισμός αυτών των προσώπων διότι μπορεί να είναι οποιοιδήποτε ακόμα και άτομα που δεν έχουν σχέση με το επιτιθέμενο υπολογιστικό σύστημα. Παράλληλα είναι πολύ πιθανόν να προσφέρουν τις "υπηρεσίες" τους σε τρομοκρατικές οργανώσεις χωρίς κανένα ενδοιασμό.

1.8.6.6 Hackers

Hackers, ονομάζονται τα άτομα που επεμβαίνουν παράνομα σε υπολογιστές επειδή απλά αντιμετωπίζουν τη διαδικασία της προσβολής της ασφάλειας υπολογιστών σαν πρόκληση για τις προγραμματιστηκές τους ικανότητες. Μπορεί να συμπεριλαμβάνουν άτομα

που έχουν σχέση με το σύστημα ή άτομα του εξωτερικού περιβάλλοντος. Η απειλή των hacker πρέπει να θεωρηθεί όσον αναφορά ως περασμένη ή ενδεχόμενη μελλοντική ζημιά. Παρόλο που οι σύγχρονες απώλειες, που οφείλονται στους hackers είναι σημαντικά μικρότερες, από τις απώλειες που οφείλονται στους κλέφτες που έχουν σχέση με το σύστημα. Ένα παράδειγμα δραστηριότητας hacker είναι η υποκλοπή του δημόσιου τηλεφωνικού συστήματος. Οι hacker συχνά λαμβάνουν περισσότερης προσοχής από τις κοινές και επικίνδυνες απειλές. Μπορούν να διακριθούν στις παρακάτω υποκατηγορίες:

1. White hat hacker – καλόβουλος, πρόκειται για άτομα που ψάχνουν τις τρωτότητες των υπολογιστικών συστημάτων και στην συνέχεια σε συνεργασία με τον κατασκευαστή επεμβαίνουν για να διορθώσουν το πρόβλημα.
2. Black hat hacker – κακόβουλος, πρόκειται για την πιο συνηθισμένη περίπτωση hacker .Αυτοί προσπαθούν να αποκτήσουν παράνομη πρόσβαση σε δίκτυα Η/Υ και Η/Υ με σκοπό την καταστροφή του συστήματος ή των δεδομένων του, την κλοπή πληροφοριών και την πρόκληση αναστάτωσης και προβλημάτων.

Ως παράδειγμα των συστημάτων και δικτύων που οι hackers μπορούν να χτυπήσουν φαίνεται στην περίπτωση που ανακαλύφθηκε το 2002. Δύο έφηβοι κατάφεραν να εισβάλλουν στο Lawrence Livermore National Laboratory και στο δίκτυο της Αμερικανικής Αεροπορίας και άλλων οργανισμών .Χρησιμοποίησαν προγράμματα “sniffer” για την υποκλοπή password και τον επαναπρογραμματισμό των Η/Υ, προκειμένου να έχουν πλήρη πρόσβαση σε όλα τα files. Επίσης τοποθέτησαν “backdoor” προγράμματα προκειμένου να μπορούν να έχουν πρόσβαση όποτε το επιθυμούσαν.*(74)*

1.8.6.7 Τρομοκράτες

Τρομοκράτες είναι άτομα που σκοπεύουν να διασπείρουν τον φόβο σχετικά με πολιτικά, κοινωνικά και ιδεολογικά ζητήματα. Αυτό το επιτυγχάνουν με την καταστροφή υπολογιστικών συστημάτων, όπως βάσεις δεδομένων κ.α., που έχουν μεγάλη σημασία, με τον εκβιασμό ότι πρόκειται να καταστρέψουν κάποιο υπολογιστικό σύστημα που κρατά σημαντικές πληροφορίες, π.χ. τα records μιας μεγάλης τράπεζας και τέλος με τη χρησιμοποίηση πληροφοριών που έχουν αποκτήσει με παράνομο τρόπο. Όπως έχουμε

αναφέρει και σε προηγούμενη παράγραφο, υπάρχουν διαφορετικά cyber terrorist "camps" και διαφορετικές μορφές επιθέσεων. Έτσι θα περιγράψουμε τέσσερις πιθανές κατηγορίες cyber terrorist και της απειλής που αυτές αντιπροσωπεύουν.

1. Πολλοί από τους από τους πιο γνωστούς ιούς όπως ο Morris worm, I LOVE YOU virus και ο Chernobyl virus είναι δουλειά μεμονωμένων ατόμων. Παράλληλα πολλές πράξεις τρομοκρατίας όχι στο ψηφιακό αλλά στον πραγματικό κόσμο με πολλά θύματα, φόβο και ψυχολογικά τραύματα είναι έργο μεμονωμένων ατόμων. Παραδείγματα τέτοια είναι, ο Ted Kaczynski (Unabomber), Tim McVeigh (βομβιστής της Οκλαχόμα) και ο John Muhammad (Washington D.C). Αν κάνουμε συνδυασμό των δύο παραδειγμάτων έχουμε το προφίλ του μοναχικού-μεμονωμένου cyber terrorist. Φυσικά η ζημιά που γίνεται από τις ψηφιακές επιθέσεις είναι κυρίως οικονομική και όχι σε ανθρώπινες ζωές. Η απειλή από αυτή την κατηγορία cyber terrorist είναι μάλλον χαμηλή αλλά όχι ανύπαρκτη.

2. Μία μικρή ομάδα εξτρεμιστών με τεχνικές ικανότητες μπορεί να κάνει χρήση αυτών για να πετύχει συνδυασμένη επίθεση στον ψηφιακό χώρο. Χαρακτηριστική είναι η περίπτωση της ιαπωνικής αίρεσης Aum Shinryko που αναφέραμε σε προηγούμενη παράγραφο. Η συγκεκριμένη ομάδα εκτέλεσε την επίθεση στο μετρό του Τόκυο σκοτώνοντας 12 αθώους πολίτες και τραυματίζοντας συνολικά 6000. Τώρα η απειλή από τέτοιες "κλειστές" ομάδες είναι μεγαλύτερη μιας και οι στόχοι τους μπορούν να πραγματοποιηθούν μέσα από το κυβερνοχώρο ευκολότερα και με περισσότερη επιτυχία.

3. Μεγάλες θρησκευτικές τρομοκρατικές ομάδες αποτελούν την τρίτη κατηγορία κυβερνοτρομοκρατών, με πιο χαρακτηριστικό παράδειγμα αυτό της οργάνωσης Al-Qaeda την οποία έχουμε αναφέρει αναλυτικά σε προηγούμενο κεφάλαιο της εργασίας. Αξίζει να προσθέσουμε εδώ ότι ο ηγέτης της οργάνωσης Osama bin Laden υπερηφανεύεται για την ύπαρξη στις τάξεις της οργάνωσης "Μουσουλμάνων επιστημόνων με μεγάλες ικανότητες".

4. Η τελευταία κατηγορία cyber terrorist αφορά τις λεγόμενες ομάδες πληροφοριακού πολέμου οι οποίες υποστηρίζονται τεχνικά και οικονομικά από συγκεκριμένα κράτη. Παραδείγματα τέτοιων κρατών είναι η Κίνα, η Ινδία, η Ρωσία, οι ΗΠΑ, η

Βόρεια Κορέα, η Τουρκία κ.α. Υπάρχουν δύο κατηγορίες τέτοιων ομάδων με διαφορετικές ικανότητες και στόχους. Η πρώτη, η οποία είναι και η επίσημη, αφορά μονάδες cyber warfare οι οποίες εξοπλίζονται και εκπαιδεύονται από τις κυβερνήσεις των κρατών για να επιτίθενται στα εχθρικά πληροφοριακά συστήματα και να προστατεύουν τα ημέτερα. Σύμφωνα με πρόσφατη αναφορά για τις δυνατότητες για παράδειγμα του Κινεζικού Στρατού στο ψηφιακό τομέα αναφέρεται η ύπαρξη Ειδικών Μονάδων Πληροφορικού Πολέμου που εκτελούν ανά τακτά χρονικά διαστήματα ασκήσεις επιθετικών και αμυντικών cyber παιγνίων, ιδιαίτερα μάλιστα εξελιγμένων. Σύμφωνα με αξιωματούχους του Αμερικανικού Υπουργείου Άμυνας από το 2001 Κινέζοι hackers έχουν καταφέρει να διεισδύσουν και να παρακολουθούν διάφορα στρατιωτικά δίκτυα όπως αυτά του U.S. Army Information System Agency, Naval Ocean Systems Center, Defense Information Systems Agency κ.ά. *(74)* Παράλληλα (αυτή είναι η δεύτερη κατηγορία) υπάρχουν ομάδες εθνικιστών πολιτών οι οποίες αρέσκονται να επιτίθενται σε υπολογιστικά συστήματα άλλων κρατών, χωρίς κάποια επίσημη ιδιότητα. Αυτό τους δίνει τη δυνατότητα να μην υπόκεινται σε τυχόν περιορισμούς που έχουν οι επίσημοι κρατικοί οργανισμοί. Φυσικά δεν είναι μόνο οι Κινέζοι που ακολουθούν τέτοιες πρακτικές. Τις ίδιες πρακτικές ακολουθεί και η Ρωσία και μάλιστα με μια διαφορετική διάσταση, αυτή του πολέμου της Τσετσενίας. Η διεθνής ενημέρωση για το τι συμβαίνει σε αυτή την γωνιά του πλανήτη είναι πολύ μικρή. Σε αυτό παίζει ρόλο και η δράση των Ειδικών Πληροφοριακών Μονάδων των Ρωσικών Αρχών. Ενδεικτικό της δράσης τους είναι το παρακάτω γεγονός: το Μάρτιο 2002 τα δύο πιο κύρια web-sites των Τσετσένων, kavkaz.org και Chechen press.com κατέρρευσαν από επιθέσεις hackers της FSB (Ρωσική Μυστική Υπηρεσία), παρότι είχαν κατασκευαστεί στις ΗΠΑ. Το συμβάν αυτό έγινε λίγο μετά από την είσοδο των Ρωσικών Ειδικών Δυνάμεων στο θέατρο της Μόσχας που είχε καταληφθεί από Τσετσένούς τρομοκράτες. Συνδυασμός των παραπάνω δύο κατηγοριών μπορεί να θεωρηθεί η Τρίτη, για την οποία υπάρχουν απλά ενδείξεις ότι υπάρχει. Το 2001 για παράδειγμα η Ταϊβάν εξαπέλυσε διάφορους cyber virus εναντίον της Κίνας. Όμως αυτοί διαδόθηκαν μέσω του Διαδικτύου σε ολόκληρο τον κόσμο και όχι μόνο στην Κίνα, επομένως η Ταϊβάν δε μπορούσε, επίσημα τουλάχιστον, να κατηγορηθεί γι'

αυτό, παρά το γεγονός ότι οι Κινεζικοί στόχοι που επλήγησαν και ο τρόπος των επιθέσεων απαιτεί τουλάχιστον κρατική πληροφόρηση. Αυτή η τελευταία υβριδική ομάδα που αναφέραμε αποτελεί και την πιο επικίνδυνη αφού μπορεί και συνδυάζει τα πλεονεκτήματα των κρατικών υπηρεσιών με την ανωνυμία και την ελευθερία των απλών hacker.

1.8.7 Στόχοι των cyber attacks

Η ανάλυση των στόχων που έχουν οι cyber attacks μπορεί να πραγματοποιηθεί αν κατανοήσουμε τις απαιτήσεις που έχουμε από ένα δίκτυο Η/Υ, αλλά και από τους ίδιους τους Η/Υ επίσης. Έτσι για παράδειγμα συνδεδεμένο με τα δίκτυα είναι ένα αυξανόμενο ευρύ φάσμα εφαρμογών (συστήματα διανομής ηλεκτρονικού ταχυδρομείου κλπ.) και τερματικού εξοπλισμού (τηλεφωνική συσκευή, υπολογιστές υπηρεσίας, προσωπικοί υπολογιστές, κινητά τηλέφωνα, ηλεκτρονικές ατζέντες. οικιακές συσκευές, βιομηχανικές μηχανές, κλπ.). Για να είναι λειτουργικό αυτό θα πρέπει πρωτίστως να εξασφαλίζεται η ασφαλής επικοινωνία. Με τον όρο αυτό νοείται κάθε μορφή επικοινωνίας που γίνεται με χρήση ψηφιακής τεχνολογίας και εξασφαλίζει την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών που διακινούνται μέσω ενός τηλεπικοινωνιακού δικτύου. Αυτά ακριβώς τα χαρακτηριστικά προσπαθούν να καταργήσουν οι cyber επιθέσεις:

- Απώλεια της εμπιστευτικότητας (confidentiality): Εμπιστευτικότητα, είναι η διασφάλιση της προσπελασιμότητας της πληροφορίας μόνον από όσους έχουν τα απαραίτητα δικαιώματα. Εξασφαλίζεται έτσι ότι οι πολύτιμες πληροφορίες και δεδομένα παραμένουν στην δικαιοδοσία μόνον αυτών που έχουν την εξουσιοδότηση να τα προσπελάσουν. Με την απώλεια της έχουμε παράνομη, απρόβλεπτη και καταστροφική διασπορά και απώλεια πληροφορίας.

- Απώλεια της ακεραιότητας (integrity): Ακεραιότητα, είναι η διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής. Η πληροφορία έχει αξία μόνον εάν γνωρίζουμε ότι είναι σωστή και ακριβής. Βασική επιδίωξη της πολιτικής προστασίας είναι ότι δεν πρόκειται με κανέναν τρόπο η πληροφορία να τροποποιηθεί ή να καταστραφεί. Η ακεραιότητα της πληροφορίας μπορεί να χαθεί είτε εσκεμμένα είτε λόγω τυχαίου γεγονότος. Αυτό πολλές φορές αποτελεί και τα πρώτο βήμα για μια επιτυχημένη επίθεση σε ένα υπολογιστικό σύστημα.

- Απώλεια της διαθεσιμότητας (availability): Διαθεσιμότητα, είναι η διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται. Μία εξίσου βασική επιδίωξη της πολιτικής προστασίας πρέπει να είναι η εξασφάλιση ότι η πληροφορία είναι πάντα διαθέσιμη για την υποστήριξη της ομαλής εξέλιξης της επιχειρηματικής και όχι μόνο δραστηριότητας. Απώλεια της διαθεσιμότητας σημαίνει απώλεια κρίσιμου χρόνου, λανθασμένες αποφάσεις και καταστροφικά αποτελέσματα.

Παράλληλα στόχος των cyber attacks είναι οι κρίσιμες υποδομές τις οποίες θα αναλύσουμε στο επόμενο κεφάλαιο διεξοδικά. Επιπλέον η φυσική καταστροφή μπορεί να θεωρηθεί στόχος αυτών των επιθέσεων. Φυσική καταστροφή αναφέρεται στην ικανότητα να πετυχαίνει κάποιος καταστροφή ή ζημιά αντικειμένου στον φυσικό κόσμο με την χρήση IT συστημάτων αποκλειστικά. Πολλές από τις κρίσιμες υποδομές όπως συστήματα μεταφοράς, εταιρείες παραγωγής ηλεκτρικής ενέργειας, παραγωγής νερού κ.ά. χρησιμοποιούν δίκτυα Η/Υ καθώς και συστήματα SCADA (Supervisory Control and Data Acquisition System) τα οποία μπορούν να γίνουν στόχος επίθεσης προκαλώντας, π.χ. προβλήματα ηλεκτροδότησης ή κυκλοφοριακό χάος. Παράλληλα μπορεί μέσω μιας cyber attack τρομοκρατική ομάδα να εισβάλλει στο σύστημα διαχείρισης εναέριας κυκλοφορίας προκαλώντας τη συντριβή των αεροσκαφών που βρίσκονται στον αέρα πάνω από μια μεγάλη πόλη. Αν και ένα τέτοιο σενάριο σε αρκετούς μπορεί να φαίνεται εξωπραγματικό οι πιθανότητες που υπάρχουν να συμβεί δεν είναι αμελητέες. Το 2001 στο Queensland της Αυστραλίας εντοπίσθηκε ιδιώτης, ο οποίος χρησιμοποιώντας το Διαδίκτυο, wireless radio και κλεμμένο control software κατάφερε να απελευθερώσει 1εκατομμύριο λίτρα απόβλητα στο ποτάμι και τις παραθαλάσσιες περιοχές της πόλης. Είχε καταφέρει να εισέλθει στο ηλεκτρονικό σύστημα διαχείρισης των αποβλήτων 44 φορές πριν τελικά εντοπισθεί και συλληφθεί την 45. *(76)*

1.8.8 Η απειλή εναντίον των κρίσιμων υποδομών

Στο Δυτικό κόσμο πολλά πράγματα στην καθημερινότητα του πολίτη θεωρούνται δεδομένα, όπως όταν πατάει τον διακόπτη του ρεύματος το φως ανάβει, όταν παίρνει κάποιο τηλέφωνο η κλήση του διεκπεραιώνεται σε λίγα δευτερόλεπτα. Όλα αυτά οφείλονται σε καλά ανεπτυγμένες και δομημένες υποδομές. Με την έννοια αυτή δεν περιγράφουμε μόνο μια συλλογή από ξεχωριστές εταιρείες και οργανισμούς, αλλά ένα δίκτυο ανεξάρτητων, ιδιωτικών

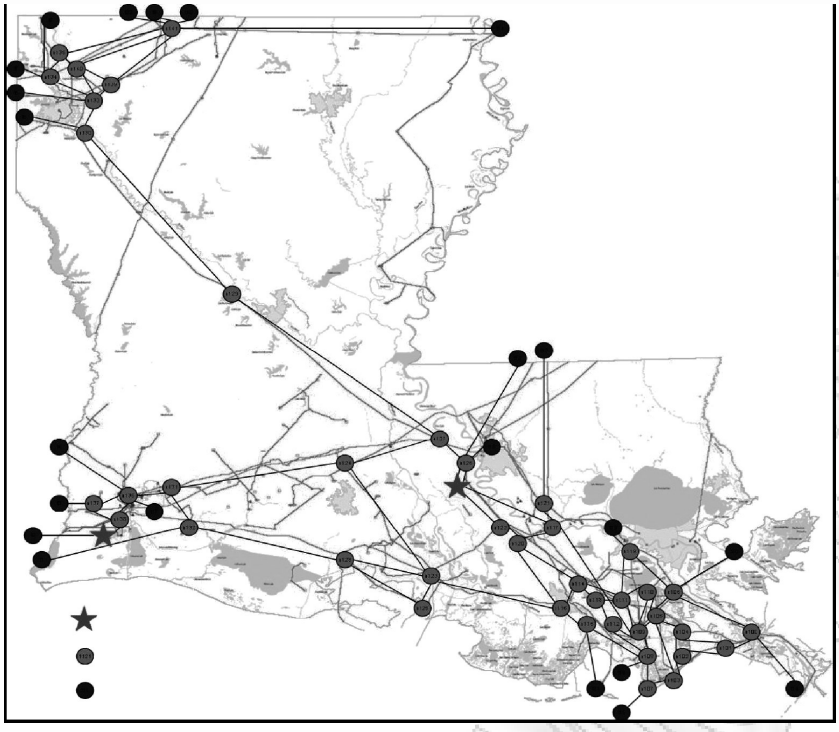
και δημόσιων εταιρειών που λειτουργούν ταυτόχρονα και παράλληλα με σκοπό την παραγωγή αγαθών και την προσφορά υπηρεσιών προς τους πολίτες.

Όλες οι μελέτες γύρω από την απειλή της Κυβερνοτρομοκρατίας συμφωνούν ότι οι βασικές υποδομές ενός κράτους αποτελούν ένα πολύ πιθανό στόχο. Δεδομένου δε, ότι χρησιμοποιούν ευρύτατα computer software, hardware και τηλεπικοινωνιακά συστήματα ο κίνδυνος από cyber επιθέσεις γίνεται ακόμα μεγαλύτερος. Παράλληλα τα τελευταία χρόνια η επαφή των μονάδων αυτών με το Διαδίκτυο είναι συνεχώς αυξανόμενη ενώ συστήματα όπως τα PCS (Process Control System) και SCADA (Supervisory Control and Data Acquisition) που χρησιμοποιούνται για τον έλεγχο αυτών των υποδομών δεν είναι απρόσβλητα. Μια σειρά από λόγοι όπως:

- Οι Η/Υ, τα δίκτυα και τα πρωτόκολλα που χρησιμοποιούνται στα PCS και SCADA δεν είναι απόρρητα αλλά βασίζονται σε εμπορικές εφαρμογές με τις γνωστές αδυναμίες
- Τα τοπικά δίκτυα συνδέονται είτε άμεσα είτε έμμεσα στο Διαδίκτυο
- Πολλές από τις υποδομές συνδέονται μεταξύ τους με αποτέλεσμα να δημιουργείτε ένα τόσο πολύπλοκο δίκτυο που είναι πολύ δύσκολο να ελεγχθεί

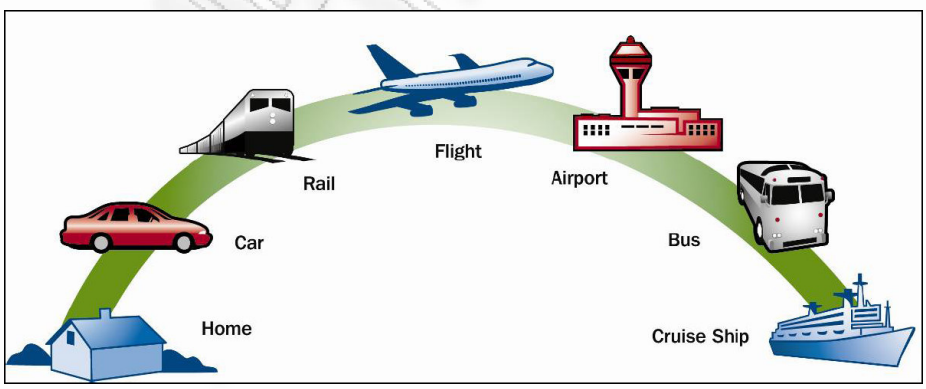
έχουν ως αποτέλεσμα να εμφανίζουν αδυναμίες όμοιες με αυτές ενός οποιαδήποτε μηχανήματος συνδεδεμένο στο Διαδίκτυο. Όμως οι οικονομικές και κοινωνικές επιπτώσεις από την κατάρρευση μιας οποιασδήποτε υποδομής από αυτές, θα είναι ανεξέλεγκτες και τεράστιες. Οι "κρίσιμες αυτές υποδομές", στις οποίες αναφερόμαστε περιλαμβάνουν τους παρακάτω τομείς:

1. Δίκτυα μεταφοράς και διανομής Ενέργειας όπως Δίκτυα αγωγών πετρελαίου και φυσικού αερίου.



ΕΙΚΟΝΑ 24: Το δίκτυο πετρελαίου και φυσικού αερίου της ΛΟΥΙΖΙΑΝΑ των ΗΠΑ.

2. Υπηρεσίες Ανάγκης όπως το Ε.Κ.Α.Β., η Πυροσβεστική Υπηρεσία οι οποίες ανταποκρίνονται στις άμεσες και έκτακτες ανάγκες των πολιτών.
3. Οι υποδομές των θαλάσσιων, αεροπορικών αλλά και χερσαίων μεταφορών με το πλέγμα των αεροδρομίων, λιμανιών και οδικών αρτηριών που περιλαμβάνουν.



ΕΙΚΟΝΑ 25: Οι σύγχρονες μεταφορές

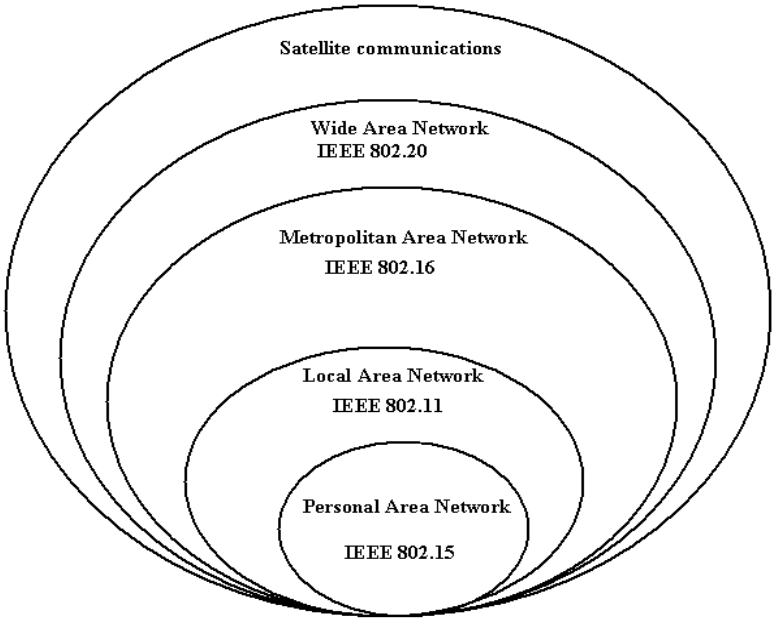
4. Οι υποδομές παροχής, αποθήκευσης, διαχείρισης και μεταφοράς του νερού. Οι υποδομές αυτές εξασφαλίζουν την ομαλή λειτουργία του αγροτικού κλάδου, της βιομηχανίας και βιοτεχνίας, την παροχή ενέργειας (Υδροηλεκτρικά εργοστάσια) αλλά και τη σταθερή και απρόσκοπτη εξυπηρέτηση αυτής της βασικής ανάγκης των νοικοκυριών.

5. Οι τραπεζικές και finance υποδομές που διαχειρίζονται τρισεκατομμύρια ευρώ τόσο τις καταθέσεις των απλών πολιτών όσο και μεγέθη αντίστοιχα του κρατικού προϋπολογισμού. Ενδεικτικά να αναφέρουμε εδώ ότι καθημερινά στις Η.Π.Α. εκτιμάται εκτελούνται ηλεκτρονικές συναλλαγές ύψους 6 τρισεκατομμυρίων δολαρίων. Σε αυτά περιλαμβάνονται συναλλαγές μέσω Α.Τ.Μ., πιστωτικές κάρτες, ηλεκτρονική μεταφορά χρημάτων κ.ά.

6. Οι υποδομές Ηλεκτρικής Ενέργειας περιλαμβάνουν τα συστήματα και τις μονάδες παραγωγής, διανομής και αποθήκευσης και έχουν αντίκτυπο όπως είναι προφανές, σε κάθε φάση της ζωής μας. Από την καθημερινή προσωπική ζωή ως τις τηλεοράσεις, τα ραδιόφωνα, την παραγωγή, τη λειτουργία των Η/Υ και δικτύων.

7. Η χημική βιομηχανία και οι υποδομές παραγωγής και διαχείρισης υλικών όπως π.χ. πυρηνικών.

8. Οι τηλεπικοινωνίες, αποτελούν μια από τις βασικότερες υποδομές στο σύγχρονο κόσμο της πληροφορίας. Ειδικότερα τις δύο τελευταίες δεκαετίες με την επανάσταση στο χώρο της επιστήμης των Η/Υ και τη συνεχώς αυξανόμενη χρήση του Διαδικτύου από το σπίτι, το χώρο εργασίας, τις Δημόσιες Υπηρεσίας και τον Ιδιωτικό φορέα πολλά καθημερινά πράγματα χωρίς αυτό, είναι αδύνατον να εκτελεσθούν. Επίσης οι Δορυφορικές επικοινωνίες αποτελούν σημαντικό τομέα στο κεφάλαιο "Τηλεπικοινωνιακές Υποδομές".



.

ΕΙΚΟΝΑ 26: Τα σύγχρονα Δίκτυα Επικοινωνιών

Όλοι οι τομείς που προαναφέραμε συνδέονται μεταξύ τους με αποτέλεσμα η οποιαδήποτε ανωμαλία στον ένα να επηρεάζει και τους υπόλοιπους. Παράλληλα όλες έχουν κύριο αντίκτυπο στην οικονομία. Σύμφωνα με τον Richard Clarke, πρώην σύμβουλο ασφαλείας της Αμερικανικής κυβέρνησης σε θέματα Τρομοκρατίας, σε περίπτωση που τρομοκράτες θελήσουν να πραγματοποιήσουν μια εκτεταμένη cyber επίθεση, η οικονομία θα αποτελούσε το βασικό τους στόχο. Παρακάτω θα αναφέρουμε ορισμένα παραδείγματα των τρωτών σημείων που εμφανίζουν αυτές οι υποδομές ξεκινώντας από τον οικονομικό-τραπεζικό τομέα.

1.8.8.1 Τραπεζικά και οικονομικά Ιδρύματα

Στηρίζονται όλο και περισσότερο στους Η/Υ και τα δίκτυα. Αυτό έχει ως συνέπεια να εμφανίζουν τρωτά σημεία τα οποία μπορούν να χρησιμοποιηθούν για DoS ή DDoS επιθέσεις για παράδειγμα. Όμως τα δίκτυα που χρησιμοποιούνται είναι κυρίως ιδιωτικά – εταιρικά και intranets με περιορισμένη εξωτερική σύνδεση π.χ. στο Διαδίκτυο, επομένως και με μικρές πιθανότητες να δεχτούν κάποιου είδους εξωτερική επίθεση.

1.8.8.2 Υποδομές πετρελαίου και φυσικού αερίου

Επιπλέον όλες **οι υποδομές πετρελαίου και φυσικού αερίου** ελέγχονται από συστήματα όπως τα SCADA και τα EMS (Energy Management Systems), τα οποία χρησιμοποιούν λειτουργικά συστήματα εμπορικού τύπου. Πληροφορίες γι' αυτά μπορεί κάποιος πολύ εύκολα να αναζητήσει σε μια βιβλιοθήκη ή στο Διαδίκτυο. Άρα τα σημεία αδυναμίας τους εύκολα εντοπίζονται από επίδοξους τρομοκράτες ή hackers. Μια τέτοιου είδους επίθεση και μάλιστα επιτυχημένη μπορεί να προκαλέσει αλυσιδωτές πολιτικές, οικονομικές και κοινωνικές αντιδράσεις από τον τομέα των μεταφορών ως την καθημερινότητα του πολίτη. Ενδεικτικά να αναφέρουμε δύο επίσημα καταγεγραμμένα περιστατικά το 1992 και το 1999 στις εταιρείες CHEVRON και GAZPROM αντίστοιχα. Στην πρώτη περίπτωση δυσαρεστημένος υπάλληλος προκάλεσε κατάρρευση των συστημάτων ασφαλείας των μονάδων αποθήκευσης σε 22 πολιτείες των ΗΠΑ. Στη δεύτερη, Ρώσος hacker κατάφερε με βοήθεια μέσα από την εταιρεία, να τοποθετήσει ένα Trojan Horse με τα οποίο ήλεγχε τη ροή φυσικού αερίου των αγωγών της.

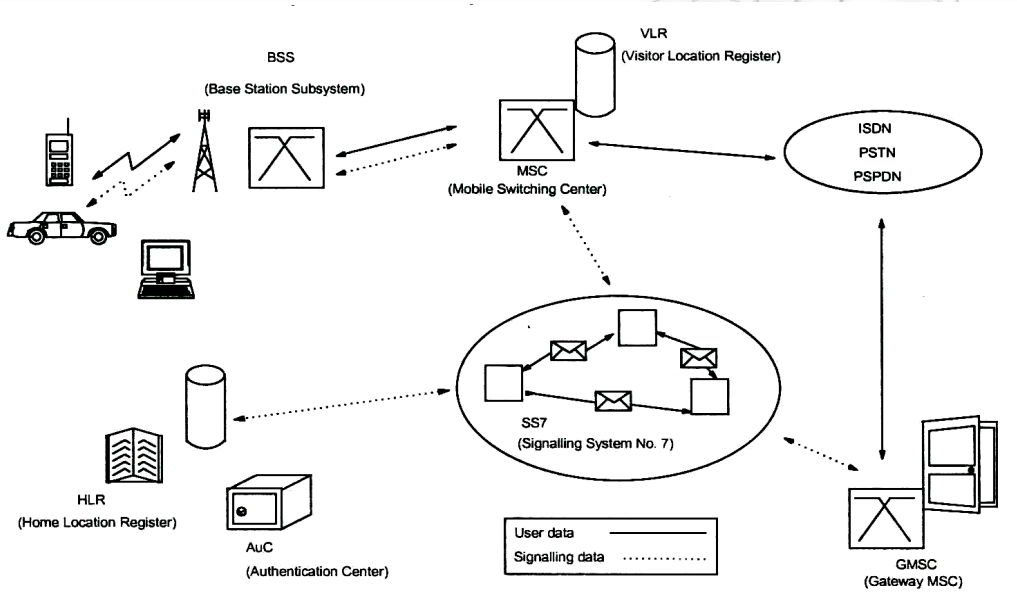
1.8.8.3 Υποδομές Νερού και Ηλεκτρικής Ενέργειας

Ένα άλλο χαρακτηριστικό παράδειγμα αποτελούν οι υποδομές ύδρευσης και άρδευσης καθώς και αυτές της παραγωγής και διανομής ηλεκτρικής ενέργειας. Ο έλεγχος των αποθεμάτων και της ποιότητας του νερού γίνεται με μηχανικά μέσα ενώ απαιτείται φυσική φύλαξη των πηγών νερού αλλά και εγρήγορση σε θέματα πιθανών cyber επιθέσεων. Οι κίνδυνοι αυξάνουν στην περίπτωση μιας κρίσης ή ενός πολέμου. Στο Queensland της Αυστραλίας συνελήφθη ντόπιος επιχειρηματίας με την κατηγορία της επίθεσης στο ηλεκτρονικό σύστημα διαχείρισης των αποβλήτων της πόλης. Η εταιρεία του είχε αναλάβει συμβόλαιο για καθαρισμό του ποταμού της πόλης από τα λήμματα που είχαν διαρρεύσει 264.000 gallons, είχαν πέσει στο ποτάμι εξαιτίας 40 συνολικά επιθέσεων που ο ίδιος επιχειρηματίας είχε εκτελέσει. Από την άλλη πλευρά η ηλεκτρική ενέργεια παράγεται και μεταφέρεται με πλήρως αυτοματοποιημένα μέσα τα οποία ελέγχονται από Η/Υ. Το 2003 ένας slammer virus χτύπησε το σύστημα ελέγχου του Πυρηνικού Εργοστασίου παραγωγής Ηλ.Ενέργειας στο Davis Besse του Οχάιο, με αποτέλεσμα να τεθεί εκτός για πέντε ώρες για λόγους ασφαλείας.

1.8.8.4 Τηλεπικοινωνίες

Το τελευταίο παράδειγμα που θα αναλύσουμε αναφέρεται στις τηλεπικοινωνιακές υποδομές και την καίρια σημασία τους σε όλες τις εκφάνσεις της σύγχρονης ζωής. Έτσι ενδεικτικά περιλαμβάνουμε:

i. Ασύρματα Δίκτυα Ευρείας Περιοχής, όπως το δίκτυο GSM ΚΑΙ 3G



ΕΙΚΟΝΑ 27: Τα στοιχεία του δικτύου GSM

Το σύστημα GSM σχεδιάσθηκε και αναπτύχθηκε εξολοκλήρου στην Ευρώπη πριν επεκταθεί στον υπόλοιπο κόσμο. Η σχεδίασή του άρχισε το 1982 και λειτούργησε το 1992 ως το πρώτο ψηφιακό κυψελωτό σύστημα κινητών επικοινωνιών. Τα βασικά δομικά χαρακτηριστικά, όπως φαίνονται και στο παραπάνω σχήμα, του συστήματος GSM είναι ο **Κινητός Σταθμός** (Mobile Station, MS) και το **Δημόσιο Επίγειο Δίκτυο Κινητών Επικοινωνιών** (Public Land Mobile Network, PLMN). Ο Κινητός Σταθμός διαχωρίζεται στην **Κινητή Συσκευή** (Mobile Equipment, ME) και στην **Κάρτα Ταυτότητας Συνδρομητή**, γνωστότερη ως **κάρτα SIM** (Subscriber Identity Module). Ο κυριότερος στόχος κατά την σχεδίαση της ασφάλειας του συστήματος GSM ήταν να γίνει το σύστημα τόσο ασφαλές όσο και το Σταθερό Δίκτυο Επικοινωνιών (PSTN). Το κυριότερο πρόβλημα προς αυτή την

κατεύθυνση και συγχρόνως η «αχίλλειος πτέρνα» του συστήματος, είναι η μετάδοση των δεδομένων μέσω του αέρα. Η ασφάλεια του GSM σχεδιάστηκε έχοντας τρεις περιορισμούς κατά νου:

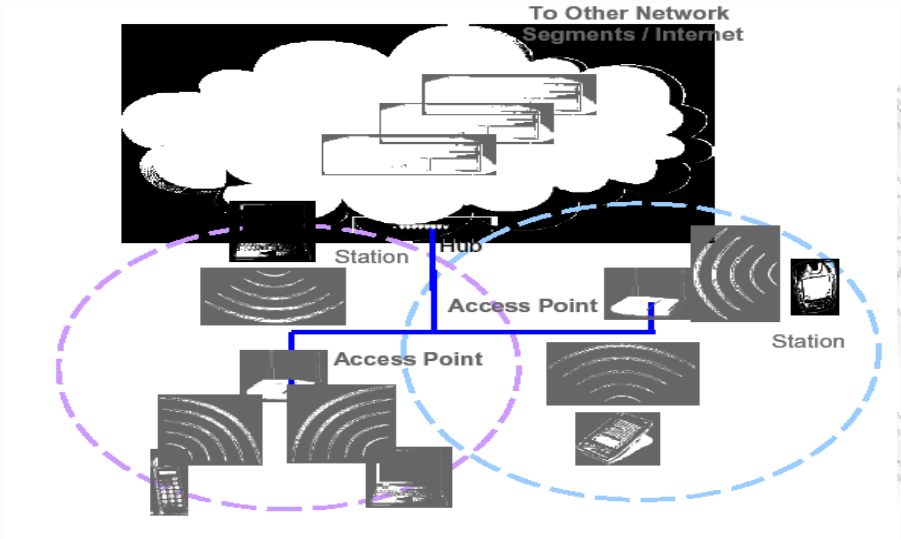
• Να μην εισαχθούν τόσοι πολλοί παράμετροι ασφάλειας ώστε να δημιουργηθούν εξωγενή προβλήματα στο σύστημα.

• Το σύστημα δεν έπρεπε να προστατεύεται από «ενεργές επιθέσεις», όπου ο «επιτιθέμενος» παρεμβαίνει στη λειτουργία του συστήματος, παρουσιάζοντας ίσως τον εαυτό του ως οντότητα του συστήματος, αφού πιστευόταν ότι κάτι ήταν πολύ δύσκολο να γίνει.

• Η εμπιστοσύνη μεταξύ των διαχειριστών σε ότι αφορά την ασφάλεια έπρεπε να ελαχιστοποιηθεί. Τα τεχνικά μέσα για την ασφάλεια του συστήματος είναι μόνο ένα μικρόμερος της συνολικής εικόνας. Η μεγαλύτερη απειλή προέρχεται από σχετικά απλές «επιθέσεις», όπως αποκάλυψη κλειδιών που χρησιμοποιούνται για κρυπτογράφηση, ανασφαλές σύστημα χρέωσης ή δολιοφθορά. Απαιτείται μια ισορροπία ανάμεσα στο κόστος και την αποτελεσματικότητα των διάφορων μέτρων που λαμβάνονται για να αποφευχθούν οι παραπάνω κίνδυνοι.

ii. Τοπικά Δίκτυα - LAN (Local Area Network) αλλά και Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Network), Δίκτυα MAN (Metropolitan Area Network).

iii. Τα WLANs παρέχουν μεγαλύτερη ευελιξία και φορητότητα, λόγω της χρήσης των σημείων πρόσβασης (Access Points – APs) για την σύνδεση των υπολογιστών και άλλων εξαρτημάτων στο δίκτυο, σε σύγκριση με τα παραδοσιακά τοπικά ενσύρματα δίκτυα (Local Area Networks - LANs), τα οποία χρησιμοποιούν καλώδια.



ΕΙΚΟΝΑ 28 :Η τοπολογία ενός Δικτύου WLAN

Οι επιθέσεις που είναι δυνατόν να δεχτεί ένα τέτοιο δίκτυο μπορούν να ταξινομηθούν σε τέσσερις βασικές κατηγορίες:

1) Λήψη πληροφοριών (snooping/foot printing). Η λήψη πληροφοριών αναφέρεται στην πρόσβαση σε απόρρητα και ευαίσθητα δεδομένα ενός δικτύου από μη εξουσιοδοτημένους χρήστες. Για την αντιμετώπιση τέτοιων καταστάσεων χρησιμοποιείτε η μέθοδος της κρυπτογράφησης. Στην περίπτωση αυτή απαιτείται η γνώση από την πλευρά του επίδοξου εισβολέα του μυστικού κλειδιού κρυπτογράφησης ή κάποια ευφυής τεχνική για την ανάκτηση των πληροφοριών από τα κρυπτογραφημένα δεδομένα.

2) Τροποποίηση Δεδομένων. Παράδειγμα τέτοιου είδους επίθεσης είναι η αλλαγή της διεύθυνσης IP του παραλήπτη στην επικεφαλίδα ενός μηνύματος, με αποτέλεσμα να προωθηθεί σε κάποιο κακόβουλο χρήστη εκτός της κρυπτογραφημένης ασύρματης ζεύξης, αντί για τον αρχικό προορισμό. Έτσι ενώ η τροποποίηση του ίδιου του περιεχομένου ενός μηνύματος δεν είναι πάντοτε εφικτή, δεν ισχύει το ίδιο για παραμέτρους που έχουν σαφώς περιορισμένο σύνολο δυνατών τιμών όπως η επικεφαλίδα της IP που προαναφέραμε.

3) Μεταμφίεση. Ο όρος αυτός αναφέρεται στην περίπτωση κατά την οποία η δικτυακή συσκευή ενός κακόβουλου χρήστη παριστάνει μια άλλη έγκυρη

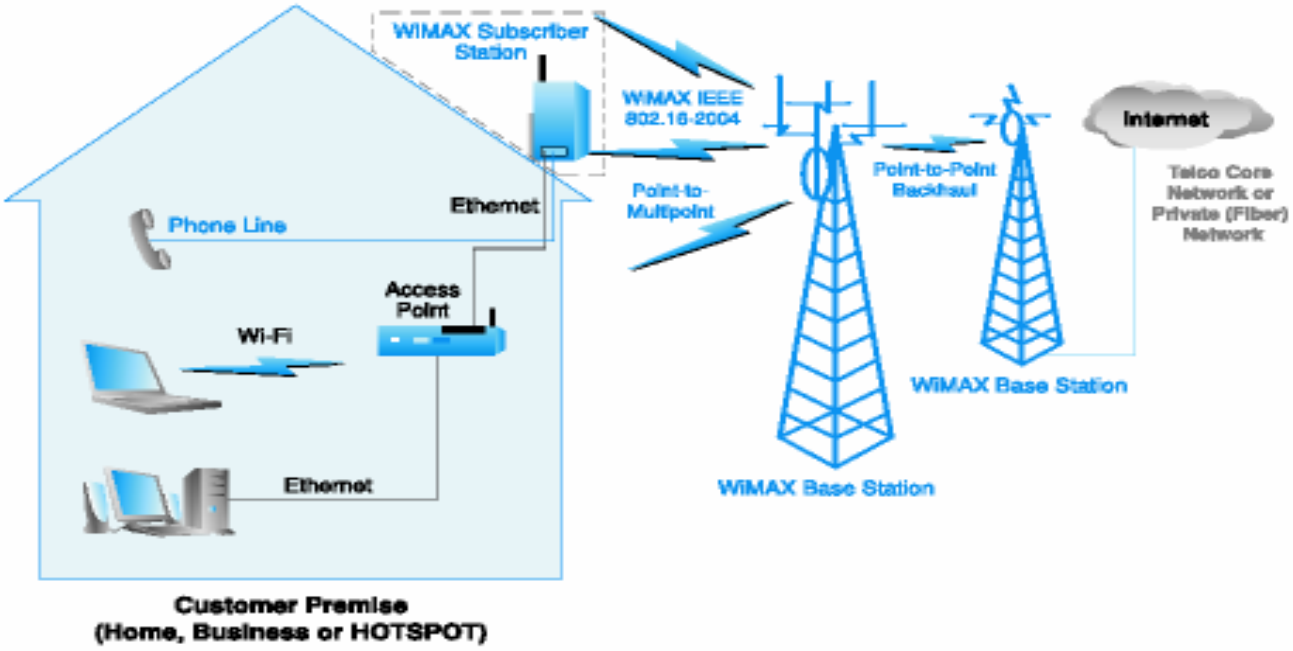
συσκευή. Από τη στιγμή που η συσκευή κατορθώσει να αναγνωρισθεί ως νόμιμη, ο κακόβουλος χρήστης αποκτά όλα τα δικαιώματα που παρέχει το δίκτυο στα εξουσιοδοτημένα μέλη του.

4) Άρνηση Υπηρεσιών. Η επίθεση αυτή διαφέρει από τις προηγούμενες, τόσο όσον αφορά τεχνική όσο και τους στόχους της. Έτσι ενώ στις άλλες ο κακόβουλος χρήστης αποκτά επιπλέον δικαιώματα, κατά την επίθεση άρνησης υπηρεσιών αφαιρούνται τα δικαιώματα από όλους τους χρήστες νόμιμους και μη. Το αντικείμενο μιας επίθεσης DoS είναι η διαταραχή της ομαλής λειτουργίας που αποτελεί στόχος. Έτσι όπως αναφέραμε και σε προηγούμενη παράγραφο, στέλνοντας ένα μεγάλο αριθμό αιτήσεων σε ένα εξυπηρετητή ιστού, εξαντλούνται οι πόροι του τελευταίου του τελευταίου, με αποτέλεσμα να μην μπορούν να εξυπηρετηθούν οι έγκυρες αιτήσεις. Ειδικά στις περιπτώσεις των ασύρματων τοπικών δικτύων οι επιθέσεις DoS υλοποιούνται σχετικά εύκολα και είναι σχεδόν αδύνατο να αποτραπούν.

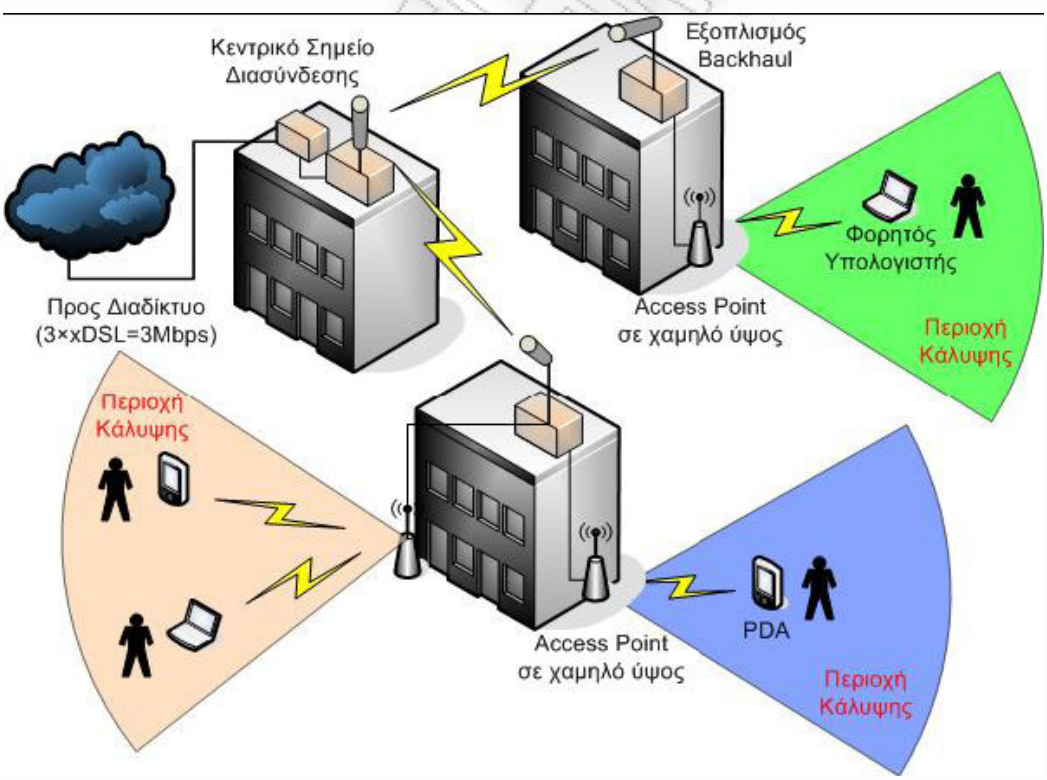
Φυσικά υπάρχουν και οι περιπτώσεις συνδυασμού των ανωτέρω μορφών επίθεσης

iv. Δίκτυα WiFi και WiFi Max

Ένα ασύρματο MAN δίκτυο βασισμένο στο ασύρματης δια επαφής πρότυπο WiMAX διαμορφώνεται με τον ίδιο σχεδόν τρόπο με ένα παραδοσιακό κυψελωτό δίκτυο, με στρατηγικά τοποθετημένους σταθμούς βάσεως. Χρησιμοποιεί μια point-to-multipoint (PMP) αρχιτεκτονική για να παρέχει υπηρεσίες σε μια ακτίνα αρκετών χιλιομέτρων (ανάλογα με τη συχνότητα). Σε περιοχές με υψηλές πυκνότητες πληθυσμού η εμβέλεια περιορίζεται γενικά από τη χωρητικότητα λόγω του περιορισμού στο διαθέσιμο φάσμα. Αυτά τα δίκτυα χρησιμοποιούνται σε μια σειρά από εφαρμογές όπως: τραπεζικά δίκτυα, δίκτυα ασφαλείας π.χ. Πυροσβεστικής, Ε.Κ.Α.Β., δίκτυα εκπαίδευσης απομακρυσμένων περιοχών, δίκτυα σύνδεσης Πανεστιμιουπόλεων, σύνδεση αγροτικών περιοχών.



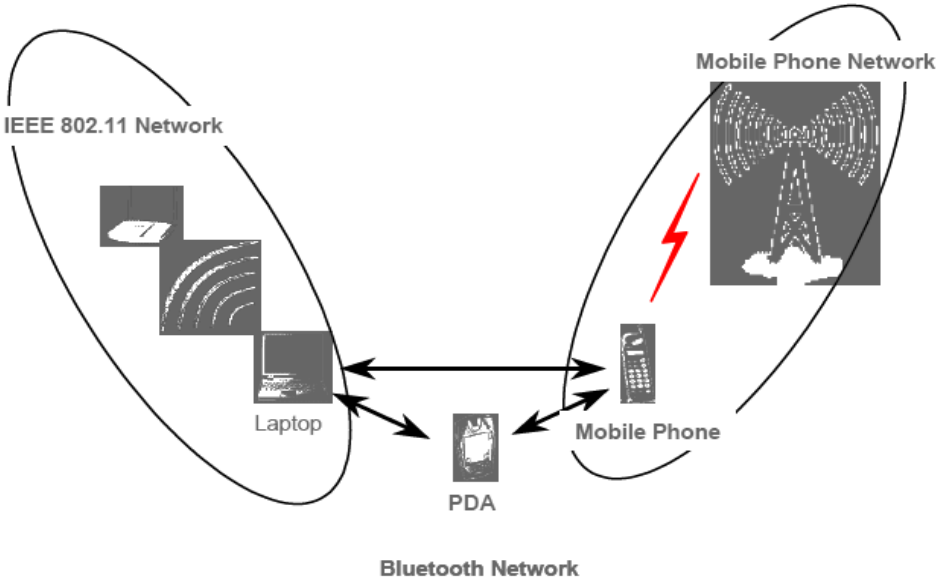
ΕΙΚΟΝΑ 29 :Τοπολογία του δικτύου WiFi Max σε αστικό περιβάλλον



ΕΙΚΟΝΑ 30: Λειτουργία Ασύρματου Δικτύου WiFi

v. Ασύρματα Ιδιωτικά Δίκτυα , όπως τεχνολογίες Bluetooth και I.R. Το Bluetooth είναι ένα απλό peer-to-peer πρωτόκολλο που δημιουργείται για να συνδέσει κινητές πληροφοριακές συσκευές πολλαπλών χρηστών (κυψελοειδή τηλέφωνα, lap-top, φορητούς υπολογιστές, ψηφιακές φωτογραφικές μηχανές, και εκτυπωτές). Παρουσιάζει μεγάλη εξάπλωση σε ιδιαίτερα σε νεαρότερες ηλικίες. Χρησιμοποιεί το IEEE 802.15 πρωτόκολλο στη ζώνη 2,4 έως 2,5 GHz με την τεχνολογία FHSS. Οι κινητές συσκευές που διαθέτουν Bluetooth αποφεύγουν την παρέμβαση από άλλα σήματα κάνοντας hopping σε μια νέα συχνότητα αφού διαβιβάσουν ή να λάβουν ένα πακέτο. Το Bluetooth σχεδιάστηκε για να επιτρέπει απλές, ασύρματες συνδέσεις χαμηλού εύρους ζώνης, χρησιμοποιώντας μια μεγάλης ταχύτητας, χαμηλής ισχύος ασύρματη τεχνολογία συνδέσεων μικροκυμάτων. Επειδή η τεχνολογία Bluetooth δεν έχει καμία απαίτηση οπτικής επαφής (αντίθετα από τις υπέρυθρες), μπορεί να λειτουργήσει μέσω των τοίχων ή από μέσα από έναν χαρτοφύλακα. Τα φορητά PC μπορούν να μεταφέρουν δεδομένα σε άλλο PC ή PDA, με τους εκτυπωτές ή να επικοινωνήσουν με κυψελοειδή δίκτυα για ασύρματη WAN πρόσβαση στα εταιρικά δίκτυα ή /και το Διαδίκτυο.

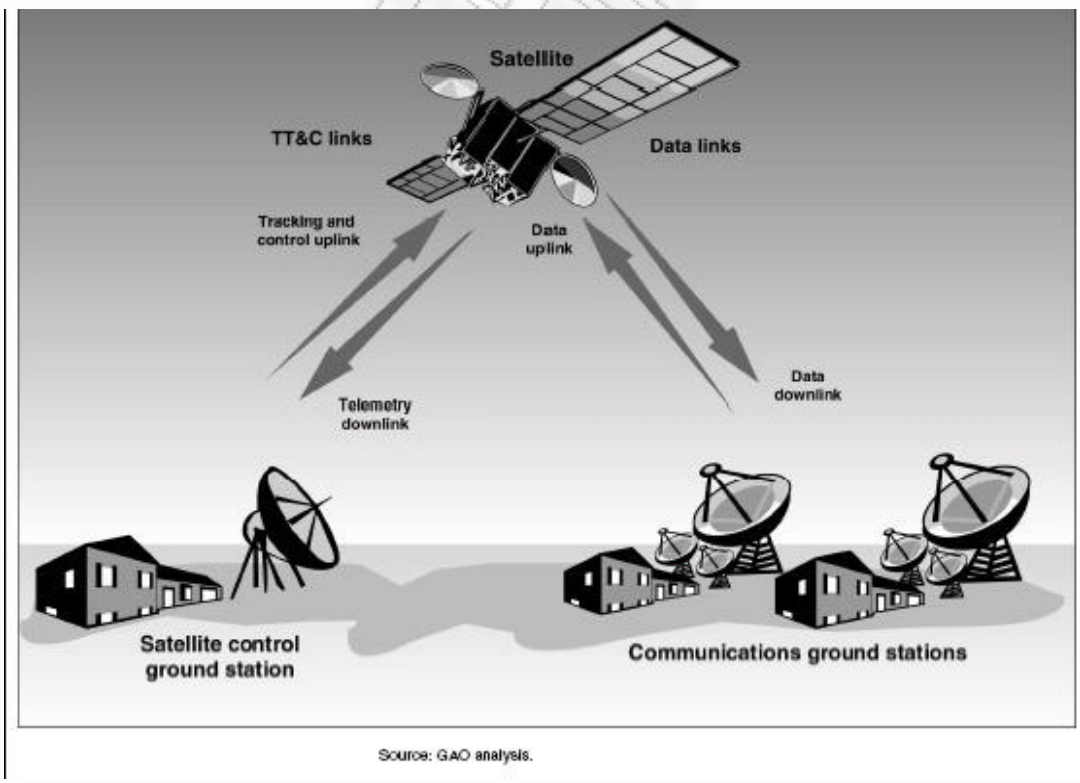
vi. Ad-Hoc Δίκτυα



ΕΙΚΟΝΑ 31:Ad-Hoc Δίκτυο για PDA

Τα Ad hoc δίκτυα, όπως τα Bluetooth, είναι δίκτυα σχεδιασμένα ώστε να συνδέουν δυναμικά απομακρυσμένες συσκευές όπως κινητά τηλέφωνα, φορητούς υπολογιστές (laptops), και PDAs. Αυτά τα δίκτυα ονομάζονται "ad hoc" εξαιτίας των ευέλικτων δικτυακών τοπολογιών τους.

vii. Δορυφορικές επικοινωνίες .Ένα Δορυφορικό Σύστημα Εμπορική χρήσης αποτελείται κυρίως από δύο βασικά συστατικά τον Σταθμό Βάσεως και το Tracking-control link και το data link των δορυφόρων όπως φαίνεται και στην παρακάτω εικόνα. Στις χρήσεις των δορυφόρων στηρίζονται μια μεγάλη ομάδα εφαρμογών όπως οι Στρατιωτικές Επικοινωνίες, η εμπορική ναυτιλία με τα δορυφορικά συστήματα επικοινωνίας, η μετάδοση τηλεοπτικών προγραμμάτων σε απομακρυσμένες περιοχές κ.α. Οι απειλές που αντιμετωπίζουν αυτής της κατηγορίας οι επικοινωνίας είναι οι εξής (1) από την ξηρά και (2) από το διάστημα. Οι επιθέσεις που πιθανόν να δεχτούν μπορεί να είναι φυσική καταστροφή των Σταθμών βάσεως, laser guns, βόμβές ηλεκτρομαγνητικού παλμού, space mines κ.ά., αλλά κυρίως εκτέλεση jamming, η χρήση malicious software (π.χ. computer



ΕΙΚΟΝΑ 32 : Τα συστατικά μέρη ενός δορυφορικού δικτύου

virus), επιθέσεις denial of service, spoofing και υποκλοπή και διαφθορά πληροφοριών και βάσεων δεδομένων του δορυφορικού συστήματος. Η κύρια μέθοδος προστασίας αυτής της κατηγορίας τηλεπικοινωνιακών υποδομών είναι η χρήση κρυπτοκάλυψης, όπως γίνεται στα στρατιωτικά τηλεπικοινωνιακά δίκτυα. Όμως σύμφωνα με την NSA η πλειοψηφία των εμπορικών δορυφορικών συστημάτων είναι σχεδιασμένα για "ελεύθερη πρόσβαση" που σημαίνει πρακτικά ότι το σήμα τους μεταδίδεται παγκοσμίως και χωρίς την οποιαδήποτε προστασία από υποκλοπή ή παραχάραξη. *(77)*

Στα πλαίσια της αναλύσεως μας στο κεφάλαιο αυτό για την απειλή που υφίστανται οι κρίσιμες υποδομές ενός κράτους, θα πρέπει να κάνουμε την παρακάτω διαπίστωση. Στις περισσότερες περιπτώσεις η διάκριση ανάμεσα στην φυσική και την cyber ασφάλεια των υποδομών είναι αδύνατη. Παραδείγματος χάριν, η φυσική ασφάλεια των μονάδων παραγωγής ηλεκτρικής ενέργειας περιλαμβάνει στοιχεία όπως τη θέση των ηλεκτρογεννητριών. την τοπολογία του δικτύου, τους πίνακες διανομής και τα κτίρια όπου στεγάζονται. Από την άλλη πλευρά το computer hardware και τα δίκτυα επικοινωνίας που ελέγχουν την παραγωγή και τη διανομή του ηλεκτρικού ρεύματος θεωρούνται φυσικά ή ηλεκτρονικά (cyber) μεγέθη. Η απόλυτη ερμηνεία της φυσικής ασφάλειας σημαίνει την προστασία των υλικών (συμπεριλαμβανομένου και των Η/Υ και δικτύων) και υποδομών από καταστροφές όπως έκρηξη, φωτιά, σεισμός κ.ά. Έτσι η cyber ασφάλεια θα μπορούσε να σημαίνει την φυσική προστασία των cyber στοιχείων. Αντίθετα περιλαμβάνει την προστασία τόσο φυσικών όσο και cyber στοιχείων όπως την αδυναμία λειτουργίας τους και τη διαφθορά τους από μη εξουσιοδοτημένους χρήστες. *(78)* Επομένως απαιτείται συνδυασμός μια σειράς μέτρων για την εξασφάλιση των υποδομών από αντισεισμικότητα των κτιρίων έως firewall software, αλλά και μιας σειράς υπηρεσιών, Υπουργείων και ανθρώπων για την επιτυχή εφαρμογή αυτών.

1.8.9 Ο οικονομικός αντίκτυπος των Cyber Attacks

Στο προηγούμενο κεφάλαιο αναλύσαμε τις κρίσιμες υποδομές και την απειλή που αυτές δέχονται από την Κυβερνοτρομοκρατία. Οι επιθέσεις που μπορούν να δεχτούν όπως και κάθε άλλος χρήστης της τεχνολογίας των Η/Υ έχουν ως εκτός των άλλων και οικονομικό κόστος. Εδώ θα αναλύσουμε το κόστος των επιθέσεων χρησιμοποιώντας ως πηγή αναφοράς τις ΗΠΑ στις οποίες, ιδιαίτερα μετά την 11/9, υπάρχει πλήρης καταγραφή των ανάλογων στοιχείων χωρίς όμως να αναλύσουμε τις μεθόδους κοστολόγησης των επιθέσεων.

1.8.9.1 Virus –Worms και κόστος

Όλοι όσοι ασχολούνται με την ασφάλεια των Η/Υ και των δικτύων σε πολλές περιπτώσεις καλούνται να απαντήσουν στο ερώτημα του οικονομικού κόστους που έχει η δράση ενός ιού. Παράλληλα με τον τρόπο δικαιολογούν και το κόστος των μέτρων που απαιτούνται για την αντιμετώπιση τους. Σύμφωνα με το (79) ο πιο καταστροφικός οικονομικά ιός μέχρι σήμερα θεωρείται ο 2000 "I Love You" virus, οι επιθέσεις του οποίου προκάλεσαν ζημιά 8,75 δισεκατομμυρίων δολαρίων $. Ακολουθούν κατά σειρά ο Code Red virus (2,62 δισεκατομμύρια δολάρια $), ο Sir Cam virus (1,15 δισεκατομμύρια δολάρια $) και ο Nımda virus (0,635 δισεκατομμύρια δολάρια $) συμπληρώνοντας την τριάδα των πιο επιζήμιων ιών. Επιπλέον έχει δημοσιευθεί και ο παρακάτω πίνακας:

ΕΤΟΣ	Κόστος σε δις. δολάρια ΗΠΑ	ΕΤΟΣ	Κόστος σε δις. δολάρια ΗΠΑ
1995	0,5	**2000**	17,1
1996	1,8	**2001**	13,2
1997	3,3	**2002**	11,1
1998	6,1	**2003**	12,5

Πίνακας 2: Πίνακας Κόστους από επιθέσεις Virus /Worms βασισμένο στο Computer Economics Inc. *Security Issues: Virus Costs Are Rising Again.*

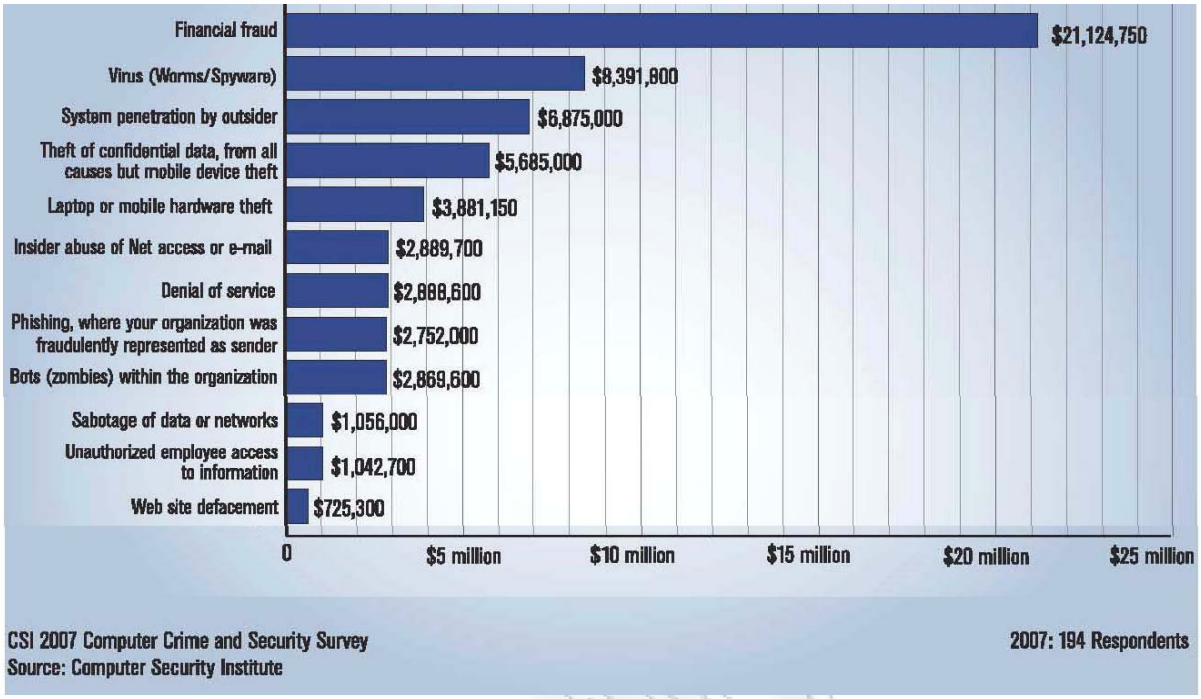
1.8.9.2 Οι υπόλοιπες κατηγορίες Cyber Επιθέσεων και κόστος

Ένα άλλο ενδιαφέρον σημείο που πρέπει να εξετάσουμε είναι το οικονομικό κόστος για οργανισμούς και εταιρίες των υπόλοιπων μορφών cyber επιθέσεων όπως DoS, DDoS, spoofing κ.ά. Έχουμε αναφέρει σε προηγούμενη παράγραφο αυτής της εργασίας ότι DDoS επίθεση είχαμε εναντίον του web-site του Διεθνούς καναλιού CNN καθώς και εναντίον του δημοφιλούς Yahoo. Οι οικονομικές απώλειες δεν περιορίζονται μόνο την περίοδο της επιθέσεως αλλά φτάνουν και σε μακροπρόθεσμα επίπεδα από την απώλεια εμπιστοσύνης των

πελατών και δυσφήμησης της συγκεκριμένης υπηρεσίας. Η πιο επιτυχημένες επιθέσεις αναμφισβήτητα είναι αυτές που εκτελούνται "από μέσα", δηλαδή από ανθρώπους που έχουν ήδη πρόσβαση στις βάσεις δεδομένων και το δίκτυο μιας εταιρείας ή ενός οργανισμού. Σε μια τέτοια περίπτωση υπάλληλος της εταιρείας Bridgeport N.J κατάφερε να τοποθετήσει μια software time bomb στον administrator του συστήματος της εταιρείας, προκαλώντας απώλειες της τάξης των 10 εκατομμυρίων $ και 2 εκατομμυρίων $ για την αποκατάσταση της βλάβης. Το ίδρυμα Mi2G της Βρετανίας έχει δημοσιεύσει τον παρακάτω πίνακα ο οποίος περιλαμβάνει εκτιμώμενο κόστος επιθέσεων όπως hacking, χρήση malicious software, spamming, DoS attacks και DDoS attacks αλλά και τον οικονομικό αντίκτυπο από την απώλεια της εμπιστοσύνης των πελατών κατά εκτίμηση. Παράλληλα παρατίθεται και δημοσιευμένο γράφημα Computer Security Institute για το έτος 2007 για ο κόστος των cyber επιθέσεων διαφόρων μορφών.

ΕΤΟΣ	**Κόστος σε δις. δολάρια $ ΗΠΑ**		**ΕΤΟΣ**	**Κόστος σε δις. δολάρια $ ΗΠΑ**	
	LOWER	**UPPER**		**LOWER**	**UPPER**
1996	0,8	1,0	**2001**	33	40
1997	1,7	2,9	**2002**	110	130
1998	3,8	4,7	**2003**	185	226
1999	19	23	**2004**	46	56
2000	25	30			

Πίνακας 3.:Πίνακας Κόστους από ηλεκτρονικές επιθέσεις κάθε είδους 1996-2004 βασισμένο στο Mi2g, *Frequently Asked Questions: SIPS and EVEDA, v1.00,*updated February 6, 2004



ΕΙΚΟΝΑ 33: Το κόστος των Cyber επιθέσεων στις ΗΠΑ για το έτος 2007

1.8.10 Η αντιμετώπιση της απειλής

Με την πάροδο του χρόνου παρατηρείται εξέλιξη των επιθέσεων που πραγματοποιούνται αλλά και αντίστοιχη εξέλιξη των αμυντικών συστημάτων για την αντιμετώπιση της Κυβερνοτρομοκρατίας. Φυσικά υπάρχουν κάποιες γενικές αρχές τις οποίες πάντα θα πρέπει να χρησιμοποιούμε τόσο ως ιδιώτες όσο και ως οργανισμοί/εταιρείες. Καταρχήν θα πρέπει να προσέχουμε τα σημεία πρόσβασης του δικτύου μας. Όπως έχουμε ήδη αναφέρει, ένας τρόπος να συλλέξει κάποιος πληροφορίες για το σύστημα μας είναι να συνδεθεί σε ένα hub στο οποίο βρίσκονται συνδεδεμένα άλλα στοιχεία δικτύου και έτσι να μπορέσει να έχει πρόσβαση σε διάφορα δεδομένα όπως, IP, ARP tables, να γνωρίζει τι υπηρεσίες τρέχουν στο δίκτυο κλπ. Συνεπώς θα πρέπει να είμαστε πολύ προσεκτικοί και να μην αφήνουμε ελεύθερα σημεία πρόσβασης στο δίκτυο μας. Αυτό το πρόβλημα γίνεται περισσότερο εμφανές στα ασύρματα δίκτυα τα οποία από την φύση τους είναι πιο ευάλωτα σε υποκλοπές.

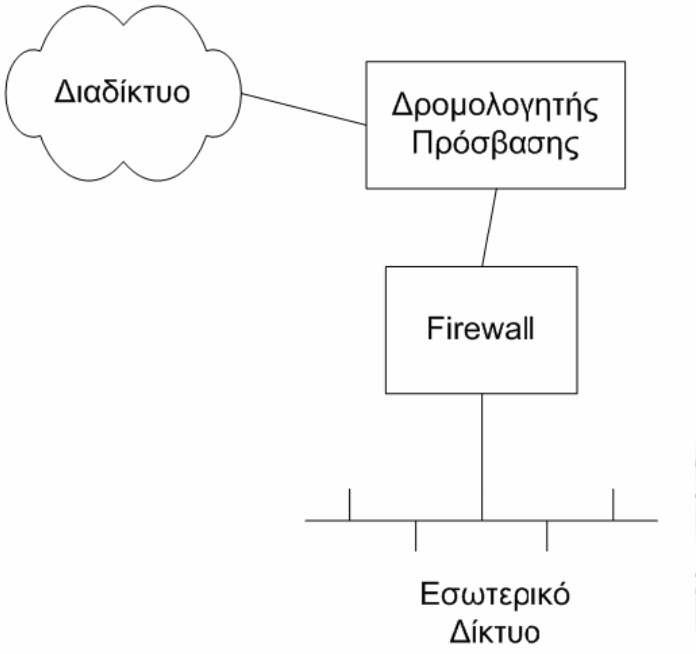
Επομένως πρέπει να είμαστε προσεκτικοί στη διαμόρφωση που χρησιμοποιούμε ενώ είναι σχεδόν επιτακτική η ανάγκη χρήσης κρυπτογραφίας. Στα πρώτα στάδια μιας επίθεσης, ο

επιτιθέμενος προσπαθεί να συλλέξει πληροφορίες σχετικά με το σύστημα. Το IP scan μπορεί να αποφευχθεί αν χρησιμοποιήσουμε IPv6. Στην περίπτωση αυτή ο επιτιθέμενος θα πρέπει να ψάξει σε ένα τεράστιο πλήθος IP διευθύνσεων, γεγονός που καθιστά εξαιρετικά δύσκολή την πραγματοποίηση του IP scan.

Πολλές επιθέσεις μπορούμε να τις αποφύγουμε λαμβάνοντας κάποια απλά διαχειριστικά μέτρα. Για παράδειγμα μια τέτοια τεχνική που θα μας έλυνε το πρόβλημα του IP spoofing είναι η απαγόρευση από τον διαχειριστή του δικτύου να εξέρχεται κίνηση από το δίκτυο με prefix διαφορετικό από αυτό του δικτύου. Ωστόσο αυτή την τεχνική δεν την εφαρμόζουν όλοι οι διαχειριστές για διάφορους λόγους που σχετίζονται κυρίως με την πολιτική που ακολουθείται από κάθε οργανισμό.

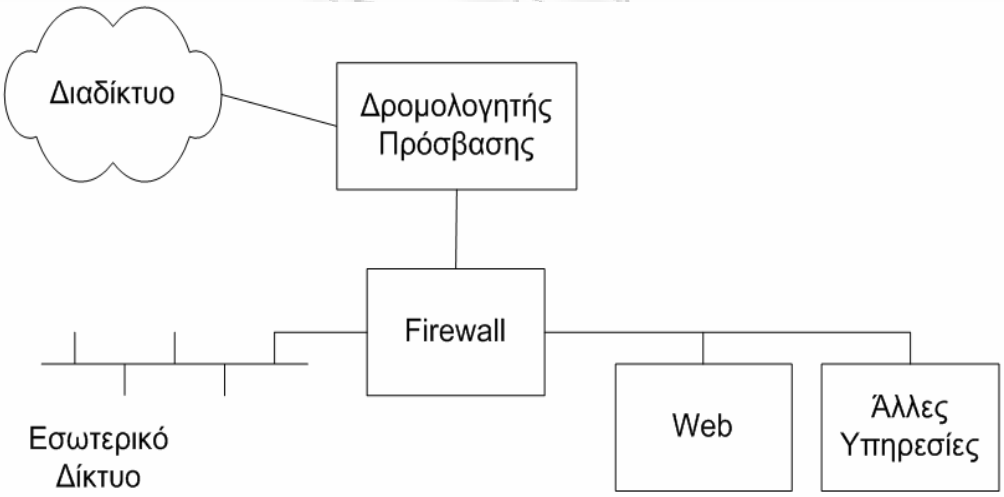
Από τα πιο σημαντικά εργαλεία για δικτυακή προστασία είναι ο firewall. Σύμφωνα με τον Marcus J.Ranum, το δημιουργό του πρώτου firewall, ο firewall είναι "Ένα σύστημα ή συνδυασμός συστημάτων που ελέγχουν την πρόσβαση και παρέχουν *ένα βαθμό ασφαλείας* μεταξύ δικτύων". Ουσιαστικά πρόκειται για ένα δρομολογητή που ελέγχει την κίνηση που περνάει μέσα από αυτόν. Άλλωστε ο πιο απλός firewall είναι ένας δρομολογητής με κατάλληλες access lists.

Για να μπορέσουμε να χρησιμοποιήσουμε με επιτυχία έναν firewall θα πρέπει πρώτα να ορίσουμε την πολιτική ασφαλείας που θα ακολουθήσουμε. Ο firewall δεν είναι τίποτα άλλο παρά ένα σύνολο κανόνων σχετικά με το ποια κίνηση θα επιτραπεί να περάσει στο δίκτυο και ποια όχι. Έτσι μπορούμε να έχουμε δύο πιθανές πολιτικές: τη "σκληρή" πολιτική, συνήθως χρησιμοποιείται στην εισερχόμενη κίνηση στο δίκτυο και στην οποία ορίζουμε ρητά ποια κίνηση θα περάσει από το τείχος και ποια όχι. Έχουμε επίσης τη "χαλαρή" πολιτική στην οποία ορίζουμε ξεκάθαρα την κίνηση που απαγορεύεται να περάσει από το τείχος και επιτρέπουμε οποιαδήποτε άλλη κίνηση. Χωρίς τη χρήση κάποιας πολιτικής είναι απίθανο να είναι αποτελεσματικός ο firewall. Παράλληλα θα πρέπει να καθορισθεί ποιο κομμάτι του δικτύου θα προστατεύει.



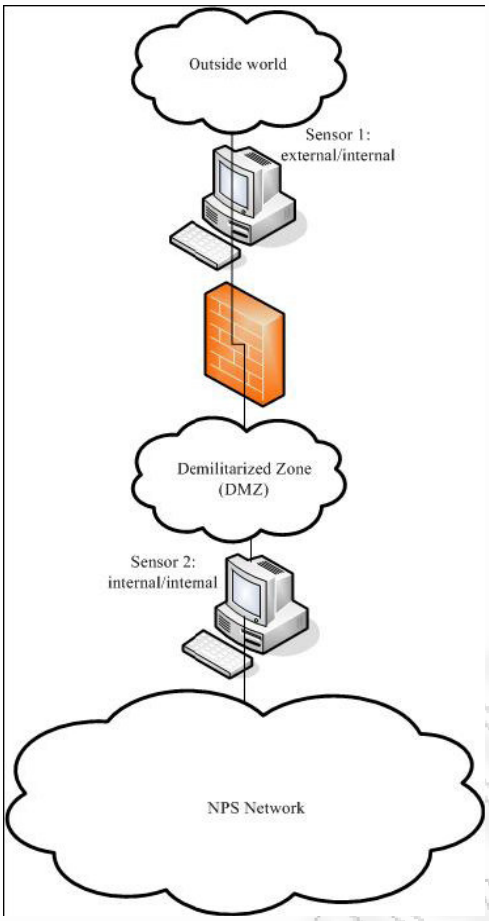
ΕΙΚΟΝΑ 34 : Firewall δικτύου

Στην περίπτωση αυτή ο firewall προστατεύει όλο το δίκτυο. Είναι η πιο απλή περίπτωση, όπου έχουμε τοποθετήσει το τείχος στην είσοδο του δικτύου.



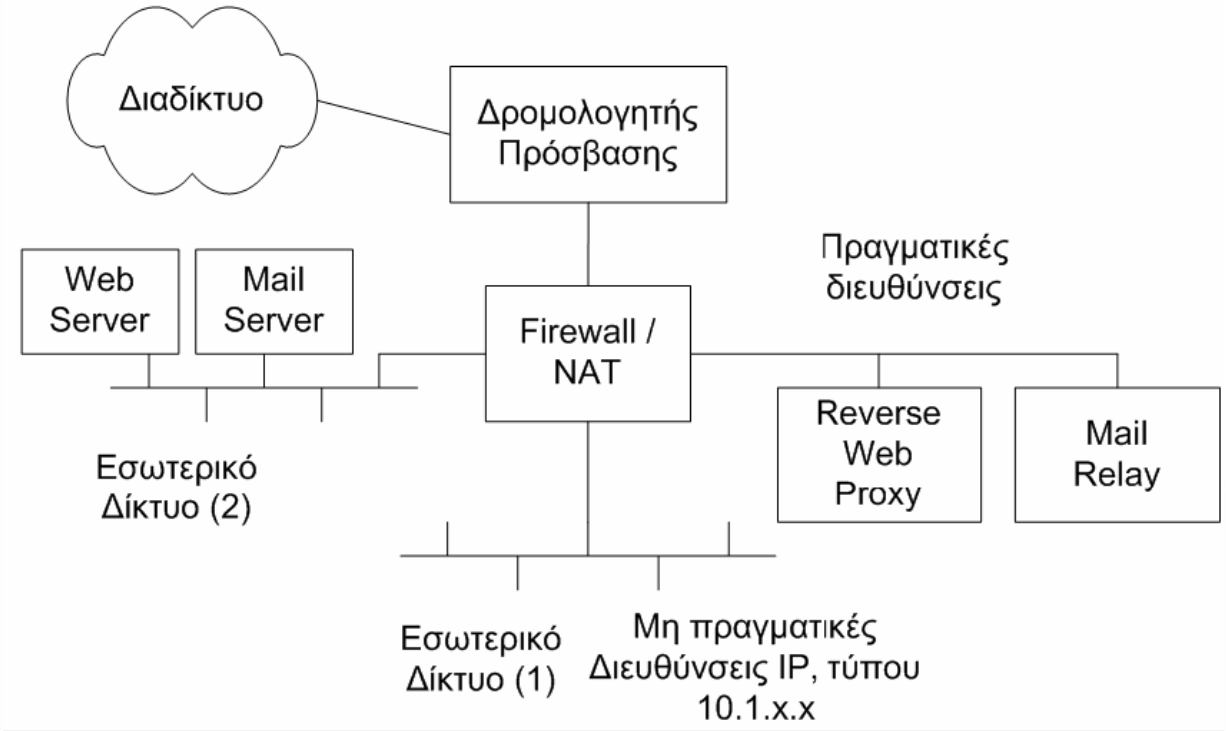
ΕΙΚΟΝΑ 35: Firewall δικτύου 2

Στη δεύτερη περίπτωση έχουμε κάποιο κομμάτι του δικτύου τοποθετημένο στη λεγόμενη αποστρατικοποιημένη ζώνη (demilitarized zone-DMZ).



ΕΙΚΟΝΑ 36: demilitarized zone-DMZ

Έτσι η πρόσβαση για παράδειγμα στο web-server ενώ το εσωτερικό δίκτυο προστατεύεται από εξωτερικές συνδέσεις. Επίσης πολλές φορές η πρόσβαση στα μηχανήματα του εσωτερικού δικτύου δεν είναι επιτρεπτή ούτε από τα μηχανήματα που βρίσκονται στην DMZ. Αντίθετα οι χρήστες του εσωτερικού δικτύου μπορούν να συνδεθούν απρόσκοπτα σε όλα τα εξωτερικά δίκτυα για κάθε επιτρεπόμενη υπηρεσία. Επομένως αυτή η πολιτική παρέχει αυξημένη πρόσβαση σε κάποια συστήματα του δικτύου χωρίς να θέτει σε κίνδυνο το υπόλοιπο.



ΕΙΚΟΝΑ 37 : Firewall δικτύου 3

Στη τρίτη περίπτωση (εικόνα 33) έχουμε πολλές ομοιότητες με την προηγούμενη. Απλά εδώ έχουμε αφήσει "ανοιχτούς" προς το internet proxy servers απαγορεύοντας τις απευθείας συνδέσεις των servers. Έτσι αν πραγματοποιηθεί κάποια επίθεση αυτή θα γίνει σε κάποιον proxy server. Επιπλέον χρησιμοποιώντας NAT μπορούμε να καταστήσουμε τα μηχανήματα του εσωτερικού δικτύου αόρατα στον εξωτερικό κόσμο.

Διαπιστώνουμε λοιπόν, ότι οι firewall αποτελούν συστήματα περιμετρικής άμυνας, δημιουργώντας ένα ιδεατό τείχος που προστατεύει το περικλειόμενο δίκτυο από επιθέσεις. Ωστόσο αυτό δεν αποτελεί πανάκεια μια και δεν μπορεί να αντιμετωπίσει επιτιθέμενους που τοποθετούνται στο εσωτερικό του firewall. Για παράδειγμα μια κοινή τακτική είναι η προσπάθεια του επιτιθέμενου να πείσει τον χρήστη να τρέξει κάποιο κακόβουλο πρόγραμμα παρουσιάζοντας το εξόχως ελκυστικό. Μια τέτοια επίθεση ένας firewall δεν μπορεί να την αντιμετωπίσει.

Πέρα όμως από τα διάφορα "εργαλεία" που μπορούμε να χρησιμοποιήσουμε για την αντιμετώπιση της Κυβερνοτρομοκρατίας, αυτό που πρέπει να έχουμε κατά νου είναι ότι

αποτελεσματική μάχη θα γίνει μόνο αν χρησιμοποιήσουμε μέτρα αντίστοιχα με αυτά για την αντιμετώπιση της "κλασικής" τρομοκρατίας. Επομένως απαιτείται ο συνδυασμός κατάλληλων νομοθετικών πρωτοβουλιών αλλά και εγρήγορση για τον εντοπισμό και την παρακολούθηση επίδοξων cyber terrorist. Άλλωστε τα τελευταία χρόνια τόσο σε εθνικό όσο και στα πλαίσια της Ε.Ε. υπάρχει νομοθετικό έργο για την εξασφάλιση της ασφάλειας όπως ο νόμος 2225/20-07-1994 (Περί προστασίας του απορρήτου των τηλεπικοινωνιών), ο νόμος 2774/22-12-1999 (για την προστασία δεδομένων προσωπικού χαρακτήρα), ο νόμος 2672/1998 (για την διακίνηση εγγράφων με ηλεκτρονικά μέσα) κ.ά.

Στον τομέα των Η/Υ από την άλλη πλευρά μια σύγχρονη μέθοδος αντιμετώπισης των cyber terrorist χρησιμοποιεί honey pots και software decoys. Με τον πρώτο γίνεται η συλλογή στοιχείων για την καλύτερη κατανόηση των επίδοξων εισβολέων. Αν υποθέσουμε έχουμε ένα δίκτυο με αρκετές διαθέσιμες διευθύνσεις, εμείς χρησιμοποιούμε μόνο ορισμένες από αυτές. Στις μη χρησιμοποιούμενες διευθύνσεις μπορούμε να στήσουμε εικονικά μηχανήματα στα οποία θα εγκαταστήσουμε κάποιο λειτουργικό με bugs και έτσι αρχίζει η επίθεση στο εικονικό μηχάνημα. Εμείς μπορούμε να παρατηρούμε λοιπόν τις κινήσεις του και να βλέπουμε τις τεχνικές που χρησιμοποιεί χωρίς να τίθεται σε κίνδυνο το σύστημα μας. Με το δεύτερο προστίθενται και άλλα επίπεδα αμύνης εναντίον των επιτιθέμενων μέσω της παραπλάνησης τους. Οι παραπάνω όροι θα αναλυθούν στα επόμενα κεφάλαια.

ΚΕΦΑΛΑΙΟ ΙΙ: ΠΑΡΑΠΛΑΝΗΣΗ

1.9 Μορφές της παραπλάνησης

Η παραπλάνηση στο φυσικό περιβάλλον

Η κύρια εφαρμογή της παραπλάνησης συναντάτε στο φυσικό περιβάλλον όπου τις περισσότερες φορές είναι ζήτημα ζωής και θανάτου με την πλήρη έννοια του όρου. Χαρακτηριστικά είναι τα ακόλουθα παραδείγματα: ψάρια που μεταμορφώνονται σε πλάσμα σχήματος μπάλας το οποίο δίνει στους διώκτες τους την εντύπωση ότι είναι απλά μια μικρή μπουκιά, κάμπιες που μεταμορφώνουν το μπροστινό τους μέρος ώστε να μοιάζει με το κεφάλι φιδιού όταν αντιληφθούν ότι βρίσκονται σε κίνδυνο και το "ευρωπαϊκό" φίδι (grass snake) που προσπαθεί να εντοπίσει πιθανούς εχθρούς ξεφυσώντας, προκειμένου να δείχνει μεγαλύτερο ενώ εκτελεί ένα χαρακτηριστικό σφύριγμα πολύ δυνατά. Στη συνέχεια παριστάνει το πεθαμένο γυρνώντας με την κοιλιά προς τα επάνω και βγάζοντας την γλώσσα έξω. *(79)*

Για τα παραπάνω είδη αλλά και για πάρα πολλά ακόμα η παραπλάνηση είναι η κύρια και φυσική τακτική επιβίωσης προσαρμοσμένη στη συμπεριφορά τους, την ανατομία και τη φυσιολογία τους. Φυσικά η παραπλάνηση χρησιμοποιείται πολλές φορές και από τα αρπακτικά είδη, αλλά και από τα φυτά ακόμα.

Η παραπλάνηση στην Ιστορία

" Ο πόλεμος στηρίζεται στην πλάνη", Sun Tzu: Η τέχνη του πολέμου

Η ανθρώπινη ιστορία είναι γεμάτη από μύθους, θρύλους αλλά και πραγματικά γεγονότα εξαπάτησης και δόλου ιδιαιτέρως δε στη στρατιωτική ιστορία. Ένας από τους πιο διάσημους θεωρητικούς της παραπάνω έννοιας είναι ο *Sun Tzu*, αρχαίος Κινέζος φιλόσοφος και στρατιωτικός, ο οποίος στο γνωστό έργο του *«Η τέχνη του πολέμου»,* αναλύει τον τρόπο χρήσης δόλιων μέσων – εξαπάτησης για τη νίκη ενάντια σε πολλές φορές υπέρτερο εχθρό.

Κλασικό παράδειγμα στρατιωτικής επιχείρησης εξαπάτησης, είναι στην Αρχαία Ελλάδα κατά τη διάρκεια του Τρωικού Πολέμου. Σύμφωνα με το μύθο, όπως μας μεταφέρεται

μέσα από τις Ραψωδίες του Ομήρου, οι Έλληνες πολιορκούσαν την πόλη της Τροίας για περίπου δέκα χρόνια χωρίς κανένα αποτέλεσμα. Τότε μετά από πρόταση του πολυμήχανου Οδυσσέα κατασκεύασαν ένα τεράστιο ξύλινο άλογο το οποίο άφησαν έξω από τα τείχη της πόλης, παρουσιάζοντάς το στους Τρώες ως δώρο από τους θεούς. Στο εσωτερικό του κατασκευάσματος αυτού, είχαν κρυφτεί 30 επίλεκτοι Έλληνες στρατιώτες. Οι Τρώες θεωρώντας ότι οι Έλληνες μετά από συνεχή αγώνα δέκα χρόνων είχαν αποσυρθεί, μετέφεραν το άλογο μέσα από τα τείχη της πόλης ως τρόπαιο για τη νίκη τους. Ξεκίνησαν λοιπόν, μια μεγάλη γιορτή προς το τέλος της οποίας υπήρξε μια δυσάρεστη έκπληξη. Οι Έλληνες στρατιώτες βγήκαν από το άλογο και άνοιξαν τις πύλες της πόλης, τα Ελληνικά στρατεύματα που ήταν σε ετοιμότητα εισήλθαν και κατέλαβαν την πόλη οριστικά.

Ακόμα και στη Βίβλο συναντάμε ανάλογα περιστατικό, όπως στο βιβλίο Γένεσης Κεφάλαιο 17. Ο γέροντας και σχεδόν τυφλός Ισαάκ είχε δύο γιους, τους Ιακώβ και Ησάβ. Ο πρώτος θέλοντας να λάβει την ευλογία και την εξουσία από τον πατέρα του τον ξεγέλασε καλύπτοντας το σώμα και το λαιμό του με κομμάτια δέρματος από αρνί. Έτσι με τη βοήθεια της μητέρας του, η οποία είχε διώξει τον έτερο γιο της Ησάβ μακριά για κάποια εργασία, κατάφερε να πάρει τη διαδοχή παριστάνοντας το δασύτριχο αδελφό του.

Με την πάροδο του χρόνου και την εξέλιξη της αμυντικής τεχνολογίας νέα συστήματα και όπλα εμφανίσθηκαν με ακόμα μεγαλύτερη καταστροφική ισχύ. Όμως οι βασικές αρχές της παραπλάνησης και του δόλου σε τακτικό αλλά και επιτελικό επίπεδο και εξακολουθούν να παραμένουν σε ισχύ. Κατά τη διάρκεια του Β΄ Παγκοσμίου Πολέμου η παραπλάνηση από την πλευρά των Συμμαχικών Δυνάμεων υπήρξε συνήθης πρακτική συμβάλλοντας καθοριστικά στη νίκη έναντι των Δυνάμεων του Άξονα, περιορίζοντας τις απώλειες σε υλικό και ανθρώπους, ιδιαίτερα αμάχους. Ο κύριος στόχος αυτής της πρακτικής ήταν η επίτευξη αιφνιδιασμού και απόκρυψης των αντικειμενικών σκοπών, των επιτελικών σχεδίων, των προετοιμασιών και των επιχειρήσεων. Ένα τέτοιο παράδειγμα είναι η επιχείρηση Barclay το 1943 *(79)*.

Η τελευταία σχεδιάσθηκε και εκτελέστηκε με σκοπό να αποκρύψει την επιχείρηση Husky – την εισβολή των Συμμάχων στην Σικελία. Περιλάβανε ψευδείς επιθέσεις και σαμποτάζ στη Νότια Γαλλία και στα Βαλκάνια, την Ελλάδα και κυρίως τη Κρήτη. Έτσι δίνονταν η εντύπωση στο Γερμανικό Γενικό Επιτελείο ότι η εισβολή στην Ευρώπη θα γινόταν

από τα Βαλκάνια, πιθανώς από την Ελλάδα χρησιμοποιώντας ως προγεφύρωμα τη Κρήτη. Αυτό είχε ως αποτέλεσμα οι Γερμανοί να μη μπορούν να αποδεσμεύσουν σημαντικές δυνάμεις, τις οποίες θα μπορούσαν να διαθέσουν για την υπεράσπιση της Ιταλικής χερσονήσου, ενώ παράλληλα ο Ιταλικός Στόλος παρέμενε στη Θάλασσα της Αδριατικής πλησίον της Βαλκανικής.

Μάλιστα για το σκοπό αυτό, οι Σύμμαχοι δημιούργησαν μια ψεύτικη Στρατιά στην ανατολική Μεσόγειο – δηλαδή μόνο στα χαρτιά – την οποία ονόμασαν 12η Στρατιά αποτελούμενη από 12 πλαστές μεραρχίες *(80).* Αυτό έκανε τον Χίτλερ ακόμα πιο ανήσυχο ισχυροποιώντας την πεποίθηση του ότι οι Σύμμαχοι θα εισβάλλουν στην Ευρώπη από τα Βαλκάνια. Οι τελευταίοι φρόντισαν η συγκεκριμένη φήμη να διαδοθεί μέσω ραδιοφωνικών μηνυμάτων, διπλών πρακτόρων και από τον εντοπισμό "τυχαία" χαρτών και διαταγών δράσης για περισσότερη αληθοφάνεια.

Παράλληλα μία ακόμα επιχείρηση λάμβανε χώρα με την κωδική λέξη Επιχείρηση Mincemeat (Κρεατόπιτα). Αυτή αφορούσε την τοποθέτηση ενός ανδρικού πτώματος στις Νότιες ακτές της Ισπανίας. Υποτίθεται ότι ο νεκρός άνδρας ήταν κάποιος σαμποτέρ – αγγελιοφόρος ο οποίος μεταφερόταν με συμμαχικό πλοίο, από το οποίο έπεσε τυχαία και πνίγηκε. Όμως το πιο σημαντικό στοιχείο ήταν ένας χαρτοφύλακας που έφερε το πτώμα και στον οποίο υπήρχαν έγγραφα και χάρτες για επικείμενη εισβολή των συμμαχικών δυνάμεων στην Ευρώπη μέσω Ελλάδας. Αυτά μεταφέρθηκαν μέσω Ισπανίας στη Γερμανία όπου έγιναν πλήρως πιστευτά.

Σύμφωνα μάλιστα με την εκτίμηση της Fremde Heere West (FHW), τη Γερμανική Υπηρεσία Αντικατασκοπείας, τα στοιχεία που βρέθηκαν ήταν απολύτως αληθή κάτι που σύμφωνα και με το Βρετανό ιστορικό Sir Michael Howard έκανε "την επιχείρηση αυτή ίσως την πιο επιτυχημένη επιχείρηση παραπλάνησης κατά το ΄Β Παγκόσμιο Πόλεμο".

Η αναφορά μας στον ΄Β Παγκόσμιο Πόλεμο δε θα ήταν πλήρης, αν δε βλέπαμε και τα παραδείγματα δόλου και εξαπάτησης που χρησιμοποίησε ο Σοβιετικός Στρατός. Οι Σοβιετικοί κατάλαβαν από νωρίς, κατά τη διάρκεια του "Μεγάλου Πατριωτικού Πολέμου", ότι η νίκη εναντίον των έντονα μηχανοποιημένων Γερμανικών Μεραρχιών θα ήταν αδύνατη χωρίς επιχειρήσεις παραπλάνησης, τις λεγόμενες maskirovska. Αυτές, ως κύριο αντικειμενικό σκοπό

είχαν την απόκρυψη μετακίνησης μεγάλου όγκου στρατευμάτων, της συγκέντρωση δυνάμεων και την προετοιμασία επιθέσεων στο αχανές πεδίο μάχης της Ρωσικής στέπας.

Η χρήση τέτοιων τεχνικών έγινε εντονότερη το 1943 με απτά αποτελέσματα στις μάχες του Στάλιγκραντ και του Κούρσο. Συγκεκριμένα στη μάχη του Στάλιγκραντ ήταν η πρώτη πραγματική επιτυχία της maskirovska. Κατά τη διάρκεια της γερμανικής προσπάθειας για την κατάληψη της πόλης, στο τέλος τους χειμώνα του 1942, οι Σοβιετικοί προσποιήθηκαν ότι ετοιμάζονταν για αντεπίθεση στην περιοχή του κεντρικού θεάτρου επιχειρήσεων κοντά στη Μόσχα. Αυτό σε συνδυασμό με την άκαμπτη αντίσταση των Σοβιετικών δυνάμεων στο Στάλιγκραντ, έδωσε στους Γερμανούς την εντύπωση ότι δεν πρόκειται να δεχθούν επίθεση οι εφοδιοπομπές τους στο νότιο τμήμα του μετώπου.

Η Σοβιετική παραπλάνηση κατάφερε να αποκρύψει τη συγκέντρωση 300.000 ανδρών, 1000 τεθωρακισμένων του Κόκκινου Στρατού και 5000 πυροβόλων, τα οποία περικύκλωσαν την Γερμανική 6η Στρατιά. Η επιτυχία της παραπλανητικής κίνησης ήταν τόσο μεγάλη ώστε η Γερμανική Διοίκηση είχε δώσει εντολή για τη μεταφορά 12 Μεραρχιών στην Ομάδα Στρατιών Κέντρο, στον κεντρικό τομέα του μετώπου τα οποία αρχικώς προορίζονταν για την περιοχή του Στάλιγκραντ και του Καυκάσου, αφήνοντας εκτεθειμένες τις γραμμές ανεφοδιασμού και τη νότια πλευρά της με ολέθρια αποτελέσματα.

Εκτός όμως από τον ΄Β Παγκόσμιο Πόλεμο και τη σύγχρονη εποχή, η παραπλάνηση στις στρατιωτικές επιχειρήσεις εξακολουθεί να χρησιμοποιείται παρά τη ραγδαία εξέλιξη των συστημάτων εντοπισμού και παρακολούθησης. Το 1991 κατά τη διάρκεια του Πολέμου του Κόλπου για την απελευθέρωση του Κουβέιτ, είχαμε τέτοιου είδους επιχειρήσεις. Μετά την εισβολή των Ιρακινών δυνάμεων τον Αύγουστο του 1990 στο Κουβέιτ, ξεκίνησε μια αμφίβια προσπάθεια παραπλάνησης με τη χρήση Δυνάμεων Πεζοναυτών και μεγάλου αριθμού πολεμικών πλοίων. Η πλειάδα αυτή των επιχειρήσεων οδήγησε τον Σαντάμ Χουσείν να πιστέψει, ότι η προσπάθεια απελευθέρωσης του Κουβέιτ θα πραγματοποιούνταν με μια αποβατική επιχείρηση στις ακτές του κρατιδίου. Έτσι καθημερινά γίνονταν αεροπορικοί βομβαρδισμοί εναντίον παράκτιων στόχων, επιθέσεις στα Ιρακινά πλοία που βρίσκονταν εντός χωρικών υδάτων του Κουβέιτ και ασκήσεις αμφίβιας εφόδου από τους Πεζοναύτες. Αυτό, είχε ως αποτέλεσμα να τοποθετηθούν στην ακτή 5 Ιρακινές Μεραρχίες αποδυναμώνοντας το υπόλοιπο μέτωπο.

Παράλληλα οι Δυνάμεις της Συμμαχίας κινήθηκαν μέσω Σαουδικής Αραβίας με κατεύθυνση από Βορρά προς Νότο πίσω από τους Ιρακινούς καθηλώνοντας τους απόλυτα. Πιο πρόσφατα κατά τη διάρκεια του πολέμου εναντίον της Γιουγκοσλαβίας η χρήση μεθόδων παραπλάνησης και από τις δύο πλευρές υπήρξε συνεχής και εκτεταμένη. Οι Σερβικές δυνάμεις χρησιμοποίησαν μια μεγάλη γκάμα μεθόδων απόκρυψης για την αντιμετώπιση ενός αντικειμενικά και καθολικά ισχυρότερου αντιπάλου. Με τον τρόπο αυτό παραπλανούσαν τα Νατοϊκά αεροσκάφη, τα οποία βομβάρδιζαν μοντέλα στόχων έναντι πραγματικών, καταφέρνοντας να προστατέψουν αποτελεσματικά τις λιγοστές δυνάμεις τους.

Ορισμός της έννοιας

Ο ακριβής ορισμός της παραπλάνησης μπορεί να δοθεί μόνο σε συνάρτηση κάθε φορά του τομέα στον οποίο αναφερόμαστε δηλαδή, αν πρόκειται για παράδειγμα για τις στρατιωτικές επιχειρήσεις, την ασφάλεια των Η/Υ κ.ά. Έτσι έχουμε τους παρακάτω ορισμούς οι οποίοι θα μας δώσουν και μια ολοκληρωμένη εικόνα πριν αναλύσουμε τα software decoys και honey pots, τα οποία αναφέρονται στην ασφάλεια των Η/Υ και δικτύων. Γενικά όμως, ο ορισμός που μπορεί να δοθεί για την παραπλάνηση είναι ο εξής: «*παραπλάνηση είναι, η διαδικασία όπου ο στόχος εκ προθέσεως αφήνετε να οδηγείτε σε λανθασμένες αντιλήψεις για τις προθέσεις και τις ενέργειες μας*». *(82)*

Η <u>*στρατιωτική παραπλάνηση*</u> περιλαμβάνει πράξεις, οι οποίες θα οδηγήσουν τους ηγέτες του εχθρού σε εσφαλμένες εκτιμήσεις για τις ικανότητες, τις προθέσεις, την ισχύ και τις επιχειρήσεις των φίλιων δυνάμεων. Πραγματοποιείται για να αυξήσει την αποτελεσματικότητα των φίλιων ενεργειών, όπλων και ελιγμών έναντι των εχθρικών δυνάμεων. *(83)*

"Ιστορική" παραπλάνηση, σύμφωνα με το θεωρητικό του πολέμου και της στρατηγικής *Sun Tzu* ορίζεται ως εξής: «*όταν είναι ικανός δείχνει ανίκανος, όταν είναι έτοιμος δείχνει ανέτοιμος, όταν βρίσκεται πλησίον δείχνει ότι είναι πολύ μακριά και όταν βρίσκεται πολύ μακριά δείχνει όταν είναι πλησίον. Επιτίθεται όταν ο εχθρός δεν είναι έτοιμος χρησιμοποιώντας μονοπάτια και πορείες που ο οποιοσδήποτε θα θεωρούσε αδύνατον να χρησιμοποιηθούν για τέτοιες ενέργειες*».

Ο ορισμός της παραπλάνησης στην επιστήμη των Η/Υ θα αναφερθεί αναλυτικά στο Κεφάλαιο IV. Οι παραπάνω ορισμοί έχουν ως κύριο χαρακτηριστικό τη λανθασμένη

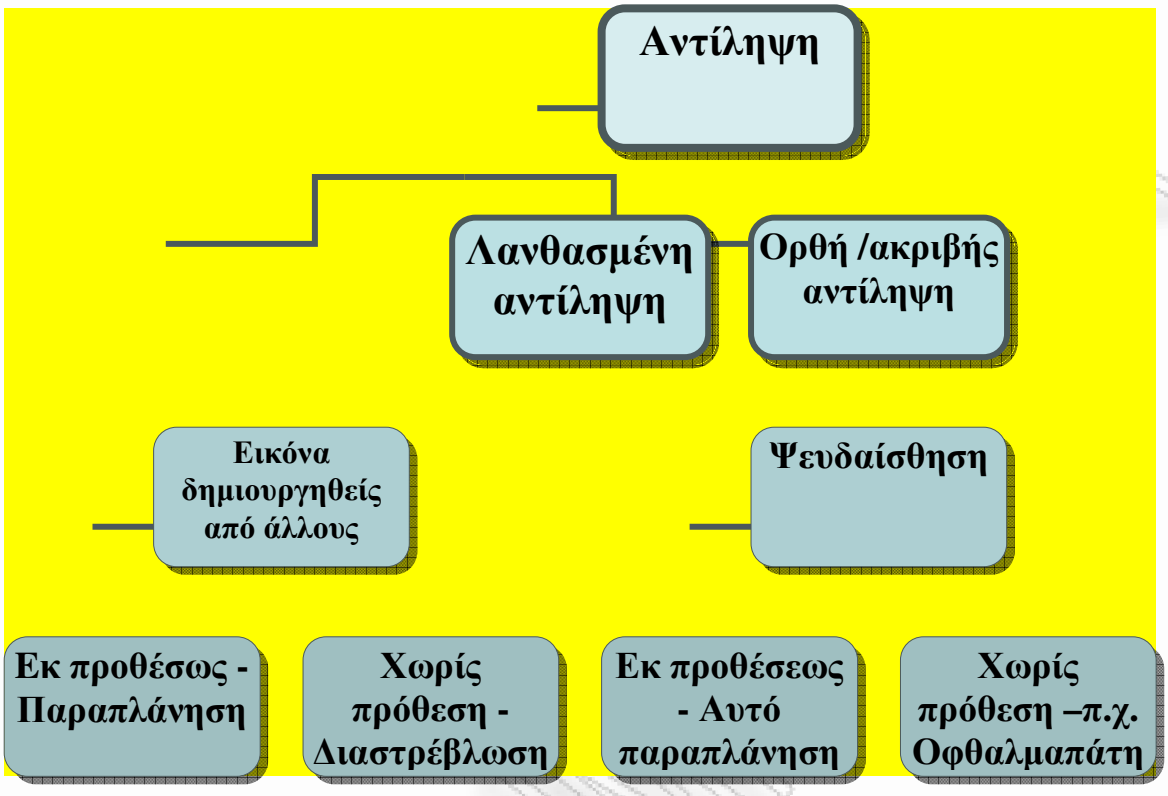
αντίληψη πραγμάτων, προθέσεων, επιλογών και καταστάσεων. Στην επόμενη παράγραφο θα γίνει αναλυτική κατανόηση της έννοιας με τη χρήση και κατάλληλου γραφήματος.

Κατανόηση της έννοιας

Τόσο η προβολή όσο και η απόκρυψη πραγμάτων χρησιμοποιούνται σε κάθε παραπλανητική ενέργεια. Όταν προβάλεται κάτι λανθασμένο θα πρέπει επιπλέον η αλήθεια να αποκρύπτεται. Παράλληλα όταν κάτι κρύβεται κάτι άλλο στη θέση του θα πρέπει να προβάλλεται για να μην υπάρχει κάποιο εμφανές κενό. Επιπλέον η παραπλάνηση περιλαμβάνει περίπλοκες πανουργίες με το συνδυασμό τόσο της απόκρυψης όσο και της προβολής πραγμάτων. Για παράδειγμα ένα honey pot μπορεί παραπλανητικά να παριστάνει ένα network server, ενώ παράλληλα μπορεί να αποκρύπτει τελείως ένα keystroke logger.

Στις περιπτώσεις αυτές όπου γίνεται χρήση παράλληλα απόκρυψης και προβολής, η παραπλάνηση μπορεί να χαρακτηρισθεί με τον ένα ή τον άλλο όρο, ανάλογα με τις προτεραιότητες που τίθενται κάθε φορά. Για παράδειγμα η ετικέτα ενός server είναι τροποποιημένη ώστε να παρουσιάζει λανθασμένο μοντέλο και αριθμό έκδοσης. Παρά το γεγονός λοιπόν ότι η ετικέτα περιέχει αυτά τα στοιχεία η πρωταρχική επιδίωξη της είναι η απόκρυψη του πραγματικού μοντέλου και της πραγματικής έκδοσης από επίδοξους hackers.

Οι Bell και Whaley έχουν αναπτύξει μια θεωρία περί της παραπλάνησης στηριζόμενοι στην άποψη ότι είναι αποτέλεσμα λανθασμένης αντίληψης όπως φαίνεται και στο παρακάτω σχήμα.



Διάγραμμα 1:Το διάγραμμα της έννοιας της αντίληψης

Σύμφωνα με την ταξινόμηση αυτή, υπάρχει διάκριση ανάμεσα στη λανθασμένη αντίληψη που δημιουργείται από τους άλλους και σε αυτή που δημιουργείται από εμάς τους ίδιους (ψευδαίσθηση), καθώς και στη διαστρέβλωση που γίνεται με πρόθεση ή ακούσια. Για να πραγματοποιηθεί η παραπλανητική ενέργεια θα πρέπει να υπάρχει συγκεκριμένη πρόθεση, η κίνηση να είναι καλά μελετημένη από τον "επιτιθέμενο", ώστε να δημιουργηθεί η ψεύτικη εικόνα στο υποψήφιο θύμα. Αυτά τα χαρακτηριστικά συναντιόνται τόσο στη στρατιωτική παραπλάνηση για παράδειγμα όσο και στο computer science. *(82)*

Δομή της παραπλάνησης

Η δομή της έννοιας της παραπλάνησης δόθηκε από τους δύο προαναφερμένους συγγραφείς περιλαμβάνοντας, τόσο την προσποίηση (δηλαδή την προβολή λανθασμένης εικόνας) όσο και την υποκρισία (δηλαδή την απόκρυψη της αλήθειας). Στον παρακάτω πίνακα γίνεται λεπτομερής ανάλυση του όρου που εξετάζουμε.

Υποκρισία (απόκρυψη της αλήθειας)		Προσποίηση (προβολή λανθασμένης εικόνας)	
Συγκάλυψη(η απαλοιφή ενός παλιού σχεδίου ή συγχώνευση του με ένα ήδη υπάρχον)	• Απαλοιφή των χαρακτηριστικών του • Συνδυασμός με τα χαρακτηριστικά ενός άλλου σχεδίου	Μίμηση(η επαναχρησιμοποίηση ενός παλαιότερου σχεδίου)	• Αντιγραφή των χαρακτηριστικών ενός άλλου σχεδίου
Μορφοποιεί (ο μετασχηματισμός ενός παλιού σχεδίου με τον συνδυασμό μαζί με ένα άλλο ση-μετατροπή)	• Προσθήκη νέων χαρακτηριστικών • Αφαίρεση παλαιότερων χαρακτηριστικών	Εφευρετικότητα (η δημιουργία ενός εντελώς νέου σχεδίου)	• Δημιουργία νέων χαρακτηριστικών
Θάμπωμα (η δημιουργία θολούρας γύρω από ένα σχέδιο μειώνοντας δραματικά τα χαρακτηριστικά το)	• Συσκότιση παλαιών χαρακτηριστικών • Προσθήκη εναλλακτικών χαρακτηριστικών	Δημιουργία δολώματος (η δημιουργία ενός επιπρόσθετου εναλλακτικού σχεδίου)	• Δημιουργία εναλλακτικών χαρακτηριστικών

Πίνακας 4 :Η δομή της παραπλάνησης

Παρατηρούμε επομένως ότι η ταξινόμηση των παραπλανητικών τεχνικών βασίζεται σε τρεις διαφορετικούς τρόπους απόκρυψης: τη συγκάλυψη, τη μετατροπή και το θάμπωμα με τις ενέργειες που κάθε μία από αυτές περιλαμβάνει. Αυτή η κατηγοριοποίηση χρησιμοποιείται τόσο στη βιβλιογραφία του computer security όσο και στο military security. Η ανάλυση του παραπάνω πίνακα μπορεί να γίνει με διάφορους τρόπους, κάθετα αλλά και οριζόντια.

Αρχικά διακρίνει δύο βασικές μορφές παραπλάνησης: την υποκρισία και την προσποίηση και δευτερευόντως παρουσιάζει την αλληλεξάρτηση μεταξύ των δύο. Δε μπορεί να υπάρξει υποκρισία χωρίς την προσποίηση και το αντίστροφο. Άλλωστε σε όλες σχεδόν τις πρακτικές εφαρμογές της παραπλάνησης γίνεται συνδυασμένη χρήση και των δύο μορφών. Όταν κάτι αποκρύπτεται κάτι άλλο υπάρχει στη θέση του ή κάτι διαφορετικό από την πραγματικότητα παρουσιάζεται.

Παράλληλα η ανάγνωση του πίνακα γίνεται και οριζόντια με αντιστοίχηση μεταξύ των υποκατηγοριών, για παράδειγμα η συγκάλυψη ταιριάζει απόλυτα με την μίμηση κ.ο.κ. Τέλος η αποτελεσματικότητα των διαφόρων μορφών παραπλάνησης γίνεται όλο και μεγαλύτερη όσο αυξάνεται ο τόνος του χρωματισμού του πίνακα από το κίτρινο προς το κόκκινο χρώμα. Θεωρούμε δηλαδή, ότι η μορφοποίηση-μετατροπή είναι πιο αποτελεσματική από τη συγκάλυψη αλλά λιγότερο αποτελεσματική από το θάμπωμα.

Η αξία της παραπλάνησης

Η ραγδαία ανάπτυξη της τεχνολογίας δε μειώνει στο ελάχιστο την αξία της παραπλάνησης. Είδαμε εξάλλου σε προηγούμενη παράγραφο ότι ακόμα και στις πιο πρόσφατες πολεμικές συγκρούσεις χρησιμοποιήθηκαν ανάλογα μέσα. Πολλές φορές λειτουργεί ως πολλαπλασιαστής ισχύος προσφέροντας μεγάλα πλεονεκτήματα, είτε στον αμυνόμενο ή στον επιτιθέμενο ανάλογα ποιος τη χρησιμοποιεί. Είναι επίκαιρη η ρήση του στρατηγού Αϊζενχάουερ ότι “καμία μεγάλη επιχείρηση δεν πρέπει να αναλαμβάνεται χωρίς

προηγουμένως τον σχεδιασμό και την εκτέλεση των απαραίτητων παραπλανητικών κινήσεων". *(84)*

Η αξία της παραπλάνησης για τον επιτιθέμενο

Η χρήση παραπλανητικών μεθόδων μπορεί να επιτρέψει στον επιτιθέμενο να πραγματοποιήσει τους στρατηγικούς και τακτικούς στόχους του ταχύτερα και με μεγαλύτερη ασφάλεια. Το 1991 κατά τη διάρκεια του Πολέμου του Κόλπου είχαμε την αντιπαράθεση ενός ολοκληρωτικά δυνατότερου αντιπάλου (Αμερικανικές και συμμαχικές δυνάμεις) με ένα πολύ πιο αδύναμο αμυνόμενο (Ιρακινές Ένοπλες Δυνάμεις).

Οι πρώτοι χρησιμοποίησαν έναν κλασικό τακτικό ελιγμό υπερκέρασης εκτελώντας επίθεση από τα Δυτικά με μεγάλη ταχύτητα, έχοντας όμως παραπλανήσει όλο το προηγούμενο διάστημα τους Ιρακινούς για τις προθέσεις τους. Τους είχαν κάνει να πιστέψουν ότι η επίθεση θα εκτελούνταν από το Νότο και την Ανατολή. Με τον τρόπο αυτό σε τέσσερις ημέρες οι Τεθωρακισμένες Μεραρχίες του Αμερικανικού Στρατού βρίσκονταν πίσω από τις Ιρακινές γραμμές και σε απόσταση 50 χλμ. από την πρωτεύουσα του κρατιδίου του Κουβέιτ πραγματοποιώντας μιας εύκολη νίκη με μηδενικές απώλειες.

Η αξία της παραπλάνησης για τον αμυνόμενο

Είναι απόλυτα κατανοητό ότι μια από τις μεθόδους που παραδοσιακά ο πιο αδύναμος χρησιμοποιεί έναντι του ισχυρότερου είναι η απάτη και ο δόλος, αφού δεν έχει τα μέσα και την δύναμη να τον αντιμετωπίσει ανοιχτά. Τεχνικές όπως η προσάρτηση και στρατολόγηση δυσαρεστημένων ή φιλόδοξων αξιωματικών του εχθρού, η κυκλοφορία ψεύτικων φημών για τις προθέσεις μας και τις δυνάμεις μας, η εικονική μετακίνηση στρατευμάτων κ.ά., είναι μόνο μερικές από τις πολύ αποτελεσματικές τεχνικές που η Βυζαντινή Αυτοκρατορία χρησιμοποιούσε κατά κόρον στη χιλιόχρονη ιστορία της για την αντιμετώπιση, σαφώς πιο δυνατών αντιπάλων, τόσο στα Ανατολικά (Πέρσες, Τουρκομάνους, Άραβες) όσο και στα Βόρεια (Βούλγαροι, Ρώσοι) σύνορα της. Με τη χρήση της παραπλάνησης ο αμυνόμενος αντιστρέφει το αρνητικό ισοζύγιο δυνάμεως προς όφελος του, αφού παρασύρει τον αντίπαλο σε ενέργειες που του στερούν τα πλεονεκτήματα που διαθέτει, ενώ από την άλλη πλευρά μεγιστοποιείται η αποτελεσματικότητα και η καταστροφικότητα των δικών του ενεργειών.

3.4 Η διαδικασία σχεδιασμού της παραπλάνησης – planning process .

Για να αναλύσει κάποιος σε βάθος την διαδικασία σχεδιασμού μιας παραπλανητικής κίνησης/ενέργειας στον τομέα του computer security θα πρέπει προηγουμένως να εξετάσει την διαδικασία όπως λειτουργεί και εφαρμόζεται στον στρατιωτικό τομέα εδώ και πολλά χρόνια και περιγράφεται από τα διάφορα εγχειρίδια. Η βασική αρχή είναι ότι δεν υπάρχει επιτυχημένη παραπλάνηση χωρίς σχέδιο παραπλανήσεως ,αντίθετα αν κάτι στηρίζεται στην τύχη κατά πάσα πιθανότητα θα αποτύχει.*(85)* Παράλληλα σύμφωνα με τους Gerwehr και Russel υπάρχουν τρεις αρχές στην διαδικασία σχεδιασμού με κυριότερη την ΄΄ο σκοπός αγιάζει τα μέσα ΄΄. Αυτή επαναλαμβάνεται και στον Frederick B.Cohen *(86)* ο οποίος παρατηρεί ότι οι περισσότερες παραπλανητικές κινήσεις σχεδιάζονται με βάση το επιθυμητό αποτέλεσμα στον αντίπαλο .Επιπλέον σύμφωνα με τους Fowler &Nesbitt έξη θεμελιώδεις αρχές πρέπει να ακολουθούνται κατά την διαδικασία σχεδιασμού ανάλογων ενεργειών προκειμένου να υπάρχουν αυξημένες πιθανότητες επιτυχίας *(87)*.Οι ίδιες υιοθετούνται και στο U.S Joint Doctrine for Military Operations /Joint Publication 3-13.4/13 JULY 2006 , για κάθε μία όμως από τις οποίες απαιτείται προηγουμένως έγκριση από προϊστάμενο κλιμάκιο .Τέλος η πιο πλήρης ανάλυση έχει γίνει από τον Barton Whaley *(88)* ο οποίος προτείνει μια διαδικασία βήμα προς βήμα αποτελούμενη από δέκα στάδια για την αύξηση των πιθανοτήτων επιτυχίας ,.Τα βήματα αυτά είναι τα εξής :

1. Σαφής καθορισμός του στρατηγικού στόχου .
2. Προσπάθεια πρόβλεψης του τρόπου αντίδρασης του στόχου.
3. Καθορισμός των σημείων που επιθυμούμε να γίνουν αντιληπτά από τον στόχο .
4. Καθορισμός των σημείων μας που επιθυμούμε να είναι κρυφά και των σημείων που θέλουμε να είναι εμφανή .
5. Ανάλυση του σχεδίου απόκρυψης .
6. Ανάλυση του σχεδίου προβολής .
7. Σχεδιασμός του επιθυμητού αποτελέσματος με την μέθοδο που θα χρησιμοποιήσουμε.

8. Ανάλυση του επιθυμητού αποτελέσματος σε αυτούς που εκτελούν την παραπλάνηση .
9. Καθορισμός των επικοινωνιακών καναλιών μέσω των οποίων θα γίνει η διάδοση του παραπλανητικού σχεδίου .
10. Αναμονή ώσπου ο στόχος να ΄΄ πέσει στην παγίδα΄΄ .

Φυσικά αυτά τα δέκα βήματα δεν αποτελούν πανάκεια .Πάντα υπάρχει το ενδεχόμενο να υπάρξει αποτυχία .Γι'αυτό το λόγο ένα εναλλακτικό σχέδιο δράσεως θεωρείται βασικό .Επιπλέον ο εκτελών το σχέδιο παραπλανήσεως θα πρέπει συνεχώς να ελέγχει κατά πόσο ο στόχος ανταποκρίνεται με τον τρόπο που έχει προβλέψει , και ανάλογα να συνεχίζει ή να διακόπτει την διαδικασία .

3.5 Παραπλάνηση , συλλογή πληροφοριών και αντι-παραπλάνηση .

Οι παραπάνω όροι αν και χρησιμοποιούνται στις στρατιωτικές εφαρμογές κυρίως , έχουν νόημα και στην ασφάλεια δικτύων και Η/Υ .Με τον όρο συλλογή πληροφοριών δεν νοούμε μόνο την κατασκοπεία αλλά γενικότερα την γνώση των αντιπάλων , του περιβάλλοντος και όλων των άλλων σημείων που συνθέτουν την ενδεχόμενη απειλή .Είναι φυσικό ότι η αποτυχία στην συλλογή πληροφοριών και η παραπλάνηση είναι στενά συνδεδεμένα γιατί η επιτυχημένη παραπλάνηση από την μία πλευρά είναι συνήθως το αποτέλεσμα της αποτυχημένης συλλογής πληροφοριών από την άλλη .Όπως έχουμε διαπιστώσει από την ιστορική ανασκόπηση σε προηγούμενη παράγραφο στον ΄ΒΠ.Π για παράδειγμα , οι παραπλανητικές κινήσεις των συμμάχων ήταν επιτυχημένες λόγω αδυναμίας των Γερμανικών μυστικών υπηρεσιών να ανακαλύψουν τις πραγματικές προθέσεις τους .Παράλληλα , κάθε παραπλανητική προσπάθεια θα πρέπει πρωταρχικά να έχει εξασφαλίσει ότι τα μέσα intelligence του αντιπάλου θα είναι λειτουργικά και ικανά να εντοπίσουν ενδεχόμενη ΄΄κίνηση΄΄ δηλαδή ΄΄κίνηση ΄΄ που εμείς επιθυμούμε να κατανοήσει αλλά , και τα δικά μας μέσα intelligence θα πρέπει να μπορέσουν να παρέχουν το κατάλληλο feedback για την ανάλογη προσαρμογή και αλλαγή στην προσπάθεια μας να παραπλανήσουμε τον αντίπαλο .

Επιπλέον η εφαρμογή της παραπλάνησης και της αντιπαραπλάνησης συνδέονται μεταξύ τους. Με τον όρο αντιπαραπλάνηση νοούμε την παραπλάνηση της παραπλάνησης .Σε όλες τις

προσπάθειες παραπλάνησης είναι αδύνατη η εξ ‘ ολοκλήρου προβολή ή απόκρυψη ενός αντικειμένου, συνεπώς πιθανές ανωμαλίες κατά την εφαρμογή της πολύ πιθανόν να εμφανιστούν. Στην περίπτωση που αυτές οι ανωμαλίες εντοπισθούν κατά την συλλογή στοιχείων –πληροφοριών η όλη διαδικασία αποτυγχάνει και καταρρέει .Ένα πιθανό λάθος θα είναι και το τελευταίο.

Θεωρητικά ο εντοπισμός μιας παραπλανητικής προσπάθειας από τον αντίπαλο πιθανόν να φαντάζει εύκολος , στην πράξη όμως τα πράγματα είναι πολύ διαφορετικά .Ειδικά αν αναφερόμαστε σε κινήσεις στρατηγικού επιπέδου όπου οι αποφάσεις λαμβάνονται στο υψηλότερο δυνατό σημείο . Ακόμα και αν κάποια ανωμαλία ή κάτι περίεργο εντοπισθεί συνήθως θεωρούμε ότι πρόκειται για κάποιο λάθος ή για κάποια παράλειψη .Ένα τέτοιο παράδειγμα υπάρχει στον ΄Β Παγκόσμιος Πόλεμος. Οι πράκτορες της Βρετανικής Μυστικής Υπηρεσίας MI6 στις Κάτω χώρες έστελναν κωδικοποιημένα σήματα στο στρατηγείο τους στο Λονδίνο .Για να εξασφαλίσουν ότι τα μηνύματα αυτά δεν ήταν πλαστά ή παραχαραγμένα όφειλαν να προσθέτουν ένα συγκεκριμένο κωδικό κάθε φορά. Περί τα μέσα του 1941 οι Γερμανικές δυνάμεις εντόπισαν ένα μυστικό ασύρματο δίκτυο στην Ολλανδία χωρίς όμως να καταφέρουν να συλλάβουν τους δράστες . Έστειλαν λοιπόν στο Λονδίνο ένα κωδικοποιημένο σήμα έρθει το οποίο όμως ήταν λάθος αφού δεν περιείχε τον κατάλληλο κωδικό.*Ο Αξιωματικός Υπηρεσίας στην MI6 θεώρησε ότι απλά ήταν ένα λάθος του πράκτορα και του έστειλε οδηγίες πώς να συντάσσει σωστά τα σήματα και τον κωδικό κάθε φορά.* Με τον τρόπο αυτό οι Γερμανικές Μυστικές Υπηρεσίες έστελναν παραπλανητικές πληροφορίες στους Εγγλέζους μέχρι το 1944 , δημιουργώντας σύγχυση στην συνολική εικόνα που είχαν οι τελευταίοι για την κατάσταση στις κατακτημένες περιοχές .*(89)*

3.6 Παγίδες της παραπλάνησης .

Η χρήση μεθόδων παραπλάνησης στον στρατιωτικό τομέα αλλά και στο τομέα της ασφάλειας των Η/Υ ελλοχεύει αρκετές παγίδες τις οποίες θα πρέπει να έχουμε υπόψη μας .Η αποφυγή αυτών είναι βασική επιδίωξη στο cyber security.

3.6.1 Παραπλάνηση που έχει αποκαλυφθεί

Στην περίπτωση αυτή ολόκληρη η κίνηση μπορεί να αποβεί καταστροφική γι' αυτόν που την σχεδίασε και την εκτέλεσε .Το 1953 ο Γάλλος στρατηγός Navarre θεώρησε το βουνό Dienbienphu ως την κατάλληλη ευκαιρία να παραπλανήσει και να παγιδεύσει τα στρατεύματα του Βιέτ Μινχ στην Ινδοκίνα .Έτσι με διάφορες παραπλανητικές κινήσεις οδήγησε τα εχθρικά στρατεύματα προς τα εκεί θεωρώντας ότι θα κατάφερνε συντριπτική νίκη. Όμως ο αντίπαλος αποδείχτηκε πιο δυνατός και διορατικός καταφέρνοντας να εντοπίσει και να καταλάβει έγκαιρα τις Γαλλικές κινήσεις και να αποκλείσει όλη την περιοχή. Αποτέλεσμα αυτής της αποτυχημένης παραπλάνησης ήταν η καταστροφή των επίλεκτων σωμάτων του Γαλλικού Στρατού , των Αλεξιπτωτιστών και της Λεγεώνας των Ξένων που είχαν αναλάβει την φύλαξη του υψώματος .Οι Γάλλοι παρά την υπεροπλία τους είχαν πιαστεί στην ίδια τους την παγίδα και μάλιστα αναγκασμένοι να πολεμήσουν μέχρις εσχάτων αφού η εκκένωση του υψώματος ήταν πρακτικά αδύνατη . Πέρα από τις απώλειες σε άνδρες και υλικό το ψυχολογικό και διεθνές αντίκτυπο στο παγκόσμιο γόητρο των Γαλλικών Ενόπλων Δυνάμεων υπήρξε καταστροφικό .

3.6.2 Νομικές παγίδες

Μία από τις δύσκολες παγίδες που έχουν να αντιμετωπίσουν οι πρακτικές που μελετάμε είναι οι νομικές προεκτάσεις αυτών των ενεργειών .Σύμφωνα με την Συνθήκη της Γενεύης η χρήση του καμουφλάζ ,της παραπλάνησης και της παραπληροφόρησης δεν απαγορεύεται , όμως αυτό που απαγορεύεται είναι ο δόλος με την εξής μορφή .Αν κερδίσουμε για παράδειγμα την εμπιστοσύνη των εχθρών ώστε να πιστέψουν ότι αν παραδοθούν θα αντιμετωπισθούν με σεβασμό στην διεθνή νομιμότητα και στην προσωπικότητα τους ,ενώ στην πραγματικότητα σκοπός μας είναι να προδώσουμε αυτή την εμπιστοσύνη .Γενικότερα όμως στην πραγματικότητα η διαφορά μεταξύ του τι ακριβώς επιτρέπεται και τι όχι είναι γκρίζα και ασαφής .Παραδείγματος χάριν η κατασκευή ψεύτικων σταθμών εκτόξευσης πυραύλων με σκοπό την δημιουργία παραπλανητικής εικόνας στον αντίπαλο είναι διαφορετική από την μεταφορά πυραύλων μέσα σε οχήματα του Ερυθρού Σταυρού ή σε νοσοκομεία .Σε αυτή την περίπτωση η παραπλάνηση μπορεί και να μην συμφωνεί με το ΄΄δίκαιο του πολέμου΄΄ ενώ

από αρκετούς μπορεί να χαρακτηρισθεί ακόμα και ανήθικη ενέργεια .Φυσικά δεν σημαίνει ότι είναι ηθικό είναι και νόμιμο ή το αντίστροφο .Έτσι πολλές φορές παραπλανητικές ενέργειες δικαιολογούνται στα πλαίσια επίτευξης ενός στόχου παρά το γεγονός ότι η νομιμότητα τους πιθανόν να είναι υπό αμφισβήτηση .

3.6.3 Οι κίνδυνοι της παθητικής και ενεργητικής παραπλάνησης

Με δεδομένους τους κινδύνους που υπάρχουν σε κάθε είδος παραπλανητική ενέργεια πολλοί από τους ΄΄επαγγελματίες ΄΄ του είδους διακρίνουν δύο κατηγορίες :την παθητική και την ενεργητική παραπλάνηση .Παθητική παραπλάνηση όπως το καμουφλάζ , η προκάλυψη κ.α αποτελούν τους πιο ασφαλείς και εύχρηστους τρόπους απόκρυψης .Χρησιμοποιώντας πάλι το στρατό μπορούμε να αναφέρουμε μια πλειάδα παραδειγμάτων ξεκινώντας από τις στολές παραλλαγής των στρατιωτών ως τα πολεμικά αεροσκάφη , τα τεθωρακισμένα οχήματα κ.α .Παράλληλα τα τελευταία χρόνια όλο και περισσότερα πολεμικά πλοία και αεροσκάφη εμφανίζονται με χαρακτηριστικά stealth μείωσης της υπογραφής τους στο radar και στα άλλα ηλεκτρονικά μέσα εντοπισμού .

Από την άλλη πλευρά τα ενεργητικά μέσα παραπλάνησης είναι περισσότερο απρόβλεπτα , πολύπλοκα και δύσκολα στην εφαρμογή .Η βασική δυσκολία προέρχεται κυρίως από την πιθανότητα ολόκληρη η προσπάθεια να έχει αποκαλυφθεί πχ τυχαία ή από ένα λάθος χωρίς όμως αυτό να έχει γίνει αντιληπτό .Παράλληλα υποβόσκει το ρίσκο από την μυστικοπάθεια που απαιτούν τέτοιες ενέργειες. Οι φίλιες δυνάμεις που δεν θα έχουν γνώση για την επιχείρηση που βρίσκεται σε εξέλιξη , πιθανόν να προβούν σε ενέργειες απρόβλεπτες και επικίνδυνες ματαιώνοντας την όλη προσπάθεια .Αυτό έχει ως συνέπεια πολλοί να καταλήγουν στο συμπέρασμα ότι στις ενεργητικές μεθόδους παραπλάνησης το ρίσκο είναι ιδιαιτέρως υψηλό και τα αποτελέσματα του υπό αμφιβολία .

ΚΕΦΑΛΑΙΟ IV Ηλεκτρονική Παραπλάνηση και Κυβερνοτρομοκρατία (cyberterrorism)

4.1 Η παραπλάνηση στον Κυβερνοχώρο (cyberspace)

Η computer security deception ορίζεται ως όλες οι ενέργειες που εκτελούνται με σκοπό να αποτρέψουν τους επίδοξους hackers από την ανάληψη δράσης .Τις περισσότερες φορές στόχος είναι ο επιτιθέμενος να μην μπει καν στην διαδικασία σύνδεσης με τον server – υποψήφιο θύμα .Η παραπλάνηση χρησιμοποιείται και για την απόκρυψη διαφόρων ΄΄αμυντικών΄΄ μέσων όπως firewalls , intrusion detection systems (IDS) , keystroke loggers και honeypots .Το βασικό μέλημα όμως είναι η μη εμφάνιση ευαίσθητων πληροφοριών πχ για την τοπολογία ενός δικτύου ,των τρωτών του σημείων κ.α τα οποία πιθανόν να αποκαλυφθούν από την αναγνώριση που θα εκτελέσει κάποιος hacker (πχ εκτελώντας scanning) .

Εκτός όμως από την εξαπάτηση για λόγους ασφαλείας που συναντάμε στο διαδίκτυο υπάρχουν πάρα πολλές περιπτώσεις εξαπάτησης του χρήστη από κακόβουλους παράγοντες , κακόβουλη παραπλάνηση - εξαπάτηση .Η επιτυχία αυτών στηρίζεται στο γεγονός ότι ο κοινός χρήστης των Η/Υ και του διαδικτύου – δηλαδή χωρίς εξειδικευμένες γνώσεις – θεωρεί αυτό που βλέπει στην οθόνη ως αυθεντικό με αποτέλεσμα να εξαπατάται .Ένα πρόσφατο παράδειγμα αποκαλύφθηκε το 2006 με ένα ψεύτικο web-site του FBI το οποίο περιείχε κάποια αυθεντικά αρχεία αλλά όλα τα υπόλοιπα δεν είχαν καμία απολύτως σχέση με την συγκεκριμένη υπηρεσία .Στον συγκεκριμένο διαδικτυακό τόπο γίνονταν προσπάθεια να παρασύρουν όσους το επισκέπτονταν να αποκαλύψουν τους κωδικούς των πιστωτικών τους καρτών καθώς και άλλα προσωπικά δεδομένα .*(90)* Παράλληλα από όσα είναι γνωστά μέχρι στιγμής , αποστέλλονταν σε μεγάλο αριθμό χρηστών του διαδικτύου κάποιο e-mail το οποίο τους ενημέρωνε για την ύπαρξη μεγάλης έκτασης υπεξαίρεσης κωδικών πιστωτικών καρτών , παριστάνοντας την εν λόγω υπηρεσία . Στην συνέχεια παρουσιάζονταν κάποιο link το οποίο τους παρέπεμπε σε ένα υποτιθέμενο web-site του FBI στο οποίο υπήρχε μία φόρμουλα με προσωπικά στοιχεία (οικογενειακή κατάσταση , κωδικοί πιστωτικών καρτών ,στοιχεία κατοικίας ,οικονομικά στοιχεία κ.α) την οποία έπρεπε να συμπληρώσουν για να μπορέσουν να ελέγξουν αν έχουν υποστεί κάποια ζημιά από την υποτιθέμενη υπεξέραιση .Στην παραπάνω

περίπτωση και το e-mail και το web-site ήταν απολύτως παραπλανητικά και ψεύτικα αφού αντί να παραπέμπουν τους χρήστες στην επίσημη διεύθυνση https://www.fbi.gov/debit_theft.html τους παρέπεμπαν στην www fbi.x-web-x.com , ενώ όσοι έκαναν χρήση της δεύτερης τα στοιχεία μεταδίδονταν σε μία Ρωσική ηλεκτρονική διεύθυνση .

Η παραπάνω περίπτωση ανήκει στη κατηγορία του phishing την οποία έχουμε αναφέρει και στο Κεφάλαιο Ι .Μία από τις πιο κοινές περιπτώσεις ηλεκτρονικής εξαπάτησης αφορά ψεύτικες επιχειρηματικές ευκαιρίες που συχνά εμφανίζονται στο Διαδίκτυο. Παράλληλα υπάρχουν ΄΄ευκαιρίες ΄΄ γρήγορου υποτίθεται κέρδους από την μεταφορά μεγάλων χρηματικών ποσών σε τραπεζικούς λογαριασμούς διαφορετικών χωρών . Η απάτη σε αυτή την περίπτωση είναι ότι ο φόρος που θα πλήρωναν οι επενδυτές θα καρπωθεί από αυτόν που θα χρησιμοποιήσει την συγκεκριμένη ευκαιρία . Επιπλέον πολλές φορές αναζητούνται υποψήφια θύματα στα οποία υπόσχονται μεγάλα κέρδη από επενδύσεις κεφαλαίων σε εταιρίες ΄΄πυραμίδες ΄΄.

Άλλη μία μορφή παραπλάνησης στον κυβερνοχώρο εμπλέκει και το social engineering δηλαδή ΄΄ να κάνουμε τους ανθρώπους να κάνουν πράγματα που σε κανονικές συνθήκες δεν θα έκαναν για ένα άγνωστο ΄΄ *(91)* Αυτό πραγματοποιείται με την χρήση διαφόρων τεχνικών οι οποίες στηρίζονται στην καλή πίστη ,την εμπιστοσύνη , την ευπιστία και πολλές φορές την αφέλεια των ανθρώπων .Έτσι υψηλής ασφαλείας Η/Υ και δίκτυα μπορούν να παραβιασθούν αν στοχεύσει ο επιτιθέμενος στο πιο αδύνατο σημείο , τον χρήστη .Παριστάνοντας για παράδειγμα τον τεχνικό σύμβουλο ή τον σύμβουλο ασφαλείας o social engineer μπορεί να πείσει το θύμα να του αποκαλύψει password ή remote access κωδικούς καταφέρνοντας να διεισδύσει στο δίκτυο που έχει στοχεύσει .

Η ικανότητα που έχει κάποιος να αντιμετωπίσει περιπτώσεις όπως αυτές που είδαμε παραπάνω εξαρτάται από το επίπεδο των εξειδικευμένων γνώσεων που κατέχει αλλά και της προσωπικής του πολλές φορές ευστροφίας . Οι προσπάθειες εξαπάτησης θα συνεχίσουν να υπάρχουν στο ψηφιακό κόσμο όπως και στον πραγματικό .Η τελική έκβαση βρίσκεται ανάμεσα στους virus writers από την μία πλευρά και τους anti-virus software vendors από την άλλη ή ανάμεσα στους hackers και τα intrusion detection systems , και με τις δύο πλευρές να προσπαθούν να υπερτερήσουν έναντι της άλλης αποδεικνύοντας την ανεπτυγμένη ευφυΐα τους .

4.2 Τα είδη της ηλεκτρονικής παραπλάνησης

Στο κεφάλαιο αυτό θα γίνει προσπάθεια κατηγοριοποίησης των διαφόρων μορφών ηλεκτρονικής παραπλάνησης βασισμένο στο σύγγραμμα των James F.Dunnigan &Albert Nofi .(92) Από την μελέτη της υπάρχουσας βιβλιογραφίας θεωρούμε ότι η παραπάνω μελέτη καλύπτει πληρέστερα το συγκεκριμένο γνωστικό αντικείμενο .Έτσι έχουμε τις παρακάτω μορφές ηλεκτρονικής παραπλάνησης .

4.2.1 Απόκρυψη – concealment

Απόκρυψη γενικά είναι η προσπάθεια παραπλάνησης του αντιπάλου με την χρήση φυσικών μεθόδων όπως το έδαφος και η βλάστηση .Αποτελεί μία από τις παλαιότερες μορφές παραπλάνησης με ευρεία χρήση στην φύση .Αντίστοιχα και στον ψηφιακό κόσμο προσφέρονται πολλές ευκαιρίες απόκρυψης .Παραδείγματος χάριν ένας hacker μπορεί να κρύψει malicious files ή software σε μερικά κρυφά directory ή σε κανονικό κώδικά εντός του συστήματος στόχου το οποίο μάλιστα να αποτελεί μέρος του ΄΄φυσικού κόσμου ΄΄ του συστήματος χωρίς να δημιουργείτε καμιά υπόνοια .Επιπλέον ως άλλη μέθοδος απόκρυψης χρησιμοποιείται η στενογραφία και η κρυπτογράφηση η οποία τα τελευταία χρόνια έχει γνωρίσει πολύ μεγάλη πρόοδο .Χαρακτηριστικό παράδειγμα αποτελεί η απόκρυψη ενός μυνήματος σε ένα ψηφιακό είδωλο , στο οποίο μερικά από τα bits που δημιουργούν το είδωλο αυτό χρησιμοποιούνται για την κωδικοποίηση του κρυφού αυτού μυνήματος χωρίς να προκαλούν καμία διέγερση στα συστήματα ασφαλείας .Με τον τρόπο αυτό εκείνοι που είναι ενήμεροι για την ύπαρξη του κρυφού μυνήματος θα πραγματοποιήσουν την αποκωδικοποίηση ενώ οι υπόλοιποι απλά θα την αγνοήσουν .*(93)*

4.2.2 Καμουφλάζ – Camouflage

Παραδοσιακά το καμουφλάζ αποτελεί μέσο παραπλάνησης που χρησιμοποιείται στις στρατιωτικές επιχειρήσεις .Για την επιτυχία του χρησιμοποιούνται μια σειρά από τεχνικά μέσα όπως δίχτυα παραλλαγής ,κατάλληλα χρώματα βαφής του προσώπου αλλά και υλικά από το φυσικό περιβάλλον όπως χόρτα , κλαδιά κ.α με σκοπό την αδυναμία αναγνώρισης του

στρατιώτη και των μέσων που διαθέτει μέσα στον φυσικό κόσμο πχ σε ένα δάσος .Στα information system κατηγορίες malicious software όπως οι logic bomb μπορούν να καμουφλαριστούν από ένα ακίνδυνο filename .Σύμφωνα με τον Emory A.Anderson απλά μερικές γραμμές κώδικα κρυμμένες ως διεφθαρμένο πλέον αρχείο σε ένα Network File Server , ήταν ικανές να δημιουργήσουν προβλήματα στο σύστημα ΄΄στόχο΄΄ *(94)* Έτσι με δεδομένο ότι διεφθαρμένα αρχεία αποτελούν ένα κοινό σύμπτωμα στα δίκτυα ήταν σχεδόν αδύνατο για τα firewalls ή τα intrusion detection systems να μπορέσουν να τα ξεχωρίσουν .Μία άλλα μορφή ηλεκτρονικού καμουφλάζ είναι τα λεγόμενα ΄΄Πασχαλινά αυγά΄΄ - ΄΄Easter eggs ΄΄ όπου διάφορα αρχεία είναι αποθηκευμένα σε τελείως διαφορετικά files .Στο web-site www.eggs .com υπάρχει μια μεγάλη γκάμα τέτοιου είδους προγραμμάτων , παράδειγμα αποτελεί ένα πρόγραμμα flight simulator κρυμμένο στο Microsoft Excel 97 .

4.2.3 Παραπληροφόρηση

Αποτελεί και αυτή κλασσικό μέσο παραπλάνησης με πολλά ιστορικά παραδείγματα .Ουσιαστικά αφορά την επινόηση και διασπορά ψευδών και κατευθυνόμενων πληροφοριών οι οποίες θα αναγκάσουν τον ΄΄στόχο ΄΄ να αντιδράσει ή να συμπεριφερθεί με τρόπο αντίθετο προς το δικό του όφελος .Για την επιτυχία τέτοιας κατηγορίας εγχειρημάτων θα πρέπει να υπάρχει πολύ καλή γνώση της συμπεριφοράς του στόχου , ώστε ανάλογα να σχεδιασθεί και πιθανόν να τροποποιηθεί η προσπάθεια παραπλάνησης του .Φυσικά η παραπληροφόρηση μπορεί να χρησιμοποιηθεί και ως αμυντικό μέσο με σκοπό την δημιουργία σύγχυσης στον ή στους επιτιθέμενους .Παραδείγματος χάριν η δημοσίευση ψευδών πληροφοριών και οδηγιών σε ένα hackers forum , για το πώς μπορεί να γίνει εκμετάλλευση των ΄΄ρωγμών΄΄ των ηλεκτρονικών συστημάτων μπορεί να προστατέψει πιο αποτελεσματικά τα διάφορα συστήματα .Βέβαια πάντα υπάρχει ο κίνδυνος ολόκληρη μια τέτοια προσπάθεια να αποδειχτεί ανώφελη μια και οι hackers δεν θα παραπλανηθούν τελικά , αν ανακαλύψουν ότι οι πληροφορίες που έχουν χρησιμοποιήσει είναι ανακριβείς . Το διαδίκτυο αποτελεί μια πολύ αποτελεσματική φόρμουλα για την διασπορά ψευδών πληροφοριών σε μεγάλο εύρος πληθυσμού , η χρήση του οποίου τα τελευταία χρόνια συνεχώς αυξάνεται .

4.2.4 Τεχνάσματα – Ruse

Αυτή η κατηγορία μεθόδου παραπλάνησης αφορά την χρήση διαφόρων μεθόδων – κόλπων – προκειμένου να κάνουμε τον εχθρό να θεωρήσει ότι είμαστε φιλικοί μαζί του ενώ στην ουσία ισχύει το αντίθετο , για παράδειγμα η χρήση εξοπλισμού του εχθρού ή στολών του εχθρού .Το IP spoofing που αναλύσαμε στις τεχνικές hacking , ανήκει σε αυτή την κατηγορία .Εδώ γίνεται προσπάθεια το ΄΄ δίκτυο – στόχος ΄΄ να θεωρήσει τον επιτιθέμενο ως φίλο .Με τον τρόπο αυτό μπορούμε να χαλκεύουμε διάφορες κατηγορίες ηλεκτρονικού ταχυδρομείου .Χαρακτηριστικό είναι το παράδειγμα του w32.Mimail.c@mm , ένα mail worm που χρησιμοποιείτε συχνά εναντίον καλά προστατευμένων sites σε επιθέσεις τύπου denial of service . Το τελευταίο διαμοιράζεται ως .zip αρχείο το οποίο περιέχει φωτογραφίες τύπου .jpg.exe δίνοντας την εντύπωση ότι με διπλό κλικ θα ανοίξουν τα αρχεία με τις φωτογραφίες που υπάρχουν στο file , ενώ στη πραγματικότητα εγκαθίστανται το worm στον Η/Υ ή το δίκτυο .*(95)* Η κατηγορία των ruse δεν χρησιμοποιείτε πολύ συχνά ως αμυντική μέθοδος αφενός λόγω νομικών κωλυμάτων ,αφετέρου εξαιτίας της δυσκολίας που υπάρχει να παριστάνει κάποιος τον hacker .

4.2.5 Ψευδής εικόνα – Display

Στόχος του παραπάνω μέτρου είναι να δώσει στον εχθρό την ψευδαίσθηση ότι κάτι υπάρχει σε μια συγκεκριμένη περιοχή – τοποθεσία ενώ στην ουσία εκεί δεν θα υπάρχει τίποτα .Παράδειγμα τέτοιου είδους ενέργειας είναι η κατασκευή ψεύτικων πυραυλικών συστημάτων από τους Σοβιετικούς κατά την διάρκεια του Ψυχρού πολέμου με σκοπό την παραπλάνηση των Αμερικανικών κατασκοπευτικών δορυφόρων .Στην περίπτωση των πληροφοριακών συστημάτων ο επιτιθέμενος αντιλαμβάνεται την επίδραση των ενεργειών του από τις αντιδράσεις του συστήματος στο οποίο εκτέλεσε την επίθεση .Αν ο ιός που χρησιμοποιείτε από τον επιτιθέμενο είναι γνωστός , τότε μπορούμε να προσομοιάσουμε τα αποτελέσματα του δίνοντας του την ψευδαίσθηση ότι η επίθεση που εκτέλεσε είναι επιτυχής .Στην πραγματικότητα θα έχουμε αποφύγει τον κίνδυνο καταστρέφοντας τον ιό χωρίς να γίνει αντιληπτό το οτιδήποτε .Επιπλέον αν πραγματοποιηθεί denial of service επίθεση , αντιμετωπίζεται πρακτικά μειώνοντας την ταχύτητα του συστήματος για να προσομοιάσουμε την επιτυχία αυτής .

4.2.6 Επίδειξη ισχύος – Demonstration

Σε αυτό το είδος της παραπλάνησης γίνεται επίδειξη ισχύος με την μετακίνηση για παράδειγμα στρατευμάτων και την εκτέλεση εκτεταμένων γυμνασίων .Από την άλλη πλευρά σε αρκετές περιπτώσεις μπορεί να δώσει στον αντίπαλο την απατηλή εικόνα ασφάλειας και να τον καθησυχάσει .Το 1973 πριν την ξαφνική επίθεση εναντίον του Ισραήλ στον Πόλεμο του Γιόμ Κιπούρ (Yom Kippur) οι Αιγυπτιακές μονάδες είχαν μετακινηθεί κοντά στα Αιγυπτιακοισραηλινά σύνορα για την εκτέλεση διαφόρων γυμνασίων .Στο τελικό στάδιο της ασκήσεως οι συμμετέχουσες δυνάμεις εισέβαλαν στο Ισραήλ έχοντας το πλεονέκτημα του αιφνιδιασμού .Όμως η επίδειξη ισχύος στα πληροφορικά συστήματα μπορεί να αποδειχτεί επιζήμια για τον αμυνόμενο μια και θα προσελκύσει φιλόδοξους hackers .Όταν η Microsoft παρουσίασε την έκδοση XP των Windows ως την πιο ασφαλή που είχε δημιουργηθεί ποτέ , σχεδόν αμέσως hackers ξεκίνησαν να αναζητούν τρωτά σημεία σε αυτό το λειτουργικό σύστημα για να τα προσβάλλουν . Το demonstration λειτουργεί πιο αποτελεσματικά στα honey pot όπου οι επιτιθέμενοι ασυναίσθητα ελέγχουν τις ικανότητες τους με σκοπό την συλλογή πληροφοριών .

4.2.7 Αντιπερισπασμός –Feint

Ο αντιπερισπασμός αποτελεί βασικό μέρος της παραπλάνησης κατά τον οποίο ο επιτιθέμενος αποσπά την προσοχή του εχθρού από την κύρια επιθετική προσπάθεια του η οποία βρίσκεται σε εξέλιξη κάπου αλλού .Κλασσικό παράδειγμα είναι ο αντιπερισπασμός που πέτυχαν οι Συμμαχικές Δυνάμεις κατά την απόβαση στην Νορμανδία το 1944.Έκαναν τους Γερμανούς να πιστέψουν ότι η κύρια προσπάθεια θα πραγματοποιούνταν σε άλλο γεωγραφικό σημείο .Όταν οι τελευταίοι ανακάλυψαν την αλήθεια ήταν ήδη πολύ αργά ,οι Σύμμαχοι είχαν ήδη δημιουργήσει στρατηγικό προγεφύρωμα στην Γαλλική ακτή .Στον ψηφιακό κόσμο ο αντιπερισπασμός έχει ανάλογη λειτουργία .Καταφέρνουμε να προσομοιάσουμε τα αποτελέσματα μιας επιτυχημένης επίθεσης στο ένα μέρος ενός δικτύου με αποτέλεσμα ο επιτιθέμενος να θεωρεί ότι εκτελεί επιτυχημένα το έργο του , ενώ στο υπόλοιπο μέρος αντιμετωπίζουμε τις επιθέσεις αποτελεσματικά .*(96)*

4.2.8 Οξυδέρκεια – insight

Η τελευταία κατηγορία παραπλανητικών πρακτικών αφορά την ύπαρξη ανεπτυγμένης αντιληπτικής ικανότητας προκειμένου να καταφέρουμε να ξεπεράσουμε την ευφυΐα του επιτιθέμενου .Πραγματοποιείται με την μελέτη των τακτικών και μεθόδων που χρησιμοποιεί ο εχθρός .Όπως στο συμβατικό έτσι και στον ψηφιακό πόλεμο οι αντιμαχόμενες πλευρές προσπαθούν να επικρατήσουν η μία στην άλλη .Μια τυπική ψηφιακή επίθεση περιλαμβάνει τα πέντε βήματα που έχουμε προαναφέρει στο Κεφάλαιο ΙΙ όπως εντοπισμός των τρωτών σημείων του στόχου , απόκτηση πρόσβασης , χρήση malicious code κ.α .Για να αντιμετωπίσουμε μερικές από τις κινήσεις αυτές θα πρέπει να έχουμε μελετήσει σε βάθος τις κινήσεις του εχθρού προλαβαίνοντας το επόμενο βήμα του .

4.3 Ηλεκτρονική παραπλάνηση και ψηφιακή άμυνα.

Στις παραπάνω παραγράφους αναλύσαμε την ηλεκτρονική παραπλάνηση ως μέσο για την εκτέλεση επιθετικών κινήσεων .Στο κεφάλαιο αυτό θα αναλυθεί ο όρος στα πλαίσια χρήσης του ως αμυντικό μέσο .

4.3.1 Το μοντέλο απόκρυψης - αποκάλυψης

Μια κοινή πρακτική στο computer security είναι απόκρυψη πραγμάτων .Συνήθως συστήματα , εσωτερικά δίκτυα και αρχεία κρύβονται με χρήση firewalls και τα αρχεία κωδικοποιούνται .Οι μέθοδοι αυτοί λειτουργούν με την άρνηση πληροφορίας στους επίδοξους hackers .Μία άλλη μέθοδος για την απόκρυψη πραγμάτων που δεν επιθυμούμε να είναι σε κοινή θέα , είναι η χρήση της ηλεκτρονικής παραπλάνησης .Με τον τρόπο αυτό ο επιτιθέμενος δεν μπορεί να διαπιστώσει την ύπαρξη και τα χαρακτηριστικά των ενός αντικειμένου .Τρεις είναι οι τρόποι που μπορεί να αποκαλυφθεί η ύπαρξη ενός αντικειμένου:

- Άμεση παρατήρηση αυτού
- Έρευνα βασισμένη σε ενδείξεις για την ύπαρξη του
- Πληροφορίες για την ύπαρξη του αντικειμένου από άλλους

Σκοπός της παραπλάνησης είναι να υπερνικήσει και τις τρεις παραπάνω μεθόδους .Στην πρώτη μέθοδο ο hacker καταφέρνει να γνωρίσει πολλά για το δίκτυο και τα συστήματα του ,την τοπολογία του και τις δυνατότητες του. Όταν τελικά καταφέρει να αποκτήσει πρόσβαση σε ένα Η/Υ χρησιμοποιεί τις αδυναμίες του για να κατασκοπεύσει τα files του ,τα προγράμματα του και την running process .Παράλληλα μέσω των network clients μπορεί να παρακολουθήσει του servres που χρησιμοποιεί .

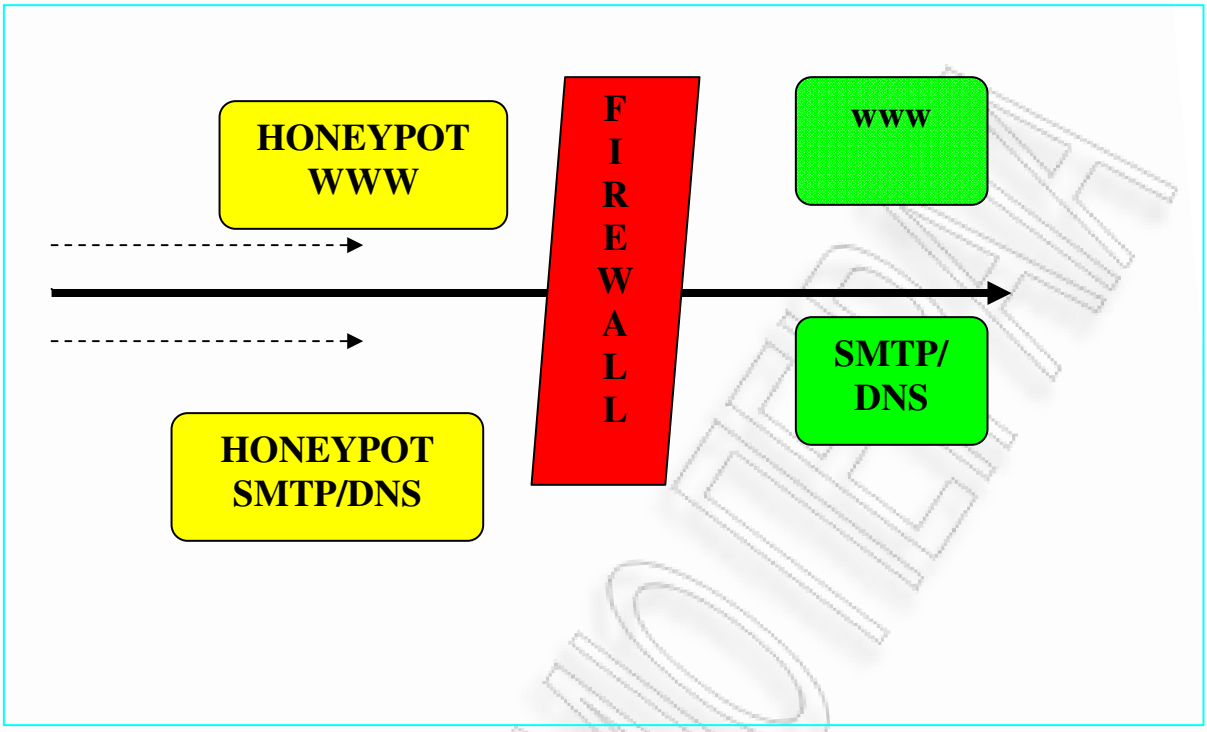
Οι hackers συχνά χρησιμοποιούν την έρευνα για να αποκτήσουν πληροφορίες για την τωρινή κατάσταση ενός δικτύου ,την τοπολογία , τις άμυνες που διαθέτει και τις αδυναμίες του .Υπάρχει μια μεγάλη γκάμα τεχνικών που χρησιμοποιείτε για τον σκοπό αυτό με πιο απλή το λεγόμενο fire walking με το οποίο διαπιστώνουμε ποια είσοδο είναι ανοιχτή και ελέγχεται από κάποιο firewall (στο fire walking γίνεται αποστολή ενός πακέτου TCP με IPTTL μέρος τοποθετημένο μόλις πριν από το firewall. Αν η απάντηση είναι το ICMP λάθος μήνυμα ΄΄ time to live exceeded in transmit΄΄ αυτό είναι μια ένδειξη ότι η TCP είσοδος είναι ανοιχτή. Στην περίπτωση που απάντηση δεν υπάρχει ή είναι ΄΄communication administratively prohibited ΄΄ τότε αποτελεί ένδειξη ότι η TCP είσοδος είναι κλειστή) .Παράλληλα αποτελεί και την πρώτη φάση από την επίθεση εναντίον ενός δικτύου .

Στην τρίτη και τελευταία περίπτωση οι πληροφορίες που αναζητούνται από τον hacker προέρχονται από άλλο άτομο/άτομα ή οργανισμό με δυνατότητες αναγνώρισης και παρακολούθησης .Η πηγή αυτών μπορεί να είναι η άμεση παρακολούθηση αλλά ακόμα και η έρευνα βασισμένη σε πιθανές ενδείξεις .Τυπικές πηγές πληροφοριών είναι οι DNS servers οι οποίοι καταγράφουν τις IP και τα domain names των Η/Υ ενός δικτύου καθώς και τα web-sites μεγάλων εταιριών που πιθανόν να περιλαμβάνουν πληροφορίες για το εσωτερικό δίκτυο της εταιρίας αλλά και τα on-line forums .

Στο επόμενο κεφάλαιο θα αναλυθούν τα honeypots τα οποία από την φύση τους είναι παθητικά μέσα με συγκεκριμένο στόχο και τα software decoys που ενδυναμώνουν την άμυνα των υπολογιστικών συστημάτων έναντι των cyber επιθέσεων .

4.3.2 Honey pot – Honey net

Η γενική ιδέα των honey pots θα μπορούσε να πει κάποιος ότι ξεκινάει ακόμα πριν από την ανακάλυψη των Η/Υ .Σκοπός είναι με την χρήση decoy δικτύου/αρχείων η παραπλάνηση του αντιπάλου .Ο ορισμός που μπορεί να δωθεί είναι ο εξής :honey pot είναι ένα σύστημα συνδεδεμένο στο Διαδίκτυο με έργο να εντοπίσει και να παγιδεύσει όσους έχουν σκοπό να παραβιάσουν τα υπολογιστικά συστήματα των υπολοίπων όπως φαίνεται και στο παρακάτω γράφημα .Honey net:είναι ένα δίκτυο που περιλαμβάνει honey pot .Τα τελευταία χρόνια η φήμη τέτοιου είδους συστημάτων αυξήθηκε δραματικά .Το πρώτο σύστημα δημιουργήθηκε το 1989 .Μέχρι το τελικό Honey net Project τον Οκτώβριο 1999 τέτοιας κατηγορίας πληροφοριακά συστήματα ήταν περισσότερο προσανατολισμένα στην κατανόηση και καταγραφή των τεχνικών και μεθόδων της κοινότητας των ΄΄black hat ΄΄ .(black hat :με τον όρο αυτό περιγράφουμε ένα κακόβουλο άτομο ή ένα hacker ο οποίος επιβουλεύεται την ασφάλεια ενός συστήματος και στόχο έχει να πετύχει μη εξουσιοδοτημένη είσοδο σε Η/Υ ή/και δίκτυο).Βασικά στελέχη του προγράμματος Honey pots υπήρξαν οι Marty Roesch , Chris Brenton , J.D Glazer ,Ed Skoudis και ο Lance Spitzner .Παρά τον αρχικό προσανατολισμό του προγράμματος η ραγδαία τεχνολογική ανάπτυξη , η αύξηση της χρήσης των Η/Υ και η απαίτηση για αποτελεσματικότερα και εξυπνότερα συστήματα ασφαλείας έδωσαν στα honey pots μεγάλη ώθηση .



Διάγραμμα 2:Σχηματικό διάγραμμα της λειτουργίας του honey pot-honey net

Δύο είναι τα κύρια είδη που χρησιμοποιούνται :τα low-interaction ή χαμηλής αλληλεπίδρασης και τα high-interaction ή υψηλής αλληλεπίδρασης .Στην πρώτη κατηγορία ονομάζονται αλλιώς shallow decoys και λειτουργούν ουσιαστικά ως μιμητές διαφόρων υπηρεσιών .Για παράδειγμα αν ένα honey pot μιμείται μια συγκεκριμένη αδυναμία χρησιμοποιώντας low-interaction service το πιο πιθανό είναι να εμφανίσει δημόσια αυτή και να περιμένει να πραγματοποιηθεί σύνδεση .Όταν η τελευταία πραγματοποιηθεί το honey pot αποστέλει εξωτερικά το συγκεκριμένο pattern που τυπικά ταιριάζει σε αυτή την αδυναμία. Είναι ευκολότερο να αναπτυχθούν σε σχέση με τα high-interactive,δεν απαιτούν τόση εξειδικευμένη γνώση και σαφώς λιγότερες πηγές .Ένα από τα μειονεκτήματα που παρουσιάζουν είναι ο περιορισμός στα όρια της αλληλεπίδρασης με το σύστημα στο οποίο εφαρμόζονται .Όταν μειώνεται η απειλή από τον επιτιθέμενο μειώνεται και το σύνολο των στοιχείων που συγκεντρώνονται .Παράλληλα τα χαμηλής αλληλεπίδρασης honey pots δεν μπορούν στην κυριολεξία να μιμηθούν την αντίδραση πραγματικών υπηρεσιών ή να προσδιορίσουν την δραστηριότητα μετά από ένα ΄΄συμβιβασμό ΄΄ ανάμεσα στον αμυνόμενο και τον επιτιθέμενο . Αντίθετα , τα high interactive honey pots έχουν μεγαλύτερη ικανότητα συγκέντρωσης

πληροφοριών ,τεχνικών και εργαλείων που χρησιμοποιούν οι hackers .Επιπλέον βασικό πλεονέκτημα που παρουσιάζουν είναι η μεγαλύτερη λεπτομέρεια στα δεδομένα που συλλέγουν .Ουσιαστικά καταγράφουν κάθε βήμα που εκτελεί ο επιτιθέμενος επακριβώς .Με τον τρόπο αυτό αναγνωρίζουν την τακτική και στρατηγική που ακολουθεί ο εχθρός και αναλύουν την συμπεριφορά του. Έτσι έχουν την δυνατότητα να καταλήγουν σε συμπεράσματα χρήσιμα για την αντιμετώπιση μελλοντικών επιθέσεων. Το μειονέκτημα όμως που παρουσιάζουν είναι ο υψηλός βαθμός πολυπλοκότητας και κινδύνου που προσθέτουν σε ένα σύστημα . Επιπλέον απαιτούν περισσότερο setup time , monitoring time και περισσότερες πηγές για να δημιουργήσουν και να διαμορφώσουν το λειτουργικό σύστημα που εφαρμόζονται .Παράλληλα υπάρχει και μια υποβόσκουσα αδυναμία , ένα honeypot το οποίο δεν ελέγχεται μπορεί να υποθάλψει εγκληματική δραστηριότητα με την καταγραφή , αποθήκευση και διανομή παράνομου υλικού όπως αριθμούς πιστωτικών καρτών

Εκτός όμως από την καταγραφή επιθέσεων τα honey pots έχουν και μια σειρά από άλλες εφαρμογές όπως η προστασία δικτύων και των δεδομένων τους δημιουργώντας σύγχυση στους επίδοξους hackers .Η ευελιξία που διαθέτουν ταιριάζει τέλεια με την δυναμική φύση των ψηφιακού κόσμου .Και οι δύο κατηγορίες honey pots παρουσιάζουν μειονεκτήματα και πλεονεκτήματα .Εξαρτάται από τις προθέσεις που έχουμε για το πια κατηγορία από τις δύο θα χρησιμοποιήσουμε .

4.3.2.1 Η λειτουργία των Honey pot – Honey net

Για την εύρυθμη και αποτελεσματική λειτουργία ενός Honey pot και ενός κατ'επέκταση Honey net απαιτείται να λαμβάνονται υπόψη τέσσερεις διαφορετικοί παράγοντες : το data control , data capture , data analysis και το data collection .

4.3.2.1.1 Honey pot Data Control

Με την εφαρμογή ενός τέτοιου συστήματος υπάρχει ο κίνδυνος ο επιτιθέμενος να χρησιμοποιεί το honey net που χρησιμοποιούμε για να πραγματοποιήσει περαιτέρω επιθέσεις στα συστήματα που δεν είναι συνδεδεμένα στα honey pots .Σκοπός επομένως του Data control είναι να καταφέρει να απαλείψει αυτό τον κίνδυνο .Προσπαθεί να εξασφαλίσει ότι από την στιγμή που ο επιτιθέμενος βρίσκεται εντός του honey net δεν θα μπορεί είτε εκούσια είτε ακούσια να βλάψει άλλα non-honey net συστήματα .Για να μπορέσει να το πετύχει αυτό θα

πρέπει να χρησιμοποιήσει μια σειρά από μέτρα με σημαντικότερο από όλα το έλεγχο της κίνησης που εξέρχεται και εισέρχεται στο σύστημα και χωρίς να γίνει αντιληπτό από τον επιτιθέμενο .Όσο μεγαλύτερη ελευθερία απολαμβάνει ο τελευταίος στο honey net τόσο μεγαλύτερος κίνδυνος υπάρχει να καταφέρει να παρακάμψει το Data control .Η ισορροπία ανάμεσα στην ελευθερία κινήσεων στο honey net και στον περιορισμό των κινήσεων τους είναι μια σημαντική απόφαση που πρέπει να ληφθεί πριν από την εφαρμογή ενός τέτοιου συστήματος .Φυσικά το Data control δεν μπορεί να εγγυηθεί εξ ολοκλήρου ότι η βλαπτική συμπεριφορά του επιτιθέμενου θα περιοριστεί εντός του honey net αλλά περιορίζει κατά πολύ τον κίνδυνο .

4.3.2.1.2 Honey pot Data capture

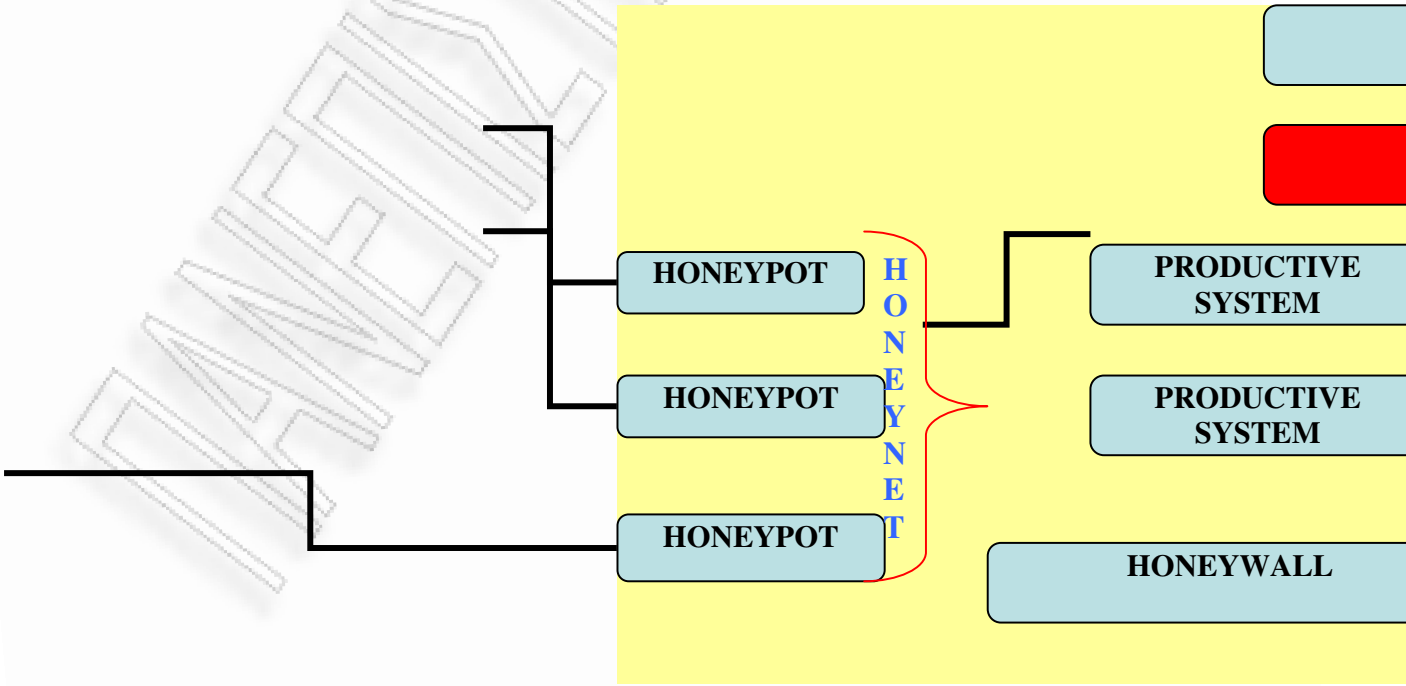
Με τον όρο αυτό περιγράφεται η παρακολούθηση των δραστηριοτήτων και των κινήσεων του επιτιθέμενου εντός του honey net .Στην συνέχεια όλα τα δεδομένα που συλλέγονται αναλύονται για τον προσδιορισμό των εργαλείων , μεθόδων και τακτικών αλλά και κάθε βήματος που εκτελείται από τον εχθρό για την υπερνίκηση του συστήματος .Στόχος του data capture είναι η συλλογή όσον το δυνατόν μεγαλύτερου όγκου δεδομένων σχετικά με τον εχθρό , χωρίς όμως να γίνει αντιληπτό από τον ίδιο ότι η συμπεριφορά του παρακολουθείτε .Φυσικά όσο μεγαλύτερος όγκος πληροφοριών συγκεντρώνεται τόσο μεγαλύτερη είναι η αξία του honey net .Αυτός δεν πρέπει να συγκεντρώνεται τοπικά διότι υπάρχει ο κίνδυνος να μορφοποιηθεί ή ακόμα και να διαγραφεί από τον επιτιθέμενο .Επομένως όλο το συγκεντρωμένο υλικό πρέπει να μεταφέρεται σε ένα ξεχωριστό σύστημα όπου και θα αποθηκεύεται .Το τελευταίο πρέπει να βρίσκεται έξω από το honey net και να μην είναι κάποιο άλλο honey pot προκειμένου να είναι αδύνατος ο εντοπισμός και η διαγραφή από τον επιτιθέμενο .

4.3.2.1.3 Honey pot Data analysis

Αποτελεί τον τρίτο παράγοντα που πρέπει να λαμβάνεται υπόψη. Ένα honey net θα είναι άχρηστο αν τα δεδομένα που συλλέγονται δεν μπορούν να αξιολογηθούν και αναλυθούν κατάλληλα σε λογικές και εφαρμόσιμες πληροφορίες .Επομένως θα πρέπει να υπάρχει ο κατάλληλος μηχανισμός ανάλυσης αυτών των δεδομένων .Συχνά ο όγκος των data που συγκεντρώνονται είναι πάρα πολύ μεγάλος με αποτέλεσμα να είναι πολύ δύσκολη αν όχι αδύνατη η ανάλυση αυτών χωρίς την χρήση διαφόρων μεθόδων .Σε αυτές μπορεί να μην υπάρχει ανθρώπινη αλληλεπίδραση ενώ υπάρχουν και μέθοδοι όπου εμφανίζεται αλληλεπίδραση .

4.3.2.1.4 Honey pot Data collection

Η παραπάνω έννοια έχει νόημα μόνο αν το honey net αποτελεί μέρος ενός κατανεμημένου περιβάλλοντος .Όλα τα δεδομένα που συγκεντρώνονται μεταφέρονται από τα διάφορα σημεία του δικτύου σε μια κεντρική τοποθεσία .Με τον τρόπο αυτό συνδυάζονται διαφορετικές πηγές μεγιστοποιώντας την αξία των πληροφοριών που θα προκύπτουν από την ανάλυση αυτών.

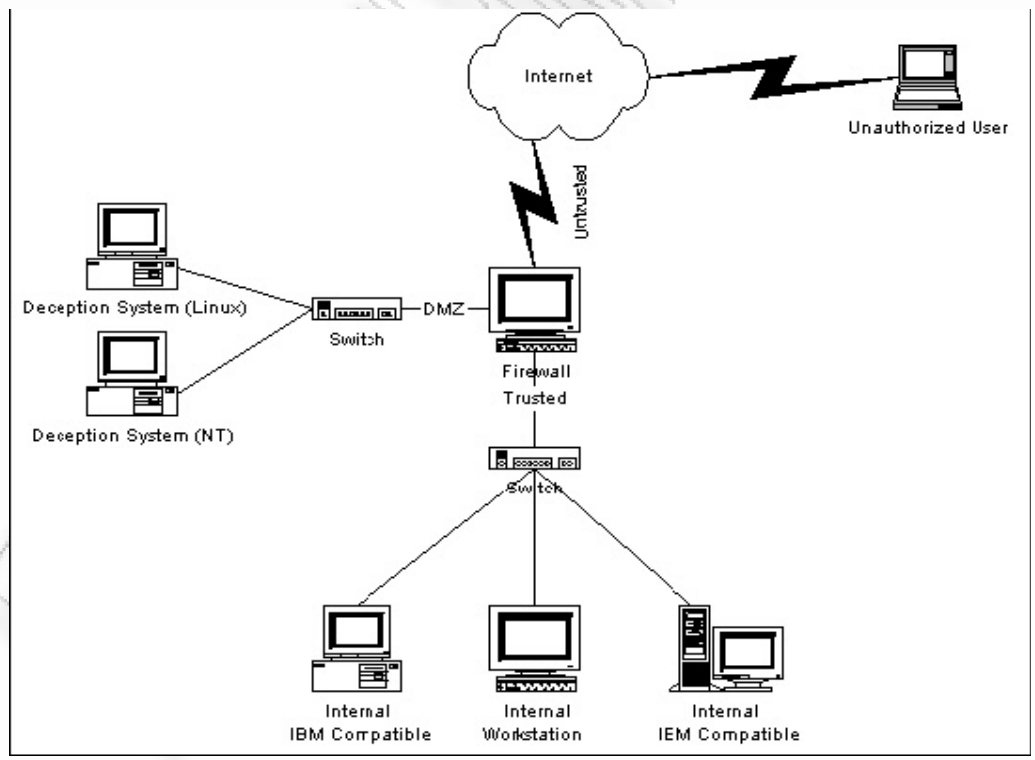


Διάγραμμα 3:Σχηματικό διάγραμμα της λειτουργίας του honey pot-honey net 2

4.3.2.2 Η τοπολογία των Honey pot – Honey net

Η επιλογή του σημείου τοποθέτησης ενός honey pot εξαρτάται και από το είδος που επιλέγουμε να χρησιμοποιήσουμε (low-high interaction). Στην παράγραφο αυτή θα αναφέρουμε τις δύο βασικές θέσεις που μπορεί να πάρει.

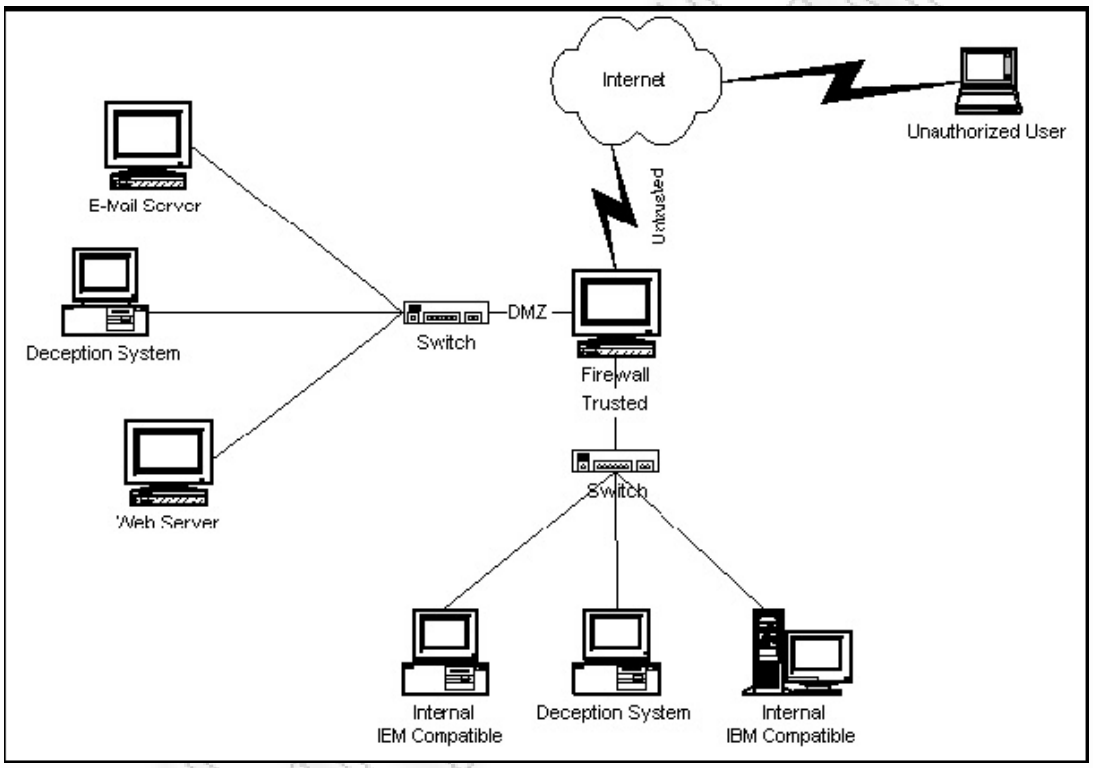
1. Τοποθέτηση του συστήματος στην DMZ ζώνη ή αλλιώς ΄΄sacrificial lamb΄΄. Με τον τρόπο αυτό απομακρύνεται ο κίνδυνος επιθέσεων στο πραγματικό δίκτυο όπως φαίνεται και στην παρακάτω εικόνα. Σε περίπτωση που ο μη εξουσιοδοτημένος χρήστης προσπαθήσει να εισέλθει στο δίκτυο scanάροντας πρώτα για τυχόν αδυναμίες , όλη η προσοχή του θα προσανατολισθεί αλλού .Στην περίπτωση αυτή το honey pot δεν έχει άμεση σύνδεση με το production network όπως φαίνεται και στην παρακάτω εικόνα .Η βασική ιδέα για αυτή την τοπολογία είναι μπορέσουμε να εγκλωβίσουμε την επιθυμία του επιτιθέμενου , δηλαδή τους δίνουμε την εντύπωση ότι έχουν αυτό που επιθυμούν .



ΕΙΚΟΝΑ 38 : Τοποθέτηση του Honey pot στην DMZ

2. Τοποθέτηση του συστήματος σε ΄΄ναρκοπέδιο΄΄ (minefield) .Στην περίπτωση αυτή το decoy system τοποθετείται ανάμεσα σε άλλα λειτουργικά συστήματα ,έμπιστα δίκτυα και έμπιστες DMZ όπως φαίνεται και στην παρακάτω εικόνα .Έτσι κατά την διάρκεια του scanning από τον επιτιθέμενο θα αποκαλυφθούν τα περιεχόμενα του honey pot ενώ το production server θα παραμείνει αλώβητο .Τοπολογία αυτής της μορφής έχουμε στα honey pots La Brea , Honey d και Mantrap.*(97)*

3.



ΕΙΚΟΝΑ 39 : Τοποθέτηση του Honey pot ως Minefield

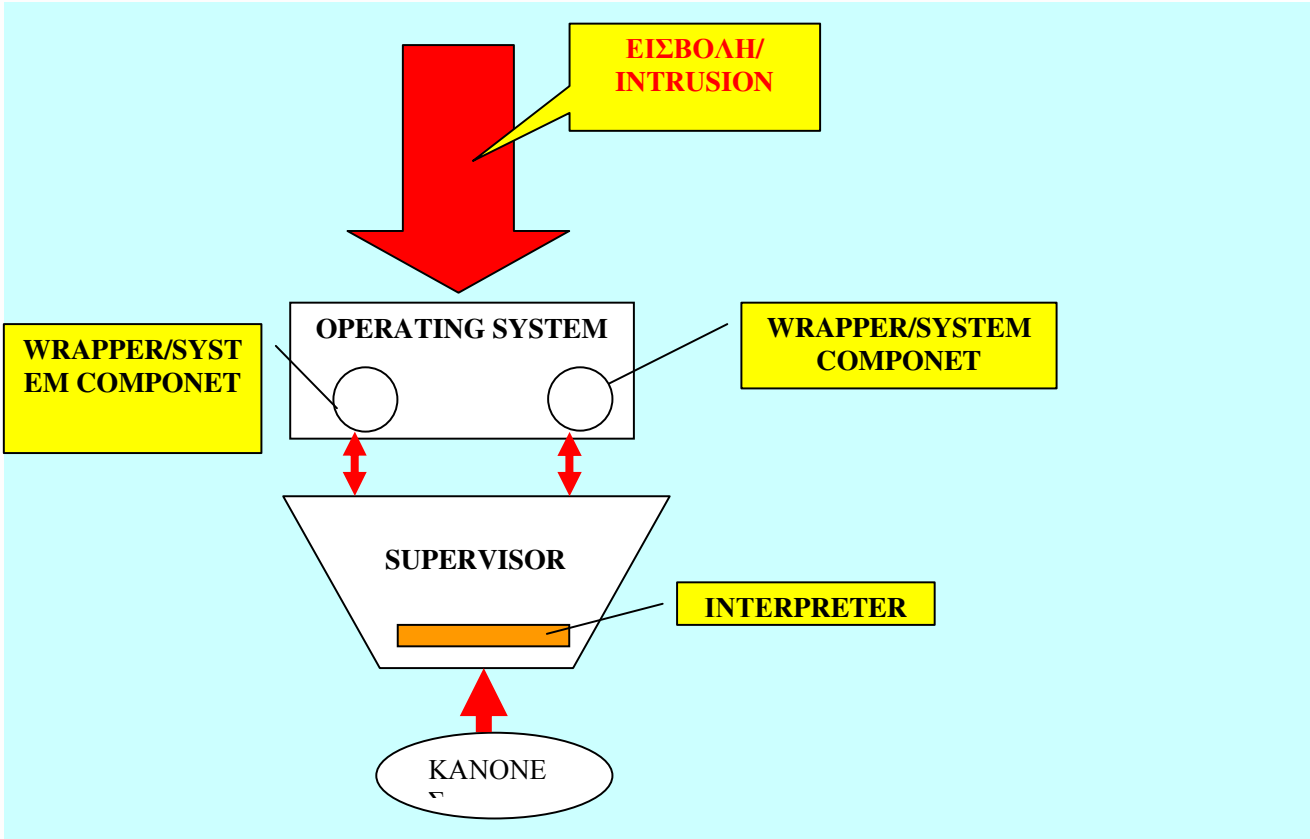
4. Proximity decoys.Στην περίπτωση αυτή το honey pot αποτελεί και αυτό μέρος του δικτύου στο οποίο ανήκουν οι κύριοι servers με αποτέλεσμα να μην υπάρχουν νομικά προβλήματα από την χρήση τους και η καταγραφή δραστηριοτήτων στο ίδιο το δίκτυο είναι εξολοκλήρου νόμιμη .Παράλληλα εξαιτίας της αμεσότητας στα production system υπάρχει η δυνατότητα του επαναπροσδιορισμού του traffic στην περίπτωση που κάποια επίθεση ανιχνευθεί .Αυτή η μέθοδος είναι ιδιαίτερα αποτελεσματική για την μη εξάπλωση worms και virus.

4.3.3 Software Decoys

Η πρώτη δημόσια εμφάνιση τέτοιων συστημάτων υπήρξε μόλις το 2001 από τους James B.Michael και Richard D.Riehle (97) με σκοπό να καλύψουν μια μεγάλη γκάμα αμυντικών δραστηριοτήτων σε Η/Υ και δίκτυα. Στόχος των software decoys είναι η προσθήκη και άλλων στρωμάτων ασφαλείας-γραμμών άμυνας τα οποία ονομάζονται software wrappers .Τα τελευταία δημιουργούν σύγχυση και αποπροσανατολισμό στον επιτιθέμενο , αποσπούν την προσοχή του δίνοντας παράλληλα την εντύπωση ότι η επίθεση που εκτελούν εκτελείται κανονικά και μάλιστα με επιτυχία.

Η ανάγκη για Software Decoys προήλθε από το γεγονός της εξέλιξης της τεχνολογίας των Η/Υ και την χρήση όλο και ΄΄εξυπνότερων ΄΄ μεθόδων επίθεσης με αποτέλεσμα τα υπάρχοντα συστήματα όπως firewalls intrusion detection system να μην μπορούν να αντιμετωπίσουν τις νέες απειλές .Παράλληλα ώθηση στον συγκεκριμένο τομέα δόθηκε από την ψηφιοποίηση του πολέμου (δικτυοκεντρικός πόλεμος) στον οποίο η ασφάλεια και η ταχύτητα αποτελούν κορυφαίες προτεραιότητες .Έτσι τα Software Decoys αποτελούν μια βιώσιμη δεύτερη γραμμή άμυνας ικανή να σταματήσει τους επίδοξους εισβολείς .

Η λειτουργία τους στηρίζεται όχι στην αντιμετώπιση μιας εισβολής με την παραδοσιακή έννοια του όρου , αλλά στην προσαρμογή σε αυτή .Η προσαρμογή έχει περισσότερο την έννοια της ανεκτικότητας ενώ παράλληλα η προσπάθεια μη εξουσιοδοτημένης εισόδου αναλύεται και μεταφέρεται σε ένα ΄΄προθάλαμο΄΄ .Σε αυτόν χρησιμοποιούνται διάφορες τεχνικές παραπλάνησης για την σύγχυση του αντιπάλου .Στην παρακάτω εικόνα φαίνεται η αρχιτεκτονική των software decoys και η χρήση των wrappers για την αντιμετώπιση των επιθέσεων .Αυτά συμβιώνουν με τα λειτουργικά συστήματα και ελέγχονται μέσω προκαθορισμένων κανόνων και οδηγιών οι οποίες ορίζουν με λεπτομέρειες τους τρόπους αντίδρασης και συμπεριφοράς .Τα συστήματα αυτά εφαρμόζονται κυρίως σε στρατιωτικά δίκτυα και συστήματα με αποτέλεσμα πολλές πληροφορίες να είναι διαβαθμισμένες .



Διάγραμμα 4 : Σχηματικό διάγραμμα της λειτουργίας του Software Decoy

4.4 Παγίδες της ηλεκτρονικής παραπλάνησης

Η χρήση της ψηφιακής παραπλάνησης ως αμυντικό μέσο εμπεριέχει πιθανώς και ορισμένες παγίδες όπως και στην περίπτωση της συμβατικής παραπλάνησης .Το βασικότερο από όλα είναι η πιθανότητα οι νόμιμοι χρήστες ενός δικτύου να διαπιστώσουν ότι η προσπάθεια τους να έχουν πρόσβαση σε ένα συγκεκριμένο directory για παράδειγμα , τους έχει οδηγήσει σε ένα τελείως διαφορετικό μονοπάτι .Ας φανταστούμε την ενόχληση που θα νιώσει κάποιος αν εργάζεται πάνω σε ένα αρχείο αλλά δεν μπορεί να σώσει τις αλλαγές που έχει κάνει σε ένα συγκεκριμένο directory ,ενώ διαπιστώνει ότι τελικά ότι το αρχείο λείπει επειδή το directory ήταν παραπλανητικό στα πλαίσια ενός honey pot-honey net .Επομένως η χρήση τέτοιων μέσων πιθανόν να επηρεάσει αρνητικά και τους νόμιμους χρήστες με δυσάρεστα και απρόβλεπτα αποτελέσματα .

Παράλληλα όταν εφαρμόζουμε μεθόδους ψηφιακής παραπλάνησης ενάντια σε hackers τα αποτελέσματα αυτής της προσπάθειας εξαρτώνται από την φύση της επιθέσεως .Έτσι ένας ερασιτέχνης από την αποτυχία της προσπάθειας του θα απογοητευθεί και θα κινηθεί ενάντια ενός άλλου πλέον συστήματος .Στην περίπτωση αυτή η παραπλάνηση θεωρείται επιτυχής .Από την άλλη πλευρά ο εντοπισμός από την πλευρά του επιτιθέμενου της cyber deception πιθανόν να προκαλέσει τους επιτιθέμενους οι οποίοι θα δουν την συγκεκριμένη κατάσταση ως πρόκληση .Αυτό θα τους οδηγήσει να προσπαθήσουν σκληρότερα χρησιμοποιώντας εναλλακτικούς τρόπους για να προσπεράσουν τα διάφορα εμπόδια .

4.5 Τρομοκράτες, κυβερνοτρομοκράτες (cyber terrorist) και ηλεκτρονική παραπλάνηση.

Σύμφωνα με πολλούς μελετητές της τρομοκρατίας οι τακτικές που χρησιμοποιούνται από τις διάφορες ομάδες είναι καθαρά παραπλανητικές από την φύση τους εξαιτίας της αίσθησης του φόβου που δημιουργούν έναντι της πραγματικής απειλής που πρεσβεύουν .Το ίδιο συμβαίνει και στην κυβερνοτρομοκρατία είτε προέρχεται από μεμωνομένα άτομα είτε από ομάδες .Για παράδειγμα ένας μοναχικός τρομοκράτης καταφέρνει να παραβιάσει την ασφάλεια ενός δικτύου. Η δημοσιότητα που θα λάβει το γεγονός αυτό είναι τεράστια .Ουσιαστικά τα ΜΜΕ θα γίνουν ένα πληρεξούσιο όργανό του στην υπηρεσία του .Οι αδυναμίες του συστήματος που πρόσβαλε θα αναπαραχθούν σε διάφορα έντυπα ηλεκτρονικά και μη ,οι κυβερνητικοί οργανισμοί θα κατηγορηθούν για ανικανότητα αποτροπής μιας τέτοιας κατάστασης και διάφοροι επίδοξοι μιμητές θα εμφανιστούν .

Ακόμα μεγαλύτερης έκτασης θα είναι η δράση τρομοκρατικής ομάδας με κατάλληλες ικανότητες και γνώσεις .Πέρα από την πραγματική διάσταση της απειλής το ψυχολογικό και πολιτικό αντίκτυπο από την δράση της θα είναι πολύ μεγαλύτερο .Φυσικά παρόμοιο γεγονός μέχρι σήμερα δεν έχει καταγραφεί (ή τουλάχιστον δεν υπάρχει ανάλογη δημοσίευση) με αποτέλεσμα αρκετοί να είναι εκείνοι που θεωρούν την όλη συζήτηση απλά μια ενοχλητική υπενθύμιση .

Για την αντιμετώπιση αυτών των ομάδων και των ικανοτήτων τους υπάρχουν μια σειρά από μέτρα , με την εφαρμογή των οποίων μπορούν να παραπλανηθούν αρκεί να λάβουμε υπόψιν μας τα εξής :

1. Πολλές από τις τρομοκρατικές οργανώσεις έχουν ιεραρχική δομή πατριαρχικού τύπου με φανατικούς οπαδούς και φωτισμένες ηγεσίες οι οποίες θεωρούνται από τους οπαδούς τους αλάθητες .Επομένως στοχεύοντας και παραπλανώντας την ηγεσία τους παραπλανάμε όλη την οργάνωση.

2. Για την αποτελεσματική λειτουργία μια τέτοιας ομάδας απαιτείται ακριβής πληροφόρηση. Έτσι εκτός από τις παραδοσιακές πηγές πληροφοριών όπως τα μέσα ενημέρωσης , άλλα μέσα όπως το διαδίκτυο εξαπλώνονται συνεχώς και με γεωμετρικούς ρυθμούς .Αυτό έχει ως αποτέλεσμα να δημιουργούνται νέοι τρόποι παραπλάνησης: η ψηφιακή παραπλάνηση .

3. Όλες οι τρομοκρατικές οργανώσεις παλεύουν να ισορροπήσουν ανάμεσα στην επιχειρησιακή αποδοτικότητα από την μία πλευρά και την ασφάλεια από την άλλη .Αυστηρά μέτρα ασφαλείας συνεπάγονται δραστική μείωση της αποτελεσματικότητας της δράσεως τους .Άρα οι επιχειρήσεις παραπλάνησης πρέπει να στοχεύουν στην απώλεια εμπιστοσύνης από την πλευρά των τρομοκρατών και στην ίδια την ασφάλεια τους , για να έχουν ως απόρροια την μείωση της αποτελεσματικότητας τους .

Η εξέλιξη των τρομοκρατικών ομάδων δείχνει ότι οδηγούμαστε σε μια πιο αποσπασματική δομή στην οποία πολλές μικρές και επικίνδυνες ομάδες με τους ίδιους πολιτικούς , θρησκευτικούς και κοινωνικούς στόχους λειτουργούν μαζί και σε συνεργασία για την επίτευξη του κοινού σκοπού .Δεν υπάρχει η αυστηρή πατριαρχική δομή , αλλά η σύνδεση μεταξύ τους είναι χαλαρή ενώ ανά πάσα στιγμή μπορεί να διακοπεί .Ως βασικό μέσο επικοινωνίας χρησιμοποιούν το διαδίκτυο και άλλες τεχνολογίες επικοινωνιών .Έτσι δεν υπάρχει κάποιο συγκεκριμένο κέντρο στο οποίο να στοχεύουν οι υπηρεσίες ασφαλείας αλλά πανσπερμία απειλών .Παράλληλα δεν περιορίζονται από εθνικά και γεωγραφικά σύνορα δυσκολεύοντας ακόμα περισσότερο την αντιμετώπιση τους .

Από την άλλη πλευρά όμως αυτή η χαλαρή δομή τους έχει ως αποτέλεσμα να υπάρχει μεγάλη ανάγκη για επικοινωνία και συντονισμό μεταξύ τους .Αυτό το σημείο πρέπει να εκμεταλλευθούμε για πραγματοποιήσουμε την ηλεκτρονική παραπλάνηση , δεδομένου της μεγάλης χρήσης των διαφόρων επικοινωνιακών μέσων και κυρίως του διαδικτύου .Με την χρήση για παράδειγμα του e-mail είναι εκτεθειμένοι στο tracing ,surveillance και cyber attack .Επιπλέον στις σύγχρονες εξτρεμιστικές ομάδες συνυπάρχει ο ΄΄κλασσικός΄΄ επιχειρησιακός

κλάδος με αυτό του ψηφιακού τομέα .Θα πρέπει επομένως αυτοί οι δύο να μπορέσουν να συντονιστούν για να πετύχουν καλύτερα αποτελέσματα .

Λαμβάνοντας υπόψη τα παραπάνω καθώς και αυτά που αναλύσαμε στο Κεφάλαιο ΙΙ μπορούμε να καταλήξουμε στον παρακάτω πίνακα *Matrix* για τις πιθανότητες παραπλάνησης. Εδώ παρουσιάζονται οι έξι κατηγορίες τρομοκρατικών ομάδων και οι τέσσερις στόχοι που πιθανόν να μπορούν να παραπλανηθούν (η ηγεσία ,το intelligence ,η ασφάλεια τους και τα δίκτυα επικοινωνιών τους) .Οι πιο πιθανοί στόχοι έχουν σκιαχθεί με κόκκινο χρώμα .Από την ανάλυση του παρακάτω πίνακα βλέπουμε ότι μερικές από τις κατηγορίες cyber terrorist είναι ευαίσθητες στην ψηφιακή/ηλεκτρονική παραπλάνηση , εξαιτίας της εξάρτησης τους από την νέα τεχνολογία .Επιπλέον διαπιστώνουμε ότι οι ομάδες που δρουν υπό καλυμμένη ή όχι κρατική υποστήριξη είναι δύσκολο να αντιμετωπισθούν με τέτοια μέσα .Το επίπεδο ασφαλείας , οργάνωσης και γνώσεων είναι συνήθως πολύ υψηλό και διαφέρει από τις υπόλοιπες οργανώσεις του είδους , παρά τις ευκαιρίες που προσφέρονται από την ηλεκτρονική παραπλάνηση στις μέρες μας .

Actors	Ηγεσία	Cyberspace intelligence	Ασφάλεια	Δίκτυα Επικοινωνιών
1.Μοναχικός τρομοκράτης	Επιχειρησιακό νους και "σώμα'' το ίδιο πρόσωπο	Το διαδίκτυο η βασική πηγή πληροφοριών	Δεν απαιτείται να έχουν εμπιστοσύνη σε άλλους	Δεν απαιτούνται τέτοια δίκτυα
2.Μικρές τεχνολογικά εκπαιδευμένες ομάδες	Ο επικεφαλής της ομάδας έχει τον άμεσο έλεγχο αυτής	Το διαδίκτυο η βασική πηγή πληροφοριών	Σφιχτή δομή οργάνωσης , με απόλυτη εμπιστοσύνη μεταξύ των μελών	Δεν απαιτούνται τέτοια δίκτυα
3.Μικρές τεχνολογικά εκπαιδευμένες ομάδες ως μέρος ενός ευρύτερου δικτύου	Ο επικεφαλής της ομάδας διαφορετικό πρόσωπο από τον επικεφαλής του δικτύου	Το διαδίκτυο η βασική πηγή πληροφοριών	Σφιχτή δομή οργάνωσης , με απόλυτη εμπιστοσύνη μεταξύ των μελών	Δεν απαιτούνται τέτοια δίκτυα
4.Μεγάλες εξτρεμιστικές ,θρησκευτικές ομάδες	Ο επικεφαλής της ομάδας έχει τον άμεσο έλεγχο αυτής	Το διαδίκτυο η βασική πηγή πληροφοριών	Δεν υπάρχει απόλυτη ασφάλεια και πλήρης εμπιστοσύνη μεταξύ των μελών	Απαιτούνται ανάλογα δίκτυα για τον συντονισμό τέτοιων ομάδων
5.Τρομοκρατικές ομάδες υποστηριζόμενες από κρατικούς φορείς	Ο επικεφαλής της ομάδας είναι πιθανόν γνωστό πρόσωπο	Υπάρχει άμεση πρόσβαση και σε άλλες πηγές πληροφοριών	Εχεμύθεια και ασφάλεια που δεν στηρίζονται στο φόβο	Απαιτούνται ανάλογα δίκτυα για τον συντονισμό τέτοιων ομάδων

6.Τρομοκρατικές ομάδες υποστηριζόμενες υπογείως από κρατικούς φορείς	Δύσκολος ο καθορισμός της ιεραρχικής δομής της οργάνωσης	Υπάρχει άμεση πρόσβαση και σε άλλες πηγές πληροφοριώ	Εχεμύθεια και ασφάλεια που δεν στηρίζονται στο φόβο	Απαιτούνται ανάλογα δίκτυα για τον συντονισμό τέτοιων ομάδων

Πίνακας 5 : Η παραπλάνηση εναντίον των Cyberterrorist

Σύμφωνα με τους Rowe και Rothstein από τα διάφορα είδη της παραπλάνησης θεωρούνται αποτελεσματικά ως αμυντικό μέσο η παραπληροφόρηση ,η δημιουργία ψεύτικης εικόνας και η οξυδέρκεια του αμυνόμενου *(98).*Αυτό σε συνδυασμό με τα στάδια της ηλεκτρονικής επίθεσης που έχουμε αναλύσει στο Κεφάλαιο ΙΙ δημιουργούν τον παρακάτω πίνακα . Σε αυτόν εμφανίζεται η βιωσιμότητα της ηλεκτρονικής παραπλάνησης στα διάφορα στάδια μιας επιθέσεως σε δίκτυο η Η/Υ .

ΣΤΟΧΟΣ ΤΗΣ ΠΑΡΑΠΛΑΝΗ-ΣΗΣ ΒΗΜΑΤΑ ΕΠΙΘΕΣΣΩΣ	ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ	ΨΕΥΤΙΚΗ ΕΙΚΟΝΑ - DISPLAYS (προσομοίωση των αποτελεσμάτων της επίθεσης)	ΟΞΥΔΕΡΚΕΙΑ-INSIGHT (πρόβλεψη του επόμενου βήματος του επιτιθέμενου)
ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΕΠΙΤΗΡΗΣΗ ΤΟΥ ΧΩΡΟΥ	Εγκαταλείπεται το Web Search	Δεν υπάρχει επίθεση , μη εφαρμόσιμη οποιαδήποτε παραπλάνηση	Δυσκολία διαχωρισμού μεταξύ των νόμιμων χρηστών και των υπολοίπων
SCANNING	Οι αυτόματοι scanners εξαπατώνται	Δεν υπάρχει επίθεση , μη εφαρμόσιμη οποιαδήποτε παραπλάνηση	Δυσκολία καθορισμού των προθέσεων που κρύβονται πίσω από το Scanning
ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΗ ΠΡΟΣΒΑΣΗ	Ο επιτιθέμενος πιθανόν να θεωρήσει μάταιη την προσπάθεια και να προσπαθήσει ξανά με άλλο τρόπο	Ο επιτιθέμενος πιθανόν να εξαπατηθεί από την φαινομενική επιτυχία	Ο επιτιθέμενος αποκαλύπτεται και μεταφέρεται στον ΄΄προθάλαμο΄΄ (software decoys)
ΔΙΑΤΗΡΗΣΗ ΤΗΣ ΠΡΟΣΒΑΣΗΣ	Ο επιτιθέμενος πιθανόν να θεωρήσει μάταιη την προσπάθεια και να αποχωρήσει	Ο επιτιθέμενος θεωρεί ότι η επίθεση του είναι επιτυχής	Ο επιτιθέμενος θεωρεί ότι η επίθεση του είναι επιτυχής

Πίνακας 6 :Ηλεκτρονική παραπλάνηση και ψηφιακές επιθέσεις

Από την μελέτη του ανωτέρω πίνακα βλέπουμε ότι η παραπλάνηση έχει περιορισμένη επιτυχία κατά το στάδιο της αναγνώρισης και του scanning .Δεν μπορούμε να είμαστε βέβαιοι για τις προθέσεις κάποιου που εκτελεί μια τέτοια ενέργεια .Επομένως δεν θα πρέπει να προσπαθούμε να την παραπλανήσουμε .Αντίθετα τα intrusion-detection system θα πρέπει να βρίσκονται σε εγρήγορση για τα επόμενα που πιθανόν να ακολουθήσουν σε μια cyber επίθεση .Η προσπάθεια απόκτησης μη εξουσιοδοτημένης πρόσβασης αποτελεί σαφή ένδειξη ότι βρισκόμαστε κατά την διάρκεια μιας επιθέσεως και θα πρέπει να την αντιμετωπίσουμε αποτελεσματικά με τα μέσα παραπλανήσεως που διαθέτουμε . Φυσικά τα honeypots software decoys αποτελούν μια δεύτερη γραμμή άμυνας στην περίπτωση αυτή καθώς και στην περίπτωση που η παράνομη είσοδος στο δίκτυο ή τον Η/Υ έχει ήδη πραγματοποιηθεί .

ΚΕΦΑΛΑΙΟ V Επίλογος –Τελικά συμπεράσματα .

Σκοπός της παρούσας εργασίας ήταν να αναδείξει τον κίνδυνο που πρεσβεύει η Κυβερνοτρομοκρατία για τις Δυτικές κοινωνίες κυρίως , εξετάζοντας παράλληλα το φαινόμενο της τρομοκρατίας , της ασφάλειας στον ψηφιακό κόσμο και τις κρίσιμες υποδομές .Παρά την πλούσια βιβλιογραφία για κάθε ένα από τα παραπάνω ξεχωριστά ελάχιστα υπάρχουν που να συνδυάζουν τις παραπάνω έννοιες .

Διαπιστώσαμε αρχικά ότι cyber terrorist έχουν τα ίδια πολιτικά , θρησκευτικά και κοινωνικά κίνητρα με τους ΄΄ παραδοσιακούς τρομοκράτες ΄΄ και στόχο να προκαλέσουν αντίστοιχη ζημιά με τους τελευταίους .Παρά την μη ύπαρξη επίσημης καταγραφής πράξεων κυβερνοτρομοκρατίας μέχρι σήμερα , η κατάσταση αναμένεται να αλλάξει δραματικά όσο οι σύγχρονες κοινωνίες όλο και περισσότερο στηρίζονται στους Η/Υ και τα δίκτυα ακόμα και για τις καθημερινές τους λειτουργίες . Παράλληλα πολλές τρομοκρατικές ομάδες αλλά και κράτη που κρύβονται πίσω από αυτές θεωρούν ότι το συγκεκριμένο επιστημονικό-επιχειρησιακό πεδίο , τους δίνει την ευκαιρία να πολεμήσουν τα ανεπτυγμένα δυτικά κράτη , αφού δεν μπορούν να κάνουν το ίδιο στο πεδίο του συμβατικού πολέμου .

Επιπλέον διαπιστώνουμε ότι η παραπλάνηση αποτελεί συνηθισμένη πρακτική τόσο στον φυσικό κόσμο όσο και στην ανθρώπινη ιστορία με τα παραδείγματα που αναφέραμε .Με βάση αυτά η έννοια της έχει περάσει νομοτελειακά και στον κόσμο της ασφάλειας των Η/Υ και δικτύων ως αμυντικό μέσο .Φυσικά πολλές φορές η ηλεκτρονική παραπλάνηση χρησιμοποιείτε και ως κακόβουλο όργανο για ανήθικους και παράνομους σκοπούς .

Είναι δεδομένο ότι από την στιγμή που μπορούμε να παραπλανήσουμε τους τρομοκράτες μπορούμε να παραπλανήσουμε και τους cyberterrorist.Τα μέσα που θα χρησιμοποιηθούν για τον σκοπό αυτό απαιτούν πιο εξειδικευμένες γνώσεις και τεχνικά μέσα .Από την άλλη πλευρά πολλά από τα ΄΄εργαλεία΄΄ των cyber επιθέσεων χρησιμοποιούνται και από λιγότερο επικίνδυνους hackers .Άρα για την αποτελεσματική αντιμετώπιση των τρομοκρατών

μπορούμε να αναπτύξουμε εξειδικευμένα μέσα στηριζόμενοι στην πολλή καλή και λεπτομερή ανάλυση των μεθόδων που χρησιμοποιούν .

Όμως παρά την καταγραφή με το πέρασμα του χρόνου διαφόρων τρομοκρατικών πράξεων σε διάφορα σημεία του πλανήτη δεν έχουμε επίσημη καταγραφή αντίστοιχων πράξεων Κυβερνοτρομοκρατίας παρά μόνο τον τελευταίο χρόνο στις ΗΠΑ .Επομένως τα συμπεράσματα που θα εξαχθούν είναι πιθανόν παρακινδυνευμένα . Η αντιμετώπιση τέτοιων απειλών στηρίζεται κατά κύριο λόγο στην πρόληψη και την συλλογή πληροφοριών και εκτελείται από επίσημες κρατικές αρχές (πχ NSA στις ΗΠΑ) , στα αρχεία και τις βάσεις δεδομένων των οποίων δεν έχουμε πρόσβαση .Παράλληλα ενώ γνωρίζουμε τόσα πολλά για την ψυχολογία του τρομοκράτη , τα αίτια του φαινομένου ,τους στόχους του , το περιβάλλον του και την φύση της απειλής , γνωρίζουμε ελάχιστα για την απειλή αυτή καθαυτή , ιδιαιτέρως ενάντια στις κρίσιμες υποδομές όπου στηρίζεται η λειτουργία των σύγχρονων κοινωνιών .

Τελικά η μελέτη του φαινομένου θα πρέπει να είναι συνεχής .Όπως συνεχώς αναβαθμίζονται και ανανεώνονται τα antivirus software ενάντια σε νέες γενιές ηλεκτρονικών ιών έτσι και οι μέθοδοι ηλεκτρονικής παραπλάνησης θα πρέπει συνεχώς να επεξεργάζονται για να προσφέρουν αποτελεσματικότερη προστασία στις συνεχώς πιο επικίνδυνες και καταστροφικές απειλές που αντιμετωπίζουμε στον ψηφιακό κόσμο .

ΚΕΦΑΛΑΙΟ VI ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Air Force and the Cyberspace mission defending the Air Force's Computer Network in the future./Shane P.Courville,Lt Col,USAF December 2007
2. www fcw.com by Josh Rogin 13Feb 2007
3. Information Warfare /An Air Force Policy for the role of Publick Affairs by Robin K.Crumn /Major USAF Alabama 1996
4. Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Pres
5. Franklin L.Ford ,Political Murder :From Tyrannicide to Terrorism(Cambridge :Harvard University Press , 1985)

International Encyclopedia of Terrorism 1997 ΄΄The Assasins :A terror cult΄΄

7.Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians: Why it has Always Failed and Why it will Fail Again*

(New York: Random House, 2002), 52-63.

8.*International Encyclopedia of Terrorism*, 1997 ed., s.v. "Terror in the French Revolution 1789-1815."

9. *International Encyclopedia of Terrorism*, 1997 ed., s.v. "Russian Anarchist Terror."

10. Martin L. Van Creveld, *The Transformation of War* (New York: The Free Press, 1991)

11. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 70.

12.Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003*

(Washington, D.C., April 2004, revised 22 June 2004), 177-178; and *Patterns of Global*

13.Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 38.

14. FM 100-20, *Military Operations in Low Intensity Conflict*, 5 December 1990; and Joint Publication 1-02,*Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, as amended through January 2003.

15. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 39.

16.Title 28, Code of Federal Regulations, Section 0.85, *Judicial Administration*, (Washington, D.C., July 2001).

17.Department of State, *Patterns of Global Terrorism 2001* (Washington, D.C., May 2002), xvi.13

18.46 *International Encyclopedia of Terrorism*, 1997 ed., s.v. "The Academic View."

19.47 Ibid., s.v. "The Official View."

20.Karl von Clausewitz, *War, Politics and Power* (Chicago: Regnery Gateway, 1962), 83.

21.David E. Long, *The Anatomy of Terrorism* (New York: THE FREE PRESS, A Division of Macmillan, Inc., 1990), 4 and 5.

22. Ehud Sprinzak, "Rational Fanatics," *Foreign Policy,* no. 120 (September/October 2000): 66-73

23.Robert Baer .Η πτώση της CIA .Εκδόσεις Μέδουσα

24.Martha Crenshaw. *The Causes of Terrorism*. Comparative Politics, pp381-385. July 1981

25. Jerrold M. Post. *Terrorist Psycho-logic: Terrorist behavior as a product of psychological forces*. Origins of Terrorism, Walter Reich (Ed). Baltimore: John Hopkins University Press. 1998.

26.David J. Whittaker (Ed.) *The Terrorism Reader*. New York: Routledge 2001.

27. Coll, S and Glasser, S. (August 7 2005) 'Terrorists turn to the Web as base for operations, Washington Post Online. Available HTTP: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138_pf.html

28. Keith Lourdeau, FBI Deputy Assistant Director, testimony before the U.S. Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February 24, 2004.

29. According to FBI officials, Al Qaeda terrorist cells in Spain used stolen credit car d information to make numerous purchases. Also, the FBI has recorded more than 9.3 million Americans as victims of identity theft in the past 12 month period. Report by the Democratic Staff of the House Homeland Security Committee, *Identity Theft and Terrorism*, July 1, 2005, p.10.

30.Alan Sipress, *An Indonesian's Prison Memoir Takes Holy War Into Cyberspace*, Washington Post, December 14, 2004, A19.

31. Jonathan Curiel, *TERROR.COM: Iraq's tech-savvy insurgents are finding supporters and lurin g suicide-bomber recruits over the Internet*, San Francisco Chronicle, July 10, 2005,[http://www.sfgate.com/cgi- bin/article.cgi?f=/c/a/2005/07/10/CURIEL.TMP]. Page 23

32. Jonathan Curiel, *Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet*, San Francisco Chronicle, July 10, 2005, A.01.

33.Jack Kelley, "Terror Groups Hide Behind Web Encryption," *USA Today*, 5 February 2001; available from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm; Internet; accessed 6 April 2004.

34. Bartom Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washingtonpost.com,* 27 June 2002; available from http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26; Internet; accessed 12 April 2004.

35.Bob Sullivan reporting for MSNBC. *Is a Larger Net Attack on the way?*

October 2002 http://www.msnbc.com/news/827209.asp?cp1=1, accessed

October 2003.

36.Dan Verton, *Black Ice: The Invisible Threat of Cyberterrorism,* McGraw-Hill, 2003, p.87.

37.Anthony Davis, *The Afghan files: Al-Qaeda documents from Kabul*, Jane's Intelligence Review, February 1, 2002.

38.Joel Leyden. *Al-Qaeda : The 39 principles of Holy War*. Israel News Agency. 4 September 2003

39.Dorothy E. Denning. *Cyberterrorism.* Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, accessed July 2003.

40. Jovi Tanada Yam. *Bracing for cyberwar*. BusinessWorld Publishing Corporation. 4 October 2001.

41. CSIS Task Force Report. *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

42.Jon Tullett. *Crying Wolf on Cyberterrorism?* SC Infosec Opinionwire. February 2003 .

43. Timothy L. Thomas. *Al Qaeda and the Internet: The Danger of "Cyberplanning"*. Parameters. Spring 2003.

44.Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Press 1999.

45.Symantec Security Response Newsletter, Oct 2003.http://securityresponse.symantec.com, accessed November 2003.

46.CSIS Task Force Report. *Cybercrime… Cyberterrorism… Cyberwarfare… Averting an Electronic Waterloo*. Washington D.C.: Center for Strategic and International Studies, 1998.

47.Using these five basic steps, often supplemented with automated intrusion tools, attackers

have successfully taken over computer systems and remained undetected for long periods of time. Ed Skoudis, *Counter Hack*, (New Jersey: Prentice Hall, 2002).

48.These include Ed Skoudis, *Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses*, (New Jersey: Prentice Hall, 2002); Winn Schwartau, *Information Warfare Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, (Publishers Group West, 1996); and Jeff Crume, *Inside Internet Security: What Hackers Don't Want You To Kno*w, (Pearson Education Limited, 2000).

49.For more about Spyware, see Spywareinfo at [http://www.spywareinfo.com/].

50.Kevin Poulsen,"War Driving by the Bay," Securityfocus.com, April 12, 2001, [http://www.securityfocus.com/news/192].

51.Anne Saita, "Antiforensics: The Looming Arms Race,"*Information Security*, May 2003, vol. 6, no. 5, p.13.

52. Janet J. Prichard and Laurie E. MacDonald Bryant University, Smithfield, RI, USA prichard@bryant.edu lemac@bryant.edu

53.Schneier, B. (2000). Semantic network attacks. *Communications of the ACM, 43* (12), 168.

54. Trojan White Paper Aelphaeis Mangarae [Igniteds.NET] May 5th 2006

55.Jason Ma.´´NPS Touts Terminator As EW Tool ´´ Oct.2005

56.Brian Krebs Washingtonpost.com Aug.2007

57.Diane Frank Federal Computer Week Aug.25 2007 vol17.no 29

58.Webpage of phpBB, http:// www .php.com

59. Webpage of community portal MySpace http:// www .myspace.com

60.The Open Source Vulnerability Database http:// www .osvdb.com

61.Feds Warn Banks About Internet Attack CNN .com

62. **N.I.S.C.C.** (http://www.niscc.gov.uk)

63. Robert J. Cleary, "Creator of Melissa Computer Virus Pleads Guilty to State and Federal

Charges" 9 December 1999;; available from <http://www.usdoj.gov/criminal/cybercrime/ melissa.htm>; Internet; accessed 11 October 2004.

64. Christopher Miller, *GAO Reviewof Weapon Systems Software*, Mar. 3, 2003, Email communication, MillerC@gao.gov.

65.Code Breakers Magazine /Security &Anti-Security – Attack &Defense .Examining Viruses by Giovanni Tropeano

66.Virus Tutorial / by Giovanni Tropeano

67. **Standard P800-S860 Rev 3.0 Effective: September 15, 2006** Virus and Malicious Code Protection Page 6 of 7

68.HIDE'N SEEK REVISITED –FULL STEALTH IS` BACK Kimmo Kasslin ,Samuli Larvala and Antti Tikkanen, Helsinki,Finland

69. THE RUSSIAN UNDERSTANDING OF INFORMATION OPERATIONS AND INFORMATION WARFARE By Timothy L. Thomas

70.Pal'chun, B.P., and R.M. Yusupov, "Obespecheniye Bezopasnosti Komp'yuternoy infosfery" ("Providing Security in the Computer Infosphere"), *Vooruzheniye, Politika, Konversiya*, No. 3, 1993, p 23.

71. **Cyber Security Challenges: Designing Efficient Intrusion DetectionSystems and Antivirus Tools** Srinivas Mukkamala, Andrew Sung and Ajith Abraham*Department of Computer Science, New Mexico Tech, USA *School of Computer Science and Engineering, Chung-Ang University, Korea Email: ajith.abraham@ieee.org,

72. **Tracking and Tracing Cyber-Attacks:Technical Challenges and Global Policy Issues**

Howard F. Lipson, Ph.D. CERT® Coordination Center

73.Department of Justice.US Attorney Southern District of California .Press Release .*President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computers .San Diego 29Sept.2003.*

74.Andrew Quinn ´´ Teen Hackers Plead Guilty to Stunning Pentagon Attack ´´ Reuters , 2002 ,www.geocities .com

75. **CYBER WARFARE AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES** INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE

76.Robert Lemos ´´ What are the real risks of Cyberterrorism ´´26 August 2004// http://zdnet.com

77. USAWC STRATEGY RESEARCH PROJECT **ASYMMETRICAL THREATS AND HOMELAND SECURITY POLICY: IS AMERICA READY FOR AN ATTACK ON ITS TELECOMMUNICATIONS NETWORKS?** By Colonel Edric A. Kirkman United States Army

78. Report for Congress Received through the CRS Web Order Code RL31556 **Critical infrastructures:What Makes an Infrastructure Critical? Updated January 29, 2003**

John Moteff, Claudia Copeland, and John Fischer Resources, Science, and Industry Division

79. AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY Second World War Deception Lessons Learned for Today's Joint Planner **Donald J. Bacon** Major, USAF Air Command and Staff College Wright Flyer Paper No. 5

180. Dudley W. Clarke, "A" Force commander, *Operation Barclay* (Maxwell AFB, Ala.: AFHRA, USAF Collection, call no. MF25242, IRIS no. 02007569, 1943

81. MILITARY DECEPTION:HIDING THE REAL – SHOWING THE FAKE Major Mark Johnson, USMC Major Jessica Meyeraan, USAF Joint Forces Staff College Joint and Combined Warfighting School Class Number 03-1I7 March 2003 Lieutenant Colonel Kim Hawthorne, USAF

82. Whaley, B. "Toward a General Theory of Deception", *The Journal of Strategic Studies*, Frank Cass, London, 5(1):178-192, March 1982.

83. Information Operations and Terrorism Dorothy E. Denning August 18, 2005

184. Thomas A. Savoie, "Are We Deceiving Ourselves?" *Military Review,* March 1987, 38.

285.Scott Gerwehr and Glenn W.Russell . The Art of Darkness :Deception and Urban Operations .RAND 2000

86. Frederick B. Cohen, Dr. *A Note on the Role of Deception in Information Protection*, 1998 http://all.net/journal/deception/deception.html, accessed September 2003.

87. Charles A. Fowler & Robert F. Nesbit. *Tactical Deception in Air-Land Warfare*. Journal of Electronic Defense. June 1995.

88. Barton Whaley. *Toward a General Theory of Deception*. The Journal of Strategic Studies, Vol. 5, No. 1, pp 178-192. March 1982.

89. Abram N. Shulsky & Gary J. Schmitt. *Silent Warfare: Understanding the*

World of Intelligence. Washington D.C.: Brassey's Inc. Third Edition, 2002.

90. Bob Sullivan reporting for MSNBC. *Fake FBI site tries to lure victims*. Sep2003. www.msnbc.com/news/974015.asp?cp1=1, accessed October 2003.

91. Kevin D. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing 2002.

92. James F. Dunnigan & Albert A. Nofi. *Victory and Deceit: Dirty Tricks at War*.William Morrow and Co. 1995.

93. Dorothy E. Denning. *Information Warfare and Security*. New York: ACM Press 1999.

94. Emory A. Anderson III. *A Demonstration of the subversion threat: Facing a critical responsibility in the defense of cyberspace*. M.S. in Computer Science 2002, Naval Postgraduate School, Monterey CA.http://library.nps.navy.mil/uhtbin/hyperion-image/02Mar_AndersonE.pdf .

95. Symantec Security Response Newsletter, Oct 2003. http://securityresponse.symantec.com

96. Neil C. Rowe. *Counterplanning Deceptions to Foil Cyber-Attack Plans*.Proceedings of the 2003 IEEE Workshop in Information Assurance, West Point, New York, June 2003. http://www.cs.nps.navy.mil/people/faculty/rowe/iacounter.htm

97. Using Honeypots Prepared by:Amit D. Lakhani Guided by:Dr. Kenneth G. Paterson Information Security Group Royal Holloway, University of London UK This disseration is

submitted to Royal Holloway, University of London as partial fulfillment for the degree of MSc in Information Security

98. James B. Michael and Richard D. Riehle. *Intelligent Software Decoys*.Proceedings of the Monterey Workshop: Engineering Automation for Software Intensive System Integration, Monterey California. Pp 178-187. June 2001.

99. Neil C. Rowe & Hy Rothstein. *Deception for Defense of Information Systems:Analogies from Conventional Warfare*. Departments of Computer Science and Defense Analysis, U.S. Naval Postgraduate School http://www.cs.nps.navy.mil/people/faculty/rowe/mildec.htm,