ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΙΣ ΔΙΕΘΝΕΙΣ ΚΑΙ ΕΥΡΩΠΑΪΚΕΣ ΣΠΟΥΔΕΣ

Διπλωματική Εργασία

Οι Συγκρούσεις στον Κυβερνοχώρο: Ο Κυβερνοπόλεμος και η Αποτροπή

Χαϊδής Λεωνίδας (ΜΘ/09044)

Επιβλέπων Καθηγητής : κ. Πλατιάς Αθανάσιος

Πειραιάς, 2012

Αφιερώνεται στους γονείς μου

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω θερμά τον καθηγητή Αθανάσιο Πλατιά για την εμπιστοσύνη που έδειξε προς το πρόσωπο μου. Επίσης, θα ήθελα να ευχαριστώ θερμά τους καθηγητές Ιωάννη Κωνσταντόπουλο και Ανδρέα Λιαρόπουλο για την υποστήριξη τους καθόλη τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγικό Σημείωμα

Ο 1ος πόλεμος στον Περσικό Κόλπο (1990-1991) κατέδειξε με μεγάλη ευκρίνεια ότι η ενσωμάτωση της τεχνολογίας στο στρατιωτικό δόγμα, στις στρατιωτικές επιχειρήσεις και δομές, προσέφερε στις ΗΠΑ και στους συμμάχους της σημαντικό συγκριτικό πλεονέκτημα κατά την διάρκεια των ένοπλων συγκρούσεων. Στις εν λόγω συγκρούσεις έγινε εκτεταμένη χρήση του αεροπορικού όπλου, των συστημάτων Διοίκησης και Ελέγχου (C^2), των Η/Υ, αλλά και των έξυπνων βομβών. Κοινός παρανομαστής των παραπάνω στοιχείων ήταν ότι η εύρυθμη λειτουργία τους στηριζόταν στην σωστή λειτουργία του λογισμικού (software) που ήταν ενσωματωμένο στους Η/Υ. Επιπλέον, ο απαιτούμενος συντονισμός των στρατιωτικών επιχειρήσεων, ο οποίος ήταν ζωτικής σημασίας για την επιτυχή έκβαση του πολέμου για τους συμμάχους, ήταν εφικτός μέσω των δικτύων των Η/Υ. Η νικηφόρα έκβαση της σύγκρουσης κατέστησε λοιπόν εμφανές ότι, η εύρυθμη διαχείριση και μεταφορά των ψηφιακών δεδομένων και πληροφοριών μέσω των δικτύων Η/Υ προσέδιδε σημαντική ισχύ στον κάτοχο τους. Ως αποτέλεσμα, το μοντέλο εφαρμογής της τεχνολογίας Η/Υ και πληροφορικής (IT: Information Technology) στις ένοπλες δυνάμεις και στις επιχειρήσεις τους οδήγησε κατά την δεκαετία του 1990 στην διεθνώς γνωστή έννοια, Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA, Revolution in Military Affairs) και επιβεβαίωσε το γεγονός ότι η σχέση τεχνολογίας και πολέμου είναι άμεση[1].

Την ίδια εποχή το διαδίκτυο (Internet) άρχισε να παίρνει μεγάλες διαστάσεις και να γίνεται ιδιαίτερα προσιτό στο ευρύ κοινό. Προς την κατεύθυνση αυτή συνέβαλε η ανάπτυξη φιλικών προς τον άνθρωπο τεχνολογικών εφαρμογών για Η/Υ. Με τον τρόπο αυτό κάθε πολίτης μιας χώρας αποκτούσε πρόσβαση σε τεράστιες βάσεις δεδομένων, αλλά και μια άνευ προηγμένου δυνατότητα επικοινωνίας με χαμηλό κόστος. Ως αποτέλεσμα, το διαδίκτυο μετατράπηκε σε ένα καθημερινό εργαλείο το οποίο μπορούσαν να χρησιμοποιήσουν τόσο οι απλοί πολίτες, όσο και οι επιχειρήσεις και οι δημόσιοι ή ιδιωτικοί φορείς, προκειμένου να εκτελούν βασικές δραστηριότητες τους με χαμηλό κόστος. Παράλληλα, άρχισαν να εμφανίζονται σταδιακά στις επιχειρήσεις τα δίκτυα Η/Υ και τα ψηφιακά συστήματα ελέγχου, μέσω των οποίων επιτυγχάνονταν η αυτοματοποίηση πολλών λειτουργικών διαδικασιών.

Με τον τρόπο αυτό, η ανθρώπινη δραστηριότητα άρχισε στις αρχές της δεκαετίας του 1990 να εκφράζεται μέσα από την διασύνδεση και την αλληλεξάρτηση των δικτύων Η/Υ και του Internet. Η τάση αυτή έφερε στην επιφάνεια την έννοια του κυβερνοχώρου, του εικονικού δηλαδή χώρου μέσω του οποίου πραγματοποιούνταν σε

[1] Κωνσταντόπουλος, Ιωάννης, *Οικονομία και Κατασκοπεία: Θεωρία και Πράξη* (Εκδόσεις Ποιότητα, Βάρη Αττικής, 2010), σελ. 137-138, 141-144

καθημερινή βάση εκατομμύρια λειτουργίες και δραστηριότητες. Σε αυτήν την περιοχή λάμβαναν καθημερινά αναρίθμητες ανταλλαγές και μεταφορές ψηφιακών δεδομένων και πληροφοριών, οι οποίες μεταφράζονταν σε κέρδος και ασφάλεια. Όπως όμως προαναφέρθηκε, στον κυβερνοχώρο είχαν πλέον σχεδόν όλοι πρόσβαση, με αποτέλεσμα, η εικονική αυτή περιοχή να μετατραπεί σταδιακά σε ένα πεδίο αντιπαράθεσης και σύγκρουσης, καθώς οι άμεσα και έμμεσα ενδιαφερόμενοι σε αυτόν επιζητούσαν ολοένα και μεγαλύτερο μερίδιο κέρδους αλλά και ασφάλειας.

Παράλληλα, λίγο πριν τα μέσα της δεκαετίας του '90 έκαναν την εμφάνιση τους οι hackers και οι διάφορες μορφές κακόβουλου λογισμικού (malware)[2], μέσω των οποίων πραγματοποιούνταν παράνομες δραστηριότητες, όπως η υπεξαίρεση διαβαθμισμένων ή μη δεδομένων από Η/Υ, η αλλοίωση ψηφιακών δεδομένων, η πρόκληση δυσλειτουργιών σε Η/Υ και δίκτυα Η/Υ, η πρόκληση τρόμου κα. Οι παράνομες αυτές δραστηριότητες αφορούσαν τόσο σε απλούς χρήστες των Η/Υ όσο και σε επιχειρήσεις και οργανισμούς που διέθεταν δίκτυα Η/Υ. Χαρακτηρίστηκαν ως συγκρούσεις στον κυβερνοχώρο και με το πέρασμα των χρόνων στιγματίστηκαν από την ολοένα και μεγαλύτερη συχνότητα τους, αλλά και από την εξειδίκευση στην τεχνολογία της πληροφορικής που έφεραν. Με δεδομένο ότι, μετά τον 1^{ο} Πόλεμο στον Περσικό Κόλπο οι Η/Υ και τα δίκτυα Η/Υ βρήκαν ευρεία εφαρμογή στις ένοπλες δυνάμεις (ΕΔ) των κρατών, ήταν φυσικό οι συγκρούσεις αυτές να επεκταθούν και στο στρατιωτικό επίπεδο. Ως αποτέλεσμα, ένα μεγάλο μέρος της ακαδημαϊκής και αμυντικής κοινότητας, άρχισε να ασχολείται ιδιαίτερα με αυτήν την νέα μορφή συγκρούσεων, η οποία έκανε καθημερινά αισθητή την παρουσία της.

Αντικειμενικός σκοπός αυτής της εργασίας είναι να παρουσιάσει τις μορφές των συγκρούσεων που λαμβάνουν χώρα στον κυβερνοχώρο, δίνοντας μεγαλύτερη έμφαση στην υψηλότερη μορφή κυβερνοσύγκρουσης, τον κυβερνοπόλεμο. Οι συγκρούσεις στον κυβερνοχώρο λαμβάνουν χώρα σε καθημερινή βάση, χωρίς να γίνονται πάντοτε αντιληπτές από το ευρύ κοινό, ενώ η βασική τους ιδιαιτερότητα είναι ότι, σε αυτές μπορεί να διαδραματίσει σημαντικό ρόλο ακόμα και ένας απλός πολίτης. Αν και μέχρι σήμερα ο αντίκτυπος τους είναι κυρίως οικονομικός ή/και ψυχολογικός, η συνεχής τεχνολογική εξειδίκευση που εμφανίζουν, προοικονομεί την δυνατότητα πρόκλησης ανθρώπινων απωλειών στο μέλλον.

Ο κυβερνοπόλεμος αποτελεί συστατικό στοιχείο του πληροφοριακού πολέμου, τον οποίο εφαρμόζουν κατά κόρον τα σύγχρονα κράτη. Από τα διάφορα παραδείγματα εφαρμογής του διαφαίνεται ότι αποτελεί συνειδητή και με ολοένα μεγαλύτερη

[2] Το κακόβουλο λογισμικό διεισδύει σε έναν Η/Υ χωρίς την έγκριση του χρήστη του. Αποστέλλεται από έναν hacker - ο ειδικός των Η/Υ που επεμβαίνει στο λογισμικό (software) χωρίς κατάλληλη εξουσιοδότηση - προκειμένου να τεθεί ο Η/Υ – αποδέκτης υπό την ομηρία του και να εκτελεί λειτουργίες, που δεν συμβαδίζουν με την θέληση του χρήστη του Η/Υ.

συχνότητα επιλογή των κρατών, προκειμένου αυτά να διασφαλίσουν τα συμφέροντα τους στο διεθνές σύστημα. Θεωρείται από τα κράτη ως μια πιο ήπια μορφή πολεμικής σύγκρουσης, καθώς δεν οδηγεί – προς το παρόν - σε ανθρώπινες απώλειες και συνεπώς είναι περισσότερο «νομιμοποιημένη» και αποδεκτή από το ευρύ κοινό. Δύναται να διεξαχθεί μεταξύ δυο ή περισσοτέρων κρατών αλλά και μεταξύ τουλάχιστον ενός κράτους και ενός Μη Κρατικού Δρώντα, που ενεργεί υπό τον έλεγχο ή υπό την εποπτεία ενός άλλου κράτους ή κρατών. Το γεγονός αυτό συνιστά μια σημαντική διαφορά σε σχέση με τις συγκρούσεις σε συμβατικό ή/και πυρηνικό επίπεδο.

Στο 1^{ο} κεφάλαιο της διπλωματικής εργασίας γίνεται προσπάθεια να προσδιοριστεί σφαιρικά η έννοια του κυβερνοχώρου, που αποτελεί την εικονική περιοχή όπου λαμβάνουν χώρα οι κυβερνοσυγκρούσεις. Πέραν τους ορισμού της έννοιας του «κυβερνοχώρου», καταδεικνύονται τα επίπεδα λειτουργίας του, τα χαρακτηριστικά του αλλά και οι δομικές αδυναμίες ή αλλιώς τα σημεία τρωτότητας του. Παράλληλα, γίνεται αναφορά στους κινδύνους που προκύπτουν από τις προαναφερόμενες αδυναμίες αλλά και τους φορείς εκμετάλλευσης αυτών των αδυναμιών.

Στο 2^{ο} κεφάλαιο δίδονται οι ορισμοί των επιθέσεων στον κυβερνοχώρο (κυβερνοεπιθέσεων) και των κυβερνοσυγκρούσεων. Γίνεται αναφορά στο «νομικό καθεστώς» των κυβερνοεπιθέσεων, αλλά και στον τρόπο με τον οποίο τα κράτη προσπαθούν να «μεταφράσουν» τον αντίκτυπο τους. Παράλληλα, δίδονται οι ορισμοί των διακριτών μορφών των κυβερνοσυγκρούσεων (Βανδαλισμός στον Κυβερνοχώρο, Κυβερνοκατασκοπεία, Κυβερνοέγκλημα, Κυβερνοτρομοκρατία, Κυβερνοπόλεμος), ενώ για την καλύτερη κατανόηση τους παρατίθενται συνοπτική περιγραφή καταγεγραμμένων κυβερνοσυγκρούσεων. Ιδιαίτερη μνεία γίνεται για τον Κυβερνοπόλεμο, ο οποίος δύναται να λάβει 2 μορφές – στρατηγικός ή επιχειρησιακός – ενώ αναλύονται τα κίνητρα για την διεξαγωγή του και τα σημεία στόχευσης του.

Όπως προαναφέρθηκε, ο κυβερνοπόλεμος δύναται να διεξαχθεί μεταξύ δυο ή περισσοτέρων κρατών αλλά και μεταξύ τουλάχιστον ενός κράτους και ενός Μη Κρατικού Δρώντα, ο οποίος ενεργεί υπό τον έλεγχο ενός άλλου κράτους ή κρατών. Για το λόγο αυτό, στο 3^{ο} Κεφάλαιο γίνεται αναφορά στην συμβολή του μη κρατικού δρώντα σε αυτήν την μορφή κυβερνοσύγκρουσης, αλλά και στις συνήθεις μορφές οργάνωσης των μη κρατικών δρώντων προκειμένου να συμμετάσχουν σε κυβερνοπόλεμο. Παράλληλα, γίνεται αναφορά στην «θετική» στάση των σύγχρονων κρατών απέναντι στον κυβερνοπόλεμο, ενώ επιλέγονται προς ανάλυση 6 κράτη (ΗΠΑ, Ρωσία, Κίνα, Ιράν, Ισραήλ και Β. Κορέα). Τα κράτη αυτά, που είτε διαθέτουν πυρηνικά όπλα είτε

προσπαθούν να αποκτήσουν[3], έχουν συνειδητά εστιάσει την προσοχή τους στην ανάπτυξη σημαντικών δυνατοτήτων κυβερνοπολέμου. Η αναφορά στα κράτη ολοκληρώνεται με την συνοπτική παράθεση των γεγονότων σε 3 γνωστές από τα ΜΜΕ κυβερνοσυγκρούσεις, οι οποίες έλαβαν χώρα στην Εσθονία το 2007, στην Γεωργία το 2008 και στο Ιράν το 2009 - 2010. Οι συγκεκριμένες περιπτώσεις εκλαμβάνονται από την πληθώρα των μελετητών των κυβερνοσυγκρούσεων ως μορφές κυβερνοπολέμου, κάθε μια από τις οποίες εισήγαγε ένα νέο στοιχείο στις συγκρούσεις στον κυβερνοχώρο.

Με δεδομένο τον ολοένα αυξανόμενο ρυθμό εκδήλωσης κυβερνοεπιθέσεων, εξετάζεται στο κεφάλαιο 4 η λειτουργία της Αποτροπής στον κυβερνοχώρο. Πέραν της παράθεσης ορισμού για την ανωτέρω στρατηγική, γίνεται μια σύντομη ιστορική αναδρομή για την εξέλιξη της στο συμβατικό και πυρηνικό επίπεδο, καθώς και μια αναφορά στις προϋποθέσεις εφαρμογή της. Παράλληλα, αναφέρονται οι βασικές μορφές της (Αποτροπή μέσω Αντιποίνων, Αποτροπή μέσω Άρνησης, κτλ), ενώ εξετάζεται αν το μοντέλο της Αποτροπής, που είναι γνωστό από το συμβατικό και το πυρηνικό επίπεδο, μπορεί να εφαρμοστεί στον κυβερνοχώρο. Στο τέλος του υπόψη κεφαλαίου παρουσιάζονται σε συντομία οι σύγχρονες τάσεις που υπάρχουν αναφορικά με την μορφή που θα πρέπει να έχει η κυβερνοαποτροπή για να είναι αποτελεσματική.

Η εργασία αυτή καταλήγει με τα συμπεράσματα που προκύπτουν από την ανάλυση των στοιχείων που περιέχονται στα προηγούμενα κεφάλαια.

[3] Οι ΗΠΑ, η Ρωσία και η Κίνα κατέχουν επισήμως πυρηνικά όπλα. Το Ισραήλ και η Βόρεια Κορέα ανεπισήμως φέρονται να κατέχουν πυρηνικά όπλα. Το Ιράν προσπαθεί να αναπτύξει το πυρηνικό του πρόγραμμα υποστηρίζοντας πως είναι για ειρηνικούς σκοπούς. Ωστόσο, η διεθνής κοινότητα θεωρεί πως το Ιράν προσπαθεί να κατασκευάσει πυρηνικά όπλα.

1. Ο Κυβερνοχώρος

1.1 Ορισμός

Μέχρι σήμερα δεν υπάρχει ένας κοινά αποδεκτός ορισμός για τον κυβερνοχώρο σε παγκόσμιο επίπεδο, αλλά ούτε και συναίνεση για το ποιες είναι οι επιπτώσεις των συγκρούσεων σε αυτόν το χώρο[4]. Μια πρώτη προσέγγιση στο ζήτημα του ορισμού θα μπορούσε να είναι η παρακάτω : «Ο κυβερνοχώρος είναι η ευρύτερη δυνατή ψηφιακή περιοχή, το ηλεκτρονικό σύμπαν που περιλαμβάνει όχι μόνο το Internet, αλλά ακόμα και όλους τους Η/Υ που δεν είναι συνδεδεμένοι σε αυτό. Στην τελευταία κατηγορία συμπεριλαμβάνονται τα διαβαθμισμένα στρατιωτικά συστήματα Η/Υ, καθώς και τα αντίστοιχα ιδιωτικά συστήματα των επιχειρήσεων και των βιομηχανιών»[5]. Ο R. Clarke[6] στο βιβλίο του "*Cyber War: The Next Threat to National Security and What to Do About it*" δίνει έναν ακόμα περιγραφικό ορισμό: «Ο Κυβερνοχώρος είναι όλα τα δίκτυα των Η/Υ σε παγκόσμιο επίπεδο, καθώς και οτιδήποτε συνδέεται και ελέγχεται από αυτά. Δεν είναι απλώς το Internet….Ο κυβερνοχώρος περιλαμβάνει το Internet αλλά και τα δίκτυα των Η/Υ που δεν έχουν πρόσβαση σε αυτό»[7]. Επιπρόσθετα σε μια διακλαδική έκδοση του αμερικανικού Υπουργείου Άμυνας (JP 1-02) αναφέρεται ο εξής ορισμός για τον κυβερνοχώρο: «Είναι μια παγκόσμια περιοχή εντός του πληροφοριακού περιβάλλοντος που αποτελείται από διασυνδεδεμένα δίκτυα υποδομών ΙΤ τεχνολογίας, συμπεριλαμβανομένων του Internet, των τηλεπικοινωνιακών δικτύων, των συστημάτων Η/Υ και των ενσωματωμένων επεξεργαστών και συσκευών ελέγχου»[8].

Από τους παραπάνω ορισμούς γίνεται κατανοητό ότι ο κυβερνοχώρος αποτελεί ένα εικονικό χώρο, ο οποίος κατασκευάστηκε από τον άνθρωπο[9]. Αφορά στο Internet αλλά και στην πληθώρα των δικτύων Η/Υ (ιδιωτικά, δημόσια, κρατικά, στρατιωτικά, ενσύρματα, ασύρματα δίκτυα Η/Υ) που είτε είναι συνδεδεμένα στο Internet είτε όχι. Σχετίζεται με την διακίνηση ψηφιοποιημένων δεδομένων και πληροφοριών μέσα από τα δίκτυα των Η/Υ, τα οποία στην σημερινή εποχή βρίσκουν εφαρμογή στις

---

[4] Ottis, R. & Lorents, P. (2010) "*Cyberspace: Definition and Implications",* In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. *Reading: Academic Publishing Limited, pp. 267-270*

[5] Ο ορισμός προέρχεται από την ηλεκτρονική έκδοση του CSMonitor, http://www.csmonitor.com/USA/Military/2011/0307/Cyberwar-glossary, accessed on 5-11-2011

[6] Ο R. Clarke διετέλεσε σύμβουλος, επί σειρά ετών, σε διάφορους Πρόεδρους των ΗΠΑ (1973-2003), γύρω από θέματα ασφάλειας, αντιτρομοκρατίας και προστασίας υποδομών. Λίγο πριν εγκαταλείψει την ενεργό δράση διετέλεσε σύμβουλος του Προέδρου Μπους σε θέματα κυβερνοασφάλειας

[7] Clarke, Richard & Knake, Robert K., *Cyber War : The Next Threat To National Security And What To Do About It* (1st Edition, HarperCollins Publishers, New York, 2010), p. 70

[8] Joint Publication 1-02 (JP 1-02) : *DoD Dictionary of Military and Associated Terms*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, p.83, accessed on May 2011

[9] Air Force Doctrine Document 3-12 (AFDD 3-12): *Cyberspace Operations,* http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf, p. 2, accessed on May 2011

βιομηχανίες, τις επιχειρήσεις, τις ένοπλες δυνάμεις, τις τράπεζες, τα χρηματιστήρια, τις τηλεπικοινωνίες κτλ. Τόσο στις ανεπτυγμένες όσο και στις αναπτυσσόμενες χώρες - σε διαφορετικό βαθμό σε κάθε μια από αυτές - τα δίκτυα Η/Υ ελέγχουν τις τραπεζικές συναλλαγές, την ροή του πετρελαίου και του φυσικού αερίου μέσα από τους κατάλληλους αγωγούς, την παροχή ηλεκτρικής ενέργειας, την υδροδότηση, την δημόσια υγεία, την εναέρια κυκλοφορία, τις τηλεφωνικές επικοινωνίες, τις μεταφορές, ενώ αποτελούν περιοχές συγκέντρωσης διαβαθμισμένων ή μη πληροφοριών. Χαρακτηριστική είναι η παραδοχή του πρώην Προέδρου των ΗΠΑ, George W. Bush το 2003 ότι, ο κυβερνοχώρος είναι το νευρικό σύστημα των αμερικανικών κρίσιμων υποδομών και το σύστημα ελέγχου της χώρας[10]. Σύμφωνα μάλιστα με επίσημη ανακοίνωση του Department of Homeland Security (DHS)[11], οι τομείς των κρίσιμων υποδομών των ΗΠΑ είναι 18 και αφορούν στα παρακάτω :

(i) Γεωργία και Τροφή *(Agriculture and Food)*

(ii) Τραπεζικές συναλλαγές και Οικονομία *(Banking and Finance)*

(iii) Χημικά *(Chemicals)*

(iv) Εμπορικές εγκαταστάσεις *(Commercial Facilities)*

(v) Επικοινωνίες *(Communications)*

(vi) Κρίσιμες Κατασκευές *(Critical Manufacturing)*

(vii) Φράγματα *(Dams)*

(viii) Αμυντική βιομηχανία *(Defense Industrial Base)*

(ix) Κυβερνητικές εγκαταστάσεις *(Government Facilities)*

(x) Υπηρεσίες Έκτακτης Ανάγκης *(Emergency Services)*

(xi) Ενέργεια *(Energy)*

(xii) Υγειονομικής Περίθαλψης και Δημόσιας Υγείας *(Healthcare and Public Health)*

(xiii) Τεχνολογία Η/Υ (IT) *(Information Technology)*

(xiv) Εθνικά Μνημεία & Εικόνες *(National Monuments and Icons)*

(xv) Πυρηνικοί Αντιδραστήρες, Πυρηνικά Υλικά και Απόβλητα *(Nuclear Reactors, Materials & Waste)*

(xvi) Συστήματα Μεταφορών *(Transportation Systems)*

(xvii) Ύδρευση *(Water)*

(xviii) Υπηρεσίες Ταχυδρομείου και Ναυτιλία *(Postal and Shipping)*

[10] Ο Αμερικανός Πρόεδρος αναφερόταν στους δημόσιους και ιδιωτικούς οργανισμούς που ασχολούνται με την γεωργία, την δημόσια υγεία, την ύδρευση, την διατροφή, τις υπηρεσίες εκτάκτου ανάγκης, την αμυντική βιομηχανία, τις μεταφορές, τις τηλεπικοινωνίες κα. Για περισσότερα βλ. Bush, George W., *National Strategy to Secure Cyberspace*, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, p. 1, accessed on May 2011

[11] Οι τομείς αυτοί θεωρούνται ουσιώδεις για την εθνική ασφάλεια, την δημόσια υγεία, την οικονομική ευρωστία των ΗΠΑ. Βλέπε ιστοσελίδα του αμερικανικού DHS, Critical Infrastructure. Available at: http://www.dhs.gov/files/programs/gc_1189168948944.shtm, accessed on April 2011

Γίνεται λοιπόν κατανοητό πως, η εύρυθμη λειτουργία πολλών πτυχών της σύγχρονης ανθρώπινης δραστηριότητας εξαρτάται από την δυνατότητα διασφάλισης της ακεραιότητας και της απρόσκοπτης ροής των ψηφιακών δεδομένων και πληροφοριών μέσα από τα υπάρχοντα δίκτυα Η/Υ.

1.2 Επίπεδα Λειτουργίας του Κυβερνοχώρου

Σύμφωνα με τον καθηγητή - ειδικό σε θέματα κυβερνοπολέμου - Martin Libicki, προκειμένου να γίνει καλύτερα κατανοητός ο κυβερνοχώρος και η λειτουργία του θα πρέπει να διακρίνουμε 3 επίπεδα λειτουργίας στα συστήματα πληροφορικής (IT systems): το φυσικό (physical layer), το συντακτικό (syntactic layer) και το σημασιολογικό (semantic layer)[12]. Το φυσικό επίπεδο αναφέρεται στο υλικό[13], δηλαδή τα μηχανικά (π.χ «κουτιά» Η/Υ, εκτυπωτές, scanners), ηλεκτρικά (π.χ καλώδια) και ηλεκτρονικά (π.χ chips, ολοκληρωμένα κυκλώματα) μέρη των δικτύων των Η/Υ. Σε περίπτωση απουσίας του φυσικού επιπέδου, δεν μπορεί να υφίσταται ένα σύστημα πληροφορικής.

Το συντακτικό επίπεδο περιλαμβάνει τις οδηγίες του κατασκευαστή και του χρήστη που δίνονται στις πληροφοριακές συσκευές (Η/Υ), αλλά και τα πρωτόκολλα μέσω των οποίων αλληλεπιδρούν οι υπόψη συσκευές. Θα πρέπει να σημειωθεί ότι οι Hackers, δηλαδή οι ειδικοί των Η/Υ οι οποίοι επεμβαίνουν στο λογισμικό (software) χωρίς κατάλληλη εξουσιοδότηση[14], δραστηριοποιούνται σε αυτό το επίπεδο.

Το σημασιολογικό επίπεδο περιλαμβάνει όλες εκείνες τις πληροφορίες που περιέχει ο Η/Υ. Σε αυτό το επίπεδο εξετάζεται η σημασιολογική ορθότητα μιας οδηγίας, η οποία μπορεί συντακτικά να είναι ορθή, ωστόσο σημασιολογικά μπορεί να είναι λάθος[15]. Π.χ η έκφραση «Η γάτα γαυγίζει» είναι συντακτικά ορθή, αλλά σημασιολογικά λανθασμένη, καθώς μια γάτα δεν μπορεί να γαυγίζει. Σε περίπτωση που κάποιος καταφέρει μια μετατροπή στην σημασιολογική ερμηνεία ενός συστήματος πληροφορικής, τότε το τελευταίο δύναται να χειραγωγηθεί. Ουσιαστικά όμως, για να επιτευχθεί κάτι τέτοιο θα πρέπει να έχει προηγηθεί παρέμβαση στο συντακτικό επίπεδο του συστήματος πληροφορικής.

[12] Libicki, Martin C., *Cyberdeterrence and Cyberwar* (RAND Corporation, Santa Monica, CA, 2009), p. 12
[13] Γαρίδης, Παναγιώτης & Δεληγιαννάκης Μανώλης, Σύγχρονο Λεξικό Πληροφορικής (Εκδόσεις Φλώρος, Αθήνα, 1993), σελ. 254
[14] Ibid, p. 251
[15] Ibid, p. 514

1.3 Χαρακτηριστικά του Κυβερνοχώρου

1.3.1 Γενικά

Όπως προαναφέρθηκε, ο κυβερνοχώρος βρίσκεται σήμερα πίσω από κάθε έκφανση της ανθρώπινης δραστηριότητας. Είναι πλήρως εξαρτημένος από την τεχνολογική ανάπτυξη, ιδιαίτερα από τις μεταβολές που συνίστανται στην τεχνολογία των Η/Υ (Information Technology: IT). Οπουδήποτε υπάρχει τέτοιου είδους τεχνολογία, δίκτυα Η/Υ, διαδίκτυο, υπάρχει και κυβερνοχώρος. Σύμφωνα με τον Clarke, ο κυβερνοχώρος βρίσκεται οπουδήποτε υπάρχει ένας Η/Υ ή ένας επεξεργαστής ή ακόμα ένα καλώδιο που συνδέεται με ένα Η/Υ[16]. Είναι με άλλα λόγια πανταχού παρών[17]. Επίσης, θα πρέπει να σημειωθεί ότι δεν υπάρχουν σαφή όρια που να περικλείουν την έννοια του κυβερνοχώρου, ενώ ως πεδίο δραστηριότητας είναι προσβάσιμος με χαμηλό κόστος (Low Cost Entry) σε οποιονδήποτε διαθέτει την απαραίτητη τεχνολογία και υποδομή[18] (πχ ένα φορητό Η/Υ και μια σύνδεση στο Internet ή έναν Η/Υ διασυνδεδεμένο στο δίκτυο Η/Υ μιας εταιρείας).

1.3.2 Το μέγεθος του Κυβερνοχώρου

Δεν θα ήταν δόκιμο να γίνει προσπάθεια υπολογισμού των διαστάσεων του κυβερνοχώρου, καθώς αποτελεί έναν ευμετάβλητο[19] εικονικό χώρο, μέσα στον οποίο διακινείται η ψηφιακή πληροφορία. Σε έκθεση της, η ITU (International Telecommunication Union) δίνει τα παρακάτω στοιχεία[20] : Ο αριθμός των χρηστών κινητής τηλεφωνίας 3ης γενιάς (3G) – δηλ. με πρόσβαση στο Internet - έχει αυξηθεί σημαντικά την τελευταία πενταετία, ενώ το 2010, ο αριθμός αυτός έφθανε τους 940 εκατομμύρια χρήστες. Επίσης, οι υπηρεσίες 3G ήταν διαθέσιμες σε 143 χώρες (2010) σε σχέση με τις 95 χώρες το 2007. Παράλληλα, ο αριθμός των χρηστών του Internet διπλασιάστηκε κατά την πενταετία 2005 – 2010, ξεπερνώντας τους 2 δις χρήστες.

Παράλληλα, είναι κοινά αποδεκτό ότι για καθαρά λόγους κερδοφορίας πολλές επιχειρήσεις κατά την διάρκεια της δεκαετίας του 1990 ενσωμάτωσαν

---

[16] Clarke & Knake, 2010: 69

[17] Borchert, Heiko & Juhl, Felix, "*Exploiting the Potential of Cyber Operations*", Jane's Defense Weekly, Vol. 48, Issue 26, 29 June 2011, p. 22

[18] Ibid

[19] Αρκεί κάποιος να αναλογιστεί τον αριθμό των ιστοσελίδων που δημιουργούνται ή παύουν να λειτουργούν καθημερινά. Αυτό αφορά κυρίως στο Internet που είναι ένα τμήμα του Κυβερνοχώρου. Αν σκεφτούμε τους ρυθμούς δικτύωσης με Η/Υ των εταιρειών και των βιομηχανιών σε καθημερινή βάση, τότε καλύπτουμε ένα ακόμα μέρος του κυβερνοχώρου.

[20] International Telecommunications Union (ITU) Facts and Figures, available at: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2010.pdf, accessed on Dec 2010

αυτοματοποιημένα συστήματα ελέγχου και απόκτησης δεδομένων (SCADA[21] systems) και δίκτυα Η/Υ στο δυναμικό τους[22], τα οποία διασυνδέονται με το Internet[23]. Πολλοί χειροκίνητοι ελεγκτικοί μηχανισμοί στην παραγωγή αντικαταστάθηκαν από ψηφιακούς επεξεργαστές. Ψηφιακά συστήματα ελέγχου ανέλαβαν την επιτήρηση της δραστηριότητας και την παραγωγική ροή. Επιπρόσθετα, για τον ίδιο λόγο, οι κυβερνήσεις των κρατών προέβησαν σε παρόμοιες κινήσεις προκειμένου να ενισχύσουν την αποτελεσματικότητα των κρατικών υποδομών, να εντείνουν τις δυνατότητες ελέγχου και επιβολής του νόμου, αλλά και για να ενισχύσουν την άμυνα τους.

Η ενσωμάτωση των δικτύων Η/Υ και της ΙΤ τεχνολογίας στον τομέα της άμυνας ξεκίνησε με έντονους ρυθμούς μετά το τέλος του ψυχρού πολέμου και συνεχίζεται μέχρι και σήμερα. Η αποκαλούμενη Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA : Revolution In Military Affairs) προέκυψε μέσα από την ενσωμάτωση νέων ψηφιακών τεχνολογικών εφαρμογών στις πλατφόρμες οπλικών συστημάτων, οι οποίες πέραν από την ενίσχυση της ακρίβειας τους, μπορούσαν να μεταφέρουν σε πραγματικό χρόνο στους λήπτες των αποφάσεων μια πλήρη εικόνα του πεδίου της μάχης. Συνέβαλλαν στην καλύτερη διοίκηση και έλεγχο των επιχειρήσεων, ενώ διευκόλυναν τις επικοινωνίες και την επιτήρηση (C^4ISR). Στόχος ήταν και εξακολουθεί να είναι η επίτευξη της πληροφοριακής υπεροχής, δηλ. της δυνατότητας συλλογής, επεξεργασίας και διανομής της πληροφορίας με απρόσκοπτο τρόπο, για τις φίλιες δυνάμεις, παρεμποδίζοντας ταυτόχρονα αυτή τη δυνατότητα στον αντίπαλο[24]. Υπό το πλαίσιο αυτό, η προαναφερόμενη δυνατότητα αναμένεται να ενισχυθεί μέσα από την λειτουργία ενός πολύπλοκου και πολυεπίπεδου «Συστήματος των Συστημάτων», το οποίο κάνοντας χρήση διαφόρων πληροφοριακών πλατφόρμων (δορυφόροι, UAVs, Α/Φ, Ε/Π, αισθητήρες, πομποί, επεξεργαστές, συσκευές επικοινωνίας) - που επεξεργάζονται ψηφιακά δεδομένα - θα μπορεί να μεταφέρει την πληροφόρηση οπουδήποτε αυτό απαιτείται[25].

Γίνεται λοιπόν σαφές ότι, οι διαστάσεις του κυβερνοχώρου - ως χώρου διακίνησης ψηφιακών δεδομένων και πληροφορίας - διαρκώς αυξάνονται, λόγω της χρήσης ολοένα και περισσότερο της ψηφιακής τεχνολογίας και των δικτύων Η/Υ σε κάθε έκφανση της ανθρώπινης δραστηριότητας.

---

[21] SCADA : Supervisory Control and Data Acquisition
[22] Clarke & Knake, 2010: 96
[23] Hunker, Jeffrey, "*Cyberwar and Cyber Power. Issues for NATO doctrine*", Research Division, NATO Defense College, Rome, Research Paper No 62, November 2010, p. 2. Available at : http://www.ndc.nato.int/research/series.php?icode=1, accessed on April 2011
[24] Dunn, Myriam, *Information Age Conflicts : A Study of the Information Revolution and a changing Operating Environment* (CSS, Zurich,2002), p. 91
[25] Libicki, Martin C., "*The Emerging Primacy of Information: A Debate on Geopolitics*", Orbis, Spring 1996, Vol. 40, No 2, p. 262

1.3.3 Η Ασυμμετρία

Στον κυβερνοχώρο διαπιστώνεται έντονα η ύπαρξη της ασυμμετρίας αναφορικά με το «ειδικό βάρος» των οντοτήτων που μπορούν να δραστηριοποιούνται σε αυτόν. Έθνη - Κράτη, οργανισμοί, επιχειρήσεις, ιδιώτες, hackers μπορούν να δραστηριοποιηθούν στον ψηφιακό χώρο ως σχετικά «ισοδύναμες» οντότητες, παρά την δυσαναλογία που μπορούν να εμφανίζουν στον φυσικό χώρο. Αυτό βέβαια εξαρτάται και από τις δυνατότητες που διαθέτει η κάθε προαναφερόμενη κατηγορία στον κυβερνοχώρο[26].

Επίσης, θα πρέπει να σημειωθεί ότι η ασυμμετρία εμφανίζεται έντονα αναφορικά με το κόστος και το ρίσκο μιας ενέργειας από μια οντότητα στον κυβερνοχώρο, σε σχέση με το κέρδος από αυτήν την ενέργεια[27]. Π.χ κάποιος θα μπορούσε να υποκλέψει με κατάλληλη τεχνική, μέσα από τον κυβερνοχώρο, δεδομένα τεράστιας χρηματικής αξίας με κόστος και ρίσκο μικρότερο σε σχέση με μια προσπάθεια υποκλοπής των ίδιων δεδομένων με φυσικό τρόπο.

Ένα ακόμα σημείο που θα πρέπει να επισημανθεί είναι ότι κάθε οντότητα που δραστηριοποιείται στον κυβερνοχώρο δεν είναι το ίδιο εξαρτημένη από αυτόν. Για παράδειγμα η εξάρτηση ενός Χ κράτους από τα συστήματα Η/Υ και το internet δεν είναι σε καμία περίπτωση ισομεγέθης με την εξάρτηση ενός Υ κράτους[28]. Χαρακτηριστικό παράδειγμα αποτελούν οι ΗΠΑ και το Αφγανιστάν. Ωστόσο, όπως επισημαίνει ο καθηγητής Joseph S. Nye, Jr , ο κυβερνοχώρος ευνοεί τους «μικρούς» αλλά δεν διαγράφει τα πλεονεκτήματα των «μεγάλων»[29].

1.3.4 Η Ανωνυμία

Ένα ακόμα χαρακτηριστικό του κυβερνοχώρου είναι η ανωνυμία που μπορεί να έχει ένας δρών μέσα σε αυτήν την περιοχή. Η ανωνυμία οφείλεται πολλές φορές στην δαιδαλώδη αρχιτεκτονική του Internet[30], αλλά και στις ικανότητες ενός χρήστη (του κυβερνοχώρου) να καλύψει τα ίχνη του χρησιμοποιώντας ορισμένες τεχνικές[31]. Επιπλέον, σήμερα η πρόσβαση στον κυβερνοχώρο είναι ιδιαίτερα εύκολη, ενώ τα σημεία πρόσβασης δεν ταυτίζονται με συγκεκριμένο χρήστη. Π.χ πολλοί διαφορετικοί

---

[26] Borchert, Heiko & Juhl, Felix, "*Exploiting the Potential of Cyber Operations"*, Jane's Defense Weekly, Vol. 48, Issue 26, 29 June 2011, p. 22
[27] Geers, Kenneth, *Strategic Cyber Security* (CCD COE Publication, Tallinn, Estonia, 2011), p.136
[28] Lewis, James A., *The Fog of Cyberwar*, ISN ETH website : http://www.isn.ethz.ch, accessed on April 2011
[29] Nye, Joseph S. Jr., "*Cyberspace diffuses, but doesn't erase state power"*, Fierce Homeland Security website : http://www.fiercehomelandsecurity.com, accessed on 26-10-11
[30] Ibid, p.136
[31] Clarke & Knake, 2010: 92

χρήστες του Internet μπορούν να χρησιμοποιήσουν τον ίδιο Η/Υ σε ένα internet Cafe μέσα σε ένα μικρό χρονικό διάστημα.

1.3.5 Απόσταση, Χρόνος και Χώρος

Στον κυβερνοχώρο δεν υφίστανται οι φυσικοί περιορισμοί στις έννοιες της απόστασης, του χρόνου και του χώρου. Μια μεταφορά ψηφιακών δεδομένων από το ένα σημείο του πλανήτη στο άλλο γίνεται με την ίδια ευκολία με μια μεταφορά δεδομένων μεταξύ 2 Η/Υ που βρίσκονται μέσα στο ίδιο σπίτι. Επίσης, η αποθήκευση των ψηφιακών δεδομένων στον κυβερνοχώρο δεν αντιμετωπίζει τις δυσκολίες της αποθήκευσης υλικών στον φυσικό χώρο[32].

1.3.6. Μεταβλητότητα

Ο κυβερνοχώρος ως ανθρώπινη κατασκευή είναι ατελής. Το λογισμικό (software) και το υλικό (hardware) δεν λειτουργούν ποτέ στο 100% της αρχικής σχεδίασης τους, γεγονός που αποδυναμώνει κάθε έννοια πρόβλεψης[33]. Το αποτέλεσμα κάθε φορά της ίδιας ενέργειας μπορεί να είναι διαφορετικό.

1.3.7 Διπλή Χρήση των «κυβερνοεργαλείων»

Μια σημαντική ιδιαιτερότητα στον κυβερνοχώρο είναι ότι τα «εργαλεία» (tools) που χρησιμοποιούνται έχουν διπλή χρήση (dual-use), δηλαδή μπορούν να χρησιμοποιηθούν για αντίθετους σκοπούς[34]. Για παράδειγμα, μια εφαρμογή που λέγεται σαρωτής τρωτότητας (vulnerabilities scanner) θα χρησιμοποιηθεί από τον διαχειριστή του δικτύου Η/Υ, προκειμένου να βρει τα πιθανά αδύναμα σημεία του δικτύου και να τα επιδιορθώσει. Με τον τρόπο αυτό θα αυξήσει την άμυνα του δικτύου. Ο ίδιος σαρωτής θα χρησιμοποιηθεί και από κάποιον που επιβουλεύεται το δίκτυο και θέλει να βρει τις τρωτότητες του για να του επιτεθεί. Σε αυτήν την περίπτωση ο σαρωτής θα χρησιμοποιηθεί για επιθετικούς σκοπούς.

---

[32] Parks, Raymond C. & Duggan, David P., "*Principles of Cyber Warfare*", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, US Military Academy, West Point, NY 5-6/6/01, Available at: http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf, accessed on February 2011.

[33] Ibid

[34] Ibid

1.3.8. Έλλειψη Συνόρων

Ένα από τα πιο σημαντικά χαρακτηριστικά του κυβερνοχώρου είναι η παντελής έλλειψη συνόρων. Ο εικονικός κόσμος του κυβερνοχώρου δεν γνωρίζει οριοθετήσεις, αντίστοιχες με αυτές του φυσικού κόσμου. Συνεπώς, οποιαδήποτε προσπάθεια προβολής των πραγματικών συνόρων των κρατών στον εικονικό κόσμο του κυβερνοχώρου είναι λανθασμένη.

1.4 Σημεία Τρωτότητας του Κυβερνοχώρου

Οι αδυναμίες που παρουσιάζονται στον κυβερνοχώρο αφορούν κυρίως στην αρχιτεκτονική του διαδικτύου (Internet), αλλά και στο λογισμικό (Software) και υλικό (Hardware) που εφαρμόζεται στους Η/Υ. Αδυναμίες στην αρχιτεκτονική τους παρουσιάζουν και τα λεγόμενα «κλειστά» δίκτυα Η/Υ. Ωστόσο, γίνεται εστίαση στο Internet, καθώς το διαδίκτυο αποτελεί πολλές φορές τον συνδετικό κρίκο μεταξύ των διακριτών «κλειστών» δικτύων Η/Υ (Intranets), μέσω συγκεκριμένων επικοινωνιακών κόμβων. Παράλληλα, το Internet αποτελεί τον σημαντικότερο δίαυλο μεταφοράς κακόβουλου λογισμικού (malware) παγκοσμίως. Συνεπώς, οι αδυναμίες στην αρχιτεκτονική του έχουν άμεσο αρνητικό αντίκτυπο στον κυβερνοχώρο. Από την άλλη μεριά, οι Η/Υ αποτελούν τα «κύτταρα» των δικτύων Η/Υ και οι αδυναμίες τους, οι οποίες δύναται να οφείλονται στα κύρια δομικά συστατικά τους (Software & Hardware) αποτελούν σημεία τρωτότητας για τον κυβερνοχώρο.

1.4.1 Η Αρχιτεκτονική του Internet

Όπως είναι γνωστό, το 1969 αποτελεί την χρονιά της «γέννησης» του Internet. Η αρχική ιδέα της σύλληψης του έγινε στα μέσα της δεκαετίας του ’60 και αφορούσε στην διασύνδεση ορισμένων Η/Υ που βρίσκονταν σε διάφορα επιστημονικά εργαστήρια πανεπιστημίων των ΗΠΑ. Αντικειμενικός σκοπός ήταν η δυνατότητα ανταλλαγής απόψεων, ιδεών και κειμένων από την επιστημονική κοινότητα. Την ίδια εποχή το αμερικανικό Πεντάγωνο εξέταζε πιθανούς τρόπους με τους οποίους θα μπορούσε να εξασφαλίσει την απρόσκοπτη επικοινωνία μέσω Η/Υ, ακόμα και μετά από πυρηνικό χτύπημα από την Σοβ. Ένωση. Για το λόγο αυτό, χρηματοδότησε ένα σχετικό πρόγραμμα έρευνας και ανάπτυξης, που αφορούσε στην δημιουργία της κατάλληλης τεχνολογικής εφαρμογής που θα πετύχαινε τον παραπάνω στόχο. Η ανάθεση του προγράμματος έγινε προς την αρμόδια υπηρεσία του Πενταγώνου, ARPA (Advanced Research Project Agency) και είχε ως αποτέλεσμα τη δημιουργία του

δικτύου ARPANET, το οποίο αποτελούνταν από 4 Η/Υ, κάθε ένας από τους οποίους βρισκόταν στα πανεπιστήμια UCSB, University of UTAH, Stanford και UCLA[35]. Με την πάροδο των ετών, το ARPANET οδήγησε σε αυτό που σήμερα είναι γνωστό ως Internet.

Σύμφωνα με τον Richard Clarke, η αρχιτεκτονική που δόθηκε στο Internet αντικατόπτριζε τις ευαισθησίες της εποχής που κατασκευάστηκε (Κίνημα των Χίπις), γεγονός που οδήγησε στο να μην υπάρχει τελικά ένας συγκεντρωτικός έλεγχος στο δίκτυο από καμία Αρχή[36], κάτι που ισχύει ακόμα και σήμερα[37]. Με τον τρόπο αυτό δόθηκε έμφαση στην αποκέντρωση του Internet και όχι στην ασφάλεια του. Οι κατασκευαστές του είχαν ως δεδομένα ότι στο Internet θα συμμετείχαν άτομα από την επιστημονική και ακαδημαϊκή κοινότητα, ενώ οι γραμμές δικτύωσης θα ήταν ελεγχόμενες. Δεν μπορούσαν να διανοηθούν ότι το Internet θα χρησιμοποιούνταν μελλοντικά από ένα τεράστιο πλήθος ανθρώπων και με τον τρόπο που χρησιμοποιείται σήμερα (έλεγχος κρίσιμων υποδομών, εμπόριο, χρηματοπιστωτικές συναλλαγές κλπ)[38]. Αξίζει να σημειωθεί ότι ορίστηκαν τότε 4 κατασκευαστικές αρχές, που ευνοούσαν την διασύνδεση νέων δικτύων με το αρχικό δίκτυο (ARPANET)[39] :

α. Κάθε ξεχωριστό δίκτυο Η/Υ θα πρέπει να υπάρχει από μόνο του. Δεν θα γίνονται εσωτερικές αλλαγές σε αυτό προκειμένου να συνδεθεί στο Internet.

β. Σε περίπτωση που ένα πακέτο δεδομένων δεν φτάσει στον προορισμό του, θα αποστέλλεται ξανά σε σύντομο χρονικό διάστημα από την πηγή.

γ. Θα υπάρχουν σημεία σύνδεσης των δικτύων, στα οποία δεν θα παρακρατούνται στοιχεία για τα πακέτα δεδομένων που μεταφέρονται στο δίκτυο.

δ. Δεν θα υπάρχει παγκόσμιος έλεγχος στο επιχειρησιακό επίπεδο.

Ως αποτέλεσμα, το Internet σήμερα παρουσιάζει τις εξής βασικές τρωτότητες, οι οποίες μεταφέρονται στον κυβερνοχώρο[40] :

α. Αδυναμία πλήρη ελέγχου στην κατεύθυνση των ψηφιοποιημένων πληροφοριών στον σωστό προορισμό. Αυτό σημαίνει ότι η αλληλογραφία μπορεί να κατευθυνθεί σε λάθος προορισμό, με την υπαιτιότητα ενός hacker.

β. Υπάρχει έλλειμμα στην κρυπτογράφηση της πληροφορίας που διακινείται στο διαδίκτυο. Αυτό ουσιαστικά σημαίνει ότι κάποιος (π.χ ένας hacker) θα μπορούσε να «δει» την αλληλογραφία κάποιου άλλου, να την τροποποιήσει ή να την διαγράψει.

---

[35] Γκισνέλ, Ζαν, *Πόλεμοι στον Κυβερνοχώρο: Μυστικές Υπηρεσίες και Internet* (Εκδόσεις Στάχυ, Αθήνα 1997), σελ. 305-312
[36] Clarke & Knake, 2010 : 81-82
[37] Knake, Robert K., "*Internet Governance in an Age of Cyber Insecurity*", CFR Special Report No56, September 2010, pp.5-6
[38] Clarke & Knake, 2010 : 83-84
[39] Ibid, p. 82
[40] Ibid, pp. 74-81

γ. Είναι πολύ εύκολη η διάδοση κακόβουλου λογισμικού (Malware[41] : Malicious Software) μέσα στο διαδίκτυο. Χαρακτηριστικά αναφέρεται ότι καταγράφονται κάθε μήνα 100 περίπου νέες υποθέσεις malware (CVE : Common Vulnerabilities and Exposures) που διαδίδονται στο Internet[42].

1.4.2 Λογισμικό (Software) και Υλικό (Hardware)

Η τρωτότητα που εμφανίζεται στον κυβερνοχώρο δεν αφορά αποκλειστικά στο Internet και τα δομικά του προβλήματα. Η εξέταση των υλικών (Hardware) και των λογισμικών (Software) που χρησιμοποιούνται στην πληροφορική τεχνολογία (IT: Information Technology) παρουσιάζει ιδιαίτερο ενδιαφέρον. Σύμφωνα με τον Martin Libicki, υπάρχει έντονος κίνδυνος για εμφάνιση τρωτότητας μέσα από την διαδικασία της λεγόμενης «Αλυσίδας Εφοδιασμού» (Supply Chain)[43]. Συγκεκριμένα υποστηρίζει ότι αν ο αγοραστής ενός υλικού ή ενός λογισμικού δεν έχει πλήρη πρόσβαση στον κώδικα των ηλεκτρονικών – δηλαδή την σειρά κωδικοποιημένων οδηγιών στην γλώσσα προγραμματισμού - που αγοράζει, τότε είναι αβοήθητος σε μια ενδεχόμενη επίθεση στον κυβερνοχώρο[44]. Ο ίδιος κίνδυνος αναφέρεται και στο στρατιωτικό εγχειρίδιο AFDD 3-12 των ΗΠΑ[45]. Σε αυτό επισημαίνεται ότι, οι ΗΠΑ βασίζονται σε μεγάλο βαθμό στα IT προϊόντα που κυκλοφορούν ευρέως στο εμπόριο – γνωστά ως προϊόντα COTS: Commercial Off-the-Shelf. Οι κατασκευαστές τους, οι πωλητές, οι πάροχοι υπηρεσιών (πχ συντήρησης) και αυτοί που τα αναπτύσσουν θα μπορούσαν να επηρεαστούν από αντιπάλους των ΗΠΑ και τελικά να παραδώσουν στις τελευταίες τροποποιημένα προϊόντα με ενσωματωμένες τρωτότητες (πχ ελαττωματικά Chips). Δηλαδή σε μια τέτοια περίπτωση, τα IT συστήματα των ΗΠΑ θα μπορούσαν να «καταρρεύσουν».

Το γεγονός ότι στην εποχή της παγκοσμιοποίησης τα διάφορα τμήματα ενός Η/Υ μπορεί να κατασκευαστούν σε διαφορετικές χώρες, ενισχύει από μόνο του την ύπαρξη μεγαλύτερης πιθανότητας για εμφάνιση τρωτότητας στο υλικό και το λογισμικό. Είναι επίσης αποδεκτό ότι, κατά την διάρκεια δημιουργίας λογισμικού – δηλαδή των προγραμμάτων και των συμβολικών γλωσσών που ελέγχουν την λειτουργία του υλικού (Hardware) και διευθύνουν την λειτουργία του – είναι πολύ πιθανό να γίνει κάποιο λάθος, το οποίο εφόσον είναι εμφανές θα διορθωθεί[46]. Ωστόσο, αν ληφθεί υπόψη ότι κάθε νέο λειτουργικό σύστημα ενός Η/Υ περιέχει κάθε φορά μεγαλύτερο αριθμό

[41] Το κακόβουλο λογισμικό ωθεί τον Η/Υ ή το δίκτυο Η/Υ να ενεργεί με τρόπο μη αποδεκτό για τους χρήστες (του Η/Υ) ή τον διαχειριστή του δικτύου.
[42] CVE List Main Page, http://cve.mitre.org/cve/index.html
[43] Libicki, 2009 : 22
[44] Ibid
[45] Air Force Doctrine Document 3-12 (AFDD 3-12): *Cyberspace Operations,* pp. 4-5. Available at : http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf, accessed on May 2011
[46] Clarke & Knake, 2010 : 89

τέτοιων εντολών, γίνεται κατανοητό ότι η πιθανότητα λάθους εγγραφής κώδικα αυξάνει, ενώ η πιθανότητα εύρεσης του μειώνεται. Χαρακτηριστικά αναφέρεται ότι, η έκδοση του λειτουργικού συστήματος Windows 95 – που θεωρείται ξεπερασμένη σήμερα – είχε κάτι λιγότερο από 10 εκατομμύρια γραμμές κώδικα, ενώ τα Windows Vista είχαν κάτι παραπάνω από 50 εκατομμύρια γραμμές κώδικα[47]. Αυτό που ανησυχεί ιδιαίτερα είναι ότι τα λάθη στο λογισμικό αναγνωρίζονται δύσκολα ακόμα και όταν αυτά βρίσκονται σε λίγες γραμμές κώδικα, ενώ δεν υπάρχει λογισμικό που να μπορεί να ελέγξει αυτήν την διαδικασία[48]. Θα πρέπει επίσης να τονιστεί ότι, οι πάροχοι λογισμικού διαθέτουν περιοδικά στους πελάτες τους επιδιορθώσεις λογισμικού (Patches), τις οποίες οι χρήστες θα πρέπει να εγκαθιστούν στο λογισμικό τους. Ωστόσο, αυτές γίνονται αντικείμενο εκμετάλλευσης από τους hackers, οι οποίοι δημιουργούν άμεσα το «αντίδοτο» σε αυτές[49]. Επιπλέον, αποτελεί συνήθη διαδικασία, αυτοί που αναπτύσσουν κώδικες να αφήνουν εσκεμμένα πίσω τους τις λεγόμενες «καταπακτές» (trapdoors), προκειμένου να μπορούν σε μελλοντικό χρόνο να επιστρέψουν και να προχωρήσουν σε αναβάθμιση του κώδικα, κάτι το οποίο εκμεταλλεύονται δεόντως οι hackers[50].

Ένα ακόμα στοιχείο που θα πρέπει να επισημανθεί είναι ότι, η τρωτότητα στο υλικό (hardware) γίνεται πιο εμφανής στην περίπτωση των ολοκληρωμένων κυκλωμάτων (Chips-Microchips), όπου κατά την φάση της κατασκευής τους – γνωστής και ως διαδικασίας των 400 βημάτων (400-step process) - μπορεί να γίνει κάποιο σκόπιμο λάθος, το οποίο δεν μπορεί να διαγνωσθεί[51]. Για το ίδιο θέμα, ο Clarke σημειώνει ότι η τρωτότητα που προκύπτει από εκατομμύρια γραμμές κώδικα (στο λογισμικό) μπορεί να προκύψει από τα εκατομμύρια κυκλώματα που θα αποτυπωθούν στα chips των Η/Υ, των Routers και των Servers[52]. Επίσης, τονίζει ότι οι περισσότεροι εξειδικευμένοι επαγγελματίες στα ολοκληρωμένα κυκλώματα δεν μπορούν να διακρίνουν εάν υπάρχει ένα πλεονάζον ή ένα λιγότερο στοιχείο σε ένα chip[53].

1.5 Απειλές στον Κυβερνοχώρο

Οι απειλές που εμφανίζονται στον κυβερνοχώρο αφορούν στην δυνατότητα εύρυθμης λειτουργίας του και χωρίζονται σε 3 κατηγορίες:

---

[47] Ibid
[48] Ibid, p. 90
[49] Libicki, 2009 : 18
[50] Clarke & Knake, 2010 : 91
[51] Clark, Wesley K. & Levin, Peter L., "*Securing the Information Highway"*, Foreign Affairs Magazine, Nov./Dec. 09, http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway, accessed on 9-12-2010
[52] Clarke & Knake, 2010 : 95
[53] Ibid

α. Απειλές από φυσικές επιθέσεις (physical attacks)[54]

Πρόκειται για επιθέσεις χωρίς την χρήση όπλων που στηρίζονται σε λογισμικό. Παράδειγμα τέτοιας απειλής είναι μια βόμβα ή ένας βαλλιστικός πύραυλος που θα χτυπήσει έναν τηλεπικοινωνιακό δορυφόρο ή ένα μεγάλο δίκτυο Η/Υ. Επίσης, ένα άλλο παράδειγμα είναι η σκόπιμη καταστροφή ενός αριθμού απαραίτητων υποδομών του κυβερνοχώρου π.χ κόψιμο καλωδίων οπτικών ινών, καταστροφή δικτύων Η/Υ, servers, routers κ.α. Οι συγκεκριμένες απειλές δεν αποτελούν αντικείμενο ανάλυσης αυτής της εργασίας.

β. Απειλές από ηλεκτρομαγνητικές επιθέσεις (electromagnetic attacks)[55]

Αφορούν σε χτυπήματα με όπλα ηλεκτρομαγνητικού παλμού (EMP weapons), τα οποία ουσιαστικά καθιστούν ανενεργούς τους Η/Υ. Οι συγκεκριμένες απειλές δεν αποτελούν αντικείμενο ανάλυσης αυτής της εργασίας.

γ. Απειλές από κυβερνοεπιθέσεις (Cyber attacks)[56]

Οι απειλές αυτές αποτελούν αντικείμενο ανάλυσης στην παρούσα εργασία. Απορρέουν από την χρήση των κυβερνοόπλων (cyber weapons) - π.χ malware, botnets, DDoS - κατά των Η/Υ και των δικτύων τους. Μέσα από την χρήση των κυβερνοόπλων, τα είδη των οποίων θα αναλυθούν στην συνέχεια – οι επιτιθέμενοι στοχοποιούν τα εξής :

(i) Την διατήρηση της διαβάθμισης των ψηφιακών δεδομένων (Confidentiality)[57]. Σε αυτήν την κατηγορία περιλαμβάνεται κάθε προσπάθεια απόκτησης πληροφορίας, χωρίς την απαιτούμενη εξουσιοδότηση. Αυτό μπορεί να προκύψει και μέσα από τον έλεγχο ροής (Traffic Analysis) των δεδομένων, καθώς δίνονται στοιχεία για το περιεχόμενο της επικοινωνίας. Θα πρέπει να σημειωθεί ότι, η παγκόσμια διασύνδεση των δικτύων Η/Υ έχει «ξεπεράσει» κατά πολύ την ασφάλεια αυτών των δικτύων[58]. Συνεπώς, ένας ικανός hacker, δραστηριοποιούμενος στο συντακτικό επίπεδο του κυβερνοχώρου, δύναται να αποκτήσει ή να παρακάμψει τις απαιτούμενες εξουσιοδοτήσεις και να αποκτήσει με παράνομο τρόπο δεδομένα και πληροφορίες.

---

[54] McConnell, Mike, "*Cyber Insecurities: the 21st Century Threatscape*", p. 32 στο συλλογικό έργο Lord, Kristin M. & Sharp, Travis (Eds), "*America's Cyber Future: Security and Prosperity in the Information Age*, Vol.2, CNAS, June 2011. Available at : http://www.cnas.org, accessed on June 2011

[55] Ibid, p. 33

[56] Ibid, pp. 33-34

[57] Geers, Kenneth, *Strategic Cyber Security* (CCD COE Publication, Tallinn, Estonia, 2011), p.137

[58] Ibid

(ii) Την ακεραιότητα των δεδομένων (Integrity)[59]. Σε αυτήν την περίπτωση περιλαμβάνεται κάθε ενέργεια που αποσκοπεί στην χωρίς εξουσιοδότηση τροποποίηση των πληροφοριών και των βάσεων δεδομένων (databases). Μια τέτοιου είδους ενέργεια ισοδυναμεί με δολιοφθορά και μπορεί να λάβει χώρα για πολιτικούς, οικονομικούς ή στρατιωτικούς σκοπούς[60].

(iii) Την διαθεσιμότητα των δεδομένων (Availability)[61]. Σε αυτήν την περίπτωση περιλαμβάνεται κάθε ενέργεια που αποσκοπεί στη διακοπή της ομαλής ροής των ψηφιακών δεδομένων. Αυτό επιτυγχάνεται μέσα από μια διαδικασία που είναι γνωστή ως DoS (Denial of Service) και η οποία θα αναλυθεί στην συνέχεια.

1.6 Φορείς Απειλών

Ο καθηγητής Martin Libicki αναφερόμενος στα άτομα που δύνανται να πραγματοποιήσουν τις απειλές από κυβερνοεπιθέσεις χωρίζει τους κινδύνους στον κυβερνοχώρο σε εξωτερικούς και εσωτερικούς[62]. Ο διαχωρισμός γίνεται με σημείο αναφοράς ένα δίκτυο Η/Υ. Σε περίπτωση που η πραγματοποίηση της απειλής προέρχεται από κάποιον που βρίσκεται εκτός του δικτύου, τότε ο κίνδυνος χαρακτηρίζεται ως εξωτερικός. Όταν η πραγματοποίηση της απειλής γίνεται από κάποιον που βρίσκεται εντός του δικτύου, τότε ο κίνδυνος είναι εσωτερικός. Οι εξωτερικοί κίνδυνοι προέρχονται από τους hackers, ενώ οι εσωτερικοί κίνδυνοι πηγάζουν από τα ίδια τα μέλη μιας ομάδας του δικτύου (Insiders) ή από τα ελαττωματικά προϊόντα της «Αλυσίδας Εφοδιασμού» (Supply Chain)[63].

1.6.1 Οι Hackers

Αρχικά η έννοια hacker είχε θετικό αντίκτυπο. Με τον όρο αυτό χαρακτηριζόταν ένα άτομο ιδιαίτερα έξυπνο, εξειδικευμένο στους Η/Υ και με γνώσεις στην τεχνολογία Η/Υ, το οποίο μπορούσε να επέμβει στο λογισμικό (software) ή/και στο υλικό (hardware) ενός Η/Υ και να τον «αναγκάσει» να εργαστεί στα λειτουργικά του όρια. Με άλλα λόγια, έθετε έναν Η/Υ σε λειτουργία πέρα των ορίων που είχαν οριστεί από τους κατασκευαστές του[64]. Επίσης, ως hacker χαρακτηριζόταν πολλές φορές ένα άτομο νεαρής ηλικίας με ερασιτεχνικές γνώσεις στην πληροφορική, το οποίο συνήθιζε να αντιγράφει πακέτα λογισμικού ή να διεισδύει σε δίκτυα Η/Υ, χωρίς να έχει την

[59] Ibid
[60] Ibid
[61] Ibid
[62] Libicki, 2009 : 13-23
[63] Ibid, p.13
[64] Geers, 2011 : 20

απαραίτητη εξουσιοδότηση. Οι ενέργειες του απέρρεαν από την αδυναμία του να ανταποκριθεί στο κόστος των λογισμικών ή στην νοοτροπία παιχνιδιού που διακατέχονταν (λόγω του νεαρού της ηλικίας)[65]. Μια άλλη προσέγγιση, θεωρούσε τον hacker ως κάποιον ειδικό της πληροφορικής, ο οποίος παραβίαζε ένα σύστημα ή δίκτυο Η/Υ, έχοντας εγκληματικά κίνητρα (π.χ βιομηχανική κατασκοπεία, εκβιασμό, τραπεζική απάτη)[66]. Με την πάροδο των ετών και την αύξηση της συχνότητας των εγκληματικών ενεργειών από hackers, η έννοια hacker απέκτησε αρνητικό νόημα[67].

Όπως έχει προαναφερθεί, οι hackers - οι οποίοι μπορεί να έχουν διάφορες ιδιότητες, π.χ απλοί ιδιώτες, εγκληματίες, υπάλληλοι υπηρεσιών πληροφοριών, στρατιωτικοί, τρομοκράτες, ακτιβιστές κτλ. - δραστηριοποιούνται στο Συντακτικό Επίπεδο (syntactic layer) του κυβερνοχώρου, το οποίο φράσσεται από διάφορες «εξουσίες» (authorities)[68]. Κάθε δίκτυο Η/Υ – όπως αυτά των εταιρειών - λειτουργεί με βάση το δίπολο Διαχειριστής Δικτύου (System Administrator ή Sysadmin) – Χρήστες (Users). Ο διαχειριστής του δικτύου κατέχει τις απαιτούμενες «εξουσίες», για να καθορίσει πως θα χρησιμοποιεί ο κάθε χρήστης τον Η/Υ του, που ανήκει στο δίκτυο Η/Υ. Στην περίπτωση ενός μεμονωμένου Η/Υ, ο διαχειριστής και ο χρήστης είναι το ίδιο πρόσωπο, οπότε ο χρήστης έχει τον πλήρη έλεγχο του Η/Υ[69].

Μέλημα των Hackers είναι να παραβιάσουν αυτές τις «εξουσίες» και να αποκτήσουν πρόσβαση στο δίκτυο, η οποία μπορεί να έχει μεγάλη διάρκεια. Για να γίνει αυτό θα πρέπει να εκμεταλλευτούν τις τρωτότητες που υπάρχουν στο λογισμικό του δικτύου ή να «πείσουν» το δίκτυο να δεχτεί τις κακόβουλες οδηγίες (σε μορφή κώδικα Η/Υ) που του δίνουν[70]. Η διαδικασία αυτή ονομάζεται «Εκμετάλλευση» (Exploit). Μια συνηθισμένη τακτική είναι η αποστολή ηλεκτρονικών μηνυμάτων που περιέχουν κακόβουλο λογισμικό προς τον χρήστη – θύμα, ενώ μια άλλη είναι να δελεάσουν κάποιον χρήστη να επισκεφτεί μια «ύποπτη» ιστοσελίδα που περιέχει malware. Και στις 2 περιπτώσεις, οι hackers αποσκοπούν στο να αποθηκευτεί αυτόματα το malware στον Η/Υ του χρήστη, για να αποκτήσουν πρόσβαση σε αυτόν[71]. Από την στιγμή που αποκτήσουν πρόσβαση στον Η/Υ ή στο δίκτυο, προσπαθούν να φαίνονται ως νόμιμοι χρήστες του ή να γίνουν οι ίδιοι Sysadmins.

Αντικειμενικοί σκοποί των Hackers είναι οι παρακάτω[72]:

α. Υπεξαίρεση δεδομένων (δηλ. παραβίαση του Confidentiality)

[65] Γαρίδης & Δεληγιαννάκης, 1993 : 251
[66] Ibid
[67] Geers, 2011 : 21
[68] Libicki, 2009 : 13
[69] Ibid
[70] Ibid, p. 18
[71] Ibid, p. 13
[72] Ibid, pp. 15-17

β. Διαταραχή (Disruption) του Η/Υ ή του δικτύου (δηλ. παραβίαση του Integrity). Η Διαταραχή λαμβάνει χώρα όταν ένα σύστημα εξαπατάται και:

(i) εκτελεί λειτουργίες που οδηγούν στο κλείσιμο του.

(ii) λειτουργεί σε ένα ποσοστό των δυνατοτήτων του

(iii) διαπράττει προφανή λάθη

(iv) εμπλέκεται με την λειτουργία άλλων συστημάτων

γ. Διαφθορά (Corruption) του Η/Υ ή του δικτύου (δηλ. παραβίαση του Integrity). Η Διαφθορά συμβαίνει όταν τα δεδομένα και οι αλγόριθμοι αλλάζονται εσκεμμένα χωρίς εξουσιοδότηση και σε βάρος της σωστής λειτουργίας τους. Ουσιαστικά, οδηγεί σε κακή ποιότητας λειτουργία του Η/Υ. Η βασική διαφορά μεταξύ Corruption & Disruption είναι ότι τα αποτελέσματα της Διαταραχής είναι άμεσα, δραστικά και εμφανή, ενώ τα αποτελέσματα του Διαφθοράς καθυστερούν και είναι επαναλαμβανόμενα.

δ. Χρήση των λοιπών δικτύων Η/Υ για διεξαγωγή DDoS (Distributed Denial of Service) επιθέσεων (δηλ. παραβίαση του Availability). Σε αυτήν την περίπτωση, πολλοί Η/Υ (Botnets) ακολουθούν τις εντολές του hacker – χωρίς την γνώση των χρηστών τους – και στέλνουν συνέχεια πακέτα δεδομένων σε έναν συγκεκριμένο προορισμό (π.χ ένα Η/Υ ή έναν server), προκειμένου να επιτευχθεί κορεσμός και ο στόχος – θύμα να μην μπορεί να επικοινωνεί με το υπόλοιπο σύστημα Η/Υ.

Οι hackers επιτυγχάνουν τους σκοπούς τους με την χρήση των κυβερνοόπλων (Cyber Weapons), τα οποία είναι προγράμματα Η/Υ που έχουν την ικανότητα να διαταράσσουν την αποθήκευση δεδομένων (data storage) ή την λογική επεξεργασίας (processing logic) των Η/Υ[73]. Διάφορες εκδόσεις αυτών των κυβερνοόπλων είναι διαθέσιμες στο διαδίκτυο. Τα πιο γνωστά cyber weapons είναι τα παρακάτω :

α. <u>Επιθετικά (Offensive)</u>

(i) <u>Virus</u>

Πρόκειται για πρόγραμμα Η/Υ, το οποίο απλώνεται εισάγοντας αντίγραφα του εαυτού του μέσα σε άλλους εκτελέσιμους κώδικες και έγγραφα. Συμπεριφέρεται όπως ένας βιολογικό ιός[74]. Είναι πρόγραμμα που περνάει από χρήστη σε χρήστη μέσω του Internet ή μέσω ενός φορητού αποθηκευτικού χώρου (π.χ flash drive) και έχει ως στόχο να διαταράξει την λειτουργία ενός Η/Υ, να δημιουργήσει ένα

[73] Wilson, Clay, "*Information Operations and Cyberwar: Capabilities and Related Policy Issues*", CRS Report for Congress, p.6. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456478&Location=U2&doc=GetTRDoc.pdf, accessed on May 2011

[74] Nugent, John H.& Raisinghani, Mahesh, *Bits and Bytes vs. Bullets and Bombs: A new Form of Warfare*, p. 34 (κεφ. 4 στο συλλογικό έργο των Janczewski, Lech J. & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)

κρυφό σημείο πρόσβασης στο σύστημα ή να αντιγράψει και να υπεξαιρέσει πληροφορίες[75].

(ii) Worm

Πρόκειται για ένα αυτό - αντιγραφόμενο πρόγραμμα, το οποίο χρησιμοποιεί ένα δίκτυο-ξενιστή για να στείλει αντίγραφα του εαυτού του σε άλλους Η/Υ στο δίκτυο. Σε αντίθεση με το Virus, δεν απαιτείται να προσκολληθεί σε ήδη υπάρχοντα προγράμματα και μπορεί να διαδοθεί μόνο του. Στοχεύει στην «μόλυνση» του δικτύου και όχι κάποιων μεμονωμένων φακέλων (files). Εκμεταλλεύεται τις τρωτότητες στο λειτουργικό σύστημα και συνήθως εγκαθιστά μια «δίοδο» ("backdoor") που επιτρέπει τον έλεγχο εξ αποστάσεως του «μολυσμένου» συστήματος[76].

(iii) Phising Scam

Πρόκειται για τρικ (trick) με το οποίο αποστέλλονται emails και αληθοφανείς ιστοσελίδες προς έναν χρήστη του Internet, προκειμένου αυτός να ξεγελαστεί και να δώσει προσωπικές πληροφορίες, όπως αριθμούς τραπεζικών λογαριασμών και κωδικούς πρόσβασης[77].

(iv) Trojan Horse

Πρόκειται για πρόγραμμα που αποκρύπτει το κακόβουλο περιεχόμενο του. Εγκαθίσταται από τον ίδιο τον χρήστη - θύμα μέσα από το άνοιγμα ενός link που περιέχεται σε ένα email ή από την ηλεκτρονική λήψη περιεχομένου (online download). Συνήθως το Trojan Horse δημιουργεί μια "backdoor" που επιτρέπει τον έλεγχο εξ αποστάσεως του «μολυσμένου» συστήματος ή εμπλέκεται σε καταστροφή δεδομένων. Δεν είναι αυτό – αντιγραφόμενο πρόγραμμα[78].

(v) Denial of Service Tool

Πραγματοποιείται με αποστολή μεγάλου όγκου δεδομένων [«πλημμύρα» (flood)] προς τον στόχο Η/Υ ή δίκτυο, με αποτέλεσμα τον κορεσμό τους και την απώλεια προσβασιμότητας σε αυτά από τους νόμιμους χρήστες τους[79].

---

[75] Clarke & Knake, 2010 : 81
[76] Meyers, C., Powers, S. & Faissol, D., "*Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches"*,p.14.Available at: http://www.osti.gov/bridge/product.biblio.jsp?osti_id=967712, accessed on June 2011
[77] Clarke & Knake, 2010 : 81
[78] Meyers, C., Powers, S. & Faissol, D., "*Taxonomies of Cyber……", p.14*
[79] Ibid, p.16

(vi) Logic Bomb

Πρόκειται για εφαρμογή λογισμικού ή σύνολο οδηγιών που προκαλούν το κλείσιμο του Η/Υ ή του δικτύου ή/και την διαγραφή των δεδομένων ή του λογισμικού του δικτύου[80].

β. Διπλής Χρήσης (Dual Use)

(i) Port Vulnerability Scanner

Πρόκειται για πρόγραμμα Η/Υ που αξιολογεί Η/Υ, συστήματα Η/Υ, δίκτυα ή εφαρμογές για τυχόν αδυναμίες[81].

(ii) Network Monitoring

Αναφέρεται σε σύστημα που ελέγχει συνεχώς ένα δίκτυο Η/Υ για εξαρτήματα που υπολειτουργούν ή έχουν καταστραφεί και ενημερώνει το διαχειριστή του συστήματος (π.χ με email) σε περίπτωση κάποιας διακοπής λειτουργίας[82].

γ. Αμυντικά (Defensive)

(i) Encryption

Είναι η κωδικοποίηση της ψηφιακής πληροφορίας, ώστε να μη είναι αναγνώσιμη σε όσους δεν διαθέτουν την κλείδα (κώδικα) αποκωδικοποίησης[83].

(ii) Firewall

Πρόκειται για ένα «τείχος προστασίας» που ρυθμίζει την ροή των δεδομένων μεταξύ δικτύων Η/Υ που έχουν διαφορετικά επίπεδα ασφαλείας[84].

1.6.2 Οι Insiders και το Supply Chain

Σύμφωνα με τον Libicki, τα κράτη έχουν 2 ακόμα μεθόδους για να αποκτήσουν πρόσβαση στα συστήματα Η/Υ. Αυτές είναι η μέθοδος των Insiders και η μέθοδος του Supply Chain. Στην πρώτη περίπτωση, κάποιος, ο οποίος είναι ήδη μέλος μιας ομάδας που δραστηριοποιείται σε ένα δίκτυο Η/Υ μιας χώρας Α, στρατολογείται από μια χώρα Β προκειμένου να κάνει δολιοφθορά στο δίκτυο της χώρας Α. Ο Insider χρησιμοποιεί

[80] Clarke & Knake, 2010 : 287
[81] *The Free Dictionary by Farlex*, available at: http://www.thefreedictionary.com
[82] Ibid
[83] Clarke & Knake, 2010 : 284
[84] *The Free Dictionary by Farlex*, available at: http://www.thefreedictionary.com

τις τεχνικές ενός hacker. Στην 2η περίπτωση, μια εταιρεία από το κράτος Α προμηθεύει το κράτος Β με «ελαττωματικά» εξαρτήματα[85] για το δίκτυο Η/Υ του, τα οποία περιέχουν κώδικα (κωδικοποιημένες οδηγίες για Η/Υ) που ανταποκρίνεται στην «θέληση» του κράτους Α ή στην «θέληση» ενός άλλου κράτους, το οποίο είναι εχθρικά διακείμενο προς το κράτος Β[86]. Οι 2 ανωτέρω περιπτώσεις υπεισέρχονται στο πεδίο δράσης των Υπηρεσιών Πληροφόρησης (Intelligence Services) και αφορούν κυρίως τα λεγόμενα «κλειστά» δίκτυα Η/Υ, δηλ. αυτά που δεν επικοινωνούν με το Internet[87].

Χαρακτηριστικό παράδειγμα Insider πιθανώς να αποτελεί η περίπτωση της αδρανοποίησης του συριακού συστήματος αεράμυνας (ραντάρ) λίγο πριν από τον βομβαρδισμό των πυρηνικών εγκαταστάσεων της Συρίας στην περιοχή Dayr az-Zawr το 2007. Στο υπόψη συμβάν εικάζεται ότι, οι Ισραηλινοί είχαν καταφέρει, μέσω Insider είτε στο ρωσικό εργαστήριο κατασκευής λογισμικού για τα συριακά ραντάρ είτε σε μια συριακή στρατιωτική μονάδα, να εμφυτεύσουν μια “trapdoor” στο λογισμικό λειτουργίας του συριακού συστήματος ραντάρ. Μέσω αυτής, κατάφεραν να αδρανοποιήσουν το σύνολο της συριακής αεράμυνας[88].

Όσον αφορά στον κίνδυνο του “supply chain” αξίζει να αναφερθεί η σοβιετική προσπάθεια υποκλοπής από τον Καναδά, στις αρχές της δεκαετίας του 1980, δυτικής εμπορικής και βιομηχανικής τεχνολογίας. Όταν έμαθαν οι ΗΠΑ ότι οι Σοβιετικοί (KGB) επιδίωκαν να υποκλέψουν από τον Καναδά τεχνολογία, που αφορούσε σε αυτοματοποιημένες αντλίες και συστήματα ελέγχου ροής αγωγών πετρελαίου και φυσικού αερίου, προμήθευσαν την γειτονική χώρα[89] με ελαττωματικό λογισμικό, το οποίο ενσωματώνονταν στα παραπάνω αυτοματοποιημένα συστήματα[90]. Οι Σοβιετικοί αφού υπέκλεψαν την υπόψη τεχνολογία, την ενσωμάτωσαν στους αγωγούς τους, οι οποίοι για ένα εύλογο χρονικό διάστημα λειτούργησαν ικανοποιητικά. Ωστόσο, σε δεδομένη χρονική στιγμή, την οποία είχαν προεπιλέξει οι ΗΠΑ μέσω του ελαττωματικού λογισμικού, οι αντλίες και οι βαλβίδες των ρωσικών αγωγών οδηγήθηκαν σε δυσλειτουργία, με αποτέλεσμα να σημειωθεί ισχυρότατη έκρηξη 3 κιλοτόνων στο δίκτυο αγωγών της ΕΣΣΔ[91].

[85] Τα εξαρτήματα αυτά μπορούν να φέρουν logic bombs ή backdoors στο λογισμικό ή στα microchips τους, με αποτέλεσμα την πρόκληση δυσλειτουργιών ή την χειραγώγηση των συστημάτων Η/Υ από απόσταση.
[86] Libicki, 2009: 22. Βλέπε επίσης παρ. 1.4.2 : *Λογισμικό (Software) και Υλικό (Hardware)*
[87] Ibid, p. 20
[88] Clarke & Knake, 2010: 7
[89] Οι ΗΠΑ είχαν ενημερώσει τον Καναδά για τις ενέργειες τους.
[90] Clarke & Knake, 2010: 92-93
[91] Ibid

2. Οι Συγκρούσεις στον Κυβερνοχώρο

2.1 Γενικά

Από την σύντομη περιγραφή που προηγήθηκε, έγινε εμφανές ότι ο αριθμός των άμεσα ενδιαφερόμενων χρηστών του κυβερνοχώρου αυξάνεται συνεχώς. Σε αυτούς συγκαταλέγονται τα κράτη, οι ένοπλες δυνάμεις, οι επιχειρήσεις, οι οργανισμοί, οι ομάδες πίεσης, οι ιδιώτες, οι εγκληματίες, οι τρομοκράτες κτλ. Ο μεγάλος αριθμός των ενδιαφερομένων σηματοδοτεί την ύπαρξη πολλών και διαφορετικών συμφερόντων στον κυβερνοχώρο, τα οποία σε πολλές περιπτώσεις συγκρούονται μεταξύ τους. Όπως είναι φυσικό, η προσπάθεια του κάθε ενός από τους προαναφερθέντες ενδιαφερόμενους να ελέγξει μερικώς ή ολικώς τον κυβερνοχώρο, για δικό του όφελος, προοικονομεί τον κίνδυνο των συγκρούσεων[92].

Ως σύγκρουση στον κυβερνοχώρο ή Κυβερνοσύγκρουση (Cyber Conflict) ορίζεται η αντιπαράθεση μεταξύ 2 ή περισσοτέρων πλευρών στην ανωτέρω περιοχή, με μια τουλάχιστον εκ των οποίων να χρησιμοποιεί κυβερνοεπιθέσεις (Cyber attacks) ενάντια των υπολοίπων[93]. Με τον όρο Κυβερνοεπίθεση νοείται κάθε σκόπιμη προσπάθεια που γίνεται από μια πλευρά για την επίτευξη Διαταραχής (Disruption) ή Διαφθοράς (Corruption) ή Κορεσμού (με αποτέλεσμα το Denial of Service) στα συστήματα Η/Υ της άλλης πλευράς. Επισημαίνεται ότι, η παράνομη άντληση δεδομένων από τα δίκτυα Η/Υ (Computer Network Exploitation: CNE) δεν χαρακτηρίζεται ως κυβερνοεπίθεση[94].

Κατά την τελευταία δεκαετία, τόσο ο αριθμός των κυβερνοεπιθέσεων, όσο και η εξειδίκευση των κακόβουλων λογισμικών που χρησιμοποιούνται σε αυτές έχουν αυξηθεί σημαντικά[95], με αποτέλεσμα την αύξηση των κυβερνοσυγκρούσεων. Σύμφωνα με ανακοίνωση[96] στα τέλη του 2010 της εταιρείας παροχής ασφάλειας στον κυβερνοχώρο Panda, από τον Ιανουάριο μέχρι τον Οκτώβριο του 2010 ανακαλύφθηκαν 20 εκατομμύρια νέα είδη κακόβουλου λογισμικού, με τις απειλές στον κυβερνοχώρο σε καθημερινή βάση να φθάνουν περίπου τις 63.000. Σημειώνεται ότι ο

---

[92] Ottis, R. & Lorents, P. (2010). "*Cyberspace: Definition….", p. 269*

[93] Ibid

[94] Libicki, 2009: 23-24. Βλέπε επίσης, Hunker, Jeffrey, " *Cyberwar and Cyber Power. Issues for NATO doctrine*", Research Division, NATO Defense College, Rome, Research Paper No 62, November 2010, p.2. Available at: http://www.ndc.nato.int/research/series.php?icode=1, accessed on April 2011. Θα πρέπει να σημειωθεί ότι πολλοί δεν θεωρούν το CNE ως είδος κυβερνοεπίθεσης γιατί δεν προκαλεί καταστροφή ή δυσλειτουργία σε έναν Η/Υ. Ωστόσο, μια κυβερνοεπίθεση στην αρχική της φάση στηρίζεται στην διείσδυση στο δίκτυο του αντιπάλου, όπως και το CNE.

[95] Carr, 2010: 5

[96] Άρθρο στις 24-11-2010 με τίτλο: "*One third of all computer viruses that exist were created in the first 10 months of 2010*", Panda Security. Available at: http://press.pandasecurity.com/news/one-third-of-all-computer-viruses-that-exist-were-created-in-the-first-10-months-of-2010/, accessed on January 2011

αντίστοιχος αριθμός για το 2009 ο αριθμός έφθανε τις 55.000. Επιπλέον, στην πρόσφατη ετήσια έκθεση της (2011 Annual Security Report[97]), η Panda ανέφερε ότι το 2011 ανακαλύφθηκαν 26 εκατομμύρια νέα είδη κακόβουλου λογισμικού, με τον αριθμό των καθημερινών απειλών στον κυβερνοχώρο να φθάνει στις 73.000 περίπου. Αξίζει να τονιστεί ότι ο αριθμός των νέων malwares για το 2011 προσεγγίζει το 1/3 από τα συνολικά 88 εκατομμύρια malwares που έχει αποκαλύψει η συγκεκριμένη εταιρεία. Θα πρέπει ακόμα να αναφερθεί ότι η Panda εκτιμά πως θα υπάρχει νέα αύξηση των malwares μέσα στο 2012.

2.2 Το «Νομικό Καθεστώς» των Κυβερνοεπιθέσεων

Παρά την δραματική αύξηση των κυβερνοεπιθέσεων, δεν έχει προκύψει μέχρι σήμερα διεθνής συνθήκη που να προσφέρει έναν νομικό ορισμό για το τι είναι η κυβερνοεπίθεση[98]. Επίσης, η εκδήλωση κυβερνοεπιθέσεων δεν λογίζεται διεθνώς ως πράξη πολέμου (Act of War), αλλά αντιμετωπίζεται από τα κράτη ως εγκληματικό φαινόμενο[99]. Τόσο σε επίπεδο ΟΗΕ όσο και σε επίπεδο περιφερειακών οργανισμών, οι κυβερνοεπιθέσεις δεν εκλαμβάνονται ως ένοπλες επιθέσεις (armed attacks), ενώ δεν υφίστανται πολυμερείς διακρατικές συμφωνίες για το θέμα[100]. Η μέχρι σήμερα πρακτική των κρατών, που έχουν δεχθεί σημαντικές κυβερνοεπιθέσεις, καταδεικνύει ότι οι ανωτέρω επιθέσεις, αν και δημιουργούν πολλές φορές σημαντικά προβλήματα, δεν επισύρουν απάντηση με φυσικό τρόπο (π.χ συμβατικά πλήγματα) από το κράτος – θύμα. Πέραν από την εκδήλωση διαμαρτυριών σε πολιτικό επίπεδο από τα κράτη που έχουν δεχτεί κυβερνοεπιθέσεις, δεν υπάρχουν επίσημες καταγραφές αντιποίνων σε οικονομικό, πολιτικό ή διπλωματικό επίπεδο ή αντίποινα στον κυβερνοχώρο με κυβερνοεπιθέσεις (retaliation in kind). Το ερώτημα βέβαια που τίθεται είναι το κατά πόσο θα είχε νόημα ένα κράτος Α (θύμα κυβερνοεπιθέσεων) να εκδηλώσει αντίποινα με κυβερνοεπιθέσεις προς ένα άλλο κράτος Β (θύτη των προαναφερόμενων κυβερνοεπιθέσεων), το οποίο διαθέτει ελάχιστες υποδομές ΙΤ τεχνολογίας.

Οι κυβερνοεπιθέσεις αποτελούν μη συμβατικό είδος επίθεσης, που προέκυψε μετά από πολλά χρόνια από την σύνταξη του καταστατικού χάρτη του ΟΗΕ, ο οποίος

---

[97] Η ετήσια έκθεση της Panda Security για το 2011 βρίσκεται στην ηλεκτρονική διεύθυνση: http://press.pandasecurity.com/wp-content/uploads/2012/01/Annual-Report-PandaLabs-2011.pdf, accessed on January 2012

[98] Carr, 2010: 31

[99] Carr, 2010: 47

[100] Libicki, 2009: 179 – 180. Μοναδική εξαίρεση αποτελεί η Ευρωπαϊκή Συνθήκη για το έγκλημα στον κυβερνοχώρο (European Convention on Cybercrime), η οποία έχει επικυρωθεί από 26 χώρες, μεταξύ των οποίων οι ΗΠΑ, το Η.Β, η Γερμανία και η Γαλλία, που συγκεντρώνουν το 25% των παγκόσμιων χρηστών του Internet. Η συνθήκη αυτή αντιμετωπίζει τις κυβερνοεπιθέσεις ως έγκλημα και όχι ως ένοπλες επιθέσεις, ώστε τα κράτη - θύματα να μπορούν να επικαλεστούν το δικαίωμα τους στην νόμιμη άμυνα, σύμφωνα με το άρθρο 51 του καταστατικού χάρτη του ΟΗΕ.

αναφέρεται στις συμβατικές επιθέσεις από τα κράτη. Οι κυβερνοεπιθέσεις, επίσης, δύναται να διεξαχθούν και από μη κρατικούς παράγοντες. Μέχρι σήμερα, η διεθνής κοινότητα δείχνει απροθυμία να αποδεχθεί τις κυβερνοεπιθέσεις ως ισότιμες με τις παραδοσιακές ένοπλες επιθέσεις που πραγματοποιούνται με συμβατικά όπλα, παρόλο που οι κυβερνοεπιθέσεις δύνανται να προκαλέσουν τραυματισμούς ή θάνατο[101]. Για το λόγο αυτό, διάφοροι μελετητές προσπάθησαν να δημιουργήσουν τα κατάλληλα αναλυτικά μοντέλα, με τα οποία θα μπορούσαν να τις προσεγγίσουν και να τις αναλύσουν. Σήμερα υπάρχουν 3 κύρια αναλυτικά μοντέλα – προσεγγίσεις για τις κυβερνοεπιθέσεις. Η πρώτη προσέγγιση είναι γνωστή ως "Instrument – Based Approach[102]" και προσπαθεί να διαγνώσει αν η ζημία που προκλήθηκε από την κυβερνοεπίθεση, μπορούσε στο παρελθόν να προκληθεί από κινητική επίθεση (kinetic attack). Π.χ με μια κυβερνοεπίθεση μπορεί να προκαλέσει την παύση λειτουργίας ενός εργοστασίου ηλεκτρικής ενέργειας. Το ίδιο αποτέλεσμα θα είχε στο παρελθόν ο βομβαρδισμός του εργοστασίου. Συνεπώς, σύμφωνα με την "Instrument – Based Approach" η συγκεκριμένη κυβερνοεπίθεση αποτελεί ένοπλη επίθεση. Η δεύτερη προσέγγιση, γνωστή ως "Effects – Based Approach", εστιάζει στον αντίκτυπο που είχε η κυβερνοεπίθεση στο θύμα. Με τον τρόπο αυτό μια κυβερνοεπίθεση κατά του χρηματοπιστωτικού συστήματος μιας χώρας, η οποία θα προκαλέσει σημαντική οικονομική ζημία στο κράτος-θύμα συνιστά ένοπλη επίθεση[103]. Η τρίτη προσέγγιση, "Strict Liability Approach", εκλαμβάνει τις κυβερνοεπιθέσεις κατά των κρίσιμων υποδομών μιας χώρας ως ένοπλες επιθέσεις και δικαιολογεί την άμεση εκδήλωση αντιποίνων ή ακόμα και την προληπτική νόμιμη άμυνα (Anticipatory Self-Defence) από τα κράτη[104].

Από τις παραπάνω προσεγγίσεις προκρίνεται συνήθως η "Effects – Based Approach", καθώς περιλαμβάνει όλες τις περιπτώσεις, που θα κάλυπτε η "Instrument – Based Approach", ενώ αναφέρεται και στις περιπτώσεις εκείνες που δεν θα μπορούσαν να προκληθούν από κινητική επίθεση (kinetic attack). Για παράδειγμα η κατάρρευση του παγκόσμιου χρηματοπιστωτικού συστήματος δεν μπορεί να προκληθεί από kinetic attack, αλλά μπορεί να συμβεί μέσω κυβερνοεπιθέσεων. Επιπρόσθετα, σε αντίθεση με την "Strict Liability Approach", η οποία αναφέρεται σε άμεση εκδήλωση αντιποίνων ή προληπτική νόμιμη άμυνα, η "Effects – Based

[101] Carr, 2010: 57. Επίσης, βλέπε Liaropoulos, Andrew (2011), *"Cyber Security and the Law of War: Legal and Ethical Aspects of Cyber Conflict"*, GPSG Working Paper # 7, p. 5. Available at: http://piraeus.academia.edu/AndrewLiaropoulos/Papers/617962/Cyber-Security_and_the_Law_of_War_The_Legal_and_Ethical_Aspects_of_Cyber-conflict, accessed on May 2011

[102] Carr, 2010: 59

[103] Ibid

[104] Ibid

Approach" δεν παραβιάζει το διεθνές δίκαιο, καθώς ακολουθεί τους διεθνώς αποδεκτούς νομικούς κανόνες και έθιμα[105].

Υπό το πλαίσιο αυτό, ο νομικός διεθνολόγος Michael N. Schmitt προχώρησε το 1999 σε μια περαιτέρω παραμετροποίηση της "Effects – Based Approach", η οποία δύναται να αποτελέσει μελλοντικά την βάση για την παγκόσμια ταξινόμηση των κυβερνοεπιθέσεων ως ένοπλες επιθέσεις. Ωστόσο, μέχρι σήμερα τα κράτη ερμηνεύουν τις κυβερνοεπιθέσεις με βάση τα δικά τους κριτήρια και εθνικά συμφέροντα[106]. Ο Schmitt όρισε έξι ποιοτικές μεταβλητές, τις οποίες προσπάθησε να ποσοτικοποιήσει μέσω αριθμητικής κλίμακας, ώστε ένας μελετητής των κυβερνοεπιθέσεων να μπορεί να εξάγει συμπέρασμα για το εάν οι υπό εξέταση κυβερνοεπιθέσεις συνιστούν ένοπλες επιθέσεις[107]. Οι έξι μεταβλητές του Schmitt είναι οι εξής:

α. Severity (δριμύτητα), η οποία εστιάζει στο εύρος και την ένταση της επίθεσης. Όσο μεγαλύτερη είναι η ζημία της κυβερνοεπίθεσης (πχ αριθμός θανόντων, εύρος περιοχής επίθεσης, ποσό ζημίας), τόσο πιο βάσιμος είναι ο ισχυρισμός ότι συνιστά ένοπλη επίθεση.

β. Immediacy (αμεσότητα), η οποία εστιάζει στην διάρκεια της κυβερνοεπίθεσης και στο χρονικό διάστημα που τα αποτελέσματα της επενέργησαν στο θύμα. Όσο μεγαλύτερη είναι η διάρκεια της επίθεσης και η επενέργεια τους, τόσο πιο βάσιμος είναι ο ισχυρισμός ότι συνιστά ένοπλη επίθεση.

γ. Directness (ευθύτητα), η οποία εστιάζει στην διασύνδεση της κυβερνοεπίθεσης με το αποτέλεσμα. Όταν η ζημία που προκαλείται έχει ως άμεσο και μοναδικό αίτιο την κυβερνοεπίθεση, τότε η τελευταία εκλαμβάνεται ως ένοπλη επίθεση. Ο ισχυρισμός αυτός γίνεται λιγότερο βάσιμος, εφόσον η ζημία είναι αποτέλεσμα και άλλων παραγόντων πέραν της κυβερνοεπίθεσης.

δ. Invasiveness (διεισδυτικότητα), η οποία εστιάζει στον χώρο που ξεκινά η επίθεση και σε αυτόν που καταλήγει. Με άλλα λόγια, εξετάζει αν παραβιάζονται τα «ηλεκτρονικά σύνορα» του θύματος. Εφόσον ισχύει αυτό, η κυβερνοεπίθεση συνιστά ένοπλη επίθεση.

ε. Measurability (μετρησιμότητα), η οποία προσπαθεί να μετρήσει ποσοτικά το μέγεθος της ζημίας από την κυβερνοεπίθεση. Όσο περισσότερο μπορεί να μετρηθεί ποσοτικά το αποτέλεσμα της κυβερνοεπίθεσης, τόσο περισσότερο η κυβερνοεπίθεση συνιστά ένοπλη επίθεση.

στ. Presumptive Legitimacy (τεκμαρτή νομιμότητα), η οποία εστιάζει στην κρατική πρακτική και στην διεθνώς αποδεκτή κρατική συμπεριφορά, σύμφωνα με το

[105] Ibid, p. 60
[106] Ibid
[107] Schmitt, Michael N. (June 1999), *"Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework"*, Columbia Journal of Transnational Law, vol. 37, pp. 885-937

διεθνές δίκαιο. Όσο πιο απόμακρη από την διεθνή νομιμότητα είναι μια κυβερνοεπίθεση, τόσο περισσότερο προσεγγίζει την παράνομη χρήση βίας και την ένοπλη επίθεση.

2.3 Τα είδη των Κυβερνοσυγκρούσεων

Οι κυβερνοσυγκρούσεις διαχωρίζονται σε 5 βασικές κατηγορίες με βάση τους δράστες, τον σκοπό των κυβερνοεπιθέσεων και το είδος της ζημίας που μπορούν να προκαλέσουν. Αυτές είναι ο Βανδαλισμός στον κυβερνοχώρο, το Κυβερνοέγκλημα, η Κυβερνοκατασκοπεία, η Κυβερνοτρομοκρατία και ο Κυβερνοπόλεμος. Πολλοί μελετητές των κυβερνοσυγκρούσεων θεωρούν ότι οι πλέον συχνές κυβερνοσυγκρούσεις είναι ο Κυβερνοκατασκοπεία και το Κυβερνοέγκλημα[108]. Θα πρέπει επίσης να σημειωθεί ότι κατά γενική ομολογία, οι διαχωριστικές γραμμές μεταξύ των κυβερνοσυγκρούσεων είναι δυσδιάκριτες, καθώς δεν είναι πάντα εμφανή τα κίνητρα και οι δράστες των επιθέσεων[109]. Χαρακτηριστικά αναφέρεται ότι ακόμα υπάρχει συζήτηση στην διεθνή κοινότητα για το αν οι κυβερνοεπιθέσεις που έλαβαν χώρα στην Εσθονία το 2007 συνιστούν κυβερνοπόλεμο από την Ρωσία ή πολιτική διαμαρτυρία ορισμένων hackers (Hactivism)[110]. Αναλυτικότερα, οι μορφές των κυβερνοσυγκρούσεων είναι οι παρακάτω[111]:

α. Βανδαλισμός στο κυβερνοχώρο (Cyber Vandalism) ή "Hactivism"

Η έννοια Hactivism προκύπτει από την ένωση των εννοιών Hacking – δηλ. η δραστηριότητα ενός hacker – και ακτιβισμός – δηλ. η δραστηριότητα με βάση κάποιον πολιτικό σκοπό. Σε αυτήν την κατηγορία λαμβάνει χώρα τροποποίηση ή καταστροφή περιεχομένου στον κυβερνοχώρο, π.χ αλλαγές στο περιεχόμενο μιας ιστοσελίδας χωρίς έγκριση (π.χ Web Defacement), ή απενεργοποίηση ενός server από υπερφόρτωση δεδομένων (data overload). Γενικά, ο βανδαλισμός στον κυβερνοχώρο

---

[108] Lewis, James A, Langevin, James R, McCaul, Michael T, Charney Scott & Lt General (USAF, ret.) Raduege Harry, "*Cyber Security Two Years Later*", A Report of the CSIS Commission on Cyber Security for the 44th Presidency, January 2011, p. 7. Available at: http://csis.org/publication/cybersecurity-two-years-later, accessed on April 2011

[109] Masters, Jonathan, *"Confronting the Cyber Threat",* CFR, 23 May 2011. Available at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577, accessed on 3/1/2012

[110] Το πρόβλημα αυτό δεν αφορά μόνο στην περίπτωση της Εσθονίας, αλλά είναι γενικό και προκύπτει καθώς δεν υφίσταται μια διεθνώς αποδεκτή νομική ορολογία που να διευκρινίζει την αντιστοιχία συγκεκριμένης κυβερνοεπίθεσης με συγκεκριμένη κυβερνοσύγκρουση. Ως αποτέλεσμα, κάθε κράτος δύναται να ερμηνεύει μια κυβερνοεπίθεση διαφορετικά. Το πρόβλημα είναι σημαντικό, καθώς από την ερμηνεία που θα δοθεί (από το κάθε κράτος) θα προκύψει και ο ενδεδειγμένος τρόπος αντίδρασης.

[111] Dunn Cavelty, Myriam, "*Cyberwar: Concept, Status Quo and Limitations*", CSS Analysis in Security Policy, No 71, April 2010. Available at: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=114442, accessed on Feb 2011

είναι αρκετά συνηθισμένος και σχετικά ακίνδυνος ως πρακτική. Τα αποτελέσματα του είναι περιορισμένα σε χρόνο. Οι πιο συνηθισμένες μορφές του είναι οι εικονικές καταλήψεις (Virtual Sit – Ins), οι βομβαρδισμοί με ηλεκτρονικά μηνύματα (Email Bombings), το hacking σε ιστοσελίδες (Web hacking) και η χρήση ιών (Viruses) και σκουληκιών (Worms)[112] κατά δικτύων Η/Υ.

Τα Virtual Sit – Ins έχουν σαν αποτέλεσμα τον αποκλεισμό των ιστοσελίδων – στόχων από το ευρύ κοινό, όταν αυτές δέχονται εσκεμμένα μεγάλο αριθμό επαναλαμβανόμενων επισκέψεων. Ο συγχρονισμός των επιτιθέμενων γίνεται με την χρήση ειδικών εφαρμογών, οι οποίες μπορεί να είναι ελεύθερα διαθέσιμες στο διαδίκτυο. Τα Email Bombings είναι ουσιαστικά επαναλαμβανόμενα emails προς έναν στόχο με σκοπό τον κορεσμό του τελευταίου και την μη δυνατότητα λήψης της κανονικής αλληλογραφίας. Το web hacking αφορά σε παράνομη είσοδο σε ιστοσελίδες και την αλλαγή του περιεχομένου τους ή σε παράνομη ανακατεύθυνση της κυκλοφορίας στον κυβερνοχώρο (π.χ ενώ έχει επιλεγεί μια ιστοσελίδα, τελικά προκύπτει άλλη στην θέση της). Τέλος, η χρήση των Viruses και των Worms έχει αναλυθεί νωρίτερα.

Χαρακτηριστική περίπτωση Hactivism διαδραματίστηκε το 1999 κατά την διάρκεια του πολέμου στο Κόσοβο[113]. Την περίοδο εκείνη δραστηριοποιήθηκε η φιλοσερβική ομάδα hackers με την ονομασία “Black Hands”, η οποία εκτέλεσε μια σειρά κυβερνοεπιθέσεων κατά των υποδομών του NATO. Στόχος τους ήταν η διατάραξη των νατοϊκών στρατιωτικών επιχειρήσεων. Όπως έγινε γνωστό, οι “Black Hands” εξαπέλυσαν επιθέσεις DDoS και απέστειλαν emails με ιούς κατά νατοϊκών, αμερικανικών και βρετανικών δικτύων Η/Υ. Η ιστοσελίδα του Λευκού Οίκου τροποποιήθηκε παράνομα, ενώ το Ηνωμένο Βασίλειο ανέφερε απώλεια δεδομένων. Επιπλέον, η ιστοσελίδα του NATO για τις πολεμικές επιχειρήσεις τέθηκε εκτός ενεργείας για μεγάλο χρονικό διάστημα.

Την πιο πρόσφατη περίπτωση διαδικτυακού βανδαλισμού αποτελεί η ομάδα “Anonymous”, τα μέλη της οποίας αντιπαθούν τον χαρακτηρισμό τους ως Hackers, ενώ θεωρούν πως ο καταλληλότερος χαρακτηρισμός για αυτά είναι “παράγοντες διαδικτυακής αφύπνισης”[114]. Οι Anonymous, οι οποίοι από το 2008 συνηθίζουν να εμφανίζονται στο διαδίκτυο με το χαρακτηριστικό προσωπείο (μουστάκι και λεπτό κάθετο γένι) που χρησιμοποιήθηκε στην ταινία “V for Vendetta” (2005), συμμετέχουν σε

---

[112] Denning, Dorothy E., *“Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”*, pp.15-24. Available at: http://www.iwar.org.uk/cyberterror/resources/denning.htm, accessed on May 2011

[113] Geers, Kenneth, “*Cyberspace and the Changing Nature of Warfare*”(keynote speech), p. 5. Available at: http://www.carlisle.army.mil, accessed on Feb 2011

[114] Λυγερού, Νεφέλη, *“Anonymous: Οι πολιτικοί ακτιβιστές του Διαδικτύου”*, σελ. 102-103, εβδομαδιαίο περιοδικό Επίκαιρα, 123ο τεύχος, 23/02-29/02/12

όλες σχεδόν τις μεγάλες κοινωνικές διαδηλώσεις των ημερών μας. Έχουν εξαπολύσει κυβερνοεπιθέσεις κατά της Scotland Yard, του FBI, της εταιρείας Sony Playstation, των κυβερνητικών ιστοσελίδων των ΗΠΑ, της Ελλάδας, του Ιράν, της Τυνησίας καθώς και άλλων χωρών[115]. Δεν διαθέτουν κάποια συγκεκριμένη δομή. Είναι άτομα που μοιράζονται κοινές ανησυχίες και προβληματισμούς, ενώ προχωρούν σε επιθέσεις στον κυβερνοχώρο βασιζόμενοι στις ιδέες τους. Αν και έχουν επιτεθεί κατά πιστωτικών οργανισμών όπως η Visa, η Mastercard και η Paypal - στο πλαίσιο υποστήριξης των "WikiLeaks" - διαβεβαιώνουν την κοινή γνώμη ότι δεν έχουν σχέση με το κυβερνοέγκλημα και την απόκτηση προσωπικού κέρδους από αυτήν την δραστηριότητα. Σε κάθε δραστηριότητα τους που αφορά σε Web Defacement συνηθίζουν να αφήνουν το παρακάτω μήνυμα προς τους κυβερνώντες: «Οι λαοί δεν πρέπει να φοβούνται τις κυβερνήσεις τους. Οι κυβερνήσεις πρέπει να φοβούνται τους λαούς. Είμαστε οι Anonymous. Είμαστε λεγεώνα. Δεν συγχωρούμε. Δεν ξεχνάμε. Να μας περιμένετε».

β. Κυβερνοέγκλημα (Cyber Crime)

Το κυβερνοέγκλημα αφορά σε διεξαγωγή κυβερνοεπιθέσεων κατά ιδιωτών ή ιδιωτικών οργανισμών (π.χ επιχειρήσεις) με σκοπό το οικονομικό όφελος για τον δράστη[116]. Σύμφωνα με έκθεση της IT εταιρείας Norton για το έτος 2010, τα 2/3 του παγκόσμιου πληθυσμού έχουν πέσει θύμα του κυβερνοεγκλήματος[117]. Το κυβερνοέγκλημα δύναται να λάβει διαφορετικές μορφές. Σε πρόσφατη έκθεση του το Chatham House[118] διαχωρίζει το κυβερνοέγκλημα σε χαμηλού επιπέδου ή σε σοβαρό και οργανωμένο κυβερνοέγκλημα. Στην πρώτη περίπτωση υπάγονται οι hackers που προσπαθούν με την παράνομη δραστηριότητα τους να κερδίσουν τον σεβασμό των υπολοίπων, να γίνουν διάσημοι για κάποια ενέργεια τους (π.χ παραβίαση ενός δικτύου Η/Υ μεγάλης επιχείρησης) ή να αποκομίσουν χρηματικό όφελος (συνήθως όχι μεγάλο). Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση του Βρετανού Gary McKinnon, ο οποίος συνελήφθηκε το 2002, καθώς είχε «εισβάλλει» σε Η/Υ του αμερικανικού Πενταγώνου, ψάχνοντας για αποδείξεις ύπαρξης εξωγήινης ζωής[119].

---

[115] Ibid

[116] Michael, Alex, "*Cyber Probing: The Politicisation of Virtual Attack*", Defence Academy of the United Kingdom, p.1. Available at: http://www.conflictstudies.org.uk/files/Cyber_Probing.pdf, accessed on Jan 2011

[117] Masters, Jonathan, *"Confronting the Cyber Threat",* CFR, 23 May 2011. Available at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577, accessed on 3/1/2012

[118] Cornish, Paul, Hughes, Rex & Livingstone, David, "*Cyberspace and the National Security of the United Kingdom: Threats and Responses*" (Chatham House, London, 2009), pp.7-11. Available at: http://www.chathamhouse.org, accessed on Dec 2010

[119] Glenny, Misha, "*Who Controls the Internet*". Available at: http://www.ft.com/intl/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html, accessed on 11/10/10

Στην δεύτερη περίπτωση υπάγονται κυρίως τα δίκτυα οργανωμένου εγκλήματος (οικονομικής φύσης), τα οποία χρησιμοποιούν τον κυβερνοχώρο για να επιτύχουν τις επιδιώξεις τους και να κερδοφορήσουν. Τα δίκτυα αυτά συνήθως στοχεύουν είτε στην υπεξαίρεση σημαντικών οικονομικών δεδομένων από επιχειρήσεις (π.χ στοιχεία πιστωτικών καρτών), τα οποία στην συνέχεια θα μεταπωλήσουν ή στην κλοπή πνευματικής ιδιοκτησίας. Σύμφωνα με εκτιμήσεις, το κόστος της δραστηριότητας τους ξεπερνά το 1 τρισεκατομμύριο δολάρια το χρόνο. Χαρακτηριστικά αναφέρεται ότι το 2007 και μόνο για το Ην. Βασίλειο διαπιστώθηκαν 255.800 υποθέσεις οικονομικής κυβερνοαπάτης, που αντιστοιχούσαν σε απώλειες 535 εκατομμυρίων λιρών[120].

Τέλος θα πρέπει να επισημανθεί ότι το κυβερνοέγκλημα θεωρείται κατά πολλούς ως το εργαστήριο όπου αναπτύσσονται, ελέγχονται και τελειοποιούνται τα κακόβουλα λογισμικά που θα χρησιμοποιηθούν στον κυβερνοπόλεμο[121].

γ. Κυβερνοκατασκοπεία (Cyber Espionage)

Περιλαμβάνει τις επιχειρήσεις στον κυβερνοχώρο που έχουν ως στόχο την συλλογή πληροφοριών σχετικά με άλλα κράτη, κυβερνήσεις ή βιομηχανίες του ιδιωτικού τομέα[122]. Η κυβερνοκατασκοπεία αποτελεί την πλέον επικρατούσα δραστηριότητα στον κυβερνοχώρο. Είναι κάτι που το κάνουν όλοι[123]. Έχει ως στόχο την άντληση δεδομένων υψηλής διαβάθμισης, τα οποία θα προσδώσουν στον κάτοχο τους συγκριτικό πλεονέκτημα σε σχέση με τους αντιπάλους του. Ιδιαίτερα, τα δεδομένα που αφορούν στις βιομηχανίες πιθανώς να ελαχιστοποιήσουν το κόστος έρευνας και ανάπτυξης ενός προγράμματος που σκοπεύει να αναπτύξει ο φορέας που διενεργεί τις επιχειρήσεις κυβερνοκατασκοπείας.

Η Κίνα θεωρείται ως η χώρα που κατέχει την πρώτη θέση παγκοσμίως στην διεξαγωγή τέτοιου είδους επιχειρήσεων[124]. Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση με την κωδική ονομασία "TITAN RAIN"[125] (2007), η οποία αφορά σε συνεχιζόμενες ενέργειες κυβερνοκατασκοπείας της Κίνας κατά του αμερικανικού Υπουργείου Άμυνας (ΥΠΑΜ) από το 2002. Όπως έχει γνωστοποιηθεί, η Κίνα κατάφερε

[120] Cornish, Paul, Hughes, Rex & Livingstone, David, "Cyberspace and the…", p.7
[121] Carr, Jeffrey, *Inside Cyber Warfare* (O'Reilly Media Inc., Sebastopol, 2010), p. 5
[122] Michael, Alex, "*Cyber Probing: The Politicisation of Virtual Attack*", p.1. Ιδιαίτερα, η συλλογή πληροφοριών αναφορικά με τις βιομηχανίες άλλων χωρών (industrial espionage) εντάσσεται στο πλαίσιο της οικονομικής κατασκοπείας. Για περισσότερα βλέπε Κωνσταντόπουλος, Ιωάννης, *Οικονομία και Κατασκοπεία: Θεωρία και Πράξη* (Εκδόσεις Ποιότητα, Βάρη Αττικής, 2010), σελ. 53 – 56.
[123] Libicki, 2009:26
[124] Υπάρχουν ενδείξεις και όχι αποδείξεις που να καταδεικνύουν ότι η Κίνα εμπλέκεται σε υποθέσεις κυβερνοκατασκοπείας.
[125] Carr, 2010: 4. Βλέπε επίσης, Cornish, Paul, Livingstone, David, Clemente, David & Yorke, Claire, "*On Cyber Warfare*" (Chatham House, London, 2010), pp. 8-9. Available at: http://www.chathamhouse.org, accessed on Dec 2010

να αποσπάσει δεδομένα της τάξης των 10 – 20 terabytes από το αδιαβάθμητο εσωτερικό δίκτυο (intranet) του αμερικανικού ΥΠΑΜ, γνωστό ως NIPRNET, το οποίο διασυνδέεται σε ορισμένα σημεία με το Internet.

Επίσης, τον Σεπτέμβριο του 2007 κατά την επίσημη επίσκεψη της στην Κίνα, η Γερμανίδα Καγκελάριος Μέρκελ δεν δίστασε να κατηγορήσει την Κίνα για διεξαγωγή επιχειρήσεων κυβερνοκατασκοπείας κατά της χώρας της. Όπως αναφέρθηκε από τα ΜΜΕ, οι κυβερνοεπιθέσεις έλαβαν χώρα κατά της γερμανικής καγκελαρίας, του ΥΠΕΞ, του Υπουργείου Οικονομικών (ΥΠΟΙΚ) και του Υπουργείου Ερευνών, με αποτέλεσμα την απώλεια μεγάλου όγκου δεδομένων (υπολογίζονται σε terabytes). Το μόνο που κατέφεραν οι Γερμανοί αξιωματούχοι ασφαλείας ήταν να ματαιώσουν την μεταφορά 160 gigabytes δεδομένων[126].

Μια ακόμα γνωστή υπόθεση κυβερνοκατασκοπείας από την Κίνα, είναι η περίπτωση “GhostNet”. Τον Μάρτιο του 2009 μια ομάδα ασφαλείας ανακάλυψε την ύπαρξη ενός κακόβουλου λογισμικού[127] σε παραπάνω από 1295 Η/Υ, σε 103 διαφορετικές χώρες του κόσμου. Οι στόχοι αφορούσαν σε πρεσβείες της Γερμανίας, της Ινδίας, της Ταϊλάνδης, του Ιράν, της Λετονίας και του Θιβέτ. Κατόπιν έρευνας διαπιστώθηκε ότι οι θύτες της επιχείρησης είχαν αποστείλει ηλεκτρονικά μηνύματα με κακόβουλο λογισμικό στα θύματα τους, στα οποία εμφανίζονταν ως «γνώριμοι» των θυμάτων τους. Με την εγκατάσταση του malware στους Η/Υ των θυμάτων τους[128], οι θύτες είχαν την δυνατότητα να υπεξαιρέσουν αρχεία και κωδικούς[129]. Επίσης, το πρόγραμμα GhostNet είχε την δυνατότητα να ενεργοποιεί τις κάμερες και τα μικρόφωνα των Η/Υ που είχε εγκατασταθεί - χωρίς να το γνωρίζουν οι χρήστες τους - και στην συνέχεια να μεταφέρει τις καταγραφές σε servers που βρίσκονταν στην Κίνα[130].

Παράλληλα, την ίδια χρονιά (2009) γνωστοποιήθηκε μια υπόθεση κυβερνοκατασκοπείας, η οποία αφορούσε στο μαχητικό αεροσκάφος (Α/Φ) 5ης γενιάς των ΗΠΑ F-35 Lightning II, το πρόγραμμα ανάπτυξης του οποίου φθάνει τα 300 δις δολ. Σύμφωνα με τα στοιχεία που διέρρευσαν, μια ομάδα hackers, που πιθανολογείται ότι ήταν Κινέζοι, εισέβαλλε στα δίκτυα Η/Υ των 3 κύριων αμυντικών βιομηχανιών που είναι υπεύθυνες για το πρόγραμμα (Lockheed Martin, Northrop Grumman και BAE Systems) και υπεξαίρεσαν στοιχεία που αφορούσαν στην διαχείριση των

[126] Libicki, 2009:25. Βλέπε επίσης, (2007) “*China’s cyber attacks*”, Strategic Comments, Vol. 13, Issue 7, pp. 1-2, accessed on 19-5-11
[127] Θα πρέπει να σημειωθεί ότι το συγκεκριμένο λογισμικό ήταν διαθέσιμο στο Internet.
[128] Ο χρήστης – θύμα του Η/Υ που θα επέλεγε να δει το συγκεκριμένο ηλεκτρονικό μήνυμα, αυτόματα ενεργοποιούσε μια αυτόματη διαδικασία, αποτέλεσμα της οποίας ήταν η εγκατάσταση του malware στον Η/Υ του. Η εν λόγω διαδικασία δεν ήταν εμφανής στον χρήστη του Η/Υ.
[129] Michael, Alex, “*Cyber Probing: The Politicisation of Virtual Attack*”, p.3.
[130] Clarke & Knake, 2010: 59

δυσλειτουργιών κατά την διάρκεια πτήσης του Α/Φ[131]. Όπως ήταν αναμενόμενο, η Κίνα αρνήθηκε οποιαδήποτε εμπλοκή της με το θέμα.

δ. Κυβερνοτρομοκρατία (Cyber Terrorism)

Με τον όρο αυτό Κυβερνοτρομοκρατία ή Ηλεκτρονική Τρομοκρατία[132] περιγράφονται όλες οι παράνομες επιθέσεις στον κυβερνοχώρο από μη κρατικούς δρώντες κατά Η/Υ, δικτύων Η/Υ αλλά και των πληροφοριών που περιέχονται σε αυτά, με σκοπό τον εκφοβισμό μιας κυβέρνησης ή του πληθυσμού μιας χώρας ή τον εξαναγκασμό τους σε αλλαγή συμπεριφοράς[133]. Μια κυβερνοεπίθεση συνιστά κυβερνοτρομοκρατία όταν εξασκεί φυσική βία κατά ατόμων ή περιουσιών, ή όταν προκαλεί τέτοια ζημία που προξενεί τον τρόμο[134]. Η κυβερνοτρομοκρατία περιλαμβάνει προμελετημένες και πολιτικά υποκινούμενες κυβερνοεπιθέσεις, ενώ πιθανοί της στόχοι είναι τα κυβερνητικά δίκτυα Η/Υ, τα οικονομικά δίκτυα, τα εργοστάσια παραγωγής ενέργειας, τα πληροφοριακά δίκτυα ελέγχου της εναέριας κυκλοφορίας κ.α[135].

Οι κυβερνοτρομοκράτες (Cyber Terrorists) μπορεί να είναι ιδεολογικά φανατισμένοι τρομοκράτες με ικανότητες στο hacking ή να είναι εντολοδόχοι hackers (γνωστοί και ως freelancers) των οποίων οι υπηρεσίες έχουν εξαγοραστεί από κάποια τρομοκρατική οργάνωση[136]. Συνήθως, διαθέτουν σημαντικά οικονομικά κεφάλαια για την διενέργεια των χτυπημάτων τους, ενώ πέρα από την διενέργεια των τρομοκρατικών χτυπημάτων, χρησιμοποιούν την τεχνολογία Η/Υ και το διαδίκτυο για σχεδιασμό επιχειρήσεων, συλλογή κεφαλαίων, διάδοση προπαγάνδας, ανταλλαγή απόψεων και στρατολόγηση[137].

Μέχρι σήμερα δεν έχει υπάρξει κάποια ιδιαίτερα σοβαρή ενέργεια κυβερνοτρομοκρατών σε βαθμό που να προκαλέσει μια πολιτική αλλαγή[138]. Σύμφωνα με ορισμένους αναλυτές του φαινομένου, οι κυβερνοεπιθέσεις που αφορούν στην κυβερνοτρομοκρατία έχουν μικρότερο αντίκτυπο στην κοινωνία σε σχέση με αυτόν ενός

[131] Dreazen, Yochi, Cole, August & Gorman, Siobhan, "*Computer Spies Breach Fighter-Jet Project*", The Wall Street Journal (WSJ.com). Available at: http://online.wsj.com/article/SB124027491029837401.html, accessed on Oct 2010.
[132] Μπόση, Μαίρη, *Περί Ορισμού της Τρομοκρατίας* (Εκδόσεις Π. Τραυλός, Αθήνα, 2000), σελ. 64
[133] Clarke & Knake, 2010: 59
[134] Ibid, p. 2
[135] Curran, Kevin, Concannon, Kevin & McKeever, Sean, *Cyber Terrorism Attacks*, pp.1-3, στο συλλογικό έργο Janczewski, Lech J., & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)
[136] Warren, M.J., *Terrorism and the Internet*, p. 2, στο συλλογικό έργο Janczewski, Lech J., & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)
[137] Curran, Kevin et al, *Cyber Terrorism Attacks*, p. 2
[138] Lewis, James Andrew, "*The Cyber War Has Not Begun*", Center for Strategic & International Studies, March 2010. Available at: http://csis.org, accessed on November 2010

«συμβατικού» τρομοκρατικού χτυπήματος[139]. Θα πρέπει όμως να σημειωθεί ότι, τα αποτελέσματα μιας ενέργειας κυβερνοτρομοκρατίας δύναται να αφορούν σε περισσότερους αποδέκτες σε σχέση με ένα «συμβατικό» τρομοκρατικό χτύπημα, ενώ ανάλογα του είδους της κυβερνοεπίθεσης αλλά και του στόχου αυτής είναι δυνατή η πρόκληση σημαντικών υλικών ζημιών[140]. Συνεπώς, η Κυβερνοτρομοκρατία ως μορφή βίας μπορεί να είναι πιο επικίνδυνη υπό προϋποθέσεις. Όπως μάλιστα υποστηρίζεται, η πιο αποτελεσματική χρήση της κυβερνοτρομοκρατίας θα επιτευχθεί σε συνδυασμό με μια «συμβατική» τρομοκρατική ενέργεια, π.χ πρόκληση δυσλειτουργίας (μέσω hacking) στις υπηρεσίες αντιμετώπισης εκτάκτων αναγκών, την στιγμή που μια έκτακτη ανάγκη έχει προκύψει από ένα «συμβατικό» τρομοκρατικό χτύπημα[141].

Το πρώτο παράδειγμα κυβερνοεπίθεσης από τρομοκράτες αφορά στους εξτρεμιστές Ταμίλ, οι οποίοι το 1998 επιτέθηκαν μέσω του διαδικτύου στις πρεσβείες της Σρι Λάνκα. Η κυβερνοεπίθεση έγινε μέσω αποστολής 800 email σε καθημερινή βάση, για χρονικό διάστημα δυο εβδομάδων (email bombing), στις πρεσβείες που υπήρχαν στην χώρα. Το περιεχόμενο του email ήταν το εξής: «Είμαστε οι Black Tigers του διαδικτύου και το κάνουμε αυτό για να διακόψουμε τις επικοινωνίες σας». Οι Ταμίλ την περίοδο εκείνη μάχονταν για την ανεξαρτησία τους και ήθελαν με τις κυβερνοεπιθέσεις να προκαλέσουν φόβο στις πρεσβείες της Σρι Λάνκα[142].

Ένα ακόμα παράδειγμα χρήσης του διαδικτύου από εξτρεμιστές αφορά στους Τσετσένους αυτονομιστές, οι οποίοι μέσω της ιστοσελίδας *www.Kavkaz.org* διέδιδαν προπαγανδιστικά μηνύματα κατά της Ρωσίας, μάζευαν χρήματα για τις δραστηριότητες τους από την τσετσενική διασπορά και δημοσίευαν φωτογραφικό - κινηματογραφικό υλικό που καταδείκνυε την σκληρότητα της Ρωσίας απέναντι στους Τσετσένους. Παράλληλα αναρτούσαν υλικό στην ιστοσελίδα τους, με το οποίο εκθείαζαν τις επιτυχίες των ένοπλων Τσετσένων κατά των Ρώσων στρατιωτών[143].

Επίσης, αξίζει να σημειωθεί ότι σύμφωνα με μαρτυρία του έγκλειστου στο Γκουαντάναμο Μαυριτανού Mohamedou Ould Slahi, η Al Qaeda είχε εξαπολύσει κυβερνοεπιθέσεις (DDoS) κατά διαφόρων ιστοσελίδων αλλά και ενάντια του server του Πρωθυπουργού του Ισραήλ. Όπως είχε επισημάνει ο Slahi, ο οποίος εργαζόταν ως διαχειριστής δικτύου σε εταιρεία - πάροχο internet στην Μαυριτανία από τον Μάιο του 2000 έως τον Ιούλιο του 2001, η Al Qaeda είχε δημοσιεύσει στο διαδίκτυο οδηγίες για

---

[139] Nye, Joseph S. Jr., "*Cyber Power*", Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p. 12. Available at: http://belfercenter.org, accessed on November 2010
[140] Μπόση, 2000 : 64-65
[141] Curran, Kevin et al, *Cyber Terrorism Attacks*, p. 2
[142] Denning, Dorothy E., "*Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*", pp.18 & 24
[143] Geers, Kenneth, "*Cyberspace and the Changing Nature of Warfare*" (keynote speech), p. 4

hacking κατά συγκεκριμένων ιστοσελίδων, δηλώνοντας παράλληλα την ημερομηνία και την ώρα της επίθεσης[144].

ε. Κυβερνοπόλεμος (Cyberwar)

Με τον όρο Κυβερνοπόλεμος (Cyber War) νοείται το σύνολο των ενεργειών που λαμβάνουν χώρα από ένα κράτος προκειμένου αυτό να διεισδύσει στα δίκτυα Η/Υ μιας άλλης χώρας, με σκοπό να προκαλέσει ζημία ή αναταραχή σε αυτά[145]. Από τον ορισμό προκύπτει ότι οι αντίπαλες οντότητες θα πρέπει να είναι εξαρτημένες σε κάποιο βαθμό από τα δίκτυα Η/Υ. Οι υπόψη ενέργειες μπορεί να προέρχονται είτε από κρατικούς λειτουργούς (π.χ μυστικές υπηρεσίες, ένοπλες δυνάμεις κτλ) είτε από ανεπίσημα διορισμένους ή υποστηριζόμενους από τα κράτη μη κρατικούς δρώντες (Non State Actors). Σε σχέση με τις προαναφερόμενες κυβερνοσυγκρούσεις θεωρείται η πιο ακραία μορφή σύγκρουσης[146]. Θα πρέπει επίσης να επισημανθεί ότι, δεν είναι λίγοι αυτοί που πιστεύουν πως η έννοια του κυβερνοπολέμου είναι αδόκιμη, καθώς η έννοια του πολέμου σχετίζεται με την βία, την καταστροφή και τον πόνο, στοιχεία τα οποία δύσκολα προκύπτουν από τις κυβερνοεπιθέσεις[147]. Υποστηρίζεται επιπλέον ότι, οι κυβερνοεπιθέσεις αποτελούν μια άλλη προσέγγιση στην υπονόμευση, το σαμποτάζ και την κατασκοπεία σε βάρος του αντιπάλου[148].

Σε αντίθεση με τον συμβατικό πόλεμο όπου το προνόμιο της χρήσης βίας ανήκει κατά αποκλειστικότητα στα κράτη, στον κυβερνοπόλεμο οι μη κρατικοί δρώντες διεκδικούν σημαντικό μερίδιο, καθώς το κόστος εισόδου στον κυβερνοχώρο είναι χαμηλό, ενώ η απόκτηση κυβερνοόπλων έχει σχεδόν μηδενικό κόστος[149]. Επίσης, στις ιδιαιτερότητες του κυβερνοπολέμου ανήκουν η μη δυνατότητα κατάληψης εδάφους, η περιορισμένη δυνατότητα για ολική καταστροφή ή αφοπλισμό του αντιπάλου και η εύνοια υπέρ του επιτιθέμενου, καθώς το διαδίκτυο σχεδιάστηκε χωρίς να δοθεί βαρύτητα στην έννοια της ασφάλειας[150]. Παράλληλα, θα πρέπει να επισημανθεί ότι σε αντίθεση με μια συμβατική σύγκρουση, η ταυτότητα των εμπλεκομένων δύναται να παραμείνει κρυφή στον κυβερνοπόλεμο, ενώ η έννοια της

---

[144] Kingsbury, Alex, "*Documents Reveal Al Qaeda Cyberattacks*". Available at: http://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks, accessed on May 2011

[145] Clarke & Knake, 2010 : 6

[146] Nye, Joseph S. Jr., "*Cyber Power*", p. 5

[147] Dunn Cavelty, Myriam, "*As likely as a visit from E.T*", THE EUROPEAN magazine. Available at: http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear, accessed on 7-1-2011.

[148] Pepera, David, "*'Cyber war? Not!' says U.K. professor*". Available at: http://www.fiercehomelandsecurity.com/story/cyber-war-not-says-uk-professor/2011-10-11, accessed on Oct. 2011

[149] Nye, Joseph S. Jr., "*Cyber Power*", p. 5.

[150] Ibid

απόστασης δεν υφίσταται πρακτικά, καθώς η μεταφορά ψηφιακών δεδομένων γίνεται σε σχεδόν μηδενικό χρόνο[151].

Ο Κυβερνοπόλεμος αποτελεί τμήμα του Πληροφοριακού Πολέμου (Information Warfare)[152]. Σύμφωνα με το διακλαδικό στρατιωτικό εγχειρίδιο των ΗΠΑ JP 3-13, οι στρατιωτικές επιχειρήσεις στον κυβερνοχώρο αποτελούν τμήμα των πληροφοριακών επιχειρήσεων (IO : Information Operations). Οι τελευταίες ορίζονται ως η ολοκληρωμένη εφαρμογή του Ηλεκτρονικού Πολέμου (EW : Electronic Warfare), των επιχειρήσεων στα δίκτυα Η/Υ (Computer Network Operations), των Ψυχολογικών Επιχειρήσεων (PSYOPS : Psychological Operations), της στρατιωτικής Παραπλάνησης (Military Deception) και της Ασφάλειας των Επιχειρήσεων (Operations Security), σε συνδυασμό με άλλες δυνατότητες υποστήριξης, με σκοπό την επιρροή, διαταραχή, διαφθορά ή τον σφετερισμό της διαδικασίας λήψης αποφάσεων του αντιπάλου, με παράλληλη προστασία στην δική μας διαδικασία λήψης αποφάσεων[153].

Οι επιχειρήσεις στον κυβερνοχώρο (Cyber Warfare) εστιάζουν στην χρήση της υπόψη περιοχής για την επίθεση κατά του προσωπικού, των εγκαταστάσεων ή του εξοπλισμού του αντιπάλου με σκοπό την υποβάθμιση, την αδρανοποίηση ή την καταστροφή της εχθρικής μαχητικής ικανότητας, με ταυτόχρονη προστασία της δικής μας μαχητικής ικανότητας. Αντικειμενικός σκοπός των ανωτέρω επιχειρήσεων είναι ο αντίπαλος να μην μπορεί να έχει ελευθερία κινήσεων στον κυβερνοχώρο[154]. Οι υπόψη επιχειρήσεις – γνωστές και ως CNO (Computer Network Operations) – λαμβάνουν τρεις κύριες μορφές[155]:

(i) Επίθεση σε δίκτυα Η/Υ ή CNA (Computer Network Attack)

Περιλαμβάνει τις επιχειρήσεις που έχουν ως σκοπό την διαταραχή, την άρνηση, την υποβάθμιση ή την καταστροφή των πληροφοριών που βρίσκονται μέσα σε Η/Υ ή δίκτυα Η/Υ ή ακόμα και την καταστροφή των Η/Υ και των δικτύων Η/Υ.

(ii) Εκμετάλλευση των δικτύων Η/Υ ή CNE (Computer Network Exploitation)

---

[151] Ibid
[152] Dunn Cavelty, Myriam, "*Cyberwar: Concept, Status Quo and Limitations*", CSS Analysis in Security Policy, No 71, April 2010.
[153] Joint Publication 3-13, *Information Operations*, 13-2-06. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf#search="JP 3-13", accessed on May 2011
[154] Alexander, Keith B., "*Warfighting in Cyberspace*", Joint Force Quarterly, issue 46, 3d quarter 2007, p. 60. Available at: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, accessed on May 2011
[155] Joint Publication 3-13, *Information Operations*, 13-2-06

Περιλαμβάνει τις επιχειρήσεις συλλογής πληροφοριών για τον αντίπαλο μέσα από τα δίκτυα Η/Υ (δηλ. Cyber Espionage).

(iii) Άμυνα στα δίκτυα Η/Υ ή CND (Computer Network Defence)

Αφορά στις επιχειρήσεις δια μέσω των δικτύων Η/Υ που στοχεύουν στην προστασία, την επίβλεψη, την ανάλυση, τον εντοπισμό και την αντιμετώπιση κάθε μη εξουσιοδοτημένης δραστηριότητας που λαμβάνει χώρα στα συστήματα και τα δίκτυα Η/Υ.

2.4 Γιατί τα κράτη επιδιώκουν τις Επιχειρήσεις στα Δίκτυα Η/Υ (CNOs)?

Γενικά, θα μπορούσε να ειπωθεί ότι τα κράτη ή οι «άτυπα εξουσιοδοτημένοι» από αυτά μη κρατικοί δρώντες μπορούν μέσω των CNOs να αποκομίσουν σημαντικά οφέλη με μικρό κόστος. Οι κύριοι λόγοι επιλογής των CNOs είναι οικονομικοί και στρατιωτικοί. Όπως έχει αναφερθεί, το σύνολο των οικονομικών και εμπορικών συναλλαγών σε παγκόσμιο επίπεδο εξαρτάται από τα δίκτυα Η/Υ, ενώ οι παραπάνω διαδικασίες δεν προστατεύονται επαρκώς από τις υπάρχουσες νομοθεσίες[156], γεγονός που τις κάνει ευάλωτες σε CNAs. Επιπλέον, είναι κοινά αποδεκτό ότι το σύνολο της πνευματικής ιδιοκτησίας, το οποίο αγγίζει αστρονομικά ποσά φυλάσσεται μέσα σε δίκτυα Η/Υ[157]. Από την άλλη μεριά, η αποτελεσματικότητα των σύγχρονων Ένοπλων Δυνάμεων (ΕΔ) είτε αυτή μεταφράζεται σε σύγχρονα οπλικά συστήματα είτε σε συστήματα διοίκησης και ελέγχου είναι εξολοκλήρου εξαρτώμενη από την τεχνολογία των Η/Υ. Επιπρόσθετα, μέσω των CNOs υπάρχει ένα σαφές παράθυρο ευκαιρίας για τα κράτη προκειμένου να επιτύχουν στρατηγικούς σκοπούς, διατηρώντας παράλληλα το στοιχείο της έκπληξης και της ανωνυμίας. Υπενθυμίζεται ότι λόγω της χαοτικής αρχιτεκτονικής του κυβερνοχώρου, οι κυβερνοεπιθέσεις μπορούν να γίνονται χωρίς να υπάρχουν σαφή ίχνη που να παραπέμπουν στους δράστες, ενώ στην περίπτωση που κάποιοι μη κυβερνητικοί δρώντες έχουν εξουσιοδοτηθεί άτυπα να εκτελούν κυβερνοεπιθέσεις εκ μέρους των κρατών, τότε τα κράτη διατηρούν το πρόσχημα της εύλογης άρνησης (plausible deniability), αναφορικά με την εμπλοκή τους σε αυτές τις επιθέσεις.

Θα πρέπει επίσης να αναφερθεί ότι τα κράτη και ιδιαίτερα οι ΕΔ τους επιδιώκουν να διεξάγουν CNEs προκειμένου να είναι επαρκώς προετοιμασμένα σε

[156] Billo, Charles & Chang, Welton, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Institute For Security Technology Studies At Dartmouth College, Hannover, 2004), p.19
[157] Ibid

περίπτωση μελλοντικών πολεμικών συγκρούσεων στο συμβατικό επίπεδο ή/και στον κυβερνοχώρο. Η διαδικασία αυτή, η οποία είναι γνωστή στην διεθνή βιβλιογραφία ως “preparing the battlefield”[158] αναφέρεται στην διείσδυση των hackers στα δίκτυα του αντιπάλου, προκειμένου να συλλέξουν σημαντικές πληροφορίες για τον αντίπαλο, αλλά και για «εμφυτεύσουν» στα εχθρικά συστήματα λογισμικό (logic bombs), το οποίο όταν ενεργοποιηθεί θα προκαλέσει ζημία στον αντίπαλο. Με τον τρόπο αυτό, τα κράτη διατηρούν το στοιχείο του αιφνιδιασμού αλλά και την δυνατότητα του πρώτου χτυπήματος (first strike capability) σε τόπο και χρόνο που εκείνα θα επιλέξουν.

Πέραν των ανωτέρω, τα κράτη κάνοντας χρήση των CNOs δεν αναγκάζονται να εμπλακούν σε συμβατικό πόλεμο που θα επιφέρει νομοτελειακά ανθρώπινες απώλειες, ενώ θα έχει μεγάλο οικονομικό κόστος για την διεξαγωγή του. Επίσης, το κόστος για την διεξαγωγή κυβερνοσυγκρούσεων είναι σαφώς μικρότερο από αυτό των συμβατικών συγκρούσεων, ενώ ο επιτιθέμενος μπορεί να επιφέρει ασύμμετρα σημαντικό πλήγμα στον αμυνόμενο, ιδιαίτερα όταν ο τελευταίος στηρίζεται σε μεγάλο βαθμό στα συστήματα Η/Υ. Τέλος, υπάρχει ασάφεια για το αν μια κυβερνοεπίθεση συνιστά πολεμική πράξη και επομένως ο επιτιθέμενος υπολογίζει σε περιορισμένες κυρώσεις για την πράξη του την οποία, λόγω της ανωνυμίας στον κυβερνοχώρο που προαναφέρθηκε, θα μπορούσε να αρνηθεί (plausible deniability).

2.5 Οι Στόχοι στον Κυβερνοπόλεμο

Ο κυβερνοχώρος αποτελεί στρατηγικό μέσο, καθώς μέσω αυτού μπορούν να δεχθούν κυβερνοεπιθέσεις τόσο οι στρατιωτικές (Military) όσο και οι μη στρατιωτικές (Civilian) υποδομές. Μάλιστα, θεωρείται ότι οι κυβερνοεπιθέσεις κατά των μη στρατιωτικών υποδομών είναι πιο εύκολες, καθώς δεν λαμβάνονται συχνά τα απαραίτητα μέτρα ασφαλείας, όπως συμβαίνει με τις στρατιωτικές εγκαταστάσεις[159]. Οι δυο βασικές κατηγορίες στόχων στον κυβερνοπόλεμο είναι οι ένοπλες δυνάμεις και οι κυβερνητικές/μη στρατιωτικές υποδομές.

Στην πρώτη περίπτωση επιδιώκεται η «απενεργοποίηση» των οπλικών συστημάτων και η διαταραχή του συστήματος διοίκησης και ελέγχου (C^2 systems) του αντιπάλου, ενώ στην δεύτερη περίπτωση επιδιώκεται η εξασθένηση της ικανότητας και της θέλησης του αντιπάλου να διεξάγει πόλεμο για μεγάλο χρονικό διάστημα[160]. Αυτό επιτυγχάνεται μέσω της προσβολής στόχων που αφορούν στον οικονομικό & βιομηχανικό τομέα αλλά και σε υπηρεσίες που δύναται να επηρεάσουν το ηθικό του

[158] Clarke & Knake, 2010: 197-200
[159] Libicki, 2009:3
[160] Geers, 2011: 138

ανθρώπινου δυναμικού[161] (π.χ παροχή ηλεκτρικού ρεύματος, νερού, υγειονομική περίθαλψη κ.α).

Χαρακτηριστικό παράδειγμα τέτοιου είδους στοχοποίησης αποτελεί η άσκηση πληροφοριακού πολέμου "Eligible Receiver" που διεξήγαγαν οι ΗΠΑ το καλοκαίρι του 1997. Σύμφωνα με τα στοιχεία που διέρρευσαν στα ΜΜΕ, μετά από τρίμηνη προετοιμασία, η εχθρική ομάδα (Red Team) διείσδυσε στα συστήματα Η/Υ του αμερικανικού ΥΠΑΜ, ενώ παράλληλα εκτέλεσε κυβερνοεπιθέσεις κατά του δικτύου παροχή ηλεκτρικής ενέργειας και των τηλεπικοινωνιών, με αποτέλεσμα να διακοπούν οι επιχειρήσεις σε διάφορες στρατιωτικές μονάδες και να μειωθεί η δυνατότητα των ΗΠΑ στην ανάπτυξη και διατήρηση στρατιωτικών δυνάμεων[162]. Η Red Team αριθμούσε συνολικά 35 άτομα (hackers) από την National Security Agency (NSA) των ΗΠΑ και έκανε χρήση Η/Υ και λογισμικού για hacking που πωλείται στο εμπόριο. Η επιτυχία των κυβερνοεπιθέσεων της συνίσταται στο γεγονός ότι κατάφερε να διεισδύσει και να πάρει τον έλεγχο των Η/Υ του κέντρου επιχειρήσεων της Διοίκησης του Ειρηνικού (Pacific Command), καθώς και του δικτύου παροχής ηλεκτρικής ενέργειας και των υπηρεσιών ανταπόκρισης σε έκτακτες ανάγκες σε 9 μεγάλες αμερικανικές πόλεις[163]. Επιπρόσθετα, η Red Team κατάφερε να επιφέρει τέτοια σύγχυση στο σύστημα διοίκησης και ελέγχου των ΗΠΑ, ώστε κανείς στην αλυσίδα διοίκησης να μην πιστεύει ότι αυτά που έβλεπε ή μάθαινε ανταποκρίνονταν στην πραγματικότητα[164].

2.6 Βασικές Μορφές Κυβερνοπολέμου

Ο Κυβερνοπόλεμος λαμβάνει 2 βασικές μορφές: α) τον Στρατηγικό Κυβερνοπόλεμο (Strategic Cyberwar), δηλ. τις κυβερνοεπιθέσεις που γίνονται με σκοπό να επηρεαστεί η κυβερνητική πολιτική του αντιπάλου μέσα από εξαναγκασμό[165] και β) τον Επιχειρησιακό Κυβερνοπόλεμο (Operational Cyberwar), δηλ. τις κυβερνοεπιθέσεις που λαμβάνουν χώρα προς υποστήριξη ενός συμβατικού πολέμου[166]. Θα πρέπει να σημειωθεί ότι κατά την διάρκεια διεξαγωγής και των 2 μορφών κυβερνοπολέμου – μέσω εκτέλεσης των CNAs – πραγματοποιούνται παράλληλα τα CNDs και CNEs, δηλαδή όλο το φάσμα των CNOs.

---

[161] Ibid
[162] Rattray, Gregory J., *Strategic Warfare in Cyberspace* (MIT Press, Cambridge, 2001), p. 385
[163] "*The Warnings? Cyberwar!", Frontline/PBS (published 24 April 2003). Available at:* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, accessed on April 2011
[164] Geers, 2011: 138
[165] Libicki, 2009: 6
[166] Ibid

2.6.1 Στρατηγικός Κυβερνοπόλεμος

Προκειμένου μια σύγκρουση στον κυβερνοχώρο να χαρακτηριστεί ως στρατηγικός κυβερνοπόλεμος (Strategic Cyberwar) θα πρέπει να ισχύουν τρεις βασικές προϋποθέσεις[167]: Πρώτον, δεν θα πρέπει να λαμβάνουν χώρα άλλες εχθροπραξίες μεταξύ των 2 αντιπάλων ή εφόσον υπάρχουν, θα πρέπει να θεωρούνται δευτερεύουσες σε σχέση με τον κυβερνοπόλεμο. Δεύτερον, η διενέργεια των κυβερνοεπιθέσεων θα πρέπει να γίνεται και από τις 2 εμπλεκόμενες πλευρές. Τρίτον, η προσφυγή στις κυβερνοεπιθέσεις σημαίνει ότι έχει αποτύχει η οικονομική, διπλωματική ή νομική προσπάθεια επίλυσης της αντιπαράθεσης.

Όπως προαναφέρθηκε, οι κυβερνοεπιθέσεις που εξαπολύονται από μια οντότητα εστιάζουν στο κράτος – στόχο αλλά και στην κοινωνία του κράτους – στόχου, με κύριο σκοπό τον επηρεασμό της κρατικής συμπεριφοράς. Ο φορέας των επιθέσεων μπορεί να είναι ακόμα και ένας μη κρατικός δρώντας, γεγονός που εγείρει το ζήτημα της δυσκολίας εφαρμογής αντιποίνων σε στόχο που δεν αποτελεί κρατική οντότητα. Ωστόσο, η άποψη που κερδίζει έδαφος διεθνώς είναι ότι, το κράτος που υποστηρίζει ή ανέχεται την δράση του υπόψη μη κρατικού δρώντα από την επικράτεια του, θα πρέπει να γίνεται αντικείμενο ελέγχου[168].

Πέραν όμως του επηρεασμού της κρατικής συμπεριφοράς με βάση τα συμφέροντα του επιτιθέμενου, ο οποίος θεωρείται ως ο εξωτερικός αντικειμενικός σκοπός (External Objective), υπάρχει και ο εσωτερικός αντικειμενικός σκοπός (Internal Objective) του κυβερνοπολέμου. Ο εσωτερικός ΑΝΣΚ (αντικειμενικός σκοπός) αφορά στην διαχείριση της σύγκρουσης, δηλ. την κλιμάκωση – αποκλιμάκωση της, την παύση της, τον περιορισμό του εύρους της κτλ.

Θα πρέπει επίσης να επισημανθεί πως ο στρατηγικός κυβερνοπόλεμος δεν αποτελεί πανάκεια για την επίτευξη όλων των στόχων των εμπλεκομένων. Υπάρχουν σαφή όρια στις δυνατότητες επιτυχίας μέσα από αυτό το είδος πολέμου. Η χρήση των κυβερνοόπλων μπορεί να γίνει για την επίτευξη περιορισμένων σκοπών (limited aims)[169]. Σε πρώτη φάση θα πρέπει να τονιστεί ότι δεν μπορεί να επιτευχθεί αφοπλισμός του αντιπάλου, ούτε αλλαγή της κυβέρνησης του κράτους – στόχου. Σε καμία περίπτωση επίσης δεν μπορεί να γίνει κατάληψη εδάφους.

Όπως γίνεται εύκολα κατανοητό, η επίτευξη των ΑΝΣΚ σχετίζεται με το μέγεθος του αντίκτυπου που μπορεί να έχουν οι κυβερνοεπιθέσεις που εξαπολύονται από τον

---

[167] Ibid, p.117
[168] Ibid
[169] Mahnken, Thomas G., "*Cyber War and Cyber Warfare*", στο συλλογικό έργο Lord, Kristin M. & Sharp, Travis (Eds), "*America's Cyber Future: Security and Prosperity in the Information Age*, Vol.2, CNAS, June 2011

επιτιθέμενο κατά του κράτους – στόχου[170]. Ωστόσο, τονίζεται ότι ο αντίκτυπος αυτός διαφέρει κατά πολύ από τον αντίκτυπο του συμβατικού πολέμου. Οι υπέρμαχοι του κυβερνοπολέμου προσπαθούν να βρουν αναλογίες του στρατηγικού κυβερνοπολέμου με τον στρατηγικό αεροπορικό βομβαρδισμό και τον πυρηνικό πόλεμο, κάτι το οποίο χαρακτηρίζεται ως παραπλανητικό, καθώς τα αποτελέσματα από τις 2 τελευταίες περιπτώσεις δεν μπορούν να συγκριθούν με αυτά των κυβερνοεπιθέσεων[171]. Συνεπώς, το στοιχείο του εξαναγκασμού που προσπαθεί να επιφέρει στον αντίπαλο ο στρατηγικός κυβερνοπόλεμος δεν μπορεί να θεωρείται δεδομένο. Βασική αιτία αποτελεί το γεγονός ότι ο εξαναγκασμός προς ένα κράτος κινείται αναλογικά με τον αριθμό των ανθρώπινων απωλειών, κάτι που ο στρατηγικός κυβερνοπόλεμος δεν μπορεί να επιφέρει[172]. Επίσης, θα πρέπει να ληφθεί υπόψη πως σε αντίθεση με τον συμβατικό πόλεμο, τα αποτελέσματα των κυβερνοεπιθέσεων χαρακτηρίζονται ως προσωρινά, γεγονός που δρα ενισχυτικά στην πεποίθηση της κοινής γνώμης για μη συναίνεση σε εξαναγκασμό[173].

Από την άλλη μεριά, υπάρχει η άποψη ότι με τον στρατηγικό κυβερνοπόλεμο μπορεί να επιτευχθεί ο εξαναγκασμός του κράτους – στόχου σε συμπεριφορά που να συμβαδίζει με τα συμφέροντα του επιτιθέμενου, αρκεί να τηρηθούν κάποιες προϋποθέσεις. Το επιχείρημα αυτό στηρίζεται στην περίφημη «Τριάδα» του Κλαούζεβιτς (Λαός – Ένοπλες Δυνάμεις – Κυβέρνηση)[174], αλλά και στον βαθμό που τα 3 συστατικά της «Τριάδας» εξαρτώνται σήμερα από τα συστήματα Η/Υ[175]. Όπως έχει επισημανθεί και νωρίτερα, η καθημερινότητα του σύγχρονου ανθρώπου στηρίζεται στους Η/Υ. Αρκεί κάποιος να εστιάσει στο μέγεθος των χρηματοοικονομικών συναλλαγών, στην παροχή ενέργειας, στις μεταφορές, στην Υγεία και σε άλλους τομείς που κάνουν χρήση των Η/Υ. Επιπλέον οι σύγχρονες ΕΔ εξαρτώνται από τα ΙΤ συστήματα και τον κυβερνοχώρο. Αρκεί κάποιος να αναλογιστεί την θέση των Η/Υ στα σύγχρονα συστήματα διοίκησης & ελέγχου (C^2 systems), την διακίνηση στρατιωτικών πληροφοριών, τις επικοινωνίες, τον έλεγχο των διαδικασιών υλικοτεχνικής υποστήριξης, τις απαιτήσεις για επιτήρηση και αναγνώριση του πεδίου της μάχης κ.α. Παράλληλα, η διαχείριση των αναγκών των πολιτών από την πολιτική ηγεσία, ο έλεγχος εφαρμογής των αποφάσεων της από τους πολίτες και η επικοινωνία με τον λαό στηρίζεται στα συστήματα Η/Υ.

---

[170] Libicki, 2009 : 118-119
[171] Mahnken, Thomas G., "*Cyber War and Cyber Warfare*", pp. 58-59
[172] Libicki, 2009: 122
[173] Ibid, p. 123
[174] Κολιόπουλος, Κωνσταντίνος, *Η στρατηγική σκέψη Από την Αρχαιότητα ως σήμερα* (Εκδόσεις Ποιότητα, Αθήνα, 2008), σελ. 154
[175] Sharma, Amit, *Cyber Wars: A Paradigm Shift from Means to Ends*, pp. 6-8, στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009)

Συνεπώς, η μη σωστή λειτουργία των δικτύων Η/Υ δύναται να επηρεάσει αρνητικά την σύγχρονη υλιστική κοινωνία σε βαθμό που να μειώνει την θέληση του λαού για πόλεμο. Δύναται ακόμα να προκαλέσει δυσχέρεια στην λειτουργική ικανότητα των ΕΔ και της πολιτικής ηγεσίας. Ωστόσο, για να παραχθεί στρατηγικό αποτέλεσμα, με βάση αυτήν την εξάρτηση από τους Η/Υ, θα πρέπει να υπάρξει ταυτόχρονη και μεγάλης κλίμακας επίθεση και στις τρεις συνιστώσες της «Τριάδας» του Κλαούζεβιτς, ώστε ένα κράτος – στόχος να οδηγηθεί σε στρατηγική παράλυση ή ανικανότητα αποτελεσματικής αντίδρασης[176]. Με τον τρόπο αυτό, θα επιτευχθεί το ιδεώδες του Σουν Τζου, δηλ. η υποταγή του αντιπάλου χωρίς την διενέργειας μάχης[177].

Λαμβάνοντας υπόψη τα παραπάνω, αξίζει να σημειωθεί ότι μέχρι σήμερα δεν έχουν παρατηρηθεί περιπτώσεις διενέργειας στρατηγικού κυβερνοπολέμου. Η μόνη εξαίρεση θα μπορούσε να είναι η περίπτωση των κυβερνοεπιθέσεων κατά της Εσθονίας το 2007, εφόσον οι Εσθονοί είχαν ανταποδώσει τις κυβερνοεπιθέσεις των Ρώσων ή είχαν δεχτεί πλήγματα στις ΕΔ τους. Η υπόψη κυβερνοσύγκρουση θα αναλυθεί σε επόμενη ενότητα. Θα πρέπει να σημειωθεί ότι, η χρήση των κυβερνοεπιθέσεων γίνεται κυρίως στο πλαίσιο άλλων μορφών συγκρούσεων, γεγονός που ενισχύει την άποψη ότι, τα κυβερνοόπλα θα χρησιμοποιηθούν στο πλαίσιο ενός επιχειρησιακού κυβερνοπολέμου.

2.6.2 Επιχειρησιακός Κυβερνοπόλεμος

Ο επιχειρησιακός κυβερνοπόλεμος (Operational Cyberwar) περιλαμβάνει τις κυβερνοεπιθέσεις (CNAs) που εξαπολύονται στην διάρκεια ενός πολέμου ή μιας ένοπλης σύγκρουσης κατά στρατιωτικών (military targets) αλλά και μη στρατιωτικών (civilian targets) στόχων. Η προσβολή μη στρατιωτικών στόχων αποκτά μεγαλύτερη σημασία, όταν μέσω αυτών επιτυγχάνεται ζημία στην διεξαγωγή στρατιωτικών επιχειρήσεων του αντιπάλου (π.χ προσβολή δικτύου τηλεπικοινωνιών). Επειδή μάλιστα λαμβάνει χώρα υποστηρικτικά στις συμβατικές συγκρούσεις, η εξαπόλυση των κυβερνοεπιθέσεων δεν θεωρείται ως κλιμάκωση της συμβατικής σύγκρουσης[178].

Προκειμένου μια σύγκρουση στον κυβερνοχώρο να χαρακτηριστεί ως επιχειρησιακός κυβερνοπόλεμος θα πρέπει να διασαφηνιστούν τα παρακάτω[179]: Πρώτον, οι επιχειρήσεις συλλογής πληροφοριών μέσω του κυβερνοχώρου (CNEs) ή αλλιώς η κυβερνοκατασκοπεία (Cyber Espionage) δεν συνιστούν επιχειρησιακό κυβερνοπόλεμο. Τα CNEs βοηθούν στην κατανόηση του στόχου, στην εύρεση της

[176] Ibid
[177] Tzu, Sun, *The Art of War* (Arcturus Publishing Limited, London, 2008), p. 34
[178] Libicki, 2009: 139
[179] Ibid, pp. 139-140

πλεονεκτικής θέσης πριν την κυβερνοσύγκρουση και στην αναγνώριση της ζημίας από την κυβερνοεπίθεση (BDA: Battle Damage Assessment), αλλά δεν αποτελούν κυβερνοεπίθεση. Δεύτερον, η φυσική επίθεση κατά των δικτύων Η/Υ, δηλ. η φυσική επίθεση κατά του φυσικού επιπέδου (physical layer) του κυβερνοχώρου, που θα προκαλέσει ζημία στα δίκτυα, δεν αποτελεί μέρος του επιχειρησιακού κυβερνοπολέμου. Τρίτον, η διενέργεια ψυχολογικών επιχειρήσεων (PSYOPS) αποτελούν τμήμα των πληροφοριακών επιχειρήσεων και δεν είναι επιχειρησιακός κυβερνοπόλεμος. Ωστόσο, θα πρέπει να τονιστεί ότι όταν στο πλαίσιο μιας συμβατικής σύγκρουσης, ένας hacker καταφέρει να διεισδύσει σε ένα δίκτυο Η/Υ και να αποστείλει emails, που θα φαίνονται ότι αποστέλλονται από ένα «νόμιμο» αποστολέα π.χ τον επικεφαλής αξιωματικό, με τα οποία θα ζητάει την οικειοθελή παράδοση των αντίπαλων στρατιωτών, τότε η ενέργεια αυτή εντάσσεται στον επιχειρησιακό κυβερνοπόλεμο.

Θα πρέπει επίσης να σημειωθεί ότι με αυτό το είδος κυβερνοσύγκρουσης δεν μπορεί κάποιος να κερδίσει συνολικά μια πολεμική σύγκρουση ή να κατακτήσει έδαφος. Τα αποτελέσματα από τις κυβερνοεπιθέσεις είναι προσωρινά και συνεπώς δεν μπορούν να εξαναγκάσουν μια σκληραγωγημένη κοινωνία από την συμβατική σύγκρουση σε οικειοθελή παράδοση[180]. Συνεπώς και σε αυτήν την περίπτωση μιλάμε για χρήση των κυβερνοόπλων για την επίτευξη περιορισμένων σκοπών (Limited aims)[181]. Επιπρόσθετα, μέσω του επιχειρησιακού κυβερνοπολέμου δεν μπορεί να επιτευχθεί η Υπεροχή στον κυβερνοχώρο (Cyber Supremacy) σε αντίθεση με την επίτευξη Υπεροχής στις άλλες περιοχές της ανθρώπινης δραστηριότητας (Ξηρά, Θάλασσα, Αέρας, Διάστημα). Δηλαδή, δεν μπορεί ο ένας αντίπαλος να απαγορεύσει εξολοκλήρου την χρήση του κυβερνοχώρου στον άλλο αντίπαλο. Αυτό οφείλεται στο γεγονός ότι ο κυβερνοχώρος δεν αποτελεί μια ενιαία περιοχή. Υπάρχει τουλάχιστον ένα τμήμα κυβερνοχώρου που αναλογεί στην κάθε αντίπαλη οντότητα[182]. Οι hacker μπορούν να αποκτήσουν πρόσβαση στην περιοχή του κυβερνοχώρου που ελέγχει ο αντίπαλος, αλλά ο τελευταίος έχει πάντα την επιλογή να αποσυνδέσει τα συστήματα του από τον κυβερνοχώρο[183] και να βρει στην συνέχεια νέα σημεία πρόσβασης σε αυτόν.

Αυτό που μπορεί να καταφέρει ο επιχειρησιακός κυβερνοπόλεμος σε μεγάλο βαθμό είναι ο αιφνιδιασμός[184] του αντιπάλου. Όπως έχει προαναφερθεί, οι κυβερνοεπιθέσεις σχετίζονται με την παραπλάνηση, καθώς εξαναγκάζουν ένα Η/Υ να

[180] Libicki, 2009: 141
[181] Mahnken, Thomas G., "*Cyber War and Cyber Warfare*"…, p. 58
[182] Libicki, pp.141-142
[183] Ibid
[184] Ibid, pp. 143-149. Επισημαίνεται ακόμα ότι, ο Σουν Τζου έδινε ιδιαίτερη σημασία στην συλλογή πληροφοριών, τον αιφνιδιασμό και την παραπλάνηση του αντιπάλου.

λειτουργήσει διαφορετικά από τον τρόπο που επιθυμεί ο χρήστης του. Συνεπώς, μετά από μια κυβερνοεπίθεση υπάρχει μια ποιοτική διαφοροποίηση αναφορικά με την λειτουργία του Η/Υ που ο χρήστης αναμένει να δει και σε αυτήν που τελικά βλέπει. Ο αιφνιδιασμός στον κυβερνοχώρο μπορεί να επιτευχθεί είτε πριν την έναρξη των συμβατικών συγκρούσεων είτε κατά την διάρκεια τους. Με δεδομένο ότι τα αποτελέσματα κάθε κυβερνοεπίθεσης είναι προσωρινά και προκειμένου ο επιτιθέμενος να διατηρεί το στοιχείο του αιφνιδιασμού θα πρέπει να έχει προηγηθεί κατάλληλη εκστρατεία κυβερνοκατασκοπείας, με την οποία θα έχουν ανακαλυφθεί οι τρωτότητες του αντιπάλου στον κυβερνοχώρο[185]. Σημαντική, επίσης, προϋπόθεση είναι ο επιτιθέμενος να διαθέτει μια ευρεία γκάμα διαφορετικών κυβερνοόπλων, καθώς ο ίδιος τρόπος επίθεσης για δεύτερη φορά δεν θα μπορέσει να επιφέρει αιφνιδιασμό στον αντίπαλο[186].

Ένα ακόμα επίτευγμα του επιχειρησιακού κυβερνοπολέμου είναι ότι δύναται να παρεμποδίσει τον αντίπαλο από την χρήση του κυβερνοχώρου για ένα εύλογο χρονικό διάστημα, δηλαδή δύναται να θέσει τον αντίπαλο εκτός δικτύου[187]. Σύμφωνα με τον καθηγητή Thomas G. Mahnken, αυτό αποτελεί το δυνατό σημείο του επιχειρησιακού κυβερνοπολέμου: η άρνηση στον αντίπαλο στην χρήση των συστημάτων Η/Υ και των δικτύων[188]. Ο φόβος που μπορεί να προκαλέσει στον αντίπαλο το αποτέλεσμα των κυβερνοεπιθέσεων μπορεί να τον οδηγήσει στην «απομόνωση», γεγονός που θα έχει αρνητικό επιχειρησιακό αντίκτυπο στην διεξαγωγή των επιχειρήσεων και την διακίνηση ζωτικών πληροφοριών για το πεδίο της μάχης. Παράλληλα, το ίδιο αποτέλεσμα μπορεί να επιτευχθεί και στο πλαίσιο μιας συμμαχίας, η οποία στηρίζεται στα δίκτυα Η/Υ για την ανταλλαγή πληροφοριών. Η ικανότητα του επιτιθέμενου να διεισδύσει στο δίκτυο που ανήκει σε έναν από τους συμμάχους, μπορεί να οδηγήσει σε έλλειψη εμπιστοσύνης μεταξύ των συμμάχων, οι οποίοι με την σειρά τους θα επιλέξουν την «απομόνωση» για μεγαλύτερη ασφάλεια[189]. Συνεπώς επέρχεται ζημία στην συνολική δικτύωση (networking) της συμμαχίας.

[185] Σύμφωνα με τον Σουν Τζου, η εκ των προτέρων γνώση για τον αντίπαλο, μπορεί να οδηγήσει στην επιτυχία.
[186] Libicki, 2009: p. 145
[187] Ibid, p. 150
[188] Mahnken, Thomas G., "*Cyber War and Cyber Warfare*"….., p. 60
[189] Libicki, 2009: 151

3. Οι Μη Κρατικοί Δρώντες και τα Κράτη στον Κυβερνοπόλεμο

3.1 Οι Μη Κρατικοί Δρώντες (Non State Actors)

Όπως προαναφέρθηκε, ο κυβερνοπόλεμος διεξάγεται από τα κράτη αλλά και από ανεπίσημα διορισμένους ή υποστηριζόμενους από τα κράτη μη κρατικούς δρώντες[190] (Non State Actors). Μέσω αυτών, τα κράτη μπορούν να διεξάγουν έμμεσα κυβερνοεπιθέσεις, χωρίς να διαφαίνεται άμεσα η σύνδεση τους με τους δράστες των επιθέσεων και συνεπώς να έχουν την δυνατότητα της εύλογης άρνησης (Plausible Deniability) για την επίθεση[191]. Οι μη κρατικοί δρώντες που χρησιμοποιούνται από τα κράτη για να διεξάγουν κυβερνοεπιθέσεις εμφανίζονται στην διεθνή βιβλιογραφία ως Cyber Militias (κυβερνοπολιτοφυλακές). Ουσιαστικά, πρόκειται για ομάδες ατόμων, οι οποίες ανεξάρτητα του βαθμού εξειδίκευσης που έχουν στην τεχνολογία πληροφορικής (IT), είναι πρόθυμες να διεξάγουν κυβερνοεπιθέσεις προκειμένου να πετύχουν ένα συγκεκριμένο πολιτικό σκοπό[192]. Θα πρέπει να σημειωθεί ότι η διασύνδεση ενός κράτους με ομάδες Cyber Militias δεν συνεπάγεται τον πλήρη έλεγχο των ομάδων αυτών από το κράτος, αλλά ούτε και την πλήρη γνώση από το κράτος για την ταυτότητα του συνόλου των μελών των εν λόγω ομάδων. Επιπλέον, αξίζει να αναφερθεί ότι, οι Cyber Militias δύναται να διεξάγουν τις επιθέσεις τους στον κυβερνοχώρο, χωρίς κατά ανάγκη αυτό να είναι αποτέλεσμα μιας άμεσης ή έμμεσης κυβερνητικής εντολής. Σε αυτήν την περίπτωση όμως, οι ενέργειες τους δεν εντάσσονται στον κυβερνοπόλεμο, αλλά στις άλλες κατηγορίες κυβερνοσυγκρούσεων που προαναφέρθηκαν με βάση τον αντικειμενικό σκοπό των επιθέσεων.

Το 1998 θεωρείται η χρονιά όπου καταγράφηκε για πρώτη φορά η δράση μιας ομάδας κυβερνοπολιτοφυλακής, η οποία δεν χαρακτηρίζεται ως κυβερνοπόλεμος. Πρόκειται για την περίπτωση της αριστερής εθνικοαπελευθερωτικής ομάδας του Μεξικό, γνωστής ως Zapatistas, η οποία από το 1994 διεξήγαγε ανταρτοπόλεμο στο Μεξικό. Το 1998 όμως δραστηριοποιήθηκε στον κυβερνοχώρο με την συνδρομή

---

[190] Οι Μη Κρατικοί Δρώντες μπορεί να είναι μεμονωμένοι ιδιώτες - hackers που «πωλούν» τις υπηρεσίες τους σε ένα κράτος για συγκεκριμένο χρονικό διάστημα χωρίς συμβόλαιο (freelancers) ή ομάδες hackers που «συνεργάζονται» με ένα κράτος, κάτι το οποίο συνηθίζεται περισσότερο. Υπάρχει βέβαια η περίπτωση ένας hacker ή μια ομάδα hackers να ενεργήσουν εντελώς αυτόνομα. Αυτό εξαρτάται από τα κίνητρα που έχουν. Σε γενικές γραμμές, τα κίνητρα αυτών των hackers είναι συνήθως οικονομικά, θρησκευτικά ή εθνικιστικά – πολιτικά.

[191] Ottis, Rain, "*Proactive Defense Tactics Against On-Line Cyber Militia*". In Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July. Reading: Academic Publishing Limited, pp. 233-237. Available at: http://www.ccdcoe.org/articles/2010/Ottis_ProactiveDefense.pdf, accessed on Sep. 2010

[192] Ibid

ευρωπαίων hackers και εξαπέλυσε κυβερνοεπιθέσεις κατά της μεξικανικής αστυνομίας, των ΗΠΑ και του χρηματιστηρίου της Φρανκφούρτης[193].

Από τότε έχουν καταγραφεί πολλές παρόμοιες δράσεις από Cyber Militias, οι περισσότερες από τις οποίες προέκυψαν σε συνέχεια τοπικών συγκρούσεων. Σύμφωνα με τον Scott Borg, ειδικό σε θέματα κυβερνοπολέμου και διευθυντή του Ινστιτούτου Ερευνών "US Cyber Consequences Unit", αποτελεί σημείο έντονου προβληματισμού, η ύπαρξη δυνατότητας πλήρους ελέγχου της δράση Cyber Militias από τα κράτη - εντολείς, ώστε να αποφευχθεί ο κίνδυνος της κλιμάκωσης σε μια σύγκρουση[194].

3.2 Μοντέλα Οργάνωσης των Cyber Militias

Οι κυβερνοπολιτοφυλακές χαρακτηρίζονται από τρία βασικά μοντέλα οργάνωσης, με βάση τις παρατηρήσεις από τον τρόπο δράσης τους μέχρι σήμερα. Στην πραγματικότητα μια κυβερνοπολιτοφυλακή μπορεί να έχει στοιχεία και από τα 3 υπόψη μοντέλα οργάνωσης. Τα μοντέλα αυτά είναι τα εξής:

(i) Το Φόρουμ (Forum)[195]

Πρόκειται για Cyber Militia που συστήνεται ειδικά για ένα γεγονός και διεξάγει κυβερνοεπιθέσεις για συγκεκριμένο πολιτικό σκοπό. Αποτελεί μια πλατφόρμα διοίκησης και ελέγχου, όπου τα πιο ενεργά μέλη του μπορούν να αναρτήσουν (στο διαδίκτυο) οδηγίες επίθεσης, επιθετικά εργαλεία και προπαγανδιστικό υλικό. Επειδή δημιουργείται ως απάντηση σε κάποιο γεγονός, συνήθως διαλύεται μετά το πέρας αυτού του γεγονότος. Ωστόσο, μπορεί να έχει κάποια μόνιμα μέλη.

Το Forum αποτελεί ένα χαλαρό δίκτυο hackers, όπου κανένας από αυτούς δεν γνωρίζει συνολικά τα άλλα μέλη, ενώ κάποιοι από αυτούς μπορούν να διασυνδέονται με το κυβερνοέγκλημα. Συνηθίζεται να υπάρχει ένας καταμερισμός ρόλων (π.χ εκπαίδευση, σχεδίαση εκστρατείας, παροχή malware κτλ), αλλά δεν υπάρχει ισχυρή διοίκηση και έλεγχος, με αποτέλεσμα το κάθε μέλος να δραστηριοποιείται με τον τρόπο που αυτό επιθυμεί. Επιπλέον, η εξειδίκευση των μελών του Forum στον κυβερνοχώρο ποικίλει.

---

[193] Dudney, Robert S., "Rise of Cyber Militias", AIR FORCE Magazine (February 2011). Available at: http://www.airforce-magazine.com/MagazineArchive/Pages/2011/February%202011/0211cyber.aspx.

[194] Ibid

[195] Rain, Ottis, "*Theoretical Offensive Cyber Militia Models*", *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC, Academic Publishing Limited, pp. 307-313. Available at: http://www.ccdcoe.org/articles/2011/Ottis_TheoreticalOffensiveCyberMilitiaModels.pdf, accessed on May 2011

Το βασικό πλεονέκτημα του είναι ότι δύναται να συγκροτηθεί σε μικρό χρονικό διάστημα και να αναλάβει δράση άμεσα. Επιπλέον, η ποικιλομορφία που εμφανίζει, αναφορικά με τα μέλη του, δημιουργεί προβλήματα στους αμυνόμενους, καθώς δυσκολεύονται να αναλύσουν και να αντιμετωπίσουν τις κυβερνοαπειλές. Μπορεί επίσης να περιλαμβάνει μέλη τα οποία δραστηριοποιούνται σε διαφορετικές χώρες, με αποτέλεσμα να είναι πιο δύσκολη η συνολική αντιμετώπιση του.

Το βασικό μειονέκτημα του Forum εστιάζει στη χαλαρότητα του δικτύου των μελών του, καθώς δεν υπάρχει συμπαγής διοίκηση και έλεγχος. Κάθε μέλος μπορεί να δράσει αυτόνομα, χωρίς να ακολουθήσει τις κεντρικές κατευθυντήριες γραμμές, με συνέπεια να υπάρξει επέκταση της σύγκρουσης. Πολλές φορές, το Forum συγκεντρώνει μεγάλο αριθμό μελών με περιορισμένες γνώσεις στην διεξαγωγή κυβερνοεπιθέσεων, γεγονός που επηρεάζει αρνητικά την επιχειρησιακή αποτελεσματικότητα του. Επιπλέον, λόγω του γεγονότος ότι τα υποψήφια μέλη δεν υποβάλλονται σε μια αυστηρή διαδικασία ελέγχου πριν από την ενσωμάτωση στους στο Forum, υπάρχει ο κίνδυνος διείσδυσης ατόμων που θα λειτουργήσουν διασπαστικά σε αυτό.

Χαρακτηριστικό παράδειγμα ενός τέτοιου μοντέλου οργάνωσης αποτέλεσε το Forum “stopgeorgia.ru”, το οποίο δραστηριοποιήθηκε κατά την διάρκεια της ένοπλης σύγκρουσης Ρωσίας – Γεωργίας το 2008. Συγκεκριμένα, το υπόψη Forum, το οποίο προστατευόταν στο διαδίκτυο με κωδικό χρήσης[196], ενεργοποιήθηκε στις 9 Αυγ. 2008, μια ημέρα μετά την έναρξη των συμβατικών επιχειρήσεων, έχοντας στο δυναμικό του 30 μέλη. Μέχρι τις 15 Σεπ. 2008 τα μέλη του “stopgeorgia.ru” είχαν ξεπεράσει τα 200 άτομα, με κάθε ένα από αυτά να διαθέτει διαφορετικό επίπεδο εξειδίκευσης στις κυβερνοεπιθέσεις. Οι επικεφαλής (έμπειροι hackers) του Forum παρείχαν στα λιγότερο έμπειρα μέλη λίστα με στόχους, στοιχεία για τις τρωτότητες αυτών και εργαλεία κυβερνοεπιθέσεων[197]. Έχοντας εθνικιστικά κίνητρα, το “stopgeorgia.ru” επιτέθηκε κατά γεωργιανών ιστοσελίδων με σκοπό να διακόψει την λειτουργία τους.

(ii) <u>Το Κελί (Cell)</u>[198]

Το Κελί περιλαμβάνει hackers διαφορετικής εξειδίκευσης και ικανότητας, οι οποίοι πραγματοποιούν κυβερνοεπιθέσεις για μια εκτεταμένη περίοδο. Σε αντίθεση με το Forum, στο Cell τα μέλη δεν είναι πολλά σε αριθμό, ενώ γνωρίζονται μεταξύ τους,

[196] Carr, 2010 : 106
[197] Ibid, pp. 15-16
[198] Rain, Ottis, “*Theoretical Offensive Cyber Militia Models*”….

χωρίς αυτό να σημαίνει ότι η ταυτότητα τους είναι γνωστή στο ευρύ κοινό. Η διαδικασία εισαγωγής σε αυτό είναι δυσκολότερη, καθώς το νέο μέλος εξετάζεται λεπτομερώς, ενώ θα πρέπει να αποδείξει ότι έχει διαπράξει παράνομες κυβερνοεπιθέσεις.

Η διοίκηση και ο έλεγχος μπορούν να βασίζονται είτε σε ένα ιεραρχικό μοντέλο ή στο μοντέλο του επίπεδου οργανισμού, όπου τα μέλη συντονίζουν τις ενέργειες μεταξύ τους, χωρίς να δίνουν ή να δέχονται εντολές. Συνήθως, τα μέλη του Cell εξαπολύουν κυβερνοεπιθέσεις για καθαρά λόγους συγκέντρωσης εμπειριών, με το web defacement να αποτελεί μια συνήθη πρακτική τους. Δεν μπορεί να αποκλειστεί η διασύνδεση των μελών του από το κυβερνοέγκλημα. Επιπλέον, η διάρκεια ζωής του Cell είναι συνήθως μεγάλη και εξαρτάται από το μέγεθος του προβλήματος που οδήγησε στην δημιουργία του.

Βασικό πλεονέκτημα του Cell είναι ότι μπορεί να κινητοποιηθεί άμεσα, δεδομένου ότι τα μέλη του γνωρίζονται μεταξύ τους. Επειδή η διαδικασία αποδοχής ενός νέου μέλους είναι πιο προσεκτική σε σχέση με το Forum, η πιθανότητα διείσδυσης σε αυτό από τρίτους είναι μικρότερη. Επίσης, λόγω της πρότερης εμπειρίας των μελών του σε κυβερνοεπιθέσεις, η αποτελεσματικότητα του είναι μεγαλύτερη, ειδικότερα κατά στόχων που δεν είναι ιδιαίτερα προφυλαγμένοι.

Το κυριότερο μειονέκτημα του Cell είναι ότι η εμπειρία των μελών του πηγάζει από την κατά το παρελθόν συμμετοχή τους σε κυβερνοεπιθέσεις, κάποιες από τις οποίες οι διωκτικές αρχές μιας χώρας έχουν καταγράψει και διασυνδέσει με συγκεκριμένα άτομα. Ως αποτέλεσμα, η γνώση των ταυτοτήτων κάποιων μελών του Cell από τις διωκτικές αρχές, δύναται να οδηγήσει στην αποκάλυψη των ταυτοτήτων και των υπολοίπων μελών. Επίσης, ο υπερβολικός εγωισμός των hackers μπορεί να λειτουργήσει αρνητικά στην δραστηριότητα του Cell. Πολλές φορές, οι hackers συνηθίζουν να αφήνουν σκοπίμως ίχνη για την επίθεση που διέπραξαν, προκειμένου να αποκτήσουν φήμη στο ευρύ κοινό αλλά και εντός της κοινότητας των hackers. Ωστόσο, η δημοσιότητα αυτή μπορεί να λειτουργήσει αντίστροφα και τόσο οι hackers όσο και το Cell, στο οποίο ανήκουν, να γίνουν αντικείμενο επικρίσεων.

Χαρακτηριστικό παράδειγμα Cell αποτελεί η περίπτωση του “Team Evil”[199], το οποίο δραστηριοποιήθηκε το 2006 διαμαρτυρόμενο για τις ισραηλινές επιχειρήσεις στην Λωρίδα της Γάζας και στο Λίβανο. Συγκεκριμένα, από τον Ιούνιο έως τον Νοέμβριο του 2006 το Cell “Team Evil” διενήργησε web defacement σε πάνω από 8.000 ιστοσελίδες σε Ισραήλ, δυτικές χώρες, Σ. Αραβία, Ινδονησία και Κίνα. Στις περισσότερες περιπτώσεις το Cell άφηνε αντί-ισραηλινά και αντί-σημιτικά συνθήματα στις ιστοσελίδες – θύματα. Σύμφωνα με ισραηλινά ΜΜΕ, το “Team Evil” αποτελούνταν

[199] Carr, 2010 : 22-23

από Μαροκινούς hackers και είχε επιτεθεί κατά το πρώτο εξάμηνο του 2006 εναντίον ισραηλινών ιστοσελίδων που ανήκαν σε πολιτικά κόμματα, τράπεζες, ΜΚΟ, νοσοκομεία και μεγάλες εταιρείες. Θα πρέπει να επισημανθεί ότι το "Team Evil" χαρακτηρίστηκε από τους ειδικούς ως ομάδα hackers με μεγάλες τεχνικές δυνατότητες.

(iii) Η Ιεραρχία (Hierarchy)[200]

Όπως προκύπτει από την ονομασία, σε αυτό το μοντέλο οργάνωσης υπάρχει μια ξεκάθαρη αλυσίδα διοίκησης και ελέγχου. Στην Hierarchy υπάρχει οργάνωση παρόμοια με αυτή των στρατιωτικών μονάδων, όπου ο διοικητής ασκεί εξουσία στα υποσύνολα της μονάδας του. Κατά αντιστοιχία με τον στρατό, κάθε υποομάδα της Hierarchy έχει έναν διακριτό ρόλο (π.χ cyber espionage, cyber attack κτλ). Η συμμετοχή σε αυτό το μοντέλο οργάνωσης μπορεί να είναι είτε συνολικά ανώνυμη (π.χ μέσω χρήσης ψευδωνύμων) είτε συνολικά επώνυμη, χωρίς αυτό να σημαίνει ότι οι ταυτότητες των μελών είναι γνωστές σε τρίτα πρόσωπα.

Σε περίπτωση που η Hierarchy υποστηρίζεται από ένα κράτος, τότε θα διαθέτει ικανούς πόρους για την διεξαγωγή πιο εξειδικευμένων δραστηριοτήτων στον κυβερνοχώρο, ενώ θα έχει παράλληλα την συνδρομή και άλλων κρατικών υπηρεσιών στο έργο της, όπως π.χ των μυστικών υπηρεσιών, γεγονός που της προσδίδει ένα συγκριτικό πλεονέκτημα σε σχέση με το Forum και το Cell. Επίσης, η ύπαρξη του ιεραρχημένου μοντέλου οργάνωσης συνεπάγεται την καλύτερη διοίκηση και έλεγχο με αποτέλεσμα την μεγαλύτερη διάρκεια επιχειρησιακής ζωής μιας τέτοιας ομάδας hackers.

Από την άλλη πλευρά, η ύπαρξη ιεραρχικής οργάνωσης σε μια ομάδα κυβερνοπολιτοφυλακής μπορεί να σημαίνει μικρότερη ευελιξία αλλά και μικρότερη δυνατότητα μεγέθυνσης της ομάδας. Υπάρχει επίσης ο κίνδυνος να εμφανιστεί στο εσωτερικό της ομάδας η παθογένεια που αφορά στην μανιώδη επιδίωξη κατάληψης των ηγετικών θέσεων της ομάδας από κάποια μέλη της, αλλά και δυσλειτουργία της ομάδας σε περίπτωση που ουδετεροποιηθούν οι προσωπικότητες – κλειδιά. Επιπλέον, τέτοιου είδους ομάδες hackers ταυτίζονται αυτόματα με συγκεκριμένα κράτη, με αποτέλεσμα αυτά να χάνουν το πλεονέκτημα της ανωνυμίας στον κυβερνοχώρο.

[200] Rain, Ottis, "*Theoretical Offensive Cyber Militia Models*". *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC, Academic Publishing Limited, pp. 307-313. Available at: http://www.ccdcoe.org/articles/2011/Ottis_TheoreticalOffensiveCyberMilitiaModels.pdf, accessed on May 2011

Χαρακτηριστικό παράδειγμα Hierarchy αποτελούν οι μονάδες κυβερνοπολιτοφυλακής που έχει εντάξει η Κίνα στα τάγματα Πληροφοριακού Πολέμου που διαθέτει.

3.3 Οι Δυνατότητες των Cyber Militias

Οι δυνατότητες που έχουν οι κυβερνοπολιτοφυλακές στην διεξαγωγή επιχειρήσεων κυβερνοπολέμου εξαρτώνται αναλογικά από την εξειδίκευση των μελών τους στην IT τεχνολογία αλλά και από τους πόρους (π.χ οικονομικούς ή υλικούς πόρους) που μπορούν να έχουν στην διάθεση τους. Συνήθως, τα Cyber Militias αποτελούνται από έναν πυρήνα «ειδικών στο hacking», οι οποίοι είναι το κέντρο βάρους της ομάδας, αναφορικά με τις δυνατότητες και την αποτελεσματικότητα της, καθώς και από τους «ερασιτέχνες», οι οποίοι είναι πολύ περισσότεροι σε αριθμό και διαθέτουν ελάχιστες γνώσεις στο hacking. Όπως γίνεται αντιληπτό, οι ελάχιστες δυνατότητες των Cyber Militias είναι αναλογικά εξαρτώμενες με τις ουσιαστικές δυνατότητες των «ερασιτεχνών». Με δεδομένο ότι η εξειδίκευση των «ειδικών στο hacking» μπορεί να διαφέρει σημαντικά, η ανάλυση των δυνατοτήτων των Cyber Militias θα εστιάσει στις κατ' ελάχιστον δυνατότητες των «ερασιτεχνών».

Οι «ερασιτέχνες» στον κυβερνοπόλεμο μπορεί να είναι[201]: α) Hackers με μηδενικές ικανότητες (Hackers Zero - Skills), οι οποίοι δεν έχουν λάβει κάποια ειδική εκπαίδευση ή δεν έχουν σχετική εμπειρία στις κυβερνοεπιθέσεις. Οι Hackers Zero-Skills ξέρουν κατ' ελάχιστο να χρησιμοποιούν ένα πρόγραμμα περιήγησης στο διαδίκτυο (web browser), να δέχονται και να αποστέλλουν emails και να εκτελούν βασικές λειτουργίες στους Η/Υ (π.χ εγκατάσταση λογισμικού, άνοιγμα φακέλων, αντιγραφή φακέλων κτλ) και β) Hackers με μηδενικούς πόρους (Hackers Zero – Resources), οι οποίοι έχουν κατ' ελάχιστο πρόσβαση σε έναν προσωπικό Η/Υ και διαθέτουν μια σύνδεση στο Internet.

Σε γενικές γραμμές οι «ερασιτέχνες» του κυβερνοπολέμου μπορούν είτε να συμμετάσχουν σε επιθετικές δραστηριότητες στον κυβερνοχώρο είτε να προσφέρουν υπηρεσίες υποστήριξης κατά την διάρκεια μιας εκστρατείας στον κυβερνοχώρο[202]. Οι βασικές επιθετικές τους δραστηριότητες συνοψίζονται σε[203]:

---

[201] Ottis, Rain, "*From Pitchforks to Laptops: Volunteers in Cyber Conflicts*". In Czosseck, C. and Podins, K. (Eds.) Conference on Cyber Conflict. Proceedings 2010. Tallinn: CCD COE Publications, pp. 97-109. Available at: http://www.ccdcoe.org/articles/2010/Ottis_FromPitchforks.pdf, accessed on Sep. 2010

[202] Ibid

[203] Ibid

α. Αυτόματες και μη αυτόματες[204] DoS (Denial of Service) κυβερνοεπιθέσεις

β. Μη εξουσιοδοτημένες αλλαγές του περιεχομένου των ιστοσελίδων (Web Defacement)

γ. Αποστολή – συνήθως - μέσω email κακόβουλου λογισμικού (malware)

δ. Συλλογή πληροφοριών για τις δυνατότητες του αντιπάλου (π.χ όρια λειτουργίας εξοπλισμού του, τρόποι αντίδρασης κτλ)

Από την άλλη μεριά, οι υποστηρικτικές δραστηριότητες των «ερασιτεχνών» των cyber militias συνοψίζονται σε[205]:

α. Προπαγάνδα και στρατολόγηση

β. Οικονομικές δωρεές ή παροχή πρόσβασης σε δίκτυα Η/Υ τα οποία στην συνέχεια θα χρησιμοποιηθούν ως στοιχεία ενός Botnet (π.χ ένας «ερασιτέχνης» δίνει τους κωδικούς του διαχειριστή δικτύου Η/Υ μιας εταιρείας σε έναν εξειδικευμένο Hacker)

γ. Αναμετάδοση οδηγιών κυβερνοεπιθέσεων

δ. Παροχή πληροφοριών στοχοποίησης, ιδιαίτερα αν ο στόχος βρίσκεται σε μια ξένη χώρα και ο «ερασιτέχνης» γνωρίζει την γλώσσα της ή πληροφορίες για αυτήν την χώρα.

ε. Παροχή πληροφοριών σχετικά με τα αποτελέσματα των επιθετικών δραστηριοτήτων των Cyber Militias σε μια χώρα, αλλά και τον αντίκτυπο που έχουν στο ανθρώπινο δυναμικό της. Αυτό επιτυγχάνεται εφόσον ο «ερασιτέχνης» διαβιεί στην χώρα – στόχο.

3.4 Τα Κράτη και ο Κυβερνοπόλεμος

Σύμφωνα με αναφορά της εταιρείας McAfee[206] (McAfee's 2008 Virtual Criminology Report) υπάρχουν περισσότερες από 120 χώρες που χρησιμοποιούν το Internet για δραστηριότητες κατασκοπείας σε πολιτικό, στρατιωτικό και οικονομικό επίπεδο. Επίσης, σε μια πιο πρόσφατη έρευνα του Κέντρου Στρατηγικών και Διεθνών Σπουδών (CSIS : Centre for Strategic and International Studies), η οποία στηρίχθηκε σε στοιχεία που προήλθαν από ανοικτές πηγές, ελέχθησαν 133 χώρες σχετικά με την

[204] Ένας τρόπος διεξαγωγής μιας τέτοιου είδους επίθεσης κατά μιας ιστοσελίδας, γίνεται αν κάποιος κρατά συνεχόμενα πατημένο το πλήκτρο "F5" στο πληκτρολόγιο του Η/Υ. Με αυτόν τον τρόπο ζητά την διαρκή ανανέωση της ιστοσελίδας. Ένας άλλος τρόπος είναι η συνεχόμενη – γρήγορη επιλογή των διασυνδέσεων (links) που υπάρχουν σε μια ιστοσελίδα, ώστε να υπερφορτωθεί η λειτουργία του server που διαχειρίζεται την ιστοσελίδα και να μην μπορεί να ανταποκριθεί σε άλλα αιτήματα χρηστών. Ωστόσο, για να έχουν αποτέλεσμα αυτές οι κυβερνοεπιθέσεις θα πρέπει να γίνονται συντονισμένα και για μεγάλη χρονική διάρκεια.

[205] Ottis, Rain, "*From Pitchforks to Laptops: Volunteers ….".*

[206] Carr, 2010: 1

ύπαρξη στρατιωτικού δόγματος ή πολιτικής που να πλαισιώνουν τις δραστηριότητες τους στον κυβερνοχώρο. Από την εν λόγω έρευνα διαπιστώθηκε ότι υπάρχουν 33 χώρες που έχουν στον στρατιωτικό σχεδιασμό ή την οργάνωση τους την έννοια του κυβερνοπολέμου (π.χ Ρωσία, Κίνα, ΗΠΑ, Ισραήλ, Ιράν, Β. Κορέα κα), ενώ σε άλλες 36 χώρες υπάρχουν μη στρατιωτικές υπηρεσίες («πολιτικές υπηρεσίες»), οι οποίες είναι υπεύθυνες για την κυβερνοασφάλεια (Ιαπωνία, Λιθουανία, Σουηδία, ΗΑΕ κα)[207].

Σύμφωνα με αναλύσεις, πάνω από 100 χώρες διαθέτουν σήμερα εξειδικευμένες μονάδες, που είναι υπεύθυνες για την διεξαγωγή επιχειρήσεων κυβερνοπολέμου[208]. Ανάμεσα στις πιο «δραστήριες» χώρες στα θέματα αυτά είναι οι ΗΠΑ, η Κίνα, η Ρωσία, το Ιράν, η Β. Κορέα και το Ισραήλ[209]. Οι χώρες αυτές θεωρείται ότι έχουν ιδιαίτερες επιθετικές ικανότητες στον κυβερνοπόλεμο, τις οποίες έχουν εκδηλώσει κατά καιρούς με την συμμετοχή τους σε διάφορά συμβάντα κυβερνοεπιθέσεων[210]. Αξίζει να σημειωθεί ότι οι προαναφερόμενες χώρες επέδειξαν ιδιαίτερο ζήλο στην ανάπτυξη επιθετικών κυβερνοόπλων, παρόλο που είτε διαθέτουν πυρηνικά όπλα είτε προσπαθούν να τα αποκτήσουν[211]. Στην συνέχεια θα γίνει μια περιγραφή των δυνατοτήτων των χωρών αυτών στον κυβερνοπόλεμο, καθώς και αναφορά στην εμπλοκή που είχαν σε διάφορα περιστατικά κυβερνοεπιθέσεων, τα οποία τράβηξαν την προσοχή της διεθνούς κοινότητας.

3.4.1 Κίνα

Η περίπτωση της Κίνας παρουσιάζει ιδιαίτερο ενδιαφέρον αναφορικά με τον τρόπο που αντιμετωπίζει τον κυβερνοχώρο και τον κυβερνοπόλεμο. Σύμφωνα με τον ειδικό σε θέματα κυβερνοπολέμου Richard Clarke, η Κίνα αφυπνίστηκε κατά την διάρκεια του 1ου πολέμου στον Περσικό Κόλπο (1990-1991), όταν είδε το Ιράκ να ηττάται εύκολα μέσα σε μικρό χρονικό διάστημα από τους συμμάχους. Την εποχή εκείνη το Ιράκ διέθετε τον 4ο σε μέγεθος στρατό σε παγκόσμιο επίπεδο, ο οποίος ήταν εξοπλισμένος με ρωσικά και κινεζικά οπλικά συστήματα[212]. Η εκτεταμένη χρήση του αεροπορικού όπλου, των συστημάτων Διοίκησης και Ελέγχου (C^2), των Η/Υ αλλά και

[207] Lewis, James A., Timlin, Katrina, "*Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization*", CSIS. Available at: http://www.unidir.org/bdd/fiche-ouvrage.php?ref_ouvrage=92-9045-011-J-en, accessed on Dec 2012

[208] Masters, Jonathan, "*Confronting the Cyber Threat*", CFR, 23 May 2011

[209] Walsh, Eddie, "*The Cyber Proliferation Threat*", CNAS, 6 Oct 2011. Available at: http://www.cnas.org/node/7108, accessed on Nov. 2011

[210] Το ζήτημα της απόδοσης με ακρίβεια της ευθύνης σε μια χώρα για την διεξαγωγή μιας κυβερνοεπίθεσης συνεχίζει να αποτελεί «πονοκέφαλο» στους ερευνητές. Ωστόσο, υπάρχουν πολλές ενδείξεις που καταδεικνύουν ότι κάποιες χώρες έχουν σαφή εμπλοκή σε περιστατικά κυβερνοεπιθέσεων.

[211] Κουσκουβέλης, Ηλίας Ι., *Εισαγωγή στις Διεθνείς Σχέσεις* (Ε' Έκδοση), (Εκδόσεις Ποιότητα, Αθήνα, 2007), σελ. 386

[212] Clarke & Knake, 2010: 49

των έξυπνων βομβών κατά την διάρκεια των επιχειρήσεων της Desert Storm θορύβησε την Κίνα, η οποία κινήθηκε προς την κατεύθυνση ανεύρεσης νέας στρατηγικής, που θα μπορούσε να ακυρώσει την νικηφόρα στρατηγική των ΗΠΑ και των συμμάχων τους.

Από τα μέσα της δεκαετίας του 1990 η Κίνα κατανόησε ότι η αριθμητική της υπεροχή σε ανθρώπινο δυναμικό ή σε συμβατικούς εξοπλισμούς απέναντι στις ΗΠΑ δεν θα της έδινε την νίκη σε έναν ενδεχόμενο πόλεμο. Οι Κινέζοι στρατηγιστές διέγνωσαν από τον Πόλεμο του Κόλπου (1990 -1991) ότι ένας μελλοντικός πόλεμος θα κριθεί περισσότερο από την δυνατότητα υποβάθμισης ή άρνησης της ροής των πληροφοριών στον εχθρό, παρά από την συμβατική δύναμη πυρός. Για το λόγο αυτό, η Κίνα περιόρισε το μέγεθος των στρατιωτικών της δυνάμεων, επένδυσε περισσότερο σε νέες τεχνολογίες (πχ τεχνολογίες πληροφορικής) και άρχισε να προσεγγίζει τις διακρατικές συγκρούσεις, δίνοντας ιδιαίτερη βαρύτητα στις έννοιες του Πληροφοριακού Πολέμου και του Κυβερνοπολέμου[213].

Την περίοδο αυτή έγιναν γνωστά στο ευρύ κοινό διάφορα συγγράμματα Κινέζων αξιωματικών που μιλούσαν για την αναγκαιότητα της πληροφοριακής υπεροχής, την χρήση των κυβερνοόπλων αλλά και τον ασύμμετρο πόλεμο. Στο πλαίσιο αυτό, ο Στρατηγός Wang Pufeng της κινεζικής Στρατιωτικής Ακαδημίας έκδωσε το 1995 το βιβλίο “The Challenge of Information Warfare”, στο οποίο μιλούσε για την έννοια της πληροφοριακής υπεροχής, ενώ ο Στρατηγός Dai Qingmin του κινεζικού Γενικού Επιτελείου Ενόπλων Δυνάμεων (ΓΕΕΔ) σημείωσε με άρθρο του, πως η πληροφοριακή υπεροχή μπορεί να επιτευχθεί μέσω προληπτικής κυβερνοεπίθεσης[214]. Το πλέον, όμως, χαρακτηριστικό παράδειγμα αποτελεί το βιβλίο “Unrestricted Warfare”[215], το οποίο εκδόθηκε το 1999 από 2 Κινέζους Συνταγματάρχες (Wang Xiangsui & Qiao Liang). Σύμφωνα με αυτό, μια αδύναμη χώρα δύναται να αντιμετωπίσει με επιτυχία δυνατότερους αντιπάλους, εφόσον κάνει χρήση μη συμβατικών μεθόδων[216]:

α. Ο αδύναμος θα πρέπει να προσαρμόζει την σύγκρουση στα οπλικά του συστήματα και να φτιάχνει όπλα που αρμόζουν στην σύγκρουση αυτή.

β. Η νέα στρατηγική δεν θα λαμβάνει υπόψη της τους παραδοσιακούς κανόνες σύγκρουσης. Συνεπώς θα επιτρέπεται η στοχοποίηση άοπλων πολιτών.

γ. Επιτρέπεται η «διαχείριση» των ξένων ΜΜΕ.

δ. Θα πρέπει να γίνεται χρήση του Κυβερνοπολέμου.

ε. Θα πρέπει να επιδιώκεται ο έλεγχος των αγορών φυσικών πόρων.

---

[213] Clarke & Knake, 2010: 50. Βλέπε επίσης, Billo & Chang, 2004: 27 - 29
[214] Ibid
[215] Το κείμενο του «Unrestricted Warfare» είναι διαθέσιμο στην παρακάτω ιστοσελίδα: http://www.globalsecurity.org/military/library/report/1999/WEBRES4.htm
[216] Clarke & Knake, 2010: 50 – 51. Δες επίσης, Billo & Chang, 2004: 30 -31

στ. Θα πρέπει να επιδιώκεται η εμπλοκή στα διεθνή νομικά όργανα, ώστε αυτά να αποφασίζουν υπέρ της Κίνας.

Με αφορμή τα ανωτέρω, η Κίνα προχώρησε στις παρακάτω κινήσεις:

α. Διατύπωση στρατιωτικού δόγματος για τον κυβερνοπόλεμο

Από τις αρχές του 21ου αι. η κινεζική κεντρική στρατιωτική επιτροπή διενήργησε μελέτη για την χρήση των πληροφοριών στον πόλεμο, ενώ το 2004 η κινεζική Λευκή Βίβλος έθεσε ως σημαίνοντα παράγοντα για την μαχητική ικανότητα των κινεζικών ΕΔ, αλλά και ως στρατηγικό προσανατολισμό την δυνατότητα λειτουργίας υπό το πλαίσιο των πληροφοριών (Informationalization). Αποτέλεσμα των ανωτέρω ήταν η δημιουργία του κινεζικού στρατιωτικού δόγματος, το οποίο συνιστά την χρήση δυνατοτήτων κυβερνοπολέμου και ηλεκτρονικού πολέμου στα πρώτα στάδια μιας σύγκρουσης[217]. Σύμφωνα με αυτό, το 3ο Τμήμα του κινεζικού ΓΕΕΔ (SIGINT: Signals Intelligence) και το 4ο Τμήμα του ΓΕΕΔ, το οποίο παρακολουθεί τον τομέα των ηλεκτρονικών αντιμέτρων και την ανάπτυξη πληροφοριακών τεχνολογιών από ερευνητικά κέντρα, είναι υπεύθυνα για τις επιχειρήσεις στον κυβερνοχώρο[218].

β. Στρατολόγηση hackers και συνεργασία με τα Cyber Militias

Υπό το παραπάνω πλαίσιο και με δεδομένο ότι στην Κίνα υπάρχει μεγάλος αριθμός ατόμων που ασχολούνται με το Internet (π.χ το 2006 ο αριθμός αυτός ήταν 162 εκατομμύρια χρήστες), ο κινεζικός στρατός διεξάγει σε ετήσια βάση διαγωνισμούς για hackers, προκειμένου να στρατολογήσει στην συνέχεια τους πιο ικανούς. Όσοι επιλέγονται εντάσσονται ως έφεδροι στον κινεζικό στρατό και υπηρετούν σε διάφορες πόλεις της Κίνας[219]. Θα πρέπει να σημειωθεί ότι υπάρχουν πολλές ομάδες κινεζικών Cyber Militias[220] που δραστηριοποιούνται στην ενδοχώρα υπό την ανοχή, την ανεπίσημη συνεργασία και τον έλεγχο του κινεζικού κράτους[221], ενώ όπως έχει αναφερθεί ο πλήρης έλεγχος αυτών των ομάδων δεν είναι πάντα εφικτός[222]. Παρόλα αυτά, σύμφωνα με το κινεζικό στρατιωτικό δόγμα, όλοι οι ανωτέρω μπορούν να λειτουργήσουν ως πολλαπλασιαστές ισχύος σε περίπτωση ενός κυβερνοπολέμου.

γ. Εκπαίδευση Αξιωματικών Κινεζικών ΕΔ στον Κυβερνοπόλεμο

Ο κινεζικός στρατός έχει συστήσει διάφορα εκπαιδευτικά κέντρα για την παροχή θεωρητικής εκπαίδευσης επί θεμάτων κυβερνοπολέμου στα στελέχη του. Τα πιο γνωστά είναι η Ακαδημία της Διοίκησης Επικοινωνιών στο Wuhan, το

---

[217] Lewis & Timlin, "*Cybersecurity and Cyberwarfare 2011…..", p. 8*

[218] Ibid. Δες επίσης, (2007) "*China's cyber attacks*", Strategic Comments, Vol. 13, Issue 7, pp. 1-2, accessed on 19-5-11

[219] Billo & Chang, 2004: 33

[220] Υπάρχουν πάνω από 250 ιστοσελίδες και forum στην Κίνα που ανήκουν σε ομάδες hackers. Βλέπε, Carr, 2010: 91

[221] Billo & Chang, 2004: 36 - 37

[222] Noonan, Sean, "*China and its Double – edged Cyber - sword*", Stratfor. Available at: http://www.stratfor.com, accessed on 9/12/2010

Πανεπιστήμιο του Zhengzhou (Συστήματα Πληροφορικής), το Πανεπιστήμιο Επιστήμης και Τεχνολογίας και το Πανεπιστήμιο Εθνικής Άμυνας στην Gangsha. Τα αντικείμενα διδασκαλίας αφορούν στην βασική θεωρία Η/Υ και εφαρμογών, την τεχνολογία δικτύων επικοινωνίας, την τεχνολογία πληροφορικής, τα ηλεκτρονικά αντίμετρα, την τεχνολογία ραντάρ, τους κανόνες κυβερνοπολέμου, την στρατηγική και τακτική κυβερνοπολέμου, την συλλογή, διαχείριση & διανομή πληροφοριών, την λήψη αποφάσεων, τα συστήματα ελέγχου, την προστασία από κυβερνοεπιθέσεις κτλ[223].

Παράλληλα, από τα τέλη τις δεκαετίας του 1990, ο κινεζικός στρατός διενεργεί ασκήσεις κυβερνοπολέμου, προκειμένου τα στελέχη του να εφαρμόσουν αυτά που έμαθαν στην διάρκεια της θεωρητικής τους εκπαίδευσης. Συγκεκριμένα, τον Οκτώβριο του 1997 πραγματοποιήθηκε η πρώτη άσκηση κυβερνοπολέμου στην στρατιωτική περιφέρεια Shenyang[224]. Η άσκηση αυτή έγινε σχεδόν παράλληλα με την αμερικανική άσκηση κυβερνοπολέμου "Eligible Receiver"[225]. Στο σενάριο της κινεζικής άσκησης προβλεπόταν η προσβολή ενός στρατιωτικού σχηματισμού από ιούς (viruses) και η αντιμετώπιση της απειλής. Από το 1997 και έπειτα, ο κινεζικός στρατός διεξήγαγε σε ετήσια βάση ασκήσεις κυβερνοπολέμου, αυξάνοντας τον βαθμό δυσκολίας τους κάθε φορά. Τα βασικά αντικείμενα των ασκήσεων αφορούσαν στην εμφύτευση «logic bombs» στα εχθρικά δίκτυα πληροφορικής, στην πληροφοριακή αναγνώριση, στην μετατροπή των στοιχείων των δικτύων, στην διανομή προπαγάνδας, στην παραπλάνηση, στην δημιουργία σταθμών κατασκοπίας στο δίκτυο κτλ[226].

δ. <u>Ανάπτυξη Εγχώριων Δυνατοτήτων σε Τεχνολογία Πληροφορικής</u>

Η Κίνα βρίσκεται τα τελευταία χρόνια σε μια προσπάθεια ανάπτυξης των εγχώριων δυνατοτήτων της στην τεχνολογία πληροφορικής (IT), είτε μέσα από την δέσμευση μεγαλύτερων ποσών του προϋπολογισμού, είτε μέσα από την προσέλκυση ξένων επενδύσεων που θα μεταφέρουν την απαιτούμενη τεχνογνωσία στην χώρα[227]. Ωστόσο, πολλές φορές η Κίνα χρησιμοποιεί και μη θεμιτές μεθόδους προκειμένου να αποκτήσει την απαιτούμενη τεχνογνωσία σε IT τεχνολογία. Μια από αυτές προκύπτει από την επιστράτευση υπηκόων ξένων κρατών, κινεζικής καταγωγής, αλλά και κινέζων υπηκόων που ζουν στο εξωτερικό (πχ φοιτητές, εργαζόμενοι, διπλωμάτες κτλ), οι οποίοι λαμβάνοντας κάποια ανταλλάγματα από το κινεζικό κράτος μεταφέρουν την απαραίτητη τεχνογνωσία στην Κίνα[228]. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση του ερευνητή του "American University" Gao Zhan, ο οποίος τον Νοέμβριο του 2003 φυλακίστηκε στις ΗΠΑ λόγω της παράνομης μεταφοράς στην Κίνα

[223] Billo & Chang, 2004: p.32
[224] Ibid, pp. 32 -33
[225] Βλέπε παρ. 2.5
[226] Billo & Chang, 2004: 33
[227] Ibid, pp. 31 & 35
[228] (2007) "*China's cyber attacks*", Strategic Comments, Vol. 13, Issue 7, pp. 1-2, accessed on 19/5/2011

μικροεπεξεργαστών που μπορούσαν να χρησιμοποιηθούν σε συστήματα ελέγχου πτήσης, οπλικά συστήματα και στην αναγνώριση στόχων[229].

Δυο ακόμα μη θεμιτές μέθοδοι που χρησιμοποιεί η Κίνα για να αναπτύξει την εγχώρια IT τεχνολογία είναι μέσω διπλωματικών πιέσεων (εκβιασμός) ή μέσω αντιγραφής τεχνολογίας πληροφορικής ξένων κρατών. Ενδεικτικά αναφέρεται ότι, όταν η Κίνα ζήτησε από την εταιρεία Microsoft (περίοδος 2003-2004) να της παραχωρήσει τον μυστικό λειτουργικό της κώδικα και η Microsoft αρνήθηκε, τότε η Κίνα την απείλησε με αποκλεισμό της από την κινεζική αγορά[230]. Λόγω του μεγάλου οικονομικού κόστους, η Microsoft τελικά συναίνεσε στην κινεζική απαίτηση, γεγονός που έδωσε την δυνατότητα στην Κίνα να δύναται να εξαπολύει "zero-day"[231] κυβερνοεπιθέσεις κατά όσων λειτουργούν τις εφαρμογές του Microsoft Office και να εγκαθιστά malware σε δίκτυα Η/Υ[232]. Επιπλέον, αξιοσημείωτο παράδειγμα αντιγραφής IT τεχνολογίας αποτελεί η περίπτωση των Router[233] της αμερικανικής εταιρείας Cisco. Η Κίνα, εκμεταλλευόμενη την ύπαρξη ενός εργοστασίου κατασκευής Routers της Cisco στην επικράτεια της, αντέγραψε την συγκεκριμένη συσκευή και προχώρησε στην δημιουργία κινεζικών απομιμήσεων που έφεραν την ετικέτα της Cisco[234]. Παράλληλα, η κινέζικη εταιρεία κατασκευής Routers, Huawei, προχώρησε στην κατασκευή και πώληση σε Ευρώπη και Ασία παρόμοιων συσκευών, με την διαφορά ότι αυτές έφεραν την ετικέτα της Huawei[235]. Όπως έγινε γνωστό, μετά από έρευνα του FBI (2007), από το 2004 οι κινεζικές απομιμήσεις πωλήθηκαν με χαμηλή τιμή σε όλο τον κόσμο, ακόμα και στις ένοπλες δυνάμεις των ΗΠΑ[236]. Από τον συνδυασμό των δυο παραπάνω γεγονότων είναι εμφανές ότι οι κινεζικές ΕΔ θα μπορούσαν να σταματήσουν την λειτουργία των περισσότερων δικτύων Η/Υ στον κόσμο.

ε. <u>Έλεγχος Κινεζικού Δικτύου από το Κράτος</u>

Το σύνολο των δικτυακών υποδομών που αποτελούν το κινεζικό Internet βρίσκονται υπό τον πλήρη έλεγχο του κράτους και η άμυνα του εξασκείται αποκλειστικά από τις μονάδες των ΕΔ που ασχολούνται με τις επιχειρήσεις στον κυβερνοχώρο[237]. Με άλλα λόγια το κινεζικό κράτος έχει την δυνατότητα να

---

[229] Billo & Chang, 2004: 28. Βλέπε επίσης, (2007) "*China's cyber attacks*", Strategic Comments, Vol. 13, Issue 7, pp. 1-2.
[230] Clarke & Knake, 2010: 55
[231] Ουσιαστικά πρόκειται για κυβερνοεπιθέσεις που την στιγμή που εξαπολύονται δεν υπάρχει τρόπος αντιμετώπιση τους. Βλέπε, Mazanec, Brian M., "*The Art of (Cyber) War*", The Journal of International Security Affairs, Spring 2009 - No 16. Available at: http://www.securityaffairs.org/issues/2009/16/mazanec.php, accessed on 10/10/11
[232] Ibid
[233] Ο Router είναι συσκευή δικτύου που είναι υπεύθυνη για την μετακίνηση των ψηφιακών πακέτων δεδομένων μεταξύ των Η/Υ. Βλέπε, http://www.thefreedictionary.com/router
[234] Clarke & Knake, 2010: 56
[235] Ibid
[236] Ibid
[237] Ibid, p. 146

αποσυνδέσει, χωρίς ιδιαίτερη αιτιολογία, το σύνολο των δικτύων του από το παγκόσμιο Internet, σε περίπτωση που θεωρήσει ότι απειλείται με κυβερνοπόλεμο. Επιπρόσθετα, μετά την απόκτηση του λειτουργικού κώδικα της Microsoft, η Κίνα, για λόγους ασφαλείας, προχώρησε σε τροποποίηση της έκδοσης του λογισμικού της εταιρείας που προοριζόταν να πωληθεί στην ενδοχώρα, ενώ παράλληλα δημιούργησε το κινεζικό λειτουργικό σύστημα με την ονομασία Kylin[238]. Με πρόσχημα την καταπολέμηση της παιδικής πορνογραφίας ξεκίνησε την τοποθέτηση του λογισμικού «Green Dam Youth Escort» σε όλους τους Η/Υ της χώρας, προκειμένου να επιτηρεί τους Η/Υ της ενδοχώρας και να έχει έγκαιρη προειδοποίηση σε περίπτωση εγκατάστασης κακόβουλου λογισμικού σε αυτούς από αντίπαλες χώρες[239]. Επιπλέον, δημιούργησε ένα ψηφιακό τείχος προστασίας (Firewall) για το κινεζικό internet με την ονομασία “Great Firewall of China”, το οποίο εξυπηρετεί σκοπούς λογοκρισίας, αλλά δύναται να θέσει, όποτε η κινεζική κυβέρνηση αποφασίσει, ολόκληρη την επικράτεια της Κίνας εκτός παγκοσμίου internet[240].

Όπως προαναφέρθηκε, η Κίνα κατέχει την πρώτη θέση σε επιχειρήσεις κυβερνοκατασκοπείας. Μέχρι σήμερα, δεν έχει εμπλακεί φανερά σε επιχειρήσεις κυβερνοπολέμου. Ωστόσο, έχουν καταγραφεί περιπτώσεις όπου κινεζικές ομάδες hackers έχουν εμπλακεί σε κυβερνοαψιμαχίες με άλλα κράτη, υπό την ανοχή του κινεζικού κράτους. Συγκεκριμένα, μετά τον βομβαρδισμό της κινεζικής πρεσβείας στην Γιουγκοσλαβία από το ΝΑΤΟ το 1999, ομάδες κινέζων hackers πραγματοποίησαν επιθέσεις DDoS κατά αμερικανικών και νατοϊκών ιστοσελίδων. Συμμαχικές κυβερνητικές υπηρεσίες δέχθηκαν βομβαρδισμό ηλεκτρονικών μηνυμάτων (email bombing), νατοϊκές ιστοσελίδες τροποποιήθηκαν χωρίς εξουσιοδότηση (web defacement), ενώ άλλες σταμάτησαν να λειτουργούν[241]. Επίσης, όταν τον Απρίλιο του 2001 ένα αμερικανικό κατασκοπευτικό αεροσκάφος EP-3 - το οποίο σύμφωνα με την Κίνα είχε παραβιάσει το κινεζικό FIR - υποχρεώθηκε από κινεζικά μαχητικά αεροσκάφη σε αναγκαστική προσγείωση στο νησί Hainan, η κινεζική ομάδα hacker “Honker Union” εξαπέλυσε DDoS κυβερνοεπιθέσεις και CNEs κατά αμερικανικών στρατιωτικών ιστοσελίδων[242].

3.4.2 Ρωσία

[238] Ibid, p. 56
[239] Ibid
[240] Ibid, p.57
[241] Clarke & Knake, 2010: 55
[242] Nazario, Jose, *Politically Motivated Denial of Service Attacks*, p. 165, στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009)

Από τα μέσα της δεκαετίας του 1990, η Ρωσία έδωσε ιδιαίτερη βαρύτητα στην ανάπτυξη των απαραίτητων στρατιωτικών δυνατοτήτων για την επίτευξη πληροφοριακής υπεροχής και ασφάλειας[243]. Το 1996, η ειδική επιτροπή για θέματα πληροφοριακής ασφάλειας του ρωσικού κοινοβουλίου εξέφρασε υποψίες σχετικά με την τεχνολογική ακεραιότητα της τότε προμήθειας τηλεπικοινωνιακού εξοπλισμού από τις ΗΠΑ. Όπως είχε αναφερθεί, ο σχετικός εξοπλισμός είχε υποστεί τεχνικές παρεμβάσεις (hacking) – χωρίς την έγκριση της Ρωσίας - και μπορούσε ανά πάσα στιγμή να οδηγήσει σε κατάρρευση το ρωσικό τηλεπικοινωνιακό σύστημα[244]. Οι Ρώσοι αξιωματούχοι διακατέχονταν από μια διαρκή ανασφάλεια, καθώς η Ρωσία υστερούσε τεχνολογικά έναντι των ΗΠΑ, για τις οποίες πίστευαν ότι ήταν πολύ ανώτερες σε θέματα κυβερνοπολέμου. Ο φόβος των Ρώσων για τις αναπτυγμένες δυνατότητες των ΗΠΑ στον κυβερνοπόλεμο έδωσε σημαντική ώθηση στην δημιουργία κατάλληλου ρωσικού δόγματος για τις επιχειρήσεις στον κυβερνοχώρο και για την ανάπτυξη των ρωσικών δυνατοτήτων στο προαναφερθέν πεδίο.

Από τα τέλη της δεκαετίας του 1990, οι Ρώσοι προσπάθησαν να επιτύχουν μια διεθνή συμφωνία για τον κυβερνοχώρο, παρόμοια με την Συνθήκη για τα Χημικά Όπλα[245]. Πάγια θέση τους ήταν ότι το ζήτημα των hackers εντός της επικράτειας μιας χώρας είναι εσωτερικό πρόβλημα και δεν πρέπει η διεθνής κοινότητα να επεμβαίνει στο εσωτερικό ενός κράτους[246]. Επιπρόσθετα, προκειμένου να αποτρέψουν τους αντιπάλους τους που θα τους απειλούσαν με πληροφοριακό πόλεμο ή κυβερνοπόλεμο, διεμήνυσαν ότι διατηρούν το δικαίωμα της χρήσης πυρηνικών όπλων ακόμα και σε αυτές τις περιπτώσεις[247].

Αρχικά, οι ρωσικές προσπάθειες για την δημιουργία δόγματος στράφηκαν προς την αναγκαιότητα χρήσης του Internet για σκοπούς προπαγάνδας, παρακολούθησης των πολιτικών αντιπάλων και για άσκηση λογοκρισίας στους αντικαθεστωτικούς. Στην συνέχεια όμως δόθηκε βαρύτητα στην ανάπτυξη κυβερνοόπλων και την χρήση τους από τις ΕΔ και τις μυστικές υπηρεσίες. Οι ρωσικές ΕΔ και οι μυστικές υπηρεσίες συνεργάστηκαν με ειδικούς στην τεχνολογία πληροφορικής (IT experts) και με την

[243] Θα πρέπει να επισημανθεί ότι η ρωσική πλευρά συνηθίζει να ταυτίζει τις επιχειρήσεις στον κυβερνοχώρο (CNOs) με τις πληροφοριακές επιχειρήσεις (IOs). Συνεπώς, οπουδήποτε γίνεται μνεία στον πληροφοριακό πόλεμο από τους Ρώσους, έμμεσα αναφέρεται και ο κυβερνοπόλεμος.

[244] Carr, 2010 : 162

[245] Η Ρωσία προσεγγίζει τα κυβερνοόπλα ως όπλα μαζικής καταστροφής. Για το λόγο αυτό θέλει να τα περιορίσει με μια ανάλογη συνθήκη. Οι ΗΠΑ έχουν επανειλημμένα εκφράσει την αντίθεση τους σε αυτό και προσεγγίζουν τις κυβερνοεπιθέσεις ως εγκλήματα, τα οποία θα πρέπει να αντιμετωπίζονται από το Δίκαιο των χωρών. Βλέπε Carr, 2009: 30, 34

[246] Η θέση αυτή της Ρωσίας έρχεται σε αντιδιαστολή με την αμερικανική στάση, η οποία εστιάζει στην αντιμετώπιση των προβλημάτων στον κυβερνοχώρο μέσω διεθνούς συνεργασίας στην επιβολή του νόμου. Οι ΗΠΑ επισημαίνουν ότι πολλοί cyber criminals παίρνουν μέρος σε cyber conflicts. Συνεπώς αν δημιουργηθεί ένα διεθνές νομικό πλαίσιο συνεργασίας κατά των cyber criminals, αυτό θα έχει αντίκτυπο και στο cyber war. Για περισσότερα βλέπε Carr, 2010 : 34 – 35 & 170 - 171

[247] Carr, 2009: 30

ακαδημαϊκή κοινότητα, προκειμένου η Ρωσία να δημιουργήσει ένα δόγμα για τον κυβερνοπόλεμο[248], αλλά και για να αναπτύξει επιθετικές και αμυντικές δυνατότητες στον κυβερνοχώρο[249]. Παράλληλα, η επίτευξη κυβερνοασφάλειας έγινε ύψιστη προτεραιότητα για τις ρωσικές μυστικές υπηρεσίες (FSB), οι οποίες το 1999 απέκτησαν αρμόδια διεύθυνση για την πληροφοριακή ασφάλεια και την ασφάλεια των Η/Υ. Ένα δείγμα των προσπαθειών της ρωσικής πλευράς για την επίτευξη κυβερνοασφάλειας φανερώθηκε το 2001 κατά την διάρκεια της παρουσίασης του επίσημου ρωσικού στρατιωτικού δόγματος – τμήμα του οποίου αποτελεί το δόγμα για τον κυβερνοπόλεμο – από τον τότε Ρώσο ΥΠΑΜ Ivanov. Ο Ivanov είχε δηλώσει τότε ότι, η χώρα του είχε ήδη πάρει τα κατάλληλα μέτρα για την αντιμετώπιση της απειλής SIGINT που έθετε στην Ρωσία το κατασκοπευτικό πρόγραμμα ECHELON της αμερικανικής NSA (National Security Agency)[250]. Με τον τρόπο αυτό έγινε εμφανές ότι η Ρωσία είχε ήδη αναπτύξει δυνατότητες κυβερνοάμυνας (CND).

Το σύγχρονο ρωσικό στρατιωτικό δόγμα που γνωστοποιήθηκε στο ευρύ κοινό τον Φεβρουάριο του 2010 θεωρεί ότι χαρακτηριστικό των μελλοντικών συγκρούσεων θα είναι η έγκαιρη ενεργοποίηση των δυνατοτήτων πληροφοριακού πολέμου[251] μιας χώρας. Μέσω αυτών, η Ρωσία θα δύναται να επιτύχει τους πολιτικούς της σκοπούς, καθώς θα έχει κερδίσει τις θετικές αντιδράσεις της διεθνής κοινότητας και δεν θα αναγκάζεται να προβεί σε χρήση στρατιωτικής βίας[252]. Για το λόγο αυτό, οι ρωσικές ΕΔ θα πρέπει να έχουν πληροφοριακές δυνατότητες, να αναπτύξουν πληροφοριακά όπλα ακριβείας και να στοχεύσουν στην επίτευξη της πληροφοριακής υπεροχής[253].

Ο πλέον γνωστός ρωσικός κρατικός φορέας για την εφαρμογή του ρωσικού δόγματος για τον κυβερνοπόλεμο είναι η Ομοσπονδιακή Επιτροπή για τις Κυβερνητικές Επικοινωνίες και την Πληροφόρηση (FAPSI), η οποία αποτελούσε στο παρελθόν τμήμα της σοβιετικής KGB. Η FAPSI συνεργάζεται με τις ρωσικές ΕΔ και ουσιαστικά έχει παρόμοιες αρμοδιότητες με την αμερικανική NSA (δηλαδή κρυπτογράφηση – αποκρυπτογράφηση, παρακολουθήσεις επικοινωνιών, συλλογή ηλεκτρονικών πληροφοριών (SIGINT) κτλ), ενώ συνηθίζει να χρησιμοποιεί κυβερνοόπλα (πχ viruses) κατά την έναρξη των συγκρούσεων[254]. Από το 2003 ορισμένα τμήματα της FAPSI έχουν ενσωματωθεί στην ρωσική μυστική υπηρεσία FSB (διάδοχος της KGB). Θα πρέπει, επίσης, να σημειωθεί ότι, όπως και η Κίνα, η Ρωσία χρησιμοποιεί ομάδες εθνικιστών hackers νεαρής ηλικίας (Russian Youth Groups), τις οποίες επιχορηγεί

[248] Billo & Chang, 2004: 107
[249] Lewis & Timlin, "*Cybersecurity and Cyberwarfare 2011…..", p. 19*
[250] Billo & Chang, 2004: 115
[251] Όπως υποσημείωση No 216
[252] Lewis & Timlin (2011), p. 19
[253] Ibid
[254] Clarke & Knake, 2010: 63. Βλέπε επίσης, Billo & Chang, 2004: 118

μερικώς, προκειμένου να διεξάγουν κυβερνοεπιθέσεις για λογαριασμό του Κρεμλίνου[255]. Το τελευταίο διατηρεί με αυτό τον τρόπο το πλεονέκτημα της εύλογης άρνησης (plausible deniability) σε περίπτωση που κατηγορηθεί ότι εμπλέκεται στις κυβερνοεπιθέσεις[256]. Παράλληλα, υπάρχουν σημαντικές ενδείξεις ότι από την εποχή της KGB, οι ρωσικές μυστικές υπηρεσίες στρατολογούσαν hackers, που εμπλέκονταν με το κυβερνοέγκλημα, για να διεξάγουν κυβερνοεπιθέσεις επ' ωφελεία του ρωσικού κράτους, παρέχοντας τους ως αντάλλαγμα την μη σύλληψη τους[257].

Από την άλλη μεριά, οι περιπτώσεις κυβερνοεπιθέσεων που έχουν καταλογιστεί στην ρωσική πλευρά είναι αρκετές. Πρώτη από όλες είναι η υπόθεση με την ονομασία "Cuckoo's Egg". Η υπόθεση αυτή, αφορά στις προσπάθειες κυβερνοκατασκοπείας που εκδήλωσε ένας Ανατολικογερμανός hacker το 1985, προκειμένου να συλλέξει στοιχεία για το αμερικανικό πρόγραμμα "Star Wars" προς όφελος της σοβιετικής KGB[258]. Μια παρεμφερής υπόθεση φέρει την ονομασία "Moonlight Maze" και αφορά στην υπεξαίρεση δεδομένων από την NASA, το αμερικανικό Πεντάγωνο, το Υπουργείο Ενέργειας, καθώς και διάφορα πανεπιστήμια και ερευνητικά κέντρα[259]. Η υπεξαίρεση ξεκίνησε τον Μάρτιο του 1998 και συνεχίστηκε για 2 τουλάχιστον χρόνια. Σύμφωνα με τα στοιχεία που αποδεσμεύτηκαν από την έρευνα, οι «εισβολείς» ήταν Ρώσοι και κατάφεραν να υποκλέψουν χάρτες στρατιωτικών εγκαταστάσεων, διαμορφώσεις στρατευμάτων και σχέδια στρατιωτικού εξοπλισμού[260]. Ωστόσο, η Ρωσία δεν αποδέχθηκε ποτέ τις κατηγορίες.

Πέρα όμως από τις περιπτώσεις κυβερνοκατασκοπείας, η ρωσική πλευρά εμπλέκεται σε υποθέσεις κυβερνοεπιθέσεων DDoS. Οι πλέον γνωστές περιπτώσεις αφορούν στα γεγονότα που έλαβαν χώρα στην Εσθονία το 2007 και στην Γεωργία το 2008, τα οποία θα αναλυθούν εκτενέστερα σε επόμενη ενότητα. Άλλες περιπτώσεις τέτοιου είδους επιθέσεων σημειώθηκαν τον Οκτώβριο του 2002 κατά ιστοσελίδων των Τσετσένων αυτονομιστών ("Kavkaz.org" & "chechenpress.org"), με θύτη την ρωσική FSB. Συγκεκριμένα, κυβερνοεπιθέσεις DDoS πραγματοποιήθηκαν στις 26 Οκτωβρίου του 2002, λίγο πριν την εισβολή των ειδικών δυνάμεων της FSB στο θέατρο της

[255] Χαρακτηριστικό παράδειγμα Ρώσων εθνικιστών hackers αποτελεί η ομάδα "Nashi", η οποία ιδρύθηκε το 2005 με σκοπό την «καταστολή» οποιασδήποτε προσπάθειας λαϊκής εξέγερσης στην Ρωσία, όπως η πορτοκαλί επανάσταση της Ουκρανίας το 2004, αλλά και την αντιμετώπιση του νεοναζισμού στην χώρα. Οι "Nashi" υποστηρίζουν το καθεστώς Putin και εμπλέκονται σε επιχειρήσεις πληροφοριακού πολέμου (προπαγάνδα στο Internet) αλλά και κυβερνοεπιθέσεων, όπως στην περίπτωση του ρώσο-γεωργιανού πολέμου το 2008.
[256] Nazario, 2009: 174
[257] Billo & Chang, 2004: 108
[258] Billo & Chang, 2004: 107. Βλέπε επίσης σχετικό άρθρο σε: http://www.streettech.com/bcp/BCPgraf/StreetTech/cuckoo.htm, accessed on Dec. 2011
[259] Σχετικό άρθρο σε: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, accessed on April 2011
[260] Ibid

Μόσχας, όπου Τσετσένοι αυτονομιστές κρατούσαν υπό ομηρία Ρώσους πολίτες[261]. Αντικειμενικός σκοπός ήταν να μην μπορέσουν οι Τσετσένοι αυτονομιστές να δημοσιοποιήσουν οπτικό υλικό από την ρωσική επιχείρηση στο διαδίκτυο, κάτι το οποίο συνήθιζαν να κάνουν κατά τις πρόσφατες συγκρούσεις τους με τους Ρώσους (1994-1996 και 1997-2001).

Παρόμοια επιθετική ενέργεια εικάζεται ότι διενήργησαν οι Ρώσοι στις 18 Ιανουαρίου του 2009 κατά 2 τουλάχιστον εταιρειών παροχής Internet στο Κιργιστάν, με αποτέλεσμα οι πολίτες του Κιργιστάν να χάσουν επαφή με τα γεγονότα εν μέσω πολιτικών αναταραχών στην χώρα τους[262]. Σύμφωνα με ορισμένους αναλυτές, η κίνηση αυτή πιθανώς να αποσκοπούσε σε άσκηση πίεσης προς της κυβέρνηση του Κιργιστάν, προκειμένου το τελευταίο να μην επεκτείνει το χρονικό διάστημα παραμονής των αμερικανικών στρατευμάτων στην αεροπορική βάση "Manas Air Base"[263]. Χαρακτηριστικά αναφέρεται ότι, όταν στις 3 Φεβρουαρίου 2009 ο Πρόεδρος του Κιργιστάν Bakiyev δήλωσε πως τα αμερικανικά στρατεύματα δεν θα παραμείνουν περαιτέρω στην χώρα του, η Ρωσία έσπευσε σε παροχή οικονομικής βοήθειας 150 εκατομμυρίων δολαρίων και σε διάθεση δανείου ύψους 2 δις δολαρίων προς το Κιργιστάν[264].

3.4.3 ΗΠΑ

Σύμφωνα με πολλούς αναλυτές, οι ΗΠΑ κρατούν τα σκήπτρα παγκοσμίως αναφορικά με τις επιθετικές δυνατότητες στον κυβερνοχώρο. Το ζήτημα της ασφάλειας στον κυβερνοχώρο απασχόλησε τους Αμερικανούς από τις αρχές της δεκαετίας του 1990, καθώς αποτέλεσαν τους πρωτοπόρους στην χρήση Η/Υ και δικτύων Η/Υ σε στρατιωτικές και μη, εφαρμογές. Για το θέμα, εκφράστηκαν, κατά καιρούς, διαφορετικές απόψεις από τις αμερικανικές δεξαμενές σκέψεις (Think Tanks) και τους διάφορους κυβερνητικούς φορείς που έχουν ως αρμοδιότητα την ασφάλεια των ΗΠΑ. Οι απόψεις αυτές συγκλίνουν σε 2 κύριες τάσεις : α) Αυτούς που διαβλέπουν μια τρομακτική απειλή για τις ΗΠΑ μέσα από τον κυβερνοχώρο (Cyber Alarmists)[265] και θεωρούν ότι θα πρέπει να παρθούν δραστικά στρατιωτικά μέτρα. Οι Cyber Alarmists πιστεύουν ότι

[261] Billo & Chang, 2004: 113-114. Επίσης, θα πρέπει να σημειωθεί όμως ότι τέτοιου είδους επιθέσεις δεν στοχεύουν μόνο τους φορείς αποσχιστικών τάσεων στην Ρωσία. Σύμφωνα με τον Ρώσο δημοσιογράφο Andrei Soldatov, οι DDoS χρησιμοποιούνται κατά κόρον στο εσωτερικό της χώρας από την κυβέρνηση, προκειμένου να καταστέλλεται κάθε φωνή αντιπαράθεσης προς το καθεστώς Putin. Για περισσότερα βλέπε άρθρο Soldatov, Andrei, "*Vladimir Putin's Cyber Warriors*", Foreign Affairs, 9 Dec 2011, accessed on Dec 2011

[262] Carr, 2010 : 38

[263] Michael, Alex, "*Cyber Probing: The Politicisation of Virtual Attack*", p.16

[264] Ibid

[265] Samaan, Jean-Loup(2010), *"Cyber Command"*, The RUSI Journal, 155:6, 16 - 21

η έλευση ενός κυβερνοπολέμου μεγάλης κλίμακας (πχ Στρατηγικός Κυβερνοπόλεμος) είναι προ των πυλών. Συνήθως βρίσκονται εντός του αμερικανικού ΥΠΑΜ (DoD) και πιο συγκεκριμένα εντός της USAF και β) Αυτούς που στέκονται κριτικά απέναντι στην νέα απειλή (Cyber Skeptics)[266], οι οποίοι τα τελευταία χρόνια βρίσκονται συνήθως στον χώρο του Υπουργείου Εσωτερικής Ασφάλειας των ΗΠΑ (DHS). Οι Cyber Skeptics αναγνωρίζουν την ενοχλητική επίδραση που έχουν οι κυβερνοεπιθέσεις, λόγω των τρωτοτήτων που υπάρχουν στις στρατιωτικές και τις λοιπές ψηφιακές υποδομές των ΗΠΑ, αλλά δεν θεωρούν ότι αυτές οι επιθέσεις θα αποτελέσουν νέες μορφές σημαντικών συγκρούσεων.

Η διχογνωμία αυτή αποτέλεσε τροχοπέδη στην προσπάθεια δημιουργίας ενός θεσμικού πλαισίου αναφορικά με την αντιμετώπιση των κυβερνοαπειλών αλλά και την διενέργεια κυβερνοεπιθέσεων από τις ΗΠΑ[267]. Το θέμα της ασφάλειας στον κυβερνοχώρο καλυπτόταν σε επίπεδο DoD από μια χαλαρή συνεργασία των μονάδων κυβερνοάμυνας του κάθε κλάδου των αμερικανικών ΕΔ, ενώ σε μη στρατιωτικό επίπεδο από τις υπηρεσίες πληροφοριών όπως η NSA, η CIA και το FBI[268]. Τα πρώτα βήματα προς την δημιουργία θεσμικού πλαισίου έγιναν επί της δεύτερης προεδρικής θητείας του George W. Bush. Σημειώνεται ότι, το 2003 ο πρώην Πρόεδρος των ΗΠΑ δήλωσε ότι ο κυβερνοχώρος είναι το νευρικό σύστημα των αμερικανικών κρίσιμων υποδομών και το σύστημα ελέγχου της χώρας και προχώρησε στην δημιουργία θέσης ειδικού συμβούλου για θέματα κυβερνοασφάλειας στον Λευκό Οίκο. Το 2004 ο κυβερνοχώρος χαρακτηρίστηκε από τον Αρχηγό των αμερικανικών ΕΔ ως περιοχή διενέργειας μαχών[269], όπως ο αέρας, η θάλασσα, η ξηρά και το διάστημα, ενώ το 2006 εκδόθηκε η Εθνική Στρατιωτική Στρατηγική για τις επιχειρήσεις στον κυβερνοχώρο (National Military Strategy for Cyberspace Operations: NMS-CO)[270]. Σύμφωνα με την NMS-CO του 2006, στόχος των ΕΔ των ΗΠΑ ήταν η επίτευξη στρατηγικής υπεροχής στην ανωτέρω περιοχή. Με τον τρόπο αυτό, οι ΗΠΑ θα είχαν την ελευθερία κινήσεων στον κυβερνοχώρο, ενώ θα αρνούνταν την ελευθερία κινήσεων στους αντιπάλους τους. Βασικά στοιχεία της NMS-CO ήταν η ανάπτυξη επιθετικών δυνατοτήτων στον κυβερνοχώρο, η σημασία του πρώτου χτυπήματος και η παραδοχή ότι στην υπόψη

---

[266] Ibid

[267] Σημαντικό εμπόδιο στην δημιουργία θεσμικού πλαισίου για τις επιχειρήσεις στον κυβερνοχώρο (CNOs) αποτέλεσε και το ζήτημα του περιορισμού των δραστηριοτήτων των εμπορικών επιχειρήσεων και εταιρειών στον κυβερνοχώρο. Μέσα από την θέσπιση περιοριστικών μέτρων που ευνοούσαν την κυβερνοασφάλεια, τα κέρδη των πολυεθνικών εταιρειών θα μειώνονταν και ως αποτέλεσμα θα αυξάνονταν οι οικονομικές πιέσεις προς την αμερικανική προεδρία.

[268] Lynn, William J, "*Defending a New Domain: The Pentagon's Cyberstrategy*", Foreign Affairs, September/October 2010. Available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, accessed on 15/10/2010

[269] Alexander, Keith B., "*Warfighting in Cyberspace*", Joint Force Quarterly, issue 46, 3d quarter 2007, p. 59. Available at: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, accessed on May 2011.

[270] Clarke & Knake, 2010: 44-47

περιοχή δεν υπάρχουν γεωπολιτικά σύνορα, ενώ εν δυνάμει στόχοι μπορούν να είναι οι μη στρατιωτικές εγκαταστάσεις. Θα πρέπει να τονιστεί ότι με βάση το κείμενο της προαναφερόμενης στρατιωτικής στρατηγικής, το DoD θα μπορούσε να διεξάγει συμβατικές ή πυρηνικές επιχειρήσεις (kinetic missions) προκειμένου να διαφυλάξει την ελευθερία κινήσεων και το στρατηγικό πλεονέκτημα των ΗΠΑ στον κυβερνοχώρο. Προκειμένου να μην υπάρξουν λανθασμένοι υπολογισμοί και αντιλήψεις από τα άλλα κράτη, τον Μάιο του 2011 οι ΗΠΑ προέβησαν στην έκδοση της Διεθνούς Στρατηγικής για τον Κυβερνοχώρο (International Strategy for Cyberspace), με την οποία διεμήνυσαν ότι διατηρούν το δικαίωμα να χρησιμοποιήσουν κάθε απαραίτητο μέσο για την διασφάλιση τους, αλλά και την διασφάλιση των συμμάχων τους και των συνεργατών τους, χωρίς αυτό να σημαίνει ότι δεν θα εξαντλήσουν όλες τις άλλες επιλογές πριν την επιλογή χρήσης στρατιωτικής βίας[271].

Μετά το συμβάν του 2008, όπου τα διαβαθμισμένα και αδιαβάθμητα δίκτυα του αμερικανικού Πενταγώνου έπεσαν θύμα ξένων hackers και απώλεσαν τεράστιο όγκο δεδομένων, οι ΗΠΑ έλαβαν πιο δραστικά μέτρα για την ασφάλεια στον κυβερνοχώρο. Επισημαίνεται ότι ο Πρόεδρος Obama χαρακτήρισε το 2009 τον κυβερνοχώρο ως στρατηγικό περιουσιακό στοιχείο των ΗΠΑ, το οποίο θα προστατευθεί με κάθε μέσο[272]. Σε συνέχεια των δηλώσεων Obama, τον Ιούνιο του 2009 ο ΥΠΑΜ των ΗΠΑ εξουσιοδότησε τον Διοικητή της αμερικανικής Στρατηγικής Διοίκησης (US Strategic Command) να δημιουργήσει υπό την διοίκηση του μια νέα διακλαδική διοίκηση με την ονομασία USCYBERCOM (Cyber Command). Η USCYBERCOM[273] θα είχε ως σκοπό την προστασία των δικτύων των αμερικανικών ΕΔ, την υποστήριξη στρατιωτικών αποστολών και αποστολών καταπολέμησης της τρομοκρατίας μέσα από τον κυβερνοχώρο και την συνεργασία με άλλους κυβερνητικούς φορείς, συμμάχους[274] και ιδιωτικές επιχειρήσεις σε θέματα κυβερνοασφάλειας. Παράλληλα, τον Σεπτέμβριο του 2010 υπογράφτηκε Μνημόνιο Συνεργασίας[275] μεταξύ του DoD και του DHS, που αφορούσε στην συνεργασία των δυο Υπουργείων σε θέματα κυβερνοασφάλειας, με

---

[271] Lewis & Timlin, (2011) "*Cybersecurity and Cyberwarfare 2011:…..*", CSIS

[272] Masters, Jonathan, *"Confronting the Cyber Threat"*, CFR, 23 May 2011. Available at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577, accessed on 3/1/2012

[273] Lynn, William J, "*Defending a New Domain……*"

[274] Τον Μάιο του 2011, ο Λευκός Οίκος εξέδωσε το *"International Strategy for Cyberspace"* με το οποίο γνωστοποιούσε διεθνώς τις αμερικανικές προσδοκίες και τα σχέδια για τον κυβερνοχώρο. Σύμφωνα με την στρατηγική αυτή, οι ΗΠΑ διαφυλάττουν το δικαίωμα της χρήσης όλων των απαραιτήτων μέτρων για την προστασία τους αλλά και για την προστασία των συμμάχων και των συνεργατών των ΗΠΑ, με την επισήμανση ότι θα εξαντλήσουν πρώτα όλες τις προοπτικές πριν από την χρήση της στρατιωτικής βίας.

[275] Το μνημόνιο συνεργασίας προβλέπει την αποστολή αξιωματούχων του DHS, με εξειδίκευση στα ζητήματα προστασίας της ιδιωτικής ζωής και των ατομικών ελευθεριών, στην NSA (η οποία λειτουργεί υπό την USCYBERCOM), καθώς και αποστολή αξιωματούχων της NSA με γνώσεις στην κρυπτογράφηση στο DHS. Παράλληλα προβλέπεται η δημιουργία ενός συντονιστικού φορέα των δυο υπηρεσιών, ο οποίος θα είναι υπεύθυνος για τον κοινό επιχειρησιακό σχεδιασμό και συντονισμό. Για περισσότερα βλέπε, Hoover, Nicholas J, *"Homeland Security, Defense Sign Cybersecurity Pact"*, Information Week, 14 Oct 2010. Available at: http://www.informationweek.com/news/government/security/227800034, accessed on 11/1/2012

σκοπό να επιτευχθεί η κάλλιστη ανταπόκριση από την ομοσπονδιακή κυβέρνηση των ΗΠΑ σε κυβερνοαπειλές κατά των ιδιωτικών και κυβερνητικών δικτύων Η/Υ της χώρας.

Σύμφωνα, μάλιστα, με την πρόσφατη «Ανασκόπηση για την Πολιτική στον Κυβερνοχώρο» (Cyber Policy Review 2011), η οποία συντάχθηκε με εντολή του Προέδρου Obama, την ευθύνη για την κυβερνοασφάλεια των ΗΠΑ μοιράζονται από κοινού το DoD και το DHS. Στο DoD υπάγεται η διακλαδική USCYBERCOM, η οποία έχει την ευθύνη για την άμυνα των δικτύων Η/Υ του DoD και για τις επιθετικές επιχειρήσεις[276] των ΗΠΑ στον κυβερνοχώρο. Υπό την USCYBERCOM υπάγονται οι αρμόδιες Διοικήσεις Κυβερνοπολέμου των Κλάδων των αμερικανικών ΕΔ, δηλ. η Army Forces Cyber Command, η 24th Air Force, η Fleet Cyber Command και η Marine Corps Cyber Command, ενώ η USCYBERCOM κάνει επιπλέον χρήση των δυνατοτήτων της NSA. Από την μεριά του το DHS, μέσω της εξειδικευμένης Διεύθυνσης του, γνωστής ως National Cyber Security Division, έχει την ευθύνη για την ασφάλεια των λοιπών κυβερνητικών δικτύων Η/Υ και συνεργάζεται με δημόσιους, ιδιωτικούς και διεθνείς φορείς για θέματα κυβερνοασφάλειας. Δεν θα πρέπει όμως να παραληφθεί να τονιστεί ότι στην " Cyber Policy Review 2011" δεν έχει προβλεφθεί θεσμικά υπεύθυνος κρατικός φορέας για την ασφάλεια των ιδιωτικών δικτύων Η/Υ στις ΗΠΑ, στα οποία στηρίζονται πολλές από τις κρίσιμες υποδομές των ΗΠΑ. Τα δίκτυα αυτά προστατεύονται σε εθελοντική βάση από ιδιωτικούς φορείς.

Πέρα από τις θεσμικές προβλέψεις για την διασφάλιση των επιχειρήσεων τους στον κυβερνοχώρο, οι ΗΠΑ έχουν δαπανήσει τα τελευταία χρόνια σημαντικά ποσά για την ανάπτυξη των κυβερνοδυνατοτήτων τους. Σημαντικό ρόλο στην ανάπτυξη των αμερικανικών δυνατοτήτων στον κυβερνοχώρο έχουν διατελέσει τα αμερικανικά πανεπιστήμια, το Υπουργείο Ενέργειας και η DARPA (Defense Advanced Research Project Agency), η οποία έχει προχωρήσει στην δημιουργία ενός πεδίου ελέγχου και εφαρμογής (National Cyber Range) των αμερικανικών κυβερνοόπλων[277]. Θα πρέπει επίσης να σημειωθεί ότι μόνο για το 2012, οι ΗΠΑ αναμένεται να δαπανήσουν 3,4 δις δολ. για τις ανάγκες των DoD & DHS στον κυβερνοχώρο[278]. Ενδεικτικά αναφέρεται επίσης ότι, το 2010 ο Αμερικανός Υφυπουργός Άμυνας William J. Lynn III, είχε δηλώσει πως μόνο το DoD διαθέτει 15000 δίκτυα Η/Υ και 7 εκατομμύρια συσκευές Η/Υ σε όλον τον κόσμο, προκειμένου να επιτύχει Διοίκηση και Έλεγχο των δυνάμεων του, υλικοτεχνική υποστήριξη, παροχή έγκαιρης πληροφόρησης και διενέργεια

[276] Ένα μέρος των επιθετικών επιχειρήσεων των ΗΠΑ στον κυβερνοχώρο διεξάγονται από την CIA. Βλέπε, Lewis & Timlin, (2011) "*Cybersecurity and Cyberwarfare 2011:…..*", CSIS

[277] Το Υπουργείο Ενέργειας διαθέτει αρκετά επιστημονικά εργαστήρια, τα οποία χρησιμοποιεί για να εξετάσει τις απειλές στον κυβερνοχώρο. Βλέπε Lynn, William J, "*Defending a New Domain……*"

[278] Masters, Jonathan, *"Confronting the Cyber Threat"*

επιχειρήσεων στο εξωτερικό[279]. Επιπρόσθετα, δεν θα πρέπει να παραληφθεί το γεγονός ότι από το 1997 οι ΗΠΑ διεξάγουν σε τακτική βάση πληθώρα ασκήσεων κυβερνοπολέμου με αυξανόμενα επίπεδα δυσκολίας κάθε έτος όπως οι ασκήσεις Eligible Receiver[280], Cyber Storm[281], Schriever Wargame[282] κτλ.

Θα πρέπει να αναφερθεί ότι, σύμφωνα με έκθεση της εταιρείας McAfee για το 2010, η οποία φέρει τον τίτλο "In the Crossfire: Critical Infrastructure in the Age of Cyberwar", οι ΗΠΑ χαρακτηρίζονται ως ιδιαίτερα ευάλωτες[283] στις κυβερνοεπιθέσεις, αλλά ταυτόχρονα αποτελούν την Νο 1 πηγή κυβερνοεπιθέσεων, με δεύτερη χώρα την Κίνα[284]. Παρόλα αυτά και με εξαίρεση την υπόθεση Stuxnet – η οποία θα αναλυθεί παρακάτω – οι ΗΠΑ δεν έχουν αφήσει σε γενικές γραμμές αρκετά δείγματα των κυβερνοεπιθέσεων τους. Το γεγονός αυτό δεν σημαίνει αναγκαστικά ότι δεν διεξάγουν κυβερνοεπιθέσεις. Αντίθετα, μπορεί να ερμηνευτεί με την παραδοχή ότι οι ΗΠΑ διενεργούν κυβερνοεπιθέσεις, καλύπτοντας με επιτυχία τα ηλεκτρονικά ίχνη τους.

Ακόμα, αξίζει να σημειωθεί ότι, οι Αμερικανοί σχεδίαζαν στον 1ο πόλεμο του Περσικού Κόλπου (1990 – 1991) να χρησιμοποιήσουν μεθόδους κυβερνοπολέμου για να καταστείλουν την ιρακινή αεράμυνα, πριν την έναρξη των αεροπορικών βομβαρδισμών[285]. Συγκεκριμένα, το σχέδιο που είχε παρουσιαστεί στον Στρατηγό Norm Schwarzkopf προέβλεπε την εισβολή ομάδων των ειδικών δυνάμεων των ΗΠΑ σε ιρακινή στρατιωτική βάση και την «μόλυνση» του ιρακινού δικτύου Η/Υ εκ των έσω. Οι αμερικανικές ομάδες θα είχαν μαζί τους hackers της USAF. Ωστόσο, το σχέδιο δεν εγκρίθηκε, καθώς θεωρήθηκε ιδιαίτερα επικίνδυνο και με μικρά ποσοστά επιτυχίας. Αντ' αυτού επιλέχθηκαν οι αεροπορικοί βομβαρδισμοί των ιρακινών ραντάρ και των θέσεων των πυραύλων εδάφους - αέρος.

Αυτό που δεν έγινε στον 1ο Πόλεμο του Κόλπου πραγματοποιήθηκε μετά από 13 περίπου χρόνια. Κατά την διάρκεια του 2ου Πολέμου στον Κόλπο, οι ΗΠΑ κατάφεραν να διεισδύσουν με επιτυχία στο κλειστό δίκτυο Η/Υ (Intranet) του ιρακινού στρατού και να αποστείλουν μηνύματα σε όλους τους Ιρακινούς στρατιωτικούς, παρακινώντας τους να παραδώσουν τα όπλα[286]. Επίσης, την εποχή εκείνη είχε προταθεί στην στρατιωτική ηγεσία η διεξαγωγή κυβερνοεπιθέσεων κατά των

[279] Lynn, William J, "*Defending a New Domain……*"
[280] Στοιχεία για την άσκηση Eligible Receiver έχουν αναφερθεί στην παρ. 2.5
[281] Η άσκηση Cyber Storm διεξάγεται από το DHS και έχει ως στόχο την πρακτική εξέταση των διαδικασιών και επικοινωνιών μεταξύ κυβερνητικών φορέων και ιδιωτικών φορέων υπό το πλαίσιο κυβερνοεπιθέσεων κατά των κρίσιμων υποδομών της χώρας.
[282] Το σενάριο της άσκησης Schriever Wargame αφορά σε μια μελλοντική πολεμική σύγκρουση των ΗΠΑ στο διάστημα και στον κυβερνοχώρο με έναν ισάξιο αντίπαλο.
[283] Οι άλλες 2 χώρες που θεωρούνται το ίδιο ευάλωτες είναι η Κίνα και η Ρωσία.
[284] Markoff, John, "*Cyberattack Threat on Rise, Executives Say*", The New York Times, 29/1/2010. Available at: http://query.nytimes.com/gst/fullpage.html?res=9805E7DF123EF93AA15752C0A9669D8B63, accessed on 16/10/2011
[285] Clarke & Knake, 2010: 9
[286] Clarke & Knake, 2010: 10 - 11

τραπεζικών λογαριασμών του Saddam Hussein σε τράπεζες του Ιράκ και άλλων χωρών, κάτι το οποίο δεν εγκρίθηκε τελικά. Η αρνητική απόφαση στηρίχτηκε στο γεγονός ότι μια τέτοια κίνηση θα αποτελούσε παραβίαση του διεθνούς δικαίου, θα δημιουργούσε προηγούμενο, ενώ δεν μπορούσαν να προβλεφθούν επακριβώς τυχόν παράπλευρες απώλειες[287]. Μια δεκαετία περίπου αργότερα, το 2011 και ενώ η επιχείρηση "Unified Protector" εξελισσόταν, οι ΗΠΑ αποφάσισαν να μην διενεργήσουν κυβερνοεπιθέσεις κατά της λιβυκής αεράμυνας, υπό τον φόβο ότι θα δημιουργούσαν προηγούμενο, το οποίο θα χρησιμοποιούσαν η Ρωσία και η Κίνα, ενώ υπήρχε περίπτωση να αποκαλυφθεί σε τρίτους η μεθοδολογία διενέργειας των αμερικανικών κυβερνοεπιθέσεων[288].

Από την άλλη μεριά, οι ΗΠΑ εμφανίζονται πολλές φορές ως αποδέκτες κυβερνοεπιθέσεων, οι οποίες πιθανολογείται ότι οφείλονται σε ανταγωνιστικές δυνάμεις όπως η Ρωσία (π.χ περίπτωση Moonlight Maze) ή η Κίνα (π.χ περίπτωση F-35). Από τις πιο σημαντικές κυβερνοεπιθέσεις που δέχθηκαν οι ΗΠΑ είναι η παραβίαση των δικτύων Η/Υ του αμερικανικού Πενταγώνου το 2008, με αποτέλεσμα να υποκλαπούν σημαντικά στοιχεία για την αμερικανική άμυνα. Όπως γνωστοποιήθηκε μετά από σχετική έρευνα, η παραβίαση των αμερικανικών δικτύων προήλθε από μια φορητή μνήμη (Flash Drive), η οποία τοποθετήθηκε σε ένα αμερικανικό στρατιωτικό laptop στην Μ. Ανατολή. Το Flash Drive περιείχε malware, το οποίο είχε τοποθετηθεί από κάποια μυστική υπηρεσία μιας άγνωστης χώρας, διαδόθηκε αστραπιαία στο δίκτυο της US Central Command και στην συνέχεια στα υπόλοιπα δίκτυα του αμερικανικού DoD. Αποτέλεσμα της κυβερνοδιείσδυσης ήταν να γνωστοποιηθούν σε μη εξουσιοδοτημένα πρόσωπα σχέδια οπλικών συστημάτων, επιχειρησιακά σχέδια δράσης και στοιχεία επιτήρησης[289].

Μια ακόμα σημαντική περίπτωση κυβερνοεπίθεσης που δέχθηκαν οι ΗΠΑ αφορά στα μη επανδρωμένα αεροσκάφη (UAVs) που διαθέτει και έλαβε χώρα τον Σεπτέμβριο του 2011. Σύμφωνα με τα στοιχεία που έχουν κοινοποιηθεί, ένας ιός Η/Υ (computer virus) διείσδυσε στο δίκτυο Η/Υ της Creech Air Force Base, η οποία χειρίζεται μέσω δορυφόρων τα αμερικανικά UAVs Predator και Reaper που χρησιμοποιούν οι ΗΠΑ στο Αφγανιστάν[290]. Ως αποτέλεσμα, απωλέσθηκαν απόρρητα στοιχεία. Πιθανολογείται ότι, ο ιός διείσδυσε μέσα από flash drives, καθώς με αυτά συνηθίζεται να γίνονται ενημερώσεις των ψηφιακών χαρτών που χρησιμοποιούν οι

---

[287] Ibid

[288] Schmitt, Eric & Shanker, Thom, "*US Debated Cyberwarfare in Attack Plan on Libya*", The New York Times, 17 Oct 2011. Available at: http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1, accessed on 5/11/2011

[289] Lynn, William J, "*Defending a New Domain……*"

[290] Shachtman, Noam, "*Computer Virus Hits US Drone Fleet*", The Wired Magazine, 7 Oct 2011. Available at: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/, accessed on 22/1/2012

σταθμοί εδάφους που ελέγχουν τις πτήσεις των UAVs, αλλά και οι μεταφορές των καταγραφών βίντεο από τον έναν Η/Υ στον άλλο[291].

3.4.4 Ισραήλ

Αν και δεν υπάρχουν πολλές αναφορές σε ανοιχτές πηγές για την στρατηγική και το δόγμα κυβερνοασφάλειας του Ισραήλ, τα υπάρχοντα στοιχεία καταδεικνύουν ότι διαθέτει ιδιαίτερα αναπτυγμένες επιθετικές δυνατότητες στον κυβερνοπόλεμο. Αξίζει να σημειωθεί ότι τον Δεκέμβριο του 2009 ο απερχόμενος Διοικητής της στρατιωτικής υπηρεσίας πληροφοριών, Στρατηγός Amos Yadlin, δήλωσε πως η απειλή από τον κυβερνοχώρο είναι πολύ μεγάλη και την σύγκρινε με τον αντίκτυπο που είχε η εισαγωγή του αεροπορικού όπλου στις πολεμικές επιχειρήσεις. Όπως επεσήμανε τότε ο Ισραηλινός αξιωματούχος, οι πολεμικές επιχειρήσεις στον κυβερνοχώρο δίνουν στις μικρές χώρες δυνατότητες που αρμόζουν στις ισχυρές δυνάμεις του πλανήτη και το Ισραήλ μπορεί χωρίς την βοήθεια τρίτων να αναπτύξει ιδιαίτερες δυνατότητες στον κυβερνοχώρο[292].

Από τα διαθέσιμα στοιχεία για τις δυνατότητες του Ισραήλ στον κυβερνοχώρο προκύπτει ότι οι επιθετικές & αμυντικές δυνατότητες κυβερνοπολέμου και η κυβερνοκατασκοπεία ασκούνται από 4 διαφορετικούς φορείς στην χώρα[293]: α) Η Μονάδα 8200[294] των IDF (ισραηλινές ΕΔ) εστιάζει και στα 3 είδη των επιχειρήσεων στον κυβερνοχώρο (CNOs), δηλ. σε CNAs, CNEs & CNDs, δίνοντας όμως ιδιαίτερη βαρύτητα στις επιθετικές επιχειρήσεις. Θεωρείται ισοδύναμη της αμερικανικής NSA, καθώς είναι υπεύθυνη για θέματα SIGINT, τηλεπικοινωνιακές παρακολουθήσεις και αποκρυπτογράφηση[295], β) Η υπηρεσία εσωτερικής ασφάλειας Shin Bet από τα τέλη της δεκαετίας του 1990 είναι υπεύθυνη για την άμυνα των κυβερνητικών δικτύων, των εθνικών υποδομών και των χρηματοπιστωτικών ιδρυμάτων, γ) Το Σώμα C^4I των ισραηλινών ΕΔ έχει ως τομέα ευθύνης τις επικοινωνίες και την οργάνωση των δυνατοτήτων κυβερνοάμυνας. Ασχολείται ιδιαίτερα με την ανάπτυξη Firewalls και την κρυπτογράφηση, ενώ τα κυβερνοπροϊόντα που παράγει χρησιμοποιούνται για την άμυνα των κρατικών υπηρεσιών (IDF, Shin Bet, Mossad) και των κρίσιμων υποδομών

---

[291] Ibid

[292] Katz, Yaakov, "*Security and Defense: Nuclear worming*", 8 Oct 2010, The Jerusalem Post. Available at: http://www.jpost.com/Features/FrontLines/Article.aspx?id=190615, accessed on 21/1/2012

[293] Lewis & Timlin (2011), pp.14-15

[294] Όπως η Κίνα και η Ρωσία έτσι και το Ισραήλ στρατολογεί hackers προκειμένου να ενισχύσει την δυναμική του στον κυβερνοχώρο. Οι hackers αυτοί βρίσκονται μπροστά στο δίλημμα της φυλάκισης ή της εργασίας στις ισραηλινές ΕΔ. Η Μονάδα 8200 του Ισραήλ στρατολογεί αυτούς τους hackers. Βλέπε, McElroy, Damien, "*Israel's Unit 8200: cyber warfare*", 30 Sep 2010, The Telegraph. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8034882/Israels-unit-8200-cyber-warfare.html, accessed on 20/12/2012

[295] Katz, "*Security and Defense: Nuclear worming*", The Jerusalem Post

της χώρας[296] (π.χ τις ισραηλινές εταιρείες ηλεκτροδότησης και υδροδότησης) και δ) Από τις 18 Μαΐου 2011 λειτουργεί στο Ισραήλ μια νέα κρατική υπηρεσία γνωστή ως National Cybernetic Taskforce, η οποία έχει αναλάβει την εξασφάλιση των κρίσιμων δικτύων της χώρας από τον κίνδυνο των hackers και την προστασία των μη κρατικών βιομηχανιών από τον κίνδυνο της κυβερνοκατασκοπείας. Επιπλέον, η National Cybernetic Taskforce ασχολείται και με την προαγωγή της πανεπιστημιακής έρευνας σε θέματα κυβερνοασφάλειας.

Από τις αρχές του 21ου αι. το Ισραήλ έχει εμπλακεί σε μια πληθώρα επιχειρήσεων στον κυβερνοχώρο, με τις πιο γνωστές να αφορούν στα γεγονότα του 2000, 2006 και 2009 με τους Παλαιστίνους hackers[297] και την Hezbollah, στην αεροπορική επιδρομή στην Συρία το 2007 και στην υπόθεση Stuxnet, η οποία λόγω της ιδιαιτερότητας της θα αναλυθεί σε επόμενη ενότητα στην συνέχεια. Συγκεκριμένα, τον Οκτώβριο του 2000, μετά την απαγωγή 3 Ισραηλινών στρατιωτών, οι Ισραηλινοί hackers διενήργησαν web defacement κατά της ιστοσελίδας της Hezbollah, ενώ εκδήλωσαν κυβερνοεπιθέσεις κατά της παλαιστινιακής οργάνωσης Hamas, της Εθνικής Παλαιστινιακής Αρχής και του Ιράν. Σε απάντηση, οι Παλαιστίνιοι hackers στοχοποίησαν ισραηλινές πολιτικές και στρατιωτικές ιστοσελίδες, τηλεπικοινωνιακούς φορείς και ΜΜΕ του Ισραήλ, καθώς και ισραηλινές τράπεζες[298]. Το 2006 πάλι και ενώ η ένταση σε πολιτικό επίπεδο μεταξύ Ισραήλ και Παλαιστινίων είχε αυξηθεί, οι Παλαιστίνιοι hackers κατάφεραν να θέσουν εκτός λειτουργίας μεγάλο αριθμό ισραηλινών ιστοσελίδων, συμπεριλαμβανομένων ιστοσελίδων τραπεζών και ιδιωτικών εταιρειών, προκαλώντας μεγάλο αρνητικό οικονομικό αντίκτυπο στο Ισραήλ. Η Hezbollah επίσης, μπόρεσε να διεισδύσει στο σύστημα επικοινωνιών του Ισραήλ, με αποτέλεσμα να γνωρίζει εκ των προτέρων για τον τόπο και χρόνο των ισραηλινών επιχειρήσεων[299]. Τέλος, το 2009, κατά την διάρκεια της ισραηλινής επιχείρησης Cast Lead στην λωρίδα της Γάζας, έλαβαν χώρα κυβερνοαψιμαχίες μεταξύ Ισραηλινών και Παλαιστίνιων Hackers, οι οποίοι επιδόθηκαν σε επιθέσεις web defacement και DDoS[300]. Σημαντικότερο γεγονός ήταν η εκδήλωση κυβερνοεπιθέσεων κατά του ισραηλινού τηλεπικοινωνιακού δορυφόρου Amos-3 από τους Παλαιστίνιους hackers[301].

Επιπρόσθετα, τον Σεπτέμβριο του 2007, οι Ισραηλινές ΕΔ (IDF) επιχείρησαν επιτυχώς αεροπορικό βομβαρδισμό συριακών εγκαταστάσεων στην περιοχή Dayr az-Zawr, καθώς υπήρχαν πληροφορίες - από τις υπηρεσίες πληροφοριών των ΗΠΑ και

[296] Ibid
[297] Στις ομάδες των Παλαιστινίων Hackers εντάχθηκαν και hackers με φιλοπαλαιστινιακά αισθήματα, των οποίων η εθνικότητα δεν προσδιορίζεται. Το ίδιο έγινε και στις κυβερνοσυγκρούσεις του 2006 και 2009.
[298] Geers, Kenneth, "*Cyberspace and the Changing Nature of Warfare*"(keynote speech), p. 6
[299] Katz, Yaakov, "*Security and Defense: Nuclear worming*", The Jerusalem Post
[300] Nazario, 2009: 170
[301] Katz, Yaakov, "*Security and Defense: Nuclear worming*", The Jerusalem Post

του Ισραήλ - ότι εκεί οι Σύριοι ετοίμαζαν παράνομα πυρηνικό εργοστάσιο με την συνεργασία της Β. Κορέας. Η ιδιαιτερότητα της υπόθεσης αυτής έγκειται στο γεγονός ότι τα ισραηλινά μαχητικά Α/Φ δεν έγιναν αντιληπτά από την συριακή αεράμυνα, καθώς τα επίγεια ραντάρ είχαν «τυφλωθεί» έπειτα από κυβερνοεπιθέσεις των ισραηλινών και με τον τρόπο αυτό τα ισραηλινά μαχητικά δεν χρειάστηκε να αντιμετωπίσουν τα συριακά μαχητικά Α/Φ στον αέρα[302]. Σύμφωνα με τον ειδικό σε θέματα κυβερνοπολέμου Richard Clarke, οι Ισραηλινοί κατάφεραν να «τυφλώσουν» την συριακή αεράμυνα με έναν από τους παρακάτω τρόπους[303]:

α. Ένα ισραηλινό UAV εξέπεμψε ηλεκτρομαγνητικούς παλμούς προς ένα από τα διασυνδεδεμένα ραντάρ της συριακής αεράμυνας, οι οποίοι στην συνέχεια «μεταφράστηκαν» από τους Η/Υ του ραντάρ ως εντολή παύσης εργασιών για όλο το σύστημα αεράμυνας για συγκεκριμένο χρονικό διάστημα.

β. Οι Ισραηλινοί είχαν καταφέρει να «σπάσουν» το λογισμικό λειτουργίας του συριακού συστήματος ραντάρ, το οποίο ήταν ρωσικής προέλευσης και να εμφυτεύσουν σε αυτό μια Trapdoor[304]. Αυτό θα μπορούσε να έχει συμβεί μέσω ενός Insider (φιλικά προσκείμενου στο Ισραήλ) που έδρασε είτε εντός του ρωσικού εργαστηρίου κατασκευής λογισμικού για τα συριακά ραντάρ, είτε μέσα σε μια συριακή στρατιωτική μονάδα.

γ. Οι Ισραηλινοί είχαν ανακαλύψει στην συριακή ενδοχώρα τις γραμμές οπτικών ινών μέσω των οποίων μεταφέρονται ψηφιακά οι εντολές λειτουργίας των ραντάρ του συριακού συστήματος αεράμυνας και ενεργοποίησαν μια πρωτοποθετημένη trapdoor στο λογισμικό, η οποία είχε δημιουργηθεί στο παρελθόν από τους ίδιους.

3.4.5 Β. Κορέα

Η Βόρεια Κορέα είναι μια χώρα που εξαρτάται σε μεγάλο βαθμό από την εξωτερική οικονομική και τεχνική βοήθεια, αλλά και από το παράνομο εμπόριο. Το ΑΕΠ της χώρας είναι μικρό, οι διαθέσιμοι φυσικοί πόροι ελάχιστοι, ενώ δεν υπάρχουν ιδιαίτερες αναπτυξιακές υποδομές (πχ IT υποδομές), γεγονός που φέρνει την Β. Κορέα σε μειονεκτική θέση στο διεθνές σύστημα. Από τις αρχές της δεκαετίας του 1990, η

[302] Άρθρο με τίτλο: *"Report: Israel used Cyberwar against Syria"*, 13/12/2007. Available at: http://www.upi.com/Top_News/Special/2007/12/13/Report-Israel-used-cyberwar-against-Syria/UPI-20671197559471/, accessed on Dec 2010

[303] Clarke & Knake, 2010: 6-8

[304] Σημειώνεται ότι η trapdoor είναι ουσιαστικά σημείο πρόσβασης στο λογισμικό (software), το οποίο αφήνουν πολλές φορές οι κατασκευαστές του προκειμένου να έχουν μελλοντικά την δυνατότητα να επέμβουν για να το διορθώσουν ή να το αναβαθμίσουν. Τις trapdoors εκμεταλλεύονται δεόντως οι hackers προκειμένου να «αναγκάσουν» το λογισμικό ενός Η/Υ να εκτελέσει εντολές τις οποίες υπό κανονικές συνθήκες δεν θα εκτελούσε.

ηγεσία της χώρας κατανόησε ότι η παραπάνω θέση έχει αρνητικό αντίκτυπο στην εθνική ασφάλεια και επέλεξε μια στρατιωτική στρατηγική, η οποία βασίζεται στην ασυμμετρία. Βάση αυτής δόθηκε βαρύτητα στην ανάπτυξη βαλλιστικών πυραύλων, πυρηνικών όπλων και δυνατοτήτων κυβερνοπολέμου[305].

Η Β. Κορέα εκμεταλλεύτηκε τις ευνοϊκές συνθήκες που προέκυψαν από το τέλος του Ψυχρού Πολέμου, και προσπάθησε με επιτυχία να προσελκύσει ξένες επενδύσεις σε ΙΤ τεχνολογία. Υπό το πλαίσιο αυτό, συνεργάστηκε με χώρες όπως η Κίνα, η Ιαπωνία, η Νότια Κορέα και η Ρωσία[306]. Θα πρέπει όμως να σημειωθεί ότι, η συνεργασία αυτή δεν είχε αντίκτυπο στην ουσιαστική βελτίωση της καθημερινότητας των βόρειο – κορεατών, αλλά εξυπηρετούσε τα σχέδια της ηγεσίας της χώρας, αναφορικά με την εθνική ασφάλεια. Χαρακτηριστικά αναφέρεται ότι από το 2000 η ηγεσία της χώρας έχει αναπτύξει ένα εσωτερικό δίκτυο Η/Υ (Intranet), γνωστό ως "Kwangmyong", μέσω του οποίου οι «προνομιούχοι» των Βόρειο – Κορεατών μπορούν να έχουν πρόσβαση σε ενημερωτικό υλικό, το οποίο όμως είναι αυστηρά ελεγχόμενο από το κράτος[307]. Αυτό που θα πρέπει να τονιστεί είναι ότι αυτό το βόρειο-κορεατικό διαδίκτυο (Kwangmyong) δεν είναι συνδεδεμένο με το παγκόσμιο Internet, στο οποίο έχουν πρόσβαση κυρίως οι βόρειο – κορεατικές ΕΔ[308] και το ΥΠΕΞ[309]. Το γεγονός αυτό σε συνδυασμό με την απουσία ΙΤ υποδομών δίνει σημαντικό αμυντικό πλεονέκτημα στην Β. Κορέα σε περίπτωση που μια άλλη χώρα ή ένας φορέας θελήσει να διεξάγει κυβερνοεπιθέσεις εναντίον της.

Όσον αφορά στον κυβερνοπόλεμο, η Β. Κορέα θεωρείται ότι δαπανά σημαντικά ποσά για την ανάπτυξη επιθετικών δυνατοτήτων, χωρίς ωστόσο να υπάρχουν επίσημα στοιχεία για αυτό. Οι επιθετικές δυνατότητες αναπτύσσονται και εξασκούνται αυστηρά από τις ένοπλες δυνάμεις (ΕΔ) και τις μυστικές υπηρεσίες της χώρας. Η ανάπτυξη των επιθετικών δυνατοτήτων κυβερνοπολέμου γίνεται σε συνεργασία με τα εγχώρια ακαδημαϊκά και ερευνητικά ιδρύματα. Συγκεκριμένα, οι βόρειο - κορεατικές ΕΔ ξεκίνησαν το 1986 ένα ερευνητικό πρόγραμμα στο Κολλέγιο Mirim γύρω από την τεχνολογία Η/Υ στο οποίο εκπαιδεύονταν στελέχη τους[310]. Επίσης, υπάρχουν ενδείξεις για την διασύνδεση διάφορων τεχνικών ακαδημαϊκών ινστιτούτων, όπως η Ακαδημία Επιστημών και τα Πανεπιστήμια Kim Il Sung & Kim Chaek, με την ανάπτυξη δυνατοτήτων κυβερνοπολέμου για τις ΕΔ της χώρας[311]. Με την σειρά της η Κρατική

[305] Billo & Chang, 2004: 76
[306] Ibid, pp, 91-96
[307] Keating, Joshua E, "*Can North Koreans Use the Internet?",* Foreign Policy Magazine, 6 Oct 2010. Available at: http://www.foreignpolicy.com/articles/2010/08/26/can_north_koreans_use_the_internet, accessed on Feb 2011.
[308] Carr, 2010: 81
[309] Keating, Joshua E, "*Can North Koreans Use……..", FP Magazine*
[310] Billo & Chang, 2004: 77-78
[311] Ibid, p. 85

Υπηρεσία Ασφάλειας (SSA) ενσωμάτωσε στις τάξεις της το ερευνητικό ίδρυμα IT τεχνολογίας Korean Computer Center, προκειμένου να βελτιώσει τις δυνατότητες της στο τομέα των παρακολουθήσεων αλλά και τις επιθετικές της δυνατότητες στον κυβερνοπόλεμο[312]. Επιπλέον, υπάρχουν αναφορές που εμπλέκουν το ερευνητικό IT ίδρυμα Pyongyang Informatics Center με την εθνική ασφάλεια της χώρας, καθώς φέρεται ότι εμπλέκεται με την ανάπτυξη δυνατοτήτων hacking και συλλογής πληροφοριών[313].

Σύμφωνα με εκτιμήσεις, οι βόρειο – κορεατικές ΕΔ διαθέτουν 10.000 – 40.000 στελέχη - hackers, τα οποία έχουν 10ετή εμπειρία σε εκδήλωση CNAs και CNEs κατά της Νότιας Κορέας[314]. Η διαδικασία επιλογής τους ξεκινά κατά την διάρκεια της πρωτοβάθμιας εκπαίδευσης, όπου διαπιστώνονται οι ικανότητες τους στους Η/Υ. Κατά την διάρκεια της δευτεροβάθμιας εκπαίδευσης τα άτομα αυτά εκπαιδεύονται στον προγραμματισμό Η/Υ και στην τεχνολογία Η/Υ, ενώ στην συνέχεια εισάγονται στο Πανεπιστήμιο "Command Automation University" (Pyongyang) όπου εκπαιδεύονται στις κυβερνοεπιθέσεις[315]. Στην συνέχεια υπηρετούν σε εξειδικευμένες μονάδες κυβερνοπολέμου όπως τα "Unit 35, 110, 121 & 204".

Συγκεκριμένα, το "Unit 110" αναλαμβάνει αποστολές αναγνώρισης, δηλ cyber espionage, ενώ κάποια στελέχη του δραστηριοποιούνται μέσα από την Κίνα[316]. Το "Unit 121" θεωρείται η πολυπληθέστερη ομάδα hackers και η πλέον εξειδικευμένη στις βόρειο – κορεατικές ΕΔ. Έχει ως αποστολή την αδρανοποίηση των δικτύων διοίκησης, ελέγχου και επικοινωνιών (C^3) της Νότιας Κορέας, με ορισμένα στελέχη του να δραστηριοποιούνται εντός της κινεζικής επικράτειας[317]. Επίσης, το "Unit 204" είναι υπεύθυνο για την εκδήλωση ψυχολογικών επιχειρήσεων μέσα από τον κυβερνοχώρο, ενώ το "Unit 35" αναλαμβάνει αποστολές που αφορούν στην εσωτερική ασφάλεια αλλά και επιθετικές αποστολές[318].

Το πιο γνωστό παράδειγμα επιθετικής δραστηριότητας των βόρειο – κορεατικών ΕΔ στον κυβερνοχώρο αποτελεί η περίπτωση τον κυβερνοεπιθέσεων κατά των ΗΠΑ και της Ν. Κορέας τον Ιούλιο του 2009. Θα πρέπει ωστόσο να σημειωθεί πρώτα ότι, από τον Μάιο του 2009 και ενώ η Β. Κορέα αντιμετώπιζε σοβαρά οικονομικά προβλήματα, λόγω της διεθνούς απομόνωσης της, προχώρησε σε παράνομη πυρηνική δοκιμή, προκειμένου να εξαναγκάσει την Δύση να συναινέσει σε

[312] Ibid, p. 82
[313] Ibid, pp. 86 -87
[314] Coleman, Kevin, "*North Korea's cyber capabilities cause alarm*", Defense Systems, 18 Aug 2011. Available at: http://defensesystems.com/blogs/cyber-report/2011/08/north-korea-cyber-capabilities.aspx, accessed on Dec 2011
[315] Clarke & Knake, 2010: 27-28
[316] Ibid
[317] Ibid
[318] Ibid

συγκεκριμένα ανταλλάγματα. Όταν η ηγεσία της χώρας διαπίστωσε ότι αυτό δεν πρόκειται να συμβεί[319], προχώρησε στις 4 Ιουλίου του 2009 (εθνική εορτή ΗΠΑ) σε δοκιμαστικές εκτοξεύσεις βαλλιστικών πυραύλων μικρής εμβέλειας (εντός της βόρειο – κορεατικής επικράτειας) και σε κυβερνοεπιθέσεις DDoS κατά αμερικανικών και νότιο – κορεατικών κυβερνητικών ιστοσελίδων και διεθνών εταιρειών.

Οι κυβερνοεπιθέσεις έλαβαν χώρα μέσω ενός δικτύου «μολυσμένων» Η/Υ – Botnet – σε τρεις φάσεις και σχεδιάστηκαν από το "Unit 110". Κατά την 1η φάση (4 – 9 Ιουλίου) διάφορες αμερικανικές ιστοσελίδες δέχθηκαν καταιγισμό ερωτήσεων (1 εκατομμύριο ερωτήσεις ανά δευτερόλεπτο) από ένα "Botnet" 40.000 «μολυσμένων» Η/Υ, με αποτέλεσμα οι ιστοσελίδες αυτές να βγουν εκτός ενεργείας. Το Botnet είχε προκύψει με υπαιτιότητα της βόρειο – κορεατικής πλευράς μέσω αποστολής κακόβουλου λογισμικού σε 40.000 Η/Υ σε όλο τον κόσμο. Στόχοι του "Botnet" ήταν το Υπουργείο Οικονομικών, οι Υπηρεσίες Πληροφοριών, η Ομοσπονδιακή Επιτροπή Εμπορίου, ο Λευκός Οίκος, το χρηματιστήριο και η εφημερίδα Washington Post[320]. Η 2η φάση (9 Ιουλίου) των επιθέσεων DDoS εκδηλώθηκε με επιτυχία κατά των νότιο – κορεατικών κυβερνητικών ιστοσελίδων, τραπεζών και μιας εταιρείας παροχής ασφάλειας στο διαδίκτυο. Αυτή την φορά χρησιμοποιήθηκε μια τροποποιημένη έκδοση του προηγούμενου κακόβουλου λογισμικού και ένα Botnet 30.000 – 60.000 «μολυσμένων» Η/Υ[321]. Η 3η και τελευταία φάση έγινε στις 10 Ιουλίου μέσω ενός Botnet 166.000 «μολυσμένων» Η/Υ από 74 χώρες και είχε ως στόχο την Ν. Κορέα, αλλά τελικά η απειλή αντιμετωπίστηκε επαρκώς[322].

Σύμφωνα με αναλυτές, η Β. Κορέα προχώρησε στις υπόψη κυβερνοεπιθέσεις προκειμένου από την μια μεριά να δείξει στις ΗΠΑ ότι μπορεί να τις βλάψει στον κυβερνοχώρο, ενώ από την άλλη μεριά για να εξετάσει τον αναγκαίο αριθμό «μολυσμένων» Η/Υ που απαιτούνται για να εξουδετερώσουν το σύστημα διοίκησης και ελέγχου της Ν. Κορέας[323]. Με τον τρόπο αυτό, σε μια ενδεχόμενη σύγκρουση με την Ν. Κορέα, η Β. Κορέα θα γνώριζε πως θα μπορούσε να παρεμποδίσει τις ΗΠΑ να λάβουν τις απαραίτητες πληροφορίες για την υποστήριξη των στρατευμάτων που διατηρούν στην Ν. Κορέα.

[319] Οι ΗΠΑ τοποθέτησαν αμυντικούς πυραύλους στην Χαβάη τον Ιούνιο του 2009 και ανακοίνωσαν την διεξαγωγή άσκησης στον κυβερνοχώρο με την ονομασία "Cyber Storm" στην οποία θα συμμετείχαν η Ιαπωνία και η Ν. Κορέα. Η Β. Κορέα εξέλαβε την άσκηση αυτή ως προετοιμασία των ΗΠΑ και της Ν. Κορέας για εισβολή στο βόρειο – κορεατικό έδαφος.
[320] Clarke & Knake, 2010: 24
[321] Ibid
[322] Ibid
[323] Ibid, p.29

3.4.6 Ιράν

Το Ιράν, όπως και η Κίνα, μετά τους πολέμους στον Περσικό Κόλπο κατανόησε την αναγκαιότητα ενσωμάτωσης της τεχνολογίας πληροφορικής στο πεδίο της μάχης και χρηματοδότησε, μέσω των εσόδων του από τις εξαγωγές πετρελαίου, διάφορα σχετικά ερευνητικά προγράμματα, με την συνεργασία ιρανικών τεχνολογικών πανεπιστημίων. Μεταξύ αυτών, συγκαταλέγεται το πρόγραμμα ανάπτυξης δυνατοτήτων κυβερνοπολέμου. Παράλληλα, επεδίωξε την στρατιωτική συνεργασία με την Ρωσία[324], η οποία όπως προαναφέρθηκε έχει αναπτύξει σημαντικές δυνατότητες στις επιχειρήσεις στον κυβερνοχώρο. Ως αποτέλεσμα, από τις αρχές του 21ου αι. υπάρχουν αναφορές που καταδεικνύουν το Ιράν ως σοβαρή απειλή για εκδήλωση κυβερνοεπιθέσεων[325].

Μετά την υπόθεση Stuxnet (2009 - 2010) – η οποία θα αναλυθεί σε επόμενη ενότητα – το Ιράν αποφάσισε να εντατικοποιήσει τις προσπάθειες του για την ανάπτυξη σημαντικών δυνατοτήτων διεξαγωγής κυβερνοπολέμου[326]. Σύμφωνα με στοιχεία από ανοιχτές πηγές, οι δυνατότητες του Ιράν στον κυβερνοπόλεμο είναι ήδη σημαντικές, με τις επιθετικές του δυνατότητες να βρίσκονται σε πολύ καλό επίπεδο[327]. Οι ΕΔ δυνάμεις της χώρας διαδραματίζουν καθοριστικό ρόλο στην εφαρμογή τους (δυνατότητες). Μέχρι σήμερα η Μονάδα που είναι αρμόδια για κυβερνοπόλεμο υπάγεται στο Σώμα των Φρουρών της Επανάστασης[328]. Η Μονάδα αυτή αριθμεί περί τα 2.400 άτομα και διαχειρίζεται ετησίως 76 εκατομμύρια δολάρια για την ανάπτυξη των δυνατοτήτων της στον κυβερνοχώρο[329]. Όπως και οι προαναφερόμενες χώρες, το Ιράν απασχολεί ομάδες πολιτών hackers, προκειμένου να αυξήσει την δυναμική του στον κυβερνοχώρο. Η πιο γνωστή από αυτές είναι η ομάδα Iranian Cyber Army, η οποία συνεργάζεται με τους Φρουρούς της Επανάστασης[330]. Παράλληλα, για σκοπούς επιτήρησης του διαδικτύου[331], το Ιράν διαθέτει από το 2011 μια αστυνομική δύναμη

---

[324] Η στρατιωτική συνεργασία με την Ρωσία δεν αφορούσε μόνο στην πώληση ρωσικού στρατιωτικού εξοπλισμού προς το Ιράν, αλλά και στην παροχή τεχνογνωσίας, ιδιαίτερα σε τεχνολογίες αιχμής. Το Ιράν επεδίωξε και πέτυχε παρόμοια στρατιωτική συνεργασία με την Κίνα και την Ινδία.

[325] Billo & Chang, 2004: 62-64

[326] Kellogg, Amy, "*Iran is Recruiting Hacker Warriors for its Cyber Army to Fight Enemies*", 14/3/2011. Available at: http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/, accessed on May 2011

[327] Άρθρο με τίτλο: *"Iranian Cyber warfare Threat Assessment"*, 13/5/2010. Available at: http://www.cyberwarzone.com/content/iranian-cyber-warfare-threat-assessment, accessed on May 2010

[328] Το Σώμα των Φρουρών της Επανάστασης αποτελεί στρατιωτική δομή που δημιουργήθηκε μετά την ισλαμική επανάσταση στο Ιράν και έχει ως στόχο την προστασία του ισλαμικού συστήματος στην χώρα. Λειτουργεί παράλληλα με τις τακτικές ΕΔ και διαθέτει χερσαίες, ναυτικές και αεροπορικές δυνάμεις.

[329] Lewis & Timlin (2011), p.15

[330] Ibid

[331] Το Internet είναι αυστηρά ελεγχόμενο στο Ιράν. Μετά τα γεγονότα του 2009 (προεδρικές εκλογές) όπου οι Ιρανοί αντιπολιτευόμενοι χρησιμοποίησαν τα social media προκειμένου να οργανώσουν διαδηλώσεις, η κυβέρνηση της χώρας προχώρησε στην σύσταση ειδική μονάδας της αστυνομίας για την επιτήρηση του Internet.

γνωστή ως Iranian Cyber Police Unit[332]. Όπως ανακοινώθηκε τον Ιούνιο του 2011, αποτελεί στόχο της κυβέρνησης η δημιουργία μια Διοίκησης Κυβερνοπολέμου (Cyber Command), η οποία θα υπάγεται στις ιρανικές ΕΔ, θα έχει αμυντικό χαρακτήρα και θα συντονίζει τις επιχειρήσεις στον κυβερνοχώρο[333].

Θα πρέπει να σημειωθεί ότι το Ιράν δεν έχει κάνει δημόσια γνωστές τις δυνατότητες τον κυβερνοπόλεμο, πλην ελαχίστων εξαιρέσεων. Χαρακτηριστικά αναφέρεται ότι, τον Δεκέμβριο του 2009 η ομάδα Iranian Cyber Army κατάφερε να επιτύχει ανακατεύθυνση των χρηστών της ιστοσελίδας κοινωνικής δικτύωσης (social media) "Twitter.com" σε ιστοσελίδες που περιείχαν αντιαμερικανικά συνθήματα[334]. Επίσης, τον Ιανουάριο του 2010 η κινεζική ιστοσελίδα Baidu - η οποία αποτελεί το αντίπαλο δέος στην Κίνα για την ιστοσελίδα "Google.cn" - τέθηκε εκτός λειτουργίας για 4 ώρες. Όπως αναφέρθηκε, υπεύθυνοι ήταν οι hackers του Iranian Cyber Army, οι οποίοι διενήργησαν web defacement στην ιστοσελίδα Baidu και ανάρτησαν στην θέση της την σημαία του Ιράν, ένα θρυμματισμένο «Αστέρι του Δαυίδ» και την επιγραφή Iranian Cyber Army. Αν και η κινεζική πλευρά εξέφρασε σκεπτικισμό για το αν οι Ιρανοί hackers βρίσκονταν πίσω από την επίθεση ή κάποια χώρα της Δύσης, η κινεζική ομάδα hacker Honker Union προχώρησε σε web defacement ορισμένων ιρανικών ιστοσελίδων και στην θέση τους ανάρτησε την κινεζική σημαία με διάφορες κινεζικές ρήσεις[335].

Η πιο πρόσφατη εκδήλωση ιρανικής επιθετικής ενέργειας στον κυβερνοχώρο είναι η υπόθεση της αναγκαστικής προσγείωσης ενός αμερικανικού UAV RQ-170 Sentinel[336] στο Ιράν στις 4 Δεκέμβριου του 2011. Σύμφωνα με την ιρανική πλευρά, το αμερικανικό UAV εκτελούσε κατασκοπευτική πτήση άνωθεν του Ιράν, όταν οι ιρανικές ΕΔ κατάφεραν με συνδυασμό τεχνικών κυβερνοπολέμου και ηλεκτρονικού πολέμου να πάρουν τον έλεγχο πτήσης του RQ-170 και να το προσγειώσουν σε ιρανικό έδαφος[337]. Αν και η υπόθεση ακόμα διερευνάται, φήμες αναφέρουν ότι το Ιράν είχε προμηθευτεί κατάλληλο εξοπλισμό ηλεκτρονικών παρεμβολών από την Ρωσία[338] και κατάφερε να επέμβει (hacking) στο σύστημα ναυτιλίας GPS του UAV[339].

---

[332] Lewis & Timlin (2011), p.15
[333] Ibid
[334] Michael, Alex, "*Cyber Probing: The Politicisation of Virtual Attack*", p.17
[335] Ibid
[336] Το UAV RQ-170 Sentinel θεωρείται ιδιαίτερα εξελιγμένο μη επανδρωμένο αεροσκάφος, το οποίο είναι αόρατο στα ραντάρ (stealth).
[337] Jennings, Gareth & Wasserbly, Daniel, "*Iran puts captured US UAV on show*", Jane's Defense Weekly, Volume 48, Issue 50, 14/12/11
[338] Ibid
[339] Άρθρο "*How Iran hacked super-secret CIA stealth drone*", Russia Today, 16/12/11. Available at: http://rt.com/usa/news/iran-drone-hack-stealth-943/, accessed on 22 Jan 2012

3.5 Σημαντικές Περιπτώσεις Κυβερνοεπιθέσεων

Στην συνέχεια θα γίνει αναφορά σε τρεις περιπτώσεις κυβερνοεπιθέσεων, οι οποίες, λόγω της πρωτοτυπίας τους, τράβηξαν το ενδιαφέρον της διεθνούς κοινότητας και κατέδειξαν τις μορφές που μπορεί να πάρει ο κυβερνοπόλεμος στην σύγχρονη εποχή. Η περίπτωση της Εσθονίας το 2007 φανέρωσε τον αρνητικό αντίκτυπο των κυβερνοεπιθέσεων DDoS πάνω στην οικονομική και κοινωνική λειτουργία μιας χώρας - στόχου, η οποία είναι εξαρτημένη από την τεχνολογία των Η/Υ και των επικοινωνιών (ICT: Information and Communications Technology). Τα γεγονότα στην Γεωργία το 2008, κατέδειξαν το πώς οι επιχειρήσεις στον κυβερνοχώρο δύναται να συμβάλλουν υποστηρικτικά στην διεξαγωγή των συμβατικών πολεμικών επιχειρήσεων (επιχειρησιακός κυβερνοπόλεμος), ενώ η περίπτωση του Stuxnet το 2009 - 2010 (Ιράν) τόνισε πως η ανάπτυξη και χρήση ενός κυβερνοόπλου ακριβείας δύναται να καταφέρει αυτό που επί χρόνια δεν μπορούσε να επιβάλει στο Ιράν η διεθνής κοινότητα, δηλ. το «πάγωμα» του πυρηνικού του προγράμματος.

3.5.1 Εσθονία 2007

Τα γεγονότα, που θα περιγραφούν στην συνέχεια, ξεκίνησαν με αφορμή την επικύρωση από το εσθονικό κοινοβούλιο τον Φεβρουάριο του 2007 του νομοσχεδίου “Forbidden Structures Law”[340], το οποίο αφορούσε στην καταστροφή εκείνων των μνημείων που καταδείκνυαν τα 50 χρόνια «κατοχής» της χώρας από την Σοβιετική Ένωση[341]. Με βάση το προαναφερθέν νομοσχέδιο, η κυβέρνηση της χώρας θα προχωρούσε στην μετακίνηση του χάλκινου αγάλματος του Στρατιώτη του Κόκκινου Στρατού[342], το οποίο είχε τοποθετηθεί από τους Σοβιετικούς στο κέντρο της εσθονικής πρωτεύουσας, μετά το πέρας του Β’ ΠΠ.

Το γεγονός αυτό προκάλεσε την έντονη αντίδραση των Ρώσων που διαβιούσαν στην Εσθονία αλλά και της ρωσικής κυβέρνησης, με συνέπεια ο Εσθονός Πρόεδρος να ασκήσει βέτο επί του νομοσχεδίου. Στην συνέχεια όμως, οι πιέσεις από τον εσθονικό λαό για την μετακίνηση του αγάλματος αυξήθηκαν, ενώ οι Ρώσοι εθνικιστές της Εσθονίας προχώρησαν σε περιφρούρηση του μνημείου, με αποτέλεσμα να ξεσπάσουν συγκρούσεις μεταξύ των εθνικιστικών ομάδων. Όταν μάλιστα, η κυβέρνηση της

[340] Clarke & Knake, 2010: 12

[341] Η ενσωμάτωση της χώρας στην ΕΣΣΔ μετά τον Β’ΠΠ εκλαμβάνονταν ως κατοχή από μεγάλη μερίδα του εσθονικού λαού.

[342] Το άγαλμα αυτό είχε στηθεί προκειμένου να υπενθυμίζει στον εσθονικό λαό την συμβολή της ΕΣΣΔ στην απελευθέρωση της Εσθονίας από τον γερμανικό ζυγό. Κάτω από το άγαλμα φυλάσσονταν τα οστά σοβιετικών στρατιωτών που έχασαν την ζωή τους στις μάχες για την απελευθέρωση της Εσθονίας. Θα πρέπει επίσης να αναφερθεί ότι κατά την διάρκεια της δεκαετίας του 1990 η εσθονική κυβέρνηση είχε προχωρήσει στην μετακίνηση άλλων σοβιετικών μνημείων, χωρίς να υπάρξει πρόβλημα.

Εσθονίας ανακοίνωσε στις αρχές Απριλίου την πρόθεση της για την έναρξη των εργασιών μετακίνησης του μνημείου, τα πνεύματα οξύνθηκαν και το μνημείο περιφρουρήθηκε από αστυνομικές δυνάμεις. Στις 26 Απριλίου και ενώ η κατάσταση ήταν ήδη τεταμένη, ξέσπασαν οδομαχίες στο Ταλίν μεταξύ Ρώσων και Εσθονών, με αποτέλεσμα ένας άνθρωπος να χάσει την ζωή του, 100 άτομα να τραυματιστούν και 1300 διαδηλωτές να συλληφθούν[343]. Παρόλα αυτά, κατά την διάρκεια της νύχτας στις 27 Απριλίου, η κυβέρνηση της Εσθονίας προχώρησε στην μετακίνηση του μνημείου[344], με αποτέλεσμα να ξεσπάσουν έντονες διαμαρτυρίες από την ρωσική εθνικιστική ομάδα Nashi, έξω από την εσθονική πρεσβεία στην Μόσχα[345]. Ταυτόχρονα, έλαβαν χώρα κυβερνοεπιθέσεις κατά εσθονικών ιστοσελίδων και ΜΜΕ.

Ο αντίκτυπος που είχαν οι κυβερνοεπιθέσεις στην Εσθονία ήταν μεγάλος, καθώς η χώρα ήταν ιδιαίτερα εξαρτημένη από την τεχνολογία της πληροφορικής και των επικοινωνιών, το Internet και τα δίκτυα των Η/Υ[346]. Το εσθονικό κράτος κατά την διάρκεια της δεκαετίας του 1990 είχε στραφεί προς την ψηφιακή τεχνολογία και την διασύνδεση των παρεχόμενων υπηρεσιών του, προκειμένου να μειώσει το κόστος των υπηρεσιών και να ικανοποιήσει τις ανάγκες του πληθυσμού της ιδιαίτερα αραιοκατοικημένης Εσθονίας[347]. Αν και το νομοθετικό πλαίσιο που κάλυπτε την παροχή ηλεκτρονικών υπηρεσιών στους Εσθονούς πολίτες θεσμοθετήθηκε επίσημα την περίοδο 2000 – 2002[348], η παροχή ηλεκτρονικών υπηρεσιών είχε ήδη ξεκινήσει από τις εσθονικές τράπεζες την δεκαετία του 1990, προκειμένου αυτές να κερδίσουν μεγάλο μερίδιο αγοράς από τις αραιοκατοικημένες περιοχές της χώρας[349]. Το εσθονικό κράτος προχώρησε στην δημιουργία ψηφιακών βάσεων δεδομένων και συστημάτων πληροφόρησης[350], ενώ οι δημόσιες και ιδιωτικές υπηρεσίες καθώς και οι βιομηχανίες υιοθέτησαν ηλεκτρονικές μεθόδους παροχής των υπηρεσιών τους[351]. Παράλληλα, δόθηκε έμφαση στην ανάπτυξη και χρήση ψηφιακών εφαρμογών που διευκολύνουν τις επικοινωνίες, όπως το γνωστό σε όλους Skype[352]. Ενδεικτικά αναφέρεται ότι το 2005 η ψηφοφορία για την εκλογή δημοτικών αρχών στην χώρα είχε γίνει μέσω Internet, ενώ

[343] Το κόστος από τις καταστροφές δημόσιας και ιδιωτικής περιουσίας κατά την διάρκεια των οδομαχιών στο Ταλίν υπολογίζεται στα 4,5 εκατομμύρια ευρώ.
[344] Το σοβιετικό μνημείο τοποθετήθηκε τελικά στο στρατιωτικό κοιμητήριο του Ταλίν στις 30 Απριλίου.
[345] Οι Nashi επιτέθηκαν εναντίον του Εσθονού Πρέσβη.
[346] Clarke & Knake, 2010: 13
[347] Tikk, Eneken, Kaska, Kadri & Vihul Liis, *International Cyber Incidents: Legal Considerations* (CCDCOE, Tallinn 2010), p. 16
[348] Από το 2000 οι ψηφιακές υπογραφές είχαν την ίδια εγκυρότητα για το εσθονικό κράτος με τις γραπτές υπογραφές.
[349] Ενδεικτικά αναφέρεται ότι το 2007 το 95% των τραπεζικών συναλλαγών γινόταν ηλεκτρονικά.
[350] Σύμφωνα με τους Tikk, Kaska και Vihul, το 2007 ο δημόσιος τομέας της Εσθονίας διέθετε 150 ψηφιακά συστήματα πληροφοριών που παρείχαν περίπου 1000 διαφορετικές ηλεκτρονικές υπηρεσίες. Επίσης, πάνω από 450 δημόσιοι οργανισμοί, 30.000 επιχειρηματίες και μεγάλος αριθμός πολιτών χρησιμοποιούσαν σε καθημερινή βάση το portal του εσθονικού κράτους "eesti.ee" προκειμένου να πραγματοποιήσουν τις συναλλαγές τους με τους διάφορους δημόσιους φορείς.
[351] Το 2008 η υποβολή των φορολογικών δηλώσεων με ηλεκτρονικό τρόπο έφτασε στο 80%.
[352] Tikk et al, 2010: 17

το 2007 τα αποτελέσματα των εξετάσεων της δευτεροβάθμιας εκπαίδευσης είχαν κοινοποιηθεί μέσω SMS[353]. Την ίδια χρονιά (2007), το 98% της εσθονικής επικράτειας είχε πρόσβαση στο Internet, ενώ η χρήση κινητής τηλεφωνίας άγγιζε το 100%. Επιπλέον, το 50% του πληθυσμού σε ηλικίες από 16-74 ετών έκανε χρήση του διαδικτύου, ενώ το 53% των νοικοκυριών διέθεταν έναν Η/Υ.

Οι κυβερνοεπιθέσεις πραγματοποιήθηκαν σε 2 διακριτές χρονικές φάσεις, οι οποίες χαρακτηρίστηκαν από διαφορετικά επίπεδα έντασης και τεχνολογικής εξειδίκευσης. Οι κυριότερες μέθοδοι που χρησιμοποιήθηκαν από τους επιτιθέμενους ήταν επιθέσεις κορεσμού κατά των εσθονικών servers (DDoS attacks), αλλαγές στο περιεχόμενο ιστοσελίδων χωρίς εξουσιοδότηση (web defacement), εκούσια κατεύθυνση των χρηστών των δικτύων σε μη επιθυμητές περιοχές των δικτύων (DNS Server attack) και καταιγισμός ανεπιθύμητων ηλεκτρονικών μηνυμάτων (email spamming)[354]. Χαρακτηριστικά αναφέρεται ότι σε μια περίπτωση web defacement, ένας hacker ανάρτησε στην ιστοσελίδα του ηγετικού πολιτικού σχηματισμού της Εσθονίας “Reform Party” μια πλαστή απολογία υπογεγραμμένη από τον Εσθονό Πρωθυπουργό, η οποία αφορούσε στην μετακίνηση του χάλκινου αγάλματος του Στρατιώτη του Κόκκινου Στρατού. Το ενδιαφέρον στοιχείο αυτής της δράσης ήταν ότι η απολογία ήταν γραμμένη στην ρώσικη γλώσσα.

Στόχοι των κυβερνοεπιθέσεων ήταν τα δημόσια και ιδιωτικά κανάλια διανομής πληροφόρησης, η εσθονική υποδομή για το Internet (π.χ εταιρείες παροχής Internet και κινητής τηλεφωνίας), οι κυβερνητικές και πολιτικές ιστοσελίδες, οι ηλεκτρονικές υπηρεσίες του ιδιωτικού τομέα (π.χ ιστοσελίδες τραπεζών και επιχειρήσεων) και κάποιοι άλλοι τυχαίοι στόχοι (π.χ γραμμή έκτακτης ανάγκης 112). Στις κυβερνητικές και πολιτικές ιστοσελίδες που χτυπήθηκαν συμπεριλαμβάνονται αυτές της κυβέρνησης, του Προέδρου της χώρας, του Πρωθυπουργού, του Κοινοβουλίου, της κρατικής υπηρεσίας ελέγχων, των Υπουργείων, των κρατικών υπηρεσιών (πχ Συμβούλιο Αστυνομίας) και του ηγετικού πολιτικού σχηματισμού “Reform Party”. Όσον αφορά στις εμπορικές υπηρεσίες που στοχοποιήθηκαν, τονίζεται ότι, το μεγαλύτερο μέρος των επιθέσεων εστίασε στις διαδικασίες e-banking των 2 σημαντικών τραπεζών της χώρας (Hansapank και SEB Eesti Uhispank), οι οποίες συγκέντρωναν το 75 – 80% της συνολικής τραπεζικής αγοράς. Επιπρόσθετα, σημειώνεται ότι οι βάσεις δεδομένων του δημόσιου και ιδιωτικού τομέα, αλλά και οι κρίσιμες υποδομές των μεταφορών και της ενέργειας δεν στοχοποιήθηκαν από τους δράστες των κυβερνοεπιθέσεων.

Η 1η Φάση των κυβερνοεπιθέσεων έλαβε χώρα από τις 27 – 29/4 και εστίασε στις κυβερνητικές ιστοσελίδες και στα ΜΜΕ. Βασίστηκε κυρίως σε απλές μεθόδους

[353] Ibid, p. 18
[354] Tikk et al, 2010: 20- 21

κυβερνοεπιθέσεων, ενώ διαπιστώθηκε λειτουργία forum στο διαδίκτυο, όπου στην ρωσική γλώσσα δίνονταν οδηγίες αλλά και κυβερνοεργαλεία (Cyber Tools) για την εκδήλωση επιθέσεων DoS[355] (Denial of Service). Λόγω της απλότητας τους, της έλλειψης σημαντικού συντονισμού και του έντονου συναισθηματικού στοιχείου που έφεραν οι επιθέσεις αυτές, χαρακτηρίστηκαν ως κυβερνοδιαδηλώσεις (Cyber Riots) και ταιριάζουν με την έννοια του Hactivism που έχει αναφερθεί νωρίτερα. Σε γενικές γραμμές οι επιθέσεις αυτές αντιμετωπίστηκαν με επιτυχία από το εσθονικό κράτος.

Η 2η Φάση των επιθέσεων έλαβε χώρα από τις 30/4 έως τις 18/5 και περιλάμβανε καλύτερα συντονισμένες και πιο εξειδικευμένες επιθέσεις, οι οποίες πραγματοποιήθηκαν σε 4 διαφορετικά κύματα. Όπως διαπιστώθηκε, χρησιμοποιήθηκαν forums στο Internet, όπου δίνονταν οδηγίες για τις κυβερνοεπιθέσεις και λίστες στόχων, ενώ έγινε ευρεία χρήση των Botnets. Αν και πολλές από αυτές τις επιθέσεις αντιμετωπίστηκαν σε ικανοποιητικό βαθμό, υπήρξαν πολλές ιστοσελίδες που τέθηκαν εκτός ενεργείας για κάποιο χρονικό διάστημα. Αναλυτικότερα :

α. Το 1ο κύμα επιθέσεων έλαβε χώρα στις 4/5 και περιελάμβανε κυβερνοεπιθέσεις DDoS με ιδιαίτερη ένταση και συγκεκριμένη εστίαση κατά συγκεκριμένων ιστοσελίδων. Οι επιτιθέμενοι μπόρεσαν να αποκρύψουν τις ταυτότητες τους είτε μέσα από τα botnets, είτε κατευθύνοντας τις επιθέσεις τους μέσω servers που εδράζονταν σε άλλα κράτη.

β. Το 2ο κύμα πραγματοποιήθηκε από τις 8 – 11/5 με την συνολική ένταση των επιθέσεων να μην ξεπερνά την αντίστοιχη των προηγούμενων εβδομάδων. Ωστόσο, την πρώτη ημέρα (8/5), οι κυβερνοεπιθέσεις DDoS έφθασαν στο 150% σε σχέση με το 1ο κύμα, ενώ στις 9/5 οι επιθέσεις κατάφεραν να θέσουν εκτός λειτουργίας τουλάχιστον 58 ιστοσελίδες. Οι επιθέσεις εστιάστηκαν κατά κυβερνητικών ιστοσελίδων και εμπορικών τραπεζών. Ενδεικτικά αναφέρεται ότι, η τράπεζα Hansapank – η μεγαλύτερη εμπορική τράπεζα της Εσθονίας - παρέμεινε κλειστή για μικρά χρονικά διαστήματα στις 9 και 10/5.

γ. Το 3ο κύμα έλαβε χώρα στις 15/5 και περιελάμβανε κυβερνοεπιθέσεις DDoS μέσω ενός Botnet 85.000 Η/Υ. Οι στόχοι σε αυτό το κύμα ήταν οι ίδιοι με το 2ο κύμα, αλλά η επίθεση αυτή δεν είχε τα αναμενόμενα αποτελέσματα, καθώς οι ομάδες αντιμετώπισης κυβερνοαπειλών της Εσθονίας είχαν φροντίσει να διευρύνουν τις ικανότητες επικοινωνίας των δικτύων. Η μόνη ουσιαστική απώλεια ήταν ότι η

[355] Μια μέθοδος που χρησιμοποιήθηκε ήταν η αποστολή συνεχών ερωτήσεων προς τους servers που είχαν αποθηκευμένες τις ιστοσελίδες – στόχους προκειμένου να διαγνωστεί η διαθεσιμότητα τους στο δίκτυο (μέθοδος Ping).

ιστοσελίδα της SEB Eesti Uhispank – 2η σε μέγεθος εμπορική τράπεζα στην χώρα – τέθηκε εκτός λειτουργίας για μικρό χρονικό διάστημα.

δ. Το 4ο κύμα των επιθέσεων πραγματοποιήθηκε στις 18/5. Περιλάμβανε κυβερνοεπιθέσεις DDoS και στόχευε κυρίως κυβερνητικές ιστοσελίδες.

Κατά την διάρκεια των επιθέσεων, η Εσθονία προσπάθησε να εξισορροπήσει τις κυβερνοαπειλές χρησιμοποιώντας τις ομάδες CERT (Computer Emergency Response Team) και πληθώρα ειδικών στην IT τεχνολογία. Παράλληλα, δέχθηκε βοήθεια από την ΕΕ και το ΝΑΤΟ, οι οποίοι απέστειλαν ειδικούς στην IT τεχνολογία για να συνδράμουν το έργο των εσθονικών ομάδων CERT. Αξίζει να σημειωθεί ότι, οι ΗΠΑ βοήθησαν στην ανεύρεση των πηγών των κυβερνοεπιθέσεων και την επιτυχή απενεργοποίηση τους, γεγονός που κατέδειξε μέρος των δυνατοτήτων των ΗΠΑ στον κυβερνοχώρο. Σε γενικές γραμμές θα μπορούσε να ειπωθεί ότι με την εμπλοκή του διεθνούς παράγοντα στο πρόβλημα της Εσθονίας, οι κυβερνοεπιθέσεις μειώθηκαν δραστικά.

Μετά το πέρας των κυβερνοεπιθέσεων και έπειτα από διενέργεια έρευνας για το περιστατικό διαπιστώθηκαν τα παρακάτω σημαντικά στοιχεία:

α. Οι επιθέσεις είχαν σημαντικό αντίκτυπο στην οικονομική και κοινωνική λειτουργία της χώρας, καθώς χρειάστηκε να αποσυνδεθεί από τον παγκόσμιο ιστό (WWW), προκειμένου να επιλύσει τα προβλήματα από τις κυβερνοεπιθέσεις. Οι Εσθονοί είχαν μάθει να ζουν μέσα από το διαδίκτυο. Στο σύνολο τους, οι συναλλαγές με δημόσιους και ιδιωτικούς φορείς λάμβαναν χώρα μέσα από το internet. Η παροχή ενημέρωσης στο εσωτερικό αλλά και στο εξωτερικό γινόταν επίσης μέσα από το διαδίκτυο. Επιπρόσθετα, οποιοσδήποτε βρίσκονταν εκτός της εσθονικής επικράτειας δεν μπορούσε να χρησιμοποιήσει τις ψηφιακές διευκολύνσεις της χώρας (π.χ ΜΜΕ, e-banking). Αν και δεν κατέστη δυνατόν να υπολογιστεί με ακρίβεια ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων στην Εσθονία, εκτιμάται ότι για μια μόνο ώρα διακοπής της λειτουργίας της ιστοσελίδας μιας εσθονικής τράπεζας, οι απώλειες της έφθαναν το 1 εκατομμύριο δολάρια[356].

β. Το υπάρχον εσθονικό νομικό πλαίσιο δεν ήταν κατάλληλα ενημερωμένο για την αντιμετώπιση των ανωτέρω κυβερνοεπιθέσεων. Υπήρχαν διαδικαστικά προβλήματα εφαρμογής του νόμου και αλληλοεπικάλυψη δικαιοδοσιών. Σε διεθνές επίπεδο, έγινε προσπάθεια από την εσθονική πλευρά να χαρακτηριστούν οι παραπάνω κυβερνοεπιθέσεις ως στρατιωτική δραστηριότητα, βάσει της οποίας μπορεί να γίνει επίκληση του άρθρου 5 της ιδρυτικής Συνθήκης του ΝΑΤΟ, κάτι το οποίο δεν

[356] Tikk et al, 2010: 22, 24 - 25

έγινε αποδεκτό (από το ΝΑΤΟ). Οι κυβερνοεπιθέσεις αντιμετωπίστηκαν τελικά ως περιπτώσεις κυβερνοεγκλήματος[357].

γ. Η πληθώρα των κυβερνοεπιθέσεων καταδείκνυε ότι αυτές προέρχονταν από το εξωτερικό. Αν και χρησιμοποιήθηκαν Η/Υ που βρίσκονταν σε 178 χώρες, ο συντονισμός τους φαίνονταν ότι προέρχονταν από την ρωσική επικράτεια. Κανείς ωστόσο, δεν μπορεί να ισχυριστεί ότι υπάρχουν αποδείξεις που να ενοχοποιούν την ρωσική κυβέρνηση. Παρόλα αυτά, αξίζει να σημειωθεί ότι, στις 27 Απριλίου 2007 το ηγετικό στέλεχος των Nashi, Konstantin Goloskokov παραδέχθηκε την εμπλοκή της ομάδας του στα γεγονότα των κυβερνοεπιθέσεων[358]. Ο Goloskokov ήταν βοηθός του αξιωματούχου της ρωσικής Δούμας (κοινοβούλιο) και μέλους του κυβερνητικού σχηματισμού, Sergei Markov, ο οποίος τον Μάρτιο του 2009 παραδέχτηκε δημόσια ότι οι κυβερνοεπιθέσεις ξεκίνησαν από τον βοηθό του και τους Nashi[359].

δ. Η ρωσική κυβέρνηση αρνήθηκε οποιαδήποτε εμπλοκή με τις κυβερνοεπιθέσεις και υποστήριξε ότι αυτές οφείλονταν σε ομάδες εθνικιστών, με τους οποίους δεν είχε καμία σχέση. Παράλληλα, όταν της ζητήθηκε από την εσθονική πλευρά, η παροχή δικαστικής συνδρομής για την περαιτέρω διερεύνηση της υπόθεσης και την εύρεση των υπευθύνων, η Ρωσία το αρνήθηκε, επικαλούμενη την έννοια της εθνικής κυριαρχίας[360].

Μετά από όλα αυτά, η Εσθονία προχώρησε στην εκπόνηση Στρατηγικής για την Ασφάλεια στον κυβερνοχώρο, ενώ το ΝΑΤΟ ίδρυσε στις αρχές του 2008 το συμμαχικό κέντρο κυβερνοάμυνας, γνωστό ως CCDCOE (Cooperative Cyber Defence Center of Excellence) στην εσθονική πρωτεύουσα. Αν και η Εσθονία υποστήριξε από την πρώτη στιγμή ότι η Ρωσία ήταν πίσω από τις κυβερνοεπιθέσεις, δεν είχε απτές αποδείξεις και δεν προέβη σε αντίποινα κατά της Ρωσίας.

3.5.2 Γεωργία 2008

Οι σχέσεις της Γεωργίας με την Ρωσία την τελευταία 20ετία χαρακτηρίζονται γενικά ως συγκρουσιακές. Κατά την προαναφερθείσα περίοδο το κύριο σημείο τριβής μεταξύ των 2 χωρών ήταν και εξακολουθεί να είναι η ρωσική υποστήριξη προς στις αποσχισθείσες περιοχές της Ν. Οσσετίας και της Αμπχαζίας. Στα τέλη του Ιουλίου του 2008 σημειώθηκαν ένοπλες συγκρούσεις μεταξύ Γεωργιανών και Νότιο – Οσσετών. Οι

[357] Ibid, pp. 26 – 27. Αξίζει να σημειωθεί ότι οι εσθονικές Αρχές κατάφεραν να φέρουν ενώπιον της Δικαιοσύνης μόνο έναν νεαρό Εσθονό φοιτητή, ρωσικής καταγωγής, ο οποίος είχε εκδηλώσει κυβερνοεπιθέσεις κατά της ιστοσελίδας του ηγετικού πολιτικού σχηματισμού “Reform Party”. Στον νεαρό Εσθονό επιβλήθηκε πρόστιμο ύψους 1350 δολ.
[358] Carr, 2010: 3
[359] Ibid, p. 118
[360] Clarke & Knake, 2010: 15 - 16

συγκρούσεις εντάθηκαν την 1η εβδομάδα του Αυγούστου, με τους Γεωργιανούς να επιχειρούν βομβαρδισμό της πρωτεύουσας της Ν. Οσσετίας (Τσκινβάλι) και εισβολή στην αποσχισθείσα περιοχή στις 7 Αυγούστου[361]. Η αντίδραση της Ρωσίας ήταν άμεση και στις 8/8 οι ρωσικές ΕΔ εκδίωξαν από την Ν. Οσσετία τους Γεωργιανούς και δημιούργησαν μια ζώνη προστασίας – επί γεωργιανού εδάφους – γύρω από την Ν. Οσσετία. Κατά αντιστοιχία, οι Αμπχάζιοι εκδίωξαν τους Γεωργιανούς που υπήρχαν στην περιοχή τους και οι Ρώσοι δημιούργησαν μια ζώνη προστασίας – επί γεωργιανού εδάφους – γύρω από την Αμπχαζία. Η κρίση ολοκληρώθηκε μετά από λίγες ημέρες με την αποχώρηση των ρωσικών στρατευμάτων από το γεωργιανό έδαφος και την ρωσική αναγνώριση της αυτονομίας των 2 παραπάνω περιοχών[362].

Αυτό που έχει ιδιαίτερη σημασία στην παραπάνω διένεξη είναι ότι, πριν από το ξέσπασμα της ένοπλης σύγκρουσης και καθόλη τη διάρκεια της, έλαβαν χώρα κυβερνοεπιθέσεις κατά γεωργιανών στόχων[363]. Σε αντίθεση με την Εσθονία, η Γεωργία δεν είχε σημαντικές πληροφοριακές υποδομές. Ενδεικτικά αναφέρεται ότι το 2007, οι χρήστες του Internet στην χώρα αντιστοιχούσαν σε ποσοστό 7%, ενώ το αντίστοιχο ποσοστό στην Εσθονία ήταν 57%[364]. Το μειονέκτημα της Γεωργίας ήταν ότι η πρόσβαση της στο διαδίκτυο γίνονταν μόνο από ξηράς και κυρίως μέσω Ρωσίας και Τουρκίας[365]. Θα πρέπει επίσης να σημειωθεί ότι την περίοδο που ξέσπασε η ένοπλη σύγκρουση, είχε ήδη ξεκινήσει η τοποθέτηση υποθαλάσσιου καλωδίου οπτικών ινών στην Μαύρη θάλασσα, με το οποίο η Γεωργία θα αποκτούσε ψηφιακή πρόσβαση στην δυτική Ευρώπη. Ωστόσο, το έργο δεν ήταν διαθέσιμο την περίοδο της κρίσης. Επιπλέον, η Γεωργία διέθετε 5 εταιρείες παροχής υπηρεσιών Internet (ISPs), με την μία εξ αυτών (Caucasus Online) να συγκεντρώνει το 90% της αγοράς[366], γεγονός που καθιστούσε την γεωργιανή πλευρά ιδιαίτερα ευάλωτη σε περίπτωση που αυτή η εταιρεία έπαυε να λειτουργεί.

Η πρώτη κυβερνοεπίθεση πραγματοποιήθηκε στις 19/7 και είχε στόχο την ιστοσελίδα του Προέδρου της χώρας Saakashvili. Ήταν κυβερνοεπίθεση DDoS και είχε ως αποτέλεσμα να τεθεί εκτός λειτουργίας η προεδρική ιστοσελίδα για τουλάχιστον 24 ώρες. Ωστόσο, το κύριο μέρος των κυβερνοεπιθέσεων έλαβε χώρα από τις 8/8, δηλ. την ημέρα που ξεκίνησαν οι συμβατικές επιχειρήσεις, με αποτέλεσμα οι ιστοσελίδες

[361] Clarke & Knake, 2010: 18
[362] Ibid
[363] Τα γεγονότα στην Γεωργία το 2008 (κυβερνοεπιθέσεις) εντάσσονται στο πλαίσιο του επιχειρησιακού κυβερνοπολέμου, παρόλο που δεν έχει αποδειχθεί μέχρι σήμερα η διασύνδεση του επίσημου ρωσικού κράτους με αυτά.
[364] Tikk et al, 2010 : 68
[365] Το μεγαλύτερο ποσοστό πρόσβασης στο Internet καλύπτονταν από την Ρωσία. Άλλα σημεία πρόσβασης στο Internet για την Γεωργία ήταν η Αρμενία και το Αζερμπαϊτζάν, που ήταν εξαρτημένα από την Ρωσία.
[366] Tikk et al, 2010: 69

που στοχοποιούνταν να παραμένουν εκτός λειτουργίας για μεγάλο χρονικό διάστημα. Οι μέθοδοι των κυβερνοεπιθέσεων που χρησιμοποιήθηκαν ήταν παρόμοιες με αυτές που έλαβαν χώρα στην Εσθονία. Η ουσιαστική τους διαφορά ήταν ότι σε αυτές τις κυβερνοεπιθέσεις ο συντονισμός των hackers διαφάνηκε από την αρχή, ενώ στην περίπτωση της Εσθονίας, ο συντονισμός υπήρξε στην δεύτερη φάση των επιθέσεων. Αναλυτικότερα, το χρονοδιάγραμμα των κυβερνοεπιθέσεων είχε ως εξής :

α. Στις 8/8, στοχοποιήθηκαν οι ιστοσελίδες της Προεδρίας, της κυβέρνησης, του ΥΠΕΞ και του ΥΠΑΜ, των ειδησεογραφικών πρακτορείων της χώρας, καθώς και μη γεωργιανές ιστοσελίδες που ήταν φιλικά προσκείμενες προς το γεωργιανό καθεστώς.

β. Στις 9/8, οι κυβερνοεπιθέσεις εστίασαν στην μεγαλύτερη εμπορική τράπεζα της χώρας, TBC. Λόγω του ανωτέρω γεγονότος διατάχθηκε η παύση λειτουργίας των servers του γεωργιανού τραπεζικού τομέα, προκειμένου να αποφευχθεί η υπεξαίρεση κρίσιμων τραπεζικών δεδομένων ή κάποια άλλη ζημία στην ψηφιακή βάση του τραπεζικού συστήματος. Σε αντίδραση, οι hackers εξαπέλυσαν επιθέσεις κατά της διεθνούς τραπεζικής κοινότητας, με τρόπο ώστε αυτές να φαίνονται ότι προέρχονται από το γεωργιανό έδαφος. Αυτό είχε ως αποτέλεσμα η διεθνής τραπεζική κοινότητα να σταματήσει τις συναλλαγές με το γεωργιανό τραπεζικό σύστημα και αυτό με την σειρά του να παραλύσει[367].

γ. Στις 10/8, στοχοποιήθηκαν οι ιστοσελίδες του γεωργιανού κοινοβουλίου, της προεδρίας, καθώς και μη κυβερνητικών οργανισμών. Οι κυβερνοεπιθέσεις διαφάνηκε ότι προέρχονταν από server της Τουρκίας.

δ. Στις 11/8, η προεδρική ιστοσελίδα τέθηκε εκτός λειτουργίας, ενώ οι hackers τοποθέτησαν σε αυτήν (web defacement) φωτογραφίες του Προέδρου Saakashvili και του Hitler, προσπαθώντας να παρομοιάσουν τον Γεωργιανό Πρόεδρο με τον Hitler. Στοχοποιήθηκαν επίσης, μερικές εμπορικές ιστοσελίδες, ενώ οι κυβερνητικές ιστοσελίδες που είχαν χτυπηθεί τις προηγούμενες μέρες παρέμεναν εκτός λειτουργίας. Σημειώνεται ότι, το γεωργιανό ΥΠΕΞ εξέδωσε ανακοίνωση σε blog, όπου φιλοξενούνταν, με την οποία κατηγορούσε την Ρωσία για διεξαγωγή κυβερνοπολέμου κατά της Γεωργίας.

ε. Τις επόμενες ημέρες οι κυβερνοεπιθέσεις συνεχίστηκαν με αμείωτη ένταση, ενώ στις 27/8 εκδηλώθηκαν οι τελευταίες επιθέσεις κατά του γεωργιανού ΥΠΕΞ. Από τις 28/8 οι επιθέσεις άρχισαν να αντιμετωπίζονται επαρκώς και να μειώνονται δραματικά σε αριθμό.

[367] Clarke & Knake, 2010: 20

Κοινός παρονομαστής στις κυβερνοεπιθέσεις ήταν ότι στην αρχή οι hackers επιδίδονταν σε web defacement των ιστοσελίδων που στοχοποιούσαν. Υπό το πλαίσιο αυτό, τοποθετήθηκαν φωτογραφίες του Προέδρου Saakashvili και του Hitler στις ιστοσελίδες της προεδρίας και του ΥΠΕΞ. Επίσης, στην ιστοσελίδα της εθνικής τράπεζας της Γεωργίας αναρτήθηκαν οι φωτογραφίες των δικτατόρων του 20ου αι, με τον Γεωργιανό πρόεδρο να βρίσκεται ανάμεσα τους. Θα πρέπει να σημειωθεί ακόμη ότι, οι hackers επιδόθηκαν σε web defacement σε αζέρικες ειδησεογραφικές ιστοσελίδες που κρατούσαν ουδέτερη ή φιλική στάση προς την Γεωργία κατά την διάρκεια της σύγκρουσης.

Το μεγαλύτερο μέρος των κυβερνοεπιθέσεων ήταν DDoS και είχαν ως σκοπό να θέσουν εκτός λειτουργίας της ιστοσελίδες που στοχοποιούσαν. Μεταξύ των στόχων ήταν διάφορα κυβερνητικά sites, οι ιστοσελίδες των γεωργιανών πρακτορείων ειδήσεων, η ιστοσελίδα της τράπεζας TBC – της μεγαλύτερη τράπεζας της χώρας – και η ιστοσελίδα των hackers της Γεωργίας[368]. Η μέση διάρκεια των επιθέσεων DDoS έφθανε τις 2 ώρες και 15 λεπτά, ενώ η μεγαλύτερη διάρκεια που καταγράφηκε ήταν 6 ώρες.

Επιπρόσθετα, λειτούργησαν στο διαδίκτυο ρωσικά blogs, forums & ιστοσελίδες, όπου δίδονταν οδηγίες και εργαλεία για κυβερνοεπιθέσεις, καθώς και λίστες στόχων. Σε αυτές τις λίστες περιλαμβάνονταν 36 ιστοσελίδες, μεταξύ των οποίων ήταν οι πρεσβείες των ΗΠΑ και του Ηνωμένου Βασιλείου στην Τιφλίδα, το γεωργιανό κοινοβούλιο, το ανώτατο δικαστήριο, το ΥΠΕΞ και διάφορα ΜΜΕ. Χαρακτηριστικά αναφέρεται η περίπτωση του forum “stopgeorgia.ru”, όπου παρέχονταν εργαλεία για επιθέσεις DDoS και λίστες στόχων για γεωργιανούς servers, χωρίς να δίνονται εντολές στα μέλη του forum για τον τρόπο επίθεσης στον στόχο επιλογής τους. Η επιλογή του τρόπου επίθεσης ήταν στην διακριτική ευχέρεια του κάθε μέλους και βασίζονταν στις δυνατότητες hacking που διέθετε[369].

Μια ακόμα μέθοδος που χρησιμοποιήθηκε, γνωστή από την περίπτωση της Εσθονίας ήταν το email spamming. Οι hackers προχώρησαν σε δημοσίευση των διευθύνσεων ηλεκτρονικού ταχυδρομείου των Γεωργιανών πολιτικών και αποστολή σε αυτούς ηλεκτρονικών μηνυμάτων με κακόβουλο λογισμικό. Εκμεταλλεύτηκαν με αυτόν τον τρόπο, την προσπάθεια που είχε κάνει στο παρελθόν η κυβέρνηση της χώρας να γίνει πιο προσιτή στους πολίτες, ανακοινώνοντας τις ηλεκτρονικές διευθύνσεις των πολιτικών.

---

[368] Παρά την επίθεση που δέχθηκαν, οι Γεωργιανοί μπόρεσαν να αντεπιτεθούν κατά ορισμένων ρωσικών ειδησεογραφικών ιστοσελίδων. Βλέπε Michael, Alex, “*Cyber Probing:* …..”

[369] Rios, Billy K., “*Sun Tzu was a Hacker: An Examination of the tactics and Operations from a Real World Cyber attack*”, στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009), p. 146

Προκειμένου να εξισορροπήσει τις κυβερνοαπειλές που δεχόταν, η γεωργιανή κυβέρνηση έκανε χρήση της ομάδας CERT που διαθέτει, ενώ δέχθηκε βοήθεια από τις αντίστοιχες ομάδες της Εσθονίας, της Γαλλίας και της Πολωνίας. Επιπλέον, η προεδρική ιστοσελίδα, η ιστοσελίδα του ΥΠΑΜ και η ιστοσελίδα του τηλεοπτικού καναλιού Rustavi2 (www.rustavi2.com) φιλοξενήθηκαν στις 9/8 από τον server της εταιρείας Tulip Systems, με έδρα την Ατλάντα των ΗΠΑ. Επίσης, η Πολωνία παραχώρησε τμήμα της ιστοσελίδας της πολωνικής προεδρίας, προκειμένου να αναρτώνται στον χώρο αυτό οι ανακοινώσεις της γεωργιανής κυβέρνησης, ενώ η κυβέρνηση της Εσθονίας φιλοξένησε σε εσθονικό server την ιστοσελίδα του γεωργιανού ΥΠΕΞ. Παράλληλα, το γεωργιανό ΥΠΕΞ μεταφέρθηκε σε blog της Google, κατόπιν συνεννόησης με την εταιρεία.

Πέραν των ανωτέρω, από την παρατήρηση των κυβερνοεπιθέσεων διαπιστώθηκαν τα εξής:

α. Έγινε ευρεία χρήση των botnets. Ο συντονισμός των επιθέσεων έγινε από Ρώσους hackers, ενώ η γλώσσα συντονισμού ήταν η ρωσική. Παρόλα αυτά, δεν υπάρχουν αποδείξεις για την διασύνδεση των hackers με το Κρεμλίνο. Ωστόσο, σύμφωνα με τον ειδικό σε θέματα κυβερνοπολέμου Jeffrey Carr, το επίπεδο της προετοιμασίας και της αναγνωριστικής προσπάθειας για το πεδίο της μάχης από τους Ρώσους hackers θα μπορούσε να γίνει μόνο με την συνεργασία του επίσημου ρωσικού κράτους ή με την συνεργασία των ρωσικών ΕΔ. Επιπλέον, υπήρξαν ενδείξεις για την δραστηριοποίηση του δικτύου κυβερνοεγκλήματος “Russian Business Network” (RBN) κατά την διάρκεια των γεγονότων, η οποία περιορίστηκε στην παροχή υπηρεσιών υποστήριξης προς τους hackers και όχι στην διεξαγωγή κυβερνοεπιθέσεων[370].

β. Αντικειμενικός σκοπός των κυβερνοεπιθέσεων ήταν να διακοπεί η παροχή πληροφόρησης των Γεωργιανών πολιτών αναφορικά με τις εξελίξεις της σύγκρουσης[371]. Η ροή πληροφόρησης από το επίσημο κράτος προς το εσωτερικό της χώρας αλλά και προς το εξωτερικό διακόπηκε[372]. Σημειώνεται ότι οι κυβερνοεπιθέσεις DDoS εστίασαν στους routers της Ρωσίας και της Τουρκίας, προκειμένου να αποκλειστεί η Γεωργία από το Internet. Με τον τρόπο αυτό, οι Γεωργιανοί έχασαν την πρόσβαση στην πληροφόρηση, ενώ δεν μπορούσαν να αποστείλουν ηλεκτρονικά μηνύματα στο εξωτερικό. Το γεγονός αυτό επηρέασε αρνητικά το ηθικό των Γεωργιανών, οι οποίοι δεν μπορούσαν να έχουν ενημέρωση για τις εξελίξεις στο εσωτερικό αλλά και για την στάση του διεθνούς παράγοντα στο γεωργιανό πρόβλημα.

[370] Tikk et al, 2010: 75
[371] Clarke & Knake, 2010: 18
[372] Η πρόσβαση των Γεωργιανών στα κανάλια BBC & CNN μπλοκαρίστηκε από τις κυβερνοεπιθέσεις.

γ. Λόγω των κυβερνοεπιθέσεων, η εθνική τράπεζα της Γεωργίας διέταξε στις 9/8 όλες τις υπόλοιπες τράπεζες να σταματήσουν να παρέχουν ηλεκτρονικές υπηρεσίες στους πελάτες τους. Η παύση αυτή διήρκησε 10 μέρες και είχε αρνητικό οικονομικό αντίκτυπο για την χώρα.

δ. Δεν ήταν εφικτό να υπολογιστεί ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων, καθώς αυτές έλαβαν χώρα παράλληλα με τις συμβατικές επιχειρήσεις, κατά την διάρκεια των οποίων καταστράφηκαν υποδομές ICT τεχνολογίας (Information and Communications Technology).

ε. Οι κυβερνοεπιθέσεις οδήγησαν σε παράλυση το σύστημα κινητής τηλεφωνίας της χώρας[373].

3.5.3 Ιράν 2009 - 2010 (Stuxnet)

Τον Ιούνιο του 2010 η λευκορωσική εταιρεία VirusBlockAda, η οποία εξειδικεύονταν στην ασφάλεια των Η/Υ, ανακάλυψε την ύπαρξη ενός κακόβουλου λογισμικού μέσα σε φορητές μνήμες Η/Υ (USB flash drives). Το υπόψη malware ονομάστηκε Stuxnet και παρουσίαζε αρκετές καινοτομίες στην αρχιτεκτονική του. Ο Stuxnet μπορούσε να παραμένει πρακτικά αόρατος στα λογισμικά αντιμετώπισης κυβερνοεπιθέσεων (τα γνωστά Anti-Virus), φρόντιζε από μόνος του για την αναπαραγωγή του και την διάδοση του στα δίκτυα των Η/Υ και επιτίθονταν σε συγκεκριμένο στόχο, όταν τον αναγνώριζε. Για τον λόγο αυτό, οι ειδικοί στην IT τεχνολογία τον χαρακτήρισαν ως τον πρώτο κατευθυνόμενο κυβερνοπύραυλο (guided cyber missile)[374]. Πέρα από αυτά τα χαρακτηριστικά, ο Stuxnet θεωρείται ως ιδιαίτερα μεγάλο και πολύπλοκο malware, το οποίο ήταν κρυπτογραφημένο[375], ενώ όταν χτυπούσε τον στόχο του, έδινε την εικόνα στα ψηφιακά συστήματα επιτήρησης ότι όλα βαίνουν καλώς, χωρίς να υφίσταται καμία ψηφιακή διαταραχή στον στόχο του[376]. Επομένως, ένας διαχειριστής δικτύου Η/Υ δεν μπορούσε να έχει κάποια προειδοποίηση για την έναρξη και την εξέλιξη της κυβερνοεπίθεσης.

Με την δημοσιοποίηση της είδησης για την δράση του Stuxnet ακολούθησαν ενδελεχείς έρευνες από πολλές εταιρείες που ασχολούνται με την ασφάλεια των Η/Υ. Τα πρώτα αποτελέσματα των ερευνών έδειξαν ότι είχε κατασκευαστεί για να

---

[373] Clarke & Knake, 2010: 20

[374] Clayton, Mark, *"Stuxnet malware is 'weapon' out to destroy….Iran's Bushehr nuclear plant?"*, the Christian Science Monitor, 21 Sep 2010. Available at: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, accessed on April 2011

[375] Ibid

[376] Broad, William J., Markoff, John & Sanger David E., *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay"*, the New York Times, 15/1/2011. Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all, accessed on 8/2/2012

προσβάλλει με μεγάλη ακρίβεια εξειδικευμένους βιομηχανικούς στόχους. Από τις έρευνες διαπιστώθηκε ακόμα ότι κατάφερε να «μολύνει» πάνω από 60.000 Η/Υ διαφόρων χωρών (Ινδία, Ινδονησία, Κίνα, Αζερμπαϊτζάν, Ν. Κορέα, Μαλαισία, ΗΠΑ, Η.Β, Αυστραλία, Φιλανδία και Γερμανία), εκ των οποίων οι περισσότεροι ήταν στο Ιράν[377].Η περαιτέρω διερεύνηση γύρω από την δραστηριότητα του κατέδειξε ότι το συγκεκριμένο malware είχε προσβάλει τα δίκτυα των Η/Υ που είχαν οι πυρηνικές εγκαταστάσεις του Ιράν[378].

Σύμφωνα μάλιστα με μελέτη της εταιρείας Symantec τον Σεπτέμβριο του 2010, η αρχική μόλυνση από τον Stuxnet έγινε στο Ιράν τον Ιούνιο του 2009[379] και στην συνέχεια διαδόθηκε στις υπόλοιπες χώρες[380]. Η επιβεβαίωση για την προσβολή των δικτύων Η/Υ των πυρηνικών εγκαταστάσεων του Ιράν έγινε από αξιωματούχους της χώρας, οι οποίοι κατέδειξαν την Δύση ως υπεύθυνη για το γεγονός. Συγκεκριμένα, τον Νοέμβριο του 2010, ο Πρόεδρος Αχμαντινεντζάντ παραδέχτηκε την διενέργεια κυβερνοεπιθέσεων με malware (το οποίο δεν κατονόμασε ως Stuxnet) κατά των φυγόκεντρων συσκευών στις ιρανικές πυρηνικές εγκαταστάσεις, τονίζοντας ωστόσο ότι, οι επιθέσεις αυτές δεν προξένησαν ιδιαίτερες ζημίες[381]. Στο ίδιο κλίμα κινήθηκαν και οι δηλώσεις του τότε επικεφαλής του ιρανικού Οργανισμού Ατομικής Ενέργειας, Ali Akbar Salehi, ο οποίος αν και παραδέχτηκε την διενέργεια κυβερνοεπιθέσεων, επεσήμανε ότι το Ιράν μπόρεσε να τις αντιμετωπίσει πριν αυτές να πάρουν διαστάσεις[382].

Αν και μέχρι σήμερα δεν υπάρχει απόλυτη συμφωνία για το ποιοι ήταν οι στόχοι του Stuxnet, οι περισσότερες απόψεις επικεντρώνονται γύρω από τις ιρανικές πυρηνικές εγκαταστάσεις της Natanz και του Bushehr[383]. Η ιδιαιτερότητα που εμφανίζουν οι συγκεκριμένες εγκαταστάσεις είναι ότι ο έλεγχος της λειτουργίας τους

---

[377] Farwell, James P. & Rohozinski Rafal *"Stuxnet and the Future of Cyber War",* Survival, 53:1, 23-40, 28/1/2011

[378] Καμία χώρα από αυτές που προσβλήθηκαν από τον Stuxnet δεν ανέφερε ζημίες στις βιομηχανικές της εγκαταστάσεις. Οι Ιρανοί αξιωματούχοι παραδέχτηκαν την κυβερνοεπίθεση από κακόβουλο λογισμικό στις πυρηνικές εγκαταστάσεις της χώρας, αλλά επεσήμαναν ότι το αντιμετώπισαν επαρκώς, χωρίς να προκληθούν σημαντικές ζημίες στις πυρηνικές εγκαταστάσεις. Βλέπε Shakarian, Paulo, *"Stuxnet: Cyberwar Revolution in Military Affairs"*, Small Wars Journal, p.4, 15/4/2011. Available at: http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf, accessed on April 2011

[379] Η δράση του Stuxnet εκτιμάται ότι είχε ξεκινήσει έναν χρόνο πριν από την ημερομηνία που η VirusBlockAda ανακάλυψε την ύπαρξη του. Υπάρχει ακόμα η άποψη ειδικών που τοποθετεί την έναρξη της δράσης τους στις αρχές του 2009.

[380] Broad et al, *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay",* the New York Times, 15/1/2011

[381] Albright, David, Brannan, Paul & Walrond, Christina, *"Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?"*, ISIS Report, 22/12/2010, p.1. Available at: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/, accessed on April 2011

[382] Ibid, p. 2

[383] Clemente, Dave, *"Reality Approaches Hype: Critical National Infrastructure and the Stuxnet Worm"*, Chatham House, 28 Sep 2010. Available at: http://www.chathamhouse.org/media/comment/view/163865, accessed on 18/2/2011

γίνονταν μέσα από ψηφιακά βιομηχανικά συστήματα ελέγχου SCADA[384] (Supervisory Control and Data Acquisition), τα οποία χρησιμοποιούσαν συγκεκριμένο τύπο λογισμικού (software) της γερμανικής εταιρείας Siemens. Ο Stuxnet, λοιπόν, είχε σχεδιαστεί για να εκμεταλλευτεί τις τρωτότητες που υπήρχαν σε αυτό το λογισμικό (Siemens Step 7)[385].

Σύμφωνα με δηλώσεις Ιρανών αξιωματούχων τον Οκτώβριο του 2010, στο παρελθόν είχε ανακαλυφθεί κακόβουλο λογισμικό στους Η/Υ του πυρηνικού αντιδραστήρα του Bushehr, το οποίο είχε μεταφερθεί σε αυτούς μέσω CDs ή Flash Drives, αλλά ωστόσο είχε αντιμετωπιστεί επαρκώς[386]. Ως πιθανοί μεταφορείς του κακόβουλου malware θεωρήθηκαν οι υπάλληλοι της ρωσικής Atomstroyeksport, που είχε αναλάβει την κατασκευή του πυρηνικού εργοστασίου. Παρά τα λεγόμενα των Ιρανών για επαρκή αντιμετώπιση του malware, το Bushehr τέθηκε σε λειτουργία με μεγάλη καθυστέρηση, γεγονός που πιθανολογείται ότι σχετίζεται με την κυβερνοεπίθεση Stuxnet κατά του δικτύου Η/Υ που έλεγχε τον πυρηνικό αντιδραστήρα[387].

Επιπλέον, θα πρέπει να σημειωθεί ότι, τον Δεκέμβριο του 2009 επιθεωρητές της IAEA είχαν διαπιστώσει ότι, για ανεξήγητους λόγους, 984 περίπου φυγόκεντρες συσκευές, που χρησιμοποιούνται για τον εμπλουτισμό ουρανίου, είχαν τεθεί εκτός λειτουργίας στην Natanz[388]. Παράλληλα, σε μεταγενέστερη αναφορά της IAEA αναφερόταν ότι οι ποσότητες εμπλουτισμένου ουρανίου που παράγονταν (στην Natanz) ήταν χαμηλές σε σχέση με το παρεχόμενο πυρηνικό καύσιμο και τον αριθμό των εν ενεργεία συσκευών φυγοκέντρησης[389]. Όπως αποκαλύφθηκε, ο Stuxnet είχε επιτεθεί στους μετατροπείς συχνοτήτων (Frequency Converters) των φυγόκεντρων συσκευών IR-1, οι οποίοι ελέγχονταν από το σύστημα SCADA που έφερε το λογισμικό της Siemens. Οι IR-1 ήταν υπεύθυνες για τον διαχωρισμό των ραδιενεργών ισοτόπων και την παραγωγή του τελικού προϊόντος (εμπλουτισμένο ουράνιο). Συγκεκριμένα, οι μετατροπείς συχνοτήτων έλεγχαν την ταχύτητα περιστροφής του στροφείου των φυγόκεντρων συσκευών IR-1, οι οποίες όταν προμηθεύονταν με εξαφθοριούχο

---

[384] Τα συστήματα SCADA στην Natanz και στο Bushehr δεν συνδέονταν με το Internet. Το δίκτυο Η/Υ των συγκεκριμένων πυρηνικών εγκαταστάσεων θεωρείται ως “Air Gapped”.

[385] Shakarian, *“Stuxnet: Cyberwar Revolution in Military Affairs”*, p. 2

[386] Kerr, Paul K, Rollins John & Theohary, Catherine A., *“The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability”,* p. 4, CRS Report for Congress, 9 Dec 2010. Available at: http://www.fas.org/sgp/crs/natsec/R41524.pdf, accessed on April 2011

[387] *“Stuxnet worm mystery: What’s the cyber weapon after?”*, the Christian Science Monitor, 24 Sep 2010. Available at: http://www.csmonitor.com/USA/2010/0924/Stuxnet-worm-mystery-What-s-the-cyber-weapon-after, accessed on 4/11/2011

[388] (2011) “*Stuxnet: targeting Iran’s nuclear programme*”, Strategic Comments, 17:2,1-3

[389] Albright et al, *“Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?”* Επίσης, σύμφωνα με ειδικούς από τα μέσα τους 2009 μέχρι τα μέσα του 2010 διαπιστώθηκε μείωση της τάξης του 23% στις εν ενεργεία συσκευές φυγοκέντρησης της Natanz. Βλέπε Farwell, James P. & Rohozinski Rafal *“Stuxnet and the Future of Cyber War”,* Survival, 53:1, 23-40, 28/1/2011

ουράνιο (UF6), το περιέστρεφαν με υπερηχητικές ταχύτητες, προκειμένου να προκύψει το εμπλουτισμένο ουράνιο. Για να γίνει αυτή η διαδικασία, οι μετατροπείς συχνοτήτων έπρεπε να διατηρούν μια συγκεκριμένη συχνότητα περιστροφής του στροφείου των IR-1, η οποία είχε καθοριστεί από τον κατασκευαστή στα 1064Hz. Ωστόσο, λόγω των δομικών αδυναμιών των IR-1[390], πολλές φορές οι συγκεκριμένες συσκευές φυγοκέντρησης έπρεπε να λειτουργούν σε μικρότερη συχνότητα προκειμένου να μην καταστραφούν και να αυξήσουν το όριο ζωής τους.

Θα πρέπει να τονιστεί ότι, κάθε φορά που απαιτούνταν από το σύστημα SCADA της Natanz μια μεταφορά οδηγιών προς τους μετατροπείς συχνοτήτων, αυτό γινόταν μέσω Η/Υ που συνδέονταν με τις συσκευές ελέγχου των μετατροπέων συχνοτήτων (PLC : Programmable Logic Controllers) και μετέδιδαν τις συγκεκριμένες οδηγίες[391]. Σε αυτό ακριβώς το σημείο έδρασε ο Stuxnet. Η μεταφορά του έγινε μέσω των προαναφερόμενων Η/Υ. Από την στιγμή που ο Stuxnet μεταφέρονταν στα PLCs μπλόκαρε την μεταφορά των οδηγιών προς τους μετατροπείς συχνοτήτων των συσκευών φυγοκέντρησης, έδινε συγκεκριμένες, δικές του, οδηγίες στους μετατροπείς συχνοτήτων, ενώ παρείχε εικόνα καλής λειτουργίας των συσκευών στα συστήματα επιτήρησης της διαδικασίας. Οι παρεχόμενες οδηγίες από τον Stuxnet αφορούσαν σε απότομες επιταχύνσεις και επιβραδύνσεις των στροφείων των συσκευών φυγοκέντρησης, με αποτέλεσμα την καταστροφή τους[392]. Με άλλα λόγια, ο Stuxnet αποτελούσε κακόβουλο λογισμικό, το οποίο είχε ως στόχο την δολιοφθορά φυσικών εγκαταστάσεων[393]. Για το λόγο αυτό, ο καθηγητής John Arquilla χαρακτήρισε την δράση του Stuxnet ως “Cybotage”[394].

Μέχρι σήμερα κανείς δεν μπορεί να αποφανθεί με σιγουριά για το μέγεθος της καταστροφής που επέφερε ο Stuxnet. Ειδικοί στον κυβερνοπόλεμο θεωρούν πως με αυτό το malware η φυσική εξέλιξη του πυρηνικού προγράμματος του Ιράν, η οποία θα οδηγούσε στην κατασκευή πυρηνικών όπλων, παρεμποδίστηκε για τουλάχιστον για 2

---

[390] Οι συσκευές φυγοκέντρησης IR-1 αποτελούν την ιρανική έκδοση των πακιστανικών συσκευών P-1, τις οποίες ο διάσημος Πακιστανός πυρηνικός επιστήμονας A.Q. Khan πούλησε παράνομα κατά το παρελθόν στο Ιράν, την Λιβύη και την Ν. Κορέα. Σύμφωνα με ειδικούς, το ποσοστό απωλειών των IR-1 λόγω αστοχίας υλικών φθάνει στο 10% ανά έτος.

[391] Shakarian, *“Stuxnet: Cyberwar Revolution in Military Affairs”*, p. 4

[392] Albright et al, *“Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?”,* p. 4

[393] Η δολιοφθορά φυσικών εγκαταστάσεων μέσω του κυβερνοχώρου είχε επιτευχθεί προγενέστερα (2009) σε πείραμα του αμερικανικού DHS (Department of Homeland Security), το οποίο αφορούσε στην διεξαγωγή κυβερνοεπίθεσης προς ένα σύστημα SCADA, που διασυνδέονταν με το Internet. Στο πείραμα αυτό, γνωστό ως “Aurora Project”, το σύστημα SCADA έλεγχε την λειτουργία γεννητριών παραγωγής ηλεκτρικής ενέργειας. Από το πείραμα αυτό, διαπιστώθηκε ότι δύναται να επιτευχθεί ζημία στο φυσικό χώρο από ενέργεια που ξεκινά από τον κυβερνοχώρο.

[394] Ο John Arquilla είναι πρόεδρος του τμήματος αμυντικής ανάλυσης στο US Naval Postgraduate School. Θεωρείται ως ένας από τους πρώτους μελετητές του κυβερνοπολέμου, Το 1993 εξέδωσε μαζί με τον David Ronfeldt το άρθρο *“Cyberwar is coming”*, το οποίο ήταν «προφητικό» αναφορικά με την εξέλιξη του κυβερνοπολέμου. Βλέπε επίσης, Arquilla, John, *“Cyberwar Is Already Upon Us”*, Foreign Policy, March/April 2012. Available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us, accessed on 28/2/2012

έτη. Επισημαίνεται ότι το 2011, ο απερχόμενος Αρχηγός της Mossad Meir Dagan δήλωσε στην ισραηλινή Κνεσσέτ ότι, το Ιράν αντιμετώπισε το τελευταίο χρονικό διάστημα τεχνικές δυσκολίες και δεν θα μπορούσε να κατασκευάσει πυρηνική βόμβα πριν από το 2015[395]. Την θέση του Dagan επιβεβαίωσε στην συνέχεια με δηλώσεις της και η Αμερικανίδα ΥΠΕΞ Hillary Clinton.

Οι δηλώσεις αυτές αποτέλεσαν κατά πολλούς ισχυρή ένδειξη για την εμπλοκή των ΗΠΑ και του Ισραήλ στην κυβερνοεπίθεση Stuxnet, κάτι το οποίο τόσο οι ΗΠΑ όσο και το Ισραήλ έχουν επίσημα αρνηθεί. Ωστόσο, σύμφωνα με δημοσιογραφικές πληροφορίες, όταν το 2008 οι Ισραηλινοί ζήτησαν από τον Πρόεδρο Bush το πράσινο φώς για τον αεροπορικό βομβαρδισμό των πυρηνικών εγκαταστάσεων του Ιράν, οι ΗΠΑ αρνήθηκαν και πρότειναν έναν διαφορετικό τρόπο αντιμετώπισης της ιρανικής αδιαλλαξίας. Όπως αναφέρεται, οι 2 χώρες εκτέλεσαν το 2009 δοκιμές του Stuxnet σε ειδικά διαμορφωμένο χώρο που προσομοίαζε τις πυρηνικές εγκαταστάσεις της Natanz. Ο χώρος αυτός ήταν εντός των ισραηλινών πυρηνικών εγκαταστάσεων στην έρημο Negev[396]. Νωρίτερα, από τις αρχές του 2008, η γερμανική εταιρεία Siemens είχε συνεργαστεί με αρμόδιο εργαστήριο (Idaho Laboratory)[397] του αμερικανικού Υπουργείου Ενέργειας, προκειμένου να ελέγξει τις τρωτότητες που παρουσίαζε συγκεκριμένος τύπος υλικού και λογισμικού που είχε πωλήσει ανά τον κόσμο και χρησιμοποιούνταν σε βιομηχανικές εγκαταστάσεις. Μεταξύ αυτών των εγκαταστάσεων συγκαταλέγονταν το πυρηνικό εργοστάσιο εμπλουτισμού ουρανίου στην Natanz.

Θα πρέπει να τονιστεί ότι, λόγω των ιδιαιτεροτήτων που παρουσίαζε η αρχιτεκτονική του Stuxnet και η εξειδίκευση του ως malware συμπεραίνεται ότι η ανάπτυξη του απαίτησε μεγάλα χρηματικά ποσά αλλά και ιδιαίτερες δυνατότητες και τεχνογνωσία στον κυβερνοχώρο που μπορούν να διαθέσουν μόνο τα κράτη[398]. Επιπρόσθετα, για την επιτυχή δραστηριοποίηση του ήταν απαραίτητη η ύπαρξη εξειδικευμένων πληροφοριών για τον στόχο αλλά και πειραματικού πεδίου εφαρμογής του malware, απαιτήσεις τις οποίες θα μπορούσαν να καλύψουν μόνο τα κράτη και όχι μη κρατικές οντότητες (πχ τρομοκρατικές οργανώσεις, ομάδες hackers ή cyber criminals)[399]. Αν και υπάρχουν τρομοκρατικές οργανώσεις που δύνανται να διαθέσουν μεγάλα χρηματικά ποσά για την ανάπτυξη κακόβουλων λογισμικών, οι οργανώσεις αυτές υστερούν σε ειδικούς στον κυβερνοχώρο και σε τεχνογνωσία. Επιπλέον, όπως αποκάλυψαν οι έρευνες, ο Stuxnet δεν είχε σκοπό την υπεξαίρεση βιομηχανικών

[395] Broad et al, *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay"*, the New York Times, 15/1/2011
[396] Ibid
[397] Επισημαίνεται ότι το Aurora Project είχε πραγματοποιηθεί σε αυτό το εργαστήριο.
[398] Kerr et al, *"The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability",* p. 2
[399] Ibid

δεδομένων, όποτε δεν μπορεί να ταυτιστεί με επιχείρηση Cyber Espionage ή Cyber Crime, τα οποία θα μπορούσε να διενεργήσει οποιοσδήποτε πέραν από ένα κράτος.

4. Η Αποτροπή

4.1 Η Αποτροπή - Ορισμός

Σύμφωνα με τον καθηγητή Κωνσταντίνο Κολιόπουλο, η Αποτροπή (Deterrence) ως έννοια της στρατηγικής αποσκοπεί στην διατήρηση του status quo με την απειλή χρήσης βίας[400]. Δηλαδή, αντικειμενικός σκοπός της Αποτροπής είναι η σταθερότητα (διατήρηση του status quo). Βασικό της στοιχείο είναι η έννοια του σχετικού κόστους. Δηλαδή, ο αντίπαλος θα πρέπει σε κάθε περίπτωση να βρίσκεται σε χειρότερη θέση, εφόσον δεν συμμορφωθεί με την απειλή. Για να επιτευχθεί αυτό, το κόστος για τον αντίπαλο θα πρέπει να είναι μεγαλύτερο εφόσον δοκιμάσει να αλλάξει το status quo, σε σχέση με το όφελος (κέρδος) που θα έχει αν επιχειρήσει αυτήν την αλλαγή. Με έναν παρόμοιο ορισμό, ο καθηγητής Martin Libicki θεωρεί πως η Αποτροπή είναι η ικανότητα να πείσεις τον αντίπαλο σου να μην σου επιτεθεί, γιατί αν το πράξει αυτό θα υπάρξουν αντίποινα από την μεριά σου[401]. Με τον τρόπο αυτό, ο Libicki προσδίδει στην απειλή του αμυνόμενου ένα πιο επιθετικό χαρακτήρα.

Από τους παραπάνω ορισμούς προκύπτει ότι η Αποτροπή λειτουργεί στη βάση του κόστους που θα έχει μια δράση για τον αντίπαλο και στηρίζεται στους ορθολογικούς υπολογισμούς του (σχέση κόστους – οφέλους) για αυτήν την δράση. Για να είναι επιτυχής θα πρέπει πάντα το κόστος να είναι μεγαλύτερο από το όφελος για τον επιτιθέμενο και αυτό θα εξασφαλίζεται από την φύση της απειλής που εκφράζει ο αμυνόμενος. Η απειλή αυτή μπορεί να μεταφράζεται είτε σε μάχη μέχρι εσχάτων για τον αμυνόμενο, προκειμένου να μην επιτρέψει την αλλαγή του status quo, ή/και σε ανάληψη επιθετικών ενεργειών από τον αμυνόμενο προκειμένου να ζημιωθεί ο αντίπαλος που επιχειρεί την αλλαγή στο status quo.

4.2 Ιστορική Αναδρομή

Η Αποτροπή αποτελεί μια παλιά πρακτική στις διεθνείς σχέσεις[402]. Αρχικά, χρησιμοποιήθηκε στην διεθνή πολιτική ως τακτική και δεν εκλαμβανόταν ως στρατηγική. Η αξία της για την διεθνή κοινότητα ενισχύθηκε όταν στις αρχές του 20ου αι. έγινε ευρέως αντιληπτό ότι οι τρέχουσες συνθήκες ήταν τέτοιες που διευκόλυναν την διενέργεια καταστροφικών πολέμων. Οι συνθήκες αυτές συνοψίζονταν στην ύπαρξη

[400] Κολιόπουλος, Κωνσταντίνος, *Η στρατηγική σκέψη Από την Αρχαιότητα ως σήμερα* (Εκδόσεις Ποιότητα, Αθήνα, 2008), σελ. 21
[401] Libicki, Martin C., "*Deterrence in Cyberspace*", pp. 16-20, High Frontier: The journal for space and missile professionals, vol. 5, No 3 (May 2009). Available at: http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf, accessed on April 2010
[402] Morgan, Patrick M., *Deterrence Now* (Cambridge University Press, Cambridge, 2003), p. 1

εξελιγμένων όπλων ακριβείας, στην αύξηση της παραγωγικότητας, στην άνθηση του εθνικισμού και στις εξελίξεις στις επικοινωνίες και στις μεταφορές. Οι συνθήκες αυτές ευνόησαν μέσα σε λίγα χρόνια το ξέσπασμα του Α'ΠΠ[403].

Ωστόσο, τα πρώτα «ψήγματα» της Αποτροπής εμφανίστηκαν μετά το 1920 με την Λίγκα των Εθνών, όπου μέσα από ένα πλαίσιο συλλογικής αποτροπής έγινε προσπάθεια να αποφευχθεί η εκδήλωση της επιθετικότητας από ένα κράτος προς ένα άλλο. Παρόλα αυτά, η ουσιαστική ανάπτυξη της θεωρίας της Αποτροπής και η μετατροπή της από τακτική των διεθνών σχέσεων σε στρατηγική έγινε μετά το τέλος του Β'ΠΠ και την εμφάνιση των πυρηνικών όπλων (Ψυχρός Πόλεμος), τα οποία «επέβαλλαν» μια ιδιόρρυθμη πυρηνική ισορροπία στο διεθνές σύστημα. Η ύπαρξη δηλαδή των πυρηνικών όπλων στα οπλοστάσια διαφορετικών κρατών προοικονομούσε ότι, οποιαδήποτε διατάραξη της ισορροπίας ισχύος στο διεθνές σύστημα θα είχε καταστροφικές συνέπειες για όλους (Αμοιβαία Πυρηνική Αποτροπή).

4.3 Προϋποθέσεις Αποτροπής

Σύμφωνα με τον διεθνολόγο Hedley Bull, η χώρα Α αποτρέπει την χώρα Β από μια συγκεκριμένη πορεία δράσης όταν υπάρχουν οι εξής προϋποθέσεις[404]:

α. Μια χώρα Α απευθύνει στην χώρα Β μια απειλή τιμωρίας ή πλήγματος της, σε περίπτωση που η χώρα Β αποτολμήσει μια συγκεκριμένη πορεία δράσης. Σε αυτήν την περίπτωση είναι απαραίτητο η χώρα Α να έχει διατυπώσει ρητά την απειλή της προς την χώρα Β.

β. Σε περίπτωση απουσίας της ανωτέρω απειλής από την χώρα Α προς την χώρα Β, τότε η τελευταία θα μπορούσε να αποτολμήσει την συγκεκριμένη πορεία δράσης. Με άλλα λόγια, η χώρα Β θα είχε τα μέσα και την θέληση να προχωρήσει σε μια επιθετική προς την χώρα Α ενέργεια, σε περίπτωση έλλειψης ξεκάθαρης απειλής από την χώρα Α.

γ. Η χώρα Β πιστεύει ότι η χώρα Α έχει την ικανότητα και την βούληση να πραγματοποιήσει την απειλή της. Για τον λόγο αυτό αποφασίζει (η χώρα Β) ότι η συγκεκριμένη πορεία δράσης δεν αξίζει τον κόπο. Στο σημείο αυτό, θα πρέπει να σημειωθεί ότι η απειλή που διατυπώνει η χώρα Α είναι αναγκαίο να είναι πιστευτή από την χώρα Β. Εφόσον ισχύει αυτό, τότε η χώρα Β θα θεωρήσει ότι η υπό υλοποίηση πορεία δράσης της είναι ανάξια λόγου ή μη ωφέλιμη. Το συμπέρασμα αυτό θα προκύψει μέσα από τους ορθολογικούς υπολογισμούς (υπολογισμούς κόστους –

[403] Ibid, p.4
[404] Bull, Hedley, *Άναρχη Κοινωνία: Μελέτη της τάξης στην παγκόσμια πολιτική* (Εκδόσεις Ποιότητα, Αθήνα, 2007 (Γ' έκδοση)), σελ. 166

οφέλους) της χώρας Β (πχ. Ποιό το όφελος από την πραγματοποίηση της πορείας; , ποιό το κόστος από την μη υλοποίηση της πορείας δράσης; , ποια η σημασία που αποδίδεται από την χώρα Β στις απειλούμενες αξίες από την έκφραση απειλής της χώρας Α; , κα).

Από την ανάλυση των παραπάνω προϋποθέσεων προκύπτει ότι η έννοια της Αποτροπής στηρίζεται σε δυο κύριους άξονες. Ο πρώτος είναι η αξιοπιστία της απειλής. Δηλαδή, θα πρέπει ο αμυνόμενος ή αλλιώς αυτός που εκφράζει την απειλή (χώρα Α) να έχει τα κατάλληλα μέσα και την θέληση να τα χρησιμοποιήσει[405], ενώ ο αντίπαλος (χώρα Β) θα πρέπει να γνωρίζει για την ύπαρξη των μέσων αυτών και για την θέληση χρησιμοποίησης τους[406]. Συνεπώς, προκύπτει ανάγκη ύπαρξης δίαυλου επικοινωνίας μεταξύ των δυο αντιπάλων. Ο δεύτερος άξονας είναι η δυνατότητα ορθολογιστικών υπολογισμών από τις δυο πλευρές. Η αποτρεπτική απειλή θα πρέπει να είναι σαφής αναφορικά με τα όρια δράσης του αντιπάλου και να στοχεύει σε αξίες που ο αντίπαλος θεωρεί ιδιαίτερης σημασίας για τον ίδιο[407]. Με τον τρόπο αυτό, η απειλή θα επιδράσει στο πνεύμα και την ψυχολογία του αντιπάλου[408], με αποτέλεσμα οι ορθολογικοί υπολογισμοί του (χώρα Β) να έχουν θετική έκβαση για την χώρα Α. Σε περίπτωση που η ηγεσία της χώρας Β δεν λειτουργεί ορθολογικά, τότε η Αποτροπή δεν μπορεί να εφαρμοστεί και η σύγκρουση είναι αναπόφευκτη.

4.4 Τα είδη της Αποτροπής

Το 1993, ο καθηγητής Patrick M. Morgan παρουσίασε στο βιβλίο του με τίτλο "Deterrence Now" δυο βασικά είδη Αποτροπής[409]: α) Την Γενική Αποτροπή (General Deterrence), όπου ο αμυνόμενος διαθέτει μια ευρεία στρατιωτική δυνατότητα και εξαπολύει γενικές απειλές που προοικονομούν την τιμωρία οποιουδήποτε σκέφτεται να του επιτεθεί και β) την Άμεση Αποτροπή (Immediate Deterrence), όπου ο ανωτέρω

[405] Gray, Colin S., *"Deterrence Resurrected: Revisiting Some Fundamentals"*, Parameters, winter 2010 – 2011),pp.99-106.Available at: http://www.carlisle.army.mil/usawc/parameters/Articles/2010winter/Gray.pdf, accessed on May 2011

[406] Κολιόπουλος, 2008 : 23. Επίσης, για να λειτουργήσει η Αποτροπή, ο αντίπαλος θα πρέπει να μπορεί να αντιληφθεί τις προθέσεις σου. Βλέπε, Shaud, John A., *"Framing Deterrence in the Twenty – First Century"*, Strategic Studies Quarterly, Fall 2009, pp. 4-7. Available at: http://www.au.af.mil/au/ssq/2009/Fall/shaud.pdf, accessed on May 2011

[407] Gray, Colin S., "*Deterrence Resurrected…."*

[408] Κουσκουβέλης, 2007: 423. Τον ψυχολογικό αντίκτυπο στον αντίπαλο από την απειλή χρήσης βίας για σκοπούς αποτροπής επισημαίνει και ο A. Beaufre στο άρθρο του *"A Strategy of Deterrence"*, το οποίο περιέχεται στο Freedman, Lawrence (Ed.), *War* (Oxford University Press, Oxford, 1994), p. 239.

[409] Morgan, 2003: 9

αμυνόμενος εξαπολύει απειλή χρήσης βίας κατά ενός συγκεκριμένου αντιπάλου, ο οποίος σκέφτεται να του επιτεθεί άμεσα[410].

Πέρα από αυτό το βασικό διαχωρισμό, η Αποτροπή μπορεί να είναι μονομερής, όταν η απειλή εκφράζεται μόνο από την μια πλευρά και αμοιβαία όταν δυο ή περισσότερα κράτη αποτρέπονται αμοιβαίως από το να πράξουν κάτι[411]. Χαρακτηριστικό παράδειγμα τέτοιου είδους αποτροπής αποτέλεσε η ψυχροπολεμική Αμοιβαία Πυρηνική Αποτροπή, η οποία στηρίζονταν στην ύπαρξη πυρηνικών όπλων στα χέρια των δυο υπερδυνάμεων (ΗΠΑ & ΕΣΣΔ), αλλά και στην θέληση τους να τα χρησιμοποιήσουν, εφόσον μια αντίπαλη υπερδύναμη προχωρούσε σε μια μη αποδεκτή ενέργεια. Βασικές συνιστώσες της επιτυχίας της ήταν ο φόβος που προκαλούσε η ενδεχόμενη χρήση των πυρηνικών όπλων, αλλά και η πεποίθηση ότι η έκβαση της σύγκρουσης δεν θα καθόριζε κάποιον ως νικητή, καθώς οι εμπλεκόμενοι στην σύγκρουση θα είχαν τεράστιο κόστος.

Μια ακόμα ταξινόμηση της Αποτροπής λαμβάνει τις παρακάτω κύριες μορφές:

α. <u>Αποτροπή μέσω παρουσίας</u> (Deterrence by presence): Επιτυγχάνεται μέσω διατήρησης συμβολικών δυνάμεων στο προς υπεράσπιση σημείο, προκειμένου να καταδειχτεί στον αντίπαλο πως σε περίπτωση επιθετικής του ενέργειας, θα υπάρξει αντίδραση (από τον αμυνόμενο), η οποία θα οδηγήσει σε γενικότερη σύγκρουση.[412]

β. <u>Αποτροπή μέσω Άμυνας</u> (Deterrence by defense): Προκύπτει από την διατήρηση ισχυρών αμυντικών δυνατοτήτων. Η ισχυρή άμυνα λειτουργεί αποτρεπτικά για τον εν δυνάμει επιτιθέμενο[413].

γ. <u>Αποτροπή μέσω Άρνησης</u> (Deterrence by Denial): Αποσκοπεί στην άρνηση αποκόμισης κερδών στον επιτιθέμενο. Η ζημιά για τον αμυνόμενο μπορεί να είναι μεγάλη, αλλά ο επιτιθέμενος δεν θα πάρει αυτό που επιδιώκει[414].

δ. <u>Αποτροπή μέσω Αντιποίνων</u> (Deterrence by Punishment): Στηρίζεται στην απειλή αντιποίνων, η οποία μπορεί να αναφέρεται και σε διαφορετικό χώρο, χρόνο και τόπο από αυτά (χώρο, χρόνο, τόπο) που επέλεξε ο αντίπαλος για να εκδηλώσει την επιθετική του ενέργεια[415].

Παράλληλα, η Αποτροπή διακρίνεται και ως εξής:

α. <u>Εθνική Αποτροπή</u>: Η Αποτροπή που επιτυγχάνεται με εθνικά μέσα[416].

---

[410] Λαμβάνοντας υπόψη τον μεγάλο αριθμό κυβερνοεπιθέσεων που πραγματοποιούνται καθημερινά, αλλά και τον σχεδόν μηδενικό χρόνο που απαιτείται για την εκδήλωση τους, θα μπορούσε να ειπωθεί ότι η Αποτροπή στον κυβερνοχώρο μπορεί να χαρακτηριστεί περισσότερο ως Άμεση.
[411] Κουσκουβέλης, 2007: 424-425
[412] Κολιόπουλος, 2008 : 23
[413] Ibid
[414] Ibid
[415] Ibid, σελ. 24
[416] Ibid

β. Διεθνής Αποτροπή: Η Αποτροπή που επιτυγχάνεται μέσω τρίτων (πχ μέσω ΝΑΤΟ)[417].

γ. Προεκτεινόμενη Αποτροπή (Extended Deterrence): Η Αποτροπή εχθρικών προσβολών σε τρίτες χώρες[418].

δ. Ενδοπολεμική Αποτροπή (Intra-war Deterrence): Λαμβάνει χώρα κατά την διάρκεια ενός πολέμου και αποσκοπεί στην αποσόβηση της κλιμάκωσης[419].

ε. Μίνιμουμ Αποτροπή (Minimum Deterrence): Η Αποτροπή του αντιπάλου μέσω ύπαρξης μικρού πυρηνικού οπλοστασίου, το οποίο είναι στραμμένο αποκλειστικά εναντίον των εχθρικών πόλεων[420].

στ. Ενεργητική Αποτροπή: Αποσκοπεί στο να πείσει, μέσω απειλής ή επιβολής τιμωρίας, τον αντίπαλο από το να σταματήσει τις ενέργειες που έχει ήδη ξεκινήσει[421].

4.5 Η Κυβερνοαποτροπή (Cyber Deterrence) και τα Προβλήματα Εφαρμογής της

Η Αποτροπή στον κυβερνοχώρο δύναται να λάβει δυο βασικές μορφές. Αυτές είναι η κυβερνοαποτροπή μέσω άρνησης (Cyber deterrence by denial) και η κυβερνοαποτροπή μέσω αντιποίνων (Cyber deterrence by punishment)[422]. Η 1η μορφή σχετίζεται με την άμυνα στον κυβερνοχώρο (Cyber Defense). Μέσω ανάπτυξης αμυντικών δυνατοτήτων σε αυτόν (CND) αποσκοπεί στην φθορά των κυβερνοεπιθέσεων του αντιπάλου και συμβάλλει στην αύξηση του κόστους σε αυτόν. Η άλλη μορφή (Cyber deterrence by punishment) είναι πιο επιθετική και εστιάζει στην εφαρμογή αντιποίνων στον κυβερνοχώρο, προκειμένου ο αντίπαλος να αποτραπεί από την έναρξη ή την περαιτέρω διεξαγωγή κυβερνοεπιθέσεων. Προϋποθέτει, λοιπόν, την ύπαρξη ανεπτυγμένων επιθετικών δυνατοτήτων στον κυβερνοχώρο (CNAs).

Για τους περισσότερους αναλυτές της Κυβερνοαποτροπής, οι δυο μορφές της θα πρέπει να λειτουργήσουν συνεργατικά, προκειμένου να επιτευχθεί το επιθυμητό αποτέλεσμα από τον αμυνόμενο[423]. Η κυβερνοαποτροπή (by denial & by punishment) έχει ως στόχο να μειώσει την πιθανότητα εκδήλωσης κυβερνοεπιθέσεων κατά του αμυνόμενου, σε ένα αποδεκτό επίπεδο, το οποίο αντιστοιχεί σε ένα αντίστοιχα αποδεκτό κόστος. Ωστόσο, αρκετοί εστιάζουν το ενδιαφέρον τους στις δυνατότητες που δύναται να προσδώσει στον αμυνόμενο η Αποτροπή μέσω αντιποίνων, καθώς η

[417] Ibid
[418] Ibid
[419] Ibid, σελ. 25
[420] Ibid
[421] Πλατιάς, Αθανάσιος & Ήφαιστος, Παναγιώτης, *Ελληνική Αποτρεπτική Στρατηγική* (Εκδόσεις Παπαζήση, Αθήνα 1992), σελ. 38
[422] Libicki, 2009: 7-8
[423] Ibid

ανάπτυξη αμυντικών δυνατοτήτων στον κυβερνοχώρο κοστίζει περισσότερο, ενώ η επίθεση έχει το πλεονέκτημα σε σχέση με την άμυνα. Ενδεικτικά αναφέρεται ότι μόνο για το 2009, οι ΗΠΑ χρειάστηκαν να ξοδέψουν περίπου 7,3 δις δολ. για την άμυνα των ομοσπονδιακών συστημάτων πληροφορικής[424]. Παρόλα αυτά, θα πρέπει να επισημανθεί πως με την Κυβερνοαποτροπή μέσω άρνησης (Cyber Defense) εξασφαλίζεται ότι οι εισερχόμενες κυβερνοεπιθέσεις θα αποτύχουν σε μεγάλο βαθμό, η εκδήλωση αντιποίνων θα είναι εφικτή, ενώ θα μπορέσουν να απορριφθούν οι χαμηλής σημασίας κυβερνοεπιθέσεις από τρίτα μέρη και να διευκολυνθεί η προσπάθεια απόδοσης της ευθύνης των επιθέσεων στον πραγματικό αυτουργό. Με τον τρόπο αυτό η στρατηγική της κυβερνοαποτροπής γίνεται ολοένα και πιο αξιόπιστη[425].

Το πρώτο ερώτημα που προκύπτει σχετικά με την Αποτροπή στον κυβερνοχώρο είναι το κατά πόσο αυτή η μορφή αποτροπής είναι αναγκαία. Οι λόγοι που καθιστούν αναγκαία της κυβερνοαποτροπή έχουν να κάνουν κυρίως με το ζήτημα της αναλογικότητας. Όταν μια χώρα έχει να αντιμετωπίσει τον κίνδυνο των κυβερνοεπιθέσεων δεν νομιμοποιείται – τουλάχιστον μέχρι σήμερα – για λήψη κινητικών μέτρων (συμβατικό ή πυρηνικό πλήγμα) κατά του αντιπάλου, καθώς κάτι τέτοιο χαρακτηρίζεται ως δυσανάλογο. Συνεπώς, εφόσον ληφθεί απόφαση για εκδήλωση αντιποίνων, αυτά θα πρέπει να είναι της ίδιας φύσης με τις κυβερνοεπιθέσεις (retaliation in kind). Από την άλλη μεριά, η πιθανότητα επιβολής διπλωματικών και οικονομικών κυρώσεων (ως αντίποινα) λόγω της διεξαγωγής κυβερνοεπιθέσεων δεν είναι εφικτή, καθώς δεν μπορεί να επιβεβαιωθεί με ακρίβεια η ταυτότητα του επιτιθέμενου. Επιπλέον, θα πρέπει να σημειωθεί ότι μέχρι σήμερα δεν έχει καταγραφεί τέτοιου είδους αντίδραση από κάποια χώρα. Παράλληλα, από την πρακτική έχει διαφανεί πως οποιαδήποτε προσπάθεια κάλυψης του ζητήματος μέσω νομικών μέτρων (ποινικές διώξεις) συναντά προβλήματα, είτε γιατί οι κυβερνοεπιθέσεις επηρεάζουν χώρες με μη συμβατά Δίκαια, είτε γιατί πολλές χώρες αρνούνται να συνεργαστούν σε νομικό επίπεδο μεταξύ τους (περίπτωση Εσθονίας – Ρωσίας για τις κυβερνοεπιθέσεις του 2007 κατά της Εσθονίας).

Το δεύτερο ερώτημα είναι αν η Αποτροπή μπορεί να εφαρμοστεί στον κυβερνοχώρο, όπως εφαρμόζεται στο συμβατικό και στο πυρηνικό επίπεδο. Σύμφωνα με τον ειδικό σε θέματα κυβερνοπολέμου Richard Clarke, η εφαρμογή της Αποτροπής στον κυβερνοχώρο παρουσιάζει πολλά προβλήματα. Το πρώτο από αυτά είναι η έλλειψη αξιοπιστίας αναφορικά με τα κυβερνοόπλα[426]. Κατά την διάρκεια του Ψυχρού Πολέμου (Ψ.Π), οι δυο υπερδυνάμεις διέθεταν πυρηνικά όπλα, τα οποία είχαν

[424] Ibid, p. 32
[425] Libicki, 2009: 73 -74
[426] Clarke & Knake, 2010: 189 - 195

δοκιμάσει κατά καιρούς σε διάφορες πυρηνικές δοκιμές. Η ύπαρξη και η καταστρεπτικότητα των όπλων αυτών ήταν δεδομένη και ευρέως γνωστή. Επίσης, υπήρχε η πεποίθηση ότι τα όπλα αυτά – όλα ή τουλάχιστον ένας αποτελεσματικός αριθμός από αυτά - παρά τις αντιξοότητες που θα αντιμετώπιζαν σε μια σύγκρουση, θα έφταναν τελικά στον στόχο τους. Κατά αναλογία, το ίδιο ίσχυε και για τα συμβατικά όπλα. Αντίθετα, η αποτελεσματικότητα των κυβερνοόπλων δεν μπορεί να θεωρείται ως δεδομένη, λόγω της μεταβλητότητας που παρουσιάζει ο κυβερνοχώρος (το αποτέλεσμα κάθε φορά της ίδιας ενέργειας μπορεί να είναι διαφορετικό). Επιπλέον, η ύπαρξη τους και η καταστρεπτικότητα τους πηγάζει από ενδείξεις και δηλώσεις κρατών, χωρίς αυτό να αποδεικνύεται στην πράξη[427]. Παράλληλα, η ανάπτυξη των επιθετικών και αμυντικών δυνατοτήτων στον κυβερνοχώρο από τα κράτη καλύπτεται από ένα πέπλο μυστικότητας. Για παράδειγμα, οι ΗΠΑ θεωρητικά κατέχουν την πρώτη θέση στα επιθετικά κυβερνοόπλα, αλλά αυτό δεν αποδεικνύεται εμπράκτως[428]. Θα πρέπει να σημειωθεί ακόμα ότι οι αμυντικές δυνατότητες μιας χώρας στον κυβερνοχώρο εξαρτώνται άμεσα από την εξειδίκευση του αρμόδιου ανθρώπινου δυναμικού στην IT τεχνολογία και στον τρόπο αντίδρασης του σε μια κυβερνοεπίθεση, στοιχεία τα οποία δεν μπορούν να θεωρηθούν παγιωμένα ή μετρήσιμα. Συνεπώς, στον κυβερνοχώρο υπάρχει έντονο το στοιχείο της αβεβαιότητας.

Ένα ακόμα πρόβλημα στο ζήτημα της κυβερνοαποτροπής είναι η απουσία διεθνούς νομικής ορολογίας για τον κυβερνοχώρο[429]. Λόγω αυτής της έλλειψης είναι δυνατόν να προκύψουν διαφορετικές στάσεις και αντιδράσεις από τους άμεσα εμπλεκόμενους στις κυβερνοσυγκρούσεις. Για παράδειγμα, μια συγκεκριμένη κυβερνοεπίθεση μπορεί να εκληφθεί από κάποιους ως πράξη πολέμου, ενώ κάποιοι άλλη να την εκλάβουν ως βανδαλισμό στον κυβερνοχώρο. Χαρακτηριστικά αναφέρεται ότι οι κυβερνοεπιθέσεις στην Εσθονία το 2007 ερμηνεύονται, ακόμα και σήμερα, διαφορετικά από τις χώρες της διεθνούς κοινότητας. Τονίζεται επίσης ότι, οι υπόψη κυβερνοεπιθέσεις χαρακτηρίστηκαν ως “Cyber Blitzkriegs” και “Preemptive digital strikes”, παρόλο που δεν συνοδεύτηκαν από συμβατικές επιχειρήσεις σε όλα τα επίπεδα (ξηρά θάλασσα, αέρα) ή δεν ήταν αποτέλεσμα της προετοιμασίας της

[427] Η καταστρεπτικότητα που εμφανίζουν τα κυβερνοόπλα σε ένα πεδίο κυβερνοδοκιμών (cyber test range) δεν σημαίνει ότι θα είναι η ίδια σε μια πραγματική κατάσταση, καθώς οι συνθήκες στο πεδίο κυβερνοδοκιμών είναι ιδανικές, ενώ κατά την διάρκεια μιας σύγκρουσης μεταβάλλονται.

[428] Τα κράτη διατηρούν ένα πέπλο μυστικότητας σχετικά με τα CNAs & CNDs που διαθέτουν προκειμένου να αιφνιδιάσουν τον αντίπαλο, τόσο κατά την εκδήλωση μιας κυβερνοεπίθεσης (zero-day exploit) όσο και κατά την εκδήλωση κυβερνοάμυνας απέναντι στον αντίπαλο. Το γεγονός αυτό δυσκολεύει την κυβερνοαποτροπή, καθώς ο αντίπαλος δεν γνωρίζει ότι το κράτος – στόχος διαθέτει τα μέσα για την εκδήλωση αντιποίνων.

[429] Kaminski, Ryan T., *“Escaping The Cyber State of Nature: Cyber Deterrence and International Institutions”,* στο Czosseck, C & Podins K. (Eds), Conference on Cyber Conflict Proceedings 2010 (CCD COE Publications, Tallinn, 2010), pp. 79 - 94

Εσθονίας για επίθεση κατά της Ρωσίας[430]. Επιπρόσθετα, ακόμα και αν σε περιφερειακό επίπεδο (πχ επίπεδο ΝΑΤΟ) προέκυπτε μια κοινά αποδεκτή νομική ορολογία για τον κυβερνοχώρο θα υπήρχαν παρόμοιοι κίνδυνοι, καθώς τίποτα δεν θα μπορούσε να εξασφαλίσει την απουσία παρερμηνειών από την Κίνα ή την Ρωσία. Για το λόγο αυτό, η προσφορότερη λύση είναι η ύπαρξη μιας κοινά αποδεκτής νομικής ορολογίας για τον κυβερνοχώρο στο επίπεδο του ΟΗΕ. Καθίσταται λοιπόν σαφές ότι, στον κυβερνοχώρο υπάρχει έντονο το πρόβλημα λανθασμένης ερμηνείας συγκεκριμένων δράσεων από τους αντιπάλους, η οποία μπορεί να οδηγήσει σε συγκρούσεις, καθιστώντας την Αποτροπή ανενεργή.

Η Ανωνυμία που παρουσιάζεται στον κυβερνοχώρο αποτελεί επίσης σημαντικό πρόβλημα, καθώς δεν μπορεί να εφαρμοστεί μια στρατηγική αποτροπής εφόσον δεν είναι γνωστή η ταυτότητα του αντιπάλου[431]. Ιδιαίτερα η κυβερνοαποτροπή μέσω αντιποίνων καθίσταται ανενεργή, καθώς δεν υπάρχει σημείο κατεύθυνσης των αντιποίνων. Κατά τη διάρκεια των συμβατικών συγκρούσεων ήταν εμφανή τόσο η ταυτότητα του αντιπάλου όσο και η φυσική του θέση. Κατά αντιστοιχία, στον Ψ.Π οι εμπλεκόμενοι γνώριζαν την ταυτότητα του αντιπάλου τους, ενώ εκμεταλλευόμενοι την τεχνολογία (δορυφόροι) μπορούσαν να προσδιορίσουν το σημείο έναρξης των επιθέσεων. Στον κυβερνοχώρο αυτό δεν είναι εφικτό. Οι Hackers, εκμεταλλευόμενοι την δαιδαλώδη αρχιτεκτονική του διαδικτύου και των λοιπών δικτύων Η/Υ, μπορούν να εξαπολύουν επιθέσεις από οποιοδήποτε σημείο θελήσουν, αποκρύπτοντας στην συνέχεια τα ίχνη τους[432]. Το πρόβλημα αυτό διογκώνεται όταν οι hackers χρησιμοποιούν τα Botnets, όποτε οι κυβερνοεπιθέσεις δύναται να ξεκινούν ταυτόχρονα από διαφορετικά σημεία και να εμπλέκουν με αυτόν τον τρόπο κράτη, τα οποία δεν έχουν καμία σχέση με αυτές.

Όπως γίνεται κατανοητό, η απόδοση της ευθύνης για μια κυβερνοεπίθεση είναι ιδιαίτερα δύσκολη. Πέρα από την χαοτική αρχιτεκτονική των δικτύων Η/Υ, δεν υπάρχει μέχρι σήμερα επαρκής τεχνολογική μέθοδος που να οδηγεί με σιγουριά στον θύτη των κυβερνοεπιθέσεων. Οι υπάρχουσες μέθοδοι έχουν μεγάλο κόστος, απαιτούν σημαντικά χρηματικά ποσά και χρόνο, ενώ στο τέλος καταλήγουν σε περιορισμένα συμπεράσματα[433]. Θα πρέπει να τονιστεί ότι, ακόμα και αν μετά από επίπονη και ενδελεχή έρευνα διευκρινιστεί η τοποθεσία που ξεκίνησε η κυβερνοεπίθεση, αυτό δεν σημαίνει ότι το κράτος (κυβέρνηση), από το οποίο έλαβε χώρα η επίθεση αυτή, είχε

---

[430] Ibid

[431] Gourley, Bob, *"Towards a Cyber Deterrent"*, 29 May 2008. Available at: http://ctovision.com/references/towards-a-cyber-deterrent/, accessed on April 2011

[432] Libicki, 2009: 43 -44

[433] Solomon, Jonathan, *"Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?"* Strategic Studies Quarterly, Spring 2011, pp.1-25. Available at:http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf, accessed on June 2011.

δώσει την εντολή εκτέλεσης της. Η κυβερνοεπίθεση μπορεί να έγινε από έναν μη κρατικό δρώντα, από έναν ακτιβιστή, ή ακόμα και από ένα κρατικό υπάλληλο, ο οποίος όμως λειτούργησε αυτόνομα χωρίς να έχει λάβει αρμοδίως σχετικές εντολές. Παράλληλα, για την επιτυχή έκβαση των ερευνών είναι αναγκαία η προθυμία των άλλων κρατών ή παραγόντων, που εικάζεται ότι εμπλέκονται με τις επιθέσεις αυτές, να συνεργαστούν με τον φορέα διεξαγωγής των ερευνών. Το παράδειγμα της Ρωσίας με την Εσθονία το 2007 καταδεικνύει ότι αυτό δεν είναι πάντα εφικτό. Επιπλέον, πολλές φορές τα κράτη επιλέγουν να μην συνεργαστούν σε τέτοιου είδους έρευνες, προφασιζόμενα ζητήματα εθνικής ασφάλειας.

Επιπρόσθετα, όταν η αμυνομένη χώρα δεν μπορεί να ταυτίσει τις κυβερνοεπιθέσεις με συγκεκριμένο αντίπαλο, τότε αδυνατεί να καταλήξει στον τρόπο με τον οποίο ο αντίπαλος λαμβάνει τις αποφάσεις για την εκτέλεση των κυβερνοεπιθέσεων. Χαρακτηριστικά στοιχεία των κυβερνοεπιθέσεων (είδος, ρυθμός, συχνότητα), καθώς και η επιλογή στόχων από τον αντίπαλο καταδεικνύουν τον γενικότερο τρόπο λειτουργίας του (Mondus Operandi), τα κίνητρα και τις επιδιώξεις του, αλλά και τον τρόπο που λαμβάνει αποφάσεις[434]. Επιπλέον, κάθε κυβερνοεπίθεση, όταν αποκαλυφθεί, μπορεί να γίνει αντικείμενο αντίστροφης μηχανικής (reverse engineering) και να καταδείξει το επίπεδο εξειδίκευσης του αντιπάλου στις κυβερνοεπιθέσεις. Συνεπώς, όταν η αμυνόμενη χώρα γνωρίσει την ταυτότητα του αντιπάλου, τότε μπορεί να αντιληφθεί καλύτερα για την ύπαρξη ή μη ορθολογικών υπολογισμών από αυτόν, να διευκρινίσει τι έχει αξία για τον αντίπαλο και να κατευθύνει την κυβερνοαποτροπή της (αντίποινα) προς το σωστό σημείο.

Ένα άλλο σημείο που καθιστά προβληματική την εφαρμογή της Αποτροπής στον κυβερνοχώρο είναι ο αριθμός των «παιχτών» που μπορούν να εμπλακούν σε μια σύγκρουση. Συγκεκριμένα, τόσο κατά την διάρκεια του Ψ.Π, όσο και στις περιπτώσεις των συμβατικών συγκρούσεων οι αντίπαλοι ήταν γνωστοί και αφορούσαν σε κράτη[435], οπότε η στρατηγική Αποτροπής στόχευε κάθε φορά προς ένα συγκεκριμένο κράτος. Υπό την απειλή αντιποίνων, η Αποτροπή έθετε σε κίνδυνο πολιτικές υποδομές, στρατιωτικές εγκαταστάσεις, ένοπλες δυνάμεις, αλλά ακόμα και άμαχο πληθυσμό του αντιπάλου. Στην περίπτωση των κυβερνοσυγκρούσεων όμως, η κατάσταση γίνεται σαφώς πιο περίπλοκη, καθώς σε αυτές μπορούν να εμπλακούν διάφοροι μη κρατικοί δρώντες (απλοί πολίτες, τρομοκράτες, ομάδες hackers κτλ), των οποίων ο ορθολογικός τρόπος λήψης αποφάσεων τίθεται πολλές φορές υπό αμφισβήτηση. Οι παράγοντες αυτοί μπορούν να λειτουργούν αυτόνομα, αλλά κάλλιστα μπορούν να διεξάγουν

[434] Libicki, 2009:50
[435] Sterner, Eric, *"Retaliatory Deterrence in Cyberspace"*, Strategic Studies Quarterly, Spring 2011, pp. 62 – 80. Available at: http://www.au.af.mil/au/ssq/2011/spring/sterner.pdf, accessed on June 2011

κυβερνοεπιθέσεις υπό την ανοχή ή τις οδηγίες ενός κράτους, το οποίο δεν επιθυμεί να έχει άμεση εμπλοκή με αυτές[436]. Ωστόσο, αν τα αντίποινα που προβλέπονται από την στρατηγική Αποτροπής στοχεύσουν έναν μη κρατικό δρώντα που δραστηριοποιείται σε μια ουδέτερη χώρα, τότε υπάρχει κίνδυνος η στρατηγική αυτή να δημιουργήσει έναν ακόμα αντίπαλο στον κυβερνοχώρο[437].

Όπως προαναφέρθηκε είναι σημαντικό, το κράτος που θέλει να αποτρέψει την διενέργεια κυβερνοεπιθέσεων σε βάρος του, να καταλήξει στο στοιχείο εκείνο που έχει ιδιαίτερη αξία για τον αντίπαλο. Στον κυβερνοχώρο, ακόμα και αν επιτευχθεί αυτό και το στοιχείο αυτό στοχοποιηθεί, δεν είναι βέβαιο ότι το κράτος που εξαπολύει τα αντίποινα θα μπορέσει να πλήξει τον στόχο του ή ότι εφόσον ο στόχος πληγεί, θα γνωστοποιηθεί η έκταση της ζημίας που επιτεύχθηκε[438]. Λόγω της μεταβλητότητας που υπάρχει στον κυβερνοχώρο, τα αποτελέσματα της αντεπίθεσης μπορεί να είναι διαφορετικά από τα αναμενόμενα. Επίσης, με δεδομένο ότι το κράτος ή ο δρώντας που στοχοποιείται γνωρίζει για την αξία του στοιχείου – στόχου του, είναι λογικό να ενισχύσει με επιπρόσθετη άμυνα το στοιχείο αυτό. Παράλληλα, εφόσον ο αντεπιτιθέμενος δεν μπορεί να μάθει για την έκταση της ζημίας που προκάλεσε με τα αντίποινα του, δεν μπορεί να ξέρει ότι η στρατηγική Αποτροπής που ακολούθησε θα επιφέρει το επιθυμητό αποτέλεσμα. Επιπλέον, τονίζεται ότι, η κατάσταση αυτή επιδεινώνεται από το γεγονός πως μετά την εκδήλωση κυβερνοεπίθεσης προς ένα στόχο ή αντίποινα προς αυτόν, αποτελεί πάγια τακτική η διόρθωση των τυχών αδυναμιών – τρωτοτήτων στο λογισμικό. Το γεγονός αυτό προοικονομεί ότι η επιτυχία των αντιποίνων έχει περιορισμένο χρόνο ζωής και δεν μπορεί να επαναλαμβάνεται για μεγάλο χρονικό διάστημα. Αντίθετα, η εκτίμηση της ζημίας από τα αντίποινα σε συμβατικό ή πυρηνικό επίπεδο είναι ευκολότερη, καθώς είναι ορατά, ενώ τα αποτελέσματα τους έχουν μεγαλύτερη διάρκεια στον χρόνο.

Επιπλέον, η επιλογή των αντιποίνων γίνεται υπό την προϋπόθεση ότι ο επιτιθέμενος διαθέτει επαρκείς IT υποδομές, οι οποίες μπορούν να στοχοποιηθούν. Ωστόσο, η κατάσταση αυτή δεν είναι πάντα ο κανόνας. Η περίπτωση της Β. Κορέας καταδεικνύει πως παρόλο που διαθέτει σημαντικές επιθετικές δυνατότητες στον κυβερνοχώρο, η χώρα αυτή δεν είναι διασυνδεδεμένη με τις άλλες χώρες στον παγκόσμιο ιστό, ενώ δεν διαθέτει επαρκείς IT υποδομές. Ακόμα, λόγω της έντονης ασυμμετρίας που υπάρχει στον κυβερνοχώρο, ένας μη κυβερνητικός παράγοντας (πχ ένας κυβερνοτρομοκράτης) δύναται να εξαπολύσει κυβερνοεπιθέσεις από μια χώρα με ανύπαρκτες IT υποδομές, κάνοντας χρήση φθηνού IT εξοπλισμού (πχ ένα laptop & μια

[436] Τέτοιες περιπτώσεις αναλύθηκαν στα γεγονότα της Εσθονίας (2007) και της Γεωργίας (2008).
[437] Sterner, E., *"Retaliatory Deterrence…."*, pp. 66-67
[438] Libicki, 2009: 52 -59

σύνδεση στο Internet). Σε αυτήν την περίπτωση, ακόμα και αν ο δράσης ταυτοποιηθεί, τα αντίποινα δεν μπορούν να αποτελέσουν αποτρεπτικό παράγοντα.

Από την άλλη μεριά, η διασύνδεση των πληροφοριακών υποδομών σε εθνικό και διεθνές επίπεδο προοικονομεί ότι υπάρχει έντονος κίνδυνος τα αντίποινα που θα εξαπολυθούν να επηρεάσουν πολλούς αποδέκτες, κάποιοι από τους οποίους είναι εντελώς αθώοι (παράπλευρες απώλειες)[439]. Με τον τρόπο αυτό θα δημιουργηθούν νέοι εχθροί για τον αμυνόμενο που εξαπέλυσε τα αντίποινα. Επισημαίνεται ότι, λόγω της διασύνδεσης των IT υποδομών, ακόμα και αν ο αμυνόμενος με τα αντίποινα του στοχοποιήσει μια εχθρική στρατιωτική IT εγκατάσταση, υπάρχει πάντα ο κίνδυνος να πληγούν και μη στρατιωτικές IT υποδομές. Επισημαίνεται ότι σύμφωνα με το Jus in Bello (Δίκαιο των Ένοπλων Συγκρούσεων) θα πρέπει να τηρούνται τρεις προϋποθέσεις κατά την διεξαγωγή των συγκρούσεων. Αυτές είναι η ασυλία των αμάχων, η αναλογικότητα και η πρόκληση περισσότερο καλού σε σχέση με το κακό μέσω των επιθετικών ενεργειών[440]. Καθίσταται λοιπόν σαφές πως, από την στιγμή που δεν μπορεί κάποιος να ελέγξει το ακριβές σημείο που θα καταλήξουν τα αντίποινα του (διασύνδεση στον κυβερνοχώρο), τότε μπορεί να πληγούν άμαχοι, περισσότεροι στόχοι και να προκληθεί πολύ περισσότερη ζημία, η οποία δεν θα αντισταθμίζεται από την αποτροπή του αντιπάλου.

Παράλληλα, προκειμένου τα αντίποινα του αμυνόμενου να επιτύχουν τον αποτρεπτικό τους σκοπό, θα πρέπει ο επιτιθέμενος να κατανοήσει ότι οι δυσλειτουργίες στις IT υποδομές του οφείλονται στα αντίποινα αυτά και όχι σε μηχανικά προβλήματα. Τέλος, σημαντικό ρόλο στην επιλογή κυβερνοαντιποίνων διαδραματίζει ο χρόνος εξαπόλυσης τους. Όπως προαναφέρθηκε, μια έρευνα για την απόδοση της ευθύνης της κυβερνοεπίθεσης απαιτεί πολύ χρόνο. Υπάρχει λοιπόν κίνδυνος, εφόσον τα αντίποινα του αμυνόμενου καθυστερήσουν να εξαπολυθούν προς τον δράστη των κυβερνοεπιθέσεων, να εκληφθούν ως εκδήλωση επιθετικής ενέργειας και όχι ως αμυντική δράση[441].

Θα πρέπει να αναφερθεί ακόμα ότι, η Αποτροπή στο συμβατικό ή το πυρηνικό επίπεδο, μέσω αντιποίνων απειλούσε βάσιμα τον αντίπαλο με μερικό ή πλήρη αφοπλισμό. Στον κυβερνοχώρο όμως αυτό δεν είναι εφικτό. Η εκδήλωση αντιποίνων μέσω κυβερνοεπιθέσεων μπορεί να επιφέρει αποτελέσματα, τα οποία έχουν

---

[439] Lan, Tang & Xin, Zhang, *"Can Cyber Deterrence Work"* στην μελέτη: "Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway", EastWest Institute, 2010, pp. 1-3. Available at: http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf, accessed on April 2011.

[440] Liaropoulos, Andrew (2011), *"Cyber Security and the Law of War: Legal and Ethical Aspects of Cyber Conflict"*, GPSG Working Paper # 7, p. 3. Available at: http://piraeus.academia.edu/AndrewLiaropoulos/Papers/617962/Cyber-Security_and_the_Law_of_War_The_Legal_and_Ethical_Aspects_of_Cyber-conflict, accessed on May 2011

[441] Libicki, 2009: 42

περιορισμένο χρόνο ζωής. Επιπλέον, ο αντίπαλος μπορεί να διεξάγει κυβερνοεπιθέσεις μέσω botnets, γεγονός που σημαίνει ότι στις επιθέσεις αυτές συμμετέχουν άθελα τους απλοί χρήστες Η/Υ, αλλά και οι ψηφιακές υποδομές ουδέτερων χωρών. Συνεπώς, ο αμυνόμενος δεν νομιμοποιείται να προβεί σε αντίποινα εναντίον τους και φυσικά δεν μπορεί να επιτύχει τον πλήρη αφοπλισμό του αντιπάλου του[442].

Επίσης, αξίζει να σημειωθεί πως η επιτυχία της κυβερνοαποτροπής δυσχεραίνεται από την ευκολία με την οποία ένας τρίτος «παίκτης» (third party) δύναται να εμπλακεί στην διένεξη δυο άλλων χωρών[443], επιδεινώνοντας την επικοινωνία μεταξύ των αντιμαχομένων. Η φανερή εκδήλωση κυβερνοεπιθέσεων και αντιποίνων μεταξύ 2 κρατών στον κυβερνοχώρο μπορεί να εκληφθεί ως παράθυρο ευκαιρίας σε τρίτα κράτη ή μη κρατικούς δρώντες (hackers) για να επέμβουν και να επιδεινώσουν την κυβερνοσύγκρουση προς όφελος τους. Επιπλέον, δεν μπορεί να απορριφθεί η περίπτωση όπου ένα τρίτο μέρος θα εμπλακεί με ψευδή ταυτότητα, προκειμένου να ενοχοποιήσει ένα άλλο κράτος ή κάποιον άλλο μη κρατικό δρώντα (False Flag Operation). Όπως γίνεται κατανοητό, η εμπλοκή τρίτων μερών σε μια κυβερνοσύγκρουση δύναται να επιδεινώσει το πρόβλημα της απόδοσης της ευθύνης για τις κυβερνοεπιθέσεις και να επιμηκύνει την κυβερνοσύγκρουση, η οποία μπορεί να κλιμακωθεί στην συνέχεια και σε άλλα επίπεδα[444]. Γίνεται σαφές ότι με την εμπλοκή τρίτων μερών στην διένεξη στον κυβερνοχώρο αφαιρείται η δυνατότητα στον αμυνόμενο, που εκδηλώνει τα αντίποινα, να μεταφέρει το παρακάτω μήνυμα στον αντίπαλο : «Θα σταματήσω τα αντίποινα, για να δω ότι έλαβες το μάθημα, ώστε να μην επαναλάβεις στο μέλλον την μη αποδεκτή πορεία δράσης σου»[445]. Ωστόσο, λόγω του ανωτέρω κινδύνου οι δυο αντίπαλες πλευρές γνωρίζουν ότι εφόσον ξεκινήσουν μια κυβερνοσύγκρουση, δεν είναι προβλέψιμο που θα καταλήξει αυτή.

Όλες οι κυβερνοεπιθέσεις δεν έχουν τον ίδιο αντίκτυπο – με βάση τουλάχιστον την effects – based approach που αναφέρθηκε στο 2^{ο} κεφάλαιο. Παράλληλα, είναι γεγονός ότι ένα κράτος μπορεί σε καθημερινή βάση να είναι αποδέκτης χιλιάδων κυβερνοεπιθέσεων. Είναι λοιπόν λογικό να ειπωθεί πως θα πρέπει τα κράτη να ορίσουν ένα κατώφλι, πέρα από το οποίο η διενέργεια κυβερνοεπίθεσης σε βάρος τους θα ενεργοποιεί αυτόματα την διαδικασία των αντιποίνων[446].Υπό το πλαίσιο αυτό, γίνεται κατανοητό πως εφόσον το κατώφλι τοποθετηθεί χαμηλά, δηλαδή

[442] Ibid, pp. 59 - 62
[443] Ibid, pp. 62 - 63
[444] Ο κίνδυνος του escalation κατά την διάρκεια πυρηνικής σύγκρουσης είναι τυπικά ανύπαρκτος, καθώς η πυρηνική διένεξη αποτελεί το μέγιστο επίπεδο σύγκρουσης. Αντίθετα μια συμβατική σύγκρουση ή μια κυβερνοσύγκρουση θα μπορούσε να κλιμακωθεί κάθετα.
[445] Libicki, Martin C., "*Deterrence in Cyberspace*", pp. 16-20, High Frontier…..
[446] Sterner, E., *"Retaliatory Deterrence…."*, pp. 75-76

συμπεριλαμβάνει τις πιο απλές κυβερνοεπιθέσεις ή ακόμα και τα CNEs, τότε υπάρχει πρόβλημα με το ζήτημα της αξιοπιστίας στην στρατηγική της κυβερνοαποτροπής. Κύρια αιτιολογία για αυτό αποτελεί το γεγονός πως μια χώρα δεν είναι δυνατόν να αντιληφθεί όλες τις κυβερνοεπιθέσεις που δέχεται, με αποτέλεσμα να μην μπορεί να απαντήσει σε όλες. Σε αυτήν την περίπτωση, ο επιτιθέμενος δύναται να εκλάβει την κατάσταση αυτή ως αδυναμία του αντιπάλου του και να δοκιμάσει τις αντοχές του και σε άλλα επίπεδα, πέραν του κυβερνοχώρου. Σύμφωνα με τον καθηγητή Martin Libicki, το κατώφλι θα πρέπει να περιλαμβάνει τις κυβερνοεπιθέσεις που επιδιώκουν σημαντική Διαταραχή ή Διαφθορά στα συστήματα Η/Υ, καθώς και πρόκληση θανάτου ή μεγάλη οικονομική ζημία σε ένα κράτος[447]. Ωστόσο, θα πρέπει να επισημανθεί ότι ο ορισμός κατωφλίου από ένα κράτος για τις μη αποδεκτές κυβερνοεπιθέσεις προς αυτό, μπορεί να εκληφθεί από τον αντίπαλο ως θέληση του κράτους να μην αντιδράσει σε περίπτωση που ο αντίκτυπος μιας κυβερνοεπίθεσης περιορίζεται πίσω από αυτό το κατώφλι.

4.6 Σύγχρονες Τάσεις

Όπως έγινε αντιληπτό από τα παραπάνω, η Αποτροπή, όπως είναι γνωστή στο συμβατικό και το πυρηνικό επίπεδο, παρουσιάζει προβλήματα εφαρμογής στον κυβερνοχώρο. Οι κυβερνοεπιθέσεις δεν μπορούν να αποτραπούν ολοκληρωτικά. Μπορούν όμως να περιοριστούν. Για το λόγο αυτό, εκφράζονται κατά καιρούς απόψεις σχετικά με το ποια μορφή θα πρέπει να λάβει η Αποτροπή για να ενταχθεί καλύτερα στον κυβερνοχώρο. Αν και ο διάλογος για την μορφή της Κυβερνοαποτροπής είναι σε εξέλιξη, ξεχωρίζουν τρεις κύριες τάσεις, εκ των οποίων η πρώτη δίνει έμφαση στην κυβερνοάμυνα, χωρίς να απορρίπτει την κυβερνοεπίθεση υπό την μορφή αντιποίνων όταν αυτό απαιτηθεί, ενώ οι άλλες δυο εστιάζουν ξεκάθαρα στις επιθετικές δυνατότητες στον κυβερνοχώρο.

Η πρώτη προσέγγιση θεωρεί πως πρέπει να δοθεί έμφαση στην κυβερνοαποτροπή μέσω άρνησης (Cyber Deterrence by Denial), αναπτύσσοντας σε εθνικό επίπεδο ιδιαίτερες αμυντικές δυνατότητες στον κυβερνοχώρο, ενώ επισημαίνει ότι θα πρέπει το πρόβλημα των κυβερνοεπιθέσεων να αντιμετωπιστεί σε διεθνές επίπεδο μέσω σύναψης διεθνών συνθηκών και συνεργασίας. Η ανάπτυξη των αμυντικών δυνατοτήτων θα πρέπει να αφορά στην παροχή καλύτερης εκπαίδευσης στο ανθρώπινο δυναμικό που ασχολείται με την κυβερνοάμυνα, αλλά και στην «θωράκιση» των κρίσιμων δικτύων Η/Υ που αφορούν στην εθνική ασφάλεια. Αυτό θα

[447] Libicki, 2009: 65-68

μπορούσε να επιτευχθεί μέσω αλλαγής της αρχιτεκτονικής των υπόψη δικτύων, ώστε αυτά να μετατραπούν σε ολοκληρωμένα οπλικά συστήματα. Επιπλέον, μέσω της σύναψης διεθνών συνθηκών για τον κυβερνοχώρο, οι οποίες θα μπορούσαν να στηριχτούν στην πρακτική παρόμοιων συνθηκών του παρελθόντος (πχ συνθήκη για την απαγόρευση των χημικών όπλων), θα πρέπει να θεσμοθετηθεί μια κοινή διεθνής νομική ορολογία για τον κυβερνοχώρο και ένας κοινά αποδεκτός τρόπος προσέγγισης των κυβερνοεπιθέσεων (πχ Effects – Based Approach), αλλά και να καθοριστούν τα επίπεδα διεθνούς συνεργασίας (δικαιώματα και υποχρεώσεις, εναρμόνιση των εθνικών Δικαίων κτλ). Όπως προαναφέρθηκε, η προσέγγιση αυτή δεν απορρίπτει την Κυβερνοαποτροπή μέσω Αντιποίνων (Cyber Deterrence by Punishment), αλλά υποστηρίζει ότι τα αντίποινα θα πρέπει να υπόκεινται στις αρχές της διεθνούς νομιμότητας.

Η δεύτερη προσέγγιση στηρίζεται στο αξίωμα του κυβερνοχώρου ότι η επίθεση υπερτερεί της άμυνας, οπότε η καλύτερη άμυνα προκύπτει μέσω της επίθεσης. Η τάση αυτή δίνει έμφαση στην ανάπτυξη ιδιαίτερων επιθετικών δυνατοτήτων στον κυβερνοχώρο και στην άμεση εκδήλωση αντιποίνων προς την κατεύθυνση από την οποία προήλθε η κυβερνοεπίθεση. Η πρακτική αυτή ονομάζεται ενεργητική άμυνα (Active Defences)[448] και μεταφέρει την ευθύνη για την εκδήλωση των αρχικών κυβερνοεπιθέσεων στις ηγεσίες των κρατών από την επικράτεια των οποίων διεξήχθηκαν οι κυβερνοεπιθέσεις. Συνεπώς, τα κράτη δεν θα μπορούν να προφασιστούν ότι οι επιθέσεις διεξήχθηκαν από ακτιβιστές του κυβερνοχώρου τους οποίους δεν ελέγχουν, καθώς θα θεωρούνται υπεύθυνα για τον πλημμελή έλεγχο τον πληροφοριακών υποδομών τους. Η προσέγγιση αυτή θεωρεί πως μεταφέροντας το βάρος στις ηγεσίες των κρατών, θα περιοριστεί η δράση των μη κρατικών δρώντων και θα υπάρξει μεγαλύτερη ευκρίνεια στην απόδοση ευθυνών για τις κυβερνοεπιθέσεις.

Η τρίτη προσέγγιση είναι πιο ακραία και θεωρεί ότι η Αποτροπή στον κυβερνοχώρο θα πρέπει να βασίζεται στον φόβο των αντιποίνων, με τα κράτη να προσπαθούν να κυριαρχήσουν το ένα στο άλλο μέσω της ανάπτυξης επιθετικών δυνατοτήτων στον κυβερνοχώρο. Ως αποτέλεσμα, τα κράτη θα οδηγηθούν στην δημιουργία ενός συστήματος ισορροπίας δυνάμεων, στο οποίο θα έχουν τον πρώτο λόγο οι Υπερδυνάμεις του κυβερνοχώρου. Κατά αναλογία με τον Ψυχρό Πόλεμο, το σύστημα αυτό θα στηρίζεται στην ύπαρξη αμοιβαίου φόβου σχετικά με τις «εξουθενωτικές» συνέπειες που θα έχει για όλους η διατάραξη της ισορροπίας στον

[448] Carr, 2010: 46

κυβερνοχώρο (Cyber MAD: Mutual Assured Debilitation)[449]. Μέσω λοιπόν της Cyber MAD, η προσέγγιση αυτή θεωρεί πως θα περιοριστούν επαρκώς οι συγκρούσεις στον κυβερνοχώρο.

[449] Crosston, Matthew D., *"World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence"*, Strategic Studies Quarterly, Spring 2011, pp. 100-116. Available at: http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf, accessed on June 2011

5. Συμπεράσματα

Όπως έχει γίνει αντιληπτό, από τις αρχές της δεκαετίας του 1990 οι Η/Υ, τα δίκτυα Η/Υ και η διασύνδεση τους αποτέλεσαν στρατηγική επιλογή για όλες τις χώρες, ιδιαίτερα τις ανεπτυγμένες. Η εφαρμογή των Η/Υ σε διάφορους τομείς της ανθρώπινης δραστηριότητας (οικονομία, επιχειρήσεις, ένοπλες δυνάμεις, τράπεζες, παιδεία, επικοινωνίες κτλ) βοήθησε στον αυτοματισμό των διαδικασιών, την μείωση του λειτουργικού τους κόστους και την αύξηση των κερδών. Ιδιαίτερα, η εφαρμογή των Η/Υ και των δικτύων τους στις ένοπλες δυνάμεις οδήγησε στην Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA) και προσέδωσε στους στρατιωτικούς σχεδιασμούς μεγαλύτερη ακρίβεια και αποτελεσματικότητα, μειώνοντας το κόστος, με παράλληλη αύξηση στην έννοια της ασφάλειας. Αν και κατά τα πρώτα χρόνια, το αρχικό επίπεδο διασύνδεσης των ανωτέρω δικτύων Η/Υ ήταν περιορισμένο, στην συνέχεια η ανάπτυξη του Internet οδήγησε σε μεγαλύτερα επίπεδα διασύνδεσης. Σήμερα λοιπόν, πολλά κράτη έχουν βασίσει την λειτουργία των κρίσιμων υποδομών τους στους Η/Υ και την δικτύωση τους.

Η αλματώδης ανάπτυξη του Internet μετά το 1990 και η ευκολία πρόσβασης σε αυτό από τον απλό χρήστη οδήγησε σε μεγαλύτερα επίπεδα διασύνδεσης και επικοινωνίας την ανθρωπότητα. Αν και στα πρώτα χρόνια ανάπτυξης του διαδικτύου, το προνόμιο της διασύνδεσης ανήκε στα κράτη και στις μεγάλες επιχειρήσεις, στην συνέχεια η δυνατότητα διασύνδεσης έγινε προνόμιο και των απλών πολιτών. Σήμερα, περισσότεροι από 2 δισεκατομμύρια άνθρωποι έχουν πρόσβαση στο Internet. Το τίμημα όμως για την παγκόσμια διασύνδεση ήταν τα χαμηλά επίπεδα ασφαλείας στο διαδίκτυο. Όπως προαναφέρθηκε, οι βασικές αρχές λειτουργίας του διαδικτύου εστίαζαν στην δυνατότητα εύκολης πρόσβασης σε αυτό, διατηρώντας χαμηλά επίπεδα ασφάλειας στους χρήστες του. Δεν πρέπει να παραβλεφθεί όμως το γεγονός ότι, το Internet δημιουργήθηκε για να εξυπηρετεί τις ανάγκες επικοινωνίας της ακαδημαϊκής κοινότητας και των αμερικανικών ενόπλων δυνάμεων, οι οποίοι αποτελούσαν περιορισμένους και «ασφαλείς» τομείς της κοινωνίας και όχι για να εξυπηρετεί τις ανάγκες ενός τόσου μεγάλου αριθμού χρηστών όπως τον σημερινό.

Σταδιακά λοιπόν, από τις αρχές της δεκαετίας του 1990 άρχισε να εμφανίζεται η έννοια του Κυβερνοχώρου, του εικονικού δηλαδή χώρου που είχε δημιουργήσει ο άνθρωπος μέσω των Η/Υ προκειμένου να επικοινωνεί και να διεκπεραιώνει με μεγαλύτερη ταχύτητα και αποτελεσματικότητα τις διάφορες δραστηριότητες του. Όπως ήταν φυσικό, η ταχεία ανάπτυξη του Κυβερνοχώρου πραγματοποιήθηκε χωρίς την προσπάθεια επαρκούς διόρθωσης των τρωτοτήτων που πήγαζαν είτε από το λογισμικό και το υλικό των Η/Υ, είτε από την δαιδαλώδη αρχιτεκτονική του διαδικτύου,

αλλά και των υπολοίπων δικτύων Η/Υ. Ως αποτέλεσμα, υπήρξαν προσπάθειες εκμετάλλευσης αυτών των αδυναμιών, από τους λεγόμενους Hackers, οι οποίοι κάνοντας χρήση των εξειδικευμένων γνώσεων τους και των κακόβουλων λογισμικών μπορούσαν να εξυπηρετούν τα προσωπικά τους συμφέροντα ή τα συμφέροντα άλλων (επιχειρήσεων, οργανωμένο έγκλημα, τρομοκρατία, κράτη κτλ).

Ο κυβερνοχώρος αποτελεί στρατηγικό μέσο, καθώς μέσω αυτού μπορούν να δεχθούν κυβερνοεπιθέσεις τόσο οι στρατιωτικές (Military) όσο και οι μη στρατιωτικές (Civilian) υποδομές. Οι συγκρούσεις σε αυτήν την περιοχή ήταν αναμενόμενη εξέλιξη, καθώς σε ένα διάστημα 20 περίπου ετών αυξήθηκαν ο αριθμός των χρηστών των Η/Υ, η διασύνδεση των δικτύων Η/Υ, η εξάρτηση από αυτά, η αποτελεσματικότητα και ο αριθμός των κακόβουλων λογισμικών, καθώς και η εξειδίκευση των Hackers. Σε αυτές έπαιρναν μέρος μεμονωμένα άτομα, αλλά ακόμα και κράτη. Οι λόγοι που οι εμπλεκόμενοι επιδίωκαν τις κυβερνοσυγκρούσεις ήταν πολλές φορές:

α. Ο ακτιβισμός. Η πολιτική αντιπαράθεση με τον αντίπαλο μέσα από τον κυβερνοχώρο.

β. Το οικονομικό κέρδος μέσα από την υπεξαίρεση οικονομικών δεδομένων, με αποτέλεσμα την οικονομική ζημία του αντιπάλου.

γ. Η απόκτηση συγκριτικού πλεονεκτήματος μέσα από την υπεξαίρεση στρατηγικών δεδομένων.

δ. Η πρόκληση φόβου και αναστάτωσης σε μια κοινωνία.

ε. Ο εξαναγκασμός του αντιπάλου προς μια αποδεκτή συμπεριφορά.

στ. Οι αναίμακτες συνέπειες από τις κυβερνοεπιθέσεις.

ζ. Η ανωνυμία στον Κυβερνοχώρο και η δυσκολία απόδοσης της ευθύνης για αυτές (δυνατότητα εύλογης άρνησης).

η. Η απουσία ενός κοινά αποδεκτού από τα κράτη νομικού πλαισίου για τις κυβερνοεπιθέσεις, το οποίο συνέτεινε στην μη συνεργασία των κρατών και την ατιμωρησία των ιθυνόντων για τις κυβερνοεπιθέσεις.

θ. Το μικρό κόστος διεξαγωγής των κυβερνοεπιθέσεων σε συνδυασμό με την δυνατότητα επιτυχίας ασύμμετρου πλήγματος σε έναν ισχυρό αντίπαλο, ακόμα και αν αυτός βρίσκεται σε μεγάλη απόσταση. Επίσης, σημειώνεται ότι το κέρδος από την διεξαγωγή της κυβερνοεπίθεσης δύναται να είναι μεγαλύτερο από το κόστος διεξαγωγής της.

ι. Το προβάδισμα της επίθεσης σε σχέση με την άμυνα στον κυβερνοχώρο.

ια. Η μεγάλη πιθανότητα αιφνιδιασμού του αντιπάλου.

Ο Κυβερνοπόλεμος προκρίνεται ως η πιο σοβαρή μορφή κυβερνοσύγκρουσης, καθώς σε αυτήν εμπλέκονται τα κράτη, ενώ οι ζημίες που μπορούν να προκληθούν

από την διεξαγωγή κυβερνοεπιθέσεων είναι σαφώς μεγαλύτερες σε σχέση με τις άλλες μορφές κυβερνοσυγκρούσεων. Αυτό οφείλεται στο γεγονός ότι τα κράτη διαθέτουν μεγαλύτερα ποσά για την έρευνα και την ανάπτυξη εξειδικευμένων κυβερνοόπλων, ενώ έχουν, σε σχέση με τους Μη Κρατικούς Δρώντες, το προβάδισμα στην τεχνογνωσία των κυβερνοεπιθέσεων.

Σε αντίθεση με τον συμβατικό πόλεμο, στον κυβερνοπόλεμο οι μη κρατικοί δρώντες διεκδικούν σημαντικό μερίδιο στην χρήση βίας, καθώς το κόστος εισόδου στον κυβερνοχώρο είναι χαμηλό, ενώ η απόκτηση απλών κυβερνοόπλων έχει σχεδόν μηδενικό κόστος. Επίσης, θα πρέπει να τονιστεί ότι κατά την διάρκεια ενός κυβερνοπολέμου δεν είναι δυνατή η κατάληψη εδάφους, η ολική καταστροφή ή ο αφοπλισμός του αντιπάλου, αλλά ούτε και η επίτευξη συνολική νίκης σε μια πολεμική σύγκρουση. Αυτά που δύναται να επιτευχθούν είναι ο περιορισμός της ελευθερίας κινήσεων του αντιπάλου στον κυβερνοχώρο εντός συγκεκριμένου χρονικού πλαισίου και ο αιφνιδιασμός του αντιπάλου. Με δεδομένο ότι ο κυβερνοπόλεμος στοχεύει στην συστημική αποδιάρθρωση του αντιπάλου, πλήττοντας μια καίρια αδυναμία του, θεωρείται ως ένα είδος πολέμου ελιγμού.

Από τις 2 βασικές μορφές του Κυβερνοπολέμου (Στρατηγικός και Επιχειρησιακός Κυβερνοπόλεμος), ο Επιχειρησιακός Κυβερνοπόλεμος, δηλ. οι κυβερνοεπιθέσεις που λαμβάνουν χώρα προς υποστήριξη ενός συμβατικού πολέμου, θεωρείται ως πιο πιθανή επιλογή για τα κράτη, καθώς είναι πιο εύκολη η επίτευξη των αντικειμενικών σκοπών του. Αντίθετα, ο Στρατηγικός Κυβερνοπόλεμος στοχεύει στην στρατηγική παράλυση του αντιπάλου και στον εξαναγκασμό του σε υιοθέτηση συγκεκριμένης συμπεριφοράς, κάτι το οποίο θεωρείται πολύ δύσκολο να επιτευχθεί. Μέχρι σήμερα δεν έχει διαφανεί πρακτικά η δυνατότητα εφαρμογής μιας τέτοιου είδους κυβερνοσύγκρουσης μεταξύ των κρατών. Αυτό οφείλεται στους εξής παράγοντες:

α. Ο κυβερνοχώρος δεν αποτελεί μια ενιαία περιοχή. Υπάρχει τουλάχιστον ένα τμήμα του που αναλογεί στην κάθε αντίπαλη οντότητα. Ακόμα και αν ένας αντίπαλος εξαναγκαστεί να «αποσυνδεθεί» από το τμήμα του κυβερνοχώρου που ελέγχει για κάποιο χρονικό διάστημα, θα έχει πάντα την επιλογή να βρει στην συνέχεια νέα σημεία πρόσβασης στον Κυβερνοχώρο.

β. Η επίδραση μιας κυβερνοεπίθεσης έχει συνήθως συγκεκριμένη χρονική διάρκεια και εξαρτάται από την κυβερνοάμυνα του αντιπάλου.

γ. Απαιτείται η χώρα – στόχος να είναι ιδιαίτερα εξαρτημένη από την τεχνολογία πληροφορικής και να έχει στηρίξει πλήρως τις κρίσιμες υποδομές της στα δίκτυα Η/Υ, χωρίς παράλληλα να έχει πάρει τα κατάλληλα μέτρα για την προφύλαξη τους.

δ. Δεν έχουν προκύψει μέχρι σήμερα από την διεξαγωγή κυβερνοεπιθέσεων ανθρώπινες απώλειες, στις οποίες οι σύγχρονες κυβερνήσεις καταδεικνύουν ευαισθησία.

Τα κράτη συνηθίζουν να χρησιμοποιούν τους Μη Κρατικούς Δρώντες προκειμένου οι τελευταίοι να διεξάγουν επιχειρήσεις κυβερνοπολέμου για λογαριασμό τους και παράλληλα να έχουν (τα κράτη) την επιλογή της εύλογης άρνησης σχετικά με την άμεση εμπλοκή τους στις κυβερνοεπιθέσεις. Η διασύνδεση τους με τους Μη Κρατικούς Δρώντες είναι χαλαρή και δεν υπάρχουν απτές αποδείξεις για την συνεργασία τους. Οι παράγοντες αυτοί οργανώνονται σε ομάδες, γνωστές ως Cyber Militias, οι οποίες ανεξάρτητα του βαθμού εξειδίκευσης που έχουν στην τεχνολογία πληροφορικής (IT), είναι πρόθυμες να διεξάγουν κυβερνοεπιθέσεις προκειμένου να πετύχουν ένα συγκεκριμένο πολιτικό σκοπό. Το φαινόμενο αυτό συναντάται έντονα στην Ρωσία και στην Κίνα. Θα πρέπει επίσης να σημειωθεί ότι, τα κράτη δεν μπορούν να έχουν τον πλήρη έλεγχο αυτών των ομάδων, αλλά ούτε πλήρη γνώση για την ταυτότητα του συνόλου των μελών τους. Συνεπώς, υπάρχει έντονος ο κίνδυνος της ανεξέλεγκτης δράσης των Cyber Militias, με αρνητικές συνέπειες για το συνεργαζόμενο κράτος.

Παρά την πάροδο μιας εικοσαετίας από τότε που ξεκίνησαν οι κυβερνοεπιθέσεις, δεν έχει υπάρξει συνολικά μιας διεθνής συμφωνία για την αντιμετώπισης τους, αλλά ούτε και μια κοινή νομική ορολογία αναφορικά με τον κυβερνοχώρο και τις δραστηριότητες μέσα σε αυτόν. Ως αποτέλεσμα, τα κράτη προσπαθούν να αντιμετωπίσουν τις κυβερνοεπιθέσεις σε εθνικό επίπεδο, χωρίς να διαφαίνεται σοβαρή προσπάθεια για μια διεθνή συνεργασία. Απόρροια αυτής της έλλειψης συνεργασίας είναι η απουσία μιας διεθνούς ρυθμιστικής Αρχής στο διαδίκτυο και κατ' επέκταση στον κυβερνοχώρο που να επιβάλλει την τάξη. Θα ήταν λοιπόν δόκιμο να ειπωθεί ότι στον κυβερνοχώρο επικρατεί αναρχία.

Σύμφωνα με έρευνες, το ενδιαφέρον των χωρών για τον κυβερνοπόλεμο είναι εδώ και χρόνια ιδιαίτερα αναπτυγμένο , καθώς τα κράτη επιθυμούν να προβάλλουν την ισχύ τους στον κυβερνοχώρο. Περισσότερες από 120 χώρες χρησιμοποιούν το Internet για δραστηριότητες κατασκοπείας σε πολιτικό, στρατιωτικό και οικονομικό επίπεδο. Πολλές χώρες έχουν εντάξει τον κυβερνοπόλεμο στον στρατιωτικό σχεδιασμό ή την οργάνωση τους (π.χ Ρωσία, Κίνα, ΗΠΑ, Ισραήλ, Ιράν, Β. Κορέα κα), ενώ σε άλλες χώρες υπάρχουν μη στρατιωτικές υπηρεσίες («πολιτικές υπηρεσίες»), οι οποίες είναι υπεύθυνες για την κυβερνοασφάλεια. Εκείνο που έχει ιδιαίτερο ενδιαφέρον είναι ότι χώρες, που είτε διαθέτουν είτε προσπαθούν να αποκτήσουν το απόλυτο όπλο (πυρηνικά) (Ρωσία, Κίνα, ΗΠΑ, Ισραήλ, Ιράν, Β. Κορέα), έχουν επιδοθεί εδώ και χρόνια

σε έναν αγώνα δρόμου προκειμένου να αποκτήσουν σημαντικές δυνατότητες κυβερνοπολέμου.

Από τα στοιχεία που υπάρχουν στις ανοιχτές πηγές, γίνεται κατανοητό πως οι ΗΠΑ πρωτοπόρησαν στην ανάπτυξη επιθετικών και αμυντικών δυνατοτήτων στον κυβερνοχώρο και αναπτύχθηκαν άνισα σε σχέση με τις υπόλοιπες χώρες. Είχαν κάθε λόγο να το κάνουν, καθώς από τις αρχές της δεκαετίας του 1990 στήριξαν την οικονομική ανάπτυξη και την άμυνα τους στα δίκτυα των Η/Υ και την διασύνδεση τους. Το γεγονός όμως αυτό δημιούργησε ένα δίλημμα ασφαλείας σε χώρες όπως η Κίνα και η Ρωσία, καθώς τα μέτρα που αύξαναν την ασφάλεια των ΗΠΑ (πχ από τα επιθετικά κυβερνοόπλα), ταυτόχρονα μείωναν την δική τους ασφάλεια. Όπως διαφάνηκε, η Κίνα, η Ρωσία και το Ιράν κατανόησαν την άνιση ανάπτυξη στον τομέα της τεχνολογίας της πληροφορικής με αφορμή τον 1^{ο} Πόλεμο του Κόλπου. Το γεγονός αυτό δημιούργησε φόβο σε αυτές τις χώρες, με αποτέλεσμα να προσπαθήσουν να εξισορροπήσουν τον ανερχόμενο κίνδυνο από τις ΗΠΑ (κεφάλαιο 3). Αντίστοιχα η Β. Κορέα λαμβάνοντας υπόψη την μειονεκτική της θέση στο διεθνές σύστημα λόγω της απομόνωσης της, κατανόησε πως μέσα από στρατηγικές ασυμμετρίας θα μπορούσε να επιβιώσει. Για το λόγο αυτό έδωσε έμφαση στην ανάπτυξη των δυνατοτήτων της στον κυβερνοπόλεμο, παράλληλα με την ανάπτυξη των βαλλιστικών πυραύλων και του πυρηνικού της προγράμματος. Από την άλλη μεριά, το Ισραήλ βρισκόμενο σε μια εχθρική περιοχή και με κύριο γνώμονα την επιβίωση του δεν μπορούσε παρά να αναπτύξει σημαντικές δυνατότητες κυβερνοπολέμου. Γίνεται λοιπόν κατανοητό ότι η προσέγγιση των παραπάνω χωρών στο ζήτημα του κυβερνοχώρου έγινε ακολουθώντας τις επιταγές της ρεαλιστικής θεώρησης των διεθνών σχέσεων.

Από την ανάλυση των κυβερνοεπιθέσεων στην Εσθονία (2007), την Γεωργία (2008) και το Ιράν (2009-2010) προκύπτουν σημαντικά συμπεράσματα. Πρώτο από όλα σημειώνεται ότι οι χώρες που είναι εξαρτημένες ιδιαίτερα από την τεχνολογία πληροφορικής και δεν λαμβάνουν σημαντικά μέτρα για την ασφάλεια στον κυβερνοχώρο είναι ιδιαίτερα ευαίσθητες στις κυβερνοεπιθέσεις και δύναται να έχουν μεγάλο οικονομικό και κοινωνικό κόστος από αυτές (περίπτωση Εσθονίας). Ωστόσο, ακόμα και οι λιγότερο εξαρτημένες χώρες από την τεχνολογία πληροφορικής, οι οποίες δεν λαμβάνουν σημαντικά μέτρα για την ασφάλεια στον κυβερνοχώρο, μπορούν να ζημιωθούν στο οικονομικό και το κοινωνικό επίπεδο (περίπτωση Γεωργίας).

Επιπλέον, υπογραμμίζεται ότι η χρήση των Μη Κρατικών Δρώντων από την Ρωσία για διεξαγωγή κυβερνοεπιθέσεων εξαναγκασμού κατά των αντιπάλων της, αποτελεί συνήθης τακτική της. Το ίδιο βέβαια συνηθίζουν να πράττουν και άλλες χώρες όπως η Κίνα και η Β. Κορέα. Δύναται λοιπόν οι κυβερνοεπιθέσεις να χρησιμοποιηθούν

από τα κράτη για την εξάσκηση πιέσεων και τον εξαναγκασμό του αντιπάλου σε συγκεκριμένη συμπεριφορά, όταν άλλου είδους πιέσεις δεν φέρουν αποτέλεσμα.

Επιπρόσθετα, διαφάνηκε ότι η διεξαγωγή κυβερνοπολέμου, επικουρικά σε έναν συμβατικό πόλεμο, έχει θετικά αποτελέσματα για τον επιτιθέμενο. Με μικρό κόστος, ο επιτιθέμενος μπορεί να επιτύχει δυσανάλογη ζημία στον αντίπαλο και να τον αιφνιδιάσει. Υπογραμμίζεται επίσης ότι η προσπάθεια αντιμετώπισης των κυβερνοαπειλών δυσχεραίνεται υπερβολικά από την ανωνυμία στον κυβερνοχώρο, αλλά και από την αδυναμία απόδοσης της ευθύνης για μια κυβερνοεπίθεση.

Παράλληλα τονίζεται ότι ο κίνδυνος από τις κυβερνοεπιθέσεις δεν αφορά μόνο τα δίκτυα Η/Υ που είναι συνδεδεμένα στο Internet, αλλά και αυτά που χαρακτηρίζονται ως “Air Gapped” . Τα δίκτυα Η/Υ που υπήρχαν στην Natanz και το Bushehr δεν διασυνδέονταν με το Internet, αλλά παρόλα αυτά έγιναν αποδέκτες κυβερνοεπιθέσεων. Αξίζει επίσης να σημειωθεί ότι με την πάροδο του χρόνου, τα κυβερνοόπλα αποκτούν μεγαλύτερη ακρίβεια ως αναφορά την επίτευξη του στόχου τους (πχ Stuxnet), ενώ τα αποτελέσματα τους, περάν του κυβερνοχώρου, μπορούν να εμφανιστούν και στον φυσικό χώρο (Stuxnet-γεννήτριες φυγοκέντρησης).

Όσον αφορά στην Αποτροπή στον Κυβερνοχώρο, αυτή παρουσιάζει προβλήματα εφαρμογής. Οι κυριότεροι λόγοι έχουν να κάνουν τόσο με την «φύση» του κυβερνοχώρου (ιδιαιτερότητες) όσο και με τις διαφορετικές προσεγγίσεις των κρατών απέναντι σε αυτόν. Σε αντίθεση με τα συμβατικά και τα πυρηνικά όπλα, τα οποία είχαν δοκιμαστεί και οι καταστροφικές δυνατότητες τους ήταν γνωστές σε όλους, οι δυνατότητες των κυβερνοόπλων καλύπτονται από ένα πέπλο μυστηρίου. Υπάρχει λοιπόν ένα έλλειμμα αξιοπιστίας αναφορικά με τα κυβερνοόπλα. Παράλληλα, τα κράτη αναπτύσσουν τις δυνατότητες τους στον κυβερνοχώρο μυστικά, με αποτέλεσμα ένας εν δυνάμει αντίπαλος τους να μην γνωρίζει ότι θα αντιμετωπίσει αυτές τις δυνατότητες σε περίπτωση σύγκρουσης και ότι θα έχει μεγάλο κόστος από αυτές. Επιπλέον, η απουσία κοινής νομικής ορολογίας για τον κυβερνοχώρο προκαλεί παρερμηνείες και λανθασμένους υπολογισμούς και ενισχύει το επίπεδο της ασάφειας που προαναφέρθηκε.

Από την άλλη μεριά, οι hackers, εκμεταλλευόμενοι την δαιδαλώδη αρχιτεκτονική του Internet και την πολυπλοκότητα των δικτύων Η/Υ, χρησιμοποιούν τις τεχνικές τους γνώσεις για να καλύπτουν τα ίχνη των επιθέσεων τους. Ως αποτέλεσμα, δεν γίνονται γνωστά η ταυτότητα του επιτιθέμενου και το σημείο που θα πρέπει να κατευθυνθούν τα αντίποινα. Αξίζει να σημειωθεί ότι, οι σύγχρονες μέθοδοι διερεύνησης των κυβερνοεπιθέσεων είναι χρονοβόρες και έχουν μεγάλο κόστος, ενώ τα αποτελέσματα τους δεν είναι πάντοτε τα αναμενόμενα. Συνεπώς, δημιουργούνται ερωτηματικά σχετικά με την νομιμότητα των πιθανών αντιποίνων από τον αντίπαλο μετά από ένα

μεγάλο χρονικό διάστημα. Επιπρόσθετα, η συνεργασία των κρατών σε διαδικασίες διερεύνησης των κυβερνοεπιθέσεων είναι συνήθως ανέφικτη, καθώς τα κράτη επικαλούνται θέματα εθνικής ασφάλειας και κυριαρχίας.

Θα πρέπει ακόμα να τονιστεί ότι, η ασυμμετρία στον κυβερνοχώρο προσφέρει την δυνατότητα σε έναν επίδοξο hacker να αποκομίσει μεγάλο κέρδος από μια κυβερνοεπίθεση, ενώ το κόστος που θα έχει για την δράση του είναι συνήθως πολύ μικρό. Η έλλειψη επαρκούς νομοθετικού πλαισίου για την αντιμετώπιση των κυβερνοεπιθέσεων σε εθνικό ή διεθνές επίπεδο και η αδυναμία αποκάλυψης της ταυτότητας ενός hacker τις περισσότερες φορές δεν λειτουργούν αποτρεπτικά.

Παράλληλα, το κλίμα ασάφειας στον κυβερνοχώρο επιδεινώνεται από την δυνατότητα εμπλοκής στις κυβερνοσυγκρούσεις πολλών και διαφορετικών «παιχτών», οι οποίοι μπορεί να είναι Κράτη ή Μη Κρατικοί Δρώντες. Ιδιαίτερα στην περίπτωση των Μη Κρατικών Δρώντων τίθεται πολλές φορές υπό αμφισβήτηση η δυνατότητα από μέρους τους για ορθολογική λήψη αποφάσεων. Η δυνατότητα εμπλοκής κάποιου τρίτου παράγοντα σε μια υπό εξέλιξη κυβερνοσύγκρουση επιδεινώνει την επικοινωνία μεταξύ των αντιμαχομένων, καθώς δεν μπορεί να διευκρινιστεί ποιος διενεργεί τελικά τις κυβερνοεπιθέσεις και ποιες είναι οι προθέσεις του (πχ κλιμάκωση ή αποκλιμάκωση;). Στην περίπτωση της διεξαγωγής κυβερνοεπιθέσεων από Μη Κρατικούς Δρώντες δεν μπορεί επίσης να εξασφαλιστεί η διασύνδεση τους με ένα κράτος, γεγονός που γεννά ερωτηματικά για την νομιμότητα εξαπόλυσης αντιποίνων κατά της χώρας από την οποία ξεκίνησαν οι κυβερνοεπιθέσεις.

Από την άλλη μεριά, η επιλογή των αντιποίνων από τον αμυνόμενο γίνεται υπό την προϋπόθεση ότι ο επιτιθέμενος διαθέτει επαρκείς ΙΤ υποδομές, οι οποίες μπορούν να στοχοποιηθούν. Ωστόσο, η κατάσταση αυτή δεν είναι πάντα ο κανόνας. Επιπλέον, η διασύνδεση των πληροφοριακών υποδομών σε εθνικό και διεθνές επίπεδο προοικονομεί ότι υπάρχει έντονος κίνδυνος τα αντίποινα που θα εξαπολυθούν να επηρεάσουν πολλούς αποδέκτες, κάποιοι από τους οποίους είναι εντελώς αθώοι (κίνδυνος παράπλευρων απωλειών). Θα πρέπει ακόμα να σημειωθεί ότι η επίδραση των αντιποίνων προς τον επιτιθέμενο είναι προσωρινή. Συνεπώς, όταν το κέρδος από την εκδήλωση της κυβερνοεπίθεσης είναι μεγάλο, τότε ο επιτιθέμενος δεν θα αποτραπεί.

Τέλος, θα πρέπει να τονιστεί ότι, ένα κράτος είναι αδύνατον να αντιληφθεί όλες τις κυβερνοεπιθέσεις που εκδηλώνονται εις βάρος του και συνεπώς μια στρατηγική Αποτροπής όλων των κυβερνοεπιθέσεων στερείται αξιοπιστίας. Σε περίπτωση όμως που ένα κράτος ορίσει ρητά ένα κατώφλι, πέρα από το οποίο η διενέργεια κυβερνοεπιθέσεων σε βάρος του θα ενεργοποιεί αυτόματα την διαδικασία αντιποίνων, υπάρχει ο κίνδυνος παρερμηνείας από τον αντίπαλο. Ο επιτιθέμενος μπορεί να εκλάβει

αυτήν την απόφαση ως θέληση του κράτους να μην αντιδράσει σε περίπτωση που ο αντίκτυπος μιας κυβερνοεπίθεσης περιορίζεται πίσω από αυτό το κατώφλι.

Λαμβάνοντας υπόψη όλα τα παραπάνω γίνεται αντιληπτό ότι, οι Κυβερνοσυγκρούσεις είναι μια πραγματικότητα, την οποία τα κράτη θα καλούνται να αντιμετωπίσουν ολοένα και περισσότερο στο μέλλον. Ιδιαίτερα, ο Κυβερνοπόλεμος διαφαίνεται ότι είτε θα αποτελέσει μια συνήθη εναλλακτική των κρατών, προτού αποφασίσουν να προβούν σε άλλου είδους συγκρούσεις, είτε θα συνοδεύει αυτές τις συγκρούσεις. Με δεδομένο την ολοένα και μεγαλύτερη εξάρτηση των κρίσιμων υποδομών των κρατών από τα δίκτυα Η/Υ, τα κράτη θα επιλέγουν την διεξαγωγή επιχειρήσεων στον κυβερνοχώρο για να προασπίζονται τα συμφέροντα τους και να εξασκούν πιέσεις στους αντιπάλους τους. Παράλληλα, λόγω της μεγάλης διασύνδεσης που υπάρχει στον κυβερνοχώρο, η διεξαγωγή κυβερνοπολέμου μεταξύ μικρού αριθμού κρατών θα δύναται να οδηγήσει στην είσοδο περισσότερων κρατών σε αυτόν (κίνδυνος από τις παράπλευρες απώλειες). Επιπλέον, με βάση την συνεχή εξέλιξη των κυβερνοόπλων και την αύξηση της αποτελεσματικότητας τους, οι συνέπειες από έναν κυβερνοπόλεμο θα γίνονται ολοένα και πιο επώδυνες. Από την άλλη μεριά, διαφαίνεται ότι η έννοια της Αποτροπής δεν μπορεί να εφαρμοστεί στον κυβερνοχώρο με την ίδια επιτυχία που είχε στο συμβατικό ή στο πυρηνικό επίπεδο. Συνεπώς, καθίσταται ως επιτακτική ανάγκη η προσέγγιση με ιδιαίτερη σοβαρότητα του φαινομένου των κυβερνοσυγκρούσεων και του κυβερνοπολέμου από την διεθνή κοινότητα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία & Άρθρα στην Ελληνική Γλώσσα

Bull, Hedley, Άναρχη Κοινωνία: *Μελέτη της τάξης στην παγκόσμια πολιτική* (Εκδόσεις Ποιότητα, Αθήνα, 2007 (Γ' έκδοση))

Γαρίδης, Παναγιώτης & Δεληγιαννάκης Μανώλης, *Σύγχρονο Λεξικό Πληροφορικής* (Εκδόσεις Φλώρος, Αθήνα, 1993)

Γκισνέλ, Ζαν, *Πόλεμοι στον Κυβερνοχώρο: Μυστικές Υπηρεσίες και Internet* (Εκδόσεις Στάχυ, Αθήνα 1997), σελ. 305-312

Κολιόπουλος, Κωνσταντίνος, *Η στρατηγική σκέψη Από την Αρχαιότητα ως σήμερα* (Εκδόσεις Ποιότητα, Αθήνα, 2008)

Κουσκουβέλης, Ηλίας Ι., *Εισαγωγή στις Διεθνείς Σχέσεις* (Ε' Έκδοση), (Εκδόσεις Ποιότητα, Αθήνα, 2007)

Κωνσταντόπουλος, Ιωάννης, *Οικονομία και Κατασκοπεία: Θεωρία και Πράξη* (Εκδόσεις Ποιότητα, Βάρη Αττικής, 2010)

Λυγερού, Νεφέλη, *"Anonymous: Οι πολιτικοί ακτιβιστές του Διαδικτύου"*, σελ. 102-103, εβδομαδιαίο περιοδικό Επίκαιρα, 123^{ο} τεύχος, 23/02-29/02/12

Μπόση, Μαίρη, *Περί Ορισμού της Τρομοκρατίας* (Εκδόσεις Π. Τραυλός, Αθήνα, 2000)

Πλατιάς, Αθανάσιος & Ήφαιστος, Παναγιώτης, *Ελληνική Αποτρεπτική Στρατηγική* (Εκδόσεις Παπαζήση, Αθήνα, 1992)

Ξενόγλωσσα Βιβλία & Άρθρα

Albright, David, Brannan, Paul & Walrond, Christina, *"Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?"*, ISIS Report, 22/12/2010. Available at: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/, accessed on April 2011

Alexander, Keith B., "*Warfighting in Cyberspace*", Joint Force Quarterly, issue 46, 3rd quarter2007. Available at: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf, accessed on May 2011.

Arquilla, John, *"Cyberwar Is Already Upon Us"*, Foreign Policy, March/April 2012. Available:http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us, accessed on 28/2/2012

Beaufre, A., *"A Strategy of Deterrence"* στο Freedman, Lawrence (Ed.), *War* (Oxford University Press, Oxford, 1994), p. 239.

Billo, Charles & Chang, Welton, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Institute For Security Technology Studies at Dartmouth College, Hannover, 2004),

Broad, William J., Markoff, John & Sanger David E., *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay"*, the New York Times, 15/1/2011. Available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all, accessed on 8/2/2012

Bush, George W., *National Strategy to Secure Cyberspace*, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, accessed on May 2011

Borchert, Heiko & Juhl, Felix, "*Exploiting the Potential of Cyber Operations*", Jane's Defense Weekly, Vol. 48, Issue 26, 29 June 2011

Carr, Jeffrey, *Inside Cyber Warfare* (O'Reilly Media Inc., Sebastopol, 2010)

Clark, Wesley K. & Levin, Peter L., "*Securing the Information Highway"*, Foreign Affairs Magazine, Nov./Dec. 09, http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway, accessed on 9-12-2010

Clarke, Richard & Knake Robert K., *Cyber War: The Next Threat to National Security And What To Do About It* (1st Edition, HarperCollins Publishers, New York, 2010)

Clayton, Mark, *"Stuxnet malware is 'weapon' out to destroy….Iran's Bushehr nuclear plant?"*, the Christian Science Monitor, 21 Sep 2010. Available at: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, accessed on April 2011

Clayton, Mark, *"Cyberwar Glossary"*, the CS Monitor, 7-3-2011. Available at: http://www.csmonitor.com/USA/Military/2011/0307/Cyberwar-glossary, accessed on April 2011

Clemente, Dave, *"Reality Approaches Hype: Critical National Infrastructure and the Stuxnet Worm"*, Chatham House, 28 Sep 2010. Available at: http://www.chathamhouse.org/media/comment/view/163865, accessed on 18/2/2011

Coleman, Kevin, "*North Korea's cyber capabilities cause alarm*", Defense Systems, 18 Aug 2011. Available at: http://defensesystems.com/blogs/cyber-report/2011/08/north-korea-cyber-capabilities.aspx, accessed on Dec 2011

Cornish, Paul, Hughes, Rex & Livingstone, David, "*Cyberspace and the National Security of the United Kingdom: Threats and Responses*" (Chatham House, London, 2009). Available at: http://www.chathamhouse.org, accessed on Dec 2010

Cornish, Paul, Livingstone, David, Clemente, David & Yorke, Claire, "*On Cyber Warfare*" (Chatham House, London, 2010). Available at: http://www.chathamhouse.org, accessed on Dec 2010

Crosston, Matthew D., *"World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence"*, Strategic Studies Quarterly, Spring 2011, pp. 100-116. Available at: http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf, accessed on June 2011

CSMonitor (24-9-2010), *"Stuxnet worm mystery: What's the cyber weapon after*. Available at: http://www.csmonitor.com/USA/2010/0924/Stuxnet-worm-mystery-What-s-the-cyber-weapon-after, accessed on 4/11/2011

Curran, Kevin, Concannon, Kevin & McKeever, Sean, *"Cyber Terrorism Attacks",* στο συλλογικό έργο Janczewski, Lech J., & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)

CVE, *"Common Vulnerabilities and Exposures List Main Page"*, http://cve.mitre.org/cve/index.html

Denning, Dorothy E., *"Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy".* Available at: http://www.iwar.org.uk/cyberterror/resources/denning.htm, accessed on May 2011

Department of Homeland Security, *"Critical Infrastructures"*, 30-11-2010. Available at: http://www.dhs.gov/files/programs/gc_1189168948944.shtm, accessed on Jan 2011

Dreazen, Yochi, Cole, August & Gorman, Siobhan, "*Computer Spies Breach Fighter-Jet Project*", The Wall Street Journal (WSJ.com). Available at: http://online.wsj.com/article/SB124027491029837401.html, accessed on Oct 2010.

Dudney, Robert S., *"Rise of Cyber Militias"*, AIR FORCE Magazine (February 2011). Available at: http://www.airforce-magazine.com/MagazineArchive/Pages/2011/February%202011/0211cyber.aspx

Dunn Cavelty, Myriam, *Information Age Conflicts: A Study of the Information Revolution and a changing Operating Environment* (CSS, Zurich, 2002)

Dunn Cavelty, Myriam, "*As likely as a visit from E.T*", the EUROPEAN magazine. Available at: http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear, accessed on 7-1-2011.

Dunn Cavelty, Myriam, "*Cyberwar: Concept, Status Quo and Limitations*", CSS Analysis in Security Policy, No 71, April 2010. Available at: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=114442, accessed on Feb 2011

Farwell, James P. & Rohozinski Rafal *"Stuxnet and the Future of Cyber War",* Survival, 53:1, 23-40, 28/1/2011

Geers, Kenneth, *Strategic Cyber Security* (CCD COE Publication, Tallinn, Estonia, 2011)

Geers, Kenneth, *"Cyberspace and the Changing Nature of Warfare"*(keynote speech). Available at: http://www.carlisle.army.mil, accessed on Feb 2011

Glenny, Misha, *"Who Controls the Internet"*, Financial Times Magazine, 8/10/10. Available at: http://www.ft.com/intl/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html, accessed on 11/10/10

Gourley, Bob, *"Towards a Cyber Deterrent"*, 29 May 2008. Available at: http://ctovision.com/references/towards-a-cyber-deterrent/, accessed on April 2011

Gray, Colin S., *"Deterrence Resurrected: Revisiting Some Fundamentals"*, Parameters, winter 2010–2011), pp.99-106. Available at: http://www.carlisle.army.mil/usawc/parameters/Articles/2010winter/Gray.pdf, accessed on May 2011

Hoover, Nicholas J, *"Homeland Security, Defense Sign Cybersecurity Pact"*, Information Week, 14 Oct 2010. Available at: http://www.informationweek.com/news/government/security/227800034, accessed on 11/1/2012

Hunker, Jeffrey, "*Cyberwar and Cyber Power. Issues for NATO doctrine*", Research Division, NATO Defense College, Rome, Research Paper No 62, November 2010. Available at: http://www.ndc.nato.int/research/series.php?icode=1, accessed on April 2011

IISS (2007), "*China's cyber attacks*", Strategic Comments Vol. 13, Issue 7. Available at: http://www.iiss.org/publications/strategic-comments/past-issues/volume-13-2007/volume-13-issue-7 , accessed on 19-5-11

IISS (2011) "*Stuxnet: targeting Iran's nuclear programme*", Strategic Comments, 17:2,1-3. Available at: http://www.iiss.org/publications/strategic-comments/past-issues/volume-17-2011/february/stuxnet-targeting-irans-nuclear-programme/mobile-edition/, accessed on April 2011

International Telecommunications Union, "ITU Facts and Figures 2010". Available at: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2010.pdf, accessed on Dec 2010

Jennings, Gareth & Wasserbly, Daniel, "*Iran puts captured US UAV on show*", Jane's Defense Weekly, Volume 48, Issue 50, 14/12/11

Kaminski, Ryan T., *"Escaping The Cyber State of Nature: Cyber Deterrence and International Institutions",* στο Czosseck, C & Podins K. (Eds), Conference on Cyber Conflict Proceedings 2010 (CCD COE Publications, Tallinn, 2010)

Katz, Yaakov, "*Security and Defense: Nuclear worming*", 8 Oct 2010, The Jerusalem Post. Available at: http://www.jpost.com/Features/FrontLines/Article.aspx?id=190615, accessed on 21/1/2012

Keating, Joshua E, "*Can North Koreans Use the Internet?",* FP Magazine, 6-10-10. Available at: http://www.foreignpolicy.com/articles/2010/08/26/can_north_koreans_use_the_internet, accessed on Feb 2011.

Kellogg, Amy, "*Iran is Recruiting Hacker Warriors for its Cyber Army to Fight Enemies*", 14/3/201. Available at: http://www.foxnews.com/world/2011/03/14/iran-recruiting-hacker-warriors-cyber-army/, accessed on May 2011

Kerr, Paul K, Rollins John & Theohary, Catherine A., *"The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability"*, CRS Report for Congress, 9 Dec 2010. Available at: http://www.fas.org/sgp/crs/natsec/R41524.pdf, accessed on April 2011

Kingsbury, Alex, "*Documents Reveal Al Qaeda Cyberattacks*". Available at: http://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks, accessed on May 2011

Knake, Robert K., "*Internet Governance in an Age of Cyber Insecurity"*, CFR Special Report No56, September 2010. Available at: http://www.cfr.org/terrorism-and-technology/internet-governance-age-cyber-insecurity/p22832, accessed on September 2010

Lan, Tang & Xin, Zhang, *"Can Cyber Deterrence Work"* στην μελέτη: "Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway", EastWest Institute, 2010. Available at: http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf, accessed on April 2011.

Lewis, James A., "*The Fog of Cyberwar"*, ISN ETH website: http://www.isn.ethz.ch, accessed on April 2011

Lewis, James A, Langevin, James R, McCaul, Michael T, Charney Scott & Lt General (USAF, ret.) Raduege Harry, "*Cyber Security Two Years Later*", A Report of the CSIS Commission on Cyber Security for the 44th Presidency, January 2011. Available at: http://csis.org/publication/cybersecurity-two-years-later, accessed on April 2011

Lewis, James Andrew, "*The Cyber War Has Not Begun*", Center for Strategic & International Studies, March 2010. Available at: http://csis.org, accessed on November 2010

Lewis, James A., Timlin, Katrina, "*Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization*", CSIS. Available at: http://www.unidir.org/bdd/fiche-ouvrage.php?ref_ouvrage=92-9045-011-J-en, accessed on Dec 2012

Liaropoulos, Andrew (2011), *"Cyber Security and the Law of War: Legal and Ethical Aspects of Cyber Conflict"*, GPSG Working Paper # 7. Available at: http://piraeus.academia.edu/AndrewLiaropoulos/Papers/617962/Cyber-Security_and_the_Law_of_War_The_Legal_and_Ethical_Aspects_of_Cyber-conflict, accessed on May 2011

Libicki, Martin C., *Cyberdeterrence and Cyberwar* (RAND Corporation, Santa Monica, CA, 2009)

Libicki, Martin C., "*The Emerging Primacy of Information: A Debate on Geopolitics*", Orbis, Spring 1996, Vol. 40, No 2.

Libicki, Martin C., "*Deterrence in Cyberspace*", High Frontier: The journal for space and missile professionals, vol. 5, No 3 (May 2009). Available at: http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf, accessed on April 2010

Lynn, William J, "*Defending a New Domain: The Pentagon's Cyberstrategy*", Foreign Affairs, September/October 2010. Available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, accessed on 15/10/2010

Mahnken, Thomas G., "*Cyber War and Cyber Warfare*", στο συλλογικό έργο Lord, Kristin M. & Sharp, Travis (Eds), "*America's Cyber Future: Security and Prosperity in the Information Age*, Vol.2, CNAS, June 2011

Markoff, John, "*Cyberattack Threat on Rise, Executives Say*", the New York Times, 29/1/2010.Available at: http://query.nytimes.com/gst/fullpage.html?res=9805E7DF123EF93AA15752C0A9669D8B63, accessed on 16/10/2011

Masters, Jonathan, *"Confronting the Cyber Threat"*, CFR, 23 May 2011. Available at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577, accessed on 3/1/2012

Mazanec, Brian M., "*The Art of (Cyber) War*", The Journal of International Security Affairs, Spring 2009 - No 16. Available at: http://www.securityaffairs.org/issues/2009/16/mazanec.php, accessed on 10/10/11

McConnell, Mike, "*Cyber Insecurities: the 21st Century Threatscape*", στο συλλογικό έργο Lord, Kristin M. & Sharp, Travis (Eds), "*America's Cyber Future: Security and Prosperity in the Information Age*, Vol.2, CNAS, June 2011. Available at: http://www.cnas.org, accessed on June 2011

McElroy, Damien, "*Israel's Unit 8200: cyber warfare*", 30 Sep 2010, The Telegraph. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8034882/Israels-unit-8200-cyber-warfare.html, accessed on 20/12/2012

Meyers, C., Powers, S. & Faissol, D., "*Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches"*. Available at: http://www.osti.gov/bridge/product.biblio.jsp?osti_id=967712, accessed on June 2011

Michael, Alex, "*Cyber Probing: The Politicisation of Virtual Attack*", Defence Academy of the United Kingdom. Available at: http://www.conflictstudies.org.uk/files/Cyber_Probing.pdf, accessed on Jan 2011

Morgan, Patrick M., *Deterrence Now* (Cambridge University Press, Cambridge, 2003)

Nazario, Jose, *Politically Motivated Denial of Service Attacks*, p. 165, στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009)

Noonan, Sean, "*China and its Double – edged Cyber - sword*", Stratfor. Available at: http://www.stratfor.com, accessed on 9/12/2010

Nugent, John H.& Raisinghani, Mahesh*, "Bits and Bytes vs. Bullets and Bombs: A new Form of Warfare"* στο συλλογικό έργο των Janczewski, Lech J. & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)

Nye, Joseph S. Jr., "*Cyberspace diffuses, but doesn't erase state power"*, Fierce Homeland Security website: http://www.fiercehomelandsecurity.com, accessed on 26-10-11

Nye, Joseph S. Jr., "*Cyber Power*", Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010. Available at: http://belfercenter.org, accessed on November 2010

Ottis, R. & Lorents, P. (2010) "*Cyberspace: Definition and Implications",* In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. *Reading: Academic Publishing Limited, pp. 267-270*

Ottis, Rain, "*Theoretical Offensive Cyber Militia Models*", *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington DC, Academic Publishing Limited, pp. 307-313. Available at:

http://www.ccdcoe.org/articles/2011/Ottis_TheoreticalOffensiveCyberMilitiaModels.pdf, accessed on May 2011

Ottis, Rain, "*Proactive Defense Tactics Against On-Line Cyber Militia*". In Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July. Reading: Academic Publishing Limited, pp. 233-237. Available at: http://www.ccdcoe.org/articles/2010/Ottis_ProactiveDefense.pdf, accessed on Sep. 2010

Ottis, Rain, "*From Pitchforks to Laptops: Volunteers in Cyber Conflicts*". In Czosseck, C. and Podins, K. (Eds.) Conference on Cyber Conflict-Proceedings 2010, Tallinn, CCD COE Publications. Available at: http://www.ccdcoe.org/articles/2010/Ottis_FromPitchforks.pdf, accessed on Sep. 2010.

Panda Security (24-11-2010), "*One third of all computer viruses that exist were created in the first 10 months of 2010*". Available at: http://press.pandasecurity.com/news/one-third-of-all-computer-viruses-that-exist-were-created-in-the-first-10-months-of-2010/, accessed on January 2011

Panda Security, *"Annual Report 2011"*. Available at: http://press.pandasecurity.com/wp-content/uploads/2012/01/Annual-Report-PandaLabs-2011.pdf, accessed on January 2012

Parks, Raymond C. & Duggan, David P., "*Principles of Cyber Warfare*", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, US Military Academy, West Point, NY 5-6/6/01, Available at: http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf, accessed on February 2011

PBS *Frontline* (24/4/2003), "*The Warnings? Cyberwar!". Available at:* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/, accessed on April 2011

Pepera, David, "*'Cyber war? Not!' says U.K. professor*". Available at: http://www.fiercehomelandsecurity.com/story/cyber-war-not-says-uk-professor/2011-10-11, accessed on Oct. 2011

Rattray, Gregory J., *Strategic Warfare in Cyberspace* (MIT Press, Cambridge, 2001)

Rios, Billy K., "*Sun Tzu was a Hacker: An Examination of the tactics and Operations from a Real World Cyber attack*", στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009)

Russia Today (16/12/11), "*How Iran hacked super-secret CIA stealth drone*". Available at: http://rt.com/usa/news/iran-drone-hack-stealth-943/, accessed on 22 Jan 2012

Samaan, Jean-Loup (2010), *"Cyber Command"*, The RUSI Journal, 155:6, 16 - 21

Schmitt, Eric & Shanker, Thom, "*US Debated Cyberwarfare in Attack Plan on Libya*", The New York Times, 17 Oct 2011. Available at: http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1, accessed on 5/11/2011

Schmitt, Michael N. (June 1999), *"Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework"*, Columbia Journal of Transnational Law, vol. 37, pp 885-937. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993, accessed on April 2011

Shachtman, Noam, "*Computer Virus Hits US Drone Fleet*", The Wired Magazine, 7 Oct 2011. Available at: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/, accessed on 22/1/2012

Shakarian, Paulo, *"Stuxnet: Cyberwar Revolution in Military Affairs"*, Small Wars Journal, 15/4/2011. Available at: http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf, accessed on April 2011

Sharma, Amit, *Cyber Wars: A Paradigm Shift from Means to Ends*, pp. 6-8, στο συλλογικό έργο Czosseck, Christian & Geers, Kenneth (Eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, Amsterdam, 2009)

Shaud, John A., *"Framing Deterrence in the Twenty – First Century"*, Strategic Studies Quarterly, Fall 2009, pp. 4-7. Available at: http://www.au.af.mil/au/ssq/2009/Fall/shaud.pdf, accessed on May 2011

Shiavash, *"Iranian Cyber warfare Threat Assessment"*, 13/5/2010. Available at: http://www.cyberwarzone.com/content/iranian-cyber-warfare-threat-assessment, accessed on May 2010

Soldatov, Andrei, "*Vladimir Putin's Cyber Warriors*", Foreign Affairs, 9 Dec 2011, accessed on Dec 2011

Solomon, Jonathan, *"Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?"* Strategic Studies Quarterly, Spring 2011, pp.1-25. Available at: http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf, accessed on June 2011

Sterner, Eric, *"Retaliatory Deterrence in Cyberspace"*, Strategic Studies Quarterly, Spring 2011, pp. 62–80. Available at: http://www.au.af.mil/au/ssq/2011/spring/sterner.pdf, accessed on June 2011

Stoll, Cliff, *"The Cuckoo's Egg".* Available at: http://www.streettech.com/bcp/BCPgraf/StreetTech/cuckoo.htm, accessed on Dec. 2011

Tikk, Eneken, Kaska, Kadri & Vihul Liis, *International Cyber Incidents: Legal Considerations* (CCDCOE, Tallinn 2010)

Tzu, Sun, *The Art of War* (Arcturus Publishing Limited, London, 2008)

US Air Force Doctrine Document 3-12 (AFDD 3-12): *Cyberspace Operations,* http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf, p. 2, accessed on May 2011

United Press International (13/12/07), *"Report: Israel used Cyberwar against Syria".* Available at: http://www.upi.com/Top_News/Special/2007/12/13/Report-Israel-used-cyberwar-against-Syria/UPI-20671197559471/, accessed on Dec 2010

US Joint Publication 1-02 (JP 1-02) : "*DoD Dictionary of Military and Associated Terms"*, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, accessed on May 2011

US Joint Publication 3-13, *Information Operations*, 13-2-06. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf , accessed on May 2011.

Walsh, Eddie, "*The Cyber Proliferation Threat*", CNAS, 6 Oct 2011. Available at: http://www.cnas.org/node/7108, accessed on Nov. 2011

Warren, M.J., "*Terrorism and the Internet"*, στο συλλογικό έργο Janczewski, Lech J., & Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, New York, 2008)

Wilson, Clay, "*Information Operations and Cyberwar: Capabilities and Related Policy Issues"*, CRS Report for Congress, p.6. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA456478&Location=U2&doc=GetTRDoc.pdf, accessed on May 2011

ΠΑΡΑΡΤΗΜΑ Α

Συντομεύσεις & Επεξήγηση Χρήσιμων Όρων

Συντομεύσεις

Α/Φ = Αεροσκάφος ή Αεροσκάφη

ΓΕΕΔ = Γενικό Επιτελείο Ενόπλων Δυνάμεων

ΕΔ = Ένοπλες Δυνάμεις

Η/Υ = Ηλεκτρονικός Υπολογιστής ή Ηλεκτρονικοί Υπολογιστές

ΥΠΑΜ = Υπουργείο Άμυνας

ΥΠΕΞ = Υπουργείο Εξωτερικών.

DHS = Department of Homeland Security

DoD = Department of Defense

FIR = Flight Information Region

ICT = Information & Communications Technology

IO = Information Operation

IT = Information Technology

SIGINT = Signals Intelligence

Επεξήγηση Χρήσιμων Όρων

Air Gapped Network = Δίκτυο Η/Υ το οποίο δεν συνδέεται με άλλο δίκτυο Η/Υ (συμπεριλαμβανομένου του Internet). Σε αυτό επιτρέπεται μόνο η εσωτερική διακίνηση των ψηφιακών δεδομένων.

Botnet = είναι ομάδα Η/Υ που έχουν «μολυνθεί» από κακόβουλο λογισμικό (malware) με τέτοιο τρόπο ώστε να μπορούν να ελέγχονται εξ' αποστάσεως διαμέσου ενός server ελέγχου και διοίκησης, από έναν hacker. Οι Η/Υ «μολύνονται» με υπαιτιότητα του hacker, ο οποίος στην συνέχεια χρησιμοποιεί το botnet για να εκτελεί DoS επιθέσεις χωρίς τις περισσότερες φορές αυτό να είναι εν γνώσει των χρηστών των Η/Υ. Οι «μολυσμένοι» Η/Υ που ανήκουν στο botnet συχνά αναφέρονται ως Zombies.

CERT = Computer emergency response team. Πρόκειται για ομάδα ειδικών στην IT τεχνολογία, οι οποίοι επεμβαίνουν στους Η/Υ και τα δίκτυα αυτών οποτεδήποτε παρουσιάζεται ένα ακούσιο ή εκούσιο πρόβλημα λειτουργίας τους, με σκοπό να το επιλύσουν.

Chat Room = εικονικός χώρος διαδραστικής ανταλλαγής μηνυμάτων σε πραγματικό χρόνο.

Computer Code = Κώδικας Η/Υ. Περιλαμβάνει τους αριθμούς, τα γράμματα και τα σύμβολα που χρησιμοποιούνται για να δοθούν οδηγίες στον Η/Υ. Ένα πρόγραμμα Η/Υ αποτελείται από κώδικα.

DDoS Attack = Distributed Denial of Service Attack. Αποτελεί είδος κυβερνοεπίθεσης όπου πολλοί Η/Υ, συνήθως από ένα Botnet στέλνουν συνέχεια πακέτα δεδομένων σε έναν συγκεκριμένο προορισμό (π.χ ένα Η/Υ ή έναν server), προκειμένου να επιτευχθεί κορεσμός σε αυτόν, ώστε να μην μπορεί να ανταποκριθεί στις απαιτήσεις επικοινωνίας των νόμιμων χρηστών και να καταστεί μη διαθέσιμος.

Domain Name System (DNS) = Είναι μια ιεραρχία Η/Υ που μετατρέπει μια διεύθυνση στο Internet (πχ. www.google.gr) σε αριθμητική διεύθυνση που γίνεται αντιληπτή από τους Η/Υ (πχ. 192.50.234.1625) ώστε να γίνει εφικτή η μεταφορά στην σωστή κατεύθυνση των ψηφιακών πακέτων δεδομένων.

Forum = εικονικός χώρος στο διαδίκτυο, όπου τα μέλη του μπορούν να ανταλλάσουν απόψεις και να συζητούν μεταξύ τους για διάφορα θέματα, μέσω αποστολής ηλεκτρονικών μηνυμάτων. Οι διαφορές με το Chat Room είναι ότι τα μηνύματα ελέγχονται πρώτα από τον «επικεφαλής» του Forum πριν αναρτηθούν σε αυτό, ενώ αρχειοθετούνται προσωρινά.

Hardware = ο φυσικός εξοπλισμός του Η/Υ. Τα μηχανικά, ηλεκτρικά και ηλεκτρονικά του μέρη.

Malware = κακόβουλο λογισμικό, το οποίο διεισδύει σε έναν Η/Υ χωρίς την έγκριση του χρήστη του. Αποστέλλεται από έναν hacker προκειμένου να τεθεί ο Η/Υ – αποδέκτης υπό την ομηρία του και να εκτελεί λειτουργίες, που δεν συμβαδίζουν με την θέληση του χρήστη του Η/Υ. Μορφές malware είναι τα viruses, worms, Trojan horses κα.

Ping = δικτυακό εργαλείο με το οποίο ελέγχεται αν ένας Η/Υ είναι διαθέσιμος μέσα σε ένα δίκτυο Η/Υ. Ουσιαστικά αποστέλλονται από έναν Η/Υ ψηφιακά πακέτα δεδομένων που φέρουν το ερώτημα της διαθεσιμότητας προς έναν άλλο Η/Υ και αναμένεται η απάντηση του ερωτώμενου Η/Υ, μέσω αποστολής απαντητικών ψηφιακών πακέτων δεδομένων. Όταν η διαδικασία αυτή γίνει συγχρονισμένα από πολλούς Η/Υ προς έναν άλλο Η/Υ, σε βαθμό που ξεπερνά τις δυνατότητες απάντησης του ερωτώμενου Η/Υ, τότε έχουμε το λεγόμενο “Ping Flood”, που έχει ως αποτέλεσμα το Denial of Service.

Router = Τύπος Server, που είναι αρμόδιος για την κατεύθυνση της κυκλοφορίας του Internet. Ουσιαστικά αποτελεί μια συσκευή εντός ενός δικτύου, η οποία μεταχειρίζεται την μεταφορά ψηφιακών μηνυμάτων μεταξύ των Η/Υ.

SCADA = Supervisory Control and Data Acquisition. Στην σημερινή εποχή οι βιομηχανικές εγκαταστάσεις διαθέτουν συστήματα SCADA προκειμένου να επιβλέπουν και να ελέγχουν όλες τις βιομηχανικές διαδικασίες (πχ παραγωγή ηλεκτρικής ή πυρηνικής ενέργειας, έλεγχος αποβλήτων, διανομή ύδατος κτλ). Τα συστήματα αυτά χρησιμοποιούν λογισμικό και συνεπώς είναι «ευαίσθητα» στις τρωτότητες που εμφανίζει το λογισμικό που χρησιμοποιούν.

Server = Ένας Η/Υ που συνήθως χρησιμοποιείται από πολλούς άλλους, προκειμένου να δώσει πληροφορίες που είναι αποθηκευμένες μέσα σε αυτόν, όπως ιστοσελίδες.

Software = Λογισμικό. Το σύνολο των προγραμμάτων που εκτελούνται στον Η/Υ

Spam = πρόκειται για μαζική αποστολή ανεπιθύμητων emails με το ίδιο περιεχόμενο προς μεγάλο αριθμό χρηστών του internet ή γενικά ενός δικτύου Η/Υ. Γίνεται συνήθως μέσω botnets.

Web Defacement = Η παράνομη αλλαγή των περιεχομένων μιας ιστοσελίδας από έναν hacker.

WWW = World Wide Web. Παγκόσμιος ιστός. Είναι το σύνολο των διασυνδεδεμένων και διαδραστικών ψηφιακών εγγράφων, που εκδίδονται ως ιστοσελίδες και είναι διαθέσιμα μέσω internet.