ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2017-18

ΕΦΑΡΜΟΣΜΕΝΗ

ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΡΕΥΝΑ & ΑΝΑΛΥΣΗ

(ΠΔ 97 /2015/ΦΕΚ 163Α'/20.08.2014)

ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ

Τμήμα Στρατιωτικών Επιστημών

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

Σχολή Μηχανικών Παραγωγής & Διοίκησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΩΣ ΠΟΛΥΔΙΑΣΤΑΣΤΟ ΣΤΡΑΤΗΓΙΚΟ ΕΡΓΑΛΕΙΟ ΚΑΙ Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΣΕ ΚΡΙΣΙΜΕΣ ΣΤΡΑΤΙΩΤΙΚΕΣ ΚΑΙ ΜΗ ΥΠΟΔΟΜΕΣ

Υπο:

Τσατσούλης Περικλής

Α.Μ.:

2015018042

ΜΑΪΟΣ 2019

Η Μεταπτυχιακή Διατριβή του Τσατσούλη Περικλή εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Καθηγητής Νικόλαος Δάρας (Επιβλέπων) ,……

Καθηγητής Νικόλαος Ματσατσίνης ,…….

Καθηγητής Νικόλαος Παπαδάκης ,…….

Αφιερωμένη

Στην Σύζυγό μου και στο

Γιο μου

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου καθηγητή κ. Δάρα Νικόλαο τον οποίο εκτιμώ πρωτίστως σαν άνθρωπο για την πολυδιάστατη προσωπικότητά του αλλά και για την λαμπρή του καριέρα του ως ακαδημαϊκός. Μου έδωσε τις βασικές κατευθύνσεις για την σύνταξη της παρούσας διατριβής αλλά με βοήθησε επίσης και με απαραίτητο συγγραφικό υλικό.

Ανάλογες θερμότατες ευχαριστίες θα ήθελα να απευθύνω σε όλους τους καθηγητές της Στρατιωτικής Σχολής Ευελπιδων, του Πολυτεχνείου Κρήτης αλλά και σε όλους τους εξωτερικούς καθηγητές και στρατιωτικούς οι οποίοι με τη διδαχή τους στα τρία εξάμηνα του μεταπτυχιακού προγράμματος συνετέλεσαν τα μέγιστα στην εκμάθηση νέων γνωστικών αντικειμένων αλλά και στην εκβάθυνση ήδη υπάρχοντων.

Επίσης θα ήθελα να ευχαριστήσω όλους τους συμφοιτητές μου για την άριστη συνεργασία μας κατά την διάρκεια των μαθημάτων, συμβάλλοντας ο ένας τον άλλον με τη διατύπωση εποικοδομητικών προβληματισμών και την ανταλλαγή απόψεων.

Τέλος οι μεγαλύτερες ευχαριστίες απευθύνονται στην σύζυγο μου Αγγελική και στο γιο μου Ηρακλή στους οποίους είναι αφιερωμένη και η διατριβή μου. Τους ευχαριστώ από τα βάθη της καρδιάς μου διότι στάθηκαν δίπλα μου κάθε στιγμή, με αποτέλεσμα η στήριξη τους να αποτελεί το ισχυρότερο κίνητρο για την βελτίωσή μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΔΙΑΤΡΙΒΗΣ

Η εμφάνιση του ηλεκτρονικού υπολογιστή και η ραγδαία εξέλιξη της τεχνολογίας οδήγησαν στην οργάνωση επικοινωνιακών δικτύων και τη δημιουργία εφαρμογών, οι οποίες θα υποστηρίζουν διάφορες ανθρώπινες δραστηριότητες, βασιζόμενες σε δίκτυα υπολογιστών. Τα δίκτυα αρχικά ήταν απομονωμένα με συνέπεια να προσφέρουν την απαιτούμενη προστασία από κακόβουλους χρήστες. Παρ' όλα αυτά, η ανάπτυξη της πληροφορικής σε συνδυασμό με την ανάγκη να τεθούν όλες αυτές οι υπηρεσίες στην ευχέρεια του πολίτη, προκειμένου να διευκολύνει την καθημερινότητα του σε όλα τα επίπεδα, τα κατέστησε ευρέως προσβάσιμα, οδηγώντας παράλληλα στην αύξηση της τρωτότητάς τους.

Σκοπός της παρούσας εργασίας είναι να παρουσιάσει τις μορφές των συγκρούσεων, που λαμβάνουν χώρα στον κυβερνοχώρο, δίνοντας ιδιαίτερη έμφαση στην πλέον διαδεδομένη μορφή κυβερνοσύγκρουσης, τον κυβερνοπόλεμο. Οι συγκρούσεις πραγματοποιούνται σε καθημερινή βάση, χωρίς να γίνονται πάντα αντιληπτές από το ευρύ κοινό, έχοντας εφαρμογή τόσο σε στρατιωτικές όσο και πολιτικές υποδομές.

Παράλληλα, θα αναλυθούν όλοι οι παράγοντες, οι οποίοι καθιστούν τον κυβερνοπόλεμο ως ένα πολυδιάστατο εργαλείο στα χέρια των σύγχρονων κρατών καθώς θεωρείται ως «όπλο», το οποίο όμως δεν προκαλεί ανθρώπινες απώλειες, προς το παρόν, αλλά ο αντίκτυπός του είναι κυρίως οικονομικός ή ψυχολογικός.

Τέλος, θα αναφερθούν παραδείγματα εφαρμογών κυβερνοπολέμου παγκοσμίως με τις επιπτώσεις, που προκάλεσαν καθώς και χρήσιμα συμπεράσματα και προτάσεις, που εξάγονται από την έρευνα.

Λέξεις Κλειδιά: Κυβερνοχώρος, Κυβερνοσύγκρουση, Κυβερνοεπίθεση, Κυβερνοπόλεμος, Κυβερνοασφάλεια

SUMMARY

The emergence of the computer and the rapid development of technology have led to the organization of communications networks and the creation of applications that support various human activities based on computer networks. The networks were initially isolated and consistently provided the required protection against malicious users. Nevertheless, the development of information technology, coupled with the need to put all these services at the citizen's convenience, in order to facilitate their daily routine at all levels, has made them widely accessible, while at the same time increasing their vulnerability.

The purpose of this paper is to present the forms of conflict taking place in cyberspace, with particular emphasis on the most prevalent form of cyber-conflict, cyberwar. Conflicts occur on a daily basis, not always perceived by the general public, with both military and civilian infrastructure.

At the same time, we will analyze all the factors that make cyberwar a multidimensional tool in the hands of modern states as it is considered a "weapon", but it does not cause human losses at present, but its impact is mainly economic or psychological.

Finally, there will be examples of cyber warfare applications worldwide with the implications they have caused and useful conclusions and suggestions extracted from the survey.

Key Words: Cyberspace, Cyber Conflict, Cyber Attack, Cyberwar, Cyber-security

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΕΙΣΑΓΩΓΗ

Από τις αρχές της δεκαετίας του 90' και πιο συγκεκριμένα στον Α' Περσικό Πόλεμο καταδεικνύεται με μεγάλη ευκρίνεια ότι η ενσωμάτωση της τεχνολογίας στο στρατιωτικό δόγμα, στις στρατιωτικές επιχειρήσεις και δομές, προσέφερε στις Η.Π.Α. και τους συμμάχους της σημαντικό συγκριτικό πλεονέκτημα κατά τη διάρκεια των ένοπλων συγκρούσεων. Στις εν λόγω συγκρούσεις έγινε εκτεταμένη χρήση αεροπορικών όπλων, των συστημάτων Διοίκησης και Ελέγχου (Command and Control), των Η/Υ αλλά και των έξυπνων βομβών. Κοινός παρανομαστής των παραπάνω στοιχείων ήταν ότι η η εύρυθμη λειτουργία τους στηριζόταν στη σωστή λειτουργία του λογισμικού (software), που ήταν εγκατεστημένο στους Η/Υ. Παράλληλα, ο απαιτούμενος συντονισμός των στρατιωτικών επιχειρήσεων ήταν εφικτός μέσω των δικτύων των Η/Υ. Η νικηφόρα έκβαση της σύγκρουσης οδήγησε στο συμπέρασμα ότι η εύρυθμη διαχείριση και μεταφορά των ψηφιακών δεδομένων και πληροφοριών μέσω των δικτύων των Η/Υ προσέδιδε ισχυρό πλεονέκτημα στον κάτοχό τους. Το γεγονός αυτό καταδεικνύει και την αμεσότητα της σχέσης μεταξύ τεχνολογίας και πολέμου.

Παράλληλα, κομβικό σημείο στην εξέλιξη του κυβερνοχώρου αποτέλεσε η υλοποίηση και ευρεία διάδοση του διαδικτύου (Internet), το οποίο σε συνδυασμό με την ανάπτυξη φιλικών προς τον άνθρωπο τεχνολογικών εφαρμογών για Η/Υ, καθιστούσε σε κάθε πολίτη εφικτή την πρόσβαση σε τεράστιες βάσεις δεδομένων με χαμηλό κόστος. Το διαδίκτυο, δρώντας ως νέο εργαλείο επικοινωνίας έδωσε νέα διάσταση στην εξυπηρέτηση των πολιτών, απλοποιώντας και διευκολύνοντας την καθημερινότητά τους. Κυβερνητικές υπηρεσίες και ιδιωτικές εταιρείες, εκμεταλλευόμενες την εξέλιξη της τεχνολογίας και υπό την απαίτηση των πολιτών για βέλτιστη παροχή υπηρεσιών, συνδέθηκαν μαζικά στο διαδίκτυο, παρέχοντας το σύνολο των υπηρεσιών τους μέσω αυτού. Επιπλέον, 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 να εκφράζεται μέσω της διασύνδεσης και αλληλεξάρτησης των δικτύων Η/Υ και Internet. Η τάση αυτή έφερε στο προσκήνιο την έννοια του κυβερνοχώρου, ενός εικονικού χώρου μέσω του οποίου πραγματοποιούνταν σε καθημερινή βάση εκατομμύρια λειτουργίες και δραστηριότητες. Παράλληλα, εντός αυτής της περιοχής λάμβαναν χώρα πληθώρα ανταλλαγών και μεταφορών ψηφιακών δεδομένων και πληροφοριών, οι οποίες μεταφράζονταν σε κέρδος και ασφάλεια. Όπως, όμως, προαναφέρθηκε στον κυβερνοχώρο είχαν πλέον όλοι άμεση πρόσβαση και ως φυσικό επακόλουθο η εικονική αυτή περιοχή μετετράπη σε πεδίο σύγκρουσης και αντιπαράθεσης συμφερόντων καθώς οι άμεσα ή έμμεσα ενδιαφερόμενοι σε αυτή επιζητούσαν μεγαλύτερο μερίδιο κέρδους και ασφάλειας.

Περί τα μέσα της δεκαετίας του 90' έκαναν την εμφάνιση τους οι hackers και οι διάφορες μορφές κακόβουλου λογισμικού (malware), 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 πανικού και τρόμου. Οι παράνομες αυτές δραστηριότητες αφορούσαν τόσο σε απλούς χρήστες των Η/Υ όσο και σε επιχειρήσεις και οργανισμούς, που διέθεταν δίκτυα Η/Υ. Παράλληλα, χαρακτηρίστηκαν ως συγκρούσεις στον κυβερνοχώρο και με το πέρασμα των χρόνων στιγματίστηκαν από την ολοένα και μεγαλύτερη συχνότητα εμφάνισής τους, αλλά και από την εξειδικευμένη τεχνολογία της πληροφορικής, που τις συνόδευε.

Τέλος, ο κυβερνοπόλεμος αποτελεί συστατικό στοιχείο του πληροφοριακού πολέμου, τον οποίο εφαρμόζουν κατά κύριο λόγο τα σύγχρονα κράτη. Θεωρείται από τα κράτη ως μία ήπια μορφή πολεμικής σύγκρουσης, η οποία δεν προκαλεί, προς το παρόν, ανθρώπινες απώλειες, προβάλλοντάς την ως μία περισσότερο «νομιμοποιημένη» και από αποδεκτή από το ευρύ κοινό επιλογή. Δύναται να διεξαχθεί μεταξύ δύο ή και περισσότερων 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 μία σημαντική διαφορά σε σχέση με τις συγκρούσεις σε συμβατικό ή πυρηνικό επίπεδο.

ΚΕΦΑΛΑΙΟ 1 ΚΥΒΕΡΝΟΧΩΡΟΣ

1.1 Ορισμός

Σε διεθνές επίπεδο αν και έχουν διατυπωθεί πολυάριθμοι ορισμοί για τον Κυβερνοχώρο δεν υπάρχει κάποιος κοινά αποδεκτός. Σύμφωνα με τον σχετικά σύντομο και εύληπτο ορισμό, που έδωσε η Υπηρεσία Ερευνών των Η.Π.Α., στο πλαίσιο αναφοράς, που συνέταξε για λογαριασμό του Κονγκρέσο, πρόκειται για «τη συνολική διαδικτύωση των ανθρώπων μέσω των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών ανεξάρτητα από τη φυσική γεωγραφία»[B30]. Ο συγκεκριμένος ορισμός είναι αρκετά εύστοχος καθώς επικεντρώνεται σε δύο βασικά χαρακτηριστικά του Κυβερνοχώρου. Πρώτον, στη μειωμένη σημασία της γεωγραφίας, καθώς οι παρεχόμενες δυνατότητες των σύγχρονων επιτευγμάτων στους τομείς της πληροφορικής και των τηλεπικοινωνιών, έχουν δημιουργήσει έναν εικονικό κόσμο (μέσω αισθητήρων, σημάτων, συνδέσεων, μεταφοράς δεδομένων), ο οποίος λειτουργεί ανεξάρτητα και πέρα από τα γεωγραφικά σύνορα και τις αποστάσεις του πραγματικού κόσμου. Δεύτερον, στη διαδραστική σχέση, που συνδέει τους χρήστες αυτού του κόσμου. Πιο συγκεκριμένα, οι εμπλεκόμενοι στον Κυβερνοχώρο έχουν τη δυνατότητα να αλληλεπιδρούν μεταξύ τους, να προβαίνουν στην ανταλλαγή απόψεων και ιδεών, να μοιράζονται πληροφορίες, να παρέχουν υποστήριξη σε κοινωνικές ομάδες, να ασκούν οικονομικές δραστηριότητες, να οργανώνουν δράσεις, να συμμετέχουν σε πολιτικούς διαλόγους. Η έννοια του Κυβερνοχώρου χρησιμοποιείται πλέον ευρέως για να περιγράψει την επικρατούσα κατάσταση με τους υπολογιστές, την τεχνολογία της πληροφορίας και τα συστήματα πληροφοριακών και επικοινωνιακών δικτύων, που στηρίζονται στη χρήση των ηλεκτρονικών υπολογιστών[Γ1].

1.2 Επίπεδα Λειτουργίας

Προκειμένου να γίνει πιο κατανοητή η έννοια του κυβερνοχώρου και η λειτουργία του, διακρίνονται τρία (3) επίπεδα λειτουργίας στα συστήματα πληροφορικής (IT Systems)[B18]:

- Φυσικό (Physical Layer)
- Συντακτικό (Syntactic Layer)
- Σημασιολογικό (Semantic Layer)

Φυσικό (Physical Layer)[A1]

Σε αυτό το επίπεδο αναφέρεται το υλικό, δηλαδή τα μηχανικά (π.χ. 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 δύναται η ύπαρξη συστήματος πληροφορικής.

Συντακτικό (Syntactic Layer)[A1]

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 συσκευές.

Σημασιολογικό (Semantic Layer)[A1]

Το σημασιολογικό επίπεδο περιλαμβάνει όλες 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 λανθασμένη. Σε περίπτωση, που κάποιος καταφέρει μια μετατροπή στη σημασιολογική ερμηνεία ενός συστήματος πληροφορικής, τότε αυτό μπορεί να χειραγωγηθεί. Παρ' όλα αυτά για να επιτευχθεί κάτι τέτοιο θα πρέπει πρώτα να έχει προηγηθεί παρέμβαση στο συντακτικό επίπεδο.

1.3 Χαρακτηριστικά Κυβερνοχώρου

Είναι δεδομένο ότι, ο κυβερνοχώρος και η ανθρώπινη δραστηριότητα είναι δύο έννοιες άρρηκτα συνδεδεμένες. Ο κυβερνοχώρος είναι πλήρως εξαρτημένος από την τεχνολογική ανάπτυξη, και ιδιαίτερα από τις μεταβολές, που παρατηρούνται στην τεχνολογία των Η/Υ. Ουσιαστικά, βρίσκεται οπουδήποτε υπάρχει ένας Η/Υ ή ένας επεξεργαστής ή ακόμα και ένα συνδεδεμένο καλώδιο σε μια τερματική συσκευή Η/Υ[B6]. Παράλληλα, τα όρια δράσης του δεν είναι ούτε σαφή ούτε προκαθορισμένα, ενώ ως πεδίο εφαρμογής είναι εύκολα προσβάσιμος με χαμηλό κόστος σε οποιονδήποτε διαθέτει την απαραίτητη τεχνολογία και υποδομή (π.χ. έναν Η/Υ, μία διαδικτυακή σύνδεση (Internet) ή έναν Η/Υ διασυνδεδεμένο στο δίκτυο Η/Υ μιας επιχείρησης)[B2]. Τα κύρια χαρακτηριστικά, που προσδιορίζουν τον κυβερνοχώρο περιγράφονται όπως παρακάτω:

- Το μέγεθος

Είναι εύκολα κατανοητό πως δεν είναι δόκιμη η προσπάθεια υπολογισμού των διαστάσεων του κυβερνοχώρου, καθώς αποτελεί μία ευμετάβλητη εικονική περιοχή, μέσα στην οποία διακινείται η ψηφιακή πληροφορία. Σύμφωνα με έκθεση της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU)[Γ6], ο αριθμός των χρηστών κινητής τηλεφωνίας με πρόσβαση στο

διαδίκτυο έχει αυξηθεί δραματικά την τελευταία δεκαετία ενώ η πρόσβαση στο διαδίκτυο μέσω κινητού τηλεφώνου έχει εξαπλωθεί στις διπλάσιες χώρες από αυτές το 2007. Επιπλέον για λόγους κερδοφορίας, πλήθος επιχειρήσεων και εταιρειών κατά τη δεκαετία του 1990 ενσωμάτωσαν αυτοματοποιημένα συστήματα ελέγχου και απόκτησης δεδομένων (SCADA systems) και δίκτυα Η/Υ στο δυναμικό τους. Το ίδιο έπραξαν και πολλές κυβερνήσεις, οι οποίες μέσω αυτής της κίνησης επεδίωξαν την ενίσχυση της αποτελεσματικότητας των κρατικών υποδομών, την επαύξηση των δυνατοτήτων ελέγχου και επιβολής του νόμου και την ενίσχυση της άμυνάς τους. Είναι λοιπόν, ξεκάθαρο, ότι, οι διαστάσεις του κυβερνοχώρου, ως περιοχής διακίνησης ψηφιακών δεδομένων και πληροφορίας, διαρκώς αυξάνονται, λόγω της εξελισσόμενης τάσης στον τομέα της ψηφιακής τεχνολογίας και των δικτύων Η/Υ, καθιστώντας την οριοθέτησή του πρακτικά αδύνατη.

- <u>Η ασυμμετρία</u>

Στον κυβερνοχώρο το χαρακτηριστικό της ασυμμετρίας αναφέρεται στις διάφορες οντότητες, οι οποίες δύναται να δραστηριοποιηθούν στο ψηφιακό χώρο ως σχετικά «ισοδύναμες», ανεξαρτήτως της υπόστασής τους στο φυσικό χώρο. Πιο συγκεκριμένα, στον κυβερνοχώρο δραστηριοποιούνται έθνη, κράτη ακόμα και μεμονωμένοι πολίτες (hackers), οι οποίοι όμως έχουν τις ίδιες αναλογίες εντός του κυβερνοχώρου[B2]. Επιπλέον, η ασυμμετρία εμφανίζεται και στη σχέση κόστους και ρίσκου με το επιδιωκόμενο κέρδος, που θα αποκομίσει κάποιος μέσα από την κυβερνοχώρο[B11](π.χ. η υποκλοπή μια τεχνικής παραγωγής προϊόντων από μία εταιρεία με υψηλή χρηματική αξία με κόστος και ρίσκο μικρότερο σε σχέση με την απόπειρα υποκλοπής των ίδιων δεδομένων με φυσικό τρόπο).

- <u>Η ανωνυμία</u>

Η ανωνυμία που δύναται να έχει ένας δρων μέσα στην περιοχή του κυβερνοχώρου είναι ένα ακόμα χαρακτηριστικό του στοιχείο. Η ανωνυμία, που αναπτύσσεται, οφείλεται πολλές φορές στη δαιδαλώδη αρχιτεκτονική του διαδικτύου σε συνδυασμό με τις ικανότητες του χρήστη, προκειμένου να καλύψει τα «ίχνη» του χρησιμοποιώντας κατάλληλες τεχνικές μεθόδους[B5]. Παράλληλα, η εύκολη πρόσβαση στον κυβερνοχώρο σε συνδυασμό με τη μη ταύτιση των σημείων πρόσβασης με συγκεκριμένο χρήστη (π.χ. πρόσβαση στο διαδίκτυο με Η/Υ ενός Internet Café από διάφορους χρήστες), ενισχύει ακόμα περισσότερο αυτό το χαρακτηριστικό γνώρισμα.

- Η απόσταση, ο χρόνος και ο χώρος

Στον κυβερνοχώρο δεν υπάρχουν περιορισμοί αναφορικά με την απόσταση, το χρόνο και το χώρο. Αυτό εύκολα προκύπτει από το γεγονός ότι μία μεταφορά δεδομένων μεταξύ δύο Η/Υ, που βρίσκονται σε μεγάλη γεωγραφική απόσταση, μπορεί να υλοποιηθεί εξίσου γρήγορα και εύκολα με την περίπτωση, που οι ίδιοι Η/Υ βρίσκονταν στον ίδιο χώρο. Παράλληλα, οι χώροι αποθήκευσης των ψηφιακών δεδομένων είναι πιο «ευέλικτοι» σε σχέση με τους φυσικούς χώρους αποθήκευσης υλικών[B29].

- Η μεταβλητότητα

Το στοιχείο της μεταβλητότητας έγγυται στο γεγονός ότι ο κυβερνοχώρος ως ανθρώπινη κατασκευή είναι ατελής, δηλαδή το λογισμικό (software) και το υλικό (hardware) δεν λειτουργούν πάντα στο 100% των κατασκευαστικών τους δυνατοτήτων με αποτέλεσμα πρώτον η πρόβλεψη να μην είναι πάντα δυνατή και δεύτερον το αποτέλεσμα της ίδιας ενέργειας να είναι διαφορετικό.

- Η διπλή χρήση των «κυβερνοεργαλείων»

Με τον όρο «κυβερνοεργαλεία» ορίζονται τα εργαλεία (tools) εκείνα τα οποία χρησιμοποιούνται στον κυβερνοχώρο. Τα εργαλεία αυτά έχουν τη δυνατότητα διπλής χρήσης (dual-use), δηλαδή μπορούν να χρησιμοποιηθούν για αντίθετους σκοπούς. Χαρακτηριστικό παράδειγμα αποτελεί ο σαρωτής τρωτότητας (vulnerabilities scanner), ο οποίος μπορεί είτε να χρησιμοποιηθεί προκειμένου να εντοπίσει τρωτά σημεία ενός δικτύου Η/Υ με σκοπό ο διαχειριστής του συστήματος να τα επιδιορθώσει, αυξάνοντας την ασφάλεια και την άμυνά του, είτε να χρησιμοποιηθεί από κάποιον διαχειριστή για να εντοπίσει τα τρωτά σημεία κάποιου άλλου δικτύου Η/Υ με απώτερο σκοπό να του επιτεθεί. Άρα, τα «κυβερνοεργαλεία» δύναται να χρησιμοποιηθούν τόσο αμυντικούς όσο και για επιθετικούς σκοπούς.

- Η έλλειψη συνόρων

Η παντελής έλλειψη συνόρων αποτελεί ένα από τα βασικότερα γνωρίσματα του κυβερνοχώρου καθώς ο εικονικός χώρος δεν υπόκειται σε οριοθετήσεις και σύνορα αντίστοιχα με αυτά του φυσικού κόσμου.

1.4 Σημεία Τρωτότητας Κυβερνοχώρου

Οι αδυναμίες, που παρουσιάζονται στον κυβερνοχώρο αφορούν κυρίως στην αρχιτεκτονική του διαδικτύου (Internet), αλλά και το λογισμικό (software) και υλικό (hardware), το οποίο εφαρμόζεται στους Η/Υ. Το Internet αποτελεί το σημαντικότερο δίαυλο μεταφοράς κακόβουλου λογισμικού (malware) παγκοσμίως με αποτέλεσμα οι αδυναμίες στην αρχιτεκτονική του να έχουν άμεσο αντίκτυπο στον κυβερνοχώρο. Παράλληλα, οι Η/Υ αποτελούν τα «κύτταρα» των δικτύων Η/Υ και οι αδυναμίες τους, οι οποίες δύναται να οφείλονται στα κύρια δομικά συστατικά τους (λογισμικό και υλικό), αποτελούν σημεία τρωτότητας για τον κυβερνοχώρο.

Αναφορικά με τις αδυναμίες, που προέρχονται από την αρχιτεκτονική του διαδικτύου και μεταφέρονται στον κυβερνοχώρο, επικεντρώνονται στα εξής[Γ8]:

- ✓ Αδυναμία πλήρη ελέγχου στην κατεύθυνση των ψηφιοποιημένων πληροφοριών προς το σωστό προορισμό. Πρακτικά, η αλληλογραφία μπορεί να κατευθυνθεί σε λάθος προορισμό, με την υπαιτιότητα ενός hacker.
- ✓ Έλλειμμα στην κρυπτογράφηση της πληροφορίας, που διακινείται στο διαδίκτυο.
- ✓ Εύκολη διάδοση κακόβουλου λογισμικού (malware software).

Σχετικά με τις αδυναμίες των δομικών συστατικών των Η/Υ , η εξέταση των υλικών και των λογισμικών, που χρησιμοποιούνται στην τεχνολογία της πληροφορικής (Information Technology) παρουσιάζει ιδιαίτερο ενδιαφέρον. Είναι δεδομένο πως τις περισσότερες φορές ο αγοραστής ενός υλικού δεν είναι σε θέση να γνωρίζει τον κώδικα των ηλεκτρονικών, που έχει χρησιμοποιηθεί κατά την κατασκευή του υλικού με αποτέλεσμα να είναι ευάλωτος σε μια ενδεχόμενη επίθεση στον κυβερνοχώρο. Παράλληλα, το γεγονός ότι στην εποχή της παγκοσμιοποίησης τα διάφορα τμήματα ενός Η/Υ μπορεί να κατασκευαστούν σε διαφορετικές χώρες, ενισχύει την πιθανότητα εμφάνισης τρωτότητας στο υλικό και το λογισμικό. Επίσης είναι πιθανό κατά τη διάρκεια δημιουργίας του λογισμικού (προγράμματα και συμβολικές γλώσσες για τον έλεγχο και τη διεύθυνση της λειτουργίας του υλικού) να πραγματοποιηθεί κάποιο λάθος, το οποίο εφόσον είναι εμφανές να διορθωθεί. Ωστόσο, αν ληφθεί υπόψη ότι κάθε νέο λειτουργικό σύστημα ενός Η/Υ περιέχει κάθε φορά μεγαλύτερο αριθμό τέτοιων εντολών, γίνεται αντιληπτό ότι η πιθανότητα λάθους κατά την εγγραφή του κώδικα αυξάνει, ενώ η πιθανότητα εύρεσής του μειώνεται[Β5].

1.5 Απειλές στον Κυβερνοχώρο

Οι απειλές που εμφανίζονται στον κυβερνοχώρο εστιάζονται στη διακοπή της εύρυθμης λειτουργίας του και διακρίνονται σε τρεις (3) κατηγορίες:

- Απειλές από φυσικές επιθέσεις (physical attacks)[B25]

Πρόκειται για επιθέσεις με τη χρήση όπλων, σε εγκαταστάσεις που στηρίζονται σε λογισμικό. Παράδειγμα τέτοιας απειλής είναι μία βόμβα, που πλήττει έναν τηλεπικοινωνιακό δορυφόρο.

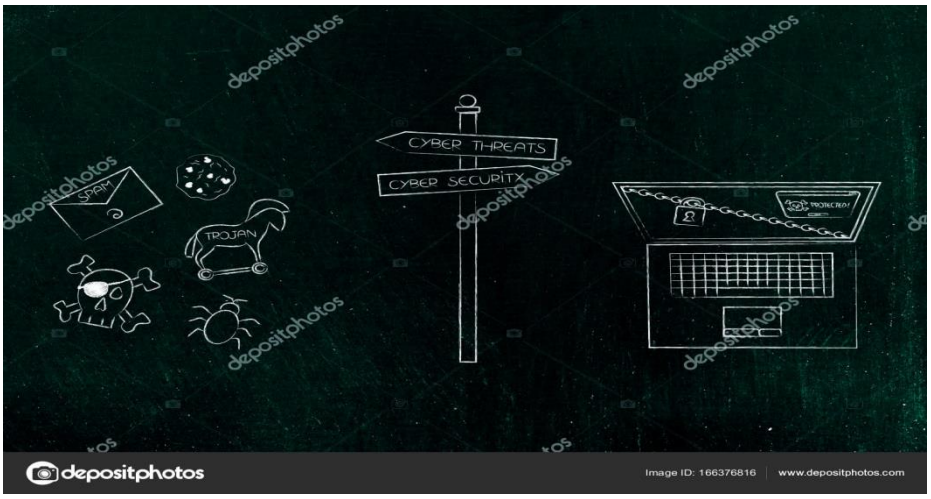
- Απειλές από ηλεκτρομαγνητικές επιθέσεις (electromagnetic attacks)[B25]

Πρόκειται για χτυπήματα με όπλα ηλεκτρομαγνητικού παλμού (EMP weapons), τα οποία ουσιαστικά καθιστούν ανενεργούς τους Η/Υ.

- Απειλές από κυβερνοεπιθέσεις (cyber attacks)[B25]

Πρόκειται για απειλές, που απορρέουν από τη χρήση των «κυβερνοόπλων» κατά των Η/Υ και των δικτύων τους. Μέσα από τη χρήση των «κυβερνοόπλων», στοχοποιούνται τα εξής:

i. Η διατήρηση της διαβάθμισης των ψηφιακών δεδομένων (Confidentiality)[B11].
ii. Η ακεραιότητα των δεδομένων (Integrity)[B11].
iii. Η διαθεσιμότητα των δεδομένων (Availability)[B11].



Εικόνα 1.1 Απειλές στον Κυβερνοχώρο

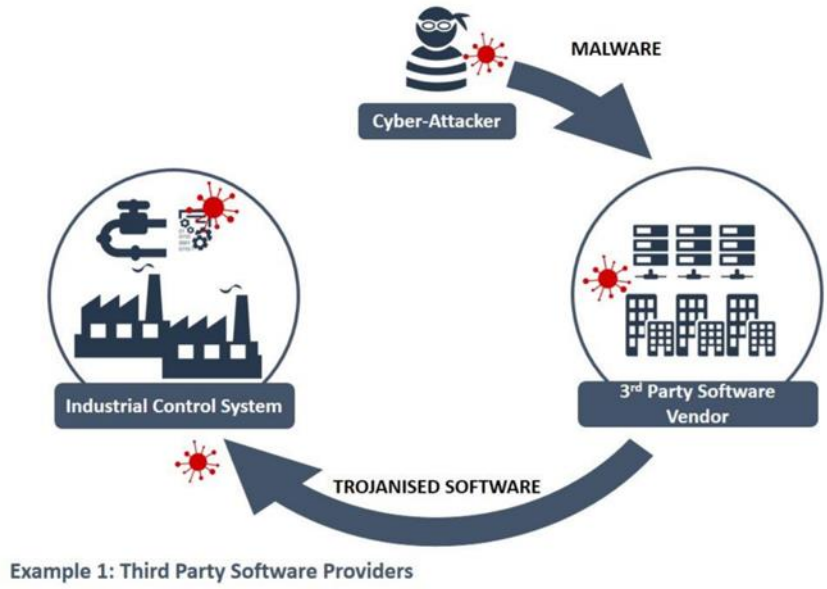
1.6 Φορείς Απειλών

Οι κίνδυνοι, που αντιμετωπίζει ο κυβερνοχώρος, διακρίνονται σε εξωτερικοί και εσωτερικοί[B28]. Ο διαχωρισμός γίνεται με σημείο αναφοράς το δίκτυο Η/Υ. Εάν ο «προσβολέας» βρίσκεται εκτός του δικτύου, τότε ο κίνδυνος χαρακτηρίζεται ως εξωτερικός, ενώ αν η απειλή προέρχεται από χρήστη εντός του δικτύου, τότε ο κίνδυνος είναι εσωτερικός. Οι εξωτερικοί κίνδυνοι προέρχονται από τους hackers, ενώ οι εσωτερικοί κίνδυνοι πηγάζουν από τα μέλη του δικτύου (Insiders) ή από τα ελαττωματικά προϊόντα της «Αλυσίδας Εφοδιασμού» (Supply Chain).

Όσον αφορά τους hackers προσπαθούν να παραβιάσουν τις βασικές «εξουσίες», που κατέχει ο διαχειριστής ενός δικτύου Η/Υ, δηλαδή τον τρόπο που θα χρησιμοποιεί ο κάθε χρήστης τον Η/Υ, που ανήκει στο δίκτυο Η/Υ. Κύρια επιδίωξή τους αποτελεί η πρόσβαση στο δίκτυο, η οποία μπορεί να έχει και μεγάλη διάρκεια, εκμεταλλευόμενοι τις τρωτότητες, που παρουσιάζει το λογισμικό, επιβάλλοντας στο δίκτυο να δεχτεί τις κακόβουλες οδηγίες. Από τη στιγμή, που θα αποκτήσουν πρόσβαση στον Η/Υ ή στο δίκτυο, φαίνονται ως νόμιμοι χρήστες του. Οι αντικειμενικοί τους σκοποί επικεντρώνονται στα κάτωθι[B11]:

- Υπεξαίρεση δεδομένων (παραβίαση του Confidentiality).
- Διαταραχή (Disruption) του Η/Υ ή του δικτύου (παραβίαση του Integrity).
- Διαφθορά (Corruption) του Η/Υ ή του δικτύου (παραβίαση του Integrity).
- Χρήση των λοιπών δικτύων Η/Υ για διεξαγωγή DDoS (Distributed Denial of Service) επιθέσεων (παραβίαση του Availability).

Από την άλλη, όσον αφορά τους Insiders και το Supply Chain, αποτελούν δύο μεθόδους πρόσβασης στα συστήματα Η/Υ. Στην περίπτωση των Insiders, κάποιος ο οποίος βρίσκεται ήδη σε ένα δίκτυο Η/Υ μιας χώρας ή μιας εταιρείας Α, στρατολογείται από μια χώρα ή μια εταιρεία Β προκειμένου να κάνει δολιοφθορά στο δίκτυο της Α. Στην άλλη περίπτωση, μια εταιρεία από το κράτος Α προμηθεύει το κράτος Β με «ελαττωματικό» υλικό για το δίκτυο Η/Υ του, το οποίο περιέχει κώδικα, που ανταποκρίνεται στη «θέληση» του κράτους Α ή στη «θέληση» ενός άλλου κράτους, το οποίο είναι εχθρικά διακείμενο προς το κράτος Β[B5].



Εικόνα 1.2 «Μόλυνση» Συστήματος Εφοδιαστικής Αλυσίδας

ΚΕΦΑΛΑΙΟ 2 ΚΥΒΕΡΝΟΣΥΓΚΡΟΥΣΕΙΣ ΚΑΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ

2.1 Ορισμοί

Ως σύγκρουση στον κυβερνοχώρο ή κυβερνοσύγκρουση (cyber conflict) ορίζεται η αντιπαράθεση μεταξύ δύο (2) ή περισσότερων πλευρών στην ανωτέρω περιοχή με μία τουλάχιστον εκ των οποίων να χρησιμοποιεί κυβερνοεπιθέσεις (cyber attacks).

Αντίστοιχα, με τον όρο «κυβερνοεπίθεση» ορίζεται κάθε σκόπιμη προσπάθεια, που λαμβάνει χώρα από μία πλευρά για την επίτευξη Διαταραχής (Disruption) ή Διαφθοράς (Corruption) ή Κορεσμού (με αποτέλεσμα το Denial of Service) στα συστήματα Η/Υ της άλλης πλευράς.

Κατά την τελευταία δεκαετία, τόσο ο αριθμός των κυβερνοεπιθέσεων, όσο και η εξειδίκευση των κακόβουλων λογισμικών, που χρησιμοποιούνται σε αυτές έχουν αυξηθεί σημαντικά, με αποτέλεσμα την αύξηση των κυβερνοσυγκρούσεων.

2.2 Μορφές και Είδη Κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις διακρίνονται σε πέντε (5) βασικές κατηγορίες με βάση τους δράστες, το σκοπό των κυβερνοεπιθέσεων και το είδος της ζημιάς, που δύναται να προκαλέσουν. Πιο συγκεκριμένα κατηγοριοποιούνται ως εξής[B5]:

- ✓ Βανδαλισμός στον Κυβερνοχώρο (Cyber Vandalism)

Σε αυτήν την κατηγορία λαμβάνει χώρα τροποποίηση ή καταστροφή περιεχομένου στον κυβερνοχώρο[B10], π.χ. αλλαγές στο περιεχόμενο μιας ιστοσελίδας χωρίς έγκριση. Γενικά, ο βανδαλισμός στον κυβερνοχώρο είναι αρκετά συνηθισμένος και σχετικά ακίνδυνος ως πρακτική. Οι πλέον διαδεδομένες μορφές του είναι οι εικονικές καταλήψεις, οι βομβαρδισμοί με ηλεκτρονικά μηνύματα, η χρήση ιών και το hacking σε ιστοσελίδες[B13]. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας αποτελεί η ομάδα «Anonymous».

- ✓ Κυβερνοέγκλημα (Cyber Crime)

Το κυβερνοέγκλημα αφορά σε διεξαγωγή κυβερνοεπιθέσεων κατά ιδιωτών ή ιδιωτικών οργανισμών με σκοπό το οικονομικό όφελος του δράστη[B27]. Το κυβερνοέγκλημα διαχωρίζεται σε χαμηλού επιπέδου και σε σοβαρό και οργανωμένο κυβερνοέγκλημα. Επιπλέον, πρέπει να επισημανθεί ότι το κυβερνοέγκλημα θεωρείται ως το εργαστήριο, όπου

αναπτύσσονται, ελέγχονται και τελειοποιούνται τα κακόβουλα λογισμικά, που θα χρησιμοποιηθούν στον κυβερνοπόλεμο.

- ✓ Κυβερνοκατασκοπεία (Cyber Espionage)

Σε αυτήν την κατηγορία εντάσσονται όλες οι ενέργειες, που εκτελούνται από διάφορες επιχειρήσεις, κράτη ή οργανισμούς και έχουν ως στόχο τη συλλογή πληροφοριών σχετικά με άλλα κράτη, κυβερνήσεις ή βιομηχανίες του ιδιωτικού φορέα[B27]. Η κυβερνοκατασκοπεία αποτελεί την πλέον διαδεδομένη δραστηριότητα στον κυβερνοχώρο. Πιο συγκεκριμένα, έχει ως στόχο την άντληση δεδομένων υψηλής διαβάθμισης, τα οποία θα προσδώσουν στον κάτοχό τους συγκριτικό πλεονέκτημα σε σχέση με τους ανταγωνιστές του. Η Κίνα θεωρείται ως η χώρα με τη μεγαλύτερη δραστηριότητα διεξαγωγής τέτοιου είδους επιχειρήσεων.

- ✓ Κυβερνοτρομοκρατία (Cyber Terrorism)

Η Κυβερνοτρομοκρατία ή Ηλεκτρονική Τρομοκρατία περιγράφεται από όλες τις 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[A5]. Μια κυβερνοεπίθεση θεωρείται κυβερνοτρομοκρατία όταν εξασκεί φυσική βία κατά ατόμων ή περιουσιών, ή όταν προκαλεί τέτοια ζημιά, προκαλώντας τον τρόμο. 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.

- ✓ Κυβερνοπόλεμος (Cyber War)

Ως κυβερνοπόλεμος ορίζεται το σύνολο των ενεργειών , που λαμβάνουν χώρα από ένα κράτος προκειμένου να διεισδύσει στα δίκτυα Η/Υ μιας άλλης χώρας, με σκοπό να προκαλέσει ζημιά ή αναταραχή σε αυτά[B6]. Οι υπόψη ενέργειες μπορεί να προέρχονται είτε από κρατικούς λειτουργούς (π.χ. μυστικές υπηρεσίες, ένοπλες δυνάμεις) είτε από διορισμένους από τα κράτη μη κρατικούς δρώντες. Σε σχέση με τις παραπάνω μορφές κυβερνοεπιθέσεων θεωρείται η πιο ακραία μορφή σύγκρουσης[B28].

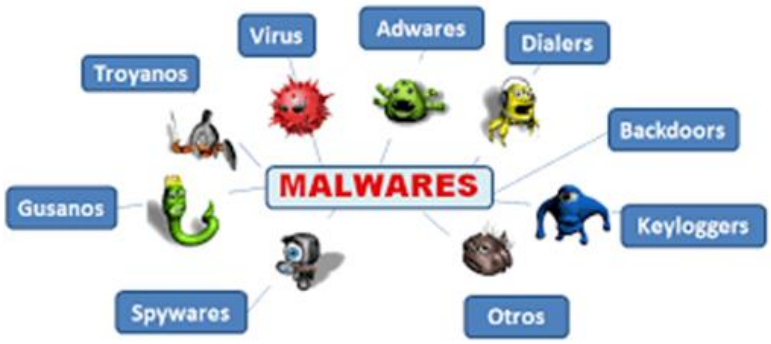
2.3 Μέσα Κυβερνοεπιθέσεων

Τα μέσα, τα οποία μπορεί να χρησιμοποιήσει μία χώρα ή μία επιχείρηση ή ακόμα και ένα άτομα κατά την εκδήλωση κυβερνοεπιθέσεων ονομάζονται «κυβερνοόπλα». Αυτά σχετίζονται είτε με τη συσκευή Η/Υ είτε με κακόβουλα προγράμματα. Τα μέσα εκδήλωσης κυβερνοεπιθέσεων διαχωρίζονται σε τρεις (3) κατηγορίες, επιθετικά, διπλής χρήσης και αμυντικά[B1].

Επιθετικά (Offensive)[B1]

Στην κατηγορία αυτή, εντάσσονται λογισμικά προγράμματα, όπως οι ιοί (viruses), τα «σκουλήκια» (worms), οι «Δούρειοι Ίπποι» (Trojan Horses), τα οποία στοχεύουν στην πρόκληση ζημιών τόσο στον Η/Υ, όσο και στο δίκτυο Η/Υ, που ανήκει. Σε γενικές γραμμές τα συγκεκριμένα προγράμματα λογισμικού επιτίθενται, διαταράσσοντας την ομαλή λειτουργία των Η/Υ ή εξασφαλίζοντας τη δυνατότητα σε κάποιον να αποκτήσει τον έλεγχο του Η/Υ ακόμα και αν βρίσκεται σε απόσταση από αυτόν.

Επιπλέον, σε αυτήν την κατηγορία εντάσσονται και τα μέσα εκείνα, τα οποία προκαλούν επιθέσεις άρνησης παροχής υπηρεσιών (DoS) με σκοπό την υπερφόρτωση του συστήματος και την αδυναμία εξυπηρέτησης των χρηστών, που το χρησιμοποιούν. Τέλος, στα επιθετικά μέσα κυβερνοεπιθέσεων περιλαμβάνονται και οι «λογικές βόμβες» («logic bombs», οι οποίες σκοπεύουν στη μείωση της ταχύτητας ενός Η/Υ, τη διαγραφή δεδομένων και την ενεργοποίηση μιας επίθεσης άρνησης παροχής υπηρεσιών (DoS).



Εικόνα 2.1 Επιθετικά Μέσα Εκδήλωσης Κυβερνοεπιθέσεων

Διπλής Χρήσης (Dual Use)[B1]

Σε αυτήν την ομάδα μέσων περιλαμβάνονται τα εργαλεία εκείνα, τα οποία μπορούν να χρησιμοποιηθούν εξίσου για επιθετικούς και αμυντικούς σκοπούς. Χαρακτηριστικό παράδειγμα αποτελεί ο σαρωτής αδυναμιών (port vulnerabilities scanner), ο οποίες περιλαμβάνει πρόγραμμα, που αξιολογεί τον Η/Υ, τα συστήματα Η/Υ, τα δίκτυα και τις

εφαρμογές για τυχόν αδυναμίες. Δεύτερο παράδειγμα αποτελεί το σύστημα ελέγχου δικτύου (network monitoring), το οποίο ελέγχει διαρκώς το δίκτυο Η/Υ για τυχόν υπολειτουργικότητα ή καταστροφή κάποιων τμημάτων του, ενημερώνοντας άμεσα το διαχειριστή του συστήματος με την αποστολή αυτοματοποιημένου ηλεκτρονικού μηνύματος (email).

Αμυντικά (Defensive)[B1]

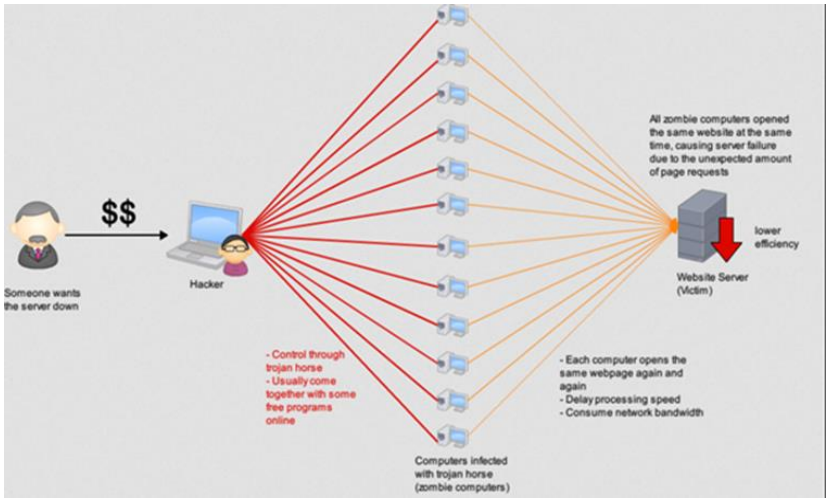
Η συγκεκριμένη κατηγορία μέσων περιλαμβάνει τα «όπλα», τα οποία δρουν επικουρικά στην ασφάλεια των συστημάτων Η/Υ. Τέτοια παραδείγματα είναι η κωδικοποίηση (encryption) της ψηφιακής πληροφορίας, ώστε να μην είναι αναγνώσιμη σε όσους δεν έχουν πρόσβαση στον κώδικα αποκωδικοποίησης και το «τείχος προστασίας» (firewall), το οποίο ρυθμίζει τη ροή των δεδομένων μεταξύ των δικτύων Η/Υ με διαφορετικά επίπεδα ασφαλείας.

2.4 Τεχνικές Κυβερνοεπιθέσεων

Τα κυβερνοόπλα, που αναφέρθηκαν δύναται να χρησιμοποιηθούν σε διάφορους συνδυασμούς προκειμένου να υλοποιήσουν μία ποικιλία τεχνικών προσβολής κάποιου στόχου. Η επιλογή της τεχνικής, που θα χρησιμοποιηθεί για την προσβολή εξαρτάται από διάφορους παράγοντες, όπως οι ικανότητες και η εμπειρία του χρήστη, οι δυνατότητες των μέσων, η φύση του στόχου. Οι πλέον διαδεδομένες τεχνικές κυβερνοεπιθέσεων είναι οι εξής[B7]:

- DoS (Denial of Service) Attack[B7]

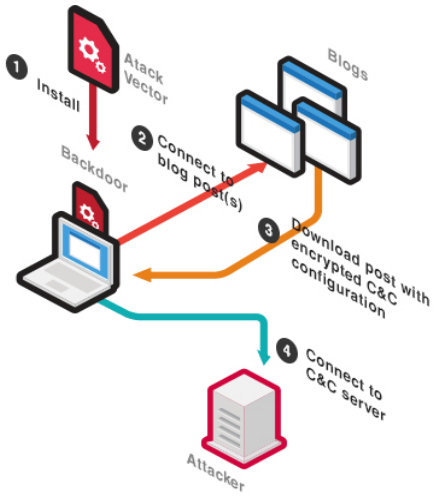
Πρόκειται για τεχνική, η οποία βασίζεται στην αποστολή μεγάλου όγκου δεδομένων προς το στόχο Η/Υ ή δίκτυο, με αποτέλεσμα τον κορεσμό και την απώλεια προσβασιμότητας σε αυτά από τους νόμιμους χρήστες.



Εικόνα 2.2 Παράδειγμα Επίθεσης DoS

- Backdoor[B7]

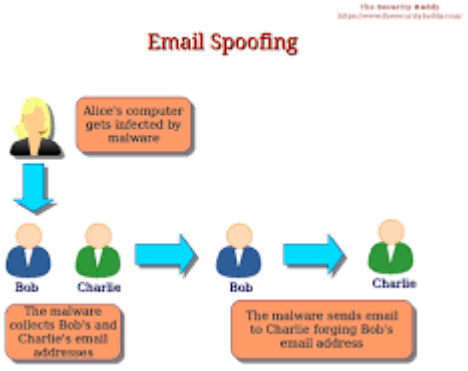
Ακολουθώντας αυτήν την τεχνική, οι κερκόπορτες (backdoors) είναι σημεία εισόδου, που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας τη συνηθισμένη διαδικασία ελέγχου πρόσβασης.



Εικόνα 2.3 Παράδειγμα Επίθεσης Backdoor

- Email Spoofing[Γ3]

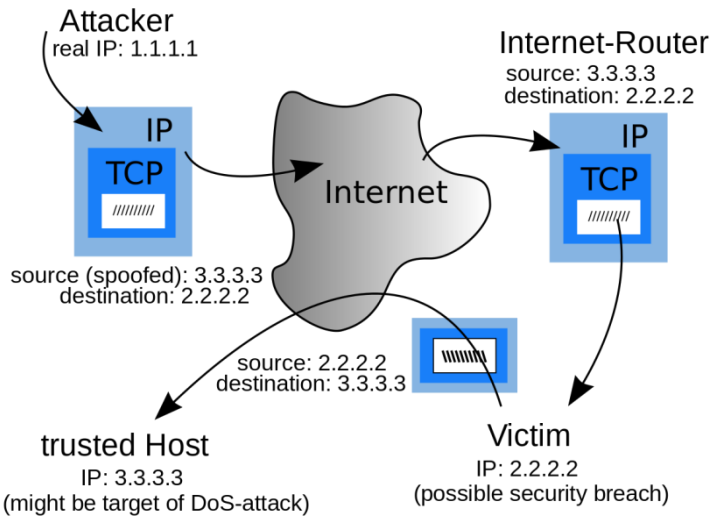
Σύμφωνα με αυτήν την τεχνική, οι πληροφορίες, που στέλνει ο αποστολέας φαίνονται εύκολα και έτσι μπορούν να αντιγραφούν ή να πλαστογραφηθούν. Αυτό κυρίως δημιουργείται από spammers (κάποια ενοχλητικά μηνύματα που παρουσιάζονται στην οθόνη του υπολογιστή μας κατά την είσοδο σε διάφορες σελίδες του διαδικτύου) και δημιουργούν πρόβλημα με λάθος κατευθύνσεις με άμεσο σκοπό την αρπαγή προσωπικών δεδομένων.



Εικόνα 2.4 Παράδειγμα Επίθεσης Email Spoofing

- IP Spoofing[Γ3]

Είναι μια τεχνική για να αποκτηθεί παράνομη πρόσβαση σε υπολογιστές με την δημιουργία πακέτων TCP/IP, χρησιμοποιώντας τη διεύθυνση και τα στοιχεία κάποιου άλλου αξιόπιστου. Οι δρομολογητές (routers) χρησιμοποιούν την διεύθυνση της IP προορισμού (destination IP) ώστε να διαδώσουν τα δεδομένα μέσω διαδικτύου αγνοώντας ή αλλάζοντας εικονικά την διεύθυνση της IP πηγής (source IP). Αυτή η διεύθυνση χρησιμοποιείται μόνο από το μηχάνημα προορισμού όταν απαντά πίσω στη πηγή. Η IP spoofing είναι αναπόσπαστο μέρος πολλών επιθέσεων στο δίκτυο.



Εικόνα 2.5 Παράδειγμα Επίθεσης IP Spoofing

- Logic Bomb[B7]

Αυτή η τεχνική εστιάζεται στην εφαρμογή λογισμικού ή συνόλου οδηγιών, που προκαλούν τη διακοπή της λειτουργίας του Η/Υ ή του δικτύου καθώς επίσης και τη διαγραφή των δεδομένων ή του λογισμικού του δικτύου.

- Digital Manipulation[B7]

Αυτή η τεχνική περιγράφει τη διάδοση ψευδούς φήμης σχετικά με την ύπαρξη νεοεμφανιζόμενου κακόβουλου λογισμικού, αλλά και με οποιοδήποτε άλλο θέμα μπορεί να οδηγήσει σε σπατάλη πόρων.

2.5 Κρίσιμες Υποδομές ως Πιθανοί Στόχοι

Πάντοτε υποδομές ενός κράτους, όπως τα αεροδρόμια, τα εργοστάσια παραγωγής ηλεκτρικής ενέργειας, οι αγωγοί πετρελαίου και φυσικού αερίου, τα τηλεπικοινωνιακά κέντρα αποτελούσαν μόνιμα στρατιωτικούς στόχους καθώς η πρόκληση φθορών ή ολικής καταστροφής τους επέφερε την αποδυνάμωση του αντιπάλου, οδηγώντας στην ευκολότερη επικράτηση στο πεδίο της μάχης[B17].

Την τελευταία εικοσαετία αυτές οι υποδομές εξακολουθούν να αποτελούν βασικούς στόχους με τη διαφορά ότι πλέον δεν χρειάζεται να πληγούν υλικά, καθώς οι περισσότερες είναι άμεσα εξαρτημένες από την ομαλή λειτουργία ηλεκτρονικών συστημάτων και δικτύων. Επομένως, συνδέονται με το πεδίο του κυβερνοχώρου και μπορούν εύκολα να πληγούν με τη μεθόδευση μιας επίθεσης εντός του πεδίου. Ως κρίσιμες υποδομές δύναται να χαρακτηριστούν εκείνες, οι οποίες ελέγχουν[B36]:

- Υπηρεσίες πληροφορικής και τηλεπικοινωνιών
- Οικονομικές υπηρεσίες
- Συστήματα παραγωγής και διάθεσης ηλεκτρικής ισχύος
- Συστήματα παραγωγής, αποθήκευσης και διανομής καυσίμων και φυσικού αερίου
- Υπηρεσίες συγκοινωνιών (οδικών, θαλάσσιων, αεροπορικών, σιδηροδρομικών)
- Υπηρεσίες υδάτινων πόρων
- Υπηρεσίες εξυπηρέτησης πολιτών
- Υπηρεσίες παροχής υγειονομικής κάλυψης

Συστήματα, που εξυπηρετούν τηλεπικοινωνιακές, ενεργειακές και χρηματοπιστωτικές υπηρεσίες καθώς και ζωτικής σημασίας υπηρεσίες για τους πολίτες θεωρούνται οι πλέον πιθανοί στόχοι, καθώς η αδρανοποίηση ή η καταστροφή τους μπορεί να εγείρει αισθήματα φόβου και ανασφάλειας στον πληθυσμό με αποτέλεσμα να πλήξει το ηθικό του, να αποσταθεροποιήσει πλήρως την οικονομία και συνεπώς να οδηγήσει στην παράλυση ενός κράτους, μεγιστοποιώντας την αποτελεσματικότητα μιας μεταγενέστερης επίθεσης με υλικά – συμβατικά μέσα[B35].

2.6 Ευνοϊκοί Παράγοντες Διεξαγωγής Κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις προσδιορίζονται από πληθώρα στοιχείων, που συνθέτουν τον ιδιαίτερο χαρακτήρα τους, επιτρέποντας την εκδήλωσή τους ευρέως. Πιο συγκεκριμένα, οι παράγοντες, που ευνοούν τη διεξαγωγή τέτοιου είδους επιθέσεων συνοψίζονται στα παρακάτω:

✓ Λόγω της ανοιχτής αρχιτεκτονικής του διαδικτύου και των άλλων δικτύων, που χρησιμοποιούν τα ίδια πρωτόκολλα επικοινωνίας, παρέχεται η δυνατότητα στον επιτιθέμενο να αποκρύψει την ταυτότητα και τις πραγματικές του προθέσεις. Ως εκ τούτου δεν είναι εφικτός ο άμεσος, χρονικά, εντοπισμός του τόπου προέλευσης της επίθεσης, ο οποίος άλλωστε δύναται να απέχει γεωγραφικά από το στόχο[Γ2].

✓ Τα κυβερνοόπλα, που διεξάγουν τις κυβερνοεπιθέσεις, έχουν μικρό κόστος, διατίθενται χωρίς ιδιαίτερους περιορισμούς σε κάθε ενδιαφερόμενο και ο χειρισμός τους επιτυγχάνεται εύκολα από τον καθένα χωρίς να απαιτούνται εξειδικευμένες γνώσεις ή σχετική εκπαίδευση. Στον αντίποδα, ο οικονομικός απολογισμός των ζημιών, που δύναται να προκληθούν, μπορεί να καταλήξει σε υπέρογκα χρηματικά ποσά[B39].

✓ Οι περισσότεροι στόχοι, όπως τα διάφορα ηλεκτρονικά συστήματα, μιας τέτοιας επίθεσης λειτουργούν βάσει λογισμικού, που παράγεται μαζικά από ιδιωτικές επιχειρήσεις, προοριζόμενο για μαζική κατανάλωση. Ως συνέπεια, τα συστήματα είναι ευάλωτα καθώς δεν δίνεται η δέουσα βαρύτητα στον τομέα της ασφάλειας τους. Αυτό δικαιολογείται εν μέρει καθώς μια τέτοια πρόνοια καθίσταται οικονομικά ασύμφορη, λόγω της προϋπόθεσης σχεδιασμού εξειδικευμένων και πολύπλοκων προγραμμάτων, η οποία επιφέρει ανάλογη αύξηση στο κόστος παραγωγής και διάθεσης του προϊόντος[B36].

✓ Τις περισσότερες φορές είναι λιγότερο αιματηρό είδος εχθροπραξίας, ωστόσο μπορεί να προκαλέσει σημαντικές καταστροφές με μακροχρόνια αποτελέσματα. Πιθανά σενάρια μπορεί να περιλαμβάνουν επιθέσεις στην ίδια την υποδομή του διαδικτύου, καθώς και σε δίκτυα, που εξυπηρετούν σκοπούς δημόσιας ωφέλειας, όπως παραποιήσεις στο ηλεκτρικό δίκτυο, διακοπές στο τηλεφωνικό σύστημα, παράλυση του τραπεζικού συστήματος, αδρανοποίηση του συστήματος ελέγχου της εναέριας κυκλοφορίας[B36].

✓ Λόγω των ανωτέρω χαρακτηριστικών ανταλλαγή κυβερνοεπιθέσεων μπορεί να διεξαχθεί ανάμεσα σε διάφορους συνδυασμούς δρώντων της διεθνούς σκηνής. Μπορεί να εμφανιστεί μεταξύ ενός κυρίαρχου κράτους και ενός μη κρατικού δρώντος, που χρηματοδοτείται από άλλο κυρίαρχο κράτος. Επίσης, μπορεί να χρησιμοποιηθεί ενάντια σε πολιτικές μιας συγκεκριμένης κυβέρνησης από ομάδες, που υπερασπίζονται το περιβάλλον, τα ανθρώπινα δικαιώματα ή άλλα ζητήματα θρησκευτικού ή πολιτιστικού χαρακτήρα. Τέλος, οι κυβερνοεπιθέσεις θεωρούνται μια ιδιαίτερα ελκυστική επιλογή δράσης για τις τρομοκρατικές ομάδες κυρίως εξαιτίας της δυνατότητας, που προσφέρουν για ανώνυμη δίχως κόστος και απομακρυσμένη δράση, ικανή να πλήξει ποικίλους στόχους και να επηρεάσει την καθημερινότητα μεγάλου αριθμού ατόμων[B17].

2.7 Σκοπός Κυβερνοεπιθέσεων

Η χρήση των κυβερνοόπλων και οι τεχνικές για την προσβολή στόχων δεν αποτελούν αυτοσκοπό. Οι κυβερνοεπιθέσεις διεξάγονται για την επίτευξη κάποιου συγκεκριμένου σκοπού. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικά όμως ανήκει σε μία από τις παρακάτω κατηγορίες[Γ4]:

- Εκμετάλλευση (Exploitation)

Σε αυτήν την περίπτωση βασικός στόχος είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών, που είναι συνδεδεμένες με αυτόν.

- Παραπλάνηση (Deception)

Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις πληροφορίες τις οποίες συλλέγει, αναλύει ή παράγει, στοχεύοντας στο σύστημα λήψης αποφάσεων του αντιπάλου.

- Καταστροφή (Destruction)

Σε αυτήν την περίπτωση, ο επιτιθέμενος, με τη χρήση πληροφοριακών συστημάτων, καθιστά αδύνατη τη λειτουργία του στόχου, καταστρέφοντας τον ίδιο ή τα συστήματα υποστήριξης, που είναι απαραίτητα για τη λειτουργία του. Ο πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου, αλλά η κρίσιμη υποδομή του. Χαρακτηριστικό παράδειγμα αποτέλεσε το 2001 στην Αυστραλία άτομο, το οποίο χρησιμοποιώντας το διαδίκτυο, έναν ασύρματο και ένα λογισμικό ελέγχου κατάφερε να αποδεσμεύσει 1 εκατομμύριο λίτρα λυμάτων στα νερά ενός ποταμού, στόχος, ο οποίος επετεύχθη μετά από 44 αποτυχημένες προσπάθειες.

- Διακοπή Λειτουργίας ή Εξουδετέρωση (Denial of Service ή Disruption)

Στην περίπτωση επιθέσεων διακοπής λειτουργίας (DoS) ή εξουδετέρωσης, ο επιτιθέμενος δεν καταστρέφει το στόχο αλλά τον θέτει εκτός λειτουργίας ή τον καθιστά αναξιόπιστο για κάποιο χρονικό διάστημα, απαγορεύοντας στους νόμιμους χρήστες την εξυπηρέτησής τους ή την πρόσβαση σε πηγές πληροφοριών.

ΚΕΦΑΛΑΙΟ 3 ΜΟΝΤΕΛΑ ΕΠΙΘΕΣΕΩΝ

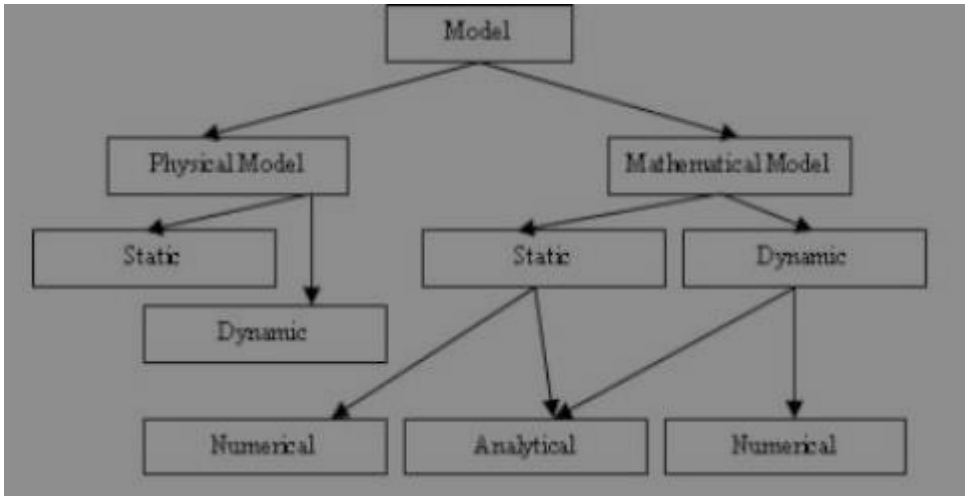
3.1 Ορισμός

Τα «μοντέλα επιθέσεων» αναφέρονται σε εξειδικευμένα προγράμματα, τα οποία έχουν ως σκοπό τον έλεγχο των συστημάτων των Η/Υ και των δικτύων Η/Υ με σκοπό την εξέταση της ασφάλειας και την ανάλυση της εκμετάλλευσης τρωτοτήτων καθώς και γενικότερα των κυβερνοεπιθέσεων σε ένα δίκτυο ή σύστημα[B3].

3.2 Κατηγορίες Μοντέλων Επίθεσης

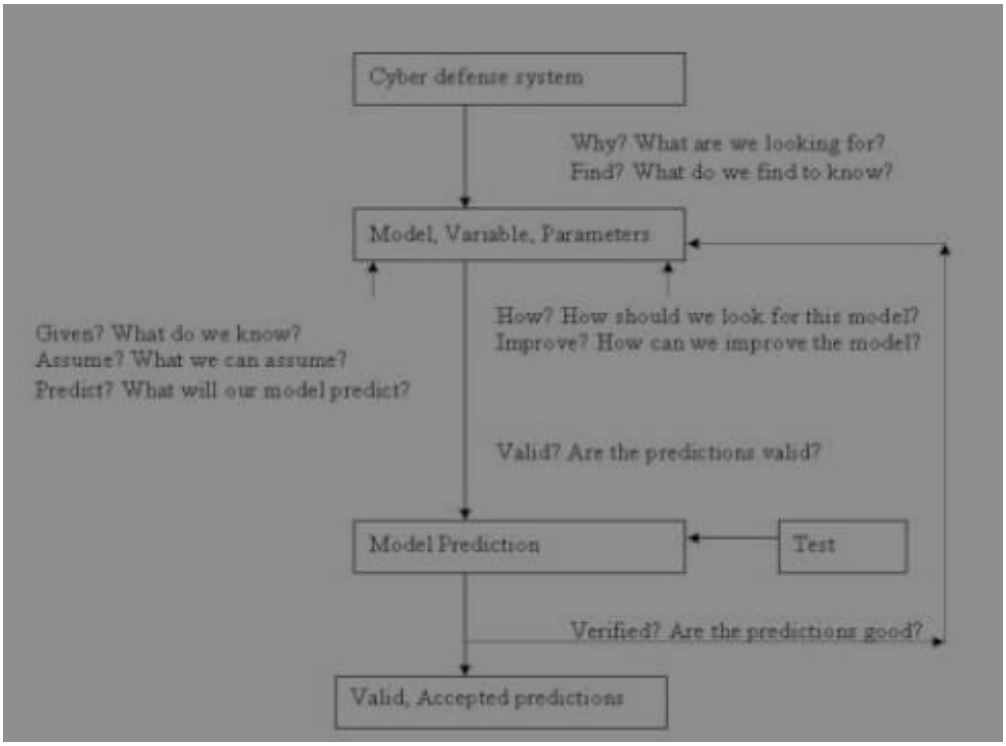
Υπάρχουν διάφορα μοντέλα , και πιο συγκεκριμένα τα ακόλουθα[B3]:

- Φυσικά μοντέλα: βασίζονται σε κάποιο είδους αναλογίας μηχανικών, ηλεκτρολογικών ή ηλεκτρονικών και υδραυλικών συστημάτων.
- Μαθηματικά μοντέλα: τα συστήματα που μπορούν να αναπαρασταθούν σε μία μορφή μαθηματικών συναρτήσεων, όπως το σύστημα προσφοράς – ζήτησης.
- Φυσικά Στατικά μοντέλα: αυτά τα φυσικά μοντέλα δεν αλλάζουν τη συμπεριφορά τους με το πέρασμα του χρόνου.
- Φυσικά Δυναμικά μοντέλα: αυτά τα φυσικά μοντέλα αλλάζουν τη συμπεριφορά τους με το πέρασμα του χρόνου, όπως τα ηλεκτρικά συστήματα.
- Μαθηματικά Στατικά μοντέλα: αυτά τα μαθηματικά μοντέλα δίνουν μια μαθηματική εξίσωση, όταν το σύστημα είναι σε ισορροπία όπως το σύστημα προσφοράς – ζήτησης.
- Μαθηματικά Δυναμικά μοντέλα: σε αυτά τα μοντέλα επιτρέπεται η αλλαγή των γνωρισμάτων παράλληλα με τη συνάρτηση του χρόνου.
- Μαθηματικά Στατικά Αναλυτικά μοντέλα: αυτά είναι μικρά μαθηματικά μοντέλα τα οποία μπορούν να λυθούν με τη χρήση παραδοσιακών μαθηματικών.
- Μαθηματικά Στατικά Αριθμητικά μοντέλα: αυτά είναι πολύπλοκα στατικά μαθηματικά μοντέλα που μπορούν να λυθούν με εξομοίωση.
- Μαθηματικά Δυναμικά Αναλυτικά μοντέλα: αυτά είναι μικρά δυναμικά μαθηματικά μοντέλα που μπορούν να λυθούν από παραδοσιακά μαθηματικά.
- Μαθηματικά Δυναμικά Αριθμητικά μοντέλα: αυτά είναι σύνθετα δυναμικά μοντέλα που μπορούν να λυθούν από εξομοίωση.



Εικόνα 3.1 Μαθηματικά Μοντέλα

Στο παρακάτω σχήμα απεικονίζεται η διαδικασία μοντελοποίησης. Περιλαμβάνει τα εξής στάδια: αρχικοποίηση του συστήματος κυβερνοάμυνας, δημιουργία του μοντέλου, των μεταβλητών και των παραμέτρων, τη μοντελοποίηση και των έλεγχο αυτής και τέλος, την αξιολόγηση.



Εικόνα 3.2 Διαδικασία μαθηματικής μοντελοποίησης

3.3 Μοντέλα Επιθέσεων

Τα μοντέλα επιθέσεων είναι κυρίως μαθηματικά και βασίζονται σε πιθανότητες, γραφήματα επιθέσεων και έννοιες της Θεωρίας Παιγνίων[B3].

3.3.1 Μοντέλα Επιθέσεων Βασιζόμενα σε Πιθανότητες

Για την εξάπλωση των ιών υπολογιστών, που μολύνουν κάτω από διαφορετικές συνθήκες, γίνεται προσπάθεια ανάπτυξης μαθηματικών μοντέλων, τα οποία βασίζονται σε πιθανότητες[B40].

Πιο συγκεκριμένα, υπάρχουν αναφορές ‘ότι οι επιθέσεις σε υπολογιστή είναι στο σύνολό τους στοχαστικές, δηλαδή ο ακριβής χρόνος της επόμενης επίθεσης είναι άγνωστος. Παρ’ όλα αυτά, όμως, στα πλαίσια πιθανοτήτων δύναται να εντοπιστεί η πιθανότητα εκδήλωσης μιας επίθεσης σε κάποια χρονική στιγμή. Η αθροιστική συνάρτηση κατανομής δίνει την πιθανότητα των στοχαστικών επιθέσεων να είναι μικρότερες ή ίσες με μία δεδομένη τιμή. Με τη χρήση διαφορικών συναρτήσεων και των σειρών Taylor, υπολογίζεται η ταχύτητα και η επιτάχυνση της εξάπλωσης.

Παράλληλα, προτείνεται ένα queueing μοντέλο για την εξάπλωση των DoS επιθέσεων στα δίκτυα Η/Υ. Το συγκεκριμένο μοντέλο αναπτύσσει έναν αλγόριθμο για την εύρεση της στάσιμης κατανομής πιθανότητας, που μπορεί να χρησιμοποιηθεί για την εύρεση άλλων ενδιαφέροντων στοιχείων απόδοσης, όπως η πιθανότητα απώλειας συνδεσιμότητας και τα ποσοστά κατανάλωσης του buffer σε συνδέσεις με μισή κανονική κίνηση και μισή κίνηση επίθεσης.

3.3.2 Μοντέλα Επιθέσεων Βασιζόμενα σε Γραφήματα Επιθέσεων

Ένα γράφημα σεναρίου αποτυχίας είναι μία συνοπτική αναπαράσταση όλων των εκτελέσιμων μονοπατιών μέσα από ένα σύστημα που παραβιάζει κάποια συνθήκη ορθότητας. Τα γραφήματα σεναρίων αναπαριστούν οτιδήποτε μπορεί να λειτουργήσει εσφαλμένα σε ένα σύστημα, δίνοντας στο μηχανικό την δυνατότητα να κατατάξει καταλλήλως τα προβλήματα[B11].

Γενικά, οι απαιτήσεις ενός συστήματος (γνωστές και ως ιδιότητες ορθότητας) μπορούν να καταταγούν σε δύο κατηγορίες, ιδιότητες ασφάλειας και ζωτικές ιδιότητες. Οι ιδιότητες ασφάλειας δηλώνουν ότι τίποτα κακό δεν πρόκειται να συμβεί στο σύστημα. Για

παράδειγμα: ένας εισβολέας δε θα αποκτήσει ποτέ τα δικαιώματα του χρήστη ή του διαχειριστή του δικτύου, ένα σφάλμα σε ένα μεμονωμένο σημείο δε θα προκαλέσει την κατάρρευση όλου του συστήματος. Οι ιδιότητες ασφαλείας μπορούν να εκφραστούν με μεταβλητές που δηλώνουν ότι το σύστημα δε θα εισέλθει σε ανασφαλή κατάσταση. Ανεπίσημα, ένα γράφημα σεναρίων που αναπαριστά παραβιάσεις κάποιας ιδιότητας ασφαλείας ενσωματώνει όλες τις περιπτώσεις που θα οδηγήσουν ένα σύστημα σε ανασφαλή κατάσταση.

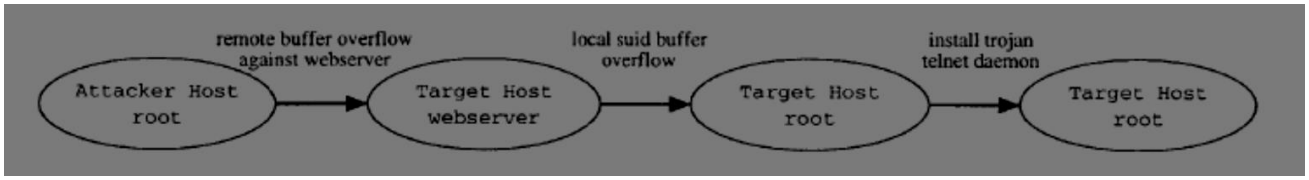
Οι ιδιότητες ασφαλείας από μόνες τους δεν είναι ικανές να εξασφαλίσουν την ορθή λειτουργία ενός συστήματος. Οι ζωτικές απαιτήσεις σχεδιάστηκαν για να καθορίσουν τις κύριες ενέργειες ενός συστήματος. Για παράδειγμα, ένα τραπεζικό σύστημα πρέπει να έχει μία απαίτηση ζωτικότητας που να δηλώνει ότι εάν προταθεί ένας τρόπος ελέγχου και είναι διαθέσιμοι οι οικονομικοί πόροι, τότε ο τρόπος ελέγχου εξασφαλίζεται. Παραβίαση μιας ζωτικής απαίτησης συμβαίνει όταν κολλήσει ένα σύστημα, είτε λόγω ολοκληρωτικού τερματισμού του είτε λόγω συμπεριφορών του που δε συνάδουν με τα έργα τα οποία πρέπει να επιτελέσει.

Καθώς τα δίκτυα των χρηστών εξαπλώνονται, είναι ολοένα και πιο σημαντικό να αυτοματοποιείται η διαδικασία αξιολόγησης των τρωτοτήτων όταν δέχονται επιθέσεις. Όταν αξιολογείται η ασφάλεια ενός δικτύου, είναι συνήθως αρκετό να θεωρήσουμε την ύπαρξη ή την απουσία μεμονωμένων τρωτοτήτων. Τα μεγάλα δίκτυα περιέχουν πολλαπλές πλατφόρμες και πακέτα λογισμικών και εφαρμόζουν ποικίλους τρόπους συνδεσιμότητας.

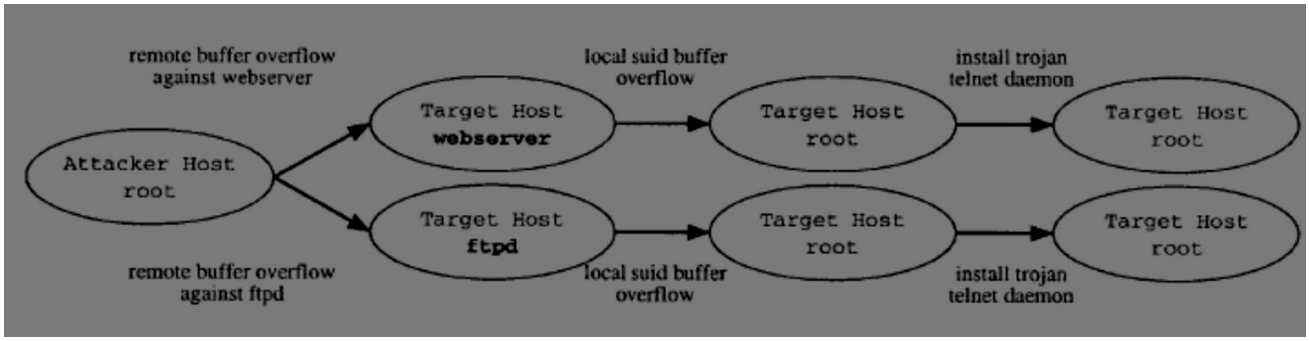
Για την αξιολόγηση της ασφάλειας ενός δικτύου χρηστών, ένα αναλυτής ασφάλειας πρέπει να λάβει υπόψη του τα αποτελέσματα των αλληλεπιδράσεων των τοπικών τρωτοτήτων και να βρίσκει τις γενικές τρύπες ασφαλείας. Σε μία τυπική διαδικασία ανάλυσης τρωτοτήτων, αρχικά τα εργαλεία σαρώσεων καθορίζουν τις τρωτότητες των ξεχωριστών χρηστών. Χρησιμοποιώντας αυτές τις πληροφορίες των τοπικών τρωτοτήτων σε συνδυασμό με άλλες πληροφορίες από το δίκτυο, όπως η συνδεσιμότητα μεταξύ των χρηστών, ο αναλυτής παράγει το γράφημα επιθέσεων. Κάθε μονοπάτι στο γράφημα επιθέσεων είναι μία σειρά από εκμεταλλεύσιμα σημεία, τα οποία καλούμε δράσεις, και που οδηγούν στη μη επιθυμητή κατάσταση. Ένα παράδειγμα μιας μη επιθυμητής κατάστασης είναι μία κατάσταση όπου ο εισβολέας έχει αποκτήσει πρόσβαση διαχειριστή σε έναν χρήστη.

Πιο αναλυτικά, κάθε στοιχείο μιας επίθεσης αναπαριστά μία μετάβαση μεταξύ δύο καταστάσεων. Μία σειρά επιθέσεων αναπαριστά μία κατευθυνόμενη διαδρομή. Όλα τα μονοπάτια επιθέσεων εναντίων ενός δικτύου μπορούν να συγχωνευτούν και να δημιουργήσουν ένα δέντρο επιθέσεων. Αυτό το δέντρο επιθέσεων μπορεί να μετατραπεί σε ένα γράφημα συνδυάζοντας τις καταστάσεις και να τις παρουσιάσει στο διαχειριστή. Οι

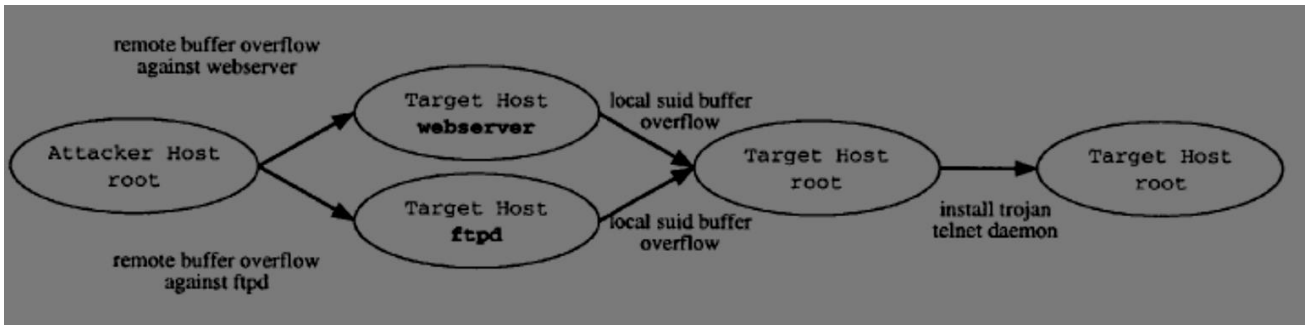
κόμβοι αναπαριστούν την τρέχουσα κατάσταση του συστήματος. Αυτό περιλαμβάνει το τρέχον επίπεδο δικαιωμάτων του εισβολέα, τα προηγούμενα δικαιώματα σε όλους τους υπολογιστές του δικτύου, και τις τροποποιήσεις που έγιναν από τον εισβολέα.



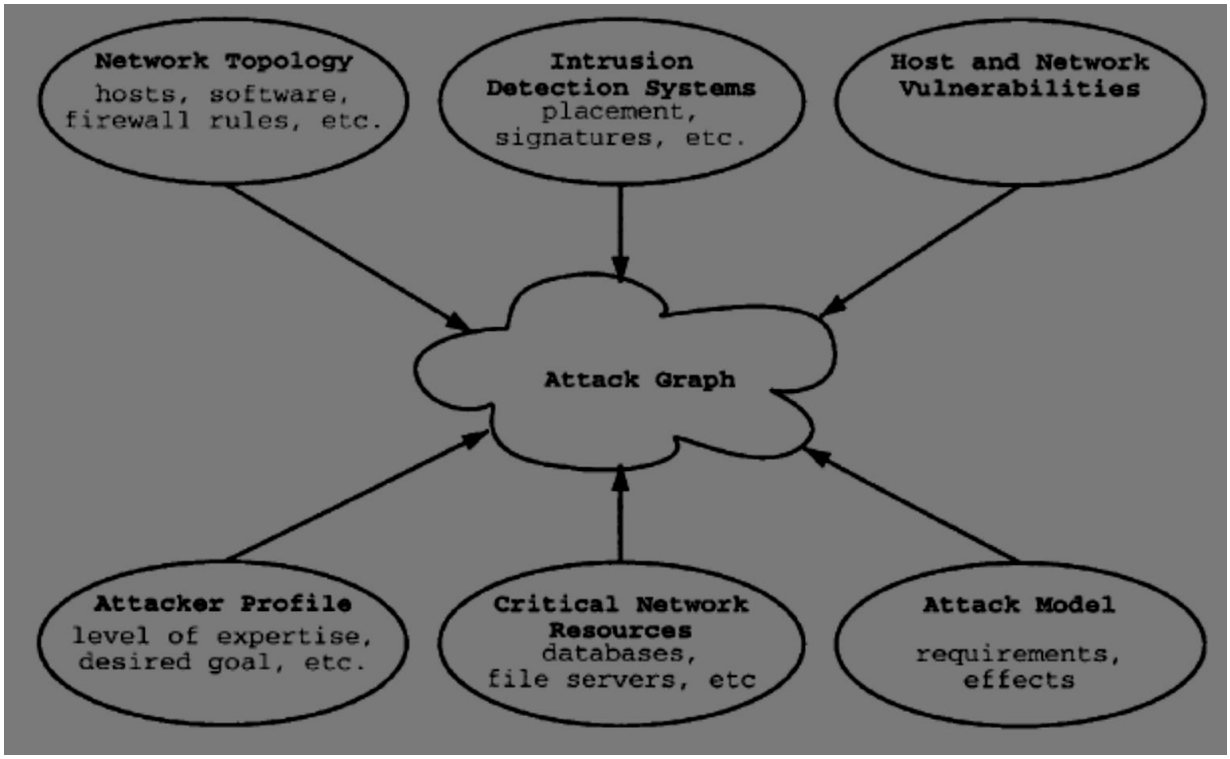
Εικόνα 3.3 Παράδειγμα διαδρομής επιθέσεων



Εικόνα 3.4 Παράδειγμα δέντρου επιθέσεων



Εικόνα 3.5 Παράδειγμα γραφήματος επιθέσεων



Εικόνα 3.6 Απαραίτητες πληροφορίες για τη δημιουργία του γραφήματος επιθέσεων

Τα γραφήματα επιθέσεων μπορούν να χρησιμοποιηθούν ως ένα χρήσιμο εργαλείο σε διάφορους τομείς της ασφάλειας δικτύων, συμπεριλαμβανομένων των: ανίχνευση διεισδύσεων, άμυνα και ανάλυση αρχών.

Το γράφημα επιθέσεων σε δίκτυα αναπαριστά μία συλλογή από πιθανά σενάρια διεισδύσεων σε ένα δίκτυο υπολογιστών. Κάθε σενάριο διείσδυσης είναι μία σειρά από βήματα του εισβολέα, που καταλήγουν σε ένα συγκεκριμένο στόχο – πρόσβαση του διαχειριστή σε ένα συγκεκριμένο χρήστη, πρόσβαση σε μία βάση δεδομένων, άρνηση πρόσβαση σε υπηρεσίες.

Ένα μοντέλο επιθέσεων σε δίκτυο είναι ένα μοντέλο επιθέσεων όπου το σύστημα είναι ένα δίκτυο υπολογιστών, ο επιτιθέμενος είναι ένας κακόβουλος παράγοντας που προσπαθεί να παρακάμψει την ασφάλεια του δικτύου, και ο αμυνόμενος αναπαριστά και τους διαχειριστές του δικτύου και τα προγράμματα ασφαλείας που είναι εγκατεστημένα στο δίκτυο. Μία μετάβαση κατάστασης σε ένα μοντέλο επιθέσεων σε δίκτυο αντιστοιχεί σε μία μόνο πράξη του εισβολέα, μία αμυντική πράξη από το διαχειριστή του δικτύου ή μία πράξη ρουτίνας του δικτύου[B14].

Συνοψίζοντας, ένα γράφημα επιθέσεων είναι μία συλλογή από σενάρια που δείχνουν πώς ένας κακόβουλος παράγοντας μπορεί να επηρεάσει την ακεραιότητα του συστήματος-στόχου. Τα γραφήματα επιθέσεων χρησιμοποιούνται για να ορίσουν ένα μέτρο έκθεσης ενός δικτύου σε κακόβουλες διεισδύσεις. Για αυτό το λόγο, είναι απαραίτητο να γίνει η διάκριση μεταξύ των αμυντικών στρατηγικών σε στατική και δυναμική άμυνα.

Όσον αφορά τη στατική άμυνα, ένα μέτρο στατικής άμυνας είναι μία μοναδική αλλαγή στην διαμόρφωση του δικτύου που ελαττώνει την έκθεση του δικτύου. Τα στατικά μέτρα περιλαμβάνουν την επιβολή μιας πιο αυστηρής πολιτικής διαχείρισης κωδικών πρόσβασης, την εφαρμογή αναβαθμίσεων ασφαλείας και πιο αυστηρούς κανόνες στο τείχος ασφαλείας[B12]. Ένα μεμονωμένο στατικό μέτρο αντιστοιχεί σε μία τροποποίηση του γραφήματος επιθέσεων, μειώνει τον αριθμό των σεναρίων που μπορεί να εκτελέσει ένας εισβολέας, αλλά δεν παρουσιάζει άλλα επιπρόσθετα εμπόδια στον επιτιθέμενο όταν η επίθεση είναι σε εξέλιξη.

Όταν αποφασίζεται μία στατική αναβάθμιση ασφάλειας, ο διαχειριστής του συστήματος μπορεί να διαθέτει έναν αριθμό επιλογών και να αξιολογεί τη σχετική αποτελεσματικότητά τους.

Από τη στιγμή που έχει παραχθεί ένα γράφημα επιθέσεων για ένα συγκεκριμένο δίκτυο για μία συγκεκριμένη ιδιότητα ασφαλείας, γίνεται η προσπάθεια να μειωθεί η έκθεση του δικτύου σε επιθέσεις. Ένα μέτρο καλύπτει μία πράξη εάν καθιστά την πράξη αναποτελεσματική για τον εισβολέα.

Όσον αφορά τη δυναμική άμυνα, τα μέτρα δυναμικής άμυνας δικτύων δεν έχουν εφαρμοστεί ακόμα πλήρως στα δίκτυα, με εξαίρεση τον χώρο των συστημάτων ανίχνευσης διεισδύσεων. Ένας δυναμικός αμυντικός μηχανισμός καταγράφει συνεχώς το δίκτυο και προσπαθεί δραστικά να εμποδίσει τον επιτιθέμενο να επιτύχει. Πρόκειται για μία ασφαλή πρόβλεψη με την οποία ένα μελλοντικό πρόγραμμα δικτύου θα γνωρίζει την κατάστασή του και η ενεργή άμυνα θα διαδραματίζει ένα μεγαλύτερο ρόλο στην ασφάλεια του δικτύου.

Στη δυναμική άμυνα, ένα σενάριο επίθεσης γίνεται ένα παιχνίδι κινήσεων από τον επιτιθέμενο και απαντήσεων από τον αμυνόμενο, επομένως είναι λογική η εφαρμογή μίας αντιμετώπισης βασισμένη στη θεωρία παιγνίων σε ό,τι αφορά την ανάλυση της αποτελεσματικότητας της δυναμικής άμυνας.

3.3.3 Μοντέλα Επιθέσεων Βασιζόμενα σε Θεωρία Παιγνίων

Η θεωρία παιγνίων χρησιμοποιεί την εκτενή μορφή για να περιγράψει τα παίγνια όπου οι παίκτες κάνουν πολλαπλές κινήσεις και βασίζουν τη στρατηγική τους κάθε φορά ανάλογα με τις πληροφορίες για τις κινήσεις που μόλις έχουν γίνει. Εδώ, καθορίζεται το πεπερασμένο δέντρο παιγνίων Τ που αναπαριστά τη σειρά παιξίματος και τις διαθέσιμες επιλογές των παικτών σε κάθε στάδιο του παιγνίου, το παίγνιο εκτενούς μορφής G, το μοντέλο επίθεσης W, τις στρατηγικές συμπεριφορών και τις απλές και μικτές στρατηγικές σύμφωνα με τις εξισώσεις του Nash. Έτσι, έχουμε μία δυναμική ανάλυση. Σε γενικές γραμμές, η μέθοδος αποτελείται από τα ακόλουθα βήματα[B11]:

- Μοντελοποίηση του δικτύου και της συμπεριφοράς του επιτιθέμενου με τις αμυντικές πράξεις που παρουσιάζονται στις μεταβάσεις κάθε κατάστασης της μηχανής.
- Εκτέλεση της γεννήτριας παραγωγής γραφημάτων επιθέσεων για την κατασκευή του δέντρου παιγνίου του μοντέλου επίθεσης.
- Εφαρμογή επαγωγής προς τα πίσω (ή κάποιου άλλου κατάλληλου αλγορίθμου βασισμένου στη θεωρία παιγνίων) για τον υπολογισμό των βέλτιστων στρατηγικών τόσο για τον επιτιθέμενο όσο και για τον αμυνόμενο.

ΚΕΦΑΛΑΙΟ 4 ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

4.1 Ορισμός

Ως «κυβερνοπόλεμος» ορίζεται το σύνολο των ενεργειών, που λαμβάνουν χώρα από ένα κράτος προκειμένου να διεισδύσει στα δίκτυα Η/Υ μιας άλλης χώρας, με σκοπό να προκαλέσει ζημιά ή αναταραχή σε αυτά. Σύμφωνα με αυτά, οι αντίπαλες οντότητες θα πρέπει να είναι «εξαρτημένες» σε κάποιο βαθμό από τα δίκτυα Η/Υ. Οι υπόψη ενέργειες δύναται να αναληφθούν τόσο από κρατικούς λειτουργούς (μυστικές υπηρεσίες, ένοπλες δυνάμεις), όσο και από μη κρατικούς δρώντες (τρομοκρατικές οργανώσεις, αυτόνομες ομάδες)[Γ5].

Σε αντίθεση με το συμβατική μορφή πολέμου, όπου η βία ασκείται κατά κύριο λόγο από τα κράτη, στον κυβερνοπόλεμο οι μη κρατικοί δρώντες κατέχουν σημαντικό πεδίο δράσης, καθώς το κόστος εισόδου στον κυβερνοχώρο είναι χαμηλό, ενώ η απόκτηση κυβερνοόπλων έχει σχεδόν μηδενικό κόστος.

4.2 Βασικές Μορφές Κυβερνοπολέμου

Ο κυβερνοπόλεμος διακρίνεται στις εξής δύο (2) βασικές μορφές[B14]:

- Στρατηγικός
- Επιχειρησιακός

Στρατηγικός Κυβερνοπόλεμος

Στον στρατηγικό κυβερνοπόλεμο εντάσσονται οι κυβερνοεπιθέσεις, οι οποίες αποσκοπούν στον επηρεασμό της κυβερνητικής πολιτικής του αντιπάλου μέσα από εξαναγκασμό.

Για να θεωρηθεί μια κυβερνοεπίθεση στρατηγικός κυβερνοπόλεμος θα πρέπει να ισχύουν τρεις (3) βασικές προϋποθέσεις[B16]:

i. Μη ύπαρξη άλλου είδους εχθροπραξιών ανάμεσα στα εμπλεκόμενα μέρη ή αν υπάρχουν να θεωρούνται δευτερεύουσας σημασίας.
ii. Διενέργεια κυβερνοεπιθέσεων από όλες τις αντίπαλες πλευρές.
iii. Αποτυχία επίλυσης της αντιπαράθεσης μέσω οικονομικών, διπλωματικών ή νομικών οδών και προσφυγή σε εκδήλωση κυβερνοεπιθέσεων.

Ωστόσο, ο επηρεασμός της κρατικής συμπεριφοράς του αντιπάλου δεν αποτελεί μοναδικό αντικειμενικό σκοπό στον στρατηγικό κυβερνοπόλεμο. Επιπλέον, σκοπός του στρατηγικού κυβερνοπολέμου είναι η διαχείριση της σύγκρουσης, δηλαδή η κλιμάκωση και αποκλιμάκωσή της, η παύση της και ο περιορισμός του εύρους της. Παράλληλα, αξίζει να αναφερθεί πως ο στρατηγικός κυβερνοπόλεμος δεν αποτελεί πανάκεια για την επίτευξη όλων των στόχων των εμπλεκομένων, καθώς υπάρχουν σαφή και προκαθορισμένα όρια επιτυχίας.

Έτσι γίνεται αντιληπτό, ότι η επίτευξη των αντικειμενικών σκοπών σχετίζεται με το μέγεθος του αντίκτυπου, που δύναται να έχουν οι κυβερνοεπιθέσεις, προς το κράτος – στόχο. Σίγουρα, ο αντίκτυπος του στρατηγικού κυβερνοπολέμου διαφέρει κατά πολύ συγκριτικά με εκείνον του συμβατικού πολέμου. Κύρια αιτία αποτελεί το γεγονός ότι ο εξαναγκασμός προς ένα κράτος σχετίζεται –κατά αναλογία- με τον αριθμό των ανθρώπινων απωλειών, που επιφέρει μία σύγκρουση, δεδομένο, που δεν υποστηρίζεται από τον κυβερνοπόλεμο καθώς η εκδήλωση κυβερνοεπιθέσεων δεν στοχεύει στην απώλεια ανθρώπινης ζωής. Επιπλέον, τα αποτελέσματα του στρατηγικού κυβερνοπολέμου θεωρούνται προσωρινά, γεγονός, που δρα ενθαρρυντικά στην άποψη της κοινής γνώμης για μη συναίνεση σε εξαναγκασμό.

Αναλύοντας την αντίθετη άποψη, όμως, συμπερασματικά προκύπτει ότι με το στρατηγικό κυβερνοπόλεμο μπορεί να επιτευχθεί εξαναγκασμός του κράτους – στόχου, αρκεί να τηρούνται ορισμένες προϋποθέσεις. Η άποψη αυτή πηγάζει από την περίφημη «Τριάδα» του Clausewitz, η οποία ενσαρκώνεται από το λαό, τις ένοπλες δυνάμεις και την κυβέρνηση, καθώς και το βαθμό εξάρτησης κάθε επιμέρους στοιχείου της «Τριάδας» από τα συστήματα Η/Υ. Αναλογιζόμενος κάποιος την καθημερινότητά του αλλά και του εν γένει συνόλου, εύκολα διαπιστώνεται ότι η ανθρώπινη ζωή σχετίζεται άμεσα με τα συστήματα Η/Υ. Καθημερινές χρηματοοικονομικές συναλλαγές, τηλεπικοινωνίες, υγεία και μεταφορές είναι κάποιοι από τους τομείς της καθημερινής ανθρώπινης δραστηριότητας, που το πιστοποιούν. Επιπροσθέτως, οι Ένοπλες Δυνάμεις, σήμερα, βασίζονται στην τεχνολογία της πληροφορικής και τον κυβερνοχώρο καθώς οι Η/Υ χρησιμοποιούνται για πληθώρα ενεργειών όπως ο χειρισμός των συστημάτων διοίκησης και ελέγχου (command and control), η διακίνηση της στρατιωτικής αλληλογραφίας, η υλοποίηση των επικοινωνιών, οι απαιτήσεις επιτήρησης και αναγνώρισης του πεδίου της μάχης. Παράλληλα, η διαχείριση των αναγκών των πολιτών από την κυβέρνηση, ο έλεγχος εφαρμογής των αποφάσεών της από τους πολίτες και η επικοινωνία με το λαό στηρίζεται σε συστήματα Η/Υ.

Καταλήγοντας, η επίτευξη στρατηγικού αποτελέσματος θα επιτευχθεί μονάχα στην περίπτωση ταυτόχρονης και μεγάλης κλίμακας κυβερνοεπίθεσης και στις τρεις συνιστώσες της «Τριάδας» προκειμένου το κράτος – στόχος να οδηγηθεί σε στρατηγική παράλυση και αδυναμία αποτελεσματικής αντίδρασης, υποκύπτοντας στη θέληση του αντιπάλου.

Επιχειρησιακός Κυβερνοπόλεμος

Ο επιχειρησιακός κυβερνοπόλεμος αφορά τις κυβερνοεπιθέσεις, οι οποίες λαμβάνουν χώρα προς υποστήριξη ενός συμβατικού πολέμου, εκδηλωμένες κατά στρατιωτικών και μη στόχων. Η προσβολή μη στρατιωτικών στόχων αποκτά μεγαλύτερη σημασία, αν αναλογιστεί κάποιος τη δυνητική ζημιά, που προκαλείται στη διεξαγωγή στρατιωτικών επιχειρήσεων (π.χ. προσβολή εγκαταστάσεων και δικτύου τηλεπικοινωνιών).

Για να θεωρηθεί μια κυβερνοεπίθεση επιχειρησιακός κυβερνοπόλεμος θα πρέπει να αποσαφηνιστούν τα εξής[B16]:

- Οι επιχειρήσεις συλλογής πληροφοριών μέσω του κυβερνοχώρου (κυβερνοκατασκοπεία) δεν θεωρούνται επιχειρησιακός κυβερνοπόλεμος.
- Η φυσική επίθεση κατά των δικτύων Η/Υ, η οποία προκαλεί καταστροφή των δικτύων δε συνιστά επιχειρησιακό κυβερνοπόλεμο.
- Η διενέργεια ψυχολογικών επιχειρήσεων αποτελεί τμήμα των πληροφοριακών επιχειρήσεων και όχι του επιχειρησιακού κυβερνοπολέμου.

Όπως αναφέρθηκε και στον στρατηγικό κυβερνοπόλεμο τα αποτελέσματα είναι προσωρινά και η χρήση των κυβερνοόπλων αποσκοπεί στην επίτευξη περιορισμένων σκοπών. Πιο συγκεκριμένα, ο επιχειρησιακός κυβερνοπόλεμος επιφέρει τον αιφνιδιασμό του αντιπάλου. Ο αιφνιδιασμός στον κυβερνοχώρο επιτυγχάνεται τόσο πριν την έναρξη των συμβατικών επιχειρήσεων όσο και κατά τη διάρκεια αυτών. Σημαντικό στοιχείο για την διατήρηση του αιφνιδιασμού αποτελεί η πλήρης και ολοκληρωμένη διενέργεια κυβερνοκατασκοπείας, προκειμένου να ανακαλυφθεί το σύνολο των αδυναμιών του αντιπάλου στον κυβερνοχώρο. Ακόμα, βασική προϋπόθεση είναι και η ύπαρξη ποικιλίας κυβερνοόπλων καθώς η πλήξη για δεύτερη φορά με το ίδιο μέσο δε θα επιφέρει τον επιδιωκόμενο αιφνιδιασμό.

Επιπλέον, το κυριότερο επίτευγμα του επιχειρησιακού κυβερνοπολέμου αποτελεί η δυνατότητα παρεμπόδισης του αντιπάλου από τη χρήση του κυβερνοχώρου για εύλογο χρονικό διάστημα. Η άρνηση στον αντίπαλο στην χρήση των συστημάτων και δικτύων Η/Υ δύναται να προκαλέσει φόβο, ο οποίος μπορεί να οδηγήσει στην «απομόνωση», έχοντας αρνητικό επιχειρησιακό αντίκτυπο στη διεξαγωγή των επιχειρήσεων και τη διακίνηση ζωτικής σημασίας πληροφοριών.

Από την άλλη μεριά, μέσω του επιχειρησιακού κυβερνοπολέμου δεν υφίσταται η δυνατότητα νίκης σε μια πολεμική σύγκρουση ή κατάληψης εδάφους. Λόγω των προσωρινών αποτελεσμάτων μια συνεκτική και σκληραγωγημένη κοινωνία δεν εξαναγκάζεται σε οικειοθελή παράδοση. Παράλληλα, ο επιχειρησιακός κυβερνοπόλεμος δεν εξασφαλίζει

υπεροχή στον κυβερνοχώρο σε αντίθεση με την υπεροχή, που εξασφαλίζεται μέσω συμβατικών συγκρούσεων στη ξηρά, τη θάλασσα, τον αέρα, καθώς ο κυβερνοχώρος δεν αποτελεί ενιαία περιοχή, διαθέτοντας τουλάχιστον ένα τμήμα του σε κάθε αντίπαλη οντότητα.

4.3 Σκοπός – Στόχοι Κυβερνοπολέμου

Ο κυβερνοπόλεμος διεξάγεται για την επίτευξη κάποιου συγκεκριμένου πολιτικού σκοπού, ο οποίος προσδιορίζεται από την στρατηγική της εκάστοτε πολιτικής ηγεσίας. Απαραίτητη προϋπόθεση για την επιτυχή εκπλήρωση πολιτικών σκοπών είναι η συμβατότητα αυτών των σκοπών με τα ιδιαίτερα χαρακτηριστικά του κυβερνοπολέμου, δηλαδή ο κυβερνοπόλεμος δεν αποσκοπεί στην κατάληψη εχθρικού εδάφους ή καταστροφή των εχθρικών ενόπλων δυνάμεων.

Κάποιοι πολιτικοί σκοποί, που δύναται να επιτευχθούν με την εκδήλωση κυβερνοπολέμου είναι οι ακόλουθοι[Γ5]:

i. Η απλή παρενόχληση του αντιπάλου στα πλαίσια προβολής των δυνατοτήτων, τονίζοντας τη σχέση μεταξύ ισχυρού – αδύναμου.
ii. Η έμμεση προειδοποίηση του ενδιαφερόμενου μέρους πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών (π.χ Ελλάδα, Ευρωπαϊκή Ένωση, Τουρκία).
iii. Η εκδίκηση για αποφάσεις, που λήφθηκαν χωρίς να εξεταστούν τα συμφέροντα της ενδιαφερόμενης χώρας (π.χ Εσθονία 2007).

Παράλληλα, ο κυβερνοπόλεμος αποτελεί στρατηγικό μέσο, καθώς μέσω αυτού υφίστανται κυβερνοεπιθέσεις τόσο στρατιωτικές όσο και μη στρατιωτικές υποδομές. Έτσι, λοιπόν, καθορίζονται δύο (2) βασικές κατηγορίες στόχων, οι οποίοι αφορούν τις ένοπλες δυνάμεις και κυβερνητικές και μη υποδομές αντίστοιχα.

Στην περίπτωση των ενόπλων δυνάμεων επιδιώκεται η «αδρανοποίηση» των οπλικών συστημάτων και η διαταραχή του συστήματος διοίκησης και ελέγχου (command and control systems) του αντιπάλου, ενώ στη δεύτερη περίπτωση επιδιώκεται η εξασθένηση της ικανότητας και της θέλησης του αντιπάλου να διεξάγει πόλεμο για μεγάλο χρονικό διάστημα, προσβάλλοντας στόχους του οικονομικού και βιομηχανικού τομέα και υπηρεσίες, οι οποίες δύναται να επηρεάσουν το ηθικό των πολιτών (π.χ. παροχή ηλεκτρικού ρεύματος, νερού και υγειονομική περίθαλψη).

4.4 Κυβερνοπόλεμος και Τρομοκρατία

Οι τρομοκρατικές οργανώσεις χρησιμοποιούν σήμερα τον Κυβερνοχώρο για την επικοινωνία και την ανταλλαγή πληροφοριών, την επαφή με τους οπαδούς τους, τη συγκέντρωση χρημάτων, νόμιμη ή παράνομη, την οργάνωση και το συντονισμό των επιχειρήσεών τους, την απόκτηση παράνομων διαβατηρίων και VISA, τον προσηλυτισμό και τη συλλογή πληροφοριών[Γ5].

Οι επικοινωνίες και η ανταλλαγή πληροφοριών των τρομοκρατικών οργανώσεων εξυπηρετείται εξαιρετικά από το διαδίκτυο. Εξειδικευμένες ιστοσελίδες μπορούν να δημιουργηθούν και να αντικατασταθούν μόλις εντοπισθούν, διαβρωθούν ή μπλοκαριστούν από κυβερνήσεις. Τα μέλη των οργανώσεων ή οι οπαδοί τους μπορούν να χρησιμοποιούν αυτές τις ιστοσελίδες για σκοπούς ανταλλαγής μηνυμάτων ή ενημέρωσης σχετικά με τις εξελίξεις στα θέατρα των επιχειρήσεων του Αφγανιστάν, του Πακιστάν, του Ιράκ κλπ.

Το διαδίκτυο επίσης αποτελεί πηγή τεχνικών πληροφοριών κάθε είδους για όπλα και οπλικά συστήματα, τρόπους κατασκευής εκρηκτικών μηχανισμών, κάλυψη και οργάνωση ενεδρών και άλλες τεχνικές.

Το διαδίκτυο αποτελεί σήμερα ένα παγκόσμιο θέατρο επιχειρήσεων για τις τρομοκρατικές οργανώσεις και τις δυνάμεις ασφαλείας των χωρών. Όμως το ίδιο το διαδίκτυο δεν αποτελεί στόχο και δεν φαίνεται να υπάρχει προς το παρόν καμία «ηλεκτρονική» τρομοκρατική οργάνωση η οποία θα εξαπέλυε μια Κυβερνοεπίθεση στο διαδίκτυο με στόχο τη διακοπή της λειτουργίας του και την καταστροφή του. Τρεις είναι οι παράγοντες, οι οποίοι καθιστούν τις Κυβερνοεπιθέσεις στο ίδιο το διαδίκτυο λιγότερο ελκυστικές για τις τρομοκρατικές οργανώσεις[Γ5]:

- Τα Κυβερνοόπλα είναι λιγότερο αποτελεσματικά σε σχέση με άλλες δυνατότητες, από την άποψη ότι δεν έχουν τις ίδιες ψυχολογικές ή πολιτικές επιπτώσεις και δεν έχουν νεκρούς.
- Η πολυπλοκότητα των Κυβερνοεπιθέσεων στις κρίσιμες υποδομές έχει μικρότερες πιθανότητες επιτυχίας.
- Το διαδίκτυο εξυπηρετεί και τους δικούς τους σκοπούς.

Όσο όμως οι τεχνικές και οι τακτικές του Κυβερνοπολέμου εξελίσσονται, και η καταστροφή κρίσιμων υποδομών των χωρών γίνεται πιο εφικτή, δεν είναι μακριά ο χρόνος που οι τρομοκρατικές οργανώσεις θα στρατολογήσουν ειδικούς στον Κυβερνοπόλεμο και θα οργανώσουν κτυπήματα, τα οποία, μπορεί μεν να μην έχουν τα θύματα της επίθεσης στους δίδυμους πύργους, αλλά θα προκαλέσουν οικονομικές καταστροφές μεγάλης έκτασης.

4.5 Κυβερνοπόλεμος και Πληροφοριακός Πόλεμος

Ο Κυβερνοπόλεμος αποτελεί ο ίδιος μια κατηγορία πολέμου με τα δικά του χαρακτηριστικά. Παρόλα αυτά, από πολλές πλευρές, παρουσιάζει ομοιότητες με τον Πληροφοριακό πόλεμο[Γ5].

Τα συμβατικά μέσα μαζικής επικοινωνίας, ο έντυπος τύπος, το ραδιόφωνο και η τηλεόραση, είναι σήμερα όλα διαθέσιμα σε ψηφιακές πλατφόρμες και μέσω του διαδικτύου έχουν απήχηση σε ένα κοινό το οποίο ξεπερνάει τα εθνικά σύνορα· είναι πλέον προσβάσιμα σε οποιονδήποτε διαθέτει μια σύνδεση διαδικτύου. Κρατικοί οργανισμοί και υπηρεσίες, καθώς και Μη Κυβερνητικές Οργανώσεις χρησιμοποιούν επίσης το διαδίκτυο για σκοπούς επικοινωνιών και ανταλλαγής πληροφοριών, καθιστάμενοι έτσι τρωτοί σε Κυβερνοεπιθέσεις.

Κατά τη διάρκεια μιας σύγκρουσης, ο έλεγχος των πληροφοριών είναι ουσιαστικός, αφενός μεν για την ενίσχυση της εσωτερικής νομιμοποίησης στο εσωτερικό της χώρας, αφετέρου δε για τη διάβρωση του ηθικού του αντιπάλου. Το διαδίκτυο, ως πολλαπλασιαστής πληροφοριών (μέσω αναμετάδοσης ή διεύρυνσης του κοινού) παρέχει ευκαιρίες για παραπληροφόρηση και διασπορά ψιθύρων, και κατά συνέπεια αποτελεί στόχο επιλογής για όλες τις πλευρές μιας αντιπαράθεσης. Η προσβολή του στόχου αυτού διενεργείται μέσω Κυβερνοεπιθέσεων, σκοπός των οποίων δεν είναι η καταστροφή των δικτύων, αλλά η εισαγωγή ψευδών πληροφοριών και η προσβολή της αξιοπιστίας τους.

Συμπερασματικά, ο Πληροφοριακός πόλεμος χρησιμοποιεί τον Κυβερνοπόλεμο ως όργανό του, μέσω του οποίου προωθεί τις θέσεις του (έστω και με παραπληροφόρηση και διασπορά ψευδών ειδήσεων) στο διαδίκτυο, παρεμποδίζοντας ταυτόχρονα την πληροφόρηση του κοινού μέσω των ιστοσελίδων του αντιπάλου του.

4.6 Κυβερνοπόλεμος και Ένοπλες Δυνάμεις

Αποστολή των Ενόπλων Δυνάμεων ήταν πάντοτε, και παραμένει, η εμπλοκή με τις Ένοπλες Δυνάμεις του εχθρού και η καταστροφή τους ή η εξουδετέρωσή τους και ο εξαναγκασμός τους σε παράδοση. Στο πλαίσιο των πολεμικών επιχειρήσεων για την εκπλήρωση της αποστολής τους, οι Ένοπλες Δυνάμεις βρίσκονται στην ανάγκη προσβολής στόχων οι οποίοι δεν σχετίζονται αυστηρά με τις Ένοπλες Δυνάμεις του εχθρού, για παράδειγμα ένα εργοστάσιο παραγωγής ηλεκτρικού ρεύματος. Η απόφαση προσβολής ενός τέτοιου στόχου λαμβάνεται σε πολιτικό επίπεδο (σε αντιδιαστολή με ένα στόχο ραντάρ, του οποίου η προσβολή αποφασίζεται σε στρατιωτικό επίπεδο), και για τον πρόσθετο λόγο ότι διακυβεύεται η πρόκληση παράπλευρων απωλειών[Γ5].

Έχουμε δεχθεί ότι ο Κυβερνοπόλεμος αποτελεί τον τέταρτο συντελεστή ισχύος του κράτους (πλην της διπλωματίας, της οικονομίας και των Ενόπλων Δυνάμεων), σχεδιάζεται και υλοποιείται στο επίπεδο της Υψηλής Στρατηγικής, και ότι συμμετέχει ισότιμα με τους άλλους τρεις στη διεξαγωγή του πολέμου. Κατά συνέπεια, η σχέση του με τις Ένοπλες Δυνάμεις και τον κλασικό πόλεμο δεν μπορεί παρά να είναι ανάλογη της σχέσης της διπλωματίας και της οικονομίας με τις Ένοπλες Δυνάμεις· η σχέση αυτή στη στρατιωτική ορολογία ονομάζεται σχέση υποστηρίζοντος - υποστηριζόμενου. Ο Κυβερνοπόλεμος υποστηρίζει τους άλλους συντελεστές ισχύος όταν η έμφαση είναι στην οικονομική, τη διπλωματική ή τη στρατιωτική πλευρά της σύγκρουσης, και υποστηρίζεται από τους άλλους όταν η έμφαση βρίσκεται στον ίδιο τον Κυβερνοπόλεμο.

Η υποστήριξη, που δύναται να παράσχει ο κυβερνοπόλεμος στις ένοπλες δυνάμεις κατά τη διάρκεια πολεμικών επιχειρήσεων, είναι πολύπλευρη και σημαντική και συνοψίζεται όπως παρακάτω[Γ5]:

- ✓ Χρησιμοποίηση ως εργαλείο διεξαγωγής του Πληροφοριακού πολέμου, για την προώθηση των θέσεών του μέσω του διαδικτύου.
- ✓ Προσβολή στόχων του εχθρού, οι οποίοι δεν μπορούν να προσβληθούν με συμβατικά στρατιωτικά οπλικά συστήματα, είτε επειδή βρίσκονται εκτός της εμβέλειάς τους, είτε λόγω της φύσης τους (δίκτυα υπολογιστών).
- ✓ Απενεργοποίηση ορισμένων στόχων, αποφεύγοντας έτσι τη φυσική τους καταστροφή, είτε για λόγους μελλοντικής χρήσης, είτε για λόγους αποφυγής πρόκλησης δυσμενών εντυπώσεων στην εχθρική και παγκόσμια κοινή γνώμη (ψυχολογικός πόλεμος).
- ✓ Προσβολή ταυτόχρονα πληθώρα στόχων σε όλη την γεωγραφική έκταση του αντιπάλου.
- ✓ Χρησιμοποίηση για την εκδήλωση του πρώτου πλήγματος στον αντίπαλο, πριν την έναρξη των πολεμικών επιχειρήσεων.

Όμως η σχέση του Κυβερνοπολέμου με τον κλασικό πόλεμο είναι λίγο πιο σύνθετη από αυτή μεταξύ των άλλων δύο συντελεστών ισχύος με αυτόν. Η εξάρτηση των Ενόπλων Δυνάμεων από τα επικοινωνιακά και πληροφοριακά συστήματα τις καθιστά ευάλωτες σε Κυβερνοεπιθέσεις. Το νέο αυτό περιβάλλον δημιουργεί ευκαιρίες προσβολής της μαχητικής ικανότητας των Ενόπλων Δυνάμεων και της ίδιας της λειτουργίας του κράτους μέσω της προσβολής των επικοινωνιακών και πληροφοριακών του συστημάτων. Σε κάθε περίπτωση, οι Ένοπλες Δυνάμεις, είναι υποχρεωμένες να διατηρούν, εκτός από επιθετικές δυνατότητες Κυβερνοπολέμου, και δυνατότητες προστασίας των συστημάτων τους τα οποία είναι εκτεθειμένα σε Κυβερνοεπιθέσεις, όπως και όλοι οι δημόσιοι και ιδιωτικοί οργανισμοί και υπηρεσίες. Επιπλέον, η εξάρτηση της χώρας από επικοινωνιακά και πληροφοριακά

συστήματα και η συνακόλουθη τρωτότητά τους παρέχει νέους στόχους στο εσωτερικό της χώρας, τους οποίους οι Ένοπλες Δυνάμεις, σε περίοδο πολέμου, πρέπει να προστατεύσουν, δεδομένου ότι οι στόχοι αυτοί είναι οι υποδομές που απαιτούνται για την καλή τους λειτουργία.

Από τη άλλη πλευρά, η απειλή της προσφυγής στον Κυβερνοπόλεμο για να είναι αξιόπιστη πρέπει να συνοδεύεται από την απειλή της προσφυγής στο συμβατικό πόλεμο, ήτοι στην πρόκληση άμεσων, σοβαρών και χειροπιαστών συνεπειών. Όμως, η υποστήριξη την οποία παρέχει ο κλασικός πόλεμος στον Κυβερνοπόλεμο περιορίζεται στην απειλή χρήσης βίας. Διότι, από τη στιγμή της προσφυγής σε κλασικό πόλεμο, η μοναδική επιλογή που έχει ο αντίπαλος είναι να ανταποδώσει και αυτός με προσφυγή σε πόλεμο, οπότε η κλιμάκωση είναι αναπόφευκτη και οι ρόλοι υποστηρίζοντος – υποστηριζόμενου αντιστρέφονται.

Η υποστηρικτική δράση του Κυβερνοπολέμου παρατηρείται επίσης και στην περίοδο της ειρήνης, οπότε η δράση του Κυβερνοπολέμου περιορίζεται στη συλλογή πληροφοριών, όσες από τις οποίες παρουσιάζουν στρατιωτικό ενδιαφέρον διαβιβάζονται στις Ένοπλες Δυνάμεις για περεταίρω ανάλογη εκμετάλλευση.

Καταλήγοντας, προκύπτουν συμπεράσματα, τα οποία επικεντρώνονται στις εξής διαπιστώσεις[Γ5]:

- Η σχέση του Κυβερνοπολέμου με τις Ένοπλες Δυνάμεις είναι σχέση υποστηρίζοντος – υποστηριζόμενου.
- Οι Ένοπλες Δυνάμεις, όπως όλοι οι δημόσιοι οργανισμοί και υπηρεσίες, είναι υποχρεωμένες να διατηρούν αμυντικές και σε κάποιο βαθμό επιθετικές δυνατότητες Κυβερνοπολέμου, για την προστασία των συστημάτων τους τα οποία είναι εκτεθειμένα σε Κυβερνοεπιθέσεις.
- Η απειλή προσφυγής στον Κυβερνοπόλεμο για να είναι αξιόπιστη πρέπει να συνοδεύεται από αντίστοιχη απειλή προσφυγής στο συμβατικό πόλεμο.
- Η υποστηρικτική δράση του Κυβερνοπολέμου στην περίοδο της ειρήνης αφορά στη συλλογή πληροφοριών ενδιαφέροντος των Ενόπλων Δυνάμεων.

4.6.1 Κυβερνοπόλεμος ως πρώτο πλήγμα

Η προετοιμασία του πρώτου πλήγματος στον πόλεμο πρέπει να γίνεται με προσοχή, έτσι ώστε αν δεν προκαλέσει τον αιφνιδιασμό του αντιπάλου, να επιβάλει την είσοδο του στον πόλεμο από μειονεκτική θέση, με τις χειρότερες δυνατές συνθήκες[Γ5].

Ιδιαίτερο ενδιαφέρον παρουσιάζει η δυνατότητα χρήσης του κυβερνοπολέμου, λόγω των ιδιαίτερων χαρακτηριστικών του, ως «εναρκτήριο λάκτισμα» των επιχειρήσεων. Η πρώτη επίθεση στον πόλεμο του 21ου αιώνα θα μπορούσε κάλλιστα να αποτελείται από μια σειρά συντονισμένων κυβερνοεπιθέσεων, σχεδιασμένων έτσι ώστε να διαμορφώσουν το πεδίο των επιχειρήσεων. Οι επιθέσεις αυτές θα μπορούσαν να συνδυαστούν με στρατιωτικά μέσα για να προκαλέσουν παραλυτικές επιπτώσεις στις κρίσιμες υποδομές της χώρας – στόχου, πριν την έναρξη των επιχειρήσεων. Ένα από τα πλεονεκτήματα της εκδήλωσης μιας τέτοιας μορφής κυβερνοεπίθεσης πριν την έναρξη των επιχειρήσεων είναι η δυνατότητα αιφνιδιασμού του αντιπάλου, ο οποίος επιτυγχάνεται χάρις στην εκδήλωση των κυβερνοεπιθέσεων χωρίς προηγούμενη στρατιωτική κινητοποίηση.

Οι κυβερνοεπιθέσεις σε στόχους στρατιωτικού ενδιαφέροντος έχουν ως σκοπό την υποβάθμιση της δυνατότητας των Ενόπλων Δυνάμεων του αντιπάλου να εκπληρώσουν την αποστολή τους, ήτοι να διεξάγουν τον πόλεμο. Στο πλαίσιο αυτό, ενδεχόμενους στόχους του πρώτου πλήγματος μέσω του κυβερνοχώρου θα μπορούσαν να αποτελούν επιλεγμένοι στόχοι που αφορούν στην προετοιμασία και τις μετακινήσεις των Ενόπλων Δυνάμεων του αντιπάλου, τα δίκτυα επικοινωνιών του προς απαγόρευση διαβίβασης εντολών και το σύστημα έγκαιρης προειδοποίησης. Μια άλλη τακτική η οποία χρησιμοποιείται σε αυτές τις περιπτώσεις, δεδομένου και του σχεδόν μηδενικού κόστους τέτοιων επιθέσεων, είναι η ταυτόχρονη προσβολή όλων των στόχων σε ολόκληρο το βάθος του αντιπάλου, και η οποία από ορισμένους Αμερικανούς αρθρογράφους χαρακτηρίζεται ως «carpet bombing» .

Στην περίπτωση χρήσης της κυβερνοεπίθεσης ως πρώτου πλήγματος, ο χρόνος εκδήλωσής της έχει ιδιαίτερη σημασία καθώς η επίθεση θα πρέπει να διεξάγεται όσο το δυνατόν αργότερα, έτσι ώστε αφενός μεν να μη δοθεί η δυνατότητα στο στόχο να εντοπίσει την τρωτότητα των συστημάτων του και να τα επισκευάσει πριν ο επιτιθέμενος εκμεταλλευτεί τις αρχικές επιπτώσεις της, ενώ αφετέρου δε να μη χαθεί το πλεονέκτημα του αιφνιδιασμού, με την εκδήλωση της κυβερνοεπίθεσης πολύ πριν την εκδήλωση της κανονικής επίθεσης με πυρά. Σημαντικός είναι επίσης ο συντονισμός της κυβερνοεπίθεσης με τις επιχειρήσεις, επειδή το πιθανότερο είναι ότι η κυβερνοεπίθεση δεν θα προκαλέσει φυσική καταστροφή και κατά συνέπεια μη αναστρέψιμες επιπτώσεις στην ικανότητα διεξαγωγής μάχης του αντιπάλου.

Συμπερασματικά, φαίνεται όλο και πιο πιθανό ότι η πρώτη επίθεση οποιασδήποτε μελλοντικής αναμέτρησης μεταξύ τεχνολογικά προηγμένων αντιπάλων θα είναι ηλεκτρονική και θα διεξαχθεί στον ή μέσω του Κυβερνοχώρου[Γ5].

4.6.2 Υποστήριξη των εν Εξελίξει Επιχειρήσεων

Από την έναρξη της θερμής σύγκρουσης, οι στρατιωτικές επιχειρήσεις διεξάγονται σύμφωνα με το εκπονηθέν προς το σκοπό αυτό σχέδιο επιχειρήσεων, το οποίο ουσιαστικά αποτελεί τον τρόπο χρήσης των διαθεσίμων στρατιωτικών μέσων για την επίτευξη του επιδιωκόμενου αντικειμενικού σκοπού. Κάθε άλλο (μη στρατιωτικό) μέσο, όπως ενδεχομένως μέσα κυβερνοπολέμου τα οποία δεν είναι οργανικά των Ενόπλων Δυνάμεων, για λόγους ενότητας της πολεμικής προσπάθειας, τίθεται υπό διοικητική ή επιχειρησιακή διοίκηση, ή επιχειρησιακό ή τακτικό έλεγχο των Ενόπλων Δυνάμεων. Η δράση των μέσων αυτών συντονίζεται με τις επιχειρήσεις μέσω της έκδοσης συγκεκριμένων αποστολών για την επίτευξη συγκεκριμένων αντικειμενικών σκοπών, οι οποίοι είναι κατάλληλοι με τη φύση τους. Στο πλαίσιο αυτό, οι αντικειμενικοί σκοποί του κυβερνοπολέμου, όταν αυτός χρησιμοποιείται για την υποστήριξη των επιχειρήσεων, περιλαμβάνουν, τους παρακάτω[Γ5]:

- Διακοπή εχθρικών επικοινωνιών και γραμμών διοικητικής μέριμνας.
- Προσβολή του εχθρικού συστήματος διοίκησης και ελέγχου.
- Παρενόχληση των στρατιωτικών μετακινήσεων.
- Προσβολή στόχων στρατιωτικού ενδιαφέροντος σε βάθος.
- Επηρεασμός της παγκόσμιας κοινής γνώμης σχετικά με τη διένεξη μέσω του διαδικτύου (παροχή υποστήριξης στον Πληροφοριακό πόλεμο).

Συμπερασματικά, η υποστήριξη των επιχειρήσεων του κλασικού πολέμου από τον κυβερνοπόλεμο, γίνεται μέσω της ανάθεσης κατάλληλων αποστολών στα μέσα του κυβερνοπολέμου, σε πλήρη συντονισμό με το γενικό σχέδιο επιχειρήσεων.

4.7 Μέτρα Συντονισμού μεταξύ Εθνικών και Διεθνών Υπηρεσιών

Κάθε χώρα είναι υπεύθυνη για την ασφάλεια των πληροφοριακών, αλλά και κάθε άλλου είδους υποδομών, εντός της επικρατείας της. Όμως μια Κυβερνοεπίθεση, του τύπου της εκτόξευσης ιού ή άλλης μορφής κακόβουλου λογισμικού, μπορεί εύκολα να διαδοθεί και πέρα από τα εθνικά σύνορα μιας χώρας. Όλες οι χώρες έχουν εμπειρία Κυβερνοεπιθέσεων, των οποίων ο βέλτιστος τρόπος αντιμετώπισης είναι η συνεργασία με άλλες χώρες[Γ5]. Χωρίς αυτή δεν είναι δυνατόν μια χώρα να αντιμετωπίσει το πολύπλευρο αυτό πρόβλημα, εκτός και αν είναι προετοιμασμένη να δεχθεί σημαντικά υψηλότερο κόστος για τα πολιτικά και στρατιωτικά υλικά που παράγει ή χρειάζεται.

Σε εθνικό επίπεδο, ο κυβερνοπόλεμος και γενικότερα η παράνομη δραστηριότητα στον κυβερνοχώρο, είναι μια υπόθεση που μας αφορά όλους. Η αντιμετώπιση αυτής της

απειλής δεν μπορεί να είναι υπόθεση των Ενόπλων Δυνάμεων ή της ΕΥΠ μόνο. Απαιτείται η ενεργητική εμπλοκή και η συνεργασία των δημοσίων οργανισμών και υπηρεσιών, των τοπικών αρχών ασφαλείας, των Παρόχων Υπηρεσιών Διαδικτύου (Internet Service Providers – ISP), των διαχειριστών των δικτύων της χώρας, των Ομάδων Αντίδρασης σε κυβερνοεπιθέσεις (CERT), της βιομηχανίας, των ιδιωτικών εταιρειών, των πάσης φύσεως ιδρυμάτων (Εκπαιδευτικών και μη) της χώρας. Η συνεργασία όλων αυτών των οργανισμών, ιδρυμάτων και υπηρεσιών διασφαλίζει την αντίδραση της πληροφοριακής υποδομής σε κυβερνοεπιθέσεις με ολοκληρωμένο και συντονισμένο τρόπο.

Όμως, η συνεργασία αυτή δεν συμβάλει μόνο στη διασφάλιση της άμυνας της χώρας. Ιδιαίτερη είναι η βοήθεια που μπορούν να παρέχουν στην περίπτωση της εκδήλωσης κυβερνοεπιθέσεων εναντίον των πιθανών αντιπάλων. Όλοι αυτοί οι οργανισμοί, τα ιδρύματα και οι υπηρεσίες διαθέτουν ειδικούς με γνώσεις επί της οργάνωσης και λειτουργίας των συστημάτων – στόχων (πληροφοριακών και υποδομών) των ενδεχομένων αντιπάλων. Οι γνώσεις αυτές των συστημάτων είναι απαραίτητες για τη σχεδίαση και υλοποίηση αποτελεσματικών τρόπων προσβολής μέσω κυβερνοεπιθέσεων.

Στο πλαίσιο αυτό, ιδιαίτερα χρήσιμη είναι η εξειδικευμένη γνώση και εμπειρία των hacker, η εκμετάλλευση των οποίων μπορεί να γίνει μέσω κατάλληλης οργάνωσης και ανάπτυξης ειδικών δραστηριοτήτων (οργάνωση σε συλλόγους, διαγωνισμοί hacking, βραβεία, κλπ). Όλη αυτή η προσπάθεια απαιτεί οργάνωση και συντονισμό μέσω ενός κεντρικού συντονιστικού οργάνου (Κέντρου ή υπηρεσίας), κάτω από κρατική εποπτεία και βοήθεια.

Συμπερασματικά, επειδή η κυβερνοαπειλή δεν στρέφεται αποκλειστικά εναντίον του δημόσιου τομέα, η στενή συνεργασία μεταξύ κυβερνητικών υπηρεσιών, του ιδιωτικού τομέα και των ιδιωτών αποτελεί κομβικό σημείο στην προσπάθεια της χώρας αφενός μεν να αντιπαρατάξει αποτελεσματική άμυνα εναντίον του ενδεχομένου κυβερνοεπιθέσεων, αφετέρου δε να αναλάβει πρωτοβουλίες εκδήλωσης κυβερνοεπιθέσεων εναντίον των πιθανών αντιπάλων.

Στο διεθνές επίπεδο, η προσπάθεια διεθνούς συνεργασίας πρέπει να ξεκινήσει από την αναθεώρηση και τη συμπλήρωση του διεθνούς νομικού πλαισίου, κατά το πρότυπο του δικαίου του πολέμου, έτσι ώστε να ελεγχθεί η μέχρι σήμερα άναρχη και χαοτική δραστηριότητα στον κυβερνοχώρο. Είναι επίσης απαραίτητη η συνεργασία μεταξύ των εθνικών φορέων, και η ίδρυση ενός Διεθνούς Παρατηρητηρίου κυβερνοεπιθέσεων για την έγκαιρη προειδοποίηση των εθνικών αρχών.

Διεθνώς καταβάλλονται ήδη προσπάθειες για το συντονισμό των δράσεων των επιμέρους χωρών, για την αντιμετώπιση του γενικότερου προβλήματος της δραστηριότητας στον κυβερνοχώρο. Από τις προσπάθειες αυτές ξεχωρίζουν αυτές του Συμβουλίου της Ευρώπης, της Ευρωπαϊκής Ένωσης και του NATO, τα οποία έχουν υιοθετήσει νομικά και επιχειρησιακά εργαλεία (μέσα) για την προστασία του (ευρωπαϊκού και NATOϊκού) κυβερνοχώρου.

Συμβούλιο της Ευρώπης

Το Νοέμβριο του 2001 το Συμβούλιο της Ευρώπης υιοθέτησε τη Σύμβαση για το κυβερνοέγκλημα η οποία ενεργοποιήθηκε την 24 Ιουλίου 2004. Η σύμβαση έχει υπογραφεί από 23 χώρες, με τις 22 από αυτές να μην την έχουν ακόμη επικυρώσει.

Ευρωπαϊκή Ένωση

Το 2004 η Ευρωπαϊκή Ένωση ίδρυσε το Ευρωπαϊκό Δίκτυο στην Υπηρεσία Πληροφοριακής Ασφάλειας (European Network in Information Security Agency – ENISA) στην Κρήτη. Αυτή η υπηρεσία αποτελεί ένα κέντρο εξειδικευμένης γνώσης, όπως και το κέντρο CDD-CoE του NATO, στο Ταλίν της Εσθονίας. Η αποστολή της ENISA περιλαμβάνει την παροχή συμβουλών και συστάσεων, ανάλυσης δεδομένων, και τη διευκόλυνση της ενημέρωσης και της συνεργασίας μεταξύ των υπηρεσιών της Ευρωπαϊκής Ένωσης και των χωρών-μελών της. Μεταξύ άλλων, η ENISA παρέχει βοήθεια στην Ευρωπαϊκή Επιτροπή και στις χώρες-μέλη όσον αφορά στο διάλογό τους με τη βιομηχανία για την επίλυση προβλημάτων που σχετίζονται με την ασφάλεια σε προϊόντα λογισμικού και υλικού.

Η ENISA βρίσκεται σε επαφή επίσης με τις κυβερνήσεις της Ευρωπαϊκής Ένωσης μέσω συνδέσμων και των αντίστοιχων εθνικών CERT. Εκδίδει μια ετήσια αναφορά των εργασιών της και παράγει θεματικές μελέτες και αναφορές πληροφοριών μετά από αίτηση των χωρών-μελών[Γ5].

NATO

Μέχρι την κυβερνοεπίθεση που δέχθηκε η Εσθονία το 2007 το NATO θεωρούσε τον κυβερνοπόλεμο μια πιθανή αλλά μακρινή απειλή. Το γεγονός ότι τα κράτη χρησιμοποιούσαν την πληροφοριακή τεχνολογία για να εισβάλουν σε δίκτυα άλλων χωρών με σκοπό τον εντοπισμό τρωτών σημείων και τη συλλογή πολιτικών, στρατιωτικών, οικονομικών, βιομηχανικών και τεχνολογικών πληροφοριών ήταν ανεκτό ως φυσιολογική δραστηριότητα[Γ5].

Η κυβερνοεπίθεση εναντίον της Εσθονίας έδωσε νέες διαστάσεις στο φαινόμενο. Ήταν μια προσπάθεια αποσταθεροποίησης της χώρας με οικονομικές επιπτώσεις. Μετά τη σύνοδο της Πράγας, το NATO ξεκίνησε την πρωτοβουλία Πρόγραμμα Κυβερνοάμυνας (Technical NATO Cyber Defense), η οποία οδήγησε στην ίδρυση του NATO Computer Response Team (NCIRT), κάτι αντίστοιχο με τα CERT.

Στις αρχές του 2008, μετά από πρόταση των εσθονικών αρχών, το NATO συμφώνησε στην ίδρυση του CCD-CoE (Cooperative Cyber Defense Center of Excellence) στο Ταλίν. Την 14 Μαΐου 2008 οι αντιπρόσωποι επτά χωρών – μελών του NATO (Εσθονία, Λετονία, Λιθουανία, Γερμανία, Ιταλία, Σλοβακία, Ιταλία) υπέγραψαν συμφωνία για την ίδρυση του κέντρου με το Διοικητή του Allied Command Transformation (ACT), τον έναν από τους δύο Στρατηγικούς Διοικητές του NATO. Το κέντρο διαθέτει σήμερα ένα επιτελείο 30 περίπου ατόμων, τα μισά εκ των οποίων θεωρούνται ειδικοί στον κυβερνοπόλεμο. Το κέντρο πρακτικά αποτελεί ένα κέντρο ανταλλαγής πληροφοριών μεταξύ των ειδικών και ενημέρωσης και εκπαίδευσης αξιωματικών του NATO επί θεμάτων κυβερνοπολέμου.

Με τις προαναφερθείσες πρωτοβουλίες, η κυβερνοάμυνα, και ο κυβερνοπόλεμος γενικότερα, εντάσσονται σήμερα στις άμεσες προτεραιότητες του NATO .

ΚΕΦΑΛΑΙΟ 5 ΑΠΟΤΡΟΠΗ

5.1 Ορισμός

Η αποτροπή ως έννοια της στρατηγικής αποσκοπεί στη διατήρηση του status quo με τη χρήση βίας, δηλαδή αντικειμενικός σκοπός της αποτροπής είναι η σταθερότητα[A2]. Βασικό της στοιχείο είναι η έννοια του σχετικού κόστους και πιο συγκεκριμένα, 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. Παράλληλα, σύμφωνα με άλλον ορισμό η αποτροπή ορίζεται ως η ικανότητα να πειστεί ο αντίπαλος να μην επιτεθεί γιατί στη συνέχεια θα υπάρξουν αντίποινα, προσδίδοντας στην απειλή του αμυνόμενου έναν πιο επιθετικό χαρακτήρα.

Κατόπιν των παραπάνω προκύπτει ότι, η αποτροπή λειτουργεί στη βάση του κόστους, που θα επιφέρει μία δράση για τον αντίπαλο και στηρίζεται στους ορθολογικούς υπολογισμούς του (σχέση κόστους – οφέλους) για αυτή 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, και σε ανάληψη επιθετικών ενεργειών από τον αμυνόμενο προκειμένου να ζημιωθεί ο αντίπαλος, που επιχειρεί την αλλαγή στο status quo.

5.2 Προϋποθέσεις Αποτροπής

Οι προϋποθέσεις, που πρέπει να υπάρχουν, ώστε μια χώρα Α να αποτρέψει μια χώρα Β από μια συγκεκριμένη πορεία δράσης, επικεντρώνονται στα κάτωθι[B14]:

- Μια χώρα Α απευθύνει στη χώρα Β μια απειλή τιμωρίας ή πλήγματος της, σε περίπτωση που η χώρα Β αποτολμήσει μια συγκεκριμένη δράση. Σε αυτήν την περίπτωση είναι απαραίτητο η χώρα Α να έχει διατυπώσει ρητά την απειλή της προς τη χώρα Β.
- Σε περίπτωση απουσίας της παραπάνω απειλής από την χώρα Α προς τη χώρα Β, τότε η τελευταία θα μπορούσε να επιχειρήσει την συγκεκριμένη πορεία δράσης. Δηλαδή, η χώρα Β θα είχε τα μέσα και την θέληση να προχωρήσει σε μια επιθετική προς τη χώρα Α ενέργεια, σε περίπτωση έλλειψης ξεκάθαρης απειλής από την χώρα Α.
- Η χώρα Β πιστεύει ότι η χώρα Α έχει την ικανότητα και τη βούληση να πραγματοποιήσει την απειλή της. Βασιζόμενη σε αυτό, αποφασίζει ότι η συγκεκριμένη

πορεία δράσης δεν προσφέρει κάποιο όφελος. Είναι σημαντικό να αναφερθεί ότι η απειλή, που διατυπώνει η χώρα Α πρέπει να είναι πιστευτή από τη χώρα Β, προκειμένου η τελευταία να θεωρήσει ότι η υπό υλοποίηση πορεία δράσης της είναι ανάξια σημασίας ή μη ωφέλιμη.

Κατόπιν των προαναφερθέντων προϋποθέσεων, προκύπτει ότι η έννοια της αποτροπής στηρίζεται σε δύο κύριους άξονες. Ο μεν πρώτος είναι η αξιοπιστία της απειλής, δηλαδή ο αμυνόμενος ή αλλιώς η πλευρά, που εκφράζει την απειλή θα πρέπει να έχει τα κατάλληλα μέσα και τη θέληση να τα χρησιμοποιήσει ενώ η αντίπαλη πλευρά θα είναι σε θέση να γνωρίζει για την ύπαρξη αυτών των μέσων και τη θέληση χρησιμοποίησής τους. Ως αποτέλεσμα, προκύπτει η ανάγκη ύπαρξης διαύλου επικοινωνίας μεταξύ των αντίπαλων πλευρών. Ο δε δεύτερος άξονας εστιάζεται στη δυνατότητα ορθολογιστικών υπολογισμών από τις δύο πλευρές. Η αποτρεπτική απειλή θα πρέπει να είναι σαφής σχετικά με τα όρια δράσης του αντιπάλου και να στοχεύει σε αξίες, που αντίπαλος θεωρεί ιδιαίτερης σημασίας για τον ίδιο. Έτσι, η απειλή θα επιδράσει στο πνεύμα και την ψυχολογία του αντιπάλου, με αποτέλεσμα οι ορθολογικοί υπολογισμοί του να έχουν θετική έκβαση για την αντίπαλη πλευρά. Σε περίπτωση μη ορθολογικής λειτουργίας, τότε η αποτροπή δε δύναται να εφαρμοστεί και η σύγκρουση θεωρείται μονόδρομος.

5.3 Είδη Αποτροπής

Σύμφωνα με διάφορες αναφορές, υπάρχουν δύο βασικά είδη αποτροπής και πιο συγκεκριμένα τα παρακάτω[Α4]:

- ✓ Γενική Αποτροπή (General Deterrence)

Στην περίπτωση αυτή, ο αμυνόμενος διαθέτει ευρεία στρατιωτική δυνατότητα και είναι σε θέση να εξαπολύσει γενικές απειλές, που προοικονομούν την τιμωρία οποιουδήποτε σκέφτεται πιθανή επίθεση.

- ✓ Άμεση Αποτροπή (Immediate Deterrence)

Στην περίπτωση αυτή, ο αμυνόμενος εξαπολύει απειλή χρήσης βίας κατά ενός συγκεκριμένου αντιπάλου, ο οποίος σκέφτεται να επιτεθεί άμεσα.

Μία ακόμα ταξινόμηση της έννοιας της αποτροπής λαμβάνει τις ακόλουθες μορφές[Α4]:

- ✓ Αποτροπή μέσω Παρουσίας (Deterrence by Presence)

Στην περίπτωση αυτή, επιτυγχάνεται μέσω διατήρησης συμβολικών δυνάμεων στο προς υπεράσπιση σημείο, προκειμένου να καταδειχτεί στον αντίπαλο, ο τρόπος

αντίδρασης (από τον αμυνόμενο), σε περίπτωση επιθετικής ενέργειας, η οποία θα οδηγήσει σε γενικότερη σύγκρουση.

- ✓ Αποτροπή μέσω Άμυνας (Deterrence by Defense)

Η συγκεκριμένη μορφή προκύπτει από τη διατήρηση ισχυρών αμυντικών δυνατοτήτων. Η ισχυρή άμυνα λειτουργεί αποτρεπτικά για τον εν δυνάμει επιτιθέμενο.

- ✓ Αποτροπή μέσω Άρνησης (Deterrence by Denial)

Αυτή η μορφή αποσκοπεί στην άρνηση αποκόμισης κερδών στον επιτιθέμενο, όπου η ζημιά για τον αμυνόμενο μπορεί να είναι μεγάλη, ταυτόχρονα, όμως, ο επιτιθέμενος δε θα πάρει αυτά, που επιδιώκει.

- ✓ Αποτροπή μέσω Αντιποίνων (Deterrence by Punishment)

Η συγκεκριμένη μορφή στηρίζεται στην απειλή αντιποίνων, η οποία μπορεί να αναφέρεται και σε διαφορετικό χώρο, χρόνο και τόπο, που επέλεξε ο αντίπαλος για να εκδηλώσει την επιθετική του ενέργεια.

Η έννοια της αποτροπής διακρίνεται επίσης και στα εξής[A4]:

- ✓ Εθνική Αποτροπή

Η αποτροπή τέτοιου είδους επιτυγχάνεται με τη χρήση εθνικών μέσων.

- ✓ Διεθνής Αποτροπή

Η αποτροπή επιτυγχάνεται μέσω τρίτων παραγόντων (π.χ. μέσω NATO).

- ✓ Προεκτεινόμενη Αποτροπή (Extended Deterrence)

Ονομάζεται η αποτροπή εχθρικών προσβολών σε τρίτες χώρες.

- ✓ Ενδοπολεμική Αποτροπή (Intra-war Deterrence)

Το συγκεκριμένο είδος αποτροπής λαμβάνει χώρα κατά τη διάρκεια ενός πολέμου και αποσκοπεί στην αποσόβηση της κλιμάκωσης.

- ✓ Μίνιμουμ Αποτροπή (minimum Deterrence)

Αναφέρεται στην αποτροπή του αντιπάλου μέσω ύπαρξης μικρού πυρηνικού οπλοστασίου, το οποίο είναι στραμμένο αποκλειστικά εναντίον των εχθρικών πόλεων.

✓ Ενεργητική Αποτροπή

Αποσκοπεί στο να πείσει, μέσω απειλής ή επιβολής τιμωρίας, τον αντίπαλο από το να σταματήσει τις ενέργειες, που έχει ήδη ξεκινήσει.

5.4 Κυβερνοαποτροπή και τα Προβλήματα Εφαρμογής της

Η αποτροπή στον κυβερνοχώρο δύναται να λάβει τις παρακάτω μορφές[B22]:

- Κυβερνοαποτροπή μέσω άρνησης (Cyber Deterrence by Denial)

Η συγκεκριμένη μορφή εστιάζει στην άμυνα στον κυβερνοχώρο, μέσω της ανάπτυξης αμυντικών δυνατοτήτων σε αυτόν, αποσκοπώντας στη φθορά των κυβερνοεπιθέσεων του αντιπάλου και συμβάλλοντας στην αύξηση του κόστους σε αυτόν.

- Κυβερνοαποτροπή μέσω αντιποίνων (Cyber Deterrence by Punishment)

Αυτή η μορφή είναι πιο επιθετική και εστιάζει στην εφαρμογή αντιποίνων στον κυβερνοχώρο, προκειμένου ο αντίπαλος να αποτραπεί από την έναρξη ή την περαιτέρω διεξαγωγή κυβερνοεπιθέσεων. Όπως είναι λογικό, προϋποθέτει την ύπαρξη και χρήση ανεπτυγμένων επιθετικών δυνατοτήτων στον κυβερνοχώρο.

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, το ενδιαφέρον εστιάζεται στις δυνατότητες, που δύναται να προσδώσει στον αμυνόμενο η αποτροπή μέσω αντιποίνων, καθώς η ανάπτυξη αμυντικών δυνατοτήτων στον κυβερνοχώρο κοστίζει περισσότερο, ενώ η επίθεση έχει το πλεονέκτημα σε σχέση με την άμυνα. Ενδεικτικά, το 2009, οι Η.Π.Α. χρειάστηκε να ξοδέψουν περίπου 7,3 δις$ για την άμυνα των ομοσπονδιακών συστημάτων πληροφορικής. Παρ' όλα αυτά, με την κυβερνοαποτροπή μέσω άρνησης 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, καθιστώντας με αυτόν τον τρόπο όλο και πιο αξιόπιστη τη στρατηγική της κυβερνοαποτροπής.

Είναι σημαντικό όμως να αναφερθούν τα προβλήματα, τα οποία παρουσιάζονται κατά την εφαρμογή της αποτροπής στον κυβερνοχώρο. Το πρώτο από αυτά προσδιορίζεται στην έλλειψη αξιοπιστίας σχετικά με τα κυβερνοόπλα. Χαρακτηριστικό παράδειγμα αποτελεί η περίοδος του Ψυχρού Πολέμου, όπου οι δύο υπερδυνάμεις διέθεταν πυρηνικά όπλα, τα

οποία είχαν δοκιμαστεί σε διάφορες πυρηνικές δοκιμές, γνωρίζοντας την δυνατότητα καταστροφής, που δύναται να επιφέρουν. Παράλληλα, υπήρχε η πεποίθηση ότι τα πυρηνικά όπως και τα συμβατικά όπλα, παρά τις αντιξοότητες, που θα αντιμετώπιζαν σε μια σύγκρουση, θα έφταναν στον τελικό τους στόχο. Αντίθετα, η αποτελεσματικότητα των κυβερνοόπλων δεν μπορεί να θεωρείται ως δεδομένη, λόγω της μεταβλητότητας, που παρουσιάζει ο κυβερνοχώρος. Επιπλέον, η ύπαρξή τους και η ισχύς τους πηγάζει από ενδείξεις και δηλώσεις κρατών, χωρίς αυτό να αποδεικνύεται πρακτικά. Παράλληλα, η ανάπτυξη των επιθετικών και αμυντικών δυνατοτήτων στον κυβερνοχώρο από τα κράτη καλύπτεται από ένα πέπλο μυστικότητας, καθώς η θεωρητικώς υπεροχή ενός κράτους σε κυβερνοόπλα δεν αποδεικνύεται εμπράκτως. Επίσης, οι αμυντικές δυνατότητες μιας χώρας στον κυβερνοχώρο εξαρτώνται άμεσα από τις γνώσεις και την εξειδίκευση του αρμόδιου ανθρώπινου δυναμικού στην τεχνολογία της πληροφορικής καθώς και από τον τρόπο αντίδρασης σε μια ενδεχόμενη κυβερνοεπίθεση, στοιχεία που σαφώς δεν είναι μετρήσιμα και σταθερά. Συμπερασματικά, καταλήγουμε στο γεγονός, ότι στον κυβερνοχώρο παρατηρείται έντονα το στοιχείο της αβεβαιότητας και της μεταβλητότητας.

Ακόμα ένα πρόβλημα, που παρουσιάζεται στο ζήτημα της κυβερνοαποτροπής είναι η απουσία διεθνούς νομικής ορολογίας για τον κυβερνοχώρο. Λόγω αυτής της έλλειψης είναι δυνατόν να προκύψουν διαφορετικές στάσεις και αντιδράσεις από τους άμεσα εμπλεκόμενους στις κυβερνοσυγκρούσεις, ερμηνεύοντας μια συγκεκριμένη κυβερνοεπίθεση κάποιοι ως πράξη πολέμου, ενώ κάποιοι άλλοι να τη θεωρούν ως βανδαλισμό στον κυβερνοχώρο. Για το λόγο αυτό, η προσφορότερη λύση είναι η ύπαρξη μιας κοινά αποδεκτής νομικής ορολογίας για τον κυβερνοχώρο στο επίπεδο του ΟΗΕ. Καθίσταται σαφές ότι, στον κυβερνοχώρο υπάρχει έντονο το φαινόμενο της λανθασμένης ερμηνείας συγκεκριμένων δράσεων από τους αντιπάλους, η οποία μπορεί να οδηγήσει σε συγκρούσεις, καθιστώντας την αποτροπή ανενεργή.

Η ανωνυμία των δρώντων στον κυβερνοχώρο αποτελεί επίσης σημαντικό πρόβλημα, καθώς δεν δύναται να εφαρμοστεί μια στρατηγική αποτροπής εφόσον δεν είναι γνωστή η ταυτότητα του αντιπάλου. Ιδιαίτερα, η κυβερνοαποτροπή μέσω αντιποίνων καθίσταται ανενεργή καθώς δεν υπάρχει σημείο κατεύθυνσης των αντιποίνων. Στον κυβερνοχώρο δεν είναι εφικτός ο εντοπισμός της ταυτότητας του αντιπάλου αλλά και της φυσικής του θέσης όπως στις συμβατικές συγκρούσεις. Οι hackers, εκμεταλλευόμενοι τη δαιδαλώδη αρχιτεκτονική των δικτύων Η/Υ και του διαδικτύου είναι σε θέση να εξαπολύουν επιθέσεις ταυτόχρονα από οποιοδήποτε σημείο θελήσουν, αποκρύπτοντας τα ίχνη τους. Κατά αυτόν τον τρόπο προκύπτει ότι η απόδοση ευθυνών για τη διεξαγωγή κυβερνοεπιθέσεων είναι ιδιαίτερα δύσκολη υπόθεση, καθώς πέρα από τη χαοτική αρχιτεκτονική των δικτύων Η/Υ, δεν υπάρχει επαρκής τεχνολογική μέθοδος, η οποία να οδηγεί με ασφάλεια στο θύτη των

κυβερνοεπιθέσεων. Οι υπάρχουσες μέθοδοι είναι αρκετά κοστοβόρες και καταλήγουν σε περιορισμένα συμπεράσματα, όπου και στην περίπτωση που ανακαλυφθεί η τοποθεσία, που ξεκίνησε μια κυβερνοεπίθεση, αυτό δεν σημαίνει αυτεπάγγελτα ότι το συγκεκριμένο κράτος είχε δώσει την εντολή εκτέλεσής της, καθώς η κυβερνοεπίθεση μπορεί να υλοποιήθηκε από μη κρατικό δρώντα, ή ακτιβιστή, ο οποίος δρα αυτοβούλως και δίχως να έχει λάβει αρμοδίως σχετικές εντολές. Παράλληλα, όταν η αμυνόμενη 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 όπως το είδος, ο ρυθμός και η συχνότητα, καθώς και η επιλογή στόχων από τον αντίπαλο καταδεικνύουν τον γενικότερο τρόπο λειτουργίας του, τα κίνητρα και τις επιδιώξεις του αλλά και τον τρόπο, που λαμβάνει αποφάσεις.

Ένα άλλο σημείο, που καθιστά προβληματική την εφαρμογή της αποτροπής στον κυβερνοχώρο είναι ο αριθμός των «παιχτών», που μπορούν να εμπλακούν σε μια σύγκρουση. Στην περίπτωση των κυβερνοσυγκρούσεων μπορούν να εμπλακούν διάφοροι μη κρατικοί δρώντες, των οποίων ο ορθολογικός τρόπος λήψης αποφάσεων τίθεται πολλές φορές υπό αμφισβήτηση. Οι παράγοντες αυτοί μπορούν να λειτουργούν αυτόνομα αλλά κάλλιστα μπορούν να διεξάγουν κυβερνοεπιθέσεις υπό την ανοχή ή τις οδηγίες ενός κράτους, το οποίο δεν επιθυμεί να έχει άμεση εμπλοκή με αυτές. Ωστόσο, αν τα αντίποινα, που προβλέπονται από την στρατηγική αποτροπής στοχεύσουν έναν μη κρατικό δρώντα, που δραστηριοποιείται σε μια ουδέτερη χώρα, τότε υπάρχει ο κίνδυνος η στρατηγική αυτή να δημιουργήσει έναν ακόμα αντίπαλο στον κυβερνοχώρο.

5.5 Σύγχρονες Τάσεις

Σύμφωνα με τα προαναφερθέντα στην προηγούμενη ενότητα, η αποτροπή όπως είναι γνωστή στο συμβατικό και το πυρηνικό επίπεδο, παρουσιάζει προβλήματα εφαρμογής στον κυβερνοχώρο. Οι κυβερνοεπιθέσεις δεν μπορούν να αποτραπούν ολοκληρωτικά, αλλά μπορούν να περιοριστούν. Σε αυτήν την βάση έχουν αναπτυχθεί τρεις τάσεις σχετικά με την μορφή, που πρέπει να λάβει η αποτροπή για να ενταχθεί καλύτερα στον κυβερνοχώρο, εκ των οποίων η πρώτη δίνει έμφαση στην κυβερνοάμυνα, χωρίς να απορρίπτει την κυβερνοεπίθεση υπό την μορφή αντιποίνων, όταν αυτό απαιτηθεί, ενώ οι άλλες δύο εστιάζουν στις επιθετικές δυνατότητες στον κυβερνοχώρο[B4].

Η πρώτη προσέγγιση θεωρεί πως πρέπει να δοθεί έμφαση στην κυβερνοαποτροπή μέσω άρνησης, αναπτύσσοντας σε εθνικό επίπεδο ιδιαίτερες αμυντικές δυνατότητες στον

κυβερνοχώρο, ενώ επισημαίνει ότι το πρόβλημα των κυβερνοεπιθέσεων θα πρέπει να αντιμετωπιστεί σε διεθνές επίπεδο μέσω σύναψης διεθνών συνθηκών και συνεργασίας. Η ανάπτυξη 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 μπορεί να επιτευχθεί μέσω αλλαγής της αρχιτεκτονικής των υπόψη δικτύων, ώστε να μετατραπούν σε ολοκληρωμένα οπλικά συστήματα. Επιπρόσθετα, μέσω της σύναψης διεθνών συνθηκών για τον κυβερνοχώρο, οι οποίες θα μπορούσαν να στηριχτούν στην πρακτική παρόμοιων συνθηκών του παρελθόντος, θα πρέπει να θεσμοθετηθεί μια κοινή διεθνής νομική ορολογία για τον κυβερνοχώρο και ένα κοινά αποδεκτός τρόπος προσέγγισης των κυβερνοεπιθέσεων, καθορίζοντας ταυτόχρονα τα επίπεδα διεθνούς συνεργασίας.

Η δεύτερη προσέγγιση στηρίζεται στο αξίωμα του κυβερνοχώρου ότι η επίθεση υπερτερεί της άμυνας, άρα η καλύτερη άμυνα προκύπτει μέσω της επίθεσης. Σύμφωνα με αυτήν την τάση, δίνεται 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 και μεταφέρει την ευθύνη για την εκδήλωση των αρχικών κυβερνοεπιθέσεων στις ηγεσίες των κρατών από την επικράτεια των οποίων διεξήχθηκαν οι κυβερνοεπιθέσεις. 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 στο φόβο των αντιποίνων, με τα κράτη να προσπαθούν να κυριαρχήσουν το ένα του άλλου μέσω της ανάπτυξης επιθετικών δυνατοτήτων στον κυβερνοχώρο. Ως αποτέλεσμα τα κράτη θα οδηγηθούν στη δημιουργία ενός συστήματος ισορροπίας δυνάμεων, στο οποίο θα έχουν τον πρώτο λόγο οι υπερδυνάμεις του κυβερνοχώρου. Κατά αναλογία με τον Ψυχρό Πόλεμο, το σύστημα θα στηρίζεται στην ύπαρξη αμοιβαίου φόβου σχετικά με τις «εξουθενωτικές» συνέπειες, που θα έχει για όλους η διατάραξη της ισορροπίας στον κυβερνοχώρο (Cyber Mutual Assured Debilitation(MAD)). Μέσω της Cyber MAD, η προσέγγιση αυτή θεωρεί πως θα περιοριστούν επαρκώς οι συγκρούσεις στον κυβερνοχώρο.

5.5.1 Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection System)

Στις μέρες μας, τα συστήματα ανίχνευσης εισβολής (intrusion detection systems (IDS)) διαδραματίζουν σπουδαίο ρόλο στην αντιμετώπιση και στην αποτροπή των κυβερνοεπιθέσεων. Πιο συγκεκριμένα, ένα σύστημα ανίχνευσης εισβολής παρακολουθεί την κυκλοφορία του δικτύου για ενδεχόμενη ύποπτη δραστηριότητα και εκδίδει ειδοποιήσεις, όταν εντοπίζει κάτι αντικανονικό. Εκτός όμως από την ανίχνευση ανωμαλιών και την αναφορά αυτών προς το χρήστη, πολλά IDS έχουν τη δυνατότητα να λαμβάνουν μέτρα όταν εντοπίζουν κακόβουλη δραστηριότητα ή ανώμαλη κίνηση, συμπεριλαμβανομένου του αποκλεισμού της επισκεψιμότητας, που αποστέλλεται από ύποπτες διευθύνσεις IP[Γ10].

Τα συστήματα ανίχνευσης εισβολών παρουσιάζονται σε διάφορες μορφές, χρησιμοποιώντας διαφορετικές μεθόδους, προκειμένου να ανιχνεύσουν κακόβουλες δραστηριότητες. Πιο συγκεκριμένα, οι τύποι των IDS είναι οι παρακάτω:

- Network Intrusion Detection System (NIDS)

Πρόκειται για σύστημα ανίχνευσης εισβολής σε δίκτυο, το οποίο αναπτύσσεται σε ένα ή περισσότερα στρατηγικά σημεία εντός του δικτύου, όπου μπορεί να παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση προς και από όλες τις συσκευές του δικτύου.

- Host Intrusion Detection Systems (HIDS)

Τα συστήματα ανίχνευσης εισβολής υποδοχής εκτελούνται σε όλους τους υπολογιστές ή συσκευές του δικτύου με άμεση πρόσβαση τόσο στο διαδίκτυο όσο και στο εσωτερικό επιχειρησιακό δίκτυο. Το πλεονέκτημα του έναντι της παραπάνω κατηγορίας είναι η δυνατότητά του να ανιχνεύει «ανώμαλα πακέτα δικτύου, που προέρχονται από το εσωτερικό της οργάνωσης ή από κακόβουλη κίνηση, που το NIDS δεν κατάφερε να ανιχνεύσει. Παράλληλα, είναι σε θέση να εντοπίσει κακόβουλη επισκεψιμότητα, που προέρχεται από τον ίδιο τον κεντρικό υπολογιστή, όπως όταν ο ξενιστής έχει μολυνθεί από κακόβουλο λογισμικό και επιχειρεί να εξαπλωθεί σε άλλα συστήματα.

- Signature – based intrusion detection systems

Πρόκειται για συστήματα ανίχνευσης εισβολής με βάση την υπογραφή, τα οποία παρακολουθούν όλα τα πακέτα, που διασχίζουν το δίκτυο και τα συγκρίνουν με μια βάση δεδομένων με υπογραφές ή χαρακτηριστικά γνωστών κακόβουλων απειλών, όπως και το λογισμικό προστασίας από ιούς (antivirus software).

- Anomaly – based intrusion detection systems

Πρόκειται για συστήματα ανίχνευσης εισβολής με βάση την ανωμαλία, τα οποία παρακολουθούν την κυκλοφορία του δικτύου και τη συγκρίνουν με μια καθορισμένη γραμμή βάσης, προκειμένου να προσδιορίσουν τι θεωρείται φυσιολογικό για το δίκτυο σε σχέση με το εύρος ζώνης, τα πρωτόκολλα, τις θύρες και άλλες συσκευές. Αυτός ο τύπος IDS ειδοποιεί τους διαχειριστές για δυνητικά κακόβουλη δραστηριότητα.

Ένας ακόμα διαχωρισμός των IDS, τα διακρίνει σε παθητικά και ενεργά. Πιο συγκεκριμένα, ένα παθητικό IDS, που ανίχνευσε κακόβουλη δραστηριότητα, θα δημιουργούσε εγγραφές ειδοποιήσεων ή ημερολογίου, αλλά δε θα έκανε καμία ενέργεια. Αντιθέτως, ένα ενεργό IDS θα δημιουργήσει ειδοποιήσεις και καταχωρήσεις καταγραφής, καθώς επίσης θα είχε τη δυνατότητα να ρυθμιστεί ώστε να λαμβάνει μέτρα, όπως το κλείδωμα διευθύνσεων IP την απενεργοποίηση πρόσβασης σε περιορισμένους πόρους.

Όσον αφορά στις δυνατότητες των συστημάτων ανίχνευσης εισβολής, αυτά παρακολουθούν την κυκλοφορία του δικτύου προκειμένου να ανιχνεύσουν διείσδυση από μη εξουσιοδοτημένες οντότητες, παρέχοντας ορισμένες ή το σύνολο των παρακάτω λειτουργιών[Γ10]:

- Παρακολούθηση της λειτουργίας των δρομολογητών, τειχών προστασίας, κεντρικών διακομιστών διαχείρισης και αρχείων, τα οποία απαιτούνται από άλλους ελέγχους ασφαλείας, που αποσκοπούν στην ανίχνευση, αποτροπή ή ανάκτηση από κυβερνοεπιθέσεις.
- Παροχή στους διαχειριστές των δικτύων τη δυνατότητα να συντονίζουν, να οργανώνουν και να κατανοούν τις σχετικές διαδρομές ελέγχου του λειτουργικού συστήματος και άλλα αρχεία καταγραφής, που συχνά είναι δύσκολο να εντοπιστούν ή να αναλυθούν.
- Παροχή φιλική διεπαφή προς το χρήστη, ώστε τα μη εξειδικευμένα μέλη του προσωπικού να μπορούν να βοηθήσουν στη διαχείριση της ασφάλειας του συστήματος.
- Παροχή μιας εκτεταμένης βάσης δεδομένων υπογραφής, προκειμένου να μπορούν να αντιστοιχιστούν οι πληροφορίες από το σύστημα.
- Αναγνώριση και αναφορά σε περίπτωση ανίχνευσης της αλλαγής των αρχείων δεδομένων.
- Πρόκληση συναγερμού και ειδοποίηση σε περίπτωση παραβίασης της ασφάλειας του δικτύου.
- Αντίδραση σε εισβολής, αποκλείοντας ή παρεμποδίζοντας τον διακομιστή.

Όσον αφορά τα πλεονεκτήματα, που παρουσιάζουν τα IDS, προσφέρουν στους οργανισμούς ορισμένα οφέλη, ξεκινώντας από την ικανότητα εντοπισμού περιστατικών

ασφαλείας. Παράλληλα, ένα IDS μπορεί να χρησιμοποιηθεί για να βοηθήσει στην ανάλυση της ποσότητας και των τύπων των επιθέσεων, προκειμένου οι οργανισμοί να χρησιμοποιήσουν αυτές τις πληροφορίες για να αλλάξουν τα συστήματα ασφαλείας τους ή να εφαρμόσουν πιο αποτελεσματικούς ελέγχους. Επιπλέον, μπορεί να βοηθήσει τις εταιρείες να εντοπίσουν σφάλματα ή προβλήματα με τις διαμορφώσεις συσκευών δικτύου τους.

Επιπρόσθετα, τα συστήματα ανίχνευσης εισβολής μπορούν να βοηθήσουν στην επιτυχή συμμόρφωση με τις κανονιστικές διατάξεις, δίνοντας στις επιχειρήσεις μεγαλύτερη προβολή στα δίκτυά τους, καθιστώντας ευκολότερη την τήρηση των κανονισμών ασφαλείας. Τέλος, τα IDS μπορούν να βελτιώσουν την ανταπόκριση ασφαλείας. Δεδομένου ότι οι αισθητήρες IDS μπορούν να εντοπίσουν κεντρικούς υπολογιστές και συσκευές δικτύου, μπορούν επίσης να χρησιμοποιηθούν για την επιθεώρηση δεδομένων εντός των πακέτων δικτύου, καθώς και για τον προσδιορισμό των λειτουργικών συστημάτων των υπηρεσιών, που χρησιμοποιούνται[Γ10].

5.5.2 Αποτροπή και Τεχνητή Νοημοσύνη (Artificial Intelligence)

Ο όρος της τεχνητής νοημοσύνης (AI) επινοήθηκε το 1956, αλλά το (AI) έχει γίνει πιο δημοφιλές σήμερα λόγω του αυξημένου όγκου δεδομένων, των προηγμένων αλγορίθμων και των βελτιώσεων στην ισχύ των υπολογιστών και την αποθήκευση των δεδομένων[Γ9].

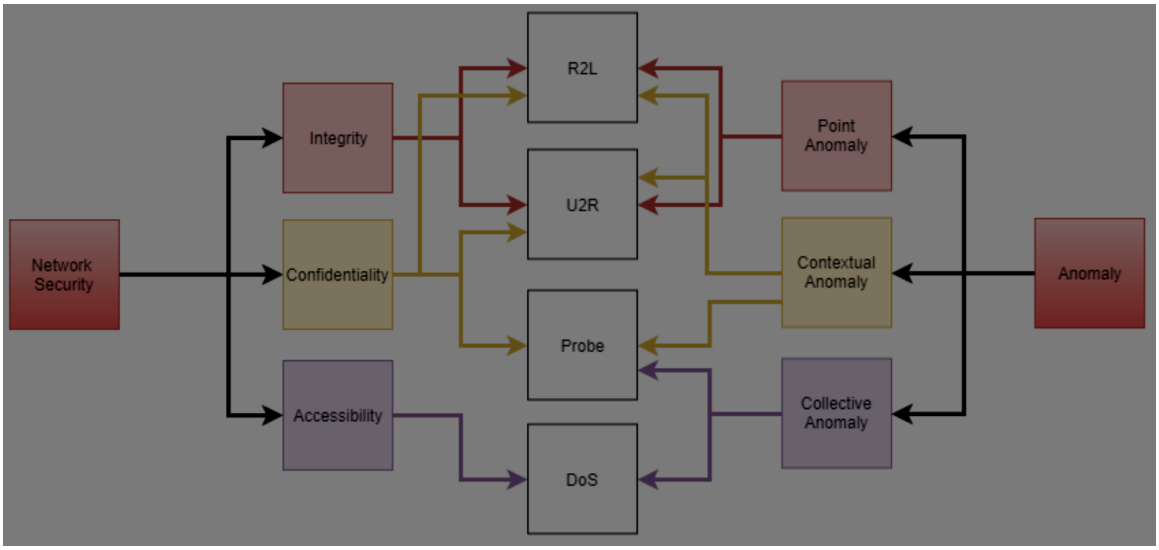
Αρχικά, η έρευνα γύρω από το AI επικεντρώθηκε σε θέματα όπως η επίλυση προβλημάτων και οι συμβολικές μέθοδοι. Τη δεκαετία του ’60, το Υπουργείο Άμυνας των ΗΠΑ ενδιαφέρθηκε για αυτόν τον τύπο εργασίας και ξεκίνησε την εκπαίδευση των υπολογιστών στη μίμηση της βασικής ανθρώπινης συλλογιστικής. Για παράδειγμα, η Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων Άμυνας (DARPA) ολοκλήρωσε τα προγράμματα χαρτογράφησης δρόμων τη δεκαετία του ’70. επίσης, η DARPA παρήγαγε ευφυείς προσωπικούς βοηθούς το 2003, πολύ πριν η Siri, Alexa και Cortana γίνουν πασίγνωστες[Γ9].

Η τεχνητή νοημοσύνη λειτουργεί με συνδυασμό μεγάλων ποσοτήτων δεδομένων με γρήγορους, επαναληπτικής διαδικασίας και ευφυείς αλγορίθμους, επιτρέποντας στο λογισμικό να μαθαίνει αυτόματα από μορφές ή χαρακτηριστικά των δεδομένων. Η τεχνητή νοημοσύνη είναι ένα πεδίο μελέτης που περιλαμβάνει πολλές θεωρίες, μεθόδους και τεχνολογίες, καθώς και τα παρακάτω κύρια υποπεδία[Γ9]:

- Machine learning (μηχανική μάθηση)
- Neural network (νευρωνικό δίκτυο)

- Deep learning (σε βάθος μάθηση)
- Cognitive computing (γνωστική υπολογιστική)
- Computer vision
- Natural language processing (NLP)

Η μέθοδος της μηχανικής μάθησης είναι ένας τρόπος ανίχνευσης ανωμαλιών σε ένα δίκτυο, καταδεικνύοντας με αυτόν τον τρόπο τη συμβολή της τεχνητής νοημοσύνης στην εύρεση και αποτροπή των κυβερνοεπιθέσεων.



Εικόνα 5.1 Συσχέτιση μεταξύ επιθέσεων δικτύου και «ανωμαλιών» δικτύου

Η μηχανική εκμάθηση είναι μια επιστήμη, η οποία επιτρέπει στους προγραμματισμένους υπολογιστές να μαθαίνουν από τα δεδομένα, που τους δίδονται. Στη διαδικασία εκμάθησης μηχανών, οι υπολογιστές μπορούν να εκπαιδευτούν στα δεδομένα (set training), που τους δίδονται και μπορούν να δείξουν την απόδοσή τους σε διαφορετικά δεδομένα (set test). Με αυτόν τον τρόπο, το πρόβλημα επιλύεται ελαχιστοποιώντας την ανθρώπινη παρέμβαση. Η μηχανική εκμάθηση χρησιμοποιείται σε πολλά μέρη όπου οι κλασικές μέθοδοι είναι αναποτελεσματικές. Πιο συγκεκριμένα, η μηχανική εκμάθηση μπορεί να συμβάλλει στην αποτροπή διεξαγωγής κυβερνοεπιθέσεων καθώς είναι σε θέση να ερμηνεύσει μεγάλα και πολύπλοκα δεδομένα, να δώσει λύσεις σε σύνθετα προβλήματα, να βρει λύσεις χωρίς εξωτερική παρέμβαση ή ενημέρωση αλλά και να ενεργεί σε μεταβλητά περιβάλλοντα.

Οι αλγόριθμοι μηχανικής μάθησης χωρίζονται σε 4 ομάδες ανάλογα με το αν τα δεδομένα κατάρτισης έχουν επισημανθεί ή όχι και σύμφωνα με την επίβλεψη εκπαίδευσης που έχουν λάβει. Αυτές είναι η επίβλεψη της μάθησης, η μη εποπτευόμενη μάθηση, η μάθηση με ημι-εποπτεύουσα μάθηση και η ενίσχυση της μάθησης[Γ9].

ΚΕΦΑΛΑΙΟ 6 ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ

6.1 Συσχέτιση Τεχνολογίας και Πολέμου

Ο πόλεμος, ανεξάρτητα από την ειδικότερη κάθε φορά μορφή του, είναι φαινόμενο ιστορικό και μεταβαλλόμενο. Εφόσον, ο πόλεμος διασταυρώνεται αναπόφευκτα με την ιστορία, διασταυρώνεται και με όλους τους επιμέρους παράγοντες, οι οποίοι αλληλεπιδρούν μεταξύ τους και την καθορίζουν, όπως είναι η οικονομία, ο πολιτισμός, η πολιτική, η θρησκεία, η γεωγραφία, το κλίμα και πολλοί άλλοι, ανάμεσα στους οποίους συγκαταλέγεται και ο παράγοντας της τεχνολογίας. Ο συνδυασμός των παραπάνω παραγόντων δημιουργεί σε κάθε χρονική στιγμή ένα πλέγμα δεδομένων, στα οποία το πολεμικό φαινόμενο οφείλει να προσαρμόζεται[A3].

Πόλεμος και τεχνολογία σχετίζονται ως εξής: πίσω από κάθε τύπο πολέμου, συναντάται ένας συγκεκριμένος πολιτισμός, δηλαδή μια κυρίαρχη κουλτούρα, που διαμορφώνεται από ποικίλες συνιστώσες (οικονομικές, ιδεολογικές, ηθικές). Μεταξύ αυτών περιλαμβάνονται τόσο ο βαθμός, όσο και τα επιμέρους επιτεύγματα της τεχνολογικής προόδου[A3]. Κατά τη διάρκεια μιας σύγκρουσης, οι εκπρόσωποι του κάθε πολιτισμού θα καταφύγουν σε εκείνα τα τεχνολογικά μέσα και τις μεθόδους, που θεωρούν ότι ανταποκρίνονται καλύτερα στην εξυπηρέτηση των κρίσιμων συμφερόντων τους. Πιο συγκεκριμένα, ενώ η τεχνολογική πρόοδος προσφέρει διαρκώς καινούργιες επιλογές και δυνατότητες στον τομέα των πολεμικών συγκρούσεων, η αξιοποίηση ή ακόμη και η κατάχρηση αυτών εξαρτάται κάθε φορά από τον τρόπο με τον οποίο, ο κάθε εμπλεκόμενος σε μια διαμάχη αντιλαμβάνεται τα συμφέροντά του και οριοθετεί τη συμπεριφορά του στον αγώνα για τη διασφάλισή τους.

Σε κάθε περίπτωση πάντως η τεχνολογική πρόοδος καθώς και τα συγκεκριμένα επιτεύγματα, που αυτή γεννά, συνδέονται άμεσα με έναν απρόβλεπτο και υποκείμενο σε προγραμματισμό παράγοντα: την έμπνευση και τη δημιουργικότητα του ανθρώπινου νου. Καταλήγοντας, ο ρόλος της τεχνολογίας στον πόλεμο δεν πρέπει να παραγνωρίζεται, αλλά ούτε και να υπερεκτιμάται, καθώς καμία δύναμη, όσο εξελιγμένη και αν είναι τεχνολογικά δεν μπορεί να στηριχτεί αποκλειστικά σ' έναν τόσο ανεξέλεγκτο και τυχαίο παράγοντα.

6.2 Συσχέτιση Τεχνολογίας και Στρατηγικής

Υπό τον όρο στρατηγική εννοούμε τη θεωρία, που αφορά στο συντονισμό και στη χρήση ή στην απειλή χρήσης κάθε διαθέσιμης μορφής βίας για την προώθηση του απώτερου πολιτικού στόχου, στον οποίο αποβλέπει ο κάθε πόλεμος. Η στρατηγική σκέψη, επειδή ουσιαστικά αποτελεί τη γέφυρα, που συνδέει την άσκηση της ένοπλης – κυρίως – βίας με την πολιτική, υπάγεται στην έννοια του πολέμου, πλην όμως γι' αυτήν γίνεται ευρύτερα αποδεκτό ότι εκσυγχρονίζεται, δηλαδή ότι μεταβάλλεται ανάλογα με τα δεδομένα κάθε εποχής[A3].

Ωστόσο, η προσφυγή στην συμπλοκή και η ειδικότερη μορφή, που αυτή θα λάβει, εξαρτάται από κάποια σταθερά στοιχεία – διαστάσεις, τα οποία αν και διακρίνονται το ένα από το άλλο, αναμειγνύονται και συνεργούν μεταξύ τους με πολλούς τρόπους και ποικίλες αναλογίες. Δε βρίσκονται σε ιεραρχική σχέση, αντιθέτως καθένα έχει ξεχωριστή βαρύτητα και τη δική του σημασία για κάθε συγκεκριμένη συμπεριφορά και επιλογή στα πλαίσια του σύνθετου φαινόμενου της στρατηγικής. Η τεχνολογία αποτελεί και πάλι έναν από αυτούς τους επιμέρους παράγοντες, η αλληλεπίδραση των οποίων, καθορίζει ως σύνολο το πώς θα διαμορφωθεί η στρατηγική αντίληψη κάθε μικρότερης ή μεγαλύτερης χρονικής περιόδου. Ως εκ τούτου, η οποιαδήποτε τεχνολογική εξέλιξη, όσο σπουδαία κι αν είναι, δεν μπορεί από μόνη της να επιφέρει μεταβολές στη στρατηγική σκέψη, εάν δεν συνδυαστεί με την ταυτόχρονη ενεργοποίηση άλλων παραγόντων.

6.3 Συσχέτιση Πληροφορίας και Επικοινωνίας με τη Στρατηγική

Στα πλαίσια ενός πολέμου ή ευρύτερα μιας πραγματικής ή ακόμη και πιθανής αντιπαράθεσης, ο όρος «πληροφορία» αναφέρεται στην κάθε είδους γνώση, είτε πρόκειται για δεδομένο, είτε απλώς για μια ανεπιβεβαίωτη πληροφορία, που σχετίζεται με τον αντίπαλο και συμβάλλει στη σύνθεση της εικόνας για την γενικότερη πολιτική, οικονομική, κοινωνική και πολιτιστική κατάσταση και τα αντίστοιχα χαρακτηριστικά του. Από τον τεράστιο όγκο των σχετικών πληροφοριών στο παρελθόν ήταν και εξακολουθεί να είναι και στις μέρες μας, ιδιάζουσας σημασίας για το κάθε εμπλεκόμενο μέρος σε μια διαμάχη, η απόκτηση ιδίως εκείνων, που παρουσιάζουν στρατιωτικό ενδιαφέρον[B3]. Στην κατηγορία αυτή ανήκουν ενδεικτικά οι γενικότερες πληροφορίες σχετικά με τις προθέσεις του αντιπάλου, την τοποθεσία, όπου βρίσκονται οι στρατιωτικές του δυνάμεις και τις κινήσεις αυτών, ώστε να πραγματοποιηθεί ο κατάλληλος επιχειρησιακός σχεδιασμός, καθώς και πληροφορίες, οι οποίες, παρέχοντας στοιχεία για τις γεωγραφικές θέσεις συγκεκριμένων εχθρικών στόχων, καθορίζουν το είδος και την ισχύ των μέσων, που θα επιλεγούν από τη συνολική δύναμη

πυρός, ώστε αυτοί να πληγούν με επιτυχία, ιδίως όταν το σημείο βολής είναι απομακρυσμένο.

Το στάδιο, το οποίο έπεται της απόκτησης των εν λόγω κρίσιμων πληροφοριών, είναι εξίσου σημαντικό. Πρόκειται για το στάδιο της αποστολής αυτών στους αρμόδιους στρατιωτικούς παράγοντες, ώστε να τις επεξεργαστούν και βάσει των συμπερασμάτων, στα οποία θα καταλήξουν, να λάβουν αναλόγως τις σχετικές με την οργάνωση και την εξέλιξη της στρατιωτικής δράσης αποφάσεις. Η επιτυχία αυτού του σταδίου εξαρτάται άμεσα από τις δυνατότητες για ταχεία, ασφαλή και ακριβή μετάδοση των πληροφοριών, που παρέχονται από τα επικοινωνιακά μέσα κάθε εποχής.

Από τα ανωτέρω συμπεραίνουμε ότι οι στρατιωτικές πληροφορίες καθώς και τα επικοινωνιακά μέσα μετάδοσής τους, επιδρούν καταλυτικά στη διεξαγωγή ενός πολέμου, επηρεάζοντας τόσο την κατάστρωση της γενικότερης στρατηγικής, όσο και την επιλογή συγκεκριμένης τακτικής. Ωστόσο, και στην περίπτωση των δύο αυτών στοιχείων, δηλαδή της πληροφορίας και της επικοινωνίας, έχουν ισχύ τα προαναφερθέντα αναφορικά με το ρόλο, τον οποίο διαδραματίζει η τεχνολογία στον πόλεμο και τη στρατηγική, καθώς η εκδήλωση και η έκβαση του πολεμικού φαινομένου, αλλά και η διαμόρφωση της στρατηγικής σκέψης ειδικότερα, εξαρτώνται από μια ποικιλία διαφορετικών παραγόντων, κανείς εκ των οποίων δεν δύναται από μόνος του να προκαλέσει την οποιαδήποτε άμεση μεταβολή στο χαρακτήρα ή στη φύση αυτών.

6.4 Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA)

Η μαζική και συνδυαστική χρήση των επιτευγμάτων της πληροφορικής και των εξελιγμένων τηλεπικοινωνιακών μέσων στις στρατιωτικές επιχειρήσεις θεωρείται ότι προκάλεσε τόσο απότομες και σημαντικές αλλαγές στο στρατιωτικό πεδίο, ώστε να παρατηρείται το φαινόμενο της «Επανάστασης στις Στρατιωτικές Υποθέσεις»[B1].

Ο όρος «Επανάσταση στις Στρατιωτικές Υποθέσεις» (Revolution in Military Affairs ή RMA) προέρχεται και αποτελεί ουσιαστικά της εξέλιξη του όρου «στρατιωτική τεχνική επανάσταση», η οποία εμφανίστηκε για πρώτη φορά τη δεκαετία του 1960 στους σοβιετικούς στρατιωτικούς κύκλους στα πλαίσια των αναλύσεων της ψυχροπολεμικής περιόδου σχετικά με το εάν η εμφάνιση των πυρηνικών όπλων συνεπαγόταν μεταβολές στο ειδικό βάρος των συμβατικών δυνάμεων κατά τη διάρκεια μιας αντιπαράθεσης και ειδικότερα με το εάν η ύπαρξη πυρηνικού οπλοστασίου ενεργούσε ως πολλαπλασιαστής ισχύος του συμβατικού οπλοστασίου[B1].

Στις Η.Π.Α., ο όρος μεταβλήθηκε για να καταδείξει ότι οι σημαντικές εξελίξεις στο στρατιωτικό τομέα δεν επέρχονται μονάχα λόγω της ενσωμάτωσης μιας νέας τεχνολογίας ή ενός μεμονωμένου τεχνολογικού επιτεύγματος, αλλά λόγω της βελτίωσης της μαχητικότητας και της αποτελεσματικότητας των στρατιωτικών δυνάμεων, που προκύπτει από τη συνδυαστική χρήση αυτών.

Σε γενικές γραμμές με τον όρο RMA εννοείται το κάθε μοντέλο στρατηγικής συμπεριφοράς, το οποίο με βασικό εργαλείο τη βέλτιστη χρήση των τεχνολογικών εξελίξεων κάθε εποχής, αποβλέπει στην υιοθέτηση μιας σειράς νέων αντιλήψεων και μεθόδων στο επιχειρησιακό επίπεδο, στην πραγματοποίηση αναδιαρθρώσεων στο εσωτερικό των ενόπλων δυνάμεων και στον εκσυγχρονισμό των οπλικών συστημάτων.

Η RMA μέσα από το πέρασμα των χρόνων και τις συνεχώς μεταβαλλόμενες καταστάσεις, που χαρακτήριζαν την εκάστοτε εποχή, διαμόρφωσε κάποια χαρακτηριστικά γνωρίσματα αλλά και τις αντίστοιχες απαιτήσεις στις οποίες θα κληθεί να ανταποκριθεί σήμερα. Πιο συγκεκριμένα, βασικό μέλημα είναι να αποφευχθεί ή να μην είναι αναγκαία η άμεση σωματική επαφή με τον εχθρό, γεγονός, που προϋποθέτει την ικανότητα να πληγεί εκείνος γρήγορα, με ακρίβεια και από μεγάλη απόσταση[A3]. Ως επακόλουθο, υποβαθμίζεται η αναγκαιότητα της διεξαγωγής καθαρά χερσαίων επιχειρήσεων και η προσοχή εστιάζεται στην αποδιοργάνωση των διοικητικών και κυρίως των πληροφοριακών κέντρων του αντιπάλου και στην αποτελεσματική συνεργασία και την ασφάλεια των αντίστοιχων ίδιων κέντρων.

Τα όπλα «ακριβείας», οι δορυφόροι, τα τηλεκατευθυνόμενα και μη επανδρωμένα αεροσκάφη, που συλλέγουν δεδομένα, η δικτύωση των χερσαίων – θαλάσσιων – εναέριων δυνάμεων με σκοπό τη συνολική εποπτεία και τη συντονισμένη δράση κατά του εχθρού, ο εξελιγμένος τηλεπικοινωνιακός εξοπλισμός, είναι μερικές μόνο από τις εφαρμογές της τεχνολογικής προόδου, που επιστρατεύτηκαν για την εκπλήρωση της αποστολής μιας νέας RMA.

Επιπλέον, σήμερα και λόγω της σύνδεσης του όρου με την επίδραση των τεχνολογικών εξελίξεων στους τομείς της πληροφορικής και της επικοινωνίας επί του τρόπου με τον οποίο οι σύγχρονοι στρατοί οργανώνονται και επιχειρούν, γίνεται λόγος για την εκδήλωση της «Πληροφοριακής Επανάστασης» στο στρατιωτικό τομέα. Ένα πρώτο καίριο ζήτημα αποτελεί ο εντοπισμός του εναρκτήριου σημείου της «Πληροφοριακής Επανάστασης», η οποία βρίσκεται ακόμη εν εξελίξει[A7]. Εξαιτίας της δυσκολίας να αποδοθεί το ξέσπασμά της στην εμφάνιση μιας και μόνης συγκεκριμένης τεχνολογίας και με δεδομένο ότι η τεχνολογία από μόνη της παρέχει απλώς τη δυνατότητα για μια στρατιωτική επανάσταση, η πραγματοποίηση της οποίας εξαρτάται από μια σειρά άλλων παραγόντων, θα

υποστηρίζαμε ότι τρεις ομάδες τεχνολογικών επιτευγμάτων οδήγησαν σε αυτήν την επανάσταση και ειδικά[B25]:

- Η εφεύρεση των μέσων μαζικής επικοινωνίας όπως το τηλέφωνο, ο ασύρματος τηλέγραφος, το ραδιόφωνο, η τηλεόραση.
- Η επινόηση των συσκευών μέτρησης, παρατήρησης και καταγραφής των ιδιοτήτων των φυσικών φαινομένων και των αντικειμένων, όπως το ταχύμετρο και το πιεσόμετρο.
- Η κατασκευή ηλεκτρονικών υπολογιστών, οι οποίοι στηρίζονται στη λειτουργία ψηφιακών κυκλωμάτων.

Η συνδυαστική χρήση των ανωτέρω τεχνολογιών επέτρεψε την κωδικοποίηση, την επεξεργασία, την πραγματοποίηση υπολογισμών και την εξαγωγή άμεσων και ακριβών συμπερασμάτων σχετικά με τα δεδομένα και τα αποτελέσματα, που προκύπτουν από τα μέσα της δεύτερης κατηγορίας, καθώς και τη γρήγορη μετάδοση όλων των παραπάνω.

Στο ευρύτερο πλαίσιο της σύγχρονης «Επανάστασης στις Στρατιωτικές Υποθέσεις» αναπτύχθηκε ο Πληροφοριακός Πόλεμος, ο οποίος αναλύθηκε ήδη κοντά σε άλλες πρακτικές, όπως πόλεμος ακριβείας, ο ψυχολογικός πόλεμος κλπ, οι οποίες θεωρείται ότι απέκτησαν τόσο μεγάλη στρατηγική βαρύτητα, ώστε να ξεπερνούν σε σπουδαιότητα τις συμβατικές μεθόδους εχθροπραξίας[B25].

Ιδιαίτερα μεγάλη διάσταση δίδεται στο ζήτημα από τα δυτικά κράτη, ιδίως από τις Η.Π.Α., οι οποίες θεωρούν ότι η «πληροφοριακή επανάσταση» εγκαινιάζει ένα καινούριο είδος πολέμου, επιφέροντας τις πλέον ριζικές μεταβολές στη διεξαγωγή πολεμικών συγκρούσεων.

6.5 Στρατηγική Λειτουργία Κυβερνοεπιθέσεων

Στις Η.Π.Α. αναπτύχθηκε μία ολόκληρη ρητορική σχετικά με τη στρατηγική αξία του κυβερνοπολέμου, βάσει της οποίας επέρχονται ριζικές αλλαγές στον τρόπο διεξαγωγής των σύγχρονων πολεμικών επιχειρήσεων. Μέσα από την εξέταση κάποιων επιμέρους ζητημάτων καταδεικνύεται πως οι κυβερνοεπιθέσεις σίγουρα αποτελούν ισχυρό όπλο για έναν αντίπαλο, όμως η δράση τους δεν μπορεί να επιφέρει καθηλωτικά αποτελέσματα στον πληττόμενο μέρος[B25].

Πιο συγκεκριμένα, υποστηρίχτηκε ότι οι κυβερνοεπιθέσεις, λόγω της έντονης καταστρεπτικής τους ικανότητας, λειτουργούν αποτρεπτικά, όπως ακριβώς και οι πυρηνικές

επιθέσεις. Μία μικρή ανάλυση των επιπτώσεων, που επιφέρει μια πυρηνική έκρηξη συγκριτικά με τις αντίστοιχες μιας κυβερνοεπίθεσης, αποδυναμώνει την παραπάνω προσέγγιση. Αρχικά, οι αποτρόπαιες και μακροχρόνιες συνέπειες της χρήσης των μέσων του πυρηνικού οπλοστασίου αποτελούν αποδεδειγμένα γεγονότα και όχι απλές εικασίες και σενάρια, όπως οι αντίστοιχης έντασης επιπτώσεις μιας κυβερνοεπίθεσης. Ο παράγοντας αυτός σε συνδυασμό με την παγκόσμια αποδοκιμασία, η οποία συνοδεύει την παραγωγή και την κατοχή πυρηνικών όπλων, έχει λειτουργήσει αποτρεπτικά για την περαιτέρω εξάπλωσή τους. Αντίστοιχα, στην περίπτωση των κυβερνοόπλων δεν παρατηρούνται τέτοια φαινόμενα, καθώς αυτά είναι εύκολα προσβάσιμα από τον οποιονδήποτε επιθυμεί να πειραματιστεί με τη χρήση τους. Επιπλέον, μια πυρηνική επίθεση μπορεί να διεξαχθεί κατά οποιουδήποτε αντιπάλου, ενώ αντιθέτως η κυβερνοεπίθεση προϋποθέτει την εξάρτηση της επιβίωσης του πληττόμενου από ηλεκτρονικά δίκτυα και πληροφορίες, γεγονός που δεν παρατηρείται σήμερα στις περισσότερες περιοχές του πλανήτη.

Όσον αφορά τη δυνατότητα υποκατάστασης των συμβατικών επιχειρήσεων από τις κυβερνοεπιθέσεις, πάλι παρουσιάζονται κάποια διφορούμενα στοιχεία, καθώς η χρήση των κυβερνοεπιθέσεων στο παγκόσμιο προσκήνιο επέφερε ανακατατάξεις των ισορροπιών στο διεθνές σύστημα διότι θέτουν διαρκώς υπό αμφισβήτηση παραδοσιακά σύμβολα οικονομικής, στρατιωτικής και διπλωματικής ισχύος, δεδομένου ότι αυτά δεν έχουν αξία στην περίπτωση διεξαγωγής μιας τέτοιου είδους επίθεσης. Παράλληλα, μια κυβερνοεπίθεση δύναται να λάβει διαφορετικές όψεις ανάλογα με τις ειδικότερες συνθήκες υπό τις οποίες τελούν οι αντίπαλες παρατάξεις σε μια διαμάχη[B22].

Πιο ειδικά, είναι γεγονός ότι η εύκολη και χωρίς ιδιαίτερο κόστος απόκτηση των κυβερνοόπλων για την εκδήλωση μιας κυβερνοεπίθεσης, καθώς και η δυνατότητα δράσης υπό την κάλυψη της ανωνυμίας είναι παράγοντες, που ενθαρρύνουν την προσφυγή σ' αυτή την πρακτική δρώντων, κρατικών και μη, οι οποίοι υστερούν σε συμβατικά μέσα, ώστε να αντισταθμίσουν τη συγκεκριμένη αδυναμία τους. Ως αποτέλεσμα επέρχεται η διάχυση και αναδιανομή της ισχύος, σε βάρος των δυνάμεων με συμβατική υπεροπλία και για τον λόγο αυτόν, πολλοί αναλυτές εντάσσουν τις κυβερνοεπιθέσεις στην ευρύτερη κατηγορία των «ασύμμετρων απειλών»[B22]. Η τρωτότητα μιας κοινωνίας απέναντι σε τέτοιου είδους επιθέσεις είναι ανάλογη του βαθμού της τεχνολογικής ανάπτυξης, ουσιαστικά αυξάνεται, όσο αυξάνεται η εξάρτηση της από τους στόχους μιας κυβερνοεπίθεσης, δηλαδή από τα ηλεκτρονικά δίκτυα και τις πληροφορίες, που διακινούνται σε αυτά.

Επιπλέον ακόμα και στην περίπτωση σύγκρουσης μεταξύ δύο εξίσου ανεπτυγμένων τεχνολογικά δυνάμεων, οι αμοιβαίες κυβερνοεπιθέσεις δεν μπορούν να καθορίσουν το αποτέλεσμα της διαμάχης, καθώς ακόμα και αν υπάρξει απόλυτη αλληλεξουδετέρωση των

κρίσιμων ηλεκτρονικών δικτύων εκατέρωθεν των αντιμαχομένων, τότε αναπόφευκτα η μάχη θα συνεχιστεί με συμβατικά όπλα μέχρι την οριστική επικράτηση της μιας δύναμης έναντι της άλλης[B38].

Ακόμα, και στην περίπτωση, στην οποία η μία εκ των δύο πλευρών διαθέτει απόλυτα εξελιγμένη τεχνολογική υποδομή στον τομέα των κυβερνοεπιθέσεων έναντι ενός αντιπάλου, ο οποίος δεν διαθέτει αντίστοιχες δικτυωμένες υποδομές, πάλι δεν μπορεί να αξιοποιηθεί στρατηγικά η πρακτική των κυβερνοεπιθέσεων.

Τέλος, σίγουρα οι κυβερνοεπιθέσεις που πραγματοποιούνται δεν υπόκεινται σε γεωγραφικούς περιορισμούς και φυσικές διαστάσεις, όπως αυτές ορίζονται στον πραγματικό κόσμο, επιτυγχάνοντας από απόσταση στόχους τεράστιας στρατηγικής σημασίας, ελαχιστοποιώντας παράλληλα τη σημασία της γεωγραφίας στα πλαίσια μιας διένεξης. Παρ' όλα αυτά, όμως, μια διαμάχη ή ένας πόλεμος δεν μπορεί να κερδηθεί αν δεν εξασφαλιστεί η υπεροχή και ο έλεγχος του εδάφους, γεγονός το οποίο προϋποθέτει πάντα τη φυσική παρουσία ικανών από άποψη αριθμού, εξοπλισμού και εκπαίδευσης χερσαίων στρατιωτικών δυνάμεων[B34]. Έτσι δεν μπορούμε να πούμε ότι η σημασία της γεωγραφικής απόστασης εξαλείφεται λόγω της ικανότητας των κυβερνοεπιθέσεων να επιφέρουν καίρια πλήγματα από μεγάλη απόσταση μεταξύ θύτη και θύμα.

ΚΕΦΑΛΑΙΟ 7 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

7.1 Ισχύοντες Κανόνες Διεθνούς Δικαίου

Παρά το γεγονός ότι η τέλεση εχθροπραξιών στον κυβερνοχώρο δεν αποτελεί από μόνη της ικανό στοιχείο προκειμένου να μεταβληθεί ριζικά η φύση του πολέμου και της στρατηγικής, ο κυβερνοχώρος είναι αναμφισβήτητα ένα ακόμη πεδίο εκμεταλλεύσιμο για την επίτευξη συγκεκριμένων στρατιωτικών στόχων στρατηγικού ή τακτικού χαρακτήρα. Έτσι, παράλληλα με την επιθυμία των κρατικών και μη δρώντων να εξασφαλίσουν την ετοιμότητά τους για αποτελεσματική δράση στον κυβερνοχώρο, τόσο αμυντικά όσο και επιθετικά, ανάλογα με τις εκάστοτε περιστάσεις, επικρατεί έντονος προβληματισμός σχετικά με τους κανόνες δικαίου σύμφωνα με τους οποίους θα πρέπει να αντιμετωπιστούν και να ρυθμιστούν οι απειλές, που δημιουργούνται για τη διεθνή ασφάλεια από τις αθέμιτες πράξεις, που τελούνται στον κυβερνοχώρο και ειδικά το θέμα των κυβερνοεπιθέσεων.

Οι προτεινόμενες λύσεις δύναται να ομαδοποιηθούν σε δύο μεγάλες κατηγορίες. Από τη μία, υπάρχει η άποψη ότι το ζήτημα μπορεί να διευθετηθεί μέσω της ενεργοποίησης και της αναλογικής εφαρμογής των ήδη υπαρχόντων κανόνων του διεθνούς δικαίου (συμβατικού και εθιμικού) και από την άλλη η άποψη ότι οι ιδιαιτερότητες, που συνδέονται με τη φύση του κυβερνοχώρου, τη λειτουργία του καθώς και με τα μέσα άμυνας και επίθεσης, που χρησιμοποιούνται σε αυτόν, επιβάλλουν τη θέσπιση καινούργιων κανόνων και την ανάπτυξη νέων θεσμικών μηχανισμών και εργαλείων, ώστε να αντιμετωπιστούν αποτελεσματικά οι κίνδυνοι, που ελλοχεύουν για την ομαλή εξέλιξη των διεθνών σχέσεων.

7.1.1 Δίκαιο της Χρήσης Βίας (jus ad bellum)

Στο κείμενο του Χάρτη των Ηνωμένων Εθνών, το οποίο υπογράφτηκε μετά τη λήξη του Β' Παγκοσμίου Πολέμου, περιλαμβάνονται μεταξύ άλλων και διατάξεις από το συνδυασμό των οποίων προκύπτει το βασικό ρυθμιστικό πλαίσιο του δικαίου της χρήσης βίας, δηλαδή ο κύριος μηχανισμός, που αποβλέπει στην επίτευξη του βασικού στόχου του ΟΗΕ, δηλαδή τη διατήρηση της διεθνούς ειρήνης και ασφάλειας, μέσω της γενικής απαγόρευσης της χρήσης βίας, ως μέσου για την επίλυση των διαφορών, που δημιουργούνται μεταξύ των μελών του Οργανισμού[B33].

Έτσι, λοιπόν, συνάγεται η απαγόρευση της χρήσης βίας στις σχέσεις μεταξύ των μελών του Οργανισμού, δηλαδή μεταξύ κυρίαρχων κρατών, με εξαίρεση αφενός τη στρατιωτική επέμβαση κατόπιν αντίστοιχης απόφασης και εξουσιοδότησης του Συμβουλίου Ασφαλείας και αφετέρου της χρήσης βίας από τον αποδέκτη μιας ένοπλης επίθεσης, ως

αυτοάμυνα. Ωστόσο, αυτές οι διατάξεις θεσπίστηκαν σε μια εποχή, όπου τόσο το φαινόμενο του κυβερνοχώρου, όσο και των αθέμιτων πράξεων που σχετίζονται μ' αυτόν, ήταν δεδομένα παντελώς άγνωστα και μη προβλέψιμα[B27]. Συνεπώς είναι εύλογο να εγείρονται πολλά επιμέρους ζητήματα, όταν γίνεται προσπάθεια αντιμετώπισης του νέου πεδίου μάχης και των εχθροπραξιών, που μπορούν να διεξαχθούν σ' αυτόν, βάσει του ρυθμιστικού πλαισίου του Χάρτη.

Αρχικά, ένα ζήτημα, που δημιουργείται, είναι κατά πόσο μια κυβερνοεπίθεση μπορεί να υπαχθεί, αφενός, στην έννοια της απαγορευμένης «χρήσης βίας», που δικαιολογεί την επέμβαση και τη λήψη των κατάλληλων κάθε φορά μέτρων εκ μέρους του Συμβουλίου Ασφαλείας και αφετέρου, στην έννοια της «ένοπλης επίθεσης», που θεμελιώνει το δικαίωμα αυτοάμυνας του κράτους – στόχου. Σύμφωνα με τα γενικώς ισχύοντα, η οποιαδήποτε επιθετική συμπεριφορά κυμαίνεται μεταξύ των εξής επιπέδων[B27]:

- Η ένταση και οι συνέπειές της είναι τόσο περιορισμένες, ώστε δε μπορεί καν να χαρακτηριστεί ως «χρήση βίας».
- Συνιστά «χρήση βίας» αλλά υπολείπεται σε σοβαρότητα μιας «ένοπλης επίθεσης».
- Πληροί της προϋποθέσεις μιας «ένοπλης επίθεσης».

Σε μια προσπάθεια ταξινόμησης των κριτηρίων, που χρησιμοποιούνται από τους διάφορους μελετητές για την υπαγωγή μιας κυβερνοεπίθεσης σε μια από τις ανωτέρω κατηγορίες, εντοπίζονται τα εξής τέσσερα[B27]:

1. Τα μέσα, που χρησιμοποιούνται για την εκτέλεση της επίθεσης
2. Η σπουδαιότητα του στόχου της επίθεσης για τα ζωτικά συμφέροντα ενός κράτους.
3. Η σοβαρότητα των επερχόμενων αποτελεσμάτων.
4. Ο βαθμός της υπαιτιότητας του επιτιθέμενου.

Για όσους προσεγγίζουν το ζήτημα αποκλειστικά βασιζόμενοι στο πρώτο κριτήριο, μια κυβερνοεπίθεση δεν μπορεί να θεωρηθεί «χρήση βίας», πόσο μάλλον «ένοπλη επίθεση», καθώς οι κυβερνοεπιθέσεις διεξάγονται με άυλα μέσα και όχι με συμβατικά, απτά όπλα των παραδοσιακών επιθέσεων[B20]. Αντιθέτως, οι προσεγγίσεις με το δεύτερο κριτήριο καταλήγουν στο συμπέρασμα ότι μια κυβερνοεπίθεση δεν εξομοιώνεται απλά με «χρήση βίας», αλλά επιπλέον εντάσσεται στην έννοια της «ένοπλης επίθεσης», όταν στοχεύει στα ηλεκτρονικά δίκτυα, που υποστηρίζουν τη λειτουργία κρίσιμων υποδομών ενός κράτους. Σύμφωνα με το τρίτο κριτήριο εάν μια επίθεση στο πεδίο του κυβερνοχώρου είναι εφικτό να προκαλέσει άμεσα τη φυσική καταστροφή υλικών αγαθών, τότε εύλογα μπορεί να

χαρακτηριστεί ως «χρήση βίας», ενώ μεταβαίνει στο επίπεδο της «ένοπλης επίθεσης» όταν οι συνέπειες της είναι τόσο αποτρόπαιες, όσο και οι συνέπειες μιας επίθεσης με συμβατικά μέσα, όπως για παράδειγμα όταν προκαλείται ή απειλείται ο τραυματισμός ή ο θάνατος ανθρώπων[B24]. Τέλος, με επίκεντρο, το τελευταίο κριτήριο, αρκεί η εχθρική πρόθεση του δράστη για το χαρακτηρισμό μιας επίθεσης στον κυβερνοχώρο ως «χρήσης βίας», ενώ το πλαίσιο εντός του οποίου λαμβάνει χώρα, η διάρκεια και η έντασή της θα καθορίσουν περαιτέρω αν συντρέχουν λόγοι, που να δικαιολογούν την εκδήλωση παθητικής ή ενεργητικής αμυντικής συμπεριφοράς, ανάλογης με αυτή που δικαιούται να εκδηλώσει το θύμα μιας «ένοπλης επίθεσης».

7.1.2 Δίκαιο του Πολέμου (jus in bello)

Με το τον όρο «δίκαιο του πολέμου», νοείται το σύνολο των συμβατικών και εθιμικών κανόνων του Διεθνούς Δικαίου, που ρυθμίζουν τη συμπεριφορά των αντίπαλων μερών κατά τη διάρκεια μιας πολεμικής αντιπαράθεσης. Στην περίπτωση τέλεσης μιας κυβερνοεπίθεσης, ενόσω οι γενικευμένες εχθροπραξίες είναι σε εξέλιξη, η εφαρμογή κάποιων εκ των αρχών του δικαίου του πολέμου, που απορρέουν από τα τρία βασικά ρυθμιστικά κείμενα της Συνθήκης της Γενεύης (1949) και τα Πρωτόκολλα, που προστέθηκαν σ' αυτές (1977), δημιουργεί ποικίλους προβληματισμούς. Ειδικότερα, πρόκειται για τις εξής αρχές[B18]:

- Την αρχή της στρατιωτικής αναγκαιότητας.
- Την αρχή της διάκρισης,.
- Την αρχή της αναλογικότητας
- Την αρχή ης ουδετερότητας

Πιο συγκεκριμένα σύμφωνα με την αρχή της στρατιωτικής αναγκαιότητας, μια στρατιωτική επίθεση εν καιρώ πολέμου είναι επιτρεπτή μόνο όταν κατευθύνεται εναντίον στόχων, οι οποίοι βάσει της φύσης τους, της τοποθεσίας τους και του σκοπού, που εξυπηρετούν, συμβάλλουν ουσιωδώς στη στρατιωτική δράση και των οποίων η ολική ή μερική καταστροφή ή αδρανοποίηση προσφέρει σαφές στρατιωτικό πλεονέκτημα, οδηγώντας σε επιτυχή τερματισμό της διαμάχης[B18]. Επομένως, απαγορευμένες θεωρούνται οι στρατιωτικές επιθέσεις σε στόχους μη στρατιωτικής σημασίας, οι οποίοι προστατεύονται. Στην περίπτωση των κυβερνοεπιθέσεων, το ζήτημα, που προκύπτει, αναφέρεται στο κατά πόσο μια τέτοιου είδους επίθεση ταυτίζεται με την έννοια της «στρατιωτικής επίθεσης» ή όχι, προκειμένου να αξιολογηθεί αν κι αυτή θεωρείται απαγορευμένη κατά των μη στρατιωτικών στόχων. Η αδυναμία κατάταξης σε και από τις δύο κατηγορίες ενισχύεται, όταν οι κυβερνοεπιθέσεις δεν επιφέρουν υλικές ζημιές και έμψυχες απώλειες, με αποτέλεσμα να μην

δύναται να χαρακτηριστούν ως «στρατιωτική επίθεση» και ως συνέπεια να μην εντάσσονται στην κατηγορία των απαγορευμένων επιθέσεων[B18]. Επιπλέον, θα πρέπει να προστεθεί και ο παράγοντας, ο οποίος επιτείνει τη σύγχυση, όσον αφορά στην ένταξη των κυβερνοεπιθέσεων στο προστατευτικό πεδίο της αρχής της στρατιωτικής αναγκαιότητας, σύμφωνα με τον οποίο πολλές από τις υποδομές, οι οποίες στηρίζουν τη λειτουργία τους σε ηλεκτρονικά δίκτυα, αποτελούν στόχους των κυβερνοεπιθέσεων, εξυπηρετώντας ταυτόχρονα με τις στρατιωτικές ανάγκες και μη στρατιωτικές, δηλαδή ανάγκες του αστικού πληθυσμού. Από την άλλη, η επίθεση σε έναν τέτοιο στόχο «διπλής χρησιμότητας», είναι ανεκτή όταν αυτός συμβάλλει αποτελεσματικά στη στρατιωτική δράση και προσφέρει σαφές στρατιωτικό πλεονέκτημα, αλλά θα πρέπει να επιδιώκεται, κατά το δυνατόν, η εξουδετέρωση και όχι η καταστροφή του. Εν κατακλείδι, αν κριθεί ότι αποτελεί στόχο αυτής της κατηγορίας μια υποδομή, που στηρίζει τη λειτουργία της σ' ένα ηλεκτρονικό δίκτυο, μια κυβερνοεπίθεση με σκοπό βλάβη του δικτύου και συνακόλουθα στην αδρανοποίηση της εγκατάστασης, πιθανότατα θα ήταν σύμφωνη με την αρχή της στρατιωτικής αναγκαιότητας[A6].

Σκοπός της αρχής της διάκρισης είναι η προστασία του αστικού πληθυσμού πολιτών και των υλικών αγαθών, που εξυπηρετούν τις ανάγκες του, μέσω της διάκρισής τους, αντιστοίχως, από τα πρόσωπα που μάχονται ενεργά, δηλαδή από τα μέλη των ενόπλων δυνάμεων και από τα αντικείμενα που εξυπηρετούν αποκλειστικά στρατιωτικούς σκοπούς. Τα μέλη των τακτικών ενόπλων δυνάμεων έχουν το δικαίωμα να συμμετέχουν άμεσα στις εχθροπραξίες, συνιστούν επιτρεπτό στόχο για την αντίπαλη παράταξη, όπως και τα στρατιωτικά αντικείμενα, ενώ προστατεύονται από ειδικούς κανόνες σε περίπτωση αιχμαλωσίας ή τραυματισμού τους. Αντιθέτως, οι απλοί πολίτες απαγορεύεται να αποτελούν στόχο επίθεσης και δεν μετέχουν ενεργά στην ένοπλη αντιπαράθεση. Στην περίπτωση των κυβερνοεπιθέσεων, τα παραπάνω όρια είναι δυσδιάκριτα. Αφενός, μια τέτοια επίθεση μπορεί να υλοποιηθεί και από πρόσωπο, που δεν εντάσσεται επισήμως στις ένοπλες δυνάμεις ενός κράτους, οπότε δημιουργείται το ερώτημα αν μεταβάλλεται αυτομάτως με τη σχετική ενέργεια η κατάσταση του προσώπου αυτού από πολίτη σε πολεμιστή. Τέλος, η διάκριση ανάμεσα σε αντικείμενα στρατιωτικού ενδιαφέροντος και μη, ισχύουν όσο ειπώθηκαν παραπάνω για την αρχή της στρατιωτικής αναγκαιότητας, δηλαδή υπάρχουν αρκετές υλικές υποδομές, που εξυπηρετούν ταυτόχρονα πολίτες και ένοπλες δυνάμεις, θέτοντας σε αμφιβολία το επιτρεπτό της στόχευσης μιας τέτοιας υποδομής[B18].

Η αρχή της αναλογικότητας απαγορεύει την άσκηση κάθε είδους και έντασης βίας, που υπερβαίνει το αναγκαίο μέτρο για την επίτευξη συγκεκριμένου στρατιωτικού στόχου. Η επέλευση παράπλευρων ζημιών κατά τη διάρκεια των εχθροπραξιών δεν ισοδυναμεί αυτομάτως με παράβαση της ανωτέρω απαγόρευσης εφόσον κρίνεται αναλογική σε σχέση με το στρατιωτικό πλεονέκτημα, που εξασφαλίζεται. Δεδομένης της παράλληλης εξυπηρέτησης

στρατιωτικών και μη αναγκών από αυτές τις υποδομές, μια κυβερνοεπίθεση στα ηλεκτρονικά δίκτυα είναι πολύ πιθανό να προκαλέσει παράπλευρες ζημιές. Οπότε ανακύπτει το ερώτημα κατά πόσο οι επιπτώσεις αυτές δικαιολογούνται ως αντιστάθμισμα των στρατιωτικών ωφελειών[B19]. Ειδικότερα δε, για την αξιολόγηση της αναλογικότητας της αντίδρασης σε μια κυβερνοεπίθεση θεωρείται ορθότερη η άσκηση άμυνας, μέσω της πλήξης των ηλεκτρονικών συστημάτων από τις οποίες αυτή προέρχεται, με τη λογική ότι οι παράπλευρες ζημιές που θα προκληθούν θα είναι πιο περιορισμένες και λιγότερο σοβαρές απ' ότι αν επιλεγούν συμβατικά όπλα ως μέσα αντεπίθεσης[B18].

Μέσω της αρχής της ουδετερότητας, η οποία εξειδικεύεται σε δύο επιμέρους αρχές, αφενός της μη ανάμειξης και αφετέρου της αμεροληψίας, προκύπτουν συγκεκριμένα δικαιώματα και υποχρεώσεις για το κράτος, που δεν επιθυμεί να λάβει μέρος σε μια εξελισσόμενη πολεμική διαμάχη. Καταρχήν, το συγκεκριμένο κράτος δικαιούται να μην διακόψει τις οποιεσδήποτε σχέσεις του με τα εμπόλεμα μέρη, ενώ παράλληλα μπορεί να αξιώνει να μην αντιμετωπίζεται η επικράτειά του ως στόχος εχθροπραξιών, αλλά ούτε και ως δίοδος για τη διέλευση στρατιωτικών δυνάμεων[B23]. Παράλληλα, υποχρεούται να μην επιτρέπει τη χρησιμοποίηση της επικράτειάς του ως βάσης για την άσκηση πολεμικών πράξεων. Ωστόσο, η διαφύλαξη της ουδετερότητας ενός κράτους στην περίπτωση των κυβερνοεπιθέσεων είναι άκρως λεπτό ζήτημα, κυρίως όταν οι επιθέσεις διεξάγονται μέσω του κυβερνοχώρου. Δεδομένης της αρχιτεκτονικής του διαδικτύου και της παγκόσμιας εμβέλειάς του, είναι εξαιρετικά εύκολο τα κυβερνοόπλα να διοχετευθούν μέσα από τους κόμβους ενός κράτους, που απέχει από μια πολεμική διαμάχη, καθιστώντας το με αυτόν τον τρόπο την πηγή μιας επίθεσης[Γ7]. Επομένως για να διατηρήσει την ουδετερότητά του ένα κράτος οφείλει σε γενικές γραμμές να μην αποτελεί τον τόπο προέλευσης κυβερνοεπιθέσεων και να ενεργεί κατάλληλα στα πλαίσια των δυνατοτήτων του, ώστε να αποτρέπει τη διέλευση των μέσων, με τα οποία διεξάγεται μια κυβερνοεπίθεση από τους διαδικτυακούς του κόμβους. Η στιγμιαία ταχύτητα με την οποία διεξάγονται ωστόσο οι συγκεκριμένες επιθέσεις δεν παρέχει τα απαραίτητα χρονικά περιθώρια και τη δυνατότητα στο ουδέτερο κράτος να ενεργήσει και να ανακόψει την εξέλιξή τους ή να προειδοποιήσει τον αποδέκτη των επικείμενων επιθετικών πράξεων, με αποτέλεσμα να δημιουργείται ο κίνδυνος της ακούσιας εμπλοκής σε μια σύγκρουση[B26].

7.1.3 Διεθνείς Συνθήκες και Συμβάσεις

Το Συμβούλιο της Ευρώπης, μπροστά στη διαρκώς αυξανόμενη εγκληματικότητα στον κυβερνοχώρο κατάρτισε το 2001 το πρώτο και μοναδικό πολυμερές, δεσμευτικό νομικό κείμενο για την αντιμετώπιση ζημιογόνων ενεργειών, που πραγματοποιούνται στον

κυβερνοχώρο του διαδικτύου και άλλων ηλεκτρονικών δικτύων, τη λεγόμενη «Σύμβαση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο». Σκοπός αυτής της σύμβασης είναι η χάραξη κοινής αντεγκληματικής πολιτικής για την προστασία του κοινωνικού συνόλου, μέσω θέσπισης των κατάλληλων κανόνων, της εναρμόνισης των εσωτερικών ποινικών νομοθεσιών των κρατών – μελών και της ενίσχυσης της συνεργασίας μεταξύ των κρατών σε διεθνές επίπεδο.

Οι κολάσιμες πράξεις διακρίνονται σε τέσσερις κατηγορίες[B37]:

- Σε προσβολές κατά της εμπιστευτικότητας, της ακεραιότητας και διαθεσιμότητας των δεδομένων και των συστημάτων.
- Σε προσβολές που σχετίζονται με Η/Υ.
- Σε προσβολές που σχετίζονται με το περιεχόμενο των δεδομένων.
- Σε προσβολές κατά της πνευματικής ιδιοκτησίας και των συγγενών δικαιωμάτων.

Παρά τα θετικά σημεία της σύμβασης, τα οποία εντοπίζονται κυρίως στα σημαντικά περιθώρια ευελιξίας, που παρέχονται στα κράτη για την αποτελεσματική αντιμετώπιση των προαναφερθέντων προσβολών και στην προώθηση των δεσμών συνεργασίας, που θα πρέπει να αναπτυχθούν μεταξύ τους για τον ίδιο λόγο, η συγκεκριμένη σύμβαση δεν παύει να είναι ένα κείμενο, που αποσκοπεί στην εναρμόνιση των επιμέρους εθνικών νομοθεσιών για την αντιμετώπιση με ομοιογενή τρόπο. Οι σχετικοί κανόνες επουδενί δεν μπορούν να τύχουν εφαρμογής, όταν μια κακόβουλη πράξη στον κυβερνοχώρο διεξάγεται με την πρωτοβουλία των επίσημων κρατικών οργάνων μιας χώρας και προκαλεί ζητήματα διεθνούς ασφάλειας. Ενδεχομένως, θα μπορούσαν να αντιμετωπιστούν μέσω των σχετικών διατάξεων ορισμένα τρομοκρατικά επεισόδια στον κυβερνοχώρο, εφόσον όμως είναι εφικτό να αποκλειστεί το ενδεχόμενο της οποιασδήποτε κρατικής ανάμειξης ή υπόθαλψης αυτών και εφόσον εμπεδωθεί η ανάγκη για συνεργασία των αρμόδιων εθνικών αρχών όχι μόνο για την πάταξη των σχετικών πράξεων μετά την τέλεσή τους, αλλά και για τον εντοπισμό των επικίνδυνων προθέσεων και την πρόληψη της υλοποίησής τους[B31].

Εκτός όμως από την Ευρωπαϊκή Σύμβαση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, έχουν διατυπωθεί κάποιες συνθήκες, οι οποίες αφορούν τον τομέα των τηλεπικοινωνιών και τον τομέα του διαστήματος. Πιο συγκεκριμένα πρόκειται για τον Καταστατικό Χάρτη και τη Σύμβαση της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU) το Δίκαιο του Διαστήματος αντίστοιχα.

Καταστατικός Χάρτης και η Σύμβαση της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU)

Από τα συγκεκριμένα κείμενα απορρέει η γενική υποχρέωση των κρατών – μελών να διασφαλίζουν ότι η λειτουργία όλων των τηλεπικοινωνιακών τους δικτύων θα πραγματοποιείται με τέτοιο τρόπο ώστε να μην δημιουργούνται επιβλαβείς παρενοχλήσεις στη λειτουργία των αντίστοιχων δικτύων των άλλων κρατών μελών και επίσης να ενεργούν κατάλληλα για την καταστολή της μετάδοσης ή της θέσης σε κυκλοφορία ψευδών ή απατηλών σημάτων κινδύνου, έκτακτης ανάγκης, ασφάλειας ή ταυτότητας και να συνεργάζονται για τον εντοπισμό και την αναγνώριση των υπό τη δικαιοδοσία τους σταθμών, που εκπέμπουν τέτοια σήματα[B32].

Με δεδομένο ότι οι ανωτέρω συμβατικές υποχρεώσεις αφορούν στο σύνολο των τηλεπικοινωνιακών δικτύων, χωρίς να υφίσταται κάποια διάκριση βάσει των αναγκών, που αυτά εξυπηρετούν, καταλαμβάνουν και τα δίκτυα, που χρησιμοποιούνται για στρατιωτικούς σκοπούς και στα οποία μπορεί να στοχεύσει μια κυβερνοεπίθεση, με αποτέλεσμα να προστατεύονται τα δίκτυα αυτά σε καιρό ειρήνης[B18]. Ωστόσο, δεν ισχύει η σχετική κάλυψη στην περίπτωση, που η κυβερνοεπίθεση έχει τέτοιο χαρακτήρα και ένταση, ώστε να εξομοιώνεται με χρήση βίας ή όταν αυτή λαμβάνει χώρα κατά τη διάρκεια ανταλλαγής πραγματικών πολεμικών πυρών.

Δίκαιο του Διαστήματος

Η Συνθήκη του Διαστήματος, που αποτελεί τον ακρογωνιαίο λίθο του Δικαίου τους Διαστήματος, υποχρεώνει τα κράτη να δραστηριοποιούνται στο μόνο για ειρηνικούς σκοπούς και να απέχουν από την άσκηση βίας. Εάν για την εκτέλεση μιας κυβερνοεπίθεσης χρησιμοποιηθεί επί παραδείγματι κάποιος δορυφόρος, τότε ενδεχομένως να είναι εφαρμόσιμες οι διατάξεις της ανωτέρω Συνθήκης[B19].

ΚΕΦΑΛΑΙΟ 8 ΜΗ ΚΡΑΤΙΚΟΙ ΔΡΩΝΤΕΣ ΚΑΙ ΚΡΑΤΗ

8.1 Μη Κρατικοί Δρώντες (Non State Actors)

Όπως έχει προαναφερθεί, ο κυβερνοπόλεμος διεξάγεται από τα κράτη αλλά και από ανεπίσημα διορισμένους ή υποστηριζόμενους από αυτά μη κρατικούς δρώντες. Μέσω αυτών, τα κράτη μπορούν να διεξάγουν έμμεσα κυβερνοεπιθέσεις, χωρίς να διαφαίνεται άμεσα η σύνδεσή τους με τους δράστες των επιθέσεων και συνεπώς να έχουν τη δυνατότητα της εύλογης άρνησης για την επίθεση. Οι μη κρατικοί δρώντες, που χρησιμοποιούνται από τα κράτη για να διεξάγουν κυβερνοεπιθέσεις εμφανίζονται στη διεθνή βιβλιογραφία ως «Cyber Militias» (κυβερνοπολιτοφύλακες). Ουσιαστικά, πρόκειται για ομάδες ατόμων, οι οποίες ανεξαρτήτως του βαθμού ειδίκευσης που έχουν στην τεχνολογία πληροφορικής, είναι πρόθυμες να διεξάγουν κυβερνοεπιθέσεις προκειμένου να πετύχουν ένα συγκεκριμένο πολιτικό σκοπό[B31]. Πρέπει να σημειωθεί, ότι η διασύνδεση ενός κράτους με ομάδες μη κρατικών δρώντων 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 αυτών των ομάδων. Επιπλέον, αξίζει να αναφερθεί, ότι οι Cyber Militias δύναται να διεξάγουν τις επιθέσεις τους στον κυβερνοχώρο, χωρίς κατά ανάγκη αυτό να είναι απόρροια μιας άμεσης ή έμμεσης κυβερνητικής εντολής. Σε αυτήν όμως την περίπτωση, οι ενέργειές τους δεν εντάσσονται στον κυβερνοπόλεμο, αλλά στις άλλες κατηγορίες κυβερνοσυγκρούσεων, που έχουν αναφερθεί σε προηγούμενο κεφάλαιο με βάση τον αντικειμενικό σκοπό των επιθέσεων.

Το 1998 θεωρείται η χρονιά, όπου καταγράφηκε για πρώτη φορά η δράση μιας ομάδας κυβερνοπολιτοφυλακής, γνωστή και ως Zapatistas, η οποία ήταν μια αριστερή εθνικοαπελευθερωτική ομάδα του Μεξικό και δραστηριοποιήθηκε στον κυβερνοχώρο με τη συνδρομή ευρωπαίων hackers, εξαπολύοντας κυβερνοεπιθέσεις κατά της μεξικανικής αστυνομίας, των ΗΠΑ και του χρηματιστηρίου της Φρανκφούρτης.

Οι κυβερνοπολιτοφύλακες χαρακτηρίζονται από τρία βασικά μοντέλα οργάνωσης, σύμφωνα με τις παρατηρήσεις από τον τρόπο δράσης τους μέχρι σήμερα. Στην πραγματικότητα μια κυβερνοπολιτοφυλακή μπορεί να έχει στοιχεία και από τα τρία μοντέλα οργάνωσης. Τα μοντέλα αυτά είναι τα παρακάτω[B31]:

- Το Φόρουμ (Forum)[B31]

Πρόκειται για ομάδα μη κρατικών δρώντων, 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

οδηγίες επίθεσης, επιθετικά εργαλεία και προπαγανδιστικό υλικό. Επειδή, δημιουργείται ως απάντηση σε κάποιο γεγονός, συνήθως διαλύεται με το πέρας αυτού του γεγονότος, ωστόσο μπορεί να διατηρεί κάποια μόνιμα μέλη.

Βασικό του πλεονέκτημα είναι ότι δύναται να συγκροτηθεί σε μικρό χρονικό διάστημα και να αναλάβει δράση άμεσα. Επιπλέον, η ποικιλομορφία, που εμφανίζει, σχετικά με τα μέλη που το απαρτίζουν, δημιουργεί προβλήματα στους αμυνόμενους, καθώς δυσκολεύονται να αναλύσουν και να αντιμετωπίσουν τις κυβερνοαπειλές.

Το βασικό του μειονέκτημα εστιάζει στη χαλαρότητα του δικτύου των μελών του, καθώς δεν υπάρχει συμπαγής διοίκηση και έλεγχος. Πρακτικά, κάθε μέλος μπορεί να δράσει αυτόνομα, χωρίς να ακολουθήσει τις κεντρικές κατευθυντήριες αρχές, με συνέπεια να υπάρξει επέκταση της σύγκρουσης. Επιπλέον, σε αυτό το είδος μοντέλου συγκεντρώνονται μέλη περιορισμένων γνώσεων αναφορικά με τη διεξαγωγή κυβερνοεπιθέσεων με αποτέλεσμα να επηρεάζεται αρνητικά η επιχειρησιακή αποτελεσματικότητά του.

- Το Κελί (Cell)[B31]

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, 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.

Ως βασικό πλεονέκτημα παρουσιάζει τη δυνατότητα άμεσης κινητοποίησης, καθώς τα μέλη του γνωρίζονται μεταξύ τους. Επειδή η διαδικασία αποδοχής ενός νέου μέλους είναι πολύ προσεκτική, η πιθανότητα διείσδυσης σε αυτό από τρίτους είναι αρκετά μικρή. Επιπλέον, 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 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 εκ των μελών του Cell από τις διωκτικές αρχές, δύναται να οδηγήσει στην αποκάλυψη των ταυτοτήτων και των υπολοίπων μελών.

Παράλληλα, πολλές φορές οι hackers στην προσπάθειά τους να αποκτήσουν φήμη στο ευρύ κοινό αφήνουν σκοπίμως ίχνη για την επίθεση που διέπραξαν με αποτέλεσμα η δημοσιότητα αυτή να λειτουργήσει αρνητικά τόσο για τους hackers όσο και για το Cell, στο οποίο ανήκουν, δεχόμενοι έντονες επικρίσεις.

- Η Ιεραρχία (Hierarchy)[B31]

Σύμφωνα και με την ονομασία, σε αυτό το μοντέλο οργάνωσης υπάρχει 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. Όπως στο στρατό κάθε υποομάδα έχει διακριτό ρόλο. Η συμμετοχή σε αυτό το μοντέλο οργάνωσης μπορεί να είναι είτε συνολικά ανώνυμη είτε συνολικά επώνυμη, χωρίς αυτό να σημαίνει ότι οι ταυτότητες των μελών είναι γνωστές σε τρίτα πρόσωπα.

Βασικό πλεονέκτημα της Hierarchy είναι το γεγονός ότι στην περίπτωση που υποστηρίζεται από ένα κράτος, τότε θα διαθέτει ικανούς πόρους για τη διεξαγωγή πιο εξειδικευμένων δραστηριοτήτων στον κυβερνοχώρο, ενώ θα έχει παράλληλα τη συνδρομή και άλλων κρατικών υπηρεσιών, όπως μυστικές υπηρεσίες, προσδίδοντάς της συγκριτική υπεροχή σε σχέση με τα δύο προαναφερθέντα μοντέλα οργάνωσης. Επιπλέον, η ύπαρξη ενός ιεραρχημένου μοντέλου οργάνωσης συνεπάγεται την καλύτερη διοίκηση και έλεγχο με αποτέλεσμα τη μεγαλύτερη διάρκεια επιχειρησιακής ζωής μιας τέτοιας ομάδας hackers.

Ως μειονέκτημα αυτού του μοντέλου θα μπορούσε να θεωρηθεί το γεγονός ότι η ιεραρχική οργάνωση και δομή μπορεί να σημαίνει μικρότερη ευελιξία και δυνατότητα μεγέθυνσης της ομάδας. Επίσης, υπάρχει ο κίνδυνος να εμφανιστεί στο εσωτερικό της ομάδας η παθογένεια, που αφορά στην μανιώδη επιδίωξη κατάληψης των ηγετικών θέσεων της ομάδας από κάποια μέλη, αλλά και δυσλειτουργία της ομάδας σε περίπτωση, που ουδετεροποιηθούν οι προσωπικότητες – κλειδιά. Επιπλέον, τέτοιου είδους ομάδες hackers ταυτίζονται με συγκεκριμένα κράτη, με αποτέλεσμα αυτά να χάνουν το πλεονέκτημα της ανωνυμίας στον κυβερνοχώρο.

Όσον αφορά τις δυνατότητες, που μπορούν να αναπτύξουν οι ομάδες μη κρατικών δρώντων, εξαρτώνται αναλογικά από την εξειδίκευση των μελών τους στην IT τεχνολογία αλλά και από τους πόρους, που έχουν στη διάθεσή τους. Σε γενικές γραμμές, οι δυνατότητες τους αφορούν είτε επιθετικές δραστηριότητες στον κυβερνοχώρο είτε συμμετοχή σε υπηρεσίες υποστήριξης κατά τη διάρκεια μιας εκστρατείας στον κυβερνοχώρο.

Οι βασικές επιθετικές τους δραστηριότητες συνοψίζονται σε[B31]:

- ✓ Αυτόματες και μη αυτόματες DoS κυβερνοεπιθέσεις.
- ✓ Μη εξουσιοδοτημένες αλλαγές του περιεχομένου των ιστοσελίδων (Web Defacement).
- ✓ Αποστολή μέσω email κακόβουλου λογισμικού (malware).
- ✓ Συλλογή πληροφοριών για τις δυνατότητες του αντιπάλου.

Οι υποστηρικτικές δραστηριότητες συνοψίζονται σε[B31]:

- ✓ Προπαγάνδα και στρατολόγηση.
- ✓ Οικονομικές δωρεές ή παροχή πρόσβασης σε δίκτυα Η/Υ, τα οποία στη συνέχεια θα χρησιμοποιηθούν ως στοιχεία ενός Botnet (π.χ. ένας «ερασιτέχνης» δίνει τους κωδικούς διαχειριστή δικτύου Η/Υ μιας εταιρείας σε έναν εξειδικευμένο hacker).
- ✓ Αναμετάδοση οδηγιών κυβερνοεπιθέσεων.
- ✓ Παροχή πληροφοριών στοχοποίησης, ιδιαίτερα αν ο στόχος βρίσκεται σε μια ξένη χώρα και ο «ερασιτέχνης» γνωρίζει τη γλώσσα της ή πληροφορίες για αυτήν τη χώρα.
- ✓ 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 στη χώρα – στόχο.

8.2 Κράτη και Κυβερνοπόλεμος

Σύμφωνα με έρευνα της εταιρείας McAfee, το 2008, υπάρχουν περισσότερες από 120 χώρες, που χρησιμοποιούν το Internet για δραστηριότητες κατασκοπείας σε πολιτικό, στρατιωτικό και οικονομικό επίπεδο. Επιπλέον, σε μια πιο πρόσφατη έρευνα του Κέντρου Στρατηγικών και Διεθνών Σπουδών, η οποία στηρίχτηκε σε στοιχεία που προήλθαν από ανοικτές πηγές, ελέχθησαν 133 χώρες σχετικά με την ύπαρξη στρατιωτικού δόγματος ή πολιτικής που να πλαισιώνουν τις δραστηριότητες τους στον κυβερνοχώρο[B20]. Από την εν λόγω έρευνα διαπιστώθηκε ότι υπάρχουν 33 χώρες που έχουν στο στρατιωτικό σχεδιασμό ή την οργάνωση τους την έννοια του κυβερνοπολέμου (π.χ. Κίνα, Ρωσία, ΗΠΑ, Ισραήλ, Β. Κορέα, Ιράν κ.α.), ενώ σε άλλες 36 χώρες υπάρχουν μη στρατιωτικές υπηρεσίες, οι οποίες είναι υπεύθυνες για την κυβερνοασφάλεια (Ιαπωνίας, Λιθουανία, Σουηδία, ΗΑΕ κ.α.).

Σύμφωνα με αναλύσεις, πάνω από 100 χώρες παγκοσμίως διαθέτουν σήμερα εξειδικευμένες μονάδες, υπεύθυνες για τη διεξαγωγή επιχειρήσεων κυβερνοπολέμου. Ανάμεσα στις πλέον «δραστήριες» εμφανίζονται η Κίνα, η Ρωσία, οι ΗΠΑ, το Ισραήλ, η Β.

Κορέα και το Ιράν. Αυτές οι χώρες θεωρείται ότι έχουν ιδιαίτερες επιθετικές ικανότητες στον κυβερνοπόλεμο, τις οποίες έχουν εκδηλώσει κατά καιρούς με τη συμμετοχή τους σε διάφορα συμβάντα κυβερνοεπιθέσεων. Στη συνέχεια θα παρατεθεί μια περιγραφή των δυνατοτήτων αυτών των χωρών στο πεδίο του κυβερνοπολέμου, καθώς και αναφορά στη συμμετοχή τους σε διάφορες περιπτώσεις κυβερνοεπιθέσεων, που απασχόλησαν τη διεθνή κοινότητα[B21].

Κίνα

Η περίπτωση της Κίνας παρουσιάζει ιδιαίτερο ενδιαφέρον αναφορικά με τον τρόπο που αντιμετωπίζει τον κυβερνοχώρο και το κυβερνοπόλεμο. Η Κίνα αφυπνίστηκε κατά τη διάρκεια του 1ου πολέμου στον Περσικό Κόλπο, όταν διαπίστωσε την εύκολη ήττα του Ιράκ από τους συμμάχους. Αξίζει να σημειωθεί πως την περίοδο εκείνη το Ιράκ διέθετε τον 4ο σε μέγεθος στρατό, εξοπλισμένο με ρώσικα και κινέζικα οπλικά συστήματα. Η εκτεταμένη χρήση του αεροπορικού όπλου, των συστημάτων Διοίκησης και Ελέγχου, των Η/Υ αλλά και των έξυπνων βομβών κατά τη διάρκεια των επιχειρήσεων της Desert Storm ώθησε την Κίνα να κινηθεί προς την κατεύθυνση ανεύρεσης νέας στρατηγικής, η οποία θα μπορούσε να ακυρώσει τη νικηφόρα στρατηγική των ΗΠΑ και των συμμάχων τους[B7].

Από τα μέσα της δεκαετίας του 1990 η Κίνα κατανόησε πως η αριθμητική υπεροχή της σε ανθρώπινο δυναμικό ή σε συμβατικό εξοπλισμό έναντι των ΗΠΑ δεν θα επέφερε το επιδιωκόμενο νικηφόρο αποτέλεσμα σε έναν ενδεχόμενο πόλεμο. Έτσι, περιόρισε το μέγεθος των στρατιωτικών της δυνάμεων, επένδυσε περισσότερο σε νέες τεχνολογίες (π.χ. τεχνολογίες πληροφορικής) και άρχισε να προσεγγίζει τις διακρατικές συγκρούσεις, δίνοντας ιδιαίτερη βαρύτητα στις έννοιες του Πληροφοριακού Πολέμου και του Κυβερνοπολέμου. Με βάση αυτά, η Κίνα προχώρησε στην υλοποίηση κάποιων κινήσεων προς αυτήν την κατεύθυνση. Πιο συγκεκριμένα, οι ενέργειές της σχετίζονταν με τα παρακάτω[B7]:

- Διατύπωση στρατιωτικού δόγματος για τον κυβερνοπόλεμο.
- Στρατολόγηση hackers και συνεργασία με ομάδες μη κρατικών δρώντων.
- Εκπαίδευση κινέζων αξιωματικών στον κυβερνοπόλεμο.
- Ανάπτυξη εγχώριων δυνατοτήτων σε τεχνολογία πληροφορικής.
- Έλεγχος κινέζικου δικτύου από το κράτος.

Όσον αφορά την εμπλοκή της σε κάποια περίπτωση κυβερνοεπίθεσης, μέχρι σήμερα δεν έχει εμπλακεί φανερά σε επιχειρήσεις κυβερνοπολέμου, αν και κατέχει την πρώτη θέση σε επιχειρήσεις κυβερνοκατασκοπείας. Ωστόσο, έχουν καταγραφεί περιπτώσεις όπου κινεζικές ομάδες hackers έχουν εμπλακεί σε κυβερνοαψιμαχίες με άλλα κράτη, υπό την ανοχή του κινέζικου κράτους. Πιο συγκεκριμένα, μετά το βομβαρδισμό της κινέζικης πρεσβείας στη Γιουγκοσλαβία από το ΝΑΤΟ το 1999, ομάδες Κινέζων hackers

πραγματοποίησαν επιθέσεις DDoS κατά αμερικανικών και νατοϊκών ιστοσελίδων. Συμμαχικές κυβερνητικές υπηρεσίες δέχθηκαν βομβαρδισμό ηλεκτρονικών μηνυμάτων, νατοϊκές ιστοσελίδες τροποποιήθηκαν χωρίς εξουσιοδότηση , ενώ άλλες σταμάτησαν να λειτουργούν. Επίσης, όταν τον Απρίλιο του 2001 ένα αμερικάνικο κατασκοπευτικό αεροσκάφος EP-3, το οποίο σύμφωνα με την Κίνα είχε παραβιάσει το κινέζικο FIR, υποχρεώθηκε από κινέζικα μαχητικά αεροσκάφη σε αναγκαστική προσγείωση, η κινέζικη ομάδα hacker «Honker Union» εξαπέλυσε DDoS κυβερνοεπιθέσεις κατά αμερικανικών στρατιωτικών ιστοσελίδων[B7].

Ρωσία

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. 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. Οι Ρώσοι αξιωματούχοι διακατέχονταν από 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 ανεπτυγμένες δυνατότητες των ΗΠΑ στον κυβερνοπόλεμο έδωσε σημαντική ώθηση στη δημιουργία κατάλληλου ρώσικου δόγματος για τις επιχειρήσεις στον κυβερνοχώρο και για την ανάπτυξη των ρωσικών δυνατοτήτων στο εν λόγω πεδίο[B8].

Αρχικά, οι ρώσικες προσπάθειες για τη δημιουργία δόγματος στράφηκαν προς την αναγκαιότητα χρήσης του Internet για σκοπούς προπαγάνδας, παρακολούθησης των πολιτικών αντιπάλων και για άσκηση λογοκρισίας στους αντικαθεστωτικούς. Στη συνέχεια, όμως, δόθηκε βαρύτητα στην ανάπτυξη κυβερνοόπλων και τη χρήση τους από τις ΕΔ και τις μυστικές υπηρεσίες[B7]. Οι ρώσικες ΕΔ και οι μυστικές υπηρεσίες συνεργάστηκαν με ειδικούς στην τεχνολογία της πληροφορικής και με την ακαδημαϊκή κοινότητα, προκειμένου η Ρωσία να δημιουργήσει ένα δόγμα για τον κυβερνοπόλεμο, αλά και για να αναπτύξει επιθετικές και αμυντικές δυνατότητες στον κυβερνοχώρο. Παράλληλα, η επίτευξη κυβερνοασφάλειας αποτέλεσε ύψιστη προτεραιότητα για τις ρωσικές μυστικές υπηρεσίες, οι οποίες το 1999 απέκτησαν αρμόδια διεύθυνση για την πληροφοριακή ασφάλεια και την ασφάλεια των Η/Υ.

Το σύγχρονο ρωσικό στρατιωτικό δόγμα, που γνωστοποιήθηκε στο ευρύ κοινό το Φεβρουάριο του 2010 θεωρεί ότι χαρακτηριστικό των μελλοντικών συγκρούσεων θα είναι η έγκαιρη ενεργοποίηση των δυνατοτήτων του πληροφοριακού πολέμου μιας χώρας. Για το λόγο αυτό, οι ρώσικες ΕΔ θα πρέπει να έχουν πληροφοριακές δυνατότητες, να αναπτύξουν

πληροφοριακά όπλα ακριβείας και να στοχεύσουν στην επίτευξη της πληροφοριακής υπεροχής[B7].

Οι περιπτώσεις κυβερνοεπιθέσεων που έχουν καταλογιστεί στη ρωσική πλευρά είναι αρκετές. Η πρώτη αναφέρεται με την ονομασία «Cuckoo's Egg» και αφορά στις προσπάθειες κυβερνοκατασκοπείας που εκδήλωσε ένας Ανατολικογερμανός hacker το 1985, προκειμένου να συλλέξει στοιχεία για το αμερικάνικο πρόγραμμα «Star Wars» προς όφελος της σοβιετικής KGB. Μια παρόμοια υπόθεση φέρει την ονομασία «Moonlight Maze» και αφορά στην υπεξαίρεση δεδομένων από τη NASA, το αμερικάνικο Πεντάγωνο, το Υπουργείο Ενέργειας, καθώς και διάφορα πανεπιστήμια και ερευνητικά κέντρα. 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., χωρίς όμως η Ρωσία να αποδέχεται ποτέ τις κατηγορίες.

Εκτός όμως, από τις υποθέσεις κυβερνοκατασκοπείας, η Ρωσία εμπλέκεται σε περιπτώσεις κυβερνοεπιθέσεων DDoS. Οι πλέον γνωστές περιπτώσεις αφορούν στα γεγονότα που έλαβαν χώρα στην Εσθονία το 2007 και στη Γεωργία το 2008. Άλλες τέτοιου είδους επιθέσεις σημειώθηκαν τον Οκτώβριο του 2002 κατά ιστοσελίδων των Τσετσένων αυτονομιστών, με θύτη τη ρώσικη FSB, οι οποίες αποσκοπούσαν στην εξουδετέρωση των Τσετσένων αυτονομιστών[B9], ώστε να μην μπορέσουν να δημοσιοποιήσουν οπτικό υλικό από τη ρωσική επιχείρηση στο διαδίκτυο.

Παρόμοια επιθετική ενέργεια εικάζεται ότι διενεργήθηκε στις 18 Ιανουαρίου του 2009 από Ρώσους κατά 2 τουλάχιστον εταιρειών παροχής υπηρεσιών Internet στο Κιργιστάν, με αποτέλεσμα οι πολίτες να χάσουν επαφή με τα γεγονότα εν μέσω πολιτικών αναταραχών στη χώρα τους. Αυτή η κίνηση αποσκοπούσε στην άσκηση πίεσης προς την κυβέρνηση του Κιργιστάν, προκειμένου το κράτος να μην επεκτείνει την περίοδο παραμονής των αμερικανικών στρατευμάτων στην αεροπορική βάση «Manas Air Base». Αποτέλεσμα αυτού ήταν στις 3 Φεβρουαρίου ο Πρόεδρος του Κιργιστάν να ανακοινώσει πως τα αμερικανικά στρατεύματα θα αποχωρήσουν από τη χώρα του, σπεύδοντας παράλληλα η Ρωσία σε παροχή οικονομικής βοήθειας 150 εκατομμυρίων δολαρίων και σε διάθεση δανείου ύψους 2 δις δολαρίων προς το Κιργιστάν[B9].

ΗΠΑ

Σύμφωνα με πολλούς αναλυτές, οι ΗΠΑ κρατούν τα σκήπτρα παγκοσμίως σχετικά με τις επιθέσεις στον κυβερνοχώρο. Το ζήτημα της ασφάλειας στον κυβερνοχώρο απασχόλησε

τους Αμερικανούς από τις αρχές της δεκαετίας του 1990, καθώς αποτέλεσαν τους πρωτοπόρους στη χρήση Η/Υ και δικτύων Η/Υ σε στρατιωτικές και μη εφαρμογές[Γ7].

Μετά το συμβάν του 2008, όπου τα διαβαθμισμένα και αδιαβάθμητα δίκτυα του αμερικάνικου Πενταγώνου έπεσαν θύμα ξένων hackers και απώλεσαν τεράστιο όγκο δεδομένων, οι ΗΠΑ έλαβαν πιο δραστικά μέτρα για την ασφάλεια στον κυβερνοχώρο. Αξίζει να σημειωθεί πως ο Πρόεδρος Obama χαρακτήρισε το 2009 τον κυβερνοχώρο ως στρατηγικό περιουσιακό στοιχείο των ΗΠΑ, το οποίο πρέπει να προστατευθεί με κάθε μέσο. Σε συνέχεια των δηλώσεων Obama, τον Ιούνιο του 2009, δημιουργείται μια νέα διακλαδική διοίκηση με την ονομασία USCYBERCOM (Cyber Command), υπό τη διοίκηση της αμερικανικής Στρατηγικής Διοίκησης. Σκοπός της USCYBERCOM θα ήταν η προστασία των δικτύων των αμερικανικών ΕΔ, η υποστήριξη στρατιωτικών αποστολών και αποστολών καταπολέμησης της τρομοκρατίας μέσα από τον κυβερνοχώρο και η συνεργασία με άλλους κυβερνητικούς φορείς, συμμάχους και ιδιωτικές επιχειρήσεις σε θέματα κυβερνοασφάλειας[Β15]. Παράλληλα, το Σεπτέμβριο του 2010 υπογράφτηκε Μνημόνιο Συνεργασίας μεταξύ του DoD και του DHS, , το οποίο αφορούσε στη συνεργασία των δύο Υπουργείων σε θέματα κυβερνοασφάλειας, με σκοπό να επιτευχθεί η βέλτιστη ανταπόκριση από την ομοσπονδιακή κυβέρνηση των ΗΠΑ σε κυβερνοαπειλές κατά των ιδιωτικών και κυβερνητικών δικτύων Η/Υ της χώρας.

Πέρα από τις θεσμικές προβλέψεις για τη διασφάλιση των επιχειρήσεων τους στον κυβερνοχώρο, οι ΗΠΑ έχουν δαπανήσει τα τελευταία χρόνια τεράστια ποσά για την ανάπτυξη των δυνατοτήτων τους στον κυβερνοχώρο. Σημαντικό ρόλο στην ανάπτυξη των αμερικάνικων δυνατοτήτων στον κυβερνοχώρο έχουν διαδραματίσει τα αμερικανικά πανεπιστήμια, το Υπουργείο Ενέργειας και η DARPA (Defence Advanced Research Project Agency), η οποία έχει προβεί στη δημιουργία ενός πεδίου ελέγχου και εφαρμογής των αμερικανικών κυβερνοόπλων[Γ7]. Επιπρόσθετα, αξίζει να αναφερθεί το γεγονός πως οι ΗΠΑ από το 1997 διεξάγουν σε τακτική βάση πληθώρα ασκήσεων κυβερνοπολέμου με αυξημένα επίπεδα δυσκολίας κάθε έτος όπως χαρακτηριστικά οι ασκήσεις Eligible Receiver, Cyber Storm, Schriever Wargame κ.α.

Σύμφωνα με έκθεση της εταιρείας McAfee το 2010, οι ΗΠΑ χαρακτηρίζονται ιδιαίτερα ευάλωτες στις κυβερνοεπιθέσεις, αλλά ταυτόχρονα αποτελούν και την κύρια πηγή κυβερνοεπιθέσεων, με δεύτερη χώρα κατά σειρά την Κίνα. Ωστόσο, με εξαίρεση την υπόθεση Stuxnet, οι ΗΠΑ δεν έχουν αφήσει αρκετά δείγματα των κυβερνοεπιθέσεων τους, χωρίς αυτό να σημαίνει ότι δεν διεξάγουν κυβερνοεπιθέσεις, αντιθέτως εύκολα μπορούμε να ερμηνεύσουμε το γεγονός αυτό ότι διενεργούν κυβερνοεπιθέσεις, καλύπτοντας με απόλυτη επιτυχία τα ηλεκτρονικά τους ίχνη[Β7].

Όσον αφορά της περιπτώσεις εμπλοκής των ΗΠΑ σε κυβερνοεπιθέσεις, αρχικά οι Αμερικανοί σχεδίαζαν κατά τη διάρκεια του Α' πολέμου στον Περσικό Κόλπο να χρησιμοποιήσουν μεθόδους κυβερνοπολέμου για να καταστείλουν την ιρακινή αεράμυνα, πριν την έναρξη των αεροπορικών βομβαρδισμών[Γ7]. Ωστόσο, το σχέδιο δεν εγκρίθηκε γιατί θεωρήθηκε άκρως επικίνδυνο και με μικρά ποσοστά επιτυχίας, καταφεύγοντας στη χρήση αεροπορικών βομβαρδισμών των ιρακινών ραντάρ και των θέσεων των πυραύλων εδάφους – αέρος.

Μετά από 13 χρόνια στον Β' πόλεμο στον Περσικό Κόλπο πραγματοποιήθηκε ότι είχε σχεδιαστεί για τον Α' πόλεμο. Πιο συγκεκριμένα, 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 παραδοθούν. Παράλληλα, την εποχή εκείνη είχε προταθεί στη στρατιωτική ηγεσία η διεξαγωγή κυβερνοεπιθέσεων κατά των τραπεζικών λογαριασμών του Saddam Hussein σε τράπεζες του Ιράκ και άλλων χωρών, κάτι το οποίο δεν εγκρίθηκε τελικά, καθώς μια τέτοια κίνηση θα αποτελούσε παραβίαση του διεθνούς δικαίου, ενώ δεν θα μπορούσαν να προβλεφθούν τυχόν παράπλευρες απώλειες. Το 2011, κατά τη διάρκεια της επιχείρησης «Unified Protector», οι ΗΠΑ αποφάσισαν να μην διενεργήσουν κυβερνοεπιθέσεις κατά της λιβυκής αεράμυνας, υπό το φόβο δημιουργίας προηγούμενο, το οποίο θα εκμεταλλεύονταν η Ρωσία και η Κίνα, ενώ υπήρχε περίπτωση να αποκαλυφθεί σε τρίτους η μεθοδολογία διενέργειας των αμερικανικών κυβερνοεπιθέσεων[Β42].

Από την άλλη μεριά, οι ΗΠΑ ήταν αρκετές φορές και δέκτες κυβερνοεπιθέσεων, οι οποίες φημολογείται ότι οφείλονται σε ανταγωνιστικές δυνάμεις όπως η Ρωσία (π.χ. περίπτωση Moonlight Maze) ή η Κίνα (π.χ. περίπτωση με F-35). Από τις πλέον σημαντικές κυβερνοεπιθέσεις, που έχουν δεχτεί οι ΗΠΑ, είναι η παραβίαση των δικτύων Η/Υ του αμερικανικού Πενταγώνου το 2008, με αποτέλεσμα να υποκλαπούν σημαντικά δεδομένα για την αμερικανική άμυνα. Κατόπιν σχετικής έρευνας, η παραβίαση των δικτύων προήλθε από μια φορητή μνήμη (flash drive), η οποία τοποθετήθηκε σε ένα αμερικανικό στρατιωτικό laptop στη Μέση Ανατολή., διαδίδοντας κακόβουλο λογισμικό στο δίκτυο της US Central Command κα εν συνεχεία στα υπόλοιπα δίκτυα του αμερικανικού DoD. Αποτέλεσμα αυτής της κυβερνοεπίθεσης ήταν να γνωστοποιηθούν σε αναρμόδια πρόσωπα σχέδια οπλικών συστημάτων, επιχειρησιακά σχέδια δράσης και στοιχεία επιτήρησης.

Μια εξίσου σημαντική περίπτωση κυβερνοεπίθεσης που δέχθηκαν οι ΗΠΑ αφορά στα μη επανδρωμένα αεροσκάφη (UAVs), που διαθέτει και έλαβε χώρα το Σεπτέμβριο του 2011. Πιο συγκεκριμένα, ένας ιός Η/Υ 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. Ως αποτέλεσμα, απωλέστηκαν απόρρητα στοιχεία και δεδομένα. Πιθανολογείται, ότι, ο ιός διείσδυσε από φορητή μνήμη καθώς με αυτόν τον τρόπο γίνονται οι ενημερώσεις των ψηφιακών χαρτών που χρησιμοποιούν οι σταθμοί εδάφους, οι οποίοι ελέγχουν τις πτήσεις των UAVs, αλλά και οι μεταφορές των καταγραφών βίντεο μεταξύ των Η/Υ.

Ισραήλ

Είναι γεγονός πως δεν υπάρχουν πολλές αναφορές σε ανοιχτές πηγές σχετικά με τη στρατηγική και το δόγμα κυβερνοασφάλειας του Ισραήλ, ωστόσο τα υπάρχοντα στοιχεία καταδεικνύουν ότι διαθέτει ιδιαίτερα αναπτυγμένες επιθετικές δυνατότητες στον κυβερνοπόλεμο.

Από τα διαθέσιμα στοιχεία αναφορικά με τις δυνατότητες του Ισραήλ στον κυβερνοχώρο προκύπτει ότι οι επιθετικές και αμυντικές δυνατότητες κυβερνοπολέμου και η κυβερνοκατασκοπεία ασκούνται από τέσσερις διαφορετικούς φορείς στη χώρα και οι οποίοι είναι:

- Η Μονάδα 8200 των IDF (ισραηλινών ΕΔ).
- Η υπηρεσία εσωτερικής ασφάλειας Shin Bet.
- Το Σώμα C^4I των ισραηλινών ΕΔ.
- Κρατική υπηρεσία με ονομασία National Cybernetic Taskforce.

Από τις αρχές του 21ου αι. το Ισραήλ έχει εμπλακεί σε μια πληθώρα επιχειρήσεων στον κυβερνοχώρο. Πιο 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. Ως απάντηση, οι Παλαιστίνιοι hackers στοχοποίησαν ισραηλινές πολιτικές και στρατιωτικές ιστοσελίδες, τηλεπικοινωνιακούς φορείς και ΜΜΕ του Ισραήλ, καθώς και ισραηλινές τράπεζες. Το 2006 και ενώ η ένταση μεταξύ του Ισραήλ και της Παλαιστίνης σε πολιτικό επίπεδο είχε αυξηθεί, οι Παλαιστίνιοι hackers κατόρθωσαν να θέσουν εκτός λειτουργίας μεγάλο αριθμό ισραηλινών ιστοσελίδων, συμπεριλαμβανομένων τραπεζών και ιδιωτικών εταιρειών, προκαλώντας ισχυρό αρνητικό αντίκτυπο στο Ισραήλ. Τέλος, το 2009, κατά τη διάρκεια της ισραηλινής επιχείρησης Cast Lead στη λωρίδα της Γάζας, έλαβαν χώρα κυβερνοαψιμαχίες μεταξύ Ισραηλινών και Παλαιστίνιων hackers, οι οποίοι επιδόθηκαν σε επιθέσεις web defacement και DDoS. Παρ' όλα αυτά, σημαντικότερη κυβερνοεπίθεση που δέχθηκε το

Ισραήλ ήταν από Παλαιστίνιους hackers κατά του ισραηλινού τηλεπικοινωνιακού δορυφόρου Amos-3.

Επιπρόσθετα, το Σεπτέμβριο του 2007, οι ισραηλινές ΕΔ (IDF) επιχείρησαν επιτυχώς αεροπορικό βομβαρδισμό συριακών εγκαταστάσεων στην περιοχή Dayr az-Zawr, καθώς γνώριζαν από τις υπηρεσίες πληροφοριών των ΗΠΑ και του Ισραήλ, ότι εκεί οι Σύριοι ετοίμαζαν παράνομα πυρηνικό εργοστάσιο με τη συνεργασία της Β. Κορέας. Η ιδιαιτερότητα αυτής της υπόθεσης έγκειται στο γεγονός ότι τα ισραηλινά μαχητικά αεροσκάφη δεν έγιναν αντιληπτά από τη συριακή αεράμυνα, καθώς τα επίγεια ραντάρ είχαν «τυφλωθεί» κατόπιν κυβερνοεπιθέσεων.

Β. Κορέα

Η Βόρεια Κορέα είναι μια χώρα, που εξαρτάται σε μεγάλο βαθμό από την εξωτερική οικονομία και τεχνική βοήθεια αλλά και από το παράνομο εμπόριο. Λόγω του περιορισμένου αποθέματος σε φυσικούς πόρους και των ελάχιστων αναπτυξιακών υποδομών σε συνδυασμό με το μικρό ΑΕΠ, η Β. Κορέα βρίσκεται σε μειονεκτική θέση στο διεθνές σύστημα. Από τις αρχές της δεκαετίας του 1990, η ηγεσία της χώρας στην προσπάθειά της να αντιστρέψει αυτήν την κατάσταση έδωσε ιδιαίτερη βαρύτητα στην ανάπτυξη βαλλιστικών πυραύλων, πυρηνικών όπλων και δυνατοτήτων κυβερνοπολέμου. Χαρακτηριστικά, αναφέρεται ότι από το 2000 η ηγεσία της χώρας είχε αναπτύξει ένα εσωτερικό δίκτυο (Intranet), μέσω του οποίου οι «προνομιούχοι» είχαν πρόσβαση σε ενημερωτικό υλικό, το οποίο όμως ήταν απόλυτα ελεγχόμενο από το κράτος[B41].

Όσον αφορά στον κυβερνοπόλεμο, η Β. Κορέα θεωρείται ότι δαπανά υπέρογκα χρηματικά ποσά για την ανάπτυξη επιθετικών δυνατοτήτων, χωρίς ωστόσο να υπάρχουν επίσημα στοιχεία γι' αυτό. Οι επιθετικές δυνατότητες αναπτύσσονται και εξασκούνται αποκλειστικά από τις ΕΔ και τις μυστικές υπηρεσίες της χώρας. Η ανάπτυξη των επιθετικών δυνατοτήτων κυβερνοπολέμου πραγματοποιείται σε συνεργασία με τα εγχώρια ακαδημαϊκά και ερευνητικά ιδρύματα.

Σύμφωνα με εκτιμήσεις, οι ΕΔ της Β. Κορέας διαθέτουν 10.000 – 40.000 στελέχη – hackers, τα οποία διαθέτουν πολυετή εμπειρία σε εκδήλωση CNAs και CNEs κατά της Ν. Κορέας. Η διαδικασία επιλογής ξεκινά από την πρωτοβάθμια εκπαίδευση, όπου διαπιστώνονται οι ικανότητες τους στους Η/Υ. Εν συνεχεία στη δευτεροβάθμια εκπαίδευση, τα συγκεκριμένα άτομα εκπαιδεύονται στον προγραμματισμό Η/Υ και στην τεχνολογία των Η/Υ και στη συνέχεια εισάγονται στο πανεπιστήμιο προκειμένου να εξειδικευτούν στις κυβερνοεπιθέσεις, επανδρώνοντας με το πέρας της εκπαίδευσής τους εξειδικευμένες μονάδες

κυβερνοπολέμου όπως τα «Unit 35, 110, 121 & 204». Κάθε μία μονάδα αναλαμβάνει διαφορετικές αποστολές , οι οποίες έχουν ως σκοπό είτε την αναγνώριση, είτε την αδρανοποίηση αντίπαλών υποδομών, είτε την εσωτερική ασφάλεια, είτε την εκδήλωση ψυχολογικών επιχειρήσεων[B41].

Το πλέον γνωστό παράδειγμα επιθετικής δραστηριότητας στον κυβερνοχώρο αποτελεί η περίπτωση των κυβερνοεπιθέσεων κατά των ΗΠΑ και της Ν. Κορέας τον Ιούλιο του 2009. Οι κυβερνοεπιθέσεις έλαβαν χώρα μέσω ενός δικτύου «μολυσμένων» Η/Υ σε τρεις φάσεις και σχεδιάστηκαν από το Unit 110. Κατά την 1η φάση διάφορες αμερικάνικες ιστοσελίδες δέχθηκαν καταιγισμό ερωτήσεων από ένα δίκτυο «μολυσμένων» Η/Υ, με αποτέλεσμα οι ιστοσελίδες να τεθούν εκτός ενεργείας. Το δίκτυο είχε προκύψει με υπαιτιότητα των βορειοκορεατών μέσω αποστολής κακόβουλου λογισμικού σε 40.000 Η/Υ σε όλον τον κόσμο. Στόχοι του δικτύου ήταν το Υπουργείο Οικονομικών, ο Λευκός Οίκος, το χρηματιστήριο και η εφημερίδα Washington Post. Η 2η φάση των επιθέσεων DDoS εκδηλώθηκε με επιτυχία κατά των νοτιοκορεάτικων κυβερνητικών ιστοσελίδων, τραπεζών και μιας εταιρείας παροχής ασφάλειας στο διαδίκτυο. Η 3η φάση έλαβε χώρα στις 10 Ιουλίου μέσω ενός δικτύου 166.000 «μολυσμένων» Η/Υ από 74 χώρες και είχε ως στόχο τη Ν. Κορέα, όμως η απειλή αντιμετωπίστηκε επαρκώς.

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 τη συνεργασία ιρανικών τεχνολογικών πανεπιστημίων. Μεταξύ αυτών συγκαταλέγεται το πρόγραμμα ανάπτυξης δυνατοτήτων κυβερνοπολέμου. Παράλληλα, επεδίωξε τη στρατιωτική συνεργασία με τη Ρωσία, η οποία είχε 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.

Σύμφωνα με ανοιχτές πηγές, οι δυνατότητες του Ιράν στον κυβερνοπόλεμο είναι ήδη σημαντικές, με τις επιθετικές του δυνατότητες να βρίσκονται σε υψηλό επίπεδο. Οι ΕΔ της χώρας διαδραματίζουν καθοριστικό ρόλο στην εφαρμογή τους. Μέχρι σήμερα η Μονάδα, που είναι αρμόδια για τη διεξαγωγή επιχειρήσεων κυβερνοπολέμου υπάγεται στο Σώμα των Φρουρών της Επανάστασης. Η Μονάδα αυτή αριθμεί περίπου 2.400 άτομα και διαχειρίζεται σε ετήσια βάση 76 εκ. δολάρια για την ανάπτυξη των δυνατοτήτων της στον

κυβερνοχώρο. Όπως και οι προαναφερθείσες χώρες έτσι και το Ιράν απασχολεί ομάδες μη κρατικών δρώντων, προκειμένου να αυξήσει τη δυναμική του στον κυβερνοχώρο. Η πλέον γνωστή είναι η ομάδα Iranian Cyber Army, η οποία συνεργάζεται με τους Φρουρούς της Επανάστασης. Επιπλέον, για σκοπούς επιτήρησης του διαδικτύου, το Ιράν διαθέτει από το 2011 μια αστυνομική δύναμη γνωστή ως Iranian Cyber Police Unit. Το 2016 δημιουργήθηκε η Διοίκηση Κυβερνοπολέμου (Cyber Command), η οποία υπάγεται στις ιρανικές ΕΔ, έχει αμυντικό χαρακτήρα και συντονίζει τις επιχειρήσεις στον κυβερνοχώρο[B41].

Αξίζει να σημειωθεί πως το Ιράν δεν έχει κάνει δημόσια γνωστές τις δυνατότητές του στον κυβερνοπόλεμο, πλην ελαχίστων περιπτώσεων. Πιο συγκεκριμένα, το 2009 η ομάδα Iranian Cyber Army κατάφερε να επιτύχει ανακατεύθυνση των χρηστών της ιστοσελίδας κοινωνικής δικτύωσης «twitter.com» σε ιστοσελίδες, που περιείχαν αντιαμερικανικά συνθήματα. Επίσης, το 2010 προέβησαν σε απενεργοποίηση 4 ωρών της κινεζικής ιστοσελίδα Baidu, αναρτώντας στη θέση του λογότυπου της ιστοσελίδας την ιρανική σημαία και την επιγραφή Iranian Cyber Army.

Μια ακόμα εκδήλωση ιρανικής κυβερνοεπίθεσης είναι η υπόθεση της αναγκαστικής προσγείωσης ενός αμερικάνικου UAV RQ – 170 Sentinel στο Ιράν στις 4 Δεκεμβρίου 2011. Σύμφωνα με την ιρανική πλευρά, το αμερικάνικο UAV εκτελούσε κατασκοπευτική πτήση άνωθεν του Ιράν, όταν οι ιρανικές ΕΔ κατάφεραν με συνδυασμό τεχνικών κυβερνοπολέμου και ηλεκτρονικού πολέμου να πάρουν τον έλεγχο πτήσης τους μέσου και να το προσγειώσουν σε ιρανικό έδαφος, χρησιμοποιώντας σύμφωνα με την έρευνα κατάλληλο εξοπλισμό ηλεκτρονικών παρεμβολών, που είχαν προμηθευτεί από τη Ρωσία, κατορθώνοντας να επέμβουν στο σύστημα ναυτιλίας GPS του UAV.

8.3 Σημαντικές Περιπτώσεις Κυβερνοεπιθέσεων

Στο παρούσα ενότητα θα αναπτυχθούν τρεις σημαντικές περιπτώσεις κυβερνοεπιθέσεων, οι οποίες, λόγω της πρωτοτυπίας τους, προσέλκυσαν το ενδιαφέρον της διεθνούς κοινότητας και κατέδειξαν τις μορφές, που δύναται να λάβει ο κυβερνοπόλεμος στη σύγχρονη αποχή. Οι περιπτώσεις αφορούν την Εσθονία το 2007, τη Γεωργία το 2008 και το Ιράν το 2009-2010. Στην περίπτωση της Εσθονίας φανερώθηκε ο αρνητικός αντίκτυπος των κυβερνοεπιθέσεων DDoS στην οικονομική και κοινωνική λειτουργία μιας χώρας-στόχου, η οποία είναι εξαρτημένη από την τεχνολογία των Η/Υ και των επικοινωνιών. Όσον αφορά στη Γεωργία, τα γεγονότα κατέδειξαν πώς οι επιχειρήσεις στον κυβερνοχώρο δύναται να συμβάλλουν υποστηρικτικά στη διεξαγωγή των συμβατικών πολεμικών συγκρούσεων, ενώ σχετικά με την περίπτωση Stuxnet το 2009-2010 (Ιράν) τονίζεται πώς η ανάπτυξη και χρήση

ενός κυβερνοόπλου ακριβείας δύναται να καταφέρει αυτό που επί χρόνια η διεθνής κοινότητα αδυνατούσε να επιβάλει στο Ιράν, το «πάγωμα» του πυρηνικού του προγράμματος.

8.3.1 Εσθονία 2007

Αφορμή για την έναρξη των γεγονότων στην Εσθονία αποτέλεσε η επικύρωση από το εσθονικό κοινοβούλιο το Φεβρουάριο του 2007 του νομοσχεδίου «Forbidden Structures Law», το οποίο αφορούσε στην καταστροφή των μνημείων, τα οποία καταδείκνυαν τα χρόνια «κατοχής» της χώρας από τη Σοβιετική Ένωση[B35]. Πιο συγκεκριμένα, η κυβέρνηση θα προχωρούσε στη μετακίνηση του χάλκινου αγάλματος του Στρατιώτη του Κόκκινου Στρατού, το οποίο είχε τοποθετηθεί από τους Σοβιετικούς στο κέντρο της εσθονικής πρωτεύουσας, μετά το πέρας του Β' Παγκόσμιου Πολέμου.

Το γεγονός αυτό προκάλεσε έντονες αντιδράσεις τόσο στους Ρώσους, που διέμεναν στη χώρα όσο και στη ρωσική κυβέρνηση, αναγκάζοντας τον Εσθονό Πρόεδρο να ασκήσει βέτο επί του νομοσχεδίου[B35]. Οι πιέσεις εκατέρωθεν ήταν έντονες και παρ' όλες τις συγκρούσεις μεταξύ εθνικιστικών οργανώσεων των δύο χωρών και πολλών διαμαρτυριών, η κυβέρνηση στις 27 Απριλίου προχώρησε στη μετακίνηση του μνημείου. Αυτό είχε ως αποτέλεσμα να ξεσπάσουν έντονες αντιδράσεις από τη ρωσική εθνικιστική ομάδα Nashi, η οποία διαμαρτυρήθηκε έξω από την εσθονική πρεσβεία στη Μόσχα. Παράλληλα, πραγματοποιήθηκε πληθώρα κυβερνοεπιθέσεων κατά εσθονικών ιστοσελίδων και ΜΜΕ.

Ο αντίκτυπος των κυβερνοεπιθέσεων ήταν μεγάλος καθώς η χώρα ήταν ιδιαίτερα εξαρτημένη από την τεχνολογία της πληροφορικής και των επικοινωνιών, το διαδίκτυο και τα δίκτυα Η/Υ. Η Εσθονία κατά τη διάρκεια της δεκαετίας του 1990, είχε στραφεί προς τη ψηφιακή τεχνολογία και τη διασύνδεση των παρεχόμενων υπηρεσιών , προκειμένου να μειώσει το κόστος των υπηρεσιών και να ικανοποιήσει τις ανάγκες του πληθυσμού της αραιοκατοικημένης Εσθονίας.

Όπως αναφέρεται, οι κυβερνοεπιθέσεις πραγματοποιήθηκαν σε δύο 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, αλλαγές στο περιεχόμενο ιστοσελίδων χωρίς εξουσιοδότηση, εκούσια κατεύθυνση των χρηστών των δικτύων σε μη επιθυμητές περιοχές των δικτύων και καταιγισμός ανεπιθύμητων ηλεκτρονικών μηνυμάτων[B35].

Στόχοι των κυβερνοεπιθέσεων ήταν τα δημόσια και ιδιωτικά κανάλια διανομής πληροφόρησης, η εσθονική υποδομή για το Internet, οι κυβερνητικές και πολιτικές ιστοσελίδες, οι ηλεκτρονικές υπηρεσίες του ιδιωτικού τομέα και κάποιοι άλλοι τυχαίοι στόχοι. Επιπρόσθετα, σημειώνεται ότι οι βάσεις δεδομένων του δημόσιου και του ιδιωτικού τομέα δεν στοχοποιήθηκαν από τους δράστες των κυβερνοεπιθέσεων.

Η 1η φάση των κυβερνοεπιθέσεων εστίασε στις κυβερνητικές ιστοσελίδες και τα ΜΜΕ. Βασίστηκε κυρίως σε απλές μεθόδους κυβερνοεπιθέσεων, ενώ διαπιστώθηκε λειτουργία forum διαδίκτυο, όπου στη ρωσική γλώσσα δίνονταν οδηγίες αλλά και κυβερνοεργαλεία για την εκδήλωση των κυβερνοεπιθέσεων. Η ένταση εκδήλωσης αυτών των κυβερνοεπιθέσεων ήταν αρκετά ήπια με αποτέλεσμα σε γενικές γραμμές να αντιμετωπιστούν με επιτυχία από το εσθονικό κράτος.

Η 2η φάση ήταν μεγαλύτερης χρονικής περιόδου και περιελάμβανε καλύτερα συντονισμένες και πιο εξειδικευμένες επιθέσεις, οι οποίες πραγματοποιήθηκαν σε τέσσερα κύματα. Πιο αναλυτικά[B35]:

- Το 1ο κύμα επιθέσεων 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.
- Το 2ο κύμα επιθέσεων είχε την ίδια ένταση, ωστόσο οι κυβερνοεπιθέσεις DDoS έφτασαν στο 150% σε σχέση με το 1ο κύμα, ενώ κατάφεραν να θέσουν εκτός λειτουργίας τουλάχιστον 58 ιστοσελίδες. Οι επιθέσεις εστιάστηκαν κατά κυβερνητικών ιστοσελίδων και εμπορικών τραπεζών.
- Το 3ο κύμα περιελάμβανε κυβερνοεπιθέσεις DDoS μέσω ενός Botnet 85.000 Η/Υ. Οι στόχοι σε αυτό το μέρος ήταν οι ίδιοι με το προηγούμενο, 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.
- Το 4ο κύμα των επιθέσεων περιελάμβανε κυβερνοεπιθέσεις DDoS και στόχευε κυρίως σε κυβερνητικές ιστοσελίδες.

Κατά τη διάρκεια των επιθέσεων, η Εσθονία προσπάθησε να εξισορροπήσει τις κυβερνοαπειλές χρησιμοποιώντας τις ομάδες CERT (Computer Emergency Response Team) και πληθώρα ειδικών στην ΙΤ τεχνολογία. Παράλληλα, δέχθηκε βοήθεια από την ΕΕ και το ΝΑΤΟ, οι οποίοι απέστειλαν ειδικούς στην ΙΤ τεχνολογία για να συνδράμουν το έργο των εσθονικών ομάδων CERT. Επιπλέον, οι ΗΠΑ συνέβαλαν στις προσπάθειες εντοπισμού των πηγών των κυβερνοεπιθέσεων και την επιτυχή απενεργοποίησή τους, καταδεικνύοντας μέρος των δυνατοτήτων τους στον κυβερνοχώρο.

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

- Οι επιθέσεις είχαν σημαντικό αντίκτυπο στην οικονομική και κοινωνική λειτουργία της χώρας.
- Το υφιστάμενο εσθονικό νομικό πλαίσιο δεν ήταν κατάλληλα ενημερωμένο για την αντιμετώπιση των ανωτέρω κυβερνοεπιθέσεων.
- Η πληθώρα των κυβερνοεπιθέσεων καταδείκνυε ότι προέρχονταν από το εξωτερικό.
- Η ρώσικη κυβέρνηση αρνήθηκε την οποιαδήποτε εμπλοκή με τις κυβερνοεπιθέσεις, ισχυριζόμενη πως αυτές προέρχονται από ομάδες εθνικιστών, με τις οποίες δεν είχε καμία σχέση.

8.3.2 Γεωργία 2008

Οι σχέσεις της Γεωργίας με τη Ρωσία την τελευταία 20ετία χαρακτηρίζονται γενικά ως συγκρουσιακές. Το κύριο σημείο τριβής αποτέλεσε η ρωσική υποστήριξη προς τις αποσχισθείσες περιοχές της Ν. Οσσετίας και της Αμπχαζίας. Στα τέλη Ιουλίου και αρχές Αυγούστου του 2008 σημειώθηκαν ένοπλες συγκρούσεις μεταξύ Γεωργιανών και Νότιο – Οσσετών αλλά και Αμπχάζιων[B7]. Οι συγκρούσεις ήταν σφοδρές από πλευράς Γεωργιανών, οι οποίοι επιχείρησαν βομβαρδισμούς στις πρωτεύουσες των παραπάνω περιοχών, λαμβάνοντας άμεση απάντηση από τις ρωσικές ΕΔ, οι οποίες δημιούργησαν ζώνες προστασίας αυτών των περιοχών, εντός γεωργιανού εδάφους. Η κρίση ολοκληρώθηκε μετά από λίγες ημέρες με την αποχώρηση των ρωσικών στρατευμάτων και την αναγνώριση της αυτονομίας των παραπάνω περιοχών.

Αξίζει να σημειωθεί πως πριν την έναρξη των ένοπλων συγκρούσεων, πραγματοποιήθηκαν κυβερνοεπιθέσεις κατά γεωργιανών στόχων, παρά το γεγονός ότι η Γεωργία δεν είχε σημαντικές πληροφοριακές υποδομές. Η πρώτη κυβερνοεπίθεση είχε ως στόχο της ιστοσελίδα του Προέδρου της χώρας. Πρόκειται για κυβερνοεπίθεση DDoS, η οποία είχε ως αποτέλεσμα να τεθεί εκτός λειτουργίας η προεδρική ιστοσελίδα για τουλάχιστον μία ημέρα[B7]. Ωστόσο, το κύριο μέρος των κυβερνοεπιθέσεων εκδηλώθηκαν παράλληλα με τις συμβατικές επιχειρήσεις με αποτέλεσμα οι ιστοσελίδες που στοχοποιούνταν να παραμένουν εκτός λειτουργίας για μεγάλο χρονικό διάστημα.

Οι μέθοδοι εκδήλωσης των κυβερνοεπιθέσεων ήταν παρόμοιες με εκείνες που χρησιμοποιήθηκαν στην Εσθονίας με τη διαφορά ότι στην περίπτωση της Γεωργίας ο συντονισμός των hackers διαφάνηκε εξ αρχής. Στόχοι των επιθέσεων αποτέλεσαν οι

ιστοσελίδες της Προεδρίας, της κυβέρνησης, του ΥΠΕΞ και του ΥΠΑΜ, των ειδησειογραφικών πρακτορείων της χώρας, καθώς και μη γεωργιανές ιστοσελίδες, οι οποίες ήταν φιλικά προσκείμενες στο γεωργιανό καθεστώς. Παράλληλα, ισχυρό πλήγμα από τις κυβερνοεπιθέσεις δέχθηκε το γεωργιανό τραπεζικό σύστημα, με επίκεντρο τη μεγαλύτερη εμπορική τράπεζα της χώρας, ενώ δεν έλειψαν οι επιθέσεις και σε κάποιες εμπορικές ιστοσελίδες. Η μέση διάρκεια των επιθέσεων DDoS έφθανε τις 2 ώρες και 15 λεπτά, ενώ η μεγαλύτερη διάρκεια που καταγράφηκε ήταν 6 ώρες[B7].

Μία ακόμη μέθοδος εκδήλωσης των κυβερνοεπιθέσεων 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. Προκειμένου να αντιμετωπίσει τις κυβερνοεπιθέσεις 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.

Από την έρευνα της περίπτωσης της Γεωργίας διαπιστώθηκαν τα εξής συμπεράσματα[B7]:

- Έγινε ευρεία χρήση των botnets με τους Ρώσους hackers να έχουν τον απόλυτο έλεγχο και συντονισμό των κυβερνοεπιθέσεων.
- Αντικειμενικός σκοπός των κυβερνοεπιθέσεων ήταν να διακοπεί η ροή πληροφόρησης των Γεωργιανών πολιτών αναφορικά με τις εξελίξεις των συμβατικών επιχειρήσεων.
- Σημειώθηκε αρνητικός οικονομικός αντίκτυπος για τη χώρα καθώς η εκδήλωση των κυβερνοεπιθέσεων, οδήγησε την εθνική τράπεζα της χώρας σε παύση παροχής ηλεκτρονικών υπηρεσιών προς τους πελάτες της για 10 ημέρες.
- Ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων δεν ήταν δυνατόν να υπολογιστεί καθώς παράλληλα λάμβαναν χώρα και οι συμβατικές επιχειρήσεις, μέσω των οποίων καταστράφηκαν υποδομές ICT τεχνολογίας (Information and Communication Technology).
- Σημειώθηκε παράλυση του συστήματος κινητής τηλεφωνίας.

8.3.3 Ιράν 2009-2010 (Stuxnet)

Τον Ιούνιο του 2010 η λευκορώσικη εταιρεία VirusBlockArea, η οποία εξειδικευόταν στην ασφάλεια των Η/Υ, ανακάλυψε ην ύπαρξη ενός κακόβουλου λογισμικού σε φορητές μνήμες Η/Υ (USB flash drives). Το υπόψη λογισμικό ονομάστηκε Stuxnet και παρουσίαζε

αρκετές καινοτομίες στην αρχιτεκτονική του. Πιο συγκεκριμένα, είχε τη δυνατότητα να παραμένει αόρατο από τα λογισμικά αντιμετώπισης κυβερνοεπιθέσεων, ενώ φρόντιζε από μόνο του για την αναπαραγωγή και διάδοσή του στα δίκτυα Η/Υ. Αυτός ήταν και ο λόγος γα τον οποίο χαρακτηρίστηκε από τους ειδικούς ως ο πρώτος κατευθυνόμενος κυβερνοπύραυλος. Εκτός όμως από αυτά τα χαρακτηριστικά, θεωρήθηκε ως ιδιαίτερα μεγάλο και πολύπλοκο λογισμικό, το οποίο ήταν κρυπτογραφημένο, ενώ όταν έπληττε το στόχο του, δεν άφηνε ίχνη κακής λειτουργίας στα ψηφιακά συστήματα επιτήρησης του, με αποτέλεσμα ο διαχειριστής του δικτύου να μην είναι σε θέση να αντιληφθεί την έναρξη και την εξέλιξη της κυβερνοεπίθεσης[B8].

Από τη δημοσιοποίηση της δράσης του Stuxnet προκλήθηκε έντονη ανησυχία σε παγκόσμιο επίπεδο, η οποία είχε ως αποτέλεσμα τους ενδελεχείς ελέγχους και έρευνες από αρμόδιες εταιρείες ασφάλειας δικτύων Η/Υ. Τα αποτελέσματα των ερευνών κατέδειξαν πως είχαν προσβληθεί κυρίως δίκτυα Η/Υ, που αφορούσαν εξειδικευμένους βιομηχανικούς στόχους, μολύνοντας Η/Υ διαφόρων χωρών αλλά κυρίως στο Ιράν με επίκεντρο της πυρηνικές εγκαταστάσεις της χώρας.

Η αρχική μόλυνση από το Stuxnet έγινε στο Ιράν τον Ιούνιο του 2009 και στη συνέχεια διαδόθηκε στις υπόλοιπες χώρες. Οι στόχοι του Stuxnet επικεντρώνονται γύρω από τις ιρανικές πυρηνικές εγκαταστάσεις της Natanz και του Bushehr. Η ιδιαιτερότητα, που εμφανίζουν οι συγκεκριμένες εγκαταστάσεις είναι ότι ο έλεγχος της λειτουργίας τους πραγματοποιούνταν από ψηφιακά βιομηχανικά συστήματα ελέγχου SCADA (Supervisory Control and Data Acquisition), τα οποία χρησιμοποιούσαν συγκεκριμένο τύπο λογισμικού της γερμανικής εταιρείας Siemens. Το Stuxnet είχε σχεδιαστεί για να εκμεταλλευτεί τις συγκεκριμένες τρωτότητες αυτού του λογισμικού[B8].

Όσον αφορά τον τρόπο δράσης του Stuxnet, το λογισμικό δρούσε στις συσκευές ελέγχου των μετατροπέων συχνοτήτων, με αποτέλεσμα κάθε φορά που απαιτούνταν από το σύστημα SCADA της Νατανζ μια μεταφορά οδηγιών προς τους μετατροπείς συχνοτήτων, το οποίο επιτυγχανόταν μέσω Η/Υ, οι οποίοι συνδέονταν με τις συσκευές ελέγχου των μετατροπέων συχνοτήτων, αφενός να εμποδίζει τη μεταφορά των οδηγιών και αφετέρου να παρέχει λανθασμένες οδηγίες προς τις συσκευές φυγοκέντρησης, οδηγώντας στην καταστροφή τους. Αξίζει να σημειωθεί πως η παραπάνω διαδικασία ολοκληρωνόταν χωρίς να υπάρχει καμία ένδειξη μη ομαλής λειτουργίας των συσκευών στα συστήματα επιτήρησης της διαδικασίας. Προφανώς, στόχος του Stuxnet ήταν η δολιοφθορά φυσικών εγκαταστάσεων και υποδομών.

Μέχρι σήμερα κανείς δεν μπορεί να υπολογίσει το κόστος καταστροφής, που επέφερε το Stuxnet. Παρ' όλα αυτά θεωρείται ότι με την εφαρμογή του συγκεκριμένου κακόβουλου

λογισμικού η φυσική εξέλιξη του πυρηνικού προγράμματος του Ιράν, η οποία θα οδηγούσε στην κατασκευή πυρηνικών όπλων, παρεμποδίστηκε για τουλάχιστον δύο χρόνια.

Τέλος, λόγω των ιδιαιτεροτήτων, που παρουσίαζε η αρχιτεκτονική του Stuxnet και η εξειδίκευση του ως malware συμπεραίνεται ότι η ανάπτυξη του απαίτησε τεράστια χρηματικά ποσά αλλά και ιδιαίτερες δυνατότητες και τεχνογνωσία στον κυβερνοχώρο. Παράλληλα, για την επιτυχή δραστηριοποίησή του ήταν απαραίτητη η ύπαρξη εξειδικευμένων πληροφοριών για το στόχο αλλά και πειραματικού πεδίου εφαρμογής του malware, απαιτήσεις τις οποίες θα μπορούσαν να καλύψουν μόνο τα κράτη και όχι μη κρατικές οντότητες[B12]. Συμπερασματικά, το Stuxnet δεν είχε σκοπό την υπεξαίρεση βιομηχανικών δεδομένων, οπότε δεν μπορεί να ταυτιστεί με επιχειρήσεις κυβερνοκατασκοπείας ή κυβερνοεγκλήματος, τις οποίες θα μπορούσε να διενεργήσει οποιοσδήποτε πέραν από ένα κράτος.

ΚΕΦΑΛΑΙΟ 9 ΣΥΜΠΕΡΑΣΜΑΤΑ

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 αναπτυγμένες. Η εφαρμογή των Η/Υ σε διάφορους τομείς της ανθρώπινης δραστηριότητας βοήθησε στον αυτοματισμό των διαδικασιών, τη μείωση του λειτουργικού 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 και προσέδωσε στους στρατιωτικούς σχεδιασμούς μεγαλύτερη ακρίβεια και αποτελεσματικότητα, μειώνοντας το κόστος, με παράλληλη αύξηση στην έννοια της ασφάλειας.

Η αλματώδης ανάπτυξη του Internet μετά το 1990 και η ευκολία πρόσβασης σε αυτό από κάθε χρήστη οδήγησε σε μεγαλύτερα επίπεδα διασύνδεσης και επικοινωνίας την ανθρωπότητα. Οι βασικές αρχές λειτουργίας του διαδικτύου εστίαζαν στη δυνατότητα εύκολης πρόσβασης σε αυτό, διατηρώντας χαμηλά επίπεδα ασφάλειας στους χρήστες του. Πρέπει, όμως, να αναφερθεί ότι το Internet δημιουργήθηκε για να εξυπηρετεί τις ανάγκες επικοινωνίας της ακαδημαϊκής κοινότητας και των αμερικάνικων ΕΔ, οι οποίοι αποτελούσαν «ασφαλείς» τομείς της κοινωνίας και όχι για να εξυπηρετεί τις ανάγκες ενός τεράστιου αριθμού χρηστών όπως συμβαίνει στις μέρες μας.

Σταδιακά από τις αρχές της δεκαετίας του 1990 άρχισε να εμφανίζεται η έννοια του Κυβερνοχώρου, του εικονικού χώρου, ο οποίος είχε δημιουργηθεί μέσω των Η/Υ προκειμένου ο άνθρωπος να επικοινωνεί και να διεκπεραιώνει με μεγαλύτερη ταχύτητα και αποτελεσματικότητα τις διάφορες δραστηριότητές του. 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 τη δαιδαλώδη αρχιτεκτονική του διαδικτύου αλλά και των υπολοίπων δικτύων Η/Υ. Ως απόρροια αυτού, υπήρξαν προσπάθειες εκμετάλλευσης αυτών των αδυναμιών, από τους λεγόμενους Hackers, οι οποίοι κάνοντας χρήση των εξειδικευμένων γνώσεών τους και των κακόβουλων λογισμικών μπορούσαν να εξυπηρετούν τα προσωπικά τους συμφέροντα ή τα συμφέροντα άλλων ομάδων.

Ο Κυβερνοχώρος αποτελεί στρατηγικό μέσο, καθώς μέσω αυτού μπορούν να δεχθούν κυβερνοεπιθέσεις τόσο οι στρατιωτικές (Military) όσο και οι μη στρατιωτικές (Civillian) υποδομές. Οι συγκρούσεις σε αυτήν την περιοχή ήταν αναμενόμενη εξέλιξη, καθώς σε ένα διάστημα είκοσι ετών αυξήθηκε δραματικά 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 (malware), καθώς και η εξειδίκευση των Hackers.

Παράλληλα, τα κυβερνοόπλα είναι γρήγορα και οικονομικά σε σχέση με τα όπλα του κινητικού πολέμου και τα αποτελέσματά τους είναι το ίδια ισχυρά. Τα κυβερνοόπλα ανάλογα με τις δυνατότητες της κάθε εποχής εξελίσσονται και μαζί με αυτά και οι τρόποι αντιμετώπισής τους. Η τεχνολογία έχει προχωρήσει και η προστασία των κρατών γίνεται με όλο και πιο ισχυρά τεχνολογικά μέσα για να μπορεί να ανταπεξέλθει. Τέλος ένα από τα προβλήματα που όσο και να αναπτυχθεί η τεχνολογία δεν μπορεί να λυθεί είναι το πρόβλημα της ανωνυμίας.

Καταλήγοντας, είναι φανερό πως ο κυβερνοπόλεμος αποτελεί ένα σχετικά καινούργιο είδος πολέμου, το οποίο από τη μία ως επί το πλείστον δεν επιφέρει οδυνηρές απώλειες ανθρώπινων ζωών, όπως η τέλεση συμβατικών επιχειρήσεων, αλλά από την άλλη είναι σε θέση να επιφέρει καίρια πλήγματα σε ένα κράτος, ειδικά όταν αυτό είναι απόλυτα «εξαρτημένο» από τα δίκτυα Η/Υ, όπως τα παραδείγματα κυβερνοεπιθέσεων στην Εσθονία και τη Γεωργία. Παρ' όλα αυτά, η εκδήλωση κυβερνοεπιθέσεων σε καμία περίπτωση δεν μπορεί να αντικαταστήσει το ρόλο του συμβατικού πολέμου καθώς μέσω του κυβερνοπολέμου δεν καταλαμβάνεται ούτε εδαφική, ούτε εναέρια, ούτε θαλάσσια υπεροχή ενός αντιπάλου έναντι του άλλου. Όμως, ο κυβερνοπόλεμος μπορεί κάλλιστα να λειτουργήσει ως προπομπός των συμβατικών επιχειρήσεων, προκαλώντας πλήρη αιφνιδιασμό, αποδιοργάνωση και αποπροσανατολισμό στις στρατιωτικές και πολιτικές υποδομές ενός κράτους, καθιστώντας το ουσιαστικά «έρμαιο» στη βούληση του αντιπάλου του.

ΚΕΦΑΛΑΙΟ 10 ΒΙΒΛΙΟΓΡΑΦΙΑ

Α. Βιβλία και Άρθρα (Ελληνικά)

1. Γαρίδης Παναγιώτης & Δεληγιαννάκης Μανώλης, Σύγχρονο Λεξικό Πληροφορικής
2. Κολλιόπουλος Κωνσταντίνος, Η στρατηγική σκέψη Από την Αρχαιότητα ως σήμερα
3. Κονδύλης Παναγιώτης, Η θεωρία του πολέμου
4. Κουσκουβέλης Ηλίας, Εισαγωγή στις Διεθνείς Σχέσεις
5. Μπόση Μαίρη, Περί Ορισμού της Τρομοκρατίας
6. Χατζηκωνσταντίνου Κώστας, Προσεγγίσεις στο Διεθνές Ανθρωπιστικό Δίκαιο

Β. Βιβλία και Άρθρα (Αγγλικά)

1. Boot Max, "War made new: Weapons, Warriors and the Making of the Modern World"
2. Borchert Heiko, "Exploiting the Potential of Cyber Operations"
3. Biddle Stephen, "Military Power: Explaining victory and refeat in modern battle"
4. Bimal Kumar Mishra, "Mathematic models on computer viruses", Applied Mathematics and Computation
5. Carr Jeffrey, "Inside Cyber Warfare"
6. Cavelty Dunn, "Cyberwar: Concept, Status Quo and Limitations"
7. Clarke and Knake, 2010
8. Clarke Richard, "Cyber War: The Next Threat to National Security And What To Do About It"
9. Crosston Matthew, "World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence", http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf
10. Curran Kevin, "Cyber Terrorism Attacks"
11. Denning Dorothy, "Activism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy"
12. Dinesh Kumar Saini, "Cyber Defense: Mathematical Modeling and Simulation"
13. Geers Kenneth, "Strategic Cyber Security"
14. Geers Kenneth, "Cyberspace and the Changing Nature of Warfare"
15. Hedley Bull, " Άναρχη Κοινωνία: Μελέτη ης τάξης στην παγκόσμια πολιτική"

16. Hunker Jeffrey, "Cyberwar and Cyber Power. Issues for NATO doctrine", http://www.ndc.nato.int/research/series.php?icode=1
17. Hoisington Matthew, "Cyberwarfare and the use force giving rise to the right of self-defense"
18. Jurich Jon, "Cyberwar and Customary International Law"
19. Kamal Ahmad, UN Report: Law of Cyberspace
20. Kaminski Ryan, "Escaping The Cyber State of Nature: Cyber Deterrence and International Institutions"
21. Libicki Martin, "Cyberdeterrence and Cyberwar"
22. Libicki Martin, "The Emerging Primacy of Information"
23. Libicki Martin, "Deterrence in Cyberspace"
24. Lyle Michael, NetSPA: A Network Security Planning Architecture"
25. Mandeles Mark, "The future of war: Organizations as weapons"
26. McConnell Mike, "Cyber Insecurties: the 21st Century Threatscape"
27. McGavran Wolfgang, "Intended Consequences: Regulating Cyber Attacks"
28. Meyers C., Powers S., Faissol D., "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches", http://www.osti.gov/bridge/product.biblio.jsp?osti_id=967712
29. Michael Alex, "Cyber Probing: The Politicisation of Virtual Attack"
30. Nye Joseph, "Cyber Power"
31. Ottis Rain, "Theoritical Offensive Cyber Militia Models"
32. Parks Raymond & Duncan David, "Principles of Cyber Warfare", http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf
33. Schaap Arie, "Cyber Warfare Operations and Use Under International Law"
34. Shackelford Scott, "From nuclear war to net war: Analogizing cyber attacks in International Law"
35. Shackelford Scott, "Estonia three years later: A progress report on combating cyber attacks"
36. Sheyner Mikhail, "Scenario Graphs and Attack Graphs"
37. Sklerov Matthew, "Solving the dilemma of state responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent"
38. Solce Natasha, "the battlefield of Cyberspace: The inevitable new military branch – The Cyber Force
39. Solomon Jonathan, "Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?", http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf

40. Sterner Eric, "Retaliatory Deterrence in Cyberspace", http://www.au.af.mil/au/ssq/2011/spring/sterner.pdf
41. Thompson Trevor, "Terrorizing the technological neighborhood watch: The alienation and deterrence of the "white hats" under the CFAA
42. Yang Wang, "A queueing analysis for the denial of service (DoS) attacks in computer networks"

Γ. Ιστότοποι

1. http://en.wikipedia.org/wiki/Cyberspace
2. http://en.wikipedia.org/wiki/Wide Area Network
3. http://en.wikipedia.org/wiki/spoofing
4. http://www.securityreport.gr
5. http://www.warandstrategy.gr/kyvernopolemos/kyvernopolemoskaiethnikistratigiki
6. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2010.pdf
7. http://www.thefreedictionary.com
8. http://cve.mitre.org/cve/index.html
9. http://www.sas.com
10. https://searchsecurity.techtarget.com/definition/intrusion-detection-system