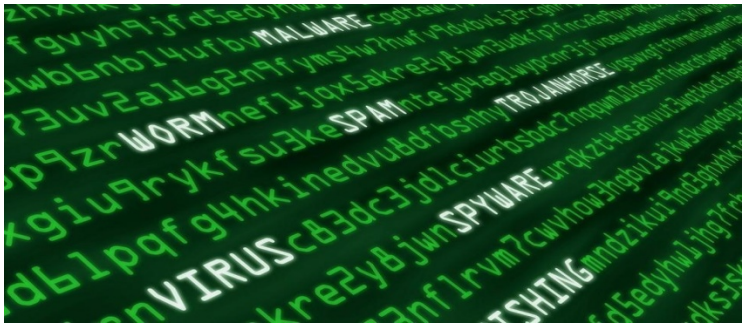
Πανεπιστήμιο Αιγαίου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Κυβερνοπόλεμος και επιθέσεις στο διαδίκτυο



Διπλωματική Εργασία

της

Σίμου Φλώρας
321/2011149

Επιβλέπουσα Καθηγήτρια :

Μήτρου Λίλιαν
Αναπληρώτρια καθηγήτρια ΜΠΕΣ

31 Οκτώβρη 2016

Περίληψη

Η Τεχνολογία Πληροφοριών και Επικοινωνιών είναι ένας κλάδος που στις μέρες μας αναπτύσσεται εκθετικά. Η ανάπτυξη αυτή εγκυμονεί διάφορους κινδύνους με αποτέλεσμα την δημιουργία μίας νέας μορφής πολέμου. Σκοπός αυτής της διπλωματικής εργασίας είναι η κατανόηση του όρου "Κυβερνοπόλεμος" σε σχέση με τις συγγενείς έννοιές του, όπως κυβερνοεπιθέσειςκαι κυβερνοχώρος. Αρχικά αναλύεται αυτή η μορφή πολέμου και διαχωρίζεται από τον κινητικό και τον ηλεκρονικό πόλεμο με την χρήση παράθεσης σχετικών παραδειγμάτων και αναπτύσσεται το αντίστοιχο νομικό πλαίσιο. Τέλος αναφέρονται οι τρόποι που κάποιος μπορεί να προκαλέσει μία επίθεση στον Κυβερνοκόσμο καθώς και οι τρόποι αντιμετώπισης μιας κυβερνοεπίθεσης.

Λέξεις κλειδιά : « Κυβερνοπόλεμος, κυβερνοεπίθεση, Κυβερνοχώρος »

Abstract

The Information and Communication Technology is a branch nowadays growing at an exponential rate. This development holds various risks, thus creating a new form of war. The aim of this diploma thesis is the understanding of the term "cyberwarfare" in relation to associated concepts, such as cyberattacks and cyberspace. First, this form of war is analyzed and distinguished from kinetic and electronic war, relevant examples are quoted, and the corresponding legal framework is explained. Furthermore, it is described how someone could cause an attack on Cyberworld, as is how cyberattacks could be tackled.

Key words : « Cyberwarfare, cyberattack, cyberspace »

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου, κυρία Μήτρου Λίλιαν,για την εμπιστοσύνη που μου έδειξε καθώς και για το ενδιαφέρον θέμα που μου ανέθεσε να αναλύσω.Επίσης ,θέλω να πω ένα ευχαριστώ ,σε όλους μου τους καθηγητές και στον καθένα ξεχωριστά ,που μέσα στα πέντε χρόνια φοίτησής μου ,με βοήθησαν και με εμψύχωσαν και να ευχαριστήσω όλους αυτούς ,που μου στάθηκαν κατά την διάρκεια της υλοποίησης της εργασίας μου.Τέλος θέλω να αφιερώσω την διπλωματική μου στους γονείς μου,και κυρίως στην μητέρα μου, που ήταν πάντα δίπλα μου και με στήριζε σε κάθε μου βήμα.

Ευχαριστώ πολύ!

Πίνακας περιεχομένων

1

Εισαγωγή

Τις τελευταίες δεκαετίες μαζί με την πρόοδο της ανθρωπότητας παρατηρήθηκε και μία ανάπτυξη στον τομέα των Τεχνολογιών Πληροφοριών και Επικοινωνιών- ΤΠΕ (Information and Communication Technologies—ICTs). Χάρη στην αναπτυξη των ΤΠΕ έχουν ισχυροποιηθεί και άλλοι κλάδοι ιδιαίτερα στον δημόσιο τομέα , όπως η Εθνική Ασφάλεια, η Εκπαίδευση, η Διακυβέρνηση, η Υγεία, η Δημόσια Ασφάλεια, καθώς επίσης και τομείς όπως η Οικονομία, οι Μεταφορές & Επικοινωνίες η Ενέργεια και η Διατροφή, που συνδέονται στενά με τις νέες ΤΠΕ.Οι σύγχρονες κοινωνίες στηρίζονται στα πληροφοριακά και επικοινωνιακά δίκτυα για τη λειτουργία των υποδομών τους και ο υψηλός βαθμός εξάρτισής τους από αυτές, τις καθιστά ευάλωτες στις κυβερνοεπιθέσεις[1]. Η επιλογή των κυβερνοεπιθέσεων φαντάζει ελκυστική, τόσο για κρατικούς, όσο και για μη κρατικούς δρώντες, αφού δεν περιορίζεται από γεωγραφικά όρια.Ακόμα υπάρχει το στοιχείο της απόκρυψης του επιτιθέμενου (ανωνυμία), ενώ το κόστος απόκτησης τέτοιων κυβερνοδυνατοτήτων είναι σχετικά χαμηλό. Επίσης, τα απαραίτητα εργαλεία (λογισμικό) και πόροι (πληροφορίες) για τη διεξαγωγή κυβερνοεπιθέσεων είναι ευρέως διαδεδομένα στους δρώντες του διεθνούς συστήματος.Ο τρόπος με τον οποίο ένα κράτος αντιμετωπίζει μία απειλή ή επιτίθεται σε ένα άλλο κράτος αποτελεί σημαντικό συντελεστή ισχύος, αλλά ταυτόχρονα και αχίλλειο πτέρνα του συστήματος του.Η ανάγκη των κρατών για προστασία από τις κυβερνοεπιθέσεις,ώθησε τα κράτη να δημιουργήσουν συνεργασίες ανάμεσα στον ιδιωτικό τομέα και στην κοινωνία των πολιτών ,αλλά και για συνεργασίες αναμεταξύ τους, με σκοπό την ορθή λειτουργία τους σαν κράτη αλλά και την ευημερία των πολιτών τους.

[1] Σύμφωνα με τον Libicki «Κάποιος μπορεί να υποστηρίξει ότι μια κυβερνοεπίθεση είναι σαν κάτι άλλο που είναι σαφώς μια πράξη πολέμου, αλλά αν δεν υπάρξει μια παγκόσμια συναίνεση ότι μια τέτοια αναλογία είναι έγκυρη τότε μια κυβερνοεπίθεση δεν μπορεί να οριστεί ως πράξη πολέμου»[1]

Είναι φανερό πλέον ότι έχει «μπεί στο παιχνίδι» ένα νέο στρατηγικό όπλο , ο Κυβερνοπόλεμος[2]. Κάθε εποχή χαρακτηρίζεται από μία νέα μορφή πολέμου και ο κυβερνοπόλεμος χαρακτηρίζει την εποχή της πληροφόρησης. Η δομή του Κυβερνοχώρου[3] είναι κατά βάση χαοτική και η απουσία μίας ανώτατης ρυθμιστικής αρχής θα ήταν καταστροφική από πλευράς άμυνας για ένα κράτος. Στο νέο αυτό πεδίο του Κυβερνοχώρου δημιουργείται μια σειρά από ερωτήματα σχετικά με την πολιτική δράση, το ρόλο του κράτους, τη διεύρυνση της έννοιας της ασφάλειας, την ανάγκη αναθεώρησης του διεθνούς δικαίου και το μεταβαλλόμενο χαρακτήρα του πολέμου. Με την ταυτοποίηση του κυβερνοχώρου ως νέο «πεδίο πολέμου» σε διεθνές επίπεδο, είναι πλέον ευρέως αποδεκτό ότι οι παραδοσιακοί κανόνες του Διεθνούς Ανθρωπιστικού Νόμου είναι επίσης εφαρμόσιμοι στις Επιθέσεις Δικτύων Υπολογιστών (Computer Network Attacks-CNAs). Η ταυτοποίηση αυτή δημιουργεί πολλές ομοιότητες ανάμεσα στον κινητικό πόλεμο[4] και στον κυβερνοπόλεμο.Μερικές αρχές του κινητικού πολέμου εφαρμόζονται στον κυβερνοπόλεμο, ενώ μερικές μπορεί στην πραγματικότητα να είναι ανταγωνιστικές προς αυτόν.

[2] Θα δωθεί ορισμός στο κεφάλαιο 2.1.

[3] Σύμφωνα με τον Dan Kuehl κυβερνοχώρο είναι ένα λειτουργικό πεδίο του οποίου ο ξεχωριστός και μοναδικός χαρακτήρας πλαισιώνεται από την χρήση ηλεκτρονικών και του ηλεκτρομαγνητικού φάσματος για να δημιουργήσει, να τροποποιήσει, να ανταλλάξει και να εκμεταλλευτεί πληροφορίες μέσω διασυνδεδεμένων συστημάτων που βασίζονται στην τεχνολογία πληροφοριών και επικοινωνίας (ICT) και τις συναφείς υποδομές τους.[2]

[4] Ορίζουμε τον κινητικό πόλεμο ως ένα πόλεμο που πραγματοποιείται στην ξηρά, τον αέρα, την θάλασσα και το διαστημικό χώρο. Όλα τα στρατιωτικά τανκ, πλοία, αεροπλάνα και στρατιώτες είναι οι πρωταγωνιστές του κινητικού πολέμου.[2]

2 *Έννοια και Γενικά Στοιχεία του Κυβερνοπολέμου*

2.1 Ορισμός

Για τον όρο «Κυβερνοπόλεμος» υπάρχουν διάφοροι ορισμοί που μπορούν να τον εξηγήσουν .Αρχικά σύμφωνα με τον Lachow, «ο όρος κυβερνοπόλεμος εστιάζεται περισσότερο στις «στρατιωτικές πτυχές του ανταγωνισμού»:

«ο κυβερνοπόλεμος αναφέρεται στη διεξαγωγή και την προετοιμασία για τη διεξαγωγή, στρατιωτικών επιχειρήσεων σύμφωνα με τις αρχές που σχετίζονται με πληροφορίες. Σημαίνει διατάραξη αν όχι καταστροφή των συστημάτων πληροφοριών και επικοινωνιών, με την ευρεία έννοια οριζόμενα να περιλαμβάνουν ακόμα και στρατιωτική κουλτούρα, στην οποία ο αντίπαλος στηρίζεται για να «γνωρίσει» από μόνος του.»[3]

Επιπρόσθετα ένας άλλος ορισμό που τον επεξηγεί είναι:

«Ένας αγώνας μεταξύ αντιτιθέμενων πλευρών που κάνουν χρήση τεχνολογίες και μεθόδους δικτύου για να αγωνιστούν για ένα πλεονέκτημα πληροφοριών στα πεδία της πολιτικής, οικονομικών, στρατιωτικών υποθέσεων και τεχνολογίας»[3]

Τέλος ο κυβερνοπόλεμος ορίζεται από τον στρατό των ΗΠΑ ως κάθε στρατιωτική πράξη που περιλαμβάνει τη χρήση ηλεκτρομαγνητικής και κατευθυνόμενης ενέργειας για τον έλεγχο του ηλεκτρομαγνητικού φάσματος ή για επίθεση στον εχθρό.Αποτελείται από τις παρακάτω τρεις κύριες συνιστώσες:

- Τη ηλεκτρονική προστασία (ΗΠ):που περιλαμβάνει παθητικά και ενεργά μέσα για την προστασία του προσωπικού και του εξοπλισμού από εχθρικό ΗΠ.

- Τη ηλεκτρονική υποστήριξη (ΗΥ) : περιλαμβάνει την υποκλοπή των ηλεκτρονικών εκπομπών του αντιπάλου για περαιτέρω εκμετάλλευση.

- Τη ηλεκτρονική επίθεση (ΗΕ)[5]: Η επίθεση σε δίκτυα ηλεκτρονικών υπολογιστών και η χρήση βίας κατά το διεθνές δίκαιο,δηλαδή η επίθεση σε δίκτυα Η/Υ με την χρήση των Η/Υ ως όπλα.[4]

2.2 Χαρακτηριστικά

Ο κυβερνοπόλεμος ,όπως και κάθε άλλη μορφή πολέμου έχει κάποια χαρακτηριστικά που τον κάνει να ξεχωρίζει από τους άλλους πολέμους.Ο κυβερνοπόλεμος σαν μία νέα μορφή πολέμου έχει κάποια ιδιαίτερα χαρακτηριστικά.Ορισμένα από αυτά είναι τα ακόλουθα[1]:

- Δεν υπάρχουν ενήμερες, ανοιχτές, δημόσιες ή πολιτικές συζητήσεις για το τι θα συνιστούσε μία δεοντολογική και συνετή πολιτική χρήσης τέτοιων όπλων.
- Είναι πολύ δύσκολο να προσδιοριστεί η πηγή των κυβερνοεπιθέσεων,το λεγόμενο «πρόβλημα της απόδοσης (attribution problem)».
- Πολλές κυβερνοεπιθέσεις δεν θα είναι φονικές και δεν θα προκαλέσουν καν μόνιμη ζημιά σε φυσικά (υλικά) αντικείμενα. Αυτό είναι βέβαια άκρως ανόμοιο με τα πυρηνικά όπλα και με όλα σχεδόν τα παραδοσιακά όπλα του πολέμου.
- Δεν υπάρχουν «εξωτικές» μονάδες κυβερνοόπλων (cyberweapons), και πάλι πολύ ανόμοια με τα πυρηνικά και τα άλλα όπλα προηγμένης τεχνολογίας, και ανόμοια ακόμα και με τα χημικά ή τα βιολογικά όπλα. Οποιοσδήποτε υπολογιστής είναι ένα δυνητικό κυβερνοόπλο και οποιοσδήποτε με προχωρημένη γνώση πληροφοριακών συστημάτων είναι ένας δυνητικός κυβερνοπολεμιστής.
- Η άμυνα είναι ακριβή και ευπαθής σε αποτυχία, ενώ η επίθεση είναι περίπου το ίδιο φθηνή: αυτό είναι παρόμοιο με τις γνωστές δυσκολίες με την πυρηνική πολιτική προστασία, με τις αντι-πυραυλικές τεχνολογίες, τη θωράκιση του σώματος, την προστασία απέναντι σε αυτοσχέδιους εκρηκτικούς μηχανισμούς.
- Ο χαμηλός βαθμός βεβαιότητας για το τι θα συμβεί με μία επίθεση, ή σε έναν πόλεμο.
- Οι μακρινές, βλαβερές παρενέργειες (παράπλευρες απώλειες) που δεν μπορούν επαρκώς να προβλεφθούν –ασθένεια, οικονομικές συνέπειες και ούτω καθεξής.

Πίσω από το δεύτερο χαρακτηριστικό,δηλαδή το «πρόβλημα της απόδοσης (attribution problem)», συναντάται η ανωνυμία.
Η ανώνυμη διαδικτυακή έκφραση αποτελεί χωρίς αμφιβολία δικαίωμα που προστατεύεται από τον νόμο. Ωστόσο, η συχνή της κατάχρηση δοκιμάζει την ελευθεριότητα του κυβερνοχώρου. Η ελευθερία έκφρασης κατοχυρώνεται στο Ελληνικό Σύνταγμα και στις διεθνείς συνθήκες προστασίας των ανθρωπίνων δικαιωμάτων (14 § 1 Σ, 10 § 1 ΕΣΔΑ, 19 § 2 ΔΣΑΠΔ, 11 ΧΘΔΕΕ). Η ανώνυμη διαδικτυακή επικοινωνία δεν είναι μόνο συνταγματικά κατοχυρωμένο δικαίωμα αλλά και αντικείμενο προστασίας που θεσπίζουν τα άρθρα 9Α Σ για την προστασία

[5] Αναλύεται στο κεφάλαιο 4.1.

των προσωπικών δεδομένων και 19 Σ για την προστασία του απορρήτου των επικοινωνιών καθώς και οι εκτελεστικοί αυτών νόμοι.[5]

Η ανωνυμία είναι μία λέξη που διχάζει τις απόψεις.Για άλλους είναι αρνητικό ,ενώ για άλλους θετικό.Αναλυτικά από τη μία δυσκολεύεται ο εντοπισμός εγκληματιών στον κυβερνοχώρο ή ακόμα και η ανίχνευση πηγών των επιθέσεων.Από την άλλη η ανωνυμία προσφέρει την ιδιωτικότητα και την εχεμύθεια κυριώς μεταξύ χάκερς ,στρατιωτικούς αξιοματούχους και της ευνικής ασφάλειας.

Η κατάργηση της ανωνυμίας είναι τεχνικά αδύνατη αφού παραβιάζεται η ατομική ελευθερία και οι ομάδες των δικαιωμάτων της ιδιωτικής ζωής,όπως προαναφέραμε παραπάνω.

Η ανωνυμία και το απόρρητο των χρηστών του διαδικτύου ήταν στόχος συζήτησης στις 15 Ιουλίου 2010.Η Βουλή των Αντιπροσώπων, η Επιτροπή στην Επιστήμη και την Τεχνολογία, η Υποεπιτροπή στην Τεχνολογία και την Καινοτομία των ΗΠΑ δεν έλειψαν από αυτή τη συζήτηση.

Συγκεκριμένα ο Robert Knake συνεργάτης Διεθνών Υποθέσεων στο Συμβούλιο Εξωτερικών Σχέσεων, αναφέρει ότι η απόδοση αντί να εντοπίζει το ακριβές πρόσωπο που πραγματοποίησε μια καταστροφική κυβερνοεπίθεση, άλλες χώρες μπορεί να θεωρούν μια μη συνεργάσιμη χώρα υπαίτια για τη μη έρευνα μιας κυβερνοεπίθεσης που εντοπίστηκε στη δικαιοδοσία της.[3]

Συμπληρωματικά ο Marc Rotenberg, Πρόεδρος του Κέντρου Πληροφόρησης Ηλεκτρονικού Απορρήτου, Τέλος έκλεισε με την κατάσταση που επικρατούσε όπου η θέσπιση απαιτήσεων απόδοσης για την αντιμετώπιση θεμάτων κυβερνο ασφάλειας χρησιμοποιήθηκε για να παρακολουθούνται οι δραστηριότητες πολιτών και να πατάχθουν αμφιλεγόμενες πολιτικές απόψεις.[3]

Ένα παράδειγμα της χρήσης των εργαλείων ανωνυμίας είναι το TOR. Το έργο TOR είναι μια online εφαρμογή λογισμικού που επιτρέπει στους πολίτες την ανώνυμη πρόσβαση στο διαδίκτυο. Λειτουργεί διανέμοντας τα «πακέτα» με την πληροφορία που στέλνουμε ή λαμβάνουμε στο Internet μέσα από ένα δίκτυο που αποτελείται κυρίως από άλλους χρήστες του δικτυου, έτσι ώστε να χάνεται η πληροφορία της αρχικής προέλευσης του κάθε πακέτου. Επίσης εφαρμόζεται κρυπτογραφία από άκρη σε άκρη, κάνοντας αδύνατη την παρακολούθηση της πληροφορίας από τρίτους. Αυτά τα εργαλεία ανωνυμίας είναι ορατά και πολλά είναι διαθέσιμα δωρεάν για να τα αποκτήσει κανείς μέσω του Διαδικτύου. Προστατεύει από μια κοινή μορφή παρακολούθησης στο Διαδίκτυο γνωστή ως «ανάλυση κυκλοφορίας δεδομένων.» Η ανάλυση κυκλοφορίας δεδομένων μπορεί να χρησιμοποιηθεί για να βρεθεί ποιος μιλάει με ποιον σε ένα δημόσιο δίκτυο. Αυτές οι πληροφορίες είναι κρίσιμες για την ανάλυση κυκλοφορίας δεδομένων, διότι γνωρίζοντας την προέλευση και τον προορισμό της κυκλοφορίας σας στο Διαδίκτυο επιτρέπει σε άλλους να παρακολουθούν τη συμπεριφορά και τα ενδιαφέροντά σας.[6]

Τέλος καλό θα είναι να αναλύθει και το πέμπτο χαρακτηριστικό της αυτοάμυνας.

Το δικαίωμα της αυτοάμυνας χρησιμοποιείται σε περιπτώσεις κατά τις οποίες υπάρχει πραγματική ή επικείμενη ένοπλη επίθεση, είτε από κρατικούς παράγοντες είτε από μη κρατικούς

παράγοντες (τρομοκράτες) τέτοια ώστε τα μέτρα που λαμβάνει το αμυνόμενο κράτος να είναι ανάλογα τόσο προς την έκταση, όσο και ως προς την ένταση των επιθέσεως που δέχεται.

Η χρήση βίας είναι ένα θέμα που βρίσκεται σε αντίθεση στο άρθρο 51 και στο άρθρο 2§4.Επεξηγηματικά το άρθρο 2§4 απαγορεύει τη χρήση βίας ενώ το άρθρο 51 επιτρέπει την εκδήλωση ενεργειών αυτοάμυνας μόνο εναντίον ένοπλης επίθεσης σε αντίθεση με το 2§4.Η αντίθεση αυτή βρίσκει απάντηση στον καταστατικό Χάρτη του ΟΗΕ που λέει ότι εάν ασκηθεί παράνομη βία από ένα κράτος σε βάρος κάποιου άλλου και η βία αυτή δεν φθάνει στο επίπεδο της «ένοπλης επίθεσης» ή δεν ισοδυναμεί με τέτοια, τότε το κράτος – θύμα δεν μπορεί να ασκήσει, με τη σειρά του, βία επικαλούμενο αυτοάμυνα.Δεν είναι μόνο το άρθρο 2§4 που διαφέρει από το άρθρο 51. Ο αντίστοιχος κανόνας του εθιμικού δικαίου[6] επιτρέπει την αυτοάμυνα και ως ένα προληπτικό μέτρο (preventive measure)για επιθέσεις,υπο συγκεκριμένες προϋποθέσεις.Όσο αφορά την προληπτική αυτοάμυνα ο καθηγητής Dinstein[7] την συγκρίνει με την ανασχετική αυτοάμυνα που ασκείται για επιθέσεις υποκείμενες και πρακτικά μη αναστρέψιμες-αναπόφευκτες.Η ανασχετικη αυτοάμυνα εφαρμόζεται μόνο εάν στα δίκτυα του κράτους-στόχου γίνουν παράνομες και μη εξουσιοδοτημένες διεισδύσεις, χωρίς να προκληθούν απώλειες ή ζημιές,με αποτέλεσμα το κράτος-στόχος να βρίσκεται σε ολοκληρωτική ηλεκτρονική επίθεση ή και ένοπλη.[7]

Στο Εγχειρίδιο του Τάλιν, βάσει του άρθρου2(4) του χάρτη Καταστατικού των Ηνωμένων Εθνών[8] στον Κανόνα 10 αναφέρει ότι «μία κυβερνοεπιχείρηση που συνιστά απειλή ή χρήση στρατιωτικής δύναμης κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε Κράτους, ή που είναι με οποιονδήποτε άλλον τρόπο ασύμφωνη με τους σκοπούς των Ηνωμένων Εθνών, είναι παράνομη».Ενώ στο άρθρο 51 του Καταστατικού των Ηνωμένων Εθνών και Κανόνας 13 αναφέρει ότι «ένα Κράτος που είναι ο στόχος μίας κυβερνοεπιχείρησης που ισοδυναμεί με ένοπλη επίθεση μπορεί να εξασκήσει το εγγενές δικαίωμά του της αυτο-άμυνας. Το αν μία κυβερνοεπιχείρηση συνιστά ένοπλη επίθεση εξαρτάται από την κλίμακα και τα αποτελέσματά της».

Ένα κομμάτι της αυτοάμυνα που μπορεί να ασκήσει ένα κράτος-θύμα είναι και η προληπτική επίθεση,αν και μερικές φορές μπορεί να αμφισβητηθεί λόγω μη αξιόπιστης απόδοσης ευθυνών.Στην περίπτωση του κυβερνοπολέμου η απόδοση ευθυνών είναι δύσκολη αφού δεν υπάρχουν γρήγορα μέσα για τον εντοπισμό του δράστη σε μία κυβερνο-επίθεση.Ένα ακόμα είδος της αυτοάμυνας θεωρείται και η αποτροπή, και συγκεκριμένα εκείνη μέσω αντιποίνων ,η οποία λαμβάνει χώρα μόνο όταν ο υποψήφιος δράστης είναι κράτος.Η αποτροπή βασίζεται στη δυνατότητα του υποψηφίου θύματος να αντιδράσει θέτοντας σε κίνδυνο τα επικοινωνιακά και πληροφοριακά συστήματα ή τις κρίσιμες υποδομές του δράστη χρησιμοποιώντας την

[6] Με τον όρο "Άγραφος νόμος" (unwritten law, ungeschriebenes Recht) χαρακτηρίζεται το σύνολο των κανόνων δικαίου που δεν υπάρχουν κάπου γραμμένοι.
[7] Yoram Dinstein είναι ένας λόγιος και Ομότιμος Καθηγητής στο Πανεπιστήμιο του Τελ Αβίβ . Είναι ειδικός στο διεθνές δίκαιο, και ένας εξέχων αρχή σχετικά με τους νόμους του πολέμου.
[8] Ο Χάρτης των Ηνωμένων Εθνών υπογράφηκε στις 26 Ιουνίου 1945, στο Σαν Φρανσίσκο, στο τέλος της Συνδιασκέψεως των Ηνωμένων Εθνών για τη Διεθνή Οργάνωση, και άρχισε να ισχύει στις 24 Οκτωβρίου 1945. Το Καταστατικό του Διεθνούς Δικαστηρίου αποτελεί αναπόσπαστο τμήμα του Χάρτη.[8]

αξιοπιστία.Για να χρησιμοποιηθεί η αξιοπιστία κάποιου κράτους –θύματος θα πρέπει να στραφεί στις απειλές χρήσης κυβερνοαντιποίνων και στην επίδειξη των κυβερνοϊκανοτήτων του συνδυάζοντας τα και με άλλες μορφές αποτροπής.Σε αντίθετη περίπτωση που το κράτος –θύμα αδυναμεί και η μόνη λύση είναι η χρήση συμβατικών και μη μέσων πολέμου.

Σωστό θα είναι να αναφερθούμε και για το πότε κάποιο κράτος θα έχει το δικαίωμα αυτοάμυνας σε περίπτωση επίθεσης σύμφωνα με τις προϋποθέσεις του άρθρου 51.Ο Schmitt αναφέρειτρείς παράγοντες που πρέπει να ληφθούν υπόψιν[3] :

- Όταν η CNA είναι τμήμα μίας ευρύτερης επιχείρησης που κορυφώνεται σε ένοπλη επίθεση προδιαγραφών άρθρου 51.
- Όταν η CNA αποτελεί ένα μη-αναστρέψιμο στάδιο μίας επικείμενης, χρονικά άμεσης και με βάση τα υπάρχοντα στοιχεία αναπόφευκτης επίθεσης.
- Όταν ο αμυνόμενος ενεργεί μεν κατά τρόπο «προληπτικό», αλλά η αντίδρασή του βρίσκεται εντός του ύστατου διαθέσιμου χρονικού πλαισίου αντίδρασης (last possible window of opportunity) για την επιτυχή απόκρουση της επίθεσης. Εννοείται ότι εάν ο αμυνόμενος δεν αντιδράσει εντός αυτού του «last possible window of opportunity», δεν θα μπορεί πλέον να προβάλει σοβαρή αυτοάμυνα διότι θα έχει καταστραφεί.

2.3 Τεχνολογικό Πλαίσιο Του Πολέμου

Με το πέρασμα του χρόνου και με την πρόοδο της κυβερνοτεχνολογίας ο κυβερνοπόλεμος γίνεται όλο και πιο εξειδικευμένος και προσαρμόζεται σε κάθε περίσταση ξεχωριστά,με αποτέλεσμα οι επιπτώσεις στο θύμα κράτος να απέχει πολύ από εποχή σε εποχή,λόγω του τεχνολογικού υποβάθρου.Στον 21ο αιώνα που ζούμε παρατηρείται αλματώδης πρόοδος στις τεχνολογίες πληροφοριών. Ο αριθμός των ενεργών ανθρώπων στον κυβερνοχώρο είναι πολύ μεγάλος. Στατιστικές δείχνουν ότι από το 2000 μέχρι και σήμερα παρατηρείται αύξηση ποσοστού κατα 566% . Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) αναφέρει ότι «το τέλος του 2014, θα υπάρχουν σχεδόν 3 δισεκατομμύρια χρήστες του Διαδικτύου, με τα δύο τρίτα από αυτούς να προέρχονται από τον αναπτυσσόμενο κόσμο[…]ο αριθμός των κινητών-ευρυζωνικών συνδρομών θα φθάσει τις 2,3 δισεκατομμύρια παγκοσμίως[…]πενήντα πέντε τοις εκατό από αυτές τις συνδρομές αναμένεται να είναι στον αναπτυσσόμενο κόσμο». Έρευνα το 2012 έδειξε ότι «το 90% των δεδομένων του κόσμου δημιουργήθηκε μόνο τα τελευταία δύο χρόνια».[9]

2.4 Νομικό πλαίσιο του πολέμου

Το 1999 ο καθηγητής Michael Schmitt[9] πρότεινε επτά κριτήρια,τα οποία υιοθετήθηκαν για την αξιολόγηση μοντέλου κυβερνοπολέμου ,και έγιναν μάλιστα στόχος σκεπτικισμού και επιφυλακτικότητας για πολλούς ανθρώπους του Διεθνούς Δικαίου.[3]

Τα κριτήρια αυτά είναι:

- Η δριμύτητα /σφοδρότητα (severity) της επίθεσης.
- Χρονική αμεσότητα (immediacy) μεταξύ της επίθεσης και των αποτελεσμάτων.
- Αιτιακή αμεσότητα (directness)μεταξύ επίθεσης και αποτελεσμάτων.
- Διεισδυτικότητα της επίθεσης (invasiveness), για τις ηλεκτρονικές άμυνες του κράτους–στόχου.
- 'Μετρησιμότητα' (measurability)των ποσοτικών αποτελεσμάτων της επίθεσης.
- Έλλειψη κατ' αρχήν νομιμότητας (ή έστω νομιμοφάνειας) (presumptive legitimacy) της επίθεσης.
- Κρατική ευθύνη (responsibility) για την επίθεση.

Πολλά νομικά πλαίσια δεν έχουν άμεση εφαρμογή στον κυβερνοπόλεμο,γιατί στον κυβερνοπόλεμος έχουμε να κάνουμε με ζημιές και βλάβες στη λειτουργία πληροφοριακών και άλλων συστημάτων που δεν επιφέρουν βλάβη σε φυσικά (υλικά) αντικείμενα ή ανθρώπους.

Ένα νομικό πλαίσιο που συσχετίζεται με τον κυβερνοπόλεμο είναι η Θεωρία του Δίκαιου Πολέμου.Η Θεωρία αυτή διαιρείται σε δύο κύρια ζητήματα.Αρχικά υπάρχει το ζήτημα του πότε μία χώρα μπορεί ηθικά να πάρει μέρος σε, ή να ξεκινήσει, έναν πόλεμο: το δίκαιο προς πόλεμον (jus ad bellum).Συμπληρωματικά το δεύτερο ζήτημα έχει να κάνει με το αν κανείς βρεθεί στον πόλεμο πότε μπορεί να πολεμήσει ηθικά,που εδώ έχουμε να κάνουμε με το δίκαιο εν πολέμω (jus in bello).

Όπως είπαν και οι Dementis και Sousa (2010) «Οι κυβερνο συγκρούσεις μπορούν να αναλυθούν υπό το πρίσμα δύο τομέων του διεθνούς δικαίου: το *jus ad bellum*, γνωστό και ως το δίκαιο διαχείρισης συγκρούσεων και το *jus in bello*, το δίκαιο του πολέμου. Το *jus ad bellum* είναι το δίκαιο που διέπει τη λύση ανάγκης στη χρήση βίας-είτε η βία είναι επιτρεπτή ή όχι, και το *jus in bello* είναι το δίκαιο που διέπει δραστηριότητες όταν το *jus ad bellum* έχει καθορίσει να χρησιμοποιηθεί η βία».[3]

Αναλυτικά για το πρώτο ζήτημα τα κριτήρια που ισχύουν στην περίπτωση αυτή είναι:

- Η Δίκαιη Αιτία
- Η Έσχατη Λύση
- Η Πιθανότητα Επιτυχίας

[9] Μιχαήλ Ν Schmitt είναι ένας διεθνής μελετητής του νόμου που ειδικεύεται στο διεθνές ανθρωπιστικό δίκαιο και η χρήση των θεμάτων βίας.

- Η Αναλογικότητα
- Η Αρμόδια Αρχή
- Η Σωστή Πρόθεση

Ένα παράδειγμα που θα βοηθήσει στην κατανόηση της ηθικότητας του πολέμου,δηλαδή της Θεωρίας του Δίκαιου Πολέμου, είναι το παρακάτω:

Έστω η χώρα Β αντεπιτίθετε στη χώρα C με μία κυβερνοεπίθεση ή μία συμβατική επίθεση, μετά από μία κυβερνοεπίθεση από την C.Για να θεωρηθεί η πράξη της Β ηθική θα πρέπει :

- Η επίθεση της C κατά της Β να ήταν άδικη και μη αμελητέα.
- Η πηγή της επίθεσης από τη C, με συντριπτική πιθανότητα, να διατάχθηκε ή να επιτράπηκε από τα υψηλότερα επίπεδα μίας κυβέρνησης.
- Αρκετά μέτρα να είχαν ληφθεί από τη χώρα Β για την πρόληψη ή την ελαχιστοποίηση της κυβερνοβλάβης που θα μπορούσε να προκαλέσει μία εχθρική χώρα ή ένας άλλος, εκτός κρατών, επιτιθέμενος μέσω του κυβερνοχώρου (χάκερς με μαύρο ή γκρι καπέλο).
- Η προσδοκώμενη ζημιά στον εχθρό (C) να είναι πιθανό να είναι ισοδύναμη με τη ζημιά που έπαθε η Β, ή να είναι η ελάχιστη αναγκαία για να σταματήσει η συνέχιση των κυβερνοεπιθέσεων.

Αν αναλύσουμε τις παραπάνω περιπτώσεις του παραδείγματος θα λυθούν πολλές απορίες.Στην περίπτωση που η επίθεση της C κατά της Β ήταν άδικη και μη αμελητέα και της δημιουργούσε ζημιά τότε κρίνουμε το είδος της ζημιάς.Εάν η ζημιά ήταν επιθετικής φύσεως τότε θεωρείται επουσιώδης ζημιά,ενώ αν είναι αμυντικής φύσεως τότε θα έπρεπε να μετρηθεί με το μέγεθος της αυξημένης ευπάθειας ή της ζημιάς στον πολιτικό πληθυσμό.Στην περίπτωση τώρα που η πηγή της επίθεσης από τη C, να διατάχθηκε ή να επιτράπηκε από τα υψηλότερα επίπεδα μίας κυβέρνησης, τότε, εάν η εθνικότητα IP μπορεί να προσδιοριστεί με μεγάλη πιθανότητα, η πηγή είναι πολύ πιθανό να είναι η ίδια η κυβέρνηση.Η τελευταία συνθήκη που αναφέρεται στο μέγεθος της ζημιάς δεν έχει γίνει τελείως ξεκάθαρη, αφού δεν υπάρχουν στοιχεία για μεγάλη ζημιά ώστε να δικαιολογεί μία μεγάλης κλίμακας συμβατική επίθεση,όπως μεγάλος αριθμός θανάτων ή η μη αναστρέψιμη παράλυση μίας οικονομίας ή ενός ζωτικού οικονομικού τομέα.

2.5 Διεθνείς Θέσεις για τον Κυβερνοπόλεμο

2.5.1 Ηνωμένες Πολιτείες Αμερικής(ΗΠΑ)

Σύμφωνα με μία έκθεση στο Κογκρέσο οι κυβερνοεπιθέσεις που γίνονταν ενάντια στην Κυβέρνηση των ΗΠ αυξάνονταν ραγδαία το 2009.Η έκθεση αυτή αναφέρει[3]:

- Την ύπαρξη υποψίας ότι πολλές από αυτές τις επιθέσεις προέρχονταν από το Κινέζικο κράτος και κρατικο-επιδοτούμενες οντότητες.

- Κατά τη διάρκεια του 2008, υπήρξαν σύνολο 54640 κυβερνοεπιθέσεις ενάντια στο Υπουργείο Άμυνας των ΗΠΑ.
- Κατά το πρώτο μισό του 2009 υπήρξαν 43785 κυβερνο περιστατικά που στόχευαν το Υπουργείο Άμυνας, όπως αναφέρει η έκθεση

Με βάση τις προτάσεις και τα προβλήματα που υπόθηκαν στην έκθεση βγήκαν και μερικά συμπεράσματα.Ορισμένα από αυτά είναι τα εξής:

- Οι κυβερνοεπιθέσεις που προέρχονται από την Κίνα αψηφούν την εύκολη ταξινόμηση.
- Η κυβερνοεπίθεση μπορεί να αναγνωριστεί από ποιόν προήλθε αφού τα κυβερνοπεριστατικά αφήνουν πίσω υπογραφές που μπορούν, με την εγκληματολογική ανάλυση, να αποκαλύψουν κάποιες φορές την υπαγωγή των υπεύθυνων δραστών σε έναν λογικό βαθμό βεβαιότητας και βοηθά να συμπληρωθεί η κατανόηση των επιτιθέμενων και των συνδέσμων τους.

Τέλος ενδιαφέρον ήταν και οι παρατηρήσεις που έγιναν από τον Dennis Blair[10] στην επιτροπή[3]:

- Ευαίσθητες πληροφορίες «κλέβονται καθημερινά τόσο από τα δίκτυα της κυβέρνησης όσο και του ιδιωτικού τομέα.»

- Οι ΗΠΑ δεν μπορούν να είναι βέβαιες ότι οι υποδομές κυβερνοχώρου τους θα είναι διαθέσιμες και αξιόπιστες σε μια κρίση.

- Οι ΗΠΑ και ο κόσμος έρχονται αντιμέτωποι με μια μεγαλύτερη τρωτότητα στη διαταραχή ως αποτέλεσμα της τάσηςπρος τη σύγκλιση της φωνής, του φαξ, του βίντεο, των υπολογιστών και των ελέγχων με τα οποία λειτουργούν οι κρίσιμες υποδομές σε ένα μόνο δίκτυο: το Διαδίκτυο. Αυτά περιλαμβάνουν και την τραπεζική, την ενέργεια και την ύδρευση.

- Οι κυβερνοαπειλές είναι όλο και πιο διακριτικές και περίπλοκες. Τον προηγούμενο χρόνο είδαμε την ανάπτυξη του «αυτο-τροποποιούμενου κακόβουλου λογισμικού, το οποίο εξελίσσεται για να καταστήσει τις παραδοσιακές τεχνολογίες ανίχνευσης ιού λιγότερο αποτελεσματικές.»

Επιπρόσθετα η κυβέρνηση των ΗΠΑ ανέπτυξε την έννοια της κυβερνοασφάλειας, την ανάπτυξη μίας συνολικής προσέγγισης και την υλοποίησή της σε λύσεις υψηλής τεχνολογίας, τέτοια ώστε να μπορεί να αντιμετωπίσει τις διάφορες προκλήσεις του κυβερνοπολέμου, με δεδομένα τα παραδοσιακά σημεία της και τα ιδιωτικά συστήματά της.

Μία από τις πιο σοβαρές προκλήσεις των ΗΠΑ για την εθνική ασφάλεια είναι η κυβερνοασφάλεια[11],και όπως λέει και ο πρόεδρος των ΗΠΑ, Barack Obama, οι ΗΠΑ δεν είναι

[10] Είναι ο πρώην Διευθυντής της Εθνικής Υπηρεσίας Πληροφοριών των ΗΠΑ και ένας συνταξιούχος ναυτικός ναύαρχος ο οποίος ήταν ο διοικητής των αμερικανικών δυνάμεων στην Ειρηνικού περιοχή.

ολοκληρωτικά προετοιμασμένοι να ανταπεξέλθουν σε αυτήν αφού δεν υπάρχει μία συγκεκριμένη εθνική πολιτική κυβερνοασφάλειας και κάποιος οργανισμός που να στοχεύει στο σκοπό αυτό με κάποιες ευθύνες και αρμοδιότητες.[10]

Άλλες εξίσου σημαντικές προκλήσεις είναι οι παρακάτω :

- Η εγκαθίδρυση μίας άμυνας πρώτης γραμμής κατά των άμεσων απειλών με τη διαμόρφωση ή ενίσχυση της κοινής αντίληψης για τις ευπάθειες των δικτύων.
- Η άμυνα απέναντι σε ένα πλήρες φάσμα απειλών με τον εμπλουτισμό των δυνατοτήτων της αμερικανικής αντικατασκοπείας.
- Η ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας για βασικές τεχνολογίες πληροφορίας.
- Η ενίσχυση του μελλοντικού περιβάλλοντος κυβερνοασφάλειας με τη διεύρυνση της κυβερνοεκπαίδευσης.
- Ο συντονισμό και την ανακατεύθυνση των προσπαθειών έρευνας και ανάπτυξης σε όλο το εύρος της Ομοσπονδιακής Κυβέρνησης.
- Η εργασία για τον καθορισμό και την ανάπτυξη στρατηγικών για την αποτροπή εχθρικής ή κακόβουλης δραστηριότητας στον κυβερνοχώρο.
- Η ανάπτυξη μιας δυνατότητας γρήγορης αντίδρασης και μιας αποτελεσματικής αντιμετώπισης κυβερνοδραστηριοτήτων από εχθρικές οντότητες.

2.5.2 Ρωσία

Το Πανεπιστήμιο της Μόσχας και ειδικά το τμήμα διεθνούς πολιτικής σε συνεργασία με το ινστιτούτο προβλημάτων διεθνούς ασφάλειας (IISP) διεξήγαγαν μελέτη σχετικά με τους κυβερνοπολέμους και τη διεθνή ασφάλεια η οποία εγκρίθηκε από το υπουργείο άμυνας της

[11] Ο ορισμός του DOD (Department of Defense =Υπουργείο Άμυνας των ΗΠΑ) των ΗΠΑ «Κυβερνοασφάλεια είναι όλες οι οργανωμένες ενέργειες οι οποίες απαιτούνται για να εξασφαλιστούν οι πληροφορίες από κάθε κίνδυνο ή ρίσκο σε όλες τους τις μορφές (ηλεκτρονικές, φυσικές), καθώς και για να εξασφαλιστούν τα συστήματα και τα δίκτυα, μέσω των οποίων γίνεται η αποθήκευση, η ανάκτηση, η επεξεργασία και η μεταφορά τους, περιλαμβανομένων των ενεργειών οι οποίες πρέπει να γίνονται, ώστε να προφυλάσσονται από εγκληματικές ενέργειες, δολιοφθορές, κατασκοπεία, ατυχήματα, και αστοχίες. Στους κινδύνους για τη Κυβερνοασφάλεια πρέπει να συμπεριληφθούν κι αυτοί που αφορούν την μείωση της εμπιστοσύνης και αξιοπιστίας των παροχέων προς τους πελάτες τους και οι οποίοι αν δεν αντιμετωπιστούν, είναι δυνατόν να επηρεάσουν αρνητικά τη σταθερότητα και περαιτέρω ανάπτυξη των πελατών τους, παραβιάζοντας την προστασία της ταυτότητας και ιδιωτικότητας των ίδιων των πελατών και των συνεργατών τους, αποδιοργανώνοντας την δυνατότητα ή επικοινωνίας ή διεξαγωγής επαγγελματικών συναλλαγών, επηρεάζοντας δυσμενώς την υγεία και προκαλώντας απώλειες και επηρεάζοντας δυσμενώς τις επιχειρήσεις της εθνικής κρίσιμης υποδομής.»[11]

χώρας.Η έρευνα αυτή ενσωμάτωσε τον κυβερνοπόλεμο σε έναν πόλεμο πληροφορίας[12] που επικεντρώνεται σε επιθέσεις κατά των συστημάτων διοίκησης –ελέγχου και λήψης αποφάσεων χωρίς να παραλείπει και τις ανθρώπινες διεργασίες.

Πιο συγκεκριμένα εστίασε στις αρχές των κυβερνοεπιχειρήσεων και άλλων δραστηριοτήτων στον κυβερνοχώρο.Ανέλυε τις κύριες ιδεολογικές και οργανωτικές δομές του κυβερνοπολέμου καθώς και την ανάπτυξη μίας στρατιωτικής δύναμης και των βασικών αρχών των κινεζικών στρατηγικών του κυβερνοπολέμου.Συμπερασματικά πάνω στην προαναφερθείσα έρευνα η ανάπτυξη μίας αντίδρασης σε αυτές τις περιπτώσεις πρέπει να οργανωθεί πάνω σε μία διεπιστημονική βάση και να περιλαμβάνει ερευνητές από διαφορετικούς κλάδους –πολιτικούς αναλυτές, κοινωνιολόγους, ψυχολόγους, στρατιωτικούς ειδικούς, και εκπροσώπους των ΜΜΕ αφού οι επιπτώσεις αυτές συμπεριλαμβάνονται σε ένα μεγάλο εύρος.[10]

Συμπληρωματικά στην συνεργασία μεταξύ της Ρωσίας και των ΗΠΑ συζητήθηκαν:

- Η τοποθέτηση ευθύνης στα μεμονωμένα κράτη να παρακολουθούν τα δικά τους δίκτυα,και
- Η διερεύνηση των δικών τους εγκληματιών μετά την υιοθέτηση ενός εγχώριου δικαίου Κυβερνοεγκλήματος και του δικαίου του πολέμου και οι άλλες μορφές δικαίου (δίκαιο της θάλασσας, του διαστήματος, το παράδειγμα πυρηνικού πολέμου).

Είναι οφθαλμοφανές ότι οι περισσότερες κυβερνοεπιθέσεις που γίνονται δεν θα είναι ανιχνεύσιμες στις πράξεις ενός έθνους κράτους και παρόλο που μπορεί να είναι δυνατόν να εντοπιστεί η τοποθεσία από όπου η επίθεση εξαπολύθηκε, τα υπεύθυνα άτομα και οι υπεύθυνοι για τη λήψη αποφάσεων είναι πολύ πιο δύσκολο να ανιχνευθούν δεδομένων των τρέχοντων τεχνολογικών εργαλείων και τεχνικών.

Σε μία τέτοια εποχή που οι κυβερνοεπιθέσεις και οι αμυντικές επιθέσεις των εθνών αυξάνονται ολοένα και πιο πολύ το γνωμικό του Γκάντι «οφθαλμός αντί οφθαλμού και σύντομα όλος ο κόσμος θα είναι τυφλός» βρίσκει εφαρμογή.

2.5.3 Ομάδας Κυβερνητικών Εμπειρογνωμώνων

Σύμφωνα με τα πρόσφατα θεσμικά έγγραφα σε Ευρωπαϊκό και Διεθνές επίπεδο και με τους παραδοσιακούς κανόνες του Διεθνούς Δικαίου οι Επιθέσεις κατά Δικτύων Υπολογιστών (CNAs) συμπεριλαμβάνονται στο Διεθνές Δίκαιο.Πιο συγκεκριμένα, τόσο στο Ευρωπαϊκό όσο και στο Διεθνές επίπεδο, η επικρατέστερη άποψη είναι ότι το διεθνές δίκαιο σχετίζεται με τις επιχειρήσεις στον κυβερνοχώρο. Δεν έλλειψε επίσης και η συμφωνία της Διεθνής Ομάδα Εμπειρογνωμόνων για την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο.

[12] Ο Lachow τον όρισε ως εξής: «ο πόλεμος πληροφοριών μπορεί να κατανοηθεί ότι αναφέρεται στην κυβερνοσύγκρουση στο επίπεδο του έθνους-κράτους περιλαμβάνοντας είτε άμεση στρατιωτική αντιπαράθεση ή έμμεσο ανταγωνισμό μέσω διατάραξης και εξαπάτησης.»[3]

Η Ομάδας Κυβερνητικών Εμπειρογνωμώνων[13] ένα ψήφισμα με θέμα «Εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στα πλαίσια της διεθνούς ασφάλειας»αναφέρουν σε μια έκκληση για μεγαλύτερη διεθνή συνεργασία μεταξύ των Κρατών, του ιδιωτικού τομέα και της κοινωνίας των πολιτών μέσα από συγκεκριμένα μέτρα:[3]

- Αφιέρωση σημαντικής «προσοχής σε μη εγκληματικές περιοχές διακρατικού ενδιαφέροντος όπως είναι ο κίνδυνος της εσφαλμένης εκτίμησης που προκύπτει από την έλλειψη κοινής αντίληψης όσον αφορά τις διεθνείς νόρμες σχετικά με την κρατική χρήση των ΤΠΕ, το οποίο θα μπορούσε να επηρεάσει την διαχείριση κρίσης σε περίπτωση μείζωντον περιστατικών.»
- Σχεδιασμός με σκοπό την ανταλλαγή των καλύτερων πρακτικών, τη διαχείριση συμβάντων, την οικοδόμηση εμπιστοσύνης, τη μείωση κινδύνου και την ενίσχυση της διαφάνειας και της σταθερότητας.»
- Αποτροπή της οικοδόμησης των ικανοτήτων για την παροχή βοήθειας σε αναπτυσσόμενες χώρες στην προσπάθειά τους να ενισχύσουν την ασφάλεια των κρίσιμων εθνικών υποδομών πληροφοριών και να γεφυρώσουν το σημερινό χάσμα στην ασφάλεια των ΤΠΕ.

2.5.4 Scott Shackelford

Ο Scott Shackelford[14] προτείνει ορισμένες μακροπρόθεσμες και βραχυπρόθεσμες προσεγγίσεις σχετικά με τις κυβερνοεπιθέσεις και τη κυβερνοσύγκρουση με την χρήση ενός συνεκτικού νομικού καθεστώτος.

Σύμφωνα με τον Shackelford μία μακροπρόθεσμη προσέγγιση θα ήταν μια πολυμερής συνθήκη στην κυβερνο ασφάλεια.Συγκεκριμένα ανέφερε ότι «Δεδομένου του συγκεχυμένου νομικού καθεστώτος, ο καλύτερος τρόπος να εξασφαλιστεί ένα περιεκτικό καθεστώς είναι μέσω από μια νέα διεθνή συμφωνία που να ασχολείται αποκλειστικά με την κυβερνοασφάλεια και το καθεστώς της στο διεθνές δίκαιο.»[3]

Μία τέτοια συνθήκη θα πρέπει να ορίζει πότε μια κυβερνοεπίθεση ανέρχεται στο επίπεδο μιας ένοπλης επίθεσης,να ξεκαθαρίζει ποιες διατάξεις του διεθνούς δικαίου εφαρμόζονται κατά τη διάρκεια ενός κυβερνοπολέμου και να παρέχει μηχανισμούς επιβολής στην περίπτωση παραβίασης.Τέλος θα πρέπει να διερευνεί ποια κράτη είναι πίσω από τις κυβερνοεπιθέσεις και να έχει την αμυντική τεχνογνωσία που χρειάζεται για να είναι ταχείς ανταποκριτές όταν συμβαίνουν δριμείς επιθέσεις.

Το τελευταίο κριτήριο για να πραγματοποιηθεί χρειάζεται τη συγκρότηση μιας Πολυεθνική Ομάδα Απόκρισης Κυβερνο Έκτακτης Ανάγκης (MCERT) για να μπορεί να δικτυώνει μεταξύ τους τα τρέχοντα δίκτυα των πάνω από 250 εθνικά δίκτυα ομάδων CERT μαζί με την ομάδα CERT του NATO που βρίσκεται στην Εσθονία.

[13] Ο όρος αυτός περιγράφει την κυβέρνηση που αποτελείται από ένα μη πολιτικό σώμα, συνήθως υποστηρίζονται από τις πολιτικές δυνάμεις και λειτουργεί σε καταστάσεις έκτακτης ανάγκης, όταν το κομματικό σύστημα δεν έχει επιτυχία στην ενσωματώνει ένα πλήρως λειτουργικό υπουργικό συμβούλιο.
[14] Αναπληρωτής Καθηγητής Εμπορικού Δικαίου και Ηθικής[12]

Αντίθετα μία βραχυπρόθεσμη προσέγγιση είναι μία πολύπλευρη συνεργασία ασφάλειας του ΝΑΤΟ με το παγκόσμιο δίκτυο των CERT με σκοπό να ξεριζώνει κρατικές επιχορηγήσεις κυβερνοεπιθέσεων,να υπερασπίζεται καλύτερα ενάντια στις κυβερνοεπιθέσεις μέσω της συγκέντρωσης πόρων και ταλέντου, και να παρέχει πολύτιμες πληροφορίες για να ξεπεραστεί το θεμελιώδες ζήτημα της απόδοσης.

3 *Διαφορές Κινητικού Πολέμου με τον Κυβερνοπόλεμο & οι Αρχές τους*

3.1 Εφαρμογή Αρχών Κινητικού Πολέμου στον Κυβερνοπόλεμο

Σύμφωνα με την Agence France Presse (Sydney, 31 January 2010)«Εάν κάποιος έβαζε βόμβα στο ηλεκτρικό δίκτυο στη χώρα μας και βλέπαμε τους βομβιστές να μπαίνουν σε αυτό θα ήταν καθαρά μια πράξη πολέμου. Αν η ίδια χώρα χρησιμοποιεί εξειδικευμένους υπολογιστές για να ρίξει το ηλεκτρικό δίκτυο, σίγουρα θα σκεφτόμουν ότι πλησιάζουμε στο να το ονομάσουμε πράξη πολέμου.»[3]

Από το παραπάνω παρατηρούμε ότι πολλές αρχές του κινητικού πολέμου βρίσκουν εφαρμογή στον κυβερνοπόλεμο.Παρακάτω παρατίθενται μερικές από αυτές.[2]

3.1.1 Κινητική αρχή του σκοπού

Η κινητική αρχή του σκοπού διευθύνει κάθε στρατιωτική επιχείρηση προς έναν καθοριστικό, αποφασιστικό και εφικτό σκοπό. Αυτό είναι σίγουρα εφαρμόσιμο στον κυβερνοπόλεμο. Τα ανταγωνιστικά πρότυπά μας συμπεριλαμβάνουν την αρχή του σκοπού ως μέρος όλων των αντιπάλων εκτός από μη εξελιγμένους επιτιθέμενους.

3.1.2 Κινητική αρχή της επίθεσης

Η κινητική αρχή της επίθεσης αδράνει, διατηρεί και εκμεταλλεύεται την πρωτοβουλία. Στον κινητικό πόλεμο, η αδράνεια των αντιπάλων δυνάμεων σημαίνει ότι το να αδράξει κανείς την πρωτοβουλία είναι δύσκολο. Στον κυβερνοπόλεμο, δεν υπάρχει σχεδόν καθόλου αδράνεια- η μετακίνηση bits είναι πολύ ευκολότερη από το να μετακινηθούν τανκ, πλοία και αεροσκάφη. Αυτό κάνει την αρχή της επίθεσης λιγότερο σχετική στον κυβερνοπόλεμο, γεγονός το οποίο πιθανόν να συμπεριλαμβάνει παράλληλη δράση και αντίδραση σε φρενήρεις ρυθμούς. Η αρχή της επίθεσης ακόμα εφαρμόζεται σε μικρότερο βαθμό εξαιτίας της αδράνειας στο μυαλό των επιτιθέμενων και των αμυνόμενων- περισσότερο ψυχολογική παρά σωματική αδράνεια.

3.1.3 Κινητική αρχή της μάζας

Η κινητική αρχή της μάζας συμπεριλαμβάνει την συγκέντρωση των επιδράσεων της δύναμης της μάχης σε συγκεκριμένο μέρος και χρόνο για να επιτευχθούν τα καθορισμένα αποτελέσματα. Η συντριπτική δύναμη είναι σε μεγάλο βαθμό άνευ σημασίας για τον κυβερνοπόλεμο εκτός από όταν εμπλέκονται επιθέσεις άρνησης υπηρεσιών (Denial-of-service-DOS)[15] οι οποίες μιμούνται πράξεις του κινητικού πολέμου. Ο κυβερνοπόλεμος διαφέρει από τον συμβατικό πόλεμο στο ότι η ικανότητα να μην γίνεται κανείς αντιληπτός και ο αιφνιδιασμός είναι άκρως σημαντικά. Άρα η μάζα δεν είναι τόσο σημαντική στον κυβερνοπόλεμο όσο στον κινητικό πόλεμο.

3.1.4 Κινητική αρχή του στρατηγήματος

Η κινητική αρχή του στρατηγήματος δηλαδή το να τοποθετείται ο εχθρός σε μειονεκτική θέση μέσω της ευέλικτης εφαρμογής ισχύος δύναμης, είναι εφαρμόσιμη στον κυβερνοπόλεμο. Ωστόσο, οι επιτιθέμενοι και οι αμυνόμενοι δεν κινούν σωματικά ή εικονικά τις δυνάμεις τους- μετακινούν το σημείο επίθεσης ή άμυνας.

3.1.5 Κινητική αρχή της ενότητας της διοίκησης

Η κινητική αρχή της ενότητας της διοίκησης διασφαλίζει την ενότητα της προσπάθειας υπό μία υπεύθυνη διοίκηση για κάθε σκοπό. Αυτό μπορεί να εφαρμοστεί στον κυβερνοπόλεμο στις περισσότερες επιχειρήσεις-ωστόσο υπάρχουν συγκεκριμένες κυβερνοεπιθέσεις, όπως το crowdsourcing και το Anonymous' Low Orbit Ion Cannon, τα οποία χρησιμοποιούν ανυποψίαστους παρευρισκόμενους ή χαλαρά ελεγχόμενους εθελοντές οι οποίοι δεν βρίσκονται στα πλαίσια εντολών του πρωταγωνιστή.

[15] Επιθέσεις άρνησης εξυπηρέτησης (Df-service attack, DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

3.1.6 Κινητική αρχή της ασφάλειας

Η κινητική αρχή της ασφάλειας εφαρμόζεται στον κυβερνοπόλεμο και δεν επιτρέπεται ποτέ στον εχθρό να αποκτήσει απροσδόκητο πλεονέκτημα. Το ρίσκο για επιχειρησιακή δύναμη στον κυβερνοπόλεμο είναι πολύ μικρότερο από τον κινητικό πόλεμο, αλλά τα ρίσκα αποτυχίας προτού επιτευχθεί το επιθυμητό αποτέλεσμα και να στραφούν τα όπλα στον ίδιο τον χρήστη είναι υψηλότερα.

3.1.7 Κινητική αρχή του αιφνιδιασμού

Η κινητική αρχή του αιφνιδιασμού δηλαδή το να χτυπήσει κανείς τον εχθρό σε χρόνο ή μέρος για το οποίο ήταν απροετοίμαστος,εφαρμόζεται στον κυβερνοπόλεμο, ίσως περισσότερο από τον κινητικό πόλεμο.

3.1.8 Κινητική αρχή της απλότητας

Η κινητική αρχή της απλότητας είναι να προετοιμάζονται καθαρά, μη περίπλοκα σχέδια και συνοπτικές οδηγίες για να εξασφαλίσει πλήρη κατανόηση. Αυτό ισχύει για τον κυβερνοπόλεμο εξαιτίας του κινδύνου αδελφοκτονίας όταν μια επιχειρησιακή μονάδα αρνείται την πρόσβαση σε κάποια άλλη ή καίει ένα όπλο σε ένα μικρότερο στόχο.

3.1.9 Διαφορές Κινητικού Πολέμου με Κυβερνοπόλεμο

Ο κυβερνοπόλεμος διαφέρει από τον κλασσικό κινητικό πόλεμο και συνεπώς απαιτεί μια ανασκόπηση των βασικών πολεμικών αρχών για να διαφοροποιηθεί από την ένοπλη σύγκρουση με την παραδοσιακή έννοια.Μερικές αρχές του κινητικού πολέμου όμως βρίσκουν εφαρμογή στον κυβερνοπόλεμο είτε με τρόπο που να μην επιρεάζει τον κυβερνοπόλεμο είτε να είναι ακόμα και ανταγωνιστικές προς αυτόν,δηλαδή οι αρχές αυτές αν ακολοθηθούν επιφέρουν την νίκη ενώ σε αντίθετη περίπτωση επιφέρουν την ήττα.

Ο κυβερνοπόλεμος είναι εκ φύσεως μια εφαρμογή της κινητικής αρχής της οικονομίας της βίας η οποία *είναι* να παρέχει την ελάχιστη ουσιώδη ισχύ μάχης σε δευτερεύοντες προσπάθειες. Επειδή ο κυβερνοπόλεμος είναι η επιτομή του ασύμμετρου πολέμου, η οικονομία βίας για τις δευτερεύοντες αλλά και τις αρχικές προσπάθειες είναι έμφυτη.Βασίζεται σε παρατηρήσεις του πως λειτουργούν τα πράγματα, διαδικτυακά και κατά την διάρκεια των ενεργών

συμπλοκών.Πρέπει να έχει επίδραση στον κινητικό κόσμο. Είναι άσκοπο εάν δεν επηρεάζει κάποιον ή κάτι στον πραγματικό κόσμο.

Πέρα από τις ομοιότητες που έχουν οι δύο αυτοί πόλεμοι έχουν και πολλές διαφορές.Ο κυβερνοπόλεμος διαφέρει από τον συμβατικό, κινητικό πόλεμο και πολλά από τα χαρακτηριστικά του βασίζονται σε ανθρώπινες αδυναμίες.Παρακάτω αναφέρονται μερικές διαφορές τους σε διάφορους τομείς βασισμένες σε αρχές.[2]

3.1.10 Η φύση του περιβάλλοντος

Ο κινητικός πόλεμος συμβαίνει στον φυσικό κόσμο, ελέγχεται από φυσικούς νόμους τους οποίους γνωρίζουμε και καταλαβαίνουμε σε σχέση με τον πόλεμο. Ο κυβερνοπόλεμος συμβαίνει σε έναν τεχνητό κόσμο, κατασκευασμένο από τον άνθρωπο, ο οποίος διαρκώς αλλάζει. Ο κυβερνοπόλεμος μπορεί να χρησιμοποιεί κάποιες αρχές από τον κινητικό πόλεμο, αλλά άλλες έχουν ελάχιστη έως καμία σημασία στον κυβερνοχώρο. Για αυτούς τους λόγους, οι αρχές του κυβερνοπολέμου είναι, τελικά, διαφορετικές από εκείνες του κινητικού πολέμου.

3.1.11 Φυσικοί περιορισμοί

Στον κυβερνοχώρο, η φυσική απόσταση δεν είναι ούτε εμπόδιο ούτε ο υποκινητής της διεξαγωγής επιθέσεων. Μια κυβερνοεπίθεση μπορεί να εκτελεστεί με ίση αποδοτικότητα από την άλλη πλευρά της γης όπως από το διπλανό δωμάτιο. Σε αντίθεση με αυτόν, στον κινητικό πόλεμο, οι επιθέσεις διεξάγονται από φυσικά αντικείμενα τα οποία πρέπει να διασχίσουν μια απόσταση. Αυτού του είδους οι επιθέσεις περιορίζονται σε όσους κατέχουν την τεχνολογία να κάνουν αυτό το αντικείμενο να διασχίσει αυτή την απόσταση. Οι επιθέσεις μπορούν να χρησιμοποιήσουν μεσάζοντα συστήματα, δίκτυα ακόμα και ανθρώπινους δράστες για να αποτρέψουν την απόδοση από τους αμυνόμενους.

3.1.12 Κινητικές επιδράσεις

Ο κυβερνοπόλεμος μπορεί να επηρεάζει άμεσα αντικείμενα στον φυσικό κόσμο καθώς και στην πιο διακριτική μορφή του μπορεί να επηρεάζει τα μυαλά αυτών που λαμβάνουν τις αποφάσεις. Ο πρώτος είναι ανάλογος με τον κινητικό πόλεμο-ο τελευταίος είναι αμιγώς μια μορφή πολέμου πληροφοριών, στον οποίο οι επιτιθέμενοι παρουσιάζουν στους αντιπάλους πληροφορίες οι οποίες οδηγούν σε κακές αποφάσεις.

3.1.13 Μυστικότητα

Ο κυβερνοχώρος είναι τεχνητός, δημιουργημένος από ανθρώπους χρησιμοποιώντας υλικό hardware και λογισμικό. Οποιεσδήποτε πράξεις κάνουν οι μαχητές σε αυτόν τον κόσμο απαιτούν κίνηση δεδομένων ή χειρισμό- κάποια bit σε μερικές ροές δεδομένων αλλάζονται για να αντικατοπτρίζουν την παρουσία τους και τις πράξεις τους. Αυτό αποτελεί καλά νέα για τους

αμυνομένους αλλά είναι χρήσιμο μόνο εάν οι αμυνόμενοι κοιτούν.Κάτι αντίστοιχο ισχύει και στον κινητικό πόλεμο.Για να κρυφτεί κανείς στο φυσικό χώρο μπορεί να χρησιμοποιήσει διάφορα καμουφλάζ.Οι μαχητές στον φυσικό κόσμο μπορούν να τροποποιήσουν το αποτύπωμα αισθητήρα τους χρησιμοποιώντας τεχνολογία μυστικότητας. Στον κυβερνοκόσμο, οι πολεμιστές δεν μπορούν να κάνουν βήματα ίσα με το να απορροφούν ενέργεια ραντάρ ή να ψυχραίνουν υπέρυθρες. Αντιθέτως, οι πρωταγωνιστές πρέπει να προσπαθήσουν να κρύψουν στοιχεία στις υπάρχουσες ροές δεδομένων. Οι αισθητήρες που αναζητούν κυβερνοεπιθέσεις πρέπει να διαχωρίζουν τα bits τα οποία είναι τέχνημα ενός επιτιθέμενου από την συντριπτική πλειοψηφία που είναι φυσιολογικές δραστηριότητες. Το να χρησιμοποιείται φυσιολογική δραστηριότητα για να διεξαχθεί μια επίθεση, καθιστά αυτό περισσότερο πολύπλοκο.

3.1.14 Μεταβλητότητα και έλλειψη συνοχής

Ο κυβερνοχώρος είναι επαρκώς μεταβλητός έτσι ώστε να μην έχει συνοχή.Όσο αφορά την έλλειψη συνοχης του κυβερνοχώρο στον φυσικό κόσμο μπορούμε να προσδοκούμε ότι μια σφαίρα θα δρα με ένα συγκεκριμένο τρόπο όταν εκτοξευτεί- μπορούμε να προβλέψουμε την διαδρομή της σφαίρας με βαλλιστική εξέταση. Κάθε φορά που κάποιος πυροβολεί μία σφαίρα, αυτή θα δράσει με τον ίδιο τρόπο, με διακύμανση εξαιτίας ελάχιστων φυσικών αιτιών. Στον κυβερνοκόσμο, τίποτα δεν μπορεί να θεωρηθεί δεδομένο με τέτοιο τρόπο. Ο κυβερνοκόσμος, ως τεχνητή κατασκευή χτισμένη από ανθρώπους, είναι ατελής. Μπορεί να αλλάξει και αλλάζει με τρόπους οι οποίοι φαίνονται χαοτικοί. Βλάβες στο λογισμικό, βλάβες στο υλικό hardware, προγράμματα λειτουργούν γρηγορότερα από το προσδοκώμενο- αυτά και χιλιάδες άλλες διακυμάνσεις προκαλούν έλλειψη προβλεψιμότητας.Στον κυβερνοπόλεμο, αυτή η έλλειψη συνοχής μετατρέπεται σε επιθέσεις οι οποίες δεν συμπεριφέρονται πάντα με τον ίδιο τρόπο, περιβάλλοντα τα οποία αλλάζουν κατά την διάρκεια μιας επίθεσης και διακυμάνσεις στην επίδοση της επίθεσης. Οι μόνες πλευρές του κυβερνοκόσμου οι οποίες δεν αλλάζουν είναι αυτές που απαιτούν τροποποίηση του φυσικού κόσμου.

3.1.15 Αξιοπιστία

Λόγω της μεταβλητότητας και της έλλειψης συνοχής ο κυβερνοχώρου δεν μπορεί να είναι και αξιόπιστος.Σύμφωνα με το παραπάνω παράδειγμα της σφαίρας στο φυσικό χώρο σε αντίθεση με τον κυβερνοκόσμο που ούτε το υλικό hardware, ούτε το λογισμικό δεν θα δουλεύει πάντα όπως αναμένεται στον κυβερνοχώρο. Αυτό ισχύει περισσότερο για το λογισμικό, αλλά έχουμε δει ασυνέπειες στο hardware, συνήθως εξαιτίας της θερμότητας ή της υπερφόρτωσης.Μια επίδραση αυτής της αρχής είναι ότι δεν μπορούμε ποτέ να είμαστε σίγουροι ότι ένα συγκεκριμένο βήμα σε μια επίθεση θα λειτουργήσει.Άλλη μια επίδραση είναι ότι οι επιθέσεις τις οποίες δεν περιμένουμε να επιτύχουν, συχνά πετυχαίνουν.

3.1.16 Ταυτότητα και προνόμια

Μια οντότητα στον κυβερνοχώρο έχει την εξουσία, την πρόσβαση ή την ικανότητα να διεξάγει οποιαδήποτε πράξη θέλει να πραγματοποιήσει ένας επιτιθέμενος. Ο στόχος του επιτιθέμενου

είναι να υποθέτει την ταυτότητα αυτής της οντότητας, με κάποιο τρόπο.Πάλι, επειδή ο κυβερνοκόσμος είναι μια καθαρά τεχνητή κατασκευή, έχει χτιστεί και ελεγχθεί από ανθρώπους και τα μέσα τους. Δεν υπάρχει μέρος του κυβερνοκόσμου που να μην ελέγχεται από ένα άτομο ή τον κυβερνοπράκτορα αυτού του ατόμου. Μερικές φορές η οντότητα με την εξουσία, την πρόσβαση ή την ικανότητα είναι ένα είδωλο(avatar). Μερικές φορές ο άνθρωπος περνά τον έλεγχο σε ένα στοιχείο λογισμικού. Αλλά υπάρχει πάντα κάτι ή κάποιος ο οποίος μπορεί να κάνει αυτό που θέλει ο κυβερνοπολεμιστής. Τα περισσότερα βήματα σε οποιαδήποτε κυβερνοεπίθεση έχουν απλά στόχο να υποθέσουν την ταυτότητα της οντότητας η οποία μπορεί να πραγματοποιήσει την επιθυμητή πράξη.

3.1.17 Διπλή χρήση

Τα μέσα του κυβερνοπολέμου είναι πάντα διπλής χρήσης, ενώ τα μέσα του κινητικού πολέμου είναι περισσότερο ενός σκοπού, με χρήση πρωταρχικά για ένα σκοπό παράβασης, άμυνας ή ανίχνευσης. Τα όπλα χρησιμοποιούνται για επίθεση, ο οπλισμός χρησιμοποιείται για άμυνα και οι αισθητήρες χρησιμοποιούνται για να εντοπίσουν τον εχθρό. Στον κινητικό πόλεμο, οι αμυνόμενοι δεν δοκιμάζουν τις άμυνές τους πυροβολώντας τα δικά τους στρατεύματα από την οπτική του εχθρού για να επιβεβαιώσουν την επιτυχία της ενέδρας. Αυτή η χρήση των αισθητήρων είναι παραβατική αλλά και αμυντική, αλλά αυτό αποτελεί εξαίρεση στον κανόνα.Οι επιτιθέμενοι και οι αμυνόμενοι στον κυβερνοπόλεμο χρησιμοποιούν τα ίδια εργαλεία. Οι επιτιθέμενοι χρησιμοποιούν σαρωτές ευπάθειας για να αναζητήσουν ευκαιρίες εκμετάλλευσης ως μέρος μιας επίθεσης. Οι αμυνόμενοι χρησιμοποιούν τους ίδιους σαρωτές ευπάθειας για να αναζητήσουν αδυναμίες στα δικά τους συστήματα. Οι συσκευές καταγραφής πακέτων προήλθαν επειδή οι διαχειριστές έπρεπε να δουν την κυκλοφορία των πακέτων για να διαγνώσουν προβλήματα στο δίκτυο. Οι επιτιθέμενοι χρησιμοποιούν την καταγραφή πακέτων για την ανακάλυψη. Οι επιτιθέμενοι συλλέγουν κώδικες εκμετάλλευσης για να χρησιμοποιήσουν ενάντια στους στόχους τους. Οι αμυνόμενοι συλλέγουν κώδικες εκμετάλλευσης για να δοκιμάσουν τα ίδια τους τα συστήματα, επειδή οι απαιτήσεις της αποστολής ή της επιχείρησης ίσως να αποτρέπουν την διασύνδεση και επειδή εκείνα τα συστήματα μπορούν να ανακτούν τις ευπάθειες από κακές αναβαθμίσεις των παρόχων.Τα κινητικά όπλα χρησιμοποιούνται ενάντια σε αντιπροσωπευτικά δείγματα των άμυνων του φυσικού κόσμου και των συστημάτων για να μελετήσουν τις επιδράσεις τους, αλλά όχι ενάντια στις πραγματικές άμυνες ή τα συστήματα εξαιτίας του κόστους-σε χρήματα αλλά και χρόνο-ανασύνθεσης των επηρεασμένων συστημάτων. Φυσιολογικά, δεν βομβαρδίζουμε τα δικά μας αντιπυραυλικά σιλό, τα τανκ, τα αεροδρόμια και τα πλοία μας. Ωστόσο, τα όπλα του κυβερνοπολέμου χρησιμοποιούνται συστηματικά ενάντια σε πραγματικές άμυνες και συστήματα (όπως και με την δοκιμασία διάτρησης) με την πεποίθηση ότι αυτά τα συστήματα μπορεί να ξαναχτιστούν με σχεδόν κανένα κόστος.

3.1.18 Έλεγχος υποδομών

Οι αμυνόμενοι και οι επιτιθέμενοι ελέγχουν ένα πολύ μικρό μέρος του κυβερνοχώρου που χρησιμοποιούν. Οποιοσδήποτε ελέγχει ένα μέρος του κυβερνοχώρου που μπορεί να χρησιμοποιήσει ο αντίπαλος, ελέγχει τον αντίπαλο, επομένως η πιο πρόσφατη τάση είναι να δοκιμάζονται τα δίκτυα κάποιου κάνοντας μια προληπτική επίθεση. Συχνά, το όριο του ελεγχόμενου κυβερνοχώρου είναι η πραγματική φυσική περίμετρος.

4 *Είδη Κυβερνοεπιθέσεων και Κυβερνοόπλων*

4.1 Κυβερνοεπιθέσεις

Όπως προαναφέραμε η κυβερνοεπίθεση βασίζεται στα δίκτυα ηλεκτρονικών υπολογιστών. Έτσι τα ανεπτυγμένα και τα αναπτυσσόμενα κράτη που στηρίζονται στα κυβερνοδίκτυα θα πρέπει να γνωρίζουν:

- Τον βαθμό της ζημιάς/πόνου
- Τη δυνατότητα απόδοσης των πηγών των επιθέσεων υπό το φως της χρήσης των προγραμμάτων ρομπότ.
- Τρόπους διατήρησης πηγών των επιθέσεων ανώνυμες.

Ο Robert Knake κατατάσσει τις κυβερνοεπιθέσεις ανάλογα με τη σοβαρότητα της απειλής που αποτελούν ξεκινώντας από εκείνες με υψηλή σοβαρότητα σε εκείνες με χαμηλότερη.

1. κυβερνοπόλεμος
2. κυβερνο κατασκοπεία
3. βίαιες επιθέσεις
4. έγκλημα
5. ενόχληση

Πάνω στο θέμα της σοβαρότητας της απειλής ο Libicki υποστηρίζει ότι ο κυβερνοπόλεμος χρησιμοποιείται περισσότερο για την ενόχληση ενός αντιπάλου (π.χ. εκνευρίζοντάς ή ενοχλώντας τον) παρά την συντριβή του, δεδομένου ότι οι μόνιμες επιδράσεις είναι φευγαλέες ενώ η απειλή της τιμωρίας δεν έχει κάνει αρκετά για την πρόληψη των κυβερνοεπιθέσεων σε στρατιωτικά και μη δίκτυα.[3]

Η απώλειες ανθρωπίνων ζωών καθώς και η καταστροφή κρίσιμων υποδομών είναι δύο τομείς που επιρεάζονται από αυτού του είδους επιθέσεις. Επίσης οι κοινωνικοοικονομικές συνέπειες και η επίπτωσή τους στους πολίτες, συνδέονται άμεσα και έμμεσα με τις συνέπειες της κατάρρευσης ή υποβάθμισης κρίσιμων ICTs στην ευημερία των πολιτών. Σύμφωνα με τη Διεθνή Ομάδα Εμπειρογνωμόνων[16] για την κατηγοριοποίηση των Κυβερνο-επιθέσεων υπάγονται και οι ίδιοι οι παράγοντες αντικτύπου.

Παρακάτω παρατίθεναται παράγοντες που αφορούν περιπτώσεις που επιφέρουν συνέπειες στον άνθρωπο και στην ακεραιότητα των υποδομών του άμεσα, από τη Διεθνή Ομάδα Εμπειρογνωμόνων στα κράτη-μέλη .[13]

Με άξονα την εμβέλειά τους (τοπική, περιφερειακή, εθνική και διεθνής) και τον χρόνο τους (κατά τη διάρκεια ή μετά το επεισόδιο),οι παράγοντες αυτοί είναι:

- Η δημόσια ασφάλεια
- Η οικονομική επίπτωση
- Η περιβαλλοντική επίπτωση στον δημόσιο και τον περιβάλλοντα χώρο
- Η αλληλεξάρτηση
- Οι πολιτικές επιπτώσεις
- Τα πολιτικά αποτελέσματα
- Οι ψυχολογικές επιπτώσεις

Αναλυτικά η δημόσια ασφάλεια περιλαμβάνει ζητήματα πληθυσμού, απώλειας ζωής, ασθένειας, σοβαρού τραυματισμού και εκκένωσης.Στην οικονομική επίπτωση εντάσσονται θέματα επίπτωσης ΑΕΠ, σημαντικότητα της οικονομικής απώλειας και/ή την υποβάθμιση των προϊόντων ή των υπηρεσιών.Στην κατηγορία αλληλεξάρτησης έχουμε αλληλεξαρτήσεις μεταξύ κρίσιμων στοιχείων υποδομής ενώ τα θέματα με τις πολιτικές επιπτώσεις αφορούν την εμπιστοσύνη.Τέλος τα πολιτικά αποτελέσματα έχουν να κάνουν με την εμπιστοσύνη της κυβέρνησης και οι ψυχολογικές επιπτώσεις με την την ψυχολογική κατάσταση του πληθυσμού.

Το 2002 ο Schmitt[3] διαχωρίζει τις επιθέσεις σε δίκτυο υπολογιστών σε τρεις κατηγορίες ανάλογα με τους στόχους που έχει η κάθε επίθεση:

- Διοικητικοί και στρατιωτικοί στόχοι
- Πολιτικοί και μη στρατιωτικοί στόχοι
- Διπλής χρήσης στόχοι.

[16] Είναι ένα συμβουλευτικό όργανο που συγκροτείται από την Ευρωπαϊκή Επιτροπή ή τις υπηρεσίες της για να τους παρέχει συμβουλές και εμπειρογνωσία και είναι αποτελούμενο από μέλη που προέρχονται από τον δημόσιο και/ή ιδιωτικό τομέα.Συνέρχεται περισσότερες από μία φορές και χωρίζεται σε δύο κατηγορίες,στις επίσημες και στις άτυπες.[14]

Επιπρόσθετα αναφέρει τα προτεινόμενα κριτήρια για την αξιολόγηση των επιπτώσεων των κυβερνοεπιθέσεων:

- «Δριμύτητα: Οι ένοπλες επιθέσεις απειλούν το σωματικό τραυματισμό ή την καταστροφή της περιουσίας σε πολύ μεγαλύτερο βαθμό από άλλες μορφές καταναγκασμού. Η σωματική ευεξία συνήθως απασχολεί την κορυφή της ιεραρχίας των ανθρώπινων αναγκών.»
- «Αμεσότητα: Οι αρνητικές επιπτώσεις του ένοπλου καταναγκασμού ή της απειλής αυτού, συνήθως συμβαίνουν με μεγάλη αμεσότητα, ενώ άλλες μορφές καταναγκασμού εξελίσσονται πιο αργά. Έτσι, η ευκαιρία του κράτους στόχου ή της διεθνούς κοινότητας να αναζητήσει ειρηνική διαμονή παρακωλύεται στην προηγούμενη περίπτωση».
- «Ευθύτητα: Οι συνέπειες του ένοπλου καταναγκσμού είναι πιο άμεσα συνδεδεμένες με το *actus reus* (ηθική παρεκτροπή, παράβαση καθήκοντος) από ότι άλλες μορφές καταναγκασμού, το οποίο συχνά εξαρτάται για να λειτουργήσει από διάφορους παράγοντες που συμβάλλουν. Επομένως, η απαγόρευση σε επιβολή αποκλείει τις αρνητικές επιπτώσεις με μεγαλύτερη βεβαιότητα.»
- «Ικανότητα εισβολής: Στον ένοπλο καταναγκασμό, η πράξη που προκαλεί τη βλάβη συνήθως εισέρχεται στο κράτος στόχο, ενώ στον οικονομικό πόλεμο οι πράξεις γενικά συμβαίνουν πέρα από τα σύνορα του στόχου. Ως αποτέλεσμα αυτού, αν και οι ένοπλες και οικονομικές πράξεις μπορεί να έχουν σχεδόν παρόμοιες επιπτώσεις, η πρώτη πράξη αντιπροσωπεύει μια μεγαλύτερη εισβολή στα δικαιώματα του κράτους στόχου και, επομένως, είναι πιο πιθανόν να διαταχθεί η διεθνής σταθερότητα.»
- «Μετρησιμότητα: Παρόλο που οι επιπτώσεις του ένοπλου καταναγκασμού είναι συνήθως εύκολο να εξακριβωθούν (π.χ. ένα συγκεκριμένο επίπεδο καταστροφής), οι συνέπειες άλλων μορφών καταναγκασμού είναι δυσκολότερο να μετρηθούν. Αυτό το γεγονός καθιστά την καταλληλότητα της καταδίκης από την κοινότητα και το βαθμό της σφοδρότητας που περιλαμβάνεται σε αυτή, λιγότερο αναξιόπιστη στην περίπτωση της ένοπλης βίας.»
- «Τεκμαιρόμενη νομιμότητα: Στις περισσότερες περιπτώσεις, είτε είναι υπό το εγχώριο ή το διεθνή δίκαιο, η εφαρμογή της βίας θεωρείται παράνομη ελλείψει συγκεριμένης εξαίρεσης όπως η αυτοάμυνα. Η γνωστική προσέγγιση είναι απαγορευτική.»
- «Υπευθυνότητα: απευθύνεται στον βαθμό στον οποίο η επίπτωσης μιας πράξης μπορεί να αποδοθεί σε ένα κράτος σε αντίθεση με άλλους φορείς. Η προϋπόθεση είναι ότι ο ένοπλος καταναγκασμός είναι εντός της αποκλειστικής αρμοδιόττας των κρατών και είναι πιο επιρρεπής στο να χρεωθεί στα κράτη, ενώ μη κρατικοί φορείς είναι ικανοί να εμπλέκονται σε μη δεσμευτική δραστηριότητα όπως η προπαγάνδα και το μποϋκοτάζ.»

Σύμφωνα με τα παραπάνω κριτήρια ο Schmitt στην ερώτηση αν μπορεί μια επίθεση σε δίκτυο υπολογιστών να εμπίψει εκτός του πεδίου εφαρμογής των «επιθέσεων» γιατί δεν χρησιμοποιεί βία,απάντησε:

«Όχι, και ακριβώς για τον ίδιο λόγο που οι ένοπλες επιθέσεις μπορεί να περιλαμβάνουν κυβερνοεπιθέσεις. «Επιθέσεις» είναι ένας όρος κανονιστικής συντομογραφίας που προορίζεται να αντιμετωπίσει συγκεκριμένες επιπτώσεις. Είναι σαφές ότι αυτό που οι σχετικές διατάξεις ελπίζουν να πετύχουν είναι η θωράκιση προστατευόμενων ατόμων από τραυματισμό ή θάνατο και προστατευόμενων αντικειμένων από ζημιά ή καταστροφή. Στο βαθμό που ο όρος «βία» είναι επεξηγήσιμος, πρέπει να θεωρηθεί στα πλαίσια των βίαιων επιπτώσεων περισσότερο από ότι

των βίαιων πράξεων. Η σημαντική ανθρώπινη φυσική ή συναισθηματική ταλαιπωρία εύλογα περιλαμβάνονται στην έννοια του τραυματισμού. Μόνιμη απώλεια περιουσιακών στοιχείων, για παράδειγμα χρημάτων, μετοχών κτλ, άμεσα μεταβιβάσιμα σε χειροπιαστή περιουσία συνιστά επίσης ζημιά ή καταστροφή. Το νόημα είναι ότι η ταλαιπωρία, η παρενόχληση ή η απλή ελάττωση στην ποιότητα ζωής δεν αρκούν, ο ανθρώπινος πόνος είναι το απαιτούμενο κριτήριο. Ως παράδειγμα, μια σημαντική αναταραχή της χρηματιστηριακής αγοράς ή του τραπεζικού συστήματος θα μπορούσε να καταρρεύσει την οικονομία αποτελεσματικά και να οδηγήσει σε ευρεία ανεργία, πείνα, ψυχική οδύνη κτλ, μια πραγματικότητα που με τραγικό τρόπο αποδείχθηκε στην Ύφεση της δεκαετίας του 1930. Εάν προκαλούσε αυτό το επίπεδο πόνου, η ΕΔΥ θα συνιστούσε μια επίθεση εντός του νοήματος του όρου στο ανθρωπιστικό δίκαιο.»[3]

Όπως προαναφέραμε παραπάνω σύμφωνα με τους παραδοσιακούς κανόνες του Διεθνούς Δικαίου οι Επιθέσεις κατά Δικτύων Υπολογιστών (CNAs) συμπεριλαμβάνονται στο Διεθνές Δίκαιο.Τα κριτήρια σχετικά με την αποτίμησης συνεπειών των επιθέσεων αυτών σύμφωνα με το Εθνικό Σχέδιο Προστασίας Υποδομών των ΗΠΑ είναι:

- Η δημόσια υγεία και ασφάλεια, δηλαδή τα αποτελέσματα στην ανθρώπινη ζωή και υλική ευημερία.
- Το οικονομικό δηλαδή οι άμεσες και έμμεσες οικονομικές απώλειες.
- Το ψυχολογικό δηλαδή η επίπτωση στο ηθικό του λαού και ο βαθμός εμπιστοσύνης των ανθρώπων στους οικονομικούς και τους πολιτικούς θεσμούς.
- Και τέλος η διακυβέρνηση/αποστολή δηλαδή οι επιπτώσεις στην ικανότητα της κυβέρνησης ή της βιομηχανίας να διατηρήσει την τάξη, να προσφέρει ζωτικές υπηρεσίες, να διασφαλίσει τη δημόσια υγεία και ασφάλεια και να διεξαγάγει αποστολές σχετικές με την εθνική ασφάλεια.

Επιπρόσθετα ο καθηγητής Irving Lachow του Πανεπιστημίου Εθνικής Άμυνας στις Ηνωμένες Πολιτείες διαχωρίζει τις κυβερνοαπειλές ανάλογα με τα τα κίνητρα, τους στόχους και τις μεθόδους που έχει η κάθε κυβερνοαπειλή ξεχωριστά.[3]

- Black Hat Hacking: στοχεύει σε άτομα ,εταιρείες και κυβερνήσεις λόγω εγωισμού ή προσωπικής εχθρότητας.Τα μέσα που χρησιμοποιεί είναι το Κακόβουλο λογισμικό, οι ιοί, τα σκουλήκια και σενάρια διείσδυσης.
- Κυβερνο έγκλημα: στοχεύει σε άτομα και εταιρείες για οικονομικό όφελος με την χρήση κακόβουλου λογισμικού για απάτη, κλοπή ταυτότητας, DdoS για εκβιασμό.
- Κυβερνο κατασκοπεία: στοχεύει σε άτομα ,εταιρείες και κυβερνήσεις λόγω οικονομικού και πολιτικού οφέλους με την βοήθεια τεχνικών για την απόκτηση πληροφοριών.
- Πόλεμος πληροφοριών:στοχεύει σε υποδομές, συστήματα δεδομένων τεχνολογίας πληροφοριών (δημόσια ή ιδιωτικά) για πολιτικό ή στρατιωτικό όφελος με πλήθος τεχνικών ή επιχειρήσεις επίθεσης ή επιρροής.

Ακόμα δεν πρέπει να λείπει ο διαχωρισμός πότε μια κυβερνοεπίθεση θεωρείται χρήση βίας ή ένοπλης επίθεσης.Οι κυβερνοεπιθέσεις οι οποίες προκαλούν φυσική ζημιά ή τραυματισμό σε ανθρώπους παρόμοια με ζημιές ή απώλειες στον παραδοσιακό πόλεμο θεωρούνται χρήση βίας και ένοπλης επίθεσης. Σε αντίθεση όμως,οι κυβερνοεπιθέσεις οι οποίες προκαλούν

επισκευάσιμη φυσική ζημιά με συνέπειες οι οποίες δεν είναι μακροχρόνιες και δεν προκαλούν τραυματισμό σε ανθρώπους δεν έχουν αντιμετωπιστεί ως χρήση βίας η ένοπλες επιθέσεις.

4.2 Είδη Κυβερνοόπλων

Στον ΗΠ οι κυβερνοεπιθέσεις χρησιμοποιούν λογισμικό ως όπλο που εξαπολύονται σε διασυνδεδεμένα δίκτυα, για να καταναγκάσουν έναν αντίπαλο ή να ζημιώσουν τη δυνατότητά του να παρέχει απαραίτητες κυβερνητικές, οικονομικές ή στρατιωτικές υπηρεσίες με σκοπό να προκαλέσουν διατάραξη ή ζημιά σε δεδομένα και κρίσιμες υποδομές,όπως για παράδειγμα διακοπή της ηλεκτρικς ενέργειας ή των αγωγών καυσίμων.[3]

Πέρα από επιθέσεις σε πληροφοριακά συστήματα και στο διαδίκτυο υπάρχουν και οι επιθέσεις κατά του λογισμικού ή ακόμα και κρυφές ενσωματωμένες επιθέσεις στο Bios[17] των υπολογιστών.

Τα κυβερνοόπλα μπορεί να στοχεύσουν και να βλάψουν μία βασική λειτουργία στρατιωτικών ιεραρχιών, δηλαδή τη διοίκηση και τον έλεγχο.Ακόμα τα όπλα ή τα οπλικά συστήματα μπορούν να αχρηστευτούν για κάποιον χρόνο ή ακόμα και να φθαρούν υλικά από ελαττωματικά μηνύματα ή διεισδύσεις στα πληροφοριακά συστήματα που τα ελέγχουν. Τέλος, τα κυβερνοόπλα θα μπορούσαν να στοχεύσουν υποδομές κοινής χρήσης, δηλαδή συστήματα και δομές τόσο για πολιτικές όσο και για στρατιωτικές χρήσεις, ή ακόμα και πολιτικούς στόχους με το σκοπό της αποθάρρυνσης, της αποδυνάμωσης ή της σύγχυσης της στρατιωτικής και πολιτικής ηγεσίας ενός εχθρού.

Όταν αναφερόμαστε σε κρυφά ενσωματωμένες επιθέσεις το πρώτο πράγμα που μας έρχεται στο μυαλό είναι η ενσωμάτωση μοναδικών αναγνωριστικών τσιπ. Τα τσιπ αυτά περιορίζουν την μυστικότητα της ταυτότητας που επιφέρει μεγάλη εγκληματική και επιβλαβή δραστηριότητα στο Διαδίκτυο.

Στην περίπτωση των επιθέσεων κατά του λογισμικού έχουμε την διείσδυση. Διεισδυτική επίθεση έχουμε όταν το κακόβουλο λογισμικό αποκτά πρόσβαση σε τμήματα του λογισμικού ή των αποθηκευμένων δεδομένων ενός υπολογιστή μέσω ενός σάιτ. Όταν φτάσει εκεί, το κακόβουλο λογισμικό μπορεί να τροποποιήσει διάφορα κομμάτια λογισμικού ή δεδομένων, να προκαλέσει κατάρρευση του συστήματος ή να αχρηστεύσει ορισμένα κομμάτια του λογισμικού, να σβήσει σκληρούς δίσκους, να στείλει μηνύματα email που παριστάνουν ότι είναι από τον χρήστη, να στείλει πληροφορίες για το λογισμικό και τα δεδομένα πίσω στον συντάκτη του κακόβουλου

[17] Το BIOS είναι το Βασικό Σύστημα Εισόδου/Εξόδου (Basic Input/Output System), κομμάτι των περισσότερων υπολογιστών, μία μορφή σχετικά απλού υλικολογισμικού (firmware) που «επιζεί» μετά από διακοπή τροφοδοσίας, και που οποιοσδήποτε υπολογιστής χρειάζεται για να ξέρει πώς να φορτώσει ένα λειτουργικό σύστημα από κάποια συσκευή πτητικής (volatile) μνήμης. (Αυστηρά μιλώντας, το BIOS δεν είναι ανάγκη να αποθηκευθεί σε ένα πραγματικό κύκλωμα υλικού, αν και τα περισσότερα έχουν αποθηκευθεί σε ένα πραγματικό κύκλωμα υλικού, αλλά είναι ανάγκη να είναι σχετικά μη πτητικό.)

λογισμικού και ούτω καθεξής. Αν αυτό το διεισδυτικό κακόβουλο λογισμικό μπορεί στη συνέχεια να σταλεί (πιθανώς σε τροποποιημένη μορφή) και να μολύνει κι άλλους υπολογιστές, είναι μία αυτοαναπαραγωγή.

Τα κυβερνοόπλα στην περίπτωση αυτή ονομάζονται κακόβουλα λογισμικά.Το «κακόβουλο λογισμικό», διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα «ξενιστή» και σε αυτό που δεν χρειάζεται «ξενιστή» και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα.Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε δύο άλλες κατηγορίες. Το ιομορφικό λογισμικό και το μη ιομορφικό λογισμικό. Στο ιομορφικό λογισμικό ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο μη ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα.

4.2.1 Είδη Κακόβουλου λογισμικού

4.2.1.1 Ιός(virus)

Ο ιός είναι ένα μικρό πρόγραμμα το οποίο προσκολλά τον εαυτό του σε άλλα προγράμματα ή αρχεία και μεταδίδεται από η/υ σε η/υ, σε δίκτυα, συσκευές αποθήκευσης κ.λπ., φτιάχνοντας αντίγραφα του εαυτού του.Επίσης, ένας ιός είναι συνήθως εφοδιασμένος και με ένα εκτελέσιμο κομμάτι λογισμικού (payload), το οποίο μπορεί να προγραμματιστεί έτσι ώστε να προκαλέσει κακόβουλα αποτελέσματα, όπως διαγραφές αρχείων, αλλοίωση δεδομένων, διαταραχή λειτουργιών κ.λπ. Σχεδόν όλοι οι ιοί προσαρτώνται σε εκτελέσιμα αρχεία, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει για ένα διάστημα σε κάποιον η/υ, χωρίς να είναι ανιχνεύσιμος, μέχρι τη στιγμή που το μολυσμένο εκτελέσιμο αρχείο θα εκτελεστεί.[15]

4.2.1.2 Κερκόπορτες (trapdoors/backdoors)

Οι κερκόπορτες είναι σημεία εισόδου που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας τη συνηθισμένη διαδικασία ελέγχου πρόσβασης. Νομότυπος σκοπός που αφορά τη διαδικασία ελέγχου και αποσφαλμάτωσης εφαρμογών, δυνητικό σημείο ευπάθειας. Τοποθετούνται και από εισβολείς για την απρόσκοπτη είσοδό τους στο Υ.Σ. σε μελλοντικό χρόνο. [15]

4.2.1.3 Λογικές βόμβες (logic bombs)

Λογικές βόμβες είναι προγράμματα που εκτελούν μια ενέργεια,η οποία παραβιάζει την πολιτική ασφαλείας ενός συστήματος όταν πληρείται κάποια λογική συνθήκη στο σύστημα (π.χ., όταν το όνομα του προγραμματιστή δε βρίσκεται στη μισθοδοσία της επιχείρησης). Πρόκειται για

κώδικα κακόβουλου λογισμικού, σχεδιασμένο να τίθεται σε εφαρμογή (να εκτελείται αυτοματοποιημένα) όταν πληρωθούν ορισμένες προϋποθέσεις, ή όταν συντρέξουν ορισμένα κριτήρια, ή, τέλος, σε μία δεδομένη χρονική στιγμή στο μέλλον. Μόλις συμβεί αυτό, ο κακόβουλος κώδικας μπορεί να διακόψει ή να καταστήσει δυσχερή τη λειτουργία ενός η/υ ή δικτύου, να διαγράψει δεδομένα, ή ακόμη και να ξεκινήσει μία επίθεση τύπου DoS /DDoS.Παρόμοιες είναι και οι χρονικές βόμβες.[15]

4.2.1.4 Δούρειοι ίπποι(Trojan horses)

Δούρειοι ίπποι είναι φαινομενικά χρήσιμα προγράμματα που περιλαμβάνουν κρυφές λειτουργίες, οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα, με συνέπεια μια απειλή στην ασφάλεια του συστήματος. Δεν αναπαράγονται μόνοι τους. Βασίζονται (ξεγελούν) (σ)τους χρήστες για την εγκατάσταση και την εκτέλεσή τους.Ο δούρειος ίππος είναι ένα μη βλαβερό πρόγραμμα, το οποίο, ωστόσο, περιέχει κατά τρόπο μη εμφανή κακόβουλο ή επιβλαβή κώδικα λογισμικού και μπορεί να προκαλέσει ζημία ή να εκτελέσει οποιαδήποτε άλλη (κακόβουλη) εργασία για την οποία είναι προορισμένος. Οι χρήστες η/υ που λαμβάνουν έναν δούρειο ίππο, παρασύρονται διότι χρησιμοποιούν ένα φαινομενικά αβλαβές πρόγραμμα ή ανοίγουν αρχεία από φαινομενικά ‘νόμιμη’ και γνωστή πηγή προέλευσης. Οι δούρειοι ίπποι μπορούν να προκαλέσουν σοβαρά προβλήματα διαγράφοντας αρχεία ή καταστρέφοντας πληροφορίες˙ μπορούν επίσης να δημιουργήσουν ηλεκτρονικές ‘κερκόπορτες’ στο σύστημα.[15]

4.2.1.5 Βακτήρια (computer bacterium or Wabbit, Rabbit)

Αναπαράγονται όπως και οι ιοί και δεν απαιτούν την ύπαρξη ξενιστή. Δεν αλλοιώνουν δεδομένα σκόπιμα. Υποβαθμίζουν τη διαθεσιμότητα των πόρων του συστήματος.[15]

4.2.1.6 Παραπλανητική πληροφόρηση (hoaxes)

Διάδοση ψευδούς φήμης σχετικά με την ύπαρξη νεοεμφανιζόμενου κακόβουλου λογισμικού, αλλά και με οποιοδήποτε άλλο θέμα μπορεί να οδηγήσει σε σπατάλη πόρων. Βασίζονται στην κοινωνική μηχανική (Social engineering).[15]

4.2.1.7 Παραπλάνηση (IP spoofing)

Με την τεχνική αυτή (γνωστή και ως IP address forgery ή host file hijack) ο επιτιθέμενος παρίσταται ψευδώς ως ο κατασκευαστής και διαχειριστής νόμιμων και ακίνδυνων ιστοσελίδων και ιστότοπων.Ο επισκέπτης που πληκτρολογεί στον η/υ του

μία διεύθυνση ορισμένης ιστοσελίδας στο διαδίκτυο,οδηγείται σε μία άλλη ιστοσελίδα, παραποιημένη. Κατά την επικοινωνία του με αυτήν τη φαινομενικά νόμιμη και φυσιολογική αλλά στην πραγματικότητα κατασκευασμένη από τρίτους, ιστοσελίδα, όλα τα στοιχεία που τυχόν εισάγει ο χρήστης καταλήγουν στους 'πλαστογράφους', οι οποίοι μπορούν ακόμη και να αναλάβουν τον έλεγχο του η/υ του ή του δικτύου στο οποίο αυτός ανήκει, με ό,τι αυτό συνεπάγεται.[4]

4.2.1.8 Κατασκοπευτικό λογισμικό (spyware)

Έχει σκοπό την παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων. Εγκαθίσταται κρυφά ξεγελώντας το χρήστη σε ένα Υ.Σ. και εκτελείται στο παρασκήνιο. Τυπικά, συγκεντρώνει πληροφορίες σχετικά με το χρήστη,π.χ., ιστοθέσεις που επισκέπτεται, κωδικούς πρόσβασης, κ.ά. Συνήθως μεταδίδεται με την εγκατάσταση προγραμμάτων (freeware, shareware), με την εγκατάσταση πρόσθετων (browser add-ons), με την επίσκεψη σε δικτυακούς τόπους. Ως spyware κατηγοριοποιούνται τα adware, tracking cookies, system monitors.[15]

4.2.1.9 Αναπαραγωγοί (worms)

Οι αναπαραγωγοί λειτουργούν με τρόπο που μοιάζει με αυτόν των ιών, επειδή μεταδίδονται από η/υ σε η/υ. Σε αντίθεση, όμως, με τους ιούς, τα 'σκουλήκια' λογισμικού έχουν την ικανότητα να ταξιδεύουν χωρίς (έστω και την ακούσια) βοήθεια προσώπων˙ αυτό επιτυγχάνεται επειδή αυτού του είδους το κακόβουλο λογισμικό εκμεταλλεύεται τα δεδομένα μεταφοράς και κινήσεως των αρχείων εντός του δικτύου. Ωστόσο, ο μεγαλύτερος κίνδυνος που παριστούν τα 'σκουλήκια' συνίσταται στο γεγονός ότι έχουν την ιδιότητα και την ικανότητα να αναπαράγουν τον εαυτό τους εντός του συστήματος ,έτσι ένας μολυσμένος η/υ μπορεί να διαβιβάζει σε άλλους (και κατ' επέκταση σε ολόκληρα δίκτυα ή συστήματα) εκατοντάδες ή και χιλιάδες αντίγραφα ενός ηλεκτρονικού 'σκουληκιού'. Το τελικό αποτέλεσμα στις περισσότερες περιπτώσεις είναι ότι τα ηλεκτρονικά 'σκουλήκια' καταναλώνουν μεγάλα ποσοστά της διαθέσιμης μνήμης ή ακόμη και του εύρους (bandwidth) των γραμμών επικοινωνιών των δικτύων, με συνέπεια μεμονωμένοι υπολογιστές, εξυπηρετητές ιστοσελίδων (web servers) ή και εξυπηρετητές δικτύων (network servers), απλά να μην μπορούν να εκτελέσουν ούτε ένα ποσοστό της φυσιολογικής λειτουργίας τους.[15]

4.2.1.10 Μικτές απειλές

Στην πράξη έχει παρατηρηθεί και η εκδήλωση 'μικτών απειλών' πολύ προηγμένου τύπου, δηλαδή επιθέσεων στις οποίες χρησιμοποιούνται με συνδυασμένο και συνδυαστικό τρόπο και χρονικά ταυτόχρονο ή/και συγχρονισμένο τα πλέον επικίνδυνα χαρακτηριστικά των ιών, των δούρειων ίππων, των ηλεκτρονικών 'σκουληκιών' και άλλων ειδών κακόβουλου λογισμικού, όλα σε μια απειλή εκμεταλλεύονται τις τρωτότητες των η/υ – εξυπηρετητών και του internet για ταχεία και εκτεταμένα αποτελέσματα.[4]

4.2.1.11 Bot (Διαδικτυακό ρομπότ)

Παράγεται από τη λέξη robot και αποτελεί λογισμικό που εκτελεί μια αυτοματοποιημένη διαδικασία που αλληλοεπιδρά με άλλες υπηρεσίες του δικτύου. Συχνά, ένα bot αυτοματοποιεί διαδικασίες (tasks) και παρέχει πληροφορίες σε υπηρεσίες που διαφορετικά θα έπρεπε να προσφέρονται από ανθρώπους. Για παράδειγμα, υπηρεσίες συγκέντρωσης πληροφοριών (web crawlers). Ένα bot μπορεί να χρησιμοποιηθεί καλόβουλα ή κακόβουλα. Στη δεύτερη περίπτωση αποτελεί παράδειγμα αναπαραγωγού που έχει σχεδιαστεί για να προσβάλει ένα Υ.Σ. και να συνδέεται πίσω σε έναν κεντρικό (ή κεντρικούς) servers. Αυτοί λειτουργούν ως κέντρο ελέγχου και μεταβίβασης εντολών (Command and Control (C&C)) για ολόκληρο το δίκτυο των προσβεβλημένων συσκευών που αποκαλείται botnet. Μια μηχανή που έχει μολυνθεί από ένα bot συχνά αναφέρεται ως zombie. Έχοντας ένα botnet, ο επιτιθέμενος μπορεί να εξαπολύσει μια πλειάδα επιθέσεων που περιλαμβάνουν DoS και διάδοση ανεπιθύμητων μηνυμάτων (spam). Συνήθως ένα bot έχει την ικανότητα να καταγράφει το πληκτρολόγιο (log keystrokes), να συλλέγει συνθηματικά, να συλλέγει καν να αναλύει IP πακέτα, να εγκαθιστά backdoors, κ.ά. Γενικά ένα bot έχει όλα τα πλεονεκτήματα ενός αναπαραγωγού αλλά είναι εξυπνότερο όσον αφορά τη φάση προσβολής του στόχου και ο κώδικάς του τροποποιείται συχνότερα. Επίσης,γίνεται δυσκολότερα αντιληπτό.[15]

4.2.1.12 Stuxnet

Το Stuxnet είναι ένα πρόγραμμα υπολογιστή που σκοπό έχει να ελέγχει ένα απομακρυσμένο σύστημα σχεδόν αυτόνομα. Τα χτυπήματα γίνονταν με επαφή ,όπως για παράδειγμα με την βοήθεια ενδιάμεσου ένα USB φλασάκι με σκοπό την πρόσβαση στον έλεγχο του συστήματος που θέλουμε να επιτεθούμε. Το κακόβουλο αυτό λογισμικό με διάφορες τεχνικές κατασκοπείας και τον έτοιμο κώδικα εξοικονομούσε χρήματα με σκοπό την εξειδίκευση του κώδικα.Σύμφωνα με το σύστημα παρακολούθησης πληροφοριών πολέμου ο στόχος της επιθέσης μπορεί να παραβιαστεί πολύ συχνά ,αφου η τεχνολογία σχεδίασης –αναπτύξης και λειτουργίας είναι φθηνή. Μερικά από τα χαρακτηριστικά του σε επίπεδο λειτουργίας του είναι[16] :

- Χρήση ενός δικτύου εντολής και ελέγχου βασισμένο σε DNS , χωρίς να τον νοίαζει αν θα γίνει αντιληπτό συγκριτικά με άλλα κακόβουλα λογισμικά.
- Χρήση πολλαπλών προγραμμάτων εκμετάλλευσης ευπαθειών (zero-day) κώδικα , για καλύτερες πρακτικές επιθέσεις .Τα σημεία ευπάθειας άγνωστα μέχρι πρώτινος δημιουργίας κάποιου λογισμικού ενημέρωσης.
- Ικανότητα προσπέλασης συστημάτων κενού αέρα,για κλοπή εγγράφου απορρήτου χαρακτήρα.

- Χρήση προεπιλεγμένου κώδικα πρόσβασης ,με στόχο την πρόσβαση σε λειτουργικά συστήματα Windows για έλεγχο των WinCCC[18] και των PCS 7[19] προγραμμάτων.
- Χρήση έτοιμου κώδικα και τεχνικές κατασκοπείας[20].

4.2.2 Κατασκοπεία

Κατασκοπεία θεωρείται η απόκτηση απόρρητων ή εμπιστευτικών πληροφοριών από μια κυβέρνηση, εταιρεία/επιχείρηση ή φυσικό πρόσωπο, χωρίς την άδεια του κατόχου των πληροφοριών. Είναι εγγενώς μυστική, όπως είναι αυτονόητο ότι είναι ανεπιθύμητη και σε πολλές περιπτώσεις παράνομη και τιμωρείται από το νόμο. Είναι ένα υποσύνολο της "συλλογής πληροφοριών", το οποίο αλλιώς μπορεί να διεξάγεται από δημόσιες πηγές και με τη χρήση απολύτως νόμιμων και ηθικών μέσων. Είναι σημαντικό να γίνει διάκριση της κατασκοπείας από την "συλλογή πληροφοριών", καθώς η τελευταία δεν συνεπάγεται αναγκαστικά την κατασκοπεία, αλλά συχνά αντιπαραβάλει πληροφορίες *open-source*.Η κατασκοπεία είναι συχνά μέρος μίας θεσμικής προσπάθειας από μια κυβέρνηση ή έχει εμπορικό ενδιαφέρον. Ωστόσο, ο όρος συνδέεται γενικά με την κρατική κατασκοπεία σε δυνητικούς ή πραγματικούς εχθρούς κυρίως για στρατιωτικούς σκοπούς. Η κατασκοπεία που αφορά τις επιχειρήσεις είναι γνωστή ως βιομηχανική κατασκοπεία.

Υπάρχουν πολλά κακόβουλα λογισμικά που είναι εργαλεία κατασκοπίας.Αυτά δεν βλάπτουν άμεσα τα πληροφοριακά συστήματα ούτε προκαλούν κατευθείαν βλάβη,αλλά μόνο μέσα από συναλλαγές πληροφοριών.Η κατασκοπία δεν έχει θεωρηθεί ως *casus belli* (συνηθισμένος ή θεμιτός λόγος για εμπλοκή σε πόλεμο) λόγος που δεν αποκλείει την περίπτωση μη στρατιωτικών αντιποίνων.

Ο πρώην διευθυντής της Εθνικής Υπηρεσίας Πληροφοριών Dennis Blair,στην Επίλεκτη Επιτροπή Πληροφοριών της Γερουσίας τον Φεβρουάριο 2010 είπε: «η υπολογιστική κρίσιμη υποδομή των ΗΠΑ «απειλείται σοβαρά» από κακόβουλες κυβερνοεπιθέσεις και κυβερνοκατασκοπεία που τώρα συμβαίνουν σε μια «άνευ προηγουμένου κλίμακα με εξαιρετική πολυπλοκότητα.»[3]

[18] Το WinCC είναι μια εξαγορά εποπτικού ελέγχου και δεδομένων (SCADA) για διεπαφή ανθρώπου-μηχανής συστήματος (HMI) από τη Siemens .
[19] Το PCS 7 είναι ένα σύστημα ελέγχου διαδικασίας της εταιρείας Siemens , η οποία συντόνισε τις λειτουργίες Simatic -Hardware- και τα συστατικά λογισμικού από το εύρος σύστημα Απόλυτα Ολοκληρωμένο Αυτοματισμού.
[20] Θα αναλυθεί στο κεφάλαιο

5 *Τρόποι Αντιμετώπισης & Τεχνικές/Οργανωτικές Λύσεις (όχι ακομα παραπομπες)*

5.1 DoS και Κακόβουλο Λογισμικό

Πολλές από αυτές τις τεχνικές των επιθέσεων DoS και της εισαγωγής κακόβουλου λογισμικού θα μπορούσαν να καταπολεμηθούν.Μερικοί τρόποι αντιμετώπισης θα μπορούσαμε να πούμε ότι είναι η επίγνωση σε θέματα ασφάλειας,το αντιβιοτικό λογισμικό,τα αυστηρά μέτρα ασφάλειας,η απομόνωση,τα εργαλεία ανίχνευσης εισβολών (IDS),η συνεργασία με οργανισμούς που προσφέρουν προϊόντα υλικού και λογισμικού,η διατυπωμένη διαδικασία ανάνηψης από προσβολή και περιορισμού Κ.Λ. και τέλος η διατυπωμένη διαδικασία επιλογής λογισμικού, παρακολούθηση των προβλημάτων ασφάλειάς του (vulnerabilities) και ενημέρωσής του.

Αναλυτικά για να καταπολεμήσουμε μία επίθεση θα πρέπει να είμαστε γνώστες σε θέματα ασφαλείας όπως για θέματα που αφορούν κακόβουλο λογισμικό ,χειρισμό εφαρμογών antivirus και αποφυγής μεταφόρτωσης και εγκατάστασης μη ελεγμένων προγραμμάτων από άγνωστες ή μη έμπιστες πηγές.Όσο αφορά το αντιβιοτικό λογισμικό θα πρέπει να γίνεται συχνή ενημέρωσή του και εξέταση των αρχείων ελέγχου για δραστηριότητα που προδίδει κακόβουλο λογισμικό.Τα αυστηρά δικαιώματα πρόσβασης και η εκτέλεση εφαρμογών με τα ελάχιστα δικαιώματα που αυτές απαιτούν (Least privilege) είναι απαραίτητα.Επίσης για την καταπολέμηση των επιθέσεων καλό θα ήταν η απομόνωση τμημάτων Π.Σ. που περιέχουν διαβαθμισμένες πληροφορίες από άλλα τμήματα που περιέχουν μη διαβαθμισμένες και αναχωμάτων ασφαλείας.Τα εργαλεία ανίχνευσης εισβολών όπως αυτά για ανίχνευση Κ.Λ. με βάση γνωστές συμπεριφορές τυπικών προγραμμάτων Κ.Λ. και με βάση συμπεριφορές που διαφέρουν από τις τυπικές συμπεριφορές έγκυρων χρηστών είναι ένας τρόπος προστασίας.Από τους τρόπους καταπολέμησης που δεν

πρέπει να παραλείψουμε είναι η συνεργασία με οργανισμούς που προσφέρουν προϊόντα υλικού και λογισμικού για προστασία από Κ.Λ. και η ενημέρωση των οργανισμών αυτών σε περίπτωση εμφάνισης προγράμματος που ενδέχεται να συνιστά Κ.Λ. αλλά δεν έχει καταγραφεί.Επιπρόσθετα η απομόνωση και η απομάκρυνση προσβεβλημένων συστημάτων, η αποκατάσταση ακεραιότητας προσβεβλημένου συστήματος και η ενημέρωση τελικών χρηστών σχετικά με ενδεχόμενες ενέργειες που οφείλουν να κάνουν οι ίδιοι σε περίπτωση εμφάνισης εφαρμογών που ενδέχεται να συνιστούν Κ.Λ πρέπει να τηρούνται.Τέλος σύμφωνα με τη διατυπωμένη διαδικασία επιλογής λογισμικού, παρακολούθηση των προβλημάτων ασφάλειάς του (vulnerabilities) και ενημέρωσής του θα πρέπει η πηγή να μην είναι μόνο έμπιστη, αλλά και να μπορεί να υποστηρίζει την παραπάνω διαδικασία.[15]

5.2 Τεχνικές Λύσεις για την Αποφυγή των Κυβερνοεπιθέσεων

Πέρα από τις μακρπρόθεσμες και βραχυπρόθεσμες προσεγγίσεις του Scott Shackelford υπάρχουν και μερικές τεχνικές λύσεις για την αποφυγή των κυβερνοεπιθέσεων[3].Μερικές από αυτές είναι:

- Hash-Based IP Trace back (Βασισμένη στον κατακερματισμό ανίχνευση της IP προς τα πίσω) – Οι δρομολογητές αποθηκεύουν τις τιμές κατακερματισμού των πακέτων δικτύου. Η απόδοση γίνεται με την ανίχνευση προς τα πίσω των τιμών κατακερματισμού μέσα από τους δρομολογητές δικτύων.
- Ingress Filtering (φιλτράρισμα εισροής) – Όλα τα μηνύματα που εισέρχονται σε ένα δίκτυο απαιτείται να έχουν μια διεύθυνση πηγής σε μια έγκυρη περιοχή, αυτό περιορίζει την περιοχή των πιθανών πηγών των επιθέσεων.
- ICMP Return to Sender (Πρωτόκολλο Ελέγχου Μηνυμάτων Διαδικτύου Επιστροφή στον Αποστολέα) – Όλα τα πακέτα που προορίζονται για το θύμα απορρίπτονται και επιστρέφονται στους αποστολείς τους.
- Overlay Network for IP Trace back (Επικαλυπτικό Δίκτυο για Ανίχνευση πίσω της IP) – Ένα επικαλυπτικό δίκτυο συνδέει όλους τους ISP ακραίους δρομολογητές με έναν κεντρικό δρομολογητή παρακολούθησης, οι προσεγγίσεις hop-by-hop χρησιμοποιούνται για να βρεθεί η πηγή.
- Trace Packet Generation (Ανίχνευση γενιάς πακέτου) (π.χ. iTrace) – Ένας δρομολογητής στέλνει ένα ICMP μήνυμα ανίχνευσης πίσω περιοδικά (π.χ. 1 ανά 20000 πακέτα) στην ίδια διεύθυνση προορισμού όπως το πακέτο δείγμα. Ο προορισμός (ή ο οριζόμενος επόπτης) συλλέγει και συσχετίζει τις πληροφορίες παρακολούθησης.
- Probabilistic Packet Marking (Πιθανολογική Σήμανση Πακέτου) – Ένας δρομολογητής προσδιορίζει τυχαία αν θα ενσωματώσει δεδομένα διαδρομής μηνύματος σε ένα μήνυμα. Αυτά τα δεδομένα διαδρομής χρησιμοποιούνται για τον προσδιορισμό διαδρομών.
- Hack back – Σε έναν ξενιστή ενσωματώνεται η υποβολή ερωτήσεων λειτουργικότητας χωρίς την άδεια του ιδιοκτήτη. Εάν ένας επιτιθέμενος ελέγχει τον ξενιστή, αυτό δεν θα τον προειδοποιήσει, οπότε οι πληροφορίες είναι πιο αξιόπιστες.
- Honey pots (Δοχεία μελιού) – Συστήματα δολώματα συλλαμβάνουν πλροφορίες για τους επιτιθέμενους που μπορούν να χρησιμοποιηθούν για την απόδοση.

- Υδατογράφησης – Τα αρχεία μαρκάρονται όπως ανήκουν στους δικαιούχους ιδιοκτήτες τους.

Οι τεχνικές αυτές ,θα πρέπει να ασφαλίζουν την ακεραιότητα τους.Το λογισμικό που χρησιμοποιείται για τον έλεγχο ταυτότητας και τα στοιχεία που χρησιμοποιούνται για την απόδοση πρέπει να προστατεύονται.

5.3 Ασφάλεια Δικτύων

Για την προστασία των δικτύων από κυβερνοεπιθέσεις σημαντικό ρόλο έχει η ενίσχυση των τεχνικών μέτρων ασφάλειας και πολιτικών ασφάλειας. Η καλύτερη λοιπόν ,άμυνα των κρίσημων υποδομών πρηροφοριών για την προστασία των δεδομένων είναι μία είς βάθος στρατηγική τοποθέτηση των συστημάτων Πληροφοριών και του προσωπικού ασφαλείας .

Από την μεριά των διαχειριστών και του προσωπικού ασφαλείας θα πρέπει

Οι διαχειριστές και το προσωπικό ασφαλείας από την μεριά τους για να βγάλουν εις πέρας αυτό το έργο θα πρέπει [3] :

- Να γνωρίζουν πώς δουλεύουν τα συστήματά τους,με σκοπό να μπορούν να προφυλάξουν τα τυχόν εκμεταλλεύσιμα σημεία τους από αυτούς που θέλουν να επιτεθούν στο σύστημα.
- Να διεξάγουν τακτικές δοκιμές διείσδυσης και ελέγχου της τεχνολογίας πληροφοριών ώστε να εξετάζουν τις τρωτότητες των συστημάτων και να εξασφαλίζουν ορθή αποτροπή.
- Να γνωρίζουν τις ικανότητες πιθανόν επιτιθέμενων και τις τελευταίες τεχνολογίες, για καλύτερη ασφάλεια από κακόβουλα λογισμικά και τεχνικές DDOS των χάκερς.

Μερικά μέτρα προστασίας για την εξάλειψη των απειλών στο διαδίκτυο μπορούμε να πούμε ότι είναι:[17]

- Antivirus and Antispyware:Προληπτική προστασία ενάντια σε όλες τις online και offline απειλές.
- Σάρωση βασισμένη στο Cloud:Αξιοποιήση ταχύτητας διαδικασίας σάρωσης, η οποία χρησιμοποιεί την online βάση δεδομένων φήμης αρχείων για να διακρίνετε τα ασφαλή αρχεία.
- Anti-Phishing:Προστασία από απόπειρες ψεύτικων websites να υποκλέψουν τα ευαίσθητα δεδομένα, όπως usernames, κωδικοί ή πληροφορίες τραπεζικών συναλλαγών και στοιχεία πιστωτικών καρτών.
- Σάρωση Καθώς Κάνετε Download τα Αρχεία:Ελαχιστοποίηση του χρόνου σάρωσης, ελέγχοντας τα μεγάλα αρχεία τη στιγμή που γίνονται download.
- Έλεγχος Αφαιρούμενων Μέσων:Μπλοκάρει τα άγνωστα CDs, DVDs, USBs & άλλα μέσα, εμποδίζοντας έτσι τη μη εξουσιοδοτημένη αντιγραφή των προσωπικών σας δεδομένων σε εξωτερικές συσκευές αποθήκευσης.

- Host-based Intrusion Prevention System (HIPS):Προσαρμόζει την συμπεριφορά του συστήματος με μεγαλύτερη λεπτομέρεια.

Η Ευρωπαϊκή Επιτροπή, μαζί με τον Ύπατο Εκπρόσωπο της Ένωσης για τις Εξωτερικές Υποθέσεις και την Πολιτική Ασφάλειας σε μία πρότασή του με στόχο να αντιμετωπίσει το ζήτημα της Ασφάλειας των Δικτύων και των Πληροφοριών (Network and Information Security—NIS) τον Φεβρουάριο του 2013 έγραψε «η ΕΕ δεν απαιτεί τη δημιουργία νέων διεθνών νομικών μέσων για τα κυβερνοζητήματα» και ότι «οι νομικές υποχρεώσεις που κατοχυρώνονται στη Διεθνή Σύμβαση για τα Ατομικά και Πολιτικά Δικαιώματα, την Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα και το Καταστατικό των Θεμελιωδών Δικαιωμάτων της ΕΕ θα έπρεπε να γίνουν επίσης σεβαστές online».[13]

5.4 Προστασία των Ψηφιακών Υποδομών

Για την προστασία των ψηφιακών υποδομών του κόσμου και μιας ευρύτερης προσπάθειας για προστασία του κυβερνοχώρου δημιουργείται μία νέα συνεργασία ανάμεσα στη Ρωσία και στις ΗΠΑ.

Η Ρωσία και οι Ηνωμένες Πολιτείες θα πρέπει να αναλάβουν από κοινού τις πολιτικές αξιολογήσεις των νομικών θεμάτων ρύθμισης του κυβερνοπολέμου, συμπεριλαμβανομένων των επιθετικών και αμυντικών δραστηριοτήτων, ειδικά στον τομέα των κρίσιμων υποδομών και των «κανόνων εμπλοκής».

5.5 Κυβερνοπροκλήσεις

Για την αποτελεσματική αντιμετώπιση των κυβερνοπροκλήσεις, θα πρέπει οι οργανισμοί ασφάλειας και οι στρατοί, να καθορίσουν τις επιχειρησιακές αποστολές, τις απαιτούμενες δυνατότητες και τις δομές στρατιωτικής δύναμης σε όλο το εύρος του κυβερνοφάσματος.Σύμφωνα με την επίσημη αμερικανική προσέγγιση, οι κυβερνητικοί οργανισμοί ασφάλειας πρέπει να αναπτύξουν συστήματα και αμυντικές διαδικασίες απέναντι στις πιο ανησυχητικές κυβερνοευπάθειες και απειλές.

Για την αποφυγή του κυβερνοτρόμου και της χρήσης του κυβερνοχώρου για εχθρικές δραστηριότητες θα ήταν καλό να γίνει μία μονιμοποίηση διαφόρων νόμων και κανόνων.Στην πρίπτωση των ΗΠΑ, θα πρέπει να δημιουργηθεί μία δομή νομικού χαρακτήρα για συνεργασία εθνών με σκοπό την αντιμετώπιση του κυβερνοπολέμου ,δηλαδή κάτι αντίστοιχο με το νομικό πλαίσιο της στρατιωτικής και ένοπλης επίθεσης.[10]

5.6 Μέτρα Μείωσης Κινδύνου Διαταραχών & Προστασία ΤΠΕ

Η Ομάδας Κυβερνητικών Εμπειρογνωμώνων[21] σε ένα ψήφισμα με θέμα «Εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στα πλαίσια της διεθνούς ασφάλειας» αναφέρουν τα μέτρα για την μείωση του κινδύνου εσφαλμένης εκτίμησης που προέρχεται από διαταραχές των ΤΠΕ[3]:

- Περαιτέρω διάλογο μεταξύ των Κρατών για τη συζήτηση των κανόνων που αφορούν την κρατική χρήση των ΤΠΕ, την μείωση του συλλογικού κινδύνου και την ασφάλεια κρίσιμων εθνικών και διεθνών υποδομών.
- Μέτρα για την οικοδόμηση εμπιστοσύνης, τη σταθερότητα και τη μείωση του κινδύνου για την αντιμετώπιση των επιπτώσεων της Κρατικής χρήσης των ΤΠΕ, συμπεριλαμβανομένων συναλλαγών των εθνικών απόψεων σχετικά με τη χρήση των ΤΠΕ σε σύγκρουση.
- Ανταλλαγές πληροφοριών σχετικά με την εθνική νομοθεσία και τις στρατηγικές ασφάλειας των εθνικών τεχνολογιών πληροφοριών και επικοινωνιών, πολιτικών και βέλτιστων πρακτικών.
- Προσδιορισμός των μέτρων για την υποστήριξη οικοδόμησης ικανοτήτων σε λιγότερο ανεπτυγμένες χώρες.
- Ανεύρεση δυνατοτήτων για ανάπτυξη κοινών όρων και ορισμών σχετικών με το ψήφισμα της Γενικής Συνέλευσης 64/25 (Ψήφισμα που εγκρίθηκε από τη Γενική Συνέλευση [στην έκθεση από την Πρώτη Επιτροπή (A/64/386)] 64/25. Εξελίξεις στον τομέα της πληροφορίας και των τηλεπικοινωνιών στα πλαίσια της διεθνούς ασφάλειας.

Μία από τις μεγαλύτερες δυσκολίες στον εντοπισμό των στόχων των εχθρών είναι οι δραστηριότητες εξαπάτησεις που δυσκολεύουν το κράτος να δημιουργήσει ένα επιχειρησιακό σχεδιασμό και να οργανώσει μια κατάλληλη στρατιωτική δύναμη.Έτσι ,για το σκοπό αυτό έχουν δημιουργηθεί διάφορες ομάδες που εργάζονται στον τομέα ανάπτυξης ιών υπολογιστών με στόχο την προστασία των πληροφοριακών πόρων από τις διάφορες εχθρικές κυβερνοδραστηριότητες.Μία άλλη τεχνική άμυνας που χρησιμοποιήθηκε στη Ρωσία είναι και η ανάπτυξη ενός κοινού συστήματος για την παροχή πληροφοριών για την ανάπτυξη του Ρωσικού Στρατού Ξηράς με στόχο την δημιουργία πληροφοριακών υποδομών για τις διεργασίες διοίκησης και ελέγχου με βάση τις νέες τεχνολογίες πληροφορίας.Ιδιαίτερη έμφαση έδειξαν και ο ρώσος πρόεδρος και ο ρώσος υπουργός άμυνας στο έργο αυτό.

[21] Τον Ιούλιο 2010, ανακοινώθηκε ότι μια ομάδα από «ειδικών κυβερνοασφάλειας και διπλωμάτες που αντιπροσώπευαν 15 χώρες συμφώνησαν σε μια σειρά συστάσεων προς τον Γενικό Γραμματέα των Ηνωμένων Εθνών για διαπραγματεύσεις για μια διεθνή συνθήκη για την ασφάλεια των υπολογιστών».

6 *Περιστατικά Κυβερνοεπιθέσεων*

Με την πρόοδος του ICTs παρατηρείται όλο ένα και περισσότερα περιστατικά κυβερνοεπιθέσεων. Οι νέες τεχνολογίες δίνουν το λιθαράκι τους στο ένα και πιο μπροστά βήμα για την αύξηση των επιθέσεων στον Κυβερνοχώρο, κατατάσσοντάς το σε ένα από τα πιο επίκαιρο φαινόμενο στην σημερινή εποχή.

6.1 Εσθονία 2007

Η Εσθονία δέχθηκε επίθεση από τέλη Απριλίου ως αρχές Μαΐου του 2007. Η επίθεση αυτή έγινε με την χρήση των Bots όπου Ρώσσοι εγκληματικοί φορείς χτύπησαν τα κοινωνικά δίκτυα της της Εσθονίας.Μετά από αυτές τις επιθέσεις ,η Εσθονία προσέγγισε το NATO για στρατιωτική βοήθεια αλλά το NATO δεν μπορούσε να χρησιμοποιήσει την τότε αρμοδιότητα και πολιτική του για να παρέμβει. Έπειτα το NATO άνοιξε Συνεργατικό Κέντρο Κυβερνο Άμυνας Αριστείας στο Ταλίν της Εσθονίας το 2008. Η Εσθονία μέχρι να γίνει το Κέντρο Κυβερνο Άμυνας Αριστείας υιοθέτησε νέα νομοθεσία και πολιτική για να αντιμετωπίσει όποιες μελλοντικές παρόμοιες επιθέσεις στην υποδομή της του Διαδικτύου.

Πάνω στην επίθεση αυτή του 2007 ο Jaak Aaviksoo, Υπουργό Άμυνας της Εσθονίας,αναφέρει:

«οι περισσότερες επιθέσεις στόχευαν στους διακομιστές της κυβέρνησης και των ειδησεογραφικών γραφείων, αλλά και οι δύο μεγαλύτερες τράπεζες της Εσθονίας υπέστησαν βαριά επίθεση. Στις σημαντικότερες στιγμές, η ποσότητα της κυβερνο κυκλοφορίας που στόχευε κυβερνητικά ιδρύματα από έξω από την Εσθονία ήταν 400 φορές υψηλότερη από το φυσιολογικό επίπεδο. ... Μερικές από τις επιθέσεις πραγματοποιήθηκαν σε κύματα και εκτελέστηκαν με πολύ ακριβή χρονισμό. Ήταν ασυνήθιστα καλά συντονισμένες και απαιτούσαν πόρους μη διαθέσιμους στον μέσο άνθρωπο. Σε κάποιο σήμειο, οι επιθέσεις πραγματοποιούνταν

σε ένα πολύ ακριβές χρονοδιάγραμμα και περιλάμβαναν ομάδες υπολογιστών – «προγράμματα ρομπότ» - τα οποία πιθανόν να ενοικιάστηκαν νωρίτερα για αυτό το σκοπό.»[3]

Βλέποντας το αποτέλεσμα της επίθεσης ο Jaak Aavikso συμπληρώνει:

«Λαμβάνοντας υπόψη το μέγεθος των υποδομών της Εσθονίας και την έκταση των επιθέσεων, ήταν μια από τις πιο σημαντικές και συντονισμένες κυβερνοεπιθέσεις ενάντια σε ένα κυρίαρχο κράτος στον κόσμο... Παρόλο που η επίθεση ανατράπηκε χωρίς μακροπρόθεσμες επιπτώσεις, υπήρξαν κάποιες άμεσες επιδράσεις που επηρέασαν όλους τους πολίτες της Εσθονίας, όπως η μη διαθεσιμότητα των διαδικτυακά τραπεζικών υπηρεσιών ή δυσκολίες στις επικοινωνίες. Σε μια χώρα που το 98% των τραπεζικών συναλλαγών γίνονται διαδικτυακά και όπου η πλειοψηφία των πολιτών συμπληρώνουν τα φορολογικά έντυπα διαδικτυακά , είμαι σίγουρος ότι μπορείτε να συνειδητοποιήσετε τον αντίκτυπο που τέτοια παρατεταμένα περιστατικά μπορεί να έχουν... Ο αντίκτυπος των επιθέσεων μεγεθύνθηκε από την ψυχολογική επίδραση και εκφοβισμό που είχε στον γενικό πληθυσμό. Εκτός από την απευθείας επίδραση του στόχου, οι κυβενοεπιθέσεις δημιούργησαν ευρεία σύγχυση και κακή επικοινωνία στο ευρύ κοινό, καθώς ήταν αδύνατη η πρόσβαση από το εξωτερικό σε πληροφορίες σχετικά με τα γεγονότα στην Εσθονία.»[3]

6.2 Γεωργία 2008

Επίσης είναι σημαντικό να αναφερθεί και ο πόλεμος μεταξύ Ρωσίας και Γεωργίας το 2008.Η Ρωσία χτύπησε την Γεωργία αποσιωπώντας τις ιστοσελίδες της κυβέρνησής της και τα μέσα ενημέρωσή της με σκοπό να μην μπορεί η κυβέρνηση να επικοινωνήσει με τον πληθυσμό της.Με την επίθεση αυτή παρέλυσαν την δημόσια διοίκηση της Γεωργίας.Οι επιθέσεις αυτές δεν έλειπαν από το επίκεντρο των συζητήσεων.Οι Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul (2008) παραθέτουν μια σειρά προτάσεων για την αντιμετώπιση των θυμάτων –περιοχών των κυβερνοεπιθέσεων μέσα από την μελέτη τους και το έργο τους. Προτείνουν ότι νέες προσεγγίσεις στο παραδοσιακό Δίκαιο των Ένοπλων Συγκρούσεων πρέπει να αναπτυχθούν ώστε να παρέχει αποτελεσματικές νομικές επιδιορθώσεις κάτω από αυτόν τομέα του δικαίου. Ο Jon Bumgarner (2009), ο Γενικός Διευθυντής του Τεχνικού Τμήματος της Μονάδας Κυβερνο-επιπτώσεων των ΗΠΑ, έκανε μια σειρά απο εντυπωσιακές παρατηρήσεις για την Γεωργία το καλοκαίρι του 2008:

«Πολλές από τις κυβερνοεπιθέσεις ήταν τόσο κοντά χρονικά στις αντίστοιχες στρατιωτικές επιχειρήσεις που πρέπει να υπήρχε κοντινή συνεργασία μεταξύ των ανθρώπων στον Ρωσικό στρατό και τους πολίτες επιτιθέμενους μέσα από τον κυβερνοχώρο. Όταν οι κυβερνοεπιθέσεις ξεκίνησαν δεν περιλάμβαναν στάδια αναγνώρισης ή χαρτογράφησης αλλά κατευθείαν πέρασαν στο είδος πακέτων που ήταν το καταλληλότερο για την εμπλοκή των ιστότοπων υπό επίθεση. Αυτό υποδεικνύει ότι η απαραίτητη αναγνώριση και η εγγραφή των σεναρίων επίθεσης έπρεπε να είχαν γίνει εκ των προτέρων. Πολλές από τις πράξεις των δραστών, όπως η εγγραφή νέων

ονομάτων ιστοχώρου και η δημιουργία νέων ιστοσελίδων, πραγματοποιήθηκαν τόσο γρήγορα που όλα τα βήματα έπρεπε να είχαν προετοιμαστεί νωρίτερα.»[3]

Ο Bumgarner προσθέτει ότι «οι διοργανωτές των κυβερνοεπιθέσεων είχαν εκ των προτέρων ειδοποίηση των προθέσεων του Ρώσικου στρατού, και πληροφορήθηκαν για τη χρονική στιγμή των επιχειρήσεων του Ρωσικού στρατού ενώ αυτές οι επιχειρήσεις πραγματοποιούνταν.»[3]

Τέλος καταλήγει στο συμπέρασμα ότι: «Από την κυβερνο εκστρατεία ενάντια στην Εσθονία τον Απρίλιο και Μάιο του 2007, οι Ρώσοι είχαν ήδη μάθει ότι μια κυβερνο εκστρατεία που πραγματοποιείται από πολίτες μπορεί να προκαλέσει σοβαρές οικονομικές και ψυχολογικές διαταραχές σε μια χώρα χωρίς να προκαλέσει κάποια σοβαρή διεθνή απόκριση. Αυτό το μάθημα ενισχύθηκε από τις εμπειρίες τους με τις κυβερνο εκστρατείες ενάντια στη Λιθουανία στο τέλος του Ιουνίου 2008 και ενάντια στο Καζακστάν τον Ιανουάριο του 2009, όπου μεγάλες τοπικές διαταραχές παρήγαγαν εντυπωσιακά μικρή κάλυψη από τον διεθνή τύπο.Η εκστρατεία ενάντια στη Γεωργία έλαβε χώρα κάτω από διαφοτικές συνθήκες, γιατί η Ρωσία είχε εμπλακεί σε απροκάλυπτη στρατιωτική δράση ενάντια στη χώρα, αλλά η συνιστώσα του κυβερνοχώρου πραγματοποιούταν ακόμα από πολίτες, και δεν υπήρχαν διεθνή αντίποινα. Με δεδομένο αυτή την ιστορία, θα ήταν πολύ αναπάντεχο αν οι μελλοντικές διενέξεις και συγκρούσεις που θα περιλαμβάνουν τη Ρωσία και τις πρώην κτήσεις ή δορυφόρους της δεν συνοδεύονται από κυβερνο εκστρατείες.»[3]

6.3 Ιαπωνία 2010

Στις 19 Σεπτεμβρίου του 2010 η Ιαπωνία υποψιαζότανε ότι μία κατανεμημένη επίθεση άρνησης εξυπηρέτησης ¨χτυπούσε¨ τις ιστοσελίδες του Υπουργείου Αμύνης και της Υπηρεσίας Εθνικής Αστυνομίας λόγω μιας διένεξης που είχε με τη Λαϊκή Δημοκρατία της Κίνας («ΛΔΚ»), όπως ανέφεραν τα μέσα. Η Ιαπωνική κυβέρνηση πήρε τα μέτρα της διατάζοντας τις κυβερνητικές οντότητες να λάβουν μέτρα αυτοάμυνας, όπως να κλείσουν τις ιστοσελίδες τους, για σύντομο χρονικό διάστημα.Οι υποψίες της Ιαπωνίας βασίζονται σε ένα περιστατικό που έγινε στις 7 Σεπτέμβρη 2010 όπου μιας Κινέζικης τράτας και δύο Ιαπωνικών οχημάτων της ακτοφυλακής κοντά σε μια αμφιλεγόμενη σειρά νησιών στην Ανατολική Θάλασσα της Κίνας συγκρούστηκαν.Η σύγκρουση αυτή δεν τελείωσε ειρηνικά καθώς η μεγαλύτερη ομάδα πειρατείας της Κίνας είχε προειδοποιήσει ότι θα επιτιθόταν σε Ιαπωνικές ιστοσελίδες ως διαμαρτυρία για το περιστατικό.[3]

6.4 Ουάσιγκτον 2011

Η επίθεση στο μετρό της Ουάσιγκτον στις 11 Σεπτεμβρίου 2011 απασχόλησε τον Καθηγητής Thomas Wingfield στην ανάλυσή του σχετικά με τον κυβερνοπόλεμο. Οι τρομοκράτες σε ώρα αιχμής χρησιμοποίησαν κακόβουλο κώδικα για να χτυπήσουν το σύστημα εντατικού λογισμικού προστασίας των αυτόματων τρένων του μετρό.Στην επίθεση αυτή χρησιμοποιήθηκαν

διακυνδυνευμένοι διοικητικοί υπολογιστές από υπαλλήλους του μετρό για την παρακολούθηση των εργασιών.

6.5 Κόσοβο 1999

Μία συνταρακτική επίθεση έγινε στο Κόσοβο στις 24 Μαρτίου του 1999, όταν το ΝΑΤΟ ξεκίνησε τους αεροπορικούς βομβαρδισμούς εναντίον της Σερβίας, επειδή η τελευταία αρνείτο να υπογράψει τη συμφωνία για το μέλλον του Κοσσυφοπεδίου. Οι βομβαρδισμοί διήρκεσαν σχεδόν 3 μήνες και ακολουθήθηκαν από χερσαία εισβολή. Πρόκειται για την πρώτη επίθεση στην ιστορία της Συμμαχίας κατά κυρίαρχου κράτους.

Στη διάρκεια των βομβαρδισμών, σύμφωνα με τη διεθνή οργάνωση προάσπισης των ανθρωπίνων δικαιωμάτων Human Rights Watch, 500 περίπου άμαχοι έχασαν τη ζωή τους σε 90 διαφορετικά επεισόδια, κατηγορώντας το ΝΑΤΟ για παραβιάσεις του διεθνούς δικαίου. Το Βελιγράδι, από την πλευρά του, έκανε λόγο για 5.000 νεκρούς αμάχους στη διάρκεια των 78ήμερων αεροπορικών επιχειρήσεων.[18]

6.6 Νατάνζ 2010

Το πρώτο χτύπημα που έκανε την αρχή για την εμφάνιση του Stuxnet ήταν τον Ιούνιο του 2010 οι Ιρανικές πυρηνικές εγκαταστάσεις που χτυπήθηκαν στο Νατάνζ.Μόλυνε πάνω από 60.000 υπολογιστές που οι περισσότεροι από αυτούς βρίσκονταν στο Ιράν, χωρίς να περιοριστεί μόνο εκεί.Από το χτύπημα αυτό επηρεάστηκαν επίσης και άλλες χώρες όπως η Ινδία, η Ινδονησία η Κίνα το Αζερμπαϊτζάν, η Φινλανδία και η Γερμανία. Ο ιός δεν έμεινε εκεί.Προχώρησε μέσα από το διαδίκτυο και σε άλλα συστήματα υπολογιστών χωρίς βέβαια να προκαλέσει τον ίδιο βαθμό ζημίας αφού η χρήση αντιδότων περιόρισε σημαντικά την εξάπλωση του μέχρι και τις 24 Ιουνίου του 2012.

6.7 Ιράν 2011

Άλλη μία επίθεση έγινε στο Ισραήλ στο Ιράν το 2011 με εναέριο χτύπημα για καθυστέρηση του πυρηνικού προγράμματος του.Το κόστος και τα οφέλη της επίθεσης αυτής δεν έμειναν ασχολίαστα. Δεν ήταν ξεκάθαρο πόσο κόστισε το πρόγραμμα Stuxnet, αλλά ήταν σίγουρα λιγότερο κόστος από ένα μόνο πολεμιστή-βομβιστή.

Τα στοιχεία βγήκαν στο φως από το Wikileaks από εμπιστευτικά τηλεγραφήματα Αμερικανών διπλωματών τον Δεκέμβριο του 2010,τα οποία δείχνουν ότι οι ΗΠΑ θα μπορούσαν να επιτρέψουν στο Ισραήλ να πετάξει πάνω από το Ιράκ.Όσοι κατατρόπωναν υπόγεια καταφύγια θα

μπορούσαν να εισχωρήσουν σε υπόγειες εγκαταστάσεις όπως την Νατάνζ. Παρόλο που οι περιορισμοί στον ανεφοδιασμό θα απέτρεπαν πιθανόν το Ισραήλ να χτυπήσει όλες τις πυρηνικές εγκαταστάσεις του Ιράν με ένα μόνο χτύπημα, τα αεροπλάνα του θα μπορούσαν να χτυπήσουν τα μέρη-κλειδιά τα οποία είναι μεγάλης σημασίας για την παραγωγή διασπάσιμου υλικού. Παρά τα καυχήματα, οι εναέριες άμυνες του Ιράν φαίνονται αμφισβητήσιμες.

Ο Γερμανός ειδικός Ralph Lagner παρουσιάζει το Stuxnet ως ένα στρατιωτικού βαθμού κυβερνοπύραυλο ο οποίος χρησιμοποιήθηκε για να εκτοξεύσει μια ολοκληρωτική κυβερνοαπεργία ενάντια στο πυρηνικό πρόγραμμα του Ιράν.[16]

6.8 GhostNet 2009

Τον Μάρτιο του 2009 ανακαλύφθηκε μία μεγάλης κλίμακας επιχείρηση κατασκοπείας από τους ερευνητές στο Information Warfare Monitor που ονομάστηκε GhostNet. Η υποδομή διοίκησης και ελέγχου αυτής της επιχείρησης βρίσκεται κυρίως στην Λαϊκή Δημοκρατία της Κίνας (ΛΔΚ) και έχει εισχωρήσει σε υψηλής σημασίας πολιτικές, οικονομικές και ΜΜΕ τοποθεσίες σε 103 χώρες. Αν και η δραστηριότητα έχει βάση κυρίως στην Κίνα, δεν υπάρχουν γερές αποδείξεις ότι η Κινέζικη κυβέρνηση εμπλέκεται στην επιχείρηση.Τα υπολογιστικά συστήματα που ανήκουν σε πρεσβείες, υπουργεία εξωτερικών και άλλα κυβερνητικά γραφεία, και τα θιβετιανά κέντρα εξορίας του Δαλάι Λάμα στην Ινδία, το Λονδίνο και την πόλη της Νέας Υόρκης διακινδύνευσαν από το GhostNet.

Τον Απριλίου στις 6 του 2010, το ίδρυμα Shadowserver και το Information Warfare Monitor εξέδωσαν μια κοινή αναφορά σχετικά με έρευνα στο κομμάτι της Κατασκοπείας στον Κυβερνοχώρο.Στην αναφορά τονίζεται το ολοένα και αυξανόμενο πρόβλημα που τίθεται από την αυξανόμενη ενσωμάτωση του εγκλήματος και της κατασκοπείας στον ιστό του παγκόσμιο κυβερνοχώρου. Η αναφορά κάνει έκκληση για ένα παγκόσμιο συνέδριο στον κυβερνοχώρο για τεθεί μια τάξη σε αυτό που αυξανόμενα μετατρέπεται σε έναν επικίνδυνα διαταραγμένο χώρο.[3]

6.9 Ιός Conficker 2009

Ένα ακόμα παράδειγμα είναι επίθεσης με Conficker 2009, μολυσματικός αλλά φαινομενικά μη καταστρεπτικός.Ο ιός αυτός είναι ένας ιός τύπου worm υπολογιστή που χτυπάει Microsoft Windows λειτουργικό σύστημα και εντοπίστηκε για πρώτη φορά το Νοέμβριο του 2008.Προκαλεί προβλήματα στο λογισμικό των Windows OS και επιθέσεις λεξικού για τους κωδικούς πρόσβασης διαχειριστή με σκοπό να τους διαδώσει.Ο ιός τύπου worm Conficker είχε προγραμματιστεί να ενεργοποιηθεί την 1η Απριλίου, και το αναπάντητο ερώτημα είναι: Θα αποδειχθεί παγκοσμίως μεγαλύτερο αστείο Πρωταπριλιά ή μήπως είναι η εποχή της πληροφορίας ισοδύναμο του θρυλικού 1962 πραγματεία Herman Kahn σχετικά με τον πυρηνικό πόλεμο, "Σκέψη για το αδιανόητο "[19].Εκτιμάται ότι 12 εκατομμύρια ή περισσότερα

μηχανήματα έχουν μολυνθεί. Ωστόσο, η ακριβής απογραφή είναι δύσκολο να αποκτηθούν αφού έχουν μολυνθεί και πολλοί άλλοι.

6.10CENTCOM

Η πρόσφατη παράβαση απόρρητων συστημάτων στο CENTCOM η οποία έγινε σε μεγάλη κλίμακα είχε ως αποτέλεσμα την απώλεια χιλιάδων απόρρητων εγγράφων. Η επίθεση αυτή έγινε με την παρέμβαση από ένα USB στικ μολυσμένο με έναν καλά καταγεγραμμένο ιό που χρησιμοποιήθηκε σκόπιμα από κάποιον σε έναν φορητό υπολογιστή ο οποίος είχε συνδεθεί με ένα απόρρητο δίκτυο.

6.11Κινέζοι Χάκερ(1998-2010)

Οι χάκερ αυτοί ήταν στραμμένοι κυρίως στο πατριωτικό χακάρισμα την λεγόμενη και πειρατεία,γνωστοί και ως συμμαχία των κόκκινων χάκερ (Red Hacker Alliance)[22] ή η ένωση Honker της Κίνας. Η συμμαχία αυτή προκήρυξε ένα έγγραφο στο οποίο ανέφεραν την πατριωτική τους αποστολή χρησιμοποιώντας δηλώσεις ο Mao Zedong.Οι κυβερνο-επιθέσεις τους συμπεριελάμβαναν τις ακόλουθες χώρες[20]:

- Την Ινδονησία του 1998 υπό την μεταχείριση των Κινέζων που ζούσαν στην Τζακάρτα
- Τις ΗΠΑ το 1999 μετά τον βομβαρδισμό της πρεσβείας στο Βελιγράδι και το 2001, έπειτα από τον θάνατο ενός κινέζου πιλότου μαχητικού F-8 του οποίου το αεροσκάφος συγκρούστηκε με ένα EP-3 αναγνωριστικό αεροσκάφος των ΗΠΑ.
- Την Ταιβάν το 1999 μετά την υπεράσπιση του Ταιβανέζου προέδρου Li Deng-Hui για μια «θεωρία δύο κρατών» και το 2000 σε συνδυασμό με τις εκλογές στην Ταιβάν
- Την Ιαπωνία το 2000 κατά την διαχείριση της σφαγής στο Nanjing κατά την διάρκεια του δευτέρου παγκοσμίου πολέμου και το 2004 σε σχέση με τα επίμαχα νησιά Diaoyu
- Το Ιράν το 2010 σε αντίποινα για την πειρατεία της Κινεζικής μηχανής αναζήτησης Baidu, από τον Ιρανικό στρατό κυβερνοχώρου.

6.12Επιθέσεις από μη κρατικές ομάδες(1995-1999)

- Το 1989 το WANK worm διείσδυσε στο δίκτυο της NASA με σκοπό να διαμαρτυρηθούν για τα πυρηνικά όπλα και την χρήση του ραδιενεργού πλουτωνίου από την NASA για να προμηθεύσει με καύσιμο το σύστημα ενίσχυσης του ανιχνευτή Galileo της NASA.

[22] Η Red Hacker Συμμαχίας (中国红客联盟) είναι μια άτυπη ομάδα Κινέζων χάκερς που σε ένα χρόνο είχε πάνω από 80.000 μέλη, καθιστώντας την μία από τις μεγαλύτερες ομάδες hacking στον κόσμο.

- Η διαδικτυακή απεργία διάρκειας μιας ώρας του Strano Network κατά των ιστοσελίδων της γαλλικής κυβέρνησης το 1995, ως διαμαρτυρία προς την πολιτική της γαλλικής κυβέρνησης σε πυρηνικά και κοινωνικά θέματα
- Οι διαδικτυακές καταλήψεις του Electronic Disturbance Theatre ενάντια ιστοσελίδων του Μεξικού, των Η.Π.Α. και οπουδήποτε αλλού αρχίζοντας το 1998 ως υποστήριξη των μεξικανών Zapatistas και αργότερα άλλων πολιτικών και κοινωνικών θεμάτων
- Οι βομβαρδισμοί email των διαδικτυακών Black Tigers ενάντια στις πρεσβείες της Σρι Λάνκα για να αντιμετωπιστεί η κυβερνητική ηλεκτρονική προπαγάνδα
- Διαδικτυακές παραμορφώσεις απο τους Team Spl0it και άλλους αντιπολεμικούς χάκερ οι οποίοι έκαναν έκκληση για λήξη των συγκρούσεων του Κοσόβου το 1999.[19]

7 *Συμπεράσματα*

Ο κυβερνοπόλεμος κάνει την εμφάνησή του καθημερινά στην εποχή μας,δηλαδή στην εποχή της πληροφορίας.Η ιστορία της πορείας του κυβερνοπολέμου μας έχει δείξει ότι με το πέρασμα του χρόνου οι επιθέσεις είναι όλο και πιο πολλές με τρομακτικά αποτελέσματαΟι περισσότερες από τις κυβερνοεπιθέσεις που γίνονται,είναι προϊόντα επιθέσεων δικτύων.Οι επιθέσεις αυτές,όπως για παράδειγμα επιθέσεις στα δίκτυα κρατικών φορέων και οργανισμών, παρ'όλο που έχουν σχετικά μικρές υλικές ζημιές , το κόστος των ζημιών που προκαλούν είναι αρκετά μεγάλο.Τα παραδείγματα των επιθέσεων στην Εσθονία και στη Γεωργία είναι δύο επιθέσεις που πρέπει να μας προβληματίζουν καθώς και πολλούς ανθρώπους του κυβερνοχώρου,όπως τον Jaak Aaviksoo, Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul και τον Jon Bumgarner.

Τα κριτήρια του μοντέλου του κυβερνοπολέμου και τα άρθρα του καταστατικού χάρτη του ΟΗΕ αναφορικά με την αυτοάμυνα και την χρήση βίας ,λόγω του ότι είναι γραμμένα σε μία εποχή όπου το επίπεδο των επιθέσεων με βάση την τεχνολογία ,δεν βρίσκουν την τέλεια εφαρμογή στις επιθέσεις του σήμερα,αν και την καλύπτουν.Αυτό συμβαίνει γιατί τα κριτήρια και τα άρθρα αυτά έχουν γραφτεί για γενικές περιπτώσεις έτσι ώστε να έχουν μεγάλη προσαρμοστικότητα και στις επιθέσεις που γίνονται τώρα και που θα γίνουν και στο μέλλον.Ένα κράτος-θύμα μπορεί να χρησιμοποιήσει το δικαίωμα της αυτοάμυνας ή το δικαίωμα της αντεπίθεσης αρκεί να καλύπτει τις αντίστοιχες νομικές προϋποθέσεις του Διεθνούς Δικαίου,για να προβεί σε τέτοιες ενέργειες καθώς και της Θεωρίας του Δίκαιου Πολέμου.

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 εξελίσσοται 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.Η ανωνυμία των επιθέσεων είναι από τα σημαντικότερα θέματα που έχουν υποθεί αλλά δεν μπορούν λυθούν.Όπως

προαναφέραμε και στην εργασία το ζήτημα της ανωνυμίας δεν μπορει να εξαλυφθεί.Είναι το «δίκοπο μαχαίρι» του πολέμου αυτού.

8 *Βιβλιογραφία*

[1] Dipert, Randall, «The Ethics Of Cyberwarfare: Journal Of Military Ethics: Vol 9, No 4», Journal of Militar Ethics, 2016

[2] David P. Duggan, Raymond C. Parks, "Principles of Cyberwarfare", IEEE Security & Privacy, vol. 9, no. , pp. 30-35, September/October 2011

[3] Reich, Pauline et al. "Cyber Warfare: A Review Of Theories, Law, Policies, Actual Incidents – And The Dilemma Of Anonymity", European Journal of Law and Technology 1.2 , 2010

[4] Βασίλειος Γ. Μακρής, Στρατιωτικός Δικαστής Β', Πτυχιακή Εργασία για το Α' Επίπεδο του Προγράμματος Μεταπτυχιακών Σπουδών του Τμήματος Νομικής του Τομέα Διεθνών Σπουδών του (Δημοκρίτειου Πανεπιστημίου Θράκης, Ακαδημαϊκά Έτη 2008 – 2009 & 2009 – 2010.), 'Η επίθεση σε δίκτυα ηλεκτρονικών υπολογιστών (computer network attack) και η χρήση βίας κατά το διεθνές δίκαιο. (Η επίθεση σε δίκτυα η/υ με τη χρησιοποίηση των η/υ και δικτύων ως όπλων.)', Νοέμβριος 2011

http://www.militaryjustice.gr/athra/epithesi_diktia_yh.pdf

[5] Αντώνιος Μπρούμας, 'Ανωνυμία στο Διαδίκτυο : Δικαίωμα ή Κατάχρηση;',2013

https://athens.indymedia.org/post/1472405/

[6] Nassr Eddin, 'Ανωνυμία στο Διαδίκτυο', 2013

http://ancap.gr/anonimia-sto-diadiktio/

[7] Δελημάτσης Κωντσταντίνος, 'Το διεθνές δίκαιο και η χρήση της ένοπλης δύναμης/ βίας',2013

https://curia.gr/to-diethnes-dikaio-kai-i-xrisi-tis-enoplis-dinamis-vias/

[8] http://www.unric.org/el/index.php?option=com_content&view=article&id=14

[9] Dunlap, Charles, "The Hyper-Personalization Of War" Scholarship.law.duke.edu.

[10] Dan Fayutkin , "The American and Russian Approaches to Cyber Challenges", 2012

[11] Αντώνιος Χαλακατεβάκης, Σπουδαστής 1ης ΔιΜα ΣΕΘΑ, 'Διεθνείς και Ελληνικές Διαστάσεις της Κυβερνοασφάλειας', 2011

[12] https://kelley.iu.edu

[13] Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis, Theodore Apostolopoulos, "A CYBER ATTACK EVALUATION METHODOLOGY", University of Economics and Business, Athens, Greece , University of the Aegean, Samos, Greece

[14]http://ec.europa.eu/transparency/regexpert/index.cfm?do=faq.faq&aide=2&Lang=EL

[15]Ασφάλεια Πληροφοριακών Συστημάτων, Σ. Κάτσικα, Δ. Γκρίτζαλη, Σ. Γκρίτζαλη(Επισ.Επιμέλεια), κδόσεις Νέων Τεχνολογιών, 2004

[16] Farwell, James and Rafal Rohozinski. "Stuxnet And The Future Of Cyber War: Survival: Vol 53, No 1". Survival , 2011

[17]http://www.meta-data.gr/net_security.shtml

[18]TVXS , ’ Η έναρξη των ΝΑΤΟϊκών βομβαρδισμών στη Σερβία’ , 24 Μαρ. 2014

http://tvxs.gr/

[19]JohnMarkoff ‘ The Conficker Worm: April Fool’s Joke or Unthinkable Disaster?’, 2009 *http://bits.blogs.nytimes.com/2009/03/19/the-conficker-worm-april-fools-joke-or-unthinkable-disaster/?_r=0*

[20] Berson, Thomas and Dorothy Denning, "Cyberwarfare", Ieeexplore.ieee.org. N.p., 2011