



PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES ΣΧΟΛΗ ΠΟΛΙΤΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ : ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ
ΣΠΟΥΔΕΣ

«Κυβερνοεπιθέσεις & βασικές μορφές αυτών, ως ασύμμετρη απειλή για
την ασφάλεια των κρατών & την πολιτική τους σταθερότητα &
προοπτικές ανάπτυξης σχετικής νομοθεσίας και «Εγχειρίδιο του Τάλλιν».

« Cyberattacks & Key forms of these, as asymmetric threat to the
security of States & their political stability & Prospects for the
development of relevant legislation and “Handbook of Tallinn”»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Χριστίνα Κοτεκίδου

Φοιτήτρια ΠΜΣ ΔΣΣΣ

ΑΜ:2223Μ020

Αθήνα, 17 Δεκεμβρίου 2024

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Καθηγητής Χαράλαμπος Παπασωτηρίου

Επίκουρος Καθηγητής Κωνσταντίνος Τσιμώνης

Αναπληρωτής Καθηγητής Ανδρέας Λιαρόπουλος



Copyright © Χριστίνα Κοτεκίδου, 2024 All rights reserved.

Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Η έγκριση της διπλωματικής εργασίας από το Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

Στα παιδιά μου , Ιωάννη Δημοσθένη και Σωτηρία Άννα,

Περίληψη

Με τη συνεχή εξάπλωση της επιρροής του διαδικτύου και των δυνατοτήτων του ακόμα και σε κρίσιμους τομείς για τη λειτουργία ενός κράτους παρατηρείται παράλληλα η ανάδειξη του φαινομένου της εξάπλωσης των κυβερνοεπιθέσεων εναντίων τόσο ιδιωτικών όσο και κρατικών θεσμών. Οι κυβερνοεπιθέσεις σήμερα αποτελούν ένα πολυδιάστατο φαινόμενο που δυνητικά μπορεί να θέσει σε άμεσο κίνδυνο τη πολιτική σταθερότητα και την εθνική ασφάλεια κρατών καθώς μπορούν να θέσουν στο στόχαστρό τους λειτουργίες και υποδομές απαραίτητες και κρίσιμες για την εύρυθμη λειτουργία ενός κράτους ενώ παράλληλα μπορούν και να στοχοποιήσουν συγκεκριμένες ομάδες του πληθυσμού με σκοπό είτε την χειραγώγηση αυτών είτε την τρομοκράτησή τους. Επιπρόσθετα οι κυβερνοεπιθέσεις αποτελούν ένα καινούριο φαινόμενο γεγονός που εγείρει ζητήματα σχετικά με τη νομοθεσία αυτών και το ρόλο που διαδραματίζουν οι διάφοροι θεσμοί στην αποτροπή τους.

Στόχος της παρούσας εργασίας αποτελεί η εξέταση του φαινομένου των κυβερνοεπιθέσεων. Αρχικά επιχειρείται ο διαχωρισμός των μορφών που αυτές λαμβάνουν και ακολούθως εξετάζεται το ιστορικό τους πλαίσιο, διάφοροι διαδικαστικοί παράγοντες καθώς και τα κίνητρα και οι επιπτώσεις που επιφέρουν. Εξετάζεται επίσης η νομική αντιμετώπιση του φαινομένου και ο ρόλος διαφόρων θεσμών.

Abstract

With the continuous spread of the influence of the internet and its potential even in critical areas for the functioning of a state, the phenomenon of the spread of cyber-attacks against both private and state institutions is emerging. Cyber-attacks today constitute a multidimensional phenomenon that can potentially pose a direct threat to the political stability and national security of states as they can target functions and infrastructure necessary and critical for the proper functioning of a state, while at the same time they can target specific groups of the population to either manipulate or terrorize them. In addition, cyber-attacks are a new phenomenon which raises questions about their legislation and the role of the various institutions in preventing them.

The purpose of this thesis is to examine the phenomenon of cyber-attacks. It begins by attempting to distinguish the forms they take and then examines their historical context, various procedural factors and the motivations and consequences they bring about. The legal response to the phenomenon and the role of various institutions are also examined.

Περιεχόμενα

Κεφάλαιο 1: Ορισμοί	9
1.1 Κυβερνοεπίθεση:	9
1.2 Κυβερνοχώρος:	9
1.3 Κυβερνοασφάλεια:	9
1.4 Cyber Strategy:	9
1.5 Cyber Diplomacy:	9
Κεφάλαιο 2: Τύποι κυβερνοεπιθέσεων	10
2.1 Denial-of-Service (DoS)/Distributed denial-of-service (DDoS):	10
2.2 Man-in-the-middle (MitM):	10
2.3 Phishing:	10
2.4 Drive-by-download attack:	10
2.5 Password Attack:	10
2.6 SQL Injection Attack:	10
2.7 Cross-site scripting (XSS) attack:	11
2.8 Eavesdropping attack:	11
2.9 Birthday attack:	11
2.10 Malware attack:	11
Κεφάλαιο 3: Διαχωρισμός σε νομική βάση	12
3.1 Κυβερνοέγκλημα:	12
3.2 Κυβερνοκατασκοπεία:	12
3.3 Κυβερνοτρομοκρατία:	12
3.4 Κυβερνοπόλεμος:	12
Κεφάλαιο 4: Οργανωτικά Ζητήματα	13
4.1 Συντονισμός	13
4.2 Συγχρονισμός	13
4.3 Διατάραξη συστήματος:	13
4.4 Στάδια	13
4.5 Ο ρόλος της Γεωγραφίας:	13
4.6 Κυβερνοόπλα	14
4.7 Αντίμετρα	14
4.8 Αμυντικές τεχνικές	15

4.8.1 Κρυπτογράφηση:	15
4.8.2 CTI:	15
4.8.3 Άμεση αντίδραση:	15
4.8.4 Τμηματοποίηση:	15
Κεφάλαιο 5: Κρατικές κυβερνοεπιθέσεις	16
Κεφάλαιο 6: Κυβερνοεπιθέσεις και ειρήνη	16
Κεφάλαιο 7: Δρώντες.....	16
7.1 Δράστες:	16
7.2 Θύματα:.....	18
Κεφάλαιο 8: Ο ρόλος του στρατού	18
Κεφάλαιο 9: Ο ρόλος των κυβερνήσεων	19
Κεφάλαιο 10: Ο ρόλος της Διπλωματίας	20
Κεφάλαιο 11: Ιστορικό των Κυβερνοεπιθέσεων – Κύρια γεγονότα.....	20
11.1 ΕΣΣΔ 1982:.....	20
11.2 Ιράκ 2003:.....	20
11.3 Ηνωμένο Βασίλειο 2007:	20
11.4 Εσθονία 2007:	21
11.5 Γεωργία 2008:	21
11.6 Stuxnet Worm 2010:	22
11.7 Συρία 2013:	22
Κεφάλαιο 12: Πολιτικές επιθέσεις	22
Κεφάλαιο 13: Κοινωνικό-πολιτισμικές επιθέσεις.....	24
Κεφάλαιο 14: Στρατηγική Κυβερνοπολέμου και οι πέντε πυλώνες κοινωνικής σταθερότητας	24
Κεφάλαιο 15: Κυβερνοεπιθέσεις και Εθνική Ασφάλεια	26
Κεφάλαιο 16: Στόχοι-Επιπτώσεις	26
16.1 Παρακώλυση πληροφοριών:	26
16.2 Αντιμετώπιση των μέτρων ασφαλείας:	27
16.3 Επιβράδυνση της διαδικασίας λήψης αποφάσεων:.....	27
16.4 Αδυναμία παροχής δημόσιων υπηρεσιών:	27
16.5 Μείωση της εμπιστοσύνης:	27
16.6 Μείωση του γοήτρου:	27
16.7 Κατασκοπεία:	27
16.8 Αντικατασκοπεία:	28

16.9 Προπαγάνδα:	28
16.10 Μονάδες Υγείας:	28
16.11 Εφοδιαστική Αλυσίδα:	28
16.12 Δίκτυα Επικοινωνίας:	29
16.13 Δίκτυο Ηλεκτροδότησης:	29
16.14 Επιχειρήσεις και Οικονομία:	29
16.15 Χρηματοπιστωτικό σύστημα:.....	30
16.16 Ευαίσθητα δεδομένα:	31
16.17 Πολιτικά κίνητρα:	31
16.18 Ψυχολογικές επιπτώσεις:.....	31
16.19 Social Media και πολιτική αναταραχή:	32
Κεφάλαιο 17: Καθεστώς και Κυβερνοεπιθέσεις – Η περίπτωση της Ρωσίας.....	33
Κεφάλαιο 18: Νομικό υπόβαθρο	36
18.1 Η Ηθική Διάσταση	36
18.2 Διεθνείς Συμφωνίες	37
18.2.1 ΗΠΑ-Ρωσία:	37
18.2.2 ΗΠΑ-Κίνα:	38
18.2.3 Ρωσία-Κίνα:	38
18.3 Διεθνείς Πρωτοβουλίες.....	38
18.3.1 Πρωτοβουλίες Ηνωμένων Εθνών:.....	38
18.3.2 Πρωτοβουλίες σε περιφερειακό επίπεδο:	38
18.3.3 Πρωτοβουλίες μη κυβερνητικών δρώντων:	39
18.3.4 NATO-ΕΕ:.....	39
18.4 Μέτρα Οικοδόμησης Εμπιστοσύνης (CBMs)	39
18.4.1 Organization for Security and Co-operation in Europe (OSCE):	39
18.4.2 The Association of Southeast Asian Nations (ASEAN):	40
18.4.3 The Organization of American States (OAS):	40
18.5 Προβλήματα στη νομοθεσία των κυβερνοεπιθέσεων	40
18.5.1 Αρχή της διάκρισης:	40
18.5.2 Απαγόρευση της εξαπάτησης (άρθρο 37):.....	41
18.5.3 Ουδετερότητα:	41
18.5.4 Διαπίστωση της προέλευσης μίας επίθεσης:	41
18.5.5 Δυσκολία διαπίστωσης των θυμάτων:.....	42

18.5.6 Χρήση Βίας:	42
18.5.7 Ευθύνη και απόδοση:.....	42
18.5.8 Άμεση συμμετοχή:.....	43
18.6 Διεθνές Δικαστήριο	43
Κεφάλαιο 19: Εγχειρίδιο του Ταλίν	44
19.1 Ιστορία του Εγχειριδίου	44
19.2 Κύριες έννοιες	45
19.2.1 Κυριαρχία	45
19.2.2 Κρατική Δικαιοδοσία	45
19.2.3 Χρήση Βίας.....	45
19.2.4 Κανόνας 110	45
Κεφάλαιο 20: Το μέλλον της Νομοθεσίας	46

Κεφάλαιο 1: Ορισμοί

1.1 Κυβερνοεπίθεση:

Είναι μια στρατηγική διείσδυσης από μη εξουσιοδοτημένο άτομο ή ομάδες στη βάση δεδομένων ενός κράτους, οργανισμού ή ατόμου. Μια κυβερνοεπίθεση θα μπορούσε να έχει πολιτικά ή οικονομικά κίνητρα. Η Kaspersky (2020) κατηγοριοποίησε την κυβερνοεπίθεση ως απειλή στον κυβερνοχώρο και περαιτέρω υποστηρίζει ότι είναι πολιτικά συλλογή πληροφοριών με κίνητρα. Ο Merriam-Webster (2020) το ορίζει ως προσπάθεια απόκτησης παράνομης πρόσβασης σε υπολογιστή ή σύστημα υπολογιστή για να προκληθούν ζημιές (Quadri, Rasaq, 2020).

1.2 Κυβερνοχώρος:

Το παγκόσμιο πεδίο εντός του περιβάλλοντος πληροφοριών που αποτελείται από αλληλένδετα δίκτυα υποδομών τεχνολογίας της πληροφορίας και αποθηκευμένα δεδομένα, συμπεριλαμβανομένου του Διαδικτύου, τηλεπικοινωνιακών δικτύων, συστημάτων υπολογιστών και ενσωματωμένων επεξεργαστών και ελεγκτών (Θεοφίλης 2018).

1.3 Κυβερνοασφάλεια:

Καλείται η διαδικασία προστασίας συστημάτων, υπολογιστών, δικτύων προγραμμάτων, προσωπικών δεδομένων από μη εγκεκριμένη πρόσβαση, επιθέσεις και απειλές. Στη διαδικασία αυτή πληροφορίες και συστήματα επικοινωνίας προστατεύονται από την μη εγκεκριμένη χρήση, τροποποίηση ή την εκμετάλλευση της συσκευής. Η κυβερνοασφάλεια καλείται και τεχνολογία προστασίας πληροφοριών και περιλαμβάνει τεχνικές προστασίας συσκευών, δικτύων προγραμμάτων και δεδομένων από ζημιές και κάθε είδους εκμετάλλευση που σχετίζεται με παραβίαση.(Oruj)

1.4 Cyber Strategy:

Αποτελεί μία εθνική πολιτική η οποία διαφέρει από κράτος σε κράτος και στόχος της είναι η αντιμετώπιση απειλών όπως οι κυβερνοεπιθέσεις, το κυβερνοέγκλημα και η κατασκοπεία. Κάθε χώρα διαθέτει τη δικιά της στρατηγική με την οποία αποτρέπει την είσοδο χάκερ στις βάσεις πληροφοριών της (Quadri, Rasaq, 2020).

1.5 Cyber Diplomacy:

Η χρήση του διαδικτύου και των ψηφιακών τεχνολογιών για διπλωματικούς σκοπούς (Bhattacharya 2022).

Κεφάλαιο 2: Τύποι κυβερνοεπιθέσεων

2.1 Denial-of-Service (DoS)/Distributed denial-of-service (DDoS):

Σε αυτό τον τύπο επίθεσης οι πόροι του συστήματος κατακλύζονται από το κακόβουλο λογισμικό έτσι ώστε να μην μπορεί να ανταποκριθεί σε αιτήματα υπηρεσίας. Κοινοί τύποι τέτοιων επιθέσεων είναι: TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack και botnets (Biju, Gopal, Prkash 2019). Αυτό μπορεί να διαταράξει κρίσιμες υπηρεσίες, την επικοινωνία και τη διάδοση πληροφοριών. Οι επιθέσεις DDoS μπορούν να εμποδίσουν κυβερνητικούς ιστότοπους, συστήματα επικοινωνίας έκτακτης ανάγκης και βασικές διαδικτυακές υπηρεσίες, που επηρεάζουν την πρόσβαση του κοινού σε πληροφορίες και την αντιμετώπιση έκτακτων περιστατικών (Digmelashvili 2023).

2.2 Man-in-the-middle (MitM):

Αυτός ο τύπος επίθεσης λαμβάνει χώρα όταν κάποιος τρίτος παρεμβάλλεται μεταξύ πελάτη και διακομιστή και ο οποίος παριστάνει ταυτόχρονα και τους δύο. Αυτού του τύπου οι επιθέσεις καταχρώνται σε πραγματικό χρόνο επικοινωνίες, συναλλαγές ή την ανταλλαγή πληροφοριών. Επιθέσεις αυτού του είδους αποτελούν οι session hijacking, IP spoofing και reply (Biju, Gopal, Prkash 2019) .

2.3 Phishing:

Αυτές οι επιθέσεις εκδηλώνονται με την αποστολή απατηλών e-mail τα οποία προέρχονται φαινομενικά να προέρχονται από έμπιστες πηγές. Τα e-mail αυτά έχουν ενσωματωμένους υπερσυνδέσμους που περιέχουν κακόβουλα λογισμικά που εν συνεχεία εγκαθίστανται στο σύστημα του υπολογιστή. Εναλλακτικά οι υπερσύνδεσμοι οδηγούν σε κάποια ιστοσελίδα από την οποία εγκαθίσταται το λογισμικό ή υποκλέπτονται μέσω αυτής προσωπικά δεδομένα. Τεχνικές που χρησιμοποιεί η μορφή του phishing είναι τα whaling, spear phishing, pharming και το deceptive (Biju, Gopal, Prkash 2019).

2.4 Drive-by-download attack:

Ένας τύπος επίθεσης με στόχο τη διάδοση κακόβουλου λογισμικού και τη παροχή πρόσβασης στο σύστημα. Η επίθεση αυτή πραγματώνεται με την εισαγωγή κακόβουλου περιεχομένου σε ιστοσελίδες το οποίο είναι δυσδιάκριτο από τους επισκέπτες. Στόχος του λογισμικού αυτού είναι να βρει αδυναμίες ασφάλειας στο σύστημα και στις εφαρμογές του (Biju, Gopal, Prkash 2019).

2.5 Password Attack:

Σε αυτή τη περίπτωση η οι κωδικοί ενός χρήστη υποκλέπτονται ή αποκωδικοποιούνται με διάφορους τρόπους, κυριότεροι εξ αυτών το sniffing της σύνδεσης στο διαδίκτυο και οι επιθέσεις λεξικού (Biju, Gopal, Prkash 2019).

2.6 SQL Injection Attack:

Η Structured Query Language (SQL) αποτελεί μία υπολογιστική γλώσσα η οποία χρησιμοποιείται για την αποθήκευση το χειρισμό και την ανάκτηση δεδομένων που

βρίσκονται σε μία βάση δεδομένων. Η γλώσσα αυτή χρησιμοποιεί απλές εντολές όπως select, delete, update. Η SQL δύναται να εκτελέσει ερωτήματα και εισάγει νέα δεδομένα στη βάση. Η επίθεση χρησιμοποιείται για τη πρόσβαση σε πληροφορίες μίας βάσης δεδομένων όπως για παράδειγμα δεδομένα πελατών και προσωπικά δεδομένα (Biju, Gopal, Prkash 2019).

2.7 Cross-site scripting (XSS) attack:

Οι επιθέσεις XSS χρησιμοποιούν πόρους ιστού τρίτων για την εκτέλεση σεναρίων στο πρόγραμμα περιήγησης ιστού του θύματος ή σε εφαρμογή με δυνατότητα δέσμης ενεργειών. Συγκεκριμένα, ο εισβολέας εισάγει ωφέλιμο φορτίο με κακόβουλη JavaScript στη βάση δεδομένων ενός ιστότοπου. Όταν το θύμα ζητά μια σελίδα από τον ιστότοπο, ο ιστότοπος μεταδίδει τη σελίδα, με το ωφέλιμο φορτίο του εισβολέα ως μέρος του σώματος HTML στο πρόγραμμα περιήγησης του θύματος, το οποίο εκτελεί το κακόβουλο σενάριο (Biju, Gopal, Prkash 2019).

2.8 Eavesdropping attack:

Μία επίθεση που είναι πολύ δύσκολο να εντοπιστεί καθώς κατά τη διάρκεια της επίθεσης δεν παρατηρείται κάποια παράξενη λειτουργία. Με αυτή την επίθεση μπορούν να υποκλαπούν δεδομένα όπως ο αριθμός πιστωτικής κάρτας, το password και λοιπές ευαίσθητες πληροφορίες. Η υποκλοπή αυτή επιτυγχάνεται κατά τη διάρκεια της μετάδοσης των δεδομένων και χωρίζεται σε δύο κατηγορίες: active και passive. Στη μεν πρώτη κατηγορία ο επιτιθέμενος προσποιείται κάποιον έμπιστο πομπό ενώ στη δε δεύτερη επιτυγχάνεται η ακρόαση του μηνύματος κατά τη μετάδοσή του στο δίκτυο (Biju, Gopal, Prkash 2019).

2.9 Birthday attack:

Αποτελεί ένα είδος κρυπτογραφικής επίθεσης και συγκαταλέγεται στη κατηγορία των επιθέσεων brute force και βασίζεται στο παράδοξο των γενεθλίων. Για την επίθεση χρησιμοποιούνται συναρτήσεις κατακερματισμού με τις οποίες ελέγχονται η ακεραιότητα μηνυμάτων, προγράμματα και ψηφιακές υπογραφές (Biju, Gopal, Prkash 2019).

2.10 Malware attack:

Η εγκατάσταση κακόβουλου λογισμικού γίνεται χωρίς την έγκριση του χρήστη και είναι γνωστή ως ιός, spyware, ransomware κ.α.. Τα λογισμικά αυτά διαδίδονται και εκτελούνται από μόνα τους αφότου προσκολληθεί σε ένα νόμιμο κώδικα και μπορούν να διαπεράσουν ακόμα και ιδιωτικά δίκτυα υποκλέπτοντας ευαίσθητες πληροφορίες και δεδομένα επιχειρηματικής και οικονομικής φύσης. Οι βασικότεροι τύποι είναι I) Virus: ένα λογισμικό που προσκολλάται σε κάποιο πρόγραμμα και δύναται να αναπαράγει και να τροποποιεί κώδικες όταν εκτελείται. II) Worms: διαδίδονται σε υπολογιστές και δίκτυα μέσα από e-mail. III) Trojans: ένα εξαιρετικά επικίνδυνο κακόβουλο λογισμικό που κρύβεται μέσα σε κάποιο άλλο πρόγραμμα και δεν αναπαράγεται. IV) Ransomware: το λογισμικό αυτό κλειδώνει τα δεδομένα του χρήστη και απαιτεί πληρωμή για την αποκατάστασή τους. παρά τον απλό του κώδικα

είναι δύσκολο να αποτραπεί αυτή η επίθεση. V) Spyware: ένα λογισμικό που κατασκοπεύει τη δραστηριότητα του χρήστη και την αναφέρει στον επιτιθέμενο.

Κεφάλαιο 3: Διαχωρισμός σε νομική βάση

3.1 Κυβερνοέγκλημα:

Μία εγκληματική δράση που περιλαμβάνει έναν ηλεκτρονικό υπολογιστή που αποτελεί το όργανο του εγκλήματος ή το όργανο που διαπράττει ένα ουσιώδες κομμάτι της παράβασης. Στόχος του κυβερνοεγκλήματος είναι να καταστήσει ένα σύστημα σαν όργανο του εγκλήματος. Αυτού του τύπου τα εγκλήματα συμβαίνουν κυρίως λόγω της ανωνυμίας, της αδυναμίας του λειτουργικού συστήματος ή την έλλειψη γνώσης του χρήστη (Uma, Padmavathi 2013). Η ειδοποιός διαφορά ανάμεσα στο κυβερνοέγκλημα και τις κυβερνοεπιθέσεις έγκειται στο σκοπό του δράστη και όχι στη φύση αυτού. Οι κυβερνοεπιθέσεις αποτελούν επιχειρήσεις που αφορούν τη δημόσια σφαίρα και στοχεύουν τα εθνικά συμφέροντα ακόμα και όταν εμπλέκουν ιδιώτες ή επιχειρήσεις (Hemen Faga 2017).

3.2 Κυβερνοκατασκοπεία:

Η χρήση τεχνικών hacking, κακόβουλων λογισμικών και λογισμικών παρακολούθησης, αποτελούν πρακτικές με τις οποίες αποκτώνται πληροφορίες που αφορούν ιδιώτες, ομάδες και κυβερνήσεις με σκοπό τον προσπορισμό οφέλους μέσα από τη χρήση παράνομων μεθόδων. Η κατασκοπεία αυτού του τύπου μπορεί να διαπραχθεί από επαγγελματίες χάκερ που δρουν από απομακρυσμένες τοποθεσίες, κατασκόπους που έχουν ειδικευθεί στη κατασκοπεία μέσω Η/Υ ή απλά μπορεί να είναι έργο ερασιτεχνών χάκερ και προγραμματιστών (Uma-Padmavathi 2013).

3.3 Κυβερνοτρομοκρατία:

Η χρήση του δικτύου για τη διεξαγωγή τρομοκρατικών δραστηριοτήτων όπως η εσκεμμένη διακοπή δικτύων με τη χρήση εργαλείων όπως οι ιοί υπολογιστή (Uma, Padmavathi 2013).

3.4 Κυβερνοπόλεμος:

Η στρατιωτική δραστηριότητα που κυρίως χρησιμοποιεί υπολογιστικά συστήματα και δίκτυα με στόχο να επιτεθεί σε αυτά του αντιπάλου. Κύριος στόχος της επίθεσης η αποστέρηση της χρήσης των συστημάτων αυτών από τον αντίπαλο ή η πρόσβαση σε λειτουργίες που διευθύνουν δομές του εχθρού. Τα συστήματα που πλήττονται μπορεί να είναι κινητά τηλέφωνα, προσωπικοί Υ/Η, στρατιωτικά συστήματα ελέγχου και συστήματα ελέγχου υποδομών (Woltag 2015).

Κεφάλαιο 4: Οργανωτικά Ζητήματα

4.1 Συντονισμός

1. Μη οργανωμένες/ασυντονιστές: δεν αποτελούν ανόργανες επιθέσεις αλλά αντίθετα επιθέσεις αυτό οργανωμένες. Οι επιθέσεις αυτές θίγουν ευαίσθητα ζητήματα όπως ο εθνικισμός, ο πατριωτισμός κ.α. και συνδέονται μέσα από εργαλεία όπως chat, forums και blogs. (Gandhi, Sousan, Laplante 2011)
2. Οργανωμένες/συντονισμένες: αυτές περιλαμβάνουν κρυφές δραστηριότητες υψηλού συντονισμού μεταξύ μίας ομάδας ατόμων όπως είναι εγκληματικά συνδικάτα ή ομάδες στρατολογημένες από κάποιο στρατό ή κυβέρνηση. (Gandhi-Sousan-Laplante 2011)

4.2 Συγχρονισμός

Οι επιθέσεις που χρησιμοποιούνται για διαμαρτυρία εξαπολύονται άμεσα, ακολουθώντας κάποιο γεγονός που έχει επισυμβεί στον πραγματικό κόσμο. Αντίθετα άλλες επιθέσεις λαμβάνουν χώρα πριν ή ταυτόχρονα με μία στρατιωτική επέμβαση σε κάποια περιοχή. Χαρακτηριστικό παράδειγμα η ρωσική επίθεση στη Γεωργία. Παράλληλα οι κυβερνοεπιθέσεις μπορεί να αποτελούν προϊόν εκδίκησης και λαμβάνουν χώρα σε συγκεκριμένες χρονικές στιγμές. Τέλος εικάζεται πως υπάρχουν κακόβουλα προγράμματα εμφωλευμένα σε συστήματα διαχείρισης υποδομών που είναι έτοιμα να ενεργοποιηθούν σε περίπτωση κρίσης συνδυαστικά με κάποια στρατιωτική επιχείρηση. (Gandhi, Sousan, Laplante 2011)

4.3 Διατάραξη συστήματος

Οι δύο κύριες οδοί με τις οποίες διαταράσσεται ένα υπολογιστικό σύστημα είναι οι συντακτικές (syntactic) και σημασιολογικές (semantic) μέθοδοι. Οι πρώτες αφορούν τη χρήση ιών, σκουληκιών, Trojan κ.α. με σκοπό τη διατάραξη του λειτουργικού συστήματος οδηγώντας στη δυσλειτουργία του συστήματος ή του δικτύου. Οι δεύτερη κατηγορία αφορά στοχεύει την γλώσσα προγραμματισμού, επηρεάζοντας έτσι την ορθότητα των πληροφοριών (Hemen Faga 2017)

4.4 Στάδια

Τα στάδια μίας τυπικής κυβερνοεπίθεσης είναι τα εξής: I) Έρευνα με σκοπό τον καθορισμό των πιθανών απειλών για τον στόχο της επίθεσης II) Παράδοση: παρακολούθηση κάποιου παράγοντα ενός μηχανήματος του οποίου κάποια ευπάθεια μπορεί να είναι εκμεταλλεύσιμη III) Παραβίαση των τρωτών σημείων και απόκτηση μη εγκεκριμένης εισόδου στο σύστημα IV) Διεξαγωγή διεργασιών μέσα από τη μηχανή με σκοπό την επίτευξη των στόχων του εισβολέα (Biju, Gopal, Prakash 2019).

4.5 Ο ρόλος της Γεωγραφίας

Παρά την υπόθεση πως η γεωγραφία δεν διαδραματίζει κάποιον σημαίνοντα ρόλο, οι εμπειρικές αποδείξεις που έχουμε οδηγούν στο συμπέρασμα πως διαδραματίζει ακόμα σημαντικό ρόλο. Για να κατανοηθεί αυτό θα πρέπει να αναφερθεί πως ο

κυβερνοχώρος υπάρχει σε τρία επίπεδα, το φυσικό, το λογικό και το γεωγραφικό εκ των οποίων μόνο το δεύτερο (που αφορά τον τρόπο με τον οποίο πέμπονται τα ηλεκτρονικά σήματα που μεταφέρουν κώδικες) είναι πέραν των φυσικών ορίων. Παράλληλα ενώ οι δυνατότητες κυβερνοπολέμου δύνανται να ξεπερνούν τα συμβατικά όρια των συγκρούσεων, εντούτοις οι αποφάσεις και οι πρακτικές του δεν είναι απολύτως ασύνδετες με τη γεωγραφία. Για παράδειγμα η απειλή κυβερνοεπίθεσης θα έπρεπε να είναι χαμηλή για τη Γεωργία της οποίας το 7% του πληθυσμού χρησιμοποιεί το διαδίκτυο, αν όπως εξετάσουμε πως οι περισσότερες γραμμές internet και οι πάροχοι δικτύου της χώρας προέρχονταν από τη Ρωσία γίνεται αντιληπτή η σημαντικότητα της γεωγραφίας (Green 2015).

4.6 Κυβερνοόπλα

Ως όπλα ορίζονται συσκευές που είναι σχεδιασμένες να σκοτώνουν, τραυματίζουν ή προκαλούν αναπηρία ή να προκαλούν ζημιές ή ολική καταστροφή. Ο ορισμός αυτός βέβαια δεν μπορεί να περιγράψει ορθά τα όπλα του κυβερνοχώρου καθώς αυτά συνήθως χρησιμοποιούνται έτσι ώστε να επιτύχουν έμμεσα αποτελέσματα και όχι να προκαλέσουν ανθρώπινες απώλειες (Robinson, Jones, Janicke 2015). Χώρες τεχνολογικά προηγμένες διαθέτουν κυβερνοόπλα όπως το EC-130H Compass Call των ΗΠΑ που είναι ένα αερομεταφερόμενο οπλικό σύστημα σε στρατιωτικό αεροσκάφος. Οι δυνατότητες του συστήματος αυτού περιλαμβάνουν τη διακοπή των επικοινωνιών διοίκησης και ελέγχου του εχθρού και τον περιορισμό του συντονισμού των δυνάμεων του αντιπάλου (Οικονόμου 2021). Το Δεκέμβριο του 2013 τα μέλη της συμφωνίας Wassenaar (για την εξαγωγή συμβατικών όπλων), έφτασαν σε συμφωνία για περιορισμούς των εξαγωγών συστημάτων επιτήρησης δικτύων IP και λογισμικών εισβολής, που χρησιμοποιούνται από ιδιώτες και κυβερνήσεις με στόχο τη διεξαγωγή επιθέσεων. Τον Ιούλιο του 2015 το γραφείο βιομηχανίας και ασφάλειας των ΗΠΑ προσπάθησε ανεπιτυχώς να εφαρμόσει τη συμφωνία καθώς η βιομηχανία προϊόντων κυβερνοασφάλειας αντέδρασε σφοδρά. Η Ευρωπαϊκή Ένωση επιθυμεί την εφαρμογή της συνθήκης Wassenaar σε λογισμικά συστήματα λαμβάνοντας υπ' όψη πως λογισμικά εισβολής και αδυναμίες zero-day μπορούν να είναι χρήσιμα σε ερευνητικό επίπεδο και αποτρέποντας την τιμωρία των ηθικών χάκερ (Giles 2017).

4.7 Αντίμετρα

Για την οικοδόμηση ενός συστήματος άμυνας εναντίων κυβερνοεπιθέσεων απαιτούνται έξι χαρακτηριστικά. Πρώτα από όλα απαραίτητοι είναι οι αισθητήρες και τα όργανα εκείνα που θα αντιλαμβάνονται έγκαιρα μία επίθεση. Ακολούθως η παρατήρηση της επίθεσης θα πρέπει να μεταφράζεται σε δεδομένα βάση των οποίων θα αποφασίζεται η απάντηση στην απειλή. Επιπλέον το αμυντικό σύστημα θα πρέπει να διαθέτει κάποιου είδους τεχνολογία αποτροπής των κυβερνοαπειλών όπως για παράδειγμα κάποιο antivirus. Σημαντικό χαρακτηριστικό είναι να μπορεί να εκτελεί αμυντικές πρακτικές γρήγορα και αποτελεσματικά. Σε τακτικό επίπεδο ένα σύστημα άμυνας πρέπει να αντιλαμβάνεται πότε επιβάλλεται η αλλαγή των αντιμέτρων που χρησιμοποιεί με άλλα αποτελεσματικότερα. Τέλος για να είναι ολοκληρωμένο θα πρέπει να έχει την ικανότητα να αναπτύσσει τον μηχανισμό του. Πέραν της

οικοδόμησης αποτελεσματικών συστημάτων η άμυνα στον κυβερνοχώρο απαιτεί την εκπαίδευση των χρηστών σε ζητήματα ασφαλείας. Η εκπαίδευση αυτή δύναται να αποτρέψει αποτελεσματικά απειλές καθώς με το τρόπο αυτό δυσχεραίνεται η προσπάθεια του εισβολέα να αντλήσει πληροφορίες από κάποιον ανυποψίαστο χρήστη. Χαρακτηριστικό παράδειγμα των συνεπειών που συμβαδίζουν με την έλλειψη εκπαίδευσης είναι η μόλυνση με το Stuxnet που προέκυψε από το usb ενός υπαλλήλου.

Υπάρχουν δύο επιλογές κυβερνοάμυνας σε εθνικό επίπεδο. Η πρώτη επιλογή αφορά την οικοδόμηση δικτύων που θα παρέχουν περιορισμένη σύνδεση από εξωτερικές συνδέσεις, κάτι που θα προϋπόθετε την ανακατασκευή των ήδη υπαρχόντων δικτύων, μιας διαδικασίας εξαιρετικά ακριβής. Η δεύτερη επιλογή κυβερνοάμυνας προϋποθέτει τη χρήση Intrusion Detection Systems (IDS) και Intrusion Protection Systems (IPS). Με τον τρόπο αυτό θα χρησιμοποιούνταν ήδη υπάρχοντα δίκτυα αλλά θα ήταν μία κοστοβόρα διαδικασία και πιθανότατα θα αποτύγχανε σε ένα βαθμό να παρεμποδίσει κακόβουλες δραστηριότητες (Krepinevich 2012).

4.8 Αμυντικές τεχνικές

4.8.1 Κρυπτογράφηση:

Η διαδικασία κωδικοποίησης δεδομένων με έναν τρόπο που μπορεί να αποκρυπτογραφηθεί μόνο από εξουσιοδοτημένα άτομα. Χρησιμοποιεί κρυπτογραφικούς αλγόριθμους και πρωτόκολλα για την προστασία των δεδομένων τόσο κατά την αποθήκευση όσο και κατά τη διάρκεια μετάδοσης, εμποδίζοντας έτσι τη μη εξουσιοδοτημένη πρόσβαση και υποκλοπή (Soni 2024).

4.8.2 CTI:

Η συλλογή και αξιολόγηση δεδομένων σχετικά με απειλές, τεχνικές και αντιπάλους με σκοπό τη δημιουργία αμυντικών τεχνικών. Περιλαμβάνει τη συνεχή παρατήρηση απειλών, σημαδιών συμβιβασμού (IoCs) και αναπτυσσόμενων κυβερνοαπειλών (Soni 2024).

4.8.3 Άμεση αντίδραση:

Στρατηγικές και πρωτόκολλα για τη ταυτοποίηση, έλεγχο και περιορισμό κυβερνοαπειλών και τη συνέχιση του κανονικού κύκλου εργασιών. Περιλαμβάνει τη δημιουργία ομάδων άμεσης δράσης, τη διεξαγωγή ασκήσεων, και την επαναφορά πληγέντων συστημάτων (Soni 2024).

4.8.4 Τμηματοποίηση:

Προβλέπει το κατακερματισμό των δικτύων ούτως ώστε να ελαχιστοποιούνται οι συνέπειες των παραβιάσεων. Στη μέθοδο αυτή χρησιμοποιούνται firewall, VPN, ACLs (Soni 2024).

Κεφάλαιο 5: Κρατικές κυβερνοεπιθέσεις

Οι κυβερνοεπιθέσεις που οργανώνονται ή υποστηρίζονται από κυβερνήσεις κρατών και επιθυμούν να επιτύχουν συγκεκριμένους πολιτικούς, οικονομικούς ή στρατιωτικούς σκοπούς. Οι κυβερνοεπιθέσεις που εξαπολύονται από κρατικούς δρώντες χαρακτηρίζονται από την πολυπλοκότητα και συχνά χρησιμοποιούν προηγμένες τεχνολογίες και εργαλεία που εξασφαλίζουν την αδυναμία του εντοπισμού τους. Στόχοι των συγκεκριμένων επιθέσεων μπορεί να αποτελέσουν οι υποδομές, κυβερνητικές υπηρεσίες αλλά και ιδιωτικές εταιρίες προκαλώντας κατά αυτό το τρόπο σοβαρές σημαντικές επιπτώσεις σε οικονομικό, πολιτικό αλλά και επίπεδο ασφαλείας. Το βασικό κίνητρο που ωθεί κρατικούς δρώντες σε τέτοιες δράσεις δεν είναι άλλο από την απόκτηση του στρατηγικού πλεονεκτήματος έναντι άλλων κρατών με σκοπό την πρόκληση αστάθειας σε αυτά καθώς και τη δημιουργία προβλημάτων όπως για παράδειγμα η κλοπή πληροφοριών και η παρεμπόδιση της λειτουργίας των υποδομών. Για την επίτευξη των κρατικών κυβερνοεπιθέσεων χωρίς τη συνακόλουθη επίρριψη της ευθύνης στο κράτος που την οργάνωσε ακολουθείται η πρακτική του να χρησιμοποιούνται από τους κρατικούς δρώντες εγκληματικά συνδικάτα ή ομάδες χακτιβιστών σκιάζοντας έτσι τον ρόλο των κρατών. Η στρατηγική αυτή των κρατών είναι απαραίτητη εφόσον σε αντίθετη περίπτωση θα βρεθούν αντιμέτωπα με διπλωματικές ή και στρατιωτικές συνέπειες (Azubuike 2023).

Κεφάλαιο 6: Κυβερνοεπιθέσεις και ειρήνη

Παρά τη χρήση κυβερνοεπιχειρήσεων κατά τη διάρκεια ένοπλων συγκρούσεων θα πρέπει να αποσαφηνιστεί πως αυτές αποτελούν κυρίως φαινόμενο που συναντάται σε περιόδους ειρήνης. Βέβαια οι ίδιες οι κυβερνοεπιθέσεις θα μπορούσαν να χαρακτηριστούν οι ίδιες σαν πολεμική δραστηριότητα, η αβεβαιότητα όμως που τις περιβάλλει τόσο σε πολιτικό όσο και σε νομικό επίπεδο δεν το επιτρέπει. Η κρυφή φύση των επιθέσεων εξάλλου συμβάλλει στο πρόβλημα της απόδοσης του δράστη και συνακόλουθα την αποφυγή της στρατιωτικής κλιμάκωσης, όπως χαρακτηριστικά αποδείχθηκε στη περίπτωση του Stuxnet (Green 2015).

Κεφάλαιο 7: Δρώντες

7.1 Δράστες:

Η ευκολία με την οποία μπορούν να βρεθεί ο εξοπλισμός για την διεξαγωγή μίας κυβερνοεπίθεσης σε συνδυασμό με το γεγονός πως δεν χρειάζεται κάποια επίσημη εκπαίδευση δημιουργεί τις συνθήκες για πολλούς διαφορετικούς δρώντες που διεξάγουν τις επιχειρήσεις αυτές. Εγκληματικά συνδικάτα, τρομοκρατικές οργανώσεις αλλά ακόμα και υπηρεσίες πληροφοριών κρατών μπορούν να προετοιμάσουν και να διεξάγουν κυβερνοεπιθέσεις (Carlin 2016).

1. Τρομοκρατικές οργανώσεις: σε αυτές περιλαμβάνονται ομάδες όπως το ISIL και η Al-Qaeda. Συγκεκριμένα η δεύτερη το 2012 δημοσίευσε βίντεο

στο οποίο συνέκρινε τις αδυναμίες των πληροφοριακών συστημάτων με αυτά στην αεροπορική ασφάλεια πριν από το 2001 και καλούσα σε μία ηλεκτρονική τζιχάντ εναντίων των ΗΠΑ. Παράλληλα οι τρομοκρατικές οργανώσεις επιζητούν την ανάπτυξη επιθετικών δυνατοτήτων στο κυβερνοχώρο, πέραν των ήδη υπαρχουσών δυνατοτήτων στρατολόγησης, χρηματοδότησης και προπαγάνδας που ήδη διαθέτουν. Συμπληρωματικά με τις τρομοκρατικές οργανώσεις λειτουργούν και αυτόνομοι υποστηρικτές που δρουν μέσω social media και λειτουργούν υπέρ των τρομοκρατών. Τρομοκρατικές ενέργειες μέσα από το κυβερνοχώρο όπως η διαρροή προσωπικών δεδομένων (e-mail, ονόματα, τηλέφωνα, διευθύνσεις) 1.000 στρατιωτικών των ΗΠΑ τον Αύγουστο του 2015 καταδεικνύουν πως ο κυβερνοχώρος αποτελεί πεδίο δράσης της σύγχρονης τρομοκρατίας (Carlin 2016). Εκτός της Al Qaeda οργανώσεις όπως η Χαμάς, η Χεζμπολάχ, η Aum Shinrikyo και η Ένοπλη Ισλαμική Ομάδα έχουν αναβαθμίσει την επιχειρησιακή τους δυνατότητα, ενώ στις ΗΠΑ οι οργανώσεις Hammerskin Nation, Stormfront, Aryan Nation, και National Alliance φέρονται να διαθέτουν τις τεχνολογικές δυνατότητες για την διεξαγωγή κυβερνοτρομοκρατίας. (Hemen Faga 2017). Οι διαδικτυακές δυνατότητες έχουν δώσει τη δυνατότητα σε τρομοκρατικές ομάδες να εκπέμπουν το μήνυμά τους και να στρατολογούν μέλη ευκολότερα καθώς και φέρουν σε επαφή ομάδες που σε άλλες συνθήκες δε θα μπορούσαν. Η ευρεία κυκλοφορία φθηνών αλλά σύνθετων τεχνολογικών προϊόντων προσφέρει σε τρομοκράτες τη δυνατότητα να συνδυάσουν τα τεχνολογικά πλεονεκτήματα με συμβατικές μεθόδους όπως έγινε στη βομβιστική επίθεση της Βομβάης το 2008 (Cornish, Livingstone, Clemente, Yorke 2010)

2. Κράτη και πληρεξούσιοι: κρατικές οντότητες όπως η Κίνα και η Ρωσία διαθέτουν τον εξοπλισμό και τη τεχνολογία για να διαρρήξουν συστήματα και να αποκτήσουν ευαίσθητες πληροφορίες ή να διαταράξουν κρίσιμες λειτουργίες. Ακόμα και υποδιαίστερες δυνάμεις όπως το Ιράν μπορούν και διεξάγουν επιζήμιες επιθέσεις, όπως το Μάρτιο το 2016 οπότε εταιρίες ασφαλείας σχετιζόμενες με τους Φρουρούς της Επανάστασης στόχευσαν τον τραπεζικό τομέα των ΗΠΑ κατακλύζοντας για 176 μέρες 46 τραπεζικά ιδρύματα. Επιπλέον οι επιθέσεις στόχευσαν και το υπολογιστικό σύστημα του φράγματος Bowman (Carlin 2016).

3. Εγκληματικά συνδικάτα και μεμονωμένοι δράστες (χάκερ). (Carlin 2016)

4. Script Kiddies: δεν διαθέτουν μεγάλες ικανότητες, κίνητρο η διασκέδασή τους (Dinicu 2014).

5. Διαδηλωτές: αυτοί που διαμαρτύρονται για κοινωνικά θέματα όπως είναι ομάδες χακτιβιστών (Dinicu 2014).

6. Μισθοφόροι: είναι εκπαιδευμένοι και κίνητρό τους είναι το οικονομικό όφελος (Dinicu 2014).

Δράστες που δεν συμμετέχουν με επιθετικό τρόπο

1. Πολυεθνικές εταιρείες και τραπεζικά ιδρύματα που μπορεί να έχουν υποστεί οικονομική κατασκοπεία, κλοπή πνευματικής ιδιοκτησίας,
2. Διεθνείς οργανισμοί που παρακολουθούν το φαινόμενο και αναπτύσσουν στρατηγικές καταπολέμησής του

Κατηγορίες δραστών κατά αυξανόμενο επίπεδο απειλής: (Βεράτης 2016)

1. Χάκερ (Hackers)
2. Αντιβιστές Χάκερ (Hactivists)
3. Οργανωμένο έγκλημα
4. Δράστες βιομηχανικής κατασκοπείας
5. Εσωτερικοί δράστες
6. Εξωτερικοί συνεργάτες/σύμβουλοι
7. Τρομοκρατικές οργανώσεις
8. Κράτη

7.2 Θύματα:

Συνηθέστερα μεμονωμένα άτομα δεν αποτελούν στόχο μαζικών επιθέσεων καθώς αυτές κυρίως εστιάζουν στις υποδομές. Οι επιπτώσεις που μπορεί να έχουν στις υποδομές μπορεί να είναι συντριπτικές (το 70% της ηλεκτροδότησης των ΗΠΑ μπορεί να πληγεί για έξι μήνες). Σε περιπτώσεις που μία πολεμική σύρραξη διαδραματίζεται οι επιθέσεις θα στοχεύσουν κυρίως στρατιωτικές και κυβερνητικές εγκαταστάσεις αλλά και χρηματοπιστωτικά ιδρύματα όπως έχει παρατηρηθεί σε πρόσφατες συγκρούσεις (Gandhi, Sousan, Laplante 2011).

Σε αντίθεση μικρότερες επιθέσεις στοχεύουν χρήστες που δεν έχουν την απαραίτητη γνώση των τεχνικών αδυναμιών του συστήματος. Υπολογίζεται πως το 93% των μη οργανωμένων επιθέσεων επηρεάζει οικιακούς χρήστες (Gandhi, Sousan, Laplante 2011).

Κεφάλαιο 8: Ο ρόλος του στρατού

Τόσο στην άμυνα όσο και στη διεξαγωγή επίθεσης στο κυβερνοχώρο οι ένοπλες δυνάμεις δύνανται να διαδραματίσουν σημαντικό ρόλο στο τομέα της εθνικής ασφάλειας. Η αύξηση των δυνατοτήτων κυβερνοασφάλειας από τις ένοπλες δυνάμεις αποτελεί μονόδρομο λόγω της αύξησης των απειλών του κυβερνοχώρου και της ολοένα και μεγαλύτερης πολυπλοκότητάς τους. Η ασφάλεια των κρίσιμων υποδομών όπως τα δίκτυα επικοινωνιών και μεταφορών επιτυγχάνεται με την ανάπτυξη κυβερνοομάδων άμεσης αντίδρασης που εντοπίζουν και ανταποκρίνονται σε περίπτωση απειλής είτε αυτή αφορά στρατιωτικούς είτε πολιτικούς στόχους.

Στόχος των ομάδων παράλληλα αποτελεί η αποκατάσταση των επιχειρησιακών δυνατοτήτων των πληγέντων στόχων. Οι στρατιωτικοί σχηματισμοί που δρουν στο κυβερνοχώρο συνεργάζονται μεταξύ τους σε διεθνικό επίπεδο σε ότι αφορά τη συλλογή και διαμοιρασμό πληροφοριών για πιθανές απειλές, ενώ παράλληλα συνεργάζονται και με πολιτικές υπηρεσίες, οργανισμούς και τον ιδιωτικό τομέα. Σε ότι αφορά το δεύτερο σκέλος, αυτό δηλαδή της διεξαγωγής επιθετικών επιχειρήσεων, η συλλογή πληροφοριών για πιθανούς στόχους και τις δυνατότητες αυτών αποτελούν τη κύρια δραστηριότητα. Για την επίτευξη αυτού του στόχου συχνά διενεργείται κυβερνοκατασκοπεία ούτως ώστε να αποκτηθούν οι απαραίτητες πληροφορίες. Συχνά χρησιμοποιούνται οι επιχειρησιακές δυνατότητες με επιθετικό τρόπο έχοντας ως στόχο την επίδειξη ισχύος έτσι ώστε να αποτρέπονται πιθανοί αντίπαλοι. Λοιπές δραστηριότητες περιλαμβάνουν την αντιμετώπιση τρομοκρατών και αντάρτικων ομάδων που χρησιμοποιούν το κυβερνοχώρο για στρατολόγηση και προπαγάνδα. Οι δυνάμεις του κυβερνοχώρου χρησιμοποιούνται συνδυαστικά με τις συμβατικές στρατιωτικές δυνάμεις και αναλαμβάνουν επιχειρήσεις όπως τη στρέβλωση των αντίπαλων επικοινωνιών-συστημάτων ελέγχου και διοίκησης ή ακόμα και τη διάδοση προπαγάνδας με στόχο τον επηρεασμό της κοινής γνώμης (Digmelashvili 2023).

Κεφάλαιο 9: Ο ρόλος των κυβερνήσεων

Οι κυβερνήσεις χρησιμοποιούν ένα πλέγμα νομικών ρυθμίσεων, στρατηγικών, ρυθμίσεων και τεχνολογικών λύσεων με σκοπό τη προστασία της εθνικής ασφάλειας από τις κυβερνοεπιθέσεις. Ο ρόλος μίας κυβέρνησης συνίσταται στο να δημιουργούν ένα στρατηγικό πλαίσιο για τη διασφάλιση των υποδομών, πληροφοριών και συστημάτων. Στο πλαίσιο αυτό αποδίδονται οι τομείς ευθυνών στους επιμέρους κυβερνητικούς οργανισμούς και αναλαμβάνει των συντονισμό των δράσεων τους. Στη φαρέτρα τους διαθέτουν όπλα όπως τη θέσπιση νόμων για τον ορισμό προτύπων και απαιτήσεων για τη κυβερνοασφάλεια καθώς και κυρώσεων για τη μη συμμόρφωση προς αυτά. Παράλληλα οι κυβερνήσεις προάγουν τη συνεργασία ανάμεσα σε κυβερνητικούς θεσμούς, τον ιδιωτικό τομέα, την ακαδημαϊκή κοινότητα και μη κυβερνητικούς θεσμούς με σκοπό την ανταλλαγή γνώσεων, πρακτικών και πόρων για την βελτιστοποίηση της κυβερνοασφάλειας. Η κυβερνοασφάλεια των υποδομών αποτελεί μία δυναμική διαδικασία η οποία απαιτεί από τις κυβερνήσεις να διεξάγουν αξιολογήσεις κινδύνου, να ενισχύουν τις ικανότητες παρακολούθησης, να πραγματοποιούν προσομοιώσεις κυβερνοεπιθέσεων με σκοπό τη διαπίστωση της ετοιμότητας των κυβερνητικών θεσμών και των ομάδων αντίδρασης. Παράλληλα πραγματοποιούν εκστρατείες ενημέρωσης και παρέχουν εκπαίδευση σε επιχειρήσεις, δημοσίους υπαλλήλους έτσι ώστε να μειωθεί το ενδεχόμενο ρίσκο των επιθέσεων. Τέλος η ανταλλαγή γνώσεων γίνεται και σε διεθνές επίπεδο μεταξύ κρατών όπως και η αντίδραση σε περιστατικά κυβερνοεπιθέσεων (Digmelashvili 2023).

Κεφάλαιο 10: Ο ρόλος της Διπλωματίας

Η διπλωματία στο κυβερνοχώρο αποτελεί μία στρατηγική ενέργεια που λειτουργεί προς το σκοπό του ελέγχου του κινδύνου μέσα από την επίλυση του προβλήματος της απόδοσης ή της αποκάλυψης μιας κυβερνοεπίθεσης. Η έννοια της διπλωματίας στο περιβάλλον των κυβερνοεπιθέσεων δεν αποτελεί ένα κομμάτι μίας στρατηγικής αλλά αντίθετα είναι στην ουσία η καθοδήγηση μιας αμυντικής στρατηγικής του κράτους στην ψηφιακή εποχή. Στη κατεύθυνση αυτή η ψηφιακή διπλωματία για να είναι στιβαρή φαίνεται πως πρέπει να υιοθετεί μία επιθετική στάση, να δρα δηλαδή σχεδόν σαν μία προληπτική επίθεση, όχι όμως να υιοθετεί μία εντελώς επιθετική πολιτική. Παράλληλα στα πλαίσια της άμυνας και της διπλωματίας θα πρέπει να υπάρχει μία σαφής στρατηγική άποψη για τον κυβερνοχώρο, καθώς αυτός είναι πλέον αλληλένδετος με τις διεθνείς σχέσεις μεταξύ κρατών, πολυεθνικών και ιδιωτών και η έλλειψη επαρκούς γνώσης αυτού από τους πολιτικούς δρώντες, συνιστά αδυναμία. (Lancelot 2020)

Κεφάλαιο 11: Ιστορικό των Κυβερνοεπιθέσεων – Κύρια γεγονότα

Το φαινόμενο των κυβερνοεπιθέσεων εντάσσεται στο ευρύτερο πλαίσιο των επιχειρήσεων πληροφοριών. Οι επιχειρήσεις αυτές κάνουν συστηματική χρήση των δυνατοτήτων του ηλεκτρονικού πολέμου, των δικτύων υπολογιστή, της στρατιωτικής παραπλάνησης (Li, Liu 2021).

11.1 ΕΣΣΔ 1982:

ο πρόεδρος Ρήγκαν των ΗΠΑ συναίνεσε στη κυβερνοεπίθεση (SCADA) εναντίων του συστήματος αγωγών της Σιβηρίας. Η επίθεση αυτή αποτέλεσε μία από τις πρώτες επιθέσεις της μορφής των λογικών βομβών και αποσκοπούσε στη διατάραξη των τεχνολογικών δυνατοτήτων της ΕΣΣΔ και να δυσχεράνει τη ροή φυσικού αερίου προς τη Δύση ζημιώνοντας την οικονομία της (Cornish, Livingstone, Clemente, Yorke 2010).

11.2 Ιράκ 2003:

Το 2003 λίγο πριν την εκδήλωση της επιχείρησης των ΗΠΑ στο Ιράκ το email του ιρακινού υπουργείου άμυνας παραβιάστηκε από τις ΗΠΑ με σκοπό να έρθουν σε επαφή με αξιωματικούς του Ιράκ και να τους ενημερώσουν πως μοναδικός σκοπός της επικείμενης επίθεσης είναι η ανατροπή του ηγέτη της χώρας Σαντάμ Χουσεΐν. Το εγχείρημα αυτό γνώρισε μία περιορισμένη επιτυχία καθώς στρατιώτες ακολουθώντας τις οδηγίες που περιλαμβάνονταν στο μέιλ αυτομόλησαν αφήνοντας τον οπλισμό τους.

11.3 Ηνωμένο Βασίλειο 2007:

Οι επιθέσεις Titan Rain το 2007 αποτέλεσαν μία από τις μεγαλύτερες παραβιάσεις κυβερνητικών τμημάτων στις ΗΠΑ και το Ηνωμένο Βασίλειο με στόχο τη συλλογή ευαίσθητων πληροφοριών. Οι επιθέσεις αποδόθηκαν στη Κίνα και φέρονται να προετοιμάζονταν ήδη από το 2002 (Cornish, Livingstone, Clemente, Yorke 2010).

11.4 Εσθονία 2007:

Η απαρχή της σημερινής μορφής των κυβερνοεπιθέσεων εντοπίζεται από τους περισσότερους μελετητές στις επιθέσεις που υπέστησαν η Εσθονία (2007) και η Γεωργία (2008). Σε ότι αφορά την υπόθεση της Εσθονίας αυτή ξεκίνησε από τη μετακίνηση του αγάλματος του Χάλκινου στρατιώτη στο Ταλίν γεγονός που γρήγορα οδήγησε σε διαμαρτυρίες και συγκρούσεις μεταξύ της ρωσικής μειονότητας της Εσθονίας και των Εσθονών. Κατά τη διάρκεια των ταραχών αυτών η Εσθονία αντιμετώπισε επιθέσεις DDoS εναντίων του τραπεζικού της συστήματος, των τηλεπικοινωνιών της και των κυβερνητικών της υποδομών οι οποίες ξεκίνησαν στις 27 Απριλίου και συνέχισαν για εβδομάδες. Οι επιθέσεις προήλθαν από 80.000 διαφορετικές διευθύνσεις IP και κατέκλυσαν μηχανές φαξ και τα κινητά τηλέφωνα Εσθονών βουλευτών. Ίχνη της επίθεσης αυτής εντοπίστηκαν σε ρωσσόφωνα φόρουμ στα οποία δίδονταν οδηγίες για τη διεξαγωγή επίθεσης. Το γεγονός πως το ενδεχόμενο εμπλοκής της επίσημης ρωσικής κυβέρνησης παραμένει ασαφές οι επιθέσεις διοργανωμένες από το πλήθος καταδεικνύουν πως ακόμα και αν αυτές διοργανώνονται ή επηρεάζονται από κράτη και κυβερνήσεις, αυτές μπορούν εύκολα να αντικρούσουν τις κατηγορίες και να αποδώσουν σαν κίνητρο των επιθέσεων τη λαϊκή οργή. Σημαντικό απότοκο των επιθέσεων του 2007 αποτελεί η συμπερίληψη των κυβερνοεπιθέσεων στο άρθρο 5 του NATO που προβλέπει πως η επίθεση εναντίων ενός μέλους της συμμαχίας υποχρεώνει τα υπόλοιπα να υπερασπιστούν το υπό επίθεση μέλος (Green 2015).

11.5 Γεωργία 2008:

Κατά τη διάρκεια της διαμάχης της Γεωργίας με τις περιοχές της Αμπχαζίας και της Νότιας Οσσετίας και την Ρωσία που υποστήριζε την ανεξαρτησία των περιοχών αυτών η Γεωργία ήρθε αντιμέτωπη με ένα κύμα κυβερνοεπιθέσεων περίπου ένα μήνα πριν από την ένοπλη επέμβαση της Ρωσίας. Αρχής γενομένης από τις 20 Ιουλίου η επίσημη ιστοσελίδα του γεωργιανού προέδρου ήρθε αντιμέτωπη με ένα botnet (machbot) που κατέκλυσε την ιστοσελίδα με πακέτα http, tcp και icmp καθιστώντας τη μη διαθέσιμη για 24 ώρες. Παράλληλα προβλήματα αντιμετώπισαν και άλλες σελίδες όπως αυτή του υπουργείου εργασίας. Η πολεμική κλιμάκωση στις 7-8 Αυγούστου σηματοδότησε και μεγάλης κλίμακας επιθέσεις σε γεωργιανές ιστοσελίδες ήδη από το απόγευμα της 7ης Αυγούστου πριν δηλαδή από την εισβολή των ρωσικών στρατευμάτων. Οι επιθέσεις επέφεραν σαν αποτέλεσμα τη διακοπή της λειτουργίας ιστοσελίδων που χρησιμοποιούσε η κυβέρνηση της Γεωργίας για την επικοινωνία της με τους κατοίκους της χώρας και με τον υπόλοιπο κόσμο καθώς και των ιστοσελίδων των τραπεζών και των υπουργείων της χώρας. Όπως και στη περίπτωση της Εσθονίας έτσι και στη Γεωργία παρήχθησαν οδηγίες για τη στοχοποίηση 36 server στη Γεωργία από τη StopGeorgia.com, ιστοσελίδας που φαίνεται να ανήκει στο Russian Business Network (RBN) σύμφωνα με το RBNExploit.com. Επιπλέον οι ΗΠΑ έδωσαν πληροφορίες πως οι επιθέσεις εναντίων των υπουργείων άμυνας, εξωτερικών και της προεδρίας της Γεωργίας προήλθαν μέσω Τουρκίας από server που επίσης σχετίζονται με τη δραστηριότητα του RBN που αποτελεί μία οργάνωση κυβερνοεγκλήματος και

συνδέεται με το οργανωμένο έγκλημα της Ρωσίας και φαίνεται να εδρεύει στην Αγία Πετρούπολη και απασχολεί πρώην πράκτορες της KGB (Robinson 2015).

11.6 Stuxnet Worm 2010:

Η ανάπτυξη του Stuxnet φαίνεται πως ξεκίνησε στις ΗΠΑ ήδη από το 2005 και επιταχύνθηκε έπειτα από προτροπή του Ισραήλ για βοήθεια των ΗΠΑ για την πραγμάτωση επιθέσεων εναντίων Ιρανικών πυρηνικών εγκαταστάσεων στο Natanz. Παρά τη πρόοδο που επιτεύχθηκε τη περίοδο 2009-10 και τις καταστροφικές συνέπειες που το Stuxnet μπορούσε να επιφέρει εμφάνισε και σημαντικά μειονεκτήματα όπως ήταν το κόστος για την ανάπτυξή του (300 εκατομμύρια δολάρια) καθώς και το υψηλό κόστος των πραγματοποιούμενων επιθέσεων σε συνδυασμό με τη μεγαλύτερη επιτυχία συμβατικότερων όπλων το κατέστησαν ασύμφορο (Benjamin 2017). Η εμπλοκή των ΗΠΑ επισήμως αμφισβητείται από τις ίδιες ωστόσο δημοσιεύματα τόσο των New York Times και της Washington Post οδηγούν στο αντίθετο συμπέρασμα. Το Stuxnet αποτέλεσε κομμάτι της μυστικής αποστολής με την ονομασία Ολυμπιακοί Αγώνες. Στο αρχικό στάδιο της επιχείρησης ένα πρόγραμμα spyware χαρτογράφησε τα συστήματα στο Natanz και ακολούθησε η μόλυνση με το Stuxnet που επιτεύχθηκε μέσω USB. Η επιχείρηση είχε σαν αποτέλεσμα τη πρόκληση ζημιάς στους φυγοκεντρητές αερίου που διυλίζουν το αέριο καθυστερώντας έτσι το ιρανικό πυρηνικό πρόγραμμα κατά δύο έτη (Green 2015). Στη περίπτωση του Stuxnet οι πολιτικές επιπτώσεις είναι δυσδιάκριτες. Θα μπορούσε να λεχθεί πως οι πολιτικές συνέπειες εντάσσονται σε ένα ευρύτερο πλαίσιο στο οποίο η επίθεση βοήθησε στο περιορισμό του ιρανικού πυρηνικού προγράμματος και την αποφυγή στρατιωτικής αντίδρασης του Ισραήλ, επομένως αποφεύχθηκε ένας περιφερειακός πόλεμος (Green 2015).

11.7 Συρία 2013:

Οι κυβερνοεπιθέσεις συχνά πραγματοποιούνται συνδυαστικά με συμβατικές στρατιωτικές επιχειρήσεις. Ένα τέτοιο παράδειγμα αποτελεί η ισραηλινή επιδρομή σε εγκατάσταση όπλων του συριακού στρατού. Η επιτυχία της επιχείρησης οφείλεται εν πολλοίς στη διείσδυση κυβερνοστρατιωτών του Ισραήλ στο συριακό δίκτυο αεράμυνας. Στόχος της επίθεσης δεν ήταν η πρόκληση ζημιάς στα δίκτυα της συριακής αεράμυνας αλλά η εξαπάτησή τους με λανθασμένες πληροφορίες ούτως ώστε να αποκρυφθούν τα πολεμικά αεροσκάφη που διεξήγαν την επιχείρηση (Pool 2013).

Κεφάλαιο 12: Πολιτικές επιθέσεις

Οι επιθέσεις που έχουν πολιτικό κίνητρο μπορούν να διεξαχθούν από εξτρεμιστικές ομάδες που χρησιμοποιούν το διαδίκτυο για τη προαγωγή της προπαγάνδας τους, τη κλοπή χρημάτων για τη χρηματοδότηση των δραστηριοτήτων τους, την επίθεση σε ιστοσελίδες και δίκτυα αντιπάλων τους. αποφάσεων (Gandhi, Sousan, Laplante 2011) Οι πολιτικές επιπτώσεις των κυβερνοεπιθέσεων ωστόσο παραμένουν συχνά ασαφείς κυρίως λόγω της μη αποδοχής της ενοχής του δράστη ή την απουσία αποδείξεων για την ενοχή αυτού. Για παράδειγμα στις επιθέσεις της Ρωσίας εναντίων της Εσθονίας

οι επιπτώσεις αφορούσαν κυρίως τη παρακώλυση ενός κομματιού του δημοσίου τομέα, γεγονός που οδήγησε τους Εσθονούς στο να κατηγορήσουν τη Ρωσία, της οποίας το πολιτικό όφελος ομοίως δε μπορεί να μετρηθεί. Παρομοίως στην επίθεση εναντίων της Γεωργίας η στρατηγική χρησιμότητα που φαίνεται να παρείχαν οι κυβερνοεπιθέσεις φαίνεται πως είναι η χρήση τους συνδυαστικά με συμβατικούς τρόπους (Green 2015). Οι επιθέσεις πολιτικής φύσης μπορούν να κατηγοριοποιηθούν περαιτέρω σε:

1. Διαμαρτυρίες εναντίων πολιτικών/κυβερνητικών αποφάσεων (Gandhi, Sousan, Laplante 2011):

Ιούνιος 1998: επίθεση χάκερ (Milworm) στην ιστοσελίδα ατομικής έρευνας της Ινδίας με σκοπό να διαμαρτυρηθούν για τη διενέργεια πυρηνικών δοκιμών

Σεπτέμβριος 1998: Πορτογάλοι χάκερ τροποποίησαν δεδομένα σε 40 server της Ινδονησίας για να διαμαρτυρηθούν για τις παραβιάσεις ανθρωπίνων δικαιωμάτων στο Ανατολικό Τιμόρ

Οκτώβριος 1999: η ιστοσελίδα της μεξικανικής προεδρίας πλήττεται σαν ένδειξη διαμαρτυρίας για τις γενοκτονίες, το ρατσισμό και την αποικιοποίηση ανά το κόσμο.

Ιούνιος 1999: χάκερ εξαπολύουν 10.000 επιθέσεις σε διάστημα πέντε ωρών καταφέροντας να διαταράξουν τραπεζικά ιδρύματα και πολυθνικές εταιρίες. Σκοπός τους η διαμαρτυρία εναντίων της συνάντησης των G8.

1999: Σέρβοι χάκερ επιτίθενται σε αμερικανικές και νατοϊκές ιστοσελίδες παραλύοντας τες και διαρρέοντας μηνύματα, εικόνες και βίντεο. Σκοπός τους η διαμαρτυρία για τον πόλεμο στη Γιουγκοσλαβία.

Δεκέμβριος 2008: Κινέζοι χάκερ επιτίθενται στη γαλλική πρεσβεία εξαιτίας της συνάντησης του Γάλλου προέδρου με τον Δαλάι Λάμα

2. Διαμαρτυρίες εναντίων νόμων (Gandhi, Sousan, Laplante 2011)

Δεκέμβριος 1995: η ομάδα Strano Network στιχοποιοί κυβερνητικές ιστοσελίδες ως αντίδραση στην κοινωνική και πυρηνική πολιτική της κυβέρνησης.

1996: διαδηλωτές διαγράφουν δεδομένα από τη σελίδα του υπουργείου δικαιοσύνης των ΗΠΑ

Μάρτιος 2001: Νοτιοκορεάτες χάκερ επιτίθενται στο υπουργείο παιδείας της Ιαπωνίας λόγω της έκδοσης αμφιλεγόμενων βιβλίων ιστορίας.

3. Διαμαρτυρία εναντίων πράξεων σχετισμένων με βία (Gandhi, Sousan, Laplante 2011)

Μάιος 1999: Κινέζοι χάκερ στοχοποιούν κυβερνητικές ιστοσελίδες των ΗΠΑ ως αντίδραση για τον βομβαρδισμό της Κινεζικής πρεσβείας στο Βελιγράδι.

Αύγουστος 1999: η ένταση μεταξύ Κίνας και Ταιβάν περνά στον κυβερνοχώρο. Η Κίνα επιτίθεται σε ταιβανέζικες κυβερνητικές σελίδες και η Ταιβάν ακολουθώντας ανεβάζουν αντικομμουνιστικά μηνύματα σε κινεζικές.

Νοέμβριος 2000: Παλαιστινιακή ομάδα (Unity) επιτίθεται στην εταιρεία Lucent που πραγματοποιεί συναλλαγές με το Ισραήλ. Ο κυβερνοπόλεμος που διεξήχθη το φθινόπωρο του 2000 θα οδηγήσει σε πτώση 8% του ισραηλινού χρηματιστηρίου.

Απρίλιος 2001: η πτώση κατασκοπευτικού αεροπλάνου των ΗΠΑ θα οδηγήσει στη παραβίαση 1.000 αμερικανικών ιστοσελίδων από κινέζους χακτιβιστές την περίοδο 28 Απριλίου-8 Μαΐου. Παράλληλα θα επιτεθούν με DDoS εναντίων του Λευκού Οίκου και των υπηρεσιών πληροφοριών. Πίσω από τις επιθέσεις εικάζεται πως βρίσκονταν τρεις διαφορετικές ομάδες χάκερ.

Αύγουστος 2001: χάκερ από τη Κίνα επιτίθενται σε σελίδες της Ιαπωνίας και ιδιαίτερα στη Yasukuni Shrine που είναι αφιερωμένη σε πεσόντες εν καιρώ πολέμου Ιάπωνες.

Κεφάλαιο 13: Κοινωνικό-πολιτισμικές επιθέσεις

Η κοινωνικό-πολιτισμική σύγκρουση μπορεί να χαρακτηριστεί ως ο ανταγωνισμός διαφορετικών ομάδων ή ατόμων για την επίτευξη ασυμβίβαστων στόχων, την απόκτηση περιορισμένων πόρων ή για την επιβολή εξουσίας. Στο πλαίσιο αυτό μπορούμε να παρατηρήσουμε την μεταφορά των εντάσεων αυτών στο κυβερνοχώρο όπως είναι οι διαδικτυακές συγκρούσεις της Ταιβάν με τη Κίνα το 1999 και της Ρωσίας με την Εσθονία (2007) και τη Γεωργία (2008) αλλά και την διαδικτυακή σύγκρουση Ισραήλ Παλαιστίνης. (Gandhi, Sousan, Laplante 2011). Οι επιθέσεις αυτές χωρίζονται σε:

1. Επιθέσεις προκληθείσες λόγω εδαφικών διαμαχών
2. Επιθέσεις προκληθείσες από ιστορικά γεγονότα και επετείους

Κεφάλαιο 14: Στρατηγική Κυβερνοπολέμου και οι πέντε πυλώνες κοινωνικής σταθερότητας

Σύμφωνα με τον Waldo η κοινωνική και κυβερνητική σταθερότητα εδράζονται σε πέντε πυλώνες. Στη στρατηγική του κυβερνοπολέμου είναι κρίσιμης σημασίας η διαφορά οποιουδήποτε από τους πυλώνες αυτούς που οδηγεί και στη καταστροφή των υπολοίπων. Στη προσέγγιση της στρατηγικής ενός κυβερνοπολέμου είναι σημαντικό να κατανοηθεί πως δεν μπορεί να διεξαχθεί από περιστασιακές επιθέσεις αλλά με τη χρήση συστηματικών αποσταθεροποιητικών επιθέσεων εναντίων του στόχου.

1. Νομιμοποίηση: αφορά την πίστη που εκφράζεται στην ικανότητα μίας κυβέρνησης να διοικεί. Για να αποκτήσει μία κυβέρνηση ισχυρή νομιμοποίηση οφείλει να προβάλλει, να υπόσχεται και να φέρνει θετικό αποτέλεσμα στη ζωή των πολιτών. Μία κυβερνοεπίθεση εναντίων αυτού του πυλώνα προσδοκά στο να δημιουργήσει μία αρνητική εικόνα για το μέλλον του πληθυσμού δημιουργώντας έτσι την αίσθηση πως η κυβέρνηση της χώρας στερείται κυβερνησιμότητας και πως το ισχύον καθεστώς δημιουργεί δυσκολίες στους πολίτες (Kallberg 2015).
2. Εξουσία: στα ολοκληρωτικά καθεστώτα η εξουσία εκλαμβάνεται ως η αποδοχή του καθεστώτος τη κάθε περίοδο. Η εξουσία και η ιεραρχία συνδέονται όταν η δομή της ιεραρχίας καθορίζει την εξουσία της κάθε θέσης. Εάν η ιεραρχία εκλείψει τότε δεν υπάρχει ηγεσία που να μπορεί να θεωρηθεί υπεύθυνη για τις πράξεις της και μοιραία τότε κάθε οργανισμός και δομή καταλήγει στην αναρχία (Kallberg 2015).
3. Θεσμική γνώση: μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζει μία κυβέρνηση είναι η διαχείριση της γνώσης. Στη περίπτωση που οι δημόσιοι λειτουργοί αποτύχουν να διαχειριστούν τη ροή της γνώσης και της πληροφόρησης τότε η κοινή γνώμη σχηματίζει την εντύπωση πως η κυβέρνηση είναι ανίκανη κάτι που αποτελεί μία έμμεση πρόκληση στην εξουσία της. Η αφθονία της πληροφορίας που διαχέεται σε όλα τα επίπεδα είναι πλέον υπερβολική και η γνώση διαχέεται μέσω του δημοσίου τομέα μέσα από έγγραφα, ενέργειες, έρευνες, δημοσιεύσεις και πολιτικές. Η αύξηση αυτή της γνώσης επιφέρει την ανάγκη για ειδίκευση η οποία με τη σειρά της δημιουργεί το πρόβλημα του συντονισμού της πληροφορίας. Εάν η έλλειψη γνώσης και συντονισμού επηρεάσει τους πολίτες υπονομεύει την θέση της κυβέρνησης. Οι κυβερνοεπιθέσεις που σαν στόχο τους έχουν τη θεσμική γνώση καταστρέφουν τη γραφειοκρατική δομή του κράτους και δημιουργούν αίσθημα θυμού στον πληθυσμό (Kallberg 2015).
4. Γραφειοκρατικός Έλεγχος: κάθε οργανισμός που μεγαλώνει σε μέγεθος και πολυπλοκότητα αντιμετωπίζει προβλήματα γραφειοκρατικής φύσης. Ο έλεγχος μπορεί επίσης να χαθεί λόγω έλλειψης συντονισμού μεταξύ φορέων, τοπικών και πολιτειακών κυβερνήσεων και άλλων ενδιαφερόμενων μερών και καθώς μία κυβέρνηση χάνει τον έλεγχο των οργανισμών της χάνεται και η δικαιοδοσία της. Παράλληλα η επέκταση της γραφειοκρατίας επεκτείνει και τα ζητήματα ελέγχου καθώς ο έλεγχος απαιτεί συντονισμό, ενώ τα ζητήματα ελέγχου μπορεί να προκύψουν λόγω ακούσιων λαθών. Στη περίπτωση απώλειας του ελέγχου επέρχονται η διαφθορά, ο νεποτισμός, η δημόσια κλοπή που οδηγούν στη λαϊκή δυσαρέσκεια (Kallberg 2015).

5. Εμπιστοσύνη: στην ανάλυση του Waldo οι έννοιες της ασφάλειας και της εμπιστοσύνης συγχέονται. Όταν οι πολίτες νιώθουν ασφάλεια, τότε έχουν εμπιστοσύνη και είναι αισιόδοξοι για το μέλλον τους και για την υποστήριξη που τους παρέχει η κυβέρνηση και έχουν εμπιστοσύνη στην κυβέρνησή τους και τις υποσχέσεις της. Σημάδια συστηματικής αποτυχίας και προβαλλόμενης ανικανότητας βλάπτουν την εμπιστοσύνη προς τη κυβέρνηση (Kallberg 2015).

Κεφάλαιο 15: Κυβερνοεπιθέσεις και Εθνική Ασφάλεια

Το 1948 διατυπώθηκε από τον Hans Morgenthau πως η εθνική ασφάλεια εξαρτάται από την ακεραιότητα των συνόρων και των θεσμών ενός κράτους. Παρά το γεγονός πως η ισχυρότερη απειλή για ένα κράτος παραμένει η άμεση στρατιωτική σύγκρουση, η ψηφιοποίηση των κρίσιμων υποδομών και η σύνδεσή τους στο διαδίκτυο δημιουργεί μία νέα υπόσταση στους κινδύνους που αντιμετωπίζει η εθνική ασφάλεια. Το 2000 ο Richard Clarke για να περιγράψει τον διαφαινόμενο κίνδυνο που θα αποτελούσε η κυβερνοκατασκοπεία και το κυβερνοέγκλημα εισήγαγε την ιδέα του ψηφιακού Περλ Χάρμπορ. Οι ελάχιστες προϋποθέσεις ψηφιακής εθνικής ασφαλείας διατυπώνονται μέσα από τρία ερωτήματα (Geers 2009):

1. Πόσο εξαρτημένες είναι οι κρίσιμες υποδομές ενός κράτους από τεχνολογίες πληροφοριών
2. Σε ποιο βαθμό η τεχνολογία πληροφοριών είναι συνδεδεμένη (και εξαρτώμενη) από το διαδίκτυο
3. Σε θεωρητικό, επίπεδο πως θα μοιάζει η πιο επιτυχημένη κυβερνοεπίθεση εναντίων των υποδομών και ένα αυτή θα λάβει διαστάσεις εθνικής απειλής ασφάλειας

Κεφάλαιο 16: Στόχοι-Επιπτώσεις

Σημαντικό κίνητρο για τη διεξαγωγή ασύμμετρων επιχειρήσεων όπως οι κυβερνοεπιθέσεις αποτελεί η δυνατότητα ομάδες να μπορούν να θέσουν με απλά και φθηνά μέσα, μεγάλες δυνάμεις και να προκαλέσουν προβλήματα σε αυτές. Υπολογίζεται μέσα σε ένα διάστημα διετίας με κόστος 50 εκατομμυρίων και τη συνδρομή περίπου 600 ατόμων μπορεί να σχεδιαστεί μία κυβερνοεπίθεση που θα παραλύσει τις ΗΠΑ, οι οποίες διαθέτουν 700 δισεκατομμύρια το χρόνο στην άμυνά τους (Cornish, Livingstone, Clemente, Yorke 2010).

16.1 Παρακώλυση πληροφοριών:

Βασικός στόχος του επιτιθέμενου είναι η παρεμπόδιση της εισόδου σε σημαντικές πληροφορίες μίας κυβερνητικής υπηρεσίας ή άλλου οργανισμού (Uma, Padmanavathi 2013), με στόχο την υιοθέτηση αποφάσεων βασιζόμενες σε πληροφορίες που έχουν σκοπίμως παραποιηθεί (Geers 2010).

16.2 Αντιμετώπιση των μέτρων ασφαλείας:

Κάθε επίθεση αποσκοπεί στο να υπερνικήσει τα μέτρα εκείνα έχουν θεσπιστεί από τη διεθνή κοινότητα για την αποτροπή ή τη μείωση της πιθανότητας εκδήλωσης μίας κυβερνοεπίθεσης. Για να επιτευχθεί ο σκοπός αυτός οι χάκερ δημιουργούν πολυπλοκότερα συστήματα ή εναλλακτικά κρύβουν το κακόβουλο λογισμικό μέσα σε μία λειτουργία επιχειρώντας να προσπελάσουν τα συστήματα ασφαλείας (Uma, Padmavathi 2013)..

16.3 Επιβράδυνση της διαδικασίας λήψης αποφάσεων:

Μία κυβερνοεπίθεση μπορεί να διαδραματίσει σημαντικό ρόλο στη παρεμπόδιση της λειτουργίας κρίσιμων τομέων όπως είναι οι υπηρεσίες έκτακτης ανάγκης και ο στρατός οδηγώντας έτσι σε απώλειες και στρατιωτικές ήττες (Uma, Padmavathi 2013).

16.4 Αδυναμία παροχής δημόσιων υπηρεσιών:

Αποκλείοντας την πρόσβαση των εξουσιοδοτημένων χρηστών στις πληροφορίες οποιουδήποτε οργανισμού ή κυβέρνησης που σχετίζεται με δημόσιες υπηρεσίες, οι επιτιθέμενοι μπορούν να προκαλέσουν διαταραχές σε τομείς όπως τραπεζικές υπηρεσίες, σιδηροδρομικές και αεροπορικές υπηρεσίες, χρηματιστήρια (Uma, Padmavathi 2013).

16.5 Μείωση της εμπιστοσύνης:

Λόγω της κλοπής των πληροφοριών η κοινή γνώμη αίρει την εμπιστοσύνη της για την ασφάλεια που παρέχει ένας οργανισμός (Uma, Padmavathi 2013).

16.6 Μείωση του γοήτρου:

Αποτελεί και τον βασικότερο στόχο των επιθέσεων καθώς οι τεχνολογική ανάπτυξη προσφέρει δυνατότητες σε διάφορα κράτη γεγονός που με τη σειρά του ενδυναμώνει το γόητρο τους έναντι άλλων αναπτυσσόμενων κρατών. Το γόητρο αυτό μπορεί να πληγεί όταν τα δίκτυα μίας χώρας διαταράσσονται από κυβερνοεπιθέσεις (Uma, Padmavathi 2013).

16.7 Κατασκοπεία:

Αποτελεί έναν στόχο μίας κυβερνοεπίθεσης καθώς δίδεται η δυνατότητα να υποκλαπούν μεγάλες ποσότητες ηλεκτρονικών δεδομένων και επικοινωνιών συμπεριλαμβανομένων ευαίσθητων πληροφοριών στρατιωτικής και πολιτικής φύσης. Οι επιχειρήσεις κατασκοπείας μπορούν να διεξαχθούν από οπουδήποτε στο πλανήτη και δύνανται να διαρρήξουν ακόμα και τα ισχυρότερα πληροφορικά συστήματα. (Geers 2010). Η οικονομική κατασκοπεία αποτελεί μία διάσταση της και ένα από τα ισχυρότερα κίνητρα των κυβερνοεπιθέσεων και υπολογίζεται πως κόστισαν 19 δισεκατομμύρια το 2012. Η κλοπή πνευματικής ιδιοκτησίας και επιχειρηματικών στρατηγικών από έτερα κράτη οδηγεί τις εταιρείες σε απώλεια όχι μόνο πολύτιμων ιδιωτικών πληροφοριών αλλά και σε δικαστικούς κινδύνους, ζημιές στη φήμη, φυγή επενδυτών και πελατών. Οι κυριότερες επιπτώσεις της οικονομικής

κατασκοπείας ωστόσο αφορούν την απώλεια του ανταγωνιστικού πλεονεκτήματος μίας οικονομίας συνολικά. (Carlin 2016).

16.8 Αντικατασκοπεία:

Ένα σημαντικό κίνητρο για τις κυβερνοεπιθέσεις καθώς συχνό είναι το φαινόμενο να υποκλέπτονται προσωπικές πληροφορίες δημοσίων υπαλλήλων ή ανάδοχων έργων του δημοσίου που αναγκαστικά έχουν παράσχει τις πληροφορίες αυτές στη κυβέρνησή τους. Οι δράντες των επιθέσεων χρησιμοποιούν τις υποκλεμμένες αυτές πληροφορίες με σκοπό τον εκβιασμό ή ακόμα και τη στρατολόγηση δημοσίων λειτουργών με στόχο να εξυπηρετήσουν τους σκοπούς τους. Υπολογίζεται πως στις ΗΠΑ έχουν υποκλαπεί με αυτό τον τρόπο οικονομικά, ιατρικά, επαγγελματικά και προσωπικά στοιχεία 21.5 εκατομμυρίων πολιτών, εκ των οποίων πολλοί βρίσκονται σε υψηλόβαθμες κυβερνητικές θέσεις, εκ των οποίων τα δύο εκατομμύρια αποτελούσαν μέλη των οικογενειών τους. (Carlin 2016).

16.9 Προπαγάνδα:

Μία άλλη διάσταση των επιθέσεων σχετίζεται με τη προπαγάνδα καθώς η διάχυσή της μέσω του κυβερνοχώρου αποτελεί ένα φθηνό αλλά αποτελεσματικό μέσο και θεωρείται ως η ισχυρότερη μορφή επίθεσης. Η ψηφιακή πληροφορία που μπορεί να λάβει τη μορφή εικόνας ή και κειμένου και που μπορεί να είναι αληθής η κατασκευασμένη αντιγράφεται και αποστέλλεται προς οποιοδήποτε σημείο. Ακόμα και πληροφορίες που έχουν λογοκριθεί από το διαδίκτυο μπορούν να κάνουν την εμφάνισή τους (Geers 2010).

16.10 Μονάδες Υγείας:

Μία από τις πτυχές των επιπτώσεων των κυβερνοεπιθέσεων στη πολιτική σταθερότητα, αποτελούν και οι επιθέσεις που στρέφονται κατά νοσοκομείων και μονάδων υγείας. Οι υποδομές αυτές αποτελούν στόχο χάκερ εδώ και πολλά χρόνια αλλά το φαινόμενο εντάθηκε με το ξέσπασμα της πανδημίας του COVID-19. Η εξήγηση πίσω από τις επιθέσεις δεν είναι άλλη από το γεγονός πως οι μονάδες υγείας διαθέτουν στις βάσεις δεδομένων τους ευαίσθητες και εμπιστευτικές πληροφορίες που μοιράζονται μεταξύ ιατρού και ασθενή. Παράλληλα τα συστήματα προστασίας των μονάδων υγείας συνήθως είναι ανεπαρκή οπότε και είναι ευαίσθητα προς κάθε μορφή κυβερνοεπίθεσης. Είναι επομένως σαφές πως η αδυναμία ενός νοσοκομείου να έχει γρήγορη πρόσβαση σε αρχεία που αφορούν φαρμακευτικές συνταγές, οδηγίες χειρουργικών επεμβάσεων και πρωτόκολλα θεραπείας μπορεί να θέσει σε κίνδυνο ακόμα και τη ζωή των ασθενών. Επιπρόσθετα η εμπειρία των κυβερνοεπιθέσεων κατά τη διάρκεια της πανδημίας του COVID-19 και η στόχευση εταιρειών που μετείχαν στη παραγωγή και διανομή των εμβολίων της νόσου καταδεικνύει τη πολιτική και κοινωνική επίπτωση που μπορούν να έχουν οι κυβερνοεπιθέσεις (Minaar 2022).

16.11 Εφοδιαστική Αλυσίδα:

Η εθνική ασφάλεια ενός κράτους μπορεί να βρεθεί σε κίνδυνο από μία κυβερνοεπίθεση όταν αυτή στοχεύει σε υποδομές και εφοδιαστικές αλυσίδες

κρίσιμων προϊόντων. Ένα τέτοιο παράδειγμα αποτελεί η επίθεση με ransomware έναντι της Colonial Pipeline το 2021. Η ομάδα Dark Side πραγματοποίησε την επίθεση κρυπτογραφώντας τους υπολογιστές της εταιρίας, απαιτώντας λύτρα για να τους ξεκλειδώσει. Οι συνέπειες της επίθεσης περιλάμβαναν ελλείψεις σε καύσιμα κατά μήκος της ανατολικής ακτής των ΗΠΑ κάτι που οδήγησε σε πανικό τους καταναλωτές ενώ δημιουργήθηκε σοβαρή οικονομική αναστάτωση (Sharma 2024).

16.12 Δίκτυα Επικοινωνίας:

Κομβικής σημασίας για τη λειτουργία ενός κράτους αποτελούν τα δίκτυα επικοινωνίας. Ο ρόλος τους αυτός τα κατατάσσει στους πιθανούς στόχους των κυβερνοεπιθέσεων. Κατά τη διάρκεια της κρίσης του 2000 μεταξύ Ισραήλ και Λιβάνου οπότε και αλληπάλληλες επιθέσεις χάκερ τόσο ισραηλινών όσο και φιλοπαλαιστινίων έλαβαν χώρα, στοχεύθηκε μεταξύ άλλων και ο τηλεπικοινωνιακός φορέας AT&T έγινε στόχος χάκερ λόγω της υποστήριξης που παρείχε στην ισραηλινή κυβέρνηση (Geers 2009).

16.13 Δίκτυο Ηλεκτροδότησης:

Η παγκόσμια διασύνδεση παρέχει μεγάλες ευκαιρίες για τη διαφοροποίηση του παγκόσμιου τοπίου και τη διατήρηση της καθημερινότητας του πληθυσμού. Ο κυριότερος στόχος προς αυτή τη κατεύθυνση δεν είναι άλλος από τα δίκτυα ηλεκτροδότησης, τα οποία σχεδιάστηκαν πριν από την ψηφιακή περίοδο. Βέβαια για το λόγο αυτό ανακατασκευάστηκαν έτσι ώστε να λειτουργούν στη ψηφιακή εποχή πλην όμως με τρόπο που άφησε σοβαρά κενά ασφαλείας. Είναι σαφές λοιπόν πως η διαδικασία εκσυγχρονισμού παρά την αύξηση της αποδοτικότητας του δικτύου προϋπόθεσε την σύνδεση του με το διαδίκτυο και συσκευές που το έκαναν ευάλωτο σε ενδεχόμενο κυβερνοεπίθεσης. Παράδειγμα μίας τέτοιας επίθεσης απόρροιας των κενών ασφάλειας του συστήματος αποτελεί η διακοπή ρεύματος στην Ουκρανία τον Δεκέμβριο του 2015 που επηρέασε 200.000 πολίτες και οφειλόταν σε κυβερνοεπίθεση. Τα συστήματα βιομηχανικού ελέγχου σαφώς είναι απαραίτητα για τη μείωση του κόστους παραγωγής αλλά πολλά από αυτά δεν διαθέτουν την απαραίτητη κρυπτογράφηση και έλεγχο ταυτότητας, γεγονός που σύμφωνα με το NSA ελκύει εισβολές στα συστήματα ελέγχου που μέχρι στιγμής αφορούν την αναγνώριση και κατανόηση των συστημάτων αυτών. Ωστόσο κρατικοί και μη κρατικοί δράστες διαθέτουν ήδη τη δυνατότητα να παρεμβληθούν και να διακόψουν βασικές υποδομές όπως δίκτυα ηλεκτρικής ενέργειας, συστήματα αστικής μαζικής μεταφοράς, εναέριας κυκλοφορίας τον έλεγχο και τα δίκτυα διανομής πετρελαίου και φυσικού αερίου (Geers 2010).

16.14 Επιχειρήσεις και Οικονομία:

Οι οικονομικές ζημιές που προκαλούνται από τις κυβερνοεπιθέσεις έχουν ένα σαφές αποτύπωμα και στη κοινωνική δομή. Εργαζόμενοι μπορούν να χάσουν την δουλειά τους ενώ οι πληγείσες εταιρίες εισφέρουν λιγότερους φόρους λόγω του μικρότερου κύκλου εργασιών που έχουν εξαιτίας των επιθέσεων. Παράλληλα οι απολυμένοι υπάλληλοι πληρώνουν με τη σειρά τους λιγότερους φόρους και υποστηρίζονται από

κυβερνητικά επιδόματα και οι δήμοι χάνουν έσοδα εξαιτίας της αδυναμίας των ιδιοκτητών να πληρώσουν φόρους ακινήτων. Μπορεί να λεχθεί δηλαδή πως οι κυβερνοεπιθέσεις δύνανται να προκαλούν μικρότερες σε βαθμό αλλά ανάλογες συνέπειες με μία οικονομική κρίση (MacDonnell Ulsch 2014). Ένα μεγάλο πεδίο διεξαγωγής κυβερνοεπιθέσεων αποτελεί η στόχευση μικρών επιχειρήσεων. Ειδικότερα στις ΗΠΑ αποτελεί ένα διαδεδομένο φαινόμενο με το 73% των ιδιοκτητών να δηλώνει πως έχει πέσει θύμα κυβερνοεπίθεσης. Ο οικονομικός αντίκτυπος είναι άμεσος με τις απώλειες να υπολογίζονται σε 2.5 δισεκατομμύρια ωστόσο οι έμμεσες συνέπειες είναι που αποτελούν το συστημικό κίνδυνο για την οικονομία και τη σταθερότητα καθώς αποθαρρύνουν τη διενέργεια συναλλαγών -το 55% του πληθυσμού των ΗΠΑ αποθαρρύνεται σύμφωνα με έρευνα-, ενώ ιδιαίτερα πλήττεται ο τραπεζικός τομέας (Hossain, Hassan 2024).

16.15 Χρηματοπιστωτικό σύστημα:

Οι κυβερνοεπιθέσεις φαίνεται πως επηρεάζουν μεταξύ άλλων και τη σταθερότητα των χρηματοπιστωτικών αγορών. Είναι χαρακτηριστικό δε πως ο μεγάλος βαθμός στον οποίο αυτές έχουν διασυνδεθεί σε παγκόσμια κλίμακα τις καθιστά ιδιαίτερα ευάλωτες στο ενδεχόμενο μίας κυβερνοεπίθεσης καθώς στο ενδεχόμενο της εκδηλώσεως της κυβερνοεπίθεσης οι αγορές μπορούν να αντιμετωπίσουν σοβαρές διακοπές της λειτουργίας τους γεγονός που οδηγεί σε οικονομικές απώλειες και στην απώλεια της εμπιστοσύνης των επενδυτών προς αυτές. Συνηθέστερα επιθέσεις DDoS καθιστούν αδύνατες τις χρηματικές συναλλαγές, ενώ επίσης κακόβουλα λογισμικά malware και ransomware παραλύουν τα τραπεζικά συστήματα για την επαναλειτουργία των οποίων απαιτούνται νέες επενδύσεις. Το δεύτερο σκέλος των επιπτώσεων στο χρηματοπιστωτικό τομέα αυτό της απώλειας εμπιστοσύνης θεωρείται και η σημαντικότερη επίπτωση σε όρους σταθερότητας καθώς η απομάκρυνση κεφαλαίων που αυτή συνεπάγεται οδηγεί σε μειωμένη επενδυτική δραστηριότητα και πιθανότητα ύφεσης. Παράλληλα αναγκάζει τα ιδρύματα να αυξήσουν τα κόστη λειτουργίας τους επενδύοντας σε τεχνολογίες ασφάλειας. Χαρακτηριστικά παραδείγματα επιθέσεων με στόχο τον χρηματοπιστωτικό τομέα αποτελούν οι επιθέσεις στη JPMorgan Chase το 2014 και αυτή ενάντια στο σύστημα SWIFT το 2016. Ιδιαίτερα στη δεύτερη περίπτωση επλήγη το σύστημα μέσω του οποίου διακινούνται οι διεθνείς τραπεζικές συναλλαγές οι οποίες και προστατεύονται από τα πλέον εξελιγμένα συστήματα ασφαλείας (Sugrowka, Malobodry ,Nastaj-Salek, Cyrkun 2024). Οι επιθέσεις ενάντια σε οικονομικά και τραπεζικά ιδρύματα συνηθέστερα αποτελεί προϊόν κυβερνοεγκλήματος και έχει ως κύριο κίνητρο τον προσπορισμό οικονομικού οφέλους, ωστόσο η συστηματική στόχευση τέτοιων θεσμών δύναται να αποτελέσει κίνδυνο για το εθνικό ισοζύγιο και να έχει σοβαρές επιπτώσεις για τη βιομηχανία και κοινωνία επηρεάζοντας έτσι την ασφάλεια και τη σταθερότητα ενός κράτους. Υπολογίζεται πως η ζημία ανέρχεται σε 1 τρισεκατομμύριο δολάρια το χρόνο σε διεθνές επίπεδο (Cornish, Livingstone, Clemente Yorke 2010).

16.16 Ευαίσθητα δεδομένα:

Τον Ιούλιο του 2015, λεπτομέρειες για 33 εκατομμύρια λογαριασμούς και προσωπικές πληροφορίες σχετικά με άτομα που είναι εγγεγραμμένα στο Ashley Madison, έναν ιστότοπο που διευκολύνει εξωσυζυγικές σχέσεις, διέρρευσαν. Το επιχειρηματικό μοντέλο του Madison ήταν το απόρρητο και η ασφάλεια, μέσω των οποίων θα χτίσουν μια σχέση εμπιστοσύνης με τους πελάτες τους (Agrafiotis 2018).

16.17 Πολιτικά κίνητρα:

Οι κυβερνοεπιθέσεις χρησιμοποιούνται για τον πολιτικό εκφοβισμό ή και εξαναγκασμό. Οι στρατηγικές του Ιράν και της Βορείου Κορέας στο τομέα του κυβερνοχώρου θεωρούνται ζωτικής σημασίας για τη προώθηση των πολιτικών τους επιδιώξεων. Χαρακτηριστικό παράδειγμα αποτελεί η επίθεση εναντίων της Sony Pictures Entertainment που όχι μόνο κατέστρεψε συστήματα της εταιρείας αλλά υπέκλεψε πνευματικά δικαιώματα και προσωπικές πληροφορίες ενώ πελάτες, εργαζόμενοι της εταιρείας και παραγωγοί απειλήθηκαν βιαίως. Η κλοπή δεδομένων έφτασε τα 100 terabyte δεδομένων που μεταξύ άλλων αφορούσαν και 47.000 κωδικούς κοινωνικής ασφάλισης. Η ομάδα που ήταν πίσω από αυτή την επίθεση ονομαζόταν Guardians of Peace και το κίνητρό της ήταν η προβολή της ταινίας The Interview μίας σατυρικής ταινίας για τον ηγέτη της Βορείου Κορέας Kim Jong Un. Η επίθεση κατάφερε να ακυρώσει την προβολή της ταινίας. Ο πολιτικός εξαναγκασμός μέσω των κυβερνοεπιθέσεων δεν λαμβάνει χώρα μόνο από κρατικούς δρώντες καθώς τρομοκρατικές οργανώσεις χρησιμοποιούν τα ίδια εργαλεία για να υπονομεύσουν την απόδοση στρατιωτικών και ιδιωτικών συστημάτων. Οι συγκρούσεις στη Συρία και το Ιράκ έδωσαν την ευκαιρία για τέτοιες επιθέσεις όπως έγινε τον Ιούνιο του 2015 οπότε η ομάδα με το όνομα Συριακός Ηλεκτρονικός Στρατός ανέλαβε την ευθύνη για την επίθεση στη σελίδα Army.mil (Carlin 2016).

16.18 Ψυχολογικές επιπτώσεις:

Λόγω της απουσίας ερευνητικών δεδομένων για τις ψυχολογικές επιπτώσεις των κυβερνοεπιθέσεων η ανάλυση στρέφεται σε δεδομένα εξαγόμενα από το κυβερνοέγκλημα και την τρομοκρατία εν γένει. Θύματα του κυβερνοεγκλήματος αναφέρουν πως βίωσαν συναισθηματική δυσφορία, που υποδηλώνει μια αίσθηση ηθικού πανικού, θυμού, φόβου, άγχους, δυσπιστίας και απώλειας αυτοπεποίθησης. Παράλληλα οι επιπτώσεις περιλαμβάνουν σε μία ευρύτερη κλίμακα την απώλεια τη αίσθησης ασφαλείας που αυξάνουν με τη σειρά τους το αίσθημα της ανασφάλειας και δημιουργούν τη τάση για υποστήριξη σκληροπυρηνικών πολιτικών. Οι μελέτες σε περιπτώσεις τρομοκρατίας (δίδυμοι πύργοι και βομβιστικές επιθέσεις στην Οκλαχόμα) έδειξαν πως τα υποκείμενα που εξετάθηκαν στα γεγονότα παρουσίασαν μεγαλύτερα επίπεδα άγχους (όπως μετρήθηκε από το επίπεδο της κορτιζόλης) από υποκείμενα που δεν έχουν δεν εκτεθεί σε ανάλογα περιστατικά. Αναλογικά αναμένουμε την παρουσίαση ίδιων συμπτωμάτων και στα θύματα κυβερνοεπιθέσεων, ενώ δημιουργούν το αίσθημα της διαδικτυακής αβεβαιότητας που μεταφράζεται σε φόβο για την ίδια τη πορεία της κοινωνίας και τη συνολική ασφάλεια (Canetti, Gross, Waismel-Manor, Levanon, Cohen 2017). Η ψυχολογική

πίεση που μπορεί να προκληθεί από τις κυβερνοεπιθέσεις στους πολίτες δύναται να διαμορφώσει και την ίδια την εξωτερική πολιτική μίας χώρας. η διαμόρφωση αυτή γίνεται σε δύο σκέλη. Σε ότι αφορά το πρώτο σκέλος έχει αποδειχθεί πως η έκθεση του κοινού σε περιστατικά κυβερνοεπιθέσεων δημιουργεί αλλαγές στην οπτική του και προκαλεί μετακινήσεις στις πολιτικές προτιμήσεις του. Παράλληλα διαβρώνεται η εμπιστοσύνη προς τους κυβερνητικούς θεσμούς και αυξάνεται η υποστήριξη για περαιτέρω επιτήρηση καθώς η δυσφορία που προκαλούν οι κυβερνοεπιθέσεις δημιουργεί τις κατάλληλες εκείνες συνθήκες για την επανεξέταση της ισορροπίας μεταξύ ιδιωτικότητας και ασφάλειας. Στο ερώτημα γιατί οι κυβερνοεπιθέσεις έχουν αυτό το αποτέλεσμα η απάντηση είναι πως εκμεταλλεύονται την αδυναμία του κυβερνοχώρου για τη σαφή και έμπιστη απόδοση του ποιος είναι ο δράστης, καθώς και την έλλειψη των απαραίτητων γνώσεων του κοινού σε συνδυασμό με το φόβο που σχετίζεται με τον κυβερνοχώρο. Οι ανωτέρω παράγοντες πλήττουν την εμπιστοσύνη της κοινωνίας προς την ασφάλεια των ψηφιακών υποδομών και την ικανότητα της κυβέρνησης πως μπορούν να αντιμετωπίσουν με τρόπο αποτελεσματικό τις καταστροφικές συνέπειες των επιθέσεων. Το ψυχολογικό αντίκτυπο που προκαλούν είναι εμφανές στις ΗΠΑ όπου το 82% της κοινής γνώμης θεωρεί τις κυβερνοεπιθέσεις ως μία κρίσιμη απειλή και τις κατατάσσει πάνω από απειλές όπως οι μεταδοτικές ασθένειες (72%), τη ρωσική στρατιωτική απειλή (44%) και την υπερθέρμανση του πλανήτη (58%). Παράλληλα ένα αντίκτυπο των επιθέσεων στη κοινή γνώμη είναι πως δημιουργεί την επιθυμία για άμεση απάντηση με στρατιωτικά μέσα ακόμα και στο ενδεχόμενο η ταυτότητα των δραστών παραμένει άγνωστη. Το κοινωνικό αντανάκλαστικό αυτό προκαλείται από τη κοινωνική οργή και αντιτίθεται στη πολιτική της μη κλιμάκωσης στο κυβερνοχώρο που συνήθως υιοθετείται. Είναι σαφές επομένως συμπέρασμα πως πράξεις πολιτικής βίας καθορίζουν την στάση της κοινής γνώμης, πως όμως η κοινωνική πίεση διαμορφώνει την εξωτερική πολιτική. Στο ερώτημα αυτό δεν υπάρχει βέβαιη απάντηση, ωστόσο υπάρχει η γενικότερη συμφωνία στη βιβλιογραφία πως η κοινή γνώμη αποτελεί παράγοντα επιρροής στις αποφάσεις για την ανάληψη στρατιωτικής δράσης. Κλασσικό παράδειγμα του μοτίβου αυτού ο δεύτερος πόλεμος του κόλπου, για τον οποίο θεωρείται πως η ανάγκη της αμερικάνικης κοινής γνώμης για αντίποινα έσπρωξε την κεντρική κυβέρνηση στη κατεύθυνση του πολέμου. Ιδιαίτερα στην περίπτωση των κυβερνοεπιθέσεων παρατηρείται το παράδοξο πως ενώ αυτές θα εκληφθούν από μία κυβέρνηση ως πράξη αποκλιμάκωσης της έντασης, η κοινή γνώμη θα πανικοβληθεί και θα υπερτιμήσει την καταστροφική δυνατότητα των επιθέσεων και θα πιέσει προς την κατεύθυνση της στρατιωτικής κλιμάκωσης. Η τάση αυτή μπορεί να εξηγηθεί από το γεγονός πως οι κυβερνοεπιθέσεις αποτελούν ένα νέο φαινόμενο οπότε και δεν υπάρχει η απαραίτητη εμπειρία και συμφωνία για το πως θα πρέπει να αντιμετωπίζονται (Shandler, Gross, Canetti 2023).

16.19 Social Media και πολιτική αναταραχή:

Το διαδύκτιο και τα Social Media έχουν τη δυνατότητα να φέρνουν σε επαφή μεγάλους αριθμούς ακτιβιστών είτε στη ψηφιακή σφαίρα είτε δίνοντας το έναυσμα για να συγκεντρωθούν και να διαμαρτυρηθούν όπως έγινε σε περιπτώσεις που τα

Social Media κάλεσαν σε διαμαρτυρία εναντίων οργανισμών όπως οι G-8, G-20, και ο Παγκόσμιος Οργανισμός Εμπορίου. Η αραβική άνοιξη που διεξήχθη σε χώρες όπως η Τунησία, η Αίγυπτος, το Μαρόκο, η Συρία, η Λιβύη, η Δυτική Σαχάρα, το Τζιμπουτί, το Σουδάν, η Υεμένη, η Σαουδική Αραβία, η Παλαιστίνη και το Ιράκ και κατέληξε στην ανατροπή πολλών καθεστώτων μας δίνει ένα σαφές παράδειγμα για τη δυνατότητα των Social Media συντονίσουν και να προκαλέσουν πολιτικές αναταραχές. Ο κίνδυνος ενέχεται στο ερώτημα ποιος μπορεί να επηρεάσει τα Social Media και προς ποιο σκοπό. Είναι γνωστό επίσης πως τρομοκρατικές ομάδες τα χρησιμοποιούν για να επιτύχουν τους σκοπούς τους, αλλά σε ότι αφορά το κομμάτι του κυβερνοπολέμου εστιάζουμε σε ομάδες χάκερ όπως οι Anonymous, που έχουν ως εφελκυστικό τη δικιά τους οπτική για τη δικαιοσύνη χρησιμοποίησαν τα Social Media για να υποστηρίξουν πολιτικόκοινωνικά κινήματα όπως τη κίνηση Occupy, ενώ έχουν στοχεύσει με τις επιθέσεις τους κυβερνήσεις (ΗΠΑ, Ισραήλ, Ουγκάντα, Τунησία) αλλά και τις αστυνομικές αρχές σε πολιτείες των ΗΠΑ (MacDonnell Ulsch 2014) .

Κεφάλαιο 17: Καθεστώτα και Κυβερνοεπιθέσεις – Η περίπτωση της Ρωσίας

Σε ότι αφορά το ερώτημα του κατά πόσο η φύση ενός καθεστώτος επηρεάζει την εμπλοκή του σε πολέμους γενικότερα και στη διεξαγωγή κυβερνοεπιθέσεων ειδικότερα δεν μπορεί να δοθεί σαφής απάντηση. ένα σύνολο ερευνών αποκάλυψε ότι όσο πιο δημοκρατικά είναι τα κράτη, είναι και λιγότερο πιθανό να εμπλακούν σε διακρατικούς πολέμους και συγκρούσεις λόγω της παρουσίας δημοκρατικών θεσμών και μεγαλύτερης συμμετοχής των πολιτών στη διαδικασία λήψης πολιτικών αποφάσεων. Σύμφωνα με αυτή τη λογική, τα δημοκρατικά κράτη θα πρέπει να είναι λιγότερο πιθανό να ξεκινήσουν κυβερνοεπιθέσεις λόγω των εγχώριων δημοκρατικών κανόνων τους και της συμμετοχής τους σε διεθνείς θεσμούς που ενθαρρύνουν περισσότερο συνεργατική συμπεριφορά στην εξωτερική πολιτική. Ένα εναλλακτικό σώμα της λογοτεχνίας έχει διαπιστώσει ότι η δημοκρατία δεν παράγει πιο ειρηνική εξωτερική πολιτική (Rosato 2003). Σύμφωνα με ορισμένους μελετητές, οι δημοκρατίες είναι το ίδιο επιρρεπείς σε συγκρούσεις όσο και τα πιο συγκεντρωτικά καθεστώτα. (Chan 1984; Weede 1984; MacMillan 2003). Παράλληλα παράγοντες όπως οι γεωπολιτικές ανησυχίες, η ισχύς, η κατανομή των πόρων και οι εδαφικές αντιπαλότητες είναι πιθανότερο να επηρεάζουν την πιθανότητα σύγκρουσης μεταξύ κρατών (Mearsheimer 2001). Σύμφωνα με αυτό το σκέλος της λογοτεχνίας, οι ρεαλιστικοί, στρατηγικοί παράγοντες είναι πιο σημαντικοί στον επηρεασμό της κρατικής συμπεριφοράς από την παρουσία της δημοκρατίας. Αν εφαρμόσουμε αυτή τη λογική στις κυβερνοσχέσεις, οι δημοκρατίες θα πρέπει να είναι εξίσου πιθανό να ξεκινήσουν με αυταρχικά κράτη κυβερνοεπιθέσεις που χρηματοδοτούνται από το κράτος. Μια τρίτη πιθανή υπόθεση είναι ότι τα δημοκρατικά κράτη μπορεί να είναι πιο πιθανό να ξεκινήσουν κυβερνοεπιθέσεις καθώς οι κυβερνοεπιθέσεις θα μπορούσαν να είναι ένα εναλλακτικό εργαλείο στη φυσική και στρατιωτική εμπλοκή. Οι κυβερνοεπιθέσεις είναι συχνά συγκαλυμμένες και η απόδοση είναι δύσκολη (Valeriano, Jensen και Manes 2018). Έτσι, σε πολλές περιπτώσεις, η χρήση μιας κυβερνοεπίθεσης θα μπορούσε να είναι μια λιγότερο δαπανηρή τακτική από ό άμεση

στρατιωτική εμπλοκή και τα δημοκρατικά κράτη θα μπορούσαν να δουν επιθετικές επιχειρήσεις στον κυβερνοχώρο ως πιο ελκυστική στρατηγική από τις φυσικές στρατιωτικές επιχειρήσεις (Hunter 2022).

Τα μέσα άσκησης της εξωτερικής πολιτικής της Ρωσίας διαιρούνται σε έξι κατηγορίες: διακυβέρνηση, οικονομία και ενέργεια, πολιτική και πολιτική βία, στρατιωτική ισχύς, διπλωματία και δημόσια ενημέρωση και αφηγηματικό πόλεμο. Σε συνδυασμό με τα παραδοσιακά αυτά μέσα η Ρωσία χρησιμοποιεί σαν όπλα πτυχές όπως ο πολιτισμός, η ιστορία, ο εθνικισμός, τα μέσα ενημέρωσης και κοινωνικής δικτύωσης, το διαδίκτυο, οι επιχειρήσεις, η διαφθορά, οι προεκλογικές υποσχέσεις και η παγκοσμιοποίηση. Γενικότερα το διαδίκτυο αντιμετωπίζεται ως ένα πεδίο μάχης (Pernik 2020). Οι ρωσικές επιχειρήσεις του κυβερνοχώρου στοχεύουν τόσο στις κοινωνίες όσο και στις ελίτ των δυτικών κρατών με αποτέλεσμα να επηρεάζουν όχι μόνο τη διαμόρφωση της κοινής γνώμης, αλλά και τη διαδικασία χάραξης πολιτικής (Λιαρόπουλος 2021)

Για τη ρωσική πολιτική η ελευθερία της έκφρασης εκλαμβάνεται ως συστημική απειλή και η χρήση αυτής στο διαδίκτυο δύναται να συμβάλει στην αποσταθεροποίησή της (μέσω της υποκίνησης χρωματιστών επαναστάσεων). Για το λόγο αυτό το Κρεμλίνο αναπαράγοντας το παράδειγμα παρόμοιων συγκεντρωτικών καθεστώτων ενισχύει την παρουσία του στο κυβερνοχώρο και στις υποδομές του, με σκοπό την διεξαγωγή επιχειρήσεων τόσο αμυντικού όσο και επιθετικού προσανατολισμού. Η στόχευση της Ρωσίας είναι κυρίως πολιτικού χαρακτήρα και επικεντρώνεται σε χώρες της ΕΕ και του ΝΑΤΟ. Στη προσπάθεια αυτή διακρίνονται επτά στρατηγικές επιρροής που χρησιμοποιούνται σε χώρες που παρουσιάζουν συγκεκριμένες αδυναμίες. Για παράδειγμα η Ελλάδα και η Βουλγαρία διαθέτουν μέσα στη πολιτική και επιχειρηματική τους τάξη ομάδες φίλα προσκείμενες στη Ρωσία, ενώ παράλληλα οι δημοκρατικοί τους θεσμοί είναι ανίσχυροι. Τέτοιες χώρες η ρωσική διπλωματία επιθυμεί να τις χρησιμοποιεί ως δούρειους ίππους μέσα στην ΕΕ και το ΝΑΤΟ. Χώρες όπως η Ουγγαρία, το Μαυροβούνιο και η Ρουμανία διαθέτουν επίσης αδύναμους θεσμούς ωστόσο δεν είναι εξαιρετικά συνδεδεμένες με τη Ρωσία, οπότε αυτή τις χρησιμοποιεί σε συγκεκριμένα ζητήματα όπως λόγου χάρη για τις ευρωπαϊκές κυρώσεις εναντίων της. Οι λοιπές στρατηγικές της περιλαμβάνουν την εκμετάλλευση (Ηνωμένο Βασίλειο), τη δαιμονοποίηση (Εσθονία και Πολωνία), την αναστάτωση (Γαλλία, Γερμανία, Ολλανδία και Σουηδία), την επιρροή (Τσεχία, Ιταλία, Λετονία και Λιθουανία). Οι πρακτικές της στο κυβερνοχώρο αφορούν τη χρήση meme, bot και αφηγήσεων σε συνδυασμό με πολιτικούς και οικονομικούς παραπληροφορητές με στόχο να επηρεάσει τη κοινή γνώμη και να παρέμβει σε ζητήματα όπως οι εκλογές. Το πλεονέκτημα που προσφέρουν τα social media στις πολιτικές επιδιώξεις της Ρωσίας είναι η δυνατότητα να προσεγγίζει και να στοχεύει συγκεκριμένες πληθυσμιακές ομάδες που βρίσκονται πολύ μακριά από την ίδια ενώ δεν διακινδυνεύει μία μεγάλης έντασης κλιμάκωση. Τα μηνύματα που αποστέλλονται συνήθως εκμεταλλεύονται διχασμούς στο εσωτερικό των δυτικών κρατών που αφορούν ζητήματα όπως η παγκοσμιοποίηση, η τεχνολογική πρόοδος, ο εθνικισμός, ο φονταμενταλισμός, η μετανάστευση και η κλιματική αλλαγή (Pernik 2020).

Η ρωσική στρατηγική φαίνεται πως δεν διστάζει να στοχεύσει την Ευρώπη και τις υποδομές της. Τον Φεβρουάριο του 2022, αρκετές ευρωπαϊκές πετρελαϊκές εγκαταστάσεις έγιναν στόχος κυβερνοεπιθέσεων, αν και το κίνητρο και ο δράστης πίσω από τις επιθέσεις είναι άγνωστα. Οι νορβηγικές εγκαταστάσεις πετρελαίου και φυσικού αερίου είναι ιδιαίτερα ελκυστικές για ρωσικές υβριδικές επιθέσεις (Pillai 2023).

Το ρωσικό στρατιωτικό δόγμα χρησιμοποιεί τις δυνατότητες των κυβερνοεπιθέσεων τόσο κατά τη διάρκεια όσο και στα προπαρασκευαστικά στάδια ενός πολέμου. Το ρωσικό δόγμα συνοψίστηκε στα γραφόμενα του Valeri Gerasimov το 2013, οπότε και συνέστησε πως μη στρατιωτικές μέθοδοι μπορούν να επιτύχουν πολιτικούς και στρατηγικούς στόχους. Οι απόψεις του Gerasimov είναι γνωστές και σαν δόγμα Gerasimov (Brose 2012).

Από τα μέσα του 2000 το ρωσικό δόγμα διαιρέθηκε σε δύο βασικές οδούς

1. Information Technical: συσκευές τεχνικής νοημοσύνης, μέσα και μέτρα για την προστασία πληροφοριών, όπλα υπερυψηλών συχνοτήτων, ραδιοηλεκτρονικά αντίμετρα, όπλα ηλεκτρομαγνητικών παλμών και ειδικό λογισμικό και υλικό.
2. Information Psychological: αφορά κυρίως τη χρήση των MME και τη χρήση μη φονικών όπλων όπως ψυχοτρονικά εργαλεία και ειδικά φαρμακευτικά προϊόντα.

Ήδη από το Μάρτιο του 2014 η Ρωσία παράλληλα με τις αμιγώς στρατιωτικές επιχειρήσεις, κατάφερε να ελέγξει τη ροή πληροφοριών χρησιμοποιώντας μέσα όπως διασπορά ψευδών ειδήσεων, επίσημες κυβερνητικές δηλώσεις, βίντεο στο YouTube, μηνύματα SMS, δολιοφθορά, κυβερνοεπιθέσεις και στρατηγικά αφηγήματα. Συγκεκριμένα σε ότι αφορά τις κυβερνοεπιθέσεις η φιλορωσική ομάδα Cyberberkut απέκτησε πρόσβαση σε τηλεφωνικές ηχογραφήσεις και στην ηλεκτρονική επικοινωνία μεταξύ αξιωματούχων της Ουκρανίας, της ΕΕ και των ΗΠΑ. (Λιαρόπουλος 2021).. Ήδη πριν την επίθεση στην Ουκρανία χρησιμοποίησε το κυβερνοόπλο Foxblade στοχεύοντας 19 κυβερνητικούς στόχους και κρίσιμες υποδομές της χώρας. Η στρατηγική της όπως διαφάνηκε χωρίζεται σε τρία διαφορετικές δράσεις: κυβερνοεπιθέσεις εναντίων της Ουκρανίας, παραβίαση του δικτύου και κατασκοπεία και επιχειρήσεις επηρεασμού της κοινής γνώμης σε παγκόσμια κλίμακα. Χρονικά παρατηρούνται τρεις φάσεις της επίθεσης. Η πρώτη διήρκεσε από τον Ιανουάριο έως τον Μάρτιο του 2022, η δεύτερη μέχρι τον Σεπτέμβριο του ίδιου έτους και η τελευταία μέχρι τον Μάρτιο του 2023. Κατά τη διάρκεια των φάσεων αυτών μπορούν να εξαχθούν συμπεράσματα για το πως η Ρωσία στόχευσε την ασφάλεια και σταθερότητα της Ουκρανίας αλλά και των συμμάχων της καθώς ενέργειές της περιλάμβαναν την παρακώλυση της λειτουργίας ενεργειακών υποδομών και δικτύων ύδρευσης και την διεξαγωγή επιχειρήσεων που στόχευαν το ηθικό της ουκρανικής κοινωνίας. Πέρα από την ίδια την Ουκρανία συμμαχικές χώρες όπως η Πολωνία αντιμετώπισαν ομάδες χακτιβιστών όπως για παράδειγμα οι NoName057(16), Killnet,

και CyberArmia Ludowa που επιτέθηκαν σε ένα ευρύ φάσμα που περιελάμβανε το δίκτυο κινητής τηλεφωνίας τις φορολογικές υπηρεσίες και την αστυνομία. Πέραν της διατάραξης της λειτουργίας της χώρας οι επιθέσεις εξυπηρέτησαν και το ρωσικό αφήγημα για τον πόλεμο διαμοιράζοντας αντι-ουκρανικό προπαγανδιστικό υλικό (Wroblewski, Wisnieewski 2023).

Κεφάλαιο 18: Νομικό υπόβαθρο

18.1 Η Ηθική Διάσταση

Τα ηθικά όρια ενός συμβατικού πολέμου προβλέπονται από τη θεωρία του δίκαιου πολέμου, που περικλείει τις ηθικές αρχές διεξαγωγής του. Οι αρχές αυτές είναι δύσκολο να εφαρμοστούν στη περίπτωση του κυβερνοπολέμου, όπως συμβαίνει με την αρχή της προσφυγής στα όπλα ως έσχατης λύσης όταν όλες οι υπόλοιπες εναλλακτικές έχουν εξαντληθεί. Αντιθέτως όμως με το συμβατικό πόλεμο η προοπτική ενός κυβερνοπολέμου ως πρώτη αντίδραση ενάντια στον εχθρό μοιάζει να είναι η ηθικότερη λύση καθώς στη περίπτωση αυτή αποφεύγεται η αιματοχυσία. Και σε αυτή τη περίπτωση ωστόσο υπάρχει ο αντίλογος πως οι στόχοι μίας στρατιωτικής επιχείρησης είναι στρατιωτικές εγκαταστάσεις όπως σαφώς έχουν οριστεί από τους νόμους και τις συνθήκες που διέπουν τον συμβατικό πόλεμο. Αντίθετα σε ότι αφορά τον κυβερνοπόλεμο η νομοθεσία δεν είναι τόσο καλά ορισμένη και ο διαχωρισμός των στρατιωτικών από τους πολιτικούς στόχους μπορεί να είναι ασαφής (Robinson, Jones, Janicke 2015). Παράλληλα οι επιπτώσεις μίας κυβερνοεπίθεσης δεν συνιστά πράξη βίας άμεσα, μπορεί όμως να αποτελέσει πράξη βίας με ένα έμμεσο τρόπο. Ας πάρουμε ως παράδειγμα το ενδεχόμενο μία επίθεση να χτυπήσει το σύστημα διαχείρισης φόρτωσης-εκφόρτωσης ενός λιμανιού. Το γεγονός αυτό εκ πρώτης όψεως δε συνιστά ναυτικό αποκλεισμό καθώς τα πλοία μπορούν να φτάσουν στο λιμάνι, εντούτοις η αδυναμία εκφόρτωσης επιβάλλει εμμέσως τον αποκλεισμό του λιμανιού (Calvo 2014). Συνοψίζοντας οι κυβερνοεπιθέσεις δεν είναι μία άμεσα βίαιη πρακτική, μπορούν όμως να έχουν ισοδύναμα βίαια αποτελέσματα με τα συμβατικά όπλα όταν στοχεύσουν κρίσιμες υποδομές για ένα πληθυσμό. Η ηθική των κυβερνοεπιθέσεων και του κυβερνοπολόμου εν γένει επιχειρείται να δομηθεί κατά Taddeo πάνω σε τρεις άξονες (Robinson, Jones, Janicke 2015):

- I) ο κυβερνοπόλεμος πρέπει να εξαπολύεται εναντίων μόνο όσων οντοτήτων απειλούν η διαταράσσουν την ομαλή λειτουργία του κυβερνοχώρου,
- II) πρέπει να εξαπολύεται με στόχο τη διατήρηση της ομαλής λειτουργίας του κυβερνοχώρου,
- III) δεν πρέπει να εξαπολύεται με στόχο τη προώθηση της ομαλής λειτουργίας του κυβερνοχώρου.

Ωστόσο οι αρχές αυτές από μόνες τους δεν επιλύουν όλα τα ζητήματα ηθικής φύσεως ενώ αδυνατούν να καθορίσουν στη πραγματικότητα το πότε και σε ποια περίπτωση είναι δικαιολογημένη μία κυβερνοεπίθεση. Έτσι κατά Lin πραγματοποιείται μία

ρεαλιστικότερη προσέγγιση εξετάζοντας τις εξής πτυχές (Robinson, Jones, Janicke 2015):

I) Επιθετικότητα: ποιες κυβερνοεπιθέσεις αποτελούν πράξης επιθετικότητας και αξίζουν στρατιωτικής απάντησης.

II) Διάκριση: πόσο ακριβείς μπορούμε να είμαστε με μία κυβερνοεπίθεση ούτως ώστε να διατηρούνται οι παράπλευρες απώλειες σε μικρό βαθμό

III) Αναλογικότητα: ποιου είδους απαντήσεις είναι ανάλογες στις κυβερνοεπιθέσεις

IV) Απόδοση: η ηθική υποχρέωση να είναι σωστή η απόδοση ευθύνης για μία επίθεση

Ένα ακόμα ζήτημα που εξετάζεται είναι η εξαπάτηση στον κυβερνοπόλεμο. Παράδειγμα εξαπάτησης είναι η τοποθέτηση κακόβουλου λογισμικού μέσα σε κάποιο κώδικα, καθώς έτσι υποκρύπτεται στρατιωτική ενέργεια σε δραστηριότητα των πολιτών. Κάθε δραστηριότητα που προσπαθεί να κρυφτεί σε δραστηριότητες των πολιτών στο κυβερνοχώρο ή η εκμετάλλευση κάποιου πολίτη για να διενεργήσει εν αγνοία του κάποια (όπως το να μεταφέρει μολυσμένο USB) δραστηριότητα συνδεδεμένη με κυβερνοεπίθεση μπορεί να εκληφθεί ως εξαπάτηση. Στόχος της οριοθέτησης της εξαπάτησης είναι η προστασία των πολιτών και τις δραστηριότητές των. Το εγχειρίδιο του Ταλίν περιλαμβάνει και αυτό οδηγίες για την εξαπάτηση στο κυβερνοπόλεμο. Παρόλο που δεν υποχρεώνει τους μετέχοντες σε μία σύγκρουση να ορίσουν ποιες ιστοσελίδες, IP και γενικότερα τεχνολογικές εγκαταστάσεις χρησιμοποιούνται για στρατιωτικούς σκοπούς εντούτοις εάν τα παραπάνω εργαλεία παρουσιαστούν ως πολιτικά ενώ έχουν ως σκοπό τη στρατιωτική τους χρήση και τη πρόκληση απωλειών τότε θεωρείται πως διενεργήθηκε εξαπάτηση. Επίσης η απόκρυψη της προέλευσης της επίθεσης δεν θεωρείται εξαπάτηση, αλλά η ώθηση στο να πειστεί ο αντίπαλος πως ο εντολέας είναι προστατευόμενο πρόσωπο είναι εξαπάτηση. Τέλος σύμφωνα με το εγχειρίδιο η διενέργεια επιθέσεων από πολιτικές υποδομές δεν εμπίπτουν αυτόματα στο πεδίο της εξαπάτησης εκτός αν πρόκειται για συγκεκριμένες προστατευμένες υποδομές όπως είναι τα νοσοκομεία (Robinson, Jones, Janicke 2015). Επίσης ένα ηθικό ζήτημα που εγείρεται είναι αυτό που αφορά την ισορροπία ανάμεσα στις ελευθερίες λόγου και την ιδιωτικότητα από τη μία και την ανάγκη για προστασία και ασφάλεια στο κυβερνοχώρο από την άλλη (Sharma 2024).

18.2 Διεθνείς Συμφωνίες

Η ανάπτυξη διεθνών συμφωνιών και μέτρων καταδεικνύει τη κοινή επίγνωση πως οι κυβερνοαπειλές υφίστανται. Τα μέτρα αυτά δεν αποτελούν δεσμευτικούς κανόνες αλλά είναι σημαντικά στη διατήρηση της ασφάλειας και της εμπιστοσύνης, μειώνοντας τη πιθανότητα συγκρούσεων.

18.2.1 ΗΠΑ-Ρωσία:

τον Ιούνιο του 2013 υπογράφηκε η πρώτη διμερής συνθήκη για τη μείωση του κινδύνου σύγκρουσης στο κυβερνοχώρο. Η συμφωνία προέβλεπε την ανταλλαγή

τεχνολογικών πληροφοριών μεταξύ της ομάδας άμεσης επέμβασης των ΗΠΑ και της αντίστοιχης ρωσικής (Giles 2017).

18.2.2 ΗΠΑ-Κίνα:

το Σεπτέμβριο του 2015 οι δύο χώρες ήρθαν σε συμφωνία για τη κυβερνοασφάλεια. Παρά το γεγονός πως δεν επιτεύχθηκε η αναμενόμενη συμφωνία σε ότι αφορά το περιορισμό των κυβερνοόπλων, η συμφωνία πέτυχε τη συμμόρφωση των συμβαλλομένων σύμφωνα με κανόνες συμπεριφοράς στο κυβερνοχώρο που να και δεν έχουν αποσαφηνιστεί πλήρως, όταν θεσπιστούν θα οριοθετήσουν τη συμπεριφορά δύο εκ των μεγαλύτερων δυνάμεων του κυβερνοχώρου (Giles 2017).

18.2.3 Ρωσία-Κίνα:

τον Μάιο του 2015 επήλθε συμφωνία που προέβλεπε την αποφυγή διεξαγωγής κυβερνοεπιθέσεων μεταξύ των συμβαλλομένων, ενώ συμφωνήθηκε η από κοινού δράση κατά τεχνολογιών που δύνανται να έχουν αποσταθεροποιητικά αποτελέσματα σε πολιτικό και κοινωνικό-οικονομικό επίπεδο (Giles 2017).

18.3 Διεθνείς Πρωτοβουλίες

18.3.1 Πρωτοβουλίες Ηνωμένων Εθνών:

σημαντικότερη πρωτοβουλία των Η.Ε. θεωρείται η GGE (Group of Governmental Experts). Στο πλαίσιο της ομάδας αυτής το διάστημα 2013-15 κατέληξε σε σημαντικά συμπεράσματα σε ότι αφορά τη νομολογία που διέπει τον κυβερνοχώρο ενώ συμφωνήθηκαν 11 μη δεσμευτικοί κανόνες για ότι αφορά τη συμπεριφορά των κρατών καθώς και μέτρα για την οικοδόμηση εμπιστοσύνης και συντονισμένης δράσης στη κυβερνοασφάλεια. Τη περίοδο 2016-17 ωστόσο απέτυχε να οικοδομήσει μία κοινή συμφωνία καθώς εγέρθηκαν ζητήματα στρατικοποίησης του κυβερνοχώρου. Τον Ιούνιο του 2019 δημιουργήθηκε μία νέα ομάδα εργασίας η OEWG (Open-Ended Working Group). Σκοπός της OEWG είναι να μελετήσει τους κανόνες που περιλήφθηκαν στις εισηγήσεις της προαναφερθείσας GGE με την πιθανότητα να αλλαχτούν κανόνες που είχαν θεσπιστεί. Παράλληλα το γενικό συμβούλιο των Η.Ε. συμφώνησε στη σύσταση μίας νέας GGE που συνεδρίασε πρώτη φορά το 2019 και αποτελείται από 25 κράτη-μέλη των Η.Ε. που έχουν επιφορτιστεί με τη μελέτη της επίδρασης του διεθνούς δικαίου στις πράξεις των κρατών στο κυβερνοχώρο (Moynihan 2019).

18.3.2 Πρωτοβουλίες σε περιφερειακό επίπεδο:

ήδη από το 2019 η GGE διεξήγε συνομιλίες με διάφορες ενώσεις (Αφρικανική Ένωση, Ε.Ε., Οργανισμός Αμερικανικών Κρατών, Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη, Ένωση Χωρών της Νοτιοανατολικής Ασίας). Σε αυτές τις συναντήσεις εκφράστηκε η πιθανότητα της συμπερίληψης του διεθνούς δικαίου για το κυβερνοχώρο σε διάφορα άλλα περιφερειακά φόρουμ. Ωστόσο διάφοροι οργανισμοί όπως είναι οι G7, G20, Ε.Ε. κ.α. απορρίπτουν την εφαρμογή των κανόνων και κυρίως την ανάπτυξη μέτρων οικοδόμησης αμοιβαίας εμπιστοσύνης όπως για

παράδειγμα μέτρα για την ανταλλαγή πληροφοριών μεταξύ κρατών, προώθηση της διαφάνειας με στόχο την αποτροπή κυβερνοεπιθέσεων κ.α. (Moynihan 2019).

18.3.3 Πρωτοβουλίες μη κυβερνητικών δρώντων:

τα τελευταία χρόνια παρατηρείται κινητικότητα πρωτοβουλιών με στόχο την περαιτέρω κατανόηση των κανόνων που θα πρέπει να διέπουν τις αλληλεπιδράσεις των κρατών στο διαδίκτυο. Τα μέλη των συναντήσεων αυτών προέρχονται από διαφόρους χώρους όπως είναι η κοινωνία των πολιτών, διάφορα think-tanks, ο τεχνολογικός τομέας και διεθνείς οργανισμοί. Στο πλαίσιο αυτό δημιουργήθηκε η GCSC (Global Commission on the Stability of Cyberspace), η οποία έχει προτείνει αρχές και κανόνες για τη σωστή χρήση του κυβερνοχώρου. Παράλληλα η Cybersecurity Tech Accord εστιάζει στην ανάπτυξη της συνεργασίας των εταιριών τεχνολογίας σε ότι αφορά τη σταθερότητα και ασφάλεια στο κυβερνοχώρο. Η Digital Peace Now αποτελεί μία πρωτοβουλία με στόχο τη διακοπή του κυβερνοπολέμου. Τις προσπάθειες αυτές πολλές φορές ηγούνται και κράτη όπως για παράδειγμα η γαλλική πρωτοβουλία Paris Call for Trust and Security in Cyberspace η οποία και υποστηρίχθηκε από 67 κράτη, 139 διεθνείς οργανισμοί και 358 ιδιωτικοί οργανισμοί (Moynihan 2019).

18.3.4 NATO-ΕΕ:

Κατά τη διάρκεια των ετών 2010 και 2011 το NATO και η ΕΕ ανέλαβαν πρωτοβουλίες για το περιορισμό των κυβερνοεπιθέσεων. Συγκεκριμένα το ψηφιακό σχέδιο της ΕΕ προβλέπει τη δημιουργία ψηφιακών ομάδων άμεσης αντίδρασης καθώς και τη διενέργεια διεθνικών προσομοιώσεων για τη κυβερνοασφάλεια. Επίσης προβλέπεται η δημιουργία μίας πανευρωπαϊκής πλατφόρμας για το κυβερνοέγκλημα. Σε ότι αφορά το NATO υιοθετήθηκε το στρατηγικό δόγμα που προέβλεπε την ανάπτυξη διαδικτυακών αμυντικών δυνατοτήτων. Στο πλαίσιο αυτό λειτούργησε το τεχνικό κέντρο άμεσης ανταπόκρισης (NCIRC). Οι δράσεις των συμμαχιών καταδεικνύουν τη σημαντικότητα των ψηφιακών απειλών (Herzog 2011). Η κοινή στρατηγική κυβερνοάμυνας της ΕΕ υιοθετήθηκε το 2014 και ορίζει τις αποδεκτές συμπεριφορές του κυβερνοχώρου σύμφωνα με τις αξίες της ΕΕ. Παράλληλα εργάζεται για τη συμπλήρωση των νομικών κενών που καταδείχθηκαν στη NIS (National Infrastructure Strategy). Παρά την επιθυμία της για τόνωση των μέτρων οικοδόμησης εμπιστοσύνης σε διεθνές επίπεδο αντιτίθεται στη δημιουργία νομικών οργάνων για θέματα του κυβερνοχώρου. Η συμμαχία από την άλλη μεριά τον Ιούνιο του 2014 επιβεβαίωσε πως το διεθνές δίκαιο έχει εφαρμογή και στο κυβερνοχώρο. Κατά αυτό τον τρόπο μπορεί να ενεργοποιηθεί το άρθρο 5 της συμμαχίας και στη περίπτωση κυβερνοεπίθεσης (Giles 2017).

18.4 Μέτρα Οικοδόμησης Εμπιστοσύνης (CBMs)

18.4.1 Organization for Security and Co-operation in Europe (OSCE):

περιλαμβάνει 56 κράτη μέλη και έχει υιοθετήσει 11 εθελοντικά μέτρα που μεταξύ άλλων περιλαμβάνουν την ανταλλαγή πληροφοριών μεταξύ κρατών την οποία

εποπτεύει η OSCE. Η έκθεση UNGGE 2015 έχει βασίσει τις προτάσεις της κατά βάση στα εθελοντικά μέτρα της OSCE (Giles 2017).

18.4.2 The Association of Southeast Asian Nations (ASEAN):

το 2012 οι υπουργοί εξωτερικών της ASEAN επιφόρτισαν το περιφερειακό φόρουμ του οργανισμού με τη προώθηση μέτρων για σταθερότητα στο κυβερνοχώρο και την προαγωγή της εμπιστοσύνης μεταξύ των μελών της. Παράλληλα ξεκίνησε η ανάπτυξη ενός σχεδίου για την ασφάλεια ICT (Giles 2017).

18.4.3 The Organization of American States (OAS):

η OAS υπήρξε πρωτοπόρα στην υιοθέτηση κοινής στρατηγικής για τη κυβερνοασφάλεια καθώς το 2004 υιοθέτησε την διαμερικανική στρατηγική για τη καταπολέμηση απειλών για την ασφάλεια στον κυβερνοχώρο. Οι πρωτοβουλίες της κυρίως αφορούσαν το κυβερνοέγκλημα και τη προστασία των υποδομών (Giles 2017).

18.5 Προβλήματα στη νομοθεσία των κυβερνοεπιθέσεων

Ο μεγαλύτερος νομικός προβληματισμός σε ότι αφορά τον κυβερνοπόλεμο είναι η αδυναμία σύνδεσης του φαινομένου με την υφιστάμενη νομολογία. Η διεθνής νομική πρακτική σε ότι αφορά τον πόλεμο διαχωρίζεται στο *jus ad bellum* που καλύπτει τη νομολογία που αφορά την απόφαση ενός κράτους να προβεί σε στρατιωτική ενέργεια και το *jus in bello* που αφορά τη ρύθμιση των στρατιωτικών συγκρούσεων. Αν και έχει επιτευχθεί συμφωνία πως οι δύο ανωτέρω κλάδοι είναι εφαρμόσιμοι στο φαινόμενο του κυβερνοπολέμου εντούτοις επικρατεί σύγχυση για το τρόπο με τον οποίο είναι εφαρμόσιμοι (Green 2015).

18.5.1 Αρχή της διάκρισης:

σύμφωνα με το διεθνές ανθρωπιστικό δίκαιο υπάρχει διάκριση μεταξύ στρατιωτικών και πολιτικών στόχων και αποδεκτή είναι μόνο η στόχευση των πρώτων. Το ζήτημα εδώ έγκειται όπως άλλωστε και στο συμβατικό πεδίο, είναι να διευκρινιστεί ποιοι είναι οι στρατιωτικοί στόχοι που είναι αποδεκτό να πληγούν μέσω κυβερνοεπιθέσεων. Κάτι τέτοιο είναι δύσκολα εφαρμόσιμο καθώς τα δίκτυα συνήθως έχουν μία διπλή χρήση τόσο από στρατιωτικούς όσο και από πολιτικούς δρώντες, αν και το ζήτημα της διπλής χρήσης δεν αποτελεί καινούρια συνθήκη υπερτονίζεται στο πλαίσιο των κυβερνοεπιθέσεων (Gesley 2010).

Ένα παντοτινό πρόβλημα των πολεμικών συγκρούσεων που βρίσκει εφαρμογή στη πρακτική των κυβερνοεπιθέσεων είναι οι αδιάκριτες επιθέσεις. Πιο συγκεκριμένα μία επίθεση με την εισαγωγή ιού σε κάποιο στρατιωτικό δίκτυο μπορεί κάλλιστα λόγω της λειτουργίας των ιών να μολύνουν όσο το δυνατόν περισσότερα συστήματα και της διασύνδεσης στρατιωτικών και πολιτικών δικτύων να πλήξει τα δεύτερα και επηρεάσει έτσι τις υποδομές και την διαχείρισή τους (Gesley 2010).

Ένα ακόμα πρόβλημα που προκύπτει είναι και η συμμετοχή των πολιτών καθώς η διεξαγωγή μίας κυβερνοεπίθεσης προϋποθέτει εξειδικευμένες γνώσεις που ένας στρατιώτης δεν κατέχει. Έτσι προκύπτει το ερώτημα πως αντιμετωπίζονται οι

συμμετέχοντες σε κυβερνοεπιθέσεις από νομικής σκοπιάς. Σύμφωνα με τη νομολογία, πολίτης είναι όποιος δεν θεωρείται πολεμιστής. Για να θεωρηθεί κάποιος πολεμιστής πρέπει να πληρούνται τέσσερα κριτήρια (διοικείται από κάποιον, φέρει κάποιο ευδιάκριτο σήμα, φέρει τα όπλα του και διεξάγει επιχειρήσεις σύμφωνα με τους νόμους και τα έθιμα του πολέμου), τα οποία στο πλαίσιο του κυβερνοπολέμου πρέπει να επανεξετασθούν (Gesley 2010).

18.5.2 Απαγόρευση της εξαπάτησης (άρθρο 37):

εξαπάτηση θεωρείται 'πράξεις που προσκαλούν την εμπιστοσύνη του αντιπάλου και τον οδηγούν να πιστέψει πως οφείλει, ή είναι υποχρεωμένος να συμφωνήσει σύμφωνα με το διεθνές δίκαιο του πολέμου με σκοπό να προδοθεί η εμπιστοσύνη του. Στο κυβερνοχώρο προσπάθεια εξαπάτησης αποτελούν οι λογικές βόμβες που μπορούν να προγραμματιστούν σκοπίμως ώστε να εκραγούν τραυματίζοντας το άτομο που άνοιξε το e-mail που τις περιείχε (Gesley 2010).

18.5.3 Ουδετερότητα:

η αρχή της ουδετερότητας παραβιάζεται στο κυβερνοπόλεμο όταν οι επιθέσεις διεξάγονται χρησιμοποιώντας το δίκτυο μίας τρίτης χώρας. Σύμφωνα με τις συμβάσεις της Χάγης η επικράτεια τρίτων κρατών είναι απαραβίαστη από τη μετακίνηση στρατευμάτων η πολεμικού υλικού στο έδαφος τρίτων κρατών, επομένως. Το ερώτημα που τίθεται είναι εάν αυτή η συνθήκη παραβιάζεται στο ενδεχόμενο χρήσης του δικτύου ή των διαδικτυακών υποδομών μίας χώρας για τη διεξαγωγή κυβερνοεπίθεσης. Η συνθήκη που θεσπίστηκε το 1907 προϋπόθετε βέβαια την ύπαρξη απτής εισβολής στρατευμάτων προς ουδέτερο κράτος και παρά την ύπαρξη του άρθρου 8 που πραγματεύεται τις τηλεπικοινωνίες η νομοθεσία δε δύναται να ξεκαθαρίσει το πότε παραβιάζεται η ουδετερότητα ενός κράτους. Παράλληλα ουδέτερα κράτη διατηρούν το δικαίωμα να θέτουν τα δίκτυά τους στη διάθεση των εμπολέμων εφόσον το κάνουν και για τα δύο μέρη (Gesley 2010).

18.5.4 Διαπίστωση της προέλευσης μίας επίθεσης:

οι κυβερνοεπιθέσεις θολώνουν τα όρια μεταξύ πολεμικών πράξεων και κοινών εγκλημάτων. Η ασάφεια αυτή προκαλείται από το γεγονός πως η πηγή της επίθεσης μπορεί εύκολα να αποκρυφθεί καθώς οι τα σήματα μπορούν να εκπέμψουν από μη στρατιωτικά δίκτυα και οι διευθύνσεις IP να είναι ψευδείς. Χαρακτηριστικό είναι το γεγονός πως το 96% των επιθέσεων δεν εντοπίζεται. Στο τοπίο αυτό συμβάλλει και η δράση των χακτιβιστικών ομάδων στις οποίες δεν είναι εύκολο να αποδοθεί σύνδεση με τη κεντρική κυβέρνηση. Από το 1999 έως το 2002 Κινέζοι χάκερ επιτέθηκαν σε πολλές ξένες ιστοσελίδες κάτι που αποθαρρύνθηκε εκ των υστέρων από τη κινεζική κυβέρνηση, ωστόσο υπάρχουν ενδείξεις για τη σύνδεσή της με τέτοιες ομάδες και η οποία πιθανή σύνδεση δημιουργεί προβληματισμό ως το προς εάν οι ομάδες αυτές μελλοντικά χρησιμοποιηθούν για επιθετικές ενέργειες. Ακόμα μεγαλύτερο αποτελεί η σύνδεση κεντρικών κυβερνήσεων με μεμονωμένους χάκερ (Gesley 2010).

18.5.5 Δυσκολία διαπίστωσης των θυμάτων:

οι δυσκολίες διάκρισης που χαρακτηρίζουν τις κυβερνοεπιθέσεις παρατηρούνται και στη διάκριση των θυμάτων αυτών. Στο συμβατικό πόλεμο τα όρια είναι ξεκάθαρα, μια βομβιστική επίθεση στα γραφεία μίας εταιρείας αποτελεί μία παράνομη ενέργεια που θέτει στο στόχαστρό της ανθρώπινες ζωές και λαμβάνει χώρα στο έδαφος ενός κράτους. Επομένως η επίθεση στρέφεται ενάντια στο έδαφος και τον πληθυσμό μίας χώρας και άρα πλήττει την ίδια την κυριαρχία της. Ωστόσο η επίθεση εναντίων ενός δικτύου περιπλέκει την κατάσταση. Η ίδια η έννοια της επίθεσης κατά το δίκαιο ερμηνεύεται ως η πρόκληση μίας βίαιης πράξης εναντίων του αντιπάλου στη φυσική της διάσταση. Ως εκ τούτου μία κυβερνοεπίθεση δεν μπορεί να θεωρηθεί ως πράξη βίας με τη στενή νομική έννοια. Ωστόσο προβλέπεται πως η ίδια η απειλή βίας με σκοπό την πρόκληση πανικού στο πληθυσμό όπως για παράδειγμα η προσβολή ενός παγκοσμίου δικτύου απαγορεύεται (Gesley 2010).

18.5.6 Χρήση Βίας:

Σημαντικό πρόβλημα αποτελεί η εννοιολόγηση της χρήσης της βίας. Σύμφωνα με την ισχύουσα προσέγγιση του χάρτη του ΟΗΕ (άρθρο 2(4)), μία πράξη που θεωρείται ως πράξη βίας τότε είναι εξ αντικειμένου παράνομη και η ανταπόδοση της πράξης από το θύμα μπορεί να επιτραπεί, ενώ εγκρίνεται η χρήση βίας με σκοπό τη διασφάλιση της διεθνούς ειρήνης και ασφάλειας. Ωστόσο παραμένει προβληματική η χρήση της υφιστάμενης νομοθεσίας για τη προσέγγιση της χρήσης βίας του κυβερνοπολέμου, παρά τις καταστροφικές συνέπειες που μπορεί μία κυβερνοεπίθεση να έχει καθώς δίνεται έμφαση στη φύση της επίθεσης και όχι στα αποτελέσματα. Μία από τις προτάσεις που έχουν διατυπωθεί για την επίλυση του προβλήματος είναι η θεωρία του Michael Schmitt που συνδυάζει τα αποτελέσματα με τη πρόθεση πίσω από μία κυβερνοεπίθεση, οπότε κάθε κυβερνοεπίθεση που προκαλεί η προβλέπεται ότι θα προκαλέσει εκτεταμένους τραυματισμούς, η καταστροφή ή θάνατο μπορεί να θεωρηθεί ως χρήση βίας σύμφωνα με το ισχύον νομικό πλαίσιο (Raboin 2011).

18.5.7 Ευθύνη και απόδοση:

Είναι γνωστό πως οι δράστες των κυβερνοεπιθέσεων δρουν μέσα στα φυσικά σύνορα κάποιου κράτους κάτι που εγείρει το ερώτημα σχετικά με την ευθύνη των κρατών για διεθνή περιστατικά κυβερνοεπιθέσεων και το επίπεδο της απόδοσης της ευθύνης που αυτά φέρουν. Η ίδια η φύση του κυβερνοχώρου προκαλεί τεράστιες δυσκολίες καθώς οι κυβερνοεπιθέσεις διεξάγονται από ειδικούς στην απόκρυψη κάτι που εμποδίζει την ανακάλυψη της χώρας προέλευσης της επίθεσης και ειδικά του δράστη της. Η δυσκολία αυτή καθιστά τις παραδοσιακές μεθόδους απόδοσης ευθύνης σύμφωνα με το διεθνές δίκαιο ανεφάρμοστες έναντι του φαινομένου των κυβερνοεπιθέσεων. Γίνεται έτσι αντιληπτό πως το κριτήριο του αποτελεσματικού ελέγχου που καθιερώθηκε μετά την υπόθεση της Νικαράγουας και ο γενικός έλεγχος που αναγνωρίστηκε με την υπόθεση Tadic δεν μπορούν να είναι εφαρμόσιμα στις κυβερνοεπιθέσεις έως ότου οι ταυτότητες των δραστών να είναι απολύτως γνωστές. Το πλαίσιο αυτό εξαναγκάζει τους κρατικούς δρώντες να εφαρμόζουν παθητικά μέτρα

ασφαλείας εναντίων των επιθέσεων τα οποία είναι συνήθως ανεπαρκή (Hemen Faga 2017).

Οι εύρεση αποδείξεων για τη προέλευση των κυβερνοεπιθέσεων είναι δύσκολη οπότε τα κράτη-θύματα συνήθως βασίζονται στη τεκμαρτή απόδοση ούτως ώστε να αποδώσουν σε κάποιο έτερο κράτος την επίθεση. Η λογική της απόδοσης αυτού του τύπου έγκειται στην αποτυχία μίας κρατικής οντότητας να επιτηρήσει και να αποτρέψει την διεξαγωγή επίθεσης μέσα από τα σύνορά της και επομένως όταν συνεχιζόμενα το έδαφός της χρησιμοποιείται ως εφαλτήριο των επιθέσεων και αποτυγχάνει ή αμελεί να διερευνήσει την επίθεση, δημιουργείται το τεκμήριο της συνεργασίας με τους δράστες (Hemen Faga 2017).

18.5.8 Άμεση συμμετοχή:

Το γεγονός πως μεγάλο μέρος των κυβερνοεπιθέσεων προέρχεται από μη κρατικούς δρώντες, των οποίων τα μέλη είναι πολίτες σύμφωνα με το διεθνές ανθρωπιστικό δίκαιο. Συνεπώς ακόμα και στη περίπτωση που οι επιθέσεις έχουν αντίκτυπο ίσο με ένοπλες επιθέσεις οι δράστες αυτών εξακολουθούν να χαρακτηρίζονται ως πολίτες όπως ορίζεται από τα άρθρα 50 και 43 του επιπρόσθετου πρωτοκόλλου Ι και του άρθρου 4 της συνθήκης της Γενεύης του 1949 εκτός εάν πληρούν τα τέσσερα κριτήρια για να χαρακτηριστούν ως μαχητές (Hemen Faga 2017).

Σε ένα άλλο επίπεδο πέραν της νομολογίας, πολίτες οι οποίοι δεν πληρούν τα κριτήρια του μαχητή, αλλά λαμβάνουν ενεργό μέρος στις εχθροπραξίες δεν μπορούν πλέον να απολαμβάνουν τα προνόμια του πολίτη και θεωρούνται ως μαχητές σε ότι αφορά τις διαδικασίες στόχευσης και κράτησης αυτών εάν πληρούνται τα εξής κριτήρια σύμφωνα με την αρχή της ενεργού συμμετοχής (Hemen Faga 2017).

Παράλληλα σκιώδες είναι το καθεστώς των ατόμων που δημιουργούν τα προγράμματα που χρησιμοποιούνται σε επιχειρήσεις κυβερνοπολέμου, αυτών που εγκαθιστούν, διαχειρίζονται και συντηρούν τα προγράμματα και αυτών που τα λειτουργούν. Τα άτομα αυτά μπορούν να χαρακτηριστούν είτε ως πολίτες είτε ως εμπόλεμοι αναλόγως των συνθηκών. Στη περίπτωση που χαρακτηριστούν ως εμπόλεμοι μπορούν να αποτελέσουν στρατιωτικούς στόχους και να συλληφθούν ως αιχμάλωτοι πολέμου (Hemen Faga 2017).

18.6 Διεθνές Δικαστήριο

Ανάμεσα σε ανεξάρτητα κράτη ο σεβασμός για την εδαφική ακεραιότητα αποτελεί ουσιαστικό θεμέλιο στις διεθνείς σχέσεις. Επομένως εχθρικές κυβερνοεπιχειρήσεις κατευθυνόμενες ενάντια στις κυβερνουποδομές που βρίσκονται στην επικράτεια άλλης χώρας, είτε είναι κυβερνητικής ιδιοκτησίας είτε όχι, απαρτίζουν μεταξύ άλλων παραβίαση της κυριαρχίας της χώρας ασχέτως εάν προκαλούν φυσικές ζημιές ή τραυματισμούς (Lancelot 2020). Η απόφαση του ICJ στην υπόθεση Νικαράγουα κατά Ηνωμένων Πολιτειών της Αμερικής και η γνωμοδότησή του στο Nuclear Weapons Advisory καθιστούν προφανές ότι, παρόλο που δεν υπάρχει νομοθεσία στον κυβερνοχώρο, η υπάρχουσα νομοθεσία είναι επαρκής για επιθέσεις στον

κυβερνοχώρο και αντικρούει τον ισχυρισμό ότι μια ένοπλη επίθεση δεν μπορεί να συμβεί λόγω έλλειψης των χρησιμοποιούμενων όπλων (Mendoza 2017).

Κεφάλαιο 19: Εγχειρίδιο του Ταλίν

19.1 Ιστορία του Εγχειριδίου

Το συγκεκριμένο εγχειρίδιο προέκυψε μέσα από την πρωτοβουλία του CCDCOE του NATO το οποίο εδρεύει στο Ταλίν της Εσθονίας. Συγκεκριμένα το 2009 ξεκίνησε η προσπάθεια για την παραγωγή ενός νομικού κειμένου το οποίο θα συνέδεε την υπάρχουσα νομοθεσία με τη νέα μορφή του ηλεκτρονικού πολέμου. Οι διαδικτυακές επιθέσεις βέβαια απασχόλησαν τη νομική κοινότητα ήδη από τη δεκαετία του 1990 και το 1999 το ναυτικό των ΗΠΑ διοργάνωσε το πρώτο σχετικό συνέδριο, ωστόσο σημεία καμπής που ώθησαν στη μεγαλύτερη ενασχόληση με το φαινόμενο των κυβερνοεπιθέσεων θεωρούνται οι χακτιβιστικές επιθέσεις εναντίον της Εσθονίας το 2007 και της Γεωργίας το 2008 μεσούσης της πολεμικής της σύγκρουσης με τη Ρωσία καθώς και η στοχοποίηση με το κακόβουλο λογισμικό *stuxnet* των ιρανικών πυρηνικών εγκαταστάσεων το 2010. Τα γεγονότα αυτά έστρεψαν τη προσοχή των κρατών πάνω στο θέμα των κυβερνοεπιθέσεων. Χαρακτηριστικά το 2010 το Ηνωμένο Βασίλειο συμπεριέλαβε τις κυβερνοεπιθέσεις στις μεγαλύτερες απειλές εθνικής ασφάλειας, ακολουθούμενο την ίδια χρονιά από τις ΗΠΑ, ενώ το 2011 εξέδωσαν το στρατηγικό δόγμα για τις επιχειρήσεις στο κυβερνοχώρο. Παράλληλα την ίδια περίοδο το παράδειγμα των ΗΠΑ ακολούθησαν και άλλα κράτη όπως ο Καναδάς, η Ρωσία ενώ και το NATO το 2010 συμπεριέλαβε την απειλή των κυβερνοεπιθέσεων και τον τρόπο αντιμετώπισής τους στο αμυντικό του δόγμα (Tallin Manual 2017).

Είναι σημαντικό να σημειωθεί πως το εγχειρίδιο του Ταλίν δεν αποτελεί ένα επίσημο κείμενο του CCDCOE του NATO αλλά τη γνώμη μίας ομάδας ειδικών οπότε και δεν αντικατοπτρίζει το δόγμα της συμμαχίας ή τις θέσεις των κρατών που την συναποτελούν παρά το γεγονός πως πολλοί από τους ειδικούς που συνέβαλαν στη δημιουργία του εγχειριδίου κατείχαν και θέσεις στη διοίκηση των κρατών τους (Tallin Manual 2017).

Το εγχειρίδιο χωρίζεται σε δύο μέρη με το πρώτο να αφορά τη νομολογία για τη κυβερνοασφάλεια ενώ το δεύτερο περιλαμβάνει τους κανόνες που διέπουν τη διαμάχη που λαμβάνει χώρα στο κυβερνοχώρο (Tallin Manual 2017).

Μέρος Α: το κομμάτι αυτό τιτλοφορείται διεθνές δίκαιο κυβερνοασφάλειας ο οποίος τίτλος δεν αποτελεί κάποιο επίσημο νομικό όρο. Επιπρόσθετα το πρώτο μέρος του εγχειριδίου χωρίζεται σε δύο κεφάλαια που ακολούθως διακρίνονται σε υποκεφάλαια που περιλαμβάνουν συνολικά 19 κανόνες.

Μέρος Β: εδώ συναντώνται τέσσερα ακόμα κεφάλαια στα οποία περιλαμβάνονται 76 συνολικά κανόνες για το τρόπο διεξαγωγής των επιχειρήσεων του κυβερνοχώρου.

19.2 Κύριες έννοιες

19.2.1 Κυριαρχία

Παρά τη διαφοροποίηση που έχει υποστεί η έννοια της κυριαρχίας, στη ψηφιακή και τεχνολογική εποχή, παραμένει κορυφαία προτεραιότητα για κάθε κράτος και τις διεθνείς σχέσεις γενικότερα. Αποτελεί άλλωστε τον πρώτο κανόνα του Εγχειριδίου του Ταλίν 2.0 που αναφέρει πως η έννοια της κυριαρχίας εφαρμόζεται και στο κυβερνοχώρο. Παράλληλα η κυριαρχία συμβολίζει την εξουσία του κράτους έναντι ατόμων, πραγμάτων και πράξεων στο κυβερνοχώρο κατά αναλογία με τη πρακτική εκτός κυβερνοχώρου (Ogurlu 2023).

19.2.2 Κρατική Δικαιοδοσία

Κάθε κράτος δικαιούται να ασκεί τρεις μορφές δικαιοδοσίας έναντι προσώπων και αντικειμένων που βρίσκονται στην επικράτειά του, καθώς και έναντι πράξεων που συμβαίνουν εκεί. Κατά αυτό το τρόπο ένα κυρίαρχο κράτος ασκεί τη δικαιοδοσία του πάνω σε κυβερνουποδομές και άτομα που μετέχουν σε κυβερνοεπιχειρήσεις στο έδαφός της, κυβερνοεπιχειρήσεις που προέρχονται ή ολοκληρώνονται στο έδαφός της και επιχειρήσεις που έχουν αντίκτυπο στο έδαφός της (Ogurlu 2023).

19.2.3 Χρήση Βίας

Σύμφωνα με το εγχειρίδιο του Ταλίν εξετάζονται οι ακόλουθοι παράγοντες για να προσδιοριστεί εάν μία ενέργεια στο κυβερνοχώρο είναι χρήση βίας που αντιστοιχεί σε επίπεδο ένοπλης επίθεσης (Mendoza 2017):

- 1.σοβαρότητα
- 2.αμεσότητα
- 3.επεμβατικότητα
- 4.μετρήσιμα αποτελέσματα
- 5.στρατιωτικός χαρακτήρας
- 6.κρατική εμπλοκή
- 7.τεκμαιρόμενη νομιμότητα

19.2.4 Κανόνες 110

Ο κανόνας ορίζει πως όλα τα κράτη υποχρεούνται να διασφαλίζουν πως όλοι οι μέθοδοι ηλεκτρονικού πολέμου που κατέχουν ή χρησιμοποιούν πρέπει να συμμορφώνονται με τους δεσμευτικούς κανόνες του δικαίου των ενόπλων συγκρούσεων (Hasam Al-Badawi 2022).

Το Δίκαιο των Ενόπλων Συγκρούσεων (LOAC) γνωστό και ως Δίκαιο του Πολέμου (LOW) και το Διεθνές Ανθρωπιστικό Δίκαιο (IHL) είναι το εθιμικό δίκαιο και το δίκαιο των συνθηκών που εφαρμόζεται στη διεξαγωγή πολέμου στην ξηρά και στις σχέσεις μεταξύ εμπόλεμων και ουδέτερων κρατών. Τέσσερις αρχές συνιστούν το LOAC. Είναι η στρατιωτική αναγκαιότητα, η αναλογικότητα, η διάκριση και η περιττή ταλαιπωρία.

Το Εγχειρίδιο του Ταλίν αναφέρει ότι το LOAC ισχύει για τις επιχειρήσεις στον κυβερνοχώρο όπως και για κάθε άλλη λειτουργία συμβατικής φύσης, αλλά υπάρχουν περιορισμοί στην εφαρμογή. Παράλληλα σύμφωνα με το Εγχειρίδιο του Ταλίν, κανένα περιστατικό στον κυβερνοχώρο από το 2012 δεν έχει φτάσει στο κατώφλι μιας ένοπλης επίθεσης. Ακόμη και οι ιστορικές επιθέσεις που αναφέρθηκαν προηγουμένως και που εκ πρώτης όψευς, θα μπορούσαν να συστήσουν μια ενέργεια αναλογική με μία ένοπλη επίθεση, όπως η κυβερνοεπίθεση στην Εσθονία το 2007, η κυβερνοεπίθεση της Ρωσίας στη Γεωργία το 2008 και η επίθεση των ΗΠΑ και του Ισραήλ με το Stuxnet στο Ιράν το 2010 εντούτοις καμία από τις παραπάνω δεν υπερέβη τις προϋποθέσεις που θέτει το εγχειρίδιο του Ταλίν (Mendoza 2017).

Κεφάλαιο 20: Το μέλλον της Νομοθεσίας

Είναι σαφές πως διεθνές νομικό πλαίσιο χρειάζεται τροποποίηση. Για να επιτευχθεί ο στόχος, το διεθνές δίκαιο να συμπεριλάβει αποτελεσματικά το φαινόμενο του κυβερνοπολέμου στη νομολογία του θα πρέπει πρωτίστως να προσαρμοστεί όπως και στο παρελθόν στις τεχνολογικές εξελίξεις οι οποίες εξάλλου αποτελούν τη κινητήρια δύναμη των κυβερνοεπιθέσεων. Παράλληλα χρειάζεται η επαναπροσέγγιση εννοιών όπως της απόδοσης, της δικαιοδοσίας και της χρήσης της βίας. Ειδικότερα για την πρώτη η παραδοσιακή προσέγγισή βασίζεται στην υπόθεση πως μία στρατιωτική επιχείρηση θα είναι ευδιάκριτη, κάτι που όμως δεν μπορεί να ισχύσει στη περίπτωση των κυβερνοεπιθέσεων καθιστώντας αναγκαία τη δημιουργία νέων θεωριών απόδοσης. Σε ότι αφορά την έννοια της δικαιοδοσίας και πάλι η ανάπτυξη της τεχνολογίας καθιστά ανεπαρκή τη τωρινή νομική της σημασία σε ότι αφορά τον κυβερνοπόλεμο. Τελευταία έννοια που απαιτείται να διαφοροποιηθεί είναι αυτή της χρήσης βίας. Πέρα από τη επαναπροσέγγιση συγκεκριμένων εννοιών σημαντική προϋπόθεση για την ανάπτυξη ενός αποτελεσματικού διακαίου για το κυβερνοπόλεμο είναι η ύπαρξη συνοχής καθώς η πραγματικότητα έχει δείξει το αντίθετο, γεγονός που επιδρά ως παράγοντάς αβεβαιότητας και που διεγείρει τις κυβερνοεπιθέσεις. Τέλος χρειάζεται η προώθηση διεθνών συμφωνιών που θα εξυπηρετήσουν το σκοπό της παγκόσμιας ενότητας για τον εντοπισμό και έλεγχο των ομάδων που διεξάγουν κακόβουλες επιχειρήσεις στο κυβερνοχώρο (Raboin 2011).

Βιβλιογραφία

Tallinn Manual on the International Law Applicable to Cyber Warfare, The NATO Cooperative Cyber Defence Centre of Excellence

Zahid Oruj, Cyber Security: Contemporary cyber Threats and National Strategies. Social Research Center Baku Azerbaijan

Callistus Francis Azubuike, Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. Nnamdi Azikiwe Journal of Political Science (NAJOPS) vol. 9, 2023

Barrie Sander, Cyber Insecurity and the Politics of International Law. European Society of International Law Volume 6, Issue 5, 9 June 2017

Θεοφίλης Ανδρέας, Οι Κυβερνοεπιθέσεις ως Μέσο Στρατηγικής. Στρατηγικόν τεύχος 2, 2018

Arindam Bhattacharya, The Necessity of Cyber-diplomacy in the Digital Age. Advocacy Unified Network September 2022

Jensen Benjamin, The Cyber Character of Political Warfare. Brown Journal of World Affairs, Fall/Winter 2017

Jibi Mariam Biju, Neethu Gopal, Anju J Prakash. Cyber Attacks and their Different Types. International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 03 March 2019

Marcin Surowka, Zbigniew Malobodry, Karolina Nastaj-Salek, Katarzyna Cyrkun, The Impact of Cyberattacks on the Stability of Global Financial Markets as a Manifestation of Economic Terrorism. Scientific Journal of Bielsko-Biala School of Finance and Law Volume 29 No 2 June 2024

Harriet Moynihan, The Application of International Law to State Cyberattacks, Sovereignty and Non-intervention. International Law Programme December 2019

James A. Green, Cyber Warfare A multidisciplinary analysis. Routledge studies in Conflict Security and Technology 2015

Sharon Matzkin, Ryan Shandler, Daphna Canetti, The Limits of Cyberattacks in Eroding Political Trust: A Tripartite Survey Experiment. The British Journal of Politics and International Relations 2023

M. Uma, G. Padmavathi, A Survey on Various Cyber Attacks and their Classification. International Journal of Network Security, Vol.15, No.5. PP.390-396, Sept. 2013

Phillip Pool, War of the Cyber World: The Law of Cyber Warfare, 47 INT'L L. 299 (2013)

Michael Robinson, Kevin Jones, Helge Janicke, Cyber Warfare: Issues and Challenges. Computers and Security 49 (2015) 70-94

Kenneth Geers, Heading off Hackers: Criminals wield Computers as Cheap, Anonymous Weapons. Per Concordia Journal of European Security and Defense Issues Volume 2

Oscar Jonsson, The Evolution of Russian Hybrid Warfare: EU/NATO. Center for European Policy Analysis, January 29, 2021

Jan Kallberg, Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations. United States Military Academy 2015

Χρήστος Βεράτης, Κυβερνοχώρος-Κυβερνοεπιθέσεις-Κυβερνοάμυνα Μέρος 1ο. Κέντρο Διεθνών Στρατηγικών Αναλύσεων (ΚΕΔΙΣΑ), 26 Νοεμβρίου 2015

Johann-Cristoph Woltag, Cyber Warfare. Max Planck Encyclopedia of Public International Law, August 2015

Robin A. Gandhi, William Sousan, Phillip A. Laplante, Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political. IEEE Technology and Society Magazine, February 2011

Δημήτριος Β. Οικονόμου, Ο Κυβερνοπόλεμος ως ασύμμετρη απειλή και το Διεθνές Ανθρωπιστικό Δίκαιο. Η Διεξαγωγή των επιχειρήσεων κατά την άμυνα και την επίθεση. Δημοκρίτειο Πανεπιστήμιο Θράκης 2021

John P. Carlin, Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats. Harvard National Security Journal / Vol. 7

Anca Dinicu, Cyber Threats to National Security. Specific Features and Actors Involved. Buletin Stiintific Nr. 2 (38) 2014

Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, Volume 4, Number 2, Summer 2011

Digmelashvili, Temur (2023) The Impact of Cyberwarfare on the National Security. Future Human Image, Volume 19, 12-19.

Robin A. Gandhi, William Sousan, Phillip A. Laplante, Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political. IEEE Technology and Society Magazine, February 2011

Ryan Shandler, Michael L. Gross, Daphna Canetti, Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis. Journal of Global Security Studies, 8(1), 2023, 1-19

Alex Calvo, Cyberwar is War. Small Wars Journal, Apr. 6 2014

Michael Robinson, Kevin Jones, Helge Janicke, Cyber warfare: Issues and Challenges. Computers and Security 49 (2015) 70-94

Jenny Gesley, Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime. Archiv des Volkerrechts, December 2010

Piret Pernik, Hacking for Influence. Per Concordia Journal of European Security and Defense Issues, Volume 10, Issue 1, 2020

Keir Giles, Prospects for the Rule of Law in Cyberspace. US Army War College (USAWC) Press, 1-24-2017

QUADRI, L.A. & RASAQ, M. O. (2020). Cyber Theatre a Fifth Domain of International Politics: In the Cyberspace, Africa and the rest of the world. AHBV Akdeniz Havzası ve Afrika Medeniyetleri Dergisi, 2(2),98-111.

Daphna Canetti, Michael Gross, Israel Waismel-Manor, Asaf Levanon, Hagot Cohen, How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks. Cyberpsychology, Behavior and Social Networking, Volume 20, Number 2, 2017

Hemen Philip Faga, The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. Baltic Journal of Law & Politics 10:1 (2017): 1–34

Ανδρέας Ν. Λιαρόπουλος, Ρωσικές Πληροφοριακές Επιχειρήσεις: Κυριαρχώντας στο Πληροφοριακό Περιβάλλον. Ναυτική Επιθεώρηση, Τεύχος 612, Τόμος 180 , 2021

Anthony Minaar, Cyberattacks and the Cybercrime Threat of Ransomware to Hospital Healthcare Services during the COVID-19 Pandemic. Acta Criminologica, October 2022

Nirob Hossain, Mahmud Hasan. The Impacts of Cyberattack on SMEs in the USA and Way to Accelerate Cybersecurity. Advances in Social Sciences Research Journal, October 2024

Wojciech Wroblewski, Michal Wisniewski, Cybersecurity in the Context of Hybrid Warfare in Ukraine: Analysis Impact on the Public Sector and Society in Poland. Central European Journal of Security Studies 2023 Vol. 1, Issue 1

Yuchong Li, Qinghui Liu, A Comprehensive Review Study of Cyber-attacks and Cyber Security: Emerging Trends and Recent Developments. Energy Reports & (2021) 8176-8186

Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare. Journal of the National Association of Administrative Law Judiciary. Volume 31, Issue 2, Article 5, 2011

Paul Cornish, David Livingstone, Dave Clemente, Claire Yorke, On Cyber Warfare. Chatham House Report, November 2010

Andrew F. Krepinevich, Cyberwarfare, a Nuclear Option?. Center for Strategic and Budgetary Assessments 2012

Meenu Sharma, Risks of Cyber Security Threats, Cyber Terrorism and Cyber Warfare: an Analysis of Impact and Countermeasures. Nanotechnology Perceptions 20 No. S13 (2024) 824-837

N. MacDonnell Ulsch, *Cyber Threat, How to Manage the Growing Risk of Cyber Attacks*. John Wiley & Sons, Inc., Hoboken, New Jersey 2014.

Keneth Geers, *The Cyber Threat to National Critical Infrastructures: Beyond Theory*. *Information Security Journal: A Global Perspective*, 18:1-7, 2009

Mr. Vivek Kumar Soni, Dr. Prena Soni. *Advanced Science: A Futuristic Approach*. Scieng Publications, 2024

Robert Brose, *Cyber War, Netwar, and the Future of Cyberdefence*. Office of the Director of National Intelligence (ODNI), Ver. 3 2012

Helmi Pillai, *Protecting Europes Critical Infrastructure from Russian Hybrid Threats*. Centre for European Reform, April 2023

Lance Hunter, Craig Albert, Joshua Rutland, *Democracy and Cyberconflict: How Regime Type Affects State-sponsored Cyberattacks*. *Journal of Cyber Policy*, April 2022

MAJ. Joshua A. Mendoza, *Cyber Attacks and the Legal Justification for an Armed Response*. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas 2017

Ioannis Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese, David Upton. *A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding how the Propagate*. *Journal of Cybersecurity*, 2018

Ebru Ogurlu, *International Law in Cyberspace: An Evaluation of the Tallin Manuals*. *Annales de la Faculte de Droit d' Istanbul* 2023

Habib Hasam Al-Badawi, *Tallin Manual as a Legal Approach Towards Cyberwarfare*. *Digital Sovereignty and Cybersecurity* 2022

<https://www.ibm.com/topics/cyber-attack>