ΙΑΝΟΥΑΡΙΟΣ 2022

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

ΚΑΛΟΔΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις, Στρατηγική και Ασφάλεια στο Πανεπιστήμιο Νεάπολις

ΚΑΛΟΔΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Πνευματικά δικαιώματα

Περιεχόμενα

ΑΚΡΩΝΥΜΙΑ 8

Κεφάλαιο 1 – Εισαγωγή 12

1.1 Εισαγωγή 12

1.2 Σκοπός 14

Κεφάλαιο 2 - Θεωρητική Θεμελίωση / Βιβλιογραφική Ανασκόπηση 15

2.1 Βιβλιογραφική Ανασκόπηση 16

Κεφάλαιο 3 - Μεθοδολογία Έρευνας 17

Κεφάλαιο 4 - Παρουσίαση δεδομένων 20

4.1 Κυβερνοχώρος 20

4.2 Κυβερνοπόλεμος 21

4.3 Κυβερνοασφάλεια 24

4.4 Κυβερνοεπιθέσεις 25

4.4.1. Παραδείγματα Κυβερνοεπιθέσεων 25

4.4.2 Τύποι κυβερνοεπιθέσεων 34

4.5 Υβριδικός Πόλεμος 38

4.6 Κυβερνοαποτροπή & Κυβερνοαντοχή 42

4.7 Ο κυβερνοπόλεμος ως σύγχρονη μορφή πολέμου 45

4.8 Κρατικοί δρώντες 46

4.8.1 ΗΠΑ 48

4.8.2 Ρωσία 50

4.8.3 Κίνα 52

4.8.4 Ιράν 53

4.8.5 Τουρκία 54

4.9 Μη κρατικοί δρώντες 55

4.9.1 Απλοί άνθρωποι/Θύματα 56

4.9.2 Χάκερς – Script Kiddies 57

4.9.3 Χάκερς/Ακτιβίστες 58

4.9.4 Χάκερς – Πατριώτες 59

4.9.5 Κυβερνοτρομοκράτες 59

4.9.6 Οργανωμένο κυβερνοέγκλημα 60

4.9.7 Κυβερνοπολιτοφύλακες 60

Κεφάλαιο 5 - Συζήτηση και Σχολιασμός Αποτελεσμάτων 61

5.1 Κατάσταση στην ΕΕ 61

5.2 Ελλάδα 63
5.3 Στρατηγικοί στόχοι αντιμετώπισης κυβερνοπολέμου – Περίπτωση Ελλάδας 66
5.3.1 Προστασία και αντοχή των κρίσιμων υποδομών 67
5.3.2 Ανάπτυξη εθνικής κυβερνοβάσης 69
5.3.3 Δίκτυο κυβερνοασφάλειας & κουλτούρα επιχειρησιακής κυβερνοασφάλειας 72
5.3.4 Ασφάλεια τεχνολογιών νέας γενιάς 73
5.3.5 Αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο 74
5.3.6 Ανάπτυξη διεθνούς συνεργασίας 74
Συμπεράσματα 75
Βιβλιογραφία 79
ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ 81

Κατάλογος Γραφικών Παραστάσεων/Εικόνων/Διαγραμμάτων

Εικόνα 1 25
Εικόνα 2 33
Εικόνα 3 39
Εικόνα 4 57

Ονοματεπώνυμο Φοιτητή: Καλοδάνης Κωνσταντίνος

Τίτλος Μεταπτυχιακής Διατριβής: Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …… από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος) Σπυρίδων Πλακούδας

Μέλος Εξεταστικής Επιτροπής: Σάββας Χατζηχριστοφής

Μέλος Εξεταστικής Επιτροπής: Μερσίλεια Αναστασιάδου

Θα ήθελα να εκφράσω τις θερμές ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Πλακούδα Σπυρίδων, για την καθοδήγηση και τη συνδρομή του.

Η παρούσα διπλωματική εργασία αφιερώνεται στα παιδιά και τη σύζυγό μου για την υποστήριξή τους και την υπομονή που έκαναν όλο το προηγούμενο διάστημα.

ΑΚΡΩΝΥΜΙΑ

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
BBC	British Broadcasting Corporation
CSIRT	Computer Security Incident Response Team
DESC	Dubai Electronic Security Center
DDOS	Distributed Denial of Service
DoD	Department of Defense
DOS	Denial of Service
ECCC	European Cybersecurity Competence Centre
FBI	Federal Bureau of Investigation
FSB	Federal'naya Sluzhba Bezopastnosti
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GRU	Glavnoye Razvedyvatelnoye Upravlenie
ICTA	Information and Communication Technologies Authority
INFOSEC	Information Security
IoT	Internet of Things
LAN	Local Area Network
MIT	Millî İstihbarat Teşkilatı
MVD	Министерство внутренних дел
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PACAC	Public Administration and Constitutional Affairs Committee
PLC	Programmable Logic Controller
RMA	Revolution in Military Affairs
SCADA	Supervisory control and data acquisition
SOC	Security Operations Center
SORM	Система оперативно-разыскных мероприятий
SSRN	Social Science Research Network
TAO	Tailored Access Operations

TGS	Turkish Ground Services
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
WAN	Wide Area Network
Γ.Ε.ΕΘ.Α.	Γενικό Επιτελείο Εθνικής Άμυνας
Ε.Δ.	Ένοπλες Δυνάμεις
Ε.Ε	Ευρωπαϊκή Ένωση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
Ε.Υ.Π.	Εθνική Υπηρεσία Πληροφοριών
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
Η/Υ	Ηλεκτρονικός Υπολογιστής
ΜΜΕ	Μέσα Μαζικής Ενημέρωσης
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΦΕΒΥ	Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών

Περίληψη

Το διαδίκτυο παρουσιάζει τα τελευταία χρόνια εξαιρετική ανάπτυξη και πολλές ευαίσθητες πληροφορίες διακινούνται μέσα από αυτό. Η ανοιχτή φύση του διαδικτύου είναι ο λόγος της ευελιξίας του, αλλά ίσως και η αιτία των σπουδαιότερων αδυναμιών του που επιτρέπει την κακόβουλη εκμετάλλευσή του από ικανούς χρήστες.

Στη σημερινή εποχή της ψηφιακής τεχνολογίας, η κυβερνοασφάλεια έχει ανέβει στην κορυφή της λίστας προτεραιοτήτων για σχεδόν κάθε οργανισμό. Πώς να διαφυλάξουν την ακεραιότητα των δεδομένων τους, πώς να προστατεύσουν τους χρήστες και τους πελάτες, αλλά και πώς να προστατεύσουν τη φήμη τους. Ο ψηφιακός πόλεμος, είτε μεταξύ εταιρειών, ατόμων ή κυβερνήσεων, είναι ο νέος τρόπος μάχης στη σύγχρονη εποχή. Είναι κρίσιμο για όλους τους οργανισμούς, μεγάλους και μικρούς, να μπορούν να προστατεύουν τα δεδομένα τους διασφαλίζοντας παράλληλα την ομαλή και συνεχή λειτουργία των συστημάτων πληροφορικής τους.

Δεδομένου ότι οι τεχνολογικές εξελίξεις καθορίζουν, σε μεγάλο βαθμό, το χαρακτήρα του πολέμου κάθε εποχής, σήμερα η «επανάσταση στην πληροφορία» οδηγεί πλέον σε μία εποχή «πολέμου πληροφοριών» ο οποίος εκδηλώνεται σε πολλά επίπεδα και ένα από αυτά είναι ο κυβερνοπόλεμος. Στην περίπτωση του κυβερνοπολέμου το πλεονέκτημα δε βρίσκεται πλέον στη μάζα ούτε στην κινητικότητα, αλλά στην κατοχή και κατάλληλη αξιοποίηση των πληροφοριών, σε σχέση πάντα με τον αντίπαλο, καθώς και στη γενικότερη εκμετάλλευση του διαδικτύου και της δυνατότητας πρόσβασης σε αυτό από οποιονδήποτε.

Ο κυβερνοπόλεμος είναι ένας πολλαπλασιαστής ισχύος, ένα όπλο χαμηλού κόστους με υψηλά αποτελέσματα, στον οποίο η εφευρετικότητα και η πρωτοτυπία διαδραματίζουν βασικό ρόλο και αποτελούν σημαντική ασύμμετρη απειλή για την εθνική ασφάλεια και ευημερία των κρατών.

Abstract

The internet has grown tremendously in recent years and a lot of sensitive information is circulating through it. The open nature of the internet is the reason for its flexibility, but also perhaps the cause of its major weaknesses that allow it to be maliciously exploited by capable users.

In today's age of digital technology, cybersecurity has risen to the top of the list of priorities for almost every organization. How to preserve the integrity of their data, how to protect users and customers, but also how to protect their reputation. Digital warfare, whether between companies, individuals or governments, is the new way of fighting in modern times. It is crucial for all organizations, large and small, to be able to protect their data while ensuring the smooth and continuous operation of their computer systems.

As technological developments largely determine the nature of war in every age, today the "information revolution" is now leading to an era of "information warfare" which manifests itself on many levels and one of them is cyber warfare. In the case of cyber warfare, the advantage is no longer in mass or mobility, but in the possession and proper use of information, always in relation to the adversary, as well as in the general exploitation of the internet and the possibility of access to it by anyone.

Cyberwarfare is a power multiplier, a low-cost weapon with high-results, in which ingenuity and originality play a key role and pose a significant asymmetric threat to states' national security and prosperity.

Κεφάλαιο 1 – Εισαγωγή

1.1 Εισαγωγή

Χωρίς αμφιβολία, η εποχή της πληροφορίας είναι εδώ, γνωστή και ως ψηφιακή εποχή, καθώς η ανθρωπότητα βρίσκεται σε διαδικασία πλήρους ψηφιακού μετασχηματισμού και οι εξελίξεις στην τεχνολογία κατέχουν σημαντική θέση στον αγώνα κάθε χώρας για ευρύτερη ανάπτυξη. Η πληροφορία είναι γνώση και η γνώση είναι δύναμη. Συνεπώς, η πληροφορία από μόνη της αποτελεί δύναμη. Η δε σημασία της για τον άνθρωπο, που αποφασίζει και δρα σύμφωνα με αυτό που πιστεύει ότι είναι πραγματικότητα και όχι σύμφωνα με την πραγματικότητα, είναι τεράστια. Η πληροφορία αποτελεί βασικό κριτήριο για τη λήψη κάθε απόφασης. Ολόκληρη η νοημοσύνη του ανθρώπου βασίζεται στην πληροφορία. Τα τελευταία χρόνια είναι απίστευτος ο όγκος των πληροφοριών που διακινείται μέσω του διαδικτύου. Οι εξελίξεις αυτές σημειώνονται με ταχείς ρυθμούς σε όλους τους τομείς της ανθρώπινης δραστηριότητας. Η συνεχής εξέλιξη και οι αλλαγές που καταγράφονται στον τομέα της τεχνολογίας αφενός προσφέρουν αμέτρητες δυνατότητες και γίνονται αναπόσπαστο κομμάτι της ζωής κάθε ανθρώπου (π.χ. κινητά τηλέφωνα, tablets, IoT, 5G, Quantum Computing κ.λπ.), καθώς η τεχνολογία της πληροφορίας και της επικοινωνίας επεκτείνεται, αφετέρου μας εκθέτει σε κινδύνους για την ασφάλεια στον κυβερνοχώρο. Οι αλλαγές σε όλες τις πτυχές της ανθρώπινης δραστηριότητας θεωρούνται και όχι άδικα ως κοσμογονικές, συμπεριλαμβανομένης της εσωτερικής ασφάλειας και της κρατικής άμυνας. Δεδομένων των απειλών του κυβερνοχώρου, η υπεράσπιση της εθνικής ασφάλειας κάθε χώρας με την αντιμετώπιση των απειλών στον κυβερνοχώρο έχει καταστεί κορυφαία προτεραιότητα για όλες τις ανεπτυγμένες χώρες. Όσο πιο τεχνολογικά προηγμένα έθνη εξαρτώνται από συστήματα πληροφοριών, τόσο πιο ευάλωτα γίνονται.

Ιστορικά, από τότε που το διαδίκτυο άρχισε να γίνεται ένα κοινό χαρακτηριστικό στη ζωή όλων των ανθρώπων, οι χάκερς θεωρούνται μια σημαντική απειλή. Αυτή η άποψη έχει επανειλημμένα εδραιωθεί και διανεμηθεί από την κάλυψη και τα σχόλια των μέσων ενημέρωσης όλα αυτά τα χρόνια. Αντίθετα, τα πρώτα είκοσι (20) χρόνια του διαδικτύου ήταν αποδεκτά ασφαλές λόγω των περιορισμένων ικανοτήτων των επιτιθέμενων, σε σύγκριση με την απειλή που παράγεται από ένα στρατιωτικοποιημένο διαδίκτυο με κρατικούς φορείς που διεξάγουν επιχειρήσεις στον κυβερνοχώρο. Στην πραγματικότητα, το διαδίκτυο έχει μια αντίστροφη τροχιά για την ασφάλειά του, έχει γίνει πιο ανασφαλής με την πάροδο του χρόνου και μετατράπηκε από απειλή για το άτομο σε απειλή για την εθνική ασφάλεια (Libicki, 2007). Η είσοδος κρατικών παραγόντων δημιουργεί έναν αμφισβητούμενο κυβερνοχώρο όπου οι πληροφορίες, η οικονομική κατασκοπεία, οι επιχειρήσεις πληροφοριών και οι ψυχολογικές επιχειρήσεις άλλαξαν ριζικά τα θεμελιώδη στοιχεία για την ασφάλεια του διαδικτύου. Ο κρατικός παράγοντας επιδιώκει να εκμεταλλευτεί τις αδυναμίες στη στοχευμένη εθνική υποδομή, τη σύνδεση της βιομηχανικής βάσης με το παγκόσμιο δικτυακό δίκτυο και να εκμεταλλευτεί το γεγονός ότι οι πληθυσμοί πλέον βασίζονται σε μεγάλο βαθμό στο διαδίκτυο. Το επιθετικό κράτος έχει ένα πλεονέκτημα στον κυβερνοχώρο λόγω των αδυναμιών στην απόδοση, που λειτουργούν ως μόνιμη πρόσκληση για τη διεξαγωγή πολέμων μεσολάβησης, χρησιμοποιώντας εγκληματικά δίκτυα ή ευθυγραμμισμένες πολιτικές ομάδες, για να πραγματοποιήσει τις επιθέσεις με μικρό κίνδυνο εντοπισμού. Αυτό απαιτεί μια τροποποιημένη άποψη για τον ρόλο του κυβερνοχώρου στην εθνική ασφάλεια.

Το διαδίκτυο πρωτοδημιουργήθηκε για να εξυπηρετήσει στρατιωτικές ανάγκες την εποχή του ψυχρού πολέμου την δεκαετία του 1960 (ARPANET - Advanced Research Project Agency). Οι δυνατότητες του Διαδικτύου επεκτάθηκαν την δεκαετία του ‘70 με την εισαγωγή του ηλεκτρονικού ταχυδρομείου και τη δυνατότητα μεταφοράς αρχείων. Στην συνέχεια, στην αρχή της δεκαετίας του ‘80 άρχισε η χρήση του συστήματος

ονοματολογίας DNS καθώς και η υιοθέτηση ενός ενιαίου πρωτοκόλλου μετάδοσης πληροφοριών. Μέχρι τα τέλη της δεκαετίας του 1980 είχαν συγχωνευθεί τα περιφερειακά δίκτυα της Αμερικής και αρκετών άλλων χωρών ώστε να αποτελέσουν την πρώτη μορφή του παγκόσμιου δικτύου και το 1991 καταργήθηκε κάθε περιορισμός για την εμπορική ελεύθερη χρήση του διαδικτύου. Το διαδίκτυο παρουσιάζει τις τελευταίες δύο δεκαετίες εξαιρετική ανάπτυξη. Αν και ξεκίνησε ως δίκτυο μεταφοράς απλών κειμένων, σήμερα, οι δυνατότητες του διαδικτύου έχουν αυξηθεί τρομερά. Στη σημερινή εποχή, αφενός η ποιότητα των παρεχόμενων υπηρεσιών διαρκώς βελτιώνεται και ολοένα και περισσότερα δίκτυα συνδέονται σε αυτό, αφετέρου παρατηρείται έλλειψη ασφάλειας κατά τη χρήση του, οπότε τίθεται το ερώτημα εάν είναι δυνατή ή όχι η προστασία της οικονομικής, βιομηχανικής και δημόσιας υποδομής από κυβερνοεπιθέσεις (Streltsov 2015).

Οποιαδήποτε στρατιωτική ενέργεια έχει στόχο να νικήσει τον αντίπαλο με τις λιγότερες πιθανές απώλειες στο συντομότερο χρονικό διάστημα. Το πεδίο μάχης στον «κυβερνοπόλεμο» είναι ο κυβερνοχώρος, δηλαδή ένα πεδίο μάχης στο φάσμα του διαδικτύου που στερείται φυσικού χώρου. Ο κυβερνοχώρος αναφέρεται στο παγκόσμιο δίκτυο ανθρώπων, επιχειρήσεων, υπηρεσιών και άλλων οντοτήτων που συνδέονται με υπολογιστές και τηλεπικοινωνίες, ανεξάρτητα από τη φυσική τους θέση.

1.2 Σκοπός

Σκοπός της παρούσης διατριβής είναι η μελέτη και ο προσδιορισμός της αξίας που έχει και του ρόλου που μπορεί να διαδραματίσει ο κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος, μεταξύ αντιπάλων ή δυνητικά αντιπάλων δυνάμεων. Επιπλέον, στην παρούσα διατριβή θα παρουσιαστούν η φύση και τα ιδιαίτερα χαρακτηριστικά του κυβερνοχώρου και του κυβερνοπολέμου και οι δυνατότητες επίτευξης πολιτικών/στρατιωτικών επιδιωκόμενων αποτελεσμάτων μιας χώρας έναντι μιας άλλης. Τέλος, θα αναφερθούν οι απειλές που αντιμετωπίζει η Ελλάδα και θα υπογραμμιστούν οι ξεχωριστές και ιδιαίτερα

χρήσιμες δυνατότητες που παρέχει στην Ελλάδα η αξιοποίηση του διαδικτύου, και κατά συνέπεια η υπεροχή στον πόλεμο μέσω αυτού και διατυπώνονται προτάσεις για την εφαρμογή αμυντικών, αλλά και επιθετικών επιχειρήσεων κυβερνοπολέμου. Η πρωτοτυπία του θέματος έγκειται στο γεγονός ότι παρουσιάζονται πολλές παράμετροι της κυβερνοασφάλειας και του κυβερνοπολέμου και θα παρουσιαστούν στρατηγικοί στόχοι που πρέπει να καθορισθούν ώστε η Ελλάδα να έχει την αποτρεπτική ισχύ να αντιμετωπίσει τις μελλοντικές προκλήσεις.

Κεφάλαιο 2 - Θεωρητική Θεμελίωση / Βιβλιογραφική Ανασκόπηση

Στη σημερινή εποχή, η ασφάλεια ενός πληροφοριακού συστήματος καθώς και η προστασία των προσωπικών δεδομένων θεωρούνται απαραίτητες. Μελέτες και αναφορές για τρέχοντα θέματα ασφάλειας δικτύων και πληροφοριών καθώς και μελέτη νέων τεχνολογιών όπως η Τεχνητή Νοημοσύνη, η Σύγχρονη Υποδομή Δικτύων (5G), οι εφαρμογές IoT εκπονούνται από την ακαδημαϊκή κοινότητα με θέμα την ασφάλεια στον κυβερνοχώρο (κυβερνοασφάλεια), τις επιθέσεις στον κυβερνοχώρο (κυβερνοεπιθέσεις) και πως ο κυβερνοχώρος έρχεται να επηρεάσει δραστικά και το μέγεθος της κάθε χώρας στη γεωστρατηγική σκακιέρα καθώς ο κυβερνοπόλεμος δεν βασίζεται σε πανάκριβους εξοπλισμούς παρά μόνο στην εξειδίκευση του ανθρώπινου δυναμικού, στην εσωτερική οργάνωση και στη στρατηγική της χώρας. Μικρές χώρες μπορούν να ταπεινώσουν μεγαλύτερες και πιο ισχυρές.

2.1 Βιβλιογραφική Ανασκόπηση

Η βιβλιογραφική ανασκόπηση δείχνει ότι δεν υπάρχει κοινή διεθνής κατανόηση του τι συνιστά κυβερνοπόλεμο (Mueller, 2014), (Chauvin, 2016). Έννοιες όπως η κατασκοπεία στον κυβερνοχώρο, η κυβερνοεπίθεση, ο πόλεμος στον κυβερνοχώρο και ακόμη και το έγκλημα στον κυβερνοχώρο συχνά συγχέονται. Για να καταδείξουν το θέμα, το 2014 οι Singer και Friedman έγραψαν ότι ο ορισμός του κυβερνοπολέμου δεν χρειάζεται να είναι περίπλοκος. Συζητώντας τα βασικά στοιχεία του πολέμου στον κυβερνοχώρο, τα θεωρούν παρόμοια με τον πόλεμο σε άλλους τομείς. Υπάρχει πάντα ένας πολιτικός στόχος και τρόπος και πάντα ένα στοιχείο βίας (Singer & Friedman, 2014). Ωστόσο, μια κυβερνοεπίθεση δεν ισοδυναμεί με κυβερνοπόλεμο. Στα μάτια του Thomas Rid, πρέπει πρώτα να είναι ξεκάθαρο εάν μια κυβερνοεπίθεση μπορεί πράγματι να χαρακτηριστεί ως πράξη πολέμου (Rid, 2013). Πολλοί άλλοι ερευνητές πιστεύουν ότι για να θεωρηθούν κάποια κυβερνοπεριστατικά ως κυβερνοπόλεμος, θα πρέπει να συνοδεύονται και από εχθροπραξίες ή ενέργειες συμβατικού πολέμου, όπως για παράδειγμα στη Γεωργία και την Ουκρανία. Παρόλο που αυτά τα έργα προσφέρουν κρίσιμες γνώσεις σχετικά με τις ενέργειες που λαμβάνουν χώρο στον κυβερνοχώρο και μπορούν να χαρακτηριστούν και ως κυβερνοπόλεμος και τις επιπτώσεις αυτής της νέας προσθήκης στην πολεμική αρένα και στον τομέα της ασφάλειας, ολοκληρώνουν ωστόσο την ανάλυσή τους χωρίς να αναφέρουν μέτρα που πρέπει να ληφθούν από τις χώρες για αντιμετώπιση τέτοιων περιστατικών.

Επίσης, το 2020 κυκλοφόρησε και η Εθνική Στρατηγική Κυβερνοασφάλειας της Ελλάδας που θέτει τα βασικά σημεία για τα επόμενα 5 χρόνια. Παρακάτω, παραθέτω ορισμένους στρατηγικούς στόχους που λείπουν από την υπάρχουσα εθνική στρατηγική ή αναφέρονται επιγραμματικά και πιστεύω ότι με την υιοθέτηση αυτών και το ορισμένες αλλαγές στο υπάρχον θεσμικό πλαίσιο για τις αρμοδιότητες των φορέων που ασχολούνται

με θέματα κυβερνοχώρου, η χώρα μπορεί να μετασχηματιστεί πλήρως αλλάζοντας ταυτόχρονα επίπεδο.

Τέλος, παρατίθενται τα αποτελέσματα μιας βιβλιογραφικής ανασκόπησης σχετικά με τους φορείς που έχουν θεσπιστεί να διαδραματίζουν κύριο ρόλο και να εφαρμόζουν πολιτικές σχετικά με τον κυβερνοχώρο στην Ελλάδα. Το κύριο ερώτημα που προκύπτει είναι αν μπορεί η συγκεκριμένη δομή μπορεί να εφαρμόσει την πολιτική και να αμυνθεί αποτελεσματικά σε κατάσταση κυβερνοεπιθέσεων ή ευρύτερου κυβερνοπολέμου.

Συνοπτικά, αυτή η διπλωματική διατριβή φιλοδοξεί να επιτύχει δύο αλληλένδετους στόχους: πρώτα απ 'όλα, να προσφέρει μία εκτενής παρουσίαση των κύριων συστατικών του κυβερνοπολέμου · και δεύτερον, να φωτίσει τα κενά που υπάρχουν στη στρατηγική της χώρας για τη διασφάλιση της εθνικής της κυριαρχίας αλλά και τη μετεξέλιξή της σε σπουδαίο φορέα του κυβερνοχώρου στη νοτιοανατολική Ευρώπη .

Κεφάλαιο 3 - Μεθοδολογία Έρευνας

Αυτή η εργασία ισοδυναμεί με μια μελέτη περίπτωσης, με άλλα λόγια «εμπειρική έρευνα που εξετάζει ένα φαινόμενο εντός της πραγματικής του διάστασης» (Yin, 2003). Η μεθοδολογία που χρησιμοποιήθηκε στην παρούσα διατριβή, παρουσιάζεται σε αυτή την ενότητα, ώστε να γίνει κατανοητός ο τρόπος της προσπάθειας εκπλήρωσης του σκοπού της διατριβής.

Κάθε μελέτη απαιτεί μια επιστημονικά εγκεκριμένη μέθοδο επεξεργασίας που παρέχει δύο από τα πιο σημαντικά χαρακτηριστικά της: ακρίβεια και επαλήθευση. Τα στάδια της μεθοδολογίας, που ακολουθήθηκαν, ήταν βασισμένα κυρίως στις ποιοτικές μεθόδους έρευνας και όχι στις ποσοτικές (Ζαφειρόπουλος 2015). Δεδομένου ότι αυτή η μελέτη εξετάζει ένα φαινόμενο το οποίο ανήκει κατά βάση στις κοινωνικές επιστήμες (Νόβα-Καλτσούνη, 2006) και που εξακολουθεί να βρίσκεται σε εξέλιξη, χρησιμοποιήθηκε

η ποιοτική μέθοδος έρευνας: ανάλυση περιεχομένου δευτερογενών πηγών (π.χ. περιοδικά, άρθρα). Αυτή η ποιοτική μέθοδος προσφέρει ευδιάκριτα πλεονεκτήματα: εξετάζει τα γεγονότα χωρίς καμία εξωτερική παρέμβαση από τον ερευνητή και, το πιο σημαντικό, «διερευνά το γιατί και πώς της λήψης αποφάσεων και όχι μόνο τι, πού, πότε. » (Bryman, 2004).

Για να διεξαχθεί μια ποιοτική έρευνα, πρέπει να ακολουθηθούν συγκεκριμένα στάδια. Το πρώτο στάδιο ήταν ο προσδιορισμός του φαινομένου και στη συνέχεια, αναζητήθηκαν συναφείς έρευνες ή προσεγγίσεις. Έπειτα, διατυπώθηκαν ερευνητικά ερωτήματα και βρέθηκαν «κενά» που η παρούσα διατριβή επέλεξε να καλύψει.

Αναλυτικότερα λοιπόν, πραγματοποιήθηκε εκτεταμένη βιβλιογραφική έρευνα (επιστημονικά άρθρα, διατριβές μεταπτυχιακές - διδακτορικές, βιβλία) ώστε να υπάρξει καταγραφή όλων όσων έχουν ήδη ειπωθεί για τη θεματολογία που πραγματεύεται η διατριβή. Επίσης, χρησιμοποιήθηκαν πρωτογενείς πηγές (π.χ. εθνική στρατηγική κυβερνοασφάλειας (2020), έγγραφα και οδηγίες διεθνών οργανισμών). Πιο συγκεκριμένα οι πηγές όπου αντλήθηκαν τα στοιχεία της έρευνας, είναι βιβλιογραφική ανασκόπηση μέσα από τεκμήρια από θεσμικούς φορείς, άρθρα σε επιστημονικά περιοδικά, μελέτες, διατριβές, πηγές αξιόπιστες και έγκυρες από το διαδίκτυο και τέλος βασικής βιβλιογραφίας. Η αναζήτηση και ο εντοπισμός των άρθρων έγινε στους παρακάτω ιστότοπους και φορείς: Academia, SSRN, Inquiries Journal, SpringerLink, Google Scholar και Wiley Online. Έτσι μέσα από τα αποτελέσματα της αναζήτησης που πραγματοποιήθηκε στους παραπάνω φορείς και ιστότοπους, κατάφερα να μελετήσω ένα αρκετά ικανοποιητικό αριθμό άρθρων. Στη συνέχεια, έγινε επεξεργασία αυτών και αναλύθηκαν και μέσω αυτής της διαδικασίας προέκυψε η ανάγκη να καταγραφούν οι στρατηγικοί στόχοι που πρέπει να ακολουθηθούν ώστε η Ελλάδα να έχει την ικανότητα αντιμετώπισης των μελλοντικών προκλήσεων που απορρέουν από τον τομέα της κυβερνοασφάλειας και γενικότερα του κυβερνοχώρου. Λόγω της ευαίσθητης φύσης αυτού

του έργου, δόθηκε επιπλέον έμφαση στη διάκριση των ψεύτικων ειδήσεων και της προπαγάνδας από τα γεγονότα και, για το σκοπό αυτό, χρησιμοποιήθηκε και τριγωνισμός πηγών.

Κεφάλαιο 4 - Παρουσίαση δεδομένων

4.1 Κυβερνοχώρος

Με τον όρο «κυβερνοχώρος», ο οποίος επικράτησε του όρου «κυβερνοδιάστημα», υποδηλώνεται το περιβάλλον που έχει δημιουργηθεί από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές. Παραδείγματα τέτοιων δικτύων αποτελούν τα τοπικά δίκτυα (LANs) – στα οποία ορισμένοι ηλεκτρονικοί υπολογιστές είναι συνδεδεμένοι μεταξύ τους, μέσα στο ίδιο δωμάτιο ή στο ίδιο κτήριο με σκοπό να εξυπηρετείται η δίοδος των πληροφοριών και να διευκολύνονται οι επικοινωνίες - και τα ευρείας εμβέλειας δίκτυα (WANs) όπως το γνωστό διαδίκτυο (Internet), το διεθνές δίκτυο για ακαδημαϊκούς και ερευνητές, τα οποία έχουν σκοπό να εξυπηρετούν τις ίδιες δραστηριότητες σε εθνικά και παγκόσμια δίκτυα.

Ο κυβερνοχώρος αναδύθηκε ως αποτέλεσμα του ανταγωνισμού ισχύος της ψυχροπολεμικής περιόδου, στις ΗΠΑ. Στο παρελθόν, οι απειλές από το εξωτερικό, μπορούσαν να αντιμετωπιστούν στο εξωτερικό. Πλέον, τα γεωγραφικά όρια δεν διασφαλίζουν τη διατήρηση της απειλής έξω από τη χώρα.

Ωστόσο, για να υπάρχει κάθε είδους χώρος, είναι απαραίτητο να υπάρχουν σταθερά σημεία αναφοράς και ο κυβερνοχώρος στερείται διαστάσεων, σαφώς καθορισμένων ορίων και ακίνητων σημείων προσανατολισμού, ενώ ο φυσικός χώρος έχει. Ο άνθρωπος και οι πράξεις του είναι τα μόνα σημεία αναφοράς μέσα σε αυτόν.

Συνεπώς, τα μηνύματα που ανταλλάσσουν οι χρήστες μέσω Η/Υ, αποτελούν τμήμα του κυβερνοχώρου, ενώ το ίδιο συμβαίνει και με την επίσκεψη στους ιστοτόπους. Ο κυβερνοχώρος όμως δεν σταματάει εκεί. Θα μπορούσε να ειπωθεί πως όλα τα παραπάνω αποτελούν απλώς την ορατή πλευρά του, μια και συνιστούν την ενσυνείδητη αποτύπωση

σε ηλεκτρονική μορφή σκέψεων ή πράξεων που προορίζονται για μελλοντική αξιοποίηση από άλλους ανθρώπους ή από τους ίδιους τους χρήστες.

Για έναν Η/Υ που δεν είναι συνδεδεμένος σε κάποιο δίκτυο, ο κυβερνοχώρος είναι ατομικός και εύκολα ελέγξιμος. Μπορεί να ρυθμιστεί έτσι ώστε να υπάρχει αποκλειστική πρόσβαση στο περιεχόμενό του και επιπλέον υπάρχει η δυνατότητα, αν ο χρήστης έχει τις κατάλληλες τεχνικές γνώσεις, να εξαφανίσει τα ίχνη των πράξεων του μέσα σε αυτόν. Δυστυχώς όμως, ο ατομικός κυβερνοχώρος έχει πολύ μικρή έκταση. Γι' αυτό, όλο και περισσότεροι άνθρωποι αποφασίζουν να "αποικίσουν" τον παγκόσμιο κυβερνοχώρο συνδέοντας τον προσωπικό υπολογιστή τους με πολλούς άλλους. Γίνονται λοιπόν μέλη μιας ευρύτερης κοινότητας και, όπως συμβαίνει σε όλες τις κοινότητες, οι πράξεις και οι παραλήψεις τους αρχίζουν να επηρεάζουν τους γύρω τους και να επηρεάζονται από αυτούς. Ως αποτέλεσμα, ένα από τα πιο δημοφιλή θέματα συζήτησης μεταξύ των χρηστών του διαδικτύου σήμερα είναι ο βαθμός στον οποίο μια διαδικτυακή κοινότητα μπορεί να ασκήσει έλεγχο στα μέλη της, καθώς και οι κανόνες που διέπουν τις σχέσεις μεταξύ των μελών της κοινότητας.

4.2 Κυβερνοπόλεμος

Τα πιο «δελεαστικά» χαρακτηριστικά της απόπειρας για εγκληματική ενέργεια στον κυβερνοχώρο είναι η αφανής ταυτότητα, το ελάχιστο κόστος και η ταχύτητα, στοιχεία που προσδίδουν πολύ χαμηλό ρίσκο σε όποια προσπάθεια. Κάθε συντονισμένη ενέργεια, η οποία αποσκοπεί να πλήξει την ισχύ ενός κράτους και για πεδίο μάχης χρησιμοποιεί τον κυβερνοχώρο, καλείται απειλή κυβερνοπολέμου. Άρα, από τη φύση του ο κυβερνοπόλεμος έχει μία τεράστια διαφορά από τον παραδοσιακό πόλεμο. Δεν υπακούει σε χρονοχωρικούς περιορισμούς, δηλαδή, δεν έχει επίσημη αρχή και τέλος, και δε

λαμβάνει χώρα σε συγκεκριμένη εδαφική έκταση. Ιστορικά, τα πρώτα σημάδια του διακρίνονται με την εμφάνιση του κυβερνοχώρου.

Η επανάσταση της πληροφορικής και των καινοτομιών που προήλθαν από αυτήν αλλάζουν την φύση της σύγχρονης αντιπαράθεσης δύο δυνητικών αντιπάλων και της μορφής των στρατιωτικών δομών, δογμάτων, στρατηγικών και τακτικών που θα χρησιμοποιηθούν σε μια ενδεχόμενη αναμέτρηση. Στον σύγχρονο πόλεμο, ούτε το πλήθος των δυνάμεων που αντιπαρατίθενται ούτε η υπεροπλία, αλλά η καλή γνώση του αντιπάλου και ο επηρεασμός της δικής του αντίληψης θα κρίνουν το αποτέλεσμα. Είναι ο πόλεμος στον οποίο η ρήση του μεγάλου θεωρητικού της στρατηγικής Carl von Clausewitz *" Η γνώση πρέπει να εξελιχθεί σε δυνατότητα"* (Carl von Clausewitz, 2012), έχει εφαρμογή όσο ποτέ άλλοτε.

Στην διεθνή βιβλιογραφία το νέο αυτό είδος πολέμου αναφέρεται με πλήθος αδόκιμων όρων οι οποίοι προσπαθούν να περιγράψουν τις δυνατότητες του και την επίδραση του στις επιχειρήσεις. Έτσι εμφανίζεται σαν «κυβερνοπόλεμος»(Cyberwar), «Πληροφοριακός ή Πληροφορικός Πόλεμος» (Information Warfare ή Info war), «Πόλεμος Δικτύων» (Net-war) ενώ παράλληλα εμπλέκεται με άλλες δραστηριότητες που περιγράφονται από επίσης συναφείς αδόκιμους όρους, όπως τις «Πληροφοριακές Επιχειρήσεις», τον «Δικτυοκεντρικό Πόλεμο», τον «Πόλεμο Διοικήσεως και Ελέγχου», τον «Πόλεμο των ΜΜΕ» κλπ.

«Κυβερνοπόλεμος» (Cyberwar) είναι το σύνολο των ενεργειών στον κυβερνοχώρο μέσω συστημάτων πληροφορικής, με σκοπό την υποβάθμιση της δυνατότητας αξιοποίησης του και απαγόρευση εκμετάλλευσής του από τον αντίπαλο, με ταυτόχρονη διατήρηση της αντίστοιχης δυνατότητας από τη φίλια χώρα. Οι τρεις βασικές μορφές του κυβερνοπολέμου είναι η προσβολή του εχθρικού πληροφοριακού συστήματος, η προστασία του αντίστοιχου φίλιου συστήματος και σε περίπτωση συμπλοκής, η υποστήριξη των στρατιωτικών επιχειρήσεων.

Σε περιόδους κρίσεως ή πολέμου, ο κυβερνοπόλεμος δεν διαφέρει και δεν διαχωρίζεται από τις κλασσικές στρατιωτικές επιχειρήσεις. Η δράση του είναι συνήθως επικουρική προς αυτές και έχει σκοπό να τις υποστηρίξει στερώντας από τον εχθρό τη δυνατότητα να πάρει τις σωστές αποφάσεις. Η πρόσβαση σε ένα πληροφοριακό σύστημα τις περισσότερες φορές προσβλέπει σε ένα ή περισσότερους από τους παρακάτω στόχους:

- Υποκλοπή πληροφοριών, με σκοπό την μείωση της αβεβαιότητας κατά την εκτέλεση των επιχειρήσεων.
- Επιθέσεις σε κρίσιμες υποδομές της χώρας - στόχου ώστε να επηρεαστεί η καθημερινότητα των πολιτών της.
- Παραπλάνηση του εχθρού, προκειμένου αυτός να αποκτήσει εσφαλμένη αντίληψη της πραγματικότητας και να χάσει την εμπιστοσύνη του στα μέσα από τα οποία αντλεί την πληροφόρηση του.
- Άρνηση παροχής υπηρεσιών (DOS, DDOS) σε ζωτικά συστήματα, ώστε να μην δύναται να τα χρησιμοποιήσει κατά την περίοδο των επιχειρήσεων, ή ακόμη και σε περίοδο ειρήνης.

Σε παγκόσμιο επίπεδο οι επιχειρήσεις κυβερνοπολέμου αναπτύσσονται οργανωμένα από κράτη που θεωρούν ότι με ελάχιστο κόστος, μπορούν να απειλήσουν ηγέτιδες δυνάμεις και να ασκήσουν από την πλευρά τους πίεση και πολιτική, όπως για παράδειγμα η Κίνα και η Ρωσία εναντίον των ΗΠΑ, το Πακιστάν εναντίον της Ινδίας κ.α. Ο κυβερνοπόλεμος είναι μια εκτεταμένη κατάσταση δικτυακών συγκρούσεων με αντιπάλους οι οποίοι είναι διατεθειμένοι να εξουθενώσουν ο ένας τον άλλο, ακριβώς όπως και στην περίπτωση του πραγματικού πολέμου, ο οποίος μπορεί να διεξαχθεί με σκληρότητα και ένταση (hard - cyberwarfare) ή με ήπια ένταση (soft - cyberwarfare).

Χαρακτηριστική είναι η εκτίμηση του Αμερικανικού Πενταγώνου (DoD, 2016), «ότι μια ομάδα από πολύ καλά συντονισμένους και προετοιμασμένους hackers, όχι περισσότερους από 30 στον αριθμό, οι οποίοι θα μπορούσαν να τοποθετηθούν στρατηγικά

σε διάφορες τοποθεσίες στον κόσμο, με ένα προϋπολογισμό λιγότερο από 10 εκατομμύρια δολάρια, θα μπορούσε να γονατίσει τις ΗΠΑ με τις μαζικές κυβερνοεπιθέσεις, που θα μπορούσε να διεξαγάγει»

Οι Ηνωμένες Πολιτείες δίνουν ιδιαίτερα μεγάλη σημασία στην προστασία της πληροφορικής υποδομής τους από κυβερνοεπιθέσεις. Χαρακτηριστικό είναι μάλιστα ότι, ενώ αρχικά αναφέρονταν στον όρο «ηλεκτρονικό Περλ Χάρμπορ» για να περιγράψουν τον κίνδυνο που προκύπτει για τη χώρα από κυβερνοεπιθέσεις, τελικά απέρριψαν τον όρο αυτό ως υπερβολικά αισιόδοξο και τον αντικατέστησαν με τον όρο «ηλεκτρονικό Βατερλώ».

Μια κυβερνοεπίθεση δεν προκαλεί άμεσα θύματα, ενώ δεν προδίδει εύκολα από πού προέρχεται. Οι ιοί των υπολογιστών και τα άλλα κυβερνο-όπλα δεν έχουν ούτε εθνόσημα, ούτε κωδικούς αριθμούς αναγνώρισης. Ο κυβερνοπόλεμος είναι, λοιπόν, ιδανικός για τη «φιλική επίλυση διαφορών», κάτι που ταιριάζει άριστα στον εργαλειακό ρόλο περί πολέμου, που φιλοδοξεί να επαναφέρει η RMA (Επανάσταση στις Στρατιωτικές Υποθέσεις) στο προσκήνιο της ανθρώπινης ιστορίας.

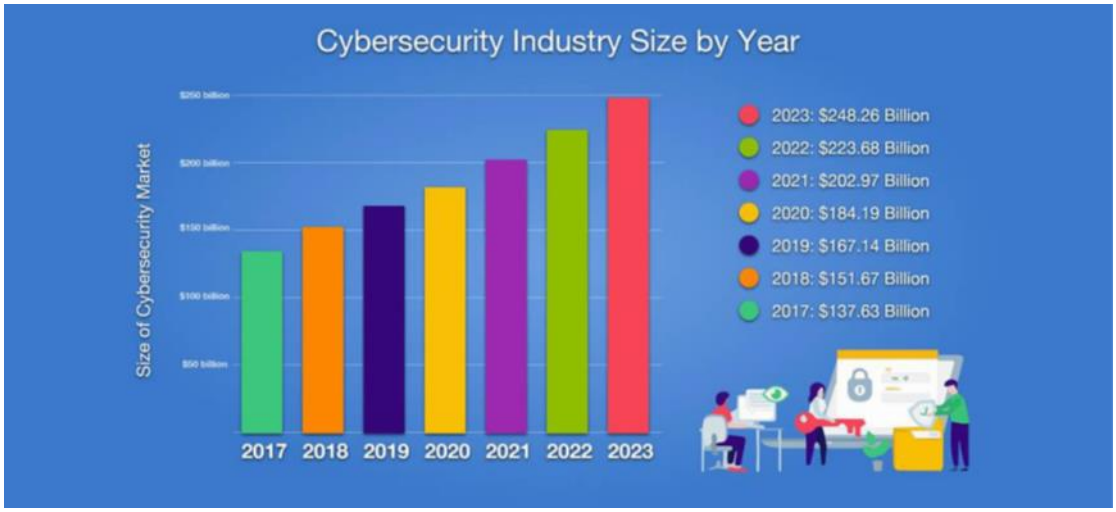
4.3 Κυβερνοασφάλεια

Η ασφάλεια στον κυβερνοχώρο ή κυβερνοασφάλεια είναι η πρακτική της προστασίας οποιωνδήποτε συστημάτων, δικτύων, λογισμικού και διαφόρων τύπων δεδομένων που συνδέονται στο διαδίκτυο από επιθέσεις στον κυβερνοχώρο κάθε είδους.

Αυτές οι επιθέσεις στον κυβερνοχώρο στοχεύουν συνήθως στην απόκτηση πρόσβασης, την τροποποίηση ή την καταστροφή ευαίσθητων πληροφοριών, αλλά μπορούν επίσης να κατευθύνονται και σε άλλους στόχους (εκβιασμός χρημάτων από χρήστες, διακοπή παραδοσιακών επιχειρηματικών διαδικασιών κ.λπ.).

Η εφαρμογή αποτελεσματικών μέτρων ασφάλειας στον κυβερνοχώρο γίνεται ολοένα και πιο δύσκολη στον σημερινό κόσμο, όπου υπάρχουν περισσότερες συσκευές

παρά άνθρωποι και οι εισβολείς γίνονται πιο καινοτόμοι. Όπως φαίνεται στην Εικόνα 1, ο τομέας της κυβερνοασφάλειας εξελίσσεται και αυξάνεται σε καθημερινή βάση. η αύξηση των επενδύσεων στον κυβερνοχώρο από το 2017 έως το 2020 είναι περίπου 47 δισεκατομμύρια, με εκτιμώμενη συνολική αξία 111 δισεκατομμυρίων έως το 2023.



Εικόνα 1

4.4 Κυβερνοεπιθέσεις

Οι επιθέσεις στον κυβερνοχώρο είναι ανεπιθύμητες προσπάθειες κλοπής, έκθεσης, αλλαγής, απενεργοποίησης ή καταστροφής πληροφοριών μέσω μη εξουσιοδοτημένης πρόσβασης σε συστήματα υπολογιστών.

4.4.1. Παραδείγματα Κυβερνοεπιθέσεων

Εσθονία 2007: Η Εσθονία δέχθηκε επίθεση στο τέλος Απριλίου του 20007. Η επίθεση αυτή πραγματοποιήθηκε από Ρώσους. Μετά τη συγκεκριμένη κυβερνοεπίθεση , η Εσθονία πλησίασε τον διεθνή οργανισμό του ΝΑΤΟ αιτούμενη βοήθεια, αλλά τη δεδομένη στιγμή δεν είχε την αρμοδιότητα ούτε και την πολιτική βούληση για να επέμβει. Στη συνέχεια, το ΝΑΤΟ εγκαινίασε το πρώτο Κέντρο Αριστείας Κυβερνοάμυνας στο Ταλίν το 2008.

Κίνα 2007: Ο οργανισμός κρατικής ασφάλειας της Κίνας δημοσιοποίησε την είδηση ότι ξένοι χάκερς από τη Ταϊβάν και τις ΗΠΑ, είχαν προβεί σε κυβερνοεπιθέσεις αποσπώντας διαβαθμισμένες πληροφορίες από κινέζικους οργανισμούς. Μετά από εξονυχιστική εξέταση του δικτύου της China Aerospace Science & της Industry Corporation, εντοπίστηκαν spyware στους Η/Υ του διαβαθμισμένου δικτύου και των διευθυντικών στελεχών.

Γεωργία 2008: Ο πόλεμος μεταξύ Ρωσίας και Γεωργίας καλοκαίρι του 2008 είναι ένα από τα βασικά παραδείγματα κυβερνοπολέμου, ο οποίος βοήθησε στη τόσο άνετη επικράτηση της πρώτης. Η Ρωσία έριξε τις ιστοσελίδες της κυβέρνησης της Γεωργίας και των ΜΜΕ της με αποτέλεσμα να μην έχει τη δυνατότητα ο Πρόεδρος και η κυβέρνηση να έχει επαφή επικοινωνίας με το λαό της χώρας. Επιπλέον, μέσω των εκτεταμένων επιθέσεων, οι Ρώσοι κατάφεραν να παραλύσουν εντελώς τον δημόσιο τομέα της Γεωργίας.

GhostNet 2009: Το GhostNet είναι το όνομα που έδωσαν οι ερευνητές του Information Warfare Monitor σε μια επιχείρηση κυβερνο-κατασκοπείας, μεγάλης κλίμακας, που ανακαλύφθηκε τον Μάρτιο του 2009 (Nagaraja, Anderson, 2009). Η επιχείρηση πιθανότατα σχετιζόταν με μια προχωρημένη επίμονη απειλή (APT) ή με έναν δράστη δικτύου που κατασκόπευε χωρίς να εντοπιστεί. Μετά από έρευνα βρέθηκε ότι η υποδομή λειτουργίας και ελέγχου του GhostNet βασίζεται κυρίως στη Λαϊκή Δημοκρατία της Κίνας και έχει διεισδύσει σε πολιτικές, οικονομικές και ΜΜΕ υψηλής αξίας, τοποθεσίες σε 103 χώρες. Τα συστήματα ηλεκτρονικών υπολογιστών που ανήκαν σε πρεσβείες, υπουργεία Εξωτερικών και άλλα κυβερνητικά γραφεία, καθώς και στα θιβετιανά κέντρα εξορίας του Δαλάι Λάμα στην Ινδία, το Λονδίνο και τη Νέα Υόρκη παραβιάστηκαν.

Ισραήλ 2009: Χάκερς εξαπέλυσαν μια άνευ προηγουμένου επίθεση στην υποδομή του Ισραήλ στο διαδίκτυο κατά τη διάρκεια της στρατιωτικής επίθεσης που πραγματοποίησε το Ισραήλ τον Ιανουαρίο εκείνου του έτους στη Λωρίδα της Γάζας και παρέλυσαν για λίγο κυβερνητικούς ιστότοπους. Το Ισραήλ υποστήριξε ότι η επίθεση, η οποία επικεντρώθηκε σε κυβερνητικούς ιστότοπους, εκτελέστηκε από τουλάχιστον μισό εκατομμύριο υπολογιστές και πραγματοποιήθηκε από τη Χεσμπολάχ.

Ιαπωνία 2010: Τον Σεπτέμβριο του 2010 η Ιαπωνία δέχτηκε επίθεση DDOS στις ιστοσελίδες του Υπουργείου Αμύνης και της αστυνομίας. Τα ιαπωνικά ΜΜΕ υποστήριξαν ότι οι επιθέσεις προήλθαν από την Κίνα λόγω περιστατικού που έλαβε χώρα στις αρχές Σεπτεμβρίου του ίδιου έτους μεταξύ ενός κινέζικου αλιευτικού σκάφους και δύο ιαπωνικών σκαφών της ακτοφυλακής κοντά σε μια αμφιλεγόμενη σειρά νησιών στην ανατολική θάλασσα της Κίνας.

Stuxnet 2010: Το Stuxnet, το σκουλήκι των υπολογιστών που διέκοψε τον πυρηνικό εμπλουτισμό του Ιράν το 2010, είναι η πρώτη περίπτωση επίθεσης σε δίκτυο υπολογιστών που είναι γνωστό ότι προκαλεί φυσική ζημιά πέρα από τα διεθνή σύνορα. Κάποιοι έχουν περιγράψει το Stuxnet ως τον προάγγελο μιας νέας μορφής πολέμου που απειλεί ακόμη και τις ισχυρότερες στρατιωτικές δυνάμεις (Middleton, 2016), (Lindsay, 2013).

Η μεθοδολογία της επίθεσης είχε τα εξής βήματα: α) όταν συνδεόταν με έναν Η/Υ που έτρεχε Windows, το Stuxnet μόλυνε τον υπολογιστή και οποιουσδήποτε αφαιρούμενους δίσκους ήταν συνδεδεμένοι με αυτόν. Κρυβόταν για να μην εντοπιστεί. β) Το Stuxnet αναζητούσε στη συνέχεια τα προγράμματα WinCC και PSC7 της SIEMENS. Αν δεν μπορούσε να εντοπίσει τα προγράμματα, εξαπλωνόταν σε άλλους Η/Υ που είναι συνδεδεμένοι με το δίκτυο. γ) Μόλις το Stuxnet εντόπιζε τα προγράμματα, διαβίβαζε τον μολυσμένο κώδικα στο σύστημα ο οποίος αναπρογραμμάτιζε τους προγραμματισμένους

λογικούς ελεγκτές (PLC). Στην περίπτωση του Ιράν, ο αναπρογραμματισμός έδωσε οδηγίες στα μηχανήματα του σταθμού της Νατάνζ (περιοχή της καρδιάς του πυρηνικού προγράμματος του Ιράν) να επιταχύνουν με αποτέλεσμα να καταστραφούν τα στροφεία των φυγοκεντριστών.

Είναι βέβαιο ότι η SIEMENS συνεργάστηκε με τις ΗΠΑ και το Ισραήλ προκειμένου να εντοπιστούν τα τρωτά σημεία στα συστήματά της ώστε να υπάρξει επιτυχία στη συγκεκριμένη επίθεση.

Καναδάς 2011 : Η καναδική κυβέρνηση ανέφερε τότε μια σοβαρή κυβερνοεπίθεση εναντίον ορισμένων οργανισμών της, συμπεριλαμβανομένου ενός ερευνητικού οργανισμού του Υπουργείο Εθνικής Άμυνας του Καναδά.

Οι διακομιστές της καναδικής κυβέρνησης είχαν χτυπηθεί από κυβερνοεπίθεση που φέρεται να εντοπίστηκε σε διακομιστές υπολογιστών που εδρεύουν στην Κίνα. Οι χάκερ απέκτησαν πρόσβαση σε διαβαθμισμένα κυβερνητικά δεδομένα και ανάγκασαν το Υπουργείο Οικονομικών και το Συμβούλιο Δημοσίου, τις κυριότερες οικονομικές υπηρεσίες του Καναδά, να αποσυνδεθούν από το διαδίκτυο.

Κακόβουλο λογισμικό "Red October", 2012: Το Red October ήταν ένα πρόγραμμα κακόβουλου λογισμικού κυβερνοκατασκοπείας που ανακαλύφθηκε τον Οκτώβριο του 2012 και αποκαλύφθηκε τον Ιανουάριο του 2013 από τη ρωσική εταιρεία Kaspersky (Kaspersky, 2013). Το κακόβουλο λογισμικό φέρεται να λειτουργούσε παγκοσμίως για έως και πέντε χρόνια πριν από την ανακάλυψη, μεταδίδοντας πληροφορίες που κυμαίνονταν από διπλωματικά μυστικά έως προσωπικές πληροφορίες. Οι κύριοι φορείς που χρησιμοποιήθηκαν για την εγκατάσταση του κακόβουλου λογισμικού ήταν μηνύματα ηλεκτρονικού ταχυδρομείου που περιείχαν συνημμένα έγγραφα που εκμεταλλεύονταν ευπάθειες στο Microsoft Word και στο Excel (Kaspersky Lab, 2014). Οι πρωταρχικοί

στόχοι της επίθεσης φαίνεται να ήταν χώρες της ανατολικής Ευρώπης, της πρώην Σοβιετικής Ένωσης και της Κεντρικής Ασίας, αν και χώρες της δυτικής Ευρώπη φαίνεται να ήταν και αυτές θύματα του εν λόγω κακόβουλου λογισμικού. Ο ιός συνέλεξε πληροφορίες από κυβερνητικές πρεσβείες, ερευνητικές εταιρείες, στρατιωτικές εγκαταστάσεις, οργανισμούς παροχών ενέργειας, πυρηνικές και άλλες κρίσιμες υποδομές.

Ν. Κορέα 2013: Τρία μεγάλα χρηματοπιστωτικά ιδρύματα της Νότιας Κορέας καθώς και οι δύο μεγαλύτεροι ραδιοτηλεοπτικοί φορείς της χώρας παρέλυσαν μετά από κυβερνοεπίθεση η οποία έμοιαζε, σύμφωνα με ειδικούς, με προηγούμενες προσπάθειες που είχαν ξεκινήσει από τη βόρεια Κορέα. Η επίθεση άφησε πολλούς Νοτιοκορεάτες ανίκανους να κάνουν ανάληψη χρημάτων από τα ATM και τους ραδιοτηλεπτικούς φορείς με λευκές οθόνες Η/Υ.

Δημοψήφισμα Αγγλίας 2016: Μια έκθεση από μια επιτροπή βρετανών μελών του κοινοβουλίου υποστηρίζει ότι ξένα κράτη όπως η Ρωσία και η Κίνα μπορεί να είχαν παρέμβει στην ψηφοφορία για το Brexit, που οδήγησε στην απόφαση της Βρετανίας να αποχωρήσει από την Ευρωπαϊκή Ένωση. Η Επιτροπή Δημόσιας Διοίκησης και Συνταγματικών Υποθέσεων (PACAC) ανέφερε την κατάρρευση του ιστότοπου εγγραφής ψηφοφόρων της βρετανικής κυβέρνησης, ο οποίος κατέρρευσε στις 7 Ιουνίου, 100 λεπτά πριν από τη λήξη της προθεσμίας εγγραφής στο δημοψήφισμα της χώρας για την ΕΕ. Αν και η κατάρριψη του ιστότοπου δεν επηρέασε ουσιαστικά το αποτέλεσμα του δημοψηφίσματος, ανάγκασε τους υπουργούς να παρατείνουν την προθεσμία για την εγγραφή ψηφοφόρων και οδήγησε σε ανησυχίες ότι δεκάδες χιλιάδες άνθρωποι μπορεί να είχαν μείνει εκτός διαδικασίας.

Αμερικάνικες Προεδρικές εκλογές 2016: Ειδικός εισαγγελέας, Ρόμπερτ Μιούλερ, ερεύνησε τα ευρήματα των αμερικανικών μυστικών υπηρεσιών και του FBI (FBI, 2018) ότι οι Ρώσοι συνωμότησαν για να επηρεάσουν τις εκλογές προς όφελος του Τραμπ. Τα ευρήματα του των αμερικάνικων υπηρεσιών ασφαλείας περιλαμβάνουν την απόκτηση μη εξουσιοδοτημένης πρόσβασης στους υπολογιστές προσώπων και οντοτήτων των ΗΠΑ που ενεπλάκησαν στις προεδρικές εκλογές των ΗΠΑ του 2016, την κλοπή εγγράφων από αυτούς τους υπολογιστές και την απελευθέρωση των κλεμμένων εγγράφων για παρέμβαση στις προεδρικές εκλογές των ΗΠΑ του 2016 κατά του δημοκρατικού κόμματος και της υποψηφίας του (Χίλαρυ Κλίντον).

Κακόβουλο λογισμικό "Petya", 2017: Μια σειρά κυβερνοεπιθέσεων που χρησιμοποιούσαν το κακόβουλο λογισμικό Petya ξεκίνησαν τον Ιούνιο του 2017 και κατέστρεψαν ιστοσελίδες ουκρανικών οργανώσεων, συμπεριλαμβανομένων τραπεζών, υπουργείων, εφημερίδων και επιχειρήσεων ηλεκτρικής ενέργειας. Οι επιθέσεις επηρέασαν αρκετές χώρες, αλλά το 80% όλων των μολύνσεων ήταν στην Ουκρανία (BBC, 2017). Η στοχευμένη επίθεση προκάλεσε κατάρρευση μέρους του τραπεζικού συστήματος της Ουκρανίας, μεγάλου αριθμού ιδιωτικών εταιριών, υπουργείων, εργοστασίων ηλεκτρισμού και των δημόσιων μεταφορών. Ορισμένοι ειδικοί πίστευαν ότι επρόκειτο για επίθεση με πολιτικά κίνητρα κατά της Ουκρανίας.

SolarWinds (ΗΠΑ) 2020: Η SolarWinds, μια μεγάλη αμερικανική εταιρεία τεχνολογίας πληροφοριών, έγινε αντικείμενο κυβερνοεπίθεσης που εξαπλώθηκε στους πελάτες της και παρέμεινε απαρατήρητη για μήνες (Department of Financial Services,2021). Ξένοι χάκερ, που ορισμένοι ανώτατοι αξιωματούχοι των ΗΠΑ πιστεύουν ότι είναι από τη Ρωσία, μπόρεσαν να χρησιμοποιήσουν τη συγκεκριμένη επίθεση για να κατασκοπεύσουν ιδιωτικές εταιρείες όπως η ελίτ εταιρεία κυβερνοασφάλειας FireEye και τα ανώτερα

κλιμάκια της κυβέρνησης των ΗΠΑ, συμπεριλαμβανομένου του Υπουργείου Εσωτερικής Ασφάλειας και του Υπουργείου Οικονομικών. Στις αρχές του 2020, χάκερ εισέβαλαν κρυφά στα συστήματα της SolarWind που εδρεύει στο Τέξας και πρόσθεσαν κακόβουλο κώδικα στο σύστημα λογισμικού της εταιρείας. Οι περισσότεροι πάροχοι λογισμικού στέλνουν τακτικά ενημερώσεις στα συστήματά τους, είτε πρόκειται για διόρθωση σφάλματος είτε για προσθήκη νέων λειτουργιών. Η SolarWinds δεν αποτελεί εξαίρεση. Ξεκινώντας ήδη από τον Μάρτιο του 2020, η SolarWinds απέστειλε άθελά της ενημερώσεις λογισμικού στους πελάτες της που περιλάμβαναν τον παραβιασμένο κώδικα. Ο κώδικας δημιούργησε μια κερκόπορτα στα συστήματα τεχνολογίας πληροφοριών του πελάτη, τα οποία οι χάκερ χρησιμοποίησαν στη συνέχεια για να εγκαταστήσουν ακόμη περισσότερα κακόβουλα λογισμικά που τους βοήθησαν να κατασκοπεύουν εταιρείες και οργανισμούς.

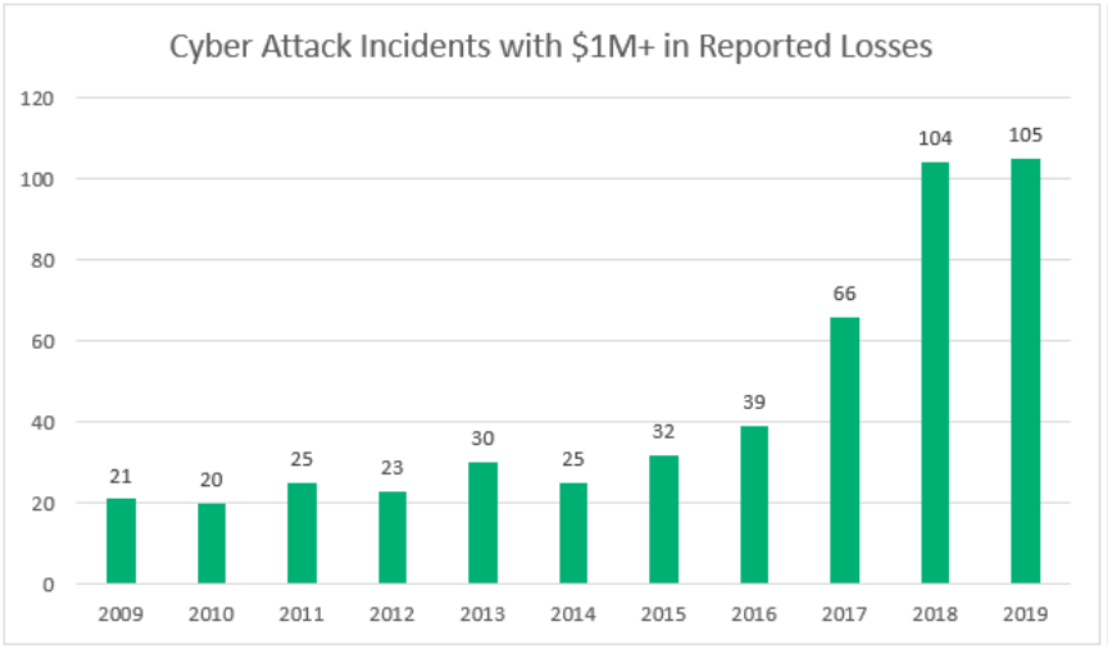
“Lebanese Cedar” APT 2021: Ένας παράγοντας απειλών που συνδέεται με τη Χεζμπολάχ, γνωστός ως Lebanese Cedar, έχει συνδεθεί με εισβολές σε τηλεπικοινωνιακούς φορείς και παρόχους υπηρεσιών διαδικτύου στις ΗΠΑ, το Ηνωμένο Βασίλειο, το Ισραήλ, την Αίγυπτο, τη Σαουδική Αραβία, τον Λίβανο, την Ιορδανία, την Παλαιστινιακή Αρχή και τα Ηνωμένα Αραβικά Εμιράτα. Η εκστρατεία hacking ξεκίνησε στις αρχές του 2020 και ανακαλύφθηκε από την ισραηλινή εταιρεία κυβερνοασφάλειας Clearsky. Σε μια έκθεση που δημοσιεύθηκε, η εταιρεία κυβερνοασφάλειας είπε ότι φαίνεται ότι οι επιθέσεις είχαν σκοπό να συγκεντρώσουν πληροφορίες και να κλέψουν τις βάσεις δεδομένων των τηλεπικοινωνιακών φορέων, που περιέχουν ευαίσθητα δεδομένα. Επίσης, πρόσθεσε ότι μπορεί κανείς να υποθέσει ότι πραγματοποιήθηκε πρόσβαση σε βάσεις δεδομένων που περιέχουν αρχεία κλήσεων και προσωπικά δεδομένα πελατών.

Colonial Pipeline (ΗΠΑ) 2021: Στις 7 Μαΐου 2021, ο Colonial Pipeline, ένα αμερικανικό σύστημα πετρελαιαγωγών που προέρχεται από το Χιούστον του Τέξας και μεταφέρει βενζίνη και καύσιμα αεριωθουμένων κυρίως στις Νοτιοανατολικές Ηνωμένες Πολιτείες, υπέστη κυβερνοεπίθεση ransomware που επηρέασε το υπολογιστικό σύστημα που διαχειρίζεται τον αγωγό (Turton and Mehrotra, 2021). Με τη βοήθεια του FBI, η εταιρία που διαχειρίζεται τον Colonial Pipeline πλήρωσε τα λύτρα που ζητήθηκαν (75 bitcoin ή 4,4 εκατομμύρια δολάρια). Στη συνέχεια, οι χάκερ έστειλαν στην εταιρία μια εφαρμογή λογισμικού για να αποκαταστήσουν το δίκτυό τους, αλλά λειτούργησε πολύ αργά. Ήταν η μεγαλύτερη κυβερνοεπίθεση σε στόχο υποδομής πετρελαίου στην ιστορία των Ηνωμένων Πολιτειών.

Ιράν 2021: Το τρέχον έτος υπήρξε πρωτόγνωρη κυβερνοεπίθεση που προκάλεσε προβλήματα επί πέντε ημέρες στο σύστημα διανομής καυσίμων στο Ιράν, προκλήθηκαν προβλήματα στην κυκλοφορία των οχημάτων στις κεντρικές οδούς της Τεχεράνης λόγω των μεγάλων ουρών που σχηματίστηκαν έξω από τα πρατήρια. Η εν λόγω επίθεση είχε τα ίδια τεχνικά χαρακτηριστικά με δύο αντίστοιχα περιστατικά του παρελθόντος, όπως επισήμαναν ειδικοί από το Ιράν. Τα δύο συμβάντα, ένα αυτό που αφορούσε το σιδηροδρομικό δίκτυο και το άλλο αυτό που σημειώθηκε στο λιμάνι Σαχίντ Ραζαεΐ, έμοιαζαν στον τρόπο της τωρινής επίθεσης. Τον Ιούλιο του 2021 λόγω κυβερνοεπίθεσης είχε πέσει το σύστημα του σιδηροδρομικού δικτύου του Ιράν, σύμφωνα με τις αρχές, προκαλώντας πρωτόγνωρο χάος. Τον Μάιο του 2020 είχε γίνει λόγος για ισραηλινή κυβερνοεπίθεση εναντίον του λιμανιού Σαχίντ Ραζαεΐ, που βρίσκεται στα στενά του Ορμούζ, από όπου περνά το ένα τρίτο του πετρελαίου παγκοσμίως που διακινείται μέσω θαλάσσης.

Ισραήλ 2021: Ο διευθυντής της ισραηλινής υπηρεσίας κυβερνοασφάλειας, Ουγκάλ Ούνα, κατά τη διάρκεια μιας διαδικτυακής συνόδου με θέμα τη διεθνή συνεργασία στην καταπολέμηση των επιθέσεων με ransomware, επιβεβαίωσε ότι το Ισραήλ δέχτηκε μεγάλη επίθεση ransomware σε δομές υγείας. Η διοίκηση του νοσοκομείου Hillel Yaffe στη Χαντέρα, στο κεντρικό Ισραήλ υπογράμμισε σε ανακοίνωσή της ότι χρησιμοποιεί εναλλακτικά συστήματα για τη θεραπεία ασθενών μετά την επίθεση.

Σαουδική Αραβία 2021: Η Saudi Aramco, το καλοκαίρι του 2021, επιβεβαίωσε ότι ορισμένα αρχεία της εταιρείας διέρρευσαν αφού χάκερ φέρεται να ζήτησαν λύτρα 50 εκατομμυρίων δολαρίων από τον πολυτιμότερο παραγωγό πετρελαίου στον κόσμο (Wethe, 2021). Το 2012, η Σαουδική Αραβία κατηγόρησε άγνωστα άτομα με έδρα εκτός του βασιλείου για μια πειρατεία εναντίον του πετρελαϊκού γίγαντα που είχε ως στόχο να διακόψει την παραγωγή από τον μεγαλύτερο εξαγωγέα αργού στον κόσμο. Η κυβερνοεπίθεση spear phishing κατέστρεψε περισσότερους από 30.000 υπολογιστές μέσα σε λίγες ώρες.



Εικόνα 2

4.4.2 Τύποι κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις μπορούν να έχουν σημαντικό αντίκτυπο στη λειτουργία ενός κράτους και στο διεθνές του καθεστώς (Fischer, 2016). Πάνω σε αυτές βασίζεται και σχεδιάζεται ο κυβερνοπόλεμος από κρατικούς ή μη δρώντες.

Οι προκλήσεις που αντιμετωπίζουν σήμερα όλοι οι ειδικοί στον τομέα της κυβερνοασφάλειας που μπορούν να δημιουργήσουν προβλήματα στις κρίσιμες υποδομές μιας χώρας, στη λειτουργία του κράτους ή ακόμα και στην εθνική της ασφάλεια, είναι οι εξής (Jang-Jaccard, 2014):

1. **Επιθέσεις cryptolocker/ransomware:** Οι επιθέσεις αυτές είναι κρίσιμες για μεμονωμένους χρήστες αλλά περισσότερο για οργανισμούς και οντότητες του κράτους. Πολύ επικίνδυνες και σε έξαρση παρουσιάζονται και οι επιθέσεις αυτού του τύπου. Πρόκειται για κακόβουλα προγράμματα που από την στιγμή που θα εκτελεστούν στον μολυσμένο υπολογιστή, κρυπτογραφούν το σύνολο των αρχείων σε αυτόν καθιστώντας τη χρήση του πρακτικά αδύνατη (cryptolocker). Σε πολλές περιπτώσεις ο hacker που κατασκεύασε το λογισμικό cryptolocker απαιτεί από τον χρήστη λύτρα, προκειμένου να του παρέχει το κλειδί αποκρυπτογράφησης των αρχείων του (ransomware). Το μεγάλο πρόβλημα εδώ δεν είναι τόσο η μόλυνση ενός μενονωμένου υπολογιστή ενός χρήστη, αλλά η περίπτωση που μολύνονται ολόκληρα δίκτυα υπολογιστών με καταστροφικά αποτελέσματα.

2. **Επιθέσεις IoT:** Η τεχνολογία IoT είναι νέα και φανταστείτε ότι σήμερα υπάρχουν ήδη 11,6 δισεκατομμύρια συσκευές IoT σε λειτουργία. Η επίθεση τέτοιων συσκευών έχει αντίκτυπο στη διακύβευση ευαίσθητων δεδομένων χρήστη. Οι συσκευές

IoT μπορούν να χρησιμοποιηθούν από οικιακή χρήση έως συστήματα υποδομής ζωτικής σημασίας.

3. **Επιθέσεις στο cloud:** Πολλές επιθέσεις γίνονται με σκοπό την παραβίαση πλατφορμών cloud για την κλοπή δεδομένων χρηστών. Αυτές οι επιθέσεις αποτελούν τεράστια απειλή για οργανισμούς ή οντότητες του κράτους.

4. **Επιθέσεις phishing - spear phishing/ Social Engineering:** Είναι από τις πιο κλασικές επιθέσεις και αντιμετωπίζονται χιλιάδες περιστατικά καθημερινά. Επιθέσεις τύπου ηλεκτρονικού ψαρέματος και κοινωνικής μηχανικής. Οι επιθέσεις αυτού του τύπου εκμεταλλεύονται την παρουσία των ατόμων στα κοινωνικά δίκτυα και την έμφυτη ανάγκη του ατόμου για επικοινωνία σε αυτά. Με τεχνικές όπως ψεύτικες καμπάνιες, κατασκευασμένα προφίλ κοινωνικών δικτύων και μηνύματα προσεκτικά κατασκευασμένα ώστε να τραβήξουν την προσοχή του μη υποψιασμένου χρήστη, ένας hacker μπορεί να αντλήσει προσωπικές πληροφορίες και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα αρχεία του χρήστη ή ακόμη και στις τραπεζικούς του λογαριασμούς.

5. **Επιθέσεις σε Blockchain & Cryptocurrency:** Πρόκειται για ένα νέο είδος επίθεσης καθώς η τεχνολογία των κρυπτονομισμάτων έχει πλέον ξεκινήσει και γίνεται ευρέως γνωστή. Πολλές εταιρείες πλέον, αλλά και εγκληματίες και τρομοκράτες χρησιμοποιούν κρυπτονομίσματα ως μέθοδο πληρωμής και ξέπλυμα χρήματος επειδή οι συναλλαγές δεν καταγράφονται σε συγκεκριμένους τύπους όπως το monero.

6. **Κυβερνοκατασκοπεία:** Αυτές οι ενέργειες επηρεάζουν την ασφάλεια ενός κράτους ή ακόμα και ενός οργανισμού (για παράδειγμα NATO, ΕΕ κ.λπ.) μέσω της διαρροής απόρρητων πληροφοριών.

7. **Ευπάθειες λογισμικού:** Οι επιθέσεις γίνονται συχνά λόγω τρωτών σημείων στο λογισμικό (software) ή μολυσμένων ενημερώσεων (updates), τρανταχτό παράδειγμα είναι η επίθεση SolarWinds που αναφέρθηκε παραπάνω.

8. **Ξεπερασμένο υλικό:** Σε πολλές περιπτώσεις το υλικό (hardware) που χρησιμοποιείται είναι παλιό και οι νέες ενημερώσεις ενδέχεται να μην είναι συμβατές με αυτό.

9. **Επιθέσεις μηχανικής μάθησης και τεχνητής νοημοσύνης:** Αυτές οι τεχνολογίες είναι πολύ πρόσφατες και θα απασχολούν τους ειδικούς πολύ από εδώ και στο εξής. Σήμερα, υπάρχει έλλειψη εμπειρογνωμοσύνης στον τομέα της κυβερνοασφάλειας για τον χειρισμό τέτοιων επιθέσεων.

10. **Επιθέσεις τύπου DOS και DDOS:** Πρόκειται για επιθέσεις άρνησης πρόσβασης (DOS) και κατανεμημένες από πολλαπλές πηγές και χώρες, επιθέσεις άρνησης πρόσβασης (DDOS). Και στις δύο περιπτώσεις ο στόχος είναι να κατακλυστεί η προσφερόμενη υπηρεσία, για παράδειγμα μια ιστοσελίδα, από χιλιάδες ταυτόχρονες αιτήσεις, με αποτέλεσμα ο εξυπηρετητής να μην μπορεί να ανταποκριθεί. Το δεύτερο είδος είναι το δυσκολότερο στην αντιμετώπιση, όπως αποδείχθηκε κι από τις επιθέσεις που δέχτηκε αριθμός κυβερνητικών ιστοσελίδων στην Ελλάδα κατά τα τελευταία έτη. Οι επιθέσεις αυτού του είδους παρουσιάζονται με όλο και μεγαλύτερη συχνότητα.

11. **Διαρροή – Απώλεια δεδομένων:** Σε μεγάλο πονοκέφαλο για τα τμήματα πληροφορικής υποστήριξης και ασφαλείας των οργανισμών αναδεικνύεται και το πρόβλημα των πολλαπλών πηγών και μέσων μέσω των οποίων μπορούν δυνητικά να

διαρρεύσουν εταιρικά δεδομένα: Ο εργαζόμενος σε ένα σύγχρονο οργανισμό διαθέτει πρόσβαση σε λογαριασμό ηλεκτρονικού ταχυδρομείου, πρόσβαση στο διαδίκτυο, αφαιρούμενα αποθηκευτικά μέσα και πρόσβαση σε διαδικτυακές υπηρεσίες τύπου cloud και έξυπνα κινητά τηλέφωνα με δυνατότητες αντίστοιχες ενός υπολογιστή. Αν δεν τηρηθούν αυστηροί κανόνες και δεν εφαρμοστούν πολιτικές ασφάλειας για την πληροφορία του οργανισμού, είναι εξαιρετικά εύκολο να υπάρχει είτε ακούσια είτε εκούσια διαρροή πληροφοριών.

12. **Insider threats:** Το πρόβλημα της διαρροής δεδομένων λόγω της σύγχρονης τεχνολογίας έρχεται σε συνάρτηση με έναν από τους μεγαλύτερους κινδύνους τα δεδομένα του οργανισμού, αυτό της απειλής από τους ίδιους τους εργαζόμενους του. Είτε λόγω άγνοιας, είτε λόγω της μη γνώσης των δυνατοτήτων των σύγχρονων υπολογιστικών συστημάτων είτε επειδή είναι κακόβουλος, ο χρήστης ενός οργανισμού μπορεί να αποτελέσει την κερκόπορτα για την απώλεια ευαίσθητων δεδομένων (Παράδειγμα Snowden).

13. **Malware Επιθέσεις – Hacking:** Πέραν των επιθέσεων που αναφέρθηκαν παραπάνω, παρατηρείται γενικά μεγάλη αύξηση στις επιθέσεις με κακόβουλο λογισμικό. Τις επιθέσεις εκτελούν μενονωμένοι χακερς ή ομάδες από χακερς, οι οποίες πολλές φορές έχουν κρατικούς φορείς για σπόνσορες. Η ρωσικής προέλευσης ομάδα Fancy Bear, το βορειο-κορεάτικο Lazarus Group είναι κάποια από αυτά. Η NSA εικάζεται πως διαθέτει το πιο εξελιγμένο τμήμα κυβερνοεπιθέσεων, γνωστό ως TAO (Tailored Access Operations).

Τα εργαλεία πληθαίνουν και οι μέθοδοι αποφυγής των μέτρων ασφαλείας που θέτουν οι οργανισμοί εξελίσσονται συνεχώς. Το σύγχρονο ψηφιακό περιβάλλον ορίζει δύο προκλήσεις: Πρώτον, συνεχή αγώνα για την ενημέρωση για τους νέους τύπους επιθέσεων και την αποτελεσματική και έγκαιρη αντιμετώπισή τους. Και δεύτερον, την εκμετάλλευση

όλων των νέων τεχνολογιών, τεχνικών και εργαλείων ώστε να συμβάλλουν ενεργά στην συλλογή πληροφοριών προς όφελος της κάθε χώρας.

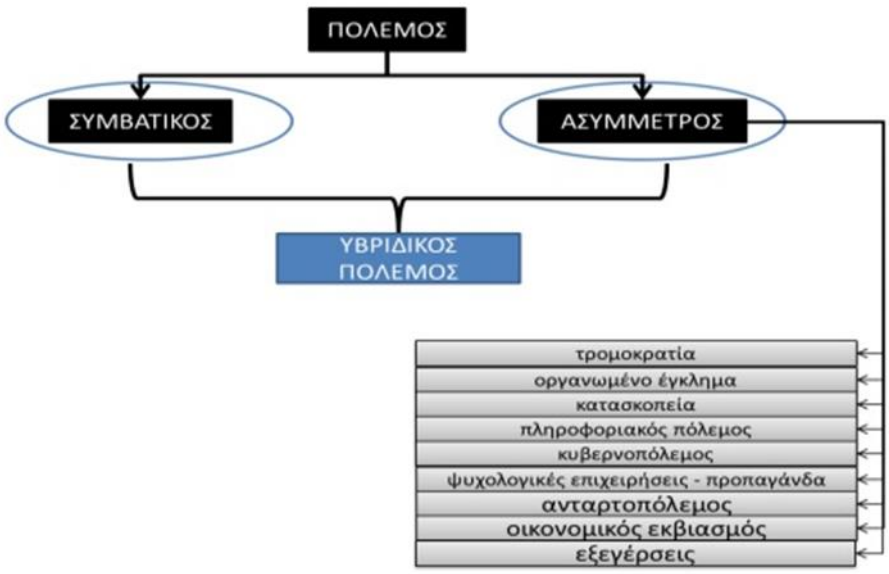
Όλες οι παραπάνω προκλήσεις, παλιές και νέες, πρέπει να αντιμετωπιστούν από τα κράτη μέσω των ειδικών τους. Μερικά από τα παραπάνω μπορούν να αντιμετωπιστούν με διασφάλιση της εφοδιαστικής αλυσίδας και αξιολογήσεις/πιστοποιήσεις πρώτα των προϊόντων ΤΠΕ και στο μέλλον των προϊόντων τεχνητής νοημοσύνης και IoT.

4.5 Υβριδικός Πόλεμος

Πολλοί θεωρητικοί και αναλυτές σε αυτόν τον αιώνα επικεντρώνονται σε έναν νέο τύπο πολέμου που είναι γνωστός ως «υβριδικός πόλεμος». Αυτός ο πόλεμος δεν έχει χαρακτηριστεί ως "παραδοσιακός" πόλεμος καθώς έχει την ικανότητα να προσαρμόζεται κάθε φορά στις συνθήκες, καθιστώντας τον, πολύπλοκο και πολυδιάστατο. Επιπλέον, ο Hoffman Frank, κορυφαίος υποστηρικτής και μελετητής του υβριδικού πολέμου, υποστήριξε ότι είναι ένας «θολός» πόλεμος στον οποίο δεν υπάρχουν σταθερές μεταβλητές αλλά τα κύρια χαρακτηριστικά του είναι η πολυπαραγοντικότητα και ποικιλία δράσεων. Δεν υπάρχει μαύρο ή άσπρο αλλά μια «νέα απόχρωση του πολέμου», γκρι (Hoffman 2007) .

Ο ιδιαίτερος χαρακτήρας αυτού του πολέμου στοχεύει να αναμείξει συμβατικές και μη συμβατικές δυνάμεις, μαχητές και πολίτες, επιτρέποντας παράλληλα τη σύνδεση φυσικών και εικονικών προοπτικών. Οι μορφές πολέμου που συνδυάζονται στον υβριδικό πόλεμο, είναι ο συμβατικός και ο ασύμμετρος πόλεμος. Αξίζει να σημειωθεί ότι ο υβριδικός πόλεμος δεν είναι μια νέα ιδέα. Ωστόσο, ο συνδυασμός μη συμβατικών ή παράτυπων τακτικών με συμβατικές είναι τόσο παλαιός όσο και το ίδιο το φαινόμενο του πολέμου. Έχει ρίζες στο παρελθόν , αλλά οι τεχνικές και τα μέσα του έχουν εξελιχθεί. Ως αποτέλεσμα, πρέπει να επισημανθούν οι επιθέσεις της 11ης Σεπτεμβρίου το 2001 και ο πόλεμος Ισραήλ-Λιβάνου το 2006, που και οι δύο θεωρούνται κομβικές για την ανάπτυξη

υβριδικών απειλών. Υβριδικός πόλεμος μπορεί να θεωρηθεί και ο αγώνας των Κούρδων στη Μέση Ανατολή για δημιουργία ανεξάρτητου κράτους, εναντίον κυρίως των Τούρκων (Plakoudas 2017). Η ραχοκοκαλιά του υβριδικού πολέμου είναι ένας συνδυασμός συμβατικού και ασύμμετρων μορφών πολέμου που περιλαμβάνει την τρομοκρατία, τις επιθέσεις στον κυβερνοχώρο, το έγκλημα, τις επιθέσεις στην οικονομία, την κοινωνία και την εσωτερική πολιτική πόλωση (Εικόνα 3). Ο παραδοσιακός πόλεμος, ο ακανόνιστος πόλεμος, η καταστροφική τρομοκρατία και ο καταστροφικός πόλεμος είναι οι τέσσερις τύποι σύγκρουσης που είναι γνωστοί (Freier 2009). Δύο από τα τέσσερα χαρακτηριστικά χρησιμοποιούνται για τη διεξαγωγή του υβριδικού πολέμου. Μάλιστα, λόγω της ποικιλίας των τρόπων του, κατατάσσεται σε προηγμένο είδος πολέμου με αμφιλεγόμενο ορισμό. Η φύση του πολέμου δεν αλλάζει, αλλά τα χαρακτηριστικά και οι τεχνικές αντιλήψεις μπορούν να αλλάξουν και να προσαρμοστούν για κάθε εποχή. Ο πόλεμος είναι ακόμα πόλεμος.



Εικόνα 3

Στην περίπτωση της προσάρτησης της Κριμαίας από τη Ρωσική Ομοσπονδία το 2014, ο υβριδικός πόλεμος ήταν ο κύριος πρωταγωνιστής. Ως αποτέλεσμα, το Δόγμα

Gerasimov εξέφρασε τη ρωσική στρατηγική σκέψη ένα χρόνο πριν από την προσάρτηση. Ο αρχηγός του ρωσικού Γενικού Επιτελείου, Valery Vasilyevich Gerasimov, δήλωσε στο άρθρο του, «Η αξία της επιστήμης έγκειται στην πρόβλεψη», ότι ο 21ος αιώνας παρουσιάζει νέες προκλήσεις, ότι δεν υπάρχουν «ορατές» γραμμές ειρήνης και πολέμου, ότι οι συγκρούσεις έχουν ασυνήθιστο μοτίβο και ότι ισχύουν διαφορετικοί κανόνες». Ο στρατιωτικός εξοπλισμός συνδυάζεται με οικονομικά και πολιτικά μέσα, υψηλή τεχνολογία και τρομοκρατία στον εκσυγχρονισμό του πολέμου. Η Ρωσία φέρεται να εγκαταλείπει τις «παραδοσιακές» στρατιωτικές επιχειρήσεις υπέρ των ασύμμετρων, σύμφωνα με τη σύγχρονη στρατιωτική ορολογία. Το δόγμα Gerasimov στοχεύει στην επίτευξη στρατηγικών και γεωπολιτικών στόχων μέσω ποικίλων μεθόδων, συμπεριλαμβανομένων των οικονομικών κυρώσεων, της επίσημης και άτυπης διπλωματίας, της αποφυγής στρατιωτικής δράσης και, τέλος, της επίδειξης υποστήριξης και βοήθειας σε συγκεκριμένο τοπικό πληθυσμό. Αυτή είναι μια εφαρμογή New Generation War.

Κάνοντας ιστορική αναδρομή για την περιοχή της Κριμαίας, γίνεται αντιληπτό ότι η Ρωσία προσπάθησε να διορθώσει το λάθος του 1954, όπου ο τότε γενικός γραμματέας της ΕΣΣΔ, Νικήτα Χρουστσόφ, αποφάσισε να παραδώσει την Κριμαία στη Σοβιετική Ουκρανία. Ουσιαστικά, τίποτα δεν άλλαξε, αλλά όταν η Σοβιετική Ένωση διαλύθηκε, η χερσόνησος προσαρτήθηκε από την Ουκρανία, ωθώντας μεγάλο αριθμό Ρώσων να αναζητήσουν επιστροφή στη Ρωσία. Το 2014, ο Ρώσος Πρόεδρος Βλαντιμίρ Πούτιν πραγματοποίησε στρατιωτικές ασκήσεις στα σύνορα Ρωσίας-Ουκρανίας έως ότου «μικροί πράσινοι» (Shevchenko, 2014) διείσδυσαν στην Κριμαία και κατέλαβαν βασικά κυβερνητικά κτήρια. Λόγω της έλλειψης σήματος ή θυρεού σε αυτές τις στολές, η ταυτότητά τους είναι άγνωστη. Την ίδια στιγμή κινητοποιήθηκαν και τοπικές παραστρατιωτικές οργανώσεις. Τα μέσα ενημέρωσης, από την άλλη πλευρά, ήταν καλά συντονισμένα, με επτά ρωσικά κανάλια να αντικαθιστούν τα ουκρανικά κανάλια,

κυβερνοεπιθέσεις κατά της Ουκρανίας στον τομέα της επικοινωνίας και η Ρωσία να ασκεί οικονομική πίεση στον τομέα του φυσικού αερίου από το 2009. Με την προσάρτηση της Κριμαίας την άνοιξη το 2014, ξέσπασε σύγκρουση στην ανατολική Ουκρανία, ωθώντας τη Μόσχα να διακόψει τις προμήθειες φυσικού αερίου της Ουκρανίας. Τον Μάρτιο του 2014, ένα δημοψήφισμα αναγνώρισε την επίσημη προσάρτηση της Κριμαίας από τη Ρωσική Ομοσπονδία (95% υπέρ). Πολλές χώρες έχουν καταδικάσει την προσάρτηση της Κριμαίας, ενώ το ΝΑΤΟ και οι ΗΠΑ έχουν συζητήσει νέες στρατηγικές για την αντιμετώπιση του υβριδικού πολέμου. Το παράδειγμα της Κριμαίας και η τακτική της Ρωσίας άνοιξαν ένα νέο κεφάλαιο στη διεξαγωγή του πολέμου, καθώς ο υβριδικός πόλεμος είναι ευέλικτος, συνδυάζοντας τακτικά και ακανόνιστα μέσα, εγκαινιάζοντας μια εξελιγμένη και προσαρμόσιμη νέα εποχή πολέμου.

Από τους «μικρούς πράσινους άντρες» στην Κριμαία μέχρι τους «μικρούς μπλε άντρες» στη Θάλασσα της Νότιας Κίνας (Cavas, 2015), η ιδέα ότι η διεθνής σύγκρουση μπορεί να έχει περισσότερο υβριδικό πόλεμο έχει αναγκάσει τις ΗΠΑ και κατ' επέκταση το ΝΑΤΟ αλλά και την ΕΕ, να τον εντάξουν σε βασικό στοιχείο της πολιτικής ασφάλειας. Το ΝΑΤΟ (NATO, 2019) και η ΕΕ (European Council, 2016) ασχολούνται πλέον έμπρακτα καθώς παράγουν πολιτικές και οδηγίες στρατηγικής που στοχεύουν στην ενίσχυση των αμυντικών δυνατοτήτων και στην πρόληψη υβριδικών επιθέσεων.

Η παραδοσιακή σύγκρουση θα συνεχίσει να υπάρχει, αλλά πλέον με όλες αυτές τις δυνατότητες που προσφέρει ειδικά ο κυβερνοχώρος αλλά και οι υπόλοιπες τεχνικές, ο υβριδικός πόλεμος θα αντικαταστήσει πλήρως τον παραδοσιακό. Η πιο χαρακτηριστική αλλαγή στον χαρακτήρα του σύγχρονου πολέμου είναι η μεικτή φύση της μάχης. Σε υβριδικούς πολέμους, μελλοντικοί αντίπαλοι (κράτη, κρατικά επιχορηγούμενες ομάδες ή αυτοχρηματοδοτούμενοι φορείς) θα εκμεταλλευτούν πρόσβαση σε σύγχρονες στρατιωτικές δυνατότητες, στον κυβερνοχώρο, καθώς και στη δυνατότητα αστικού πολέμου (συγκρούσεις εντός πόλεων). Επίσης, τα κράτη μπορούν να αλλάξουν τις

συμβατικές τους μονάδες σε ακανόνιστους σχηματισμούς και να υιοθετήσουν νέες τακτικές όπως έκαναν οι Φενταγίν στο Ιράκ το 2003 και «οι μικροί πράσινοι άντρες» στην Κριμαία το 2014. Το μέλλον μπορεί να δείξει ότι ο υβριδικός πόλεμος είναι πραγματικά αποτελεσματικός από χώρες με μικρές δυνατότητες σε σχέση με χώρες με μεγάλες, βαριές και ιεραρχικές οργανώσεις που είναι δογματικά άκαμπτες (Glenn 2009).

4.6 Κυβερνοαποτροπή & Κυβερνοαντοχή

Το NATO ορίζει την κυβερνοαποτροπή (NATO, 2015) ως την απειλή βίας προκειμένου να αποθαρρύνει έναν αντίπαλο στο να κάνει μια ανεπιθύμητη ενέργεια. Αυτό μπορεί να επιτευχθεί μέσω της απειλής αντιποίνων (αποτροπή με τιμωρία) ή με άρνηση και αντιμετώπιση των αντιπάλων σκοπών (αποτροπή με άρνηση).

Από την άλλη πλευρά ως ανθεκτικότητα ορίζεται η ικανότητα ενός κράτους ή οργανισμού να προετοιμάζεται και να προσαρμόζεται στις μεταβαλλόμενες συνθήκες και να έχει τη δυνατότητα να αντέχει και να ανακάμπτει γρήγορα από κυβερνοεπιθέσεις. Η ανθεκτικότητα και η αποτροπή αποτελούν μέρος μιας ολοκληρωμένης στρατηγικής στον κυβερνοχώρο όπου οι τακτικές ενδέχεται να επικαλύπτονται σε άμυνα, ανθεκτικότητα, αποτροπή και άλλους στρατηγικούς χώρους.

Τη τελευταία δεκαετία, υπήρξε αυξανόμενη στρατηγική συζήτηση σχετικά με την ανθεκτικότητα στον κυβερνοχώρο ως μία συνιστώσα μιας ευρύτερης στρατηγικής για την καταπολέμηση των επιθέσεων στον κυβερνοχώρο. Εμφανίστηκε τα τελευταία χρόνια επειδή τα παραδοσιακά μέτρα ασφάλειας στον κυβερνοχώρο δεν επαρκούν πλέον για την προστασία των χωρών και ειδικότερα των κρίσιμων οργανισμών τους από το κύμα επίμονων επιθέσεων (APT). Η ανθεκτικότητα στον κυβερνοχώρο ξεκινά με την ολοκλήρωση των βασικών αρχών της ασφάλειας στον κυβερνοχώρο. Αυτό περιλαμβάνει την επιδιόρθωση ευπαθειών, τον εντοπισμό και τον μετριασμό των απειλών και την

εκπαίδευση των εργαζομένων για το πώς να υπερασπιστούν την ασφάλεια ενός ή περισσότερων οργανισμών.

Πολυάριθμοι οργανισμοί, κοινότητες και ειδικοί έχουν κυκλοφορήσει στρατηγικές και έρευνες γύρω από την αποτροπή και την ανθεκτικότητα στον κυβερνοχώρο, όπως π.χ το Υπουργείο Άμυνας των ΗΠΑ (Department of Defense), η Πολεμική Αεροπορία των ΗΠΑ (USAF), η Διοίκηση Κυβερνοχώρου των ΗΠΑ (USCYBERCOM) κλπ.

Η σχέση μεταξύ ανθεκτικότητας και αποτροπής είναι ιδιαίτερα σημαντική όταν εξετάζεται ο κυβερνοχώρος στρατηγικά. Η ανθεκτικότητα είναι ένα μεγάλο μέρος μιας στρατηγικής αποτροπής σε σύγκριση με προηγούμενους τύπους συγκρούσεων (π.χ. πυρηνική αποτροπή). Η οικοδόμηση της ανθεκτικότητας στον κυβερνοχώρο, ειδικότερα στα συστήματα επικοινωνιών – πληροφορικής, ενισχύει την αμυντική ικανότητα, ενώ ταυτόχρονα λειτουργεί αποτρεπτικά στους επιτιθέμενους ενδυναμώνοντας τα συστήματα με σκοπό να είναι πολύ δύσκολο ή δαπανηρό για να επιτεθούν.

Πέρα από αυτό, οι χώρες πρέπει να αναπτύξουν ανθεκτικότητα σε κάθε μέρος των κρίσιμων, για τη λειτουργία τους, οργανισμών, από τη χαρτογράφηση διαδικασιών έως τη διαθεσιμότητα υπηρεσιών μηχανικής έως την κρίσιμη εξάρτηση από τον προμηθευτή. Ο στόχος της ανθεκτικότητας στον κυβερνοχώρο είναι αρκετά σαφής: να εξασφαλιστεί η λειτουργική συνέχεια με ελάχιστο αντίκτυπο. Αλλά η πραγματικότητα μπορεί να είναι πιο δύσκολο να προσδιοριστεί, επειδή επί του παρόντος δεν υπάρχει τρόπος μέτρησης της ανθεκτικότητας στον κυβερνοχώρο. Για να μπορέσει μία χώρα να λογίζεται ως ανθεκτική στις κυβερνοεπιθέσεις ή στην προσπάθεια κυβερνοπολέμου πρέπει να ανταποκριθεί σε μια επίθεση, διατηρώντας την εμπιστοσύνη των πολιτών, απορροφώντας τον αντίκτυπο και να επιστρέψει τάχιστα στην καθημερινή της λειτουργία.

Η διαφορά τώρα με την κυβερνοασφάλεια έγκειται στα εξής: η κυβερνοασφάλεια αποτελείται από τεχνολογίες, διαδικασίες και μέτρα που έχουν σχεδιαστεί για την προστασία συστημάτων, δικτύων και δεδομένων από εγκλήματα και επιθέσεις στον

κυβερνοχώρο. Η αποτελεσματική ασφάλεια στον κυβερνοχώρο μειώνει τον κίνδυνο επίθεσης στον κυβερνοχώρο και προστατεύει οντότητες, οργανισμούς και άτομα από τη σκόπιμη εκμετάλλευση συστημάτων, δικτύων και τεχνολογιών. Από την άλλη πλευρά, η ανθεκτικότητα στον κυβερνοχώρο εξετάζει ένα ευρύτερο πεδίο εφαρμογής όπου περιλαμβάνει την ασφάλεια στον κυβερνοχώρο και την ανθεκτικότητα των κρίσιμων οργανισμών για τη λειτουργία του κρατικού μηχανισμού (Björck, 2015). Η κυβερνοασφάλεια είναι αποτελεσματική χωρίς να διακυβεύεται η χρηστικότητα των συστημάτων και υπάρχει ένα ισχυρό σχέδιο συνέχειας για την επανέναρξη των εργασιών, εάν η επίθεση στον κυβερνοχώρο είναι επιτυχής. Η ανθεκτικότητα στον κυβερνοχώρο βοηθά τις χώρες να κατανοήσουν ότι οι χάκερ έχουν το πλεονέκτημα των καινοτόμων εργαλείων, του στοιχείου της έκπληξης, του στόχου και μπορούν να είναι επιτυχημένοι στην προσπάθειά τους. Αυτή η ιδέα βοηθά τις χώρες να προετοιμαστούν, να αποτρέψουν, να ανταποκριθούν και να επανέλθουν με επιτυχία στην επιδιωκόμενη ασφαλή κατάσταση. Αυτή είναι μια ουσιαστική αλλαγή, καθώς η χώρα πλέον βλέπει την ασφάλεια ως εργασία πλήρους απασχόλησης και ενσωματώνει τις βέλτιστες πρακτικές ασφάλειας στις καθημερινές λειτουργίες. Σε σύγκριση με την κυβερνοασφάλεια, η ανθεκτικότητα στον κυβερνοχώρο απαιτεί από την χώρα να είναι πιο ευέλικτη στον χειρισμό επιθέσεων.

Είναι σημαντικό να αναφερθεί ότι για πρώτη φορά ο όρος της ανθεκτικότητας στον κυβερνοχώρο αναφέρθηκε σε επίσημη στρατηγική κυβερνοασφάλειας το 2014, συγκεκριμένα στη στρατηγική κυβερνοασφάλειας του Ντουμπάι. Το DESC δημιούργησε αυτή τη στρατηγική [κυκλοφορεί πλέον η δεύτερη έκδοση, (Dubai Electronic Security Center, 2017)]για να βοηθήσει την ασφάλεια του Ντουμπάι στον κυβερνοχώρο από τους κινδύνους με στόχο την υποστήριξη της ανάπτυξης, της καινοτομίας και της οικονομίας. Από το 2020, μετά η Ελλάδα και τα Ηνωμένα Αραβικά Εμιράτα διαμόρφωσαν πλέον το πλαίσιο μιας στρατηγικής συμμαχίας που εκτείνεται όχι μόνο στους τομείς της οικονομικής συνεργασίας, αλλά και στους τομείς της άμυνας και της εξωτερικής

πολιτικής. Μπορεί η Ελλάδα να επωφεληθεί μέσω στενότερης συνεργασίας σε θέματα κυβερνοασφάλειας.

4.7 Ο κυβερνοπόλεμος ως σύγχρονη μορφή πολέμου

Βασισμένη στην ιδέα του Σοβιετικού στρατιωτικού Νικολάι Ογκάρκοφ για «στρατιωτική τεχνολογική επανάσταση», η Επανάσταση στις Στρατιωτικές Υποθέσεις (RMA - Revolution in Military Affairs) υποδηλώνει κάτι περισσότερο από απλή τεχνολογική μετατόπιση. Η RMA μπορεί να περιγραφεί ως μια αποφασιστική ανακάλυψη στην αποτελεσματικότητα μάχης λόγω της δραστικής αλλαγής στη τεχνολογία, τη στρατηγική κουλτούρα, την οργάνωση, το δόγμα, την εκπαίδευση και τις τακτικές. Είναι η εφαρμογή της τεχνολογίας σε στρατιωτικά συστήματα σε συνδυασμό με καινοτόμες ιδέες και οργανωτική προσαρμογή (Metz, 1995). Στο έργο του Andrew Krepinevich για την RMA (Krepinevich, 2006), γίνεται αναφορά στον σχεδιασμό και την κατασκευή, με τη βοήθεια υπολογιστών, αποτελεσμάτων με προηγμένες προσομοιώσεις, ενισχύοντας έτσι τις ικανότητες των στρατιωτικών οργανισμών.

Σε αυτό το πλαίσιο, θα μπορούσε να υποστηριχθεί ότι ο κυβερνοπόλεμος θα πρέπει να θεωρηθεί ως η σημερινή επανάσταση στις στρατιωτικές υποθέσεις. Ως αποτέλεσμα, η κούρσα των εξοπλισμών στον κυβερνοχώρο έχει ήδη γιγαντωθεί μέσω ειδικών δορυφορικών συστημάτων, συστημάτων κατευθυνόμενης ενέργειας και συστημάτων που βασίζονται στην τεχνητή νοημοσύνη για την άμυνα των δικτύων. Τα προϊόντα κυβερνοχώρου και ρομποτικής μετά από δεκαετίες προσπάθειας, καινοτομίας και πειραματισμού, αποτελούν τους βασικούς πυλώνες της επόμενης Επανάστασης στις Στρατιωτικές Υποθέσεις. Χωρίς αμφιβολία, οι νέες πολεμικές ικανότητες έφερναν πάντα ανωτερότητα σε κρίσιμες στιγμές (Anders, 2011). Το ίδιο ισχύει για τα δίκτυα επικοινωνιών και πληροφορικής των σύγχρονων στρατών. Όπως απολαμβάνουν οι σύγχρονοι στρατοί καλύτερα πλεονεκτήματα στην υπεροχή πληροφοριών χάρη στα δίκτυα

επικοινωνιών και πληροφορικής και στις προηγμένες υποδομές δικτύου, αυτά τα πλεονεκτήματα δημιουργούν επίσης ευκαιρίες για εκμετάλλευση από τους αντιπάλους (Lewis, 2015).

Από στρατιωτική άποψη, θα ήταν σωστό να ειπωθεί ότι ο κυβερνοπόλεμος εξαρτάται από την υπεροχή πληροφοριών και έλεγχο αυτών κατά την φάση της μάχης, ώστε το ένα μέρος να βρίσκεται σε σύγχυση. Ο κυβερνοπόλεμος συνεπάγεται όχι μόνο μια τεχνολογική ανακάλυψη αλλά και ένα σύνολο δραστικών βελτιώσεων στην οργάνωση, το δόγμα, την έννοια και τη στρατιωτική σκέψη.

4.8 Κρατικοί δρώντες

Όπως ήδη έχει επισημανθεί παραπάνω, η σημασία του κυβερνοχώρου είναι πανταχού παρούσα στη σημερινή εποχή: από τον ρόλο του στις εθνικές οικονομίες, στο εμπόριο, στον πολιτικό διάλογο, στη χρήση του ως εργαλείο καταναγκασμού και κατασκοπείας και την αντιληπτή κεντρική του θέση ως έναν από τους καθοριστικούς παράγοντες επιτυχίας στον πόλεμο. Το γεγονός ότι η κυβερνοεξάρτηση έχει γίνει τόσο διαδεδομένη στην κοινωνία, με πολύπλοκες διασυνδέσεις μεταξύ διαφόρων τομέων, έχει αυξήσει την ευπάθεια σε επιθέσεις εναντίον του ευρύτερου κοινωνικού συνόλου και στρατιωτικών υποδομών. Υπάρχει λοιπόν αυξημένη εστίαση στην κυβερνοάμυνα εντός των ενόπλων δυνάμεων και των οργανισμών εθνικής ασφάλειας σε πολλά μέρη του κόσμου. Στο πλαίσιο του στρατού, αναφέρθηκε στην προηγούμενη ενότητα ότι, ο κυβερνοχώρος έχει αναγνωριστεί ως μια νέα πέμπτη αρένα, πέρα από την ξηρά, θάλασσα, αέρα και διάστημα, στα οποία μπορούν να εκτελεστούν στρατιωτικές επιχειρήσεις (Hathaway, 2017). Οι επιχειρήσεις, που ονομάζονται επιχειρήσεις κυβερνοχώρου, περιλαμβάνουν τόσο επιθετικές όσο και αμυντικές ενέργειες και μπορεί να εκτελεστούν ανεξάρτητα ή ως συμπλήρωμα του συμβατικού πολέμου. Καθώς τόσο οι κρατικοί όσο και οι μη κρατικοί φορείς αξιοποιούν ολοένα και περισσότερο τις ικανότητες στον

κυβερνοχώρο για να επιτύχουν τους στρατηγικούς τους στόχους, ο ανταγωνισμός στον κυβερνοχώρο εντείνεται. Ωστόσο, παρά την αυξανόμενη σημασία του κυβερνοχώρου στην παγκόσμια πολιτική, την οικονομία και την άμυνα, δεν είχε πραγματοποιηθεί συνολική αξιολόγηση της εθνικής ισχύος στον κυβερνοχώρο – μέχρι τώρα.

Αναφορικά με τις χώρες που έχουν τη δυνατότητα να διαδραματίσουν τον ρόλο του κρατικού δρώντα σε θέματα κυβερνοπεριστατικών, το International Institute for Strategic Studies (IISS, 2021) κυκλοφόρησε το 2021 μια μελέτη που μετράει τις δυνατότητες στον κυβερνοχώρο και την εθνική ισχύ δεκαπέντε χωρών, καθώς και ένα νέο πλαίσιο για την κατανόηση της παγκόσμιας κρατικής ικανότητας στον κυβερνοχώρο και τον τρόπο κατάταξής τους. Ένα από τα βασικά σημεία της συνολικής αξιολόγησης που προκύπτει από τη μελέτη, είναι ότι οι ΗΠΑ είναι η συντριπτικά κυρίαρχη παγκόσμια δύναμη στον κυβερνοχώρο, ενώ ο πλησιέστερος αντίπαλος της Κίνας είναι δύσκολο να την φτάσει την επόμενη δεκαετία. Μέσα από την έρευνα προκύπτει ότι η Κίνα έχει σημειώσει σημαντική πρόοδο στην ενίσχυση των δυνατοτήτων της από το 2014, αλλά δεν είναι αρκετά κοντά για να κλείσει το χάσμα με τις ΗΠΑ. Αυτό που κάνει τη μελέτη του IISS διαφορετική από τις προηγούμενες μετρήσεις των δυνατοτήτων κυβερνοασφάλειας των χωρών βάσει δεικτών, είναι μια πιο ολοκληρωμένη ποιοτική ανάλυση του ευρύτερου οικοσυστήματος στον κυβερνοχώρο μιας χώρας, συμπεριλαμβανομένου του τρόπου με τον οποίο διασταυρώνεται με τη διεθνή ασφάλεια, τον οικονομικό ανταγωνισμό και τις στρατιωτικές υποθέσεις. Οι χώρες κρίθηκαν με βάση επτά κατηγορίες:

α) στρατηγική και δόγμα

β) διακυβέρνηση, διοίκηση και έλεγχος

γ) βασική ικανότητα πληροφοριών στον κυβερνοχώρο

δ) ενδυνάμωση και εξάρτηση στον κυβερνοχώρο

ε) ασφάλεια στον κυβερνοχώρο και ανθεκτικότητα

στ) παγκόσμια ηγεσία στις υποθέσεις του κυβερνοχώρου

ζ) επιθετική ικανότητα στον κυβερνοχώρο.

Σύμφωνα με τη μελέτη, οι ΗΠΑ είναι η μόνη χώρα με ισχυρές δυνάμεις σε όλες τις παραπάνω κατηγορίες. Η συνεργασία μεταξύ επιχειρήσεων, κυβέρνησης και πανεπιστημίων επισημάνθηκε ως σημαντικό πλεονέκτημα που διαθέτουν οι ΗΠΑ έναντι των υπολοίπων χωρών. Η δεύτερη βαθμίδα δυνάμεων στον κυβερνοχώρο περιλαμβάνει την Κίνα, τη Ρωσία, το Ηνωμένο Βασίλειο, τη Γαλλία, τον Καναδά, το Ισραήλ και την Αυστραλία, καθεμία από τις οποίες έχει κορυφαίες δυνάμεις παγκοσμίως σε ορισμένες από τις άνω κατηγορίες. Λόγω της μεγάλης και αυξανόμενης εγχώριας ψηφιακής-βιομηχανικής ικανότητας της Κίνας, η μελέτη καταλήγει στο συμπέρασμα ότι αυτή τη στιγμή βρίσκεται στην ταχύτερη τροχιά για να περάσει στην πρώτη βαθμίδα μαζί με τις ΗΠΑ. Αλλά αυτό δεν θα συμβεί τουλάχιστον για την επόμενη δεκαετία, καθώς η όχι καλή ασφάλεια και η αδύναμη ανάλυση πληροφοριών θα την κρατήσουν πίσω από τις ΗΠΑ.

Στην τρίτη βαθμίδα βρίσκονται κράτη στα πρώτα στάδια της ανάπτυξης ισχύος στον κυβερνοχώρο, όπως η Ινδία, η Ιαπωνία, το Ιράν, η Ινδονησία, η Μαλαισία, το Βιετνάμ και η Βόρεια Κορέα. Προκύπτει από την έρευνα ότι όλα έχουν δυνατά ή πιθανά δυνατά σημεία σε ορισμένες κατηγορίες, αλλά σημαντικές αδυναμίες σε άλλες. Η Ιαπωνία, με την κορυφαία στον κόσμο βιομηχανία υψηλής τεχνολογίας, κρίθηκε ως η καλύτερη για να ανέβει στη δεύτερη βαθμίδα μακροπρόθεσμα.

Τα κράτη ως δρώντες στον κυβερνοπόλεμο και οι μη κρατικοί δρώντες

Ο κυβερνοπόλεμος διεξάγεται από τα κράτη μέσω υπηρεσιών και οργανισμών αλλά και από ανεπίσημα υποστηριζόμενους από τα κράτη, μη κρατικούς δρώντες.

4.8.1 ΗΠΑ

Σύμφωνα με πολλούς αναλυτές και αρκετές αναλύσεις (βλ. παραπάνω), οι ΗΠΑ κρατούν τα σκήπτρα παγκοσμίως αναφορικά με τις επιθετικές δυνατότητες στον κυβερνοχώρο. Το ζήτημα της ασφάλειας στον κυβερνοχώρο απασχόλησε τους

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

Επισημαίνεται ότι ο Πρόεδρος Obama χαρακτήρισε το 2009 τον κυβερνοχώρο ως στρατηγικό περιουσιακό στοιχείο των ΗΠΑ, το οποίο πρέπει να προστατευθεί με κάθε μέσο. Σε συνέχεια των δηλώσεων Obama, τον Ιούνιο του 2009 ο ΥΠΑΜ των ΗΠΑ εξουσιοδότησε τον Διοικητή της αμερικανικής Στρατηγικής Διοίκησης (US Strategic Command) να δημιουργήσει υπό την διοίκηση του μια νέα διακλαδική διοίκηση με την ονομασία USCYBERCOM (Cyber Command).

Η Διοίκηση Cyber των ΗΠΑ (USCYBERCOM) ιδρύθηκε το 2010 και είναι μια Ενιαία Διοίκηση Μάχης βασισμένη σε ικανότητες παρόμοιες με τη Διοίκηση Ειδικών Επιχειρήσεων των ΗΠΑ και είναι η κύρια οργάνωση του στρατού τόσο για επιθετικές όσο και για αμυντικές ενέργειες στον κυβερνοχώρο. Αυτή τη στιγμή διοικείται από τον Στρατηγό Paul Nakasone, ο οποίος υπηρετεί ταυτόχρονα ως Διευθυντής της Υπηρεσίας Εθνικής Ασφάλειας (NSA). Οι δύο οργανισμοί έχουν στενή σχέση συνεργασίας. Το 2018, η κυβέρνηση Τραμπ αναβάθμισε την USCYBERCOM. Οι τρεις βασικές της αρμοδιότητες είναι :

-Παροχή διασφάλισης της αποστολής του Υπουργείου Άμυνας (DoD) με κύρια αρμοδιότητα τη λειτουργία και την προστασία των αμυντικών πληροφοριακών δικτύων.

-Αντιμετώπιση των στρατηγικών απειλών για τις Ηνωμένες Πολιτείες και διασφάλισης των εθνικών συμφερόντων.

-Βοήθεια σε επιχειρησιακούς κλάδους των υπόλοιπων επιτελείων (αεροπορίας, στρατού, ναυτικού) να επιτύχουν τις αποστολές τους μέσω του κυβερνοχώρου.

Ο κυβερνοχώρος είναι βασικός τομέας για τον στρατό των ΗΠΑ. Είναι επίσης όλο και πιο σημαντικός για τον σύγχρονο κόσμο γενικά. Όπως φαίνεται στις διάφορες

παραβιάσεις και επιθέσεις ransomware που έχουν έρθει στο φως, η κυβερνοασφάλεια για την άμυνα εκτείνεται πολύ πέρα από το Υπουργείο Άμυνας. Όλοι οι οργανισμοί για την εθνική ασφάλεια σε συνεργασία με την USCYBERCOM έχουν την αρμοδιότητα να λειτουργούν στον κυβερνοχώρο χωρίς διακοπή.

4.8.2 Ρωσία

Οι δυνατότητες της Ρωσίας στον κυβερνοχώρο είναι πολύ προηγμένες και η Μόσχα έχει επιδείξει προθυμία να χρησιμοποιήσει επιθετικά τον κυβερνοχώρο σε καταστάσεις παρά τον συμβατικό πόλεμο ιδίως για να επηρεάσει πολιτικά και οικονομικά τα γειτονικά κράτη και να αποτρέψει τους αντιπάλους της.

Πρόσφατες επιχειρήσεις στον κυβερνοχώρο—όπως το η προσπάθεια εμπλοκής στις αμερικάνικες εκλογές το 2016 (επίθεση στο δημοκρατικό κόμμα) και η επίθεση στο ουκρανικό ηλεκτρικό δίκτυο—δείχνουν ότι οι δυνατότητες και οι τακτικές στον κυβερνοχώρο της Ρωσίας συνεχίζουν να εξελίσσονται και να προσαρμόζονται. Η Εσθονία, η Γεωργία και η Ουκρανία έχουν χρησιμεύσει ως τόποι δοκιμών των δυνατοτήτων στον κυβερνοχώρο της Ρωσίας, παρέχοντας ευκαιρίες σε αυτήν να βελτιώσει τις τεχνικές και τις διαδικασίες της στον κυβερνοχώρο, ενώ ταυτόχρονα επιδεικνύει τις δυνατότητές της στην παγκόσμια σκηνή για να επηρεάσουν ή να αποτρέψουν τους αντιπάλους της Ρωσίας.

Κρατικοί φορείς, όπως η GRU και FSB, πιστεύεται ότι διαδραματίζουν τον σημαντικότερο ρόλο στις ρωσικές επιθετικές επιχειρήσεις στον κυβερνοχώρο. Ο κυβερνοχώρος συνεχίζει να είναι αποκλειστικό κτήμα των υπηρεσιών ασφαλείας του κράτους. Η Ομοσπονδιακή Υπηρεσία Ασφαλείας (FSB) φαίνεται να είναι επίσης ο κύριος παράγοντας της Ρωσίας για τον συντονισμό της κυβερνοπροπαγάνδας και των εκστρατειών παραπληροφόρησης. Επιπλέον, η FSB διατηρεί και λειτουργεί το SORM, το εσωτερικό σύστημα επιτήρησης του κυβερνοχώρου (Soldatov, Borogan, 2015). Άλλες υπηρεσίες που σχετίζονται με τον κυβερνοχώρο είναι η Ομοσπονδιακή Υπηρεσία

Εποπτείας των τηλεπικοινωνιών, τεχνολογιών πληροφορικής και μαζικών επικοινωνιών (Roskomnadzor), η οποία είναι υπεύθυνη για την επίβλεψη των μέσων ενημέρωσης, συμπεριλαμβανομένων των ηλεκτρονικών μέσων. Ακόμα, η Διεύθυνση Κ του Υπουργείου Εσωτερικών (MVD) επικεντρώνεται στο έγκλημα στον κυβερνοχώρο. Τέλος, ο ρωσικός στρατός εισήλθε τα τελευταία χρόνια στην αρένα του κυβερνοχώρου χωρίς να υπάρχουν πολλές πληροφορίες.

Οι ομάδες hacking στον κυβερνοχώρο ή οι ομάδες προηγμένων επίμονων απειλών (APT) ήταν το κεντρικό τμήμα της εργαλειοθήκης της Ρωσίας. Ενώ, απευθείας συνδέσεις με τη ρωσική κυβέρνηση είναι δύσκολο να αποδειχθούν καθώς η ρωσική κυβέρνηση αρνείται ότι χορηγεί οποιεσδήποτε ομάδες χάκερ. Βέβαια, υπάρχει ένας αριθμός ομάδων των οποίων οι δραστηριότητες είναι στενά ευθυγραμμισμένες με τους στόχους και τη στρατηγική του Κρεμλίνου. Η Ρωσία δεν είναι μοναδική από αυτή την άποψη:
Η Κίνα, το Ιράν, η Βόρεια Κορέα είναι γνωστό ότι αναθέτουν σε εξωτερικούς συνεργάτες τις δραστηριότητές τους. Πλέον, πιστεύεται ότι γίνονται πιο προσαρμοσμένες προσεγγίσεις, με την καθοδήγηση κυρίως της FSB και άλλων κρατικών φορέων μέσω ανάπτυξης κακόβουλου λογισμικού για επίθεση σε συγκεκριμένα τρωτά σημεία των αντίπαλων συστημάτων. Η συνέχιση πάντως της χρησιμοποίησης ομάδων εκτός του στενού πυρήνα του κράτους γίνεται για την ανωνυμία που προσφέρουν όσο και για την ευκολία που μπορούν να κινητοποιηθούν.

Αν και ο ρωσικός στρατός, όπως αναφέρθηκε ήδη, άργησε να ενσωματώσει τον κυβερνοχώρο τόσο για δομικούς όσο και για δογματικούς λόγους, το Κρεμλίνο έχει επισημάνει ότι σκοπεύει να ενισχύσει την επίθεση καθώς και τις αμυντικές δυνατότητες στον κυβερνοχώρο των ενόπλων δυνάμεών της με τη δημιουργία ειδικής στρατιωτικής μονάδας κυβερνοχώρου, που αναφέρεται πλέον ως Κέντρο Κυβερνοάμυνας υπαγόμενο στο Γενικό Επιτελείο. Η σύγκρουση στη Γεωργία παρείχε το πρώτο πρακτικό παράδειγμα

όπου οι συμβατικές επιχειρήσεις του ρωσικού στρατού είχαν συγχρονιστεί με τις επιχειρήσεις στον κυβερνοχώρο.

Σύμφωνα με τον James Clapper, πρώην διευθυντή της Εθνικής Υπηρεσίας Πληροφοριών επί προεδρίας Ομπάμα, Ρώσοι χάκερ είχαν διεισδύσει σε δίκτυα βιομηχανικού ελέγχου των ΗΠΑ που ήταν υπεύθυνα για τη λειτουργία κρίσιμης σημασίας υποδομή. Ο στόχος των χάκερ φαίνεται να ήταν η ανάπτυξη της δυνατότητας απομακρυσμένης πρόσβασης και διακοπής των συστημάτων ελέγχου σε περίπτωση εχθροπραξιών. Η κυβερνοεπίθεση στη SolarWinds που αναφέρθηκε σε προηγούμενη ενότητα, ήρθε να επιβεβαιώσει αυτή την υποψία.

Η Ρωσία γνωρίζει ότι δεν μπορεί να βασιστεί μόνο σε συμβατικές τακτικές αν θέλει να αντιπαρατεθεί με οργανισμούς σαν το ΝΑΤΟ που έχει ηγέτιδα δύναμη τις ΗΠΑ και για αυτό το λόγο εξελίσσει και ενσωματώνει τις επιχειρήσεις στον κυβερνοχώρο.

4.8.3 Κίνα

Η Λαϊκή Δημοκρατία της Κίνας (ΛΔΚ) διατηρεί μια ισχυρή ικανότητα στο να διεξάγει επιχειρήσεις στον κυβερνοχώρο μέσω της συνδυασμένης χρήσης του διαδικτύου και των ψυχολογικών επιχειρήσεων, της προπαγάνδας των μέσων ενημέρωσης και των δυνατοτήτων ηλεκτρονικού πολέμου.

Η Κίνα διαθέτει εξελιγμένες δυνατότητες στον κυβερνοχώρο και αυτό αποδεικνύεται από τον τεράστιο αριθμό των επιθέσεων και των γεγονότων κατασκοπείας που διαπράττει η χώρα. Η Εθνική Αντικατασκοπεία των Η.Π.Α. χαρακτηρίζει τις δραστηριότητες αυτές ως ανερχόμενες σε επίπεδο στρατηγικής θεωρώντας τες ως απειλή για το εθνικό συμφέρον των ΗΠΑ. Οι επιθετικές προσπάθειες συλλογής της Κίνας φαίνεται να αποσκοπούν στη συγκέντρωση δεδομένων και μυστικών (στρατιωτικών, εμπορικών κ.λπ.) που θα υποστηρίξουν και θα προωθήσουν την οικονομική ανάπτυξη της χώρας, τις επιστημονικές και τεχνολογικές ικανότητες, τη στρατιωτική ισχύ κ.λπ.—όλα με

στόχο την εξασφάλιση στρατηγικού πλεονεκτήματος σε σχέση με ανταγωνιστικές χώρες και αντιπάλους.

Οι ικανότητες στον κυβερνοχώρο της Κίνας την καθιστούν χώρα πρώτου επιπέδου, της οποίας οι ικανότητες είναι συγκρίσιμες με αυτές της Ρωσίας και άλλων μεγάλων κρατών. Επίσημα, η Κίνα, σύμφωνα με έρευνα (Morgus *et al, 2019*), ξοδεύει κοντά 154,3 δισεκατομμύρια δολάρια ετησίως για τον στρατό της, αν και ο αριθμός αυτός είναι πιθανώς

πιο κοντά στα 190 δισεκατομμύρια δολάρια, αν ληφθεί υπόψη το «ανεπίσημο». Ο ακριβής αμυντικός προϋπολογισμός της Κίνας είναι απόρρητος, και επομένως είναι δύσκολο να εκτιμηθεί το σύνολο που δαπανάτα στον κυβερνοχώρο. Σίγουρα πάντως τα χρηματικά ποσά που δίνονται για την ανάπτυξη δυνατοτήτων στον κυβερνοχώρο, είναι σημαντικά.

Η Κίνα, μέσω της κρατικής πρωτοβουλίας «Made In China 2025» επιδιώκει να κατευθύνει απαραίτητα κονδύλια για την επίτευξη αυτάρκειας σε κρίσιμους τομείς όπως για παράδειγμα της πληροφορικής, που θα μπορούσε να οδηγήσει σε απώλεια του πλεονεκτήματος των Η.Π.Α σε αυτήν την περιοχή. Η Κίνα έχει επίσης επενδύσει σημαντικά χρηματικά ποσά σε κρίσιμες τεχνολογίες, όπως η τεχνητή νοημοσύνη και ο κβαντικοί υπολογιστές, οι οποίες και οι δύο έχουν ποικιλία πιθανών στρατιωτικών εφαρμογών, όπως τα συστήματα μάθησης και η κρυπτογραφία.

4.8.4 Ιράν

Το Ιράν επενδύει αρκετά για να επεκτείνει την ικανότητά του στον κυβερνοπόλεμο, καθώς είναι αντιληπτό ότι είναι ο μόνος τομέας που μπορεί να ανταγωνιστεί τις αντίπαλες χώρες (Ισραήλ, ΗΠΑ κλπ). Το Ιράν βασίζεται σε ομάδες χακερ ή σε άλλες οργανώσεις, προκειμένου να αυξήσει την δυναμική του στον κυβερνοχώρο. Η πιο γνωστή οργάνωση στην οποία βασίζεται, είναι η Χεζμπολάχ -η οποία για τον κυβερνοχώρο έχει μία ομάδα που ονομάζεται Cyber Hezbollah. Επίσης, η πιο γνωστή

ομάδα χάκερ είναι η Iranian Cyber Army, η οποία συνεργάζεται με τους Φρουρούς της Επανάστασης. Άλλες ομάδες χάκερ που συνεργάζονται με τους Φρουρούς της Επανάστασης είναι η ομάδα Ashiyane (Amit, 2010) και οι Basij (Congressional Research Service, 2020), οι οποίοι αμείβονται για να κάνουν επιχειρήσεις στον κυβερνοχώρο για λογαριασμό του καθεστώτος, παρέχουν μεγάλο μέρος του ανθρώπινου δυναμικού για τις κυβερνοεπιχειρήσεις του Ιράν.

Υπήρξαν επίσης σημαντικές εικασίες σχετικά με την ανάμειξη της κυβέρνησης του Ιράν σε διάφορα περιστατικά hacking, συμπεριλαμβανομένης της Voice of America, και της ολλανδικής εταιρείας DigiNotar (συμβάν του 2011) που εκδίδει πιστοποιητικά ασφαλείας. Οι επιπτώσεις από την τελευταία περίπτωση ήταν σημαντικές και επηρέασαν μια σειρά από οντότητες, συμπεριλαμβανομένων των δυτικών υπηρεσιών πληροφοριών και ασφάλειας, Yahoo, Facebook, Twitter και Microsoft. Επιπλέον, η υπόθεση DigiNotar έδειξε στο δυτικό κόσμο ένα νέο και ανησυχητικό επίπεδο πολυπλοκότητας από την πλευρά του Ιράν και τις δυνατότητές του. Ωστόσο, από τις πιο εντυπωσιακές επιχειρήσεις κυβερνοπολέμου θεωρείται η υπόθεση της αναγκαστικής προσγείωσης ενός αμερικανικού UAV στο Ιράν στο τέλος του 2011 (4/12/2011). Σύμφωνα με τα όσα ειπώθηκαν από την ιρανική πλευρά, το UAV εκτελούσε κατασκοπευτική πτήση πάνω από το έδαφος του Ιράν, όταν οι ιρανικές ένοπλες δυνάμεις κατάφεραν με συνδυασμό τεχνικών κυβερνοπολέμου και ηλεκτρονικού πολέμου να πάρουν τον έλεγχο πτήσης του UAV και να το προσγειώσουν σε ιρανικό έδαφος. Ορισμένοι ειδικοί είχαν αναφέρει ότι το Ιράν είχε στη διάθεσή του κατάλληλο εξοπλισμό ηλεκτρονικών παρεμβολών που είχε προμηθευτεί από την Ρωσία και κατάφερε να επέμβει με τεχνικές hacking στο σύστημα GPS του UAV.

4.8.5 Τουρκία

Η Τουρκία αναφέρεται στη συγκεκριμένη ενότητα όχι γιατί πλησιάζει κάποια από αυτές τις χώρες σε δυνατότητες κυβερνοπολέμου, αλλά γιατί λόγω εγγύτητας με την

Ελλάδα είναι ο βασικός αντίπαλος γεωστρατηγικά και θα πρέπει να αναφερθεί η κατάσταση στην οποία βρίσκεται στον τομέα της κυβερνοασφάλειας.

Στη θεσμική βάση, υπάρχει η Αρχή Τεχνολογιών Πληροφορικής και Επικοινωνίας (ICTA), το Τουρκικό Γενικό Επιτελείο, η ASELSAN (η κορυφαία αμυντική εταιρεία της Τουρκίας), η HAVELSAN (τουρκική εταιρεία αμυντικού λογισμικού) και η TUBITAK (το ινστιτούτο επιστημονικής έρευνας της κυβέρνησης της Τουρκίας). Όλοι αυτοί οι οργανισμοί ασχολούνται με θέματα κυβερνοασφάλειας εντός Τουρκίας. Υπάρχει μια συνεχής προσπάθεια να ενταχθούν όλες αυτές οι μεμονωμένες προσπάθειες κάτω από μια κυβερνητική ομπρέλα από τα τέλη του 2008.

Σήμερα, το ICTA, παρόμοιο με το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), εργάζεται σε συνεργασία με σχετικούς εθνικούς και διεθνείς εταίρους για την αύξηση της ικανότητας ασφάλειας στον κυβερνοχώρο της Τουρκίας από το 2004. Ως μέλος της Διεθνούς Πολυμερούς Συνεργασίας κατά του κυβερνοπολέμου, το ICTA παρέχει εκπαίδευση σχετικά με μελέτες κυβερνοασφάλειας στις αρχές των χωρών, όπως το Αζερμπαϊτζάν, η Αλβανία, η Βοσνία-Ερζεγοβίνη, η Γεωργία, το Καζακστάν, η Κιργιζία, το Κοσσυφοπέδιο, η Αίγυπτος, η Μογγολία, το Σουδάν, το Τατζικιστάν, το Τουρκμενιστάν. Οι κυβερνητικές υπηρεσίες, οι στρατιωτικοί φορείς και ο ιδιωτικός τομέας στην Τουρκία χρησιμοποιούν μεμονωμένες λύσεις κατά των επιθέσεων στον κυβερνοχώρο. Για παράδειγμα, σήμερα οι περισσότερες κυβερνητικές υπηρεσίες βασίζονται σε ξένες λύσεις, ενώ το τουρκικό Γενικό Επιτελείο (TGS) και η Εθνική Υπηρεσία Πληροφοριών (MIT) χρησιμοποιούν τοπικές λύσεις ασφάλειας στον κυβερνοχώρο που αναπτύχθηκαν από την HAVELSAN. Επιπλέον, η TUBITAK παρουσιάζει εγχώριες λύσεις κρυπτογράφησης σε όλους τους φορείς της κυβέρνησης, στρατιωτικά ιδρύματα και ιδιωτικούς τομείς.

4.9 Μη κρατικοί δρώντες

Ο κυβερνοπόλεμος λόγω της ανωνυμίας που προσφέρει ο κυβερνοχώρος μπορεί να διεξαχθεί από χώρες αλλά και από μη κρατικούς δρώντες οι οποίοι είναι ομάδες, μεμονωμένα άτομα ή και οργανώσεις χρηματοδοτούμενοι ή υποστηριζόμενοι από τα κράτη (Ziolkowski, 2013). Οι χώρες έχουν τη δυνατότητα για διεξαγωγή κυβερνοεπιχειρήσεων μέσω αυτών των μη κρατικών δρώντων, χωρίς να διαφαίνεται η σύνδεση μαζί τους και επομένως να έχουν την επιλογή της εύλογης άρνησης (Plausible Deniability) για τις κυβερνοεπιθέσεις που ορισμένα άλλα κράτη μπορεί να τις χρεώσουν σε αυτές.

Ορισμένοι τύποι μη κρατικών δρώντων παρουσιάζονται παρακάτω. Βέβαια, αρκετές φορές ορισμένες ομάδες που αναφέρονται παρακάτω συμπίπτουν και γενικά το να κάνουμε μια σαφή διάκριση μεταξύ τους είναι, σε πολλές περιπτώσεις, μάταιο, καθώς σε παγκόσμιο επίπεδο υπάρχουν διαφορετικοί ορισμοί, νομικά πλαίσια και πολιτικές απόψεις.

4.9.1 Απλοί άνθρωποι/Θύματα

Ο πιο συνηθισμένος δράστης στον κυβερνοχώρο είναι, φυσικά, ο απλός πολίτης ο οποίος κάνει χρήση του διαδικτύου για διάφορους νόμιμους σκοπούς, όπως η περιήγηση και η χρήση διαδικτυακών υπηρεσιών. Σε αυτή την κατηγορία εντάσσονται οικιακοί τελικοί χρήστες καθώς και εργαζόμενοι εταιρειών, οργανισμών ή κυβερνήσεων, με κοινό χαρακτηριστικό τους ότι οι ενέργειες και τα κίνητρα είναι καθαρά ατομικά και κυρίως καλοήθη. Είναι, λοιπόν, οι απλοί χρήστες που μπορεί κάποιοι να χρησιμοποιηθούν εν αγνοία τους σε φάση κυβερνοεπίθεσης. Ειδικότερα, σε περιπτώσεις όμως κυβερνοπεριστατικών αυτή η ομάδα ανθρώπων είναι ως επί το πλείστον παθητική ή δρα έμμεσα, π.χ. σαν «ζόμπι» θύμα ενός botnet (μια συλλογή υπολογιστών συνδεδεμένων στο διαδίκτυο των οποίων οι άμυνες ασφαλείας έχουν παραβιαστεί και ο έλεγχος έχει εκχωρηθεί σε κακόβουλο μέρος).

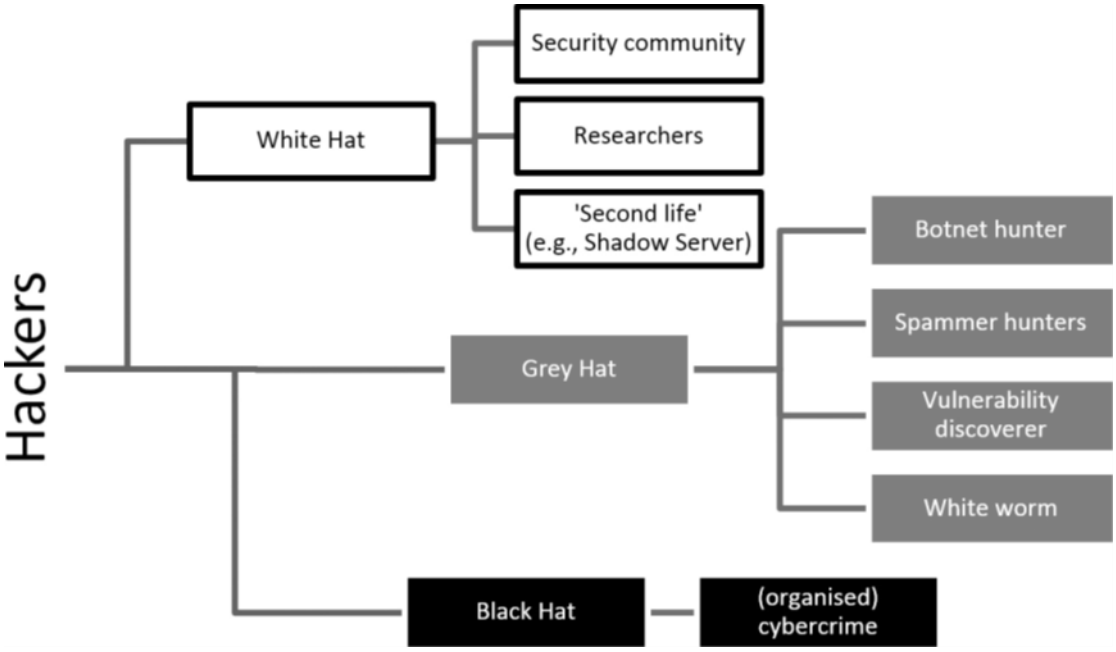
4.9.2 Χάκερς – Script Kiddies

Σε αυτή την κατηγορία εντάσσονται οι λεγόμενοι χάκερ ή αν γίνεται λόγος για νεότερα άτομα, τότε η ονομασία τους είναι script kiddies.

Η διαφορά τους έγκειται περισσότερο στη διαφορά της ηλικίας που κάνει τους μεν χακερς να δρουν με άκρως επαγγελματικό τρόπο (πολλές φορές έναντι αμοιβής) και τα script kiddies να δρουν βάση ενθουσιασμού, με κύριο μέλημά τους την προβολή των κατορθωμάτων τους σε κάποια σελίδα κοινωνικής δικτύωσης. Τα κοινά αυτών των δύο ομάδων είναι το ενδιαφέρον για την κυβερνοπειρατεία, τη τεχνολογία της πληροφορίας και κυρίως τη συγκίνηση της πρόκλησης.

Αναφορικά με την κοινότητα των χάκερ εξελίχθηκε σε τρεις κύριες ομάδες:

- White hat
- Grey hat
- Black hat



Εικόνα 4

Συχνά, οι χάκερ χωρίς κακόβουλη πρόθεση αναφέρονται ως white hat ή ηθικοί (ethical) χάκερ. Εκεί κατατάσσονται ερευνητές και ειδικοί στην ασφάλεια των πληροφοριακών συστημάτων και των δικτύων. Η δεύτερη ομάδα που προέκυψε ονομάζεται grey hat. Αυτοί οι χάκερ συχνά υποστηρίζουν την ευρύτερη κοινότητα, κάνοντας τον κυβερνοχώρο πιο ασφαλή, χρησιμοποιώντας τις δεξιότητές τους. Όμως επειδή δρούν χωρίς την κατάλληλη εξουσιοδότηση και γενικά χωρίς τη συγκατάθεση των στόχων των πράξεων τους, η δράση τους μερικές φορές θεωρείται εγκληματική. Ένα παράδειγμα των grey hat χακερς είναι η ανάληψη ενεργειών κατά των botnet και να μοιραστούν απαραίτητες πληροφορίες για εξάλειψη τρωτών σημείων λογισμικών ή υλικών. Τέλος, η τελευταία ομάδα (black hat) χρησιμοποιεί παρόμοιες γνώσεις με τις πάνω ομάδες για να εκβιάσουν τα θύματά τους. Τα μέλη αυτής της ομάδας χρησιμοποιεί τις δεξιότητες και τις γνώσεις της κυρίως για προσωπικό κέρδος, για να κερδίσει παράνομα χρήματα κλέβοντας σημαντικές πληροφορίες ή εκβιάζοντας άλλους με άρνηση σημαντικών για αυτούς υπηρεσιών.

4.9.3 Χάκερς/Ακτιβίστες

Ο ακτιβισμός στο hacking (hactivism) είναι η χρήση πόρων του κυβερνοχώρου ως μέσο γενικής διαμαρτυρίας ή για την προώθηση μιας εκφρασμένης ιδεολογίας ή πολιτικής ατζέντας. Ο ακτιβισμός στον κυβερνοχώρο μπορεί επίσης, έμμεσα, να χρησιμοποιηθεί ως μέθοδος για την επίτευξη υποκείμενων, κρυφών πολιτικών, στρατιωτικών ή εμπορικών στόχων. Εργαλεία που χρησιμοποιούνται από τους χάκερ – ακτιβιστές είναι οι παραμορφώσεις ιστοσελίδων, ανακατευθύνσεις πόρων στο διαδίκτυο, DOS επιθέσεις, κλοπή πληροφοριών, εικονικές ιστοσελίδες κλπ.

Η ομάδα των "Anonymous" θεωρείται πολλές φορές ως αρχέτυπο ενός χάκερ ακτιβιστή (Olson, 2012). Αποτελείται από μια μικτή ομάδα ατόμων, που περιλαμβάνει από script kiddies έως black hat χάκερς, συνδεδεμένους μέσω εφαρμογών ή υπηρεσιών κοινωνικής δικτύωσης. Έχουν αναλάβει την ευθύνη για πολλά σημαντικές, ευρέως δημοσιοποιημένες κυβερνοεπιθέσεις τα τελευταία χρόνια, κερδίζοντας ευρεία προσοχή και μερικές φορές και την αποδοχή του ευρύτερου κοινωνικού συνόλου. Στο ίδιο πλαίσιο βρίσκεται και ο διεθνής μη κερδοσκοπικός οργανισμός MME, Wikileaks.

4.9.4 Χάκερς – Πατριώτες

Οι πατριώτες χάκερ δρουν μεμονωμένα ή σε ομάδες και έχουν ως κύριο κίνητρο να βοηθήσουν ή να υποστηρίξουν τις δικές τους χώρες σε μια συνεχιζόμενη σύγκρουση ή πόλεμο, πραγματοποιώντας διάφορες ανατρεπτικές ενέργειες στον κυβερνοχώρο που απευθύνονται στον εχθρό του κράτους.

Οι Κινέζοι χάκερς παραδοσιακά είχαν και συνεχίζουν να έχουν ιδιαίτερη τάση προς το πατριωτικό hacking (Hvistendahl, 2010). Η πιο γνωστή πατριωτική κινέζικη ομάδα είναι η «Red Hacker Alliance» ή «Honker Union of China».

Η Ρωσία φιλοξενεί επίσης μια ενεργή συλλογικότητα πατριωτών χάκερς. Αυτό έγινε εμφανής κατά τις επιθέσεις DOS του 2007 με στόχο την Εσθονία, στον απόηχο της διαμάχης για τη μετεγκατάσταση του μνημείου του πολέμου της Σοβιετικής Ένωσης και πάλι το 2008, όταν η Γεωργία έγινε στόχος ανάλογων επιθέσεων σε συνδυασμό με τη συμβατική στρατιωτική εισβολή των ρωσικών δυνάμεων.

4.9.5 Κυβερνοτρομοκράτες

Οι τρομοκράτες είναι εξτρεμιστές που δεν διστάζουν να κάνουν χρήση ακραίων μέσων, όπως τη καταστροφική βία κατά της ατομικής ή δημόσιας περιουσίας, σε επιδίωξη των πολιτικών τους στόχων ή των ιδεολογικών τους επιδιώξεων. Οι κυβερνοτρομοκράτες είναι τακτικά συνηθισμένοι χάκερ και χρησιμοποιούν τεχνολογίες υπολογιστών και δικτύων για να πραγματοποιήσουν τις επιθέσεις.

Υπάρχουν πολλοί που υποστηρίζουν ότι ο κίνδυνος της τρομοκρατίας μέσω του κυβερνοχώρου είναι υπαρκτός και άλλοι ερευνητές που διαφωνούν (Schneier 2010).

4.9.6 Οργανωμένο κυβερνοέγκλημα

Το οργανωμένο έγκλημα στον κυβερνοχώρο μπορεί, κατά κάποιο τρόπο, να θεωρηθεί ως ανάλογο του αντίστοιχου στον πραγματικό κόσμο. Ο κυβερνοχώρος επιτρέπει σε άτομα από διαφορετικά μέρη του κόσμου να συνδεθούν και να σχηματίσουν εγκληματικά δίκτυα που μοιράζονται έναν κοινό στόχο ή συμφέρον. Η επικοινωνία αυτών και οι συνεννοήσεις τους γίνονται κατά βάση μέσω του dark web.

Οι ομάδες, στο οργανωμένο κυβερνοέγκλημα, τείνουν να είναι αρκετά μικρές και πολλές φορές τα κέρδη τους είναι πραγματικά τεράστια. Για παράδειγμα, σύμφωνα με μελέτη που έγινε από την εταιρία ασφαλείας Sophos, ομάδα που σχετιζόταν με το κυβερνοέγκλημα κατάφεραν να κλέψουν 900 εκατομμύρια δολάρια το 2011 στη Βραζιλία.

4.9.7 Κυβερνοπολιτοφύλακες

Ως κυβερνοπολιτοφυλακή μπορεί να οριστεί ως μια ομάδα εθελοντών που είναι πρόθυμοι και ικανοί να πραγματοποιήσουν κυβερνοεπιθέσεις προκειμένου να επιτευχθεί ένας πολιτικός στόχος (Lorents, 2010) . Χρησιμοποιούν για επικοινωνία, ένα φόρουμ στο

διαδίκτυο ή μια υπηρεσία μέσων κοινωνικής δικτύωσης. Επίσης, θα πρέπει να επισημανθεί ότι η διασύνδεση μιας χώρας με ομάδες κυβερνοπολιτοφυλάκων δεν συνεπάγεται τον πλήρη έλεγχο των ομάδων αυτών από τη χώρα, αλλά ούτε και την πλήρη γνώση από τη χώρα για την ταυτότητα του συνόλου των μελών αυτών των ομάδων. Βάσει αυτού, πρέπει να τονισθεί ότι, οι κυβερνοπολιτοφύλακες μπορούν να διεξάγουν κυβερνοεπιθέσεις, χωρίς κατά ανάγκη αυτό να απορρέει από μία άμεση ή έμμεση κυβερνητική εντολή.

Κεφάλαιο 5 - Συζήτηση και Σχολιασμός Αποτελεσμάτων

Βάσει των δεδομένων που παρουσιάστηκαν στο κεφάλαιο 4, τα οποία αφορούν τον κυβερνοχώρο και ορισμένα είναι βασικά συστατικά του κυβερνοπολέμου, καθώς και η ανάλυση των σημαντικών χωρών που έχουν αυξημένες δυνατότητες σε θέματα κυβερνοπολέμου είτε σε παγκόσμιο επίπεδο είτε σε τοπικό (πχ Τουρκία), σε αυτό το κεφάλαιο γίνεται αναφορά στο πώς η ΕΕ και ειδικότερα η Ελλάδα αντιμετωπίζουν το θέμα της κυβερνοασφάλειας. Ειδικότερα, για την Ελλάδα παρατίθενται στρατηγικοί στόχοι που θα ήταν καλό να υλοποιήσει ώστε να εξελιχθεί και να διαδραματίσει σπουδαίο ρόλο, αρχικά, σε τοπικό επίπεδο (νοτιανατολική Ευρώπη).

5.1 Κατάσταση στην ΕΕ

Η κυβερνοασφάλεια βρίσκεται στο επίκεντρο του ψηφιακού μετασχηματισμού της Ευρωπαϊκής Ένωσης. Γενικά, παρατηρείται τα τελευταία χρόνια μία συνεχής προσπάθεια η ΕΕ να βγει στο προσκήνιο και να διαδραματίσει σημαντικό ρόλο σε θέματα κυβερνοασφάλειας και αποτροπής κυβερνοπολέμου και κυβερνοεπιθέσεων στα κράτη – μέλη της. Για το σκοπό αυτό, έχει ξεκινήσει διαδικασία εκσυγχρονισμού της ΕΕ με την έκδοση πολιτικών και οδηγιών με θέματα τη διασφάλιση προϊόντων πληροφορικής – επικοινωνιών μέσω κοινού πλαισίου αξιολόγησής τους, συστήματα AI και γενικότερα ζητήματα διασφάλισης επικοινωνιών και πληροφορικής.

Επιπλέον, σύμφωνα με τη στρατηγική ασφάλειας Cyber που δημοσιεύτηκε τον Δεκέμβριο του 2020, η Ευρωπαϊκή Ένωση πρέπει να δημιουργήσει μια ισχυρή "ασπίδα στον κυβερνοχώρο" (cyber shield) με σκοπό να προστατεύσει τους πολίτες, τις βιομηχανίες και τις αξίες της. Για να γίνει αυτό, η Ένωση επενδύει σε θέματα κυβερνοασφάλειας όπως είναι το ολοκληρωμένο δίκτυο Επιχειρησιακών Κέντρων Ασφάλειας (SOC), ενισχύοντας παράλληλα τη βιομηχανία της κυβερνοασφάλειας και δεξιότητες για τη διασφάλιση της αυτονομίας της. Το Πρόγραμμα Ψηφιακής Ευρώπης (Digital Europe Programme) θα ενισχύσει τις δυνατότητες της Ένωσης για ανθεκτικότητα και προστασία τόσο των πολιτών όσο και των οργανισμών της με στόχο –μεταξύ άλλων– τη βελτίωση της ασφάλειας των προϊόντων επικοινωνιών - πληροφορικής και των υπηρεσιών.

Οι δραστηριότητες θα έχουν ως στόχο:

- Υποστήριξη της ανάπτυξης υποδομής κυβερνοασφάλειας.
- Ενίσχυση της υιοθέτησης της ασφάλειας στον κυβερνοχώρο, ειδικά σε τομείς που επηρεάζονται από την πανδημία COVID-19 και την επακόλουθη οικονομική κρίση
- Υποστήριξη της εφαρμογής της σχετικής νομοθεσίας της ΕΕ και των πολιτικών πρωτοβουλιών:

α) Στρατηγική κυβερνοασφάλειας,

β) Ασφάλεια πληροφοριακών συστημάτων και δικτύων (NIS Directive)

γ) Cybersecurity Act

δ) Κανονισμός για την ευρωπαϊκή βιομηχανία κυβερνοασφάλειας

ε) Κέντρο Τεχνολογίας και Ερευνητικής Ικανότητας (ECCC)

στ) Network of National Coordination Centres

ζ) Cybersecurity Blueprint and Joint Cyber Unit

η) The 5G cybersecurity toolbox

Σκοπός είναι η αύξηση της ευαισθητοποίησης και προώθησης των δεξιοτήτων και της εκπαίδευσης στον κυβερνοχώρο. Όλες οι δραστηριότητες λαμβάνουν δεόντως υπόψη τις θεμελιώδεις αξίες, ιδίως που σχετίζονται με την ιδιωτικότητα και την προστασία των δεδομένων.

5.2 Ελλάδα

Οι εσωτερικές προκλήσεις ασφάλειας και οι εγνωσμένες απειλές σε ευρωπαϊκό και διεθνές επίπεδο τοποθετούν την Ελλάδα, λόγω της υψηλής γεωστρατηγικής της αξίας, στο επίκεντρο των ψηφιακών απειλών και καταδεικνύουν την κρισιμότητα της παρούσας κατάστασης.

Στην Ελλάδα τη τελευταία δεκαετία άρχισαν να γίνονται ορισμένες ουσιαστικές παρεμβάσεις με σκοπό να τεθούν οι βάσεις για να μπορέσει η χώρα να ακολουθήσει το τρένο των εξελίξεων στον τομέα της κυβερνοασφάλειας και να μπορέσει γιατί όχι και να χρησιμοποιήσει υπέρ της, ενέργειες στον κυβερνοχώρο που θα μπορούσαν να την καταστήσουν σοβαρό παίχτη στη γεωπολιτική σκακιέρα της περιοχής.

Το θεσμικό πλαίσιο της χώρας που δείχνει τους κύριους παίχτες σε θέματα κυβερνοασφάλειας είναι το παρακάτω:

1) Με το νόμο 3649/2008: Άρθρο 4 §7. «Η Ε.Υ.Π. αποτελεί Τεχνικής Φύσεως Αρχή Ασφαλείας Πληροφοριών (INFOSEC) και μεριμνά, σύμφωνα με τις διατάξεις της παρ. 4 του άρθρου 2 του π.δ. 325/2003 (ΦΕΚ 273 Α'), για την ασφάλεια των εθνικών επικοινωνιών και συστημάτων τεχνολογίας πληροφοριών, καθώς και για την πιστοποίηση του διαβαθμισμένου υλικού των εθνικών επικοινωνιών. Η πιστοποίηση παρέχεται έναντι καταβολής ηλεκτρονικού παραβόλου, το ύψος του οποίου καθορίζεται με κοινή απόφαση του Πρωθυπουργού και του Υπουργού Οικονομικών».

§8.« Ορίζεται ως η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων, η οποία μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών

επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής, σύμφωνα με τις διατάξεις της παρ. 3 του άρθρου 2 του π.δ. 325/2003.»

2) Με το νόμο 4577/2018 οποίος ενσωμάτωσε την Οδηγία 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου: Άρθρο 8 «1.Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team CSIRT εφεξής «αρμόδια CSIRT»), η οποία καλύπτει τους τομείς του Παραρτήματος Ι και τις υπηρεσίες του Παραρτήματος ΙΙ του παρόντος, και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ.»

3) Με το ΠΔ 96/2020: Άρθρο 5. «Διεύθυνση Κυβερνοχώρου Είναι αρμόδια: α) για τεχνικής φύσεως θέματα ασφάλειας πληροφοριών (Εθνική Αρχή INFOSEC) και ειδικότερα για την ασφάλεια των εθνικών επικοινωνιών, των συστημάτων τεχνολογίας πληροφοριών, καθώς και για την αξιολόγηση και πιστοποίηση των διαβαθμισμένων συσκευών και συστημάτων ασφάλειας επικοινωνιών και πληροφορικής,

β) για την αξιολόγηση και πιστοποίηση κρυπτοσυστημάτων, καθώς και την υποστήριξη των Ενόπλων Δυνάμεων (Ε.Δ.) και των υπηρεσιών του δημοσίου τομέα σε θέματα κρυπτασφάλειας (Εθνική Αρχή CRYPTO),

γ) για την εξασφάλιση των εθνικών ηλεκτρονικών συσκευών τηλεπικοινωνιών από διαρροές λόγω ανεπιθύμητων, ηλεκτρομαγνητικών και μη μεταδόσεων (Εθνική Αρχή TEMPEST),

δ) ως Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT), εντός του εθνικού πλέγματος Κυβερνοασφάλειας που καθορίζει η Εθνική Αρχή Κυβερνοασφάλειας, για τις κυβερνοεπιθέσεις εναντίον των δημοσίων φορέων της χώρας, που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του Γ.Ε.ΕΘ.Α. (CSIRT). Ειδικότερα, υποστηρίζει την Προεδρία της Κυβέρνησης και τα Υπουργεία, με εξαίρεση το Υπουργείο

Εθνικής Άμυνας, για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων, εναντίον τους.»

4) Με το Π.Δ. 40/2020: Άρθρο 43. «Γενική Διεύθυνση Κυβερνοασφάλειας. 1. Η Γενική Διεύθυνση Κυβερνοασφάλειας έχει ως στρατηγικούς στόχους: (α) τη χάραξη ενιαίας πολιτικής Κυβερνοασφάλειας στο πλαίσιο της ελληνικής και ενωσιακής νομοθεσίας για την Κυβερνοασφάλεια και τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, όπως αυτές εκάστοτε ορίζονται νομοθετικά. Η Γενική Διεύθυνση Κυβερνοασφάλειας αποτελεί την Εθνική Αρχή Κυβερνοασφάλειας που έχει οριστεί κατά τις διατάξεις του ν. 4577/2018 (Α' 199). Η ενιαία πολιτική Κυβερνοασφάλειας διαμορφώνεται στο λαμβάνοντας υπόψη τις διατάξεις: ι) του ν. 4577/2018, ιι) της Οδηγίας (ΕΕ) 2016/1148/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194, 19.07.2016), ιιι) του Εκτελεστικού Κανονισμού (ΕΕ) 2018/151 της Επιτροπής, της 30ης Ιανουαρίου 2018, που θεσπίζει κανόνες για την εφαρμογή της Οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 26, 31.01.2018), όπως ισχύουν, (β) την εισήγηση προς την ΓΓΤΤ για την επικαιροποίηση των βασικών απαιτήσεων ασφαλείας των συστημάτων δικτύου και πληροφοριών για την επίτευξη υψηλού επιπέδου ασφαλείας των συστημάτων αυτών, κατ' επιταγή των διατάξεων της Οδηγίας (ΕΕ) 2016/1148/ΕΚ και των συστημάτων δικτύου και πληροφοριών της κεντρικής δημόσιας διοίκησης, κατά την κείμενη νομοθεσία, (γ) την επικαιροποίηση της λίστας των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) που έχει οριστεί με την υπ' αριθ. 1027 απόφαση του Υπουργού Επικρατείας για θέματα ψηφιακής διακυβέρνησης με θέμα «Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α' 199)» (Β' 3739), (δ) τη συνεργασία με τις συναρμόδιες για την Κυβερνοασφάλεια

αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο για την επίτευξη των εθνικών στόχων για την διασφάλιση του υψηλού επιπέδου ασφαλείας και την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών, σε συμμόρφωση με τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων, GDPR) (EEL 119, 04.05.2016). Μεταξύ άλλων, η Γενική Διεύθυνση Κυβερνοασφάλειας συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών κ.λπ., (ε) τη διαμόρφωση και παρακολούθηση εφαρμογών και υπηρεσιών μέσω του τομέα Κυβερνοασφάλειας και τη διασφάλιση της βέλτιστης χρήσης τους προς όφελος της κοινωνίας των πολιτών, (στ) την ενίσχυση της επιστημονικής έρευνας και ανάπτυξης καινοτόμων υπηρεσιών, εφαρμογών και εξοπλισμού, (ζ) την εκπροσώπηση της χώρας ως Εθνική Αρχή Κυβερνοασφάλειας καθώς και το συντονισμό των εκπροσώπων συναρμόδιων φορέων σε όλους τους ευρωπαϊκούς και διεθνείς οργανισμούς, καθώς και στις διεθνείς διακρατικές σχέσεις, (η) το χειρισμό θεμάτων και τη συνεργασία με εποπτευόμενους φορείς και υπηρεσίες σε ζητήματα σχεδιασμού και εφαρμογής πολιτικών και δράσεων για την Κυβερνοασφάλεια.»

Όπως προκύπτει από τα παραπάνω, φαίνεται να υπάρχει ένας κατακερματισμός αρμοδιοτήτων μεταξύ τριών φορέων (ΕΥΠ, ΓΕΕΘΑ, Υπουργείο Ψηφιακής Διακυβέρνησης), το οποίο δεν είναι καλό για το συντονισμό ενεργειών είτε σε περίπτωση ειρήνης είτε σε περίπτωση κρίσεων.

5.3 Στρατηγικοί στόχοι αντιμετώπισης κυβερνοπολέμου – Περίπτωση Ελλάδας

Όπως συμβαίνει σε κάθε νέο επίτευγμα τεχνολογικής ανάπτυξης, έτσι και στην κυβερνοασφάλεια, που αποτελεί αναπόσπαστο κομμάτι όλων των νέων τεχνολογιών, προβάλλονται συγκεκριμένοι τομείς, ώστε να επιτευχθούν οι στόχοι που έχουν καθορισθεί.

Για την επόμενη δεκαετία αυτοί οι θεμελιώδεις τομείς θα είναι οι λεγόμενοι «στρατηγικοί στόχοι». Παρακάτω, παρατίθενται και αναλύονται περαιτέρω οι στρατηγικοί στόχοι που θα πρέπει να έχει η Ελλάδα, αλλά και κάθε σύγχρονο κράτος για το μετέπειτα διάστημα, που σκοπό έχουν την ασφαλή πορεία:

α) Προστασία και αντοχή των κρίσιμων υποδομών

β) Ανάπτυξη εθνικής κυβερνοβάσης

γ) Δίκτυο κυβερνοασφάλειας & κουλτούρα επιχειρησιακής κυβερνοασφάλειας

δ) Ασφάλεια τεχνολογιών νέας γενιάς

ε) Αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο

στ) Ανάπτυξη διεθνούς συνεργασίας

5.3.1 Προστασία και αντοχή των κρίσιμων υποδομών

Ως κρίσιμες υποδομές θεωρούνται: «Οι υποδομές στις οποίες στεγάζονται πληροφορικά συστήματα όπου αν υπάρξει τρωτό σημείο στην λειτουργία του απόρρητου, την ακεραιότητα ή την πρόσβαση στα δεδομένα τα οποία επεξεργάζονται, μπορεί να ανοίξει τον δρόμο για ανθρώπινες απώλειες, μεγάλης έκτασης οικονομικές ζημιές, έκθεση της εθνικής ασφάλειας ή και διατάραξη της δημόσιας τάξης». Οι εν λόγω υποδομές που παρέχουν στους πολίτες τις αναγκαίες για την καθημερινότητά τους υπηρεσίες αποτελούν κύριο στόχο των κυβερνοεπιθέσεων και αποσκοπούν να διακόψουν την ομαλή λειτουργία τους. Στον εν λόγω τομέα, η Ελλάδα εναρμονίστηκε με την Οδηγία 2016/1148/ΕΕ (ευρέως γνωστή ως NIS Directive), με την οποία θεσπίστηκαν μέτρα για την επίτευξη υψηλού

επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών και η αρμοδιότητα αυτή ανήκει όπως παρουσιάστηκε παραπάνω στη Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ. Τα μέτρα αφορούν φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών, όπως η ενέργεια, οι μεταφορές, οι τράπεζες, ο τομέας της υγείας, η διανομή νερού, η ψηφιακή υποδομή, αλλά και υπηρεσίες online αγοράς, μηχανής αναζήτησης και cloud computing. Η συγκεκριμένη εναρμόνιση κινείται προς τη σωστή κατεύθυνση, αλλά και άλλες δράσεις πρέπει να γίνουν και εθνικά αλλά και ευρωπαϊκά μέσω της νέας ευρωπαϊκής οδηγίας (NIS Directive 2).

Περαιτέρω δράσεις θα πρέπει να συνεχίσουν να εκτελούνται με ακόμη μεγαλύτερη συνέπεια, λαμβάνοντας υπόψη τις εναλλασσόμενες κυβερνοαπειλές και τις εθνικές ανάγκες που προκύπτουν δεδομένων των τεχνολογικών εξελίξεων. Για αυτόν τον σκοπό η προστασία των κρίσιμων υποδομών πρέπει να οριστεί ως ένας εκ των στρατηγικών στόχων. Μέσω της λήψης μέτρων έναντι των κυβερνοαπειλών με σκοπό την προστασία του δημόσιου και του ιδιωτικού τομέα, επιδιώκεται η αύξηση της εθνικής αντίστασης. Στις εργασίες που θα πραγματοποιηθούν σε αυτό το πλαίσιο, θέματα όπως η πληροφοριακή ασφάλεια -σύμφωνα με τα διεθνή πρότυπα- στον δημόσιο και ιδιωτικό τομέα, και η παραμονή των εγχώριας παραγωγής δεδομένων στην χώρα θα διαδραματίσουν «ρόλο-κλειδί». Επιπλέον, στις προτεραιότητές θα πρέπει να περιλαμβάνεται η δημιουργία ελεγκτικών μηχανισμών και η εφαρμογή ρυθμίσεων σε ορισμένους τομείς, η δημιουργία πλάνων ετοιμότητας έκτακτης ανάγκης και ταυτόχρονα η μεγαλύτερη ενασχόληση και καλύτερη προσέγγιση των βιομηχανικών διεργασιών (SCADA) που στην Ελλάδα ακόμα βρίσκονται σε νηπιακό στάδιο. Στόχος, λοιπόν, θα πρέπει να είναι η όσο το δυνατόν αποτελεσματικότερη προστασία των κρίσιμων υποδομών και της εθνικής περιουσίας στον κυβερνοχώρο απέναντι σε κυβερνοαπειλές, όπως και η περαιτέρω ενδυνάμωση των ικανοτήτων στον τομέα της κυβερνοασφάλειας, της κυβερνοανθεκτικότητας και στη θωράκιση έναντι του κυβερνοπολέμου.

5.3.2 Ανάπτυξη εθνικής κυβερνοβάσης

Μία από τις σημαντικότερες συνιστώσες για την προάσπιση της εθνικής κυβερνοασφάλειας και την αντιμετώπιση κυβερνοαπειλών και ενός γενικότερου κυβερνοπολέμου, είναι η εξασφάλιση εξειδικευμένου προσωπικού. Προκειμένου να αντιμετωπίσει η Ελλάδα τις ανάγκες της σε αυτόν τον τομέα, κρίνεται αναγκαία η αύξηση του γνωστικού επιπέδου και της εμπειρίας του ήδη υπάρχοντος ανθρώπινου δυναμικού που θα εκτελέσει τις εν λόγω ενέργειες, αλλά και η εξειδίκευσή του.

Στο πλαίσιο αυτό, με στόχο την αύξηση του επιπέδου ετοιμότητας απέναντι σε κυβερνοαπειλές και στην πιθανότητα κυβερνοπολέμου θα πρέπει το στελεχιακό δυναμικό που ήδη υπάρχει να βοηθηθεί ώστε να βελτιώσει τις ικανότητες του. Επίσης, με στόχο την αύξηση της επάρκειας, κρίνεται σκόπιμο να πραγματοποιούνται συνεχώς σε εθνικό και διεθνές επίπεδο ασκήσεις και εκπαιδεύσεις στον τομέα της κυβερνοασφάλειας. Επιπροσθέτως, προκειμένου να αναπτυχθεί η εξειδίκευση στην κυβερνοασφάλεια και να της προσδωθεί η δέουσα επαγγελματική αξία, θα πρέπει να επιδιωχθεί η καθιέρωση των προγραμμάτων για την κυβερνοασφάλεια και τους σχετικούς με αυτήν τομείς στα πανεπιστήμια και να γίνουν οι προβλεπόμενες ενέργειες που θα αποσκοπούν στην αύξηση του βαθμού εξειδίκευσης όσων ασχολούνται με το εν θέματι αντικείμενο. Ένα από τα θέματα της εποχής είναι ότι θα πρέπει η κουλτούρα της κυβερνοασφάλειας και κατ'επέκταση του κυβερνοπολέμου να γίνει αντιληπτή από το σύνολο των πολιτών. Τα θεμέλια αυτής της κουλτούρας όμως εξαρτώνται από την εξασφάλιση του ανώτατου βαθμού αντίληψης, την σημασία της ασφαλούς χρήσης της τεχνολογίας και τον ενστερνισμό της από το κοινωνικό σύνολο. Τέλος, προτείνεται η δημιουργία ξεχωριστού κλάδου (Cyber) εντός των Ενόπλων Δυνάμεων, όπως έχει αρχίσει και συμβαίνει και σε άλλες χώρες (πχ ΗΠΑ, Κίνα) πέραν του Στρατού Ξηράς (ΣΞ), Πολεμικού Ναυτικού (ΠΝ),

Πολεμικής Αεροπορίας (ΠΑ) με στελέχη που θα εξειδικεύονται σε θέματα κυβερνοασφάλειας και κυβερνοπολέμου.

Για να είναι ένα κράτος όσο το δυνατό περισσότερο αυτάρκης στον τομέα της κυβερνοασφάλειας, της αποτροπής των κυβερνοεπιθέσεων και του κυβερνοπολέμου, είναι αναγκαίο να ενσωματωθούν νέες τεχνολογίες και η αύξηση και εξάπλωση της χρήσης λύσεων τοπικής και εθνικής κυβερνοασφάλειας. Αυτό μπορεί να επιτευχθεί με τόνωση της εγχώριας βιομηχανίας σε προϊόντα επικοινωνιών – πληροφορικής και στη θεσμοθέτηση πλαισίου πιστοποιήσεων των συστημάτων αυτών. Σαν χώρα, θεμελιώδης στόχος πρέπει να είναι η πρωτοπορία στον τομέα της κυβερνοασφάλειας και των εργασιών που εκτελούνται με την ανάπτυξη και εξέλιξη του ιδιωτικού τομέα, την εξασφάλιση της ενίσχυσης της οικονομίας μέσω της αύξησης των εξαγωγών και τον καθορισμό κατευθύνσεων στην τεχνολογία. Για την εξέλιξη του συστήματος κυβερνοασφάλειας απαιτείται η ανάπτυξη της συνεργασίας του δημόσιου, του ακαδημαϊκού και του ιδιωτικού τομέα. Οι εν λόγω συνεργασίες θα συμβάλουν άμεσα στην εξέλιξη των τοπικών και εθνικών προϊόντων. Ιδιαίτερα οι startup εταιρίες που τώρα ξεκινούν να δραστηριοποιούνται στην επιχειρηματικότητα, την έρευνα, την ανάπτυξη -και ειδικότερα κυρίως μικρές και μεσαίες επιχειρήσεις ιδιωτικού τομέα- θα επωφεληθούν από τους ήδη υπάρχοντες μηχανισμούς ενώ προβλέπεται να δημιουργηθούν και άλλοι μηχανισμοί στήριξης που θα ενισχύσουν αυτήν την βοήθεια.

Ειδικότερα, στους πρωταρχικούς στόχους πρέπει να περιλαμβάνονται η προάσπιση της κυβερνοασφάλειας με εθνικά προϊόντα και ιδιαίτερα η προστασία των κρίσιμων υποδομών με εθνικές λύσεις ασφάλειας. Η εξάρτηση από την Κίνα και άλλες χώρες (Ταϊβάν, Νότια Κορέα, Σιγκαπούρη, Τουρκία) για την κατασκευή εξαρτημάτων για συστήματα πληροφοριών ή προϊόντα γενικής τεχνολογίας (για παράδειγμα μικροτσίπ) είναι εκπληκτική. Η εφοδιαστική αλυσίδα μερών ή ολόκληρου συστήματος επικοινωνιών – πληροφορικής μπορεί να επηρεαστεί από κακόβουλο υλικό ή λογισμικό. Στο πλαίσιο

αυτό, και δεδομένης της μαζικής εισαγωγής προϊόντων ΤΠΕ (τεχνολογίες πληροφορικής επικοινωνιών) ή εξαρτημάτων (μικροτσίπ) λόγω του έντονου ψηφιακού μετασχηματισμού των δυτικών χωρών, δεν μπορεί να αποκλειστεί ότι αναξιόπιστες εταιρείες ή ακόμη και προμηθευτές πίσω από συγκεκριμένες χώρες ενδέχεται να θέτουν σε κίνδυνο την ασφάλειά τους. Για το λόγο αυτό, οι χώρες της ΕΕ αλλά και η Ελλάδα εσωτερικά πρέπει να σχεδιάσουν και να οδηγηθούν στη παραγωγή των δικών τους προϊόντων και εξαρτημάτων ΤΠΕ. Μια τέτοια στρατηγική θα βοηθούσε όχι μόνο στη δημιουργία καλύτερων αλυσίδων εφοδιασμού όσον αφορά την ασφάλεια στον κυβερνοχώρο, αλλά και στη μείωση της εξάρτησης από χώρες με ασταθές γεωπολιτικό περιβάλλον.

Έτερος θεμελιώδης στόχος πρέπει να είναι τα προϊόντα και οι υπηρεσίες που παράγονται από εθνικούς πόρους να διατεθούν προς τον υπόλοιπο κόσμο. Προς την επίτευξη αυτού του στόχου και προκειμένου να καταστούν ανταγωνιστικά στην διεθνή αγορά, θα πρέπει να υπάρχει δοκιμή (τεστ) ικανότητας απόδοσης και κυβερνοασφάλειας και να χορηγείται πιστοποιητικό από εθνικό μηχανισμό που θα δημιουργηθεί. Επίσης, ο μηχανισμός αυτός θα εξασφαλίσει τον έλεγχο όσον αφορά θέματα κυβερνοασφάλειας για προϊόντα ξένης προέλευσης που χρησιμοποιούνται Ελλάδα.

Παράδειγμα επίθεσης SolarWinds (2020): Στα μέσα Δεκεμβρίου του 2020 ανακαλύφθηκε η μεγαλύτερη κυβερνοεπίθεση που δέχθηκαν οι ΗΠΑ (Congressional Research Service, 2021). Η συγκεκριμένη εταιρία κυκλοφόρησε ένα update για τα συστήματά της, τα οποία υπήρχαν σε δεκάδες εταιρίες και κυβερνητικές υπηρεσίες (πχ Υπουργείο Ενέργειας, Εθνική Αρχή Διαχείρισης Πυρηνικών Όπλων κλπ), το οποίο ήταν παγιδευμένο να εισάγει backdoors αποκτώντας συνεχή πρόσβαση για σχεδόν ένα χρόνο μέχρι να εντοπιστεί, καθώς δεν αξιολογήθηκαν ποτέ ορισμένα από τα συστήματα της SolarWinds ή και το λογισμικό ανανέωσης για τα συστήματα της εταιρίας.

Εκτός από την αύξηση του επιπέδου ασφάλειας που προσφέρει ο έλεγχος όλου ή μέρους ΤΠΕ, οι αξιολογήσεις – πιστοποιήσεις αναβαθμίζουν το επιπέδου της χώρας στο

τεχνολογικό πεδίο και τονώνουν την εγχώρια βιομηχανία σε προϊόντα πληροφορικής και επικοινωνιών. Πιο συγκεκριμένα, όταν μία εταιρία μπορεί να πάρει την πιστοποίηση για προϊόν της με πιο εύκολες διαδικασίες (εντός της χώρας της), αυτή η εταιρία μπορεί άμεσα να προωθήσει το εν λόγω προϊόν σε υπόλοιπες στις οποίες αναγνωρίζεται αυτή η πιστοποίηση (πχ ΕΕ).

5.3.3 Δίκτυο κυβερνοασφάλειας & κουλτούρα επιχειρησιακής κυβερνοασφάλειας

Οι κυβερνοαπειλές γίνονται όλο και πιο πολυσύνθετες, ο εντοπισμός τους δύσκολος και εξαπλώνονται ως απειλή της εθνικής ασφάλειας. Εκτός από τις επιθετικές μεθόδους όπως οι επιθέσεις ransomware και το phishing, εμφανίζονται και κάποιες που έχουν σαν σκοπό να προκαλέσουν μεγάλης κλίμακας ζημιές όπως οι APT (Advanced Persistent Threat), των οποίων η πρόβλεψη αλλά και ο εντοπισμός είναι εξαιρετικά δύσκολοι. Το να αναχαιτιστούν τέτοιου είδους απειλές είναι άμεσα συνδεδεμένο με την εξέλιξη, σε προχωρημένο επίπεδο, των προγραμμάτων εξειδίκευσης, την ανάλυση των συνεχών απειλών και των μακρόπνοων εργασιών για την ωρίμανση των ομάδων αντιμετώπισης.

Με ένα ενιαίο δίκτυο κυβερνοασφάλειας, αυτός που εργάζεται στον τομέα της κυβερνοασφάλειας ή αυτός που ενδιαφέρεται για αυτήν, δηλαδή άτομα από κάθε τομέα, αποκτούν την δυνατότητα συμμετοχής μέσω συνεργασίας διαμοιρασμού γνώσης κι εμπειρίας.

Ο διαμοιρασμός της γνώσης και της πληροφορίας στην κυβερνοασφάλεια αποτελεί πλέον σημείο – κλειδί και θα πρέπει να υπάρξει ποικιλομορφία και αύξηση των πηγών. Λόγω αυτού είναι αναγκαία η δημιουργία ενός σύγχρονου SOC (Security Operation Center) για την εποπτεία των κρίσιμων υποδομών από κακόβουλες ενέργειες που μπορούν να είναι κάποιες μεμονωμένες κυβερνοαπειλές ή ένας εκτεταμένος κυβερνοπόλεμος. Έτσι,

στόχος πρέπει να είναι η δημιουργία, με αλληλεπίδραση 24/7, σε εθνική εμβέλεια, ενός ζωντανού ενεργού οργανικού δικτύου Κυβερνοασφάλειας.

Στο πλαίσιο του δικτύου κυβερνοασφάλειας θα πρέπει να προσθεθούν και οι διεθνείς συνεργασίες εντός και εκτός ΕΕ. Ειδικότερα, στην ΕΕ θα πρέπει να αρχίσει να γίνεται χρήση της εργαλειοθήκης Cyber Diplomacy Toolbox. Μόλις πρόσφατα τα κράτη μέλη της ΕΕ κατέβαλαν προσπάθειες να την αναπτύξουν για την αντιμετώπιση κυβερνοεπιθέσεων. Αυτό το έργο πρέπει να ολοκληρωθεί, ώστε η εργαλειοθήκη της Ένωσης να καταστεί πλήρως λειτουργική. Με την χρήση της θα μπορούν τα κράτη – μέλη να βάζουν κυρώσεις έναντι επιτιθέμενων, λειτουργώντας αποτρεπτικά. Γενικά, η εργαλειοθήκη της κυβερνοδιπλωματίας είναι συμπληρωματική προς τις ενέργειες μεμονωμένων κρατών μελών, αλλά η από κοινού λειτουργία θα επέτρεπε στα κράτη μέλη της ΕΕ να είναι πιο αξιόπιστα και να στείλουν ένα ισχυρότερο μήνυμα.

Η κυβερνοασφάλεια συνιστά πλέον αναπόσπαστο κομμάτι της Εθνικής Ασφάλειας. Έτσι, σε ανώτατο επίπεδο άσκησης της εθνικής πολιτικής, στόχος είναι να λαμβάνονται υπόψη και θέματα που αφορούν την κυβερνοασφάλεια, η οποία θα πρέπει να περιλαμβάνεται στα αμυντικά ζητήματα και να λαμβάνονται υπόψη και τα στοιχεία που αφορούν τον κυβερνοχώρο και την προστασία από υβριδικές απειλές.

5.3.4 Ασφάλεια τεχνολογιών νέας γενιάς

Σε αυτήν την στρατηγική, ένα από τα σημαντικά θέματα που χρήζουν αξιολόγησης θα πρέπει να είναι οι εφαρμογές τεχνολογίας νέας γενιάς, που και στην Ελλάδα ξεκίνησαν να βρίσκονται στο επίκεντρο. Οδεύουμε προς μια ψηφιακή εποχή διασυνδεδεμένων συστημάτων (Τεχνολογία 5G, Internet of Things - IoT, Quantum Computing, κτλ) από την οποία δεν υπάρχει επιστροφή και η ασφαλής τους χρήση είναι στοιχεία που μπορούν να ενισχύσουν την εθνική οικονομική ανάπτυξη. Σε συνδυασμό με τα προαναφερθέντα,

και η τεχνολογία της τεχνητής νοημοσύνης (AI) θα συμβάλει στην εξέλιξη τεχνολογιών σε τοπικό και εθνικό επίπεδο και στο πλαίσιο της κυβερνοασφάλειας.

5.3.5 Αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο

Η μεταφορά των αδικημάτων στον Κυβερνοχώρο, απειλές για τα δικαιώματα και τις ελευθερίες ατόμων και επιθέσεις που έχουν στόχο πληροφοριακά συστήματα συνιστούν ζητήματα με τα οποία έρχονται αντιμέτωποι όλες οι ανεπτυγμένες χώρες και εργάζονται αδιαλείπτως για την επίλυσή τους. Ως εκ τούτου, προκειμένου ο αγώνας ενάντια στο έγκλημα στον κυβερνοχώρο για την μελλοντική περίοδο να είναι πιο δυναμικός απαιτείται η αύξηση του ανθρώπινου δυναμικού σε εθνικό επίπεδο, με τεχνολογικές δυνατότητες. Στον αγώνα κατά του εγκλήματος στον κυβερνοχώρο, ιδιαίτερα σε διεθνές επίπεδο, προκύπτει η ανάγκη συνεργασίας. Ο πιο αποτελεσματικός τρόπος για να φτάσει κανείς στην πηγή του εγκλήματος και στον δράστη είναι ο διαμοιρασμός της πληροφορίας με προϋπόθεση την ανάπτυξη της διεθνούς συνεργασίας.

5.3.6 Ανάπτυξη διεθνούς συνεργασίας

Στον κυβερνοχώρο δεν υπάρχουν οριοθετημένα σύνορα. Κάθε λεπτό, κάθε δευτερόλεπτο, ο κυβερνοχώρος αποκτά μία δομή ολοένα και πιο διευρυμένη με την σύνδεση νέων συσκευών, συστημάτων και χρηστών.

Ο καθορισμός πολιτικής στην κυβερνοασφάλεια συνδέεται με την παρέμβαση σε όλα τα περιστατικά του κυβερνοχώρου. Υπάρχουν διμερείς και πολυμερείς συνεργασίες, όπου πραγματοποιούνται ανταλλαγές εμπειριών, γνώσεων αλλά και κατευθύνσεων για ενέργειες στον διεθνή μηχανισμό της κυβερνοασφάλειας.

Η Ελλάδα θα πρέπει να αναπτύξει ακόμα περισσότερο τις δυνατότητές της στην αποτροπή και αντιμετώπιση κυβερνοαπειλών ή κυβερνοπολέμου μέσω των διεθνών οργανισμών που είναι μέλος (ΕΕ ή NATO), αλλά και μέσω διμερών συνεργασιών με

περισσότερο ανεπτυγμένες τεχνολογικά χώρες που στρατηγικά μοιράζονται ίδιες γεωστρατηγικές θέσεις (πχ Ισραήλ, Ηνωμένα Αραβικά Εμιράτα κλπ).

Συμπεράσματα

Τα τελευταία χρόνια είμαστε μάρτυρες της συνεχούς βελτίωσης των τεχνολογιών πρόσβασης στο διαδίκτυο, που επιτρέπουν τη συνεχή σύνδεση στο διαδίκτυο των προσωπικών μας Η/Υ με μεγάλες ταχύτητες. Οι τεχνολογίες αυτές κάνουν ακόμα πιο σημαντικό το θέμα της ασφάλειας μιας και ο αυξημένος χρόνος σύνδεσης, καθώς και η διαθεσιμότητα μεγαλύτερου εύρους πρόσβασης, κάνει τους Η/Υ και ευκολότερους, αλλά και ελκυστικότερους στόχους. Τέλος, η πληροφορία παίζει πλέον ρόλο-κλειδί στη λειτουργία του παγκόσμιου συστήματος.

Ο κυβερνοπόλεμος πραγματοποιείται σε ένα τεχνητό περιβάλλον, κατασκευασμένο από τον άνθρωπο, που είναι χαοτικό και ατελές και έχει θέσει υπό αναθεώρηση τις παραδοσιακές αρχές πολέμου. Ειδικότερα, ο κυβερνοπόλεμος:

- Αποτελεί πολλαπλασιαστή ισχύος, όπλο με μικρό σχετικά κόστος αλλά με συγκριτικά μεγάλα αποτελέσματα, στον οποίο πρωτεύοντα ρόλο παίζει η εφευρετικότητα και η πρωτοτυπία.
- Είναι ένα μέσον προβολής ισχύος που δεν εξαρτάται από την γεωγραφία και αυτό είναι κάτι που συμβαίνει για πρώτη φορά στην ανθρώπινη ιστορία. Μέχρι τώρα, η στρατιωτική ισχύς και η γεωγραφία είχαν μια στενή αλληλεπιδραστική σχέση. Όμως ο κυβερνοπόλεμος είναι απαλλαγμένος από τους περιορισμούς του χώρου.
- Σκοπεύει στην «αχίλλειο πτέρνα» κάθε σύγχρονης χώρας, την ολοένα και αυξανόμενη «δικτύωση» μέσω ηλεκτρονικών πληροφορικών συστημάτων, τόσο της κοινωνίας γενικά, όσο και των ενόπλων δυνάμεων. Είναι μια εκτεταμένη

κατάσταση διαδικτυακών συγκρούσεων με αντιπάλους οι οποίοι είναι διατεθειμένοι να εξουθενώσουν ο ένας τον άλλο.

- Γίνεται ολοένα και περισσότερο πιο ισχυρός στο σύγχρονο πεδίο της μάχης και επηρεάζει την εξέλιξη του στρατού σε πολλές χώρες καθώς και την ανάπτυξη των εξοπλιστικών τεχνολογιών.

Η αξία του κυβερνοπολέμου αυξάνεται και με την ψηφιοποίηση των τεχνολογιών του συμβατικού πολέμου ενώ η χρήση περισσότερο περίπλοκων μηχανημάτων δημιουργεί κινδύνους και αδυναμίες που δίνουν τη δυνατότητα στις μονάδες κυβερνητικού πολέμου να προξενήσουν μεγαλύτερη βλάβη απ' ότι στο παρελθόν. Την τελευταία δεκαπενταετία, η ολοένα και στενότερη αλληλεξάρτηση της παγκόσμιας κοινωνίας μέσου του κυβερνοχώρου έχει αλλάξει τον τρόπο με τον οποίο η ανθρωπότητα επικοινωνεί, συναλλάσσεται αλλά και αντιλαμβάνεται την παγκόσμια ασφάλεια. Η ανάπτυξη της πληροφοριακής τεχνολογίας επιτρέπει την ταχύτατη μετάδοση δεδομένων, ξεπερνώντας τους γεωγραφικούς περιορισμούς του παρελθόντος. Πλέον αυτό που έχει επιτευχθεί με την παγκοσμιοποίηση και την ανάπτυξη της τεχνολογίας, είναι η διαγραφή των περιορισμών του χρόνου, του χώρου και των γεωγραφικών περιορισμών (Γιαλλουρίδης 2014).

Η ανάδειξη του κυβερνοχώρου ουσιαστικά υποβαθμίζει την έννοια της γεωγραφίας, τόσο ως παράγοντας μιας εθνικής πολιτικής ταυτότητας, όσο και ως διάσταση του πολέμου και της στρατηγικής. Μια συντονισμένη επίθεση στα τηλεπικοινωνιακά, μεταφορικά και ενεργειακά δίκτυα μιας χώρας, τα οποία σήμερα εξαρτώνται από δίκτυα υπολογιστών, μπορεί να διακόψει για ημέρες τις βασικές λειτουργίες της και να την καταστήσει ευάλωτη σε μία επακόλουθη κλασσική στρατιωτική επίθεση.

Σε μία περίοδο όπου ο κυβερνοπόλεμος χαρακτηρίζεται ήδη ένα άλλο, παράλληλο και εξίσου σημαντικό, πεδίο πολέμου, το οποίο δύναται να συμβάλει με μικρό κόστος στη διεξαγωγή ενός συμβατικού πολέμου, ή απλώς ως ένα πεδίο αναίμακτης αντιπαραθέσεως

σε κρίσεις, κάτι που βλέπουμε όλο και πιο συχνά τα τελευταία χρόνια, στο πεδίο των ελληνο-τουρκικών σχέσεων δεν πρέπει να αναμένεται τίποτα άλλο από διαρκείς κυβερνο-απειλές και κυβερνοεπιθέσεις.

Απέναντι στην τεράστια δύναμη που αποτελεί η τουρκική TUBITAK και η MIT, και τα υπό αυτό παρακλάδια του που στηρίζουν την όλη προσπάθεια, την αντίστοιχη υποστήριξη του Γενικού Επιτελείου (με τη δική του δομή για κυβερνοπόλεμο) και η οργανωμένη δύναμη εκατοντάδων στρατευμένων hackers, με ισχυρά πατριωτικά και θρησκευτικά κίνητρα (όπως αναφέρει η μελέτη του Holt), υπάρχει η ΕΥΠ, το ΓΕΕΘΑ και η Εθνική Αρχή Κυβερνοασφάλειας με όσα μέσα τους παρέχει το ελληνικό κράτος. Σκόπιμο είναι να μην υπάρχουν φορείς με παράλληλες και αλληλοκαλυπτόμενες αρμοδιότητες και ταυτόχρονα να δημιουργηθεί ξεχωριστός κλάδος (Cyber) εντός των Ενόπλων Δυνάμεων καθώς ο κυβερνοπόλεμος πλέον είναι άρρηκτα δεμένος με τον συμβατικό πόλεμο.

Γενικά, ο κυβερνοπόλεμος έχει περισσότερο στρατηγική παρά τακτική σημασία, και μπορεί να είναι αποτελεσματικότερος έως και ιδιαίτερα επωφελής σε περίοδο ειρήνης, παρά σε περίοδο πολέμου, διότι η συλλογή κατάλληλων πληροφοριών και η χρήση τους την πλέον «κατάλληλη» στιγμή, αποτελεί ισχυρό όπλο και επιφέρει σημαντικό χτύπημα στον αντίπαλο.

Οι κυβερνοεπιθέσεις εναντίον κρίσιμων υποδομών ή χρηματοοικονομικών συστημάτων θα μπορούσαν να αναστατώσουν την καθημερινή ζωή και να εμποδίσουν οποιαδήποτε απάντηση στην επιθετικότητα που θα εκδηλωνόταν στην άλλη άκρη του κόσμου. Οι απαντήσεις δεν είναι εύκολες και το καλύτερο το οποίο μπορούν να κάνει η Ελλάδα είναι να μετριάσει τις αδυναμίες της εσωτερικής ασφάλειας μέσω ενός μείγματος άμυνας, επίθεσης και ανθεκτικότητας. Αυτό θα απαιτήσει μεγαλύτερες και πιο συστηματικές επενδύσεις σε αυτό που κάποτε ονομαζόταν "πολιτική άμυνα" - σκλήρυνση

της ασφάλειας ζωτικής σημασίας υποδομών, υλικοτεχνικών εγκαταστάσεων και δικτύων επικοινωνιών κατά μιας πιθανής ψηφιακής διαταραχής - κατάρρευσης.

Βιβλιογραφία

Amit, Iftach Ian (2010), “Cyber [Crime/War],” DEFCON 18.

Björck *et al* (2015), “Cyber Resilience – Fundamentals for a Definition”, AISC, volume 353, Springer, https://doi.org/10.1007/978-3-319-16486-1_31

Bryman, Alan (2004), “Research Methods and Organization Studies”, Taylor & Francis e-Library.

Cavas, Christopher (2015), “China’s ‘Little Blue Men’ Take Navy’s Place in Disputes,” Defense News, available at: https://www.defensenews.com/naval/2015/11/03/chinas-little-blue-men-take-navys-place-in-disputes/

Chauvin, Justine (2016), “Cyber War Will Not Take Place”, Interstate - Journal of International Affairs

Clausewitz, Carl (2012), “Principles of War”, Courier Corporation

European Council, “JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response”, JOIN(2016) 18 final

Fischer, Eric (2016), “Cybersecurity Issues and Challenges: In Brief”

Freier N. (2009),“The defense identity crisis: It's a hybrid world”, Defense Technical Information Center

Glenn R.(2009), “Thoughts on “Hybrid” Conflict”, Small Wars Journal LLC.

Hathaway, Melissa and Spidalieri, Francesca (2017), “THE NETHERLANDS CYBER READINESS AT A GLANCE”, Potomac Institute for Policy Studies

Hoffman, FG (2007), “Conflict in the 21st century: The rise of hybrid wars”, Potomac Institute for Policy Studies

Hvistendahl, M.(2010), “China’s Hacker Army,” Foreign Policy.

Jang-Jaccard, Julian and Nepal, Surya (2014), “A survey of emerging threats in cybersecurity”.

Kaspersky Lab (2014), "The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies"

Krepinevich, Andrew (2006), “Calavry to computer, the pattern of military revolutions”, The National Interest n37.

Lewis, James (2015), “The role of offensive cyber operations in NATO’s collective defense”, CCDCOE

Lindsay J. (2013), “Stuxnet and the Limits of Cyber Warfare”, Security Studies, Volume 22, Issue 3, https://doi.org/10.1080/09636412.2013.816122

Libicki, Martin (2007), “Conquest in cyberspace: National security and information warfare”

Lorents, Peeter and Rain Ottis (2011),“Cyberspace: Definition and Implications”, Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US

Metz, Steven and Kievit, Jame (1995), “Strategy and Revolution in Military Affairs: From theory to policy”, US Army

Morgus, Robert *et al* (2019),” Are China and Russia on the Cyber Offensive in Latin America and the Caribbean?” , Florida International University.

Middleton, Alex (2016), “Stuxnet: The World's First Cyber... Boomerang?”, Interstate - Journal of International Affairs

Mueller, Benjamin (2014), “The laws of war and cyberspace: on the need for a treaty concerning cyber conflict”, London School of Economics and Political Science

Nagaraja, Shishir and Anderson Ross (2009), “The snooping dragon: social-malware surveillance of the Tibetan movement”, University of Cambridge

NATO REVIEW (2015), available at: https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html

New York State Department of Financial Services, (2021), “Report on the SolarWinds Cyber Espionage Attack and Institutions’ Response”

Olson, P. (2012), “We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency,” Little, Brown and Company.

O’ Anders, Adam (2011), “Roman Light Infantry and the art of combat”, University of Cardiff

Plakoudas, Spyridon (2017), “The Syrian Kurds and the Democratic Union Party: The Outsider in the Syrian War”, Mediterranean Quarterly, Duke University Press, Volume 28, Number 1, pp. 99-116

Rid, Thomas (2013), “Cyber War Will Not Take Place”, Oxford University Press

Shevchenko, Vitaly (2014), “‘Little Green Men’or ‘Russian invaders’?” BBC News, available at: https://www.bbc.com/news/world-europe-26532154

Singer, Peter and Friedman, Allan (2014), “Cybersecurity: What Everyone Needs to Know”, p.68,p.121

Soldatov, Andrei and Borogan, Irina (2015), *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries,* Public Affairs.

Streltsov (2015), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly, A/70/174

Yin, Robert (2003), "Case Study Research: Design and Methods", SAGE Publications

Ziolkowski, Katharina (2013), "Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy", NATO Cooperative Cyber Defence Centre of Excellence

Ζαφειρόπουλος (2015), "Πώς γίνεται μια επιστημονική εργασία;", σελ. 281-323, Αθήνα, Εκδόσεις ΚΡΙΤΙΚΗ

Νόβα-Καλτσούνη, Χ. (2006), "Μεθοδολογία εμπειρικής έρευνας στις κοινωνικές επιστήμες", Αθήνα: Gutenberg

Γιαλλουρίδης Χ. & Αναστασιάδου, Μερσίλεια, " Πολιτιστική Διπλωματία και Ήπια Ισχύς", Εικόνες Κρατών, 2014, σελ. 111

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

BBC News (2017), "Global ransomware attack causes chaos", available at https://www.bbc.com/news/technology-40416611

Congressional Research Service (2020),"Iranian Offensive Cyber Attack Capabilities", available at: https://crsreports.congress.gov/

Congressional Research Service (2021), "SolarWinds Attack—No Easy Fix", available at: https://crsreports.congress.gov/product/pdf/IN/IN11559

DoD (2016),"Hack the Pentagon" Fact Sheet, available at: https://dod.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf

Dubai Electronic Security Center (2017), "DUBAI CYBER SECURITY STRATEGY", Version 2.0., available at: https://u.ae/-/media/About-UAE/Strategies/Dubai-Cyber-Security-Strategy.ashx

FBI (2018), "RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS", available at: https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

IISS (2021), "Cyber Capabilities and National Power: A Net Assessment", available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

Kaspersky (2013), "Red October", available at: https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide

Schneier B (2010), "Threat of 'cyberwar' has been hugely hyped," CNN, available at: http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html

Turton William and Mehrotra Kartikay,(2021), “Hackers Breached Colonial Pipeline Using Compromised Password”, Bloomberg, available at: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Wethe David, (2021), “Saudi Aramco Confirms Data Leak After Reported Cyber Ransom”, Bloomberg, available at: https://www.bloomberg.com/news/articles/2021-07-21/saudi-aramco-confirms-data-leak-after-reported-cyber-extortion

Εθνική Αρχή Κυβερνοασφάλειας (2020), “ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025” available at: https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf