ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ & ΠΟΛΙΤΙΣΜΟΥ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ ΑΣΦΑΛΕΙΑΣ»

«ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ» ΝΕΑ ΜΟΡΦΗ ΠΟΛΕΜΟΥ;

Η ΔΙΕΥΡΥΝΣΗ ΤΗΣ ΕΝΝΟΙΑΣ ΚΑΙ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ ΣΤΗ ΣΥΓΧΡΟΝΗ ΕΠΟΧΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αριστοτέλης Π. Σαμαρτζίδης

Αθήνα, 2017

Τριμελής Επιτροπή
Χαράλαμπος Παπασωτηρίου, Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)
Κωνσταντίνος Υφαντής, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου
Ανδρέας Λιαρόπουλος, Επίκουρος Καθηγητής Πανεπιστημίου Πειραιά

Αφιερωμένη σε όσους στήριξαν τις προσπάθειες μου
τόσο σε οικογενειακό όσο και σε επαγγελματικό επίπεδο.

Σελίδα σκόπιμα κενή

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DNS	Domain Name System
DMZ	Demilitarized Zone
DODIN	Department of Defence Intranet
DOS	Denial of Service
FEDCIRC	Federal Computer Incident Response Center
FIRST	Forum for Incident Response Teams
GAO	General Accounting Office
IP	Internet Protocol
LAN	Local Area Network
NIPC	National Infrastructure Protection Centre
NSA	National Security Agency
RAM	Rapid Access Memory
R/CERTS	Regional Computer Emergency Response Teams
SIGINT	Signal Intelligence
URL	Uniform Resource Locator
WAN	Wide Area Network

Σελίδα σκόπιμα κενή

Ευχαριστίες

Ευχαριστώ τους γονείς μου που πίστεψαν σε αυτό που ήθελα να κάνω, την σύζυγο μου που με στήριξε στις δύσκολες στιγμές της επαγγελματικής μου καριέρας και τους καθηγητές μου που με εφοδίασαν με τα απαραίτητα εργαλεία για να διευρύνω τις γνώσεις μου.
Ιδιαίτερες ευχαριστίες στον Αντγο εα.κύριο Μαυρόπουλο Παναγιώτη για τη συμβολή και την υποστήριξη του στην υλοποίηση αυτής της διπλωματικής εργασίας.

Σελίδα σκόπιμα κενή

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα σκόπιμα κενή

Περίληψη

Η εποχή της πληροφορίας άλλαξε τις συνθήκες της ανθρώπινης δραστηριότητας, σε βασικούς τομείς, όπως κοινωνικό, οικονομικό, πολιτικό, πολιτισμικό κτλ. Η βελτίωση στις επικοινωνίες με κύριο χαρακτηριστικό τις υψηλές ταχύτητες, η γρήγορη μετάδοση πληροφοριών, καθώς και η ανταλλαγή αυτών στηρίχτηκε στην «Ψηφιακή επανάσταση». Αποτέλεσε δηλαδή την Τρίτη κοσμοϊστορική αλλαγή μετά την Αγροτική και Βιομηχανική επανάσταση. Ο ηλεκτρονικός υπολογιστής, η εξέλιξη της τεχνολογίας οδήγησαν στην περαιτέρω οργάνωση επικοινωνιακών δικτύων και δημιούργησαν εφαρμογές προκειμένου να υποστηρίξουν ανθρώπινες δραστηριότητες, οι οποίες για τη λειτουργία τους στηρίζονται σε δίκτυα υπολογιστών. Η εξέλιξη αυτών των δικτύων οδήγησε στο διαδίκτυο, οι υπηρεσίες του οποίου τέθηκαν στη διάθεση των πολιτών, δόθηκε η δυνατότητα της προσβασιμότητα τους από τον ευρύ πληθυσμό, ενώ παράλληλα η ταχύτητα με τη χρήση της νέας τεχνολογίας αυξήθηκε. Όλα αυτά οδήγησαν παράλληλα στην αύξηση της τρωτότητας τους.

Η τρωτότητα αυτή, αν συνδυαστεί με τη βελτιωμένη έκδοση των Κυβερνοόπλων του μέλλοντος, θα καταστήσει τον Κυβερνοχώρο ένα νέο πεδίο ανταγωνισμού, και τον Κυβερνοπόλεμο μια πραγματική πρόκληση για την Κυβερνοασφάλεια των κρατών.

Κυβερνοπόλεμος έχει οριστεί η προσπάθεια, από ένα έθνος - κράτος να αποκτήσει πρόσβαση σε υπολογιστές ή δίκτυα άλλου έθνους, με σκοπό την πρόκληση ζημιάς ή αναστάτωσης. Ο Κυβερνοπόλεμος είναι ένας από τους τέσσερις πυλώνες ισχύος του κράτους (οικονομία, διπλωματία και στρατιωτική ισχύς) και συνεπώς εντάσσεται στη σχεδίαση της Υψηλής Στρατηγικής ενός κράτους προκειμένου να υλοποιηθεί ο πολιτικός σκοπός σε σχέση με κάποιον αντίπαλο. Η αποκλειστική προσφυγή σε αυτόν θα αποτελούσε μια απλή παρενόχληση ή προειδοποίηση μιας χώρας πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών για τους κινδύνους που διατρέχει, αν αρνηθεί τη θετική ψήφο και η εκδίκηση για τυχόν αποφάσεις που ελήφθησαν χωρίς να ληφθούν υπόψη τα συμφέροντα της ενδιαφερόμενης χώρας. Ιδιαίτερα όταν μέσα στο παγκόσμιο περιβάλλον υπάρχει ασυμμετρία μεταξύ δυο κρατών στην ισχύ τους τότε, είναι η πιο ιδεατή λύση για το μέρος εκείνο της αντιπαράθεσης που είναι λιγότερο ισχυρό, διότι με τον τρόπο αυτό εκμεταλλευόμενο έναν γρήγορο, σχετικά φτηνό και αποτελεσματικό τρόπο μπορεί να υπονομεύσει τις κρίσιμες αλλά τρωτές υποδομές του αντιπάλου .

Την τελευταία δεκαετία, η σημασία των επιχειρήσεων στον Κυβερνοχώρο έχει γίνει εμφανέστερη.

Η εξέλιξη αυτή θα μπορούσε να θέσει σε κίνδυνο την εθνική μας ασφάλεια, αν οι Κυβερνοεπιθέσεις στρεφόταν εναντίον στρατιωτικών, κυβερνητικών ή κρίσιμων υποδομών δικτύων επικοινωνιών και πληροφορικής. Κατά συνέπεια, θα πρέπει να επικεντρωθούμε στην ανάπτυξη δυνατοτήτων οι οποίες θα μας επιτρέψουν να εισέλθουμε δυναμικά στον Κυβερνοχώρο και να προστατευθούμε έναντι ενδεχόμενων Κυβερνοαπειλών.

Ο κίνδυνος η Ελλάδα να βρεθεί απροετοίμαστη, όσον αφορά στη διασφάλιση των πλέον κρίσιμων εθνικών συμφερόντων στο μελλοντικό περιβάλλον ασφαλείας είναι, αν όχι σίγουρος, τουλάχιστον ορατός. Και μόνο το γεγονός, ότι η Τουρκία έχει ήδη οργανώσει από ετών το δικό της Κέντρο Κυβερνοπολέμου, σημαίνει πολλά για τη διαφορά επιπέδου όσον αφορά στη σοβαρότητα αντιμετώπισης του θέματος, την αξιολόγησή του, την ποιότητα του στελεχιακού δυναμικού και την ταχύτητα λήψης αποφάσεων.

Γίνεται λοιπόν κατανοητό ότι οι Ε.Δ. πρέπει να διαθέτουν την δυνατότητα και την ικανότητα της διασφάλισης εκτός των άλλων, της αδιάλειπτης λειτουργίας κρίσιμων υποδομών του κράτους, προκειμένου αυτό να καθίσταται αυτόνομο και να “πορεύεται εν ειρήνη” και ομαλότητα.

Λέξεις -κλειδιά: Πληροφορία ,Διαδίκτυο, Κυβερνοχώρος, Κυβερνοπόλεμος, Κυβερνοεπιθέσεις

Cyber Warfare: A new kind of War;
National Defense mechanism against this kind of warfare.

Aristotelis Samartzidis

Abstract

The era of information has changed the conditions of human activity in key areas such as social, economic, political, cultural, etc. The improvement in communications, characterized by high speeds, the rapid transmission of information and the exchange of information, was based on the "Digital Revolution". It was the third global change since the Agricultural and Industrial Revolution. The computer, the evolution of technology, led to the further organization of communication networks and created applications to support human activities, which are based on computer networks. The development of these networks led to the internet, the services of which were made available to citizens, accessibility was made available to the general public, and speed with the use of new technology increased. All this has led to increased vulnerability.

Vulnerability, in combination with modern Cyber capabilities, will make Cyberspace a new field of competition, and Cyber war a real challenge for State Cyber Security.

Cyber war has been used by a nation-state to achieve access to computers or networks of another nation for the purpose of causing damage or disruption. Cyber war is one of the four pillars of state power (economy, diplomacy, and military power), and is therefore part of the design of a state's High Strategy in order to realize the political purpose in relation to an opponent. Exclusive recourse to the Cyber war would be a simple harassment, or a warning of a country prior to making important decisions in international organizations about the risks it is going through, if it rejects the positive vote and revenge for any decisions taken without taking into account the interests of the concerned country. Particularly when there is an asymmetry between the two states in the world, the Cyber war is the most ideal solution for that part of the confrontation that is less powerful, because in this way taking advantage of a fast, relatively cheap and efficient way can undermine the critical but vulnerable infrastructure of the opponent.

Over the last decade, the importance of business in Cyberspace has become more prominent. This development could jeopardize our national security if Cyber-attacks were directed against military, governmental or critical communications and information network

infrastructures. Consequently, we should focus on developing capabilities that will enable us to dynamically enter the Cyberspace and protect against potential cyber threats.

The risk that Greece is unprepared for securing the most critical national interests in the future security environment is, if not certain, at least visible. And the fact that Turkey has already organized its own Center for Cyberwar for years means a lot to the difference in the level of seriousness of the issue, its evaluation, the quality of the executive staff and the speed of decision making.

It is therefore understood that the armed forces must be capable and able to secure, inter alia, the continued operation of critical state infrastructures in order to become autonomous and to "go in peace" and normality.

Keywords: Information, Internet, Cyberspace, Cyberwar, Cyber attacks

«ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ» ΝΕΑ ΜΟΡΦΗ ΠΟΛΕΜΟΥ;

Η ΔΙΕΥΡΥΝΣΗ ΤΗΣ ΕΝΝΟΙΑΣ ΚΑΙ ΤΩΝ ΜΗΧΑΝΙΣΜΩΝ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

ΣΤΗ ΣΥΓΧΡΟΝΗ ΕΠΟΧΗ

Αριστοτέλης Π.Σαμαρτζίδης

1. Εισαγωγή

Αν θέλουμε να συγκρίνουμε τη σημερινή εποχή με τις προηγούμενες θα διαπιστώσουμε ότι οι αντικαταστάθηκαν οι δραστηριότητες του ανθρώπου με εξελιγμένες πράξεις που υλοποιούνται από ηλεκτρονικούς υπολογιστές με αποτέλεσμα τα αυτοκίνητα να αντικατασταθούν με υπολογιστές με τέσσερις τροχούς τα αεροπλάνα με υπολογιστές με φτερά και ακουστικά βαρηκοΐας. με υπολογιστές που σε βοηθάνε να ακούς[1].

Η βελτίωση στις επικοινωνίες με κύριο χαρακτηριστικό τις υψηλές ταχύτητες η γρήγορη μετάδοση πληροφοριών καθώς και η ανταλλαγή αυτών στηρίχτηκε στην «Ψηφιακή επανάσταση», δηλαδή στα ψηφιακά λογικά κυκλώματα τα οποία σχεδιάστηκαν,κατασκευάστηκαν,παρήχθησαν,αναπτύχθηκαν,χρησιμοποήθηκαν, με χαμηλό κόστος ψηφιακών λογικών κυκλωμάτων και με αυτό τον τρόπο οδηγηθήκαμε σε ευρεία χρήση ηλεκτρονικών υπολογιστών, δικτύων και τηλεπικοινωνιών. Αποτέλεσε δηλαδή την Τρίτη κοσμοϊστορική αλλαγή μετά την Αγροτική και Βιομηχανική επανάσταση[2].

Η εποχή της πληροφορίας άλλαξε τις συνθήκες της ανθρώπινης δραστηριότητας, σε βασικούς τομείς, όπως κοινωνικό, οικονομικό, πολιτικό, πολιτισμικό κτλ[3].

Η πληροφορία αποτελεί γνώση και η γνώση αποτελεί δύναμη και επομένως η πληροφορία αποτελεί δύναμη από μόνη της. Με βάση την πληροφορία ο άνθρωπος αποφασίζει και δρα σύμφωνα με αυτό που πιστεύει, ότι είναι πραγματικότητα. Η νοημοσύνη του ανθρώπου βασίζεται σε αυτή. Η λήψη μιας απόφασης βασίζεται στην πληροφορία. Ο στρατιωτικός κλάδος, ο οποίος με τη χρήση των νέων τεχνολογιών ανέπτυξε, μέσα από τους τομείς της επικοινωνίας και της πληροφορικής, νέες δυνατότητες για τις επιθετικές και αμυντικές του επιλογές .

[1] Julian Assange and others , Η ελευθερία και το μέλλον του Διαδικτύου :Η ανάλυση του εκδότη των Wikileaks (Αθήνα Ποιότητα 2013).
[2] Παναγιώτης Κονδύλης Η Θεωρία του Πολέμου εκδόσεις Θεμέλιο 1999 σελ 345.
[3] Max Boot ,War made New :Weapons, warriors,and the Making of the Modern World ,Penguin Groop inc 2006 σελ 313-317.

Ο ηλεκτρονικός υπολογιστής ,η εξέλιξη της τεχνολογίας οδήγησαν στην περαιτέρω οργάνωση επικοινωνιακών δικτύων και δημιούργησαν εφαρμογές προκειμένου να υποστηρίξουν ανθρώπινες δραστηριότητες, οι οποίες για τη λειτουργία τους στηρίζονται σε δίκτυα υπολογιστών. Για την εξυπηρέτηση στρατιωτικών αναγκών δημιουργήθηκε το Διαδίκτυο την εποχή του ψυχρού πολέμου, την δεκαετία του 1960. Οι δυνατότητες του Διαδικτύου επεκτάθηκαν με την εισαγωγή του ηλεκτρονικού ταχυδρομείου και τη δυνατότητα μεταφοράς αρχείων.

Στην αρχή τα δίκτυα ήταν απομονωμένα, και προσέφεραν εγγενή προστασία από κακόβουλους χρήστες. Με σκοπό όλες αυτές οι υπηρεσίες να τεθούν στη διάθεση των πολιτών σε συνδυασμό με την συνεχή ανάπτυξη της πληροφορικής, δόθηκε η δυνατότητα της προσβασιμότητα τους από τον ευρύ πληθυσμό προκειμένου να διευκολυνθεί η συνεργασία μεταξύ των υπηρεσιών, και του πολίτη στην καθημερινότητα, ενώ παράλληλα η ταχύτητα με τη χρήση της νέας τεχνολογίας αυξήθηκε. Όλα αυτά οδήγησαν παράλληλα στην αύξηση της τρωτότητας τους.

Αρχές της δεκαετίας του 1980, επήλθε η χρήση του συστήματος ονοματολογίας DNS[4], με αποτέλεσμα μέχρι τα τέλη της δεκαετίας αυτής, να συγχωνευθούν 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. Η μαζική επικοινωνία επιτυγχάνεται διαμέσου του διαδικτύου[5]. Χρησιμοποιείται πλέον από μεγάλα και αναπτυγμένα κράτη για την παραγωγή και τον έλεγχο της ηλεκτρικής ενέργειας, για την υδροδότηση, τα δίκτυα μαζικής μεταφοράς και των έκτακτων αναγκών. Ουσιαστικά το διαδίκτυο αποτελεί τη δομή και τη βάση της καθημερινότητας των σύγχρονων κοινωνιών.

Η τρωτότητα των δικτύων άρχισε να φαίνεται από την εκδήλωση κυβερνοεπιθέσεων εναντίον διαφόρων χωρών, οργανισμών, εταιρειών, οι οποίες αποτέλεσαν το καινούριο είδος απειλής, το οποίο μέχρι το 2007 ήταν περιορισμένο σε συγκεκριμένο χώρο όπου δραστηριοποιούνταν χάκερ, μυστικές υπηρεσίες των χωρών καθώς σε δραστηριότητες που αφορούσε την κατασκοπεία στον βιομηχανικό τομέα. Εξαιτίας των περιπτώσεων αυτών διαπιστώθηκε, ότι υπόθεση μιας Κυβερνοεπίθεσης ή ακόμη και ενός Κυβερνοπολέμου[6] εναντίον μιας χώρας είναι πλέον πραγματικότητα. Οι συνέπειες την περίοδο εκείνη ήταν

[4] Domain Name System

[5] Υπηρεσίες Κοινωνικής δικτύωσης .Kelly Gable ,Cyber Apocalypse now Vanderbilt Journal of Transnational Law,Jan 2010 σελ 8

[6] Δημήτριος Καντερές Υποστράτηγος εα:"Κυβερνοπόλεμος –Ένα νέο είδος πολέμου για τον 210 αιώνα ¨Αμυντική Επιθεώρηση ,Ιανουάριος 2004 σελ44

σχετικά περιορισμένες και δεν υπήρξαν ανθρώπινες απώλειες ή φυσικές καταστροφές. Παρόλα αυτά, η διακοπή της λειτουργίας των κρατικών υπηρεσιών αλλά και των δραστηριοτήτων, που αφορούν τόσο σε δημόσια η ιδιωτική δραστηριότητα, για μεγάλο χρονικό διάστημα, είχε άμεσες αρνητικές επιπτώσεις στην καθημερινότητα χιλιάδων πολιτών και στην οικονομία.

Η δεδομένη βελτίωση των επικοινωνιών και της πληροφορικής θεωρείται ότι θα οδηγήσει σε αύξηση της τρωτότητας των δικτύων και *των* υποδομών μιας χώρας· η τρωτότητα αυτή, αν συνδυαστεί με τη βελτιωμένη έκδοση των Κυβερνοόπλων του μέλλοντος, θα καταστήσει τον Κυβερνοχώρο ένα νέο πεδίο ανταγωνισμού, και τον Κυβερνοπόλεμο μια πραγματική πρόκληση για την Κυβερνοασφάλεια των κρατών[7].

Ο Κυβερνοπόλεμος αντιστοιχεί σε νέα μορφή πολέμου, με ανόμοια χαρακτηριστικά, που έχει ως αποτέλεσμα, ότι αποτελεί πυλώνα της ισχύς του κράτους, ικανό, με τη συνδρομή των άλλων συντελεστών, να επιτυγχάνει, έστω και περιορισμένους πολιτικούς σκοπούς. Η σχέση του προς τις Ένοπλες Δυνάμεις (όπως και γενικότερα με τους άλλους συντελεστές ισχύος του κράτους), είναι σχέση υποστηρίζοντος – υποστηριζόμενου. Υπό το πρίσμα της στρατηγικής, ο Κυβερνοπόλεμος βρίσκεται στο επίπεδο της Υψηλής Στρατηγικής, όπου γίνεται η ενορχήστρωση των συντελεστών ισχύος του κράτους για την επίτευξη τεθέντων πολιτικών σκοπών[8].

Με δεδομένο ότι η τεχνολογία εξελίσσεται, είναι πολύπλοκη και αναγκαιεί η αλληλεπίδραση πολλών παραγόντων και συνισταμένων γίνεται εύκολα αντιληπτό, ότι η διαχείριση της ασφάλειας αποτελεί δύσκολο και πολύπλοκο καθήκον, αφού ο κάθε χρήστης επηρεάζεται από την διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα και το απόρρητο δεδομένων και υπηρεσιών.

Στην παρούσα διατριβή θα αναλυθεί και θα παρουσιασθεί ένα φαινόμενο που έχει ήδη εξελιχθεί σε μηχανισμό αποδιάρθρωσης ενός κυρίαρχου κράτους, αυτό του κυβερνοπολέμου ως πολλαπλασιαστή ισχύος, και σε σχέση με την ασφάλεια στο διαδίκτυο. Αποτελείται από πολλές παραμέτρους, γι' αυτό το λόγο έχει επιλεχθεί να γίνει ανάλυσή του σε εύρος, καλύπτοντας όσες το δυνατόν περισσότερες από αυτές και όχι σε βάθος, για κάποιες συγκεκριμένες.

[7] http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-stratigiki Κυβερνοπόλεμος και Εθνική Στρατηγική Π.Μαυρόπουλος

[8] Ο όρος Υψηλή Στρατηγική χρησιμοποιήθηκε για πρώτη φορά από τον Liddell Hart και έκτοτε υιοθετήθηκε από τους στρατηγιστές, οπαδούς και μη της θεωρίας του Hart. Βλέπε B. H. Liddell Hart, Strategy, Εκδόσεις Meridian, 1991, σελ. 322

Στο πρώτο κεφάλαιο αναλύεται η έννοια του κυβερνοχώρου και του κυβερνοπολέμου και τα βασικά τους χαρακτηριστικά. Στο δεύτερο κεφάλαιο επιχειρείται μια αναφορά σχετικά με τα βασικά στοιχεία του κυβερνοπολέμου, το περιβάλλον πληροφοριών καθώς και τις ευπάθειες των δικτύων ΗΥ και του διαδικτύου. Στο τρίτο κεφάλαιο γίνεται μια αναφορά στην ασφάλεια στο διαδίκτυο και αναλύεται η προσπάθεια για την αντιμετώπιση κυβερνοεπιθέσεων/εγκλήματος στον κυβερνοχώρο, καθώς και την αντιμετώπιση των κυβερνοεπιθέσεων από τα κράτη. Στο τέταρτο κεφάλαιο εξετάζεται η δυνατότητα κυβερνοπολέμου από τα γειτονικά κράτη καθώς και το πώς ο κυβερνοπόλεμος μπορεί να χρησιμοποιηθεί ως συντελεστής ισχύος για την Ελλάδα. Στη συνέχεια αναπτύσσονται τα συμπεράσματα για το φαινόμενο του κυβερνοπολέμου, που αποτελεί πλέον πραγματικότητα, προκειμένου να αντιμετωπιστεί ο κυβερνοπόλεμος αλλά και να χρησιμοποιηθεί για εξυπηρέτηση εθνικών σκοπών, ως πλεονέκτημα της Ελλάδας απέναντι σε άλλες «μεγαλύτερες» χώρες, και ειδικά απέναντι στην Τουρκία.

2. Σκοπός

Σκοπός της παρούσης διατριβής είναι, να διερευνηθούν οι απειλές κυβερνοπολέμου, αυτές δηλαδή, που έχουν να κάνουν με την προσβολή του πληροφοριακού συστήματος μιας χώρας, καθώς και η επισήμανση καθώς και ανάλυση των κινδύνων για την προστασία αυτής.

Τονίζεται επίσης η ιδιαιτερότητα και σπουδαιότητα του κυβερνοπολέμου ως «πολλαπλασιαστή ισχύος» μεταξύ αντιπάλων ή δυνητικά αντιπάλων δυνάμεων. Επίσης, διακρίνονται και επισημαίνονται οι ιδιαίτερες και χρήσιμες δυνατότητες που παρέχει στη χώρα μας η αξιοποίηση του διαδικτύου, η υπεροχή στον πόλεμο ως επακόλουθου αυτών των δυνατοτήτων και προτείνονται ενέργειες των κατάλληλων μέτρων για τη διεξαγωγή αμυντικών, αλλά και επιθετικών επιχειρήσεων κυβερνοπολέμου, σε όλο το φάσμα της εθνικής ισχύος.

3. Προϋποθέσεις

Η διατριβή προκειμένου να είναι σε θέση να καλύψει το θέμα του Κυβερνοπολέμου, που προσβάλει τα κρίσιμες υποδομές των χωρών μέσα από τον Κυβερνοχώρο, κάνει τις ακόλουθες παραδοχές :

α. Στόχος των κυβερνοεπιθέσεων και των επιχειρήσεων πληροφοριακού πολέμου θα συνεχίσουν να είναι οι δομές και τα συστήματα επικοινωνιών και πληροφορικής[9].

β. Τα δίκτυα, που αφορούν στις κρίσιμες και καίριες δομές[10] της κοινωνίας, παράλληλα στο δημόσιο αλλά και στον ιδιωτικό τομέα θα παρουσιάσουν συνέχεια και αύξηση.

γ. Το Διαδίκτυο (Internet) τόσο στην παρούσα μορφή, όσο και σε πιο εξελιγμένη στο μέλλον, θα συνεχίσει να είναι ο κύριος φορέας για τη δικτύωση εφαρμογών, στις κρίσιμες δομές (infrastructures) του δημοσίου, αλλά και του ιδιωτικού τομέα.

δ. Το Διαδίκτυο (Internet) θα ακολουθεί τη βασική σχεδίαση του πλέγματος με επιμέρους τοπικά δίκτυα, δίκτυα πανεπιστημίων, εθνικά και διεθνή καθώς και από ιστούς.

ε. Θα ενταθεί η κακόβουλη χρήση του διαδικτύου από εθνικούς και μη φορείς με νεότερους και πιο εξελιγμένους τρόπους και σε τέτοιους ρυθμούς, ώστε η προστασία των δικτυακών υπολογιστών να γίνεται πιο δύσκολη.

στ. Το μοντέλο client/server θα παραμείνει αναλλοίωτο και όλες οι υπηρεσίες του Internet θα βασίζονται σε αυτό. Δεν θα υπάρξει επίσης αλλαγή σε όλες εκείνες τις δομές, που είτε προσφέρουν πρόσβαση σε ταχύτατους υπερυπολογιστές, είτε ελέγχουν τη ροή και διακίνηση των δεδομένων των προγραμμάτων, των αρχείων και τέλος του ηλεκτρονικού – ταχυδρομείου, για προσωπική και ομαδική επαφή των μελών του Internet και άλλων μη - Internet δικτύων.

ζ. Το διεθνές νομικό πλαίσιο θα εξακολουθήσει να εφαρμόζεται με υστέρηση σε σχέση με την τεχνολογική εξέλιξη, ενώ τα επιμέρους εθνικά νομικά πλαίσια θα συνεχίσουν να έχουν σημαντικές διαφοροποιήσεις σε σχέση με το πόσο τεχνολογικά και οικονομικά είναι ανεπτυγμένα τα κράτη , που τα σχεδιάζουν και τα υλοποιούν.

η. Ο Κυβερνοπόλεμος θα συνεχίσει να υφίσταται επηρεάζοντας την εξέλιξη και τη διεξαγωγή των επιχειρήσεων.

θ. Η βελτίωση των εφαρμογών των πληροφοριακών συστημάτων, αφορά το παγκόσμιο επίπεδο και θα συνεχίσει να αποτελεί συνεχή διαδικασία.

---

[9] Κυβερνοπόλεμος και Εθνική Στρατηγική Π.Μαυρόπουλος
http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-stratigiki

[10] Κρίσιμες υποδομές είναι οι φυσικές και ηλεκτρονικές υποδομές που είναι απαραίτητες για τη διασφάλιση των βασικών λειτουργιών του κράτους.
http://www.warandstrategy.gr/images/Article-Images/ Κυβερνοπόλεμος και Εθνική Στρατηγική/Παναγιώτης Μαυρόπουλος Σελ .4

ι. Θα υπάρξει συνέχεια στις περιφερειακές συγκρούσεις τα επόμενα χρόνια σε μικρή και μεσαία κλίμακα χωρίς αλλαγή των αρχών του πολέμου στα πεδία των συγκρούσεων.

ια. Μειονεκτήματα και αδυναμίες θα συνεχίσουν να παρουσιάζουν όλα τα συστήματα ηλεκτρονικών και συλλογής πληροφοριών.

Οι επιπτώσεις των Κυβερνοεπιθέσεων εναντίον των κρατικών υποδομών διακρίνονται από ρεαλιστικότητα και έχουν προφανείς και μακροχρόνιες επιπτώσεις. Κύριος στόχος να τρομοκρατηθεί ο λαός και να εξαναγκαστεί να σταματήσει να υποστηρίζει τον πόλεμο[11] ή την πρόκληση ζημιών σε τέτοια έκταση ώστε να αναγκαστεί η κυβέρνηση να επανεκτιμήσει το ρίσκο που ανέλαβε με την προσφυγή στον πόλεμο. Επίσης μια διακοπή σε όλα τα στάδια παραγωγής και διανομής ηλεκτρικής ενέργειας για μεγάλο χρονικό διάστημα θα προκαλούσε σοβαρές επιπτώσεις στο σύστημα υγείας.

[11] Το ίδιο υποστήριξε και ο Giulio Duhet, Ιταλός θεωρητικός της αεροπορικής ισχύος, ότι θα κατάφερνε η αεροπορία με το βομβαρδισμό στόχων στα μετόπισθεν του εχθρού. Giulio Douhet, The command of the air, translated by Dino Ferrari, Air Force History and Museums Program, Washington, DC, 1998.

Σελίδα σκόπιμα κενή

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ
ΚΥΒΕΡΝΟΧΩΡΟΣ - ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

1.1 Ορισμός Έννοιας Κυβερνοχώρου

Η αξία της πληροφορίας αναγνωρίστηκε πριν από περίπου 2500 χρόνια, όταν ο Sun Tzu αναφέρθηκε σε αυτήν με την γνωστή ρήση : Αν γνωρίζεις τον εχθρό και τον εαυτό σου δεν χρειάζεται να ανησυχείς για την έκβαση εκατό μαχών[12]. Η αξία της πληροφορίας, αναγνωρισμένη για μεγάλο χρονικό διάστημα, οδήγησε σε μια ιδιαίτερη κατηγορία υπηρεσιών που είχαν ως σκοπό να συλλέξουν, αξιοποιήσουν, επεξεργαστούν και διανείμουν τις πληροφορίες.

Ο Κυβερνοχώρος[13] δημιουργήθηκε σταδιακά λόγω εξέλιξης της επιστήμης και της τεχνολογίας, και αποτελεί έναν ιστό διασυνδεδεμένων δικτύων, όπου αποθηκεύονται πάσης φύσεως πληροφορίες. Επίσης στον ιστό αυτό, ανάλογα με τις δυνατότητες των χωρών, συνδέονται και οι υποδομές τους με αποτέλεσμα , καθημερινά μέσω του ιστού, να διεξάγεται πολύ μεγάλο ποσοστό της καθημερινής δραστηριότητας του πλανήτη.

Ο όρος Κυβερνοχώρος όπως αυτός διατυπώθηκε από την Υπηρεσία Ερευνών των ΗΠΑ, είναι η δικτύωση των ανθρώπων μέσα από ένα δίκτυο υπολογιστών και τηλεπικοινωνιών, χωρίς να υπάρχουν γεωγραφικοί περιορισμοί[14]. Επιτεύχθηκε ουσιαστικά η εξάλειψη των εμποδίων που προκαλούσαν οι γεωγραφικοί παράγοντες καθώς και οι μεγάλες αποστάσεις που είχαν αρνητική επίδραση και η διαδραστικότητα που χαρακτηρίζει την δομή αυτών των δικτύων[15].

Παραδείγματα τέτοιων δικτύων διακρίνονται στα τοπικά δίκτυα, όπου είναι συνδεδεμένοι περισσότεροι από δύο ηλεκτρονικοί υπολογιστές και αποτελούν τα τοπικά δίκτυα (LANs) και μπορεί να βρίσκονται χωροταξικά μέσα στο ίδιο δωμάτιο, κτίριο, έτσι ώστε να μπορούν να επικοινωνούν μεταξύ τους και να υπάρχει ροή δεδομένων καθώς και στα 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.

---

[12] Sun Tzu,The Art of War ,Κεφάλαιο 3 Σελ 40,Εκδόσεις Επικοινωνίες .Αθήνα 2004
[13] Hayles Catherine "The seduction of Cyberspace" Minnesota University 1993 σελ 174
[14] Ariee Shaap Cyber Warfare Operations Air Force Law review 2009 σελ.121
[15] Jack Goldsmith and W.Tim Ποιος ελέγχει το Ιντερνετ 2007 Εκδόσεις Ποντίκι σελ 79-100.

Κυβερνοχώρος[16] θα μπορούσαμε να πούμε, ότι αποτελεί το χώρο εκείνο στον οποίο αποτυπώνεται η ανθρώπινη δραστηριότητα. Σύνολο ανθρώπινων πράξεων αποτυπωμένο σε μαγνητικό υλικό. Εκτός όμως από την καθημερινή δραστηριότητα μέρος του Κυβερνοχώρου αποτελεί η αποτύπωση των κατάλοιπων, που αφήνουν οι πράξεις ή οι παραλείψεις μας. Ο Κυβερνοχώρος διαθέτει τεράστια έκταση, ενώ μέχρι σήμερα δεν έχει γίνει προσπάθεια προκειμένου να μπορέσει κάποιος να την περιγράψει ή να χαράξει τα σύνορά της.

Κυβερνοχώρος[17] είναι ο χώρος που έχει δημιουργηθεί χάρη στην επιστήμη της Κυβερνητικής, στον οποίο το μόνο σταθερό σημείο αναφοράς, λόγω του χαώδους περιβάλλοντος, είναι ο άνθρωπος και οι δραστηριότητες του. Δηλαδή, το σύνολο των ανθρώπινων πράξεων στο χώρο αυτό, αποτυπωμένο σε μαγνητικό υλικό[18].

Δεν διαθέτει διαστάσεις, όρια και καθορισμένα σημεία προσανατολισμού. Η οργάνωση και η λειτουργία του Κυβερνοχώρου, όπως έχει σχεδιαστεί και αναπτυχθεί είναι χαοτική, ενώ με βάση την αρχή που ρυθμίζει τη λειτουργία του, επιτρέπεται η δραστηριοποίηση ατόμων, πολιτικών ομάδων και κρατών, οι ενέργειες των οποίων αποτελούν προϊόντα, τόσο μη νόμιμης υποκλοπής πληροφοριών, όσο και προσπάθειας να επιβάλουν την θέλησή τους, σε ανταγωνιστές ή αντιπάλους τους.

Όλες οι δραστηριότητες μας καταγράφονται καθημερινά με τη χρήση του Η/Υ μας. Έτσι τμήμα του Κυβερνοχώρου αποτελούν τα μηνύματα που ανταλλάσσουμε μέσω Η/Υ, ενώ το ίδιο συμβαίνει και με τις Web σελίδες ή τα άλλα αρχεία που τοποθετούμε στο Internet ή στο σκληρό μας δίσκο. Αυτά αποτελούν μια διεργασία κατά την οποία αποτυπώνουμε σε ηλεκτρονική μορφή και έχοντας συναίσθηση όλων των σκέψεων, ιδεών, πράξεων σε ηλεκτρονική μορφή, προκειμένου είτε να τα μεταφέρουμε, είτε να τα επεξεργαστούμε σε άλλη χρονική στιγμή εμείς οι ίδιοι (ημερολόγια, κείμενα ή πληροφορίες που καταγράφηκαν για μελλοντική επεξεργασία κλπ.) ή άλλοι (παραλήπτες μηνυμάτων, αναγνώστες αρχείων, χρήστες μιας βάσης δεδομένων κ.λπ.).

---

[16] Ο όρος κυβερνοχώρος αποδίδεται στο συγγραφέα επιστημονικής φαντασίας William Gibson και συγκεκριμένα πρωτοεμφανίστηκε στο έργο του Neuromancer (Νευρομάντης) το 1984:
"Μία ομόφωνη παραίσθηση που βιώνεται καθημερινά από δισεκατομμύρια νόμιμους χρήστες, σε κάθε χώρα, από παιδιά που μαθαίνουν μαθηματικές αρχές... Μία γραφική απεικόνιση δεδομένων απομονωμένων από κάθε υπολογιστή στο ανθρώπινο σύστημα. Αδιανόητη περιπλοκότητα. Γραμμές φωτός εκτείνονται στο μή-χώρο της διανόησης, ομάδες και αστερισμοί πληροφοριών. Όπως τα φώτα μιας πόλης υποχωρούν..."

[17] Hayles Catherine The seduction of Cyber space University of Minnesota press 1993 σελ 174.

[18] Η Ψηφιακή Στρατιωτική Κοινωνία ,Σύγγραμα ΣΣΕ Κεφ 5 σελ 1

Επίσης μετά από την καθημερινή εργασία στον ΗΥ είναι δυνατόν να δούμε τη δραστηριότητά μας στο διαδίκτυο, αφού η μνήμη του ΗΥ (cache) αλλά και του παρόχου μας περιέχει τις σελίδες, που αναζητήσαμε και επισκεφθήκαμε κατά τη διάρκεια της ενασχόλησης μας. Επομένως, γίνεται αντιληπτό ότι κάθε δραστηριότητά μας (τι μας απασχόλησε, πόσο χρόνο ασχοληθήκαμε με αυτά και οι ενέργειες, επιλογές άλλων σελίδων, αγορές κλπ.), είναι εύκολο να ελεγχθεί από άτομα, τα οποία διαθέτουν απλή γνώση λειτουργίας του ηλεκτρονικού υπολογιστή και μπορούν εύκολα να έχουν πρόσβαση σε αυτόν.

Όταν ένας υπολογιστής δεν είναι συνδεδεμένος σε κάποιο δίκτυο, τότε ο Κυβερνοχώρος (ορατός και αφανής) είναι ατομικός και μπορεί έτσι εύκολα να ελεγχθεί. Μπορούμε να ρυθμίσουμε τον υπολογιστή έτσι ώστε να περιορίζουμε την πρόσβαση στο περιεχόμενό του μόνο από εμάς, ενώ παράλληλα μας δίνεται η δυνατότητα, αν φυσικά το γνωρίζουμε, να τροποποιήσουμε ή και να διαγράψουμε ίχνη από τις ενέργειες (π.χ. διαγράφοντας αρχεία ή registry remarks με τρόπο, που να είναι αδύνατη η επαναφορά τους).

Η παραπάνω κατάσταση είναι μικρής αξία και μικρής έκτασης λόγω περιορισμών. Αυτό οδήγησε τους ανθρώπους να διασυνδεθούν με άλλους ανθρώπους μέσω του υπολογιστή δημιουργώντας το παγκόσμιο δίκτυο. Εντάσσονται σε μια ευρύτερη κοινότητα με αποτέλεσμα, να υπάρχει ένας αλληλοεπηρεασμός από πράξεις και παραλήψεις μεταξύ των μελών του δικτύου.

Γραπτοί και άγραφοι νόμοι για τη λειτουργία και τους κανόνες συμπεριφοράς στο διαδίκτυο και στον παγκόσμιο ιστό είναι λογικό να υπάρχουν και να εξελίσσονται παράλληλα με την εξέλιξη του κυβερνοχώρου. Επιπλέον εξελίσσονται οι μέθοδοι που θα χρησιμοποιηθούν για την εφαρμογή τους καθώς και οι ποινές που θα επιβάλλονται στους παραβάτες. Μέσα από την κατανόηση τεχνικών περιοδικών και του ημερήσιου τύπου ανακαλύπτονται λύσεις και ενημερώνονται οι ενδιαφερόμενοι. Το ίδιο το διαδίκτυο αποτελεί πηγή αναζήτησης πληροφοριών (ίσως τη σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες – θέσεις (Sites).

Ο Κυβερνοχώρος αποτελεί σύνολο μέσων, το οποίο ενσωματώνει το σύνολο των δραστηριοτήτων που αφορούν τις τηλεφωνικές συνδιαλέξεις, τα δεδομένα που μεταφέρονται, τη χρήση του ηλεκτρονικού ταχυδρομείου, τις οικονομικές συναλλαγές που πραγματοποιούνται με χρήση ηλεκτρονικών υπολογιστών, όλες εκείνες τις υπηρεσίες που παρέχουν πληροφορίες με τη χρήση του διαδικτύου, τις τηλεδιασκέψεις που λαμβάνουν χώρα

με τη χρήση του διαδικτύου καθώς και τα μέσα μαζικής ενημέρωσης, που στηρίζουν τη λειτουργία τους στο διαδίκτυο.

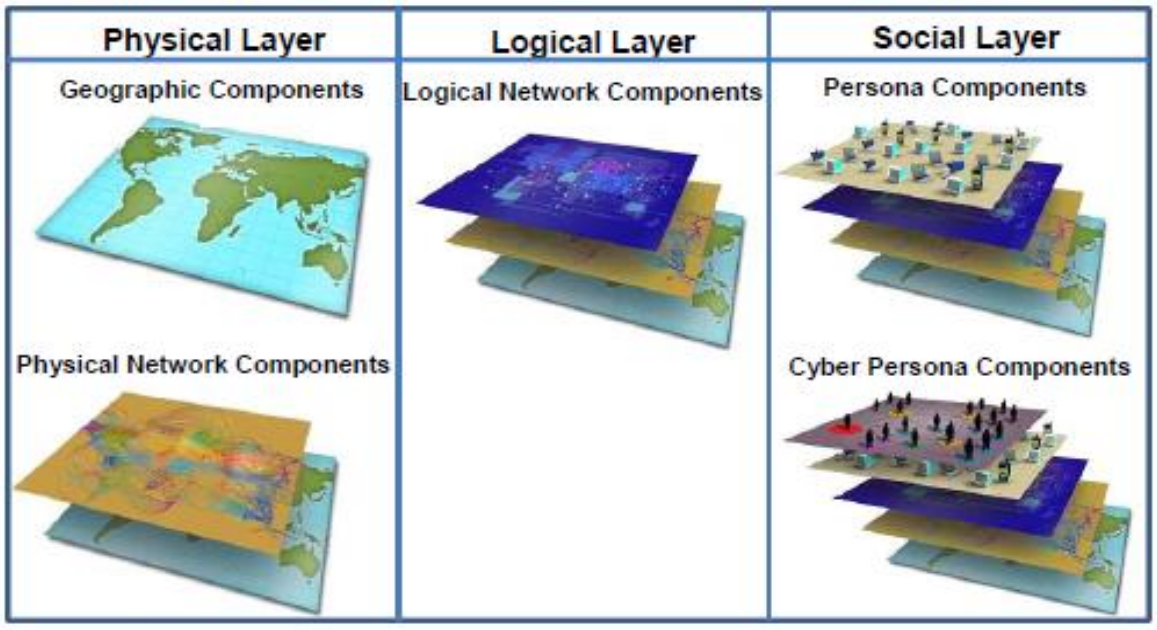
Ο κυβερνοχώρος[19], ενώ είναι ένας παγκόσμιος τομέας στο περιβάλλον πληροφόρησης, αποτελεί τμήμα μίας πεντάδας αλληλεξαρτώμενων περιοχών, ενώ οι άλλες είναι οι φυσικοί τομείς του αέρα, της γης, της ναυτιλίας και του διαστήματος. Καθώς οι αεροπορικές επιχειρήσεις βασίζονται σε αεροπορικές βάσεις στην ξηρά ή σε πλοία στη θάλασσα, οι επιχειρήσεις στον κυβερνοχώρο βασίζονται σε ένα αλληλεξαρτώμενο δίκτυο υποδομών πληροφορικής, συμπεριλαμβανομένου του Διαδικτύου, τηλεπικοινωνιακά δίκτυα, συστήματα υπολογιστών και ενσωματωμένους επεξεργαστές και ελεγκτές, καθώς και στο περιεχόμενο που διέρχεται μέσα από αυτά τα στοιχεία. Επίσης βασίζονται σε συνδέσμους και κόμβους που διαμένουν στους φυσικούς τομείς και εκτελούν λειτουργίες τόσο στον κυβερνοχώρο και τους φυσικούς τομείς. Για παράδειγμα, οι διακομιστές δικτύου μπορεί να βρίσκονται σε σταθμούς εδάφους ή στη θάλασσα επί των πολεμικών πλοίων, και οι ασύρματες μεταδόσεις δικτύου διέρχονται μέσω του αέρα και του διαστήματος καθώς και υποβρύχια. Ομοίως, οι δραστηριότητες στον κυβερνοχώρο μπορούν να επιτρέψουν την ελευθερία δράσης για δραστηριότητες σε φυσικούς τομείς. Οι δραστηριότητες στις φυσικές περιοχές μπορούν να δημιουργήσουν αποτελέσματα και μέσω του κυβερνοχώρου επηρεάζοντας το ηλεκτρομαγνητικό φάσμα (EMS[20]), ή τη φυσική υποδομή. Η σχέση μεταξύ του χώρου και του κυβερνοχώρου είναι μοναδική σε όλα σχεδόν οι λειτουργίες εξαρτώνται από τον κυβερνοχώρο και ένα κρίσιμο τμήμα του κυβερνοχώρου μπορεί να παρέχεται μέσω χωρικών λειτουργιών. Ο χώρος παρέχει μια βασική επιλογή παγκόσμιας συνδετικότητας για επιχειρήσεις κυβερνοχώρου.

Ο κυβερνοχώρος αποτελείται από πολλά διαφορετικά και συχνά επικαλυπτόμενα δίκτυα, καθώς και κόμβους (οποιαδήποτε συσκευή ή λογική τοποθεσία με διεύθυνση πρωτοκόλλου Internet [IP] ή άλλη διεύθυνση με ανάλογο αναγνωριστικό) σε αυτά τα δίκτυα και τα δεδομένα συστήματος (όπως πίνακες δρομολόγησης τα στηρίξουν). Παρόλο που δεν είναι όλοι οι κόμβοι και τα δίκτυα παγκοσμίως συνδεδεμένοι ή προσπελάσιμοι κυβερνοχώρος εξακολουθεί να συνδέεται όλο και περισσότερο. Τα δίκτυα μπορούν να είναι σκόπιμα απομονωμένα ή να έχουν διαιρεθεί σε θύλακες χρησιμοποιώντας στοιχεία ελέγχου πρόσβασης, κρυπτογράφηση, διαφορετικά πρωτόκολλα ή φυσικό διαχωρισμό. Με εξαίρεση

[19] Joint Publication 3-12 2013 Cyberspace Operations Σελ J2(US Joint Staff publication)
[20] EMS :Electromagnetic Spectrum

τον φυσικό διαχωρισμό, οι υπόλοιπες περιορίζουν την πρόσβαση. Η δυνατότητα για επιχειρήσεις στον κυβερνοχώρο μπορεί να επηρεαστεί από νομικές, πολιτικές παραμέτρους , ή επιχειρησιακούς περιορισμούς. Ωστόσο, η προσαρμογή σε περιορισμούς δεν επιτρέπει κατ 'ανάγκη την πρόσβαση σε έναν στόχο.

Ο κυβερνοχώρος μπορεί να περιγραφεί με όρους τριών επιπέδων[21]: φυσικό δίκτυο, λογικό δίκτυο και το cyber-persona. Καθένα από αυτά αντιπροσωπεύει ένα επίπεδο στο οποίο μπορεί να υπάρχει δυνατότητα για επιχειρήσεις στον κυβερνοχώρο. Το φυσικό στρώμα δικτύου του κυβερνοχώρου αποτελείται από το γεωγραφικό και τα συστατικά του φυσικού δικτύου. Είναι το μέσο στο οποίο μετακινούνται τα δεδομένα.



Σημείωση: Αναδημοσίευση του γραφήματος από το Joint Publication 3-12 2013 Cyberspace Operations (US Joint Staff publication)

Η γεωγραφική συνιστώσα είναι οι θέσεις σε ξηρά, αέρα, θάλασσα ή διάστημα όπου τα στοιχεία του δικτύου διαμένουν. Ενώ τα γεωπολιτικά όρια μπορούν εύκολα να διασχίζονται στον κυβερνοχώρο με ρυθμό πλησιάζοντας την ταχύτητα του φωτός, εξακολουθούν να υπάρχουν ζητήματα κυριαρχίας συνδεδεμένα με τους φυσικούς τομείς.

[21] Joint Publication 3-12 2013 Cyberspace Operations Σελ I 2(US Joint Staff publication)

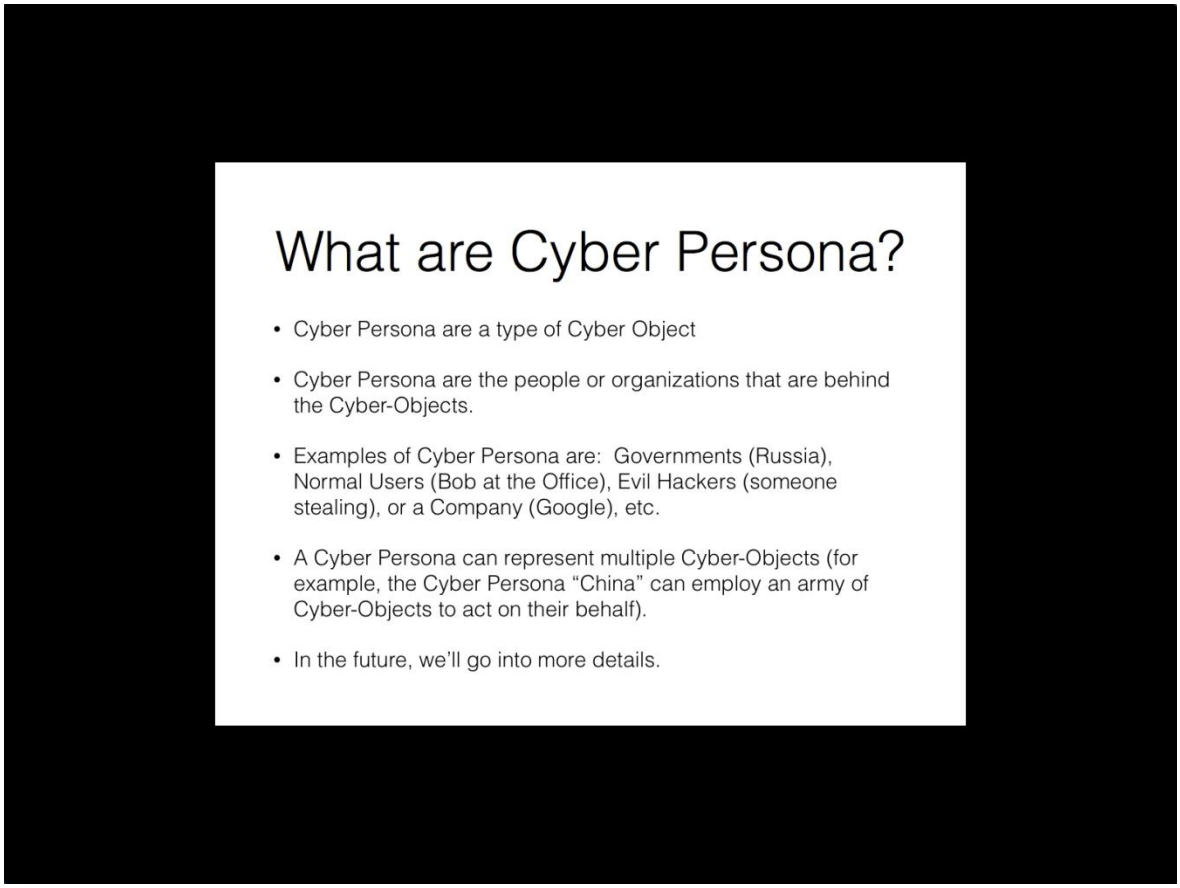
Το φυσικό δίκτυο αποτελείται από το υλικό, το λογισμικό συστημάτων και την υποδομή (ενσύρματη, ασύρματη, καλωδιακή σύνδεση, σύνδεσμοι EMS, δορυφόρο και οπτικό) που υποστηρίζει το δίκτυο καθώς και οι φυσικοί σύνδεσμοι (καλώδια, καλώδια, ραδιοσυχνότητα, δρομολογητές, διακόπτες, διακομιστές και υπολογιστές). Ωστόσο, το επίπεδο του φυσικού δικτύου χρησιμοποιεί λογικές δομές όπως μια πρωταρχική μέθοδο ασφάλειας (π.χ., διασφάλιση πληροφοριών και ακεραιότητας (π.χ., εικονικά ιδιωτικά δίκτυα που μετακινούνται μέσω του κυβερνοχώρου). Αυτός είναι ένας πρωταρχικός στόχος για την παρακολούθηση ηλεκτρονικών σημάτων (SIGINT)[22], συμπεριλαμβανομένης της εκμετάλλευσης δικτύου ηλεκτρονικών υπολογιστών, καταγραφής ηλεκτρονικών πληροφοριών, με ευφυΐα ανοιχτού κώδικα και ανθρώπινη νοημοσύνη. Είναι το πρώτο σημείο αναφοράς για τον καθορισμό της δικαιοδοσίας και της εφαρμογής των αρχών. Είναι επίσης η πρωταρχική δομή για γεωχωρική νοημοσύνη, η οποία μπορεί επίσης να συμβάλει στη χρήση χρήσιμων δεδομένων στόχευσης στον κυβερνοχώρο.

Στο λογικό επίπεδο δικτύου περιέχονται εκείνα τα στοιχεία του δικτύου που σχετίζονται μεταξύ τους κατά τρόπο που αφαιρείται από το φυσικό δίκτυο, δηλ. η μορφή ή οι σχέσεις δεν συνδέονται με ατομικό, συγκεκριμένο μονοπάτι ή κόμβο. Ένα απλό παράδειγμα είναι ένας ιστότοπος που φιλοξενείται σε διακομιστές σε πολλές φυσικές τοποθεσίες όπου μπορεί να υπάρχει όλο το περιεχόμενο πρόσβαση μέσω ενός μοναδικού εντοπιστή πόρων (URL). Για παράδειγμα, η ιστοσελίδα Defence Knowledge Online υπάρχει σε πολλούς διακομιστές σε πολλές τοποθεσίες στους φυσικούς τομείς, αλλά αντιπροσωπεύεται ως ενιαία διεύθυνση URL στον Παγκόσμιο Ιστό. Ένα πιο περίπλοκο παράδειγμα λογικό επίπεδο είναι το μη ασφαλές δίκτυο δρομολογητών πρωτοκόλλου Internet (NIPRNET)[23] του Department of Defence.

[22] Sigint: Signal Intelligence

[23] Το Δίκτυο Δρομολογητών Πρωτοκόλλου Διαδικτύου (IP (NIPRNet) είναι ένα ιδιωτικό δίκτυο IP που χρησιμοποιείται για την ανταλλαγή μη ταξινομημένων πληροφοριών μεταξύ των χρηστών του ιδιωτικού δικτύου, συμπεριλαμβανομένων των πληροφοριών που υπόκεινται στους ελέγχους διανομής Το NIPRNet παρέχει επίσης στους χρήστες του πρόσβαση στο Internet.Το NIPRNet αποτελείται από δρομολογητές πρωτοκόλλου Internet που ανήκουν στο Υπουργείο Άμυνας των Ηνωμένων Πολιτειών (DOD). Δημιουργήθηκε στη δεκαετία του 1980 και διοικείται από τον Οργανισμό Άμυνας Πληροφοριακών Συστημάτων (DISA) για να αντικαταστήσει την προηγούμενη MILNET. Τις τελευταίες δεκαετίες,το NIPRNet έχει αναπτυχθεί ταχύτερα από ό, τι μπορεί να παρακολουθήσει το Υπουργείο Άμυνας των ΗΠΑ. Το DoD δαπάνησε 10 εκατομμύρια δολάρια το 2010 για να καταγράψει τη σημερινή κατάσταση του NIPRNet, σε μια προσπάθεια να αναλύσει την επέκτασή του και να εντοπίσει μη εξουσιοδοτημένους χρήστες, για τους οποίους υπάρχουν υποψίες ότι έχουν μπεί αθόρυβα στο δίκτυο .Η έρευνα NIPRNet, η οποία χρησιμοποιεί λογισμικό IPSonar που αναπτύχθηκε από την Lumeta Corporation, εξέτασε επίσης την αδυναμία ασφάλειας που προκαλείται από τη διαμόρφωση του δικτύου.

Το στρώμα cyber-persona[24] αντιπροσωπεύει ακόμη υψηλότερο επίπεδο και χρησιμοποιεί τους κανόνες που ισχύουν στο λογικό δίκτυο στον κυβερνοχώρο, κανόνες που ισχύουν στο επίπεδο λογικού δικτύου για να αναπτύξει μια ψηφιακή αναπαράσταση μιας ταυτότητας ατόμου ή οντότητας στον κυβερνοχώρο. Η cyberpersonalayer αποτελείται από τους ανθρώπους που βρίσκονται στο δίκτυο.



Σημείωση: Αναδημοσίευση του γραφήματος από το Joint Publication 3-12 2013 Cyberspace Operations (US Joint Staff publication)

Ο όρος Cyber-persona μπορεί να αφορά σε ένα πραγματικό πρόσωπο ή οντότητα, ενσωματώνοντας κάποια βιογραφικά ή εταιρικά δεδομένα, e-mail και διευθύνσεις IP, ιστοσελίδες, αριθμούς τηλεφώνου κλπ. Ωστόσο, ένα άτομο μπορεί να έχει πολλαπλές προσωπικότητες του κυβερνοχώρου, οι οποίες μπορεί να διαφέρουν ανάλογα με το βαθμό στον οποίο είναι πραγματικά ακριβής. Ένα άτομο cyber-persona μπορεί να έχει πολλούς

[24] Joint Publication 3-12 2013 Cyberspace Operations σελ I 2 (US Joint Staff publication)

χρήστες. Κατά συνέπεια, η στόχευση στον κυβερνοχώρο είναι δύσκολη. Επειδή μπορεί να είναι άτομα του κυβερνοχώρου με πολύπλοκα στοιχεία σε πολλές εικονικές τοποθεσίες, και συνήθως δεν συνδέονται μόνο με τη φυσική τοποθεσία ή τη μορφή, απαιτούνται σημαντικές δυνατότητες συλλογής και ανάλυσης πληροφοριών ώστε να αποκτηθεί επαρκής γνώση και κατανόηση της κατάστασης ενός cyber-persona για την αποτελεσματική στόχευση και τη δημιουργία του επιθυμητού αποτελέσματος του.

Τα δίκτυα πληροφοριών του Υπουργείου Άμυνας (DODIN) είναι παγκοσμίως διασυνδεδεμένα, με δυνατότητες για την συλλογή, επεξεργασία, αποθήκευση, διάδοση και διαχείριση πληροφοριών κατόπιν αιτήματος σε όσους τις χρειάζονται είτε είναι, πολιτικοί είτε στρατιωτικοί είτε προσωπικό υποστήριξης επιχειρήσεων. Το DODIN περιλαμβάνει ιδιόκτητες και μισθωμένες επικοινωνίες καθώς και συστήματα υπολογιστών, λογισμικό (συμπεριλαμβανομένων εφαρμογών), δεδομένα, υπηρεσίες ασφαλείας, και συστήματα εθνικής ασφάλειας.

1.2 Ορισμός έννοιας Κυβερνοπόλεμου

Εάν θυμηθούμε την έννοια του Πολέμου όπως αποτυπώθηκε από τον Clausewitz[25] θα εστιάσουμε στην προσπάθεια της επιβολής της θέλησης του δράστη στον αντίπαλο του. Έτσι και για το είδος αυτό του πολέμου, η χαοτική κατάσταση του Κυβερνοχώρου επηρεάζει την οργάνωση και τη λειτουργία του επιτρέποντας την επιβολή της θέλησης της μιας πλευράς στους αντιπάλους της άλλης. Όμως εδώ δεν χρειάζεται η Στρατιωτική Ισχύς, όπως καθορίζονται στα συγγράμματα του Clausewitz για να επιβληθεί η θέληση του ενός στον άλλο, αλλά η πληροφοριακή υποδομή που διαθέτουν τα αντίπαλα μέρη.

Διαδίκτυο θεωρούμε χιλιάδες ή και εκατομμύρια υπολογιστών που είναι διασυνδεδεμένοι και αποτελούν κομμάτια επιμέρους δικτύων και μέσα από τα οποία γίνεται διακινούνται δεδομένα κάθε μορφής[26]. Το διαδίκτυο βασίζεται στη λειτουργία με χρήματα και εξοπλισμό των ιδιωτών, καθόσον δεν εντάσσεται σε κάποιο οργανωμένο σύνολο, χωρίς να διοικείται από κάποια μορφής διοίκηση. Εμφανίστηκε στα τέλη της δεκαετίας του ΄60 και πριν από αυτή τη μορφή διασύνδεσης υπήρχαν δίκτυα ηλεκτρονικών υπολογιστών που

[25] Carl Von Clausewitz On War University Of Princeton 1989 ,σελ 63-78.
[26] https://sites.google.com/site/eisagogestadiktyaypologiston1/diadiktyo-internet

εξυπηρετούσαν εμπορικές , πανεπιστημιακές, στρατιωτικές, κυβερνητικές λειτουργίες έχοντας όμως διακριτό χαρακτήρα[27].

Δηλαδή προσφέρεται ως ένας χώρος, με δυνατότητα διάπραξης «ηλεκτρονικών» εγκλημάτων και «κυβερνοεγκλημάτων», ενώ προσφέρεται η δυνατότητα μετεξέλιξης του «κυβερνοχώρου» για διενέργεια ανθρώπινης αντιπαράθεσης, όπου είναι εξαιρετικά δύσκολο να ασκηθεί έλεγχος και να τεθούν κανόνες.

Ξεκινώντας από τα βασικά, την έννοια του κυβερνοπολέμου-Cyberwarfare[28] θα μπορούσαμε να την ορίσουμε ως πόλεμο στον οποίο χρησιμοποιείται ο υπολογιστής και το διαδίκτυο (το λεγόμενο Hacking) για να επιτευχθεί σαμποτάζ ή κατασκοπεία. Σύμφωνα με το βιβλίο «Cyberwar»[29], ως κυβερνοπόλεμος έχει οριστεί η προσπάθεια, από ένα έθνος - κράτος να αποκτήσει πρόσβαση σε υπολογιστές ή δίκτυα άλλου έθνους, με σκοπό την πρόκληση ζημιάς ή αναστάτωσης.

Η διεθνής βιβλιογραφία διαθέτει πλήθος αδόκιμων όρων με τους οποίους γίνεται η περιγραφή, αναλύονται οι δυνατότητές του και η επίδρασή του στις επιχειρήσεις. Έτσι παρουσιάζεται ως «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.

Με τον όρο «Πληροφοριακό ή Πληροφορικό Πόλεμο[30]» δίνεται ιδιαίτερη βαρύτητα στην έννοια της πληροφορίας. Η σύνδεση του πολέμου με την πληροφορία ήταν διαρκής, ωστόσο μέσα από τον έλεγχο και την αξιοποίηση κάθε καίριας πληροφορίας επιτυγχάνεται η ακρίβεια, η συντομία και με ελάχιστες δαπάνες αποτελεσματική επιχείρηση.

Κύρια χαρακτηριστικά εγκληματικών ενεργειών στον κυβερνοχώρο είναι η απουσία ταυτότητας, το μικρό κόστος και η ταχύτητα, στοιχεία που διακρίνονται για το πολύ χαμηλό ρίσκο σε όποια προσπάθεια. Η συντονισμένη ενέργεια, που προσπαθεί να πλήξει την ισχύ ενός κράτους χρησιμοποιώντας τον κυβερνοχώρο, καλείται απειλή κυβερνοπολέμου.

[27] Jeffrey Kelsey Hacking into international Humanitarian Law: The principles of distinction and neutrality in the age of Cyber Warfare Michigan Law Review 2008.
[28] https://en.wikipedia.org/wiki/Cyberwarfare
[29] Richard A. Clarke, former National Coordinator for Security, Cyber war (2010) σελ12
[30] Κώστας Γρίβας Ο Πόλεμος στον 21^{ο} Αιώνα Εκδόσεις Επικοινωνίες Αθήνα 1999 σελ 28

Οι κύριες διαφορές του κυβερνοπολέμου από τον κλασσικό πόλεμο εστιάζεται στο γεγονός, ότι δεν υφίσταται χρονικούς και χωρικούς περιορισμούς, δηλαδή, δεν έχει αρχή και τέλος, και δε καταλαμβάνει συγκεκριμένη εδαφική έκταση. Η εμφάνιση του κυβερνοχώρου, στον οποίο μάλλον κινείται, αποκάλυψε τον κυβερνοπόλεμο σαν να είναι η σκιά του.

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, το αποτέλεσμα δεν κρίνεται από το πλήθος των δυνάμεων την 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 «Η γνώση πρέπει να εξελιχθεί σε δυνατότητα[31]» (Knowledge must become capability), έχει εφαρμογή όσο ποτέ άλλοτε.

Κυβερνοπόλεμος είναι η αμυντική ή και επιθετική χρήση πληροφοριών και πληροφορικών συστημάτων από κάθε αντίπαλο, με σκοπό την πρόσβαση, εκμετάλλευση ή καταστροφή της αντιπάλου πληροφορίας ή ενός αντιπάλου πληροφορικού συστήματος και ταυτόχρονα η προστασία των ημετέρων αντιστοίχων[32]. 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.

Εξετάζοντας τις περιπτώσεις κυβερνοπολέμου, διαπιστώνουμε ότι συνήθως αυτές οργανώνονται και υλοποιούνται από κράτη, τα οποία με ελάχιστο κόστος έχουν τη δύναμη να προσβάλλουν ηγετικά κράτη και να ασκήσουν από την πλευρά τους πίεση και πολιτική, όπως για παράδειγμα η Κίνα και η Ρωσία εναντίον των ΗΠΑ, η Ινδία εναντίον του Πακιστάν κ.α.

Έτσι ο κυβερνοπόλεμος[33] αποτελεί σειρά δικτυακών συγκρούσεων με σκοπό την εξουθένωση του αντιπάλου, χωρίς επιπτώσεις σε ανθρώπινα θύματα, που θα επέφερε ο

[31] Carl von Clausewitz Μεγάλος θεωρητικός της Στρατηγικής.
[31] Κώστας Γρίβας Ο Πόλεμος στον 21ο Αιώνα Εκδόσεις Επικοινωνίες Αθήνα 1999 σελ 28
[32]http://greeknation.blogspot.gr/2014/10/blog-post_455.html
[33] https://powerpolitics.eu/cyber warfare ο πόλεμος που δεν βλέπεις

κανονικός πόλεμος. Η διεξαγωγή του έχει μάλιστα κλιμακούμενη ένταση, σκληρή (hard - cyberwarfare), και ήπια (soft - cyberwarfare).

Εκτιμήσεις από το Αμερικανικό Πεντάγωνο, αναφέρουν την δυνατότητα που έχει 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»

Για τις Ηνωμένες Πολιτείες η προστασία της πληροφορικής υποδομής τους από κυβερνοεπιθέσεις έχει μεγάλη σημασία . Χαρακτηριστικό είναι μάλιστα ότι, ενώ αρχικά αναφέρονταν στον όρο «ηλεκτρονικό Περλ Χάρμπορ[34]» 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».

Χαρακτηριστικά μιας κυβερνοεπίθεσης είναι ότι, δεν έχει ως αποτέλεσμα άμεσα θύματα, διατηρεί την απόκρυψη της, διότι δεν εντοπίζεται εύκολα. Δεν είναι δυνατή η αναγνωρισιμότητα της εθνικότητας των διαφόρων όπλων της, όπως των ιών των υπολογιστών, ούτε διαθέτει κωδικούς αριθμούς αναγνώρισης. Ο κυβερνοπόλεμος είναι, λοιπόν, ιδανικός για τη «φιλική επίλυση διαφορών».

Ο κυβερνοχώρος αποτελεί το πρόσφορο έδαφος, για να τελεστούν ενέργειες και πράξεις, οι οποίες θα επιφέρουν ζημιές και καταστροφές, τόσο σε απλούς πολίτες όσο και σε κυβερνητικές δραστηριότητες, σε τοπικό και διεθνή χώρο. Αυτό συμβαίνει, διότι ο χώρος του διαδικτύου είναι ανοιχτός σε όλους με αποτέλεσμα η εγκληματική ή τρομοκρατική δραστηριότητα να μεταφέρεται με επιτυχία, θα μπορούσαμε να πούμε, και ανωνυμία και στο χώρο του διαδικτύου. Επειδή αποτελεί σύνολο μικρότερων δικτύων αποτελεί ιδιαίτερη πρόκληση για τη στοχοποίηση του[35].

Δηλαδή, είναι ένα είδος πολέμου που ξεχωρίζει για την ευρύτητά του, το νεωτερισμό του, την τεχνολογική του υπεροχή. Ο Κυβερνοπόλεμος είναι η χρήση των πληροφοριακών

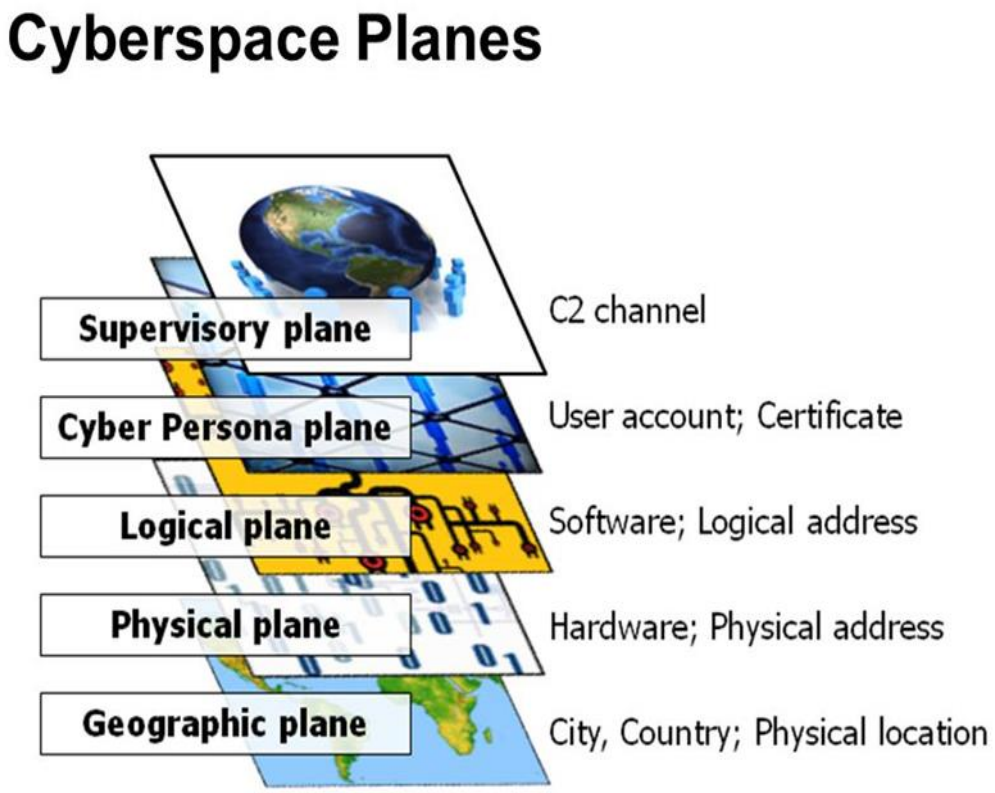
[34] Ο Richard Bejtlich, διευθύνων σύμβουλος ασφαλείας της Mandiant εταιρείας που παρέχει λύσεις ασφάλειας, μιλώντας σε συνέδριο της Αμερικανικής Πολεμικής Αεροπορίας είπε ότι το 100% από τις εισβολές που έχει κληθεί να αντιμετωπίσει αφορούν σε επιθέσεις πολύ σύνθετες και επαγγελματικές. Όσοι τις έκαναν ήταν σε θέση να πάρουν ότι στοιχεία ήθελαν από τις υπηρεσίες που είχαν στοχοποιήσει.
[35] Ahmad Kamal UN report Law of Cyber Space 2005 σελ 77

συστημάτων για να πλήξουμε την εικονική προσωπικότητα ενός ατόμου ή ομάδας ατόμων. Είναι η επίθεση που εκτελείται εναντίον συστημάτων υπολογιστών μέσω hacking. Οι επιθέσεις των hackers διαφέρουν βέβαια σημαντικά. Υπάρχουν hackers που το κάνουν απλά για διασκέδαση, επιδεικνύοντας την ικανότητά τους, αλλά υπάρχουν και hackers που φτάνουν στα άκρα προκαλώντας πλήρη παράλυση σε συστήματα υπολογιστών. Το hacking δυνητικά μπορεί να γονατίσει τον κρατικό μηχανισμό μιας χώρας. Συνεπώς, αυτή η μορφή πολέμου εγείρει τεράστιο ζήτημα εθνικού ενδιαφέροντος, αλλά και ανησυχίας και γι' αυτό το λόγο, αρκετά κράτη ενσωματώνουν στο στρατιωτικό τους δόγμα τον κυβερνοπόλεμο.

Θέλοντας να αναλύσουμε τον όρο «Πόλεμος Δικτύων» (Net war)[36], θα λέγαμε ότι είναι μια χαμηλής έντασης αναμέτρηση, που εκτελείται από μη ομάδες (τρομοκράτες, ακτιβιστές, μυστικές υπηρεσίες, αντάρτες και άτομα που ενεργούν αυτόνομα), οι οποίες δεν είναι κατά ανάγκη στρατιωτικές, προσβάλλοντας στόχους στρατιωτικούς, όπως δίκτυα παροχής ενέργειας, Οργανισμούς κοινής ωφέλειας, τραπεζικά δίκτυα, δίκτυα ενημέρωσης τα οποία επηρεάζουν τη ζωή και τη λειτουργία του κράτους.

Το επιχειρησιακό περιβάλλον είναι σύνθετο ανάλογα με τις συνθήκες, τις περιστάσεις και τις επιρροές που επηρεάζουν την απασχόληση των ικανοτήτων και τις επιπτώσεις από τις αποφάσεις που θα ληφθούν. Η συνεχιζόμενη πρόοδος των επικοινωνιών και η εξελισσόμενη τεχνολογία των υπολογιστών που συνεπάγεται σε μείωση σημαντικά του κόστος απόκτησης περιπλέκει σημαντικά την διενέργεια επιχειρήσεων. Οι συντελεστές που επηρεάζουν τις επιχειρήσεις ποικίλλουν ανάλογα με την αποστολή. Ο πρώτος παράγοντας είναι η πλήρης κατανόηση του κυβερνοχώρου και η σχέση με τους φυσικούς τομείς. Η τεχνολογία των πληροφοριών και των επικοινωνιών εξελίσσεται ταχέως, αναγκάζοντας τις κυβερνήσεις και τους στρατιωτικούς να επανεξετάσουν το πλαίσιο εντός του οποίου λειτουργούν. Η ταχύτητα στη ροή των ειδήσεων στα blogs, η κοινωνική δικτύωση και ανταλλαγή μηνυμάτων, η ταχεία ροή πληροφοριών έχει αλλάξει τον κοινωνικό ιστό του κόσμου. Η ικανότητα των κοινωνικών δικτύων στον κυβερνοχώρο και η παρότρυνση της λαϊκής υποστήριξης καθώς και η εξάπλωση της ιδεολογίας δεν είναι γεωγραφικά περιορισμένη, το οποίο έχει σημαντικές επιπτώσεις στην εθνική ασφάλεια.

[36] Αφορά συγκρούσεις που σχετίζονται με πληροφορίες σε μεγάλο επίπεδο μεταξύ εθνών ή κοινωνιών. Αυτό σημαίνει προσπάθεια διατάραξης ή καταστροφής αυτού που ο πληθυσμός-στόχος γνωρίζει ή πιστεύει ότι ξέρει για τον εαυτό του και τον κόσμο γύρω του. Μπορεί να περιλαμβάνει διπλωματία, προπαγάνδα και ψυχολογικές εκστρατείες, πολιτική ή πολιτισμική ανατροπή, εξαπάτηση ή παρεμβολή στα τοπικά μέσα ενημέρωσης, διείσδυση δικτύων υπολογιστών και βάσεων δεδομένων και προσπάθειες προώθησης αντιφρονούντων ή αντιπολιτευτικών κινημάτων σε δίκτυα υπολογιστών.



Σημείωση: Αναδημοσίευση του γραφήματος από το Key Terrain in Cyberspace: Seeking the High Ground in 6th Annual NATO Conference on Cyber conflict,Tallin,Estonia,2014.

Η τεχνολογία των πληροφοριών και των επικοινωνιών και άλλες προηγμένες τεχνολογίες χρησιμοποιούνται από ένα ευρύ φάσμα κρατικών και μη κρατικών φορέων και αντιπροσωπεύουν έναν φθηνό τρόπο να αποτελέσουν σημαντική απειλή για τις χώρες. Η εφαρμογή του χαμηλού κόστους του κυβερνοχώρου και οι ικανότητες αυτού μπορεί να έχει δυσανάλογες επιπτώσεις σε ένα έθνος που εξαρτάται από την τεχνολογία ή οργάνωση. Αυτό δίνει τη δυνατότητα σε αντιπάλους που δεν μπορούν να χρησιμοποιήσουν παραδοσιακές στρατιωτικές δυνάμεις να επιτύχουν τον σκοπό τους με ασύμμετρες εναλλακτικές λύσεις.

Επιπρόσθετα, οι εξελιγμένες δυνατότητες του κυβερνοχώρου για το οργανωμένο έγκλημα ή άλλων μη κρατικών οργανώσεων μπορούν να χρησιμοποιηθούν και να παρέχουν κακόβουλο λογισμικό ως υπηρεσία.

1.3 Είδη Κυβερνοπολέμου

Ο κυβερνοπόλεμος διακρίνεται όπως και ο κλασσικός πόλεμος σε δύο μορφές των οποίων τα κύρια χαρακτηριστικά αναλύονται όπως παρακάτω:

1.3.1 Επιθετικές Επιχειρήσεις Κυβερνοπολέμου. Επιδιώκεται η καταστροφή του αντίπαλου πληροφοριακού συστήματος, και η εκμηδένιση της θέλησης του για την διενέργεια οποιασδήποτε μορφής κυβερνοπόλεμου, εναντίον των φίλιων δυνάμεων ή συστημάτων.

Αν και το ψηφιακό πεδίο μάχης διαφοροποιεί εν μέρει την μέχρι σήμερα άποψη για την έννοια του πολέμου, εντούτοις οι διοικητές και το προσωπικό συνεχίζουν να παίρνουν αποφάσεις στηριζόμενοι σε ατελείς πληροφορίες. Η αδυναμία επιφέρει την απαίτηση για υψηλής ετοιμότητας τμήματα διαμέσου συνεχούς εκπαίδευσης.

Η επίθεση[37] διακρίνεται σε δύο στάδια :

(1) Στοχοποίηση με κύριο αντικείμενο αναζήτηση και εντοπισμό στόχων, που δύναται να είναι εχθρικοί, τον προσδιορισμό τους (φίλια κυριαρχία στις πληροφορίες) και στην ανάλυση τους (δημιουργία φίλιου σχεδίου επιχειρήσεων).

(2) Την προσβολή των στόχων, με παραποίηση και διαγραφή δεδομένων, και κυριαρχία επί του αντιπάλου στο πληροφοριακό σύστημα.

Έτσι από την περίοδο της ειρήνης πραγματοποιείται η συλλογή πληροφοριών που θα χρησιμοποιηθούν για την επίτευξη των παραπάνω, η ανάπτυξη μεθοδολογιών βελτίωσης του κύκλου απόφασης/δράσης καθώς και η διατάραξη του ανάλογου κύκλου του αντιπάλου.

1.3.2 Αμυντικές επιχειρήσεις Κυβερνοπολέμου. Κύριος στόχος και σκοπός των αμυντικών επιχειρήσεων η προστασία των φίλιων πληροφοριακών συστημάτων με μέτρα που λαμβάνονται για την προστασία του υλικού, λογισμικού και των πληροφοριών, από εχθρική προσέγγιση και αναρμόδια άτομα που ενδεχομένως θα επιφέρει επισφαλείς επεμβάσεις στο υλικό και λογισμικό ή και απώλεια των πληροφοριών καθώς επίσης προσβολή του φίλιου πληροφοριακού συστήματος με ιούς.

Οι ιοί κρύβονται σε προγράμματα υπολογιστών (και συχνά στη μνήμη (RAM)). Έχουν την ιδιότητα να προσκολλώνται σε άλλα προγράμματα και τα συνοδεύουν, όταν αυτά αντιγράφονται σε άλλους δίσκους ή στο δίκτυο. Με την κατάλληλη ενεργοποίηση τους διαταράσσονται τα προγράμματα, στα οποία έχουν προσκολληθεί. Εάν προσβάλλει τη μνήμη

[37] Κάθε ενέργεια που λαμβάνει χώρα στον κυβερνοχώρο και στοχεύει κατά της ισχύος μιας χώρας ή κατά ενός μη κρατικού δρώντα (πρόσωπα, οργανισμούς, εταιρίες, κτλ) ονομάζεται κυβερνοπόλεμος (cyberwarfare). http://www.xronos.gr/arthra/kyvernopolemos-yparkti-pagkosmia-asymmetri-apeili

(RAM), τότε δύνανται οι ιοί να επηρεάσουν περισσότερα προγράμματα, καθώς εκτελούνται το ένα μετά το άλλο. Μπορούν να ομαδοποιηθούν στις παρακάτω κατηγορίες :

(1) Αυτοί οι οποίοι δεν επηρεάζουν τη μνήμη (NON TSR FILE VIRUS).

(2) Εκείνοι οι οποίοι προσβάλουν το λειτουργικό, που ενεργοποιείται κατά την εκκίνηση.

(3) Εκείνοι οι οποίοι ενεργούν σε όλα τα μέτωπα (MULTI-PARTED VIRUS).

(4) Ιοί συνοδοί (COMPANION VIRUS).

(5) Ιοί πολυμορφικοί (POLYMORPHIC VIRUS).

(6) Ιοί μη εμφανείς (STEALTH VIRUS).

(7) Ιοί Δούρειοι ίπποι (TROJAN HORSE).

(8) Ιοί εγγράφων κειμένου (MACRO VIRUS) .

Για την ανίχνευση και εντοπισμό των παραπάνω ιών χρησιμοποιούνται διάφορα προγράμματα ανίχνευσης (Virus Scanners) με διαφορετικούς τρόπους λειτουργίας (Checksum Scanner, Heuristic Scanner, ενσωμάτωση ως Firmaware στη Rom του συστήματος). Η προστασία αυτή μπορεί να επιτευχθεί με κατάλληλο λογισμικό, που θα πρέπει να εξασφαλίζει :

(1) Απαγόρευση της πρόσβασης

(2) Εντοπισμό των τυχών παραβιάσεων

(3) Απομόνωση συστήματος

(4) Απόκρυψη – Παραπλάνηση

Σημείωση: Αναδημοσίευση του γραφήματος από το https://www.theengineer.co.uk/issues/1-november-2010/defending-against-the-cyber-threat/

1.4 Χαρακτηριστικά του Κυβερνοπολέμου

Τα ιδιαίτερα χαρακτηριστικά αυτής της ιδιότυπης μορφής συρράξεως είναι :

α. «Διακριτικότητα», με την οποία δίνεται η δυνατότητα, να χρησιμοποιηθεί σε περιπτώσεις που η συμβατική στρατιωτική ισχύς είναι άχρηστη.

β. Ο κυβερνοπόλεμος δεν έχει περιορισμούς στο χώρο[38]. Διαθέτει προβολή ισχύος ανεξάρτητη από τη γεωγραφία. Με την εφαρμογή της πληροφορικής μέχρι τώρα, η στρατιωτική ισχύς και η γεωγραφία είχαν μια στενή αλληλεπιδραστική σχέση. Στόχοι όπως, χρηματιστήρια ή δομές τηλεπικοινωνιών μιας χώρας, μπορούν να προσβληθούν από οποιοδήποτε σημείο του πλανήτη.

γ. Η προβολή ισχύος με τα κυβερνοόπλα δεν απαιτεί υποδομές .

[38] Parks Raymond C & Dugan David P 'Principles of Cyber Warfare' 2001 Proceedings of the 2001 IEEE,Workshop of Information Assurance and Security ,US Military Academy,West Point, NY 5-6/01

δ. Ο κυβερνοπόλεμος είναι μια μορφή επιχειρήσεων, που μπορούμε να πούμε ότι είναι 24/7/365, δηλαδή δεν εξαρτάται από χρονικούς περιορισμούς, από καιρικές συνθήκες και από το εάν υπάρχει ειρήνη ή πόλεμος.

ε. Ο κυβερνοπόλεμος είναι ένας πραγματικός, αλλά αφανής και διακριτικός πόλεμος, ο οποίος ωστόσο θέτει νέα ζητήματα ηθικής και νομιμότητας και απειλεί ακόμη περισσότερο να ταυτίσει την ειρήνη με τον πόλεμο, ενισχύοντας την γκρίζα ζώνη μεταξύ αυτών των δύο, ιδιαίτερα μετά την «ασύμμετρη επίθεση» της 11ης Σεπτεμβρίου και της κήρυξης του πολύχρονου «Πολέμου ενάντια στην Τρομοκρατία», ο οποίος σήμερα βρίσκεται υπό εξέλιξη.

στ. Οι αντίπαλοι δύναται να είναι νεαρής ηλικίας άτομα ή πολύπλοκα συμφέροντα που διεισδύουν στα συστήματα πληροφοριών για μια σειρά παράνομων δραστηριοτήτων.

ζ. Δεν υπάρχει καθορισμένο πεδίο μάχης με όρια και γραμμές ή «πρώτη γραμμή». Οι στρατηγικοί στόχοι μπορεί να είναι το ίδιο τρωτοί σε επίθεση ανεξαρτήτως χώρου, όπως στο θέατρο πολέμου, στην κρατική διοίκηση και στις επικοινωνίες.

Ο Κυβερνοπόλεμος, αν και ανεξάρτητο είδος πολέμου, είναι δυνατόν να θεωρηθεί μέρος του πολέμου διοικήσεως και ελέγχου με την ευρεία έννοια του όρου. Λαμβάνοντας υπ' όψη ότι, στόχος του είναι να επηρεάσει την αντίληψη και εικόνα του αντιπάλου - εχθρού για την υφιστάμενη κατάσταση, προκειμένου να τον οδηγήσει σε εσφαλμένες αποφάσεις, προσπαθεί άμεσα ή έμμεσα :

α. Να προσβάλει τα μέσα εκείνα από τα οποία (δορυφορικά συστήματα, ραντάρ κλπ.) παίρνει τις πληροφορίες, καθώς και τα αποθηκευτικά μέσα.

β. Να προσπαθήσει να παραπλανήσει τον εχθρό σχετικά με την θέση και τις δυνατότητες των μονάδων του. Λόγω του γεγονότος, ότι τα συστήματα επικοινωνιών και πληροφορικής είναι στόχοι κατά τις επιχειρήσεις κυβερνοπολέμου, για τον λόγο αυτό τηρούνται «κλειστά» και απομονωμένα από τα υπόλοιπα δίκτυα, ώστε να μπορούν λειτουργούν και να επιβιώνουν.

Άρα, ο κυβερνοπόλεμος αποτελεί μια δυνατότητα, η οποία προσβάλει το πεδίο των πληροφοριακών επιχειρήσεων, προβάλλοντας τις δυνατότητες του και μπορεί να αποτελέσει ρόλο «πολλαπλασιαστή ισχύος», σε μελλοντικές διενέξεις - συρράξεις.

1.5 Είδη Κυβερνοεπιθέσεων

Με βάση το είδος της απειλής οι κυβερνοεπιθέσεις, διακρίνονται :

α. Κατασκοπεία - εθνικές παραβιάσεις ασφάλειας :

Απόκτηση πληροφοριών από εχθρικές δυνάμεις, κυβερνήσεις, ανταγωνίστριες εταιρείες κοκ.

β. Δολιοφθορά :

Χρήση ΗΥ και δορυφόρων για στρατιωτικές επιθέσεις, προκειμένου να επιφέρουν ζημιά σε εξοπλισμό. Έτσι μια τέτοια ενέργεια μπορεί να επιφέρει προβλήματα στην ανταλλαγή emails, στη λειτουργία των συστημάτων εναέριας κυκλοφορίας, στον έλεγχο κυκλοφορίας των τραίνων, να επηρεάσει τη λειτουργία των ηλεκτρικών δικτύων, να επηρεάσει τη λειτουργία του χρηματοπιστωτικού συστήματος, να προσβάλει τα συστήματα ασφαλείας και λειτουργίας πυρηνικών αντιδραστήρων ή τη λειτουργία των φραγμάτων.

γ. Κλοπή Ηλεκτρικής Ενέργειας :

Στις ΗΠΑ επικρατεί η επίσημη άποψη ότι, η μεταφορά ηλεκτρικού ρεύματος ενδέχεται να αποτελεί κυβερνοπόλεμο[39].

Αντίστοιχα κατά τη διάρκεια κρίσεως ή πολέμου, ο κυβερνοπόλεμος αποτελεί ενέργεια, που σκοπό έχει, να υποστηρίξει τις φίλιες ενέργειες αποτρέποντας 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 :

α. Υποκλοπή πληροφοριών.

β. Παραπλάνηση του εχθρού.

γ. Άρνηση παροχής υπηρεσιών (Denial of Service-DOS[40]) σε ζωτικά συστήματα, ώστε να μην δύναται να τα χρησιμοποιήσει κατά την περίοδο των επιχειρήσεων, ή ακόμη και σε περίοδο ειρήνης.

[39] https://www.newsbeast.gr/weekend/arthro/2696832/weekend-sfakianakis-i-polemi-pleon-tha-ginonte-mesa-apo-to-diadiktio

δ. Αλλοίωση αποτελεσμάτων εκλογικών αναμετρήσεων, δημοσκοπήσεων διαρροής στοιχείων πολιτικών κομμάτων, κοκ.[41]

ε. Αλλοίωση ιστοσελίδων κρατικού, στρατιωτικού ή κοινωνικού ενδιαφέροντος με επέμβαση στο περιεχόμενο των ιστοσελίδων με απώτερο σκοπό τη δημιουργία εντυπώσεων και όχι μόνο[42].

στ. Εισαγωγή ψευδών δεδομένων στον κυβερνοχώρο δημοφιλών ηλεκτρονικών δικτύων, προκειμένου να επηρεάσουν κοινωνικές ομάδες και απόψεις.

ζ. Πρόκληση διαταραχών στις Ένοπλες Δυνάμεις, με παρέμβαση στα δίκτυα επικοινωνιών, προκειμένου να επιτευχθεί αποκλεισμός και να τεθεί σε κίνδυνο το προσωπικό[43].

1.6 Παραδείγματα Επιθέσεων στο Διαδίκτυο

Χαρακτηριστικά παραδείγματα αλλά και σχετικά πρόσφατα περιστατικά κυβερνοπολέμου αναφέρονται παρακάτω :

α. Στις 2 Ιουνίου 1996, η εφημερίδα TIMES του Λονδίνου, έγραφε ότι τράπεζες του Τόκιο, της Νέας Υόρκης και του Λονδίνου, πλήρωσαν 500 εκατομμύρια δολάρια σε «κυβερνο-τρομοκράτες», που είχαν αποδείξει ότι μπορούν να παγώσουν τη λειτουργία των ηλεκτρονικών υπολογιστών των τραπεζών αυτών. Σε διάστημα τριών ετών είχαν επιχειρήσει περισσότερες από 40 επιθέσεις στον τραπεζικό κυβερνοχώρο.

β. Το Γενικό Λογιστήριο των ΗΠΑ (General Accounting Office, GAO)[44] υπολογίζει, ότι γίνονται περίπου 250.000 επιθέσεις το χρόνο στα στρατιωτικά δίκτυα Η/Υ του Πενταγώνου με ποσοστά επιτυχίας περίπου 65% στο να έχουν κάποια πρόσβαση. Από αυτές οι 500 εβδομαδιαίως είναι σοβαρές, με την έννοια ότι έχουν δόλιες προθέσεις. Δεν είναι

[40] A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources. http://searchsecurity.techtarget.com/definition/denial-of-service
[41] http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn
[42] Παράδειγμα αποτελεί η ανάρτηση σημαίας των Σκοπίων στην ιστοσελίδα του Υπουργείου Δικαιοσύνης (10 Οκτ 2010) http://www.ines.gr/97/simaia-ton skopion sto site tou ypourgeiou
[43] Martin Libicki What is information warfare National Defense University, Institute for National Strategic Studies, 1995
[44] https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

δηλαδή τυχαίες επιθέσεις από hackers, γεγονός που συμβαίνει καθημερινώς, αλλά οργανωμένες επιθέσεις.

γ. Με βάση ανακοινώσεις του ρωσικού υπουργείου εσωτερικών, και την οποία ανακοίνωσε με τη σειρά του το Associated Press[45], το 1999 hackers εισέβαλαν στα υπολογιστικά συστήματα της Gazprom (της μεγαλύτερης ρωσικής εταιρείας πετρελαίου) και «πετυχαίνοντας τον έλεγχο του συστήματος διαχείρισης της ροής φυσικού αερίου σε όλη τη χώρα». "Ενεργώντας στο εσωτερικό της Gazprom, οι χάκερ μπόρεσαν να ξεπεράσουν την ασφάλεια της εταιρείας και να εισέλθουν στο σύστημα που ελέγχει τις ροές φυσικού αερίου σε αγωγούς. Ο "κεντρικός πίνακας διανομής φυσικού αερίου" ήταν "για κάποιο χρονικό διάστημα" υπό τον έλεγχο των εξωτερικών χρηστών, με τη χρήση προγράμματος «Δούρειου ίππου», το οποίο επιφέρει επιβλαβείς υπολογιστικούς κωδικούς σε ένα καλοφτιαγμένο πρόγραμμα.

δ. Σύμφωνα με την Ιαπωνική αστυνομία, στόχος επιθέσεων[46] στα δίκτυα τους έγιναν κρατικές οργανώσεις και μεγάλες επιχειρήσεις χωρίς να είναι γνωστή η προέλευση των δραστών. Ερευνητές της αστυνομίας παρατήρησαν, πως το κοινό χαρακτηριστικό όλων των θυμάτων αποτελούσε ο κατασκευαστής των δικτύων τους, που ανήκε στην ίδια εταιρεία, η οποία ήταν κομμάτι της παραθρησκευτικής οργάνωσης Aleph[47]. Με κατάλληλο λογισμικό της μορφής, security trapdoors είχε πρόσβαση όπου και όταν το ήθελε. Η ίδια μάλιστα παρέδωσε ένα "ασφαλές" τηλεπικοινωνιακό δίκτυο για το ιαπωνικό υπουργείο άμυνας. Η Aleph δεν είναι άγνωστη στο διεθνές κοινό. Το όνομα ήταν Aum Shinri Kyo αποτελεί παλιά ονομασία και ήταν υπεύθυνη για την επίθεση με το αέριο των νεύρων Σαρίν στο μετρό του Τόκιο πριν από μερικά χρόνια.

ε. Στη Μέση Ανατολή η σύγκρουση μεταξύ Ισραήλ και Παλαιστινίων έχει λάβει τη μορφή του ηλεκτρονικού τζιχάντ. Οι μέθοδοι που χρησιμοποιούνται από τους Παλαιστίνιους είναι τροποποίηση ιστοσελίδων, εισβολές σε συστήματα, DDos, αποστολή ιών (Worms[48], Trojan Horses). Έχουν προσβάλει τις τοποθεσίες του Ισραηλινού Κοινοβουλίου (Knesset),

[45] http://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system
[46] http://www.eeei.gr/interbiz/articles/sarin.htm
[47] https://www.japantimes.co.jp/news/2017/11/13/national/crime-legal/offices-aum-successor-adelph-raided-recruiting-practices/#.WkKsKVVl-vM
[48] Ένα σκουλήκι υπολογιστή (computer worm) είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού. Βικιπαίδεια

του Υπουργείου Εξωτερικών, της Τράπεζας του Ισραήλ, το χρηματιστήριο του Tel-Aviv, τον κύριο πάροχο διαδικτύου και του Ισραηλινού Στρατού (Israel Defense Forces, IDF). Αντίστοιχα οι υποστηρικτές του Ισραήλ έχουν επιτεθεί με DDos εναντίον των ιστοσελίδων της Παλαιστινιακής Αρχής, της Hezbollah και της Hamas.

στ. Άλλο περιστατικό κυβερνοπολέμου είναι η διένεξη μεταξύ Ινδίας και Πακιστάν σχετικά με το Κασμίρ τον Μάιο του 2013. Υποστηρικτές του Πακιστάν επιτέθηκαν τροποποιώντας ιστοσελίδες του Ινδικού Κοινοβουλίου, του Τηλεοπτικού σταθμού"Zee"[49], διαφόρων εφημερίδων, του Κέντρου Ατομικών ερευνών "Bhabha" κλπ. Ειδικά από το Κέντρο Ατομικών ερευνών υποκλάπηκαν 5 Mb ευαίσθητων πληροφοριών. Ταυτόχρονα πραγματοποιήθηκαν επιθέσεις σε ιστοσελίδες των ΗΠΑ. Ο αριθμός των επιθέσεων αυξάνεται εντυπωσιακά ανά έτος.

ζ. Μία από τις μεγαλύτερες κυβερνο-επιθέσεις των τελευταίων χρόνων πραγματοποιήθηκε την Παρασκευή 24 Οκτ 2016[50], με αποτέλεσμα τεράστιος αριθμός ιστοσελίδων στη Μεγάλη Βρετανία να τεθεί ταυτόχρονα εκτός λειτουργίας. Οι χάκερς χρησιμοποίησαν οικιακές συσκευές συνδεδεμένες στο Ίντερνετ, όπως κάμερες κλειστού κυκλώματος και εκτυπωτές για να φέρουν εις πέρας την επίθεσή τους. Ανάμεσα στις ιστοσελίδες που επλήγησαν από την επίθεση ήταν το Twitter και το Spotify. Αναλυτές ασφαλείας υποστηρίζουν ότι για την επίθεση χρησιμοποιήθηκε το «Internet of Things», δηλαδή οικιακές συσκευές οι οποίες έχουν τη δυνατότητα σύνδεσης στο Διαδίκτυο. Όπως αναφέρει σε δημοσίευμά του το βρετανικό ειδησεογραφικό δίκτυο BBC, οι περισσότερες από τις ιστοσελίδες που επλήγησαν χρησιμοποιούν την εταιρεία Dyn, η οποία είναι κάτι σαν διαδικτυακός «τηλεφωνικός κατάλογος» που κατευθύνει τους χρήστες στην ηλεκτρονική διεύθυνση όπου είναι αποθηκευμένη μια ιστοσελίδα. Τέτοιου είδους υπηρεσίες αποτελούν βασικό θεμέλιο για το Διαδίκτυο.

η. Μια μαζική επίθεση DDoS [Distributed Denial of Service] ξεκίνησε στις 21 Οκτ 2016[51] στοχεύοντας τις υποδομές της εταιρείας Dyn, η οποία φιλοξενεί και ορισμένους DNS servers. Όπως μπορείτε να καταλάβετε, το αποτέλεσμα αυτής της ενέργειας ήταν κάποιες από τις δημοφιλέστερες τοποθεσίες Web του κόσμου, να βρεθούν για αρκετή ώρα offline. Πιο

[49] https://www.hackread.com/indias-zee-television-network-hacked-by-bangladeshi-hackers/
[50] http://www.kathimerini.gr/880759/article/texnologia/diadiktyo/kyverno-epi8esh-eplh3e-taytoxrona-xiliades-istoselides
[51] http://gr.pcmag.com/internet/23891/news/mazike-epithese-ddos-enantion-dns-host-stis-epa

συγκεκριμένα, σύμφωνα με αναφορά στο Hacker News[52], από την επίθεση επηρεάστηκαν, μεταξύ άλλων, οι παρακάτω ιστοσελίδες: Twitter, Etsy, Github, Soundcloud, Spotify, Reddit.

Σημείωση: Αναδημοσίευση του γραφήματος από το http://www.pinsdaddy.com/cyber-security-and-cyber-war

θ. Σύμφωνα με το BBC[53], κυβερνοεπίθεση δέχτηκαν τα συστήματα παροχής υπηρεσιών του NHS (Εθνικό σύστημα Υγείας) της Βρετανίας με αποτέλεσμα πολλά νοσοκομεία να αναγκαστούν να παραπέμψουν σε άλλα νοσοκομεία τα επείγοντα περιστατικά. Την εξέλιξη αυτή επιβεβαίωσε και η διοίκηση της δημόσιας υπηρεσίας υγείας NHS σε επίσημη ανακοίνωσή της, χωρίς ωστόσο να διευκρινίζει τον ακριβή τρόπο με τον οποίο επηρεάζονται τα συστήματα IT.

ι. Στις 4 Σεπτεμβρίου 2007, οι Financial Times αποκάλυψαν πως στις αρχές του περασμένου Ιουνίου οι υπολογιστές στο γραφείο του υπουργού Άμυνας των ΗΠΑ, Robert Gates, είχαν δεχτεί υπερπόντιες «επισκέψεις». Το περιστατικό αυτό σημειώθηκε μόλις οκτώ ημέρες ύστερα από τα παράπονα της Γερμανίδας καγκελαρίου Angela Merkel για αντίστοιχες επιθέσεις. Στόχο αποτέλεσαν σύμφωνα με δημοσίευμα της εφημερίδας Guardian και τα γραφεία του Foreign Office στο Λονδίνο. Αφετηρία της επίθεσης σύμφωνα με τις αρχές ήταν η Κίνα.

[52] https://thehackernews.com/
[53] http://newpost.gr/kosmos/607354/prwtofanhs-kybernoepithesh-sygklonizei-ton-planhth-xtyphthhkan-nosokomeia-ypoyrgeia-kai-megales-etaireies

ια. Άλλο περιστατικό κυβερνοπολέμου είναι η αρπαγή της Catia[54] το 2008 , ένα πρωτοφανές πλήγμα σε μεγάλη γαλλική πολεμική βιομηχανία (Dassault). Λόγω της ιδιαιτερότητάς του, το συμβάν παρέμεινε επί μακράν κρυφό και σήμερα ελάχιστοι γνωρίζουν τα ακριβή γεγονότα. Ανάμεσα σε αυτούς, ένας 55χρονος Έλληνας μαθηματικός και προγραμματιστής, κάτοικος Αθηνών και ο 40χρονος Άγγλος συνεργάτης του, που ζει στο δυτικό Λονδίνο. Παρά τις ελάχιστες μεταξύ τους συναντήσεις, κατάφεραν να παραβιάσουν τα συστήματα ασφαλείας της γαλλικής βιομηχανίας, απέκτησαν πρόσβαση στο εσωτερικό δίκτυο και υπέκλεψαν το λογισμικό που χρησιμοποιούσε η εταιρεία για την κατασκευή των νέας γενιάς μαχητικών αεροσκαφών Mirage 2000. Το λογισμικό με την κωδική ονομασία Catia θεωρείται το ακριβότερο σε όλη την αγορά και το κόστος της «επίθεσης» ξεπέρασε τα 360 εκατ. δολάρια. Αξιωματικοί της ΕΛ.ΑΣ αποκάλυψαν ότι οι δράστες «έσπασαν» το λογισμικό σε υποπρογράμματα, τα οποία πούλησαν στο Διαδίκτυο. Περισσότεροι από 2.500 χρήστες, μεταξύ αυτών και ανταγωνιστικές πολεμικές βιομηχανίες, αγόρασαν τμήματα του λογισμικού αντιγράφοντας απόρρητα σχέδια και ευαίσθητες πληροφορίες. Οι ξένοι πράκτορες σε συνεργασία με τους αστυνομικούς της Δίωξης Ηλεκτρονικού Εγκλήματος εντόπισαν τους δύο hackers και σε βάρος τους ασκήθηκε δίωξη. Η υπόθεση εκκρεμεί στη Δικαιοσύνη.

ιβ. Τέλος, σύμφωνα με άρθρο της Βρετανικής εφημερίδας "Telegraph", η Ρωσία[55] επιχείρησε επιτυχώς κυβερνοπόλεμο κατά της Γεωργίας, λίγο πριν την πρόσφατη σύρραξη. Στις 8 Αυγούστου του 2008, η ιστοσελίδα της Ν. Οσσετίας δέχθηκε επίθεση DDoS λίγες ώρες μετά την επίθεση του Πυροβολικού των Γεωργιανών Δυνάμεων σε χωριά της Ν. Οσσετίας. Στις 9 Αυγούστου, hackers αντικατέστησαν την ιστοσελίδα του Υπουργείου Εξωτερικών της Γεωργίας με κολλάζ φωτογραφιών του Γεωργιανού Προέδρου Mikheil Saakashvili και του Αδόλφου Χίτλερ. Άλλες Γεωργιανές ιστοσελίδες που χτυπήθηκαν από hackers είναι του Υπουργείου Εσωτερικών καθώς και του Υπουργείου Άμυνας. Τέλος, η Εθνική Τράπεζα της Γεωργίας δέχθηκε επιθέσεις DDoS.

ιγ. Το πιο πρόσφατο παράδειγμα κυβερνοπολέμου, το οποίο βέβαια δεν έχει αποδειχθεί αλλά υπάρχουν σοβαρές υπόνοιες για την επίδρασή του, αποτελεί η προσπάθεια από πλευράς της Ρωσίας να επηρεάσουν την εκλογική αναμέτρηση των δύο υποψηφίων για την προεδρεία των ΗΠΑ με αποτέλεσμα να υπάρξει αντίδραση με απέλαση διπλωματών και

[54] https://www.scmagazine.com/hacker-arrested-in-greece-for-stealing-selling-weapons-data/article/554157/
[55] http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

κυρώσεις σε ρωσικές υπηρεσίες πληροφοριών. Όλη αυτή η διαδικασία σκοπό είχε, να προκαλέσει πολιτική αναταραχή και ανασφάλεια κατά τη διάρκεια της προεκλογικής περιόδου μιας υπερδύναμης, με ότι αυτό συνεπάγεται στην ασφάλεια της και την λειτουργία της. Η υποψία και μόνο παρέμβασης ξένων δυνάμεων στα εσωτερικά πολιτικά πεπραγμένα δημιουργεί αμφιβολία για την ασφάλεια απλών υποδομών της καθημερινότητας αλλά και σύνθετων διαδικασιών ασφαλείας και υποδομών[56].

1.7 Στρατηγική λειτουργία των κυβερνοεπιθέσεων

Οι σύγχρονες δομές και οι πυλώνες λειτουργίας των αναπτυγμένων κρατών στηρίζονται ολοένα και περισσότερο στη χρήση των δικτύων και των πληροφοριακών συστημάτων. Είναι λοιπόν δυνατόν, να θεωρήσουμε ότι αλλάζει ο τρόπος με τον οποίο επιχειρούν πλέον οι αντίπαλοι; Μπορεί δηλαδή να θεωρηθεί, ότι ο κυβερνοπόλεμος θα αντικαταστήσει την κλασσική μορφή του πολέμου ακόμα μάλιστα και τον πυρηνικό πόλεμο ;

Θα πρέπει να αναλύσουμε το τι επιδιώκει η κάθε μορφή απειλή. Αναλύοντας λοιπόν την πυρηνική αποτροπή, που επιφέρει η δυνατότητα χρήσης πυρηνικών όπλων από ένα κράτος, σε συνδυασμό με την ικανότητα του να διεξάγει εκτεταμένη μορφή κυβερνοπολέμου, θα μπορούσαμε να καταλήξουμε στα εξής συμπεράσματα :

α. Ο πυρηνικός παράγοντας έχει ήδη δοκιμαστεί και αποτελεί ένα γεγονός του οποίου τα μακροχρόνια και καταστροφικά αποτελέσματα δεν μπορεί να αμφισβητηθούν από τον οποιοδήποτε. Από την άλλη πλευρά, οι επιπτώσεις μιας κυβερνοεπίθεσης δεν είναι δυνατόν να προβλεφθούν και αποτελούν εικασίες[57]. Η καταστροφικότητα των πυρηνικών όπλων έχει λειτουργήσει αποτρεπτικά στην εξάπλωση τους. Κάτι τέτοιο δεν παρατηρείται στα όπλα του Κυβερνοχώρου για τα οποία υπάρχει ευκολία στην απόκτηση τους και στη χρήση τους. Παράλληλα, εάν σκεφτούμε, ότι για να εξασφαλιστεί με επιτυχία μια κυβερνοεπίθεση θα πρέπει να ληφθεί υπόψη η εξάρτηση του στόχου κράτους από τα δίκτυα. Σε αντίθεση μια πυρηνική επίθεση μπορεί να εξαπολυθεί σε όλους τους αντιπάλους.[58]

β. Οι δυνατότητες για συμβατικές επιθέσεις αποτελεί τον κύριο σκοπό κάθε κρατικής οντότητας. Η ψηφιακή επανάσταση ενεργοποίησε και συνεχίζει να ενεργοποιεί δυνάμεις που επιφέρουν αλλαγές στην ισορροπία του διεθνούς συστήματος, αφού θέτουν σε

[56] http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn
[57] Martin Libicki Conquest in Cyberspace Cambridge University Press 2007 σελ 40 -41
[58] Martin Libicki Conquest in Cyberspace Cambridge University Press, 2007 σελ 42 -43

αμφισβήτηση τα καθιερωμένα σύμβολα οικονομικής ισχύος, σε συνδυασμό με τα αντιστοιχα της στρατιωτικής και διπλωματικής ισχύος. Η ευκολία και η χαμηλού κόστους απόκτηση εργαλείων και μέσων για επιθέσεις στον Κυβερνοχώρο, είναι τα κίνητρα για την απόκτηση τέτοιων όπλων και την προσφυγή σε τέτοιου είδους επιθέσεις. Το γεγονός αυτό προκαλείται διάχυση και αναδιανομή της ισχύος σε βάρος δυνάμεων, που διαθέτουν συμβατική υπεροπλία. Γι' αυτό τον λόγο οι επιθέσεις στον Κυβερνοχώρο εντάσσονται στην κατηγορία των ασύμμετρων απειλών. Δηλαδή γίνεται κατανοητό, ότι τα συμβατικά όπλα είναι εκείνα που θα καθορίσουν την τελική έκβαση της σύγκρουσης ανεξάρτητα εάν υπάρχει υπεροχή ενός εκ των δύο αντιπάλων σε ηλεκτρονικά δίκτυα και δυνατότητα κυβερνοπολέμου[59].

Επίσης είναι αυτονόητο, ότι ο έλεγχος του εδάφους μιας περιοχής αποτελεί τον απώτερο στρατηγικό σκοπό κάθε αντιπαράθεσης. Επομένως η κατάληψη ή η επικράτηση στον Κυβερνοχώρο, δεν εξασφαλίζει τη νίκη. Δηλαδή η σημασία της γεωγραφίας δεν μπορεί να εξαλειφθεί από την ικανότητα κυβερνοεπιθέσεων ανεξάρτητα από το πόσο μεγάλη απόσταση χωρίζει τα αντιμαχόμενα μέρη[60].

[59] Παναγιώτης Κονδύλης Η Θεωρία του Πολεμου Θεμέλιο Οκτώβριος 2004 σελ 370
[60] Ανδρέας Λιαρόπουλος Η Γεωγραφία και η πληροφόρηση ως διαστάσεις της Παγκόσμιας Ασφάλειας Εισήγηση στο 7ο Πανελλήνιο Γεωγραφικό Συνέδριο Οκτ 2004.
http://www.geo.aegean.gr/ege2004/program/prog15a.htm

Σελίδα σκόπιμα κενή

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ

« Δεν υπάρχει κώδικας Ασφάλειας - Ότι κλειδώνει, ξεκλειδώνει…»[61]

2.1 Βασικά Στοιχεία

Είναι γεγονός ότι, με την πρόοδο των επικοινωνιακών και πληροφοριακών συστημάτων, κατέστη δυνατή η διασύνδεση αυτών σε παγκόσμιο επίπεδο δίνοντας τη δυνατότητα πρόσβασης στην επικοινωνιακή και πληροφοριακή υποδομή μιας χώρας, από οποιοδήποτε σημείο του πλανήτη. Αυτή η εξέλιξη, εκτός από την τεχνολογική πρόοδο, αποτέλεσε και πεδίο για την ανάπτυξη κινδύνων.

Έτσι οι τέσσερις διαστάσεις που αποτελούσαν το κλασσικό πεδίο αντιπαραθέσεων αντίπαλων δυνάμεων (ξηράς, θάλασσας, αέρος και διαστήματος), αυξήθηκαν σε πέντε με την προσθήκη του κυβερνοχώρου, γνωστού διεθνώς ως «Cyberspace».

Στην Ελλάδα, όσον αφορά τις Ένοπλες Δυνάμεις, τη Δημόσια Διοίκηση, τα Σώματα Ασφαλείας, καθώς και την Πολιτική Ηγεσία, ακολουθούνται τα Νατοϊκά και διεθνή πρότυπα ασφαλείας. Τα υιοθετούμενα μέτρα ασφαλείας, έχουν αποδειχθεί μέχρι τώρα σχετικά επαρκή, γεγονός που δεν πρέπει να δημιουργεί εφησυχασμό και αδράνεια. Αντίθετα, σε ένα περιβάλλον διαρκώς μεταβαλλόμενο και τεχνολογικά εξελισσόμενο, όπου οι επιθέσεις κυβερνοπολέμου μπορούν να εκδηλωθούν από τον οποιονδήποτε, από οποιοδήποτε μέρος του κόσμου και οποιαδήποτε χρονική στιγμή και περίοδο, θα πρέπει να μας δημιουργεί ανησυχία και κατά συνέπεια διαρκή προσπάθεια στην αναζήτηση νέων τεχνολογιών, διαδικασιών αλλά και «φρέσκων» ιδεών, για την εξασφάλιση μεγαλύτερης ασφάλειας και αξιοπιστίας των συστημάτων πληροφοριών και επικοινωνιών με σκοπό την επιβίωσή τους αλλά και την αύξηση των δυνατοτήτων της χώρας μας έναντι των δυνητικών αντιπάλων της.

Ο Κυβερνοπόλεμος περιέχει τα στοιχεία του Πληροφορικού πολέμου, τα οποία δεν είναι ρεαλιστικά αυτή την στιγμή.

[61] Kevin Mitnick ο οποίος χαρακτηρίστηκε ως ένας από τους μεγαλύτερους Αμερικανούς χάκερς που είχε εισβάλλει σε πολλά τηλεπικοινωνιακά δίκτυα, κλέβοντας δεδομένα. Ο πρώτος που του επιβλήθηκε η ποινή να μην ξανακουμπήσει υπολογιστή.

Τα είδη του κυβερνοπολέμου διακρίνονται ως εξής[62]:

α. Πληροφοριακή τρομοκρατία (Information Terrorism)

Η χρήση των Η/Υ προκειμένου να παραβιαστούν τα πληροφοριακά συστήματα, ιδιωτικών ή κυβερνητικών οργανισμών, χωρίς να διακοπεί η λειτουργία τους (Computer Hacking) και να υποκλαπούν πληροφορίες ή να αναληφθεί ο έλεγχος της λειτουργίας τους, προκειμένου να χρησιμοποιηθούν τρομοκρατικούς σκοπούς.

β. Σημασιολογικές επιθέσεις (Semantic Attacks)

Στην κατηγορία αυτή ανήκουν οι επιθέσεις, με τις οποίες το σύστημα που προσβάλετε, ενώ δείχνει ότι λειτουργεί κανονικά στην πραγματικότητα παράγει αποτελέσματα, τα οποία είναι παραποιημένα ή εσφαλμένα. Η διάκριση με την επίθεση hackers είναι ότι η τελευταία έχει ως αποτέλεσμα τη δυσλειτουργία του μέσου, που δέχεται την επίθεση ή την ολική κατάρρευση του.

γ. Πόλεμος Προσομοιώσεων (Simulation Warfare)

Η εμφάνιση του ηλεκτρονικού υπολογιστή και η τεχνολογική εξέλιξη είχε ως αποτέλεσμα, να αναπτυχθούν επικοινωνιακά δίκτυα και να δημιουργηθούν εφαρμογές, προκειμένου να υποστηρίξουν δραστηριότητες, η λειτουργία των οποίων, βασίζεται σε δίκτυα υπολογιστών. Ήταν απομονωμένα, δηλαδή προσέφεραν προστασία από κακόβουλους χρήστες. Η συνεχής όμως ανάπτυξη της πληροφορικής, η βελτίωση των προγραμμάτων και των υπηρεσιών κατέστησε επιτακτική την ανάγκη να τεθούν όλες αυτές οι υπηρεσίες στην υπηρεσία του πολίτη, και η χρήση της νέας τεχνολογίας, τα κατέστησε ευρέως προσβάσιμα και οδήγησε στην αύξηση της τρωτότητας τους.

Η περαιτέρω βελτίωση της τεχνολογίας των επικοινωνιών και της πληροφορικής αναμένεται να προκαλέσει αντίστοιχη αύξηση της τρωτότητας των δικτύων και των υποδομών των κρατών, ενώ συνδυαζόμενη με τη αποτελεσματικά Κυβερνοόπλα, θα καταστήσει τον Κυβερνοχώρο ένα νέο πεδίο ανταγωνισμού, και τον Κυβερνοπόλεμο μια πραγματική πρόκληση για την Κυβερνοασφάλεια των κρατών.

[62] Dr Martin C. Libicki Ph.D. in economics, University of California, Berkeley; M.A. in city and regional planning, University of California, Berkeley; S.B. in mathematics, Massachusetts Institute of Technology

2.2 Περιβάλλον πληροφοριών

Οι Κυβερνήσεις, οι κυβερνητικές και μη οργανώσεις, οι Βιομηχανίες και τα Στρατιωτικά Επιτελεία κατά τη σχεδίαση και διεξαγωγή πολιτικής - επιχειρήσεων στη σημερινή εποχή, την εποχή της πληροφορίας (Information Age) αντιμετωπίζουν ένα αυξανόμενα σύνθετο από πλευράς πληροφοριών περιβάλλον, που ονομάζεται Παγκόσμιο Πληροφοριακό Περιβάλλον (ΠΠΠ). Το ΠΠΠ περιέχει το σύνολο των ιδιωτών, οργανισμών και συστημάτων γενικότερα, που συλλέγουν, επεξεργάζονται και διανέμουν πληροφορίες σε εθνικά και διεθνή ακροατήρια, και κατά το πλείστον είναι εκτός ελέγχου της Κρατικής Εξουσίας ή του Στρατού της χώρας.

Τα στοιχεία από τα οποία αποτελείται το ΠΠΠ, είναι τα παρακάτω :

α. Πληροφοριακές Υποδομές (Παγκόσμια - Εθνική - Αμυντική).

β. Στρατιωτικό Πληροφοριακό Περιβάλλον.

γ. Πολιτικοί Αρχηγοί.

δ. Μέσα Μαζικής Επικοινωνίας.

ε. Βιομηχανία.

στ. Διεθνείς Οργανισμοί.

ζ. Κυβερνήσεις άλλων Κρατών.

η. Συνδυασμένα Συστήματα Επιτήρησης.

2.3 Ευπάθειες δικτύων Η/Υ - Διαδικτύου

«Ευπάθεια», εννοούμε την αδυναμία που δύναται να εκμεταλλευτεί ένα άτομο ή μια ομάδα προκειμένου να επιτύχει κάτι, που δεν δικαιούται να κάνει υπό κανονικές συνθήκες ή δεν αποτελεί φυσιολογική και προβλεπόμενη χρήση του δικτύου ή κάποιου συγκεκριμένου συστήματος σε αυτό.

Λόγω της επέκτασης και της ανάπτυξης του διαδικτύου (τόσο σε επίπεδο πλήθους χρηστών, όσο και σε επίπεδο παρεχόμενων υπηρεσιών), υπάρχει μεγάλη διακίνηση πληροφοριών, που δημιουργεί την απαίτηση για προστασία των δεδομένων, αφού τυχόν μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες είναι σχετικά εύκολη,

ανιχνεύεται δύσκολα και έχει καταστρεπτικές συνέπειες για την εύρυθμη λειτουργία οργανισμών (οικονομικών, στρατιωτικών, πολιτικών) και κρατών. Το πρόβλημα της ασφάλειας στο Διαδίκτυο, απασχολεί έντονα, και έχει κινητοποιήσει κρατικούς και μη φορείς ασφαλείας, την επιστημονική κοινότητα και εξειδικευμένες εταιρίες, που ασχολούνται με το αντικείμενο προκειμένου να το επιλύσουν.

Η ευπάθεια των δικτύων Η/Υ και του διαδικτύου οφείλεται στα παρακάτω :

α. Σχεδιαστικά σφάλματα πρωτοκόλλων και λογισμικού.

β. Τα αρχικά πρωτόκολλα, όταν σχεδιάστηκαν, δεν αποτέλεσαν στοιχεία ασφαλείας με αποτέλεσμα να παρουσιάζονται κενά.

γ. Σφάλματα - αδυναμίες στις ρυθμίσεις των δικτυακών εφαρμογών.

δ. Η ανοικτή φύση ευνοεί την ανέξοδη, δύσκολη στην ανίχνευση και ταχεία προσβολή του δικτύου και των πρωτοκόλλων του.

ε. Δεν κρυπτογραφείται μεγάλο μέρος των πληροφοριών, που διακινείται και έτσι υπάρχει ζήτημα εμπιστευτικότητας.

στ. Δεν υπάρχει έμπειρο και εξειδικευμένο προσωπικό.

2.4 Δυνατότητες εκμετάλλευσης των ευπαθειών του διαδικτύου

α. Παράνομη πρόσβαση (illegal Access[63])

Με τον όρο αυτό καθορίζεται κάθε ενέργεια για διεισδύσει και πρόσβαση με τον κατάλληλο τρόπο, σε ξένα συστήματα υπολογιστών.

β. Αθέμιτη παγίδευση - υποκλοπή (illegal interception[64])

Αυτή γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα δίκτυο υπολογιστών, μη εξαιρουμένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που «μεταφέρει» τέτοια στοιχεία.

γ. Επέμβαση σε δεδομένα (Data interference[65])

Είναι η εκ προθέσεως η καταστροφή, η διαγραφή, η χειροτέρευση (deterioration), η μεταβολή (alteration), ή η απόκρυψη (suppression) δεδομένων χωρίς δικαίωμα.

δ. Επέμβαση σε σύστημα (System Interference[66]).

Είναι η εκ προθέσεως σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση (Inputting), μεταφορά (transmitting),

[63] https://e-crime.ro/ecrime/site/index.php/home_en/materiale_documentare/acces_ilegal/
[64] www.icsd.aegean.gr/website_files/proptyxiako/76085723.doc
[65] https://www.usip.org/sites/default/files/MC1/MC1-Part2Section16.pdf
[66] https://www.usip.org/sites/default/files/MC1/MC1-Part2Section16.pdf

καταστροφή (damaging), διαγραφή (deleting), χειροτέρευση (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression).

Σημείωση: Αναδημοσίευση του γραφήματος από το https://www.cio.com.au/article/589943/unsw-offer-first-australian-course-cyber-war-peace/

Σελίδα σκόπιμα κενή

ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ
ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

3.1 Γενικά

Η διακίνηση πληροφοριών στο διαδίκτυο συνήθως είναι προσωπικά δεδομένα, για τα οποία υπάρχει το ατομικό δικαίωμα να μην γίνονται γνωστά σε τρίτα πρόσωπα. Έτσι απαιτεί ασφάλεια και μυστικότητα στη χρήση του διαδικτύου. Βασικές αρχές όπως η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας. Ουσιαστικά αυτές οι αρχές έχουν εφαρμογή και στον δαιδαλώδη κυβερνοχώρο. Αποτελεί λοιπόν περίπλοκο και δύσκολο ζήτημα ο έλεγχος του κυβερνοχώρου, προκειμένου να γίνεται με τέτοιο τρόπο και σε τέτοιο βαθμό ώστε να μην έρχεται σε αντίθεση με τις παραπάνω Αρχές.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο τεχνικά όσο και νομικά. Κάθε τεχνικός τρόπος που αποσκοπεί στην ασφάλεια του διαδικτύου, δύναται να εξουδετερωθεί από ένα άλλο τρόπο «αντιασφάλειας»[67]. Ο νομοθέτης λόγω της ταχύτατης εξέλιξης αδυνατεί να παρακολουθεί τις εξελίξεις και τις κοινωνικές επιπτώσεις. Δηλαδή, οι αλλαγές του κυβερνοχώρου, είναι τόσο ραγδαίες, που, εάν το θέμα δεν «σταθεροποιηθεί» κάπου από τεχνολογικής απόψεως, ο νομοθέτης αδυνατεί να λάβει μέτρα, σε ουσιαστικό ή δικονομικό επίπεδο.

Η ασφάλεια πληροφοριακών συστημάτων καθώς και η ασφάλεια υπολογιστικών συστημάτων[68], αποτελεί πεδίο της πληροφορικής. Για να γίνει η σχεδίαση ασφαλών πολιτικών στα πληροφοριακά συστήματα, αυτή πρέπει να είναι απόλυτα συνδεδεμένη με τεχνικές, διαδικασίες και διοικητικά μέτρα καθώς και με ηθικό - κοινωνικές αντιλήψεις, αρχές και παραδοχές, για να προφυλαχθεί από απειλή τυχαία ή σκόπιμη. Οι πολιτικές ασφαλείας, θα πρέπει να επιτρέπουν την απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων, ακολουθώντας αποκέντρωση, να υπάρχει η δυνατότητα αντικατάστασης και η αρχή της άμυνας σε βάθος. Αρχικά μπορεί να γίνει ο εντοπισμός, η αξιολόγηση και στη

[67] http://www.elesme.gr/elesmegr/periodika/t19/t19_03.htm

[68] Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα γνωστικό πεδίο της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Συγγενικά γνωστικά πεδία είναι η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία. Ασφάλεια Πληροφοριακών Συστημάτων (Επιμέλεια Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης), Εκδόσεις Νέων Τεχνολογιών, 2004.

συνεχεία η διαμόρφωση ενός θεωρητικού πλαισίου για το σχεδιασμό πολιτικών σχεδιασμού ασφάλειας.

Βασικά σημεία στη διαδικασία σχεδιασμού ασφαλών πολιτικών, αποτελούν ο εντοπισμός και χαρακτηρισμός ως εμπιστευτικών των πληροφοριών που πρόκειται να χρησιμοποιηθούν και να προστατευθούν. Εκτός από τις αρχές της Ακεραιότητας Πληροφοριών, την Εμπιστευτικότητα και τη Διαθεσιμότητα Πληροφοριών οι πολιτικές ασφάλειας θα πρέπει να εμπεριέχουν και τους όρους αυθεντικότητα, εγκυρότητα, μοναδικότητα και μη αποποίηση.

Ο καθορισμός της πολιτικής ασφάλειας του πληροφοριακού συστήματος[69] θα πρέπει να καλύπτουν οι ακόλουθες κατηγορίες :

α. Θέματα προσωπικού

β. Φυσική ασφάλεια

γ. Έλεγχος πρόσβασης στο πληροφοριακό σύστημα

δ. Διαχείριση υλικών και λογισμικών

ε. Νομικές υποχρεώσεις

στ. Διαχείριση της πολιτικής ασφάλειας

ζ. Οργανωτική δομή

η. Σχέδιο συνέχισης λειτουργίας

Όταν εφαρμόζουμε μια πολιτική ασφαλείας επιδιώκουμε :

α. Κάλυψη των λειτουργιών από τα μέτρα και τις οδηγίες προστασίας

β. Επικαιροποίηση των τεχνολογικών εξελίξεων

Γίνεται αντιληπτό ότι, επειδή το θέμα είναι δυναμικό και η τεχνολογία καλπάζει, μπορούμε με τροποποιήσεις ή προσθήκες, η πολιτική ασφαλείας να καλύπτει αλλαγές ή επεκτάσεις στο πληροφοριακό σύστημα. Επιπλέον πρέπει να διακρίνεται από σαφήνεια καθώς και εύκολη κατανόηση, από τεχνολογική ανεξαρτησία και καταλληλόλητα ανάλογα με τον οργανισμό που απευθύνεται.

Προκειμένου να μπορεί να παρουσιάζει επιτυχία μια πολιτική ασφάλειας, πρέπει να εξυπηρετεί ορισμένους σκοπούς, για τους οποίους σχεδιάζεται και αυτοί διακρίνονται στην δυνατότητα υποστήριξης των στόχων της επιχείρησης, τη συμμετοχή της διοικήσεως, την προσαρμογή στο περιβάλλον, όπου θα εφαρμοσθεί, την κατάλληλη εκπαίδευση των χρηστών, να μπορεί να αξιολογηθεί με ευκολία και αμεσότητα στην πρόσβαση. Η δυνατότητα τακτικών και πλήρων ενημερώσεων αποτελεί ουσιώδη αναγκαιότητα.

[69] https://el.wikipedia.org/wiki/ Ασφάλεια_ πληροφοριακών_συστημάτων

Χαρακτηριστικά της πολιτικής ασφάλειας αποτελούν τα παρακάτω :

α. Ακεραιότητα

Αυτή αφορά τη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια σταθερή και επιθυμητή κατάσταση χωρίς τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και απαγόρευση στην πρόσβαση και χρήση του συστήματος από αναρμόδια άτομα.

Εάν λοιπόν σκεφτούμε τη λειτουργία, μια εφημερίδας που χρησιμοποιεί το διαδίκτυο για να δημοσιεύει τα άρθρα της θα αποζητούσε την ασφάλεια προκειμένου να αποτρέψει και να εμποδίσει τη δράση χάκερ που μπορεί να τροποποιήσει τις πληροφορίες στα κείμενα. Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι το 1995, άγνωστοι παράκαμψαν τα μέτρα ασφάλειας στην εφημερίδα Ελευθεροτυπίας και μετέδωσαν την είδηση για πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο.

β. Διαθεσιμότητα

Με τον όρο διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων εννοούμε την εξασφάλιση της άμεσης χρήσης των πληροφοριακών συστημάτων από τους χρήστες όποτε απαιτείται η χρήση τους.

Εδώ κύριος στόχος των επιθέσεων είναι να δημιουργήσουν τις κατάλληλες συνθήκες ώστε τα συστήματα να μην είναι διαθέσιμα, δηλαδή να υπάρχει μια άρνηση υπηρεσιών (DOS attack[70]), με σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι[71] είτε προσωρινά, είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Έτσι το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή χαμηλής χωρητικότητας δημοσιεύεται σε ιστοσελίδα, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.

γ. Εμπιστευτικότητα

Με τον όρο αυτό χαρακτηρίζουμε την κατάσταση εκείνη, κατά την οποία ευαίσθητες πληροφορίες πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

---

[70] Επιθέσεις άρνησης εξυπηρέτησης (Df-service attack, DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.Αν και ο όρος αφορά κυρίως δικτυακές υπηρεσίες, δεν περιορίζεται μόνο σε αυτές αλλά αναφέρεται και σε άλλα πεδία όπως ο μικροεπεξεργαστής (CPU) όπου μία αντίστοιχη επίθεση καταναλώνει τους πόρους του μικροεπεξεργαστή. Ασφάλεια Πληροφοριακών Συστημάτων (Επιμέλεια Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης), Εκδόσεις Νέων Τεχνολογιών, 2004.

[71] http://www.hellenica.de/Technologia/Ypologistis/InformationSecurity.html

Για την απώλεια πληροφοριών δεν απαιτείται πάντα η χρήση της ψηφιακής υποκλοπής, αλλά μπορεί να γίνει με κλασσικές μεθόδους, όπως με την κλοπή υπολογιστών ή σκληρών δίσκων, που δεν έχουν ασφαλισθεί. Μελέτες σε αριθμό εταιρειών έδειξαν, ότι ένα μεγάλο ποσοστό από τέτοιες απώλειες πληροφοριών προήλθε από κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας.

3.2 Προσπάθεια αντιμετώπισης Κυβερνοεπιθέσεων / εγκλήματος στον κυβερνοχώρο

Ο ερχομός και η διάδοση των τεχνολογιών του διαδικτύου έχει αναγκάσει τα κοινοβούλια και τα δικαστήρια των κρατών ανά την υφήλιο, να προσπαθήσουν να διατηρήσουν μια ισορροπία μεταξύ της ελεύθερης διακίνησης των πληροφοριών και της προστασίας των πνευματικών δικαιωμάτων. Ένας τρόπος που προσπαθούν τα δικαστήρια να βρουν την ιδανική ισορροπία είναι εφαρμόζοντας το δόγμα της δίκαιης χρήσης του Internet[72]. Θεωρητικά και το ξεφύλλισμα ακόμη σελίδων του διαδικτύου μπορεί να αποτελέσει παραβίαση του copyright.

Κατ' αυτόν τον τρόπο μπορούμε να αναφερθούμε στα νομικά προβλήματα που προκύπτουν από την μεταφορά αρχείων ήχου και εικόνας[73] στον υπολογιστή μας, όπως και στην μεταφορά αρχείων μεταξύ ομότιμων υπολογιστών[74] παρακάμπτοντας τους κεντρικούς εξυπηρετητές δικτύου. Στην τελευταία αυτή περίπτωση είχαμε και την δίκη των «A&M Records v. Napster», όπου είχαμε την καταδίκη του Napster, το οποίο ήταν ένα πρόγραμμα υπηρεσία του Internet, που διευκόλυνε τη μεταφορά μουσικών αρχείων μεταξύ των συνδρομητών του. Μια τρίτη κατάσταση που εγείρει νομικά προβλήματα είναι η τοποθέτηση σε δικτυακούς τόπους του Internet και επομένως διαθέσιμα σε όλους, εργασίες με κατοχυρωμένα πνευματικά δικαιώματα[75].

3.3 Αντιμετώπιση των κυβερνοεπιθέσεων από τα κράτη

Εσθονία

[72] Fair Use on the Internet

[73] Streaming media is multimedia that is constantly received by and presented to an end-user while being delivered by a provider. The verb "to stream" refers to the process of delivering or obtaining media in this manner; the term refers to the delivery method of the medium, rather than the medium itself, and is an alternative to file downloading, a process in which the end-user obtains the entire file for the content before watching or listening to it.Wikipedia

[74] Peer-to-peer File Sharing Peer-to-peer file sharing is the distribution and sharing of digital media using peer-to-peer (P2P) networking technology. P2P file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content.[1] The nodes (peers) of such networks are end-user computers and distribution servers (not required).Wikipedia

[75] Posting and Storage

Την 27η Απριλίου του 2007 η πληροφοριακή υποδομή της Εσθονίας δέχθηκε μια συντονισμένη επίθεση DDoS[76] σε μεγάλη έκταση, η οποία διήρκεσε περίπου τρεις εβδομάδες. Οι επιπτώσεις στην καθημερινότητα των πολιτών, αλλά και γενικότερα στη δυνατότητα της χώρας να λειτουργήσει, ήταν σοβαρές.

Ο πολιτικός σκοπός της κυβερνοεπίθεσης, αν δεχθούμε τον ισχυρισμό της εσθονικής κυβέρνησης, ότι αυτή οργανώθηκε από τη Ρωσία, ήταν η τιμωρία της Εσθονίας για τη μετακίνηση ενός μνημείου προς τιμή του Κόκκινου Στρατού από το κέντρο της πρωτεύουσας Ταλλίν στις παρυφές της πόλης.

Το περιστατικό αυτό παρουσιάζει ιδιαίτερο ενδιαφέρον, διότι ήταν η πρώτη φορά που το διαδίκτυο χρησιμοποιήθηκε ως εργαλείο εθνικής πολιτικής, με στόχο τις υποδομές ενός κράτους.

Πόλεμος Ρωσίας - Γεωργίας

Μία ακόμη πιο ενδιαφέρουσα, από στρατιωτική άποψη, περίπτωση αποτελεί ο πόλεμος Γεωργίας – Ρωσίας, ο οποίος ξέσπασε την 7η Αυγούστου του 2008, όταν η Γεωργία επιτέθηκε στην αποσχισθείσα περιοχή της Νότιας Οσσετίας. Οι ρωσικές δυνάμεις απέκρουσαν την επίθεση και προήλαυσαν στο έδαφος της Γεωργίας. Η επίθεσή τους όμως δεν άρχισε στο έδαφος, αλλά στον κυβερνοχώρο. Στα πλαίσια των κυβερνοεπιχειρήσεων οι κυριότερες κυβερνητικές ιστοσελίδες στη Γεωργία υπέστησαν επιθέσεις, με αντικατάσταση του περιεχομένου τους ή απαγόρευση της πρόσβασης σε αυτές, και εξουδετερώθηκαν από τις πρώτες φάσεις της αντιπαράθεσης. Η υποβάθμιση της δυνατότητας της Γεωργίας να παρουσιάσει τη δική της άποψη για την κρίση μέσω του Υπουργείου της των Εξωτερικών υπέσκαψε τη δυνατότητά της να διαμορφώσει την παγκόσμια κοινή γνώμη.

Η αξία του επεισοδίου αυτού έγκειται στο γεγονός ότι οι κυβερνοεπιχειρήσεις εκδηλώθηκαν μεταξύ κρατικών οντοτήτων, στα πλαίσια της υποστήριξης επιχειρήσεων κλασικού πολέμου.

Προσβολή συστήματος διαχείρισης λυμάτων

Τρίτο επεισόδιο, αφορά στην προσβολή ενός πυρηνικού εργοστασίου του Ιράν και η υποβάθμιση της δυνατότητας της χώρας να παράγει απεμπλουτισμένο ουράνιο, υλικό απαραίτητο για την κατασκευή πυρηνικών όπλων. Ο ιός STUXNET, ο οποίος προσβάλει το

[76]Internetική επίθεση που γίνεται σε ένα data center και μπλοκάρει στην ουσία τη διακίνηση δεδομένων από και προς αυτό. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. http://www.digitalattackmap.com/understanding-ddos/

λογισμικό των συστημάτων ελέγχου του εργοστασίου πυρηνικής ενέργειας φέρεται να έχει κατασκευαστεί σε κρατικά εργαστήρια.

Η συγκεκριμένη περίπτωση παρουσιάζει ενδιαφέρον διότι επιβεβαιώνει την τρωτότητα των υποδομών μιας χώρας σε επιθέσεις μέσω του κυβερνοχώρου, και η χρήση των κυβερνοδυνατοτήτων για τη διεξαγωγή παρεμποδιστικού πολέμου.

Αμερικανικές Προεδρικές εκλογές 2016

Στο επίκεντρο του διεθνούς ενδιαφέροντος έχει βρεθεί το ζήτημα των κυβερνοεπιθέσεων, με τον ίδιο τον Ντόναλντ Τραμπ να παραδέχεται για πρώτη φορά, την Τετάρτη, ότι η Ρωσία βρίσκεται πίσω από τις κυβερνοεπιθέσεις με στόχο τις αμερικανικές εκλογές. Στην πρώτη του συνέντευξη Τύπου μετά τις εκλογές, ο Τραμπ είπε: «Ο κ. Πούτιν δεν έπρεπε να το έχει κάνει αυτό. Πιστεύω ότι η Ρωσία ήταν πίσω από την επίθεση αυτή, αλλά τέτοιες επιθέσεις εναντίον μας εξαπολύουν και άλλες χώρες».[77]

Η αναφορά αυτή του εν αναμονή προέδρου τον εμφανίζει να συμφωνεί με τις εκτιμήσεις των αμερικανικών μυστικών υπηρεσιών, οι οποίες κατήγγειλαν εδώ και λίγους μήνες τη δράση Ρώσων χάκερ με στόχο το Δημοκρατικό Κόμμα, αλλά και σε μικρότερο βαθμό το Ρεπουμπλικανικό.

Σημείωση: Αναδημοσίευση του γραφήματος από το
http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

Η Κίνα, η Βόρεια Κορέα, η Ρωσία και το Ισραήλ έχουν δείξει τις ικανότητές τους στον τομέα. Ενδεικτικά αναφέρεται ότι Ρώσοι hackers έχουν επιτεθεί κατά των υποδομών της

[77] http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

Εσθονία, της Λιθουανίας, της Γεωργίας και του Καζακστάν, ενώ το Ισραήλ αχρήστευσε το δίκτυο αεράμυνας της Συρίας κατά την επιχείρηση Orchard.

Οι ΗΠΑ δίνουν ιδιαίτερα μεγάλη σημασία στην προστασία της πληροφορικής υποδομής τους από κυβερνοεπιθέσεις, οι οποίες αναδεικνύονται σε νέο σημείο τριβής με την Κίνα, την οποία και θεωρούν σημαντική ασύμμετρη απειλή.

Χαρακτηριστικό παράδειγμα των πρακτικών, που εφαρμόζουν οι Κινέζοι είναι αυτό που συμβαίνει στις ελληνικές τηλεπικοινωνίες τα τελευταία χρόνια : δύο πολύ μεγάλες κινεζικές εταιρείες, η ZTE και η Huawei, έχουν σαρώσει τις προμήθειες των τηλεπικοινωνιακών οργανισμών της χώρας μας. Οι τιμές που δίνουν στους διαγωνισμούς, είναι περίπου στο 50% αυτών που δίνουν οι παραδοσιακοί προμηθευτές (Ericsson, Siemens, Alcatel κλπ.) με αποτέλεσμα να τους ανατίθενται σχεδόν όλες οι προμήθειες βασικών τηλεπικοινωνιακών υποδομών, όπως είναι τα κυκλώματα για συνδέσεις Internet. Αντίστοιχη τάση υπάρχει και σε άλλες ευρωπαϊκές χώρες, αλλά πιθανόν στην Ελλάδα το φαινόμενο αυτό να έχει πάρει μεγαλύτερες διαστάσεις. Είναι αναμενόμενο, λοιπόν, διεθνείς οργανισμοί όπως το ΝΑΤΟ, να δείξουν στο άμεσο μέλλον μεγαλύτερο ενδιαφέρον για το «μίγμα» των τηλεπικοινωνιακών υποδομών των χωρών - μελών του ΝΑΤΟ.

Σχετικά με ΗΠΑ και Κίνα, είναι ενδεικτικό ότι οι μεν ΗΠΑ από το 1998 αναγνώρισαν επίσημα τον πληροφορικό πόλεμο ως ένα νέο χώρο διεξαγωγής επιχειρήσεων, εκδίδοντας και το ανάλογο «δόγμα», η δε Κίνα, η οποία οργανωτικά δείχνει να προηγείται, δημιούργησε και τέταρτο κλάδο στις Ένοπλες Δυνάμεις της, αυτόν του Πληροφορικού Πολέμου, δίπλα στους κλάδους Στρατού Ξηράς, Ναυτικού και Αεροπορίας.

Στον Ευρωπαϊκό χώρο η κατάσταση δεν θα μπορούσε να είναι διαφορετικά .Οι Βρυξέλλες, που διαχειρίζονται ευαίσθητα ηλεκτρονικά δεδομένα των 28 κρατών–μελών της Ένωσης καθώς και τα ηλεκτρονικά συστήματα διοίκησης του ενιαίου νομίσματος, ενίσχυσαν πρόσφατα τις μεθόδους προστασίας των δικτύων τους, σε μια προσπάθεια αντιμετώπισης του κινδύνου διείσδυσής τους από χάκερ. Ανώτατα στελέχη της Ένωσης καλούνται τώρα να χρησιμοποιούν μόνο κρυπτογραφημένα συστήματα ηλεκτρονικού ταχυδρομείου για τις μεταξύ τους επικοινωνίες, ενώ η Κομισιόν διεύρυνε πρόσφατα τη συνεργασία της με τις υπηρεσίες ηλεκτρονικής ασφάλειας του ΝΑΤΟ. Η Βορειοατλαντική Συμμαχία, που είχε πέσει και αυτή θύμα κυβερνοεπιθέσεων εντός του 2016, έχει καταστήσει τη διασφάλιση των δικτύων της ως κύρια προτεραιότητα.[78]

[78] http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

«Είναι προφανές ότι πολλά θεσμικά όργανα της Ευρώπης –αλλά και πέρα από αυτήν– στα οποία περιλαμβάνεται η Κομισιόν, δέχονται ολοένα και περισσότερες κυβερνοεπιθέσεις από διάφορες κατευθύνσεις.

Οι απειλές αυτές είναι επίμονες, επιθετικές, ιδιαίτερα επικίνδυνες και δυνητικά καταστροφικές», είπε, μιλώντας στους Financial Times, ο επίτροπος Ασφαλείας της Ε.Ε., σερ Τζούλιαν Κινγκ[79]. Οι πλέον καταστροφικές κυβερνοεπιθέσεις είναι εκείνες οι οποίες επιδιώκουν να υποσκάψουν την εμπιστοσύνη των πολιτών στους δημοκρατικούς θεσμούς, εκτιμά ο σερ Τζούλιαν. Παρότι η Ρωσία βρίσκεται στο επίκεντρο των ευρωπαϊκών ανησυχιών περί ασφαλείας των δικτύων, πηγές της Κομισιόν αρνούνται να κατονομάσουν την πηγή των επιθέσεων αυτών. «Διάφοροι χάκερ μοιράζονται και αξιοποιούν τα ίδια εργαλεία και μεθόδους, για να αποκρύψουν την ταυτότητά τους, αξιοποιώντας ανώνυμους διακομιστές», ανέφερε εκπρόσωπος της Ευρωπαϊκής Επιτροπής.

Σημείωση: Αναδημοσίευση του γραφήματος από το http:// usdefensewatch.com/wp content/uploads/2016/09/china-US-cyber-warfare.jpg

Για την προστασία της πληροφοριακής τους υποδομής, οι ΗΠΑ έχουν ιδρύσει μία σειρά από κέντρα, όπου αναφέρονται τα περιστατικά και τα οποία αντιμετωπίζουν τις επιθέσεις, όπως :

[79] http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

α. Το Εθνικό Κέντρο Προστασίας Υποδομής (National Infrastructure Protection Centre, NIPC[80]) που διευθύνεται από το FBI.

β. Το Ομοσπονδιακό Κέντρο Αντίδρασης (Federal Computer Incident Response Center, FedCIRC).

γ. Περιφερειακές Ομάδες Αντίδρασης (Regional Computer Emergency Response Teams, R/CERTS).

δ. Κέντρα Ανάλυσης και Διανομής Πληροφοριών (Information Sharing and Analysis Centers), και

ε. Αντίστοιχες Ομάδες Αντίδρασης του Στρατού (Army Computer Emergency Response Team, A/CERT), Κεντρική και Τοπικές.

Τέλος, στις 23 Ιουνίου του 2009, ο Αμερικανός Υπουργός Άμυνας, Robert Gates, υπέγραψε το μνημόνιο ίδρυσης της Διοίκησης Κυβερνοπολέμου US Cyber Command (USCYBERCOM[81]), που υπάγεται στην USSTRATCOM και διευθύνεται από το Διοικητή της National Security Agency (NSA), Keith Alexander.

Αντίστοιχες Υπηρεσίες έχει ιδρύσει και ο Καναδάς, σε διεθνές δε επίπεδο υπάρχει το Φόρουμ για τις Ομάδες Αντίδρασης (Forum for Incident Response Teams, FIRST).

[80] The National Infrastructure Protection Center (NIPC) was a unit of the United States federal government charged with protecting computer systems and information systems critical to the United States infrastructure. It was founded in 1998 by President Bill Clinton's Presidential Decision Directive 63. It was originally created as a branch of the FBI.In 2003, the NIPC was transferred to the Department of Homeland Security. The NIPC was eventually[when?] disbanded, with other federal government organizations taking on its responsibilities.

[81] Η κυβερνητική εντολή των Ηνωμένων Πολιτειών (USCYBERCOM) είναι μια Εντολή Ενιαίας Εντολής Καταπολέμησης της Στρατηγικής Διοίκησης των ΗΠΑ . Η Διοίκηση ενοποιεί την κατεύθυνση των κυβερνοχώρων , ενισχύει τις δυνατότητες του κυβερνοχώρου DoD και ενσωματώνει και ενισχύει την τεχνογνωσία του κυβερνοχώρου της DoD.
Η USCYBERCOM δημιουργήθηκε το 2009 στην έδρα της Υπηρεσίας Εθνικής Ασφάλειας (NSA) στο Fort George G. Meade , Maryland . Χρησιμοποιεί δίκτυα NSA και διευθύνεται από τον Διευθυντή του Οργανισμού Εθνικής Ασφάλειας από την ίδρυσή του. Αν και δημιουργήθηκε αρχικά με μια αμυντική αποστολή, θεωρείται όλο και περισσότερο ως επίθεση. Στις 18 Αυγούστου 2017, ανακοινώθηκε ότι η USCYBERCOM πρόκειται να αναδειχθεί σε καθεστώς πλήρους και ανεξάρτητης Ενιαίας Εντολής Εντοπισμού.

Σελίδα σκόπιμα κενή

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ
ΔΥΝΑΤΟΤΗΤΕΣ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ ΕΛΛΑΔΟΣ ΚΑΙ ΤΟΥΡΚΙΑΣ

4.1 Γενικά

Στο κεφάλαιο αυτό γίνεται μια αναφορά στις δυνατότητες Κυβερνοπολέμου που διαθέτει η Ελλάδα και η Τουρκία ο οποίος δύναται να αποτελέσει ένα πεδίο αντιπαράθεσης τόσο σε ειρηνική περίοδο όσο και σε μια ενδεχόμενη εμπόλεμη κατάσταση των δύο κρατών στο μέλλον. Τις τελευταίες δεκαετίες λαμβάνει χώρα μεταξύ Ελλάδας και Τουρκίας μια συνεχή σύγκρουση χαμηλής έντασης (low intensity warfare) στην οποία κυριαρχούν η στρατιωτική και πολιτική πίεση, η κατασκοπεία και ο ψυχολογικός πόλεμος με κύριο εργαλείο την εξαγωγή πολιτισμού[82]. Στην πραγματικότητα ωστόσο η τουρκική απειλή αποδεικνύεται πολύ πιο σύνθετη περιλαμβάνοντας τον κυβερνοπόλεμο αλλά και ένα πλήθος δραστηριοτήτων από τον ευρύτατο χώρο του μη κανονικού πολέμου (irregular warfare), όπως η λαθρομετανάστευση, οι παραστρατιωτικές επιχειρήσεις και το οργανωμένο έγκλημα. Η εν λόγω συστράτευση στα πλαίσια μιας σφαιρικής προσέγγισης (comprehensive approach) τακτικών συμβατικού, μη κανονικού πολέμου και κυβερνοπολέμου προσδίδει ξεκάθαρα στην Τουρκία χαρακτηριστικά υβριδικής απειλής (hybrid threat).[83] Ο Κυβερνοπόλεμος, πιο πολύ ως όρος παρά ως προς το περιεχόμενό του και τη σημασία του, δεν είχε συμπεριληφθεί, μέχρι πρότινος στις εκτιμήσεις που αφορούν την στρατιωτική ισχύ της Τουρκίας ή σε διάφορα υποθετικά σενάρια θερμού επεισοδίου ή και γενικότερης εμπλοκής. Αυτό βέβαια έχει αλλάξει τα τελευταία χρόνια και πλέον έχει γίνει κατανοητή η σημασία μιας ισότιμης αντιμετώπισης στη μορφή αυτή πολέμου.

4.2 Τουρκία

Παράλληλα με τις συνεχείς παραβιάσεις τόσο τουρκικών αεροσκαφών όσο και από πολεμικά σκάφη διεξάγεται ένας ανηλεής πόλεμος μεταξύ Ελλήνων και Τούρκων hackers στο διαδίκτυο. Έτσι θύματα από ελληνικής πλευράς αυτής της διαμάχης έχουν πέσει ιστοσελίδες, όπως το www.defencenet.gr, το www.ardin.gr, αλλά και η ιστοσελίδα της ΕΠΟ. Επίσης ιστοσελίδες υπουργείων έχουν κατά περιόδους γευτεί την επίσκεψη των γειτόνων μας.
τους. Η Τουρκία εκδήλωσε το ενδιαφέρον για την απόκτηση υποδομών και εκπαιδευμένου προσωπικού σε πληροφοριακού περιεχομένου επιχειρήσεων στα πλαίσια του κυβερνοπολέμου από πολύ νωρίς με την παροχή κονδυλίων για την απόκτηση του

[82] https://www.thinknews.gr/politiki/tourkia-os-yvridiki-apili/
[83] https://www.thinknews.gr/politiki/tourkia-os-yvridiki-apili/

τεχνολογικού εξοπλισμού και την εκπαίδευση του κατάλληλου προσωπικού και έχει ήδη δημιουργήσει σημαντικές υποδομές και δυναμικό ώστε να αποτελεί μια από τις πρωτοπόρες χώρες του ΝΑΤΟ στον τομέα του κυβερνοπολέμου.

Μεταξύ των τουρκικών υποδομών είναι το ULAK (ακρωνύμιο στην τουρκική για Ομάδα Ανταποκρίσεως σε Συμβάντα Ασφάλειας Υπολογιστών, ή CSIRT, Computer Security Incident Response Team), το οποίο ιδρύθηκε με σκοπό την προστασία εθνικών δικτύων υπολογιστών, τον εντοπισμό και την ταυτότητα των εισβολέων και την ενημέρωση των διαχειριστών των δικτύων με τις πληροφορίες και τα στοιχεία που συγκεντρώθηκαν.

Η καρδιά του τουρκικού συστήματος κυβερνοάμυνας – κυβερνοπολέμου είναι το περίφημο Κέντρο Επιστημονικών και Τεχνολογικών Ερευνών TUBITAK, γνωστό μέχρι τώρα για τις έρευνές του, μεταξύ άλλων, στον τομέα της άμυνας και της αμυντικής βιομηχανίας, αλλά όχι και για τη συμμετοχή του στην περιοχή που αποτελεί το θέμα μας. Στο TUBITAK υπάγεται το ελάχιστα γνωστό στη χώρα μας ILTAREN[84], καθώς επίσης και εντός αυτού το ακόμη πιο άγνωστο UEKAE[85], άλλως Διεθνές Ινστιτούτο Ερευνών στην Ηλεκτρονική και Κρυπτολογία. Το τελευταίο έχει σημαντική δραστηριότητα στον τομέα ηλεκτρονικής τεχνολογίας και στον τομέα της ασφάλειας πληροφοριών, με ενεργό ρόλο και συμμετοχή στο ΝΑΤΟ, στον τομέα των δραστηριοτήτων του.

Οι τουρκικές δυνατότητες στον τομέα αυτό είναι ανάλογες της προσπάθειας που καταβάλλεται από ετών και των σημαντικών κονδυλίων που διετέθησαν και διατίθενται ακόμη. Μεταξύ αυτών, περιλαμβάνονται η ανάπτυξη του εθνικού λογισμικού Pardus (με βάση το Linux) για εφαρμογές στην άμυνα, η παραγωγή κλειδών κρυπτογραφήσεως με πιστοποίηση ΝΑΤΟ, η ανάπτυξη και διάθεση στο ΝΑΤΟ ειδικών συσκευών απτόμενων του τομέα της ασφάλειας, η παραγωγή εργαλείων για κυβερνοεπιθέσεις (ιοί), κ.ά.

Όλο αυτό το δυναμικό είναι πλήρως ενταγμένο στο Γενικό Επιτελείο της Τουρκίας και λειτουργεί ως ένα απόλυτα συντονισμένο και συγκροτημένο σύνολο, με σαφείς εφαρμογές στο στρατιωτικό τομέα.
κρατική δράση.

4.2.1 Οι «Πολεμιστές του Διαδικτύου»

[84] Ileri Teknoloji Arastirma Enstitusu ή Κέντρο Ερευνών Προκεχωρημένης Τεχνολογίας ιδρύθηκε για να διασφαλίσει ότι τα κανάλια επικοινωνίας στις διαδικασίες που διεξάγονται από την TÜBİTAK μπορούν να διαχειριστούν από ένα μόνο κέντρο και να αυξήσουν την αποδοτικότητα των διαδικασιών.
[85] Ulusal Elektronik ve Kriptoloji Arastirma Enstitusu. The National Research Institute of Electronics and Cryptology of Turkey (Turkish: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), shortly UEKAE, is a national scientific organization with the aim of developing advanced technologies for information security. UEKAE is the most prominent and also the founder (first) institute of the TÜBİTAK.

Εκατοντάδες hackers της γειτονικής χώρας, με δομή και οργάνωση στρατιωτικού σώματος, φαίνεται να λειτουργούν στο πλαίσιο ενός οργανωμένου δικτύου, ενταγμένου στο τουρκικό Γενικό Επιτελείο, και ελεγχόμενου με διάφορους τρόπους από αυτό. Η παρουσία των Τούρκων hackers ενέχει όλες τις εγγενείς δυσκολίες που εμφανίζει κάθε προσπάθεια περιγραφής αναρχικών ή μεμονωμένων ατόμων, εσωστρεφών κατά βάση και συνδεόμενων με μία κοινή ενασχόληση, την επιμονή, τον ζήλο και την αφοσίωση ενός φανατικού σε μία δραστηριότητα, από την οποία αισθάνεται ότι καταξιώνεται μέσω των αποτελεσμάτων της.

Ως εκ τούτου, μια πρώτη προσέγγιση των Τούρκων hackers δεν μπορεί να δώσει παρά ένα γενικό μόνο περίγραμμα των δραστηριοτήτων τους, το οποίο παρά ταύτα εμφανίζει ιδιαίτερο ενδιαφέρον. Τούτο καθίσταται ακόμη μεγαλύτερο, αν η ύπαρξη εκατοντάδων Τούρκων hackers θεωρηθεί στο πλαίσιο ενός οργανωμένου δικτύου, που υπάγεται στο τουρκικό Γενικό Επιτελείο και ελέγχεται από αυτό, μια εκτίμηση για την οποία υπάρχουν όλες οι ενδείξεις.

Με τους Τούρκους να ακολουθούν σε όλα τις διεθνώς ακολουθούμενες πρακτικές με την πλέον κοινή από αυτές την «επιστράτευση» των hackers από τις αρμόδιες Κυβερνητικές Υπηρεσίες, κάτι που είδαμε ακόμη μία φορά στην περίπτωση της ρωσικής εισβολής στη Γεωργία , η στρατολόγηση σε οργανωμένη βάση των Τούρκων «Πολεμιστών του Διαδικτύου» από το Γενικό Επιτελείο της χώρας τους και η καθοδήγησή τους από συγκεκριμένη Διεύθυνση αυτού θεωρούνται δεδομένες.

Η μάλλον έντονη παρουσία των Τούρκων στον συγκεκριμένο τομέα αποτέλεσε την αιτία ειδικής μελέτης, με τίτλο "The Attack Dynamics of Political and Religiously Motivated Hackers", από τον δρα Thomas Holt,[86] , η οποία έγινε ύστερα από συνεντεύξεις με δέκα ενεργούς Τούρκους hackers και δεδομένα από έξι φόρουμ που χρησιμοποιούν στο διαδίκτυο.

Εδώ αξίζει να τονίσουμε ότι τα φόρουμ των hackers είναι ένας βασικός τρόπος έμμεσης ή άμεσης μεταβιβάσεως γνώσεων και πληροφοριών μεταξύ τους. Μέσω αυτών, παρέχεται η δυνατότητα προσβάσεως σε «εργαλεία» που παρέχονται δωρεάν και μπορούν να τα κατεβάσουν[87].

[86] J. Holt is a professor in the School of Criminal Justice at Michigan State University whose research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. His work has been published in various journals including Crime and Delinquency, Deviant Behavior, the Journal of Criminal Justice, and Youth and Society.

[87] ProRat Trojan, ProAgent, ProRat cigicilogger & backport, ο πλέον γνωστός Trojian Turkojan 4.0 Gold Edition, ο Trojan Turkojan 2 και η Melissa virus source code.

Όσο κι αν ακούγεται παράξενο, υπάρχει μία ιστοσελίδα (http://www.cyber-warrior.org/), η οποία εμφανίζεται να ανήκει σε οργάνωση και έχει ως έμβλημα τα αρχικά CW88, με το "C" να εμφανίζεται μεγεθυσμένο (πράσινο σε λευκό φόντο) ως ημισέληνος και το "W" ως αστέρι. Αυτό που παρουσιάζει μεγάλο ενδιαφέρον είναι το κείμενο στην τουρκική γλώσσα, όπου κάτω από τον τίτλο "Cyber Warrior Tim" (το Tim είναι η τουρκική απόδοση του αγγλικού team), η μετάφραση του οποίου στην ελληνική παρέχει αρκετά εντυπωσιακά στοιχεία : «Η ομάδα μας, που ιδρύθηκε το 2001, συνεχίζει χωρίς διακοπή το έργο της. Σε αυτή τη χρονική περίοδο, η «Cyber Warrior» «κατέβασε» αρκετές ιστοσελίδες και πέρασε σε εκατοντάδες άτομα την αντίληψη ότι πρέπει να αμύνονται στις επιθέσεις των hackers». Το κείμενο προκαλεί την ευαισθητοποίηση των χρηστών προετοιμάζει το έδαφος για μελλοντική τους κινητοποίηση.

Συνεχίζοντας τη μελέτη του εν λόγω κειμένου, προκύπτει το μάλλον πρωτοφανές φαινόμενο της δράσεως τους με νομική κάλυψη, στοιχεία που καταδεικνύει όχι μόνο την προφανή ανοχή των Αρχών αλλά και την ενθάρρυνσή τους να ενεργούν στο πλαίσιο ενός κρατικού ελέγχου. Για την ακρίβεια, αναφέρεται το ακόλουθο : «Το 2007, ολοκληρώθηκαν οι νόμιμες διαδικασίες, σχετικά με τη δράση της ομάδας μας και έτσι καλύφθηκε το νομικό κενό που υπήρχε. Κατόπιν τούτου, η ομάδα μας συνεχίζει νόμιμα το έργο της από το 2007,στα πλαίσια των νόμων. Από εδώ μπορείτε να δείτε την αποστολή της ομάδας μας και τα μέχρι τώρα πεπραγμένα μας».

Αυτό που είναι ακόμη πιο ενδεικτικό είναι ο τρόπος με τον οποίο είναι οργανωμένοι οι Τούρκοι hackers, ο οποίος έχει όλα τα στοιχεία μιας κανονικής στρατιωτικής δομής. Εκτός από τη δομή, χαρακτηριστική είναι επίσης η χρήση συγκεκριμένων όρων, όπως "istihabarat", που σημαίνει κατασκοπία, η ανάλογη χρήση ενός ακόμη στρατιωτικού όρου, του "logistic destek", που σημαίνει λογιστική υποστήριξη και η ακόμη ενδεικτικότερη χρήση του όρου "akinci", που σημαίνει επιδρομέας, και που είναι ένας παραδοσιακός όρος των Τούρκων, χρησιμοποιούμενος από την εποχή της Οθωμανικής Αυτοκρατορίας μέχρι και σήμερα, κάτι μεταξύ καταδρομέα και επιδρομέα, με τις γνωστές καταστροφικές επιδόσεις.

Τέλος, εξίσου ενδεικτική των τουρκικών ενεργειών θεωρείται η αποκάλυψη, κατά τη δικαστική διερεύνηση της υπόθεσης Ergenekon, ότι το τουρκικό Γενικό Επιτελείο έστησε και διαχειριζόταν σαράντα δύο ιστοσελίδες, ανάμεσα στις οποίες ήταν γνωστοί δικτυακοί τόποι με ιδιαίτερα ανθελληνικό περιεχόμενο. Πρόκειται για τις ιστοσελίδες

[88] Cyber Warrior is a person who engages in cyberwarfare, whether for personal reasons or out of patriotic or religious belief. Cyberwarfare may be pursued either to defend computer and information systems, or to attack them. Cyber-warriors come in different forms, depending on their roles, but all deal with information security in one form or another. https://www.techopedia.com/definition/28615/cyber-warrior

members.tripod.com/camerian-volunteer, greekmurderers.net, cameria.org, yunanli.com και pontuslu.com.

Στην Ελλάδα, τόσο η ΕΥΠ όσο και η τουρκική ΜΙΤ διαθέτουν ειδικές υπηρεσίες που ασχολούνται με τον κυβερνοπόλεμο. Αξίζει να σημειωθεί ότι η μεγαλύτερη στρατιωτική βάση υποκλοπών της Τουρκίας υπάγεται εξολοκλήρου στην ΜΙΤ και έχει λάβει ως πρότυπο τις αμερικανικές αντίστοιχες υπηρεσίες πληροφοριών[89]. Εκεί απασχολούνται αξιωματικοί, πράκτορες των μυστικών υπηρεσιών, επιστήμονες με ειδικές γνώσεις στην σύγχρονη τεχνολογία, ειδικοί εμπειρογνώμονες, γλωσσολόγοι στην αραβική γλώσσα και τεχνικοί που ασχολούνται ειδικά στον κυβερνοχώρο και στη λεγόμενη technical intelligence, την signal intelligence και τις υποκλοπές[90].

Αποτελεί κοινό μυστικό ότι όλες οι επιθέσεις εναντίον ιστοσελίδων ελληνικών κρατικών θεσμών, όπως υπουργεία και υπηρεσίες προέρχονται από τη γειτονική χώρα. Το ίδιο ισχύει και για την επίθεση εναντίον της ιστοσελίδας του Έλληνα πρωθυπουργού. Μπορεί παλαιότερα οι ένοπλες δυνάμεις των δύο χωρών να έφθασαν κοντά στη σύγκρουση, αλλά πλέον τα θερμά επεισόδια είναι τα ψηφιακά.

Μέχρι σήμερα η μεγαλύτερη απειλή υπήρξε η τουρκική ομάδα χάκερ Aslan Neferler Tim[91]. Αυτή ήταν που επιτέθηκε μέχρι και στην ιστοσελίδα του Πρωθυπουργού της Ελλάδας, με αφορμή τις αντιδράσεις στελεχών της ελληνικής πολιτικής ηγεσίας και αρκετών δημοσιογράφων, απέναντι στην πρόθεση να χρησιμοποιηθεί ο ναός της Αγίας Σοφίας στην Κωνσταντινούπολη για μουσουλμανική προσευχή. Φέρεται να είχαν αφήσει το εξής μήνυμα: «Σε μας πέφτει το καθήκον να αντιδράσουμε στην αντίδραση Ελλάδας για την ανάγνωση του Κορανίου στην Αγία Σοφία. Τσίπρα μην εκπλήσσεσαι, μην μας κάνεις να χάσουμε την υπομονή μας».[92]

4.3 Ο Κυβερνοπόλεμος ως Πολλαπλασιαστής Ισχύος για την Ελλάδα

Η χώρα μας, η οποία διατηρεί ανοικτά μέτωπα (Αιγαίο, Κυπριακό, Δυτική Θράκη) με την Τουρκία, από την οποία δέχεται απειλές στον Κυβερνοχώρο ενώ μια μορφή επιθετικού πολέμου σε μια μελλοντική αντιπαράθεση θα πρέπει να θεωρούνται οι επιθέσεις σε

[89] https://slpress.gr/ethnika/o-akirychtos-cyberpolemos-ton-chaker/
[90] http://id-ont.blogspot.gr/2017/12/blog-post_43.html
[91] https://katohika.gr/diethni/o-akirixtos-kivernopolemos-ton-xaker/
[92] http://www.triklopodia.gr/tourkoi-xakers-riksame-istoselida-ellina-prothipourgou-tsipra-kaneis-xasoume-ipomoni-mas-ul/

στρατιωτικά και κυβερνητικά δίκτυα ηλεκτρονικών υπολογιστών. Για τον λόγο αυτό είναι αναγκαία η προετοιμασία για αυτό το είδος πολέμου.

Για να δούμε πως θα μπορούσε να χαρακτηρισθεί δυναμική μια αντιπαράθεση στα πλαίσια του Κυβερνοχώρου και για την ανάδειξη της δυναμικής που παρέχουν τα αποτελέσματα του Κυβερνοπολέμου «ως πολλαπλασιαστή ισχύος» μεταξύ δυνητικά αντιπάλων δυνάμεων θα πρέπει να μελετήσουμε κάποιες απόψεις και γνώμες, που έχουν κατά καιρούς διατυπωθεί από ειδικούς του χώρου :

Άρθρο στην εφημερίδα Washington Post[93] την άνοιξη του 1998 περιγράφει την ανησυχία που προκάλεσε η διείσδυση με το κατάλληλο λογισμικό σε στρατιωτικά δίκτυα κατά τη διάρκεια ασκήσεως ενώ ομάδα της NSA (Εθνική Υπηρεσία Ασφαλείας), χρησιμοποιώντας λογισμικό από σελίδες του Internet που απευθύνονταν σε hackers, κατάφερε να θέσει εκτός λειτουργίας εντός ημερών το δίκτυο ηλεκτρικής ενέργειας των ΗΠΑ και να διεισδύσει σε μεγάλης σπουδαιότητας στοιχεία του ΣΔΕΠ της Διοικήσεως Ειρηνικού. Ταυτόχρονα, η ομάδα αυτή κατόρθωσε να αποτρέψει τον εντοπισμό της στην συντριπτική πλειοψηφία των περιπτώσεων.

Το σύστημα που περιέχει, τους μηχανισμούς συλλογής πληροφοριών, επεξεργασίας τους, τους μηχανισμούς αξιολόγησης και λήψης αποφάσεων, τις διαδικασίες πρόβλεψης και χειρισμού κρίσεων, τους μηχανισμούς εξασφάλισης της παθητικής αμυντικής ασφάλειας των πληροφοριών μέσα από το πρίσμα της κρυπτογραφίας, και της ενεργητικής ασφάλειας της μέσα από το πρίσμα της κρυπτανάλυσης, αποτελεί «εθνικό όπλο» ύψιστης στρατιωτικής σημασίας για την άσκηση εξωτερικής και αμυντικής πολιτικής.

Επίσης, είναι φανερό ότι ο κάτοχος της «πληροφορίας» είναι και ο κυρίαρχος του παιχνιδιού, αλλά και η διαχείριση της πληροφορίας είναι το ισχυρότερο όπλο. Η πληροφορία αντιπροσωπεύει την ήπια μορφή ισχύος που διαθέτει ένα κυρίαρχο κράτος, η οποία όμως είναι αποτελεσματικότερη της σκληρής ισχύος, δηλαδή της στρατιωτικής δύναμης του εν λόγω κράτους. Συνεπώς, για να επιβληθεί κανείς δεν είναι απαραίτητο να είναι στρατιωτικά ισχυρός, αλλά αρκεί να μπορεί να διαχειριστεί έξυπνα την «πληροφορία», δηλαδή να μπορεί να «πείσει» απευθυνόμενος στο «λογικό» του ανθρώπου.

Το διαδίκτυο είναι ο πλέον κατάλληλος χώρος για το «παιχνίδι της διαχείρισης της πληροφορίας», διότι είναι ο χώρος που τη «βλέπουμε», την «κατανοούμε», την «εκλογικεύουμε» και έτσι αυτή «ενσωματώνεται». Δεδομένου ότι οι κοινωνικές συμπεριφορές μπορούν να προβλεφθούν, ο συναισθηματικός καταναγκασμός, δηλαδή ένα

[93] http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm

είδος ψυχολογικών επιχειρήσεων, μπορεί να είναι ο πλέον αποτελεσματικός πόλεμος, μίας «μικρής» χώρας κατά μίας άλλης μεγαλύτερής της, δηλαδή της Ελλάδας κατά της Τουρκίας, χρησιμοποιώντας τον κυβερνοπόλεμο ως πολλαπλασιαστή της ισχύος της.

Στον κυβερνοπόλεμο, πυρήνας στο πεδίο της μάχης δεν θεωρείται η χρήση βίας, αλλά οι σκέψεις και τα συναισθήματα που προκαλούνται από τη διακίνηση των πληροφοριών. Τυπικά, οι σχετικοί όροι περιγράφουν μία ψυχολογικής έντασης μάχη, συγκριτικά με την παραδοσιακή της σωματικής έντασης, ή αργότερα της μάχης μέσω των μηχανών που εξακολουθούσαν να στοχεύουν ύλη και όχι μυαλό ή καρδιά.

Μία από τις βασικές αιτίες επιλογής αυτού του είδους μάχης αποτελεί το οικονομικό συμφέρον. Σίγουρα οι σφαίρες είναι πιο ακριβές από το χαρτί και τα αεροσκάφη από τον ηλεκτρονικό υπολογιστή. Αυτό είναι και το πλεονέκτημα στην περίπτωση της Ελλάδας, διότι δίνοντας έμφαση σε πολλαπλασιαστές ισχύος, όπου επενδύοντας «λίγα» έχεις τη δυνατότητα να πετύχεις «πολλά», και αυτό σημαίνει να επενδύσει στον κυβερνοπόλεμο, μπορεί να κάνει αποτελεσματικότερη διαχείριση και χρήση των αμυντικών της δαπανών, γεγονός τεράστιας σημασίας εφόσον τα κονδύλια που διατίθενται για τις αμυντικές δαπάνες είναι περιορισμένα και ειδικά στην παρούσα περίοδο, λόγω οικονομικής κρίσης. Συνεπώς, με χαμηλότερο κόστος, σε σχέση με τη χρήση άλλων όπλων, να έχει το μέγιστο δυνατό όφελος.

Η Ελλάδα, έχοντας ως μόνιμη στρατιωτική απειλή για την κυριαρχία της, την Τουρκία, δεν έχει άλλη επιλογή, παρά να «παίξει» ασύμμετρα, εκμεταλλευόμενη τα πλεονεκτήματά της και μειώνοντας τα πλεονεκτήματα του αντιπάλου της, σκοπεύοντας στην «αχίλλειο πτέρνα» του, που όπως σε κάθε σύγχρονη κοινωνία, είναι η ολοένα και αυξανόμενη «δικτύωση» μέσω ηλεκτρονικών πληροφορικών συστημάτων, τόσο της κοινωνίας της Τουρκίας, όσο και των ενόπλων δυνάμεών της. Οι ελληνικές ένοπλες δυνάμεις βρίσκονται πάντα σε ιδιαίτερη ετοιμότητα. Τα τελευταία χρόνια, μάλιστα, έχουν γίνει πολλά βήματα, κυρίως στον τομέα της κυβερνοάμυνας.[94]

Το Κέντρο Αντιμετώπισης Κυβερνοπεριστατικών (ΚΑΚ) που υπάγεται στην Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ (ΔΙΚΥΒ), έχει ως αντικείμενο την προστασία των κρίσιμων Συστημάτων Επικοινωνιών και Πληροφορικής (ΣΕΠ) (Communication and Information Systems, CIS). Το Κέντρου Αντιμετώπισης Κυβερνοπεριστατικών, παρακολουθεί σε 24ώρη βάση τη σωστή λειτουργία όλων των στρατιωτικών δικτύων, εντοπίζει κυβερνοπεριστατικά και θα προβαίνει στις απαραίτητες ενέργειες για την αντιμετώπισή τους.

[94] https://slpress.gr/ethnika/o-akirychtos-cyberpolemos-ton-chaker

Στην εφαρμογή Κυβερνοάμυνας, εκτός από τις άνωθι τεχνολογίες, το ΚΑΚ υλοποιεί τα ακόλουθα βήματα και δράσεις:

- Εκτίμηση Τρωτοτήτων (Vulnerability Assessment) σε περιοδική βάση.
- Εφαρμογή ασφαλούς αρχιτεκτονικής των δικτύων με χρήση τριών (3) επιπέδων δικτύων [Demilitarized Zone (DMZ), ενδιάμεσα και εσωτερικά δίκτυα] και ταυτόχρονα κατάλληλη ρύθμιση των δρομολογητών (routers) και των εξυπηρετητών DNS, έτσι ώστε να υπάρχει πλήρης έλεγχος της κυκλοφορίας.
- Περιοδική εκτέλεση ελέγχων διείσδυσης (penetration testing) και ασκήσεων κυβερνοεπιθέσεων από κατάλληλα εκπαιδευμένες ομάδες (red teams) σε όλα τα συστήματα ΣΕΠ.

Παρ' όλα αυτά, οι ανωτέρω υποδομές δεν θα μπορούσαν ποτέ να αρκέσουν, εάν δεν συνοδεύονται από κατάλληλη ευαισθητοποίηση του μέσου χρήστη ίντερνετ, μέσα από ενημερωτικές καμπάνιες σχετικά με ασφαλή χρήση του διαδικτύου, καθότι ο ανθρώπινος παράγοντας αποτελεί το μεγαλύτερο ποσοστό κινδύνου αναφορικά με εισχώρηση εχθρικών στοιχείων.[95]

[95] https://securityreport.gr/magazine-archive/year-2015/item/1087-kyvernopolemos-kai-ellada

Σελίδα σκόπιμα κενή

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ
ΣΥΜΠΕΡΑΣΜΑΤΑ

5.1 Γενικά

Εάν θέλουμε να συνοψίσουμε τη σημασία του Κυβερνοπολέμου ,τις δυνατότητες του και το μέλλον που βρίσκεται μπροστά μας τόσο σε παγκόσμιο όσο και σε εθνικό επίπεδο θα πρέπει να λάβουμε υπόψη τα παρακάτω σημεία[96]:

α. Η εποχή που οι υπολογιστές και τα δίκτυα αυτών ήταν προνόμιο των κρατικών υποδομών έχει περάσει και πλέον όλοι έχουν τη δυνατότητα να εκμεταλλευθούν τις δυνατότητες που παρέχει ο κυβερνοχώρος, όχι μόνο με τη νόμιμη διαδικασία. Έτσι δίνεται η δυνατότητα προσβολής κρίσιμων υποδομών μιας χώρας, καταστρέφοντας σταθμούς παραγωγής ηλεκτρικής ενέργειας ή ανοίγοντας φράγματα υδάτων.

β. Η απειλή του Κυβερνοπολέμου είναι υπαρκτή, πραγματική, τα Κυβερνοόπλα είναι ευρέως διαθέσιμα και εξελίσσονται ταχύτατα, και οι επιθέσεις βρίσκονται σε εξέλιξη.

γ. Ο Κυβερνοχώρος μπορεί να περιγραφεί ως ένα άναρχο σύστημα το οποίο περιλαμβάνει τη δραστηριότητα χάκερ, ακτιβιστών - χάκερ, οργανωμένου εγκλήματος, καθώς και δραστηριότητες βιομηχανικής κατασκοπίας, τρομοκρατικών οργανώσεων .

δ. Η εφαρμογή των επιχειρήσεων του κυβερνοπολέμου πρέπει να διέπεται από δίκαιο όπως αυτό εφαρμόζεται στις διεθνείς συμφωνίες. Προς το παρόν, πολλά κρίσιμα θέματα που σχετίζονται με τον Κυβερνοπόλεμο παραμένουν άλυτα. Σήμερα, δεν υπάρχει κανένα διεθνές, νομικά δεσμευτικό εργαλείο, το οποίο να χαρακτηρίζει την Κυβερνοεπίθεση απειλή για την εθνική ασφάλεια μιας χώρας.

ε. Ο Κυβερνοπόλεμος είναι ένας από τους τέσσερις πυλώνες[97] ισχύος του κράτους (οικονομία, διπλωματία και στρατιωτική ισχύς) και συνεπώς εντάσσεται στη σχεδίαση της Υψηλής Στρατηγικής ενός κράτους προκειμένου να υλοποιηθεί ο πολιτικός σκοπός σε σχέση με κάποιον αντίπαλο.

στ. Πολιτικοί σκοποί, οι οποίοι θα μπορούσαν να επιδιωχθούν με την αποκλειστική προσφυγή στον Κυβερνοπόλεμο, είναι η απλή παρενόχληση, η προειδοποίηση χώρας πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών για τους κινδύνους που

[96] http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-stratigiki
[97] http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe

διατρέχει αν αρνηθεί τη θετική ψήφο καθώς και η αντίδραση για πράξεις που έγιναν χωρίς να ληφθούν υπόψη τα συμφέροντα της ενδιαφερόμενης χώρας[98].

ζ. Αποστολή του Κυβερνοπολέμου είναι η ασφάλεια των κρίσιμων υποδομών του κράτους παρέχοντας προστασία σε όλα τα κεντρικά συστήματα, δημόσιων και ιδιωτικών, από ενδεχόμενες επιθέσεις υποβάθμισης της λειτουργίας τους και πρόκληση λειτουργικών ή φυσικών βλαβών, και η διενέργεια βλαβών στον αντίπαλο, όπως χαράσσει η εθνική στρατηγική ασφάλεια.

η. Οι στόχοι του Κυβερνοπολέμου, κατά σειρά φθίνουσας σοβαρότητας, είναι :

(1) Οι κρίσιμες υποδομές μιας χώρας.

(2) Ο επηρεασμός της παγκόσμιας κοινής γνώμης μέσω του πληροφοριακού πολέμου.

(3) Τα συστήματα επικοινωνιών και πληροφορικής των Ενόπλων Δυνάμεων.

θ. Αποτελεί το παρόν και το μέλλον του σύγχρονου πολέμου. Τα διαδικτυακά όπλα αυξάνονται ανεξέλεγκτα, ραγδαία και επικίνδυνα μέρα με τη μέρα, ενώ, παράλληλα, «το σχοινί που κρατάει την ασφάλεια του διαδικτύου συμπαγή έχει αρχίσει να μετατρέπεται σε κλωστή». Ο «κυβερνοπόλεμος» έχει πάρει πλέον τα "ηνία" στον πόλεμο της πληροφορίας καθώς, στο όνομά του, ξοδεύονται τρισεκατομμύρια δολάρια, ενώ αποτελεί μία από τις πιο ανελισσόμενες και σημαντικές απειλές για τη διεθνή ασφάλεια και ειρήνη. Έχοντας ξεπεράσει το όριο της «εικονικής υπόστασης», έχοντας προκαλέσει φυσικές, απτές και τρομακτικές καταστροφές σε μία εποχή που όλα είναι ηλεκτρονικά, ο «κυβερνοπόλεμος» ήρθε για να μείνει και, μοιραία, να κυριαρχήσει[99].

ι. 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 :

(1) Αποτελεί έναν πολλαπλασιαστή ισχύος, μικρού σχετικά κόστους και μεγάλα αποτελέσματα, στον οποίο πρωτεύοντα ρόλο παίζει η εφευρετικότητα και η πρωτοτυπία.

(2) 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.

[98] http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe
[99] https://powerpolitics.eu/cyber-warfare ο πόλεμος που δεν βλέπεις

(3) 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, 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).

(4) 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.

(5) Ο σκληρός κυβερνοπόλεμος με τη μορφή της κυβερνοτρομοκρατίας (cyberterrorism[100]) ή με τη γενικότερη έννοιά του που εκφράζεται με τον νέο όρο «κυβερνοέγκλημα» (cybercrime[101]), έχει σαν σκοπό την ολική καταστροφή των δικτύων επικοινωνίας του αντιπάλου οργανισμού ή κράτους, έτσι ώστε να παραλύσουν οι ζωτικές λειτουργίες του, με βλάβες οι οποίες είναι δύσκολο να αποκατασταθούν άμεσα.

(6) Η Κυβερνοάμυνα απαιτεί μία σειρά από μηχανισμούς, διαδικασίες και συνεχώς ανεπτυγμένες και δοκιμασμένες δυνατότητες, με σκοπό την πρόληψη, τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση, την αποκατάσταση και την εξαγωγή συμπερασμάτων, στην περίπτωση των κυβερνοεπιθέσεων, που έχουν σαν στόχο να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριακών υποδομών.[102]

(7) Υποστηρικτές της Πληροφοριακής Κοινωνίας εκτιμούν ότι, η ανάδειξη του Κυβερνοχώρου ουσιαστικά δεν υπόκειται σε γεωγραφικούς περιορισμούς, ως παράγοντας μιας εθνικής πολιτικής ταυτότητας, όσο και ως διάσταση του πολέμου και της στρατηγικής.

---

[100] Είναι η χρήση του Διαδικτύου για τη διεξαγωγή βίαιων πράξεων που έχουν ως αποτέλεσμα, ή απειλούν, απώλεια ζωής ή σημαντική σωματική βλάβη, προκειμένου να επιτευχθούν πολιτικά οφέλη μέσω εκφοβισμού . Θεωρείται επίσης μερικές φορές ως πράξη τρομοκρατίας στο Διαδίκτυο, όπου οι τρομοκρατικές δραστηριότητες, συμπεριλαμβανομένων πράξεων σκόπιμης, μεγάλης κλίμακας διαταραχών των δικτύων υπολογιστών, ιδίως των προσωπικών υπολογιστών που συνδέονται με το Διαδίκτυο μέσω εργαλείων όπως ιούς υπολογιστών, ιούς τύπου worms ή άλλα κακόβουλα σενάρια είναι μεταχειρισμένα.

[101] Το έγκλημα στον κυβερνοχώρο ή το έγκλημα που σχετίζεται με τον υπολογιστή είναι εγκληματικότητα που περιλαμβάνει υπολογιστή και δίκτυο . Ο υπολογιστής μπορεί να έχει χρησιμοποιηθεί για τη διάπραξη εγκλήματος ή μπορεί να είναι ο στόχος. Τα εγκλήματα στον κυβερνοχώρο μπορούν να οριστούν ως: «Αδικήματα που διαπράττονται κατά ατόμων ή ομάδες προσώπων με ποινικό κίνητρο για να προξενήσουν σκόπιμα τη φήμη του θύματος ή να προκαλέσουν σωματική ή πνευματική βλάβη ή απώλεια στο θύμα, άμεσα ή έμμεσα, σύγχρονα τηλεπικοινωνιακά δίκτυα όπως το Διαδίκτυο (δίκτυα που περιλαμβάνουν αλλά όχι μόνο αίθουσες συνομιλίας, ηλεκτρονικά μηνύματα, πίνακες ανακοινώσεων και ομάδες) και κινητά τηλέφωνα (Bluetooth / SMS / MMS). Το έγκλημα στον κυβερνοχώρο ενδέχεται να απειλήσει την ασφάλεια ενός ατόμου ή τη χρηματοοικονομική του κατάσταση.

[102] http://www.armynow.net/askisi-panoptis-ola-ta-senaria-kybernopolemou/

Ωστόσο μέσα από τις αλλαγές που επιφέρει η Πληροφοριακή Επανάσταση και ο Κυβερνοπόλεμος αποδεικνύεται , ότι η γεωγραφία συνεχίζει να αποτελεί μια σημαντική διάσταση της πολιτικής και της παγκόσμιας ασφάλειας.

(8) 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.

(9) 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.

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.

ια. Σε αντίθεση με τον συμβατικό πόλεμο οι εμπλεκόμενοι στις επιχειρήσεις του κυβερνοπολέμου και ιδιαίτερα οι μη κρατικοί παράγοντες διεκδικούν σημαντικό μερίδιο στη χρήση βίας διότι το κόστος είναι χαμηλό και η απόκτηση δυνατοτήτων και λογισμικού είναι πλέον πολύ φτηνή. Κατά τη διάρκεια αυτού του είδους πολέμου δεν καταλαμβάνεται εχθρικό έδαφος ούτε επιτυγχάνεται η καταστροφή εξ ολοκλήρου του αντιπάλου ούτε αφοπλισμός αυτού. Επιτυγχάνεται όμως ο περιορισμός στην ελευθερία στις κινήσεις των αντιπάλων στον κυβερνοχώρο μέσα σε συγκεκριμένα χρονικά πλαίσια καθώς και ο αιφνιδιασμός αυτού. Αποτελεί δηλαδή ένα είδος πολέμου ελιγμού.

ιβ. Η Παγκοσμιοποίηση περιπλέκει το θέμα του Κυβερνοπολέμου, σε σχέση με την προσβολή των κρίσιμων υποδομών μιας χώρας. Η επιλογή των στόχων θα πρέπει να γίνεται με ιδιαίτερη προσοχή και περίσκεψη, προκειμένου να μην προκαλέσει ζημιά σε τρίτες χώρες των οποίων οι υποδομές εξαρτώνται ή απλώς συνδέονται με τις υποδομές της χώρας – στόχου. Αυτό με τη σειρά του μπορεί να προκαλέσει επί τούτου (ad hoc) δημιουργία συμμαχιών για να ανατρέψει την υφιστάμενη κατανομή ισχύος οδηγώντας σε αρνητικά αποτελέσματα για τον επιτιθέμενο.

ιγ. Δεν είναι απίθανη η εμφάνιση ολοκληρωτικού ή περιορισμένου Κυβερνοπολέμου μεταξύ δύο αντιμαχόμενων, αλλά ακόμη πιθανότερη είναι η κλιμάκωσή του με την προσφυγή στον κλασικό πόλεμο, για την επίτευξη αποφασιστικών αποτελεσμάτων και την οριστική επίλυση της διένεξης.

ιδ. Ο Κυβερνοπόλεμος διεθνώς έχει πάρει τεράστιες διαστάσεις και οι περισσότερες χώρες επιδεικνύουν έντονη δραστηριότητα προκειμένου να επικρατήσουν στο χώρο. Για την επίτευξη των παραπάνω επενδύουν σε εξειδικευμένο προσωπικό, εκπαίδευση, σύγχρονες δομές και υλικό, στα πρέπει να επενδύσει και η χώρα μας[103].

ιε. Μέσα από τον Κυβερνοχώρο δίνεται η δυνατότητα κρατικοί και μη δρώντες να μπορέσουν να μειώσουν και τα πλεονεκτήματα των αντιπάλων και κατά προτίμηση των πιο ισχυρών από αυτούς σε ότι αφορά την συμβατική στρατιωτική ισχύ. Ιδιαίτερα όταν μέσα στο παγκόσμιο περιβάλλον υπάρχει ασυμμετρία μεταξύ δυο κρατών στην ισχύ τους τότε, ο Κυβερνοπόλεμος είναι η πιο ιδεατή λύση για το μέρος εκείνο της αντιπαράθεσης που είναι λιγότερο ισχυρό, διότι με τον τρόπο αυτό εκμεταλλευόμενο έναν γρήγορο, σχετικά φτηνό και αποτελεσματικό τρόπο μπορεί να υπονομεύσει τις κρίσιμες αλλά τρωτές υποδομές του αντιπάλου .

ιστ. Η χρήση του διαδικτύου από τρομοκρατικές οργανώσεις έχει πλέον διευρυνθεί σε μεγάλο βαθμό προκειμένου να χρησιμοποιηθεί αυτό για μια μεγάλη ποικιλία στόχων και σκοπών χωρίς να αποκλείεται και η πρόκληση μέσω των ενεργειών αυτών και της απώλειας ανθρώπινης ζωής. Με τα μέχρι σήμερα δεδομένα, το ίδιο το διαδίκτυο δεν αποτελεί στόχο και ακόμα δεν έχει εντοπιστεί «ηλεκτρονική» τρομοκρατική οργάνωση, η οποία να διαθέτει την ικανότητα και τα μέσα να εξαπολύσει μια Κυβερνοεπίθεση στο διαδίκτυο με στόχο τη διακοπή της λειτουργίας του και την καταστροφή του. Οι λόγοι για τους οποίους οι Κυβερνοεπιθέσεις δεν αποτελούν λύσεις για τις τρομοκρατικές οργανώσεις είναι :

(1) Η επίπτωση των Κυβερνοόπλων δεν είναι το ίδιο αποτελεσματική εάν συγκριθούν με άλλες κατηγορίες όπλων, διότι δεν επιφέρουν τις ίδιες ψυχολογικές ή πολιτικές επιπτώσεις και επιπλέον δεν έχουν νεκρούς.

(2) Η χρήση για την επίθεση μέσω διαδικτύου σε κρίσιμες υποδομές αποτελεί μία ενέργεια που είναι πολύπλοκη και δεν επιφέρει εξασφαλισμένη επιτυχία.

(3) Το διαδίκτυο εξυπηρετεί και τους δικούς τους σκοπούς για την εξάπλωση των ιδεών και των αντιλήψεων καθώς και για τον προσηλυτισμό νέων μελών.

[103] http://www.geetha.mil.gr/media/adispo/ANAKOINOSEIS/imerida/CYBERWAR/DELTIA/conclusions.pdf

ιζ. Προκειμένου να αντιμετωπιστεί η εξελισσόμενη απειλή του Κυβερνοπολέμου είναι απαραίτητες σοβαρές και συνεπείς επενδύσεις πάνω στη νέα τεχνολογία, καθώς και συνεργασία με τα Εκπαιδευτικά Ιδρύματα της εντός και εκτός της χώρας.

ιη. Σήμερα ο κυβερνοπόλεμος εστιάζεται στον οικονομικό, κυρίως, έλεγχο μιας χώρας ώστε να επηρεαστεί η ισχύς της χώρας. Οι κρίσιμες υποδομές και οι βασικοί πόροι αντιμετωπίζουν σήμερα σημαντικές απειλές, κυρίως λόγω της εκτεταμένης χρήσης του διαδικτύου και της υιοθέτησής του ως κύριας επικοινωνιακής πλατφόρμας[104].

ιθ. Η οργάνωση ενός Κράτους η μιας συγκροτημένης οντότητας, η οποία αποτελεί στόχο, είναι η βασική προϋπόθεση προκειμένου να επιλεγεί ως στόχος Κυβερνοπολέμου. Έτσι με αυτήν την παραδοχή μπορούμε να θεωρήσουμε ότι μόνο τα κράτη ή οι υπερεθνικές οργανώσεις κρατών (συμμαχίες) αποτελούν στόχο επιχειρήσεων Κυβερνοπολέμου. Δεν μπορεί να υπάρξει απειλή ή η χρήση βίας στο πλαίσιο του Κυβερνοπολέμου, εναντίον χωρών με φτωχή επικοινωνιακή και πληροφοριακή υποδομή, εάν αυτή δεν συνοδεύεται με απειλή ή χρήση παραδοσιακού πολέμου.

κ. Η επιτυχής διεξαγωγή επιχειρήσεων Κυβερνοπολέμου προϋποθέτει αντίληψη των απαιτήσεων της νέας αυτής μορφής πολέμου, στενή συνεργασία των φορέων εμπλέκονται, σε εθνικό και διεθνές επίπεδο.

κα. Η Τουρκία, η FYROM, η Αλβανία, η Βουλγαρία, η Μεγάλη Βρετανία, η Ιταλία, η Γαλλία, οι ΗΠΑ, η Ρωσία, η Κίνα, η Γεωργία και η Al Qaeda θα πρέπει να αποτελέσουν οι στόχοι ενδιαφέροντος των υποδομών που ασχολούνται με τον κυβερνοχώρο.

κβ. Το υπάρχων διεθνές νομικό πλαίσιο δεν θέτει περιορισμούς ή απαγορεύσεις στις επιχειρήσεις Κυβερνοπολέμου. Θα πρέπει όμως η εφαρμογή τους να υπόκειται σε νομικούς περιορισμούς με κοινή απόφαση των κρατών μέσα στα στενά πλαίσια των διεθνών συμφωνιών. Πολλά κρίσιμα θέματα που σχετίζονται με τον Κυβερνοπόλεμο δεν έχουν λυθεί για την παρούσα περίοδο και αυτό διακρίνεται εύκολα, καθόσον μέχρι σήμερα δεν υπάρχει κανένα διεθνές, νομικά δεσμευτικό, κείμενο ή εργαλείο από το οποίο να φαίνεται, ότι μια Κυβερνοεπίθεση αποτελεί απειλή για την εθνική ασφάλεια μιας χώρας. Πυλώνες της ισχύος ενός κράτους είναι η οικονομία, η διπλωματία και η στρατιωτική ισχύς[105]. Ο Κυβερνοπόλεμος αποτελεί τον τέταρτο πυλώνα ισχύος του κράτους και ως εκ τούτου αποτελεί εργαλείο και μέσο για τη σχεδίαση της Υψηλής Στρατηγικής ενός κράτους προκειμένου να επιτευχθεί ο καθοριζόμενος πολιτικός σκοπός σε σχέση με κάποιον αντίπαλο. Η αποκλειστική προσφυγή στον Κυβερνοπόλεμο θα αποτελούσε μια απλή παρενόχληση, η

[104] http://www.geetha.mil.gr/media/adispo/ANAKOINOSEIS/imerida/CYBERWAR/DELTIA/conclusions.pdf
[105] http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe/

προειδοποίηση χώρας πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών για τους κινδύνους που διατρέχει, αν αρνηθεί τη θετική ψήφο και η εκδίκηση για τυχόν αποφάσεις που ελήφθησαν χωρίς να ληφθούν υπόψη τα συμφέροντα της ενδιαφερόμενης χώρας.

Η συνεχής βελτίωση των τηλεπικοινωνιών με τις υψηλές ταχύτητες στο διαδίκτυο, επιτρέπουν τη συνεχή σύνδεση στο διαδίκτυο των προσωπικών μας Η/Υ με μεγάλες δυνατότητες με αποτέλεσμα να τίθεται θέμα ασφαλείας, διότι 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.

5.2 Ενέργειες που πρέπει να γίνουν σε Εθνικό επίπεδο[106]

α. Μονομερής δήλωση από την Ελλάδα ότι θεωρεί τον Κυβερνοχώρο μέρος όπου ασκεί εθνική κυριαρχία. Προς υποστήριξη της δήλωσης να ασκήσει έλεγχο στα Κυβερνοσύνορα, εξασφαλίζοντας μέσα για την απαγόρευση της κίνησης του διαδικτύου που προέρχεται από Υπηρεσίες Παροχής Υπηρεσιών (ISP) ή χώρες από τις οποίες προέρχονται οι Κυβερνοεπιθέσεις.

β. Υιοθέτηση - αναθεώρηση – συμπλήρωση του εθνικού νομικού πλαισίου που αφορά στη δραστηριότητα στον Κυβερνοχώρο.

γ. Σύναψη διμερών συμφωνιών με άλλες χώρες για την παροχή υποστήριξης στον εντοπισμό του ίχνους των Κυβερνοεπιθέσεων στην πηγή τους, έτσι ώστε να εντοπιστούν οι δράστες και να προσαχθούν σε δίκη ή να εκδοθούν.

δ. Συνεργασία στο πλαίσιο του ΟΗΕ με σκοπό :

- Την καθιέρωση κοινά αποδεκτών αρχών οι οποίες θα ρυθμίζουν τη δραστηριότητα στον Κυβερνοχώρο.
- Την αναθεώρηση του δικαίου του πολέμου έτσι ώστε να λαμβάνει υπόψη του τον ήδη διεξαγόμενο Κυβερνοπόλεμο.

ε. Σύνταξη μελέτης για το πόσο ευπαθής είναι η κρίσιμη υποδομή διαστήματα, έτσι για την οργάνωση αποτελεσματικής άμυνας εναντίον ενδεχόμενων Κυβερνοεπιθέσεων.

θ. Συνεργασία δημοσίου και ιδιωτικού τομέα.

5.3 Μέτρα που πρέπει να ληφθούν σε στρατηγικό – επιχειρησιακό επίπεδο (εθνικά)[107]

[106] http://www.warandstrategy.gr/images/Article-Images/ Κυβερνοπόλεμος και Εθνική Στρατηγική.

α. Μελέτη και σύνταξη κατάλληλου δόγματος Κυβερνοάμυνας – Κυβερνοπολέμου της χώρας, και παρουσίασή του σε κυβερνητικό επίπεδο με εκτεταμένη δημοσιογραφική κάλυψη.

β. Σύνταξη της Εθνικής Πολιτικής Κυβερνοασφάλειας και Κυβερνοπολέμου, όπως επίσης και της Εθνικής Στρατηγικής Κυβερνοασφάλειας και Κυβερνοπολέμου.

γ. Γενικότερα, για την προστασία των κρίσιμων υποδομών και των βασικών πόρων απαιτείται:

- Διαρκής εκπαίδευση για απόκτηση γνώσεων και ευαισθητοποίηση.
- Εφαρμογή βέλτιστων πρακτικών και διαδικασιών διασφάλισης.
- Ανάπτυξη και βελτίωση συστήματος διαχείρισης ασφάλειας πληροφοριών.
- Συμμόρφωση με πρότυπα ασφάλειας πληροφοριών και σχετική πιστοποίηση.[108]

δ. Μελέτη των δημόσιων και ιδιωτικών υποδομών της χώρας και έκδοση εγγράφου με τις κρίσιμες υποδομές οι οποίες χρήζουν προστασίας, κατά το πρότυπο των ΗΠΑ[109] και άλλων χωρών (Ολλανδία, Αυστραλία). Διεξαγωγή περιοδικών ελέγχων και δοκιμών για τον εντοπισμό της τρωτότητας των υποδομών, και του τρόπου αποκατάστασής της.

ε. Αναδιοργάνωση των σημείων διασύνδεσης της χώρας μας στο διαδίκτυο ώστε να είναι δυνατή η απομόνωση της χώρας σε περίπτωση που δεχθεί Κυβερνοεπίθεση μεγάλης κλίμακας, και ελεγχόμενη επανασύνδεση στο διαδίκτυο μετά τη διασφάλιση της απόκρουσης της απειλής.

στ. Απομόνωση όλων των στρατιωτικών δικτύων επικοινωνιών και πληροφορικής από το διαδίκτυο, και αυστηρή τήρηση των υφιστάμενων κανόνων ασφαλείας.

ζ. Σχεδίαση και υλοποίηση ενός μακροπρόθεσμου ερευνητικού προγράμματος για την ανακάλυψη Κυβερνοόπλων, σύμφωνα με τις ελληνικές επιχειρησιακές απαιτήσεις που θα συνταχθούν από όλους τους εμπλεκόμενους φορείς, υπό την αιγίδα της Διοίκησης Κυβερνοπολέμου.

η. Μελέτη της τρωτότητας των ελληνικών συστημάτων επικοινωνιών και πληροφορικής, όπως επίσης και των υποδομών που υποστηρίζονται από ανάλογα συστήματα, και οργάνωση της άμυνάς τους με βάση ένα μακροπρόθεσμο σχέδιο.

θ. Καθορισμό Κανόνων Εμπλοκής Κυβερνοπολέμου.

---

[107] Κυβερνοπόλεμος και Εθνική Στρατηγική Π.Μαυρόπουλος http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-stratigiki

[108] http://www.geetha.mil.gr/media/adispo/ANAKOINOSEIS/imerida/CYBERWAR/DELTIA/conclusions.pdf

[109] Οι ΗΠΑ τον Οκτώβριο του 1997 εξέδωσαν για πρώτη φορά το Critical Foundation, Protecting America's Infrastructures, το οποίο έκτοτε αναθεωρούν τακτικά. Διαθέσιμο στην ιστοσελίδα http://fas.org/sgp/library/pccip.pdf, (τελευταία επίσκεψη την 20 Φεβ 2012).

ι. Τροποποίηση της διαδικασίας Αμυντικής Σχεδίασης, έτσι ώστε να περιλάβει θέματα Κυβερνοπολέμου, με τη σύσταση σχετικής υποεπιτροπής, έτσι ώστε να σχεδιαστεί ορθολογικά η απόκτηση μελλοντικών δυνατοτήτων Κυβερνοπολέμου.

Επίλογος

Η επιστήμη του πολέμου έχει προ πολλού εισέλθει στην εποχή της πληροφορικής. Τα θέματα του Κυβερνοπολέμου παρουσιάζουν αυξητικό εθνικό ενδιαφέρον και ανησυχία. Όλες οι πολιτικές και στρατιωτικές αντιπαραθέσεις έχουν πλέον μια Κυβερνοδιάσταση, της οποίας η έκταση και οι επιπτώσεις είναι δύσκολο να προβλεφθούν.

Οι δράστες των Κυβερνοεπιθέσεων έχουν στη διάθεσή τους μια μεγάλη ποικιλία αποτελεσματικών στρατηγικών και τακτικών Κυβερνοπολέμου. Την τελευταία δεκαετία, η σημασία των επιχειρήσεων στον Κυβερνοχώρο έχει γίνει εμφανέστερη.

Η εξέλιξη αυτή θα μπορούσε να θέσει σε κίνδυνο την εθνική μας ασφάλεια, αν οι Κυβερνοεπιθέσεις στρεφόταν εναντίον στρατιωτικών, κυβερνητικών ή κρίσιμων υποδομών δικτύων επικοινωνιών και πληροφορικής. Κατά συνέπεια, θα πρέπει να επικεντρωθούμε στην ανάπτυξη δυνατοτήτων οι οποίες θα μας επιτρέψουν να εισέλθουμε δυναμικά στον Κυβερνοχώρο και να προστατευθούμε έναντι ενδεχόμενων Κυβερνοαπειλών[110].

Ο κίνδυνος η Ελλάδα να βρεθεί απροετοίμαστη, όσον αφορά στη διασφάλιση των πλέον κρίσιμων εθνικών συμφερόντων στο μελλοντικό περιβάλλον ασφαλείας είναι, αν όχι σίγουρος, τουλάχιστον ορατός. Και μόνο το γεγονός, ότι η Τουρκία έχει ήδη οργανώσει από ετών το δικό της Κέντρο Κυβερνοπολέμου, σημαίνει πολλά για τη διαφορά επιπέδου όσον αφορά στη σοβαρότητα αντιμετώπισης του θέματος, την αξιολόγησή του, την ποιότητα του στελεχιακού δυναμικού και την ταχύτητα λήψης αποφάσεων. Ο Clausewitz, με τη διορατικότητα και την αναλυτική του σκέψη, διέβλεψε ότι «κάθε εποχή έχει το δικό της είδος πολέμου, τους δικούς της περιορισμούς και τις δικές της ιδιαίτερες προκαταλήψεις[111]». Η εποχή μας, η εποχή της πληροφορικής, δεν εξαιρείται, έχει το δικό της πόλεμο, τον Κυβερνοπόλεμο.

Επιγραμματικά θα μπορούσαμε να πούμε ότι στο αμιγές στρατιωτικό σκέλος, η σημασία της Κυβερνοάμυνας είναι αυτονόητη. Σκοπός των στρατιωτικών δυνάμεων ενός κράτους είναι η εξασφάλιση της εθνικής κυριαρχίας και εσωτερικής ασφάλειας των πολιτών.

Διασφαλίζοντας οι Ε.Δ. εκτός των άλλων, την αδιάλειπτη λειτουργία των ανωτέρω κρίσιμων υποδομών κάθε κράτους, αυτό καθίσταται αυτόνομο και "πορεύεται εν ειρήνη" και ομαλότητα. Όσο η λειτουργία και η οργάνωση των σύγχρονων κυβερνήσεων, κοινωνιών και

[110] http://docplayer.gr/46419492-Dokimia-oi-apories-enos-aploy-politoy-toy-ypostratigoy-e-a-konstantinoy-argyropoyloy.html

[111] Carl von Clausewitz, On War, Edited and Translated by M. Howard and Peter Paret, Princeton University Press, 1989, Book Eight "War Plans", Chapter Three "Independence of the Elements of War", σελ. 593. ("…every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions.")

Οργανισμών βασίζεται στην πληροφορική επιστήμη, τόσο μεγαλύτερη είναι η εκ των πραγμάτων απαίτηση προφύλαξης των κρίσιμων υποδομών αλλά και των εθνικών πληροφοριών, προκειμένου η κοινωνία να συνεχίσει να λειτουργεί ομαλά.[112]

[112] http://www.cyberinsurancegreece.com/ereynes/kyvernoamyna/

Πηγές - Βιβλιογραφία

Ελληνόγλωσση βιβλιογραφία

Ανδρέας Λιαρόπουλος Η Γεωγραφία και η πληροφόρηση ως διαστάσεις της Παγκόσμιας Ασφάλειας Εισήγηση στο 7ο Πανελλήνιο Γεωγραφικό Συνέδριο Οκτ 2004.

Δημήτριος Καντερές Υποστράτηγος εα:" Κυβερνοπόλεμος –Ένα νέο είδος πολέμου για τον 210 αιώνα ¨Αμυντική Επιθεώρηση ,Ιανουάριος 2004

Κώστας Γρίβας Ο Πόλεμος στον 21ο Αιώνα Εκδόσεις Επικοινωνίες Αθήνα 1999

Παναγιώτης Κονδύλης Η Θεωρία του Πολέμου εκδόσεις Θεμέλιο 1999

Η Ψηφιακή Στρατιωτική Κοινωνία , Σύγγραμα ΣΣΕ Κεφ 5

Έργα μεταφρασμένα στην ελληνική γλώσσα

Jack Goldsmith and W.Tim Ποιος ελέγχει το Ιντερνέτ 2007 Εκδόσεις Ποντίκι

Sun Tzu,The Art of War ,Κεφάλαιο 3 Σελ 40,Εκδόσεις Επικοινωνίες .Αθήνα

Ξενόγλωσση βιβλιογραφία

Ahmad Kamal UN report Law of Cyber Space 2005

Alexander Kevin B., Warfighting in Cyberspace, JOINT FORCES Q., 31 July 2007, http://www.military.com/forums/0,15240,143898,00.html.

Ariee Shaap Cyber Warfare Operations Air Force Law review 2009

B. H. Liddell Hart, Strategy, Εκδόσεις Meridian, 1991

Carl von Clausewitz, On War, Edited and Translated by M. Howard and Peter Paret, Princeton University Press, 1989, Book Eight "War Plans", Chapter Three "Independence of the Elements of War"

Giulio Douhet, The command of the air, translated by Dino Ferrari, Air Force History and Museums Program, Washington, DC, 1998

Hayles Catherine "The seduction of Cyberspace" Minnesota University 1993

Jeffrey Kelsey Hacking into international Humanitarian Law:The princiles od distinction and neutrality in the age of Cyber Warfare Michigan Law Review 2008.

Joint Publication 3-12 2013 Cyberspace Operations Σελ J2(US Joint Staff publication

Kelly Gable ,Cyber Apocalypse now Vanderbilt Journal of Transnational Law,Jan 2010

Martin Libicki What is information warfare 1995 National Defense University, Institute for National Strategic Studies

Martin Libicki Conquest in Cyberspace Cambridge University Press, 2007

Max Boot ,War made New :Weapons, warriors,and the Making of the Modern World ,Penguin Groop inc 2006

Miller Robert A. and Kuehl Daniel T., Cyberspace and the "first battle" in 21st century war, Defense Horizons, N. 68, September 2009, Center for Technology and National Security Policy, National Defense University

Parks Raymond C & Dugan David P 'Principles of Cyber Warfare' 2001 Proceedings of the 2001

Richard A. Clarke, Cyber War: The Next Threat to National Security and What to Do About It Army Cyber Institute, West Point, 2016

Todd Graham H., Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition, The Air Force Law Review Cyber Law Edition, Vol. 64, 20 November 2009

Δημοσιεύσεις – Άρθρα

Π.Μαυρόπουλος Κυβερνοπόλεμος και Εθνική Στρατηγική

http://www.warandstrategy.gr/kyvernopolemos/16-kyvernopolemos-kai-ethniki-

Ένας κυβερνοπόλεμος προ των πυλών, Καθημερινή 15 Οκτ 2017

http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

Κυβερνοτρομοκρατία Γιώργος Επιτήδειος 2000

http://www.eeei.gr/interbiz/articles/sarin.htm

Κυβερνο-επίθεση εφημερίδα Καθημερινή 25 Οκτ 2016

http://www.kathimerini.gr/880759/article/texnologia/diadiktyo/kyverno-epi8esh-eplh3e-taytoxrona-xiliades-istoselides

Μαζική επίθεση DDoS εναντίον DNS Host στις ΗΠΑ Περιοδικό PC 21 Οκτ 2016
http://gr.pcmag.com/internet/23891/news/mazike-epithese-ddos-enantion-dns-host-stis-epa

Παγκόσμιος τρόμος από την κυβερνοεπίθεση ,Newsroom
http://newpost.gr/kosmos/607354/prwtofanhs-kybernoepithesh-sygklonizei-ton-planhth-xtyphthhkan-nosokomeia-ypoyrgeia-kai-megales-etaireies

Ενας κυβερνοπόλεμος προ των πυλών εφημερίδα Καθημερινή 15 Ιαν 2017
http://www.kathimerini.gr/891836/article/epikairothta/kosmos/enas-kyvernopolemos-pro-twn-pylwn

Παραβατικότητα και Ποινικό Δίκαιο στον Κυβερνοχώρο Πανεπιστήμιο Αιγαίου 2011
www.icsd.aegean.gr/website_files/proptyxiako/76085723.doc

Ασφάλεια πληροφοριακών συστημάτων
https://el.wikipedia.org/wiki/ Ασφάλεια πληροφοριακών συστημάτων

Η Τουρκία ως ΥβριδικήΑπειλή Think News Τσακωνίτης Απόστολος Αυγ. 30, 2017
https://www.thinknews.gr/politiki/tourkia-os-yvridiki-apili/

Ο ακήρυχτος κυβερνοπόλεμος των χάκερ SL Press.gr Νεφέλη Λυγερού 24 Δεκεμβρίου 2017
https://slpress.gr/ethnika/o-akirychtos-cyberpolemos-ton-chaker/

Κυβερνοπόλεμος και Ελλάδα Τεχνολογίες hacking, ασφάλεια και διεθνές δίκαιο Security Report.gr 18 Φεβρουαρίου 2015
https://securityreport.gr/magazine-archive/year-2015/item/1087-kyvernopolemos-kai-ellada

Κυβερνοχώρος-Κυβερνοεπιθέσεις- Κυβερνοάμυνα Kedisa Χρήστος Βεράτης 26 Νοεμβρίου 2015
http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe

Ασκηση ΠΑΝΟΠΤΗΣ: Όλα τα σενάρια κυβερνοπολέμου κατά της Ελλάδας 3 Ιουν 2017
http://www.armynow.net/askisi-panoptis-ola-ta-senaria-kybernopolemou

Cyber-Warfare ο πόλεμος που δεν βλέπεις powerpolitics.eu
https://powerpolitics.eu/cyber-warfare ο πόλεμος που δεν βλέπεις

http://www.geetha.mil.gr/media/adispo/ANAKOINOSEIS/imerida/CYBERWAR/DELTIA/conclusions.pdf

Hacking of Government Computers Exposed 21.5 Million People, by Julie Hirschfeld Davis New York Times July 9 ,2015 https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Hacker Takes Over Russian Gas System by Associated Press
http://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system

Hacker arrested in Greece for stealing, selling weapons data ,SC Media 30 Jan 2008
https://www.scmagazine.com/hacker-arrested-in-greece-for-stealing-selling-weapons-data/article/554157/

Georgia: Russia 'conducting cyber war The Telegraph By Jon Swaine 11 Aug 2008
http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

Cybercrime offences
https://www.usip.org/sites/default/files/MC1/MC1-Part2Section16.pdf

U.S. Studies a New Threat: Cyber Attack By Bradley Graham Washington Post Staff Writer Sunday, May 24, 1998
http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm