ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΙΣ ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑ ΒΑΛΚΑΝΙΚΩΝ, ΣΛΑΒΙΚΩΝ ΚΑΙ ΑΝΑΤΟΛΙΚΩΝ ΣΠΟΥΔΩΝ
ΑΝΩΤΑΤΗ ΔΙΑΚΛΑΔΙΚΗ ΣΧΟΛΗ ΠΟΛΕΜΟΥ

Διπλωματική Εργασία

«ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΑΠΕΙΛΩΝ. ΣΥΓΚΡΙΤΙΚΗ ΑΝΑΛΥΣΗ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ ΓΙΑ ΤΗΝ ΕΛΛΑΔΑ»

του

Νικόλαου Τερεζή

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΥΡΙΑΚΟΣ ΜΙΚΕΛΗΣ

ΔΕΚΕΜΒΡΙΟΣ 2018

Σελίδα Σκόπιμα Κενή

Αφιερωμένη
στη γυναίκα μου και τα παιδιά μου Κική, Χρήστο και Χριστίνα.
Χωρίς εσάς τίποτα δεν θα γινόταν πραγματικότητα.
Σας ευχαριστώ για την αγάπη, την υπομονή και την υποστήριξη.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα της διπλωματικής μου εργασίας, επίκουρο καθηγητή του πανεπιστημίου Μακεδονίας κ. Κυριάκο Μικέλλη για την πολύτιμη καθοδήγηση του κατά την διάρκεια εκπόνησης αυτής της εργασίας. Επίσης θέλω να ευχαριστήσω τους γονείς και την αδερφή μου για την αγάπη τους.

Σελίδα Σκόπιμα Κενή

«Δηλώνω υπευθύνως ότι όλα τα στοιχεία σε αυτή την εργασία τα απέκτησα, τα επεξεργάστηκα και τα παρουσιάζω σύμφωνα με τους κανόνες και τις αρχές της ακαδημαϊκής δεοντολογίας, καθώς και τους νόμους που διέπουν την έρευνα και την πνευματική ιδιοκτησία. Δηλώνω επίσης υπευθύνως, ότι όπως απαιτείται από τους κανόνες, αναφέρομαι και παραπέμπω στις πηγές όλων των στοιχείων που χρησιμοποιώ και τα οποία δεν συνιστούν πρωτότυπη δημιουργία μου»

Νικόλαος Χ. Τερεζής

Σελίδα Σκόπιμα Κενή

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ ΚΑΙ ΣΧΗΜΑΤΩΝ

Σελίδα Σκόπιμα Κενή

ΠΕΡΙΛΗΨΗ

Ο Clausewitz στη μελέτη του περί πολέμου διέκρινε σχεδόν προφητικά, ότι κάθε εποχή έχει το δικό της είδος πολέμου, με τους δικούς του περιοριστικούς όρους και τις δικές του ιδιόμορφες προκαταλήψεις. Η εποχή που ζούμε είναι η εποχή της πληροφορίας και ο πόλεμος που τη χαρακτηρίζει είναι ο ασύμμετρος, διακεκριμένη μορφή του οποίου, είναι ο κυβερνοπόλεμος. Ο αντικειμενικός σκοπός του είναι η εκμετάλλευση της τεχνολογικής υποδομής του αντιπάλου εναντίον του. Παράλληλα ευσεβής πόθος αυτών που τον υιοθετούν ως πρακτική, είναι η κατάκτηση της υπέρτατης στρατηγικής ικανότητας σύμφωνα με τον Σουν Τζου, να κερδίζεις δηλαδή, δίχως να πολεμάς.

Ο κυβερνοχώρος είναι η νέα περιοχή εκδήλωσης αυτού του πολέμου σύμφωνα με τον William J. Lynn. Γι' αυτό και του έχει αποδοθεί ο όρος του πέμπτου πεδίου επιχειρήσεων. Η ισχύς που αναπτύσσουν οι παράγοντες του διεθνούς συστήματος στον κυβερνοχώρο είναι σχεδόν αδύνατο να καθοριστεί και σ' αυτό συμβάλλει ο ολοένα αυξανόμενος ρόλος και η δυναμική των μη κρατικών δρώντων. Μέσα και μέσω αυτού ταυτόχρονα, αμφισβητείται η Βεστφαλιανή έννοια της κυριαρχίας καθώς και η κυριαρχία της αλληλεξάρτησης, με αποτέλεσμα ο εγχώριος κρατικός έλεγχος να αποδυναμώνεται.

Η στοχοποίηση των κρίσιμων υποδομών των κρατών και το υψηλό ποσοστό επιτυχίας των κυβερνοεπιθέσεων καταδεικνύουν, ότι η ανθρωπότητα επικεντρώνοντας την προσοχή της στην πρόοδο, οικοδόμησε το μέλλον της σε μια δυνατότητα που δεν έμαθε να προστατεύει. Η Ελλάδα ως μέλος της ΕΕ και του ΝΑΤΟ, έχει εκπονήσει τη δική της στρατηγική για την ασφάλεια του κυβερνοχώρου. Μπορεί ωστόσο να αποκομίσει χρήσιμα συμπεράσματα, μελετώντας τις στρατηγικές άλλων κρατών, προσαρμόζοντας τις προβλέψεις τους στις δικές της ανάγκες. Όσο ο κυβερνοπόλεμος θα εξελίσσεται, τόσο μεγαλύτερα περιθώρια βελτίωσης της στρατηγικής θα υπάρχουν. ΗΠΑ, Κίνα και Εσθονία, αποτελούν εξαιρετικές περιπτωσιολογικές μελέτες, η καθεμιά για τους δικούς της λόγους. Αν μπορεί η μελέτη τους να οδηγήσει σε νέες καινοτόμες ιδέες, μένει να το διαπιστώσουμε…

Σελίδα Σκόπιμα Κενή

ΕΙΣΑΓΩΓΗ

Σε όλη τη διάρκεια της ανθρώπινης ιστορίας, η γνώση και η πληροφορία θεωρήθηκαν πάντοτε ισοδύναμες με την εξουσία. Οι πληροφορίες ειδικότερα ήταν πάντα ιστορικά ένας πολλαπλασιαστής δυνάμεων (Δελίμπασης 2009, 95). Χαρακτηριστικό της επίδρασης και του αντίκτυπου που έχουν οι πληροφορίες είναι, ότι η σημερινή εποχή χαρακτηρίζεται ως εποχή της πληροφορίας. Σ' αυτή έχουμε την ανάπτυξη του κυβερνοχώρου, ενός απόλυτα τεχνητού περιβάλλοντος, αποτελούμενου από αναρίθμητα δίκτυα, που δεν μπορεί να προσδιοριστεί με συμβατικό τρόπο, αλλά ταυτόχρονα μεταβάλλει αμετάκλητα τη συμπεριφορά κρατικών και μη κρατικών δρώντων όπως και αυτή των ιδιωτών.

Σε μια δικτυωμένη κοινωνία, η τοπική αλλά και η παγκόσμια διασύνδεση των σύγχρονων συστημάτων πληροφοριών υψηλής ταχύτητας, είναι το μεγαλύτερο πλεονέκτημα τους και ταυτόχρονα η μεγαλύτερη πιθανή ευπάθεια αυτών, καθώς παρέχει την πύλη, μέσω της οποίας μπορούν να πραγματοποιηθούν όλες οι μη εξουσιοδοτημένες εισβολές (Δελίμπασης 2009, 96). Αυτό προκύπτει, διότι η τεχνολογία στο χώρο των πληροφοριών και της επικοινωνίας παρουσιάζει αλματώδη πρόοδο προκαλώντας βαθιά εξάρτηση των κοινωνιών από αυτές, παραβλέποντας σε πολλές περιπτώσεις τα θέματα ασφαλείας. Το 2010, η κυβέρνηση των ΗΠΑ, μέσω της στρατηγικής Εθνικής Ασφάλειας προειδοποίησε, ότι «οι ίδιες οι τεχνολογίες που μας δίνουν ώθηση να ηγηθούμε και να δημιουργήσουμε, δίνουν ώθηση παράλληλα και σ' αυτούς που επιδιώκουν να διαταράξουν και να καταστρέψουν» (Betz J 2011, 11).

«Το διαδίκτυο μετατοπίζει την εξουσία με τρόπους που ποτέ δεν θα μπορούσαμε να φανταστούμε», προειδοποίησε μέσω ενός ντοκιμαντέρ το BBC θεωρώντας, ότι ο κυβερνοχώρος «επαναπροσδιορίζει τον πόλεμο (Betz, Journal in Strategic Affairs 2012, 692). Ο κυβερνοχώρος σήμερα συνιστά ένα νέο πεδίο επιχειρήσεων. Οι διεξαγόμενες επιχειρήσεις εντός αυτού, αμυντικές και επιθετικές, συνθέτουν μια νέα μορφή πολέμου, τον κυβερνοπόλεμο. Αυτή η μορφή του πολέμου μπορεί να θεωρηθεί ως ένας ασφαλής τρόπος, μέσω του οποίου μπορεί ένα λιγότερο ισχυρό κράτος ή μη κρατικός δρώντας να αμφισβητήσει την κυριαρχία και την ισχύ ενός ισχυρότερου κράτους. Ο Clarke θεωρεί ως σχεδόν σίγουρο το γεγονός, ότι οι περισσότεροι μελλοντικοί πόλεμοι θα «συνδυάζονται με

τον κυβερνοπόλεμο» (Betz, Cyber Power in Strategic Affairs: Neither Untinkable nor Blessed 2012, 696).

Τον Ιούνιο του 2010, ο υπουργός άμυνας Λέον Πανέτα κατέθεσε ενώπιον της Επιτροπής Ένοπλων Υπηρεσιών της Γερουσίας, ότι «*το επόμενο Περλ Χάρμπορ που θα αντιμετωπίσουμε, θα μπορούσε να προκληθεί από μια κυβερνοεπίθεση*» (Betz J 2011, 11). Γεγονότα όπως οι επιθέσεις άρνησης υπηρεσιών εναντίον ιστοτόπων της εσθονικής και της γεωργιανής κυβέρνησης ή ο ιός Stuxnet, που στόχευε στην απενεργοποίηση των ιρανικών πυρηνικών φυγοκεντρητών φαίνεται να δείχνουν, ότι η εποχή του κυβερνοπολέμου έχει ήδη φτάσει (Gartzke 2013, 41).

Με ποιες μορφές συναντάμε τον κυβερνοπόλεμο όμως και ποιοί είναι οι στόχοι που επιδιώκονται μέσω αυτού; Τι προκλήσεις εγείρει για την κυριαρχία των κρατών; Είναι έτοιμη η παγκόσμια κοινότητα να τον αντιμετωπίσει; Έχει δημιουργήσει τις προϋποθέσεις γι' αυτό; Ποια η στρατηγική της Ελλάδας για την αντιμετώπιση των κυβερνοαπειλών; Επιδέχεται βελτίωσης; Αυτή είναι μια σειρά εύλογων ερωτημάτων όταν προσπαθεί κανείς να προσεγγίσει το θέμα.

Ένας αξιόπιστος τρόπος για να απαντηθούν αυτά τα ερωτήματα είναι να μελετηθούν οι στρατηγικές κυβερνοασφαλείας άλλων κρατών. Αναπόφευκτα μέσα από μια νοερή συγκριτική ανάλυση αυτών και την ενδεχόμενη ταύτιση της Ελλάδας με ορισμένους από τους αντικειμενικούς σκοπούς τους να μπορούν να εξαχθούν χρήσιμα συμπεράσματα για την χώρα μας. Η Ελλάδα ως μέλος της ΕΕ και του ΝΑΤΟ, έχει ευθυγραμμίσει την πολιτική της για την αντιμετώπιση των απειλών στον κυβερνοχώρο, με αυτές των υπερεθνικών οργανισμών και ως ένα σημείο ανταποκρίνεται στις απαιτήσεις των καιρών.

Ωστόσο ο κυβερνοπόλεμος λόγω της φύσης του μεταβάλλεται και εξελίσσεται διαρκώς, γεγονός το οποίο επιβάλλει συνεχή εγρήγορση και διαρκή προσπάθεια βελτίωσης του αμυντικού μηχανισμού των κρατών. Ο εφησυχασμός αποτελεί την «κερκόπορτα» για την άμυνα και την ασφάλεια στον κυβερνοχώρο και η αλήθεια είναι, ότι ο περίγυρος της Ελλάδας δεν επιτρέπει κάτι τέτοιο.

Απαιτείται να γίνει αντιληπτό, ότι περιθώρια βελτίωσης υπάρχουν και θα υπάρχουν πάντα. Αφετηρία για την χώρα μας θα πρέπει να αποτελέσει η αναθεώρηση του υφιστάμενου νομικού πλαισίου τουλάχιστον σε εθνικό επίπεδο, προκειμένου να μπορεί να ανταποκριθεί στις προκλήσεις που εγείρει ο

κυβερνοχώρος. Η Ελλάδα οφείλει να θωρακίσει τον μέσο κοινό χρήστη, καθώς αυτός αποτελεί τον σύγχρονο «δούρειο ίππο» για την ασφάλεια των δημόσιων και ιδιωτικών δικτύων της. Μέσω των ενεργειών της πρέπει να αποδεικνύει διαρκώς, ότι δεν έχει μόνο τη θέληση να αντιμετωπίσει τις απειλές στον κυβερνοχώρο καθώς αυτό ως ένα βαθμό είναι αναμενόμενο. Πιο σημαντικό είναι να έχει τη θέληση να προετοιμαστεί γι' αυτό, να επιτυγχάνει μικρές νίκες κάθε ημέρα προκειμένου να αποκτήσει τα αντανακλαστικά και κυρίως τις δυνατότητες να αντιδράσει όταν απαιτηθεί.

«Ο κυβερνοχώρος είναι …….. μια νέα περιοχή εκδήλωσης πολέμου»

''William J. Lynn'

US Deputy Secretary of Defense'

ΚΕΦΑΛΑΙΟ «Α»

ΚΥΒΕΡΝΟΧΩΡΟΣ ΤΟ ΝΕΟ ΠΕΔΙΟ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΟΡΙΣΜΟΙ

Σήμερα δεν υπάρχει ένας διεθνώς αναγνωρισμένος ορισμός που να αποδίδει την έννοια του κυβερνοχώρου. Η πατρότητα του όρου ανήκει στον William Gibson, συγγραφέα ιστοριών επιστημονικής φαντασίας, ο οποίος έπλασε κατά την διάρκεια της δεκαετίας του 1980 τη συγκεκριμένη λέξη, χωρίς ιδιαίτερη περίσκεψη, ψάχνοντας μια λύση για να αποτυπώσει με υποβλητικό τρόπο τους ευφάνταστους συλλογισμούς του σχετικά μ' έναν εναλλακτικό κόσμο εικονικής πραγματικότητας, όπου οι μετέχοντες βλέπουν, ακούν και νοιώθουν, ακόμη και με τη βοήθεια των προσομοιώσεων (Παπαδούλη 2009, 10). Μάλιστα σε μια συνέντευξη του αργότερα ανέφερε ότι «*φαινόταν σαν ένας όρος αποτελεσματικός, μοδάτος ... υποβλητικός και ουσιαστικά χωρίς νόημα. Άφηνε να εννοηθούν πράγματα αλλά δεν είχε καμία πραγματική σημασιολογική έννοια, ακόμη και για μένα*» (Betz J 2011, 36).

Το Υπουργείο Άμυνας των ΗΠΑ ορίζει τον κυβερνοχώρο, ως το παγκόσμιο περιβάλλον το οποίο δημιουργείται από τα διασυνδεδεμένα δίκτυα των τεχνολογικών πληροφοριακών υποδομών, συμπεριλαμβανομένου και του διαδικτύου, τα δίκτυα τηλεπικοινωνιών, τα συστήματα ηλεκτρονικών υπολογιστών και τους ενσωματωμένους επεξεργαστές και συσκευών ελέγχου συστημάτων. Αυτός ο ορισμός εκτιμάται ότι είναι ο πιο πλήρης, καθώς αναγνωρίζει την αλληλεξάρτηση μεταξύ του φυσικού και του πληροφοριακού τομέα. Ορίζει επίσης τον κυβερνοχώρο ως το σύνολο των υποδομών πληροφόρησης, το οποίο περιλαμβάνει, αλλά δεν περιορίζεται στο Διαδίκτυο (Ronald J Deibert n.d., 5).

Μια άλλη εκδοχή, πιο συνοπτική, η οποία ωστόσο υποδηλώνει την ανεξαρτησία του από τους φυσικούς περιορισμούς του εδάφους, προέρχεται από την υπηρεσία ερευνών των ΗΠΑ, στα πλαίσια αναφοράς που συνέταξε για

λογαριασμό του Κογκρέσου. Πρόκειται λοιπόν για «τη συνολική δικτύωση των ανθρώπων μέσω των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών ανεξάρτητα από τη φυσική γεωγραφία» (Παπαδούλη 2009, 11). Τέλος, σύμφωνα με τον καθηγητή κ. Λιαρόπουλο Α.[1] κυβερνοχώρος είναι ένα παγκόσμιο πεδίο εντός του περιβάλλοντος πληροφοριών, πλαισιωμένο από τη χρήση ηλεκτρονικών και του ηλεκτρομαγνητικού φάσματος όπου δημιουργούνται, αποθηκεύονται, τροποποιούνται, ανταλλάσσονται και εκμεταλλεύονται πληροφορίες μέσω δικτύων χρησιμοποιώντας τεχνολογίες επικοινωνιών και πληροφοριών.

Ο κυβερνοχώρος σύμφωνα με το σχετικό δόγμα[2] των Ηνωμένων Πολιτειών αποτελεί το πέμπτο πεδίο επιχειρήσεων μη υπολειπόμενο σε σημαντικότητα των υπολοίπων τεσσάρων (της γης, του αέρα, της θάλασσας και του διαστήματος). Είναι διαφορετικό από τα άλλα πεδία από πολλές απόψεις, ωστόσο η πιο σημαντική διαφορά του αφορά το γεγονός, ότι είναι ένα περιβάλλον ολοκληρωτικά κατασκευασμένο από τον άνθρωπο (Betz J 2011, 35). Οι ΗΠΑ πρωτοπόρος σε θέματα στρατηγικής έχουν συστήσει μια ειδική στρατιωτική διοίκηση (USCYBERCOM), η οποία είναι υπεύθυνη για τις επιχειρήσεις στον κυβερνοχώρο, λειτουργώντας ως συνδετικός κρίκος του υπουργείου εθνικής άμυνας και του γενικού επιτελείου. Στην πραγματικότητα δεν είναι η μόνη χώρα που έχει αντιληφθεί τον κυβερνοχώρο ως ένα νέο πεδίο επιχειρήσεων. Πολλά άλλα κράτη αναπτύσσονται αντίστοιχα ενεργά στον χώρο, συντάσσοντας δόγματα και συστήνοντας Διοικήσεις – Διευθύνσεις με συνέπεια, μια νέα κούρσα κυβερνοεξοπλισμών να αναδύεται στον ορίζοντα.

Η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ διακρίνει τον κυβερνοχώρο σε περιοχή:

α. Ελεύθερης πρόσβασης όπου διεξάγονται επιχειρήσεις κυβερνοχώρου, συλλογή πληροφοριών και πληροφοριακές επιχειρήσεις.

β. Απαγορευμένης πρόσβασης (deep web), όπου λαμβάνουν χώρα επιθετικές επιχειρήσεις κυβερνοχώρου.

[1] Από παρουσίαση του καθηγητή Λιαρόπουλου Α. στο 4ο Πανελλήνιο Συνέδριο Εφαρμοσμένων Οικονομικών στις 23 Νοεμβρίου με θέμα «Cyberspace Governance and State Sovereignty: A difficult Relationship»

[2] Joint Publication 3 – 12 Cyberspace Operations σελ I - 1

Ολοκληρώνοντας κρίνεται σκόπιμο να αναφερθεί, ότι ο κυβερνοχώρος ως έννοια προκαλεί την παραδοσιακή αντίληψη βασικών εννοιών όπως οι διεθνείς σχέσεις, η πολιτική της ισχύος, η εθνική ασφάλεια, η κυριαρχία και τα σύνορα[3].

ΜΗΧΑΝΙΣΜΟΙ ΚΑΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΥΒΕΡΝΟΧΩΡΟΥ

Ο κυβερνοχώρος ως πεδίο επιχειρήσεων παρουσιάζει αρκετές ομοιότητες με αυτό του διαστήματος σε ότι αφορά την ασάφεια και την αδυναμία καθορισμού των διαστάσεων. Σύμφωνα με το καθηγητή M. Libicki, ένας τρόπος για να κατανοηθεί καλύτερα είναι να θεωρηθεί ότι αποτελείται από τρία στρώματα: το φυσικό επίπεδο, το συντακτικό επίπεδο που βρίσκεται πάνω από το φυσικό και το σημασιολογικό επίπεδο που ίσταται άνωθεν των δύο προηγούμενων (Libicki 2009, 12).

Το φυσικό επίπεδο (physical layer) αποτελείται από την ηλεκτρική ενέργεια, οπτικές ίνες, καλώδια και τα κουτιά των επεξεργαστών, που υποστηρίζουν τα πληροφοριακά συστήματα[4]. Αφαίρεση του φυσικού επιπέδου συνεπάγεται και εξαφάνιση των συστημάτων (Libicki 2009, 12). Από τα τρία επίπεδα είναι το μοναδικό το οποίο παρουσιάζει τρωτότητα σε μια φυσική επίθεση. Ωστόσο μια τέτοια επιλογή θα είχε ως συνέπεια την απώλεια της δυνατότητας εξαπάτησης και χειραγώγησης του συστήματος.

Το συντακτικό επίπεδο (syntactic layer) περιέχει τις οδηγίες που οι σχεδιαστές και οι χρήστες εισάγουν στο πληροφοριακό σύστημα καθώς και τα πρωτόκολλα μέσω των οποίων αλληλεπιδρούν τα συστήματα μεταξύ τους, όπως αναγνώριση συσκευών, δρομολόγηση, μορφοποίηση εγγράφων, χειρισμός βάσης δεδομένων κλπ. Είναι το επίπεδο, μέσω του οποίου η κυβερνοπειρατεία (hacking) στοχεύει, να διεκδικήσει την εξουσία των πληροφοριακών συστημάτων, έναντι των σχεδιαστών και των χρηστών τους (Libicki 2009, 12). Το συντακτικό επίπεδο θα μπορούσε να ειπωθεί ότι ταυτίζεται με το λογισμικό (δηλ. τα προγράμματα), το οποίο εισάγεται σε κάθε πληροφοριακό σύστημα και είναι υπεύθυνο για την επεξεργασία των πληροφοριών.

---

[3] Liaropoulos, Great Power Politics in Cyberspace: US and China are drawing the lines between confrontation and cooperation 2013, 157

[4] Από παρουσίαση του καθηγητή Λιαρόπουλου Α. στο 4ο Πανελλήνιο Συνέδριο Εφαρμοσμένων Οικονομικών στις 23 Νοεμβρίου με θέμα «Cyberspace Governance and State Sovereignty: A difficult Relationship»

Το σημασιολογικό επίπεδο (semantic layer) περιέχει δεδομένα / πληροφορίες που έχουν νόημα για τον άνθρωπο και τη γνωστική λειτουργία του κυβερνοχώρου.[5] Είναι οι πληροφορίες που περιέχει το σύστημα και υποστηρίζουν τη λειτουργία του. Ορισμένες από αυτές τις πληροφορίες, όπως π.χ πίνακες αναζήτησης διευθύνσεων ή κωδικοί ελέγχου εκτυπωτή, προορίζονται για το χειρισμό του συστήματος. Είναι σημασιολογικές στη μορφή αλλά συντακτικές στο σκοπό (Libicki 2009, 12). Σε αυτό το επίπεδο εξετάζεται η σημασιολογική ορθότητα μιας οδηγίας, η οποία μπορεί συντακτικά να είναι ορθή, αλλά σημασιολογικά να είναι λάθος (Χαίδης 2012, 7). Η σημασιολογία είναι σημαντική, διότι ο τρόπος με τον οποίο οι όροι γίνονται αντιληπτοί καθορίζουν τις προσδοκίες, οι οποίες με τη σειρά τους είναι σημαντικές για τη διαμόρφωση της πολιτικής χρήσης. Στο λεξιλόγιο του κυβερνοχώρου υπάρχουν έννοιες και όροι στα οποία μπορεί να αποδοθεί διαφορετική ερμηνεία[6].

Ο κυβερνοχώρος αν και ασαφής ως προς τη φύση του, δεδομένου των τριών επιπέδων από τα οποία αποτελείται, βρίσκεται αναντίρρητα πίσω από κάθε πτυχή της ανθρώπινης δραστηριότητας. Μέσω των επιδράσεων του, κυρίως έχει καταστεί εφικτό από την ακαδημαϊκή κοινότητα και όχι μόνο, να του αποδοθούν χαρακτηριστικά προκειμένου να μπορεί να αποκτήσει έστω και μια υποτυπώδη υπόσταση.

Σύμφωνα με την καθηγήτρια Choucri, ο κυβερνοχώρος χαρακτηρίζεται από **παροδικότητα** (αντικαθιστά το συμβατικά προσωρινό με το σχεδόν στιγμιαίο), **φυσικότητα** (ξεπερνά τους περιορισμούς της γεωγραφίας και της φυσικής θέσης), **διαπερατότητα** (διαπερνά σύνορα και δικαιοδοσίες), **ρευστότητα** (δηλώνει συνεχείς μετατοπίσεις και αλλαγές), **συμμετοχικότητα** (μειώνει τους φραγμούς στον ακτιβισμό και την πολιτική έκφραση), **αδυναμία καταλογισμού** (αποκρύπτει τις ταυτότητες των δρώντων και τη σύνδεση τους με τις κακόβουλες ενέργειες) και **έλλειψη ανάληψης ευθυνών** (παρακάμπτει τους μηχανισμούς υπευθυνότητας)[7].

Η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ, όπως είναι απολύτως φυσιολογικό, εστιάζει σε εκείνα τα χαρακτηριστικά του κυβερνοχώρου, στα οποία οφείλεται ο απειλητικός χαρακτήρας του και περιλαμβάνουν:

[5] Ομοίως με παραπάνω
[6] Liaropoulos, Great Power Politics in Cyberspace: US and China are drawing the lines between confrontation and cooperation 2013, 157
[7] Ομοίως με παραπάνω.

α. Τον εκμηδενισμό των αποστάσεων

β. Την μη ύπαρξη κεντρικής διακυβέρνησης και κεντρικού ελέγχου

γ. Τους διαφορετικούς νόμους σχετικά με τη χρήση, τη παραβατικότητα και το έγκλημα

δ. Την δυνατότητα ανωνυμίας ή δήλωσης ψευδούς ταυτότητας

ε. Την δυνατότητα πραγματοποίησης κακόβουλης/παράνομης ενέργειας σε οποιονδήποτε, από οπουδήποτε, με μικρό κόστος και με μικρή πιθανότητα εντοπισμού[8].

Επιπλέον ο κυβερνόχωρος χαρακτηρίζεται από το γεγονός ότι στερείται «μιας κοινής γλώσσας», δηλαδή μιας σειράς από έννοιες και όρους που θα συμφωνήσουν όλες οι πλευρές[9]. Αυτός εκτιμάται ότι είναι και ο λόγος, που ενώ όλος ο κόσμος αντιλαμβάνεται τον κυβερνόχωρο ως έννοια, υπάρχουν τόσο πολλές και συνάμα τόσο διαφορετικές ερμηνείες στη χρήση του γεγονός, το οποίο αποδεικνύεται από το ευρύ φάσμα των αντικειμενικών σκοπών που επιδιώκονται μέσω αυτού.

Σε κάθε περίπτωση, ο κυβερνοχώρος είναι μια συνάθροιση πολλών παραγόντων, των οποίων οι σχέσεις δεν σταθεροποιούνται ποτέ μόνιμα (Betz J 2011, 38). Είναι ο χώρος όπου τον κυρίαρχο ρόλο κατέχει η επίθεση γεγονός το οποίο οφείλεται στο γεγονός, ότι το Διαδίκτυο σχεδιάστηκε βασικά ως ανοιχτό δίκτυο για να μοιραστεί και όχι να προστατεύσει τις πληροφορίες. Επομένως, τα περισσότερα συστήματα που συνδέονται με δίκτυα είναι ευάλωτα στη διείσδυση[10].

ΙΣΧΥΣ ΚΑΙ ΚΥΒΕΡΝΟΧΩΡΟΣ

Η ισχύς ως όρος αναφέρεται γενικώς στη δυνατότητα να ενεργεί κανείς θετικά ή αρνητικά (με διαταγή ή απαγόρευση), πάνω σε κάποιον ή σε κάτι. Ισχύς είναι επίσης η δυνατότητα πρόκλησης ή παραγωγής αποτελεσμάτων τα οποία δεν θα συνέβαιναν διαφορετικά. Τέλος σύμφωνα με ορισμό προερχόμενο από την πολιτική οικονομία «ισχύς είναι η δύναμη που μπορεί να χρησιμοποιηθεί

[8] Από παρουσίαση της ΔΙΚΥΒ/ΓΕΕΘΑ με τίτλο Κυβερνοπόλεμος μια σύγχρονη σύγκρουση. http://www.securityproject.gr/presentations/2018/day1/papageorgiou.pdf
[9] Liaropoulos, Great Power Politics in Cyberspace: US and China are drawing the lines between confrontation and cooperation 2013, 157.
[10] Ομοίως με παραπάνω.

αποτελεσματικά», δηλαδή δύναμη αλλά και ικανότητα αποτελεσματικής χρήσης της (Κουσκουβέλης 2007, 140-141).

Τα ανωτέρω σε μια απόπειρα συγχώνευσης μπορούν να αποδοθούν περιγραφικά με τον ορισμό, ότι ισχύς είναι όταν «...ο Α έχει εξουσία πάνω στον Β στο βαθμό που μπορεί να επιβάλλει στον Β να κάνει κάτι που ο Β δεν θα έκανε αλλιώς» (Betz J 2011, 43). Η συγκεκριμένη προσέγγιση ταυτίζεται με αυτή του Clauzewitz για τον πόλεμο το οποίον θεωρεί ως πράξη βίας που υποχρεώνει τον εχθρό να κάνει το θέλημα μας. Από αυτή την διαισθητική έννοια της ισχύος πηγάζει η ιδέα ότι η ισχύς είναι η ικανότητα ενός κράτους να επιστρατεύσει τους πόρους του για να προωθήσει τα συμφέροντά του ενάντια στα συμφέροντα άλλου κράτους (Betz J 2011, 43).

Η ισχύς παράγεται μόνο μέσω των αλληλεπιδράσεων των κοινωνικών οντοτήτων ή των διεθνών παραγόντων και δεν έχει λόγο ύπαρξης εκτός της κοινωνικής ή σε επίπεδο διεθνών σχέσεων δράσης. Δεν υπάρχει χωρίς τις σχέσεις μέσω των οποίων εκφράζεται και είναι φανερή μόνο από τις επιπτώσεις που έχει σε άλλους (Betz J 2011, 42). Δεν είναι εγγενής, αλλά πρέπει να παραχθεί με κάποιο τρόπο μέσω της αξιοποίησης των συντελεστών που χαρακτηρίζουν κάθε παράγοντα του διεθνούς συστήματος και στους οποίους αποφάσισε να επενδύσει, προκειμένου μέσω της αύξησης των φορτίων ισχύος να διαμορφώσει την θέση του στο παγκόσμιο γίγνεσθαι. Οι συντελεστές διακρίνονται :

α. Στους υλικούς ή αντικειμενικούς, οι οποίοι περιλαμβάνουν την γεωγραφία, τον πληθυσμό, τις πηγές πλούτου και τις ένοπλες δυνάμεις.

β. Στους λειτουργικούς, οι οποίοι περιλαμβάνουν το πολιτικό σύστημα, τη διοίκηση, την ικανότητα στρατιωτικής κινητοποίησης και τη θέση στο διεθνές σύστημα.

γ. Στους υποκειμενικούς, οι οποίοι περιλαμβάνουν την ηγεσία και το διεθνές κύρος.

Τα τελευταία χρόνια με το δεδομένο, ότι ο κυβερνοχώρος αποτελεί και επίσημα το πέμπτο πεδίο επιχειρήσεων, έχει αναπτυχθεί μια θεματολογία σχετικά με τον όρο «cyber-power» ή ισχύς του κυβερνοχώρου (κυβερνο-ισχύς). Ειδικότερα ο συγκεκριμένος όρος έχει γίνει πιο συνηθισμένος στην συζήτηση περί ασφάλειας

και στρατηγικής και είναι πιθανό να κερδίσει ακόμα μεγαλύτερο μερίδιο ενδιαφέροντος στο εγγύς μέλλον (Betz J 2011, 43).

Η ισχύς εκλαμβάνει διαφορετικές εκφάνσεις με νοηματικό περιεχόμενο που δεν είναι εύκολο να διαχωρίσει κανείς, καθώς στη πράξη οι έννοιες συχνά αλληλεπικαλύπτονται. Μπορεί να εμφανίζεται ως δύναμη σηματοδοτώντας την υλική πλευρά της, τα φυσικά μέσα δηλαδή με τα οποία δύναται κανείς να επιβάλλει τη βούληση του. Επίσης μπορεί να εμφανίζεται ως εξουσία δηλαδή ως ηθική ή και πολιτική δυνατότητα που επιτρέπει την άσκηση της ισχύος. Τέλος, δύναται να παρουσιάζεται ως επιρροή που αφορά τον τομέα του συναισθήματος αλλά και τον εσωτερικό ψυχολογικό κόσμο του ατόμου (Κουσκουβέλης 2007, 141-143).

Η κυβερνο-ισχύς, ως το σύνολο των δυνάμεων που κυκλοφορούν στον συγκεκριμένο πεδίο, παρουσιάζεται και με τις τρείς ανωτέρω εκφάνσεις ενώ αναμφίβολα έχει την ικανότητα να δημιουργεί επιρροή διαμορφώνοντας τις αποφάσεις και κυρίως τις ενέργειες εκείνων που δρουν μέσα και μέσω του κυβερνοχώρου. Οποιαδήποτε χρήση της λέξης «ισχύ» με ταυτόχρονη χρησιμοποίηση του συνθετικού «cyber (κυβερνο)» μπορεί να είναι μόνο υποκειμενική. Δεν ορίζει τον πυρήνα της φύσης της ισχύος, εκτός του ότι υπονοεί ότι η ισχύς λειτουργεί στο περιβάλλον του «κυβερνοχώρου», όπως οπουδήποτε αλλού όπου υπάρχουν κοινωνικές ή διεθνείς σχέσεις (Betz J 2011, 43).

Ο καθηγητής κ. Κουσκουβέλης αναφέρει, ότι για να κατανοήσουμε την ισχύ στο πλαίσιο συγκεκριμένων πολιτικών καταστάσεων του εσωτερικού ή του διεθνούς πολιτικού αγώνα αλλά και για να μελετήσουμε καλύτερα την έννοια και τη μορφή της, θα πρέπει να γνωρίζουμε και αν όχι να επιχειρούμε, να προσδιορίσουμε τα χαρακτηριστικά της : τον κάτοχο της ισχύος, το μέγεθος της, τον τομέα δραστηριοτήτων στον οποίο μπορεί να εφαρμοσθεί, την αποτελεσματικότητα της, το σημείο ισορροπίας και το κόστος χρήσης της (Κουσκουβέλης 2007, 143).

Η προσπάθεια κατανόησης της κυβερνο-ισχύος ωστόσο, παρουσιάζει ιδιαιτερότητες, που σχετίζονται κυρίως με την ασάφεια και την αβεβαιότητα που συνοδεύει σχεδόν όλα τα στοιχεία που θεωρούνται χαρακτηριστικά της. Από τη μέχρι τώρα χρήση της και τα αποτελέσματα της επίδρασης της προκύπτει, ότι υπάρχει δυσκολία στις πλείστες περιπτώσεις, να καθοριστεί ο κάτοχος της και το

μέγεθος αυτής. Ο τομέας των δραστηριοτήτων που μπορεί να εφαρμοσθεί είναι ιδιαίτερα ευρύς επηρεάζοντας ένα μεγάλο φάσμα των κοινωνικών και κρατικών δραστηριοτήτων, ενώ μεγάλη διακύμανση παρουσιάζει και το κόστος απόκτησης της.

Προς επίρρωση των ανωτέρω αναφέρεται ότι πολλές από τις ανησυχίες που εκφράζουν οι κυβερνήσεις, οφείλονται στον πολλαπλασιασμό των δρώντων στον κυβερνοχώρο (Betz J 2011, 38). Μέχρι τώρα οι τρείς βασικές θεωρήσεις των διεθνών σχέσεων προτείνουν, ότι οι βασικοί παράγοντες του διεθνούς συστήματος είναι τα κράτη (ρεαλισμός), τα κράτη και οι διεθνείς οργανισμοί (πλουραλισμός), ή οι τάξεις (μαρξισμός) (Κουσκουβέλης 2007, 143). Όλοι τους και πολύ περισσότερο τα κράτη είναι προφανώς σημαντικοί παράγοντες και θα συνεχίσουν να είναι, ωστόσο η δικτυακή παρουσία τους και η δυνατότητα απόκτησης επιρροής σ' αυτό το πεδίο έχει ανταγωνιστές φορείς προερχόμενους από ένα ευρύ φάσμα. Οι φορείς ποικίλλουν από μεμονωμένους πολίτες, έως κοινωνικές οργανώσεις και εμπορικές επιχειρήσεις, από τρομοκράτες και αντάρτες μέχρι κλάδους κρατικής εξουσίας (π.χ στρατιωτικές μονάδες, υπηρεσίες πληροφοριών κ.λπ.). Ο καθένας επιδιώκει να χρησιμοποιήσει τον κυβερνοχώρο, για να επιδιώξει τους δικούς του σκοπούς, είτε μεμονωμένα είτε σε συνεννόηση και συνεργασία με άλλους παράγοντες (Betz J 2011, 38-39).

Επιπλέον η μείωση του χρόνου και η ελαχιστοποίηση των αποστάσεων λόγω της στιγμιαίας σύνδεσης - επαφής που παρέχει ως δυνατότητα ο κυβερνοχώρος, αυξάνει τις πιθανότητες επηρεασμού των παραγόντων του διεθνούς συστήματος από μορφές ισχύος, που στο παρελθόν περιορίζονταν από τον φυσικό και χρονικό διαχωρισμό (Betz J 2011, 39).

Στον παγκόσμιο κυβερνοχώρο, η αλληλεξάρτηση και η διασύνδεση των μαζικά δικτυωμένων συσκευών και χρηστών μεταβάλλει αμετάκλητα την παραδοσιακή δυναμική της αιτίας και του αποτελέσματος (Betz J 2011, 40). Η ισχύς στον κυβερνοχώρο δεν δημιουργήθηκε απλά για να υπάρχει, αλλά μάλλον για να υποστηρίζει την επίτευξη μεγαλύτερων στόχων ... από τους ήδη υπάρχοντες συντελεστές της εθνικής ισχύος - πολιτική, διπλωματία, πληροφορίες, ένοπλες δυνάμεις και οικονομία (Betz J 2011, 44).

Η ισχύς παρουσιάζεται στον κυβερνοχώρο με τέσσερις μορφές:

α. Υποχρεωτική κυβερνο-ισχύς (Compulsory cyber - power)

Η πρώτη μορφή ισχύος στον κυβερνοχώρο είναι η απευθείας χρήση εξαναγκασμού από έναν δρώντα του κυβερνοχώρου σε μια προσπάθεια να τροποποιήσει τη συμπεριφορά και τις συνθήκες ύπαρξης ενός άλλου. Αυτή η μορφή είναι υποχρεωτική, με την έννοια ότι επιβάλλει σε κάποιον να ενεργεί σύμφωνα με τη θέληση αυτού που την εφαρμόζει. Ο εξαναγκασμός μπορεί επίσης να ασκηθεί και από μη κρατικούς φορείς, ενώ η μορφή της υποχρεωτικής ισχύος στον κυβερνοχώρο μπορεί να βρεθεί στις αλληλεπιδράσεις μεταξύ μη κρατικών δρώντων και κρατών και μεταξύ μη κρατικών δρώντων. Κάθε ένας με πρόσβαση στον κυβερνοχώρο και τις απαιτούμενες δεξιότητες και γνώσεις μπορεί, υποθετικά, να ασκήσει υποχρεωτική ισχύ στον κυβερνοχώρο εναντίον άλλου (Betz J 2011, 45).

β. Θεσμική κυβερνο-ισχύς (Institutional cyber - power)

Η θεσμική ισχύς υπάρχει όταν ένας παράγοντας είναι σε θέση να επηρεάσει τους τρόπους με τους οποίους ενδιάμεσοι θεσμικοί οργανισμοί λειτουργούν, δημιουργώντας τις συνθήκες και τις προϋποθέσεις που θα του επιτρέψουν να καθοδηγεί, να κατευθύνει και να περιορίζει τις πράξεις και τις συνθήκες ύπαρξης των άλλων. Επίσης ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί για να επηρεάσει τις απόψεις ξένων ακροατηρίων μέσω του θεσμού των μέσων ενημέρωσης (Betz J 2011, 47).

γ. Δομική κυβερνο-ισχύς (Stuctural cyber – power)

Η δομική ισχύς λειτουργεί, για να διατηρήσει τις δομές στις οποίες βρίσκονται οι δρώντες και οι οποίες σε μεγάλο βαθμό, επιτρέπουν ή περιορίζουν τις ενέργειες που ενδεχομένως επιθυμούν να αναλάβουν σε σχέση με άλλους παράγοντες με τους οποίους είναι άμεσα συνδεδεμένοι. Η συγκεκριμένη μορφή ισχύος λειτουργεί τόσο για να διατηρήσει το status quo όσο και για να το διαταράξει. (Betz J 2011, 48 - 50)

δ. Παραγωγική κυβερνο-ισχύς (Productive cyber – power)

Η παραγωγική κυβερνο-ισχύς αποτελεί το θεμέλιο για τις άλλες μορφές ισχύος στον κυβερνοχώρο. Χωρίς κοινωνικές οντότητες δεν υπάρχουν κοινωνικές σχέσεις μέσω των οποίων να εκδηλώνεται η ισχύς. Ένα από τα πιο προφανή

παραδείγματα του τρόπου με τον οποίο τα κράτη επιδεικνύουν παραγωγική κυβερνο-ισχύ είναι μέσω της κατασκευής φορέων απειλής στον κυβερνοχώρο. Με τον προσδιορισμό ορισμένων παραγόντων ως απειλών για την εθνική ασφάλεια, τα κράτη μπορούν να ακολουθήσουν πολιτικές και στρατηγικές σχεδιασμένες για να τους αντιμετωπίσουν ως νόμιμους στόχους άλλων μορφών κρατικής εξουσίας. Η παραγωγική κυβερνο-ισχύς συνδέει επίσης, τις στρατιωτικές και πολιτικές δυνάμεις στον πόλεμο και στοχεύει να διαμορφώσει τις συνθήκες προς όφελος του στρατηγικού δρώντα. Αυτό είναι ιδιαίτερα εμφανές στη χρήση της ήπιας ισχύος που στοχεύει να κερδίσει τις καρδιές και τα μυαλά, είτε πριν τη σύγκρουση είτε μετά. Σε μια εποχή που χαρακτηρίζεται από τη «στρατηγική επικοινωνία» και τη «δημόσια διπλωματία», η παραγωγική κυβερνο-ισχύς είναι ίσως η πιο σημαντική μορφή της κυβερνο-ισχύος. (Betz J 2011, 50 - 51)

ΚΥΒΕΡΝΟΧΩΡΟΣ ΚΑΙ ΚΥΡΙΑΡΧΙΑ

Ο όρος κυριαρχία σε λεξικό νομικής ορολογίας αναφέρεται ως ανώτατη εξουσία ή κανόνας, ως ανώτατη πολιτική εξουσία ενός ανεξάρτητου κράτους, ή ως το ίδιο το κράτος (Franzese 2009, 8). Στα κράτη της δύσης έχει επικρατήσει, ότι δεν είναι καθαρά πολιτική, νομική ή στρατηγική έννοια αλλά ένας συνδυασμός αυτών. Γενικώς μέσω αυτής υπονοείται η «ανώτατη εξουσία» μέσα σε «εδαφικά οριοθετημένα» κράτη με τρόπο που να κρατά μία κυβέρνηση έξω από τις υποθέσεις μιας άλλης κυβέρνησης (Ayers 2016).

Η κυριαρχία είναι σημαντική και θεμελιώδης έννοια για την τρέχουσα διεθνή τάξη καθώς όχι μόνο υποδηλώνει την εξουσία μέσα σε μια διακριτή εδαφική οντότητα, αλλά παράλληλα υπονοεί και την ένταξη στο σύγχρονο σύστημα κρατών. (Liaropoulos, ETH zurich CSS 2014) Επίσης της έχει αποδοθεί, από τον επιστημονικό κύκλο των διεθνών σχέσεων που ασχολείται με τις ενέργειες και τις προθέσεις των κρατών, ο χαρακτηρισμός της «κυρίαρχης μεταβλητής του διεθνούς συστήματος». Ωστόσο, όπως έχει παρατηρήσει ο Robert Keohane, η κυριαρχία ως έννοια συζητείται συχνότερα από ό, τι ορίζεται (Betz J 2011, 57).

Σε αντίθεση με την έννοια της ισχύος, η οποία συνήθως θεωρείται θεμελιώδης για την κοινωνική αλληλεπίδραση και το σύνταγμα, η κυριαρχία είναι μια έννοια η οποία προέρχεται εξ ολοκλήρου από την πολιτική. Εάν η ισχύς ενυπάρχει στις πολιτικές σχέσεις, η κυριαρχία εξαρτάται από τις επικρατούσες

πολιτικές θεωρίες και πρακτικές της εποχής, αν και τείνει σε μεγαλύτερο ή μικρότερο βαθμό να ενσωματώνεται στην ιδέα ότι είναι ή πρέπει να είναι μια ανώτερη αρχή μέσα σε μια εδαφική πολιτική οντότητα. Στη σύγχρονη εποχή, η κυριαρχία συνδέεται στενά με τη φύση του κράτους, χωρίς την οποία δεν μπορεί να έχει υπόσταση με τη συνήθη έννοια της (Betz J 2011, 56).

Ο Stephen Krasner[11] υποστηρίζει ότι υπάρχουν τέσσερις τρόποι με τους οποίους γίνεται αντιληπτή η έννοια της κυριαρχίας στο διεθνές σύστημα. Πρόκειται για την εγχώρια κυριαρχία, την κυριαρχία της αλληλεξάρτησης, τη διεθνή νομική κυριαρχία και τη Βεστφαλιανή κυριαρχία (Betz J 2011, 57).

Η **εγχώρια κυριαρχία** αναφέρεται στον τρόπο οργάνωσης της δημόσιας εξουσίας σε ένα κράτος και στο επίπεδο αποτελεσματικού ελέγχου που μπορούν να ασκήσουν αυτές οι αρχές. Τα πολιτικά συστήματα όλων των μορφών και μεγεθών, είναι υπεύθυνα για τη ρύθμιση και τον έλεγχο των εξελίξεων στην επικράτειά τους. **Η κυριαρχία της αλληλεξάρτησης** σχετίζεται με την ικανότητα των δημόσιων αρχών να ελέγχουν τις διασυνοριακές κινήσεις, που αφορούν ροές ανθρώπων, υλικών και ιδεών. Εάν ένα κράτος δεν εξασφαλίσει αποτελεσματικό έλεγχο των συνόρων του, είναι βέβαιο ότι θα αποτύχει να ελέγξει τι συμβαίνει στην επικράτειά του. Κατά συνέπεια, η απώλεια της κυριαρχίας αλληλεξάρτησης έχει τη δυνατότητα να επηρεάσει την εγχώρια κυριαρχία. **Η διεθνής νομική κυριαρχία** βλέπει τα πράγματα λίγο διαφορετικά, δεδομένου ότι ασχολείται ιδιαίτερα με την αμοιβαία αναγνώριση των κρατών στο διεθνές σύστημα. Τέλος η **Βεστφαλιανή κυριαρχία,** υπογραμμίζει το δικαίωμα των κρατών να καθορίζουν την διακυβέρνηση και την πολιτική τους ελεύθερα από την επιρροή εξωτερικών παραγόντων. (Liaropoulos, ETH zurich CSS 2014)

Οι συζητήσεις που αφορούν την επίδραση του κυβερνοχώρου στην κυριαρχία του κράτους, περιγράφουν τη διάβρωση της ως αναπόφευκτη συνέπεια της παγκόσμιας ανταλλαγής πληροφοριών και της μειωμένης συνάφειας της φυσικής επικράτειας στον κυβερνοχώρο (Betz J 2011, 55-56). Το ανωτέρω, αποτελεί μάλλον, φυσική συνέπεια της έλλειψης διακριτών συνόρων μεταξύ των κρατών στον κυβερνοχώρο.

[11] Ο Stephen David Krasner (γεννημένος στις 15 Φεβρουαρίου 1942, Νέα Υόρκη) είναι καθηγητής διεθνών σχέσεων στο Πανεπιστήμιο του Στάνφορντ και πρώην Διευθυντής Σχεδιασμού Πολιτικής στο Υπουργείο Εξωτερικών των Ηνωμένων Πολιτειών, θέση που κατείχε από το 2005 μέχρι τον Απρίλιο του 2007.

Είναι λοιπόν δυνατόν, τα κράτη να ασκήσουν την εξουσία και τον έλεγχό τους σε έναν δίχως σύνορα και σχετικά αναρχικό «κυβερνο-κόσμο»; Παραφράζοντας την έννοια της διεθνούς τάξης του Hedley Bull, θα μπορούσε κανείς να υποστηρίξει, ότι η άσκηση κρατικής κυριαρχίας στον κυβερνοχώρο είναι ένα απαραίτητο βήμα για την καθιέρωση μιας διεθνούς τάξης στο συγκεκριμένο πεδίο. Σύμφωνα με τον Bull, τα κράτη ενεργούν με τέτοιο τρόπο, ώστε να διαφυλάσσουν τη διεθνή τάξη, διότι η διατήρηση της είναι προς το δικό τους συμφέρον. Μια επιπλέον ερώτηση που τίθεται είναι αν τα κράτη θα ενεργήσουν με τον ίδιο τρόπο για να διατηρήσουν τη διεθνή τάξη στον κυβερνοχώρο (Liaropoulos, ETH zurich CSS 2014). Όσο προκλητικό ακούγεται ένα τέτοιο εγχείρημα η εκτίμηση είναι, ότι η εξασφάλιση της κυριαρχίας πρέπει να αποτελεί πάγια επιδίωξη των κρατών. Μ' αυτόν τον τρόπο αφενός θα καταστεί σαφής η εξουσία μέσα στη ξεχωριστή εδαφική οντότητα που ορίζει το κράτος αφετέρου, θα υποδηλώσει την ένταξη αυτού στο σύγχρονο σύστημα των κρατών. Βέβαια όπως θα καταδειχθεί στη συνέχεια, αυτό σε κάποιες μορφές κυριαρχίας μπορεί να επιτευχθεί και σε άλλες όχι. Σημαντικό δεδομένο που πρέπει να ληφθεί υπόψη είναι, ότι ο κυβερνοχώρος δεν υποσκάπτει απαραίτητα την κυριαρχία σε όλες τις μορφές της (Betz J 2011, 58).

Συγκεκριμένα δεν έχει σχεδόν καμία επίδραση στη διεθνή νομική κυριαρχία, καθώς δεν αποτελεί άμεση πρόκληση για την ακεραιότητα της διεθνούς νομικής κυριαρχίας ως πηγή εξουσίας. Αντίθετα έχει σημαντικές επιπτώσεις στη Βεστφαλιανή έννοια της κυριαρχίας καθώς παραβιάσεις αυτού του είδους της κυριαρχίας προκύπτουν από εξωτερικούς παράγοντες, που επιβάλλουν αλλαγές ή καθορίζουν τη δομή και τη λειτουργία της εσωτερικής πολιτικής εξουσίας. Η πιο προφανής περίπτωση επίδρασης του κυβερνοχώρου στη βεστφαλιανή κυριαρχία, είναι στη άσκηση της υποχρεωτικής κυβερνο-ισχύος (compulsory cyber-power). Οι επιχειρήσεις δικτύων υπολογιστών εναντίον στόχων σε άλλη χώρα, παραβιάζουν a priori τη βεσταφαλιανή κυριαρχία ανεξάρτητα αν οι συνθήκες που συμβαίνει αυτό κάθε φορά διαφέρουν σημαντικά. Χαρακτηριστικά παραδείγματα αποτελούν τόσο οι κυβερνο-επιθέσεις της Ρωσίας εναντίον της Εσθονίας και της Γεωργίας το 2007 και 2008 αντίστοιχα, όσο και το σκάνδαλο εμπλοκής της στις τελευταίες Αμερικανικές εκλογές.

Στη περίπτωση της εγχώριας κυριαρχίας, η οποία αναφέρεται στους τρόπους με τους οποίους διεξάγεται η εσωτερική λειτουργία του κράτους, ο κυβερνοχώρος επηρέασε σημαντικά την εσωτερική εξουσία και τον έλεγχο και εκτιμάται ότι θα συνεχίσει να το πράττει και στο μέλλον. Οι επιδράσεις του παρατηρούνται σε ένα ευρύ φάσμα πολιτικών καταστάσεων, από φιλελεύθερες δημοκρατίες, έως αυταρχικά καθεστώτα. Οι αντιδράσεις των κρατών, στη προσπάθειά τους να ρυθμίσουν τη χρήση του κυβερνοχώρου από τους πολίτες τους, εντός των δικών τους συνόρων, περιλαμβάνουν τη θέσπιση ιδιαίτερης νομοθεσίας και νέων δομών για τη διαχείριση του κυβερνοχώρου και των σχετικών κανονισμών αυτού.

Ο σημαντικότερος αντίκτυπος του κυβερνοχώρου παρατηρείται στην κυριαρχία της αλληλεξάρτησης. Αυτό προκύπτει ως αποτέλεσμα της διαδικασίας της παγκοσμιοποίησης και του διεθνικού χαρακτήρα που παρουσιάζει η απρόσκοπτη ροή των πληροφοριών πέρα από τα εθνικά σύνορα. Αν και η εγχώρια εξουσία δεν επηρεάζεται απαραίτητα από την μειωμένη κυριαρχία αλληλεξάρτησης, ο εγχώριος έλεγχος συχνά αποδυναμώνεται (Betz J 2011, 69).

Μολονότι η επίτευξη της κυριαρχίας στον κυβερνοχώρο και στις τέσσερις μορφές της αποτελεί δύσκολο εγχείρημα δεν υποδηλώνει ότι τα κράτη θα πρέπει να πάψουν να την επιδιώκουν. Σύμφωνα με τον Πάτρικ Φραντσέζε[12], η εδραίωση της κρατικής κυριαρχίας στον υπόψη χώρο απαιτεί κατ' ελάχιστο την αναγνώριση της, από τους υπόλοιπους κρατικούς δρώντες και επιπλέον το ίδιο το κράτος να δύναται να εφαρμόσει μέτρα ελέγχου στον κυβερνοχώρο του, ως απτή απόδειξη αυτής.

Ο ίδιος επιπλέον πρότεινε στην μελέτη του πέντε θέματα, για τα οποία τα κράτη θα πρέπει να ενεργήσουν κατάλληλα, προκειμένου να δημιουργήσουν τις προϋποθέσεις επίτευξης της κρατικής κυριαρχίας στον κυβερνοχώρο ως κάτωθι:

α. Δημιουργία ενός διεθνούς οργανισμού για την ανάπτυξη της κυριαρχίας στο κυβερνοχώρο. Για να γίνει κάτι τέτοιο πράξη, τα κράτη πρέπει να επιδείξουν συναίνεση σε ότι αφορά τις βασικές αρχές και τους κανόνες από τους οποίους θα προκύψει αυτός ο διεθνής οργανισμός. Μια πιθανή αρχή θα μπορούσε να είναι π.χ, ότι «κάθε κράτος έχει δικαίωμα πρόσβασης στον κυβερνοχώρο για ειρηνικούς

[12] Ο Πάτρικ Φραντσέζε είναι αντισυνταγματάρχης του Αμερικανικού Στρατού και οι απόψεις του έχουν αναγραφεί σε άρθρο με τίτλο « Sovereignty in Cyberspace : can it exist?»

σκοπούς, ωστόσο τα κράτη έχουν έννομο συμφέρον να διεκδικήσουν και να προστατεύσουν την κυριαρχία τους στον κυβερνοχώρο». Οι μεγάλες κυβερνοδυνάμεις – Κίνα, Ρωσία και ΗΠΑ – θα βρεθούν αναμφίβολα, στην πρώτη γραμμή μιας τέτοιας πρωτοβουλίας. Τροχοπέδη ωστόσο αναμένεται να αποτελέσουν οι αντικρουόμενες απόψεις τους για την καλύτερη δυνατή διακυβέρνηση του κυβερνοχώρου. (Liaropoulos, ETH zurich CSS 2014)

β. Τα συμφέροντα των κρατών πάντα υπερισχύουν και τελικά ανατρέπουν τα αρχικά ουτοπικά ιδανικά, αγαθών ως προς το χαρακτήρα πρωτοβουλιών για την εξασφάλιση της κυριαρχίας στον κυβερνοχώρο. Όσο τα συμφέροντα των κρατών θα γίνονται πιο ξεκάθαρα και θα αυξάνονται και όσο η τεχνολογία θα εξελίσσεται τα κράτη θα επιδιώκουν να ασκούν όλο και μεγαλύτερο έλεγχο στον κυβερνοχώρο.

γ. Ιδιαίτερα σημαντική είναι η πρακτική που θα εφαρμόσει εν τέλει το κράτος για να διασφαλίσει την κυριαρχία του. Παρόλο που ένα κράτος έχει τη δυνατότητα καθορισμού της χώρας προέλευσης μιας κυβερνοεπίθεσης, σπάνια κοινοποιεί τη παραβίαση της κυριαρχίας του καθώς αυτό συνιστά παράλληλα, δημόσια παραδοχή της αδυναμίας του να την περιχαρακώσει και να τη θωρακίσει.

δ. Η διευκρίνιση των δρώντων στον κυβερνοχώρο είναι ζωτικής σημασίας. Αυτό δύναται να επιτευχθεί μέσω της εποπτείας του ανωτέρω προτεινόμενου διεθνή οργανισμού και της συμφωνίας μεταξύ των κρατών σχετικά με την ανάγκη παρακολούθησης και εντοπισμού συγκεκριμένων παραγόντων στον κυβερνοχώρο.

ε. Τέλος τα κράτη θα πρέπει να έχουν την ικανότητα να προστατεύουν τα σύνορά τους και να αντιδρούν άμεσα, σε οποιαδήποτε παραβίαση της κυριαρχίας τους. Για να επιτευχθεί αυτό τα κράτη θα πρέπει να μπορούν να καταφύγουν στη χρήση ισχύος, όπως θα ενεργούσαν στην περίπτωση παραβίασης της κυριαρχίας τους σε άλλους τομείς.

Ο κυβερνοχώρος παρέχει μια σειρά από προκλήσεις στην κυριαρχία, τις οποίες τα κράτη απλά δεν έχουν την πολυτέλεια να αγνοήσουν. Ο τομέας του κυβερνοχώρου αντικατοπτρίζει το σημερινό διεθνές σύστημα, όπου τα εθνικά συμφέροντα, οι γεωπολιτικές φιλοδοξίες και οι ιδεολογίες θα συγκρουστούν αναπόφευκτα (Liaropoulos, ETH zurich CSS 2014). Αναμφίβολα η κυριαρχία στο

υπόψη χώρο αποτελεί μια προέκταση της γενικότερης έννοιας της κυριαρχίας των κρατών. Ενδεχόμενη πρόκληση ή απειλή της κυριαρχίας στον κυβερνοχώρο δύναται να έχει άμεσες επιπτώσεις στην ανεξαρτησία και αυτονομία τους. Η κυριαρχία γενικότερα δεν πρέπει να θεωρείται ούτε δεδομένη ούτε μη συνδεόμενη με τον κυβερνοχώρο. Μέχρι τώρα φαίνεται πως το κύριο πρόβλημα είναι η έλλειψη διάθεσης για συναίνεση και συνεργασία από τα κράτη, καθώς ο κυβερνοχώρος αποτελεί ένα επιπλέον πεδίο αντιπαράθεσης.

«Κάθε εποχή έχει το δικό της είδος πολέμου, με τους δικούς του περιοριστικούς όρους και τις δικές του ιδιόμορφες προκαταλήψεις»

''Carl Von Clausewitz''

ΚΕΦΑΛΑΙΟ «Β»

Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

ΟΡΙΖΟΝΤΑΣ ΤΟΝ ΚΥΒΕΡΝΟΠΟΛΕΜΟ

Ο πόλεμος ως φαινόμενο αποτελούσε ανέκαθεν ένα μέσο έκφρασης της ισχύος των ομάδων και αργότερα των κρατών. Σύμφωνα με τον Clausewitz, ο πόλεμος ορίζεται ως «πράξη βίας με σκοπό την επιβολή της θέλησης μας στον εχθρό»[13] . Είναι ο ενδεικνυόμενος τρόπος δηλαδή μέσω του οποίου, ένας δρών επιχειρεί να κυριαρχήσει έναντι κάποιου άλλου, προκειμένου να επιτύχει τους αντικειμενικούς τους σκοπούς, κυριότερος εκ των οποίων είναι η εξασφάλιση της ίδιας της κυριαρχίας του και γιατί όχι η επαύξηση των φορτίων ισχύος του.

Η εξέλιξη της επιστήμης και της τεχνολογίας, καθώς και επίσης και της δομής και του τρόπου λειτουργίας των σύγχρονων κρατών, δημιούργησε ευκαιρίες χρήσης και άλλων μέσων για την επιβολή της θέλησης μας επί του αντιπάλου. (Μαυρόπουλος 2014). Ένα από αυτά τα μέσα είναι ο κυβερνοπόλεμος, μια καταναγκαστική πράξη, η οποία περιλαμβάνει επίθεση σε ηλεκτρονικούς υπολογιστές, οι οποίοι είναι διασυνδεδεμένοι σε δίκτυο. Επίθεση σε δίκτυο σημαίνει διατάραξη, υποβάθμιση ή καταστροφή της πληροφορίας. Η έννοια του όρου «καταναγκαστική», συνδέεται με τη χρήση ισχύος, η οποία σκοπό έχει να αλλάξει ή να διατηρηθεί το πολιτικό status quo. (Junio 2013, 126)

Ο κυβερνοπόλεμος επίσης θα μπορούσε να χαρακτηριστεί ως μια κατάσταση σύγκρουσης, μεταξύ δύο ή περισσοτέρων πολιτικών δρώντων, η οποία χαρακτηρίζεται ως σκόπιμη εχθρική και κοστοβόρα χρήση κυβερνοεπιθέσεων, εναντίον των κρίσιμων πολιτικών και στρατιωτικών υποδομών του αντιπάλου, με πρόθεση να αποσπάσει πολιτικές παραχωρήσεις, να μειώσει την ικανότητα του αντιπάλου να αμυνθεί ή να ανταποδώσει χρησιμοποιώντας συμβατική δύναμη και να περιορίσει τον δρώντα από στρατηγικούς σκοπούς. (Liff 2012, 408)

[13] Carl von Clausewitz, στο «Περί του Πολέμου» Βάνιας Ε' Έκδοση Θεσσαλονίκη 1999 σελ,31

Ο κυβερνοπόλεμος απαιτεί επακόλουθες επιπτώσεις στον φυσικό κόσμο ή αλλιώς αυτό που αποκαλούν οι ειδικοί επί στρατιωτικών θεμάτων κινητική επίδραση. (Graw 2013, 112) Ο Nye ορίζει τον κυβερνοπόλεμο, ως εχθρική ενέργεια στον κυβερνοχώρο, η οποία έχει επίδραση που ενισχύει ή είναι ισοδύναμη με χρήση μεγάλης κινητικής βίας. (Brandon Valeriano & Ryan Maness 2014, 348) Τέλος σύμφωνα με τον Αρχιπλοίαρχο (εα) Αντωνόπουλο Δ.[14] κυβερνοπόλεμος είναι η εκμετάλλευση της υποδομής και των διαδικασιών που έχει αναπτύξει ο αντίπαλος… εναντίον του.

Το είδος αυτό του πολέμου παρουσιάζει σαφείς διαφορές από τον παραδοσιακό πόλεμο. Συγκεκριμένα :

α. Δεν προσδιορίζεται γεωγραφικά

β. Απαιτεί ελάχιστο κόστος

γ. Διεξάγεται ταχύτατα

δ. Χαρακτηρίζεται ως ακήρυχτος πόλεμος

ε. Ανήκει στις μορφές του ασύμμετρου πολέμου, δηλαδή είναι αόρατος ως προς την ταυτότητα του επιτιθεμένου, μη προβλέψιμος και τεράστιας καταστροφικότητας. (Γιαννακόπουλος 2010, 2)

Ένα σημείο διαφωνίας ανάμεσα στους κόλπους της ακαδημαϊκής κοινότητας, είναι αν η πρόκληση φυσικών απωλειών είναι αναγκαία προϋπόθεση, ώστε ο κυβερνοπόλεμος να θεωρηθεί πόλεμος με την κλασσική έννοια του όρου. Από τη μέχρι τώρα εφαρμογή του έχει διαπιστωθεί, ότι είναι δύσκολο τα κυβερνοόπλα να προκαλέσουν φονικά αποτελέσματα. (Junio 2013, 126). Δεν είναι λίγοι άλλωστε αυτοί που ισχυρίζονται, ότι «τα πακέτα δεδομένων δεν είναι ικανά να κρατήσουν έδαφος». (Liff 2012, 403)

ΜΟΡΦΕΣ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ

Στρατηγικός Κυβερνοπόλεμος

[14] Ο Αρχιπλοίαρχος (εα) Αντωνόπουλος Δ.ΠΝ ανήκει στον πυρήνα των στελεχών που συγκρότησαν και συνέβαλλαν στην ανάπτυξη της Διεύθυνσης Κυβερνοάμυνας του ΓΕΕΘΑ (ΔΙΚΥΒ) http://www.kathimerini.gr/954351/article/epikairothta/ellada/ellhnotoyrkikos-polemos-xaker

Μια εκστρατεία κυβερνοεπιθέσεων που ξεκινά από μια οντότητα εναντίον ενός κράτους και της κοινωνίας του, κυρίως αλλά όχι αποκλειστικά, με σκοπό να επηρεάσει τη συμπεριφορά του κράτους-στόχου, είναι στρατηγικός κυβερνοπόλεμος. Η επιτιθέμενη οντότητα μπορεί να είναι ένας κρατικός ή μη κρατικός δρώντας. Αν ο επιτιθέμενος είναι μη κρατική οντότητα, είναι δύσκολο για το κράτος στόχο να αντιδράσει προσβάλλοντας στόχο αναλόγου σπουδαιότητας ως αντίποινα. Μια περίπτωση ωστόσο είναι να κινηθεί ενάντια στα κράτη που υποστηρίζουν ή ενισχύουν τη μη κρατική οντότητα, να ενεργεί επιθετικά στον κυβερνοχώρο στρέφοντας την αντίδραση του προς αυτά. (Libicki 2009, 117)

Τα κράτη μπορούν να βρεθούν εμπλεκόμενα σε κυβερνοπόλεμο με έναν από τους δύο τρόπους: μέσω εσκεμμένης πρόκλησης ή μέσω κλιμάκωσης. Ένας κυβερνοπόλεμος μπορεί να προκύψει σκόπιμα, από την πεποίθηση ενός κράτους, ότι μπορεί να κερδίσει πλεονεκτήματα έναντι άλλου, διακόπτοντας τη λειτουργία ή προκαλώντας σύγχυση στα πληροφοριακά του συστήματα. Μπορεί επίσης να ξεκινήσει ως μια κλιμάκωση κρίσης, η οποία θα συνοδευτεί από τις επακόλουθες προσπάθειες αντιστάθμισης της. Και στις δύο περιπτώσεις, η εκδήλωση του κυβερνοπολέμου σημαίνει, ότι η πρωτογενής αποτροπή απέτυχε. Ωστόσο, η δευτερογενής αποτροπή, η οποία στηρίζεται στην ικανότητα να καθιερωθούν «κόκκινες» γραμμές μέσω της πράξης του κυβερνοπολέμου μπορεί να επιτύχει. (Libicki 2009, 118)

Και στις δύο περιπτώσεις, πρέπει να θεωρείται ότι τα κράτη συμμετέχουν στον κυβερνοπόλεμο για να επιτύχουν συγκεκριμένους αντικειμενικούς σκοπούς, και ότι η συμμετοχή τους δεν αποτελεί αυτοσκοπό. Τα κράτη δεν μπορεί να θεωρηθούν εξ ολοκλήρου ορθολογικοί δρώντες, με την έννοια ότι έχουν πάντα τη δυνατότητα να εκτιμούν ψύχραιμα το κόστος και τα κέρδη ενός πολέμου. Ο κυβερνοπόλεμος έχει εξωτερικούς και εσωτερικούς αντικειμενικούς στόχους. Ο εξωτερικός στόχος είναι ο κυρίαρχος λόγος για την εφαρμογή του κυβερνοπόλεμου (π.χ., να καταβάλλει η μια πλευρά την άλλη ώστε να ενεργεί αυτή σύμφωνα με τη θέληση της). Ο εσωτερικός στόχος αφορά τη διαχείριση των συγκρούσεων και την αποφυγή της κλιμάκωσης της βίας. (Libicki 2009, 118)

Ο στρατηγικός κυβερνοπόλεμος χρησιμοποιείται για να ενημερώσει την αντίπαλη πλευρά, ότι τα συστήματά της δεν είναι τόσο αξιόπιστα, ώστε να μπορεί

να αντέξει οικονομικά να συμμετάσχει σε έναν τέτοιο αγώνα. Μια συνήθης αλληλουχία ενεργειών περιλαμβάνει, έναν επιτιθέμενο ο οποίος σβήνει τα φώτα μιας μεγάλης πόλης στόχου. Η πράξη (και όχι ο επιτιθέμενος, ο οποίος διατηρείται όσο το δυνατόν περισσότερο στο παρασκήνιο) προσελκύει την προσοχή της ηγεσίας του κράτους-στόχου, η οποία αντιλαμβάνεται ότι οι υποδομές του κράτους είναι ευάλωτες. Στη συνέχεια, δεσμεύεται, ότι μια τέτοια ενέργεια δεν θα ξανασυμβεί και μόλις αρχίσει να νιώθει ότι πλησιάζει στην επίτευξη της επιτυχίας, ο επιτιθέμενος κινείται ξανά ενάντια στον αρχικό στόχο ή αλλάζει την υποδομή - στόχο προκαλώντας επίδραση, που είναι εξίσου κρίσιμη και αντιληπτή από το σύνολο της κοινωνίας. Αυτό πέραν του ότι σηματοδοτεί ότι τα τρωτά σημεία του κράτους εξακολουθούν να υφίστανται, επιτυγχάνει όχι μόνο να μειώσει την αξιοπιστία της ασφάλειας του συστήματος πληροφοριών του κράτους στόχου, αλλά και να μειώσει την αξιοπιστία της ηγεσίας του, να εξασφαλίσει ασφαλείς συνθήκες στους πολίτες του. Στην πραγματικότητα, η ίδια η επίθεση δεν είναι τόσο το θέμα, όσο είναι να εδραιωθεί μια γενική αίσθηση στον κοινωνικό ιστό του κράτους στόχου ότι τα συστήματα πληροφοριών της άλλης πλευράς είναι εύθραυστα και αναξιόπιστα. (Libicki 2009, 126 - 127)

Μια από τις μεγαλύτερες προκλήσεις κατά τη διεξαγωγή εκστρατείας στον κυβερνοχώρο είναι να διασφαλιστεί ότι το πρώτο χτύπημα δεν δημιουργεί συνθήκες που θα αμβλύνουν τις επιδράσεις του δεύτερου. Ειδικότερα οι επιτιθέμενοι μπορούν να λάβουν μέτρα για να επιβραδύνουν τις προσπάθειες των κρατών θυμάτων να γίνουν λιγότερο ευάλωτα, όπως είναι τα εξής (Libicki 2009, 127 - 128) :

α. Να προκαλούν σφάλματα που μοιάζουν σαν να μπορούσαν να προκύψουν από αποτυχίες λογισμικού και μεταβατικές συνθήκες και όχι από επιθέσεις αυτές καθαυτές.

β. Να βρίσκουν τρόπους να εξετάσουν το σύστημα στόχο σε μια αντίδραση, που είναι λιγότερο πιθανό να προκαλέσει αλλαγές στο σύστημα ως αντίδραση (οι αμυνόμενοι είναι λιγότερο πιθανό να κάνουν ριζικές αλλαγές εάν πιστεύουν ότι έχουν νικήσει τους επίδοξους επιτιθέμενους).

γ. Να εκτελούν επίθεση εναντίον συγκεκριμένων τρωτών σημείων του συστήματος του αντιπάλου παρά εναντίον των γενικών τρωτών σημείων.

δ. Να αναζητούν και να επιλέγουν στόχο, που δεν προτίθεται να δημοσιοποιήσει τις επιδράσεις της επίθεσης είτε για λόγους διατήρησης του κύρους μεταξύ των συμμάχων του, είτε για αποφυγή οικονομικού κόστους. Με αυτόν τον τρόπο μια συγκεκριμένη αδυναμία, η οποία έγινε αντικείμενο εκμετάλλευσης μπορεί να χρησιμοποιηθεί και πάλι εναντίον άλλου στόχου.

ε. Να αξιοποιούν τις αδυναμίες του συστήματος το συντομότερο, προτού μπορέσει το προσβαλλόμενο κράτος να τις απομονώσει και να καταστούν άχρηστες.

στ. Να επιδιώκουν την εκμετάλλευση των τρωτών σημείων που μπορεί να αποκαλυφθούν μόνο από μια επίπονη αναζήτηση.

θ. Να επιλέγουν τύπους επιθέσεων που είναι σχετικά ανθεκτικές στα απλά αντίμετρα, όπως η αποσύνδεση συστημάτων, τα οποία δεν θα έπρεπε να έχουν συνδεθεί εξαρχής.

Τέλος θα πρέπει να επισημανθεί, πως ο στρατηγικός κυβερνοπόλεμος δεν αποτελεί πανάκεια για την επίτευξη όλων των στόχων των εμπλεκομένων. Υπάρχουν σαφή όρια στις δυνατότητες επιτυχίας μέσα από αυτό το είδος πολέμου. Η χρήση των κυβερνοόπλων μπορεί να γίνει για την επίτευξη περιορισμένων σκοπών. Οι υπέρμαχοι του κυβερνοπόλεμου προσπαθούν να βρουν ομοιότητες κατ' αναλογία του στρατηγικού κυβερνοπολέμου με το στρατηγικό αεροπορικό βομβαρδισμό και τον πυρηνικό πόλεμο, κάτι το οποίο είναι σαφώς παραπλανητικό, καθώς τα αποτελέσματα των δύο τελευταίων περιπτώσεων δεν μπορούν να συγκριθούν με αυτά των κυβερνοεπιθέσεων. Επίσης θα πρέπει να ληφθεί υπόψη πως σε αντίθεση με τον συμβατικό πόλεμο, τα αποτελέσματα του κυβερνοπολέμου χαρακτηρίζονται ως προσωρινά, γεγονός που δρα ενισχυτικά στην πεποίθηση της κοινής γνώμης για μη συναίνεση σε εξαναγκασμό. (Χαίδης 2012, 40)

Επιχειρησιακός Κυβερνοπόλεμος

Ο επιχειρησιακός κυβερνοπόλεμος αποτελείται από επιθέσεις στον κυβερνοχώρο κατά την διάρκεια συμβατικού πολέμου ενάντια στρατιωτικών και πολιτικών στόχων που σχετίζονται με τις Ένοπλες Δυνάμεις του αντιπάλου. Αν και δεν συνιστά χρήση ωμής ισχύος, μπορεί να αποτελέσει ένα αποφασιστικό

πολλαπλασιαστή ισχύος εφόσον χρησιμοποιηθεί προσεχτικά, διακριτικά και με ακρίβεια στον κατάλληλο χρόνο. (Libicki 2009, 139)

Η συζήτηση για τον επιχειρησιακό κυβερνοπόλεμο απαιτεί διευκρίνιση δύο θεμάτων. Πρώτον, ότι δεν μπορεί να κερδίσει από μόνος του ένα συνολικό πόλεμο. Αποτελεί μια λειτουργία υποστήριξης και είναι πιθανό να παραμείνει με αυτό το ρόλο και στο μέλλον. Επίσης δεν μπορεί να καταλάβει έδαφος, ούτε θέτει σε κίνδυνο τις ζωές των ανθρώπων. Τα άμεσα αποτελέσματα των κυβερνοεπιθέσεων, αν ποτέ ανακαλυφθούν, μπορούν συχνά να αντιστραφούν εντός ωρών ή το πολύ, εβδομάδων. Οι κυβερνοεπιθέσεις πιθανόν να είναι πολύ αδύναμες για να εξαναγκάσουν έναν πληθυσμό να παραδοθεί, ιδιαίτερα αν έχει προλάβει να σκληραγωγηθεί από τις ακραίες συνθήκες ενός πραγματικού πολέμου που διεξάγεται ταυτόχρονα. Δεύτερον, το ζήτημα της κυριαρχίας στον κυβερνοχώρο δεν έχει νόημα και συνεπώς δεν είναι ο καταλληλότερος στόχος για τον επιχειρησιακό κυβερνοπόλεμο. Η επίτευξη της κυριαρχίας είναι αδύνατη επειδή ο κυβερνοχώρος δεν είναι ενιαία περιοχή. (Libicki 2009, 140-141)

Ο επιχειρησιακός κυβερνοπόλεμος μπορεί να παίξει τρεις βασικούς ρόλους: Μπορεί να παρακωλύσει τις δυνατότητες των αντιπάλων γρήγορα, αν αυτοί αιφνιδιαστούν. Μπορεί να χρησιμοποιηθεί ως αιχμή του δόρατος σε περιορισμένες περιπτώσεις, παρέχοντας ένα προσωρινό αλλά δυνητικά αποφασιστικό στρατιωτικό πλεονέκτημα. Μπορεί επίσης να εμποδίσει τον αντίπαλο να χρησιμοποιεί με αυτοπεποίθηση τα συστήματά του. Οι κυβερνοεπιθέσεις αποσκοπούν στην εξαπάτηση και η ουσία της εξαπάτησης είναι η διαφορά ανάμεσα σε αυτό που αναμένει ο αντίπαλος και σε αυτό που τελικά λαμβάνει και συνιστά τον αιφνιδιασμό του. Βασική αποστολή του επιχειρησιακού κυβερνοπολέμου, είναι η εκτέλεση αιφνιδιαστικών επιθέσεων παρέχοντας παράλληλα περιορισμένες επιλογές για επαναλαμβανόμενες επιθέσεις καθώς είναι δύσκολο να αιφνιδιάσεις το ίδιο αντίπαλο δύο φορές με τον ίδιο τρόπο. (Libicki 2009, 142 - 143)

Ο αιφνιδιασμός, τόσο σε στρατηγικό όσο και σε επιχειρησιακό επίπεδο, λειτουργεί διαφορετικά στον κυβερνοχώρο από ότι στον φυσικό χώρο. Ο στρατηγικός αιφνιδιασμός είναι ανάλογος της χρήσης του κυβερνοπολέμου λίγο πριν ή στην αρχή μιας στρατιωτικής εμπλοκής. Ο επιχειρησιακός αιφνιδιασμός εξακολουθεί να είναι εφικτός ακόμα και μετά την έναρξη του πολέμου και την

επακόλουθη θωράκιση των δικτύων του στόχου, απόρροια των αυξημένων μέτρων συναγερμού από την επίθεση. Μόλις ξεκινήσει μια αιφνιδιαστική επίθεση, ο επιχειρησιακός κυβερνοπόλεμος είναι πιθανό να αλλάξει από όπλο γενικού σκοπού σε όπλο για ειδικές περιπτώσεις και κατά ειδικών στόχων. Τέτοιοι στόχοι θα διερευνηθούν διεξοδικά για να ανακαλυφθούν ασυνήθιστα ευάλωτα σημεία, των οποίων η εκμετάλλευση εξαρτάται από κρίσιμο χρονοδιάγραμμα (Libicki 2009, 149)

Ο επιχειρησιακός κυβερνοπόλεμος μπορεί επίσης να χρησιμοποιηθεί, για να καταστήσει τον εχθρό επιφυλακτικό με τη χρήση των δικτύων, με απώτερο σκοπό να οδηγηθεί στην απομόνωση για να εξασφαλίσει τις οργανικές δυνατότητές του. Αυτό είναι ένα αρκετά πιθανό κίνητρο για μια κυβερνοεπίθεση στην ειρήνη, το αποτέλεσμα όμως θα μπορούσε να είναι πιο έντονο κατά τη διάρκεια του πολέμου. Οι οργανισμοί έχουν τη φυσική τάση, να κλείνονται στον εαυτό τους όταν απειλούνται. Ο ρόλος του επιχειρησιακού κυβερνοπολέμου είναι η στοχοποίηση αυτών των τάσεων. Ο αντίπαλος θα πρέπει να γνωρίζει συνεχώς τη πιθανότητα - και ιδιαίτερα τις συνέπειες - μιας επιτυχημένης κυβερνοεπίθεσης. (Libicki 2009, 150)

Κατά ειρωνικό τρόπο, ένας άλλος ρόλος για τον επιχειρησιακό κυβερνοπόλεμο είναι η δημιουργία και όχι η καταστροφή, συνήθως άχρηστων, πληροφοριών. Τη σημερινή εποχή, η καταστροφή των πληροφοριών έχει γίνει σχεδόν αδύνατη καθώς οι πηγές πληροφοριών πολλαπλασιάζονται, όπως και οι τρόποι πρόσβασης σε αυτές. Αυτό που μπορεί να κάνει ο επιχειρησιακός κυβερνοπόλεμος είναι, να δημιουργήσει κανάλια μέσω των οποίων μεταδίδεται ένας τεράστιος όγκος πληροφοριών στους αντιπάλους, προκαλώντας την υπερφόρτωση των πληροφοριακών τους συστημάτων. (Libicki 2009, 152)

Παρά το γεγονός ότι η σημερινή εποχή χαρακτηρίζεται ως η εποχή της πληροφορίας ο επιχειρησιακός κυβερνοπόλεμος δεν θα πρέπει να θεωρείται η αρχή και το τέλος των στρατιωτικών επιχειρήσεων. Αν επεκταθεί η χρήση του τόσο πολύ, θα καταλήξει να μην μπορεί να ανταποκριθεί στον υποστηρικτικό του ρόλο. Όσοι εφαρμόζουν τον επιχειρησιακό κυβερνοπόλεμο γνωρίζουν, ότι οι καλύτερες επιθέσεις στον κυβερνοχώρο έχουν περιορισμένη διάρκεια ζωής και πρέπει να χρησιμοποιούνται με φειδώ. Ο επιχειρησιακός κυβερνοπόλεμος εάν εφαρμοστεί ορθά μπορεί να αποτελέσει καθοριστικό παράγοντα στην εξέλιξη των

επιχειρήσεων. Αν και ο κόσμος δεν έχει βιώσει μέχρι σήμερα επιχειρησιακό κυβερνοπόλεμο η καλύτερη εικασία για το τι είναι περιλαμβάνει ότι (Libicki 2009, 158):

α. Είναι άμεσος, αιφνιδιαστικός και με σκοπό την εκμετάλλευση των τρωτοτήτων του αντιπάλου.

β. Είναι ένα προσεκτικά συγκροτημένο σύνολο εξακριβωμένων στόχων και χρονικών επιδράσεων.

γ. Είναι μια υγρή κουβέρτα τοποθετημένη στην κορυφή των φιλοδοξιών του αντιπάλου για την ανάπτυξη δικτυοκεντρικών επιχειρησιακών δυνατοτήτων.

ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΠΟΛΙΤΙΚΗ

Ο πόλεμος, σύμφωνα με τον καθηγητή Κουσκουβέλη, θεωρείται ένα σημαντικό εργαλείο της πολιτικής, καθώς είναι η συνέχιση της με άλλα μέσα. (Κουσκουβέλης 2007, 325) Τα κράτη, σε περίπτωση αντιπαράθεσης με άλλες κρατικές ή μη οντότητες κινητοποιούν όλα τα διαθέσιμα μέσα τους προκειμένου να αξιοποιήσουν βέλτιστα την κατεχόμενη ισχύ τους. Η ενορχήστρωση των ανωτέρω διαθέσιμων μέσων, τα οποία το κράτος έχει στη διάθεση του, για τη διεξαγωγή του πολέμου ή τη διαχείριση μιας κρίσης γενικότερα, με σκοπό την επίτευξη του πολιτικού σκοπού του πολέμου, αποτελεί το προνομιακό πεδίο της υψηλής στρατηγικής. (Μαυρόπουλος 2014) Ο κυβερνοπόλεμος, παρά το γεγονός ότι το δεύτερο συνθετικό της λέξης (πόλεμος) παραπέμπει στις Ένοπλες Δυνάμεις δεν αφορά μόνο αυτές. Αφορά το κράτος στο σύνολο του διότι οι απειλές του απευθύνονται σε όλους τους τομείς της κυβερνητικής δραστηριότητας.

Οι τέσσερις βασικοί – καίτοι όχι μοναδικοί – συντελεστές, με βάση τους οποίους μπορεί να αξιολογηθεί σχετικά και να προσδιοριστεί η ισχύς των κρατών είναι οι εξής (Μποζίνης & Μικέλης 2018, 40) :

α. Οικονομικός

β. Δημογραφικός

γ. Τεχνολογικός

δ. Στρατιωτικός

Ως μέρος του τεχνολογικού συντελεστή ισχύος ο κυβερνοπόλεμος αποτελεί ένα μέσο στη διάθεση της κυβέρνησης ενός κράτους, ένα εργαλείο, για την αντιμετώπιση μιας κρίσης και τη διατήρηση της ισορροπίας ισχύος πετυχαίνοντας το αναίμακτα και καθαρά. Η δυνατότητα αυτή οδήγησε υψηλόβαθμό αξιωματικό των Ενόπλων Δυνάμεων των ΗΠΑ, να δηλώσει ότι η τεχνολογία της πληροφορίας είναι το δώρο της Αμερικής στον πόλεμο[15], υπονοώντας ότι δίνει την δυνατότητα επίτευξης του σκοπού αποφεύγοντας παράλληλα τα έξοδα και τις απώλειες που ένας πραγματικός πόλεμος επισύρει. Υπερθεματίζοντας σ' αυτό θα μπορούσαμε να ισχυριστούμε, ότι ο κυβερνοπόλεμος ενδεχομένως να αποτελεί τον πλέον ενδεδειγμένο τρόπο προκειμένου να γίνει πράξη αυτό που αποτελεί κορωνίδα της στρατηγικής του Σούν Τζού, ότι δηλαδή η ακμή της ικανότητας είναι να κερδίζεις δίχως να πολεμάς.

Οι πολιτικοί σκοποί, οι οποίοι επιδιώκονται χρησιμοποιώντας ως μέσο τον κυβερνοπόλεμο, είναι η απλή παρενόχληση με σκοπό την υπενθύμιση των δυνατοτήτων στον αντίπαλο, η έμμεση προειδοποίηση πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών και τέλος η εκδίκηση για αποφάσεις που ληφθήκαν εις βάρος των συμφερόντων της ενδιαφερόμενης χώρας. (Μαυρόπουλος 2014)

ΑΠΕΙΛΕΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Παρά τα αναμφισβήτητα οφέλη, τα οποία παρέχει ο κυβερνοχώρος στην ανθρωπότητα, ιδιαίτερα μέσα από τις υπηρεσίες του διαδικτύου (internet), αποτελεί ταυτόχρονα και κατά γενική ομολογία ένα χώρο τέλεσης κακόβουλων πράξεων και επιχειρήσεων, οι οποίες απευθύνονται τόσο κατά των ανθρώπων όσο κατά κρατικών αλλά και μη κρατικών δρώντων. Είναι κοινή διαπίστωση, ότι οι δυνατότητες αλλά και η αποτελεσματικότητα των ενεργειών τους αυξάνονται με τρόπο ανάλογο με τον οποίο αυξάνεται και η εξάρτηση των σημερινών κοινωνιών και των ανθρώπων από το διαδίκτυο και τη τεχνολογία.

Ο πρώην πρόεδρος των ΗΠΑ Μπάρακ Ομπάμα σε άρθρο του στην Wall Street Journal επιβεβαίωσε τα ανωτέρω ομολογώντας, ότι «…τα συστήματα υπολογιστών σε κρίσιμους τομείς της οικονομίας των ΗΠΑ, συμπεριλαμβανομένου της πυρηνικής και της χημικής βιομηχανίας, παρουσιάζουν διαρκώς μια αυξητική

[15] Karatzogianni, The Politics of Cyberconflict 2006, 99

τάση σε ότι αφορά την στοχοποίηση τους. Σε μια μελλοντική σύγκρουση μ' έναν αντίπαλο, ο οποίος δεν θα είναι σε θέση να αντιπαρατάξει στρατιωτική ισχύ ανάλογη με αυτή των ΗΠΑ, θα επιδιώξει να εκμεταλλευτεί τις τρωτότητες των δικτύων υπολογιστών στο εσωτερικό της χώρας. Θέτοντας εκτός ενεργείας το τραπεζικό σύστημα θα μπορούσε να πυροδοτήσει μια οικονομική κρίση. Η έλλειψη καθαρού πόσιμου νερού ή λειτουργικών νοσοκομείων θα μπορούσε να θέσει σε κίνδυνο την δημόσια υγεία. Ενώ έχει διαπιστωθεί στο παρελθόν ότι η διακοπή και η απώλεια ρεύματος μπορεί να προκαλέσει στασιμότητα σε επιχειρήσεις, πόλεις και ολόκληρες περιοχές». (Lindsay 2014/2015, 29) Αυτή η δημόσια παραδοχή της «αχίλλειου πτέρνας» μιας υπερδύναμης όπως οι ΗΠΑ, μιας χώρας η οποία οδηγεί τις εξελίξεις στη τεχνολογία σε παγκόσμιο επίπεδο, οδηγεί στο συμπέρασμα, ότι οι χώρες οι οποίες εξαρτώνται σε μεγάλο βαθμό από την πληροφοριακή υποδομή και την τεχνολογία, ακόμα και αν πρόκειται για υπερδυνάμεις, όπως οι ΗΠΑ, αντιμετωπίζουν την απειλή να βρεθούν σε μειονεκτική θέση κατά τη διάρκεια μιας αντιπαράθεσης, πριν ακόμη ξεκινήσουν οι στρατιωτικές επιχειρήσεις.

Οι επιχειρήσεις στον κυβερνοχώρο εστιάζουν στην χρήση της υπόψη περιοχής για την επίθεση κατά του προσωπικού, των εγκαταστάσεων ή του εξοπλισμού του αντιπάλου με σκοπό την υποβάθμιση, την αδρανοποίηση ή την καταστροφή της εχθρικής μαχητικής ικανότητας, με ταυτόχρονη προστασία της δικής μας μαχητικής ικανότητας. Αντικειμενικός σκοπός των ανωτέρω επιχειρήσεων είναι ο αντίπαλος να μην μπορεί να έχει ελευθερία κινήσεων στον κυβερνοχώρο. Οι υπόψη επιχειρήσεις - γνωστές και ως CNO (Computer Network Operations) - λαμβάνουν τρείς μορφές: την επίθεση σε δίκτυα Η/Υ (Computer Network Attack – CNA), την εκμετάλλευση των δικτύων Η/Υ (Computer Network Exploitation – CNE) και την άμυνα στα δίκτυα Η/Υ (Computer Network Defence) (Χαίδης 2012, 35).

Ποιες είναι ωστόσο οι απειλές που μπορούν να πυροδοτήσουν τις επιχειρήσεις στον κυβερνοχώρο και τι συνιστά τελικά κυβερνοαπειλή; Κάθε μη εξουσιοδοτημένη προσπάθεια πρόσβασης σ' ένα σύστημα ελέγχου ή δίκτυο, μέσω της χρήσης ενός διαύλου ροής πληροφοριών, ονομάζεται κυβερνοαπειλή (Γιαννακόπουλος 2010). Οι απειλές στον κυβερνοχώρο χρησιμοποιώντας ως κριτήριο την μέθοδο και τον τρόπο εφαρμογής τους κατανέμονται σε τρείς κατηγορίες. Πρόκειται για απειλές από φυσικές και ηλεκτρομαγνητικές επιθέσεις

και από κυβερνοεπιθέσεις. Οι τελευταίες, που αποτελούν και αντικείμενο της μελέτης, αναφέρονται στη χρήση Η/Υ για πολιτικούς ή στρατηγικούς σκοπούς. Χαρακτηρίζονται από την επιθυμία και την ικανότητα του επιτιθέμενου να διακόψει την λειτουργία των Η/Υ και των δικτύων τους ή να καταστρέψει φυσικούς στόχους μέσω του κυβερνοχώρου και είναι αποτέλεσμα της χρήσης κυβερνοόπλων. (Kello 2013, 19)

Στον κυβερνοχώρο οι απειλές ομαδοποιούνται σε κατηγορίες κυρίως με βάση το σκοπό για τον οποίο εκτελούνται. Οι κατηγορίες τους κατά αυξανόμενο επίπεδο σε ότι αφορά την επίδραση που μπορούν να επιφέρουν είναι:

α. Μεμονωμένοι Χάκερς - Κράκερς

β. Ακτιβιστές Χάκερς

γ. Εσωτερικοί δράστες χωρίς πρόθεση

δ. Ομάδες χάκερς – κράκερς

ε. Δράστες βιομηχανικής κατασκοπίας

στ. Οργανωμένο έγκλημα

ζ. Φυσικές και περιβαλλοντολογικές επιθέσεις

η. Τρομοκρατικές οργανώσεις

θ. Εσωτερικοί δράστες και Εξωτερικοί συνεργάτες/σύμβουλοι με πρόθεση

ι. Χώρες

Η στοχοποίηση των επιτιθέμενων περιλαμβάνει (Χαίδης 2012, 16-17) :

α. Τη διατήρηση της διαβάθμισης των ψηφιακών δεδομένων (Confidentiality). Σ’ αυτή τη κατηγορία περιλαμβάνεται κάθε προσπάθεια απόκτησης πληροφορίας, χωρίς την απαιτούμενη εξουσιοδότηση. Αυτό μπορεί να προκύψει και μέσα από τον έλεγχο ροής των δεδομένων (Traffic Analysis), καθώς δίδονται στοιχεία για το περιεχόμενο της επικοινωνίας.

β. Την ακεραιότητα των δεδομένων (Integrity). Σ’ αυτή τη περίπτωση περιλαμβάνεται κάθε ενέργεια που αποσκοπεί στη χωρίς εξουσιοδότηση τροποποίηση των πληροφοριών και των βάσεων δεδομένων (databases)

γ. Τη διαθεσιμότητα των δεδομένων (Avalaibility). Σ' αυτή τη περίπτωση περιλαμβάνεται κάθε ενέργεια που αποσκοπεί στη διακοπή της ομαλή ροής των ψηφιακών δεδομένων μέσω μιας διαδικασίας γνωστής και ως Denial of Service (DoS).

Οι φυσικοί στόχοι των επιθέσεων μπορεί να είναι στρατιωτικές και μη στρατιωτικές υποδομές. Στην πρώτη περίπτωση επιδιώκεται η απενεργοποίηση των οπλικών συστημάτων και η διαταραχή του συστήματος διοίκησης και ελέγχου του αντιπάλου ενώ στη δεύτερη περίπτωση επιδιώκεται η εξασθένηση της ικανότητας και της θέλησης του αντιπάλου να διεξάγει πόλεμο για μεγάλο χρονικό διάστημα (Χαίδης 2012, 37). Σε κάθε περίπτωση αυτό που επιδιώκεται είναι η ανάπτυξη μηχανισμών, διαδικασιών και δυνατοτήτων, για τον έλεγχο, την επιρροή και την καταστροφή του κυβερνοχώρου του αντιπάλου.

Το πρώτο βήμα προκειμένου να καταστεί εφικτή η απόκτηση δυνατότητας εκτέλεσης επίθεσης, περιλαμβάνει την ανάπτυξη του κατάλληλου κυβερνοόπλου. Αυτό, όταν ο στόχος είναι οι μη στρατιωτικές υποδομές μπορεί να αποδειχθεί ιδιαίτερα εύκολο καθώς αποτελούνται από συστήματα δίχως ασφάλεια από κατασκευής (Peterson 2013, 1). Τα κυβερνοόπλα είναι κώδικες Η/Υ, οι οποίοι χρησιμοποιούνται ή έχουν σχεδιασθεί για να χρησιμοποιηθούν με σκοπό την απειλή ή την πρόκληση φυσικής, λειτουργικής ή ψυχικής βλάβης σε κατασκευές, συστήματα ή ανθρώπους (Brandon Valeriano & Ryan Maness 2014, 352).

Η διαδικασία προκειμένου να επιτεθεί ένα κράτος ή οργανισμός, απαιτεί αρχικά την γνώση της κρίσιμης υποδομής του αντιπάλου κάτι το οποίο ενδεχομένως να γίνει ή από ανοιχτές πηγές ή να προκύψει ως προϊόν πληροφοριακών επιχειρήσεων ανάλογα με το είδος του στόχου. Αυτό θα δώσει την δυνατότητα να διαπιστωθούν οι αδυναμίες του πιθανού στόχου και να υποδείξει τον τρόπο μέσω του οποίου θα επιτευχθεί η αναγκαία πρόσβαση στο λειτουργικό (hardware) και το λογισμικό (software) αυτού. Κατόπιν οι επιλογές για τον επιτιθέμενο είναι (Peterson 2013, 2) :

α. Η δημιουργία ενός απλού επιθετικού όπλου με το οποίο ο επιτιθέμενος εκμεταλλευόμενος την έλλειψη του έλεγχου αυθεντικότητας, δύναται να προκαλέσει την πτώση του συστήματος ή την μη ορθή λειτουργία του θέτοντας το εκτός ενεργείας.

β. Η δημιουργία ενός μέτριου επιθετικού όπλου μέσω του οποίου γίνεται γνωστή η διαδικασία λειτουργίας του προσβαλλόμενου συστήματος, επιτρέποντας του να καταστρέψει φυσικά ένα υποσύστημα του, το οποίο θα χρειαστεί χρόνο για να αποκατασταθεί.

γ. Η δημιουργία ενός πολύπλοκου επιθετικού όπλου, το οποίο επεμβαίνει στη λειτουργία του προσβαλλόμενου συστήματος με τρόπο που δεν γίνεται αντιληπτός.

Τα κυβερνο-όπλα προφανώς διαφέρουν στον τύπο, τη διάκριση, τη χρήση και την εφαρμογή. Υπάρχουν τέσσερεις μέθοδοι, τις οποίες έχουν στην διάθεσή τους οι εμπνευστές των συγκρούσεων στον κυβερνοχώρο. (Brandon Valeriano & Ryan Maness 2014, 353-354):

α. Παραμόρφωση ιστοσελίδων ή βανδαλισμός (Website Defacement or Vandalism)

Είναι η απλούστερη μορφή, η οποία έχει σκοπό την κατάληψη της ιστοσελίδας «θύματος» για λίγες ώρες ή μέρες, προβάλλοντας κάποιο μήνυμα ή κάποια εικόνα, η οποία έχει σκοπό την προσβολή της. Γενικώς αυτοί οι τύποι επιθέσεων περιέχουν ένα στοιχείο προπαγάνδας. Είναι επίσης και μια μορφή ελέγχου που ο επιτιθέμενος υποδηλώνει στο στόχο, ότι έχει την δυνατότητα να ελέγξει τις επιχειρήσεις του κυβερνοχώρου τους.

β. Κατανεμημένη άρνηση υπηρεσιών (Distributed Denial of Service – DdoS)

Αυτή η μορφή επιχειρεί να κατακλύσει ιστοσελίδες (internet sites), διακομιστές (servers) ή δρομολογητές (routers) με αιτήσεις για πολύ περισσότερα δεδομένα από αυτά που μπορούν να διαχειριστούν ή να επεξεργαστούν. Τελικός σκοπός είναι να κλείσει η τοποθεσία εμποδίζοντας έτσι την χρήση ή την πρόσβαση.

γ. Εισβολή (Intrusion)

Οι εισβολές περιλαμβάνουν ιούς τύπου trojans[16], trapdoors[17] και backdoors[18] οι οποίοι είναι μη εξουσιοδοτημένο λογισμικό που προστίθεται σ' ένα

[16] Ένας Δούρειος ίππος ή Trojan είναι ένα είδος κακόβουλου λογισμικού που συχνά μεταμφιέζεται ως νόμιμο λογισμικό. Οι δούρειοι ίπποι μπορούν να χρησιμοποιηθούν από τους χάκερ που

πρόγραμμα και επιτρέπει μελλοντική πρόσβαση στην ιστοσελίδα. Οι ιοί απαιτείται να προστεθούν στο λογισμικό, μπορούν να παραμείνουν αδρανείς για μακρύ χρονικό διάστημα, να διαδοθούν δίχως προειδοποίηση και να μετατραπούν σε κακόβουλα προγράμματα μόλις γίνουν επιχειρησιακά. Ο σκοπός των trapdoors και των backdoors είναι η κλοπή ευαίσθητου και διαβαθμισμένου υλικού από ασφαλείς ιστοσελίδες. Η διαφορά των trojans και των trapdoors είναι, ότι οι τελευταίοι δεν χρειάζονται ανθρώπινη παρέμβαση για να ξεκινήσουν την εκτέλεση της λειτουργίας τους σε αντίθεση με τους πρώτους.

δ. Διεισδύσεις (Infiltrations)

Οι Διεισδύσεις μαζί με κάποιες περιπτώσεις εισβολών, είναι οι μέθοδοι που μπορούν να λογιστούν ως πράξη πολέμου σύμφωνα με διακήρυξη του Υπουργείου Εθνικής Άμυνας των ΗΠΑ από το 2011. Οι διεισδύσεις διαφέρουν από τις εισβολές στις μεθόδους που χρησιμοποιούνται για να διαπεράσουν το σύστημα στόχο. Υπάρχουν πέντε κύριες μέθοδοι διεισδύσεων: logic bombs, ιοί (viruses), worms, packet sniffers και keystroke logging. Όλες οι μέθοδοι είναι επιθέσεις ακριβείας, οι οποίες επιδιώκουν την απόκτηση συγκεκριμένων δεδομένων ή εξαναγκάζουν τους Η/Υ ή τα δίκτυα να αναλαμβάνουν έργα, τα οποία υπό κανονικές συνθήκες δεν θα το έπρατταν.

Η αναφορά στις μεθόδους επιθέσεων στον κυβερνοχώρο ολοκληρώνεται με τις προηγμένες επίμονες απειλές (Advanced Persistent Threat's - APTs), οι οποίες έχουν εφαρμογή σε οποιαδήποτε από τις τέσσερις μεθόδους που αναφέρθηκαν παραπάνω. Οι APT διαφέρουν από τις παραδοσιακές μεθόδους. Είναι προσαρμοσμένες στο προσβαλλόμενο σύστημα, κινούνται πιο αργά για να αποφευχθεί η ανίχνευση τους, οι προθέσεις τους είναι συνήθως πιο κακόβουλες και προηγμένες ενώ σχεδόν σίγουρα προέρχονται από κράτη και οι στόχοι τους

προσπαθούν να αποκτήσουν πρόσβαση στα συστήματα των χρηστών. Οι χρήστες τυπικά εξαπατούνται από κάποια μορφή κοινωνικής μηχανικής για τη φόρτωση και την εκτέλεση Trojans στα συστήματά τους. https://en.wikipedia.org/wiki/Trojan_horse_(computing)

[17] Οι θύρες παγίδευσης, που επίσης αναφέρονται ως backdoors, είναι κομμάτια κώδικα ενσωματωμένα σε προγράμματα από τους προγραμματιστές για να αποκτήσουν γρήγορα πρόσβαση αργότερα, συχνά κατά τη διάρκεια της δοκιμής ή της φάσης αποσφαλμάτωσης. Εάν ένας αδίστακτος προγραμματιστής αφήνει σκόπιμα αυτόν τον κώδικα ή απλά ξεχνά να το αφαιρέσει, εισάγεται μια πιθανή τρύπα ασφαλείας. Οι χάκερ συχνά εγκαταλείπουν ένα backdoor σε προηγουμένως συμβιβασμένα συστήματα για να αποκτήσουν αργότερα πρόσβαση. Οι πόρτες των παγίδων είναι σχεδόν αδύνατο να αφαιρεθούν με αξιόπιστο τρόπο. Συχνά, η αναδιαμόρφωση του συστήματος είναι ο μόνος σίγουρος τρόπος. https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door

[18] Όπως παραπάνω.

είναι πολύ πιο συγκεκριμένοι. Ο όρος προέκυψε το 2006 για εισβολές που εντοπίστηκαν στην Κίνα. Οι στόχοι APT περιλαμβάνουν κυβερνητικές και στρατιωτικές υπηρεσίες της Δύσης, ένα ευρύ φάσμα επιχειρήσεων σε βιομηχανίες ιδιαίτερης σημασίας για την αναπτυξιακή στρατηγική της Κίνας, θρησκευτικούς αντιφρονούντες, υποψηφίους των Προεδρικών Αμερικανικών εκλογών διεθνή ινστιτούτα της Ασίας και ακόμα τη Διεθνή Ολυμπιακή Επιτροπή. (Lindsay 2014/2015, 20-21)

ΣΤΟΧΟΙ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ

Γενικά

Οι στόχοι του κυβερνοπολέμου καθορίζονται ανάλογα με το είδος των επιχειρήσεων που διεξάγει ένας δρώντας στον κυβερνοχώρο και διακρίνονται σε στόχους επιθετικών και αμυντικών επιχειρήσεων. Προτεραιότητα στη στοχοποίηση των επιθετικών επιχειρήσεων λαμβάνουν οι κρίσιμες υποδομές ενός κράτους καθώς τυχόν επιτυχή προσβολή τους θα επιφέρει αποφασιστικό αποτέλεσμα στην εξέλιξη της αντιπαράθεσης. Αντίθετα οι στόχοι των αμυντικών επιχειρήσεων επικεντρώνονται στη πρόληψη, τον εντοπισμό, την αξιολόγηση, την αντιμετώπιση και την αποκατάσταση των προσβαλλόμενων στόχων από κυβερνοεπιθέσεις. Επιπλέον στοχεύουν στη διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών και την προστασία των κρίσιμων υποδομών.

Κρίσιμες Υποδομές

Τα σύγχρονα κράτη, καθώς αναπτύσσονται αυξάνουν την εξάρτησή τους από μια σειρά διασυνδεδεμένων και όλο και περισσότερο τρωτών κρίσιμων υποδομών για την αποτελεσματική τους λειτουργία. Αυτές οι διασυνδεδεμένες και αλληλοεξαρτώμενες υποδομές, όχι μόνο έχουν αυξήσει σημαντικά την καθημερινή αποτελεσματικότητα σχεδόν κάθε τμήματος της κοινωνίας, αλλά έχουν ταυτόχρονα εισαγάγει νέα είδη τρωτότητας με αποτέλεσμα να αποτελούν σήμερα νέους τύπους στρατηγικών στόχων. (Μαυρόπουλος 2014, 10) Κρίσιμες υποδομές ή Υποδομές Ζωτικής Σημασίας (ΥΖΣ) θεωρούνται οι φυσικές και/ή ηλεκτρονικές υποδομές, τα περιουσιακά στοιχεία, τα συστήματα ή μέρη αυτών, τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής, της κοινωνικής ευημερίας των μελών της

και των οποίων η διακοπή λειτουργίας ή η καταστροφή, θα είχε σημαντικό αντίκτυπο για τη χώρα και τις βασικές λειτουργίες του κράτους.

Οι Κυβερνοεπιθέσεις εναντίον των υποδομών μιας χώρας έχουν πραγματικές, προφανείς και μακροχρόνιες, άμεσες και έμμεσες επιπτώσεις. Ως τέτοιες, μπορούν να έχουν ως απώτερο στόχο την τρομοκράτηση του λαού και τον εξαναγκασμό του, να αποσύρει την υποστήριξή του στον πόλεμο ή την πρόκληση ζημιών σε έκταση που να αναγκάσει την κυβέρνηση να επανεκτιμήσει το ρίσκο που ανέλαβε με την προσφυγή στον πόλεμο. (Μαυρόπουλος 2014, 11) Η πρώτη επίδραση είναι απόρροια της απώλειας εμπιστοσύνης του ανθρώπινου δυναμικού της χώρας στον κρατικό μηχανισμό, ενώ η δεύτερη είναι αποτέλεσμα της παρατεταμένης διακοπής παροχής υπηρεσιών από τις προσβληθείσες υποδομές.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι κρίσιμες υποδομές που διασυνδέονται με το διαδίκτυο μέσω των Συστημάτων Βιομηχανικού Ελέγχου ICS (Industrial Control Systems). Πρόκειται για γενικό όρο, ο οποίος περιλαμβάνει πολλούς τύπους συστημάτων ελέγχου, όπως τα συστήματα Επίβλεψης, Ελέγχου και Συλλογής Δεδομένων SCADA (Supervision, Control and Data Acquisition), τα Συστήματα Κατανεμημένου Ελέγχου DCS (Distributed Control Systems) και άλλα μικρότερα συστήματα ελέγχου, λόγω της ευκολίας πρόσβασης και κατά συνέπεια προσβολής τους. (wikipedia 2018) Στην αρχή τα συστήματα ICS ήταν απομονωμένα από τα δίκτυα υπολογιστών, χρησιμοποιούσαν εταιρικό υλικό και λογισμικό και δικά τους πρωτόκολλα για την επικοινωνία με τον κεντρικό υπολογιστή. Η ευρεία διαθεσιμότητα των σχετικά φθηνών συσκευών με ενσωματωμένες διεπαφές με το πρωτόκολλο διαδικτύου, (Internet Protocol – IP) επέφερε θεμελιώδεις αλλαγές τα τελευταία χρόνια. Το γεγονός αυτό εξέθεσε τα συστήματα ICS στους κινδύνους από το διαδίκτυο· κακόβουλα προγράμματα και χάκερ.(Μαυρόπουλος 2014, 11) Οι επιθέσεις σε τέτοια συστήματα έχουν σημαντικές επιπτώσεις στην ομαλή λειτουργία των ελεγχόμενων συστημάτων, τα αποτελέσματα των οποίων είναι ορατά και στον φυσικό κόσμο.

Οι κρίσιμες υποδομές, οι οποίες είναι δυνατόν να αποτελέσουν στόχους του Κυβερνοπολέμου με διαφορετική ιεράρχηση κάθε φορά, είναι οι υποδομές:

α. Εθνικής Άμυνας και Ασφάλειας.

β. Πληροφορικής και Δικτύων Επικοινωνιών δημοσίων και ιδιωτικών.

γ. Οικονομικών και τραπεζικών υπηρεσιών.

δ. Συστήματος παραγωγής και διάθεσης ηλεκτρικής ενέργειας.

ε. Συστήματος παραγωγής, αποθήκευσης και διανομής καυσίμων και φυσικού αερίου.

στ. Υδάτινων πόρων.

ζ. Συγκοινωνιών (οδικών, σιδηροδρομικών, αεροπορικών, θαλασσίων, ποταμίων)

η. Εξυπηρέτησης πολιτών.

θ. Παροχής υγειονομικών υπηρεσιών. (Μαυρόπουλος 2014, 12-14)

«Έχουμε οικοδομήσει το μέλλον μας σε μια δυνατότητα που δεν μάθαμε να προστατεύουμε».

''George Tenet''

ΚΕΦΑΛΑΙΟ «Γ»

Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ

ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Η έκταση που έχει αποδοθεί σήμερα στον κυβερνοπόλεμο και η ενδεχόμενη επίδραση που μπορεί να έχει έναντι κρατικών και μη κρατικών δρώντων, έχει προκαλέσει μια μεγάλη συζήτηση και ταυτόχρονα έντονο προβληματισμό, σχετικά με το νομικό πλαίσιο που εντάσσεται και τους κανόνες δικαίου από τους οποίους πρέπει να διέπεται ώστε να αντιμετωπιστεί διεθνώς. Το σημερινό διεθνές νομικό σύστημα βασίζεται σε αρχές, οι οποίες διαμορφώνονται από τις συνήθεις πρακτικές των κρατών. Είναι σημαντικό να κατανοηθεί ότι το διεθνές δίκαιο δεν λειτουργεί όπως το αντίστοιχο εσωτερικό στα κράτη, γεγονός το οποίο σημαίνει ότι δεν υπάρχουν εγγυημένες παρά μόνο αναμενόμενες συνέπειες για την παραβίαση του. Επιπλέον απαραίτητη προϋπόθεση για να έχει ισχύ, είναι τα κράτη να έχουν αναγνωρίσει το διεθνές δίκαιο και να αποδέχονται να υπόκεινται σ' αυτό (Bell 2018, 23). Η νεωτεριστική φύση του πολέμου στον κυβερνοχώρο και η επακόλουθη έλλειψη διεθνών εθίμων ή πρακτικών αντιμετώπισης του θέματος, δημιούργησαν ένα κενό στο διεθνές δίκαιο επιτρέποντας στα κράτη να εκφράσουν διαφορετικές απόψεις για το πώς θα πρέπει να εφαρμόζεται στη περίπτωση του κυβερνοπολέμου.

Ο κυβερνοπόλεμος ως φαινόμενο πρόσφατο στη διεθνή σκηνή, όπως έχει ήδη αναφερθεί, στερείται ενός σαφούς και συνοπτικού ορισμού. Αυτή η αδυναμία και η έλλειψη συνοχής όσον αφορά τον ορισμό, του τι συνιστά πράξη πολέμου στον κυβερνοχώρο, επιτρέπει στα κράτη να κάνουν χρήση κυβερνοόπλων μεταξύ τους, δίχως να διεξάγουν πρακτικά από νομικής απόψεως, μια επιθετική ενέργεια.

Το άρθρο 51 του Χάρτη των Ηνωμένων Εθνών ορίζει, ότι μόνο μια ένοπλη επίθεση δημιουργεί το δικαίωμα των κρατών να καταφύγουν σε βίαια αμυντική δράση. (Δελίμπασης 2009, 97) Η γενικότερη διαπίστωση είναι ότι απαγορεύει τη

χρήση βίας μεταξύ των μελών του, εκτός της περίπτωσης χορήγησης εξουσιοδότησης για ανάληψη επιθετικής ενέργειας από το Συμβούλιο Ασφαλείας ή της περίπτωσης αυτοάμυνας.

Επίσης στο 1^{ο} άρθρο του ψηφίσματος 3314 της 14^{ης} Δεκεμβρίου 1974 της Γενικής Συνέλευσης των Η.Ε καθορίζεται η έννοια της επίθεσης, ως «η χρήση ένοπλης βίας από ένα κράτος εναντίον της κυριαρχίας, της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας ενός άλλου κράτους ή χρήση βίας με ένα άλλο τρόπο μη συνεπή με το χάρτη των Η.Ε». (Wilmshurst 2008). Αντίστοιχα στο 3^{ο} άρθρο του ψηφίσματος αναφέρονται εφτά πράξεις, που μπορούν να θεωρηθούν ως επιθετικές, καθεμία εκ των οποίων περιλαμβάνει φυσική ένοπλη δύναμη ή κινητική ενέργεια από κράτος, όπως ο βομβαρδισμός μιας πόλης, η εισβολή σε έδαφος τρίτης χώρας από ένοπλες δυνάμεις ή ο αποκλεισμός ενός λιμανιού (Bell 2018, 23). Κοινό χαρακτηριστικό και των εφτά ανωτέρω περιπτώσεων είναι ότι προϋποθέτουν την παρουσία ενόπλων δυνάμεων ή ομάδων, οι οποίες εκπροσωπούν πάντα ένα κρατικό δρώντα, ο οποίος ενεργεί ή επιτρέπει σε τρίτο κράτος να ενεργήσει επιθετικά έναντι άλλου κράτους. Ο διεθνώς αποδεκτός ορισμός της επιθετικότητας έχει αποδειχθεί εξαιρετικά σημαντικός για την παγκόσμια σταθερότητα, ωστόσο δεν καλύπτει επαρκώς τον πόλεμο στον κυβερνοχώρο.

Οι επιθέσεις στον κυβερνοχώρο όμως, παραβιάζουν άλλους διεθνείς νόμους όπως το ψήφισμα 2625, καθιστώντας περίπλοκη την ανταπόκριση στις επιθέσεις στον κυβερνοχώρο. Το ψήφισμα 2625 του ΟΗΕ αναφέρει, ότι «κάθε κράτος έχει καθήκον να απέχει από την οργάνωση, την υποκίνηση, τη συνδρομή ή τη συμμετοχή σε πράξεις εμφύλιων συγκρούσεων ή τρομοκρατικών πράξεων σε άλλο κράτος ... όταν οι πράξεις αναφέρονται σε απειλή ή χρήση βίας. Η λέξη «υποκίνηση» υποδεικνύει, ότι εάν ένα κράτος ενθάρρυνε ιδιώτες του, να διενεργήσουν επιθέσεις στον κυβερνοχώρο εναντίον άλλου κράτους, τότε ως ηθικός αυτουργός είναι ένοχος παραβίασης του διεθνούς δικαίου. Ωστόσο, αυτό προϋποθέτει ότι οι πράξεις ενάντια της κυριαρχίας στον κυβερνοχώρο είναι πράγματι πράξεις επιθετικότητας και οι επιθέσεις στον κυβερνοχώρο συνιστούν χρήση βίας, πράγμα που δεν συμβαίνει στην πραγματικότητα εξαιτίας της φυσικής διάστασης του ψηφίσματος 3314 και της έλλειψης αναφοράς σ' αυτό, του στοιχείου του κυβερνοπολέμου (Bell 2018, 25-26).

Για την αντιμετώπιση του θέματος υπάρχουν δυο κυρίαρχες προσεγγίσεις. Αφενός, ότι το ζήτημα μπορεί να διευθετηθεί μέσω της ενεργοποίησης και της αναλογικής εφαρμογής των ήδη υπαρχόντων κανόνων του διεθνούς δικαίου (συμβατικού και εθιμικού) και αφετέρου, ότι οι ιδιαιτερότητες που συνδέονται με τη φύση του κυβερνοχώρου, τη λειτουργία του καθώς και τα μέσα άμυνας και επίθεσης που χρησιμοποιούνται σ' αυτόν, επιβάλλουν την θέσπιση καινούργιων κανόνων και την ανάπτυξη νέων θεσμικών μηχανισμών και εργαλείων, ώστε να αντιμετωπιστούν αποτελεσματικά οι κίνδυνοι, που ελλοχεύουν στην ομαλή εξέλιξη των διεθνών σχέσεων (Παπαδούλη 2009, 51).

Για τη δεύτερη περίπτωση, οποιαδήποτε προσπάθεια ανάπτυξης ενός εξειδικευμένου νομικού πλαισίου, ειδικά προσαρμοσμένου στην αντιμετώπιση πιθανών βίαιων ενεργειών στον κυβερνοχώρο, εξαρτάται από την επιτυχία του να εντάξει τις σύγχρονες πληροφοριακές επιχειρήσεις και κατά συνέπεια τον κυβερνοπόλεμο, μέσα στην έννοια της αυτοάμυνας. Πρωτίστως όμως θα πρέπει η διεθνής κοινότητα και το διεθνές νομικό σύστημα, αφενός να προσδιορίσουν ως έννοια τον κυβερνοπόλεμο εξασφαλίζοντας ότι αυτή θα απολαμβάνει καθολικής συναίνεσης, αφετέρου να ορίσουν το όριο πέρα από το οποίο μια ενέργεια στον κυβερνοχώρο, θα συνιστά επιθετική ενέργεια και θα νομιμοποιεί την αντίδραση και τη καταφυγή στα όπλα, στο πλαίσιο της αυτοάμυνας.

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΠΟΔΟΣΗΣ ΕΥΘΥΝΩΝ ΚΑΙ Η ΑΠΟΤΡΟΠΗ

Το πρόβλημα της απόδοσης ευθυνών

Ένα από τα πιο επικίνδυνα και δυνητικά απειλητικά χαρακτηριστικά του κυβερνοπολέμου αφορά την ανωνυμία που παρέχει. Ο David Clark και η Susan Landau επισημαίνουν, ότι το θέμα της απόδοσης ευθυνών είναι κρίσιμο και δύσκολο να ξεπεραστεί, στην προσπάθεια να αποτραπούν οι κυβερνοεπιθέσεις. Όπως ισχυρίζονται « *..η αντίδραση απαιτεί να γνωρίζουμε με πλήρη βεβαιότητα ποιοι είναι οι επιτιθέμενοι*» (Gartzke 2013, 46). Ο Martin Libicki συμπεριλαμβάνει τις επιθέσεις από κυβερνοόπλα στη κατηγορία του μη προφανή πολέμου, στην οποία η ταυτότητα της εμπόλεμης πλευράς και ακόμη το γεγονός του ίδιου του πολέμου είναι πλήρως ασαφή (Mazanec 2013, 421).

Ο έλεγχος αυθεντικότητας της πηγής μιας κυβερνοεπίθεσης, είναι συνήθως δύσκολη υπόθεση ακόμα και τη σημερινή εποχή όπου η πρόοδος της τεχνολογίας είναι αλματώδης. Πέντε χαρακτηριστικά μιας σύγκρουσης στον κυβερνοχώρο συμβάλουν στο ανωτέρω πρόβλημα. Πρώτον, η ευκολία του πολλαπλασιασμού των κυβερνοόπλων, που σημαίνει ότι εκτός από την δυνατότητα εκτόξευσης πιο περίπλοκων επιθετικών ενεργειών, αυξάνει εκθετικά και τον αριθμό των επιτιθέμενων. Δεύτερον, η προσπάθεια απόδειξης της ταυτότητας ή της τοποθεσίας οποιουδήποτε από τους επιτιθέμενους συνιστά τεράστια πρόκληση, διότι ο κυβερνοχώρος παρέχει στον επιτιθέμενο έναν υπερβολικό βαθμό ανωνυμίας. Τρίτον, όπου καθίσταται δυνατός ο εντοπισμός της διεύθυνσης διαδικτυακού πρωτοκόλλου (IP) της προέλευσης των επιθέσεων, η απόδοση ευθύνης και συνάμα η οργάνωση μιας τιμωρητικής αντίδρασης, μπορεί να μην αποδειχθεί ορθή επιλογή, διότι το ανωτέρω γεγονός δεν συνεπάγεται απαραίτητα και γνώση της ταυτότητας του χειριστή. Τέταρτον, επειδή ένα κακόβουλο λογισμικό διασχίζει πολλαπλές δικαιοδοσίες και δικλείδες ασφαλείας δικτύων με ευκολία, η προσπάθεια απόκτησης αποδείξεων μετά την επίθεση θα είναι δύσκολη χωρίς αποτελεσματική διεθνή συνεργασία. Πέμπτον, ακόμα και αν επιλυθούν όλες οι αναφερόμενες επιπλοκές είναι πιθανό, ότι η απόδοση δεν θα είναι αρκετά γρήγορη για έγκαιρα αντίποινα. Μέχρι τη στιγμή που θα γίνει γνωστή η ταυτότητα τους, οι δράστες ενδέχεται να έχουν μετακινηθεί πέρα από την ικανότητα του θύματος να αντιδράσει και να απαντήσει (Kello 2013, 33).

Αυτή η δυσκολία στην απόδοση ευθύνης της επίθεσης, έχει δημιουργήσει το ξεχωριστό πλεονέκτημα «της πρώτης κίνησης», με το οποίο ο επιτιθέμενος προσπαθεί να κατακλύσει τη κυβερνοάμυνα του αντιπάλου, πριν μπορέσει να εντοπίσει την πηγή της επίθεσης ή εναλλακτικά, μπορεί να επιδιώξει να εξαπατήσει το στόχο ώστε να πιστέψει ότι η επίθεση διεξάγεται από άλλο δρώντα. Ένα χαρακτηριστικό παράδειγμα μια τέτοιας περίπτωσης αποτελεί η επίθεση στα συστήματα ηλεκτρονικών υπολογιστών τύπου DoS, γνωστή ως «Solar Sunrise», η οποία εντοπίστηκε αρχικά στο Ισραήλ και στα Ηνωμένα Αραβικά Εμιράτα και πιστεύεται ότι σχεδιάστηκε από πράκτορες μυστικών υπηρεσιών. Ωστόσο οι επόμενες έρευνες κατέληξαν στο συμπέρασμα, ότι διεξήχθησαν από δύο έφηβους στην Καλιφόρνια (Mazanec 2013, 422)

Σε άλλη περίπτωση μπορεί η προσπάθεια απόδοσης ευθύνης μιας επίθεσης στον κυβερνοχώρο, που αφορά κυρίως κρατικό δρών, να στεφθεί με επιτυχία αλλά να συναντήσει την άρνηση ανάληψης ευθύνης από το φερόμενο ως δράστη κράτος. Στην καλύτερη περίπτωση οι κυβερνήσεις, όταν τους απαγγέλλονται κατηγορίες, ότι παραγγέλλουν επιθέσεις ή κατασκοπεία στον κυβερνοχώρο, τις αποφεύγουν κατηγορώντας γι' αυτό πολίτες τους, με την ιδιότητα του ακτιβιστή χάκερ (hacktivist[19]). Το ανωτέρω αποτελεί συνήθη πρακτική σήμερα των Κινέζων και των Ρώσων (Patterson 2011, 129). Μια κυβερνοεπίθεση με τέτοια κατάληξη, είναι η γνωστή ως «Night Dragon». Στόχος της ήταν πέντε πολυεθνικές εταιρείες πετρελαίου και η κλοπή τεράστιου όγκου (gigabytes) πολύ ευαίσθητων εμπορικών πληροφοριών, σχετικά με τις δραστηριότητες ανάπτυξης της δυτικής βιομηχανίας παραγωγής ενέργειας. Οι ερευνητές κατόρθωσαν να εντοπίσουν την επίθεση σε διευθύνσεις διαδικτυακού πρωτοκόλλου (IP address) στο Πεκίνο και επιβεβαίωσαν, ότι τα εργαλεία που χρησιμοποιήθηκαν στην επίθεση ήταν σε μεγάλο βαθμό κινεζικής προέλευσης, καθώς επίσης και ότι οι επιθέσεις διεξήχθησαν μεταξύ 9:00 π.μ. και 5:00 μ.μ. ώρα Πεκίνου (αντανακλώντας την πιθανότητα να έχει πραγματοποιηθεί η επίθεση από κυβερνητικό ή συνδεόμενο με την κυβέρνηση, προσωπικό). Ωστόσο παρ' όλες τις αποδείξεις ότι η επίθεση ήταν κινεζικής προέλευσης, ενορχηστρωμένη πιθανότατα από την ίδια την κυβέρνηση, ήταν αδύνατο να της αποδοθεί επισήμως. Για την επίθεση οι Κινέζοι αξιωματούχοι ισχυρίστηκαν, ότι δεν είχαν κανένα ρόλο με την υπόψη δραστηριότητα όπως ήταν αναμενόμενο (Mazanec 2013, 422).

Η σημαντικότερη στρατηγική συνέπεια του προβλήματος καταλογισμού, είναι ότι αποδυναμώνει την αποτροπή. Για ορισμένους αναλυτές όπως ο Richard Betts, η αποτροπή δεν λειτουργεί στον κυβερνοχώρο και αυτό οφείλεται στο πρόβλημα της απόδοσης. Ο αναπληρωτής υπουργός άμυνας των ΗΠΑ William Lynn το 2010 έγραψε, «*ότι ενώ ένας πύραυλος συνήθως έχει διεύθυνση επιστροφής, ένας ιός υπολογιστή δεν έχει*». Πράγματι καθ' όλη τη διάρκεια του ψυχρού πολέμου, η απόδοση μιας ενδεχόμενης επίθεσης δεν αποτελούσε θέμα, δεδομένου ότι όλα τα

[19] Ο ακτιβιστής του Διαδικτύου είναι αυτός που κάνει χρήση της τεχνολογίας για την προώθηση μιας πολιτικής ατζέντας ή μιας κοινωνικής αλλαγής. Ο ακτιβισμός στο διαδίκτυο έχει τις ρίζες του στην κουλτούρα και την ηθική των χάκερ και οι άξονές του συχνά σχετίζονται με την ελευθερία του λόγου, τα ανθρώπινα δικαιώματα ή την ελευθερία των κινήσεων πληροφοριών. https://en.wikipedia.org/wiki/Hacktivism

μέρη μπορούσαν να εντοπίσουν την πηγή προέλευσης ενός πυραύλου, σχετικά γρήγορα (Patterson 2011, 130).

Το ανωτέρω γεγονός σε συνδυασμό με τις αποδεδειγμένα καταστροφικές συνέπειες της χρήσης των πυρηνικών για την ανθρωπότητα, το κόστος κατασκευής ή απόκτησης και τη διεθνή αποδοκιμασία που συνόδευε την κατοχή τους, συνέβαλλαν στην αποτροπή χρήσης και διασποράς τους, εξασφαλίζοντας για την ανθρωπότητα σταθερότητα και ισορροπία έστω και εύθραυστη. Αντίθετα, η απόκτηση δυνατότητας εκτόξευσης επίθεσης στον κυβερνοχώρο, μπορεί να επιτευχθεί δίχως ιδιαίτερο κόστος από οποιονδήποτε και κάτω από άκρα μυστικότητα. Η διασπορά των κυβερνοόπλων είναι ιδιαίτερα ευρεία και γίνεται αντιληπτή όταν είναι ήδη πολύ αργά για τον προσβαλλόμενο. Απαιτεί γνώσεις προγραμματισμού, οι οποίες διατίθενται απλόχερα στο διαδίκτυο (Dark Web), λίγες γραμμές κώδικα, ώστε να φτιαχτεί ένας ιός και υποψήφιους δράστες, οι οποίοι σε αντίθεση με τους ολιγάριθμους κατόχους πυρηνικών την εποχή του ψυχρού πολέμου, είναι αναρίθμητοι. Όλα τα παραπάνω σε συνδυασμό με την αδυναμία απόδοσης ή καταλογισμού ευθύνης, αποτελούν τροχοπέδη στην έννοια της αποτροπής.

Η αποτροπή

Σύμφωνα με τον καθηγητή Κωνσταντίνο Κολιόπουλο, η αποτροπή (deterrence) ως έννοια της στρατηγικής αποσκοπεί στη διατήρηση του status quo με την απειλή χρήσης βίας (Χαίδης 2012, 90). Ο όρος αποτροπή στα κοινά λεξικά, αναφέρεται ως η ενέργεια να «εμποδίσει κάτι από το να συμβεί ή να προκαλέσει κάποιον να μην κάνει κάτι». Στη σφαίρα της ασφάλειας στον κυβερνοχώρο, το «να κάνει κάτι» ισοδυναμεί με επίθεση, χειραγώγηση, εκμετάλλευση και / ή απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα και δίκτυα υπολογιστών (Burton 2018, 5). Ο Glenn Snyder, ορίζει την αποτροπή σε γενικές γραμμές ως τη παρεμπόδιση των άλλων υπό την απειλή κυρώσεων ή υπόσχεσης ανταμοιβής. Ο ίδιος διευκρινίζει, ότι η αποτροπή είναι μια ευρύτερη έννοια από ό, τι πιστεύουν οι περισσότεροι και ότι δεν χρειάζεται να στηρίζεται σε στρατιωτική δύναμη (Nye 2016/2017, 52-53). Η αποτροπή λειτουργεί στη βάση της σχέσης κόστους οφέλους και για να είναι επιτυχής, θα πρέπει πάντα το κόστος να είναι μεγαλύτερο

από το όφελος για τον επιτιθέμενο και αυτό θα εξασφαλίζεται από τη φύση της απειλής που εκφράζει ο αμυνόμενος (Χαίδης 2012, 90).

Ο William Kaufman υποστηρίζει, ότι η αποτροπή αποτελείται ουσιαστικά από δύο βασικά στοιχεία. Πρώτον, από την εκπεφρασμένη πρόθεση αυτού που αποτρέπει να υπερασπιστεί ένα συγκεκριμένο συμφέρον. Δεύτερον, από την αποδεδειγμένη ικανότητα του να επιτύχει πράγματι την υπεράσπιση του εν λόγω συμφέροντος ή να επιβάλει τέτοιο κόστος στον επιτιθέμενο, ώστε ακόμη και αν μπορέσει να πετύχει τον σκοπό του, να φαίνεται ότι δεν αξίζει την προσπάθεια γι' αυτόν (Libicki 2009, 7). Η αποτροπή πρέπει να λειτουργεί στο μυαλό του εισβολέα. Κάθε πιθανός εισβολέας θα πρέπει να είναι αναγκασμένος να σταθμίσει την προσπάθεια που απαιτείται για να κάνει μια επίθεση ενάντια στο αναμενόμενο όφελος αυτής. Παράλληλα η αποτροπή συνιστά και μια ψυχολογική διαδικασία, που εξαρτάται από τις αντιλήψεις τόσο των παραγόντων όσο και των στόχων, καθώς και από την ικανότητα επικοινωνίας αυτών των απόψεων με σαφήνεια. Ο Robert Jervis και άλλοι θεωρητικοί, έχουν περιγράψει πολλές περιπτώσεις αποτυχίας της αποτροπής λόγω εσφαλμένης αντίληψης. (Nye 2016/2017, 53)

Ωστόσο ακόμα και αν όλα τα ανωτέρω εξασφαλιστούν, αναγκαία και απαραίτητη συνθήκη προκειμένου να επιτευχθεί η αποτροπή είναι, ο αντίπαλος να σκέφτεται και να ενεργεί ορθολογικά. Σε αντίθετη περίπτωση η αποτροπή είναι καταδικασμένη να αποτύχει και η σύγκρουση μεταξύ των αντιμαχόμενων συγκεντρώνει πολλές πιθανότητες. Ιστορικά έχει αποδειχθεί σε αρκετές περιπτώσεις κατά την διάρκεια του ψυχρού πολέμου με πιο χαρακτηριστική αυτή της κρίσης των πυραύλων στην Κούβα (Burton 2018). Χαρακτηριστικό παράδειγμα στη σημερινή εποχή αποτελεί η κυβέρνηση της Β. Κορέας, η πολιτική της οποίας, ούτε διευκολύνει την επικοινωνία ούτε διακρίνεται για τον ορθολογισμό στη διαδικασία λήψης αποφάσεων.

Τα ερωτήματα που προκύπτουν λοιπόν είναι, αν η αποτροπή είναι αναγκαία στον κυβερνοχώρο και επιπλέον αν μπορεί να εφαρμοστεί το ίδιο επιτυχημένα, με τον τρόπο που αυτό επιτεύχθηκε την εποχή του ψυχρού πολέμου, γεγονός το οποίο συνέβαλλε τα μέγιστα, ώστε να χαρακτηριστεί ως ένα από τα πιο σταθερά διαστήματα σε πολιτικό επίπεδο. Οι λόγοι που καθιστούν αναγκαία την κυβερνοαποτροπή έχουν να κάνουν κυρίως με το ζήτημα της αναλογικότητας (Χαίδης 2012, 95). Το νομικό καθεστώς αντιμετώπισης των κυβερνοεπιθέσεων,

όπως αναφέρθηκε ανωτέρω, είναι ασαφές και δεν εξουσιοδοτεί τα κράτη για λήψη κινητικών μέτρων που θα περιλαμβάνει συμβατικό ή πυρηνικό πλήγμα κατά του επιτιθέμενου. Συνεπώς αποτελεί μονόδρομο το γεγονός, ότι εφόσον ληφθεί η απόφαση για εκδήλωση αντιποίνων, αυτά θα πρέπει να είναι ίδιας φύσης με τις κυβερνοεπιθέσεις. Σε ότι αφορά το δεύτερο ερώτημα σύμφωνα με τον ειδικό σε θέματα κυβερνοπολέμου Richard Clarke, η εφαρμογή της αποτροπής στον κυβερνοχώρο παρουσιάζει αρκετά προβλήματα σημαντικότερο εκ των οποίων είναι η έλλειψη αξιοπιστίας σε ότι αφορά τα κυβερνοόπλα και κυρίως την καταστροφικότητα τους (Χαίδης 2012, 95). Η ιστορία κατέδειξε, ότι η πυρηνική αποτροπή κρίθηκε αποτελεσματική και μέρος αυτής της επιτυχίας οφειλόταν εν μέρει, στα ορατά φρικαλέα αποτελέσματα που μπορούσαν να προκαλέσουν οι πυρηνικές εκρήξεις. Αντίθετα οι επιδράσεις των κυβερνοεπιθέσεων δεν είναι ορατές και δεν δημιουργούν την ίδια αίσθηση σοκ (Burton 2018, 7).

Η αποτροπή στον κυβερνοχώρο δύναται να λάβει δυο βασικές μορφές. Αυτές είναι η κυβερνοαποτροπή μέσω άρνησης και η κυβερνοαποτροπή μέσω αντιποίνων. Η πρώτη μορφή σχετίζεται με την άμυνα στον κυβερνοχώρο. Μέσω ανάπτυξης αμυντικών δυνατοτήτων αποσκοπεί στην φθορά των κυβερνοεπιθέσεων του αντιπάλου και συμβάλλει στην αύξηση του κόστους σ' αυτόν. Η άλλη μορφή είναι πιο επιθετική και εστιάζει στην εφαρμογή αντιποίνων στον κυβερνοχώρο, προκειμένου ο αντίπαλος να αποτραπεί από την έναρξη ή την περαιτέρω διεξαγωγή κυβερνοεπιθέσεων (Χαίδης 2012, 94). Η αποτροπή μέσω αντιποίνων προϋποθέτει την ύπαρξη ανεπτυγμένων επιθετικών δυνατοτήτων στον κυβερνοχώρο. Ωστόσο η αδυναμία απόδοσης της ευθύνης των κυβερνοεπιθέσεων, αποτελεί μακροχρόνιο πρόβλημα, καθώς αν δεν μπορεί να διευκρινιστεί η ταυτότητα του επιτιθέμενου με συνέπεια, η αποτροπή να μην είναι εφικτή. (Burton 2018, 6) Ταυτόχρονα ελλοχεύει πάντα ο κίνδυνος η επιβολή αντιποίνων να εφαρμοστεί σε λάθος δρώντα, γεγονός το οποίο αποδυναμώνει όχι μόνο τη λογική της αποτροπής αλλά συμβάλλει στη δημιουργία ενός νέου εχθρού (Libicki 2009, 41).

Για τους περισσότερους αναλυτές, οι δύο μορφές της κυβερνοαποτροπής θα πρέπει να λειτουργήσουν συνεργατικά, προκειμένου να επιτευχθεί το επιθυμητό αποτέλεσμα από τον αμυνόμενο. Η κυβερνοαποτροπή και με τις δύο μορφές της, έχει ως στόχο να μειώσει την πιθανότητα εκδήλωσης κυβερνοεπιθέσεων κατά του

αμυνόμενου, σε ένα αποδεκτό επίπεδο, το οποίο αντιστοιχεί σε ένα ανάλογα αποδεκτό κόστος (Χαίδης 2012, 94).

Πέραν των δύο προαναφερόμενων μορφών αποτροπής, υπάρχουν και δύο μηχανισμοί, η λειτουργία των οποίων μπορεί να συμβάλλει στην αποθάρρυνση ενός δρώντα να εκδηλώσει κυβερνοεπιθέσεις. Ο πρώτος αφορά τις ενέργειες που θα ρυμουλκήσουν έναν δρώντα να αντιληφθεί, ότι το κόστος μιας ενέργειας υπερβαίνει το όφελος μέσω της ταυτόχρονης εμπλοκής του. Αν και δεν συνιστά αποτροπή με την στενή έννοια του όρου, η εμπλοκή αναφέρεται στην ύπαρξη διαφόρων αλληλεξαρτήσεων που κάνουν μια επιτυχημένη επίθεση να επιβάλλει ταυτόχρονα σοβαρό κόστος στον επιτιθέμενο, όπως και στο θύμα. Εάν υπάρχουν οφέλη από το υφιστάμενο status quo και τη συνέχιση του, ένας πιθανός αντίπαλος μπορεί να μην επιτεθεί υπό τον φόβο ότι θα χάσει κάτι πολύτιμο, γεγονός το οποίο συμβάλλει στην αποτροπή του (Nye 2016/2017, 58).

Ο δεύτερος μηχανισμός είναι η ύπαρξη και εφαρμογή κανόνων σε όλα τα επίπεδα. Οι κανονιστικές σκέψεις μπορούν να αποτρέψουν τις επιθετικές ενέργειες ενός δρώντα μέσω της ανάδειξης του ενδεχόμενου κόστους τόσο στη φήμη του, όσο και στην ήπια ισχύ του, το οποίο μπορεί να υπερβαίνει τα όποια κέρδη θα αποκτήσει από μια δεδομένη επίθεση. Οι κανόνες κατά αντίστοιχο τρόπο με την εμπλοκή, μπορούν να επιβάλουν κόστος σε έναν εισβολέα, ακόμη και αν η επίθεση δεν αποτράπηκε από την άμυνα ή από την απειλή αντιποίνων. Αντίθετα ωστόσο από την εμπλοκή, είναι απαραίτητος κάποιος βαθμός απόδοσης της ενέργειας σε δρώντα, προκειμένου να μπορούν να λειτουργήσουν οι κανόνες (Nye 2016/2017, 60).

Η αποτροπή στον κυβερνοχώρο είναι περιοριστική, στο βαθμό που επιδιώκει να μειώσει τη συνολική συχνότητα και τη σοβαρότητα των επιθέσεων και να διαμορφώσει τη συμπεριφορά του εισβολέα. Όπως υποστηρίζει ο Uri Tor, η αποτροπή στον κυβερνοχώρο επιδιώκει να «αναβάλει, να περιορίσει και να διαμορφώσει μια σειρά συνεχιζόμενων συγκρούσεων με διάφορους παράγοντες, παρά να αποτρέψει όλες τις επιθέσεις που συμβαίνουν κάθε στιγμή (Burton 2018, 14).

Αν η αποτροπή είναι δύσκολη και αβέβαιη ως διαδικασία, όταν εφαρμόζεται σε εθνικά κράτη, τότε είναι ακόμα δυσκολότερη, όταν απευθύνεται σε μη κρατικούς

φορείς. Οι τελευταίοι είναι λιγότερο δεσμευμένοι από κανόνες στις διεθνείς αλληλεπιδράσεις τους, λειτουργούν με τον δικό τους τρόπο, αποδέχονται υψηλότερα επίπεδα κινδύνου, έχουν μεγαλύτερη ανοχή σε μέτρα τιμωρίας και σε ορισμένες περιπτώσεις είναι δυνατόν να επιδιώκουν τα μέτρα αντιποίνων (Burton 2018, 14). Ο πρώην προέδρος των ΗΠΑ George W. Bush το 2006 δήλωσε χαρακτηριστικά ότι *« ..οι εχθροί που αντιμετωπίζουμε σήμερα είναι διαφορετικοί από πολλές απόψεις από τον εχθρό που αντιμετωπίσαμε στον Ψυχρό Πόλεμο. Σε αντίθεση με τη Σοβιετική Ένωση, οι τρομοκράτες που αντιμετωπίζουμε σήμερα κρύβονται σε σπηλιές και σκιές ... δεν έχουν σύνορα να προστατεύσουν, ούτε πρωτεύουσα να υπερασπιστούν. Δεν μπορούν να αποτραπούν*.. » (Burton 2018, 17).

Επιπρόσθετα ορισμένα κράτη, κυρίως η Ρωσία και η Κίνα, τείνουν να αναθέτουν ή να ιδιωτικοποιούν τις κυβερνοδυνατότητες τους σε συνδεόμενες ομάδες (εθνικιστικές οργανώσεις), οι οποίες διενεργούν επιθέσεις στον κυβερνοχώρο εκ μέρους τους. Υπό αυτή την έννοια, η απειλή πλέον δεν προέρχεται από μη κρατικούς φορείς, αλλά από φορείς που συνδέονται με το κράτος και κατευθύνονται από αυτό, αλλάζοντας τη δυναμική της αποτροπής με άγνωστους τρόπους και θέτοντας ερωτήματα που δεν έχουν εξεταστεί ακόμα (Burton 2018, 16).

Οι τελευταίες εξελίξεις, οι οποίες δρομολογούνται από το NATO Cooperative Cyber Defence Center of Excellence και το εγχειρίδιο του Ταλίν (Tallinn Manual 2.0), προτείνουν την εμφάνιση ποικίλων νομικών μέτρων για την αποτροπή μη κρατικών φορέων, συμπεριλαμβανομένης της δέσμευσης της δραστηριότητάς τους στα κράτη μέσω διεθνών νομικών μηχανισμών. Αν οι μη κρατικοί παράγοντες θεωρηθούν ότι δεν λειτουργούν μεμονωμένα, αλλά ότι συνδέονται και αλληλεπιδρούν σε συντονισμό με το σύστημα του εκάστοτε εθνικού κράτους, τότε η αποτροπή στον κυβερνοχώρο μπορεί να μην αποδειχθεί ακατόρθωτη (Burton 2018, 17) .

Η αύξηση του κόστους των επιθέσεων στον κυβερνοχώρο και η μείωση των οφελών μέσω ποικίλων μηχανισμών είναι μια στρατηγική που επιτυγχάνει αποτελέσματα μέσω της επιμονής στον σκοπό. Μια προσαρμοσμένη προσέγγιση που αναγνωρίζει το ρόλο ενός ποικίλου φάσματος, αποτελούμενου από παράγοντες που επιδιώκουν την αποτροπή και απειλών οι οποίες δύναται να

αποτραπούν και η οποία περιλαμβάνει νομικές, κοινωνικές, κανονιστικές και τεχνολογικές προσεγγίσεις για την αποτροπή, μπορεί να αποφέρει μεγαλύτερα οφέλη (Burton 2018, 27). Η αποτροπή ακόμα και αν δεν επιτυγχάνεται τέλεια, είναι προτιμότερη επιλογή από το να μην επιδιώκεται καθόλου. Η εξέλιξη της τεχνολογίας μπορεί να προσδώσει μελλοντικά δυνατότητες που θα καταστήσουν την απόδοση των πράξεων στον κυβερνοχώρο λιγότερο προβληματική διαδικασία. Ήδη από το 2012 ο υπουργός Άμυνας των ΗΠΑ ισχυριζόταν, ότι τα 2/3 των περιστατικών μπορούσαν να ανιχνευθούν (Libicki, rand.org 2017, 2). Επιπλέον πάντα υπάρχει η πιθανότητα τα κράτη μελλοντικά να συνειδητοποιήσουν την ανάγκη θεσμοθέτησης ενός κοινού νομικού πλαισίου, το οποίο αφενός να δικαιολογεί την προσφυγή στη χρήση ένοπλης βίας, εφόσον απαιτείται και αφετέρου να προβλέπει αυστηρές ποινές για όσους αποδεδειγμένα εκτελούν επιθέσεις ή παράνομες πράξεις στον κυβερνοχώρο.

Η ΑΜΥΝΑ ΚΑΙ Η ΙΣΟΡΡΟΠΙΑ ΜΕ ΤΗΝ ΕΠΙΘΕΣΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η ισορροπία μεταξύ άμυνας και επίθεσης στον κυβερνοχώρο αποτελεί ένα κρίσιμο και ενδεχομένως αναπάντητο ερώτημα σήμερα. Από την υπάρχουσα βιβλιογραφία δεν προκύπτει σαφής απάντηση, που να τυγχάνει συνολικής αποδοχής, γεγονός το οποίο αποτυπώνεται στις διαφορετικές πολιτικές (αμυντικές ή επιθετικές) που υιοθετούνται από τους παράγοντες του διεθνούς συστήματος.

Οι υπεύθυνοι σχεδιασμού ασφαλείας πληροφοριακών συστημάτων προειδοποιούν επανειλημμένα, ότι στον τομέα του κυβερνοχώρου, η επίθεση έχει το πλεονέκτημα. (Kello 2013, 27) Ο Kenneth Lieberthal και ο Peter Singer συμφωνούν με τον ανωτέρω ισχυρισμό, επειδή αφενός το Internet σχεδιάστηκε, ώστε να διανέμεται η πληροφορία εύκολα και να μην διακόπτεται η ροή της και αφετέρου, διότι προσφέρει πολλές αδυναμίες προς εκμετάλλευση. (Slayton 2016, 76) Δεν είναι λίγοι οι ερευνητές που ισχυρίζονται, ότι ακόμα και αν η άμυνα στον κυβερνοχώρο διέθετε απεριόριστο προϋπολογισμό, δεν θα μπορούσε να περιορίσει την πιθανότητα διενέργειας εισβολών, καθώς συνεχώς ανακαλύπτονται νέα τρωτά σημεία (Krepinevich 2012, 45).

Αντίθετα υπάρχουν σκεπτικιστές, που ισχυρίζονται ότι η άμυνα έχει το πλεονέκτημα και όχι η επίθεση. Η σύσταση μιας σοβαρής άμυνας για την αντιμετώπιση μιας μεγάλης επίθεσης στον κυβερνοχώρο, απαιτεί κατ' ελάχιστο την

δυνατότητα ανίχνευσης και παρεμπόδισης των εισβολών σε εθνική κλίμακα. (Krepinevich 2012, 45). Το συμπέρασμα, ωστόσο της ανωτερότητας της άμυνας είναι μόνο κατά το ήμισυ πλήρες, καθώς αγνοεί ή υποβαθμίζει το άλλο μισό της στρατηγικής εικόνας, που έχει να κάνει με το τεράστιο κόστος που απαιτείται για τη συγκρότηση άμυνας, ενάντια σε μια κυβερνοεπίθεση. Οι πιο συχνά εμφανιζόμενες απαιτήσεις, οι οποίες θα επιφέρουν κόστος είναι (Kello 2013, 27-30) :

α. Η δυσκολία πρόβλεψης και ανίχνευσης της επίθεσης. Το εύρος και το πλήθος των άγνωστων αδυναμιών καθιστά δύσκολη την πρόβλεψη και ανίχνευση της επίθεσης στον κυβερνοχώρο, περιπλέκοντας τη σχεδίαση και λήψη των απαιτούμενων μέτρων για την αντιμετώπιση της.

β. Η άμυνα μέσω άρνησης. Η πιθανότητα ο κακόβουλος κώδικας μιας κυβερνοεπίθεσης να δύναται να επιχειρεί, μη ανιχνεύσιμος στα πληροφοριακά συστήματα του αμυνόμενου, είναι ίσως το πιο ανησυχητικό χαρακτηριστικό του στρατηγικού τοπίου στον κυβερνοχώρο. Το γεγονός αυτό επιτρέπει στον εισβολέα να στερήσει από την άμυνα την ικανότητα να διαχειρίζεται τη δική της προστασία. Παράλληλα η δυνατότητα του κακόβουλου λογισμικού να παράγει πολλαπλές εκδόσεις του εαυτού του σημαίνει, ότι οι παραλλαγές απειλής κατά τη διάρκεια μιας κυβερνοεπίθεσης είναι θεωρητικά απεριόριστες, με συνέπεια την αύξηση του κόστους για τη αντιμετώπιση της.

γ. Η σύνθετη επιφάνεια άμυνας. Τα συστήματα υπολογιστών καθίστανται πιο περίπλοκα σε όλα τα στάδια σχεδιασμού και χρήσης. Καθώς η πολυπλοκότητα του λογισμικού και του υλικού αυξάνεται, το ίδιο συμβαίνει και με το κόστος τόσο για τον επιτιθέμενο όσο και για τον αμυνόμενο. Το αποτέλεσμα είναι μια θεμελιώδης ανισορροπία μεταξύ επίθεσης και άμυνας. Ενώ ο επιτιθέμενος πρέπει να αποφασίσει μόνο τις διαδικασίες παρεισφρήσεως στο πληροφοριακό σύστημα και επιλογής της μορφής επίθεσης που θα χρησιμοποιήσει, ο αμυνόμενος πρέπει να προστατεύει συνεχώς το δίκτυο του από μια τεράστια γκάμα πιθανών επιθέσεων γεγονός το οποίο αναμφισβήτητα εκτοξεύει το κόστος.

δ. Ο κατακερματισμός της άμυνας. Μια προληπτική στρατηγική επιδιώκει να εξουδετερώσει τις απειλές προτού μπορέσουν να πραγματοποιηθούν. Ωστόσο είναι δύσκολη η εφαρμογή προληπτικών αμυνών,

διότι η εξουσιοδότηση εκτέλεσης επίθεσης όπως αντίστοιχα και στην άμυνα, σπάνια χορηγείται στους χειριστές των συστημάτων που υπόκεινται σε επίθεση. Αντίθετα, τέτοιου είδους εξουσιοδότηση παρέχεται σε κυβερνήσεις και εταιρείες παροχής υπηρεσιών διαδικτύου, οι οποίοι είναι αμφίβολο αν γνωρίζουν πότε λαμβάνει χώρα μια επίθεση. Αυτός ο κατακερματισμός των ευθυνών στον τομέα της άμυνας, αποτελεί έναν περιοριστικό παράγοντα κατά τη διαμόρφωση μιας συνεκτικής και ολοκληρωμένης απάντησης σε μια επίθεση στον κυβερνοχώρο.

ε. Οι κίνδυνοι προερχόμενοι από την αλυσίδα εφοδιασμού. Τα πληροφοριακά συστήματα βασίζονται ολοένα και περισσότερο σε ιδιωτικούς κατασκευαστές για ανεφοδιασμό σε εξαρτήματα και ανταλλακτικά. Κατά συνέπεια η αλυσίδα εφοδιασμού αποτελεί ένα τρωτό σημείο των συστημάτων και ταυτόχρονα πηγή κινδύνων. Μέσω αυτής, ξένοι πράκτορες ή ιδιωτικοί κατασκευαστές δύναται να προτοποθετούν λογισμικό και εξαρτήματα με κακόβουλο περιεχόμενο, με σκοπό την δημιουργία προϋποθέσεων για επίθεση ή εκμετάλλευση. Η προστασία έναντι των κινδύνων της αλυσίδας εφοδιασμού απαιτεί συντονισμό από τις κυβερνήσεις και τις βιομηχανίες του κλάδου της τεχνολογίας των πληροφοριών και επιπλέον την επένδυση σημαντικών ποσών για την προμήθεια υλικών από πιστοποιημένους συνεργάτες.

Ερευνητές και στρατιωτικοί στοχαστές, έχουν καθορίσει μέσω τριών διακριτών τρόπων, την ισορροπία μεταξύ επίθεσης και άμυνας στον κυβερνοχώρο όπως παρακάτω (Slayton 2016, 78-79):

α. Με βάση το σχετικό κόστος επίθεσης και άμυνας. Μέσα από την παραδοσιακή θεωρία για την επίθεση και την άμυνα, η ισορροπία καθορίζεται πιο συχνά ως η αναλογία του κόστους επίθεσης, εναντίον μιας περιοχής και του κόστους για την υπεράσπιση της. Αρκετοί ερευνητές επεκτείνουν αυτή την προσέγγιση στον κυβερνοχώρο, επικεντρώνοντας το ενδιαφέρον τους στο σχετικό κόστος άμυνας και επίθεσης. Ο συναγωνισμός στον κυβερνοχώρο παρουσιάζεται ως μια διαδικασία όπου επικρατεί η επίθεση. Γι' αυτό και αν τόσο ο επιτιθέμενος όσο και ο αμυνόμενος διαθέτουν τα ίδια μέσα σε μια σύγκρουση, θα επικρατήσει ο επιτιθέμενος.

β. Με βάση την αποτελεσματικότητα της επίθεσης στον κυβερνοχώρο. Μια δεύτερη έννοια του πλεονεκτήματος της κυβερνοεπίθεσης υπονοεί, ότι οι

επιθετικές επιχειρήσεις είναι χαμηλού κόστους και υψηλής απόδοσης σε αντίθεση με τις αμυντικές, οι οποίες είναι κοστοβόρες και μη αποτελεσματικές στην πλειοψηφία τους. Αυτή η αίσθηση του επιθετικού πλεονεκτήματος διαφέρει από την αρχική, στο γεγονός ότι επικεντρώνεται περισσότερο στην απόδοση της επίθεσης. Αυτό δικαιολογείται από το γεγονός ότι θα ήταν απίθανο οι εγκληματίες στον κυβερνοχώρο να επέμεναν στις δραστηριότητες τους, αν ο ανταγωνισμός ευνοούσε την άμυνα. Σ' αυτή την περίπτωση το έγκλημα δεν αποδίδει. Προς επίρρωση των ανωτέρω ο John Arquilla ανέφερε ότι το 2007 οι κυβερνοεπιθέσεις στην Εσθονία κόστισαν στους επιτιθέμενους πολύ λίγο, αλλά είχαν υψηλή απόδοση λαμβάνοντας υπόψη τον αντίκτυπο τους στην αποδιοργάνωση της κυβέρνησης της Εσθονίας.

γ. Το πλεονέκτημα της πρώτης κίνησης. Ορισμένοι ισχυρίζονται, ότι αυτοί που εκτελούν τις κυβερνοεπιθέσεις, δεν απολαμβάνουν τα πλεονεκτήματα που παρέχει ο αιφνιδιασμός της πρώτης κίνησης, ιδιαίτερα όταν αυτό αφορά «αμιγώς» διαδικτυακές συγκρούσεις, διότι μια τέτοια επιλογή, δεν θα καταστήσει τις ικανότητες του εχθρού στον κυβερνοχώρο εντελώς αναποτελεσματικές. Ωστόσο, ακόμα κι αν αυτό το επιχείρημα είναι αποδεκτό, τα πλεονεκτήματα της πρώτης κίνησης δεν πρέπει να περιορίζονται μόνο στον κυβερνοχώρο. Η ικανότητα διατάραξης της ικανότητας και της αποτελεσματικότητας του συστήματος διοίκησης και ελέγχου μιας στρατιωτικής δύναμης, μπορεί να θεωρηθεί ότι θέτει τις προϋποθέσεις επίτευξης μιας αποφασιστικής εδαφικής νίκης.

Αν και έχει αφεθεί να εννοηθούν πολλές αντιλήψεις σχετικά με την ισορροπία μεταξύ επίθεσης και άμυνας, σπάνια αυτή έχει καθοριστεί με ακρίβεια ή έχει λειτουργήσει για να καταστήσει δυνατή την εμπειρική μέτρηση. Η συνάρτηση της άμυνας και της επίθεσης είναι σχετική. Η απόλυτη μέτρηση του κόστους της επίθεσης, έχει νόημα μόνο σε σχέση με τις δαπάνες του αμυνόμενου. Η χρησιμότητα της επίθεσης στον κυβερνοχώρο ισοδυναμεί με την αξία του επιθετικού στόχου (π.χ. κατοχή εδάφους, κλοπή μυστικών, απόκτηση ελέγχου ενός υπολογιστή), μείον το ελάχιστο κόστος επίτευξής του. Αντίστοιχα η χρησιμότητα της άμυνας, αναφέρεται στην αξία του αμυντικού στόχου (π.χ. διατήρηση εδάφους, διατήρηση της μυστικότητας, διατήρηση του ελέγχου ενός υπολογιστή) μείον το ελάχιστο κόστος άμυνας αυτού. Όταν η χρησιμότητα είναι μεγαλύτερη για την επίθεση από ότι για την άμυνα, τότε η κατάσταση μπορεί να

ειπωθεί ότι ευνοεί την πρώτη και το αντίστροφο. Ορισμένοι αναλυτές επιπλέον επικεντρωμένοι στις τεχνολογικές δυνατότητες του κυβερνοχώρου, δηλώνουν ότι η ταχύτητα, η «ευκολία χρήσης» και η «ευελιξία» της τεχνολογίας των πληροφοριών, είναι χαρακτηριστικά που ευνοούν την επίθεση (Slayton 2016, 82).

ΚΕΦΑΛΑΙΟ «Δ»

ΣΤΡΑΤΗΓΙΚΕΣ ΚΡΑΤΩΝ

ΓΕΝΙΚΑ

Έχοντας αναφερθεί στα προηγούμενα κεφάλαια στον κυβερνοχώρο και τις προκλήσεις που θέτει στην ασφάλεια και την κυριαρχία των κρατών, οι οποίες μπορεί να προέρχονται τόσο από κρατικούς όσο και από μη κρατικούς δρώντες, κρίνεται σκόπιμο να αναφερθούν οι στρατηγικές ορισμένων κρατών, που έχουν υιοθετηθεί για την αντιμετώπιση τους. Η πρόθεση μέσα από την παράθεση διαφορετικών στρατηγικών είναι, να προκύψει αβίαστα μια σύγκριση μεταξύ τους, λαμβάνοντας υπόψη τα μεγέθη των κρατών, τους διαφορετικούς αντικειμενικούς σκοπούς που επιδιώκουν και την εμπειρία τους σε περιστατικά κυβερνοπολέμου.

ΣΤΡΑΤΗΓΙΚΗ ΗΠΑ

Οι ΗΠΑ συνδέουν την δική τους εξέλιξη και πρόοδο ως «μοναχική» υπερδύναμη του κόσμου, με την άνοδο του διαδικτύου και την αυξανόμενη κεντρική θέση του κυβερνοχώρου σε όλες τις εκφάνσεις του σύγχρονου κόσμου (The White House 2018, 1). Επιπλέον είναι απολύτως φυσικό ως ηγέτιδα χώρα στο τομέα της τεχνολογίας, να είναι σε εξαιρετικά μεγάλο βαθμό εξαρτώμενη από το διαδίκτυο και τον κυβερνοχώρο, ώστε να θεωρούνται αναπόσπαστα στοιχεία της οικονομικής, κοινωνικής και πολιτικής ζωής της Αμερικής. Η ασφάλεια στον κυβερνοχώρο για τις ΗΠΑ στηρίζεται σε δύο πυλώνες, τόσο σε πολιτικό όσο και σε στρατιωτικό.

Τον Σεπτέμβριο του τρέχοντος έτους η Αμερικανική κυβέρνηση επικύρωσε και δημοσίευσε την εθνική στρατηγική των ΗΠΑ, σχετικά με την ασφάλεια της χώρας στον κυβερνοχώρο. Σύμφωνα με τον John Bolton, σύμβουλο του Λευκού Οίκου για θέματα εσωτερικής ασφάλειας, η αναθεωρημένη στρατηγική αποτελούσε αναγκαιότητα. Πρόθεση της αμερικανικής κυβέρνησης, δεν ήταν η επίδειξη διάθεσης για εκτέλεση περισσότερων επιθετικών επιχειρήσεων στον κυβερνοχώρο αλλά, να τεθούν οι βάσεις της αποτροπής που θα υιοθετήσει, η οποία θα καταστήσει σαφές στους αντιπάλους της ότι ενδεχόμενη εμπλοκή μαζί

τους σε επιχειρήσεις θα τους προκαλέσει κόστος μεγαλύτερο απ' αυτό που μπορούν να αντέξουν (Bing 2018).

Μέσω της στρατηγικής αποτυπώνεται η πρόθεση κυβέρνησης των ΗΠΑ (The White House 2018, 1):

α. Να υπερασπιστεί το εσωτερικό της χώρας προστατεύοντας τα δίκτυα, τα πληροφοριακά συστήματα, τις λειτουργίες τους και τα αρχεία που έχουν αποθηκευμένα.

β. Να προωθήσει την αμερικανική ευημερία προάγοντας μια ασφαλή, ακμάζουσα ψηφιακή οικονομία, ενισχύοντας παράλληλα την εγχώρια καινοτομία.

γ. Να διατηρήσει την ειρήνη και την ασφάλεια, ενισχύοντας την ικανότητα των ΗΠΑ, σε συνεννόηση με συμμάχους και εταίρους, να αποτρέπει και αν χρειαστεί να τιμωρεί όσους χρησιμοποιούν ηλεκτρονικά εργαλεία (κυβερνοόπλα) για κακόβουλους σκοπούς.

δ. Να επεκτείνει την αμερικανική επιρροή στο εξωτερικό και να δημιουργήσει τις προϋποθέσεις ενίσχυσης και ανάπτυξης των βασικών αρχών ενός ανοιχτού, διαλειτουργικού, αξιόπιστου και ασφαλούς διαδικτύου.

Η σύνταξη της στρατηγικής για την ασφάλεια στον κυβερνοχώρο αποτέλεσε ουσιαστικά την αναγνώριση των ΗΠΑ, ότι έχουν εμπλακεί σε έναν διαρκή ανταγωνισμό με στρατηγικούς αντίπαλους, κράτη παρίες και τρομοκρατικά – εγκληματικά δίκτυα στο υπόψη πεδίο. Επίσης αποτέλεσε την παραδοχή, ότι ως χώρα παρουσιάζει τρωτότητα σε κυβερνοεπιθέσεις, οι οποίες εκτοξεύονται ενάντια στις κρίσιμες υποδομές της κατά την διάρκεια της ειρήνης. Παράλληλα αναγνωρίζει, ότι μια καθαρά τεχνοκρατική προσέγγιση στον κυβερνοχώρο είναι ανεπαρκής για να αντιμετωπίσει τη φύση των νέων απειλών. Ως κύριους αντίπαλους της δε, κατονομάζει την Ρωσία, την Κίνα, το Ιράν και τη Β. Κορέα αφήνοντας να εννοηθεί σαφώς, ότι τα εν λόγω κράτη χρησιμοποιούν τον κυβερνοχώρο με σκοπό, να υπονομεύουν την οικονομία, τη δημοκρατία και να υποκλέπτουν πνευματική ιδιοκτησία των ΗΠΑ (The White House 2018, 2).

Για την Αμερικανική κυβέρνηση οδηγό της στρατηγικής της θα αποτελέσει η αποτροπή μέσω της απειλής επιβολής κόστους, είτε με χρήση κυβερνοόπλων είτε με κινητικά μέσα, επιδιώκοντας να αποθαρρύνουν τους επίδοξους εισβολείς και να

αποφύγουν περαιτέρω κλιμάκωση. Στηρίζεται σε τέσσερις άξονες έκαστος εκ των οποίων υπηρετεί έναν αντικειμενικό σκοπό και καθορίζει μια σειρά ενεργειών προκειμένου να επιτευχθεί.

Ο πρώτος άξονας της στρατηγικής είναι η προστασία του Αμερικανικού λαού του εσωτερικού της χώρας και του αμερικανικού τρόπου ζωής. Στο πλαίσιο του κυβερνοχώρου, ζωτικής σημασίας αξία έχει η παροχή προστασίας των πληροφοριακών δικτύων είτε κρατικών είτε ιδιωτικών. Για να επιτευχθεί αυτό απαιτείται μια σειρά συντονισμένων ενεργειών, από την κυβέρνηση των Ηνωμένων Πολιτειών, την ιδιωτική βιομηχανία και τον Αμερικανικό λαό, οι οποίες θα εστιάζουν στην προστασία των κυβερνητικών δικτύων, στην προστασία των υποδομών ζωτικής σημασίας και στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Αντικειμενικό σκοπό αποτελεί η διαχείριση των κινδύνων, που αφορούν την ασφάλεια του κυβερνοχώρου, ώστε να αυξηθούν τα επίπεδα ασφάλειας και ανθεκτικότητας των εθνικών πληροφοριακών συστημάτων (The White House 2018, 6).

Ο πρώτος άξονας της στρατηγικής αποτελείται από τρείς επιμέρους επιδιώξεις. Η πρώτη αφορά την ασφάλεια των ομοσπονδιακών δικτύων και των πληροφοριών. Η κυβέρνηση των ΗΠΑ στοχεύει να συγκεντρώσει ορισμένες αρχές στο εσωτερικό της ομοσπονδιακής κυβέρνησης, να βελτιώσει την ικανότητα αντίληψης των απειλών στον κυβερνοχώρο, καθώς και τη δυνατότητα διαχείρισης του ομοσπονδιακού συστήματος ανεφοδιασμού και να ενδυναμώσει τις συνθήκες ασφαλείας μεταξύ των αντισυμβαλλόμενων και της κυβέρνησης. Οι ενέργειες που θα επιτρέψουν την επίτευξη αυτής της επιδίωξης είναι (The White House 2018, 6-8) :

α. Η περαιτέρω συγκεντρωτική διαχείριση και εποπτεία της αστικής ασφάλειας του κυβερνοχώρου, μέσω της κατάλληλης αξιοποίησης του αρμόδιου υπουργείου για την ασφάλεια του εσωτερικού της χώρας (Department of Homeland Security – DHS).

β. Η εκμετάλλευση της τεχνολογίας πληροφοριών από τις διαδικασίες διαχείρισης κινδύνου, που εφαρμόζουν οι επικεφαλείς των πληροφοριών (Chief Information Officer – CIO) για την εκτέλεση των αποστολών των οργανισμών τους.

γ. Η εξασφάλιση του συστήματος εφοδιασμού σε ότι αφορά τις διαδικασίες προμηθειών, εξασφαλίζοντας ότι οι τεχνολογίες που αναπτύσσουν οι κρατικές – κυβερνητικές υπηρεσίες, θα είναι ασφαλείς και αξιόπιστες.

δ. Η ενίσχυση της ασφάλειας στον κυβερνοχώρο όσων εταιριών συνεργάζονται με κρατικές και κυβερνητικές υπηρεσίες, ιδιαίτερα με αυτές του υπουργείου εθνικής άμυνας. Πιο συγκεκριμένα η στρατηγική καθορίζει τις επτά πιο κρίσιμες, που θα έχουν προτεραιότητα όσον αφορά την ανταλλαγή πληροφοριών με κυβερνητικούς εταίρους: της εθνικής ασφάλειας, της ενέργειας, του τραπεζικού και χρηματοπιστωτικού τομέα, της υγείας και της ασφάλειας, των επικοινωνιών, της τεχνολογίας των πληροφοριών και των μεταφορών (Fazzini 2018).

ε. Η υιοθέτηση από τη κυβέρνηση βέλτιστων και καινοτόμων πρακτικών που αφορούν, την προμήθεια υλικών τεχνολογίας αιχμής, την επένδυση στην ανάπτυξη και την εφαρμογή πρότυπων πρωτοβουλιών, σε νέους και αναδυόμενους τομείς ενδιαφέροντος.

Η δεύτερη επιδίωξη σκοπεύει στην παροχή ασφάλειας στις κρίσιμες υποδομές. Η ευθύνη κατανέμεται τόσο στην κυβέρνηση όσο και τον ιδιωτικό τομέα. Πρόθεση αποτελεί η προτεραιοποίηση ανάληψης δράσεων, που θα μειώσουν την δυνατότητα των προηγμένων αντιπάλων των ΗΠΑ, να προκαλέσουν μεγάλες ή μακροχρόνιες διαταραχές σε υποδομές ζωτικής σημασίας. Επίσης η αποτροπή κακόβουλων ενεργειών μέσω της επιβολής κόστους στους επίδοξους εισβολείς ή σ’ αυτούς που χρηματοδότησαν τις ενέργειες αυτών, εκμεταλλευόμενοι ένα ευρύ φάσμα εργαλείων, όπως μεταξύ άλλων, διώξεις και οικονομικές κυρώσεις στο πλαίσιο μιας ευρύτερης στρατηγικής αποτροπής (The White House 2018, 8-10).

Η τρίτη επιδίωξη των πρώτου άξονα της στρατηγικής των ΗΠΑ περιλαμβάνει την καταπολέμηση του κυβερνοεγκλήματος και την βελτίωση της διαδικασίας αναφοράς των κυβερνοπεριστατικών. Αυτό θα επιτευχθεί με την πρόβλεψη των απαραίτητων νομικών αρχών και την διάθεση πόρων, με σκοπό την καταπολέμηση της διακρατικής εγκληματικότητας στο κυβερνοχώρο. Επιπλέον η συνεργασία της δικαιοσύνης με τον ιδιωτικό τομέα θα συμβάλλει στην αντιμετώπιση των προκλήσεων, που παρουσιάζουν οι τεχνολογίες που παρέχουν ανωνυμία και δυνατότητα κρυπτογράφησης. Οι κατά προτεραιότητα ενέργειες

προβλέπουν την βελτίωση της διαδικασίας αναφοράς περιστατικών και της ανταπόκρισης, τον εκσυγχρονισμό των νόμων περί ηλεκτρονικής επιτήρησης και εγκληματικότητας στον τομέα των υπολογιστών, στη μείωση των απειλών από διεθνικές εγκληματικές οργανώσεις στον κυβερνοχώρο, στη βελτίωση της κατανόησης του τρόπου ενεργείας των εγκληματιών του κυβερνοχώρου, που βρίσκονται στο εξωτερικό και τέλος στην ενίσχυση της ικανότητας επιβολής του νόμου των εταίρων για την καταπολέμηση της εγκληματικής δραστηριότητας στον κυβερνοχώρο (The White House 2018, 10-11).

Ο δεύτερος άξονας της στρατηγικής των ΗΠΑ στοχεύει στην προώθηση της Αμερικανικής ευημερίας. Σκοπός είναι η διατήρηση της επιρροής των Ηνωμένων Πολιτειών στο χώρο της τεχνολογίας και στην ανάπτυξη του κυβερνοχώρου. Η σχεδίαση για την επίτευξη του περιλαμβάνει (The White House 2018, 14):

α. Την ενθάρρυνση δημιουργίας μιας ανθεκτικής ψηφιακής οικονομίας, δεδομένου ότι αυτή είναι άρρηκτα συνδεδεμένη με την εθνική ασφάλεια, διαμορφώνοντας και προωθώντας πρότυπα που θα ενισχύουν την ασφάλεια της και την ζωτικότητα της αμερικανικής αγοράς και καινοτομίας.

β. Την ενδυνάμωση και την προστασία της εφευρετικότητας των Ηνωμένων Πολιτειών μέσω της οποίας αποσκοπούν στη διατήρηση του στρατηγικού πλεονεκτήματος στον κυβερνοχώρο. Αυτό θα επιτευχθεί υιοθετώντας θεσμούς και προγράμματα που θα προάγουν την ανταγωνιστικότητα, θα καταπολεμήσουν την κλοπή πνευματικής ιδιοκτησίας και θα προωθήσουν τις διαδικασίες διευκρίνησης του εκάστοτε εισβολέα.

γ. Την δημιουργία και ανάπτυξη ενός εξειδικευμένου εργατικού δυναμικού, στον τομέα του κυβερνοχώρου, αξιοποιώντας πλήρως το ταλέντο του εγχώριου πληθυσμού και παράλληλα προσελκύοντας τους λαμπρότερους επιστήμονες από το εξωτερικό.

Ο τρίτος άξονας της αμερικανικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο είναι η διατήρηση της ειρήνης μέσω της ισχύος. Κυρίαρχο στόχο του αποτελεί, ο προσδιορισμός, η αντιμετώπιση, η διατάραξη, η υποβάθμιση και η αποτροπή συμπεριφορών στον κυβερνοχώρο, οι οποίες είναι αποσταθεροποιητικές και αντίθετες με τα συμφέροντα των ΗΠΑ. Παράλληλα αποσκοπεί στη διατήρηση της υπέρτερης θέσης τους, έναντι των υπόλοιπων

κρατών, μέσα και μέσω του κυβερνοχώρου. Η υλοποίηση του θα στηριχθεί (The White House 2018, 20-21):

α. Στην ενδυνάμωση της σταθερότητας στον κυβερνοχώρο, μέσω της υιοθέτησης κανόνων υπεύθυνης κρατικής συμπεριφοράς, με βάση το διεθνές δίκαιο και τη λήψη μέτρων οικοδόμησης εμπιστοσύνης, για τη μείωση του κινδύνου συγκρούσεων, που προέρχονται από κακόβουλη δραστηριότητα στον κυβερνοχώρο.

β. Στην απόδοση ευθυνών και την αποτροπή μη αποδεκτών συμπεριφορών στον κυβερνοχώρο αξιοποιώντας όλα τα διαθέσιμα μέσα εθνικής εξουσίας. Αυτά περιλαμβάνουν τα διπλωματικά, τις πληροφορίες, τα στρατιωτικά (κινητικά και στο πεδίο του κυβερνοχώρου), τα οικονομικά, καθώς και τις δυνατότητες επιβολής του νόμου. Επιδίωξη των ΗΠΑ αποτελεί, η τυποποίηση της διαδικασίας ανάληψης ενεργειών και επίτευξης συνεργασίας με άλλα συμμαχικά κράτη, σε ότι αφορά την απόδοση και την αποτροπή κακόβουλων δραστηριοτήτων στον κυβερνοχώρο. Αυτό θα καταστεί δυνατό με την εφαρμογή ολοκληρωμένων στρατηγικών που θα επιβάλλουν ταχείες και δαπανηρές συνέπειες σε όσους επιβουλεύονται τα αμερικανικά συμφέροντα.

Ο τέταρτος και τελευταίος άξονας αναφέρεται στην πρόοδο και την εξέλιξη της Αμερικανικής επιρροής. Αντικειμενικός σκοπός του εν λόγω άξονα, είναι η διατήρηση της μακροπρόθεσμης προσβασιμότητας, της διαλειτουργικότητας, της ασφάλειας και της αξιοπιστίας του διαδικτύου, το οποίο υποστηρίζει και ενισχύεται από τα συμφέροντα των ΗΠΑ. Επιμέρους στόχοι που θα καταστήσουν δυνατή την επίτευξη του είναι (The White House 2018, 24-26):

α. Η προώθηση ενός προσβάσιμου, διαλειτουργικού, αξιόπιστου και ασφαλούς διαδικτύου εξασφαλίζοντας ότι αυτή η προσέγγιση θα αποτελέσει τη διεθνή πρακτική και πρότυπο. Επιδίωξη είναι η αποτροπή των κρατών, ιδίως αυτών με αυταρχικά καθεστώτα, να αντιμετωπίζουν το διαδίκτυο ως πολιτική απειλή και υπό το πρόσχημα της ασφάλειας ή της καταπολέμησης της τρομοκρατίας να το μετατρέπουν σε διαδίκτυο υπό τον έλεγχο τους.

β. Η οικοδόμηση διεθνούς δυναμικής στον κυβερνοχώρο μέσω πρωτοβουλιών για την δημιουργία των απαιτούμενων ικανοτήτων που θα το καταστήσουν αυτό εφικτό. Στόχο των ΗΠΑ αποτελεί η οικοδόμηση στρατηγικών

εταιρικών σχέσεων, που θα βασίζονται σ' ένα κοινό όραμα για ένα διαδίκτυο που θα εξασφαλίζει την ασφάλεια στο κυβερνοχώρο και θα ενθαρρύνει τις επενδύσεις και τη δημιουργία νέων οικονομικών αγορών. Επιπλέον η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των εταίρων, θα επιτρέψει τη βέλτιστη υπεράσπιση των κρισίμων υποδομών και των συστημάτων εφοδιασμού τους. Η διατήρηση της ηγετικής θέσης των ΗΠΑ στην οικοδόμηση συνεργατικής ικανότητας στον κυβερνοχώρο, είναι ζωτικής σημασίας για τη διατήρηση της αμερικανικής επιρροής έναντι των ανταγωνιστών της.

Σε πλήρη ευθυγράμμιση με τη στρατηγική του Λευκού Οίκου βρίσκεται και το Δόγμα των Ενόπλων Δυνάμεων των ΗΠΑ, το οποίο παρέχει οδηγίες για τη σχεδίαση, εκτέλεση και αξιολόγηση των επιχειρήσεων στον κυβερνοχώρο (Joint Chiefs of Staff 2018, xvii). Αρμόδιος φορέας για την σχεδίαση και διεξαγωγή αυτών είναι η Αμερικανική Διοίκηση Κυβερνοχώρου (USCYBERCOM), η οποία εκτελεί την αποστολή της εξασφαλίζοντας την ασφάλεια, λειτουργία και άμυνα του δικτύου πληροφοριών του Υπουργείου Άμυνας (Department Of Defence Information Network - DODIN), υπερασπίζοντας το έθνος από μια κυβερνοεπίθεση και παρέχοντας υποστήριξη στους Διοικητές των Επιχειρησιακών Σχηματισμών (Combatant Commanders – CCDR's) στον κυβερνοχώρο (Joint Chiefs of Staff 2018, ix).

Ειδικότερα οι μορφές των επιχειρήσεων μέσα στον κυβερνοχώρου και μέσω αυτού που αναλαμβάνονται από τις Ένοπλες Δυνάμεις των ΗΠΑ είναι (Joint Chiefs of Staff 2018, xi):

α. Παροχής προστασίας του δικτύου πληροφοριών του υπουργείου άμυνας, οι οποίες περιλαμβάνουν τις ενέργειες εκείνες που απαιτούνται για τη δημιουργία και διατήρηση της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότητας του δικτύου.

β. Αμυντικές, οι οποίες περιλαμβάνουν αποστολές των κυβερνοδυνάμεων για την υπεράσπιση του αμερικανικού κυβερνοχώρου από ενεργές απειλές.

γ. Επιθετικές, οι οποίες είναι αποστολές που στόχο έχουν την προβολή ισχύος μέσα και μέσω ξένων κυβερνοχώρων για την υποστήριξη και πλαισίωση των ενεργειών των επιχειρησιακών σχηματισμών.

Αναμενόμενα η σημασία της υποστήριξης των επιχειρήσεων κυβερνοχώρου στις στρατιωτικές επιχειρήσεις αυξάνεται σε άμεση αναλογία με την εξάρτηση της διακλαδικής δύναμης στο υπόψη πεδίο (Joint Chiefs of Staff 2018, I-8). Επιδίωξη των διακλαδικών διοικητών είναι η ενσωμάτωση των εν λόγω επιχειρήσεων σε άλλες κινητικού χαρακτήρα, με απώτερο σκοπό τη δημιουργία συντονισμένων και συγχρονισμένων αποτελεσμάτων, που απαιτούνται για την υποστήριξη ολοκλήρωσης της αποστολής τους (Joint Chiefs of Staff 2018, I-1). Μέσω αυτών επιδιώκουν να επιτύχουν ή να διατηρήσουν την ελευθερία κινήσεων τους στον κυβερνοχώρο, να αρνηθούν αντίστοιχα την ελευθερία δράσης στον αντίπαλο, να επιτύχουν τους αντικειμενικούς τους στόχους και παράλληλα να επιτρέψουν και άλλες επιχειρησιακές δραστηριότητες. Προκειμένου να καταστεί αποτελεσματική η ενσωμάτωση των επιχειρήσεων του κυβερνοχώρου στο φυσικό πεδίο, απαιτεί την ενεργό συμμετοχή όσων εμπλέκονται στη σχεδίαση και την εκτέλεση αυτών, σε κάθε φάση των διακλαδικών επιχειρήσεων που χρήζουν υποστήριξης.

Ο καθορισμός των σχέσεων διοίκησης είναι ζωτικής σημασίας για τις αμερικανικές ΕΔ, για την εξασφάλιση της έγκαιρης και αποτελεσματικής εμπλοκής δυνάμεων, καθώς οι επιχειρήσεις κυβερνοχώρου απαιτούν ενότητα διοίκησης και προσπάθειας. Οι διακλαδικές δυνάμεις, ως στρατηγική έχουν υιοθετήσει τον κεντρικό σχεδιασμό σε συνδυασμό με την αποκεντρωμένη εκτέλεση στις επιχειρήσεις (Joint Chiefs of Staff 2018, iv-11). Ειδικότερα οι επιχειρήσεις στον κυβερνοχώρο απαιτούν συνεχή και λεπτομερή συντονισμό, δεδομένου ότι λαμβάνουν χώρα σ’ ένα παγκόσμιο θέατρο επιχειρήσεων, εξαιτίας της μη ύπαρξης γεωγραφικών δεσμεύσεων αλλά και του ρόλου των ΗΠΑ ως υπερδύναμη, που επιβάλλει την εμπλοκή τους σε ολόκληρη την υφήλιο. Αυτή η συνθήκη δημιουργεί την ανάγκη ενός δυναμικού πλαισίου διοικήσεως και ελέγχου, που να μπορεί να προσαρμοστεί στις συνεχείς αλλαγές, τις αναδυόμενες απειλές και το άγνωστο. Τα κρίσιμα σημεία επίτευξης συγχρονισμού των επιχειρήσεων στον κυβερνοχώρο, είναι η διατήρηση της γνώσης της τακτικής κατάστασης και η αξιολόγηση των πιθανών επιπτώσεων επί της διακλαδικής δύναμης οποιασδήποτε σχεδιαζόμενης επιχείρησης σ’ αυτόν (Joint Chiefs of Staff 2018, iv-18).

ΣΤΡΑΤΗΓΙΚΗ ΚΙΝΑΣ

Γενεσιουργό αιτία για την επένδυση της Κίνας στην ανάπτυξη δυνατοτήτων στον κυβερνοχώρο αποτέλεσε ο πόλεμος του κόλπου στις αρχές του 1990. Η εξέλιξη του πολέμου, στην οποία σημαντικό ρόλο διαδραμάτισε η τεχνολογική ανωτερότητα των ΗΠΑ, ώθησε τους Κινέζους ηγέτες να διαπιστώσουν πόσο αναχρονιστικές ήταν οι δικές τους συμβατικές δυνατότητες. Έκτοτε κάθε αναφορά τους στην επιχείρηση «Dessert Storm» γίνεται με την ονομασία «zhongda biange», δηλαδή η μεγάλη μεταμόρφωση (Patterson 2011, 121) .

Στο διάστημα που μεσολάβησε η Κίνα παρουσίασε σημαντική πρόοδο, καθώς αντιλήφθηκε, ότι μέσω του κυβερνοχώρου μπορεί να ανατρέψει τους περιορισμούς που επιβάλλει η γεωγραφική της θέση. Στην πραγματικότητα ο κυβερνοχώρος επιτρέπει στην Κίνα να ασκήσει προβολή ισχύος, μέσω της διενέργειας κυβερνοπολέμου σε παγκόσμια κλίμακα, διασπώντας την απομόνωση στην οποία την θέτουν, τόσο οι αχανείς χερσαίες μάζες από τα δυτικά, όσο και η θάλασσα από τα ανατολικά, όπου κυριαρχούν οι ναυτικές δυνάμεις των ΗΠΑ. Παράλληλα της επιτρέπει να αξιοποιήσει γεωστρατηγικά το τεράστιο πληθυσμιακό δυναμικό της (Γρίβας n.d.).

Στα τέλη του 2016 η Κίνα παρουσίασε την εθνική της στρατηγική για την ασφάλεια στον κυβερνοχώρο. Κίνητρο για την έκδοση της στρατηγικής αποτέλεσε η ανάγκη για τη διασφάλιση της κυριαρχίας και της ασφάλειας του κράτους και της ανάπτυξης του κυβερνοχώρου[20]. Επιδίωξη της κυβέρνησης της Κίνας είναι ο έλεγχος του διαδικτύου, καθώς ανέκαθεν υπήρχε η πεποίθηση, ότι οι μη ελεγχόμενες πληροφορίες υπονομεύουν το καθεστώς. Μάλιστα για την Κίνα η όλη ιδέα του διαδικτύου είναι χτισμένη γύρω από τον έλεγχο των πληροφοριών μέσω λογοκρισίας, γεγονός το οποίο αποτελεί εντελώς διαφορετική προσέγγιση σε σχέση με τη Δύση. Στην ουσία από τη στιγμή που το διαδίκτυο ανάχθηκε σε δημοφιλή δημόσια πλατφόρμα επικοινωνίας για την κυβέρνηση της Κίνας, το ερώτημα δεν ήταν, αν θα ελέγξουν το διαδίκτυο και τη διανομή των πληροφοριών, αλλά πως θα το ελέγξουν (Raud 2016, 6).

Σύμφωνα με τη στρατηγική της Κίνας η έλλειψη ασφάλειας στον κυβερνοχώρο επισύρει μια σειρά προκλήσεων και κινδύνων για το κράτος και τους

[20] Central Cyber Security and Informatization Committee Office 2016

πολίτες του. Οι επιπτώσεις της αποτυπώνονται στην πολιτική και οικονομική ασφάλεια. Επίσης οι επιβλαβείς πληροφορίες στο διαδίκτυο φαλκιδεύουν την πολιτιστική ασφάλεια, ενώ η τρομοκρατία και τα παράνομα εγκλήματα υπονομεύουν την αντίστοιχη κοινωνική. Παράλληλα ο διεθνής ανταγωνισμός για την εκμετάλλευση του κυβερνοχώρου ή την απαγόρευση εκμετάλλευσης του από τον αντίπαλο, είναι σε άνοδο. Αυτό αποδεικνύεται από την εντατικοποίηση των εξοπλισμών στο υπόψη πεδίο με αποτέλεσμα την αμφισβήτηση της παγκόσμιας ειρήνης, δικαιώνοντας τις ανησυχίες των Κινέζων[21].

Κυρίαρχη επιδίωξη και στρατηγικός στόχος της Κίνας ,είναι να καταστεί διαδικτυακή δύναμη. Η τακτική που θα ακολουθήσει περιλαμβάνει την υιοθέτηση καινοτομίας στην εφαρμογή της αναπτυξιακής αντίληψης, την προώθηση της ειρήνης στον κυβερνοχώρο, την ενίσχυση της απόκτησης γνώσης σε θέματα κινδύνου και κρίσεων και τον συντονισμό της ενεργού άμυνας και της αποτελεσματικής αντίδρασης του κράτους με γνώμονα πάντα την εθνική ασφάλεια[22].

Η αντίληψη της Κίνας είναι, ότι ένας ασφαλής και σταθερός κυβερνοχώρος που θα παρέχει ευημερία, έχει μεγάλη σημασία για όλες τις χώρες και τον κόσμο. Γι' αυτό και δηλώνει πρόθυμη να συνεργαστεί με άλλες χώρες, ώστε να ενισχυθεί η επικοινωνία, να διευρυνθεί η συναίνεση, να επεκταθεί η συνεργασία και να συμβάλλει ενεργά αφενός στην προώθηση μετασχηματισμού του παγκόσμιου συστήματος διακυβέρνησης του Διαδικτύου και αφετέρου στην προστασία της ειρήνης και την ασφάλειας στον κυβερνοχώρο. Οι αρχές που θέτουν το πλαίσιο και αποτελούν οδηγό της στρατηγικής της Κίνας, είναι ο σεβασμός της διατήρησης της κυριαρχίας εκάστου κράτους στον κυβερνοχώρο, η ειρηνική χρήση του, η διακυβέρνηση του με βάση τον νόμο και ο συντονισμός και συγχρονισμός της ανάπτυξης και της ασφάλειας των δικτύων [23].

Η Κίνα εκτιμά ότι η ασφάλεια των δικτύων της δεν αποτελεί αποκλειστικά δικό της συμφέρον αλλά και παγκόσμιο, λόγω του τεράστιου αριθμού των κινέζων

[21] Όπως παραπάνω.
[22] Όπως παραπάνω.
[23] Όπως παραπάνω.

χρηστών του διαδικτύου. Οι άξονες πάνω στους οποίους θα στηριχθεί η στρατηγική της είναι[24] :

α. Η υπεράσπιση της κυριαρχίας του κυβερνοχώρου. Η Κίνα δηλώνει αποφασισμένη να αντιταχθεί σε κάθε πράξη που θα υπονομεύσει την πολιτική εξουσία του κράτους και την εθνική της κυριαρχία μέσω του διαδικτύου. Στο πλαίσιο αυτό θα επιστρατεύσει κάθε πρόσφορο μέσο συμπεριλαμβανομένου της οικονομίας, της επιστήμης και της τεχνολογίας και της στρατιωτικής ισχύος προκειμένου να προστατεύσει τις πληροφοριακές εγκαταστάσεις και συστήματα.

β. Η αποφασιστική περιφρούρηση της εθνικής ασφάλειας. Ο άξονας αυτός θα στηριχθεί στην πρόληψη, την παύση και την τιμωρία οποιουδήποτε, είτε προερχόμενου από το εσωτερικό είτε από το εξωτερικό, επιχειρήσει να προδώσει, αποσχίσει, ανατρέψει ή υποκινήσει την ανατροπή του πολιτικού καθεστώτος της Κίνας κάνοντας χρήση του διαδικτύου. Ουσιαστικό ρόλο στην επίτευξη αυτού του στόχου, αναμφίβολα θα διαδραματίσει η ικανότητα της αποτροπής, τομέας στον οποίο η Κίνα επενδύει σε σταθερή βάση.

γ. Η προστασία των κρισίμων υποδομών, οι οποίες σχετίζονται με την εθνική ασφάλεια, την εθνική οικονομία και τον βιοπορισμό των πολιτών γενικότερα. Σύμφωνα με τη στρατηγική της Κίνας, η προστασία των πληροφοριακών υποδομών και των δεδομένων από επιθέσεις στον κυβερνοχώρο αποτελεί κοινή ευθύνη της κυβέρνησης, των επιχειρήσεων και ολόκληρης της κοινωνίας. Αυτό θα επιτευχθεί με την δημιουργία και εφαρμογή συστήματος επιθεώρησης ασφάλειας δικτύων, την ενίσχυση της διαχείρισης της ασφάλειας του συστήματος εφοδιασμού και τη διεξαγωγή ελέγχων ασφαλείας σε σημαντικά προϊόντα και υπηρεσίες τεχνολογίας, που σχετίζονται με την πληροφορική και προμηθεύονται το πολιτικό κόμμα, τα κυβερνητικά όργανα και οι σημαντικές βιομηχανίες.

δ. Η ενίσχυση της οικοδόμησης κουλτούρας δικτύων και του διαδικτύου γενικότερα. Επιδίωξη της κυβέρνησης είναι η καλλιέργεια και η πρακτική εφαρμογή των θεμελιωδών αρχών του σοσιαλισμού, η ανάπτυξη και αναβάθμιση κουλτούρας δικτύων και η ένταξη σ' αυτά των ισχυρών πνευματικών και ακαδημαϊκών δυνάμεων της χώρας. Έμφαση επίσης θα δοθεί στην προώθηση της

[24] Όπως παραπάνω.

ψηφιοποίησης και της διάδοσης του πολιτισμού μεταξύ της Κίνας και άλλων χωρών. Τελικός στόχος είναι η δημιουργία ενός υγιούς περιβάλλοντος, που θα συμβάλλει θετικά στην ανάπτυξη της νεολαίας αποτέλεσμα το οποίο θα επέλθει από τη κοινή προσπάθεια της κυβέρνησης των κοινωνικών οργανώσεων, των κοινοτήτων των σχολείων και των ίδιων των οικογενειών.

ε. Η καταπολέμηση της τρομοκρατίας και των εγκλημάτων στον κυβερνοχώρο. Αυτό θα επιτευχθεί με την ενδυνάμωση των δυνατοτήτων των δικτύων σε ότι αφορά την καταπολέμηση της τρομοκρατίας, της κατασκοπίας και κλοπής.

στ. Η βελτίωση του συστήματος διακυβέρνησης των δικτύων. Απόφαση της κινέζικης κυβέρνησης είναι η επιτάχυνση της δημιουργίας ενός συστήματος διακυβέρνησης δικτύων, που θα συνδυάζει την απαιτούμενη νομική πλαισίωση με νόμους, που θα ανταποκρίνονται στις απαιτήσεις του κυβερνοχώρου, την διοικητική και δημόσια επίβλεψη, την αυτοπειθαρχία του ιδιωτικού τομέα, την τεχνική υποστήριξη και την κοινωνική εκπαίδευση.

ζ. Η εδραίωση της ασφάλειας των δικτύων με την προσκόλληση στην ανάπτυξη που θα βασίζεται στην καινοτομία. Αυτό περιλαμβάνει την επικέντρωση στην ασφάλεια του λογισμικού και επίσπευση της προώθησης και εφαρμογής της ασφάλειας, καθώς και προϊόντων, που θα χαίρουν της κυβερνητικής εμπιστοσύνης. Επιπλέον θα επιδιώξει την ανάπτυξη των υποδομών δικτύου και τον εμπλουτισμό πληροφοριακού περιεχομένου στον κυβερνοχώρο. Την δημιουργία και βελτίωση του εθνικού συστήματος υποστήριξης τεχνολογίας δικτύων. Την ενίσχυση της βασικής θεωρίας της ασφάλειας δικτύων και της έρευνας σε σημαντικά θέματα. Την ενίσχυση της τυποποίησης της ασφάλειας δικτύων, της πιστοποίησης και της διαπίστευσης και μεγαλύτερη χρήση των προτύπων για την τυποποίηση της συμπεριφοράς του κυβερνοχώρου. Τέλος σημαντικά σ’ αυτόν τον άξονα θα συμβάλλει η προώθηση της εκπαίδευσης στον κυβερνοχώρο με κατάλληλο εκπαιδευτικό υλικό, το οποίο θα εισαχθεί στο σχολείο και τις αίθουσες διδασκαλίας.

η. Η βελτίωση της ικανότητας προστασίας στον κυβερνοχώρο. Για την Κίνα ο κυβερνοχώρος είναι το νέο όριο εθνικής κυριαρχίας. Πρόθεση της είναι η δημιουργία μιας δύναμης προστασίας δικτύων, που θα είναι ανάλογη του διεθνούς

κύρους της και συμβατή με τις άλλες δυνάμεις του κυβερνοχώρου. Επιπλέον θα αναπτύξει δυναμικές μεθόδους άμυνας και ασφάλειας δικτύων, που θα επιτρέψουν την έγκαιρη διαπίστωση και αποτελεσματική αντιμετώπιση παράνομων διεισδύσεων.

θ. Η ενδυνάμωση ενεργής και αποτελεσματικής διεθνούς συνεργασίας στον κυβερνοχώρο, η οποία θα επέλθει μέσω της εμβάθυνσης του διαλόγου με τις άλλες χώρες και με την υποστήριξη της προσπάθειας των Ηνωμένων Εθνών να διαδραματίσουν ηγετικό ρόλο στην προώθηση της ανάπτυξης παγκοσμίως αποδεκτών διεθνών κανόνων για τον κυβερνοχώρο. Επίσης με την προώθηση του σχεδίου «Belt and Road[25]» και τη βελτίωση του επιπέδου της διεθνούς επικοινωνίας και της διασύνδεσης μεταξύ των κρατών.

Ωστόσο χαρακτηρίζεται τουλάχιστον αντιφατικό το γεγονός, ότι παρά την εκπεφρασμένη στρατηγική της για διεύρυνση της διεθνούς συνεργασίας αυτή, να μην αποδέχεται το διεθνές δίκαιο ως κύριο ρυθμιστή του κυβερνοχώρου, αλλά να προτιμά κάθε κράτος να θέτει τους δικούς του κανόνες. Επιπρόσθετα η Κίνα έχει επικρίνει το εγχειρίδιο του Ταλίν ως προσπάθεια χειραγώγησης του κυβερνοχώρου μέσω του νόμου. (Raud 2016, 7). Η ανωτέρω διαπίστωση σε συνδυασμό με την υφιστάμενη βιβλιογραφία, οδηγεί στο συμπέρασμα ότι η Κίνα πέραν της επίσημης στρατηγικής για την ασφάλεια στον κυβερνοχώρο, η οποία αποτελεί ουσιαστικά την επίσημη τοποθέτηση - δέσμευση του κράτους απέναντι στο διεθνές ακροατήριο του, διαφαίνεται να έχει κρυφή ατζέντα ειδικά σε ότι αφορά τον κυβερνοπόλεμο. Άλλωστε η συγκεκριμένη μορφή επιχειρήσεων περιγράφεται σε πολλές πηγές της στρατιωτικής βιβλιογραφίας ως μια επαναστατική μέθοδος στις στρατιωτικές υποθέσεις (Lindsay 2014/2015, 30)

Όπως αναφέρθηκε παραπάνω η οπτική της Κίνας διαφέρει από αυτή των χωρών της Δύσης. Αυτό δεν αποτελεί πλέον υπόθεση αλλά γεγονός, το οποίο αποτυπώθηκε πρώτη φορά μέσω του Οργανισμού Συνεργασίας της Σαγκάης (Shangai Cooperation Organisation – SCO) του οποίου η Κίνα είναι μέλος. Κοινή πεποίθηση του οργανισμού είναι ότι η υπεροχή του έθνους – κράτους πρέπει να μεταφέρεται και στον κυβερνοχώρο. Αυτό πρακτικά δίνει το δικαίωμα στο κράτος

[25] Το σχέδιο «Belt and Road» ή «yi dai yi lu» αποτελεί τον δρόμο του μεταξιού του 21ου αιώνα και εκφράζει το μεγαλόπνοο σχέδιο του προέδρου Xi Jinping. Συνίσταται από μια ζώνη χερσαίων διαδρόμων και ένα δρόμο θαλάσσιων λωρίδων που στοχεύουν στην οικονομική και εμπορική σύνδεση της Κίνας με την Ασία, Αφρική και την Ευρώπη (Kuo n.d.).

να ελέγχει τους χρήστες που βρίσκονται εντός των ορίων του είτε είναι εγχώριοι είτε αλλοδαποί, ενέργεια η οποία είναι συμβατή με την πολιτική κουλτούρα της Κίνας, όπου προτεραιότητα έχει η διατήρηση της κοινωνικής τάξης συγκριτικά με τον σεβασμό της ιδιωτικότητας (Raud 2016, 7).

Σύμφωνα με τον Kellermann[26], η κινεζική φιλοσοφία περί κυβερνοπολέμου, βασίζεται στη λεγόμενη θεωρία των «1000 κόκκων άμμου». Η συγκεκριμένη θεωρία πρεσβεύει, ότι αντί για μια μεγάλη επίθεση είναι προτιμότερο να εξαπολύεις έναν μεγάλο αριθμό μικρών επιθέσεων, επιδιώκοντας κατά κάποιον τρόπο, να περάσεις μέσα από τις χαραμάδες των συστημάτων ασφαλείας του εχθρού. Όσον αφορά τον κυβερνοχώρο, οι μικροσκοπικής κλίμακας επιθέσεις επιδιώκεται να θεωρηθούν ασήμαντα συμβάντα και να μην αξιολογηθούν καν από τα συμβατικά συστήματα κυβερνοασφάλειας, επιτρέποντας έτσι στον επιτιθέμενο να εισέλθει σε πληροφοριακά συστήματα τοποθετώντας κακόβουλο λογισμικό (Γρίβας n.d.).

Μια άλλη άποψη, η οποία είναι άμεσα συνδεόμενη με την ανωτέρω φιλοσοφία, θεωρεί ότι βάση της συμπεριφοράς όσο και της στρατηγικής αντίληψης της Κίνας για τον ασύμμετρο πόλεμο γενικά και τον κυβερνοπόλεμο ειδικότερα, αποτέλεσε το βιβλίο δύο συνταγματαρχών του Κινεζικού Στρατού, Qiao Liang και Wang Xiangsui[27]. Σ' αυτό περιγράφεται η στρατηγική που πρέπει να υιοθετήσει η Κίνα ως ασθενέστερη χώρα, ώστε να επιβληθεί ενός τεχνολογικά υπέρτερου εχθρού έξω από το πεδίο εφαρμογής της σκληρής στρατιωτικής δύναμης. Στο ίδιο βιβλίο οι δύο συγγραφείς αναγνωρίζουν ως κύρια αδυναμία των ενόπλων δυνάμεων των ΗΠΑ[28] την εξάρτηση τους από τα δικτυοκεντρικά συστήματα από την εκμετάλλευση των οποίων η Κίνα δύναται να αποκτήσει ένα ασύμμετρο πλεονέκτημα. (Raud 2016, 9).

---

[26] Ο Tom Kellermann, είναι αντιπρόεδρος της εδρεύουσας στη Βοστώνη εταιρείας πληροφορικής ασφάλειας Core Security Technologies. Υποστηρίζει ότι η Κίνα έχει τις μεγαλύτερες δυνατότητες κυβερνοεπίθεσεων στον πλανήτη και ενδέχεται να είναι σε θέση να διεξαγάγει μια επίθεση εναντίον των ΗΠΑ έναντι της οποίας οι τελευταίες να μην είναι σε θέση να αντιδράσουν, ενώ οι ζημιές που θα υποστούν θα είναι κατακλυσμιαίες (Γρίβας n.d.).

[27] Το βιβλίο φέρει τον τίτλο Απεριόριστος Πόλεμος. Η πρώτη έκδοση του βιβλίου στην Αγγλική γλώσσα έγινε από έναν άγνωστο εκδότη από τον Παναμά με τίτλο «Το κύριο σχέδιο της Κίνας για την καταστροφή της Αμερικής» και στο εξώφυλλο του περιείχε το παγκόσμιο κέντρο εμπορίου να καίγεται. Αυτές οι προσθήκες θεωρήθηκαν ως παρερμηνείες του κειμένου που δεν προορίζονταν από τους αρχικούς συντάκτες.(https://en.wikipedia.org/wiki/Unrestricted_Warfare)

[28] Ένα άλλο γεγονός που χαρακτηρίζει την συμπεριφορά της Κίνας στον κυβερνοχώρο επίσης είναι η αντιπάθεια για τις ΗΠΑ τις ενέργειες των οποίων χρησιμοποιεί συχνά ως δικαιολογία για τις αντίστοιχες δικές της (Raud 2016, 7).

Αυτοί που ασχολούνται με τη στρατηγική στην Κίνα ισχυρίζονται, ότι εκτελώντας κεκαλυμμένη επίθεσή εναντίον των πληροφοριακών συστημάτων ενός αντιπάλου από απόσταση, εκτός του βεληνεκούς των οπλικών συστημάτων του, είναι δυνατόν να προκαλέσουν παράλυση της οργάνωσης του, να επιδράσουν στη διαδικασία της στρατηγικής λήψης αποφάσεων καθώς και στην εθνική του οικονομία (Lindsay 2014/2015, 31).

Στην υλοποίηση της στρατηγικής του κυβερνοπολέμου συμμετέχουν φορείς από όλες τις εκφάνσεις της κοινωνικής ζωής της Κίνας. Οι κύριοι εκφραστές βέβαια είναι τα κρατικά – κυβερνητικά όργανα, τα οποία έχουν την ευθύνη καθορισμού της πολιτικής. Οι ένοπλες δυνάμεις οι οποίες είναι ο φορέας που εκτελεί τις επιχειρήσεις στον κυβερνοχώρο κάνοντας χρήση των κυβερνοόπλων. Ανεξάρτητες ομάδες χάκερς, οι οποίες λειτουργούν είτε αυτόνομα υποκινούμενες από πατριωτικό ένστικτο, είτε καθοδηγούμενες από το κράτος επιλογή η οποία αξιοποιεί βέλτιστα το τεράστιο ανθρώπινο δυναμικό της χώρας. Τέλος συμμετοχή έχει και η ακαδημαϊκή κοινότητα, η οποία διεξάγει μελέτες που καλύπτουν ένα ευρύ φάσμα δραστηριοτήτων κυρίως σε ότι αφορά την εξέλιξη κυβερνοόπλων.

Για τη χάραξη πολιτικής, το Κρατικό Συμβούλιο (State Council) είναι αυτό που συνήθως υιοθετεί νέες πρωτοβουλίες, συμπεριλαμβανομένων εκείνων στον κυβερνοχώρο, αλλά υπάρχουν αρκετές κυβερνητικές υπηρεσίες επιφορτισμένες με την εκτέλεση πολιτικής. Το υπουργείο βιομηχανίας και πληροφοριακής τεχνολογίας[29] (Ministry of Industry and Information Technology – MIIT) το οποίο αντικαθιστά το κρατικό συμβούλιο και έχει έργο ανάλογο με αυτό του υπουργείου για την ασφάλεια του εσωτερικού των ΗΠΑ. Το υπουργείο δημόσιας ασφάλειας (Ministry of Public Security) το οποίο ασχολείται με το κυβερνοέγκλημα, την προστασία των κρίσιμων υποδομών ενώ παράλληλα είναι υπεύθυνο για την λειτουργία του μεγάλου τείχους προστασίας της Κίνας στο διαδίκτυο(Great Firewall of China[30]). Το υπουργείο κρατικής ασφάλειας (Ministry of State Security) του οποίου οι προσπάθειες επικεντρώνονται στην αντιμετώπιση των αυτονομιστικών

[29] Στο έργο του που αφορά την αντιμετώπιση των κυβερνοεπιθέσεων συνεπικουρείται από το National Computer Network Emergency Response Technical Team/ Coordination Centre of China (CNCERT) το οποίο είναι μη κυβερνητικό τεχνικό κέντρο που ιδρύθηκε το 2002.

[30] Το Μεγάλο Τείχος προστασίας της Κίνας (GFW) είναι ο συνδυασμός των νομοθετικών δράσεων και των τεχνολογιών που επιβάλλει η Λαϊκή Δημοκρατία της Κίνας για τη ρύθμιση του Διαδικτύου στο εσωτερικό της χώρας. Ο ρόλος της στη λογοκρισία του Διαδικτύου στην Κίνα είναι η παρεμπόδιση της πρόσβασης σε επιλεγμένες ξένες ιστοσελίδες και η επιβράδυνση της διασυνοριακής διαδικτυακής κυκλοφορίας. (https://en.wikipedia.org/wiki/Great_Firewall)

ενεργειών, της τρομοκρατίας και του θρησκευτικού εξτρεμισμού απειλές που για το κομουνιστικό κόμμα είναι οι επικινδυνότερες (Raud 2016, 16-17).

Σε ότι αφορά το σκέλος των ενόπλων δυνάμεων το τελευταίο διάστημα βρίσκονται σε μια διαδικασία μεταρρυθμίσεων με την ημερομηνία ολοκλήρωσης να παραμένει άγνωστη. Μέχρι πρότινος την ευθύνη για την εκτέλεση επιχειρήσεων στον κυβερνοχώρο την είχαν το 3ο (3/PLA) και το 4ο (4/PLA) τμήμα του Γενικού Επιτελείου του Λαϊκού Απελευθερωτικού Στρατού (PLA), ενώ όπως φαίνεται θα τα διαδεχθεί η Δύναμη Στρατηγικής Υποστήριξης (Strategic Support Force – SSF) η ίδρυση της οποίας ήταν ένα αναμενόμενο βήμα στο πλαίσιο του εκσυγχρονισμού των ενόπλων δυνάμεων (Raud 2016, 24).

Βασική αποστολή του 3ου/PLA ήταν η συλλογή πληροφοριών μέσω συλλογής σημάτων (Signal Intelligence), τα οποία ήταν προϊόν υποκλοπής σημάτων είτε τηλεπικοινωνιών (Communication Intelligence - COMMINT) είτε ηλεκτρονικών (Electronic Intelligence – ELINT). Πιο πρόσφατα ο ρόλος του επικεντρώθηκε στις επιχειρήσεις εκμετάλλευσης και στην κατασκοπία στον κυβερνοχώρο (Raud 2016, 22). Η οργάνωση του υπόψη τμήματος περιλαμβάνει και άλλα υποτμήματα, τα οποία αναλαμβάνουν ακόμα πιο εξειδικευμένες αποστολές με κριτήριο ή το προς εξέταση αντικείμενο (χώρα) ή το είδος των επιχειρήσεων. Άξιο αναφοράς είναι το APT – 1[31], το οποίο εκτιμάται ως ένας από τους πιο παραγωγικούς και επικίνδυνους δρώντες της Κίνας στον κυβερνοχώρο.

Αντίστοιχα το 4ο/ PLA, είναι ο φορέας που ασχολείται με τα ηλεκτρονικά αντίμετρα και είναι υπεύθυνος για την διεξαγωγή ηλεκτρονικού πολέμου. Πιο πρόσφατα του ανατέθηκε επιπλέον η αποστολή εκτέλεσης επιθέσεων στον κυβερνοχώρο ως αποτέλεσμα υιοθέτησης ενός πιο επιθετικού δόγματος στο πλαίσιο του πληροφοριακού πολέμου από τις ένοπλες δυνάμεις της Κίνας. Η οργάνωση του, όπως και στο 3ο τμήμα, περιλαμβάνει άλλα υποτμήματα που αναλαμβάνουν πιο εξειδικευμένες αποστολές. Ιδιαίτερο ενδιαφέρον παρουσιάζουν αυτά που έχουν επικεντρωθεί στην αντιμετώπιση του αμερικανικού συστήματος C4ISR. Η συγκεκριμένη αποστολή έχει τις ρίζες της στην κινεζική ιστορία που

[31] Το APT-1 έχει επιδείξει την ικανότητά να παρεισφρύει στο δίκτυο του θύματος και να το επαναλαμβάνει συνεχώς επί σειρά ετών (η μεγαλύτερη αναγνωρισμένη περίοδος που υπερβαίνει τα τέσσερα χρόνια) προκειμένου να αποκτήσει πρόσβαση στην πνευματική του ιδιοκτησία, τα επιχειρηματικά σχέδια ή τεχνολογικά πρότυπα (Raud 2016, 23).

αναφέρει, ότι η κατανόηση της πληροφορίας είναι το κλειδί για την νίκη (Raud 2016, 24).

Ο διάδοχος των παραπάνω δύο φορέων όπως αναφέρθηκε είναι η Δύναμη Στρατηγικής Υποστήριξης (SSF). Ο συγκεκριμένος φορέας θα αποτελέσει τον κύριο εκφραστή της νέας στρατηγικής «τριάδας» της Κίνας, ο οποίος θα αναλάβει τον έλεγχο των πυρηνικών επιχειρήσεων και των επιχειρήσεων στο διάστημα και στον κυβερνοχώρο. Αυτοί οι τομείς επισημάνθηκαν στην Λευκή Βίβλο του 2015 ως οι τρείς «κρίσιμοι τομείς» για την άμυνα της Κίνας (Raud 2016, 25).

Ο Ναύαρχος Yin Zhuo[32] του Πολεμικού Ναυτικού, ο οποίος πιστεύεται ότι έχει άμεσες συνδέσεις με τη δημιουργία του SSF, δήλωσε τον Ιανουάριο του 2016 ότι το κύριο καθήκον του θα είναι η διασφάλιση των τοπικών πλεονεκτημάτων του στρατού στον τομέα της αεροδιαστημικής, του διαστήματος, του κυβερνοχώρου και των ηλεκτρομαγνητικών πεδίων μάχης. Ο Yin πιστεύει επίσης, ότι ο ίδιος φορέας θα αναλάβει ευθύνες για την υπεράσπιση της πολιτικής υποδομής, για την αύξηση της ασφάλειας των χρηματοπιστωτικών ιδρυμάτων της Κίνας καθώς και της καθημερινής ζωής των ανθρώπων γενικότερα.

Από τα ανωτέρω διαφαίνεται ότι ο SSF θα είναι υπεύθυνος για κάθε πτυχή του πολέμου των πληροφοριών, συμπεριλαμβανομένων των πληροφοριών, της τεχνικής αναγνώρισης, του κυβερνοπολέμου και του ηλεκτρονικού πολέμου, οι οποίες είναι κεντρικές στη στρατηγική σκέψη της Κίνας σχετικά με τον ασύμμετρο πόλεμο και την προληπτική επίθεση. Γενικά, αυτή η επιθυμητή κυριαρχία στο χώρο της πληροφορίας αποτελεί ουσιαστικό μέρος της στρατηγικής σκέψης της Κίνας, η οποία βλέπει τη παράλυση και το σαμποτάζ των επιχειρησιακών συστημάτων και τα συστημάτων διοίκησης του εχθρού ως το κλειδί για την επίτευξη κυριαρχίας σε όλους τους άλλους τομείς: αέρα, θάλασσα και γη (Raud 2016, 25).

Τέλος ιδιαίτερα σημαντική συμβολή στην στρατηγική της Κίνας στον κυβερνοχώρο κατέχουν οι ανεξάρτητες ομάδες από χάκερς. Στη Κίνα λειτουργούν έως και 250 ομάδες πατριωτών χάκερ που εκτελούν κατά παραγγελία του κόμματος, ένα ευρύ φάσμα λειτουργιών στον κυβερνοχώρο, από παρενόχληση και

[32] Ο Yin Zhuo γεννήθηκε το Σεπτέμβριο του 1945, είναι μέλος του Κομμουνιστικού Κόμματος της Κίνας και κομισάριος του Λαϊκού Απελευθερωτικού Στρατού στη Fuzhou της Κίνας. Ο Yin εκπαιδεύτηκε στο Πανεπιστήμιο του Παρισιού και στη Γαλλική Ναυτική Ακαδημία.

παρακολούθηση εσωτερικών διαφωνιών ενός κράτους έως την στοχευμένη παραποίηση ιστότοπων και στην εκτέλεση περίπλοκων επιχειρήσεων κατασκοπείας, επιθέσεων άρνησης υπηρεσιών στον κυβερνοχώρο (Patterson 2011, 123). Ενδεικτική της δυναμικής που προσδίδουν αυτές οι ομάδες στην δράση της Κίνας στον κυβερνοχώρο είναι η αποτύπωση της τεράστιας αριθμητικής διαφοράς ανθρώπινου δυναμικού «κυβερνοπολεμιστών» μεταξύ ΗΠΑ και Κίνας που ανέφερε ο Paller[33]. Σύμφωνα με τον Αμερικανό αναλυτή, στη Κίνα εκτιμάται ότι υπάρχουν 30.000 με 40.000 άνθρωποι ικανοί να διεξάγουν επιχειρήσεις κυβερνοπολέμου υψηλών απαιτήσεων, ενώ οι αντίστοιχοι άνθρωποι στις ΗΠΑ είναι περίπου 1000 (Γρίβας n.d.).

ΣΤΡΑΤΗΓΙΚΗ ΕΣΘΟΝΙΑΣ

Στο άκουσμα της Εσθονίας το μυαλό όλων συνειρμικά και όχι άδικα συνδέεται με την πρώτη εκδήλωση κυβερνοεπιθέσεων που έλαβε χώρα σε παγκόσμια κλίμακα εναντίον κράτους το 2007. Η New York Times αποκάλεσε αυτή την επίθεση ως τον πρώτο αληθινό πόλεμο στον κυβερνοχώρο, ο Εσθονός υπουργός εθνικής άμυνας τον προσδιόρισε ως μια κατάσταση εθνικής ασφάλειας, ενώ, ο επικεφαλής της επιτροπής για τον συντονισμό της κυβερνοάμυνας της Εσθονίας την απέδωσε τον χαρακτηρισμό της τρομοκρατικής ενέργειας (Lene Hansen & Helen Nissenbaum 2009, 1168).

Η Εσθονία παρά το μικρό της φυσικό μέγεθος ήταν ανέκαθεν πρωτοπόρος σε θέματα τεχνολογίας πληροφορικής στον κυβερνοχώρο. Μάλιστα πολύ πριν τα συμβάντα του 2007 είχε επιτύχει μια μακρόχρονη εθνική συνεργασία στον τομέα της ασφάλειας των τεχνολογιών της πληροφορικής και της επικοινωνίας μεταξύ εμπορικών, κυβερνητικών και ακαδημαϊκών φορέων. Ήδη από τα τέλη της δεκαετίας του 1990, εξέχοντα παραδείγματα στον τομέα αυτό περιελάμβαναν, τη συνεργασία μεταξύ των εμπορικών τραπεζών για την παροχή ασφαλών τραπεζικών υπηρεσιών μέσω διαδικτύου (Internet banking) από το 1996, τη δημιουργία υποδομής ηλεκτρονικής αναγνώρισης, που θα επέτρεπε την έναρξη ψηφιακής εξακρίβωσης της ταυτότητας και των ψηφιακών υπογραφών σε εθνικό επίπεδο, από το 1999 και την ανάπτυξη υποδομής υλικών και υπηρεσιών, για την

[33] Ο Alan Paller, είναι διευθυντής ερευνών στη σχολή κυβερνοασφάλειας του SANS Institute, ο οποίος θεωρεί ότι έχει ήδη ξεσπάσει κυβερνοπόλεμος μεταξύ των ΗΠΑ και της Κίνας, αλλά και άλλων χωρών.

έναρξη της ηλεκτρονικής ψηφοφορίας στις εθνικές εκλογές του 2005 (Kaska 2013, 7). Μάλιστα το αποτέλεσμα της συνεργασίας της κυβέρνησης και του ιδιωτικού φορέα ήταν αυτό που την κατέστησε πρωτοπόρο στην ψηφιακή νεωτερικότητα αποδίδοντας της τον τίτλο «e-stonia» (Lene Hansen & Helen Nissenbaum 2009, 1169).

Τα κυριότερα διδάγματα που προέκυψαν μετά από τις κυβερνοεπιθέσεις το 2007 για την Εσθονία ήταν (Lindau 2012, 61):

α. Η εμφανής έλλειψη ειδικών στον κυβερνοχώρο σε εκπαιδευτικό επίπεδο.

β. Ότι μέχρι τότε τα θέματα ασφάλειας του κυβερνοχώρου δεν ανήκαν στις προτεραιότητες της κυβέρνησης. Η εξέλιξη των επιθέσεων κατέδειξε, ότι δίχως τη συμβολή του ιδιωτικού τομέα, που είχε ανάλογη εμπειρία, οι επιθέσεις θα είχαν διαρκέσει περισσότερο με καταστροφικότερα αποτελέσματα για τη χώρα καθώς ο δημόσιος φορέας παρουσιάστηκε παθητικός και με έλλειψη σχεδίου δράσης.

γ. Ότι η συνεργασία μεταξύ ιδιωτικού και δημόσιου τομέα αποδείχτηκε εξαιρετικά επωφελής και καθοριστικής σημασίας για την αντιμετώπιση των κυβερνοεπιθέσεων.

δ. Την ανάγκη για διασυνοριακή συνεργασία που αφορά την διερεύνηση εγκλημάτων και επιθέσεων, καθώς και τη δημιουργία νομικού πλαισίου για θέματα σχετικά με τον κυβερνοχώρο.

Έκτοτε η Εσθονία έχοντας αξιολογήσει τα λάθη της έχει διορθώσει τα κακώς κείμενα αποδεικνύοντας έμπρακτα τη ρήση, *«επιτρέπεται να πέσεις, επιβάλλεται να σηκωθείς»*, αναπτύσσοντας μια εξαιρετική στρατηγική για την ασφάλεια στον κυβερνοχώρο την οποία αναθεωρεί κάθε τριετία. Μάλιστα η στρατηγική της το 2008 ήταν τέτοια που οι Αμερικάνοι την υιοθέτησαν πλήρως[34]. Η πιο πρόσφατη έκδοση αφορά το διάστημα 2014 – 2017 και σύμφωνα με το αναγραφόμενο σ' αυτή χρονοδιάγραμμα, το περασμένο Μάιο παρουσιάστηκε από τον αρμόδιο υπουργό ο απολογισμός της.

[34] Ο Jan Priisalu (ειδικός σε θέματα ασφάλειας στον κυβερνοχώρο και συνιδρυτής της Defence League Cyber Unit) ανέφερε σχετικά ότι το 2008 η στρατηγική της Εσθονίας για την ασφάλεια στον κυβερνοχώρο ήταν νέα για τον κόσμο. Η πιο ισχυρή δύναμη στον κόσμο (ΗΠΑ) την αντέγραψε και αν σε αντιγράφει η πιο ισχυρή χώρα τότε σημαίνει ότι είσαι στην κορυφή του κόσμου.

Το όραμα της κυβέρνησης, το οποίο αποτελεί οδηγό για την σχεδίαση και εφαρμογή της στρατηγικής της είναι « η Εσθονία να είναι σε θέση να εξασφαλίσει την εθνική ασφάλεια και να υποστηρίξει τη λειτουργία μιας ανοικτής, χωρίς αποκλεισμούς και ασφαλούς κοινωνίας». Ο τετραετής στόχος της στρατηγικής για την ασφάλεια στον κυβερνοχώρο είναι να αυξήσει τις δυνατότητες ασφάλειας στον κυβερνοχώρο και να ευαισθητοποιήσει τον πληθυσμό για τις απειλές που προέρχονται απ' αυτόν, διασφαλίζοντας έτσι τη συνεχή εμπιστοσύνη στον κυβερνοχώρο (Ministry of Economic Affairs and Communication 2014, 7-8).

Σύμφωνα με τη στρατηγική για την ασφάλεια του κυβερνοχώρου της Εσθονίας, οι κύριες προκλήσεις προκύπτουν από την εκτεταμένη και αυξανόμενη εξάρτηση από την πληροφοριακή υποδομή και τις ηλεκτρονικές υπηρεσίες του κρατικού μηχανισμού, της οικονομία της και του πληθυσμό της. Ως εκ τούτου, τα βασικά πεδία στα οποία επικεντρώνεται η στρατηγική για την ασφάλεια στον κυβερνοχώρο είναι η διασφάλιση ζωτικών υπηρεσιών, η αποτελεσματικότερη καταπολέμηση του εγκλήματος στον κυβερνοχώρο και η ανάπτυξη των εθνικών αμυντικών ικανοτήτων. Πρόσθετες υποστηρικτικές δραστηριότητες που θα συμβάλλουν στα ανωτέρω περιλαμβάνουν: τη διαμόρφωση του νομικού πλαισίου, την προώθηση της διεθνούς συνεργασίας και επικοινωνίας, την ευαισθητοποίηση και τη διασφάλιση της εξειδικευμένης εκπαίδευσης, καθώς και την ανάπτυξη τεχνικών λύσεων (Ministry of Economic Affairs and Communication 2014, 6).

Για να εξασφαλιστεί η δυνατότητα παροχής εθνικής άμυνας στον κυβερνοχώρο, οι πολιτικοί και στρατιωτικοί πόροι του κράτους πρέπει να μπορούν να ενταχθούν σε ένα λειτουργικό σύνολο υπό την καθοδήγηση των πολιτικών αρχών και να είναι διαλειτουργικοί με τις δυνατότητες των διεθνών εταίρων. Ταυτόχρονα σε διεθνές επίπεδο, πρέπει να διασφαλισθεί η διατήρηση ενός ελεύθερου και ασφαλούς κυβερνοχώρου, καθώς και ο κεντρικός ρόλος της Εσθονίας στην καθοδήγηση και την ανάπτυξη της διεθνούς πολιτικής για την ασφάλεια στον κυβερνοχώρο σε διεθνείς οργανισμούς, καθώς και σε κοινότητες με όμοια νοοτροπία (Ministry of Economic Affairs and Communication 2014, 6) .

Το σχέδιο δράσης της στρατηγικής έχει δομηθεί κατά τέτοιο τρόπο, που να καθιστά την Εσθονία έτοιμη να δεχθεί και να αντιμετωπίσει κυβερνοεπιθέσεις με τρόπο αποτελεσματικό που να μην προκαλεί παράλυση των καθημερινών ενεργειών της κοινωνίας (Lindau 2012, 49).

Ο πρώτος στόχος της στρατηγικής είναι η εξασφάλιση της προστασίας των πληροφοριακών συστημάτων στα οποία βασίζονται σημαντικές υπηρεσίες. Αυτό θα επιτευχθεί με την πρόβλεψη ύπαρξης εναλλακτικών λύσεων για σημαντικές υπηρεσίες, τη δημιουργία σχέσεων αλληλεξάρτησης μεταξύ σημαντικών υπηρεσιών και την θωράκιση της υποδομής των υπηρεσιών τεχνολογίας πληροφοριών και επικοινωνιών. Ιδιαίτερη συμβολή επίσης έχει η ανάπτυξη δυνατότητας διαχείρισης απειλών στον κυβερνοχώρο, τόσο από τον δημόσιο όσο και από τον ιδιωτικό τομέα, η εισαγωγή ενός εθνικού συστήματος παρακολούθησης για την ασφάλεια στον κυβερνοχώρο, η εξασφάλιση της ψηφιακής συνέχειας του κράτους και η προώθηση της διεθνούς συνεργασίας για την προστασία της υποδομής των κρίσιμων πληροφοριών (Ministry of Economic Affairs and Communication 2014, 8-9).

Ο δεύτερος στόχος αφορά την ενίσχυση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο μέσω της ανάπτυξης των κρατικών δυνατοτήτων ανίχνευσης εγκλημάτων, την ευαισθητοποίηση του κοινού σχετικά με τους κινδύνους και την προώθηση της διεθνούς συνεργασίας κατά του εγκλήματος στον κυβερνοχώρο. Ο τρίτος στόχος αναφέρεται στην ανάπτυξη των δυνατοτήτων εθνικής άμυνας στο κυβερνοχώρο. Η επίτευξη του προβλέπει τον συγχρονισμό της στρατιωτικής σχεδίασης για την αντιμετώπιση αστικών περιστατικών επείγουσας ανάγκης, την ανάπτυξη συλλογικής άμυνας και διεθνούς συνεργασίας, την ανάπτυξη δυνατοτήτων στρατιωτικής άμυνας και την καταβολή προσπάθειας, ώστε να καταστεί σαφής ο ρόλος την ασφάλειας στον κυβερνοχώρο για την εθνική άμυνα της χώρας (Ministry of Economic Affairs and Communication 2014, 9-10).

Μέσω του τέταρτου στόχου η Εσθονία στοχεύει να αναπτύξει ικανότητες διαχείρισης των εξελισσόμενων απειλών στον κυβερνοχώρο. Προκειμένου να καταστεί αυτό δυνατό, θα επιδιώξει την δημιουργία της επόμενης γενιάς επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο, τη σύναψη συμβάσεων με εξωτερικούς συνεργάτες για παροχή λύσεων σε θέματα κυβερνοασφάλειας, την υποστήριξη ανάπτυξης εγχώριων επιχειρήσεων για το ίδιο θέμα και την αποτροπή κινδύνων μέσω καινοτόμων λύσεων (Ministry of Economic Affairs and Communication 2014, 11-12).

Επιδίωξη μέσω του πέμπτου και τελευταίου στόχου είναι η ανάπτυξη της δυνατότητας εκτέλεσης δραστηριοτήτων μεταξύ διαφόρων τομέων. Αυτό επιβάλλει

την προσαρμογή του νομικού πλαισίου προκειμένου να συμπεριλάβει στις διατάξεις του την αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο. Επιπλέον επιτάσσει την ανάπτυξη της εξωτερικής πολιτικής που σημαίνει επένδυση στις συνεργασίες με τα γειτονικά κράτη, τους διεθνείς οργανισμούς αλλά και την Ευρωπαϊκή Ένωση. Επιδίωξη είναι να δοθεί έμφαση στην ανάπτυξη κοινής αντίληψης για τους κινδύνους που προέρχονται από τον κυβερνοχώρο, στην από κοινού εφαρμογή διεθνών νομικών κανόνων και μέτρων οικοδόμησης εμπιστοσύνης, στην προστασία των θεμελιωδών δικαιωμάτων και ατομικών ελευθεριών, καθώς και στη διακυβέρνηση του Διαδικτύου (Ministry of Economic Affairs and Communication 2014, 12).

Αρμόδιος φορέας για την υλοποίηση της στρατηγικής είναι το υπουργείο οικονομικών σχέσεων και επικοινωνίας. Αρωγός στην προσπάθεια του και άξιο αναφοράς λόγω της καινοτομίας που εισάγει, είναι το Estonian Defence League's Cyber Unit (EDL CU), ένας οργανισμός που είναι αποτέλεσμα συνεργασίας του δημόσιου και ιδιωτικού τομέα. Για την στελέχωση του ο συγκεκριμένος φορέας στηρίζεται στην εθελοντική προσφορά πολιτών, με εξειδικευμένες γνώσεις σε πληροφοριακά συστήματα και συστήματα επικοινωνιών. Βασικοί αντικειμενικοί σκοποί του είναι (Lene Hansen & Helen Nissenbaum 2009, 11):

α. Η ανάπτυξη δικτύου συνεργασίας που θα συνδυάζει την εμπειρογνωμοσύνη των δύο φορέων (δημόσιου – ιδιωτικού).

β. Η βελτίωση της ασφάλειας των κρίσιμων υποδομών μέσω της τακτικής ανταλλαγής πληροφοριών και της διάδοσης βέλτιστων πρακτικών ενίσχυσης της ετοιμότητας τους για λειτουργία κατά τη διάρκεια μιας κατάστασης κρίσης.

γ. Η προώθηση της ενημέρωσης και της κατάρτισης των μελών του μέσω συνεχούς εκπαίδευσης τόσο σε εγχώρια προγράμματα όσο και σε διεθνή.

Στον τομέα της εκπαίδευσης η Εσθονία δίνει ιδιαίτερη βαρύτητα επιδιώκοντας να καλύπτει τις εκπαιδευτικές ανάγκες όλου του φάσματος των ηλικιών. Την αρχή κάνει το Information Technology Foundation for Education (HITSA), το οποίο προσφέρει εκπαίδευση σε παιδιά προσχολικής και σχολικής ηλικίας, συμπεριλαμβανομένου των γονιών και των εκπαιδευτικών, για την ασφαλή χρήση και τους κινδύνους του διαδικτύου. Επιπλέον το πανεπιστήμιο τεχνολογίας του Ταλίν σε συνεργασία με το πανεπιστήμιο του Tartu έχουν εισαγάγει ένα

διεθνές πρόγραμμα μεταπτυχιακών σπουδών για την ασφάλεια του κυβερνοχώρου, ενώ σε συνεργασία με το κέντρο 2CENTRE[35], εισήγαγε ένα πρόγραμμα μεταπτυχιακών σπουδών στην ψηφιακή εγκληματολογία.

Η Εσθονία μετά τις κυβερνοεπιθέσεις του 2007, ανέλαβε πρωτοβουλίες σε διεθνές επίπεδο, προκειμένου να αναχθεί η ασφάλεια στον κυβερνοχώρο στο επίκεντρο του πολιτικού ενδιαφέροντος. Παράλληλα διαδραμάτισε ενεργό ρόλο στη δημιουργία του NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), του οποίου η έδρα βρίσκεται στο Ταλίν. Το κέντρο αξιοποιείται για την ανταλλαγή πληροφοριών μεταξύ των ειδικών και για την ενημέρωση - εκπαίδευση των αξιωματικών του ΝΑΤΟ επί θεμάτων Κυβερνοπολέμου (Μαυρόπουλος 2014, 24). Μέσω αυτού η ασφάλεια στον κυβερνοχώρο έγινε μέρος της πολιτικής του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης (Ministry of Economic Affairs and Communication 2014, 4).

[35] Το κέντρο αριστείας της 2CENTRE για την εγκληματικότητα στον κυβερνοχώρο της Εσθονίας αποτελεί κομμάτι του δικτύου κέντρων αριστείας 2CENTRE της Ευρωπαϊκής Ένωσης, όπου επαγγελματίες του χώρου εκπαιδεύονται στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

ΚΕΦΑΛΑΙΟ «Ε»

ΣΤΡΑΤΗΓΙΚΗ ΕΛΛΑΔΑΣ

ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΛΛΑΔΑΣ ΣΗΜΕΡΑ, ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ.

Το πλαίσιο της Ευρωπαϊκής Ένωσης

Η Ελλάδα ως χώρα μέλος της Ευρωπαϊκής Ένωσης (ΕΕ), έχει την υποχρέωση οι πολιτικές της να συμβαδίζουν με τις αντίστοιχες του πολυεθνικού οργανισμού. Η ασφάλεια στον κυβερνοχώρο είναι ένα θέμα που έχει απασχολήσει έντονα την ΕΕ. Ήδη από το 2004 ίδρυσε τον Ευρωπαϊκό Οργανισμό ENISA[36] για την ασφάλεια των πληροφοριών και των δικτύων, στο Ηράκλειο της Κρήτης, το οποίο είναι κέντρο εμπειρογνωμοσύνης για την ΕΕ, τα κράτη μέλη, τον ιδιωτικό τομέα και τους πολίτες της (Σχης (ΠΖ) Πετούμενος Η. 2016).

Από το 2013 η ΕΕ είχε καταρτίσει την στρατηγική της για την κυβερνοασφάλεια, στην οποία ως όραμα ανέφερε την πρόθεση για τη δημιουργία των προϋποθέσεων ώστε, ο κυβερνοχώρος της να καταστεί ο ασφαλέστερος στον κόσμο βασιζόμενος ισχυρά στην προστασία και την προώθηση των ανθρωπίνων δικαιωμάτων. Οι πέντε αρχικές στρατηγικές της προτεραιότητες αφορούσαν την (European Commission 2013, 4-5):

α. Την επίτευξη ανθεκτικότητας στον κυβερνοχώρο.

β. Τη δραστική μείωση του εγκλήματος στον κυβερνοχώρο.

γ. Την ανάπτυξη πολιτικής και ικανοτήτων στον κυβερνοχώρο σύμφωνα με την Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ).

[36] Ο οργανισμός ENISA λειτουργεί με βάση τον ευρωπαϊκό κανονισμό 460/2004 ο οποίος στη συνέχεια αντικαταστάθηκε από τον 526/2013. Οι δράσεις της μπορούν να διακριθούν σε τρείς τομείς:

α. Παροχή συμβουλών και συστάσεων στην Ευρωπαϊκή επιτροπή και στα κράτη – μέλη για νομοθετικές πράξεις και μέτρα, καθώς και σύνταξη μελετών για ζητήματα ασφαλείας στον κυβερνοχώρο της Ένωσης.

β. Δραστηριότητες που υποστηρίζουν τη χάραξη και την εφαρμογή της πολιτικής ασφάλειας στον κυβερνοχώρο.

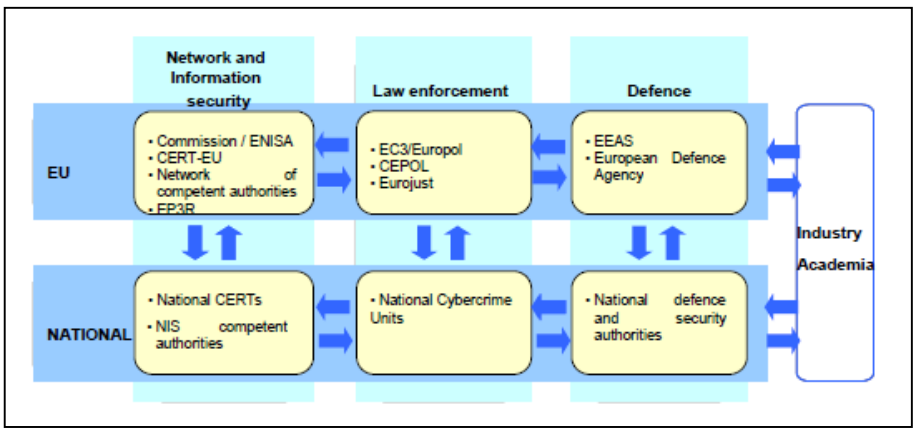
γ. Στενή επιχειρησιακή συνεργασία με τους αρμόδιους φορείς των κρατών – μελών και των άλλων διεθνών οργανισμών [από παρουσίαση της Έδρας Διακλαδικού Αμυντικού Προσανατολισμού (ΕΔΑΠ) της Ανωτάτης Διακλαδικής Σχολής Πολέμου (ΑΔΙΣΠΟ)] .

δ. Την ανάπτυξη βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο.

ε. Την καθιέρωση συνεκτικής διεθνούς πολιτικής στον κυβερνοχώρο για την Ευρωπαϊκή Ένωση και προώθηση των βασικών αξιών της.

Η ευρωπαϊκή ένωση λαμβάνοντας υπόψη ότι στην εφαρμογή της στρατηγικής ενδέχεται να εμπλέκονται διαφορετικά νομικά πλαίσια και δικαιοδοσίες, θεώρησε αυτονόητο να αποσαφηνίσει τους ρόλους και τις ευθύνες των εμπλεκόμενων φορέων. Παράλληλα κατέληξε στο συμπέρασμα, ότι η κεντρική ευρωπαϊκή εποπτεία δεν ήταν η απάντηση στο πρόβλημα (European Commission 2013, 17).

Σύμφωνα με την στρατηγική της, οι εθνικές κυβερνήσεις είναι οι πλέον κατάλληλες για την οργάνωση της πρόληψης και της αντιμετώπισης των περιστατικών ή επιθέσεων στον κυβερνοχώρο μέσω των καθιερωμένων πολιτικών και νομικών πλαισίων. Ταυτόχρονα η ΕΕ αναγνωρίζει, ότι οι απειλές στον κυβερνοχώρο δεν περιορίζονται από σύνορα και κατά συνέπεια μια αποτελεσματική εθνική αντίδραση, ενδεχομένως να απαιτεί συχνά και τη δική της συμμετοχή. Προκειμένου λοιπόν να επιτευχθεί η ασφάλεια στον κυβερνοχώρο, η ΕΕ θεωρεί ότι οι δραστηριότητες πρέπει να στηρίζονται στους πυλώνες, ασφάλεια δικτύων και πληροφοριών (Network and Information Security – NIS), επιβολή του νόμου και ετοιμότητα κυβερνοάμυνας, οι οποίοι λειτουργούν και αλληλεπιδρούν μεταξύ τους τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο. Ο μηχανισμός αντιμετώπισης των κυβερνοαπειλών στο πλαίσιο της ΕΕ αποτυπώνεται στη εικόνα που ακολουθεί (European Commission 2013, 17).



Εικόνα 1: Μηχανισμός Αντιμετώπισης Επιθέσεων στον Κυβερνοχώρο στην ΕΕ

Για την ΕΕ εξαιρετικά σημαντική ήταν και παραμένει η πρόκληση της ευαισθητοποίησης του κοινού, καθώς θεωρεί ότι ο μέσος κοινός χρήστης έχει σημαντικό ρόλο στην ασφάλεια των δικτύων και των πληροφοριακών συστημάτων (European Commission 2013, 8). Ως εκ τούτου είναι επιτακτική ανάγκη, ο χρήστης να γνωρίζει τους κινδύνους που αντιμετωπίζει στο διαδίκτυο και να προτρέπεται να λαμβάνει τα απαιτούμενα μέτρα προφύλαξης. Κύριοι παράγοντες στην εκστρατεία ενημέρωσης της ΕΕ είναι ο οργανισμός ENISA και η Ευρωπαϊκή Επιτροπή. Ορισμένες από τις πρωτοβουλίες τους περιλαμβάνουν την πρόταση ενός οδικού χάρτη απόκτησης του Network and Information Security Driving Licence[37], την οργάνωση «πρωταθλήματος» κυβερνοασφάλειας μεταξύ ανωτάτων εκπαιδευτικών ιδρυμάτων, την ετήσια οργάνωση της ενημερωτικής προσπάθειας του μήνα ασφάλειας στον κυβερνοχώρο κ.α.

Ιδιαίτερα σημαντική επιπλέον, ήταν η πρωτοβουλία της ΕΕ να καταστεί αυτόνομη σε ότι αφορά την παραγωγή προϊόντων κυβερνοασφάλειας. Αντικειμενικός σκοπός ήταν να τεθούν οι προϋποθέσεις δημιουργίας μιας «ενιαίας ψηφιακής αγοράς» στο πλαίσιο της ΕΕ, που θα περιλαμβάνει στοιχεία υλικού και λογισμικού που χρησιμοποιούνται σε κρίσιμες υποδομές. (European Commission 2013, 12).Πρόσφατα μάλιστα η ΕΕ αποφάσισε την επένδυση ποσού 9,2 δισ. ευρώ στο νέο πρόγραμμα «Ψηφιακή Ευρώπη», προκειμένου να αυξηθεί η διεθνής ανταγωνιστικότητα της ΕΕ, καθώς και να αναπτυχθούν – ενισχυθούν οι στρατηγικές ψηφιακές ικανότητες της (Εθνικό Κέντρο Τεκμηρίωσης 2018).

Το 2016 η ΕΕ επικαιροποίησε την στρατηγική της με την οδηγία 1148/2016. Οι σημαντικές τροποποιήσεις αφορούν την υποχρέωση των κρατών να ορίσουν τις επιχειρήσεις που παρέχουν βασικές ή ζωτικής σημασίας υπηρεσίες, όπως ενέργεια, μεταφορές, υγεία κ.α. Επιπλέον για τις συγκεκριμένες επιχειρήσεις, οι οποίες ορίζονται ως φορείς εκμετάλλευσης βασικών υπηρεσιών, καθορίζεται η υποχρέωση κοινοποίησης άνευ καθυστέρησης στην αρμόδια εθνική αρχή συμβάντων με σοβαρό αντίκτυπο στη λειτουργία των ανωτέρω υπηρεσιών. Κριτήρια τα οποία χαρακτηρίζουν τη σοβαρότητα των συμβάντων είναι ο αριθμός των χρηστών που επηρεάζει το συμβάν, η διάρκεια του και το γεωγραφικό εύρος

[37] Το Network and Information Security Driving Licence είναι ένα εθελοντικό πρόγραμμα πιστοποίησης ενισχυμένων δυνατοτήτων και ικανοτήτων στον χώρο των επαγγελματιών της τεχνολογίας των πληροφοριών (π.χ Διαχειριστές δικτυακών τόπων).

της περιοχής που επηρεάζεται απ' αυτό. Αντίστοιχα μέτρα προβλέπονται και για τους παρόχους ψηφιακών υπηρεσιών[38] (Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο 2016, 11-12).

Στο πλαίσιο της οδηγίας προβλέπεται επίσης η ίδρυση ομάδων αντιμετώπισης έκτακτων αναγκών στα δίκτυα Η/Υ (Computer Incident Response Teams) και η σύσταση - λειτουργία ομάδος συνεργασίας, (Cooperation Group) αποτελούμενη από εκπροσώπους των κρατών μελών της ευρωπαϊκής επιτροπής και του οργανισμού ENISA, για την υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας (Βαγενά 2017).

Η στρατηγική κυβερνοασφάλειας της Ελλάδας σήμερα

Η Ελλάδα από το Μάρτιο του 2018, προσαρμοζόμενη με την οδηγία 1148/18 της ΕΕ, προέβη στην αναθεώρηση της εθνικής στρατηγικής κυβερνοασφαλείας με την υπουργική απόφαση 3218/18. Η πολιτεία με τη συγκεκριμένη απόφαση, στοχεύει στη βελτίωση της διαδικτυακής ασφάλειας, εξασφαλίζοντας την ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των κρίσιμων υποδομών και την εμπιστευτικότητα της διακινούμενης ψηφιακής πληροφορίας, διασφαλίζοντας παράλληλα τις αρχές της ανοιχτής κοινωνίας, τις συνταγματικές ελευθερίες και τα ατομικά δικαιώματα (3218/2018 2018, 3).

Οι εμπλεκόμενοι φορείς στην εθνική στρατηγική κυβερνοασφαλείας κατανέμονται σε δύο επίπεδα, στο στρατηγικό και το επιχειρησιακό. Στο πρώτο επίπεδο ανήκει η Εθνική Αρχή Κυβερνοασφάλειας, η οποία σύμφωνα με το Προεδρικό Διάταγμα 82/2017 (Α΄ 117) συστάθηκε και λειτουργεί στην Γενική Γραμματεία Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης. Κύρια αποστολή της είναι να καλύψει το οργανωτικό και συντονιστικό κενό ανάμεσα στους φορείς που δραστηριοποιούνται στην Ελλάδα, στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στον δημόσιο όσο και στον ιδιωτικό. Επιπλέον ορίζεται υπεύθυνη, να αποτιμά, να αναθεωρεί και να επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας όποτε κρίνεται αναγκαίο ή το αργότερο κάθε τριετία. Η Εθνική Αρχή Κυβερνοασφάλειας, ασκεί τις αρμοδιότητές της με τη συνδρομή ενός Εθνικού Συμβουλευτικού Οργάνου /

[38] Στους παρόχους ψηφιακών υπηρεσιών περιλαμβάνονται ηλεκτρονικά καταστήματα, οι μηχανές αναζήτησης και οι υπηρεσίες νεφουπολογιστικής (cloud computing) (Βαγενά 2017).

Φόρουμ, στο οποίο συμμετέχουν εμπλεκόμενοι φορείς δημόσιου και ιδιωτικού τομέα σε στενή συνεργασία με το εθνικό Computer Emergency Response Team (CERT) (3218/2018 2018, 2 & 4).

Η εθνική υπηρεσία πληροφοριών (ΕΥΠ) είναι ο φορέας που έχει αναλάβει τον ρόλο της εθνικής αρχής αντιμετώπισης ηλεκτρονικών επιθέσεων (εθνικό CERT) και της τεχνικής φύσεως αρχή ασφαλείας πληροφοριών (INFOSEC) (Ν. 3649/2008-ΦΕΚ39/Α 2008). Ως εθνικό CERT έχει τις παρακάτω αρμοδιότητες[39]:

α. Αντιμετώπιση ηλεκτρονικών επιθέσεων, κυρίως κατά του δημοσίου τομέα και των κρίσιμων υποδομών.

β. Ανάλυση και αξιολόγηση περιστατικών ασφαλείας.

γ. Ανάπτυξη στρατηγικής αντιμετώπισης απειλών, καθώς και συλλογή, επεξεργασία και διακίνηση των σχετικών πληροφοριών.

δ. Συνεργασία με άλλα Εθνικά και μη CERT, με τις αντίστοιχες υπηρεσίες άλλων χωρών και διεθνών οργανισμών, καθώς και τους φορείς του δημοσίου και ιδιωτικού τομέα.

ε. Διενέργεια ελέγχων ασφαλείας σε πληροφοριακά συστήματα του δημόσιου τομέα και έκδοση γενικών οδηγιών για την διασφάλισή τους.

Ως Τεχνικής Φύσεως Αρχή Ασφαλείας, σύμφωνα με το ΠΔ 325/2003 (ΦΕΚ 273 Α'), προβαίνει στην αξιολόγηση και πιστοποίηση των συσκευών και συστημάτων ασφαλείας επικοινωνιών πληροφορικής (Ν. 3649/2008-ΦΕΚ39/Α 2008). Επιπρόσθετα, είναι η υπεύθυνη αρχή για την αξιολόγηση και πιστοποίηση των κρυπτογραφικών συστημάτων και την παραγωγή Εθνικών Κλειδών[40].

Στο επιχειρησιακό επίπεδο ανήκουν μεταξύ άλλων, οι ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRT), γνωστές επίσης ως «ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams — CERT) του δημοσίου και του ιδιωτικού τομέα, επιφορτισμένες με την αντιμετώπιση των κυβερνοπεριστατικών (κυβερνοάμυνα) στο πλαίσιο των αρμοδιοτήτων τους (3218/2018 2018, 4).

[39] Από παρουσίαση της Έδρας Διακλαδικού Αμυντικού Προσανατολισμού (ΕΔΑΠ) της Ανωτάτης Διακλαδικής Σχολής Πολέμου (ΑΔΙΣΠΟ)
[40] Όπως παραπάνω.

Βασικές αρχές της Εθνικής Στρατηγικής Κυβερνοασφάλειας αποτελούν (3218/2018 2018, 3). :

α. Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου, ο οποίος θα ρυθμίζεται στη βάση εθνικών, ευρωπαϊκών και διεθνών κανόνων, προτύπων και ορθών πρακτικών και στον οποίο οι πολίτες και οι φορείς του δημόσιου και ιδιωτικού τομέα θα δραστηριοποιούνται και θα αλληλεπιδρούν με ασφάλεια, σύμφωνα με τις αξίες που διέπουν ένα κράτος δικαίου, όπως ενδεικτικά της ελευθερίας, της δικαιοσύνης και της διαφάνειας.

β. Η συνεχής βελτίωση των δυνατοτήτων της χώρας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και τη διασφάλιση της επιχειρησιακής συνέχειας.

γ. Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.

δ. Η ανάπτυξη ισχυρής κουλτούρας ασφάλειας των πολιτών του δημόσιου και ιδιωτικού τομέα, αξιοποιώντας τις σχετικές δυνατότητες της ακαδημαϊκής κοινότητας και εν γένει των φορέων του δημόσιου και ιδιωτικού τομέα.

Επιδίωξη της εθνικής στρατηγικής ασφαλείας αρχικά είναι ο ορισμός των φορέων που θα συμμετέχουν στην εφαρμογή της καθώς και των κρίσιμων υποδομών της χώρας. Ακολουθεί η αποτίμηση της επικινδυνότητας σε εθνικό επίπεδο, που θα βασίζεται στην αναγνώριση, ανάλυση και αποτίμηση των επιπτώσεων των κινδύνων, ώστε να καθοριστούν οι επιβαλλόμενες υποχρεώσεις παροχής προστασίας των κρίσιμων υποδομών. Απόρροια της αποτίμησης επικινδυνότητας είναι ο καθορισμός των βασικών ή ελάχιστων απαιτήσεων ασφαλείας, που οι φορείς οφείλουν να εφαρμόζουν, ώστε να επιτύχουν ένα θεμελιώδες και κοινό επίπεδο ασφαλείας.

Η στρατηγική καθορίζει επίσης την υποχρέωση κατάρτισης σχεδίου έκτακτης ανάγκης που σκοπό θα έχει αφενός, τον καθορισμό των κριτηρίων, ώστε να χαρακτηριστεί ένα περιστατικό κρίσιμο αφετέρου, τον προσδιορισμό των διαδικασιών, των δράσεων και των αρμόδιων φορέων για την αντιμετώπιση του. Ιδιαίτερο ρόλο για την αντιμετώπιση των περιστατικών ασφαλείας φέρουν οι

ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT).

Τέλος, στόχο της στρατηγικής αποτελεί η καταγραφή και βελτίωση του υφιστάμενου θεσμικού πλαισίου και των δομών που λειτουργούν για την εξυπηρέτηση των στόχων της Εθνικής Στρατηγικής και αφορούν (3218/2018 2018, 5-6) :

α. Νομοθετικές ρυθμίσεις, ρόλους και αρμοδιότητες φορέων που σχετίζονται με την Κυβερνοασφάλεια (πχ επεξεργασία προσωπικών δεδομένων, ηλεκτρονικές επικοινωνίες, άρση του απορρήτου των επικοινωνιών, ακεραιότητα και διαθεσιμότητα των δικτύων κλπ).

β. Κανονιστικές πράξεις που εξειδικεύονται ανά τομέα (πχ τραπεζικό) και η ως τώρα επίπτωσή τους στη βελτίωση της Κυβερνοασφάλειας (πχ κανονισμοί και ελεγκτικός ρόλος της Τράπεζας της Ελλάδος).

γ. Δομές, φορείς και υπηρεσίες, του ιδιωτικού ή δημόσιου τομέα, που έχουν επιχειρησιακό ρόλο στη διασφάλιση της Κυβερνοασφάλειας (πχ ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRTs).

δ. Υφιστάμενα σχέδια αντιμετώπισης έκτακτων αναγκών (όπως Εγνατία, Ξενοκράτης[41] κλπ).

ε. Ευρωπαϊκές και άλλες διεθνείς οδηγίες και κανονισμούς σχετικά με την ασφάλεια των δικτύων και πληροφοριών, καθώς και των κρίσιμων υποδομών.

Η αξιολόγηση των προβλέψεων της στρατηγικής και της ετοιμότητας των εμπλεκόμενων φορέων επιτυγχάνεται μέσω των εθνικών και διεθνών ασκήσεων ετοιμότητας, όπου δίνετε η δυνατότητα εντοπισμού και ευπάθειας των συστημάτων τεχνολογίας, πληροφορικής και επικοινωνίας. Τέλος ζωτικής σημασίας παράγοντας στην επιτυχή εφαρμογή της στρατηγικής, αποτελεί η ενεργή συμμετοχή της κοινωνίας, η οποία θα επιτευχθεί μέσω της ευαισθητοποίησης, σχετικά με τις απειλές και τις επιπτώσεις που σχετίζονται με την κυβερνοασφάλεια.

[41] Το σχέδιο Ξενοκράτης αφορά την αποτελεσματική αντιμετώπιση καταστροφικών φαινομένων για την προστασία της ζωής, της υγείας και της περιουσίας των πολιτών, καθώς και την προστασία του φυσικού περιβάλλοντος και συντάχθηκε από την Γενική Γραμματεία Πολιτικής Προστασίας (ΓΓΠΠ) (Γενική Γραμματεία Πολιτικής Προστασίας n.d.)

Η ΚΥΒΕΡΝΟΑΜΥΝΑ ΤΗΣ ΕΛΛΑΔΑΣ ΜΕΣΩ ΤΩΝ ΕΝΟΠΛΩΝ ΔΥΝΑΜΕΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΝΑΤΟ

Το πλαίσιο του ΝΑΤΟ

Το ΝΑΤΟ, μετά τις κυβερνοεπιθέσεις στην Εσθονία το 2007, μερίμνησε για την ενίσχυση των δυνατοτήτων του στον τομέα της κυβερνοάμυνας. Το 2014, στη σύνοδο της Ουαλίας αναθεωρήθηκε η πολιτική κυβερνοάμυνας της Συμμαχίας και αναβαθμίστηκε ο ρόλος και η σημασίας της, με χαρακτηριστικό δείγμα την πρόβλεψη δυνητικής εφαρμογής του άρθρου 5, στην περίπτωση που κάποιο μέλος δεχθεί κυβερνοεπίθεση[42]. Ωστόσο η μεγαλύτερη αλλαγή στην ιστορία του ΝΑΤΟ σε ότι αφορά την κυβερνοάμυνα, έλαβε χώρα στη σύνοδο της Βαρσοβίας το 2016, όταν η συμμαχία επίσημα ανακήρυξε τον κυβερνοχώρο ως επιχειρησιακή διάσταση (Kovacs n.d., 22).

Το στρατηγικό δόγμα του ΝΑΤΟ από το 2010, δεσμεύει την συμμαχία να αναπτύξει περαιτέρω την δυνατότητα, αποτροπής, ανίχνευσης, άμυνας και ανάκτησης από κυβερνοεπιθέσεις, χρησιμοποιώντας την διαδικασία σχεδίασης, ώστε να ενισχύσει και να συντονίσει τις εθνικές δυνατότητες κυβερνοάμυνας, θέτοντας όλα τα μέλη υπό κεντρική προστασία στον κυβερνοχώρο (Schmitt 2013). Καθορίζει επίσης, ότι τα κράτη μέλη της συμμαχίας πρέπει να έχουν ετοιμότητα για επιθέσεις στον κυβερνοχώρο προερχόμενες ,είτε από κρατικούς, είτε από μη κρατικούς δρώντες (Szentgali n.d., 84).

Στο πλαίσιο αυτό η πολιτική του ΝΑΤΟ για τον κυβερνοχώρο καθορίζει, την κυβερνοάμυνα ως ένα από τα κύρια καθήκοντα της συλλογικής άμυνας της συμμαχίας. Πρώτη προτεραιότητα της, αποτελεί η προστασία των επικοινωνιακών συστημάτων της Συμμαχίας (North Atlantic Treaty Organization 2018). Η ανωτέρω πολιτική συνίσταται από τις παρακάτω αρχές[43]:

α. Το ΝΑΤΟ θα πρέπει να είναι σε θέση να υπερασπίσει τα συμφέροντα του στον κυβερνοχώρο, το ίδιο αποτελεσματικά όπως και στα άλλα πεδία.

β. Θα πρέπει να υπάρχει η δυνατότητα εφαρμογής του Διεθνούς Δικαίου στον κυβερνοχώρο.

[42] Από παρουσίαση της Έδρας Διακλαδικού Αμυντικού Προσανατολισμού (ΕΔΑΠ) της Ανωτάτης Διακλαδικής Σχολής Πολέμου (ΑΔΙΣΠΟ)
[43] Όπως παραπάνω

γ. Κάθε μέλος είναι υπεύθυνο για την προστασία των εθνικών δικτύων του, που πρέπει να είναι συμβατά με αυτά της συμμαχίας και των λοιπών μελών.

δ. Ενίσχυση της ευαισθητοποίησης και της εκπαίδευσης – κατάρτισης των χρηστών. Διοργάνωση ασκήσεων κάθε έτος (Cyber coalition, Locked Shields), με ευρεία συμμετοχή του ιδιωτικού τομέα και άλλων συνεργαζόμενων χωρών εκτός της συμμαχίας.

ε. Δέσμευση για ενίσχυση της ανταλλαγής πληροφοριών μεταξύ των μελών και την αμοιβαία συνδρομή στην πρόληψη, στην άμβλυνση των αποτελεσμάτων και στην ανάκτηση από επιθέσεις.

στ. Στενή συνεργασία με την ΕΕ[44]. Το ΝΑΤΟ συνεργάζεται επίσης μεταξύ άλλων, με τα Ηνωμένα Έθνη (ΟΗΕ) και τον Οργανισμό για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ) (North Atlantic Treaty Organization 2018).

ζ. Έμφαση στη συνεργασία με τον ιδιωτικό τομέα και ειδικότερα τη βιομηχανία[45].

Στις 16 Φεβρουαρίου 2017, οι υπουργοί άμυνας των χωρών της συμμαχίας ενέκριναν ένα επικαιροποιημένο σχέδιο δράσης για την άμυνα στον κυβερνοχώρο, καθώς και έναν οδικό χάρτη για τη χρήση του κυβερνοχώρου ως τομέα επιχειρήσεων. Αντικειμενικό σκοπό αποτελεί η επαύξηση της ικανότητας των Συμμάχων να συνεργάζονται, να αναπτύσσουν ικανότητες και να ανταλλάσσουν πληροφορίες. Επιπλέον το ΝΑΤΟ έχει ενσωματώσει την άμυνα στον κυβερνοχώρο στις πρωτοβουλίες Έξυπνης Άμυνας (Smart Defence). Η ενέργεια αυτή δίνει τη δυνατότητα στις χώρες να συνεργαστούν, προκειμένου να αναπτύξουν και να διατηρήσουν ικανότητες, που υπό κανονικές συνθήκες δεν θα είχαν την οικονομική δυνατότητα, με σκοπό να αποδεσμεύσουν πόρους για την ανάπτυξη άλλων ικανοτήτων. Το σχέδιο Έξυπνης Άμυνας για την υπεράσπιση του κυβερνοχώρου,

[44] Στις 5 Δεκεμβρίου 2017, οι Υπουργοί του ΝΑΤΟ και της ΕΕ συμφώνησαν να εντείνουν τη συνεργασία μεταξύ των δύο οργανισμών σε διάφορους τομείς, συμπεριλαμβανομένης της ασφάλειας στον κυβερνοχώρο και της άμυνας (North Atlantic Treaty Organization 2018).

[45] Το ΝΑΤΟ και οι σύμμαχοί του μέσω της συνεργασίας τους με τον χώρο της βιομηχανίας για τον κυβερνοχώρο (NATO Industry Cyber Partnership), εργάζονται για να ενισχύσουν τις σχέσεις τους. Η συνεργασία αυτή βασίζεται σε υπάρχουσες δομές και περιλαμβάνει οντότητες του ΝΑΤΟ, εθνικές ομάδες αντιμετώπισης έκτακτων καταστάσεων πληροφορικής (CERT) και εκπροσώπους της βιομηχανίας των κρατών μελών του ΝΑΤΟ (North Atlantic Treaty Organization 2018).

μέχρι στιγμής, περιλαμβάνει την πλατφόρμα κοινής χρήσης πληροφοριών για κακόβουλα προγράμματα (MISP), το πρόγραμμα MN CD2 (Smart Multinational Cyber Defense Capability Development) και το πολυεθνικό πρόγραμμα εκπαίδευσης και κατάρτισης στον τομέα της ψηφιακής άμυνας (MN CD E & T) (North Atlantic Treaty Organization 2018).

Οι υπεύθυνες αρχές για την κυβερνοάμυνα σε επίπεδο ΝΑΤΟ είναι [46]:

α. Το Βορειοατλαντικό Συμβούλιο (North Atlantic Council - NAC) έχει την πολιτική εποπτεία υψηλού επιπέδου για την εφαρμογή της πολιτικής κυβερνοάμυνας.

β. Το Συμβούλιο Διαχείρισης Κυβερνοάμυνας του ΝΑΤΟ (Cyber Defense Management Board – CDMB), είναι υπεύθυνο για τον συντονισμό της κυβερνοάμυνας σε πολιτικό και στρατιωτικό επίπεδο.

γ. Το NATO Consultation Command and Control (NC3) Board, έχει συμβουλευτικό ρόλο για τις τεχνικές και την εφαρμογή των διαφόρων πτυχών της κυβερνοάμυνας, με τεχνική υποστήριξη και προτάσεις για την ολοκλήρωση πληροφοριακών συστημάτων.

δ. Η Υπηρεσία Επικοινωνιών και Πληροφοριών του ΝΑΤΟ (NATO Communications and Information Agency- NCIA) που ιδρύθηκε το 2012, με τομέα ενδιαφέροντος τον κυβερνοχώρο και τα συστήματα επικοινωνιών πληροφορικής, είναι υπεύθυνη για την οργάνωση και λειτουργία του Νατοϊκού CERT [NATO Computer Incident Response Capabilitiy (NCIRC) Coordination Centrer] για την απόκριση στα κυβερνοπεριστατικά. Το NCIRC λειτουργεί στη Μονς (Βέλγιο), έχοντας αναλάβει πλήρεις επιχειρησιακές αρμοδιότητες από το 2014. Έχει καθοριστικό ρόλο στην αντιμετώπιση οποιασδήποτε επίθεσης στον κυβερνοχώρο εναντίον της Συμμαχίας. Διαχειρίζεται και συντονίζει την αντιμετώπιση των κυβερνοπεριστατικών, σε συνεργασία με τα αντίστοιχα CERT's των κρατών – μελών και παρέχει έγκαιρη προειδοποίηση και πληροφόρηση για την αντιμετώπιση απειλών στον κυβερνοχώρο.

ε. Το Νατοϊκό Συνεργατικό Κέντρο Αριστείας Κυβερνοάμυνας (Cooperative Cyber Defence Center of Excellence - CCDCoE). Το NATO CIRC και το CCD

[46] Από παρουσίαση της Έδρας Διακλαδικού Αμυντικού Προσανατολισμού (ΕΔΑΠ) της Ανωτάτης Διακλαδικής Σχολής Πολέμου (ΑΔΙΣΠΟ)

CoE, συνεργάζονται στενά με τις αντίστοιχες αρχές της Ε.Ε. (CERT-EU και ENISA).

Στη διάσκεψη κορυφής των Βρυξελλών το 2018, οι ηγέτες των συμμάχων συμφώνησαν να δημιουργήσουν ένα νέο κέντρο επιχειρησιακής λειτουργίας στον κυβερνοχώρο, στο πλαίσιο της ενισχυμένης δομής διοίκησης του ΝΑΤΟ. Πρόθεση της συμμαχίας είναι μέσω αυτής της ενέργειας, να ενισχύσει την άμυνα του ΝΑΤΟ στον κυβερνοχώρο και να συμβάλει στην ενσωμάτωση του κυβερνοχώρου στον προγραμματισμό και τις επιχειρήσεις του σε όλα τα επίπεδα (North Atlantic Treaty Organization 2018).

Η κυβερνοάμυνα στις Ελληνικές Ένοπλες Δυνάμεις

Οι Ελληνικές ένοπλες δυνάμεις σύμφωνα με το διακλαδικό δόγμα τους «περί επιχειρήσεων στον κυβερνοχώρο», είναι εκπαιδευμένες και θεσμικά προετοιμασμένες για πάσης φύσεως ενδεχόμενα είτε επιθετικού είτε αμυντικού χαρακτήρα. Οι συγκεκριμένες επιχειρήσεις διεξάγονται για συγκεκριμένη χρονική περίοδο, είτε ανεξάρτητα είτε σε συντονισμό με άλλες μορφές επιχειρήσεων, προκειμένου να παρέχουν υποστήριξη. Δεν αποσκοπούν στην στοχοποίηση του προσωπικού ούτε στην καταστροφή των δικτύων, αλλά προσβλέπουν είτε στην κυβερνοάμυνα, είτε στην εκμετάλλευση των πληροφοριών του αντιπάλου δικτύου (Σχης (ΠΖ) Πετούμενος Η. 2016, 49).

Το ΓΕΕΘΑ αποτελεί την Εθνική Αρχή Ασφαλείας και είναι υπεύθυνο για την ασφάλεια των πληροφοριών σε εθνικό και συμμαχικό επίπεδο. Είναι ο φορέας με μέριμνα του οποίου εκδίδεται ο Εθνικός Κανονισμός Ασφάλειας (ΕΚΑ) (σε συνεργασία με την ΕΥΠ). Η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ είναι υπεύθυνη για αντιμετώπιση των κυβερνοεπιθέσεων, καθώς και για την προστασία των πληροφοριακών δικτύων & υποδομών των ΕΔ. Για το σκοπό αυτό, οργανώνει και λειτουργεί το στρατιωτικό CERT, το οποίο συνεργάζεται με το αντίστοιχο εθνικό, με άλλους διεθνείς δημόσιους και ιδιωτικούς φορείς καθώς και με τις αντίστοιχες στρατιωτικές αρχές των κρατών – μελών της ΕΕ και του ΝΑΤΟ[47].

Η ΔΙΚΥΒ/ΓΕΕΘΑ ως αρμόδιος φορέας έχει εκπονήσει μέχρι σήμερα την στρατιωτική στρατηγική κυβερνοάμυνας, το δόγμα επιχειρήσεων κυβερνοχώρου,

[47] Όπως παραπάνω.

την πολιτική κυβερνοάμυνας, το τεχνικό σχέδιο δράσεως ανάπτυξης κυβερνοάμυνας στις ΕΔ και ένα τεχνικό εγχειρίδιο ασφαλείας προσωπικού υπολογιστή[48]. Τα δύο πρώτα είναι διαβαθμισμένα έγγραφα, στα οποία δεν είναι δυνατή η πρόσβαση ωστόσο είναι βέβαιο ότι αποτελούν την βάση, στην οποία στηρίζεται το οικοδόμημα της άμυνας των ΕΔ στον κυβερνοχώρο.

Η πολιτική άμυνας των ΕΔ στον κυβερνοχώρο αποτελεί ένα ενδιάμεσο στάδιο στην αλυσίδα υλοποίησης της κυβερνοάμυνας, μεταφράζοντας τις γενικές κατευθύνσεις της στρατιωτικής στρατηγικής και του δόγματος σε χαμηλότερου επιπέδου κατευθύνσεις. Σκοπός της είναι να καθορίσει το βασικό πλαίσιο υλοποίησης της κυβερνοάμυνας στις ΕΔ, ώστε μέσα από συγκεκριμένες διαδικασίες και μέτρα, να παρέχεται στα φίλια συστήματα επικοινωνιών και πληροφορικής η απαιτούμενη προστασία από τις ραγδαία εξελισσόμενες απειλές στον κυβερνοχώρο (ΓΕΕΘΑ/ΔΙΚΥΒ 2014, 1).

Λαμβάνοντας υπόψη την ποικιλία και την εκτεταμένη διασπορά των πληροφοριακών υποδομών των Γενικών Επιτελείων (ΓΕ) είναι σαφές, ότι απαιτείται συντονισμός προκειμένου να αποφευχθεί αλληλοεπικάλυψη των υφιστάμενων προσπαθειών και να επιδιωχθεί διαλειτουργικότητα, διασυνδεσιμότητα και μέγιστη αξιοποίηση του εξειδικευμένου προσωπικού. Ο ρόλος αυτός έχει αποδοθεί στη ΔΙΚΥΒ/ΓΕΕΘΑ, υπό την οποία ενεργούν και λειτουργούν τα αρμόδια τμήματα πληροφορικής των ΓΕ[49]. Η συνεργασία και ο συντονισμός μεταξύ όλων των ανωτέρω φορέων, επιτυγχάνεται μέσω του Κέντρου Αντιμετώπισης Κυβερνοπεριστατικών (ΚΑΚ), το οποίο παρακολουθεί όλα τα στρατιωτικά δίκτυα των ΓΕ επί 24ώρου βάσεως (ΓΕΕΘΑ/ΔΙΚΥΒ 2014, 2). Παράλληλα λόγω των εθνικών και διεθνών επεκτάσεων συγκεκριμένων υποδομών των Συστημάτων Επικοινωνιών και Πληροφορικής (ΣΕΠ) των ΕΔ, λαμβάνονται προβλέψεις για την ασφάλεια τους στη διασύνδεση τους, λόγω συνεργασίας και διαλειτουργικότητας με υπουργεία, ΕΥΠ, Αστυνομία και υπηρεσίες του ΝΑΤΟ και της ΕΕ.

[48] Από παρουσίαση της ΔΙΚΥΒ/ΓΕΕΘΑ η οποία έχει αναρτηθεί στο http://www.dideap.mil.gr/files/dikyv.pdf

[49] Στο ΓΕΣ έχει υπαχθεί το ΚΕΠΥΕΣ (Κέντρο Πληροφορικής Υποστήριξης Ελληνικού Στρατού), στο ΓΕΝ λειτουργεί το Γραφείο Κυβερνοάμυνας υπό τον Α΄ Κλάδο ενώ στο ΓΕΑ λειτουργεί το 3^{ο} Τμήμα (Ασφάλεια και Κυβερνοάμυνα) υπό τον Γ΄ Κλάδο (Σχης (ΠΖ) Πετούμενος Η. 2016, 50).

Η αντιμετώπιση των κυβερνοπεριστατικών γίνεται μέσω του ΚΑΚ και τον συντονισμό της ΔΙΚΥΒ και περιλαμβάνει (ΓΕΕΘΑ/ΔΙΚΥΒ 2014, 3-4):

α. Προετοιμασία και εκπαίδευση με την οποία επιτυγχάνεται ανάπτυξη προτύπων και διαδικασιών, που καλύπτουν όλο τον κύκλο εργασιών αντιμετώπισης κυβερνοπεριστατικών.

β. Αποτροπή, η οποία επιδιώκεται με την κοινοποίηση πολλαπλών επιπτώσεων, από ενδεχόμενη μη εφαρμογή των κανόνων ασφαλείας, από εσωτερικούς χρήστες ή προσπάθεια παραβίασης των ΣΕΠ. Ταυτόχρονα επιδιώκεται μέσω των πολλαπλών και ως ένα σημείο επικαλυπτόμενων μηχανισμών, άμυνα σε βάθος με την οποία εξασφαλίζεται, ότι η αποτυχία ή η αστοχία ενός μέτρου προστασίας θα καλυφθεί από τα υπόλοιπα.

γ. Διενέργεια τακτικών ή έκτακτων ελέγχων ασφαλείας, εκτιμήσεων τρωτότητας και ελέγχων διείσδυσης.

δ. Εντοπισμό σε πραγματικό ή κοντά σε πραγματικό χρόνο και αποτελεσματική αντιμετώπιση κάθε ύποπτης δραστηριότητας στον κυβερνοχώρο από το ΚΑΚ.

ε. Επαναφορά του πληγέντος συστήματος και επανάκτηση των δεδομένων του. Επιπλέον γίνεται πλήρης καταγραφή όλων των ενεργειών που πραγματοποιήθηκαν και των δεδομένων που συλλέχθηκαν, με σκοπό την ανάλυση της επίθεσης και την εξαγωγή συμπερασμάτων (Lessons Learned).

Την πολιτική κυβερνοάμυνας συμπληρώνει το Τεχνικό Σχέδιο Δράσης για την Ανάπτυξη της Κυβερνοάμυνας στις ΕΔ, που εκδόθηκε την ίδια χρονιά και είναι εναρμονισμένο με τον ΕΚΑ. Η σύνταξη του κρίθηκε αναγκαία, λόγω της ανάγκης για ύπαρξη ενός αναλυτικού οδηγού απαιτούμενων ενεργειών για την εφαρμογή της άμυνας και της ασφάλειας σε τεχνικό επίπεδο, προκειμένου να τεθεί ένα κοινό πλαίσιο δράσης για όλους τους εμπλεκόμενους φορείς (ΓΕΕΘΑ 2014, 1).

Το ανωτέρω σχέδιο περιλαμβάνει μια δέσμη είκοσι μέτρων για την ανάπτυξη δυνατοτήτων κυβερνοάμυνας, όπου για κάθε ένα περιγράφονται οι κίνδυνοι από την απουσία του, καθώς και οι τρόποι εφαρμογής του. Τα κυριότερα από αυτά αναφέρονται σε (ΓΕΕΘΑ 2014, 1):

α. Καταγραφή όλου του υλικού και λογισμικού που χρησιμοποιείται σε ΣΕΠ από τις ΕΔ.

β. Ασφαλή διαμόρφωση και ρύθμιση όλων των ΣΕΠ ανάλογα της χρήσης τους.

γ. Κατάλληλη εκπαίδευση του προσωπικού.

δ. Παρακολούθηση της δραστηριότητας των δικτύων σε πραγματικό χρόνο.

ε. Εντοπισμό των αδυναμιών και τρωτοτήτων των συστημάτων.

στ. Εντοπισμό και αντιμετώπιση κυβερνοπεριστατικών.

ζ. Διενέργεια δοκιμών και ελέγχων ασφαλείας των συστημάτων.

η. Ανατροφοδότηση συμπερασμάτων και μαθημάτων από την ανάλυση περιστατικών και τη διεξαγωγή εκπαίδευσης – ασκήσεων.

Επιπρόσθετα οι ΕΔ έχοντας αντιληφθεί, ότι όλες οι επιθέσεις έχουν ως στόχο τον χρήστη, επιδιώκουν να τον μετατρέψουν σε ακρογωνιαίο λίθο της στρατηγικής τους[50]. Γι' αυτό τον σκοπό έχουν προχωρήσει στην έκδοση τεχνικού εγχειριδίου ασφαλούς ρύθμισης και χρήσης Η/Υ, καθώς και οδηγού ασφαλούς χρήσης των μέσων κοινωνικής δικτύωσης από τα στελέχη των ΕΔ. Επιπλέον οι ΕΔ διοργανώνουν από το 2010 την εθνική άσκηση «ΠΑΝΟΠΤΗΣ» με τη συμμετοχή φορέων του δημοσίου, ιδιωτικού και ακαδημαϊκού τομέα στην οποία δίνεται έμφαση στην αντιμετώπιση επιθέσεων, που έχουν επίπτωση σε εθνικό επίπεδο, προκειμένου να αξιολογηθούν το προσωπικό (χρήστες και ειδικοί), οι διαδικασίες και η ανθεκτικότητα των υποδομών. Παράλληλα λαμβάνουν μέρος σε ανάλογες ασκήσεις στο πλαίσιο του ΝΑΤΟ και της ΕΕ.

Δεδομένου ότι ο κυβερνοπόλεμος παρουσιάζει μια δυναμική εξέλιξη, οι ΕΔ δεν μένουν άπραγες. Διαρκώς επανεξετάζουν και αξιολογούν το υφιστάμενο πλαίσιο και προσπαθούν να προσαρμοστούν στις υφιστάμενες συνθήκες. Ορισμένες από τις κυριότερες δράσεις της ΔΙΚΥΒ/ΓΕΕΘΑ σε εξέλιξη, είναι η επικαιροποίηση του τεχνικού εγχειριδίου ασφαλείας Η/Υ, η ενεργοποίηση διακλαδικού κέντρου αντιμετώπισης κυβερνοπεριστατικών, η εκκίνηση της

[50] Σύνθημα που χρησιμοποιείται σε παρουσιάσεις και ενημερωτικές καμπάνιες είναι «Η Κυβερνοάμυνα είναι υπόθεση όλων» [Από παρουσίαση της Έδρας Διακλαδικού Αμυντικού Προσανατολισμού (ΕΔΑΠ) της Ανωτάτης Διακλαδικής Σχολής Πολέμου (ΑΔΙΣΠΟ)]

διαδικασίας για σύνταξη εθνικής στρατηγικής κυβερνοασφαλείας, ενώ εξετάζεται ο μετασχηματισμός της ΔΙΚΥΒ σε Διακλαδική Διοίκηση Επιχειρήσεων Κυβερνοχώρου (ΔΙΔΕΚ).

ΚΕΦΑΛΑΙΟ «ΣΤ»

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΤΗΣ ΕΛΛΑΔΑΣ

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τις τελευταίες δύο δεκαετίες, εκατομμύρια άνθρωποι σε όλο τον κόσμο έχουν επωφεληθεί από την ραγδαία ανάπτυξη και την εκμετάλλευση των τεχνολογιών πληροφορικής και επικοινωνιών. Παρατηρούμε μια ψηφιακή επανάσταση, που μεταμορφώνει βαθιά τις κοινωνίες μας (International Telecommunication Union 2018, vi). Πέραν όμως των αναμφισβήτητων πλεονεκτημάτων που παρέχουν, επισύρουν και κινδύνους για κρατικούς και ιδιωτικούς φορείς, καθώς και για τους πολίτες.

Οι απειλές προκύπτουν αρχικά από τα χαρακτηριστικά του κυβερνοχώρου. Το γεγονός ότι ξεπερνά τους γεωγραφικούς περιορισμούς, διαπερνά τα σύνορα, μειώνει τους φραγμούς στον ακτιβισμό και την πολιτική έκφραση και παράλληλα αποκρύπτει τις ταυτότητες των δρώντων σε συνδυασμό με την παροχή κατάλληλου εδάφους για μη ανάληψη ευθυνών, δημιουργεί σαφείς ευκαιρίες εκδήλωσης κακόβουλων ενεργειών σε παγκόσμια κλίμακα.

Η ισχύς στον κυβερνοχώρο είναι μια έννοια ασαφής καθώς σε αρκετές περιπτώσεις δεν γνωρίζουμε τον κάτοχο της, το μέγεθος της, τον τομέα δραστηριοτήτων στον οποίο μπορεί να εφαρμοσθεί, την αποτελεσματικότητα της, το σημείο ισορροπίας και το κόστος χρήσης της. Η σημαντικότερη δε μορφή της, η παραγωγική κυβερνο-ισχύς, συνδέει τις στρατιωτικές και πολιτικές δυνάμεις, στην προσπάθεια της να εφαρμόσει στρατηγική ήπιας ισχύος, στοχεύοντας κυρίως στην καρδιά και το μυαλό του ανθρώπου.

Ο κυβερνοχώρος είναι ένα άναρχο σύστημα και παρέχει μια σειρά από προκλήσεις στην κυριαρχία, τις οποίες τα κράτη δεν πρέπει να αγνοήσουν. Ο κυβερνοπόλεμος έχει σημαντικές επιπτώσεις στην Βεστφαλιανή έννοια της κυριαρχίας, καθώς δύναται υπό προϋποθέσεις να επιβάλλει αλλαγές ή να καθορίσει την δομή και τη λειτουργία της εσωτερικής πολιτικής εξουσίας. Επιπλέον η εδραίωση της κρατικής κυριαρχίας στον υπόψη χώρο απαιτεί κατ’ ελάχιστο την αναγνώριση της, από τους υπόλοιπους κρατικούς δρώντες και επιπλέον το ίδιο το

κράτος να δύναται να εφαρμόσει μέτρα ελέγχου στον κυβερνοχώρο του, ως απτή απόδειξη αυτής.

Ο κυβερνοπόλεμος διακρίνεται σε στρατηγικό και επιχειρησιακό. Ο πρώτος διεξάγεται για να επιβάλλει στην αντίπαλη πλευρά την θέληση του επιτιθέμενου, αποδεικνύοντας την αδυναμία της να αμυνθεί. Ο δεύτερος χρησιμοποιείται κατά την διάρκεια συμβατικού πολέμου ενάντια πολιτικών ή στρατιωτικών στόχων.

Το υφιστάμενο νομικό πλαίσιο δεν περιλαμβάνει τις κυβερνοεπιθέσεις στις πράξεις που μπορεί να θεωρηθούν επιθετικές και κατά συνέπεια οι εν λόγω ενέργειες δεν μπορούν να προκαλέσουν την ενεργοποίηση του άρθρου 51 του χάρτη των Η.Ε. Επιπλέον το πρόβλημα της απόδοσης ευθυνών, συμβάλλει αρνητικά στον προσδιορισμό του υπεύθυνου των επιθέσεων, παρά την εξέλιξη της τεχνολογίας και αποδυναμώνει την αποτροπή.

Στο κυβερνοχώρο η σχέση μεταξύ επίθεσης και άμυνας φαινομενικά ευνοεί την πρώτη, γιατί έχει την πρωτοβουλία των κινήσεων και το κόστος είναι συγκριτικά μικρότερο από ότι στην άμυνα. Στην πραγματικότητα ωστόσο προκύπτει, ότι η απόλυτη μέτρηση του κόστους της επίθεσης έχει νόημα μόνο σε σχέση με τις δαπάνες του αμυνόμενου.

Οι στρατηγικές κυβερνοασφάλειας των τριών ξένων χωρών επιλέχθηκαν με κριτήριο να παρουσιαστεί:

α. Η ιδεατή περίπτωση των ΗΠΑ, που λόγω της αναμφισβήτητης ισχύος τους έχουν ισχυρή δυνατότητα κυβερνοάμυνας και παράλληλα διατηρούν αντίστοιχες δυνατότητες επίθεσης σε παγκόσμια κλίμακα, ενισχύοντας την αποτροπή ανταποκρινόμενη πλήρως στον ρόλο τους ως υπερδύναμη.

β. Η περίπτωση της Κίνας, ως μια χώρα που επιθυμεί στοχευόμενα να δημιουργήσει τις προϋποθέσεις να αντιπαρατεθεί έναντι ενός ισχυρότερου συμβατικού αντιπάλου.

γ. Η περίπτωση της Εσθονίας, ως μια χώρα που ήταν ανέκαθεν τεχνολογικά προηγμένη και παράλληλα είναι από τις λίγες χώρες που έχουν εμπειρία κυβερνοπολέμου.

Η Ελλάδα έχει καταρτίσει στρατηγική κυβερνοασφάλειας και κυβερνοάμυνας σε επίπεδο πολιτικό και ΕΔ σαφώς εναρμονισμένες στα πλαίσια της ΕΕ και του

ΝΑΤΟ, τουλάχιστον σε επίπεδο σχεδίασης. Παράλληλα η Ελλάδα μπορεί να δει αρκετούς κοινούς στόχους και να λάβει αρκετά διδάγματα από τις χώρες η στρατηγική των οποίων παρουσιάστηκε.

ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΤΗΣ ΕΛΛΑΔΑΣ

Όπως διαπιστώθηκε η στρατηγική της Ελλάδας στην αντιμετώπιση των κυβερνοαπειλών είναι επίκαιρη και σύμφωνη με το πλαίσιο που καθορίζουν οι υπερεθνικοί οργανισμοί στους οποίους συμμετέχει. Η διαφορά του κυβερνοπόλεμου από τον συμβατικό, είναι ότι αυτός συμβαίνει καθημερινά δοκιμάζοντας τις αντοχές και τα αντανακλαστικά του συστήματος. Κατά συνέπεια οι εμπλεκόμενοι με την κυβερνοάμυνα μιας χώρας ή ενός οργανισμού λαμβάνουν εμπειρίες, οι οποίες κατάλληλα εκμεταλλευόμενες μπορούν να βελτιώνουν διαρκώς τις αδυναμίες τους.

Ενέργειες οι οποίες εκτιμάται, ότι θα συμβάλουν θετικά στη βελτίωση της υφιστάμενης στρατηγικής είναι :

α. Η μονομερής δήλωση από την Ελλάδα ότι θεωρεί τον κυβερνοχώρο της μέρος όπου ασκεί εθνική κυριαρχία (Μαυρόπουλος 2014, 38).

β. Η αναθεώρηση – συμπλήρωση του εθνικού νομικού πλαισίου, που αφορά στη δραστηριότητα στον κυβερνοχώρο (Μαυρόπουλος 2014, 39).

γ. Η ενεργή συμμετοχή σε κάθε διεθνή πρωτοβουλία είτε σε επίπεδο συμμαχιών είτε σε επίπεδο πολυεθνικών οργανισμών, προκειμένου να καταστεί δυνατή η καθιέρωση κοινά αποδεκτών αρχών, οι οποίες θα ρυθμίζουν την δραστηριότητα στον κυβερνοχώρο και θα προκαλέσουν την αναθεώρηση του δικαίου του πολέμου.

δ. Η υιοθέτηση της προληπτικής επίθεσης ως αμυντικής τακτικής.

ε. Η επιδίωξη για ακόμα περεταίρω βελτίωση της συνεργασίας μεταξύ δημόσιου και ιδιωτικού φορέα, καθώς η ασφάλεια και η άμυνα εν γένει στον κυβερνοχώρο είναι υποχρέωση όλων.

στ. Η συμμετοχή στην εκδήλωση των ενεργειών που θα συμβάλουν να καταστεί εφικτή η «ενιαία ψηφιακή ευρωπαϊκή αγορά», προκειμένου να διασφαλιστεί η αλυσίδα εφοδιασμού με συνέπεια, τα υλικά και το λογισμικό που θα

χρησιμοποιούνται από τον δημόσιο και ιδιωτικό τομέα να πληρούν τις προϋποθέσεις ασφαλείας της ΕΕ.

ζ. Η περεταίρω εκμετάλλευση των ανώτατων εκπαιδευτικών ιδρυμάτων, που ασχολούνται με τον χώρο της πληροφορικής, ώστε με την ανάλογη χρηματοδότηση να επιδιώκεται η ανάπτυξη πρότυπων κυβερνοόπλων, που θα συμβάλουν στην κυβερνοάμυνα και στην δυνατότητα προληπτικών κυβερνοεπιθέσεων.

η. Η εισαγωγή της ενημέρωσης για την κυβερνοασφάλεια σε όσες βαθμίδες εκπαίδευσης απαιτείται, προκειμένου να θωρακιστεί ο χρήστης που είναι ούτως ή άλλως ο κύριος στόχος των επιθέσεων.

θ. Η δημιουργία αυστηρών προδιαγραφών λειτουργίας δικτύων, ιδιαίτερα αυτών του δημοσίου τομέα συμπεριλαμβανομένου των στρατιωτικών και διενέργεια τακτικών και έκτακτων ελέγχων υλοποίησης τους.

ι. Οι ενέργειες σύστασης εικονικής εχθρικής ομάδος (Red Team), η οποία θα έχει ως αποστολή την εκτέλεση έκτακτων επιθέσεων περιορισμένου χαρακτήρα, ώστε να διαπιστώνεται η ετοιμότητα του κρατικού μηχανισμού.

ια. Η συστηματική παρακολούθηση των σημείων διασύνδεσης της χώρας στο διαδίκτυο κατά τρόπο, ώστε να είναι δυνατή η απομόνωση της χώρας μας σε περίπτωση που δεχθεί κυβερνοεπίθεση μεγάλης κλίμακας και ελεγχόμενη επανασύνδεση σ' αυτό μετά τη διασφάλιση της απόκρουσης της απειλής (Μαυρόπουλος 2014, 39).

ιβ. Η σύσταση εθελοντικής οργάνωσης στο πρότυπο του Estonian Defence League's Cyber Unit, που είναι αποτέλεσμα συνεργασίας του δημόσιου και ιδιωτικού τομέα με σκοπό την εκμετάλλευση των Ελλήνων χάκερ και την επιστράτευση τους στην επίτευξη του κοινού σκοπού.

ιγ. Η μελέτη και υιοθέτηση κανόνων εμπλοκής κυβερνοπολέμου με σκοπό την πρόβλεψη και το καθορισμό του απαιτούμενου βαθμού αποκέντρωσης τόσο σε επίπεδο λήψης αποφάσεων όσο και σε επίπεδο ανάληψης ενεργειών.

ΕΠΙΛΟΓΟΣ

Οι θεωρίες της παγκοσμιοποίησης, της παγκόσμιας κοινωνίας των πολιτών και των διεθνικών δικτύων, σε συνδυασμό με τη διαρκώς αναπτυσσόμενη εξάρτηση των κρατών από τη τεχνολογία, επιδρούν αρνητικά στην ισχύ και την κυριαρχία του κράτους, ενώ παράλληλα τροφοδοτούν την άνοδο εκείνου, που ο James Rosenau εύστοχα αποκαλεί «*sovereignty – free actors*» (Deibert n.d., 529). Αν σ' αυτούς τους δρώντες προστεθούν και τα κράτη που υιοθετούν τακτικές ανάλογες, εκμεταλλευόμενα την ανωνυμία και την αδυναμία απόδοσης ευθυνών, γίνεται αντιληπτό, ότι ο κυβερνοχώρος μεταβάλλεται σ' ένα περιβάλλον επικίνδυνο με λεπτές ισορροπίες.

Τα κράτη σε επίπεδο πρόθεσης και σχεδίασης διαπιστώθηκε, ότι έχουν λάβει όλα τα απαραίτητα μέτρα προκειμένου να μπορούν να ανταποκριθούν σ' αυτή την πρόκληση. Η παγκοσμιοποίηση και η δικτύωση συνέβαλλαν θετικά προς αυτή την κατεύθυνση. Η προστασία των κρίσιμων υποδομών της χώρας από κυβερνοεπιθέσεις αποτελεί τον ακρογωνιαίο λίθο της στρατηγικής ασφαλείας στον κυβερνοχώρο. Επιτυχής απόκρουση ενδεχόμενης αιφνιδιαστικής επίθεσης, θα προκαλέσει απώλεια του πλεονεκτήματος της πρώτης κίνησης και αύξηση του κόστους για τον αντίπαλο.

Η επένδυση στην αποτροπή ακόμα και αν αυτή δεν μπορεί να είναι τόσο επιτυχής όσο την εποχή του ψυχρού πολέμου, θα πρέπει να αποτελέσει βασικό άξονα των στρατηγικών κυβερνοασφαλείας των κρατών, μηδέ εξαιρουμένου της Ελλάδας. Η αποτροπή θεωρείται επιτυχής αφενός, όταν έχουν ληφθεί όλα τα απαιτούμενα μέτρα που θα μετατρέψουν την σχεδίαση σε εφαρμογή αφετέρου, όταν ο εχθρός αντιλαμβάνεται το μέγεθος του ρίσκου που διατρέχει. Κορωνίδα της προσπάθειας αυτής, πρέπει να αποτελέσει η προσαρμογή του νομικού πλαισίου, ώστε να προβλέπει την αναλογική εφαρμογή των κανόνων του διεθνούς δικαίου και την ένταξη των επιθέσεων και των παράνομων πράξεων στον κυβερνοχώρο στο πλαίσιο της αυτοάμυνας. Στο ερώτημα άμυνα ή επίθεση, η ορθότερη απάντηση είναι, ανάπτυξη αμυντικών δυνατοτήτων και ταυτόχρονη διατήρηση ικανότητας εκτόξευσης προληπτικής επίθεσης, γεγονός το οποίο επιβάλλει την ανάπτυξη ανάλογων κυβερνοδυνατοτήτων σε εθνικό επίπεδο.

Η Ελλάδα είναι μια χώρα ανεπτυγμένη και κατά συνέπεια οι υποδομές της εξαρτώνται ολοένα και περισσότερο από τη τεχνολογία πληροφορικής και επικοινωνιών. Παράλληλα το ευρύτερο γεωπολιτικό περιβάλλον στο οποίο ανήκει, περιλαμβάνει κράτη φαινομενικά ισχυρότερα αλλά και ασθενέστερα, που θα μπορούσαν το κάθε ένα για τους δικούς του αντικειμενικούς σκοπούς, να εκμεταλλευθεί τον κυβερνοπόλεμο εναντίον της, είτε σε συνδυασμό με επιχειρήσεις κινητικού χαρακτήρα, είτε όχι. Η αντιμετώπιση των απειλών μπορεί να γίνει μέσω μιας στοχευόμενης στρατηγικής, άξονες της οποίας θα πρέπει να αποτελούν ο ενημερωμένος χρήστης, ένα άγρυπνο σύστημα ανίχνευσης και ταχείας αντίδρασης και η εφαρμογή καινοτόμων ιδεών, ώστε να δύναται να αντιμετωπίζει όχι μόνο της απειλές του σήμερα αλλά του αύριο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

3218/2018, Υπουργική Απόφαση. «enisa.europa.eu.» *www.enisa.europa.eu.* 7 Μάρτιος 2018. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGR.pdf/ (πρόσβαση Νοέμβριος 14, 2018).

Ayers, Cynthia E. «U.S. ARMY WAR COLLEGE.» *csl.army.mil.* Δεκέμβριος 2016. http://www.csl.army.mil/AllPublications.aspx (πρόσβαση Οκτώβριος 28, 2018).

Bell, Cameron H. «Cyber Warfare and International Law: The Need for Clarity.» *TOWSON UNIVERSITY OF INTERNATIONAL AFFAIRS VOL LI, NO2*, 2018: 21 - 43.

Betz J, David & Stevens, Tim. *Cyberspace and the State.* Routledge, 2011.

Betz, David. *Cyber Power in Strategic Affairs: Neither Untinkable nor Blessed.* Routledge, 2012.

—. «Journal in Strategic Affairs.» *www.Journal in Strategic Affairs.* Οκτώβριος 2012. http://dx.doi.org/10.1080/01402390.2012.706970 (πρόσβαση Αύγουστος 2, 2018).

Bing, Christopher. *Reuters.* 20 Σεπτέμβριος 2018. https://uk.reuters.com/article/us-usa-cyber/white-house-pledges-to-step-up-cyber-offense-on-hackers-idUKKCN1M031I (πρόσβαση Νοέμβριος 11, 2018).

Brandon Valeriano & Ryan Maness. *The Dynamics of Cyber Conflict Between rival Antagonists, 2001 - 11.* SAGE, 2014.

Burton, Joe. «NATO Coopoaretive Cyber Defence Center of Excellence.» *ccdcoe.org.* 2018. https://ccdcoe.org/publication-library.html (πρόσβαση Οκτώβριος 25, 2018).

«Central Cyber Security and Informatization Committee Office.» *cac.gov.cn.* 27 Δεκέμβριος 2016. http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (πρόσβαση Νοέμβριος 15, 2018).

Clausewitz, Carl von. *Περί του Πολέμου.* Θεσσαλονίκη: Βάνιας, 1999.

David Betz & Tim Stevens. *Cyberspace and the State.* Routledge.

Deibert, Ronald J. *Black Code: Cencorship, Surveillance and the militarisation of Cyberspace.* SAGE Publications.

enisa.europa.eu. «enisa.europa.eu.» *www.enisa.europa.eu.* Νοέμβριος 2016. https://www.enisa.europa.eu/publications/ncss-good-practice-guide (πρόσβαση Νοέμβριος 11, 2018).

European Commission. «eeas.europa.eu.» *eeas.europa.eu.* 7 Φεβρουάριος 2013. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (πρόσβαση Νοέμβριος 24, 2018).

Fazzini, Kate. *CNBC.* 21 Σεπτέμβριος 2018. https://www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html (πρόσβαση Νοέμβριος 11, 2018).

Franzese, Patrick W. *Sovereignty in Cyberspace: Can it exist?* Διατριβή, HEINONLINE, 2009.

Gartzke, Erik. «The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.» *International Security*, 2013: 41 - 73.

Graw, Gary Mc. *Cyber War Will Take Place (Unless We Build Security In).* Routledge, 2013.

International Telecommunication Union. «itu.int.» *www.itu.int.* 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf (πρόσβαση Νοέμβριος 21, 2018).

Joel Brenner & Jon R. Lindsay. «Debating the Chinese Cyber Threat.» *International Security*, 2015: 191 - 195.

Joint Chiefs of Staff, US. «jcs.mil.» *www.jcs.mil.* 8 Ιούνιος 2018. http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/ (πρόσβαση Οκτώβριος 17, 2018).

Jon R. Lindsay, Lucas Kello. «Correspondence: A Cyber Disagreement.» *International Security*, 2014: 181 - 192.

Junio, Timothy J. *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate.* Routledge, 2013.

Karatzogianni, Athina. *Cyber Conflict and Global Politics.* Abingdon: Routledge, 2009.

—. *The Politics of Cyberconflict.* Abingdon: Routledge, 2006.

Kaska, Kadri & Osula, Anna - Maria & LTC Stinissen, Jan. «ccdcoe.org.» *www.ccdcoe.org.* 2013. https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html (πρόσβαση Νοέμβριος 20, 2018).

Kello, Lucas. «The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.» *International Security*, 2013: 7 - 40.

Kovacs, Laszlo. «armyacademy.ro.» *www.armyacademy.ro.* https://www.armyacademy.ro/reviste/rev1_2018/KOVACS.pdf (πρόσβαση Νοέμβριος 26, 2018).

Krepinevich, Andrew F. «csbaonline.» *csbaonline.org.* 2012. https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option (πρόσβαση Νοέμβριος 1, 2018).

Kuo, Lily and Kommenda, Niko. *theguardian.com.* https://www.theguardian.com/cities/ng-interactive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer (πρόσβαση Νοέμβριος 18, 2018).

Lene Hansen & Helen Nissenbaum. «Digital Disaster, Cyber Security, and the Copenhagen School.» *International Studies Quarterly*, 2009: 1155 - 1175.

Liaropoulos, Andrew. «ETH zurich CSS.» *http://www.css.ethz.ch.* 30 Ιανουάριος 2014. http://www.css.ethz.ch/en/services/digital-library/publications/publication.html/188212 (πρόσβαση Σεπτέμβριος 24, 2018).

Liaropoulos, Andrew. «On Cyber - terrorism: Redefining Terror in Cyberspace.» Στο *POLITIKA Annual Journal 2014 Terrorisma in a Global Context*. Politics and public administration association : The Hong Kong University .

—. «Great Power Politics in Cyberspace: US and China are drawing the lines between confrontation and cooperation.» *PANORAMA of global security environment* , 2013: 155 - 166.

Libicki, Martin. «rand.org.» *τοποθεσία της rand.org.* 2009. www.rand.org/pdfrd/pubs/monographs/MG877// (πρόσβαση Οκτώβριος 20, 2018).

—. «rand.org.» *www.rand.org.* 2017. https://www.rand.org/pubs/authors/l/libicki_martin_c.html (πρόσβαση Οκτώβριος 28, 2018).

Liff, Adam P. *Cyberwar: A New 'Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War.* Routledge, 2012.

Lindau, Katri. «cs.tlu.ee.» *www.cs.tlu.ee.* 2012. www.cs.tlu.ee/teemad/get_file.php?id=195 (πρόσβαση Νοέμβριος 21, 2018).

Lindsay, Jon R. «The impact of China on Cybersecurity: Fiction and Friction.» *International Security*, 2014/2015: 7 - 47.

Mazanec, Gregory D. koblentz & Brian M. «Viral Warfare: The Security implications of Cyber and Biological Weapons.» *Comparative Strategy*, 2013: 418 - 434.

Ministry of Economic Affairs and Communication. «mkm.ee.» *www.mkm.ee.* 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (πρόσβαση Νοέμβριος 20, 2018).

North Atlantic Treaty Organization. *www.nato.int.* 16 Ιούλιος 2018. https://www.nato.int/cps/en/natohq/topics_78170.htm (πρόσβαση Νοέμβριος 23, 2018).

Nye, Joseph. «Deterrence and Dissuasion in Cyberspace.» *International Security*, 2016/2017: 44 - 71.

Patterson, George. «Cyberwar: The United States and China Prepare For the Next Generation of Conflict.» *Comparative Strategy*, 2011: 121 - 133.

Peterson, Dale. *Offensive Cyber Weapons: Construction, Development, and Employment.* Routledge, 2013.

Raud, Mikk. «CCDCOE.» *ccdcoe.org.* 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (πρόσβαση Νοέμβριος 17, 2018).

Ronald J Deibert, Rafal Rohozinski and Masashi Crete - Nishihata. «Cyclones in Cyberspace: Information shaping and denial in the 2008 Russia - Georgia war.»

Schmitt, Michael N. *Tallinn Manual on the International Law.* Νέα Υόρκη: Cambridge University Press, 2013.

Slayton, Rebecca. «What is the Cyber Offence - Defense Balance?: Conceptions, Causes, and Assesment.» *Inernational Security*, 2016: 72 - 109.

Stone, John. *Cyber War Will Take Place!* Routledge, 2012.

Szentgali, Gergely. *folyoiratok.uni-nke.hu.* https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-20131-szentgali.original.pdf (πρόσβαση Νοέμβριος 24, 2018).

The White House. «The White House, National-Cyber-Strategy of the USA.» *whitehouse.gov.* Σεπτέμβριος 2018. www.whitehouse.gov/wp-content/uploads/2018/.../National-Cyber-Strategy.pdf (πρόσβαση Νοέμβριος 12, 2018).

Valeriano, Ryan C. Maness & Brandon. «The Impact of Cyber Conflict on International Interactions.» *Armed Forces and Society*, 2016: 301 - 323.

wikipedia. *wikipedia.org.* 4 Οκτώβριος 2018. en.wikipedia.org/wiki/Industrial_control_system (πρόσβαση Οκτώβριος 23, 2018).

Wilmshurst, Elizabeth. «Definition Of Aggression.» *United Nations Audiovisual Library of International Law.* 2008. www.un.org/law/avl (πρόσβαση Οκτώβριος 19, 2018).

Βαγενά, Ευαγγελία. *Professional it security.* 19 Ιούλιος 2017. https://www.itsecuritypro.gr/nis-nea-odigia-gia-tin-kyvernoasfalia/ (πρόσβαση Νοέμβριος 22, 2018).

ΓΕΕΘΑ. «ΓΕΕΘΑ.» *www.geetha.mil.gr.* Μάρτιος 2014. http://www.geetha.mil.gr/media/pdf-arxeia/2014/cyberdefence/texniko_sxedio_drasis_gia_tin_anaptixi_kivernoaminas_stis_ED.pdf (πρόσβαση Νοέμβριος 26, 2018).

ΓΕΕΘΑ/ΔΙΚΥΒ. «geetha.mil.gr.» *www.geetha.mil.gr.* Φεβρουάριος 2014. http://www.geetha.mil.gr/media/dikib/cyberdefence/cyberpolicy.pdf (πρόσβαση Νοέμβριος 26, 2018).

Γενική Γραμματεία Πολιτικής Προστασίας. *civilprotection.gr.* https://www.civilprotection.gr/el/γενικό-σχέδιο-πολιτικής-προστασίας (πρόσβαση Νοέμβριος 28, 2018).

Γιαννακόπουλος, Βασίλειος. «GEOStrategy.» *www.geostrategy.gr.* 29 Δεκέμβριος 2010. www.geostrategy.gr (πρόσβαση Σεπτέμβριος 23, 2018).

Γρίβας, Κωνσταντίνος. «Ο ρόλος του κυβερνοπολέμου στην κινεζική γεωστρατηγική.» *eclass.uoa.gr.* https://eclass.uoa.gr (πρόσβαση Νοέμβριος 14, 2018).

Δελίμπασης, Δημήτριος. «Information Warfare Operations Within the Concept of Individual Self Defence.» Στο *Cyber Conflict and Global Politics*, του/της Καρατζογιάννη Αθηνά, 95-112. Routledge, 2009.

Εθνικό Κέντρο Τεκμηρίωσης. 14 Ιούνιος 2018. www.ekt.gr/el/news/21953 (πρόσβαση Νοέμβριος 22, 2018).

Ευρωπαϊκό Κοινοβούλιο & Συμβούλιο. «eur-lex.europa.eu.» *www.eur-lex.europa.eu.* 19 Ιούλιος 2016. https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016&from=EN (πρόσβαση Νοέμβριος 23, 2018).

Κουσκουβέλης, Ηλίας. *Εισαγωγή στις Διεθνείς Σχέσεις.* Αθήνα : Εκδόσεις Ποιότητα, 2007.

Μαυρόπουλος, Παναγιώτης. «Πόλεμος και Στρατηγική.» 19 Ιανουάριος 2014. www.warandstrategy.gr (πρόσβαση Σεπτέμβριος 18, 2018).

Μποζίνης & Μικέλης. «Νέες Τεχνολογίες στις Διεθνείς Σχέσεις: Η περιπτωσιολογική Μελέτη της Ρομποτικής και των Drones ως Συντελεστών Ισχύος

μέσω μιας Σύγχρονης Θεωρητικής Προσέγγισης.» *Αεροπορική Επιθεώρηση*, Αύγουστος 2018: 38 - 55.

Ν. 3649/2008-ΦΕΚ39/Α. «ΙΣΟΚΡΑΤΗΣ Τράπεζα Νομικών Υπηρεσιών.» *www.dsanet.gr.* 3 Μάρτιος 2008. http://www.dsanet.gr/Epikairothta/Nomothesia/n3649_08.htm (πρόσβαση Νοέμβριος 22, 2018).

Παπαδούλη, Μάρθα. *Οι επιθέσεις στον κυβερνοχώρο: Τι είναι και ποιούς προβληματισμούς δημιουργούν.* Διπλωματική Εργασία, Θεσσαλονίκη: Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2009.

Σχης (ΠΖ) Πετούμενος Η. «Η Κυβερνοάμυνα στις Ένοπλες Δυνάμεις.» *Αθηνά*, Δεκέμβριος 2016: 40 - 55.

Χαίδης, Λεωνίδας. *Οι Συγκρούσεις στον Κυβερνοχώρο: Ο κυβερνοπόλεμος και η Αποτροπή.* Διπλωματική Εργασία, Πειραιάς: Πανεπιστήμιο Πειραιά, 2012.