ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ
ΚΑΙ ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ

*του Παναγιώτη Μαυρόπουλου**

1. ΕΙΣΑΓΩΓΗ

Η εμφάνιση του ηλεκτρονικού υπολογιστή και η εξέλιξη της τεχνολογίας οδήγησε στην οργάνωση επικοινωνιακών δικτύων και τη δημιουργία εφαρμογών οι οποίες υποστηρίζουν διάφορες ανθρώπινες δραστηριότητες και για τη λειτουργία τους βασίζονται σε δίκτυα υπολογιστών. Τα δίκτυα ήταν κατ' αρχήν απομονωμένα και κατά συνέπεια πρόσφεραν εγγενή προστασία από κακόβουλους χρήστες. Η ανάπτυξη όμως της πληροφορικής και η ανάγκη να τεθούν όλες αυτές οι υπηρεσίες στην υπηρεσία του πολίτη, έτσι ώστε να διευκολυνθούν και να επιταχυνθούν οι συναλλαγές των πολιτών τόσο με τις διάφορες υπηρεσίες όσο και μεταξύ τους, όπως επίσης και η οικονομία κλίμακας η οποία επιτυγχάνεται με τη χρήση της νέας τεχνολογίας, τα κατέστησε ευρέως προσβάσιμα και οδήγησε στην αύξηση της τρωτότητάς τους.

Οι Κυβερνοεπιθέσεις εναντίον της Εσθονίας, τον Απρίλιο - Μάιο του 2007, ανέδειξαν αυτή την τρωτότητα των δικτύων και κατ' επέκταση των χωρών σε ένα είδος απειλής το οποίο μέχρι τότε ήταν περιορισμένο και αφορούσε τους χάκερ, τις μυστικές υπηρεσίες των χωρών και τη βιομηχανική κατασκοπεία. Τα γεγονότα αυτά κατέδειξαν ότι η κάποτε υποθετική πιθανότητα μιας Κυβερνοεπίθεσης ή ακόμη και ενός Κυβερνοπολέμου εναντίον μιας χώρας είναι πλέον πραγματικότητα. Στη συγκεκριμένη περίπτωση, οι συνέπειες ήταν σχετικά περιορισμένες και δεν υπήρξαν ανθρώπινες απώλειες ή φυσικές καταστροφές. Παρόλα αυτά, η διακοπή της λειτουργίας των κρατικών υπηρεσιών και της δημόσιας και ιδιωτικής οικονομικής δραστηριότητας για μεγάλο χρονικό διάστημα είχε άμεσες αρνητικές επιπτώσεις στην καθημερινότητα χιλιάδων πολιτών και στην οικονομία της Εσθονίας.

Η περαιτέρω βελτίωση της τεχνολογίας των επικοινωνιών και της πληροφορικής αναμένεται να προκαλέσει αντίστοιχη αύξηση της τρωτότητας των δικτύων και των υποδομών μιας χώρας· η τρωτότητα αυτή, συνδυαζόμενη με τη βελτίωση της αποτελεσματικότητας των Κυβερνοόπλων του μέλλοντος, θα καταστήσει τον Κυβερνοχώρο ένα νέο πεδίο ανταγωνισμού, και τον Κυβερνοπόλεμο μια πραγματική πρόκληση για την Κυβερνοασφάλεια των κρατών.

2. ΓΕΝΙΚΑ

α. Ιστορική ανασκόπηση

Η αξία των πληροφοριών για μια ενδεχόμενη αντιπαράθεση μεταξύ δύο ή περισσοτέρων οργανωμένων ομάδων (όχι απαραίτητα στρατιωτικών) έχει υπογραμμιστεί από τον Sun Tzu 2.500 χρόνια πριν με τη φράση «Αν γνωρίζεις τον εχθρό και τον εαυτό σου, δεν χρειάζεται να φοβάσαι για την έκβαση εκατό μαχών[1]». Η αξία αυτή δεν αμφισβητήθηκε ποτέ κατά τη διάρκεια αυτών των 2.500 χρόνων, αντίθετα οδήγησε στη

[1] Sun Tzu, *The Art of War*, Εκδόσεις Επικοινωνίες ΑΕ, Αθήνα 2002, Μετ. Πάνος Πικραμένος, Κεφάλαιο ΙΙΙ Το σπαθί τη θήκη, σελ. 40.

ίδρυση και οργάνωση ιδιαίτερων υπηρεσιών οι οποίες ασχολούνται αποκλειστικά με τη συλλογή, την αξιολόγηση, την επεξεργασία και τη διανομή πληροφοριών.

Η κατασκοπία, ελλείψει άλλων μέσων, ήταν η πρώτη μέθοδος η οποία χρησιμοποιήθηκε, και εξακολουθεί να χρησιμοποιείται ανελλιπώς, για τη συλλογή πληροφοριών. Η μέθοδος αυτή προϋποθέτει τη φυσική παρουσία κατασκόπων στην περιοχή ενδιαφέροντος, γεγονός που από μόνο του συνιστά έκθεση σε κίνδυνο, στην περίπτωση αποκάλυψής τους.

Η κατασκοπία στην αρχαιότητα αφορούσε αποκλειστικά τις στρατιωτικές αντιπαραθέσεις, διεξαγόμενη κατά βάση μεταξύ κρατικών οντοτήτων. Με την οικονομική πρόοδο που επήλθε και κυρίως με τη βιομηχανική επανάσταση, η κατασκοπία ως μέθοδος συλλογής χρήσιμων πληροφοριών επεκτάθηκε και μεταξύ των ιδιωτικών εταιρειών, όπου κυρίαρχο ρόλο διαδραμάτιζε το οικονομικό συμφέρον. Έτσι λοιπόν η κατασκοπία, εκτός της κλασσικής της μορφής, απέκτησε και οικονομική συνιστώσα με την εισαγωγή του όρου «βιομηχανική κατασκοπία».

Με την εξέλιξη της επιστήμης και της τεχνολογίας, και ειδικότερα της (μικρο)ηλεκτρονικής, εμφανίσθηκαν νέες μέθοδοι παρακολούθησης και συλλογής πληροφοριών, όπως η χρήση «κοριών» σε τηλεφωνικά δίκτυα και η παρακολούθηση των ασυρμάτων επικοινωνιών με σκοπό την υποκλοπή πληροφοριών. Ειδικότερα στο στρατιωτικό τομέα, η τεχνολογική αυτή εξέλιξη οδήγησε στην υπέρβαση της απλής συλλογής πληροφοριών, με ανάπτυξη δυνατοτήτων επηρεασμού του συστήματος λήψεως αποφάσεων του αντιπάλου με την εισαγωγή ψευδών πληροφοριών, μια τεχνική γνωστή ως παραπλάνηση (ενεργητικά μέτρα).

Η περαιτέρω εξέλιξη της τεχνολογίας οδήγησε στην ανακάλυψη του υπολογιστή, ο οποίος επιτάχυνε τις διαδικασίες επεξεργασίας των δεδομένων και επέτρεψε την αποθήκευση μεγάλου όγκου πληροφοριών σε ηλεκτρονικά μέσα. Όσο οι υπολογιστές ήταν αυτοδύναμοι, ο μόνος τρόπος υποκλοπής πληροφοριών ήταν η φυσική παρουσία στο χώρο όπου ήταν εγκατεστημένοι, η οποία αντιμετωπιζόταν με τη βελτίωση των μέτρων φυσικής ασφάλειας, οπότε οι μέθοδοι συλλογής πληροφοριών δεν άλλαξαν ουσιαστικά. Παρά την ανάπτυξη μεθόδων για την εξ αποστάσεως υποκλοπή πληροφοριών (για παράδειγμα η ανάγνωση της οθόνης του υπολογιστή από απόσταση μέχρι και 80 μέτρα) προϋπόθεση ήταν η φυσική παρουσία κατασκόπων στην περιοχή ενδιαφέροντος.

Τη δεκαετία του 1970 εμφανίσθηκαν στις ΗΠΑ τα πρώτα δίκτυα υπολογιστών, εισάγοντας μια ακόμη διάσταση στην ανθρώπινη δραστηριότητα, τον Κυβεροχώρο (Cyberspace) ή για να είμαστε πιο ακριβείς, πολλούς μικρούς Κυβερνοχώρους, κατ' αρχήν απομονωμένους μεταξύ τους. Όμως, η εποχή των δικτύων των υπολογιστών, και κατά συνέπεια της διασύνδεσης της ανθρώπινης γνώσης ήταν πραγματικότητα. Η διασύνδεση των υπολογιστών σε δίκτυα, έδινε (θεωρητικά) τη δυνατότητα σε κάθε υπολογιστή του δικτύου να έχει πρόσβαση σε όλες τις πληροφορίες που ήταν αποθηκευμένες στο δίκτυο, είτε τοπικά στους υπολογιστές του δικτύου, είτε στους διακομιστές του. Έτσι λοιπόν διευρύνθηκε ο κύκλος των σημείων από τα οποία θα μπορούσε κάποιος να υποκλέψει πληροφορίες. Θεωρητικά κάποιος θα μπορούσε από έναν υποσταθμό του δικτύου που βρισκόταν στην Ευρώπη να υποκλέπτει πληροφορίες που ήταν αποθηκευμένες σε στοιχεία του δικτύου που βρισκόταν στην Αμερική. Ακόμη χειρότερα, θα μπορούσε να παραποιήσει

τις αποθηκευμένες πληροφορίες, οδηγώντας έτσι το «στόχο» του στη λήψη αποφάσεων που βασιζόταν σε παραποιημένα στοιχεία.

Όσο όμως εξελισσόταν η τεχνολογία των υπολογιστών, τόσο αναπτύσσονταν τεχνικές υπονόμευσης των δικτύων. Εκτός της υποκλοπής πληροφοριών, ιδιαίτερη σημασία απέκτησε η υποβάθμιση ή ακόμη και η διακοπή της λειτουργίας των υπολογιστών ή/και των δικτύων με την εισαγωγή κακόβουλων προγραμμάτων. Η ενασχόληση με αυτού του είδους την παράνομη δραστηριότητα ξεκίνησε ως παιχνίδι από ανήσυχους έφηβους, οι οποίοι πολύ σύντομα ονομάσθηκαν χάκερ, άτομα με εξειδικευμένες γνώσεις στους υπολογιστές και «άρρωστο μυαλό», τα οποία ήθελαν να δοκιμάσουν τις δυνατότητές τους και τις αντοχές των συστημάτων-στόχων. Ταυτόχρονα άρχισε να αναπτύσσεται ο τομέας της ασφάλειας των υπολογιστικών συστημάτων και των δικτύων. Πολύ γρήγορα η κατάσταση εξελίχθηκε σε μια διελκυστίνδα μεταξύ των χάκερ και των προγραμματιστών του λογισμικού ασφαλείας, η οποία συνεχίζεται με αμείωτη ένταση μέχρι σήμερα, με τους δεύτερους να βρίσκονται πάντοτε ένα βήμα πίσω από τους πρώτους. Πολύ γρήγορα οι υπηρεσίες ασφαλείας των χωρών και διάφορες πολιτικές οργανώσεις (απελευθερωτικά και αυτονομιστικά κινήματα, τρομοκρατικές οργανώσεις, ακτιβιστές, κλπ) μπήκαν στο παιγνίδι.

Κομβικό σημείο στην εξέλιξη του θέματος αποτέλεσε η υλοποίηση και ευρεία διάδοση του διαδικτύου (Internet), η οποία με την επακόλουθη υλοποίηση της εφαρμογής του World Wide Web ή απλώς Web[2] και άλλων σχετικών εφαρμογών, επέτρεψε τη διασύνδεση υπηρεσιών και ατόμων. Το νέο εργαλείο επικοινωνίας έδωσε νέα διάσταση στην εξυπηρέτηση των πολιτών, απλοποιώντας και διευκολύνοντάς την. Οι κυβερνητικές υπηρεσίες και οι ιδιωτικές εταιρείες, εκμεταλλευόμενες την εξέλιξη της τεχνολογίας και υπό την απαίτηση των πολιτών για καλύτερη παροχή υπηρεσιών, συνδέθηκαν μαζικά στο διαδίκτυο παρέχοντας τις υπηρεσίες τους προς τους πολίτες μέσω αυτού.

Από τη στιγμή όμως της εγκατάστασης του διαδικτύου, άνοιξαν οι ασκοί του Αιόλου. Κάθε επί μέρους δίκτυο που συνδέεται στο διαδίκτυο, αποτελεί έναν δυνητικό στόχο ηλεκτρονικών επιθέσεων, από οποιοδήποτε σημείο του κόσμου. Έτσι, η κατάργηση των συνόρων της γνώσης, προκάλεσε ταυτόχρονα την έκθεση των υπολογιστικών συστημάτων στις ορέξεις του κάθε κακόβουλου και επιδέξιου χρήστη. Τα εργαλεία υποβάθμισης ή/και διακοπής της λειτουργίας των υπολογιστικών συστημάτων εξελίχθηκαν, με αποτέλεσμα την ανάπτυξη δυνατοτήτων επιθέσεων εναντίον της επικοινωνιακής και πληροφοριακής υποδομής διαφόρων χωρών, με καταστροφές υπολογιστών, δικτύων και μέσων αποθήκευσης δεδομένων, και παράλληλη ανάπτυξη σχετικών δογμάτων και πολιτικών. Η εποχή του Κυβερνοπολέμου είχε ήδη αρχίσει.

Όμως, η εξέλιξη στον τομέα της πληροφορικής συνεχίστηκε αμείωτη. Οι υπολογιστές εισέβαλαν σε κάθε μορφή της ανθρώπινης δραστηριότητας (δημόσιας και ιδιωτικής) και σήμερα συναντάμε τη χρήση τους, και μάλιστα σε διασυνδεδεμένη μορφή, στην οικονομία, την υγεία, την παιδεία, τη βιομηχανία, τις μεταφορές, την ενέργεια, τη διακυβέρνηση, κλπ., ήτοι σε όλες τις υποδομές μιας χώρας. Προοδευτικά, οι τεχνολογικά προηγμένες χώρες έφθασαν στο σημείο οι κρίσιμες υποδομές τους να εξαρτώνται από υπολογιστικά συστήματα και δίκτυα. Για λόγους εξυπηρέτησης του πολίτη, τηλεδιάγνωσης

---

[2] Το World Wide Web ξεκίνησε ως ένα έργο του ευρωπαϊκού ερευνητικού κέντρου CERN, με το κωδικό όνομα ENQUIRE, από τους επιστήμονες Tim Berners-Lee το 1989 και τον Robert Cailliau το 1990.

βλαβών, τηλεεργασίας, πολλές από τις υποδομές αυτές διασυνδέθηκαν με το διαδίκτυο, εκτιθέμενες έτσι σε ηλεκτρονικές επιθέσεις μέσω του διαδικτύου.

Συμπερασματικά, αυτό που σήμερα αποκαλείται Κυβερνοχώρος δημιουργήθηκε σταδιακά, χάρις στην εξέλιξη της επιστήμης και της τεχνολογίας, και αποτελείται από έναν ιστό διασυνδεδεμένων δικτύων στα οποία είναι αποθηκευμένες παντός είδους πληροφορίες και όπου συνδέονται, σε μικρότερο ή μεγαλύτερο βαθμό ανάλογα με την κατά περίπτωση χώρα, οι υποδομές των χωρών και μέσω του οποίου διεξάγεται προοδευτικά όλο και μεγαλύτερο μέρος της ανθρώπινης δραστηριότητας. Η οργάνωση και η λειτουργία του Κυβερνοχώρου, εξ αιτίας του τρόπου ανάπτυξής του και της απουσίας σχετικής ανώτατης ρυθμιστικής αρχής είναι χαοτική, επιτρέποντας έτσι τη δραστηριοποίηση ατόμων, πολιτικών ομάδων ή κρατών, τα οποία προβαίνουν σε ενέργειες παράνομης υποκλοπής πληροφοριών και επιβολής της θέλησής τους σε εν δυνάμει ανταγωνιστές ή αντιπάλους τους. Η προσπάθεια επιβολής της θέλησης του δράστη στον αντίπαλό του έχει χαρακτηριστεί πριν από 200 περίπου χρόνια από τον Clausewitz ως πόλεμος[3]. Δεδομένου όμως ότι το μέσον επιβολής που είχε στο μυαλό του ο μεγάλος Πρώσος θεωρητικός του πολέμου ήταν η στρατιωτική ισχύς, είναι επιβεβλημένη η διάκριση του πολέμου που διεξάγεται στον Κυβερνοχώρο με ηλεκτρονικά μέσα από τον κλασσικό πόλεμο, με την προσθήκη αναλόγου προθέματος. Το νέο είδος πολέμου, του οποίου σκοπός παραμένει η επιβολή της θελήσεως του ενός αντιπάλου στον άλλον (όπως στον κλασσικό πόλεμο), και τα μέσα διεξαγωγής του οποίου αντί της απειλής ή χρήσης στρατιωτικής βίας είναι η πληροφοριακή υποδομή, ονομάσθηκε Κυβερνοπόλεμος.

β. Απειλή

Η πρόοδος που παρουσίασε η τεχνολογία της πληροφορικής και η εκθετική αύξηση της χρήσης και του μεγέθους του διαδικτύου τις τελευταίες δύο δεκαετίες, έφεραν στο προσκήνιο μία νέα απειλή ασφαλείας, τις επιθέσεις μέσω ή εναντίον του Κυβερνοχώρου ή Κυβερνοεπιθέσεις. Όλες οι χώρες οι οποίες εξαρτώνται σε μεγάλο βαθμό από την πληροφοριακή υποδομή και τα δίκτυα υπολογιστών για τη λειτουργία των κρίσιμων υποδομών τους, όπως ο οικονομικός τομέας, η ενέργεια, οι τηλεπικοινωνίες, τα δίκτυα πετρελαίου και φυσικού αερίου, οι μεταφορές, τα δίκτυα ύδρευσης των πόλεων, οι υπηρεσίες εκτάκτων αναγκών και η ηλεκτρονική διακυβέρνηση, αντιμετωπίζουν αυτή την απειλή. Για μια χώρα, οι πιθανές επιπτώσεις των Κυβερνοεπιθέσεων είναι σοβαρές, από τη διατάραξη της καθημερινότητας των πολιτών της μέχρι την υπονόμευση της κυριαρχίας της.

Σε ένα άναρχο σύστημα όπως ο Κυβερνοχώρος, οι δράστες οι οποίοι επιδίδονται σε παράνομες δραστηριότητες, ομαδοποιούνται γενικώς σε κατηγορίες, κυρίως με βάση το σκοπό για τον οποίο δραστηριοποιούνται. Οι κατηγορίες των δραστών, κατά αυξανόμενο επίπεδο απειλής, είναι:

---

[3] Carl von Clausewitz, *On War*, Edited and Translated by M. Howard and Peter Paret, Princeton University Press, 1989, Book One "On the nature of war", Chapter One "What is war?", σελ. 75 ("War is an act of force to compel our enemy to do our will").

(1) Χάκερ (Hackers)

(2) Ακτιβιστές-χάκερ (Hactivists)

(3) Οργανωμένο έγκλημα

(4) Δράστες βιομηχανικής κατασκοπίας

(5) Εσωτερικοί δράστες

(6) Εξωτερικοί συνεργάτες/σύμβουλοι

(7) Τρομοκρατικές οργανώσεις

(8) Χώρες

Το μεγαλύτερο μέρος της δραστηριότητας που παρατηρείται σήμερα στον Κυβερνοχώρο ποικίλει από την απλή εισβολή σε ένα σύστημα και τον έλεγχό του για λόγους πρόκλησης και περιέργειας, μέχρι την εισβολή σε ένα σύστημα για λόγους εκδίκησης, κλοπής πληροφοριών, πρόκλησης, παρενόχλησης, υπεξαίρεσης χρημάτων ή πρόκλησης εσκεμμένης τοπικής βλάβης σε υπολογιστές ή καταστροφής μεγαλύτερης έκτασης σε υποδομές. Οι επιπτώσεις της κατηγορίας αυτής των Κυβερνοεπιθέσεων που εκδηλώνονται από χάκερ, ακτιβιστές χάκερ, το οργανωμένο έγκλημα, τη βιομηχανική κατασκοπία και τους εσωτερικούς δράστες, οι οποίες μπορεί να είναι ιδιαίτερα σοβαρές και δεν πρέπει να υποτιμώνται, χαρακτηρίζονται ως χάκινγκ, κυβερνοβλάβες, κλοπή, εκδίκηση, κατασκοπία, οργανωμένο έγκλημα και εμπίπτουν στη δικαιοδοσία της επιβολής του νόμου και της απονομής δικαιοσύνης[4] και δεν εξετάζονται στα πλαίσια της παρούσας μελέτης.

γ. Μέσα εκδήλωσης Κυβερνοεπιθέσεων[5]

Υπάρχουν δύο μέσα τα οποία μια χώρα, μια οργάνωση ή κάποιο άτομο θα μπορούσε να χρησιμοποιήσει για την εκδήλωση Κυβερνοεπιθέσεων εντός ή μέσω του Κυβερνοχώρου· ο υπολογιστής και τα κακόβουλα προγράμματα. Στη διεθνή βιβλιογραφία και αρθρογραφία, τα μέσα αυτά αποκαλούνται Κυβερνοόπλα (Cyber weapons).

(1) Υπολογιστής

Ο υπολογιστής αποτελεί σήμερα το βασικό εργαλείο με το οποίο σχεδιάζονται και από το οποίο εκδηλώνονται οι Κυβερνοεπιθέσεις. Στο πλαίσιο αυτό του ρόλου του, ο υπολογιστής μπορεί να χαρακτηριστεί ως όπλο διεξαγωγής Κυβερνοπολέμου (Κυβερνοόπλο). Μία συνηθισμένη περίπτωση χρήσης του υπολογιστή σήμερα είναι αυτή στην οποία ο έλεγχός του έχει αναληφθεί από άγνωστο άτομο με την εγκατάσταση κατάλληλου λογισμικού, έτσι ώστε να χρησιμοποιηθεί για την εκτόξευση επιθέσεων DDoS,

---

[4] Steven Hildreth, *Cyberwarfare*, CRS Report for (US) Congress, 19 June 2001, διαθέσιμο στην ιστοσελίδα http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL_30735_06192001.pdf (τελευταία επίσκεψη την 21 Ιαν 2010).

[5] Στο μη ειδικό τύπο παρατηρείται συνήθως μια σύγχυση μεταξύ των όρων «μέσα» και «τεχνικές». Για λόγους σαφήνειας και μόνο, στην παρούσα μελέτη μέσα θεωρούνται οι υπολογιστές, τα κακόβουλα προγράμματα, και τα «ειδικά κατασκευασμένα» υλικά ή ανταλλακτικά επικοινωνιακών και πληροφοριακών συστημάτων τα οποία χρησιμοποιούνται για την εκδήλωση μιας Κυβερνοεπίθεσης. Από τη άλλη πλευρά, τεχνικές θεωρούνται οι τρόποι χρήσης των μέσων για την επίτευξη του σκοπού μιας Κυβερνοεπίθεσης.

εν αγνοία του χειριστή του, για λόγους απόκρυψης της ταυτότητας του δράστη. Στην ορολογία του Κυβερνοπολέμου ένας τέτοιος υπολογιστής ονομάζεται zombie ή bot.

(2) Κακόβουλα προγράμματα (malware – malicious software)

Ο όρος κακόβουλα προγράμματα είναι ένας γενικός όρος ο οποίος αναφέρεται σε ενοχλητικό ή επιβλαβές λογισμικό (προγράμματα, δέσμες ενεργειών ή μακροεντολές) που έχει σχεδιαστεί για να μολύνει, να καταστρέψει, να τροποποιήσει ή να προκαλέσει άλλου είδους προβλήματα σε έναν υπολογιστή ή πρόγραμμα, χωρίς να το γνωρίζει ο ιδιοκτήτης του. Ο χαρακτηρισμός «κακόβουλο» αναφέρεται στην πρόθεση του δημιουργού του λογισμικού. Υπάρχουν διάφοροι τύποι κακόβουλων προγραμμάτων, το κάθε ένα με δικό του τρόπο λειτουργίας, όπως παρακάτω:

(α) Trojan Horse

(β) Worm

(γ) Keylogger

(δ) Sniffer

(ε) Spyware

δ. Τεχνικές Κυβερνοεπιθέσεων

Τα Κυβερνοόπλα που προαναφέρθηκαν μπορούν να χρησιμοποιηθούν σε διάφορους συνδυασμούς για να υλοποιήσουν μια ποικιλία τεχνικών προσβολής κάποιου στόχου. Η επιλογή της τεχνικής που θα χρησιμοποιηθεί για την προσβολή εξαρτάται από διάφορους παράγοντες, όπως οι δεξιότητες και η εμπειρία του χρήστη, οι δυνατότητες των όπλων, η φύση του στόχου και άλλους. Οι πλέον συνηθισμένες γνωστές τεχνικές Κυβερνοεπιθέσεων είναι οι ακόλουθες.

(1) Denial of Service (DoS) Attack[6]

(2) Backdoor

(3) E-mail spoofing

(4) IP Address spoofing

(5) Logic Bomb

(6) Digital manipulation (Παραποίηση δεδομένων)

ε. Σκοπός των Κυβερνοεπιθέσεων

Η χρήση των Κυβερνοόπλων και οι τεχνικές για την προσβολή διαφόρων στόχων δεν αποτελούν αυτοσκοπό. Οι Κυβερνοεπιθέσεις διεξάγονται για την επίτευξη κάποιου συγκεκριμένου σκοπού. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικώς όμως ανήκει σε μία από τις παρακάτω κατηγορίες:

---

[6] Στο κείμενο διατηρούνται οι αγγλικοί όροι δεδομένου ότι αφενός δεν υπάρχει επίσημη αντιστοίχηση ορολογίας, αφετέρου μια απλή μετάφραση θα έδινε φαιδρά αποτελέσματα.

(1) Εκμετάλλευση (exploitation)

Στην περίπτωση της εκμετάλλευσης βασικός στόχος του δράστη είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών που είναι συνδεδεμένες με αυτόν.

(2) Παραπλάνηση (deception)

Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις πληροφορίες τις οποίες αυτός συλλέγει, αναλύει ή παράγει, στοχεύοντας ουσιαστικά στο σύστημα λήψης αποφάσεων του αντιπάλου.

(3) Καταστροφή (destruction)

Στην περίπτωση της καταστροφής ο επιτιθέμενος, μέσω της χρήσης πληροφοριακών συστημάτων, καθιστά αδύνατη τη λειτουργία του στόχου, καταστρέφοντας τον ίδιο ή τα συστήματα υποστήριξης που είναι απαραίτητα για τη λειτουργία του. Στην περίπτωση αυτή πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου, αλλά η κρίσιμη υποδομή του. Το 2001, στην Αυστραλία συνελήφθη ένα άτομο το οποίο, χρησιμοποιώντας το διαδίκτυο, έναν ασύρματο και λογισμικό ελέγχου πέτυχε να αποδεσμεύσει 1 εκατομμύριο λίτρα λυμάτων στα νερά ενός ποταμού. Ο δράστης πέτυχε το στόχο του μετά από 44 αποτυχημένες προσπάθειες[7].

(4) Διακοπή λειτουργίας ή εξουδετέρωση (denial of service ή disruption)

Στην περίπτωση επιθέσεων διακοπής λειτουργίας (DoS) ή εξουδετέρωσης ο επιτιθέμενος δεν καταστρέφει το στόχο αλλά τον θέτει εκτός λειτουργίας ή τον καθιστά αναξιόπιστο για κάποια χρονική περίοδο, απαγορεύοντας στους νόμιμους χρήστες την εξυπηρέτησή τους ή την πρόσβαση σε πηγές πληροφοριών.

3. Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΕΘΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

α. Γιατί η χρήση Κυβερνοδυνατοτήτων συνιστά πόλεμο;

Ο Clausewitz στο έργο του «Περί Πολέμου», ορίζει τον πόλεμο ως «πράξη βίας με σκοπό την επιβολή της θέλησής μας στον εχθρό[8]», άποψη η οποία είναι σήμερα αποδεκτή από τη συντριπτική πλειονότητα των στρατηγικών αναλυτών. Από τη μελέτη του έργου του μεγάλου Πρώσου θεωρητικού του πολέμου προκύπτει ότι το μόνο μέσο που είχε στο μυαλό του για την επιβολή της θέλησης ήταν η στρατιωτική ισχύς του κράτους. Η θεώρηση αυτή δικαιολογείται πλήρως εάν λάβουμε υπόψη μας το κοινωνικοπολιτικό, πολιτισμικό και στρατιωτικό πλαίσιο που επικρατούσε στην εποχή του και μέσα στο οποίο αναπτύχθηκαν οι ιδέες του.

Όμως, η εξέλιξη της επιστήμης και της τεχνολογίας, καθώς επίσης και της δομής και του τρόπου λειτουργίας των σύγχρονων κρατών, δημιούργησε ευκαιρίες χρήσης

---

[7] Critical Infrastructure, Threats and Terrorism, US Army Training and Doctrine Command, 10 Aug 2006, διαθέσιμο στην ιστοσελίδα www.fas.org/irp/threat/terrorism/sup2.pdf (τελευταία επίσκεψη την 20 Ιαν 2010).

[8] Carl von Clausewitz, *On War*, Edited and Translated by M. Howard and Peter Paret, Princeton University Press, 1989, Book One "On the nature of war", Chapter One "What is war?", σελ. 75 ("War is an act of force to compel our enemy to do our will").

και άλλων μέσων για την επιβολή της θέλησής μας επί του αντιπάλου. Ένα από αυτά τα μέσα είναι οι Κυβερνοδυνατότητες, οι οποίες εξαιτίας των ιδιαίτερων χαρακτηριστικών τους αποτελούν οργανωμένες δυνατότητες προσβολής στόχων του αντιπάλου μέσω της επικοινωνιακής και πληροφοριακής του υποδομής (συμπεριλαμβανομένης και της ίδιας). Η ποικιλία των στόχων που μπορούν να προσβληθούν, η έκτασή τους, η ταχύτητα προσβολής τους και η σοβαρότητα των επιπτώσεων της προσβολής για τον αντίπαλο καθιστούν τον Κυβερνοπόλεμο ικανό να επηρεάσει τη θέληση του αντιπάλου, παθητικά (αποτροπή) ή ενεργητικά (πειθαναγκασμός). Κατά συνέπεια, η χρήση των Κυβερνοδυνατοτήτων πληροί τους όρους του ορισμού του πολέμου, όπως μας παραδόθηκε από τον Clausewitz, και έτσι η χρήση των Κυβερνοδυνατοτήτων επί ενός αντιπάλου για την επίτευξη πολιτικών σκοπών μπορεί να χαρακτηριστεί ως πόλεμος και ειδικότερα Κυβερνοπόλεμος[9]. Ενδεχομένως, με τις τεχνολογικές δυνατότητες που υφίστανται σήμερα, να μην μπορεί ακόμη να επιφέρει αποφασιστικά αποτελέσματα, λόγω και της μη διαθεσιμότητας κατάλληλων στόχων σε όλες τις χώρες, και ιδιαίτερα τις λιγότερο αναπτυγμένες (τουλάχιστον δεν έχει αναφερθεί ανάλογο περιστατικό), αλλά σίγουρα μπορεί να επηρεάσει τις αποφάσεις του αντιπάλου του που σχετίζονται με τα δικά του συμφέροντα. Κατά συνέπεια, στους παραδοσιακούς συντελεστές ισχύος του κράτους, πρέπει πλέον να προσθέσουμε και τις οργανωμένες Κυβερνοδυνατότητες προσβολής στόχων του αντιπάλου. Τα πλεονεκτήματα (οικονομικά, ηθικά, κλπ) έναντι της φυσικής καταστροφής είναι αυταπόδεικτα.

β. Σχέση του Κυβερνοπολέμου με την πολιτική

Σήμερα, οι αναλυτές των Διεθνών Σχέσεων και της Στρατηγικής θεωρούν ότι οι παράγοντες (ή συντελεστές) ισχύος ενός κράτους, οι οποίοι μπορούν να χρησιμοποιηθούν για την επιβολή της θέλησής του σε ενδεχόμενο αντίπαλο είναι τρεις: Η οικονομία, η διπλωματία και η στρατιωτική ισχύς. Πολλοί αναλυτές επιχειρηματολογούν υπέρ της συμπερίληψης των Πληροφοριών στους συντελεστές ισχύος του κράτους, ενώ ακόμη λιγότεροι είναι αυτοί που υποστηρίζουν ότι η ισχύς ενός κράτους αποτυπώνεται μόνο στην οικονομία του, οι δε άλλοι συντελεστές αποτελούν παράγωγα, μη δυνάμενοι να υπάρξουν χωρίς ισχυρή οικονομία. Από την άλλη πλευρά, υπάρχουν ορισμένοι αναλυτές οι οποίοι ισχυρίζονται ότι ο ρόλος της διπλωματίας είναι συντονιστικός και κατά συνέπεια δεν αποτελεί συντελεστή ισχύος. Αποδοχή συναντούν οι απόψεις του καθηγητή του πανεπιστημίου του Harvard των ΗΠΑ και Υφυπουργού Άμυνας στην κυβέρνηση του προέδρου των ΗΠΑ Bill Clinton, Joseph Nye, περί Ήπιας Ισχύος[10], η οποία όμως από μόνη της (σε αντίθεση με τους άλλους συντελεστές) δεν είναι ικανή να επιτύχει αποφασιστικά αποτελέσματα.

Οι κρατικές οντότητες, σε περίπτωση αντιπαράθεσης με άλλες κρατικές οντότητες ή οργανώσεις, για την επίτευξη των επιδιώξεών τους κινητοποιούν όλους τους παράγοντες ισχύος τους. Συνεπώς, η χρήση της στρατιωτικής ισχύος, η οποία παραπέμπει στη θερμή σύγκρουση, τις υλικές καταστροφές και τις απώλειες ανθρώπινης ζωής, είναι ένα μόνο από τα μέσα επίλυσης διακρατικών διαφορών, εκτός της οικονομίας και της

---

[9] Στα πλαίσια της παρούσας μελέτης ο όρος «πόλεμος» χρησιμοποιείται μόνο στην περίπτωση της θερμής σύγκρουσης, ενώ στην περίπτωση της χρήσης των άλλων συντελεστών ισχύος του κράτους για την επίλυση μιας κρίσης χρησιμοποιούνται οι όροι οικονομικός ή διπλωματικός πόλεμος, όπως επίσης και Κυβερνοπόλεμος.

[10] Joseph S. Nye Jr., *Ήπια Ισχύς*, Εκδόσεις Παπαζήση, 2005, (Η ήπια ισχύς είναι η ικανότητα να ελκύεις τους άλλους και να επηρεάζεις τη γνώμη τους).

διπλωματίας. Σύμφωνα με τις κρατούσες αντιλήψεις, η πλειονότητα των κρατών, για την επίλυση των διαφορών της, θα προσέφευγε στη χρήση της στρατιωτικής ισχύος αφού πρώτα είχε εξαντλήσει τα άλλα διαθέσιμα μέσα. Μάλιστα, η χρήση της οικονομίας και της διπλωματίας για την επιβολή της θέλησής μας στον αντίπαλο είναι τόσο συνηθισμένη που συνήθως διαλάθει της προσοχής.

Η ενορχήστρωση των διαθεσίμων μέσων τα οποία το κράτος έχει στη διάθεσή 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[11].

Συνεπώς, η χρήση του Κυβερνοπολέμου για την επίτευξη πολιτικών σκοπών πρέπει να σχεδιάζεται σε επίπεδο Υψηλής Στρατηγικής, ήτοι σε κυβερνητικό – πολιτικό επίπεδο. Η χρήση του όρου «πόλεμος» δεν πρέπει να μας παρασύρει έτσι ώστε να συσχετίζουμε τον Κυβερνοπόλεμο αποκλειστικά με τις Ένοπλες Δυνάμεις για δύο λόγους. Πρώτον, οι Κυβερνοδυνατότητες δεν αφορούν μόνο τις Ένοπλες Δυνάμεις αλλά διαπερνούν οριζόντια όλους του τομείς της κυβερνητικής δραστηριότητας. Δεύτερον, οι στόχοι (είτε για προστασία (δικοί μας) είτε για προσβολή (του αντιπάλου)) είναι κατά βάση μη στρατιωτικοί και κατά συνέπεια η προστασία ή/και η προσβολή τους θέτει ένα θέμα νομιμότητας (στο πλαίσιο του δικαίου του πολέμου) και κατά συνέπεια απαιτεί απόφαση σε υψηλό κυβερνητικό επίπεδο.

Συμπερασματικά, ο Κυβερνοπόλεμος αποτελεί ένα ακόμα μέσο (πλέον των τριών παραδοσιακών) στη διάθεση της κυβέρνησης ενός κράτους για την επίλυση μιας κρίσης.

γ. Σκοπός[12] του Κυβερνοπολέμου

Ο Κυβερνοπόλεμος δεν είναι αυτοσκοπός, αλλά διεξάγεται για την επίτευξη κάποιου συγκεκριμένου πολιτικού σκοπού ο οποίος προσδιορίζεται στα πλαίσια της Υψηλής Στρατηγικής από την εκάστοτε πολιτική ηγεσία της χώρας. Απαραίτητη προϋπόθεση για τη δυνατότητα του Κυβερνοπολέμου να επιτύχει την εκπλήρωση πολιτικών σκοπών είναι η συμβατότητα των σκοπών αυτών με τα ιδιαίτερα χαρακτηριστικά του Κυβερνοπολέμου. Για παράδειγμα, θα πρέπει να αποκλεισθεί ως σκοπός του Κυβερνοπολέμου η καταστροφή των Ενόπλων Δυνάμεων του εχθρού ή η κατάληψη εδάφους, αποστολές οι οποίες ανατίθενται σε ειδικά οργανωμένα και εξοπλισμένα τμήματα του κράτους, και συγκεκριμένα στις Ένοπλες Δυνάμεις.

Πολιτικοί σκοποί οι οποίοι θα μπορούσαν να επιτευχθούν χρησιμοποιώντας ως μέσο[13] τον Κυβερνοπόλεμο είναι οι παρακάτω:

---

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

[12] Στο πλαίσιο της μελέτης αυτής η σημασιολογική σχέση του σκοπού με τους στόχους είναι σχέση όλου και επιμέρους, γενικού και ειδικού. Σκοπός είναι η γενική επιδίωξη, στόχοι είναι οι επιμέρους εφαρμογές, τα στάδια που οδηγούν στην επίτευξη του γενικού σκοπού. Δηλαδή, οι στόχοι εξειδικεύουν και συγκεκριμενοποιούν σε διακεκριμένες φάσεις τη γενική έννοια του σκοπού, Γ. Μπαμπινιώτης, Λεξικό της νέας ελληνικής γλώσσας.

[13] Για λόγους ακριβείας, και στο πλαίσιο εργασίας Σκοπός-Μέσα-Τρόποι, θα πρέπει να διευκρινίσουμε ότι για την επίτευξη του πολιτικού Σκοπού του πολέμου, το Μέσο είναι οι

- Η απλή παρενόχληση με σκοπό την υπενθύμιση των δυνατοτήτων στον αντίπαλο (αυτό που στα πλαίσια του κλασσικού πολέμου θα ονομάζαμε επίδειξη δύναμης (Show of force)).
- Η έμμεση προειδοποίηση του ενδιαφερομένου μέρους πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών για τους κινδύνους που διατρέχει αν αρνηθεί τη θετική ψήφο. Ένα κλασικό παράδειγμα, αν και δεν αφορά τον Κυβερνοπόλεμο, είναι η αύξηση των επεισοδίων στο Αιγαίο πριν τις αποφάσεις της Ευρωπαϊκής Ένωσης όσον αφορά στην ένταξη της Τουρκίας στην Ευρωπαϊκή Ένωση, εις βάρος της Ελλάδος.
- Η εκδίκηση για τυχόν αποφάσεις που ελήφθησαν χωρίς να ληφθούν υπόψη τα συμφέροντα της ενδιαφερόμενης χώρας, όπως θα μπορούσε να ήταν η άρνηση θετικής ψήφου σε διεθνή οργανισμό. Αυτό λειτουργεί επίσης και ως προειδοποίηση για μελλοντικές ενέργειες. Το κλασσικό πλέον παράδειγμα είναι οι Κυβερνοεπίθεση που δέχθηκε η Εσθονία μετά την απομάκρυνση ενός μνημείου του Β' Παγκοσμίου Πολέμου από το κέντρο του Ταλλίν. Αν και δεν έχει αποδειχθεί, εκτιμάται ότι δράστες των Κυβερνοεπιθέσεων ήταν η ρωσική μειονότητα της Εσθονίας και η Ρωσία.

δ. Στόχοι του Κυβερνοπολέμου

(1) Γενικά

Όπως προαναφέρθηκε, ο Κυβερνοπόλεμος μπορεί να αποτελέσει ένα μέσο για την επίτευξη του πολιτικού σκοπού του πολέμου. Η χρήση του Κυβερνοπολέμου ως μέσου επίτευξης κάποιου σκοπού, προϋποθέτει την εκδήλωση Κυβερνοεπιθέσεων εναντίον στόχων, των οποίων η συντονισμένη προσβολή θα συμβάλει τελικά στην επίτευξη του εν λόγω σκοπού. Οι στόχοι αυτοί, η προσβολή των οποίων επιφέρει αποφασιστικό αποτέλεσμα στην εξέλιξη της αντιπαράθεσης, σχετίζονται με τις υποδομές της χώρας στόχου, και μάλιστα με τις κρίσιμες, στο μέτρο που αυτές είναι προσβάσιμες στους δράστες των Κυβερνοεπιθέσεων. Συνεπώς, οι προσβάσιμες κρίσιμες υποδομές μιας χώρας αποτελούν το γενικό στόχο του Κυβερνοπολέμου.

(2) Κρίσιμες υποδομές[14]

Τα σύγχρονα κράτη, καθώς αναπτύσσονται αυξάνουν τη 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. Η προσβολή τους μπορεί να παραλύσει την κοινωνία, χωρίς να είναι απαραίτητη η φυσική καταστροφή τους. Σε πολλές περιπτώσεις, ουσιαστική παράλυση μπορεί να επιτευχθεί με πολύ φθηνότερα

Κυβερνοδυνατότητες, ενώ ο τρόπος χρήσης τους είναι η προστασία των φιλίων συστημάτων και η προσβολή των αντίστοιχων εχθρικών (Κυβερνοπόλεμος).

[14] Κρίσιμες υποδομές είναι οι φυσικές και ηλεκτρονικές υποδομές που είναι απαραίτητες για τη διασφάλιση των βασικών λειτουργιών του κράτους.

(ηλεκτρονικά) μέσα. Σήμερα, είναι πλέον δυνατή η δημιουργία χάους χωρίς αιματοκύλισμα, διακοπής λειτουργίας χωρίς φυσική καταστροφή.

Οι Κυβερνοεπιθέσεις εναντίον των υποδομών μιας χώρας έχουν πραγματικές, προφανείς και μακροχρόνιες επιπτώσεις. Ως τέτοιες, μπορούν να έχουν ως απώτερο στόχο την τρομοκράτηση του λαού και τον εξαναγκασμό του να αποσύρει την υποστήριξή του στον πόλεμο[15] ή την πρόκληση ζημιών σε έκταση που να αναγκάσει την κυβέρνηση να επανεκτιμήσει το ρίσκο που ανέλαβε με την προσφυγή στον πόλεμο. Μια παρατεταμένη διακοπή της παραγωγής και διανομής ηλεκτρικής ενέργειας θα είχε σοβαρές επιπτώσεις στο σύστημα υγείας. Αποτυχία των υπηρεσιών έκτακτης ανάγκης στις μεγάλες πόλεις δεν θα προκαλούσε μόνο το θάνατο αυτών που θα χρειαζόντουσαν αυτές τις υπηρεσίες, αλλά και την απώλεια της εμπιστοσύνης των πολιτών στη δυνατότητα της κυβέρνησης να παράσχει βασικές υπηρεσίες και προστασία στους πολίτες της. Όσο θα γινόταν γνωστό ότι οι Κυβερνοεπιθέσεις έχουν επιπτώσεις και σε άλλες υποδομές, όπως οι επικοινωνίες, οι μεταφορές και το νερό, τα επίπεδα του φόβου και απώλειας εμπιστοσύνης θα άρχιζαν να έχουν επιπτώσεις στο βασικό κοινωνικό ιστό. Από την άλλη πλευρά, οι Κυβερνοεπιθέσεις εναντίον της οικονομικής υποδομής υποσκάπτουν τη δυνατότητα των επιχειρήσεων να λειτουργούν κανονικά και εγείρει ερωτήματα μεταξύ των πολιτών σχετικά με την ασφάλεια των προσωπικών τους οικονομικών, συμπεριλαμβανομένων των συντάξεων, των μικροεπενδύσεων και των αποταμιεύσεων.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι κρίσιμες υποδομές που διασυνδέονται με το διαδίκτυο μέσω των Συστημάτων Βιομηχανικού Ελέγχου ICS[16] (Industrial Control Systems), λόγω της ευκολίας πρόσβασης και κατά συνέπεια προσβολής τους. Τα συστήματα ICS για βιομηχανικές εγκαταστάσεις, συστήματα διανομής ζωτικών αγαθών (ηλεκτρικό ρεύμα, νερό, καύσιμα κλπ) και συστήματα μεταφορών και κίνησης (σιδηρόδρομοι, συστήματα διαχείρισης κίνησης, ταχυδρομικές υπηρεσίες, κλπ) τα οποία μέχρι πριν λίγα χρόνια ήταν αδιανόητα, υλοποιήθηκαν με τη βοήθεια της προηγμένης τεχνολογίας των επικοινωνιών και της πληροφορικής. 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. Αισθητήρες, μηχανές και διακόπτες σήμερα όλο και συχνότερα διαθέτουν τις δικές τους διευθύνσεις IP και χρησιμοποιούν το πρωτόκολλο του διαδικτύου (IP) για σκοπούς επικοινωνίας. Το γεγονός αυτό εξέθεσε τα συστήματα ICS στους κινδύνους από το διαδίκτυο· κακόβουλα προγράμματα και χάκερ. Οι επιθέσεις σε τέτοια συστήματα προκαλούν προβλήματα στην ομαλή λειτουργία των ελεγχόμενων συστημάτων και τελικά χάος.

---

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

[16] Ο όρος ICS είναι ο γενικός όρος 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.

(3) Στοχοποίηση των κρίσιμων υποδομών

Για να αποκτηθεί μια εικόνα των υποδομών μιας χώρας, απαιτείται η χαρτογράφησή τους, μια διαδικασία η οποία δεν αποτελεί προνομιακό πεδίο του Κυβερνοπολέμου[17]. Έτσι λοιπόν προκύπτει ένας χάρτης πληροφοριών των υποδομών των πιθανών αντιπάλων, κατά το αντίστοιχο του χάρτη πληροφοριών της διάταξης μάχης του εχθρού που χρησιμοποιούν οι Ένοπλες Δυνάμεις.

Η απλή χαρτογράφηση των υποδομών, δημοσίων και ιδιωτικών, του πιθανού αντιπάλου δεν είναι ιδιαίτερα δύσκολη, δεδομένου ότι τα σχετικά στοιχεία μπορούν να συγκεντρωθούν σχετικά εύκολα μέσω ανοικτών πηγών. Δεν είναι όμως κάθε υποδομή εκμεταλλεύσιμη από την άποψη της δυνατότητας υποβάθμισης ή διακοπής της λειτουργίας της. Η τρωτότητά της σχετίζεται άμεσα με τα διαθέσιμα μέσα και την καταλληλότητά τους για την προσβολή της. Συνεπώς, η απλή καταγραφή των υποδομών του κάθε πιθανού αντιπάλου αποτελεί την αφετηρία για τη σύνταξη της λίστας των ενδεχόμενων στόχων. Μια υποδομή η οποία δεν υποστηρίζεται από κανένα σύστημα επικοινωνιών - πληροφορικής δεν παρουσιάζει ενδιαφέρον από πλευράς Κυβερνοπολέμου, και κατά συνέπεια δεν έχει καμία έννοια να περιληφθεί στη λίστα των στόχων του, η οποία έτσι περιορίζεται σε μία η οποία περιλαμβάνει μόνο τις εκμεταλλεύσιμες υποδομές. Οίκοθεν νοείται ότι οι σχετικές λίστες στόχων είναι δύο: Η μία των δικών μας υποδομών για λόγους προστασίας (αμυντικό σκέλος) και η άλλη που αφορά στον πιθανό αντίπαλο, για λόγους προσβολής (επιθετικό σκέλος).

Το επόμενο στάδιο της διαδικασίας συγκρότησης της λίστας των στόχων του Κυβερνοπολέμου είναι η ιεράρχησή της. Η ιεράρχηση της λίστας επιβάλλεται για λόγους ανεπάρκειας των μέσων σε σχέση με τους στόχους ή, στην περίπτωση της επάρκειας, της προτεραιότητας προσβολής τους. Η ιεράρχηση της λίστας των στόχων γίνεται με βάση συγκεκριμένα κριτήρια, τα οποία μεταβάλλονται ανάλογα με τη φάση στην οποία βρίσκεται η αντιπαράθεση. Για παράδειγμα, πριν την αποκάλυψη της κρίσης οι αμιγώς οικονομικοί στόχοι έχουν προτεραιότητα, την περίοδο της κινητοποίησης πριν τη θερμή σύγκρουση η έμφαση δίνεται στις συγκοινωνίες και τα συστήματα συντονισμού του κρατικού μηχανισμού, ενώ κατά τη διάρκεια της θερμής σύγκρουσης στοχοποιούνται κατά προτεραιότητα αδυναμίες που σχετίζονται με τις υποδομές των Ενόπλων Δυνάμεων. Βέβαια, η διάκριση αυτή δεν είναι απόλυτη. Για παράδειγμα. ενώ ένα φράγμα δεν σχετίζεται άμεσα με τις Ένοπλες Δυνάμεις, αν η καταστροφή του πρόκειται να παρεμποδίσει τις συγκοινωνίες στρατηγικής σημασίας, τότε αποκτά ανάλογο ενδιαφέρον. Συνεπώς, η ιεράρχηση των κρίσιμων υποδομών του αντιπάλου είναι μια δυναμική διαδικασία η οποία εξαρτάται από τη γενική εκτίμηση της καταστάσεως και το χρονικό σημείο της αντιπαράθεσης.

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

- Πληροφορικής και επικοινωνιών (δημοσίων και ιδιωτικών)

---

[17] Από την άλλη πλευρά, ούτε η προσβολή των υποδομών αποτελεί προνομιακό πεδίο του Κυβερνοπολέμου, αλλά αποτελεί σταθερή επιδίωξη, για την επίτευξη της οποίας διατίθεται κάθε διαθέσιμη κατάλληλη δυνατότητα που μπορεί να συμβάλει στην υποβάθμιση ή τη διακοπή της λειτουργίας τους, με βάση ένα γενικό σχέδιο διαχείρισης της κρίσης.

- Οικονομικών υπηρεσιών
- Συστήματος παραγωγής και διάθεσης ηλεκτρικής ισχύος
- Συστήματος παραγωγής, αποθήκευσης και διανομής καυσίμων και φυσικού αερίου
- Συγκοινωνιών (οδικών, σιδηροδρομικών, αεροπορικών, θαλασσίων, ποταμίων)
- Υδατίνων πόρων
- Εξυπηρέτησης πολιτών
- Παροχής υγειονομικών υπηρεσιών

Μετά την προηγηθείσα ανάλυση, η αποστολή του Κυβερνοπολέμου μπορεί να ορισθεί ως η προστασία των κρίσιμων υποδομών του κράτους μέσω της προστασίας[18] όλων των δικτυοκεντρικών συστημάτων, δημόσιων και ιδιωτικών, από ενδεχόμενες επιθέσεις που θα είχαν ως στόχο την υποβάθμιση της λειτουργίας τους και την πρόκληση λειτουργικών ή φυσικών βλαβών, και η πρόκληση αντιστοίχων αποτελεσμάτων στον αντίπαλο, στα πλαίσια της χαραχθείσας εθνικής στρατηγικής ασφαλείας.

(4) Τα επικοινωνιακά και πληροφοριακά συστήματα και το διαδίκτυο ως στόχοι

Στόχο θα μπορούσαν επίσης να αποτελέσουν τα επί μέρους επικοινωνιακά και πληροφοριακά δίκτυα, στα οποία είναι αποθηκευμένες διάφορες πληροφορίες, ή και το ίδιο το διαδίκτυο ως σύνολο. Η προσβολή των επί μέρους δικτύων και του διαδικτύου δεν φαίνεται πιθανή, εξαιτίας του γεγονότος ότι αυτό χρησιμοποιείται από ολόκληρο τον κόσμο και κατά συνέπεια και από τους ενδεχόμενους αντιπάλους. Πιθανή προσβολή και υποβάθμιση ή και διακοπή της λειτουργίας του θα είχε επιπτώσεις ακόμη και στον ίδιο τον επιτιθέμενο, αλλά, κυρίως σε τρίτες χώρες, προκαλώντας τη δυσαρέσκειά τους και ενδεχομένως απρόβλεπτες αντιδράσεις από μέρους τους.

Από την άλλη πλευρά, το διαδίκτυο ως σύνολο είναι σχεδόν αδύνατο να προσβληθεί. Ο κορμός του είναι ανθεκτικός λόγω του μεγέθους του και της δομής του, η οποία παρουσιάζει έναν εγγενή πλεονασμό, ο οποίος λειτουργεί ως ασπίδα προστασίας του. Η μέχρι σήμερα εμπειρία έχει αποδείξει ότι η αναδρομολόγηση της κίνησης του διαδικτύου μέσω εναλλακτικών κόμβων, για την αντιμετώπιση προβλημάτων δρομολόγησης της κίνησης, είναι εφικτή. Η χαοτική και χωρίς καμία λογική δομή του διαδικτύου, δεν επιτρέπει επίσης τη συστηματική μελέτη της ανάλυσης της κίνησης στο διαδίκτυο, μέσω της οποίας θα προέκυπτε η σχετική αξία των κόμβων του και με βάση αυτή η κατάρτιση σεναρίων καταστροφής του. Οι δυνατότητες αυτόματης αναδρομολόγησης της κίνησης του διαδικτύου είναι τόσες πολλές, που κάθε προσπάθεια διακοπής της λειτουργίας του μέσω της καταστροφής διακομιστών, είναι πραγματική ουτοπία.

Όμως το διαδίκτυο σήμερα μπορεί να μην είναι τόσο ανθεκτικό όσο πιστεύουν ορισμένοι ειδικοί, δεδομένης της τάσης για οργάνωση κεντρικών hub του

[18] Ως προστασία γενικώς νοείται η ελαχιστοποίηση τυχόν διακοπών, ο περιορισμός της συχνότητας εμφάνισής τους, η αντιμετώπισή τους, ο γεωγραφικός τους περιορισμός και η ελαχιστοποίηση των επιπτώσεων τους.

δικτύου με σκοπό τον καλύτερο έλεγχο της φυσικής του υποδομής. Ένας τρόπος προσβολής του διαδικτύου ως συνόλου, ο οποίος έχει χρησιμοποιηθεί στο παρελθόν, είναι η προσβολή των διακομιστών DNS (Domain Name Servers). Οι διακομιστές DNS είναι αυτοί που μεταφράζουν τις διευθύνσεις του διαδικτύου τύπου www.name.com, σε διευθύνσεις πρωτοκόλλου διαδικτύου IP (αριθμητικές). Οι διακομιστές DNS, 13[19] συνολικά για ολόκληρο το διαδίκτυο, παρέχουν υπηρεσίες σε όλους τους χρήστες, και έτσι κάθε επίθεση εναντίον τους υποδηλώνει προσπάθεια διακοπής λειτουργίας ολόκληρου του διαδικτύου. Από τις επιθέσεις DDoS εναντίον των διακομιστών DNS του διαδικτύου, ξεχωρίζουν δύο· η μία της 21 Οκτ 2002[20] και η δεύτερη της 6 Φεβ 2007[21]. Οι επιθέσεις αυτές ήταν διαφορετικές τόσο σε έκταση όσο και στο σκοπό τους, επειδή η επίθεση εκδηλώθηκε ταυτόχρονα εναντίον όλων των διακομιστών. Οι δράστες και τα κίνητρα των επιθέσεων είναι άγνωστα. Την 21 Οκτ 2002 διακόπηκε η λειτουργία των 9 από τους 13 διακομιστές, ενώ την 6 Φεβ του 2007 διακόπηκε η λειτουργία 2 μόνο διακομιστών DNS.

ε. Κυβερνοπόλεμος και τρομοκρατία

Οι τρομοκρατικές οργανώσεις χρησιμοποιούν σήμερα τον Κυβερνοχώρο για την επικοινωνία και την ανταλλαγή πληροφοριών, την επαφή με τους οπαδούς τους, τη συγκέντρωση χρημάτων, νόμιμη ή παράνομη, την οργάνωση και το συντονισμό των επιχειρήσεών τους, την απόκτηση παράνομων διαβατηρίων και VISA, τον προσηλυτισμό και τη συλλογή πληροφοριών.

Οι επικοινωνίες και η ανταλλαγή πληροφοριών των τρομοκρατικών οργανώσεων εξυπηρετείται εξαιρετικά από το διαδίκτυο. Εξειδικευμένες ιστοσελίδες μπορούν να δημιουργηθούν και να αντικατασταθούν μόλις εντοπισθούν, διαβρωθούν ή μπλοκαριστούν από κυβερνήσεις. Τα μέλη των οργανώσεων ή οι οπαδοί τους μπορούν να χρησιμοποιούν αυτές τις ιστοσελίδες για σκοπούς ανταλλαγής μηνυμάτων ή ενημέρωσης σχετικά με τις εξελίξεις στα θέατρα των επιχειρήσεων του Αφγανιστάν, του Πακιστάν, του Ιράκ κλπ.

Το διαδίκτυο επίσης αποτελεί πηγή τεχνικών πληροφοριών κάθε είδους για όπλα και οπλικά συστήματα, τρόπους κατασκευής εκρηκτικών μηχανισμών, κάλυψη και οργάνωση ενεδρών και άλλες τεχνικές.

Το διαδίκτυο αποτελεί σήμερα ένα παγκόσμιο θέατρο επιχειρήσεων για τις τρομοκρατικές οργανώσεις και τις δυνάμεις ασφαλείας των χωρών. Όμως το ίδιο το διαδίκτυο δεν αποτελεί στόχο και δεν φαίνεται να υπάρχει προς το παρόν καμία «ηλεκτρονική» τρομοκρατική οργάνωση η οποία θα εξαπέλυε μια Κυβερνοεπίθεση στο διαδίκτυο με στόχο τη διακοπή της λειτουργίας του και την καταστροφή του. Τρεις είναι οι παράγοντες οι οποίοι καθιστούν τις Κυβερνοεπιθέσεις στο ίδιο το διαδίκτυο λιγότερο ελκυστικές για τις τρομοκρατικές οργανώσεις[22].

---

[19] Οι 9 διακομιστές είναι εγκατεστημένοι στις ΗΠΑ, ενώ οι άλλοι τέσσερις στην Ιαπωνία, τη Σουηδία, την Ολλανδία και τη Μ. Βρετανία, Factsheet, Root Server Attack on 6 Feb 2007, 1 Mar 2007, διαθέσιμο στη ιστοσελίδα www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf (τελευταία επίσκεψη την 11 Φεβ 2010).

[20] Στο ίδιο.

[21] Στο ίδιο.

[22] *Cyber Warfare*, Johns Hopkins Model United Nations Conference XII, March 5-8, 2009, Baltimore, Maryland, US.

- Τα Κυβερνοόπλα είναι λιγότερο αποτελεσματικά σε σχέση με άλλες δυνατότητες, από την άποψη ότι δεν έχουν τις ίδιες ψυχολογικές ή πολιτικές επιπτώσεις και δεν έχουν νεκρούς.
- Η πολυπλοκότητα των Κυβερνοεπιθέσεων στις κρίσιμες υποδομές έχει μικρότερες πιθανότητες επιτυχίας
- Το διαδίκτυο εξυπηρετεί και τους δικούς τους σκοπούς.

Όσο όμως οι τεχνικές και οι τακτικές του Κυβερνοπολέμου εξελίσσονται, και η καταστροφή κρίσιμων υποδομών των χωρών γίνεται πιο εφικτή, δεν είναι μακριά ο χρόνος που οι τρομοκρατικές οργανώσεις θα στρατολογήσουν ειδικούς στον Κυβερνοπόλεμο και θα οργανώσουν κτυπήματα, τα οποία, μπορεί μεν να μην έχουν τα θύματα της επίθεσης στους δίδυμους πύργους, αλλά θα προκαλέσουν οικονομικές καταστροφές μεγάλης έκτασης.

ζ. Ολοκληρωτικός και περιορισμένος Κυβερνοπόλεμος

Οι έννοιες του ολοκληρωτικού και του περιορισμένου Κυβερνοπολέμου αναφέρονται στον κλασικό πόλεμο. Στον ολοκληρωτικό πόλεμο επιδιώκεται η ολοκληρωτική ήττα του αντιπάλου με τον εξαναγκασμό του σε συνθηκολόγηση άνευ όρων (όπως η Γερμανία στο Β' Παγκόσμιο Πόλεμο), ενώ στον περιορισμένο πόλεμο οι αντιμαχόμενοι, και κατά βάση ο επιτιθέμενος, θέτουν περιορισμούς στον πολιτικό σκοπό του πολέμου και κατά συνέπεια στα μέσα που θα χρησιμοποιήσουν και στο γεωγραφικό χώρο διεξαγωγής των επιχειρήσεων (όπως η περίπτωση του πολέμου των νήσων Malvinas ή Falkland). Ένα βασικό θέμα που αντιμετωπίζεται στην περίπτωση αυτή είναι αυτό της κλιμάκωσης του περιορισμένου πολέμου σε ολοκληρωτικό.

Ας δούμε όμως πώς οι έννοιες αυτές μεταφέρονται στο πεδίο του Κυβερνοπολέμου. Είναι γενικώς παραδεκτό σήμερα ότι είναι αδύνατον η άνευ περιορισμών προσβολή όλων των τρωτών σημείων της υποδομής μιας χώρας να προκαλέσει την άνευ όρων συνθηκολόγησή της. Βέβαια δεν υπάρχει ανάλογο προηγούμενο για να είναι δυνατή η επιβεβαίωση ή απόρριψη της συγκεκριμένης άποψης. Κατά συνέπεια, η έννοια του ολοκληρωτικού Κυβερνοπολέμου μπορεί μεν να έχει εφαρμογή στην προσπάθεια επίτευξης αποφασιστικού αποτελέσματος, αλλά δεν ισχύει όσον αφορά στο τελικό αποτέλεσμα. Αντίθετα, η επιλογή πολιτικών σκοπών πλην της πλήρους υποταγής του αντιπάλου, είναι μια εφικτή επιλογή για τον Κυβερνοπόλεμο και είναι δυνατόν να επιτύχει αποτελέσματα. Γενικώς όμως, η επίτευξη αποφασιστικών αποτελεσμάτων, όπως και στην περίπτωση του οικονομικού πολέμου, μπορεί να επιτευχθεί μόνον όταν οι επιχειρήσεις του Κυβερνοπολέμου συνδυάζονται με επιχειρήσεις του παραδοσιακού πολέμου, οπότε τα αποτελέσματα είναι χειροπιαστά, άμεσα και ιδιαίτερα καταστροφικά, επηρεάζοντας το θυμικό του λαού και υποσκάπτοντας έτσι τη θέλησή του για την υποστήριξη της υπόθεσης του πολέμου.

Στην περίπτωση του κλασικού πολέμου, η προσφυγή στον περιορισμένο πόλεμο έχει ως στόχο συνήθως την κατάληψη εδάφους, η οποία μπορεί να έχει μόνιμο χαρακτήρα ή να χρησιμοποιηθεί για διαπραγματευτικούς σκοπούς. Εφόσον όμως στην περίπτωση του Κυβερνοπολέμου δεν είναι εφικτός ένας τέτοιος αντικειμενικός σκοπός, τότε για ποιο λόγο θα επιλεγόταν η προσφυγή σε αυτό το είδος του πολέμου; Η επιλογή

του περιορισμένου Κυβερνοπολέμου θα μπορούσε να υπηρετήσει τους παρακάτω σκοπούς:

- Επίδειξη δύναμης
- Εκφοβισμό πριν τη λήψη αποφάσεων που σχετίζονται με τη χώρα – δράστη
- Εκδίκηση για αποφάσεις της χώρας θύματος που λήφθηκαν και επηρεάζουν αρνητικά τη χώρα – δράστη.
- Προληπτικά για την αποφυγή της διατάραξης της ισορροπίας ισχύος

Στις άλλες περιπτώσεις, δεδομένου ότι ο δράστης μάλλον επιδιώκει την αποκάλυψη της ταυτότητάς του, έστω και αν δεν τη διαφημίζει ο ίδιος, η αντίδραση σε επίπεδο Κυβερνοπολέμου είναι μάλλον πιθανή[23]. Η ανταπόδοση των Κυβερνοεπιθέσεων είναι πιθανόν να οδηγήσει σε κλιμάκωση και τελικά σε γενίκευση του Κυβερνοπολέμου μεταξύ των δύο αντιπάλων, ήτοι σε ολοκληρωτικό Κυβερνοπόλεμο. Οι επιπτώσεις των Κυβερνοεπιθέσεων στον αντίπαλο εξαρτώνται από το βαθμό ανάπτυξής του και το βαθμό διείσδυσης της πληροφορικής τεχνολογίας στο διοικητικό μηχανισμό, τη βιομηχανία, το εμπόριο κλπ. Η κατάσταση αυτή είναι πιθανό να οδηγήσει σε αδιέξοδο και σε ενδεχόμενη συμφωνία διακοπής των επιχειρήσεων Κυβερνοπολέμου. Δεν είναι όμως απίθανο να οδηγήσει το ένα από τα δύο μέρη, ενδεχομένως αυτό που υφίσταται τις σοβαρότερες συνέπειες, να προσφύγει στον παραδοσιακό πόλεμο για την οριστική επίλυση της κρίσης.

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

η. Κυβερνοπόλεμος και παγκοσμιοποίηση

Η παγκοσμιοποίηση είναι ένας όρος ο οποίος εμφανίσθηκε στο παγκόσμιο λεξικό τα τελευταία χρόνια και αποτέλεσε το «κόκκινο πανί» για ένα μεγάλο μέρος των πολιτικών ακτιβιστών. Σύμφωνα με τον καθηγητή Μπαμπινιώτη, παγκοσμιοποίηση είναι «η δημιουργία μιας παγκόσμιας οικονομικής ζώνης, παγκόσμιας αγοράς, όπου τα προϊόντα θα κινούνται ελεύθερα· η μετατροπή της οικουμένης σε μια ενιαία οικονομική, πολιτική και πολιτιστική επικράτεια[24]».

Όμως, αυτή είναι μια διαδικασία η οποία άρχισε την επαύριο της εμφάνισης του ανθρώπου στη γη, και η οποία δεν επιβλήθηκε από καμία «περίεργη» δύναμη, αλλά από το χαρακτήρα του ανθρώπου ως κοινωνικού όντος και την ανάγκη του για επιβίωση. Έτσι, οι πρώτες πρωτόγονες κοινωνίες με την πάροδο του χρόνου σταδιακά ομαδοποιήθηκαν και δημιούργησαν ευρύτερες κοινωνικές ομάδες. Όσο τα μέσα

---

[23] Παρόλα αυτά, η Εσθονία, η οποία κατηγόρησε ως υποκινητή των Κυβερνοεπιθέσεων που δέχθηκε τον Απρίλιο Μάιο του 2007 τη Ρωσία, δεν αντέδρασε επιθετικά, ενδεχομένως διότι υπέστη στρατηγικό αιφνιδιασμό και δεν ήταν προετοιμασμένη να αντιδράσει. Εξάλλου αυτό ήταν και το πρώτο επεισόδιο αυτού του είδους. Βέβαια, έστω και αν ήταν προετοιμασμένη να αντιδράσει, η ανάληψη ενός τέτοιου εγχειρήματος εναντίον μιας χώρας της οποίας οι Κυβερνοδυνατότητες έχουν τόσο διαφημιστεί (από τις ΗΠΑ) είναι άλλο θέμα.

[24] Γ. Μπαμπινιώτης, *Λεξικό της νέας ελληνικής γλώσσας*, Εκδόσεις Κέντρο Λεξικολογίας ΕΠΕ, Αθήνα, Ιαν 2002.

επικοινωνίας βελτιωνόταν, τόσο οι επαφές μεταξύ των μέχρι τότε απομονωμένων κοινωνιών αυξανόταν, δημιουργώντας έτσι ένα πλέγμα οικονομικών, πολιτισμικών και άλλων δεσμών και κατά συνέπεια αυξάνοντας συνεχώς το βαθμό αλληλεξάρτησης μεταξύ τους. Η αύξηση αυτού του βαθμού αλληλεξάρτησης, σε σχέση με το χρόνο, ήταν εκθετική. Συμπερασματικά, μπορούμε να πούμε ότι η παγκοσμιοποίηση είναι η φυσική τάση εξέλιξης της παγκόσμιας κοινωνίας. Η με κάθε τρόπο, γλωσσικό, πολιτισμικό ή οικονομικό, ομογενοποίηση της κοινωνίας μας φαίνεται να είναι αναπόφευκτη[25].

Η τεχνολογική ανάπτυξη των τελευταίων χρόνων προκάλεσε την εντατικοποίηση των διακρατικών και διαπροσωπικών οριζόντιων επαφών, προκαλώντας έτσι μια σχετική απαξίωση των συνόρων μεταξύ των κρατών. Ως συνέπεια, σήμερα παρατηρείται μια διασύνδεση και επακόλουθη αλληλεξάρτηση των υποδομών, ιδιαίτερα μεταξύ γειτονικών χωρών. Όπως καταδείχθηκε από τις επανειλημμένες κρίσεις σε σχέση με το σύστημα μεταφοράς φυσικού αερίου της Ρωσίας προς την Ευρώπη, οι υποδομές των κρατών είναι διασυνδεδεμένες πλέον σε τέτοιο βαθμό που η καταστροφή της υποδομής μιας χώρας επηρεάζει αρνητικά τις αντίστοιχες υποδομές, σε ποικίλο κατά περίπτωση βαθμό, άλλων χωρών. Η διασύνδεση και η εξ αυτής αλληλεξάρτηση των υποδομών, θεωρούμενη από τη σκοπιά του Κυβερνοπολέμου, αποτελεί ευχή και κατάρα ταυτόχρονα. Από τη μία πλευρά μια χώρα Α μπορεί να προσβάλλει τις υποδομές μιας χώρας Β, έχοντας στην πραγματικότητα ως στόχο τη χώρα Γ, «γειτονική»[26] (από άποψη υποδομών) της Β. Για παράδειγμα, η «αθόρυβη» παραποίηση των στοιχείων που αφορούν το χρέος μιας ή περισσοτέρων χωρών στη βάση δεδομένων του Διεθνούς Νομισματικού Ταμείου ή, ακόμη χειρότερα, μιας ιδιωτικής τράπεζας θα προκαλούσε χάος και παγκόσμια αναταραχή, έστω και προσωρινά.

Από την άλλη πλευρά, η προσβολή των υποδομών μιας χώρας Α από Κυβερνοεπιθέσεις εκδηλούμενες από μια χώρα Β, ενδεχομένως να προκαλέσει το συνασπισμό των χωρών των οποίων οι υποδομές επηρεάζονται, εναντίον της χώρας Β. Για παράδειγμα, ενδεχόμενη προσβολή των αγωγών ενέργειας (φυσικού αερίου και πετρελαίου) της Τουρκίας από την Ελλάδα, θα προκαλούσε τη δυσαρέσκεια, αν όχι την οργή των κρατών, συμμάχων ή μη της Ελλάδος, που μπορεί να φθάσει μέχρι του σημείου δημιουργίας νέων συμμαχιών, οι οποίες θα ανατρέψουν το υφιστάμενο σύστημα συμμαχιών και κατά συνέπεια του διεθνούς καταμερισμού ισχύος.

θ. Σχέση Κυβερνοπολέμου με τον πληροφοριακό πόλεμο

Ο Κυβερνοπόλεμος αποτελεί ο ίδιος μια κατηγορία πολέμου με τα δικά του χαρακτηριστικά. Παρόλα αυτά, από πολλές πλευρές, παρουσιάζει ομοιότητες με τον Πληροφοριακό πόλεμο.

Τα συμβατικά μέσα μαζικής επικοινωνίας, ο έντυπος τύπος, το ραδιόφωνο και η τηλεόραση, είναι σήμερα όλα διαθέσιμα σε ψηφιακές πλατφόρμες και μέσω του διαδικτύου έχουν απήχηση σε ένα κοινό το οποίο ξεπερνάει τα εθνικά σύνορα· είναι πλέον προσβάσιμα σε οποιονδήποτε διαθέτει μια σύνδεση διαδικτύου. Κρατικοί οργανισμοί και

---

[25] Δεν είναι δε σίγουρο ότι η δημιουργία του παγκόσμιου χωριού στην οποία με ταχύτητα οδηγούμαστε, είναι και απευκταία.

[26] Η έννοια της λέξης «γειτονική» στη συγκεκριμένη περίπτωση είναι αρκετά ευρεία. Για ορισμένες υποδομές, για παράδειγμα οικονομικές, δύο χώρες μπορεί να «γειτνιάζουν», έστω και αν είναι γεωγραφικά απομακρυσμένες.

υπηρεσίες, καθώς και Μη Κυβερνητικές Οργανώσεις χρησιμοποιούν επίσης το διαδίκτυο για σκοπούς επικοινωνιών και ανταλλαγής πληροφοριών, καθιστάμενοι έτσι τρωτοί σε Κυβερνοεπιθέσεις.

Κατά τη διάρκεια μιας σύγκρουσης, ο έλεγχος των πληροφοριών είναι ουσιαστικός, αφενός μεν για την ενίσχυση της εσωτερικής νομιμοποίησης στο εσωτερικό της χώρας, αφετέρου δε για τη διάβρωση του ηθικού του αντιπάλου. Το διαδίκτυο, ως πολλαπλασιαστής πληροφοριών (μέσω αναμετάδοσης ή διεύρυνσης του κοινού) παρέχει ευκαιρίες για παραπληροφόρηση και διασπορά ψιθύρων, και κατά συνέπεια αποτελεί στόχο επιλογής για όλες τις πλευρές μιας αντιπαράθεσης. Η προσβολή του στόχου αυτού διενεργείται μέσω Κυβερνοεπιθέσεων, σκοπός των οποίων δεν είναι η καταστροφή των δικτύων, αλλά η εισαγωγή ψευδών πληροφοριών και η προσβολή της αξιοπιστίας τους.

Στην πραγματεία του «Η τέχνη του πολέμου» ο Κινέζος στρατηγός και φιλόσοφος Sun Tzu διατείνεται ότι η τέχνη του πολέμου βασίζεται στην παραπλάνηση[27]. Η σχετικά πρόσφατη αντιπαράθεση μεταξύ Ρωσίας και Γεωργίας τον επιβεβαιώνει· ο Πληροφοριακός πόλεμος ήταν παρών από την αρχή μέχρι και το τέλος της αναμέτρησης. Στη συγκεκριμένη περίπτωση η έννοια του Κυβερνοπολέμου συγκλίνει με αυτή του Πληροφοριακού πολέμου, του οποίου αποτελεί εργαλείο. Η συγκεκριμένη περίπτωση καταδεικνύει επίσης τα όρια του Κυβερνοπολέμου σε σχέση με τον Πληροφοριακό πόλεμο. Οι βασικές επίσημες ιστοσελίδες της Γεωργίας οι οποίες δέχθηκαν επιθέσεις και εξουδετερώθηκαν από την αρχή της σύγκρουσης, μεταφέρθηκαν εκτός της χώρας, στις ΗΠΑ και την Πολωνία. Συνεπώς, «είναι ψευδαίσθηση στη σημερινή εποχή να πιστεύουμε ότι μια χώρα θα μπορούσε να απομονωθεί πληροφοριακά μόνο μέσω Πληροφοριακού πολέμου[28]»· η πολλαπλότητα των μέσων επικοινωνιών σήμερα είναι τέτοια που διασφαλίζει τη ροή των πληροφοριών από και προς τη χώρα – στόχο.

Συμπερασματικά, ο Πληροφοριακός πόλεμος χρησιμοποιεί τον Κυβερνοπόλεμο ως όργανό του, μέσω του οποίου προωθεί τις θέσεις του (έστω και με παραπληροφόρηση και διασπορά ψευδών ειδήσεων) στο διαδίκτυο, παρεμποδίζοντας ταυτόχρονα την πληροφόρηση του κοινού μέσω των ιστοσελίδων του αντιπάλου του.

ι. Κυβερνοπόλεμος και Ένοπλες Δυνάμεις

(1) Γενικά

Αποστολή των Ενόπλων Δυνάμεων ήταν πάντοτε, και παραμένει, η εμπλοκή με τις Ένοπλες Δυνάμεις του εχθρού και η καταστροφή τους ή η εξουδετέρωσή τους και ο εξαναγκασμός τους σε παράδοση. Στο πλαίσιο των πολεμικών επιχειρήσεων για την εκπλήρωση της αποστολής τους, οι Ένοπλες Δυνάμεις βρίσκονται στην ανάγκη προσβολής στόχων οι οποίοι δεν σχετίζονται αυστηρά με τις Ένοπλες Δυνάμεις του εχθρού, για παράδειγμα ένα εργοστάσιο παραγωγής ηλεκτρικού ρεύματος. Η απόφαση προσβολής ενός τέτοιου στόχου λαμβάνεται σε πολιτικό επίπεδο (σε αντιδιαστολή με ένα στόχο ραντάρ, του οποίου η προσβολή αποφασίζεται σε στρατιωτικό επίπεδο), και για τον

---

[27] Sun Tzu, *The Art of War*, Εκδόσεις Επικοινωνίες ΑΕ, Αθήνα 2002, Μετ. Πάνος Πικραμένος, Κεφάλαιο Ι Ο σχεδιασμός, σελ. 27.

[28] European Security and Defense Assembly, Assembly of Western European Union, Fifty-fifth session, Document A/2022, *Cyber warfare*, 3 December 2008, διαθέσιμο στην ιστοσελίδα http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2008/2022.pdf, (τελευταία επίσκεψη την 27 Ιαν 2010).

πρόσθετο λόγο ότι διακυβεύεται η πρόκληση παράπλευρων απωλειών. Δεν είναι βέβαια απίθανη η εξουσιοδότηση του Στρατιωτικού Διοικητή για προσβολή οποιουδήποτε στόχου, κάτω από ορισμένες προϋποθέσεις. Το μέσον προσβολής του εργοστασίου είναι κατά βάση στρατιωτικό, διότι μόνο οι Ένοπλες Δυνάμεις διαθέτουν τέτοιες δυνατότητες. Αν όμως είναι δυνατή η απενεργοποίηση ή και η καταστροφή του με Κυβερνοόπλα, γιατί θα έπρεπε να προσβληθεί με στρατιωτικά μέσα;

Έχουμε δεχθεί ότι ο Κυβερνοπόλεμος αποτελεί τον τέταρτο συντελεστή ισχύος του κράτους (πλην της διπλωματίας, της οικονομίας και των Ενόπλων Δυνάμεων), σχεδιάζεται και υλοποιείται στο επίπεδο της Υψηλής Στρατηγικής, και ότι συμμετέχει ισότιμα με τους άλλους τρεις στη διεξαγωγή του πολέμου. Κατά συνέπεια, η σχέση του με τις Ένοπλες Δυνάμεις και τον κλασικό πόλεμο δεν μπορεί παρά να είναι ανάλογη της σχέσης της διπλωματίας και της οικονομίας με τις Ένοπλες Δυνάμεις· η σχέση αυτή στη στρατιωτική ορολογία ονομάζεται σχέση υποστηρίζοντος - υποστηριζομένου. Ο Κυβερνοπόλεμος υποστηρίζει τους άλλους συντελεστές ισχύος όταν η έμφαση είναι στην οικονομική, τη διπλωματική ή τη στρατιωτική πλευρά της σύγκρουσης, και υποστηρίζεται από τους άλλους όταν η έμφαση βρίσκεται στον ίδιο τον Κυβερνοπόλεμο.

Η υποστήριξη την οποία μπορεί να παράσχει ο Κυβερνοπόλεμος στις Ένοπλες Δυνάμεις κατά τη διάρκεια των πολεμικών επιχειρήσεων είναι πολλαπλή, όπως φαίνεται παρακάτω:

- Μπορεί να χρησιμοποιηθεί ως εργαλείο διεξαγωγής του Πληροφοριακού πολέμου, για την προώθηση των θέσεών του μέσω του διαδικτύου.
- Μπορεί να προσβάλει στόχους του εχθρού οι οποίοι δεν μπορούν να προσβληθούν με συμβατικά στρατιωτικά οπλικά συστήματα, είτε επειδή βρίσκονται εκτός της εμβελείας τους, είτε λόγω της φύσης τους (δίκτυα υπολογιστών).
- Μπορεί να απενεργοποιήσει ορισμένους στόχους, αποφεύγοντας έτσι τη φυσική τους καταστροφή, είτε για λόγους μελλοντικής χρήσης, είτε για λόγους αποφυγής πρόκλησης δυσμενών εντυπώσεων στην εχθρική και παγκόσμια κοινή γνώμη (ψυχολογικός πόλεμος).
- Μπορεί να προσβάλει πολλούς στόχους ταυτόχρονα, σε όλη την έκταση της χώρας του αντιπάλου.
- Μπορεί να χρησιμοποιηθεί για την εκδήλωση του πρώτου πλήγματος στον αντίπαλο, πριν την έναρξη των πολεμικών επιχειρήσεων.

Όμως η σχέση του Κυβερνοπολέμου με τον κλασικό πόλεμο είναι λίγο πιο σύνθετη από αυτή μεταξύ των άλλων δύο συντελεστών ισχύος με αυτόν. Η εξάρτηση των Ενόπλων Δυνάμεων από τα επικοινωνιακά και πληροφοριακά συστήματα τις καθιστά ευάλωτες σε Κυβερνοεπιθέσεις. Το νέο αυτό περιβάλλον δημιουργεί ευκαιρίες προσβολής της μαχητικής ικανότητας των Ενόπλων Δυνάμεων και της ίδιας της λειτουργίας του κράτους μέσω της προσβολής των επικοινωνιακών και πληροφοριακών του συστημάτων. Σε κάθε περίπτωση, οι Ένοπλες Δυνάμεις, είναι υποχρεωμένες να διατηρούν, εκτός από

επιθετικές δυνατότητες Κυβερνοπολέμου, και δυνατότητες προστασίας των συστημάτων τους τα οποία είναι εκτεθειμένα σε Κυβερνοεπιθέσεις, όπως και όλοι οι δημόσιοι και ιδιωτικοί οργανισμοί και υπηρεσίες. Επιπλέον, η εξάρτηση της χώρας από επικοινωνιακά και πληροφοριακά συστήματα και η συνακόλουθη τρωτότητά τους παρέχει νέους στόχους στο εσωτερικό της χώρας, τους οποίους οι Ένοπλες Δυνάμεις, σε περίοδο πολέμου, πρέπει να προστατεύσουν, δεδομένου ότι οι στόχοι αυτοί είναι οι υποδομές που απαιτούνται για την καλή τους λειτουργία.

Από τη άλλη πλευρά, η απειλή της προσφυγής στον Κυβερνοπόλεμο για να είναι αξιόπιστη πρέπει να συνοδεύεται από την απειλή της προσφυγής στο συμβατικό πόλεμο, ήτοι στην πρόκληση άμεσων, σοβαρών και χειροπιαστών συνεπειών. Όμως, η υποστήριξη την οποία παρέχει ο κλασικός πόλεμος στον Κυβερνοπόλεμο περιορίζεται στην απειλή χρήσης βίας. Διότι, από τη στιγμή της προσφυγής σε κλασικό πόλεμο, η μοναδική επιλογή που έχει ο αντίπαλος είναι να ανταποδώσει και αυτός με προσφυγή σε πόλεμο, οπότε η κλιμάκωση είναι αναπόφευκτη και οι ρόλοι υποστηρίζοντος – υποστηριζομένου αντιστρέφονται.

Η υποστηρικτική δράση του Κυβερνοπολέμου παρατηρείται επίσης και στην περίοδο της ειρήνης, οπότε η δράση του Κυβερνοπολέμου περιορίζεται στη συλλογή πληροφοριών, όσες από τις οποίες παρουσιάζουν στρατιωτικό ενδιαφέρον διαβιβάζονται στις Ένοπλες Δυνάμεις για περεταίρω ανάλογη εκμετάλλευση.

Συμπερασματικά:

- Η σχέση του Κυβερνοπολέμου με τις Ένοπλες Δυνάμεις είναι σχέση υποστηρίζοντος – υποστηριζομένου.
- Οι Ένοπλες Δυνάμεις, όπως όλοι οι δημόσιοι οργανισμοί και υπηρεσίες, είναι υποχρεωμένες να διατηρούν αμυντικές και σε κάποιο βαθμό επιθετικές δυνατότητες Κυβερνοπολέμου, για την προστασία των συστημάτων τους τα οποία είναι εκτεθειμένα σε Κυβερνοεπιθέσεις.
- Η απειλή προσφυγής στον Κυβερνοπόλεμο για να είναι αξιόπιστη πρέπει να συνοδεύεται από αντίστοιχη απειλή προσφυγής στο συμβατικό πόλεμο.
- Η υποστηρικτική δράση του Κυβερνοπολέμου στην περίοδο της ειρήνης αφορά στη συλλογή πληροφοριών ενδιαφέροντος των Ενόπλων Δυνάμεων.

(2) Ο Κυβερνοπόλεμος ως πρώτο πλήγμα[29]

Η προετοιμασία του πρώτου πλήγματος στον πόλεμο πρέπει να γίνεται με προσοχή, έτσι ώστε αν δεν προκαλέσει τον αιφνιδιασμό του αντιπάλου (περίπτωση Perl Harbor) να επιβάλει την είσοδο του στον πόλεμο από μειονεκτική θέση, με τις χειρότερες δυνατές συνθήκες.

---

[29] Στην εποχή του ψυχρού πολέμου, οι χώρες του ΝΑΤΟ πίστευαν ότι η πρώτη επίθεση των Σοβιετικών θα αφορούσε σε μια πυρηνική έκρηξη χαμηλού ύψους με στόχο την καταστροφή των ηλεκτρονικών συστημάτων, μέσω της δημιουργίας ισχυρότατου Ηλεκτρομαγνητικού Παλμού (Electromagnetic Pulse).

Ιδιαίτερο ενδιαφέρον παρουσιάζει η δυνατότητα χρήσης του Κυβερνοπολέμου, λόγω των ιδιαίτερων χαρακτηριστικών του, ως «εναρκτήριο λάκτισμα» των επιχειρήσεων. Η πρώτη επίθεση στον πόλεμο του 21ου αιώνα θα μπορούσε κάλλιστα να αποτελείται από μια σειρά συντονισμένων Κυβερνοεπιθέσεων, σχεδιασμένων έτσι ώστε να διαμορφώσουν το πεδίο των επιχειρήσεων. Οι επιθέσεις αυτές θα μπορούσαν να συνδυαστούν με στρατιωτικά μέσα για να προκαλέσουν παραλυτικές επιπτώσεις στις κρίσιμες υποδομές της χώρας – στόχου, πριν την έναρξη των επιχειρήσεων. Ένα από τα πλεονεκτήματα της εκδήλωσης μιας τέτοιας μορφής ενορχηστρωμένης Κυβερνοεπίθεσης πριν την έναρξη των επιχειρήσεων είναι η δυνατότητα αιφνιδιασμού του αντιπάλου, ο οποίος επιτυγχάνεται χάρις στην εκδήλωση των Κυβερνοεπιθέσεων χωρίς προηγούμενη στρατιωτική κινητοποίηση.

Οι Κυβερνοεπιθέσεις σε στόχους στρατιωτικού ενδιαφέροντος έχουν ως σκοπό την υποβάθμιση της δυνατότητας των Ενόπλων Δυνάμεων του αντιπάλου να εκπληρώσουν την αποστολή τους, ήτοι να διεξάγουν τον πόλεμο. Στο πλαίσιο αυτό, ενδεχόμενους στόχους του πρώτου πλήγματος μέσω του Κυβερνοχώρου θα μπορούσαν να αποτελούν επιλεγμένοι στόχοι που αφορούν στην προετοιμασία και τις μετακινήσεις των Ενόπλων Δυνάμεων του αντιπάλου, τα δίκτυα επικοινωνιών του προς απαγόρευση διαβίβασης εντολών και το σύστημα έγκαιρης προειδοποίησης. Μια άλλη τακτική η οποία χρησιμοποιείται σε αυτές τις περιπτώσεις, δεδομένου και του σχεδόν μηδενικού κόστους τέτοιων επιθέσεων, είναι η ταυτόχρονη προσβολή όλων των στόχων σε ολόκληρο το βάθος του αντιπάλου, και η οποία από ορισμένους Αμερικανούς αρθρογράφους χαρακτηρίζεται ως carpet bombing[30].

Στην περίπτωση χρήσης της Κυβερνοεπίθεσης ως πρώτου πλήγματος, ο χρόνος εκδήλωσής της έχει ιδιαίτερη σημασία· η επίθεση θα πρέπει να διεξάγεται όσο το δυνατόν αργότερα, έτσι ώστε αφενός μεν να μη δοθεί η δυνατότητα στο στόχο να εντοπίσει την τρωτότητα των συστημάτων του και να τα επισκευάσει πριν ο επιτιθέμενος εκμεταλλευτεί τις αρχικές επιπτώσεις της, ενώ αφετέρου δε να μη χαθεί το πλεονέκτημα του αιφνιδιασμού, με την εκδήλωση της Κυβερνοεπίθεσης πολύ πριν την εκδήλωση της κανονικής επίθεσης με πυρά. Σημαντικός είναι επίσης ο συντονισμός της Κυβερνοεπίθεσης με τις επιχειρήσεις, επειδή το πιθανότερο είναι ότι η Κυβερνοεπίθεση δεν θα προκαλέσει φυσική καταστροφή και κατά συνέπεια μη αναστρέψιμες επιπτώσεις στην ικανότητα διεξαγωγής μάχης του αντιπάλου.

Συμπερασματικά, φαίνεται όλο και πιο πιθανό ότι η πρώτη επίθεση οποιασδήποτε μελλοντικής αναμέτρησης μεταξύ τεχνολογικά προηγμένων αντιπάλων θα είναι ηλεκτρονική και θα διεξαχθεί στον ή μέσω του Κυβερνοχώρου.

(3) Υποστήριξη κατά τη διάρκεια των επιχειρήσεων

Από την έναρξη της θερμής σύγκρουσης, οι στρατιωτικές επιχειρήσεις διεξάγονται σύμφωνα με το εκπονηθέν προς το σκοπό αυτό σχέδιο επιχειρήσεων, το οποίο ουσιαστικά αποτελεί τον τρόπο χρήσης των διαθεσίμων στρατιωτικών μέσων για την επίτευξη του επιδιωκόμενου Αντικειμενικού Σκοπού. Κάθε άλλο (μη στρατιωτικό) μέσο,

---

[30] Ο χαρακτηρισμός carpet bombing δόθηκε στον τρόπο βομβαρδισμού της γερμανικής πόλης Δρέσδης, στο τέλος του Β' παγκοσμίου Πολέμου, σύμφωνα με την οποία τα βομβαρδιστικά των συμμάχων βομβάρδιζαν αδιακρίτως ολόκληρη την πόλη υπό τύπο σάρωσης, μέχρι τη μετατροπή της σε ερείπια.

όπως ενδεχομένως μέσα Κυβερνοπολέμου τα οποία δεν είναι οργανικά των Ενόπλων Δυνάμεων, για λόγους ενότητας της πολεμικής προσπάθειας, τίθεται υπό διοικητική ή επιχειρησιακή διοίκηση, ή επιχειρησιακό ή τακτικό έλεγχο των Ενόπλων Δυνάμεων. Η δράση των μέσων αυτών συντονίζεται με τις επιχειρήσεις μέσω της έκδοσης συγκεκριμένων αποστολών για την επίτευξη συγκεκριμένων Αντικειμενικών Σκοπών, οι οποίοι είναι κατάλληλοι με τη φύση τους. Στο πλαίσιο αυτό, οι Αντικειμενικοί Σκοποί του Κυβερνοπολέμου όταν αυτός χρησιμοποιείται για την υποστήριξη των επιχειρήσεων, περιλαμβάνουν, χωρίς να εξαντλούνται, τους παρακάτω:

- Διακοπή εχθρικών επικοινωνιών και γραμμών Διοικητικής Μερίμνης.
- Προσβολή του εχθρικού συστήματος Διοίκησης και Ελέγχου.
- Παρενόχληση των στρατιωτικών μετακινήσεων.
- Προσβολή στόχων στρατιωτικού ενδιαφέροντος σε βάθος.
- Επηρεασμός της παγκόσμιας κοινής γνώμης σχετικά με τη διένεξη μέσω του διαδικτύου (παροχή υποστήριξης στον Πληροφοριακό πόλεμο).

Συμπερασματικά, η υποστήριξη των επιχειρήσεων του κλασικού πολέμου από τον Κυβερνοπόλεμο, γίνεται μέσω της ανάθεσης κατάλληλων αποστολών στα μέσα του Κυβερνοπολέμου, σε πλήρη συντονισμό με το γενικό σχέδιο επιχειρήσεων.

ια. Μέτρα συντονισμού μεταξύ εθνικών αλλά και διεθνών υπηρεσιών

(1) Γενικά

Κάθε χώρα είναι υπεύθυνη για την ασφάλεια των πληροφοριακών, αλλά και κάθε άλλου είδους υποδομών, εντός της επικρατείας της. Όμως μια Κυβερνοεπίθεση, του τύπου της εκτόξευσης ιού ή άλλης μορφής κακόβουλου λογισμικού, μπορεί εύκολα να διαδοθεί και πέρα από τα εθνικά σύνορα μιας χώρας. Όλες οι χώρες έχουν εμπειρία Κυβερνοεπιθέσεων, των οποίων ο βέλτιστος τρόπος αντιμετώπισης είναι η συνεργασία με άλλες χώρες. Χωρίς αυτή δεν είναι δυνατόν μια χώρα να αντιμετωπίσει το πολύπλευρο αυτό πρόβλημα, εκτός και αν είναι προετοιμασμένη να δεχθεί σημαντικά υψηλότερο κόστος για τα πολιτικά και στρατιωτικά υλικά που παράγει ή χρειάζεται.

(2) Εθνικό επίπεδο

Ο Κυβερνοπόλεμος και γενικότερα η παράνομη δραστηριότητα στον Κυβερνοχώρο, είναι μια υπόθεση που μας αφορά όλους· μια εθνική υπόθεση. Όπως κατέδειξε η εμπειρία της Εσθονίας, οι επιπτώσεις ενδεχόμενων Κυβερνοεπιθέσεων επηρεάζουν την καθημερινότητα της συντριπτικής πλειονότητας των πολιτών της χώρας. Η αντιμετώπιση αυτής της απειλής δεν μπορεί να είναι υπόθεση των Ενόπλων Δυνάμεων ή της ΕΥΠ μόνο. Απαιτείται η ενεργητική εμπλοκή και η συνεργασία των δημοσίων οργανισμών και υπηρεσιών, των τοπικών αρχών ασφαλείας, των Παρόχων Υπηρεσιών Διαδικτύου (Internet Service Providers – ISP), των διαχειριστών των δικτύων της χώρας, των Ομάδων Αντίδρασης σε Κυβερνοεπιθέσεις (CERT), της βιομηχανίας, των ιδιωτικών εταιρειών, των πάσης φύσεως ιδρυμάτων (Εκπαιδευτικών και μη) της χώρας. Η συνεργασία όλων αυτών των οργανισμών, ιδρυμάτων και υπηρεσιών διασφαλίζει την αντίδραση της

πληροφοριακής υποδομής σε Κυβερνοεπιθέσεις με ολοκληρωμένο και συντονισμένο τρόπο.

Όμως, η συνεργασία αυτή δεν συμβάλει μόνο στη διασφάλιση της άμυνας της χώρας. Ιδιαίτερη είναι η βοήθεια που μπορούν να παρέχουν στην περίπτωση της εκδήλωσης Κυβερνοεπιθέσεων εναντίον των πιθανών αντιπάλων. Όλοι αυτοί οι οργανισμοί, τα ιδρύματα και οι υπηρεσίες διαθέτουν ειδικούς με γνώσεις επί της οργάνωσης και λειτουργίας των συστημάτων – στόχων (πληροφοριακών και υποδομών) των ενδεχομένων αντιπάλων. Οι γνώσεις αυτές των συστημάτων είναι απαραίτητες για τη σχεδίαση και υλοποίηση αποτελεσματικών τρόπων προσβολής μέσω Κυβερνοεπιθέσεων.

Στο πλαίσιο αυτό, ιδιαίτερα χρήσιμη είναι η εξειδικευμένη γνώση και εμπειρία των χάκερ, η εκμετάλλευση των οποίων μπορεί να γίνει μέσω κατάλληλης οργάνωσης και ανάπτυξης ειδικών δραστηριοτήτων (οργάνωση σε συλλόγους, διαγωνισμοί χάκινγκ, βραβεία, κλπ). Όλη αυτή η προσπάθεια απαιτεί οργάνωση και συντονισμό μέσω ενός κεντρικού συντονιστικού οργάνου (Κέντρου ή υπηρεσίας), κάτω από κρατική εποπτεία και βοήθεια.

Συμπερασματικά, επειδή η Κυβερνοαπειλή δεν στρέφεται αποκλειστικά εναντίον του δημόσιου τομέα, η στενή συνεργασία μεταξύ κυβερνητικών υπηρεσιών, του ιδιωτικού τομέα και των ιδιωτών αποτελεί κομβικό σημείο στην προσπάθεια της χώρας αφενός μεν να αντιπαρατάξει αποτελεσματική άμυνα εναντίον του ενδεχομένου Κυβερνοεπιθέσεων, αφετέρου δε να αναλάβει πρωτοβουλίες εκδήλωσης Κυβερνοεπιθέσεων εναντίον των πιθανών αντιπάλων.

(3) Διεθνές επίπεδο

Στο διεθνές επίπεδο, η προσπάθεια διεθνούς συνεργασίας πρέπει να ξεκινήσει από την αναθεώρηση και τη συμπλήρωση του διεθνούς νομικού πλαισίου, κατά το πρότυπο του δικαίου του πολέμου, έτσι ώστε να ελεγχθεί η μέχρι σήμερα άναρχη και χαοτική δραστηριότητα στον Κυβερνοχώρο. Είναι επίσης απαραίτητη η συνεργασία μεταξύ των εθνικών φορέων, και η ίδρυση ενός Διεθνούς Παρατηρητηρίου Κυβερνοεπιθέσεων για την έγκαιρη προειδοποίηση των εθνικών αρχών.

Διεθνώς καταβάλλονται ήδη προσπάθειες για το συντονισμό των δράσεων των επιμέρους χωρών, για την αντιμετώπιση του γενικότερου προβλήματος της δραστηριότητας στον Κυβερνοχώρο. Από τις προσπάθειες αυτές ξεχωρίζουν αυτές του Συμβουλίου της Ευρώπης, της Ευρωπαϊκής Ένωσης και του ΝΑΤΟ, τα οποία έχουν υιοθετήσει νομικά και επιχειρησιακά εργαλεία (μέσα) για την προστασία του (ευρωπαϊκού και ΝΑΤΟϊκού) Κυβερνοχώρου.

(α) Συμβούλιο της Ευρώπης

Το Νοέμβριο του 2001 το Συμβούλιο της Ευρώπης υιοθέτησε τη Σύμβαση για το Κυβερνοέγκλημα[31] η οποία ενεργοποιήθηκε την 24 Ιουλίου 2004. Η σύμβαση έχει υπογραφεί από 23 χώρες, με τις 22 από αυτές να μην την έχουν ακόμη επικυρώσει.

---

[31] Counsil of Europe, Convention on Cybercrime, Budapest, 23 XI.2001, διαθέσιμο στην ιστοσελίδα http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, (τελευταία επίσκεψη την 11 Φεβ 2010).

(β) Ευρωπαϊκή Ένωση

Το 2004 η Ευρωπαϊκή Ένωση ίδρυσε το Ευρωπαϊκό Δίκτυο στην Υπηρεσία Πληροφοριακής Ασφάλειας (European Network in Information Security Agency – ENISA[32]) στην Κρήτη. Αυτή η υπηρεσία αποτελεί ένα κέντρο εξειδικευμένης γνώσης, όπως και το κέντρο CDD-CoE του NATO, στο Ταλίν της Εσθονίας. Η αποστολή της ENISA περιλαμβάνει

> «την παροχή συμβουλών και συστάσεων, ανάλυσης δεδομένων, και τη διευκόλυνση της ενημέρωσης και της συνεργασίας μεταξύ των υπηρεσιών της Ευρωπαϊκής Ένωσης και των χωρών-μελών της. … Μεταξύ άλλων, η ENISA παρέχει βοήθεια στην Ευρωπαϊκή Επιτροπή και στις χώρες-μέλη όσον αφορά στο διάλογό τους με τη βιομηχανία για την επίλυση προβλημάτων που σχετίζονται με την ασφάλεια σε προϊόντα λογισμικού και υλικού[33]».

Η ENISA βρίσκεται σε επαφή επίσης με τις κυβερνήσεις της Ευρωπαϊκής Ένωσης μέσω συνδέσμων και των αντίστοιχων εθνικών CERT. Εκδίδει μια ετήσια αναφορά των εργασιών της και παράγει θεματικές μελέτες και αναφορές πληροφοριών μετά από αίτηση των χωρών-μελών.

(γ) NATO

Μέχρι την Κυβερνοεπίθεση που δέχθηκε η Εσθονία το 2007 το NATO θεωρούσε τον Κυβερνοπόλεμο μια πιθανή αλλά μακρινή απειλή. Το γεγονός ότι τα κράτη χρησιμοποιούσαν την πληροφοριακή τεχνολογία για να εισβάλουν σε δίκτυα άλλων χωρών με σκοπό τον εντοπισμό τρωτών σημείων και τη συλλογή πολιτικών, στρατιωτικών, οικονομικών, βιομηχανικών και τεχνολογικών πληροφοριών ήταν ανεκτό ως φυσιολογική δραστηριότητα. Η Κυβερνοεπίθεση εναντίον της Εσθονίας έδωσε νέες διαστάσεις στο φαινόμενο. Ήταν μια προσπάθεια αποσταθεροποίησης της χώρας με οικονομικές επιπτώσεις. Μετά τη σύνοδο της Πράγας, το NATO ξεκίνησε την πρωτοβουλία Πρόγραμμα Κυβερνοάμυνας (Technical NATO Cyber Defense), η οποία οδήγησε στην ίδρυση του NATO Computer Response Team (NCIRT), κάτι αντίστοιχο με τα CERT.

Στις αρχές του 2008, μετά από πρόταση των εσθονικών αρχών, το NATO συμφώνησε στην ίδρυση του CCD-CoE (Cooperative Cyber Defense Center of Excellence[34]) στο Ταλίν. Την 14 Μαΐου 2008 οι αντιπρόσωποι επτά χωρών – μελών του NATO (Εσθονία, Λετονία, Λιθουανία, Γερμανία, Ιταλία, Σλοβακία, Ιταλία) υπέγραψαν συμφωνία για την ίδρυση του κέντρου με το Διοικητή του Allied Command Transformation (ACT), τον έναν από τους δύο Στρατηγικούς Διοικητές του NATO. Το κέντρο διαθέτει σήμερα ένα επιτελείο 30 περίπου ατόμων, τα μισά εκ των οποίων θεωρούνται ειδικοί στον Κυβερνοπόλεμο. Το κέντρο πρακτικά αποτελεί ένα κέντρο ανταλλαγής πληροφοριών μεταξύ των ειδικών και ενημέρωσης και εκπαίδευσης αξιωματικών του NATO επί θεμάτων Κυβερνοπολέμου.

---

[32] http://www.enisa.europa.eu

[33] European Security and Defense Assembly, Assembly of Western European Union, Fifty-fifth session, Document A/2022, *Cyber warfare*, 3 December 2008, διαθέσιμο στην ιστοσελίδα http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2008/2022.pdf, (τελευταία επίσκεψη την 11 Φεβ 2010).

[34] http://www.ccdcoe.org.

Με τις προαναφερθείσες πρωτοβουλίες, η Κυβερνοάμυνα, και ο Κυβερνοπόλεμος γενικότερα, εντάσσονται σήμερα στις άμεσες προτεραιότητες του ΝΑΤΟ[35].

ιβ. Επιπτώσεις των επιχειρήσεων Κυβερνοπολέμου εναντίον χωρών οι οποίες δεν διαθέτουν την απαιτούμενη υποδομή αλλά και ανάπτυξη σε αντίστοιχα θέματα Κυβερνοπολέμου.

Απαραίτητη προϋπόθεση για τη διεξαγωγή επιχειρήσεων Κυβερνοπολέμου εναντίον μιας χώρας, είναι η καλή επικοινωνιακή και πληροφοριακή της υποδομή , και η μέσω αυτής διασύνδεση όλων των επί μέρους δικτύων και συστημάτων σε ένα υπερδίκτυο. Η εξέλιξη αυτή κατέστη δυνατή μέσω της εξέλιξης της τεχνολογίας στους τομείς των επικοινωνιών και της πληροφορικής. Οι αναπτυγμένες χώρες πέτυχαν τη διασύνδεση των υπηρεσιών τους, με αντάλλαγμα την επιδείνωση της τρωτότητάς τους σε ενδεχόμενες Κυβερνοεπιθέσεις. Οι πιο αναπτυγμένες από αυτές υλοποίησαν συστήματα ICS για τη διοίκηση και τον έλεγχο των υποδομών τους μέσω επικοινωνιακών και πληροφοριακών συστημάτων, καθιστώντας έτσι τον εαυτό τους τον απόλυτο στόχο των Κυβερνοεπιθέσεων.

Από την άλλη πλευρά, υπάρχουν χώρες των οποίων η επικοινωνιακή και πληροφοριακή υποδομή βρίσκεται σε νηπιακό επίπεδο, με υποτυπώδη διασύνδεση μεταξύ των δικτύων και των συστημάτων μεταξύ τους και αυτών με το διαδίκτυο. Επιπλέον, οι υποδομές τους παραμένουν απομονωμένες, χωρίς εξελιγμένα συστήματα διοίκησης και ελέγχου. Από την άποψη αυτή, τέτοιες χώρες αποτελούν φτωχό στόχο για ενδεχόμενες επιχειρήσεις Κυβερνοπολέμου. Η όποια πιθανότητα επιτυχούς διεξαγωγής Κυβερνοεπιχειρήσεων εναντίον χωρών με φτωχή επικοινωνιακή και πληροφοριακή υποδομή, απαιτεί κατ' ελάχιστον φυσική παρουσία δραστών στο χώρο λειτουργίας των συστημάτων, γεγονός που καθιστά ένα τέτοιο εγχείρημα τουλάχιστον επισφαλές. Εναντίον τέτοιων χωρών, οι επιχειρήσεις Κυβερνοπολέμου, αν τελικά διεξάγονται, είναι πρωτόγονες και αμφιβόλου αποτελεσματικότητας, αποκλείοντας έξυπνες τακτικές συλλογής πληροφοριών ή υποβάθμισης ή και διακοπής της λειτουργίας των συστημάτων. Οι μόνες επιχειρήσεις οι οποίες μπορούν να έχουν κάποια θετικά αποτελέσματα είναι οι Κυβερνοεπιχειρήσεις στα πλαίσια του Πληροφοριακού Πολέμου, με στόχο την παρεμπόδιση της παρουσίασης των απόψεων της χώρας – στόχου στην παγκόσμια κοινή γνώμη, μέσω Κυβερνοεπιθέσεων σε ιστοσελίδες μέσων μαζικής επικοινωνίας και παροχής πληροφοριών.

Στην περίπτωση της σύγκρουσης μεταξύ χωρών ή οργανώσεων με φτωχή πληροφοριακή υποδομή (αμφοτέρων ή μόνο του ενός των εμπολέμων), η προσπάθεια επιβολής της θελήσεων του ενός των εμπολέμων στον άλλο, η οποία αποτελεί και τον απόλυτο σκοπό του πολέμου, στα πλαίσια του Κυβερνοπολέμου, μπορεί να επιδιωχθεί με σοβαρές πιθανότητες επιτυχίας, μόνο όταν αυτή συνοδεύεται από απειλή ή χρήση παραδοσιακού πολέμου. Η κλασική περίπτωση επιτυχούς διεξαγωγής Κυβερνοπολέμου εναντίον χώρας με φτωχή επικοινωνιακή και πληροφοριακή υποδομή είναι η σύγκρουση μεταξύ της Ρωσίας και Γεωργίας τον Αύγουστο του 2008, για το θέμα της Νότιας Οσσετίας.

---

[35] European Security and Defense Assembly, Assembly of Western European Union, Fifty-fifth session, Document A/2022, *Cyber warfare*, 3 December 2008, διαθέσιμο στην ιστοσελίδα http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2008/2022.pdf (τελευταία επίσκεψη την 7 Φεβ 2010).

Παρόλα αυτά, αν και κάποια οντότητα μπορεί να μη συγκεντρώνει τις προϋποθέσεις ώστε να αποτελεί στόχο Κυβερνοεπιθέσεων, μπορεί κάλλιστα να οργανώσει και να διεξαγάγει επιχειρήσεις Κυβερνοπολέμου εναντίον επικοινωνιακά και πληροφοριακά προηγμένων αντιπάλων της.

Συμπερασματικά, απαραίτητη προϋπόθεση για την επιλογή μιας πολιτικής οντότητας (χώρας ή οργάνωσης) ως στόχου Κυβερνοπολέμου είναι η οργάνωσή της έτσι ώστε να παρουσιάζει κατάλληλο στόχο. Με την έννοια αυτή, μόνο τα κράτη ή οι υπερεθνικές οργανώσεις κρατών (συμμαχίες) μπορούν να αποτελέσουν στόχο επιχειρήσεων Κυβερνοπολέμου, διότι μόνο αυτά έχουν την κατάλληλη δομή η οποία επιτρέπει την οργάνωση δικτύων επικοινωνιών και πληροφορικής για τη αποτελεσματικότερη λειτουργία τους, το συντονισμό τους και την εξυπηρέτηση των πελατών – πολιτών. Η απειλή ή η χρήση βίας στο πλαίσιο του Κυβερνοπολέμου, εναντίον χωρών με φτωχή επικοινωνιακή και πληροφοριακή υποδομή, θα πρέπει να συνοδεύεται πάντοτε με απειλή ή χρήση παραδοσιακού πολέμου.

4. ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΕΛΛΗΝΙΚΕΣ ΕΝΟΠΛΕΣ ΔΥΝΑΜΕΙΣ

α. Σχέση των ελληνικών Ενόπλων Δυνάμεων με τον Κυβερνοπόλεμο

Η παρούσα μελέτη επιχειρηματολογεί υπέρ της θεώρησης του Κυβερνοπολέμου ως ενός (τετάρτου) συντελεστού ισχύος της χώρας, του οποίου η εμπλοκή στην επιδίωξη τεθέντων πολιτικών σκοπών θα πρέπει να γίνεται στο επίπεδο της Υψηλής Στρατηγικής από τα κατάλληλα κυβερνητικά όργανα. Το μόνο κατάλληλο κυβερνητικό όργανο, υπεύθυνο για τον καθορισμό της πολιτικής εθνικής ασφάλειας και το συντονισμό των εμπλεκομένων στο θέμα κυβερνητικών οργάνων και υπηρεσιών είναι το Κυβερνητικό Συμβούλιο Εξωτερικών και Άμυνας (ΚΥΣΕΑ). Το ΚΥΣΕΑ όμως είναι όργανο πολιτικής, σε πολύ υψηλό επίπεδο, το οποίο συνέρχεται ad hoc και δεν διαθέτει μόνιμο προσωπικό· επίσης ως όργανο πολιτικής δεν μπορεί να αναλάβει έργο διοίκησης και ελέγχου ενός οργάνου ή μιας υπηρεσίας υπεύθυνης για τον Κυβερνοπόλεμο. Αναγκαστικά, η διοίκηση και ο έλεγχος της δραστηριότητας του Κυβερνοπολέμου πρέπει να ανατεθεί σε κάποιο Υπουργείο, προκειμένου να υπάρχει η δυνατότητα υλοποίησης ληφθέντων αποφάσεων σε όλη την επικράτεια και η εξασφάλιση της συνεργασίας μεταξύ όλων των εμπλεκομένων φορέων. Σήμερα, καμία κυβερνητική υπηρεσία ή οργανισμός δεν φαίνεται να είναι υπεύθυνη για τη σχεδίαση, το συντονισμό και τη διεξαγωγή επιχειρήσεων Κυβερνοπολέμου (και ιδίως επιθετικών). Το πλέον κατάλληλο υπουργείο για να φιλοξενήσει μια τέτοια δραστηριότητα, είναι το Υπουργείο Εθνικής Άμυνας (ΥΕΘΑ), για τους παρακάτω λόγους:

- Είναι ο αρμόδιος φορέας για την άμυνα της χώρας.
- Οι Ένοπλες Δυνάμεις διαθέτουν ορισμένα ιδιαίτερα χαρακτηριστικά (οργάνωση και πειθαρχία) που τις καθιστούν αξιοποιήσιμες από την εκάστοτε πολιτική εξουσία για την αντιμετώπιση κρίσεων (σχέδιο ΞΕΝΟΚΡΑΤΗΣ) οι οποίες δεν σχετίζονται άμεσα με την αποστολή τους.
- Το ΓΕΕΘΑ διαθέτει εμπειρία στη διοίκηση και τον έλεγχο αναλόγων δραστηριοτήτων (Ηλεκτρονικός Πόλεμος, Πληροφοριακός Πόλεμος).

- Οι Ένοπλες Δυνάμεις έχουν την ευθύνη της προστασίας των κρίσιμων υποδομών της χώρας, από τις οποίες, άμεσα ή έμμεσα, εξαρτάται η καλή τους λειτουργία και κατά συνέπεια η εκπλήρωση της αποστολής τους.
- Οι Ένοπλες Δυνάμεις διαθέτουν δεκαετή εμπειρία στη διοίκηση και τον έλεγχο δραστηριοτήτων Κυβερνοάμυνας.
- Είναι διεθνής πρακτική οι δραστηριότητες Κυβερνοπολέμου να υπάγονται, ως επί το πλείστον, στα Υπουργεία Αμύνης.

(1) Παρούσα κατάσταση

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (CERT)

Με το νόμο 3646 της 3 Μαρ 2008, η Εθνική Υπηρεσία Πληροφοριών «ορίζεται ως η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων[36], η οποία μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής, …»[37]. Ανεξάρτητα από τον τρόπο ερμηνείας της φράσης «… ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων …» ο συντάκτης του νόμου δεν φαίνεται να προβλέπει την ανάληψη επιθετικών ενεργειών, στο πλαίσιο είτε της αντίδρασης σε ενδεχόμενη Κυβερνοεπίθεση, είτε στο πλαίσιο προληπτικής Κυβερνοεπίθεσης προς υποστήριξη επιδιωκόμενων εθνικών σκοπών, γεγονός εξάλλου που αποδεικνύεται και από την έλλειψη πρόβλεψης για την ίδρυση σχετικής Υπηρεσίας ή Μονάδος υπεύθυνης για τη διεξαγωγή επιθετικών επιχειρήσεων Κυβερνοπολέμου.

Από τη διατύπωση επίσης φαίνεται ότι η Κυβερνοαπειλή, κατά την άποψη του συντάκτη της διάταξης, αφορά σε «δίκτυα επικοινωνιών, εγκαταστάσεις αποθήκευσης πληροφοριών και συστήματα πληροφορικής …», χωρίς καμία αναφορά στις υποδομές της χώρας, η προσβολή των οποίων θα μπορούσε να έχει σοβαρές επιπτώσεις στη λειτουργία του κράτους.

Ένα άλλο πρόβλημα το οποίο αναδεικνύεται από την πρόβλεψη του νόμου είναι η αποσπασματική αντιμετώπιση του θέματος της Κυβερνοαπειλής. Εφόσον το κράτος αποφάσισε να ασχοληθεί με το θέμα θα έπρεπε να ακολουθήσει προσέγγιση εκ των άνω προς τα κάτω, ήτοι να ορίσει το γενικό συντονιστικό όργανο, και αν δεν υπάρχει να το δημιουργήσει, σε επίπεδο Υψηλής Στρατηγικής, και στη συνέχεια να εξειδικεύσει τις ευθύνες και το ρόλο της κάθε υπηρεσίας στο συγκεκριμένο θέμα. Η πολιτική Κυβερνοασφάλειας λάμπει δια της απουσίας της.

(2) Πιθανοί ανταγωνιστές

Όπως προαναφέρθηκε, οι επιχειρήσεις Κυβερνοπολέμου, στη μορφή της Κυβερνοκατασκοπίας ή της συλλογής πληροφοριών Κυβερνοπολέμου (footprinting), διεξάγονται από του καιρού της ειρήνης. Οι επιχειρήσεις αυτές αναμένεται να ενταθούν σε περιπτώσεις κρίσεων (οικονομικών, διπλωματικών ή στρατιωτικών) ή ενδεχόμενου πολέμου. Η κατάσταση αυτή απαιτεί από μέρους της χώρας μας εγρήγορση και κατάλληλη προετοιμασία σε επίπεδο Κυβερνοπολέμου. Οι χώρες οι οποίες ήδη διεξάγουν ή ενδεχομένως να διεξάγουν στο μέλλον επιχειρήσεις Κυβερνοπολέμου εις βάρος της χώρας

---

[36] Cyber Emergency Reaction Team (CERT)

[37] Νόμος Υπ' Αριθ. 3649, 3 Μαρ 2008, Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις.

μας, μπορούν και πρέπει να προσδιοριστούν με βάση συγκεκριμένα κριτήρια Κυβερνοαπειλής, όπως τα παρακάτω:

- Χώρες οι οποίες αποτελούν ήδη στρατιωτική απειλή (Τουρκία).
- Χώρες με τις οποίες οι διπλωματικές μας σχέσεις βρίσκονται σε κάποιου βαθμού κρίση (FYROM).
- Γειτονικές χώρες οι οποίες, παρά τη σημερινή πολιτική, οικονομική ή στρατιωτική τους αδυναμία, πρέπει να αποτελούν αντικείμενο συνεχούς ενδιαφέροντος (Αλβανία, Βουλγαρία)
- Χώρες με παγκόσμια ενδιαφέροντα (ΗΠΑ, Κίνα, Ρωσία).
- Χώρες με τοπικά συμφέροντα στην περιοχή των Βαλκανίων και της ευρύτερης περιοχής της ανατολικής Μεσογείου (Ιταλία, Μεγάλη Βρετανία, Γαλλία).
- Μη γειτονικές χώρες στις οποίες διαβιούν πληθυσμοί ελληνικής καταγωγής και οι οποίες παρουσιάζουν σχετική πολιτική αστάθεια με ενδεχόμενο να διακινδυνεύσει η ζωή πολιτών τους ελληνικής καταγωγής (Γεωργία).
- Τρομοκρατικές οργανώσεις οι οποίες μπορεί να στραφούν εναντίον της χώρας μας εξ αιτίας της συμμετοχής της στο ΝΑΤΟ και (λιγότερο) στην Ευρωπαϊκή Ένωση ή της συμμετοχής ελληνικού προσωπικού στις επιχειρήσεις του Αφγανιστάν (Al Qaeda).

Συμπερασματικά, οι χώρες – οργανώσεις οι οποίες πρέπει να αποτελέσουν από σήμερα αντικείμενο Κυβερνοενδιαφέροντος, λόγω της πιθανής εξέλιξής τους σε στρατιωτικές απειλές ή Κυβερνοαπειλές είναι, κατά σειρά προτεραιότητας, η Τουρκία, η FYROM, η Αλβανία, η Βουλγαρία, η Μεγάλη Βρετανία, η Ιταλία, η Γαλλία, οι ΗΠΑ, η Ρωσία, η Κίνα, η Γεωργία και η Al Qaeda.

β. Πλεονεκτήματα που προκύπτουν από τις επιχειρησιακές δυνατότητες διεξαγωγής επιχειρήσεων Κυβερνοπολέμου από τις ελληνικές Ένοπλες Δυνάμεις.

Η σοβαρότητα του θέματος του Κυβερνοπολέμου έχει γίνει κατανοητή από την πλειονότητα των χωρών, οι οποίες έχουν λάβει ήδη μέτρα για την οργάνωση του σχετικού τομέα και την ανάπτυξη επιχειρησιακών δυνατοτήτων Κυβερνοπολέμου, η κάθε μία σε διαφορετικό βαθμό. Στη χώρα μας, παρά τα θετικά πρώτα βήματα με την ίδρυση της ΔΙΚΥΒ, απαιτείται κατ' αρχήν ο ενστερνισμός της σοβαρότητας του θέματος από τη στρατιωτική και πολιτική μας ηγεσία και η ανάληψη σοβαρής προσπάθειας για την ανάδειξη του Κυβερνοπολέμου σε ένα πραγματικό συντελεστή ισχύος του κράτους. Ειδικότερα για τις Ένοπλες Δυνάμεις, οι οποίες αναπόφευκτα θα φέρουν το βάρος της προσπάθειας αυτής, η ευθύνη τους είναι σοβαρή και μεγάλη, έτσι ώστε να αποκτήσουν επιχειρησιακές δυνατότητες διεξαγωγής επιχειρήσεων Κυβερνοπολέμου, οι οποίες σήμερα λείπουν από το οπλοστάσιό τους. Τα πλεονεκτήματα από την απόκτηση τέτοιων δυνατοτήτων είναι προφανή:

- Η χώρα αποκτά αποτρεπτικές ικανότητες στον Κυβερνοχώρο, οι οποίες εμμέσως ενισχύουν τη γενική αποτρεπτική ικανότητά της.

- Παρέχεται στην πολιτική ηγεσία της χώρας ένα όργανο Κυβερνοπολέμου το οποίο λείπει σήμερα, και το οποίο εκτιμάται ότι θα απαιτηθεί στο μέλλον.
- Οι Ένοπλες Δυνάμεις αποτελούν το σημείο αναφοράς για τη διεθνή συνεργασία της χώρας σε θέματα Κυβερνοπολέμου.
- Με επίκεντρο τις Ένοπλες Δυνάμεις, προκαλείται συσπείρωση των δυνάμεων Κυβερνοπολέμου της χώρας (κυβερνητικές υπηρεσίες και οργανισμοί, βιομηχανία, εκπαιδευτικά ιδρύματα), οι οποίες έτσι αποκτούν ένα μοναδικό σημείο αναφοράς και ένα συντονιστικό όργανο των δραστηριοτήτων στον Κυβερνοχώρο.
- Η χώρα αποκτά δυνατότητες για την οργάνωση της άμυνάς της εναντίον ενδεχόμενων Κυβερνοεπιθέσεων.
- Αποκτώνται δυνατότητες διεξαγωγής Κυβερνοκατασκοπίας και συλλογής πληροφοριών για την καλύτερη εκτίμηση της Κυβερνοαπειλής και την οργάνωση της άμυνάς της.
- Η χώρα αποκτά έναν πολλαπλασιαστή της στρατιωτικής της ισχύος και ένα μέσο υποστήριξης των επιχειρήσεων του παραδοσιακού πολέμου.

γ. Προϋποθέσεις / απαιτήσεις για την επίτευξη ικανής επιχειρησιακής δυνατότητας σε επιθετικές και αμυντικές επιχειρήσεις Κυβερνοπολέμου.

Η απόκτηση επιχειρησιακών δυνατοτήτων διεξαγωγής επιχειρήσεων Κυβερνοπολέμου, όπως και το γενικότερο πρόβλημα της ανάδειξης του Κυβερνοπολέμου ως θέματος μείζονος σημασίας, όχι μόνο για τις Ένοπλες Δυνάμεις, αλλά και τη χώρα γενικότερα, δεν είναι εύκολη υπόθεση ούτε και απλή.

Κατά πρώτον πρέπει να υπερνικηθεί η αδράνεια της γραφειοκρατίας των Ενόπλων Δυνάμεων, η οποία εν πολλοίς έχει προσκολληθεί στα απηρχαιωμένα συμπεράσματα του Β’ ΠΠ, σε ό,τι αφορά τη διεξαγωγή των επιχειρήσεων, όπως αυτά καθορίστηκαν στα αμερικανικά εγχειρίδια εκστρατείας. Η ελληνική στρατιωτική σκέψη είναι ανύπαρκτη. Οι αρετές της προσωπικής γενναιότητας και του θάρρους αποτελούν πράγματι το θεμέλιο του στρατιωτικού επαγγέλματος, όμως από μόνες τους δεν μπορούν να εξασφαλίσουν την επιτυχή έκβαση ενός ενδεχόμενου πολέμου. Η ταχύτατη τεχνολογική εξέλιξη μετέβαλε τη φύση του πολέμου όπως ήταν γνωστός τον προηγούμενο αιώνα· η εποχή του ηρωικού πολέμου έχει παρέλθει (ανεπιστρεπτί;). Απαιτείται λοιπόν μια θεμελιώδης αλλαγή της κουλτούρας του προσωπικού των Ενόπλων μας Δυνάμεων προς την κατεύθυνση των πολλαπλασιαστών ισχύος όπως ο Ηλεκτρονικός Πόλεμος, ο Πληροφοριακός Πόλεμος και ο Κυβερνοπόλεμος. Η αλλαγή της κουλτούρας αυτής, η οποία για τα δεδομένα των ελληνικών Ενόπλων Δυνάμεων είναι επανάσταση, για να είναι αποτελεσματική, χρειάζεται προσέγγιση εκ των άνω προς τα κάτω. Συνεπώς, η πρώτη και θεμελιωδέστερη προϋπόθεση είναι ο ενστερνισμός από την πολιτική και στρατιωτική ηγεσία του ΥΕΘΑ της σοβαρότητας του θέματος και της σημασίας του στην ενίσχυση της ικανότητας της χώρας μας στην αντιμετώπιση σύγχρονων προκλήσεων. Μέχρι σήμερα η ηγεσία μας, καλυπτόμενη πίσω από το ενδεχόμενο ενός πολέμου του τύπου της βιομηχανικής εποχής με την Τουρκία, απέφυγε τον εναρμονισμό της με το βηματισμό των άλλων χωρών του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης, στην αναθεώρηση του δόγματος και

την παράλληλη θεώρηση απειλών νέου τύπου, όπως η τρομοκρατία. Όμως τα χαρακτηριστικά του Κυβερνοπολέμου είναι διαφορετικά από αυτά της τρομοκρατίας· η επικάλυψη που παρουσιάζει με τον κλασικό πόλεμο καθιστά την αγνόησή του θεμελιώδες σφάλμα και την απόλυτη συνταγή αποτυχίας.

Το θέμα του Κυβερνοπολέμου είναι ένα θέμα που ξεπερνάει τα στενά όρια των Ενόπλων Δυνάμεων· είναι θέμα εθνικής ασφάλειας. Ως τέτοιο καλύπτει ένα ευρύ φάσμα και αφορά κυβερνητικές υπηρεσίες και οργανισμούς, τη βιομηχανία και τα εκπαιδευτικά μας ιδρύματα. Η επιτυχής λοιπόν ενασχόληση με το θέμα απαιτεί εκτεταμένη και συγκεκριμένη συνεργασία με τα άλλα εμπλεκόμενα υπουργεία (για λόγους όχι μόνο συντονισμού, αλλά και υποστήριξης της γενικής προσπάθειας, σε επίπεδο χρηματοδότησης και προσωπικού), τη βιομηχανία (για τον έλεγχο της εφαρμογής των σχεδιασθησομένων μέτρων ασφαλείας και την άντληση εξειδικευμένης γνώσης η οποία δεν υπάρχει στις Ένοπλες Δυνάμεις) και την ακαδημαϊκή κοινότητα (για την υλοποίηση ερευνητικών προγραμμάτων και την παραγωγή κατάλληλου επιστημονικού προσωπικού).

Η οργάνωση – αναδιοργάνωση του τομέα του Κυβερνοπολέμου πρέπει να τεθεί σε νέες βάσεις. Ο Κυβερνοπόλεμος δεν πρέπει να παραμείνει μία ακόμη Διεύθυνση στην ατελείωτη σειρά των Διευθύνσεων του ΓΕΕΘΑ. Το διακύβευμα στην περίπτωση αυτή είναι πολύ σοβαρότερο και πολύ μεγαλύτερο για να ταφεί σε ένα βαθύ σημείο επάλληλων επιπέδων διοικήσεως. Οι βασικές αρχές στις οποίες πρέπει να θεμελιωθεί η δομή του Κυβερνοπολέμου περιλαμβάνουν, χωρίς να εξαντλούνται, τις παρακάτω:

- Άμεση πρόσβαση της νέας υπηρεσίας στην πολιτική ηγεσία για λόγους ταχύτητας λήψης αποφάσεων.
- Διευκόλυνση της συνεργασίας με τις εμπλεκόμενες κυβερνητικές υπηρεσίες και οργανισμούς, τη βιομηχανία και τα εκπαιδευτικά ιδρύματα για να διασφαλιστεί η εύκολη πρόσβαση των φορέων αυτών στη δομή του Κυβερνοπολέμου.
- Σαφή διάκριση του επιτελικού από το εκτελεστικό σκέλος του φορέα.

Το προσωπικό του Κυβερνοπολέμου, οι «Κυβερνομαχητές», πρέπει να διαθέτουν ιδιαίτερες ικανότητες. Οι ικανότητες αυτές αποκτώνται μετά από μακροχρόνια εκπαίδευση και εμπειρία – ενασχόληση με το θέμα. Η ιδιοσυγκρασία των ατόμων αυτών (χάκερ) τα οποία είναι κατάλληλα, είναι ιδιαίτερη και κατά συνέπεια απαιτούνται ιδιαίτερες μέθοδοι για τον εντοπισμό και τη στρατολόγησή τους. Σε κάθε περίπτωση, η αποτελεσματικότητα των επιχειρήσεων του Κυβερνοπολέμου εξαρτάται από την καταλληλότητα του προσωπικού και την ύπαρξη ενός κατάλληλα οργανωμένου προγράμματος εκπαίδευσης (συμπεριλαμβανομένων και των ασκήσεων).

Όπως έχει κατ' επανάληψη τονιστεί στην παρούσα μελέτη, επιτυχής και αποτελεσματική χρήση επιχειρήσεων Κυβερνοπολέμου για την επίτευξη πολιτικών σκοπών της χώρας απαιτεί διεθνή συνεργασία σε πολλά επίπεδα. Κατά συνέπεια, πρωταρχικό μέλημα του φορέα Κυβερνοπολέμου θα πρέπει να είναι η σχεδίαση και υλοποίηση ενός εκτεταμένου προγράμματος διεθνούς συνεργασίας. Η συνεργασία με τις λοιπές χώρες του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης είναι εξασφαλισμένη, μέσω ενός καλά οργανωμένου και δοκιμασμένου πλαισίου συνεργασίας· το μόνο που απαιτείται είναι η δραστηριοποίηση της χώρας μας έτσι ώστε να φθάσει στο επίπεδο των άλλων χωρών, εκμεταλλευόμενη την

εμπειρία τους. Η συνεργασία με τις γειτονικές και λοιπές βαλκανικές χώρες μπορεί να επιτευχθεί με πρωτοβουλία της δικής μας πλευράς με σκοπό να εξασφαλίσει τη συνεργασία τους σε περιπτώσεις εντοπισμού και προσαγωγής σε δίκη δραστών Κυβερνοεπιθέσεων εναντίον των συνεργαζομένων χωρών. Μια τρίτη κατηγορία συνεργασιών που πρέπει να επιδιωχθεί είναι αυτή με χώρες που είναι προηγμένες σε θέματα Κυβερνοπολέμου (για παράδειγμα Ρωσία, Κίνα, Ισραήλ, Ινδία, Πακιστάν), υπό την αίρεση των δεσμεύσεων που απορρέουν από την κατάστασή μας ως χώρας-μέλους του ΝΑΤΟ και της Ευρωπαϊκής Ένωσης.

Η διεξαγωγή επιχειρήσεων Κυβερνοπολέμου απαιτεί ένα πρόγραμμα οργάνωσης του τομέα του Κυβερνοπολέμου (επιτελικό και εκτελεστικό βραχίονα), στρατολόγησης εξειδικευμένου προσωπικού και προμήθειας ή/και ανάπτυξης Κυβερνοόπλων. Η επιτυχής υλοποίηση ενός τέτοιου προγράμματος απαιτεί το σχεδιασμό του στο πλαίσιο της υφιστάμενης (και κατάλληλα προσαρμοσμένης) διαδικασίας Αμυντικής Σχεδίασης. Η Αμυντική Σχεδίαση, μέσω της εκτίμησης της ποιότητας και της έκτασης της Κυβερνοαπειλής, της σύνταξης κατάλληλων σεναρίων Κυβερνοπολέμου, ειδικής επιχειρησιακής σχεδίασης των σεναρίων και κατάλληλης ανάλυσης των αποτελεσμάτων από την, προς το σκοπό αυτό συγκροτούμενη, υποεπιτροπή Κυβερνοπολέμου της επιτροπής Αμυντικής Σχεδίασης, προσδιορίζει ορθολογικά και πέραν πάσης αμφισβήτησης την οργάνωση και το προσωπικό και υλικό που απαιτούνται για την επιτυχή αντιμετώπιση της υφιστάμενης και ενδεχόμενης Κυβερνοαπειλής εναντίον της χώρας μας.

Θεμελιώδης προϋπόθεση της επιτυχούς διεξαγωγής επιχειρήσεων Κυβερνοπολέμου, με δεδομένη την ύπαρξη κατάλληλης οργάνωσης, προσωπικού και μέσων, είναι η κατάλληλη προετοιμασία από του καιρού της ειρήνης. Η προετοιμασία αυτή αφορά στη διεξαγωγή επιχειρήσεων Κυβερνοπολέμου, του τύπου της Κυβερνοκατασκοπίας και της συλλογής τεχνικών πληροφοριών, οι οποίες διεξάγονται στον Κυβερνοχώρο των ενδεχόμενων αντιπάλων. Η διεξαγωγή επιχειρήσεων αυτού του τύπου, οι οποίες είναι διαφορετικές από τις συνήθεις στρατιωτικές δραστηριότητες και απαιτούν έγκριση σε υψηλό πολιτικό επίπεδο είναι μια ιδιαίτερα λεπτή υπόθεση. Μια τέτοια δραστηριότητα απαιτεί αποφασιστική πολιτική βούληση, η οποία δεν πρέπει να θεωρείται δεδομένη, ειδικά εφόσον δεν έχει καν τεθεί το θέμα.

Συμπερασματικά, η επιτυχής διεξαγωγή επιχειρήσεων Κυβερνοπολέμου προϋποθέτει θεμελιώδη αλλαγή νοοτροπίας του προσωπικού των Ενόπλων Δυνάμεων και ειδικότερα της πολιτικής και στρατιωτικής ηγεσίας, στενή συνεργασία όλων των εμπλεκόμενων φορέων σε εθνικό και διεθνές επίπεδο, κατάλληλη οργάνωση του φορέα του Κυβερνοπολέμου, κατάλληλη επιλογή και εκπαίδευση του προσωπικού, συμμετοχή στη διαδικασία Αμυντικής Σχεδίασης μέσω ειδικής προς το σκοπό αυτό ιδρυθεισόμενης υποεπιτροπής της επιτροπής Αμυντικής Σχεδίασης και πολιτικής βούλησης.

δ. Αναγκαιότητα ίδρυσης Διοίκησης Κυβερνοπολέμου στις Ένοπλες Δυνάμεις, καθώς και πιθανή οργάνωσή της.

Σήμερα, διάφοροι οργανισμοί του δημοσίου, εκτός των Ενόπλων Δυνάμεων, έχουν σημαντικές υποχρεώσεις όσον αφορά στην τρωτότητα των δικτύων υπολογιστών. Οι Ένοπλες Δυνάμεις έχουν τη γενική ευθύνη της υπεράσπισης του μέρους εκείνου των εθνικών υποδομών, το οποίο σχετίζεται με την εκτέλεση της αποστολής τους, αλλά δεν έχουν ηγετικό ρόλο σε σχέση με την ασφάλεια των δικτύων σε εθνικό επίπεδο. Είναι

προφανές ότι σε κυβερνητικό επίπεδο (επίπεδο Υψηλής Στρατηγικής) δεν υπάρχει φορέας υπεύθυνος για το συντονισμό των όποιων φορέων υπάρχουν διάσπαρτοι στον κρατικό μηχανισμό αλλά και στον ιδιωτικό τομέα της χώρας, και που θα μπορούσαν να αξιοποιηθούν στο πλαίσιο της σχεδίασης και διεξαγωγής επιχειρήσεων Κυβερνοπολέμου.

Η έλλειψη ενός κατάλληλα οργανωμένου και επανδρωμένου φορέα αποτελεί μια κρίσιμη αδυναμία στη δυνατότητα της χώρας να αντιμετωπίσει απειλές Κυβερνοπολέμου και να αντιδράσει ανάλογα, και συνεπάγεται έλλειψη συντονισμού μεταξύ των υπηρεσιών του δημοσίου και αυτών με τον ιδιωτικό τομέα για τη σύνταξη ενός σχεδίου και την υιοθέτηση ενός μηχανισμού άμυνας εναντίον της σύγχρονης απειλής. Η ίδρυσή του είναι πλέον ένα επείγον θέμα σε υψηλό πολιτικο-στρατιωτικό επίπεδο, έτσι ώστε να διασφαλιστεί ότι η χώρα μελλοντικά θα διαθέτει τις απαιτούμενες δυνατότητες για την αντιμετώπιση Κυβερνοαπειλών και τη διεξαγωγή επιθετικών επιχειρήσεων Κυβερνοπολέμου.

Ο Κυβερνοπόλεμος είναι θέμα εθνικής ασφαλείας. Το επίπεδό του είναι κατηγορηματικά ανώτερο αυτού των Ενόπλων Δυνάμεων. Η δραστηριοποίησή του εντός του πλαισίου των Ενόπλων Δυνάμεων οφείλεται σε συγκεκριμένους λόγους, όπως απαριθμούνται στην ανάλογη υποπαράγραφο της παρούσας μελέτης, οι οποίοι λίγο έχουν να κάνουν με τη σπουδαιότητά του για την πολιτική εθνικής ασφαλείας. Όμως, η ενασχόληση των Ενόπλων Δυνάμεων με τον Κυβερνοπόλεμο έγινε μάλλον για λόγους εναρμόνισης της χώρας μας με τις υπόλοιπες χώρες-μέλη του ΝΑΤΟ και όχι για την κάλυψη πραγματικών αναγκών.

Η ευκαιρία για τις Ένοπλες Δυνάμεις έχει παρουσιαστεί προ πολλού και αυτές δεν πρέπει να την αφήσουν ανεκμετάλλευτη. Παρακινούμενες από τα αισθήματα της ευθύνης και του καθήκοντος, αρετές διαχρονικές που πάντοτε ενέπνεαν το σύνολο του προσωπικού τους, πρέπει να δημιουργήσουν έναν φορέα εθνικού επιπέδου, ο οποίος θα αποτελέσει το όχημα για την αφύπνιση των αρμοδίων λοιπών οργάνων της πολιτείας και την ανάδειξη του προβλήματος του Κυβερνοπολέμου σε θέμα εθνικής ασφάλειας που θα συμπαρασύρει τους υπόλοιπους ενδιαφερόμενους δημόσιους και ιδιωτικούς φορείς στην οργάνωση του τομέα του Κυβερνοπολέμου· το πρόβλημα υπάρχει και η λύση του απαιτεί επίδειξη στιβαρής και υπεύθυνης ηγεσίας.

Ένα σοβαρό θέμα που θα πρέπει να ληφθεί υπόψη όσον αφορά στην ανάληψη ηγετικού ρόλου από τις Ένοπλες Δυνάμεις στο θέμα του Κυβερνοπολέμου και το οποίο θα πρέπει να επιλυθεί στα αρχικά στάδια, ενδεχομένως ακόμα και με αλλαγή της αποστολής των Ενόπλων Δυνάμεων, είναι ότι η εμπλοκή του στρατού θα σημάνει αυτόματα τη δράση του στο εσωτερικό της χώρας και σε δραστηριότητες που περιλαμβάνουν είσοδο σε δίκτυα, παρακολούθηση τηλεπικοινωνιών, είτε για τον εντοπισμό της τρωτότητας των δημόσιων και ιδιωτικών συστημάτων είτε για την οργάνωση της άμυνας των συστημάτων και την αποτελεσματική προστασία τους. Αυτές όμως είναι δραστηριότητες οι οποίες βρίσκονται εκτός της αποστολής του Στρατού και, δεδομένου και του σχετικά πρόσφατου ιστορικού των Ενόπλων Δυνάμεων στην Ελλάδα, θα προκαλούσαν ποικίλες και απόλυτα δικαιολογημένες αντιδράσεις.

Μια τέτοια προσπάθεια απαιτεί την απαλλαγή του προς δημιουργία νέου φορέα από τα δεσμά της γραφειοκρατίας και την ανάδειξή του σε ένα πραγματικό συντελεστή ισχύος της χώρας, ο οποίος μόνο για λόγους Διοίκησης και Ελέγχου θα

λειτουργεί στα πλαίσια των Ενόπλων Δυνάμεων. Ένας τέτοιος φορέας μπορεί να είναι του τύπου μιας κατάλληλα οργανωμένης Διοίκησης Κυβερνοπολέμου. Η ίδρυση βέβαια μιας τέτοιας Διοίκησης εγείρει πολλά και σημαντικά οργανωτικά θέματα, μη συνυπολογιζομένων των θεμάτων της ίδρυσης εκ του μηδενός μιας ακόμη Διοικήσεως και της αντίστοιχης αύξησης της οροφής των Ενόπλων Δυνάμεων, όπως επίσης και θέματα Διοικήσεως και Ελέγχου.

Η αποστολή της Διοίκησης Κυβερνοπολέμου ουσιαστικά θα «αναπτυχθεί» σταδιακά, μετά την ίδρυσή της. Υπάρχουν όμως ορισμένες λειτουργίες που είναι ουσιαστικές, και οι οποίες εξετάζονται στη συνέχεια.

- Υπάρχουν πλευρές του Κυβερνοπολέμου που απαιτούν συντονισμό σε εθνικό επίπεδο και κατά συνέπεια η Διοίκηση θα πρέπει να αποτελεί ένα εθνικό μέσο, το οποίο θα υπηρετεί την Υψηλή Στρατηγική. Θα πρέπει να δέχεται οδηγίες και κατευθύνσεις, να αναφέρεται, και να συνεργάζεται με υπηρεσίες σε διάφορα επίπεδα.
- Η δραστηριότητα της Διοίκησης θα είναι αμυντική και επιθετική ταυτόχρονα. Η συμβίωση των δύο είναι αμοιβαία επωφελής. Η αναζήτηση τρωτών σημείων για την εισβολή στα συστήματα των αντιπάλων αποκαλύπτει ταυτόχρονα και τα δικά μας τρωτά σημεία, ενώ ο εντοπισμός των δικών μας τρωτών σημείων αποκαλύπτει συνήθως τρόπους εισβολής στα Κυβερνοσυστήματα του αντιπάλου.
- Βασική μέριμνα της Διοίκησης θα πρέπει να αποτελέσει η χαρτογράφηση των συστημάτων επικοινωνιών και πληροφορικής όλων των πιθανών αντιπάλων και η μελέτη των ηλεκτρονικών υποσυστημάτων των κύριων οπλικών συστημάτων (έρευνα).
- Αποστολή επίσης της Διοίκησης θα πρέπει να αποτελέσει η εκπόνηση ενδεχομένων σχεδίων, τόσο αμυντικών όσο και επιθετικών.
- Η Κυβερνοκατασκοπία είναι μια δραστηριότητα την οποία θα πρέπει η Διοίκηση να αναπτύξει από του καιρού της ειρήνης για την υποστήριξη ενδεχόμενων επιχειρήσεων Κυβερνοπολέμου, όποτε αυτές διεξαχθούν.

Όπως σε κάθε οργανισμό του οποίου αποστολή είναι η διεξαγωγή επιχειρήσεων, κεντρικό ρόλο στη Διοίκηση Κυβερνοπολέμου πρέπει να διαδραματίζει ένα κέντρο το οποίο θα αποτελεί την καρδιά όχι μόνο της Διοίκησης Κυβερνοπολέμου, αλλά και της παρακολούθησης και του ελέγχου της δραστηριότητας στον «ελληνικό» κυβερνοχώρο· το Κέντρο Συντονισμού Επιχειρήσεων Κυβερνοπολέμου (ΚΣΕΚ). Η λειτουργία του κέντρου θα πρέπει να είναι 24ωρη, με αποστολή την παρακολούθηση της δραστηριότητας στον Κυβερνοχώρο, και την έγκαιρη ενημέρωση όλων των εμπλεκομένων φορέων περί της εκδήλωσης επικείμενων ή σε εξέλιξη Κυβερνοεπιθέσεων. Προϋπόθεση της έγκαιρης αντίδρασης του Κέντρου, είναι η διασύνδεσή του με όλους του ενδιαφερόμενους φορείς μέσω επικοινωνιακών και πληροφοριακών δικτύων. Επίσης, ανάλογα με την εξουσιοδότησή του, το Κέντρο θα μπορούσε να ενεργοποιήσει επιθετικά μέτρα Κυβερνοπολέμου, ως αντίποινα ενδεχόμενης Κυβερνοεπιθέσεως, για λόγους ταχύτητας αντίδρασης.

5. ΜΕΛΛΟΝΤΙΚΕΣ ΕΞΕΛΙΞΕΙΣ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΠΟΛΕΜΟΥ

Οι υφιστάμενες δυνατότητες διεξαγωγής Κυβερνοπολέμου, σε συνδυασμό με το υφιστάμενο επίπεδο των υποδομών επικοινωνιακών και πληροφοριακών δικτύων δεν επιτρέπουν προς το παρόν τη διεξαγωγή αυτοδύναμου Κυβερνοπολέμου, παρά μόνο σε περιορισμένη κλίμακα και πάντοτε σε συνδυασμό με την απειλή χρήσης βίας και πολύ πιθανή τελική κλιμάκωσή του σε θερμή σύγκρουση.

Όμως, η ανακοπή της τεχνολογικής προόδου είναι αδύνατη. Αντίθετα, στο μέλλον πρόκειται να εξελίσσεται με ολοένα αυξανόμενο ρυθμό, ιδιαίτερα στους τομείς των ηλεκτρονικών, των επικοινωνιών και της πληροφορικής. Το κράτος και οι μεγάλες επιχειρήσεις και οργανισμοί θα εξαρτώνται όλο και περισσότερο από την τεχνολογία των επικοινωνιών και της πληροφορικής. Ως συνέπεια, οι δυνατότητες διεξαγωγής Κυβερνοπολέμου θα συνεχίσουν να εξελίσσονται και θα γίνουν ευρύτερα διαθέσιμες· επίσης θα συνεχίσουν να προηγούνται από τα αντίστοιχα αντίμετρα.

Οι επιθέσεις DoS/DDoS που είδαμε στην περίπτωση της Εσθονίας, στο μέλλον θα πάρουν ένα εντελώς καινούργιο νόημα, στο πλαίσιο ενός καλύτερα σχεδιασμένου και διευρυμένου Κυβερνοπολέμου. Στην περίπτωση αυτή οι προσβαλλόμενες υπηρεσίες δεν θα είναι απλώς αυτές που παρέχουν πρόσβαση στο διαδίκτυο, αλλά τα συστήματα που παρέχουν υποστήριξη σε κρίσιμες υποδομές εθνικού επιπέδου, συστήματα τα οποία δεν είναι σχεδιασμένα να αντέχουν σε παρατεταμένη διακοπή της λειτουργίας τους. Μια παρατεταμένη διακοπή της λειτουργίας του συστήματος παραγωγής και διανομής ηλεκτρικού ρεύματος, για παράδειγμα, θα έχει σοβαρές επιπτώσεις στο σύστημα υγείας και άλλων υπηρεσιών εκτάκτων αναγκών. Μια διακοπή του συστήματος αντιμετώπισης επειγόντων περιστατικών σε μεγάλες πόλεις δεν θα έχει επιπτώσεις μόνο στη ζωή των ατόμων που χρειάζονται αυτές τις υπηρεσίες, αλλά θα έχει ως συνέπεια την απώλεια της εμπιστοσύνης του λαού στη δυνατότητα της κυβέρνησης να παράσχει βασικές υπηρεσίες οι οποίες θεωρούνται δεδομένες. Όσο γίνεται γνωστό ότι οι επιθέσεις έχουν επιπτώσεις σε άλλες υποδομές όπως οι επικοινωνίες, οι μεταφορές και το νερό, το επίπεδο του φόβου και της απώλειας εμπιστοσύνης θα αρχίσει να επηρεάζει το βασικό κοινωνικό ιστό. Επιθέσεις εναντίον της οικονομικής υποδομής θα υποβαθμίσουν τις δυνατότητες των επιχειρήσεων να λειτουργούν κανονικά και ο λαός θα αρχίσει να αμφιβάλει για τη ασφάλεια των προσωπικών οικονομικών του, συμπεριλαμβανομένων των συντάξεων, των επενδύσεων και των αποταμιεύσεων.

Η εξέλιξη της τεχνολογίας θα επιτρέψει την ανακάλυψη Κυβερνοόπλων βελτιωμένου τύπου, ενώ ταυτόχρονα θα αυξήσει τον αριθμό των κρίσιμων υποδομών των χωρών οι οποίες θα εξυπηρετούνται με συστήματα ICS. Ο συνδυασμός αυτός θα αυξήσει την καταστρεπτικότητα των επιχειρήσεων Κυβερνοπολέμου. Αυτή η αύξηση της καταστρεπτικότητας με τη σειρά της θα επιτρέψει στον Κυβερνοπόλεμο να επιδιώξει την επίτευξη σοβαρότερων πολιτικών σκοπών, όπως επίσης και να παράσχει καλύτερη υποστήριξη στους άλλους συντελεστές ισχύος του κράτους.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

α. Ο Κυβερνοπόλεμος πέρασε από την εποχή των αθώων ερασιτεχνών, των οποίων η φιλοδοξία έφθανε μέχρι την πραγματοποίηση δωρεάν τηλεφωνικών κλήσεων

μέσω του διεθνούς τηλεφωνικού δικτύου, στην εποχή των υστερόβουλων επαγγελματιών οι οποίοι έχουν πλέον τη δυνατότητα να προσβάλλουν τις κρίσιμες υποδομές μιας χώρας, καταστρέφοντας σταθμούς παραγωγής ηλεκτρικής ενέργειας ή ανοίγοντας φράγματα υδάτων.

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

γ. Ο Κυβερνοχώρος είναι ένα άναρχο σύστημα στο οποίο δραστηριοποιούνται διάφορες κατηγορίες δραστών, όπως χάκερ, ακτιβιστές-χάκερ, οργανωμένο έγκλημα, δράστες βιομηχανικής κατασκοπίας, εσωτερικοί δράστες, εξωτερικοί συνεργάτες/σύμβουλοι, τρομοκρατικές οργανώσεις και χώρες.

δ. Τίποτα στο υφιστάμενο διεθνές νομικό πλαίσιο δεν απαγορεύει ρητά τις επιχειρήσεις Κυβερνοπολέμου. Όμως, η εφαρμογή τους θα πρέπει να υπόκειται σε νομικούς περιορισμούς οι οποίοι θα έχουν συμφωνηθεί από κοινού από όλα τα κράτη, στα πλαίσια διεθνών συμφωνιών. Προς το παρόν, πολλά κρίσιμα θέματα που σχετίζονται με τον Κυβερνοπόλεμο παραμένουν άλυτα. Σήμερα, δεν υπάρχει κανένα διεθνές, νομικά δεσμευτικό, εργαλείο το οποίο να χαρακτηρίζει την Κυβερνοεπίθεση απειλή για την εθνική ασφάλεια μιας χώρας.

ε. Ο Κυβερνοπόλεμος αποτελεί τον τέταρτο πυλώνα ισχύος του κράτους (με τους άλλους τρεις να είναι η οικονομία, η διπλωματία και η στρατιωτική ισχύς) και συνεπώς εντάσσεται στη σχεδίαση της Υψηλής Στρατηγικής ενός κράτους για την επίτευξη του εκάστοτε καθοριζομένου πολιτικού σκοπού σε σχέση με κάποιον αντίπαλο.

στ. Πολιτικοί σκοποί οι οποίοι θα μπορούσαν να επιδιωχθούν με την αποκλειστική προσφυγή στον Κυβερνοπόλεμο είναι η απλή παρενόχληση, η προειδοποίηση χώρας πριν τη λήψη σημαντικών αποφάσεων στο πλαίσιο διεθνών οργανισμών για τους κινδύνους που διατρέχει αν αρνηθεί τη θετική ψήφο και η εκδίκηση για τυχόν αποφάσεις που ελήφθησαν χωρίς να ληφθούν υπόψη τα συμφέροντα της ενδιαφερόμενης χώρας.

ζ. Ως αποστολή του Κυβερνοπολέμου μπορεί να ορισθεί η προστασία των κρίσιμων υποδομών του κράτους μέσω της προστασίας όλων των δικτυοκεντρικών συστημάτων, δημόσιων και ιδιωτικών, από ενδεχόμενες επιθέσεις που θα είχαν ως στόχο την υποβάθμιση της λειτουργίας τους και την πρόκληση λειτουργικών ή φυσικών βλαβών, και η πρόκληση αντιστοίχων αποτελεσμάτων στον αντίπαλο, στα πλαίσια της χαραχθείσας εθνικής στρατηγικής ασφαλείας.

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

- Οι κρίσιμες υποδομές μιας χώρας.
- Ο επηρεασμός της παγκόσμιας κοινής γνώμης μέσω του πληροφοριακού πολέμου.
- Τα συστήματα επικοινωνιών και πληροφορικής των Ενόπλων Δυνάμεων.

θ. Ο Κυβερνοπόλεμος είναι μια δραστηριότητα η οποία δεν σχετίζεται αποκλειστικά με τις Ένοπλες Δυνάμεις, και η σχέση του προς αυτές μπορεί να είναι μόνο σχέση υποστηρίζοντος – υποστηριζομένου. Φαίνεται όλο και πιο πιθανό ότι η πρώτη ενέργεια – επίθεση οποιασδήποτε μελλοντικής αναμέτρησης μεταξύ τεχνολογικά προηγμένων αντιπάλων θα είναι ηλεκτρονική και θα διεξαχθεί στον ή μέσω του

Κυβερνοχώρου. Η υποστήριξη των επιχειρήσεων του κλασικού πολέμου από τον Κυβερνοπόλεμο, γίνεται μέσω της ανάθεσης κατάλληλων αποστολών στα μέσα του Κυβερνοπολέμου, σε πλήρη συντονισμό με το γενικό σχέδιο επιχειρήσεων.

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

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

ιβ. Ο Πληροφοριακός πόλεμος χρησιμοποιεί τον Κυβερνοπόλεμο ως όργανό του, μέσω του οποίου προωθεί τις θέσεις του (έστω και με παραπληροφόρηση και διασπορά ψευδών ειδήσεων) στο διαδίκτυο, παρεμποδίζοντας ταυτόχρονα την πληροφόρηση του κοινού μέσω των ιστοσελίδων του αντιπάλου του.

ιγ. Ο Κυβερνοχώρος παρέχει σε κρατικούς και μη κρατικούς δρώντες την ευκαιρία να αντισταθμίσουν το πλεονέκτημα των ισχυρότερων από αυτούς αντιπάλων από την άποψη της συμβατικής στρατιωτικής ισχύος. Σε μια αντιπαράθεση δύο χωρών όπου παρουσιάζεται ασυμμετρία όσον αφορά στη θέση τους στο παγκόσμιο σύστημα ισχύος, ο Κυβερνοπόλεμος αποτελεί ελκυστική επιλογή για το λιγότερο ισχυρό αντίπαλο, λόγω του ότι παρέχει έναν γρήγορο, σχετικά φτηνό και αποτελεσματικό τρόπο για την υπονόμευση των κρίσιμων, πλην όμως τρωτών, υποδομών του αντιπάλου.

ιδ. Οι τρομοκρατικές οργανώσεις έχουν από καιρού προχωρήσει σε ευρεία χρήση του διαδικτύου για την εξυπηρέτηση μιας μεγάλης ποικιλίας σκοπών, οι οποίοι στο μέλλον θα συμπεριλάβουν την πρόκληση ανθρωπίνων απωλειών. Όμως το ίδιο το διαδίκτυο δεν αποτελεί στόχο και δεν φαίνεται να υπάρχει προς το παρόν καμία «ηλεκτρονική» τρομοκρατική οργάνωση η οποία θα εξαπέλυε μια Κυβερνοεπίθεση στο διαδίκτυο με στόχο τη διακοπή της λειτουργίας του και την καταστροφή του. Τρεις είναι οι παράγοντες οι οποίοι καθιστούν τις Κυβερνοεπιθέσεις στο ίδιο το διαδίκτυο λιγότερο ελκυστικές για τις τρομοκρατικές οργανώσεις.

- Τα Κυβερνοόπλα είναι λιγότερο αποτελεσματικά σε σχέση με άλλες δυνατότητες, από την άποψη ότι δεν έχουν τις ίδιες ψυχολογικές ή πολιτικές επιπτώσεις και δεν έχουν νεκρούς.
- Η πολυπλοκότητα των Κυβερνοεπιθέσεων στις κρίσιμες υποδομές έχει μικρότερες πιθανότητες επιτυχίας
- Το διαδίκτυο εξυπηρετεί και τους δικούς τους σκοπούς.

ιε. Η εξελισσόμενη απειλή του Κυβερνοπολέμου απαιτεί σοβαρές και συνεπείς επενδύσεις στη νέα τεχνολογία και συνεργασία με τα Εκπαιδευτικά Ιδρύματα της χώρας.

ιζ. Το κόστος της επένδυσης στον τομέα του Κυβερνοπολέμου είναι γενικώς μικρότερο σε σχέση με αυτό της ασφάλειας όπως αυτή είναι γνωστή μέχρι σήμερα. Το μεγαλύτερο κόστος της επένδυσης αφορά στους ανθρώπινους πόρους, οι οποίοι αποτελούν το κλειδί για κάθε σχετική προσπάθεια. Η δημιουργία εξειδικευμένου προσωπικού είναι μία ακριβή και χρονοβόρα διαδικασία.

ιθ. Απαραίτητη προϋπόθεση για την επιλογή μιας πολιτικής οντότητας (χώρας ή οργάνωσης) ως στόχου Κυβερνοπολέμου είναι η οργάνωσή της έτσι ώστε να παρουσιάζει κατάλληλο στόχο. Με την έννοια αυτή, μόνο τα κράτη ή οι υπερεθνικές οργανώσεις κρατών (συμμαχίες) μπορούν να αποτελέσουν στόχο επιχειρήσεων Κυβερνοπολέμου. Η απειλή ή η χρήση βίας στο πλαίσιο του Κυβερνοπολέμου, εναντίον χωρών με φτωχή επικοινωνιακή και πληροφοριακή υποδομή, θα πρέπει να συνοδεύεται πάντοτε με απειλή ή χρήση παραδοσιακού πολέμου.

κ. Οι χώρες – οργανώσεις οι οποίες πρέπει να αποτελέσουν από σήμερα αντικείμενο ελληνικού Κυβερνοενδιαφέροντος, λόγω της πιθανής εξέλιξής τους σε στρατιωτικές απειλές ή Κυβερνοαπειλές είναι, κατά σειρά προτεραιότητας, η Τουρκία, η FYROM, η Αλβανία, η Βουλγαρία, η Μεγάλη Βρετανία, η Ιταλία, η Γαλλία, οι ΗΠΑ, η Ρωσία, η Κίνα, η Γεωργία και η Al Qaeda.

κα. Σήμερα, καμία κυβερνητική υπηρεσία ή οργανισμός δεν φαίνεται να είναι υπεύθυνη για τη σχεδίαση και διεξαγωγή (επιθετικών) επιχειρήσεων Κυβερνοπολέμου. Το πλέον κατάλληλο υπουργείο για να φιλοξενήσει μια τέτοια δραστηριότητα, είναι το ΥΕΘΑ, και ειδικότερα το ΓΕΕΘΑ.

κβ. Η επιτυχής διεξαγωγή επιχειρήσεων Κυβερνοπολέμου προϋποθέτει θεμελιώδη αλλαγή νοοτροπίας του προσωπικού των Ενόπλων Δυνάμεων και ειδικότερα της πολιτικής και στρατιωτικής ηγεσίας, στενή συνεργασία όλων των εμπλεκόμενων φορέων σε εθνικό και διεθνές επίπεδο, κατάλληλη οργάνωση του φορέα του Κυβερνοπολέμου, κατάλληλη επιλογή και εκπαίδευση του προσωπικού, συμμετοχή στη διαδικασία Αμυντικής Σχεδίασης μέσω ειδικής προς το σκοπό αυτό ιδρυθεισόμενης υποεπιτροπής της επιτροπής Αμυντικής Σχεδίασης και πολιτικής βούλησης.

κγ. Είναι επιτακτική ανάγκη ίδρυσης ενός οργάνου Κυβερνοπολέμου, το οποίο θα λειτουργεί ως σημείο αναφοράς. Επειδή ο Κυβερνοπόλεμος, όπως και κάθε πόλεμος, είναι κρατική υπόθεση, ένα τέτοιο όργανο ιδανικά θα έπρεπε να τεθεί υπό την άμεση εποπτεία της κυβέρνησης, δεδομένου ότι αφορά όλους του τομείς της κυβερνητικής δραστηριότητας. Για πρακτικούς λόγους η ευθύνη οργάνωσης και λειτουργίας θα πρέπει να ανατεθεί σε έναν από τους εμπλεκόμενους φορείς, με καταλληλότερο, λόγω οργάνωσης, εμπειρίας και μεγαλύτερης συνάφειας, το Υπουργείο Εθνικής Αμύνης. Ο ρόλος του οργάνου βέβαια, αν και θα λειτουργεί στο πλαίσιο των Ενόπλων Δυνάμεων, θα είναι ευρύτερος, εξυπηρετώντας ευρύτερους στόχους οι οποίοι σχετίζονται με θέματα εθνικής ασφαλείας. Στο πλαίσιο αυτό, θα παρέχει βοήθεια σε θέματα Κυβερνοεπεισοδίων σε όλα τα Υπουργεία και συμβουλές για την καλύτερη προστασία των κρίσιμων υποδομών στον ιδιωτικό τομέα.

7. ΠΡΟΤΑΣΕΙΣ

α. Μέτρα που πρέπει να ληφθούν σε πολιτικό επίπεδο

(1) Μονομερής δήλωση από την Ελλάδα ότι θεωρεί τον Κυβερνοχώρο μέρος όπου ασκεί εθνική κυριαρχία. Προς υποστήριξη της δήλωσης να ασκήσει έλεγχο στα

Κυβερνοσύνορα, εξασφαλίζοντας μέσα για την απαγόρευση της κίνησης του διαδικτύου που προέρχεται από Υπηρεσίες Παροχής Υπηρεσιών (ISP) ή χώρες από τις οποίες προέρχονται οι Κυβερνοεπιθέσεις.

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

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

(4) Συνεργασία στο πλαίσιο του ΟΗΕ με σκοπό:

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

(5) Εισαγωγή κατευθύνσεων Κυβερνοασφάλειας στα τμήματα Πληροφορικής των πανεπιστημίων και χρηματοδότηση ερευνητικών προγραμμάτων και μεταπτυχιακών και διδακτορικών σπουδών με θέμα την Κυβερνοασφάλεια, με απώτερο στόχο την παραγωγή εξειδικευμένου προσωπικού το οποίο μελλοντικά θα στελεχώσει σχετικές θέσεις του ιδιωτικού και δημόσιου τομέα.

(6) Εκπόνηση μελέτης τρωτότητας της κρίσιμης υποδομής της χώρας (δημόσιας και ιδιωτικής) και περιοδική ενημέρωσή της σε τακτά διαστήματα, έτσι ώστε να αποτελέσει τη βάση για την οργάνωση αποτελεσματικής άμυνας εναντίον ενδεχόμενων Κυβερνοεπιθέσεων.

(7) Υιοθέτηση της προληπτικής επίθεσης ως αμυντικής τακτικής.

(8) Εκχώρηση του δικαιώματος λήψης απόφασης για την εκδήλωση προληπτικής Κυβερνοεπίθεσης σε κατάλληλο επίπεδο, για λόγους ταχύτητας αντίδρασης εξαιτίας του ελάχιστου χρόνου που απαιτείται για την εκδήλωση της Κυβερνοεπίθεσης του εχθρού.

(9) Αποκατάσταση συνεργασιών μεταξύ δημοσίου και ιδιωτικού τομέα στο εσωτερικό της χώρας, όπως επίσης και με άλλες χώρες και πολυεθνικούς οργανισμούς.

β. Μέτρα που πρέπει να ληφθούν σε στρατηγικό – επιχειρησιακό επίπεδο

(1) Ίδρυση Διοίκησης Κυβερνοπολέμου, με κατάλληλη οργάνωση και επάνδρωση και με εκπροσώπηση όλων των εμπλεκομένων φορέων του δημόσιου και ιδιωτικού τομέα.

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

(3) Σύνταξη της Εθνικής Πολιτικής Κυβερνοασφάλειας και Κυβερνοπολέμου, όπως επίσης και της Εθνικής Στρατηγικής Κυβερνοασφάλειας και Κυβερνοπολέμου.

(4) Συμπερίληψη του θέματος του Κυβερνοπολέμου σε όλα τα σχετικά θεσμικά κείμενα (Εθνική Στρατιωτική Στρατηγική).

(5) Μελέτη των δημόσιων και ιδιωτικών υποδομών της χώρας και έκδοση εγγράφου με τις κρίσιμες υποδομές οι οποίες χρήζουν προστασίας, κατά το πρότυπο των ΗΠΑ[38] και άλλων χωρών (Ολλανδία, Αυστραλία). Διεξαγωγή περιοδικών ελέγχων και δοκιμών για τον εντοπισμό της τρωτότητας των υποδομών, και του τρόπου αποκατάστασής της.

(6) Σχεδίαση και διεξαγωγή μιας ετήσιας, αυτοδύναμης άσκησης Κυβερνοπολέμου εθνικού επιπέδου, κατά το πρότυπο της σειράς των ασκήσεων CYBER STORM των ΗΠΑ. Συμμετοχή στην άσκηση όλων των εμπλεκομένων οργανισμών και υπηρεσιών, δημοσίων και ιδιωτικών, καθώς και των εκπαιδευτικών ιδρυμάτων της χώρας.

(7) Συμμετοχή σε ΝΑΤΟϊκές, Ευρωπαϊκές (της ΕΕ) και διακρατικές ασκήσεις Κυβερνοπολέμου.

(8) Συστηματική παρακολούθηση των χωρών Τουρκίας, FYROM, Αλβανίας, Βουλγαρίας, Μεγάλης Βρετανίας, Ιταλίας, Γαλλίας, ΗΠΑ, Ρωσίας, Κίνας, Γεωργίας και της Al Qaeda από την άποψη της δραστηριότητάς τους στον Κυβερνοχώρο των σχετικών δυνατοτήτων τους· μελέτη της τρωτότητας των συστημάτων τους σε Κυβερνοεπιθέσεις.

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

(10) Απομόνωση όλων των στρατιωτικών δικτύων επικοινωνιών και πληροφορικής από το διαδίκτυο, και αυστηρή τήρηση των ΥΦΙΣΤΑΜΕΝΩΝ κανόνων ασφαλείας.

(11) Οργάνωση της εκπαίδευσης στον Κυβερνοπόλεμο με στόχο την παραγωγή εξειδικευμένου προσωπικού. Εισαγωγή σχετικών μαθημάτων σε όλα τα παραγωγικά σχολεία των Ενόπλων Δυνάμεων. Οργάνωση ειδικού σχολείου για την εκπαίδευση προσωπικού που έχει άμεση σχέση με τον Κυβερνοπόλεμο, από όλες τις υπηρεσίες του Δημοσίου και του ιδιωτικού τομέα.

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

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

(14) Οργάνωση των χάκερ σε συλλόγους. Μέσω της οργάνωσης, της χρηματοδότησης και των συλλογικών δραστηριοτήτων θα είναι δυνατός ο έλεγχος και η κατεύθυνσή τους σε μια συντονισμένη και οργανωμένη προσπάθεια. Οι σύλλογοι αυτοί θα αποτελέσουν και τη δεξαμενή εξειδικευμένου προσωπικού από όπου θα γίνεται η επιλογή και πρόσληψη του προσωπικού του Κυβερνοπολέμου. Επίσης, ο εντοπισμός του

---

[38] Οι ΗΠΑ τον Οκτώβριο του 1997εξέδωσαν για πρώτη φορά το *Critical Foundation, Protecting America's Infrastructures*, το οποίο έκτοτε αναθεωρούν τακτικά. Διαθέσιμο στην ιστοσελίδα http://fas.org/sgp/library/pccip.pdf, (τελευταία επίσκεψη την 20 Φεβ 2010).

κατάλληλου προσωπικού θα επιτρέψει και την επιστράτευσή του σε κατάλληλες ειδικότητες.

(15) Μελέτη και υιοθέτηση Κανόνων Εμπλοκής Κυβερνοπολέμου σε συνδυασμό με κατάλληλους Ενδείκτες Κυβερνοεπιθέσεων.

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

8. ΕΠΙΛΟΓΟΣ

Η επιστήμη του πολέμου έχει προ πολλού εισέλθει στην εποχή της πληροφορικής. Τα θέματα του Κυβερνοπολέμου παρουσιάζουν αυξητικό εθνικό ενδιαφέρον και ανησυχία. Όλες οι πολιτικές και στρατιωτικές αντιπαραθέσεις έχουν πλέον μια Κυβερνοδιάσταση, της οποίας η έκταση και οι επιπτώσεις είναι δύσκολο να προβλεφθούν. Οι δράστες των Κυβερνοεπιθέσεων έχουν στη διάθεσή τους μια μεγάλη ποικιλία αποτελεσματικών στρατηγικών και τακτικών Κυβερνοπολέμου.

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

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

Ο Clausewitz, με τη διορατικότητα και την αναλυτική του σκέψη, διέβλεψε ότι «κάθε εποχή έχει το δικό της είδος πολέμου, τους δικούς της περιορισμούς και τις δικές της ιδιαίτερες προκαταλήψεις[39]». Η εποχή μας, η εποχή της πληροφορικής, δεν εξαιρείται, έχει το δικό της πόλεμο, τον Κυβερνοπόλεμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ -ΑΡΘΡΟΓΡΑΦΙΑ

1. Abrams Marshall, Joe Weiss, *Malicious Control System Cyber Security Attack Case Study, Maroochy Water Services*, Australia, August 2008, διαθέσιμο στην ιστοσελίδα http://csrc.nist.gov/sec-cert/ics/papers.html.

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

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

3. Arkin William M., *The Cyber Bomb in Yugoslavia*, washingtonpost.com, October 25, 1999, διαθέσιμο στην ιστοσελίδα http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

4. Bridis Ted & Sullivan Eileen, *US Video Shows Hacker Hit on Power Grid*, SFGATE.COM (SAN. FRAN. CHRON.), Sept. 27, 2007, http://www.sfgate.com/cgibin/article.cgi?f=/n/a/2007/09/26/national/w165704D09.DTL&type=politics.

5. Carafano James and Weitz Richard, Combating Enemies Online: State-Sponsored and Terrorist Use of the Internet, Backgrounder, No. 2105, February 8, 2008, διαθέσιμο στην ιστοσελίδα http://www.heritage.org/Research/nationalSecurity/upload/bg_2105.pdf.

6. Clausewitz Carl von, *On War*, Edited and Translated by M. Howard and Peter Paret, Princeton University Press, 1989.

7. Coleman Kevin, *Cyber Warfare Doctrine*, The Technolytics Institute, 1 June 2008, διαθέσιμο στην ιστοσελίδα http://www.technolytics.com/Cyber_Warfare_Doctrine_Public_Version.pdf.

8. Conti Gregory and Surdu John, *Army, Navy, Air Force and Cyber – Is it Time for a Cyberwarfare Branch of Military?*, IAnewsletter, Vol 12 No 1, Spring 2009, διαθέσιμο στην ιστοσελίδα http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf.

9. Counsil of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, διαθέσιμο στην ιστοσελίδα http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

10. Critical Infrastructure, *Threats and Terrorism*, US Army Training and Doctrine Command, 10 Aug 2006, διαθέσιμο στην ιστοσελίδα www.fas.org/irp/threat/terrorism/sup2.pdf.

11. Department of Homeland Security, National Cyber Security Division, Cyber Storm Exercise Report, 2009, διαθέσιμο στην ιστοσελίδα http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf.

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

13. European Security and Defense Assembly, Assembly of Western European Union, Fifty-fifth session, Document A/2022, *Cyber warfare*, 3 December 2008, διαθέσιμο στην ιστοσελίδα http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2008/2022.pdf.

14. Franzese Patrick W., *Sovereignty in cyber space: can it exist?*, The Air Force Law Review, Cyber Law Edition, Volume 64, 20 Nov 2009, Maxwell Air Force Base, Alabama διαθέσιμο στην ιστοσελίδα www.afjag.af.mil/library.

15. Geers Kenneth, US representative, Cooperative Cyber Defence Center of Excellence, Tallin, Esthonia, *Cyberspace and the changing nature of warfare*, διαθέσιμο στην ιστοσελίδα

http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf.

16. Hart Basil H. Liddell, *Strategy*, Εκδόσεις Meridian, 1991.

17. Hildreth Steven, *Cyber warfare*, CRS Report for (US) Congress, 19 July 2001.

18. Information Assurance, Situation in Switzerland and Internationally, Semi-annual report, 2009/1 (January – June), διαθέσιμο στην ιστοσελίδα http://wwww.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=en.

19. Institute for security technology studies at Dartmouth College, *Cyber Warfare: An analysis of the means and motivations of selected nation states*, Dec 2004.

20. Johns Hopkins Model United Nations Conference XII *Cyber Warfare*, March 5-8, 2009, Baltimore, Maryland, US.

21. Libicki Martin C., *Cyber Deterrence and Cyberwar*, RAND Corporation, 2009, διαθέσιμο στην ιστοσελίδα http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

22. Miller Robert A. and Kuehl Daniel T., *Cyberspace and the "first battle" in 21st-century war*, Defense Horizons, N. 68, September 2009, Center for Technology and National Security Policy, National Defense University, διαθέσιμο στην ιστοσελίδα http://www.ndu.edu/press/dh/DH68.pdf.

23. NATO Cooperative Cyber Defense Center of Excellence, *Cyber Attracts Against Georgia: Legal Lessons Identified*, 22 November 2008, διαθέσιμο στην ιστοσελίδα http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

24. New Cyber Security Operations Center to enhance cyber warfare capability, Ανακοίνωση του Υπουργείου Αμύνης της Αυστραλίας, 2 Μαΐου 2009.

25. Nye Joseph S. Jr., *Ήπια Ισχύς*, Εκδόσεις Παπαζήση, 2005.

26. Schaap Arie J., *Cyber warfare operations: Development and use under international law*, The Air Force Law Review Cyber Law Edition, Vol. 64, 20 November 2009, διαθέσιμο στην ιστοσελίδα www.afjag.af.mil/library.

27. Sun Tzu, *The Art of War*, Εκδόσεις Επικοινωνίες ΑΕ, Αθήνα 2002, Μετ. Πάνος Πικραμένος.

28. TechWeb.Com, Technocyclopedia, *Denial of Service Attack*, διαθέσιμο στην ιστοσελίδα http://www.techweb.com/encyclopedia/defineterm.jhtml?term=denialofserviceattack.

29. *The Air Force Law Review, Cyber Law Edition, Volume 64, 20 Nov 2009*, Maxwell Air Force Base, Alabama διαθέσιμο στην ιστοσελίδα www.afjag.af.mil/library/

30. Todd Graham H., *Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition*, The Air Force Law Review Cyber Law Edition, Vol. 64, 20 November 2009 διαθέσιμο στην ιστοσελίδα www.afjag.af.mil/library.

31. US DoD, Quadrennial Defense Review, Feb 2010, διαθέσιμο στην ιστοσελίδα http://www.defense.gov/QDR.

32. Waters Gary, Ball Desmond and Dudgeon Ian, Australia and Cyber-Warfare, The Australian National University διαθέσιμο στην ιστοσελίδα http://epress.anu.edu.au/cyber_warfare_citation.html.

33. Κολιόπουλος Κωνσταντίνος, *Η στρατηγική σκέψη από την αρχαιότητα έως σήμερα*, Εκδόσεις Ποιότητα, Αθήνα, 2008.

34. Μπαμπινιώτης Γεώργιος, *Λεξικό της νέας ελληνικής γλώσσας*, Εκδόσεις Κέντρο Λεξικολογίας ΕΠΕ, Αθήνα, Ιαν 2002.

35. Νόμος Υπ' Αριθ. 3649, 3 Μαρ 2008, Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις.

Αναφορά στο άρθρο: Μαυρόπουλος Παναγιώτης. *Κυβερνοπόλεμος και Εθνική Στρατηγική*. Πόλεμος και Στρατηγική, 19 Ιαν 204, www.warandstrategy.gr.

** Ο Παναγιώτης Μαυρόπουλος είναι Αντγος ε.α.*