Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών

Τμήμα Διεθνών, Ευρωπαϊκών και Περιφερειακών Σπουδών

Π.Μ.Σ. Διεθνείς και Ευρωπαϊκές Σπουδές

Ειδίκευση: Διεθνές Δίκαιο και Διπλωματικές Σπουδές

Διπλωματική Εργασία

«ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ, ΜΙΑ ΣΥΓΧΡΟΝΗ ΠΑΓΚΟΣΜΙΑ ΑΠΕΙΛΗ ΚΑΙ ΤΑ ΖΗΤΗΜΑΤΑ ΔΙΕΘΝΟΥΣ ΔΙΚΑΙΟΥ ΠΟΥ ΑΝΑΚΥΠΤΟΥΝ»

Φοιτήτρια: Αικατερίνη Δεληγιάννη του Γεωργίου

Αρ. Μητρώου: 1214Μ003

Επιβλέπων Καθηγητής: κ. Περράκης Ε. Στέλιος

Αθήνα 2015

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Το τέλος του Ψυχρού Πολέμου στις αρχές της δεκαετίας του ΄90 και η μετατροπή του σύγχρονου διεθνούς συστήματος από διπολικό σε πολυπολικό αποτέλεσε μια θεμελιώδη καινοτομία αναφορικά με την θεώρηση των διεθνών σχέσεων. Ο πρώτος πόλεμος στον Περσικό Κόλπο (1990-1991) απέδειξε ολοφάνερα, ότι η χρήση της τεχνολογίας στις στρατιωτικές επιχειρήσεις και δομές προσέφερε στις ΗΠΑ και στους Συμμάχους ένα σημαντικό πλεονέκτημα κατά την διάρκεια των ενόπλων συρράξεων. Η επιτυχής έκβαση για τους Συμμάχους οφείλεται στην εκτεταμένη χρήση ηλεκτρονικών υπολογιστών, « έξυπνων βομβών» και στην σωστή λειτουργία του λογισμικού που ήταν ενσωματωμένος στους ηλεκτρονικούς υπολογιστές. Το αποτέλεσμα του πολεμικού αυτού φαινομένου εγκαινίασε μια καινούργια στρατηγική στα πλαίσια της Επανάστασης στις Στρατιωτικές Υποθέσεις (RMA, Revolution in Military Affairs). Σύμφωνα με τον Andrew Marshall «Μια επανάσταση στις στρατιωτικές υποθέσεις είναι μια σημαντική αλλαγή στη φύση του πολέμου που επέφερε την καινοτόμο εφαρμογή των νέων τεχνολογιών, οι οποίες σε συνδυασμό με τις δραματικές αλλαγές στο στρατιωτικό δόγμα και στις λειτουργικές και οργανωτικές έννοιες, μεταβάλλει ριζικά το χαρακτήρα και τη συμπεριφορά των στρατιωτικών λειτουργιών»[1]. Την ίδια περίδο το Διαδίκτυο γίνεται προσιτό στο ευρύ κοινό και χαρακτηριστικό πλέον γνώρισμα της μεταψυχροπολεμικής εποχής είναι η ολοένα και αυξανόμενη εξάρτηση της κοινωνίας από την πληροφορία. Η παγκόσμια κοινωνία μεταβάλλεται ραγδαία σε μια κοινωνία της πληροφορίας, ενώ η ευρεία χρήση της ψηφιακής τεχνολογίας δημιούρησε νέα δεδομένα και επιπτώσεις σε ποικίλους τομείς της ανθρώπινης δραστηριότητας. Τόσο οι απλοί πολίτες όσο και οι επιχειρήσεις χρησιμοποιούν το Ίντερνετ για τις καθημερινές τους δραστηριότητες με σχετικά χαμηλό κόστος φέρνοντας έτσι στην επιφάνεια την έννοια του κυβερνοχώρου, του εικονικού δηλαδή χώρου, όπου διεξάγονται καθημερινά εκατομμύρια μεταφορές

[1] http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html

δεδομένων και πληροφοριών. Ο χώρος όμως αυτό μπορεί εύκολα να μετατραπεί και σε πεδίο δειξαγωγής συγκρούσεων καθώς και παράνομων δραστηριοτήτων όπως η υπεξαίρεση και η αλλοίωση ψηφιακών δεδομένων, αν λάβει κανείς υπόψη του την ραγδαία εμφάνιση διαφόρων μορφών κακόβουλου λογισμικού. Ιδιαίτερα μετά την διεξαγωγή του Πρώτου Περσικού Πολέμου , οι συγκρούσεις στον κυβερνοχώρο επεκτάθηκαν και στο πεδίο των Ενόπλων Δυνάμεων. Η ριζική αυτή αλλαγή που επέφερε η πληροφοριακή επανάσταση έχει αντίκτυπο και στο πεδίο του Διεθνούς Δικαίου αλλά και της εθνικής ασφάλειας. Ενώ μέχρι τώρα η τελευταία αφορούσε απειλές κατά της εδαφικής κυριαρχίας και ακεραιότητας ενός κράτους, τώρα πλέον απειλούνται διάφορα πληροφοριακά συστήματα, όπως το φορολογικό, το τραπεζικό, τα οποία στηρίζουν την λειτουργία τους στο Διαδίκτυο. Σταδιακά εμφανίσθηκαν νέοι όροι όπως ο πληροφοριακός πόλεμος, ο κυβερνόπολεμος , μια ειδικότερη μορφή του, ο οποίος θα αποτελέσει και το αντικείμενο της παρούσας εργασίας, ο κυβερνοχώρος και οι κυβερνοεπιθέσεις, όροι τους οποίους θα αναπτύξουμε στην συνέχεια. Όλη αυτή η συνεχώς μεταβαλλόμενη κατάσταση και οι κίνδυνοι που ελλοχεύουν, οδήγησε ένα μεγάλο μέρος της ακαδημαϊκής κοινότητας να ασχοληθεί με την νέα αυτή παγκόσμια απειλή, τον κυβερνοπόλεμο, ο οποίος παρουσιάζει αρκετές ιδιαιτερότητες αλλά και μεγάλες αποκλίσεις από την παραδοσιακή έννοια του πολέμου.

Πρωταρχικός στόχος της εργασίας αυτής είναι όχι μόνο η μελέτη και παρουσίαση ενός σύγχρονου φαινομένου, του Κυβερνοπολέμου, ο οποίος αποτελεί συστατικό στοιχείο του Πληροφοριακού Πολέμου και συνδέεται με τον τελευταίο με μια σχέση ειδικού προς γενικό αλλά και η νομική προσέγγιση του ζητήματος, δηλαδή η αναγωγή των ιδιαίτερων χαρακτηριστικών του στο υπάρχον νομικό πλαίσιο Διεθνούς Δικαίου. Ο όρος Πληροφοριακός Πόλεμος χρησιμοποιείται για να αποδώσει κυρίως την ένοια της στρατηγικής θεωρίας, πυρήνας της οποίας είναι η πληροφορία [2]. Επιπρόσθετα θα γίνει μια προσπάθεια επεξήγησης και αποσαφηνισμού και άλλων επιμέρους όρων που συνθέτουν το φαινόμενο του κυβερνοπολέμου, όπως κυβερνοχώρος

[2] Γρίβας Κ., « Ο Πόλεμος στον 21^{ο} αιώνα», Εκδ. Επικοινωνίες Α.Ε, Αθήνα , 1999, σελ. 28

κυβερνοεπιθέσεις, όπλα - τεχνικές αυτών, κρατικοί δρώντες και κρίσιμες κρατικές υποδομές.

Στο πρώτο κεφάλαιο της διπλωματικής εργασίας γίνεται προσπάθεια να προσδιοριστεί σφαιρικά η έννοια του Κυβερνοπολέμου, κάνοντας ενδελεχή αναφορά στις μορφές που μπορεί αυτός να λάβει, στους στόχους και τα κίνητρα τέλεσης του. Επιπρόσθετα θα αναλυθεί η συμμετοχή τόσο των κρατών όσο και των μη κρατικών δρώντων στις συγκρούσεις και τις επιχειρήσεις που λαμβάνουν χώρα, ενώ τέλος θα γίνει μια ενδεικτική αναφορά σε τέσσερα προηγμένα τεχνολογικά κράτη, τα οποία έχουν υπάρξει στο παρελθόν και θύτες και θύματα των Κυβερνοεπιθέσεων. Αναλύεται η έννοια του Κυβερνοχώρου, του πεδίου αντιπαράθεσης, όπου λαμβάνουν χώρα οι συγκρούσεις και οι κυβερνοεπιθέσεις. Πρόκειται στην ουσία για έναν εικονικό χώρο ή αλλιώς ένα «θέατρο επιχειρήσεων», μην δυναμένο να εντοπιστεί σε συγκεκριμένο γεωγραφικό πλάτος και μήκος. Επιπλέον θα αναλυθούν τα χαρακτηριστικά του, τα επίπεδα λειτουργίας του αλλά και τυχόν δομικές αδυναμίες. Επίσης στο κεφάλαιο αυτό θα γίνει σύντομη αναφορά και στο Διαδίκτυο (Internet), το οποίο αποτελε το βασικότερο σήμερα μέσο μαζικής επικοινωνίας και ένα αυτοτελές σύστημα δημιουργώντας το δικό του Κυβερνοχώρο . Θα αναφερθούμε ακόμη στις πρώιμες μορφές του αλλά και στο ρόλο του στη σύγχρονη εποχή.

Στο δεύτερο κεφάλαιο αναλύονται τα διάφορα είδη επιχειρήσεων στον κυβερνοχώρο, κατηγορία των οποίων αποτελούν και οι κυβερνοεπιθέσεις, το « νομικό» καθεστώς αυτών, οι στόχοι οι οποίοι βάλλονται από αυτές αλλά και τα «όπλα» που χρησιμοποιούνται για την διεξαγωγή τους. Τέλος θα γίνει καταγραφή ορισμένων περιστατικών κυβερνοεπιθέσεων που σημειώθηκαν τις τελευταίες δεκαετίες στο χώρο της διεθνούς σκηνής και των συνεπειών που αυτές επέφεραν.

Στο τρίτο και τελευταίο κεφάλαιο θα ασχοληθούμε με την νομική αντιμετώπιση του φαινομένου και τους σχετικούς προβληματισμούς που εγείρονται σχετικά με αυτό από την σκοπιά του Διεθνούς Δικαίου. Θα γίνει μια προσπάθεια αναγωγής των ιδιαίτερων χαρακτηριστικών και των αποτελεσμάτων του

Κυβερνοπολέμου στο νομικό πλαίσιο του συμβατικού διεθνούς δικαίου, θα αναφερθούμε σε ορισμένες διατάξεις του Καταστατικού Χάρτη του ΟΗΕ σχετικά τη χρήση βίας και την ένοπλη επίθεση καθώς και στο διεθνές εθιμικό δίκαιο που ισχύει σήμερα αναφορικά με το δικαίωμα αυτοάμυνας. Επίσης θα αναφερθούμε στο Εγχειρίδιο του Ταλίν. Πρόκειται για ένα σημαντικό εγχείρημα αποτελούμενο από 95 άρθρα, ωστόσο μη νομικά δεσμευτικά κείμενο ,το οποίο συντάχθηκε από μια Διεθνή Ομάδα Εμπειρογνωμόνων το 2013, η οποία μελέτησε την δυνατότητα αναλογικής εφαρμογής του δικαίου της χρήσης βίας και του ΔΑΔ στον Κυβερνοπόλεμο. Τέλος θα εξαχθούν ορισμένα συμπεράσματα που προκύπτουν από την μελέτη και ανάλυση του φαινομένου, ενώ θα προταθούν διάφορες λύσεις που μπρορούν να υιοθετηθούν σε εθνικό αλλά και διεθνές επίπεδο για την αποτελεσματικότερη πρόληψη και αντιμετώπιση της παγκόσμιας αυτής απειλής.

ΚΕΦΑΛΑΙΟ Α΄ Κυβερνοπόλεμος, μια ειδικότερη μορφή του Πληροφοριακού Πολέμου

1.1 Η έννοια του του Κυβερνοπολέμου και οι στόχοι του

Ο Κυβερνοπόλεμος αποτελεί τμήμα του Πληροφοριακού Πολέμου και για αυτό κρίνεται σκόπιμο πριν προχωρήσουμε στην εννοιολογική ανάλυση του πρώτου, να περιγράψουμε πρώτα με συντομία τον σύνθετο όρο του Πληροφοριακού Πολέμου. Η έννοια αυτή αναπτύχθηκε για πρώτη φορά μετά το τέλος του Περσικού Πολέμου (Φεβρουάριος 1991), με την υιοθέτηση μιας νέας στρατηγικής αντίληψης, η οποία διαφοροποείται από τις αυτές του παρελθόντος εξαιτίας της ιδιαιτερότητας της. Πιο συγκεκριμένα, πλέον για την θετική έκβαση των επιθέσεων και συγκρούσεων πρωταρχικό και θεμελιώδη ρόλο αποτελεί ο αποτελεσματικός έλεγχος και η ορθή διαχείριση κάθε κρίσιμης πληροφορίας [3] και όχι άλλοι παράγοντες που λάμβάνονταν υπόψη σε έναν συμβατικό πόλεμο μεταξύ των κρατών. Η στρατηγική που υιοθετείται από τις εκάστοτε δυνάμεις

[3] Λιαρόπουλος Ανδ. : Η Γεωγραφία και η Πληροφόρηση ως διαστάσεις της παγκόσμιας ασφάλειας. Ο Κυβερνοχώρος ως το νέο γεωπολιτικό παράδειγμα στην εποχή της πληροφόρησης., 7Ο Πανελλήνιο Γεωγραφικό Συνέδριο 14-17 Οκτωβρίου 2004, συνεδρία με θέμα : Ανθρωπογεωγραφία και Κοινωνία , http://www.srcosmos.gr/srcosmos/showpub.aspx?aa=6328, σελ 4-5 της Εισήγησης

που συμμετέχουν στον Πληροφοριακό Πόλεμο διαφέρει άρδην από τις ένοπλες συγκρούσεις που λάμβαναν χώρα αποκλειστικά στο έδαφος , στον εναέριο χώρο καθώς κ στα θαλάσσια ύδατα. Η στρατιωτική υπεροχή επιτυγχάνεται πλέον από την σωστή αξιοποίηση των δεδομένων και πληροφοριών που συλλέγονται ανεξάρτητα από την πολεμική ισχύ των αντίπαλων μερών.

Με τον όρο Κυβερνοπόλεμος νοείται κάθε ενέργεια και κάθε μη εξουσιοδοτημένη προσπάθεια πρόσβασης σε ένα σύστημα ελέγχου ή γενικότερα στα δίκτυα Η/Υ μιας χώρας ή ενός μη κρατικού δρώντα, με σκοπό να προκαλέσει βλάβη και ζημία σε αυτά. Επιδίωξη των ενεργειών αυτών είναι όχι μόνο η συλλογή των απαραίτητων πληροφοριών που είναι αποθηκευμένες σε δίκτυα σχετικά με μείζονα στρατιωτικά ζητήματα αλλά και η παραποίηση τους, με απώτερο σκοπό οι τελευταίες να εκτελούν κάποιες εργασίες ή λειτουργίες που δεν ήταν μέσα στους σκοπούς των σχεδιαστών τους ή δεν είναι αποδεκτές από αυτούς καθώς και στην λήψη λανθασμένων αποφάσεων από τα αρμόδια όργανα και φορείς. Ωστόσο δεν έχει δοθεί ένας επίσημος όρος για τον Κυβερνοπόλεμο στα πλαίσια του ΟΗΕ. Αρκετοί επίσης υποστηρίζουν, ότι ο όρος αυτός (κυβερνοπόλεμος) δεν ευσταθεί, προβάλλοντας ως επιχείρημα ότι η έννοια του πολέμου είναι άμεσα συνυφασμένη με την άσκηση βίας καθώς και την πρόκληση υλικών καταστροφών κάτι που δεν συμβαίνει με τις κυβερνοεπιθέσεις τουλάχιστον άμεσα[4] .

Οι βασικοί στόχοι του κυβερνοπολέμου εντοπίζονται σε δύο πεδία, το πρώτο είναι ο χώρος των Ενόπλων Δυνάμεων και το δεύτερο οι κρίσιμες υποδομές ενός κράτους ακόμη και αυτές που δεν αποτελούν κρατική ιδιοκτησία. Στην πρώτη περίπτωση επιδιώκεται η αποδυνάμωση των στρατιωτικών δυνάμεων και η διαταραχή του συστήματος διοίκησης και ελέγχου (C^2 systems) του αντιπάλου. Στην δεύτερη περίπτωση στόχος είναι οι κρίσιμες υποδομές (critical infrastructure) κάθε κράτους, οι οποίες εάν στοχοποιηθούν, εκτίθεται σε κίνδυνο

[4] Dun Cavelty, Myriam, " As likely as a visit from E.T", The European Magazine , http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear

η ασφάλεια του ιδίου του κράτους καθώς και η ικανότητα του να συμμετέχει σε οποιαδήποτε πολεμική σύγκρουση για μεγάλο χρονικό διάστημα.

Τα υπολογιστικά συστήματα που ελέγχουν τις υποδομές [5] «κοινής ωφελείας» αλλά και διάφορες βιομηχανικές διεργασίες ,όπως η παραγωγή και διανομή ηλεκτρικού ρεύματος, συλλογή και διανομή πόσιμου νερού, συλλογή των λυμάτων, αγωγοί πετρελαίου και φυσικού αερίου, ενσύρματα και ασύρματα δίκτυα επικοινωνιών, δορυφορικά συστήματα, έλεγχος εναέριας κυκλοφορίας, διαχείριση κυκλοφορίας οχημάτων, πυρηνικά εργοστάσια, τραπεζικά και χρηματιστηριακά δίκτυα, αναφέρονται διεθνώς ως SCADA (: Supervisory Control And Data Acquisition systems) [6]. Το ζήτημα όμως που ανακύπτει στο σημείο αυτό έγκειται στον προσδιορισμό των κρίσιμων υποδομών κάθε κράτους, εφόσον δεν υπάρχει κάποιος επίσημος ορισμός, ούτε κάποια αντικειμενικά κριτήρια κοινώς αποδεκτά. Η Γενική Συνέλευση του ΟΗΕ αναφέρει ότι κάθε κράτος θα πρέπει να προσδιορίσει το ίδιο τις κρίσιμες πληροφοριακές υποδομές του κάτι που έχουν ήδη πράξει αρκετά κράτη καθώς και η Ευρωπαική Ένωση[7]. Ο προσδιορισμός των κρίσιμων υποδομών των κρατών περιπλέκεται από το γεγονός ότι στις περισσότερες περιπτώσεις, η πλειοψηφία των κρισίμων υποδομών ανήκει στον ιδιωτικό τομέα. Αναμφισβήτητα όμως το ζήτημα των κρισίμων υποδομών συνδέεται με την έννοια της ‘εθνικής ασφάλειας’ ενός κράτους. Ένα παράδειγμα τέτοιας στοχοποίησης ήταν η άσκηση « Eligible Receiver », η οποία πραγματοποιήθηκε στις ΗΠΑ το καλοκαίρι (Ιούνιος) του 1997. Σύμφωνα με στοιχεία που ήλθαν στην δημοσιότητα συμμετείχαν μετά από τρίμηνη προετοιμασία , η Εθνική Υπηρεσία Ασφαλείας, η Κεντρική Υπηρεσία Πληροφοριών, η Υπηρεσία Αμυντικών

[5] Ο όρος υποδομή αναφέρεται σε θεμελιώσεις εγκαταστάσεις και συστήματα που διαθέτει ένα κράτος και περιλαμβάνει τόσο τις τεχνικές δομές όσο τις ποικίλες δημόσιες υπηρεσίες που βελτιώνουν τις συνθήκες διαβίωσης των πολιτών του. https://en.wikipedia.org/wiki/Infrastructure

[6] https://en.wikipedia.org/wiki/SCADA

[7] Στην Ε.Ε. έχει εκδοθεί η Οδηγία 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008 ‘’σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους’’ (Επίσημη Εφημερίδα της Ε.Ε., L 345/75, 23.12.2008). Με βάση την Οδηγία αυτή κάθε κράτος – μέλος πρέπει να ορίσει τις δικές του κρίσιμες υποδομές οι οποίες είναι συγχρόνως και ευρωπαϊκές υποδομές ζωτικής σημασίας (ΕΥΖΣ), ως ‘ΕΥΖΣ’ δε νοούνται ‘’οι υποδομές ζωτικής σημασίας που βρίσκονται εντός των κρατών μελών και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο σε δύο τουλάχιστον κράτη μέλη

Πληροφοριών, το Υπουργείο Εξωτερικών, το Υπουργείο Δικαιοσύνης και η εχθρική ομάδα Red Team[8]. Η τελευταία διείσδυσε στα συστήματα Ηλεκτρονικών Υπολογιστών του Αμερικανικού ΥΠΑΜ ενώ πραγματοποίησε και κυβερνοεπιθέσεις κατά του δικτύου παροχής ηλεκτρικής ενέργειας και των τηλεπικοινωνιών, γεγονός που αποτέλεσε τροχοπέδη στην διεξαγωγή στρατιωτικών επιχειρήσεων [9]. Η Κόκκινη Ομάδα (Red Team) αποτελούνταν από 35 hackers της National Security Agency (NSA) - Υπηρεσία Εθνικής Ασφάλειας[10], κατάφερε να διεισδύσει σε ηλεκτρονικούς υπολογιστές του κέντρου επιχειρήσεων της Διοίησης του Ειρηνικού (Pacific Command) , στο δίκτυο παροχής ηλεκτρικής ενέργειας όπως επίσης και σε δίκτυα υπηρεσιών ανταπόκρισης σε έκτακτες ανάγκες σε 9 μεγάλες αμερικανικές πόλεις [11].

1.2 Τα ιδιαίτερα χαρακτηριστικά του γνωρίσματα και οι διάφορες μορφές εκδήλωσης του

Από την φύση του ο Κυβερνοπόλεμος διαφοροποιείται αρκετά από τον παραδοσιακό πόλεμο λόγω των ιδιαίτερων χαρακτηριστικών του, που θα αναλύσουμε στην συνέχεια. Καταρχήν το είδος αυτό του πολέμου δεν υπάγεται σε χρονοχωρικούς περιορισμούς εφόσον δεν πραγματοποιείται σε συγκεκριμένη εδαφική έκταση. Κατά συνέπεια είναι δύσκολο να προσδιοριστεί γεωγραφικά. Χαρακτηρίζεται επίσης ως ακήρυχτος πόλεμος, διότι ποτέ κανένα κράτος δεν έχει αναλάβει επίσημα την ευθύνη κάποιας κυβερνοεπίθεσης. Επίσης, για την διεξαγωγή του απαιτείται ελάχιστο κόστος, ενώ η ταχύτητα με την οποία πραγματοποιούνται οι κυβερνοεπιθέσεις μέσα στον κυβερνοχώρο είναι ένα ακόμη χαρακτηριστικό του γνώρισμα. Επιπλέον ανήκει στις μορφές του ασύμμετρου πολέμου, διότι χαρακτηρίζεται από αόρατα χτυπήματα, είναι μη προβλέψιμος με αποτέλεσμα να καθίσταται ιδιαίτερα δυσχερής η ταυτοποίηση της πηγής προέλευσης των κυβερνοεπιθέσεων. Ακόμη και εάν τελικά επιτευχθεί η ταυτοποίηση, αυτή θα είναι αρκετά χρονοβόρα. Χαρακτηριστικό παράδειγμα στις επιθέσεις του 2007 στην Εσθονία όπου χρησιμοποιήθηκαν εκατοντάδες

[8] https://en.wikipedia.org/wiki/Eligible_Receiver_97
[9] Rattray, Gregory J.., “Strategic Warfare in Cyberspace, Mit Press Cambridge" ,2001, p.385
[10] https://en.wikipedia.org/wiki/National_Security_Agency
[11] http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

χιλιάδες υπολογιστές που βρίσκονταν στις Η.Π.Α., την Αίγυπτο, το Περού, τη Ρωσική Ομοσπονδία και την ίδια την Εσθονία (χωρίς οι κάτοχοι των ηλεκτρονικών υπολογιστών να γνωρίζουν τίποτε στη συντριπτική πλειοψηφία των περιπτώσεων.Έτσι βέβαια εξασφαλίζεται και η ανωνυμία των επιτιθέμενων. Εξαιτίας των ιδιαίτερων γνωρισμάτων που προαναφέραμε, ο κυβερνοπόλεμος συνιστά μια παγκόσμια ασύμμετρη απειλή και καθίσταται επιτακτική ανάγκη η υιοθέτηση μιας στρατηγικής όπου θα εξασφαλίζει την μέγιστη δυνατή ασφάλεια στην μετάδοση και ανταλλαγή των πληροφοριών ιδίως σε ζητήματα που αφορούν την εθνική ασφάλεια ενός κράτους.

Οι βασικές μορφές του Κυβερνοπολέμου είναι δύο : α) Ο Στρατηγικός Κυβερνοπόλεμος (Strategic Cyber war), ο οποίος περιλαμβάνει τις κυβερνοεπιθέσεις που αποσκοπούν στο να επηρεάσουν την κυβερνητική πολιτική του αντιπάλου και β) ο Επιχειρησιακός (Operational Cyber war) δηλαδή όλες εκείνες οι κυβερνοεπιθέσεις που αποβλέπουν στην διεξαγωγή και υποστήριξη ενός συμβατικού πολέμου.

1.2.1 Στρατηγικός Κυβερνοπόλεμος

Για να ενταχθεί μια κυβερνοεπίθεση στην έννοια του στρατηγικού Κυβερνοπολέμου θα πρέπει να συντρέχουν σωρευτικά τρείς προυποθέσεις. Πρώτον δεν θα πρέπει παράλληλα να διεξάγονται άλλες εχθροπραξίες μεταξύ των δύο αντίπαλων πλευρών ή εάν συμβαίνουν να θεωρούνται δευτερεύουσες σε σχέση με τον Κυβερνοπόλεμο. Δεύτερη προϋπόθεση είναι να συμμετέχουν στις κυβερνοεπιθέσεις και οι δύο πλευρές ενώ τρίτον θα πρέπει να έχει προηγουμένως καταβληθεί κάθε δυνατή οικονομική και διπλωματική προσπάθεια. Να επισημάνουμε ότι ως φορέας των επιθέσεων μπορεί να είναι και μη κρατικός δρώντας , γεγονός που εγείρει ποικίλα ζητήματα. Να επισημάνουμε ότι η μορφή αυτή του πολέμου δεν πρέπει να αποτελεί πανάκεια σχετικά με όλους τους επιδωκόμενους στόχους των αντίπαλων πλευρών. Η χρήση του πρέπει να αποβλέπει στην επίτευξη συγκεκριμένων στόχων (limited

aims)[12]. Σε καμία περίπτωση πάντως δεν μπορεί να γίνει κατάληψη εδάφους. Ένα άλλο ζήτημα του στρατηγικού κυβερνοπολέμου είναι τα αποτελέσματα που επιφέρει συγκριτικά με αυτά που δημιουργεί ο συμβατικός πόλεμος. Αναμφισβήτητα το στοιχείο του εξαναγκασμού του αντίπαλου δεν είναι δεδομένο στον Στρατηγικό Κυβερνοπόλεμο. Αυτό οφείλεται στο γεγονός ότι ο εξαναγκασμός ενός κράτους είναι άρρηκτα συνδεδεμένος με το σύνολο των ανθρώπινων απωλειών, κάτι που ο Στρατηγικός Κυβερνοπόλεμος δεν μπορεί να προκαλέσει[13]. Ωστόσο υπάρχει και η αντίθετη άποψη, ότι ο εξαναγκασμός ενός κράτους μπορεί να επιτευχθεί αν πληρούνται ορισμένες προϋποθέσεις , η οποία στηρίζεται κυρίως στην γνωστή και εκλαϊκευμένη « Τριάδα του Κλαούζεβιτς» (Λαός- Ένοπλες Δυνάμεις- Κυβέρνηση)[14] αλλά και στην αλληλεξάρτηση των τριών αυτών στοιχείων μεταξύ τους αλλλά και με το Διαδίκτυο [15] . Μέχρι σήμερα δεν έχει διαπιστωθεί περίπτωση στρατηγικού Κυβερνοπολέμου. Θα μπορούσε να αποτελέσει εξαίρεση η περίπτωση της Εσθονίας το 2007 εάν οι Εσθονοί είχαν ανταποδώσει τις κυβερνοεπιθέσεις των Ρώσων.

1.2.2 Επιχειρησιακός Κυβερνοπόλεμος

Η μορφή αυτή πολέμου περιλαμβάνει τις κυβερνοεπιθέσεις που λαμβάνουν χώρα κατά την διάρκεια ενός πολέμου ή μιας ένοπλης σύρραξης κατά στρατιωτικών αλλά και μη στρατιωτικών στόχων. Πολλές φορές μάλιστα η προσβολή των τελευταιών όπως για παράδειγμα ένα δίκτυο τηλεπικοινωνιών μπορεί να προκαλέσει ανεπανόρθωτη ζημιά στις επιχειρήσεις του αντιπάλου. Και στην περίπτωση αυτού του πολέμου δεν μπορεί κανείς να κατακτήσει

---

[12] Mahnken, Thomas G. , " Cyber War and Cyber Warfare" , στο έργο Lord, Kristin M. and Sharp , Travis, " America' s Cyber Future : Security and Prosperity in the Information Age", 2011

[13] Libicki M. C.. "Cyberdeterrence and cyberwar", RAND Corporation, 2009, σελ. 122

[14] Κολιόπουλος Κ., Η Στρατηγική Σκέψη από την αρχαιότητα μέχρι σήμερα , Εκδ. Ποιότητα, Αθήνα , 2008, σελ.154

[15] https://www.scribd.com/doc/212579520/200804-%CE%97-%CE%A0%CE%91%CE%A1%CE%91%CE%94%CE%9F%CE%9E%CE%97-%CE%A4%CE%A1%CE%99%CE%91%CE%94%CE%91-%CE%A4%CE%9F%CE%A5-%CE%9A%CE%9B%CE%91%CE%9F%CE%A5%CE%96%CE%95%CE%92%CE%99%CE%A4%CE%A3

έδαφος και οι στόχοι που επιδιώκονται είναι περιορισμένοι (limited aims)[16] . Να επισημάνουμε ακόμη ότι ούτε και σε αυτή την μορφή πολέμου δεν είναι εφικτή η υπεροχή στον Κυβερνοχώρο (Cyber Sypremacy) όπως συμβαίνει στον Συμβατικό Πόλεμο με την κατάληψη για παράδειγμα χερσαίων εκτάσεων ή αντίστοιχα στον εναέριο χώρο ή στα θαλάσσια ύδατα.

Ένα μεγάλο πλεονέκτημα του πολέμου αυτού είναι το αίσθημα αιφνιδιασμού που προκαλεί στον αντίπαλο καθώς επίσης και η παραπλάνηση. Βασικός άλλωστε στόχος μιας κυβερνοεπίθεσης είναι να διαφοροποιήσει την λειτουργία ενός Ηλεκτρονικού Υπολογιστή από αυτή που είχε αρχικά κατασκευαστεί και ανέμενε να δει ο χρήστης του . Απόροια αυτής της ποιοτικής διαφοροποίησης είναι ο αιφνιαδιασμός του αντιπάλου και η παραπλάνηση αυτού, κάτι βέβαια που για να επιτευχθεί καλύτερα θα πρέπει να έχει προηγηθεί μια κυβερνοκατασκοπεία δηλαδή η ανακάλυψη των αδύναμων σημείων της αντίπαλης παράταξης μέσα στον κυβερνοχώρο. Μια από τις δυνατότητες του πολέμου αυτού είναι να θέσει τον αντίπαλο εκτός δικτύου για ορισμένο χρονικό διάστημα. Όπως άλλωστε υποστηρίζει και ο Thomas Mahnken το βασικό προτέρημα της μορφής αυτής του πολέμου είναι η άρνηση απέναντι στον αντίπαλο της χρήσης των δικτύων[17].

2. <u>Οι μη κρατικοί δρώντες και τα Κράτη στον Κυβερνοπόλεμο</u>

Όπως έχουμε ήδη αναφέρει σε προηγούμενη ενότητα, ένα από τα βασικά χαρακτηριστικά του κυβερνοπολέμου είναι η δυσκολία ταυτοποίησης της ταυτότητας της πηγής προέλευσης των κυβερνοεπιθέσεων. Αυτό επιτυγχάνεται κυρίως με ένα πλήθος μεθόδων όπως είναι η χρήση των παραπληνητικών διευθύνσεων internet (IP spoofing). Σε αντίθεση με ότι συμβαίνει στον συμβατικό πόλεμο, ο Κυβερνοπόλεμος μπορεί να διεξαχθεί όχι μόνο από κρατικούς φορείς αλλά και από μη κρατικούς δρώντες και μεμονωμένα άτομα. Υπάρχουν δύο κατηγορίες μη κρατικών δρώντων. Η πρώτη που είναι και η

[16] Mahnken, Thomas G. , " Cyber War and Cyber Warfare, , στο έργο Lord, Kristin M. and Sharp , Travis, " America' s Cyber Future : Security and Prosperity in the Information Age", 2011, σελ.58

[17] Mahnken, Thomas G. , " Cyber War and Cyber Warfare", στο έργο Lord, Kristin M. and Sharp , Travis, " America' s Cyber Future : Security and Prosperity in the Information Age", 2011, σελ. 60

συνηθέστερη, αφορά μεμονωμένους ιδιώτες οι οποίοι είναι γνωστοί διεθνώς ως hackers και δρουν ανεξάρτητοι μεν, συνεργαζόμενοι όμως με το κράτος το οποίο τους προσφέρει αντίστοιχα κάποια χρηματική αμοιβή[18] Η δεύτερη περίπτωση αφορά τους hackers, οι οποίοι δρούν εντελώς αυτόνομα. Τα κίνητρα και των δύο κατηγοριών είναι ως επί το πλείστον οικονομικά αλλά κάποιες φορές και πολιτικά.ή προσωπικά.

Ο επιτιθέμενος μπορεί να είναι και ένα de facto όργανο κάποιου κράτους, το οποίο δρα υπό ορισμένες προϋποθέσεις. Στην υπόθεση Νικαράγουα κατά των ΗΠΑ, το Διεθνές Δικαστήριο της Χάγης αποφάνθηκε ότι για να καταλογιστούν οι πράξεις των contras στο κράτος των ΗΠΑ είναι απαραίτητη η ύπαρξη πραγματικού - αποτελεσματικού ελέγχου (effective control) μεταξύ των πράξεων της συγκεκριμένης ομάδας και του ανωτέρω κράτους [19] . Επίσης το Εφετειακό Τμήμα του ICTY στην υπόθεση Tadic για να αναγνωρίσει και να αποδώσει την ευθύνη των πράξεων των στρατιωτικά οργανωμένων ενόπλων δυνάμεων έθεσε ως κριτήριο την ύπαρξη ενός ολοκληρωτικού ελέγχου (overall control). Πιο συγκεκριμένα για να αποδοθεί η ευθύνη τέτοια πράξεων στο κράτος όπως αναφέρει και το Δικαστήριο "… has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group … regardless of any specific instructions by the controlling State concerning the commission of each of those acts" [20]. Το κριτήριο του αποτελεσματικού ελέγχουθα πρέπει να υπάρχει και στις κυβερνοεπιθέσεις που πραγματοποιούνται από μεμονωμένα άτομα. Εξαιτίας της μεγάλης δυσκολίας απόδειξης τόσο του τόπου όσο και των προσώπων που εκτελούν τις κυβερνοεπιθέσεις επιβάλλεται να υιοθετηθούν νέα και πιο αποτελεσματικά επίπεδα ελέγχου για λόγους αποδεικτικής βεβαιότητας. Αναλυτικά για τον καταλογισμό ευθύνης στα κράτη για πράξεις που τελούνται στον Κυβερνοχώρο από μη κρατικούς δρώντες και τις προϋποθέσεις, ώστε να αποδοθεί ευθύνη σε αυτά, θα εξεταστούν στο τρίτο κεφάλαιο της εργασίας.

[18] https://en.wikipedia.org/wiki/Freelancer
[19] http://www.icj-cij.org/docket/index.php?p1=3&p2=3&code=sh&case=75&k=0e&p3=0 (ICJ Reports , 1986)
[20] http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

Μια άλλη διθνώς αναγνωρισμένη ονομασία των μη κρατικών δρώντων που συνεργάζονται με τα κράτη για να εκτελούν κυβερνοεπιθέσεις είναι η Cyber Militias [21]. Οι ομάδες αυτές αποτελούνται από μέλη των οποίων οι γνώσεις στην χρήση των ηλεκτρονικών υπολογιστών και γενικότερα της Πληροφορικής ποικίλουν. Τα μέλη των ομάδων αυτών διεξάγουν κυβερνοεπιθέσεις για την επίτευξη αποκλειστικά πολιτικών στόχων. Και σε αυτή την περίπτωση δεν χρείαζεται μεν να υπάρχει πλήρης έλεγχος αλλά οπωσδήποτε αποτελεσματικός, μεταξύ των πράξεων τους και του κράτους που τους προσλαμβάνει για να φέρουν εις πέρας μια αποστολή.

Οι Cyber Militias διακρίνονται από τρία βασικά μοντέλα οργάνωσης τα οποία είναι τα εξής [22] :

I) Το Forum αποτελεί μια ήπια σχετικά μορφή hackers όπου τα μέλη μεταξύ τους είναι πιθανό και να μην γνωρίζονται. Τις περισσότερες φορές συστήνονται για την διεξαγωγή κυβερνοεπιθέσεων ορμώμενοι από πολιτικά κίνητρα. Μόλις επιτύχουν τον στόχο τους συνήθως διαλύονται. Δεν υπάρχει κάποιο αυστηρό σύστημα διοίκησης με αποτέλεσμα το κάθε μέλος να μπορεί να δρα σχετικά ανεξάρτητα. Το βασικότερο πλεονέκτημα του ανωτέρω μοντέλου είναι η ταχύτητα με την οποία συστήνεται καθώς και η ποικιλομορφία μεταξύ των μελών του η οποία καθιστά αρκετά δυσχερέστερο τον εντοπισμό τους. Το μειονέκτημα είναι το γεγονός που ήδη αναφέραμε ότι δηλαδή δεν υπάρχει συμπαγής διοίκηση με αποτέλεσμα το κάθε μέλος να λειτουργεί αυτόνομα χωρίς να υπάρχει μια κοινή γραμμή πλεύσης με αποτέλεσμα να ελαττώνεται η αποδοτικότητα της ομάδας. Χαρακτηριστικό παράδειγμα ενός τέτοιου μοντέλου αποτέλεσε το stopgeorgia.ru [23] το οποίο εμφανίσθηκε και έδρασε το 2008 κατά την διάρκεια του πολέμου μεταξύ Γεωργίας και Ρωσίας. Για την ακρίβεια συστάθηκε στις 9 Αυγούστου του 2008 αρχικά με 30 μέλη τα οποία όμως συνεχώς αυξάνονταν. Έχοντας εθνικιστικά κίνητρα το stopgeorgia.ru προέβη σε

[21] https://books.google.gr/books?id=vub26dKsmpIC&pg=PA110&lpg=PA110&dq=cyber+militias+and+political+hackers&source=bl&ots=BVdJducePW&sig=9if5eN4D-XezyS07p0UWYUzCgno&hl=el&sa=X&ved=0CJcBEOgBMA9qFQoTCKit4vLDt8gCFclXFAodcasH7g#v=onepage&q=cyber%20militias%20and%20political%20hackers&f=false

[22] http://uscyberlabs.com/blog/2012/02/15/cyber-militia-models-offensive/

[23] https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War

κυβερνοεπιθέσεις κατά γεωργιανών σελίδων με σκοπό να αναστείλουν την λειτουργία τους.

II) Το Κελί (Cell) αποτελείται από hackers με μεγάλη εξειδίκευση οι οποίοι προβαίνουν σε κυβερνοεπιθέσεις για μεγάλο χρονικό διάστημα και των οποίων η δράση δεν είναι τόσο σύντομη όσο του forum. Τα μέλη αριθμητικά δεν είναι πολλά αλλά γνωρίζονται μεταξύ τους. Οι λόγοι που δρουν τα μέλη του Cell είναι κυρίως προσωπικοί για την απόκτηση για παράδειγμα εμπειριών. Βασικό πλεονέκτημα του Cell είναι η άμεση κινητοποίηση τους δεδομένου ότι τα μέλη γνωρίζονται μεταξύ τους. Βασικό μειονέκτημα αποτελεί η ύπαρξη της προηγούμενης εμπειρίας των μελών του Cell η οποία καθιστά πιο εύκολο τον εντοπισμό τους. Χαρακτηριστικό παράδειγμα τέτοιου μοντέλου αποτελεί το Team Evil το οποίο συστήθηκε το 2006 ως αντίδραση στις ισραηλινές επιχειρήσεις στις Λωρίδες της Γάζας και στο Λίβανο. Για την ακρίβεια το Team Evil μέσα σε ένα εξάμηνο πραγματοποίησε web defacement[24] σε πάνω από 8000 ιστοσελίδες σε Ισραήλ, Σ. Αραβία, Ινδονησία, Κίνα αφήνοντας συνήθως αντι-ισραηλινά συνθήματα στις ιστοσελίδες.

III) Ιεραρχία (Hierarchy) [25], σε αυτό το μοντέλο οργάνωσης υπάρχει ένα αυστηρό σύστημα διοίκησης και ελέγχου και κάθε υποσύνολο του μοντέλου αυτού έχει το δικό του διακριτό ρόλο. Η ύπαρξη ιεραρχικής οργάνωσης έχει διττό χαρακτήρα. Από την μια η ύπαρξη της συνεπάγεται την καλύτερη διοίκηση και κατά συνέπεια μεγαλύτερη διάρκεια επιχειρησιακής ζωής. Από την άλλη η αυστηρή ιεραρχική οργάνωση μπορεί να οδηγήσει σε μικρότερη ευελιξία. Χαρακτηριστικό παράδειγμα τέτοιου μοντέλου συνιστούν οι ομάδες που έχει δημιουργήσει η Κίνα στα τάγματα Πληροφοριακού Πολέμου που διαθέτει.

[24] https://en.wikipedia.org/wiki/Website_defacement

[25] Rain , Otiits, , " Theoretical Offensive Cyber Militia Models". Proceedings of the 6th International Conference on Information Warfare and Security , Washington DC, Academic Pyblishing Limited, p. 307-313

Τα Κράτη και ο Κυβερνοπόλεμος

Σύμφωνα με έρευνα που πραγματοποιήθηκε από το Κέντρο Στρατηγικών και Διεθνών Σπουδών (Centre for Strategic and International Studies) κατόπιν ελέγχου που διενεργήθη σε 133 χώρες , διαπιστώθηκε ότι 33 χώρες έχουν στην στρατιωτική τους οργάνωση τον όρο του Κυβερνοπολέμου (π.χ Ρωσία, ΗΠΑ, Κίνα, Ισραήλ) ενώ πάνω από 100 χώρες διαθέτουν εξειδικευμένες μονάδες που ασχολούνται αποκλειστικά με την διεξαγωγή κυβερνοεπιθέσεων [26] .Στη συνέχεια της εργασίας θα γίνει αναφορά σε ορισμένες χώρες όπως η Ρωσία, οι ΗΠΑ, η Κίνα, το Ιράν και το Ισραήλ δεδομένου ότι είναι οι χώρες με την πιο έντονη συμμετοχή σε περιπτώσεις κυβερνοεπιθέσεων που έχουν καταχωρηθεί σε διεθνές επίπεδο και απασχόλησαν την διεθνή κοινότητα.

2.1 Κίνα

Σύμφωνα με τον Richard Clarke ενεργοποιήθηκε έντονα κατά την διάρκεια του Περσικού Πολέμου (1990-91) όταν είδε το Ιράκ να ηττάται από τους συμμάχους. Η χρήση αεροπορικού όπλου αλλά και των έξυπνων βομβών κατά την διάρκεια των επιχειρήσεων της Desert Storm ανησύχησε και προβλημάτισε εντόνως την Κίνα η οποία αναζήτησε νέα στρατηγική και μεθόδους με σκοπό να αντιμετωπίσει τις ΗΠΑ και τους συμμάχους της. Η Κινέζικη ηγεσία συνειδητοποίησε ότι η υπεροχή έναντι των αντιπάλων της δεν θα επέλθει με την αύξηση των στρατιωτικών της δυνάμεων όπως συνηθίζεται σε έναν συμβατικό πόλεμο αλλά με το να επενδύσει σε νέες τεχνολογίες ρίχνοντας το βάρος στις έννοιες του Κυβερνοπολέμου και των κυβερνοεπιθέσεων. Χαρακτηριστικό παρ'αδειγμα από το οποίο διαφαίνεται η υιοθέτηση αυτής της νοοτροπίας είναι το βιβλίο του «Unrestricted Warfare» [27] το οποίο εκδόηκε το 1999 από δύο

[26] Masters, Jonathan, "Confronting the Cyber Threat, CFR,2011, (http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577)

[27] http://www.globalsecurity.org/military/library/report/1999/WEBRES4.htm

Κινέζους Συνταγματάρχες και σύμφωνα με το οποίο μια αδύναμη σχετικά χώρα δύναται να αντιμετωπίσει ισχυρότερους αντιπάλους της εάν χρησιμοποιήσει μη συμβατικές μεθόδους. Σταδιακά και ήδη από τις αρχές του 21ου αιώνα δημιουργήθηκε το κινέζικο στρατιωτικό δόγμα το οποίο έδινε μεγάλη βαρύτητα στον Κυβερνοπόλεμο , στην ανάπτυξη νέων πληροφοριακών τεχνολογιών και στις επιχειρήσεις στον Κυβερνοχώρο. Απόροια αυτού του δόγματος είναι η στενή συνεργασία πολλές φορές του κινεζικού κράτους με ποικίλες ομάδες Cyber Militias οι οποίες δραστηριοποιούνται στο εσωτερικό του κράτους και βρίσκονται υπό τον αποτελεσματικό αλλά όχι πλήρη έλεγχο του ανωτέρω.[28] Για την υλοποίηση των ανωτέρω στόχων το κινέζικο κράτος έχει φροντίσει να εκπαιδεύσει τον στρατό του με την σύσταση διαφόρων εκπαιδευτικών χώρων σε θέματα Κυβερνοπολέμου το πιο γνωστό από τα οποία αποτλεί η Ακαδημία της Διοίκησης Επικοινωνιών στο Wuhan , στα οποία διδάσκονται οι βασικοί κανόνες και η στρατηγική του Κυβερνοπολέμου καθώς και τρόποι αντιμετώπισης των κυβερνοεπιθέσεων.[29] Εκτός από την εκπαίδευση την θεωρητική του κινεζικού στρατού, πραγματοποιούνται ετησίως και ασκήσεις κυβερνοπολέμου με βασικά αντικείμενα την εμφύτευση « logic bombs» σε ηλεκτρονικά δίκτυα των αντιπάλων, την πληροφοριακή αναγνώριση, την κυβερνοκατασκοπεία με απώτερω σκοπό την παραπλάνηση του εχθρού[30]. Η Κίνα τις τελευταίες δεκαετίες καταβάλλει μια συνεχή προσπάθεια για την ανάπτυξη της τεχνολογίας στο τομέα της Πληροφορικής και την αύξηση της τεχνογνωσίας επενδύοντας σημαντικά ποσά από τον εγχώριο προυπολογισμό της είτε μέσω ξένων επενδύσεων. Εν κατακλείδι η Κίνα κατέχει την πρώτη θέση σε ζητήματα κυβερνοεπιθέσεων και κυβερνοκατασκοπείας , ενδεικτικά θα γίνει μνεία σε ορισμένα περιστατικά όπου είχε πρωταγωνιστικό ρόλο το Κινέζικο κράτος. Ύστερα από τον βομβαρδισμό τη νύχτα της 7ης Μαΐου 1999 της Κινέζικης Πρεσβείας στο Βελιγράδι από αεροσκάφη του ΝΑΤΟ[31] , η Κίνα απέρριψε κατηγορηματικά τους ισχυρισμούς των ΗΠΑ ότι ο βομβαρδισμός

[28] https://www.stratfor.com/
[29] Billo C. and Chang W. “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations States”, Institute for security technology studies at Darmouth College, Hannover ,2004, p.32
[30] Billo C. and Chang W. “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations States”, Institute for security technology studies at Darmouth College, Hannover, p. 33
[31] http://news.in.gr/world/article/?aid=299202

οφειλόταν στην επιλογή λανθασμένου στόχου από αξιωματούχους της αμερικανικής Κεντρικής Υπηρεσίας Πληροφοριών (CIA) [32], με αποτέλεσμα να προβεί ως αντίποινα. Πιο συγκεκριμένα όμαδες hackers προέβησαν σε κυβερνοεπιθέσεις κατά αμερικανικών ιστοσελίδων ενώ σημειώθηκαν ριζικές αλλαγές στο περιεχόμενο πολλών νατοϊκών ιστοσελίδων χωρίς προηγούμενη άδεια . Επίσης το 2014 ασκήθηκε για πρώτη φορά δίωξη σε βάρος πέντε Κινέζων αξιωματικών του στρατού για κυβερνοκατασκοπεία από τις ΗΠΑ, κατηγορώντας τους για κυβερνοεπίθεση σε αμερικανικές εταιρείες και υποκλοπή εμπορικών μυστικών. Με την απόφαση αυτή οι αρχές κατηγορούν για πρώτη φορά δημοσίως την Κίνα για κυβερνοκατασκοπεία. Σύμφωνα με τις ΗΠΑ στόχος των κινέζων χάκερ ήταν αμερικανικές εταιρείες στο χώρο της πυρηνικής ενέργειας και μετάλλων καθώς και η υποκλοπή πληροφοριών που θα έβλαπταν κυριώς οικονομικά τις ΗΠΑ. Από την πλευρά της η Κίνα απέρριψε όλες τις κατηγορίες των Αμερικανών. [33]

.2.2 Ρωσία

Όπως και η Κίνα έτσι και η Ρωσία γνωρίζοντας αρκετά καλά ότι θα υστερούσε έναντι των ΗΠΑ σε θέματα ηλεκτρονικής διακυβέρνησης και μη θέλοντας να οδηγηθεί σε κατάρρευση συμβάλλοντας και η ίδια στην υπεροχή των ΗΠΑ στον Κυβερνοχώρο, ανέπτυξε από την δεκαετία του 1990 ένα δόγμα σχετικά με τις επιχειρήσεις της στον Κυβερνοχώρο και την ανάπτυξη κυρίως κυβερνοόπλων , τα οποία θα χρησιμοποιούνταν από τον Ρωσικό Στρατό και τις μυστικές υπηρεσίες. Στόχος της Ρωσίας ήταν η ανάπτυξη των επιθετικών και αμυντικών της ικανοτήτων στον Κυβερνοχώρο[34]. Η πιο γνωστή κρατική υπηρεσία που συνέβαλε στην εφαρμογή του ρωσικού δόγματος ήταν η FAPSI ή Ομοσπονδιακό Γραφείο Κρατικών Επικοινωνιών και Πληροφοριών, αρμόδια για την ασφάλεια των κυβερνητικών ανακοινώσεων. Ο ρόλος της είναι παρόμοιος με την Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ (NSA). Τον

[32] http://news.in.gr/world/article/?aid=300629
[33] http://tvxs.gr/news/ellada/psyxros-kybernopolemos-metaksy-ipa-kai-kinas
[34] Lewis, James Timlin , Katrina, " Cybersecurity and Cyberwarfare 2011 :Preliminary Assessment of National Doctrine and Organization",CSIS, p.19

Σεπτέμβριο του 1991 η FAPSI διαλύθηκε σε διάφορα ανεξάρτητα τμήματα όπως η FSB (Ομοσπονδιακή Υπηρεσία Ασφάλειας) και η SVR (Εξωτερική Υπηρεσία Πληροφοριών)[35].

Στη συνέχεια θα αναφέρουμε ορισμένες από τις περιπτώσεις κυβερνοεπιθέσεων στις οποίες ενεπλάκη η Ρωσία. Τον Οκτώβριο του 2002 η FSB πραγματοποίησε κυβερνοεπιθέσεις σε ιστοσελίδες Τσετσένων Αυτονομιστών λίγο πριν την εισβολή των δυνάμεων της FSB στο θέατρο της Μόσχας, όπου οι Τσετσένοι Αυτονομιστές κρατούσαν υπό ομηρία Ρώσους πολίτες[36] . Μια άλλη γνωστή περίπτωση είναι η υπόθεση Moonlight Moze κατά την οποία Αμερικάνοι αξιωματούχοι ανακάλυψαν ότι hackers είχαν εισβάλλει σε συστήματα πληροφορικής της NASA, του Πενταγώνου, του Υπουργείου Ενέργειας καθώς και σε ιδιωτικά πανεπιστήμια και σε ερευνητικά εργαστήρια με σκοπό να υποκλέψουν αρχεία καθώς και χάρτες των στρατιωτικών εγκαταστάσεων όπως επίσης και διάφορα σχέδια στρατιωτικού υλικού.Η όλη επιχείρηση ξεκίνησε τον Μάρτιο του 1998 και συνεχίστηκε για δύο χρόνια. Το Υπουργείο Άμυνας ύστερα από έρευνες που διεξήγαγε κατέληξε στην Ρωσία η οποία όμως ποτέ δεν παραδέχθηκε οποιαδήποτε ανάμειξη στην υπόθεση[37]. Τέλος να αναφέρουμε ότι η Βρεττανική GYARDIAN έγραψε πως η FSB έχει ξεκινήσει ένα εγχείρημα για την δημιουργία ενός τύπου διαδικτύου με βασική γλώσσα την κυριλλική, το οποίο θα είναι ανεξάρτητο από τον παγκόσμιο ιστό (www). Το κρίσιμο βέβαια ερώτημα είναι κατά πόσο οι ρωσικές Αρχές θα αποφασίσουν να αποχωρήσουν από την «Διαδικτυακή Εταιρεία Ονοματοδοσίας και Αριθμοδότησης» (ICANN), δημιουργώντας μια αντίστοιχη ρωσόφωνη για τον έλεγχο της διακίνησης των πληροφοριών στον κυβερνοχώρο.

2.3 ΗΠΑ

Αναμφισβήτητα η Αμερική κατέχει εδώ και αρκετές δεκαετίες τα ηνία σε θέματα κυβερνοεπιθέσεων, εφόσον ήταν από τα πρώτα κράτη που έκανε χρήση των

[35] https://en.wikipedia.org/wiki/FAPSI
[36] Billo C. and Chang W. “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations States”, Institute for security technology studies at Darmouth College, Hannover, p. 113-114
[37] http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

Ηλεκτρονικών Υπολογιστών και γενικότερα των τεχνολογικών επιτευγμάτων ακόμη και στο χώρο των Ενόπλων Δυνάμεων. Η ασφάλεια στον κυβερνοχώρο επιτυγχάνεται μέσα από την συνεργασία των αμερικανικών Ενόπλων Δυνάμεων αλλά και την ύπαρξη διαφόρων υπηρεσιών πληροφοριών όπως η NSA, η CIA και το FBI [38]. Το 2004 ο Αρχηγός των Ενόπλων Δυνάμεων της Αμερικής εξομοίωσε τον κυβερνοχώρο με τα άλλα πεδία διεξαγωγής των συγκρούσεων (ξηρά, αέρας , θάλασσα) . Δύο χρόνια αργότερα το 2006 εκδόθηκε και η Εθνική Στρατιωτική Στρατηγική για τις επιχειρήσεις στον κυβερνοχώρο (National Military Strategy for Cyberspace Operations) . Στόχος της είναι να περιγράψει τον κυβερνοχώρο ως ένα πεδίο στο οποίο διεξάγονται στρατιωτικές επιχειρήσεις, ανταλλάσσονται και αποθηκεύονται δεδομένα μέσω δικτυακών συστημάτων. Γίνεται επίσης μνεία στις απειλές και τους κινδύνους που ελλοχεύουν μέσά σε αυτόν καθώς και στα τρωτά του σημεία. Αναφέρει ως στόχο των ΗΠΑ την στρατηγική υπεροχή στον κυβερνοχώρο. Για την ενσωμάτωση των λειτουργιών του ανωτέρω στην εθνική άμυνα απαιτείται σύμφωνα με την Εθνική Στρατηγική η ανεύρεση ενός στρατηγικού πλαισίου στο οποίο θα έχουν ληφθεί υπόψη όλα τα τρωτά σημεία του Κυβερνοχώρου αλλά και οι αλλαγές που πρέπει να γίνουν, όπου κριθεί σκόπιμο, για την επίτευξη της στρατηγικής υπεροχής των ΗΠΑ[39]. Τον Μαϊο του 2011 κυκλοφόρησε και η Διεθνής Στρατηγική για τον Κυβερνοχώρο (International Strategy for Cyberspace), σύμφωνα με την οποία πρέπει να υιοθετηθεί ένα μοντέλο διακυβέρνησης για την ασφάλεια του Διαδικτύου που θα περιλαμβάνει την συνεργασία μεταξύ των κυβερνήσεων, κρατικών φορέων, των απλών πολιτών καθώς και της ακαδημαϊκής κοινότητας[40].

Τέλος, σύμφωνα με την Διεθνή Στρατηγική, οι ΗΠΑ διαφυλλάτουν το δικαίωμα να κάνουν χρήση οποιουδήποτε μέτρου για την προστασία την δική τους και των συμμάχων τους τονίζοντας όμως ότι θα εξαντλήσουν πρώτα όλα τα δυνατά μέσα πριν προβούν στο έσχατο μέσο , την χρήση στρατιωτικής βίας. Οι ΗΠΑ μετά τις κυβερνοεπιθέσεις που δέχτηκαν το 2008 από hackers , οι οποίοι

[38] https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain
[39] https://gssd.mit.edu/search-gssd/site/national-military-strategy-cyberspace-60365-sun-06-16-2013-1531
[40] https://www.justsecurity.org/17729/time-u-s-international-strategy-cyberspace/

κατάφεραν να υποκλέψουν διαβαθμισμένο και αδιαβάθμητο υλικό, έλαβαν δρακόντεια μέτρα για την προστασία των κυβερνητικών και μη δικτύων της χώρας. Στα τέλη Σεπτεμβρίου του 2010 υπογράφτηκε το Σύμφωνο Συνεργασίας, πέντε σελίδων, μεταξύ του Υπουργείου Εσωτερικής Ασφάλειας (DHS) και του Υπουργείου Άμυνας (DoD) για θέματα ασφάλειας στον κυβερνοχώρο. Στόχος την συμφωνίας αυτής ήταν να δημιουργηθεί ένα πλαίσιο συνεργασίας μεταξύ των υπαλλήλων από το DHS το DoD και την Εθνική Υπηρεσία Ασφαλείας [41].

Ήδη από τον Πρώτο Πόλεμο του Περσικού Κόλπου προσπάθησαν να αντιμετωπίσουν τους Ιρακινούς σκεπτόμενοι την διεξαγωγή κυβερνοεπιθέσεων. Ωστόσο το σχέδιο δεν υλοποιήθηκε διότι δεν θεωρήθηκε ιδιαίτερα ασφαλές με αποτέλεσμα να χρησιμοποιηθούν αμερικανικές βόμβες. Τελικά στον Πρώτο Πόλεμο του Περσικού Κόλπου οι Αμερικανοί κατάφεραν να διεισδύσουν σε ιρακινές ιστοσελίδε. να παραπλανήσουν και να αιφνιδιάσουν τους αντιπάλους τους στέλνοντας μηνύματα σε μέλη του Ιρακινού Στρατού να αφήσουν τα όπλα τους [42].

Ωστόσο, οι ΗΠΑ παρά το πλήθος των κυβερνοεπιθέσεων τις οποίες έχουν πραγματοποιήσει έχουν αποτελέσει πολλάκις στο παρελθόν και θύμα κυβερνοεπιθέσεων από χώρες με αντικρουόμενα συμφέροντα. Μια περίπτωση που έχουμε ήδη αναφέρει παραπάνω είναι η Moonlight Maze για την οποία οι ΗΠΑ κατηγόρησαν την Ρωσία. Μια εξίσου σοβαρή περίπτωσης κυβερνοεπίθεσης ήταν, όταν το 2008 παραβιάστηκαν τα δίκτυα των ηλεκτρονικών υπολογιστών του Πενταγώνου και υποκλάπηκαν σημαντικά στοιχεία που αφορούσαν την αμερικανική άμυνα. Η παραβίαση πραγματοποιήθηκε με την βοήθεια μιας συσκευής της λεγόμενης flash drive, η οποία τοποθετήθηκε σε έναν στρατιωτικό φορητό υπολογιστή σε μια βάση στη Μέση Ανατολή. Ο ξένος πράκτορας χρησιμοποίησε το flash drive για να «μολύνει» υπολογιστές, συμπεριλαμβανομένων και αυτών που η Κεντρική Στρατιωτική Διοίκηση χρησιμοποιούσε για την επίβλεψη των ζωνών πολέμου

[41] http://www.darkreading.com/risk-management/homeland-security-defense-sign-cybersecurity-pact/d/d-id/1093324?

[42] Clarke R and Knake R.K, “Cyberwar : The Next Threat to National Security And What To do about it, HarperCollins Publishers, New York, 2010, p.10-11

στο Ιράκ και στο Αφγανιστάν. Το αποτέλεσμα του όλου εγχειρήματος ήταν απόρρητα στοιχεία και επιχειρησιακά σχέδια να μεταφερθούν σε servers ξένων δυνάμεων μέσα σε λίγα μόνο λεπτά. Σύμφωνα μάλιστα με τον υφυπουργό Άμυνας των ΗΠΑ William J. Lynn, σε άρθρο του στο Journal ofForeign Affairs. «Πρόκειται για το χειρότερο εφιάλτη ενός διαχειριστή δικτύων: ένα ανεξέλεγκτο πρόγραμμα που δρα σιωπηλά, σχεδιασμένο να μεταφέρει επιχειρησιακά σχέδια στα χέρια κάποιου άγνωστου αντίπαλου»[43]. Μια ακόμη περίπτωση κυβερνοεπίθεσης που δέχτηκαν οι ΗΠΑ στα αεροσκάφη (UAVs) ήταν τον Σεπτέμβριο του 2011, όταν ένας ιός υπολογιστών «μόλυνε» τα δίκτυα της Creach Air Force Base ,η οποία είναι υπεύθυνη για τα αμερικανικά UAVs Predator και Reaper τα οποία πετούν πάνω από απομακρυσμένα αποστολές στο Αφγανιστάν και σε άλλες ζώνες μάχης [44].

2.4 Βόρεια Κορέα

Το κράτος αυτό για να ενισχύσει την θέση του στο διεθνές σύστημα αλλά και για να βελτιώσει τις αμυντικές και επιθετικές του ικανότητες αποφάσισε να ρίξει περισσότερο βάρος στις κυβερνοεπιθέσεις επενδύοντας μεγάλα ποσά από τον ετήσιο προϋπολογισμό του σε πυραύλους, πυρηνικά όπλα καθώς και οποιοδήποτε νέο τεχνολογικό επίτευγμα, ώστε να εξασφαλίσει την υπεροχή που αναζητούσε έναντι των αντιπάλων του. Έτσι το 2000 η Βόρεια Κορέα προχώρησε στην δημιουργία του Kwangmyong, ενός εθνικού intranet . Η ειδοποιός διαφορά αυτού του δικτύου σε σχέση με τα υπόλοιπα παγκόσμια δίκτυα είναι ότι αυτό είναι προσβάσιμο μόνο μέσα στην Βόρεια Κορέα και πουθενά αλλού και μάλιστα έχουν κυριώς πρόσβαση το Υπουργείο Εξωτερικών και οι Ένοπλες Δυνάμεις [45] .

---

[43] http://www.antinews.gr/action.read/%CE%9A%CF%8C%CF%83%CE%BC%CE%BF%CF%82/%CE%97-%CE%91%CE%BC%CE%B5%CF%81%CE%B9%CE%BA%CE%AE-%CE%B4%CE%AD%CF%87%CF%84%CE%B7%CE%BA%CE%B5-%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE-%CE%B5%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7/5.84847

[44] http://www.wired.com/2011/10/virus-hits-drone-fleet/

[45] https://en.wikipedia.org/wiki/Kwangmyong_(network)

Οι επιθετικές της δυνατότητες στον Κυβερνοχώρο αναπτύσσονται με ραγδαίους ρυθμούς εξαιτίας της καλής συνεργασίας με πολλά Πανεπιστήμια και ερευνητικά κέντρα γενικά. Για παράδειγμα το 1986 οι Ένοπλες Δυνάμεις ξεκίνησαν το 1986 ένα ερευνητικό πρόγραμμα στο Κολλέγιο Mirim σχετικά με τα δίκτυα των ηλεκτρονικών υπολογιστών με σκοπό να λάβουν τις απαραίτητες γνώσεις τα στελέχη τους [46]. Σύμφωνα με επίσημα στοιχεία που έχουν δημοσιοποιηθεί , η Βόρεια Κορέα διαθέτει 10-30.000 άτομα για να διενεργούν κυβερνοεπιθέσεις και να βρίσκονται σε ετοιμότητα για να διενεργούν τρομακρατικές επιθέσεις εις βάρος της Νότιας Κορέας. Πρόκειται για άτομα εκπαιδευμένα , με δεκαετή εμπειρία σε θέματα τρομοκρατίας, πειρατείας και γενικότερα κυβερνοπολέμου.[47] Αναφορικά με τις εντάσεις που επικρατούν μεταξύ Βόρειας και Νότιας Κορέας , πρέπει να αναφέρουμε τις « μαζικές» κυβερνοεπιθέσεις που διενήργησε η Βόρεια Κορέα το καλοκαίρι του 2009 εναντίον της Νότιας Κορέας και των ΗΠΑ. Στις 4 Ιουλίου του 2009 η Βόρεια Κορέα προχώρησε σε εκτοξεύσεις πυραύλων μικρής εμβέλειας καθώς και σε κυβερνοεπιθέσεις κατά αμερικανικών και νότιο- κορεατικών κυβερνητικών ιστοσελίδων. Ο τρόπος με τον οποίο «χτυπήθηκαν» τα αμερικανικά δίκτυα ήταν ο εξής: Αρκετές αμερικανικές ιστοσελίδες δέχτηκαν ένα εκατομμύριο σχεδόν ερωτήσεις μέσα σε λίγα δευτερόλεπτα από ένα «Botnet» [48] περίπου 40.000 υπολογιστών με αποτέλεσμα να τεθούν εκτός λειτουργίας. Στόχοι αυτής της επίθεσης ήταν οι Υπηρεσίες Πληροφοριών, το Υπουργείο Οικονομικών, το χρηματιστήριο και ο Λευκός Οίκος. [49]

3. Ο Κυβερνοχώρος

3.1 Ορισμός

[46] Billo, Charles and Chang, Welton, “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States(Institute for security technology studies at Dartmouth College, Hannover, 2004
[47] https://defensesystems.com/blogs/cyber-report/2011/08/north-korea-cyber-capabilities.aspx
[48] https://en.wikipedia.org/wiki/Botnet
[49] Clarke R and Knake R.K, “Cyberwar : The Next Threat to National Security And What To do about it, HarperCollins Publishers, New York, 2010, p. 24

Ως Κυβερνοχώρος (cyberspace) [50] ορίζεται ως μια νοητή περιοχή η οποία χρησιμοποιείται για την ανταλλαγή και αποθήκευση των δεδομένων. Η κατανόηση αυτής της νέας έννοιας «κυβερνοχώρος» διαμορφώθηκε από δύο άρθρα του Γουόρεν ΜακΚάλλοχ που δημοσιεύθηκαν το 1943 και το 1944 αντίστοιχα. Και οι δύο δημοσιεύσεις ασχολούνταν με υπολογισμούς αντιδράσεων σε νευρικά συστήματα ζώντων οργανισμών σύμφωνα με τα ερεθίσματα του περιβάλλοντος. Συμπέρανε ότι η τοπολογία του νευρικού συστήματος δεν υποδεικνύει κάποια τάξη με την έννοια της ιεραρχίας. Επιπρόσθετα σημείωσε «ότι η τυπική περιγραφή του νευρικού συστήματος δεν είναι δυνατή με τα εργαλεία της κλασικής δυαδικής λογικής» αλλά με την έννοια της ετεραρχίας, δηλαδή της συνεργατικής και συνδυασμένης δράσης. Από αυτή την άποψη γνωστοποίησε αυτό που αποκαλείται χαοτική ανάπτυξη του κυβερνοχώρου, αλλά και της συνδυαστικής ικανότητας (ετεραρχίας) που αντιδρά στην καθορισμένη ιεραρχία πραγμάτων [51]. Εκείνος που χρησιμοποίησε τον όρο για να περιγράψει σε ένα διαφορετικό επίπεδο τον συνδυασμό της τεχνολογίας υπολογιστών και των τηλεπικοινωνιών ήταν κατά τον von Joachim Paul ο δημοσιογράφος και φιλόσοφος των ΜΜΕ Τζον Πέρρυ Μπάρλοου (John Perry Barlow), ο οποίος διακήρυξε ότι χρειάζεται να αναπτυχθούν νέες μεταφορικές έννοιες, νέοι κανόνες και πρότυπα συμπεριφοράς για το δίκτυο πληροφοριών του νέου κόσμου[52]. Στην ουσία είναι ένας εικονικός χώρος ο οποίος αποτελεί κατασκεύασμα του ανθρώπου[53] . Περιλαμβάνει το σύνολο των παγκοσμίων δικτύων των υπολογιστών και των περιφερειακών συσκευών (πχ. Εκτυπωτές, routers, modems, servers). Σύμφωνα με ένα ορισμό που δίνει ο R. Clarke: «Ο Κυβερνοχώρος είναι το σύνολο των δικτύων των ηλεκτρονικών υπολογιστών σε παγκόσμιο επίπεδο καθώς και οτιδήποτε συνδέεται και

[50] Η ελληνική λέξη 'κυβερνοχώρος' είναι μεταφραστικό 'δάνειο' από την αγγλική λέξη 'cyberspace', την οποία επινόησε ο συγγραφέας έργων επιστημονικής φαντασίας *William Gibson*, στην προσπάθειά του να περιγράψει το όραμά του για ένα παγκόσμιο δίκτυο η/υ που θα συνέδεε ανθρώπους, μηχανές και πληροφορίες. Βέβαια, η λέξη 'cyberspace' είναι εμπνευσμένη από την επιστήμη των cybernetics (κυβερνητική), η οποία με τη σειρά της ετυμολογικά βασίζεται στο ελληνικό ρήμα 'κυβερνώ'.

[51] https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82

[52] https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82

[53] http://fas.org/irp/doddir/usaf/afdd3-12.pdf (p.. 2-3)

ελέγχεται από αυτά [54]. Κατά τον ορισμό που δόθηκε από την Υπηρεσία Ερευνών των ΗΠΑ ο Κυβερνοχώρος αποτελεί « την συνολική διαδικτύωση των ανθρώπων μέσω των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών ανεξάρτητα από την φυσική γεωγραφία» . Πρόκειται για έναν ορισμό από τον οποίο ρητά προκύπτει ένα βασικό χαρακτηριστικό του Κυβερνοχώρου, η λειτουργία του ανεξάρτητα απόγεωγραφικά σύνορα και αποστάσεις του πραγματικού κόσμου.

Όπως γίνεται αντιληπτό ο Κυβερνοχώρος είναι ευρύτερη έννοια από το Internet, κάτι που θα αναλυθεί πιο σχολαστικά και στην συνέχεια της εργασίας. Αρκετοί επιστήμονες και μελετητές θεωρούν ότι ο Κυβερνοχώρος αποτελεί παγκόσμια κληρονομιά της ανθρωπότητας (common heritage of mankind) και για αυτό κρίνεται επιβεβλημένη η θέσπιση νέων κανόνων διεθνούς δικαίου [55]. Εκτός λοιπόν από το Διαδίκτυο , ο Κυβερνοχώρος περιλαμβάνει το σύνολο των εσωτερικών δικτύων που εξυπηρετούν δημόσιες υπηρεσίες, τράπεζες, επιχειρήσεις στον ιδωτικό τομέα, χρηματιστήρια, τηλεπικοινωνίες , τις Ένοπλες Δυνάμεις (πχ τα δίκτυα οπλικών συστημάτων), την δημόσια υγεία, τα νοσοκομεία, την εναέρια κυκλοφορία, την ύδρευση. Ο κυβερνοχώρος θα μπορούσε να χαρακτηρισθεί και ως ένας «προσβάσιμος παγκόσμιος ψηφιακός χώρος».

Συμπερασματικά, η έννοια του Κυβερνοχώρου δημιουργήθηκε σταδιακά με την βοήθεια της τεχνολογικής εξέλιξης αλλά και της επιστήμης και συνιστά έναν ιστό διασυνδεδεμένων δικτύων στα οποία είναι αποθηκευμένες διάφορες πληροφορίες και όπου συνδέονται, ανάλογα με την κάθε χώρα, οι υποδομές των χωρών και μέσω του οποίου διεξάγονται καθημερινά εκατομμύρια ανθρώπινες δραστηριότητες ορισμένες από τις οποίες αναφέραμε και προηγουμένως [56]. Η οργάνωση και η λειτουργία του Κυβερνοχώρου είναι χαοτική δίνοντας έτσι την δυνατότητα σε άτομα χωρίς κάποια άδεια και εντελώς

[54] Ο ορισμός αυτός δόθηκε από τον R. Clarke στο βιβλίο του “Cyberwar : The Next Threat to National Security And What To do about it” Harper Collins Publishers, New York, 2010
[55] Kamal Ahmad, “The Law of Cyber-Space – An Invitation to The Table of Negotiations”, United Nations Institute of Training and Research (UNITAR), 2005
[56] http://www.onalert.gr/stories/kybernoxwros-kybernoamyna-xarakthristika-stoxoi/29371

αυθαίρετα να προβαίνουν σε ενέργειες παράνομης υποκλοπής πληροφοριών και δεδομένων. Επίσης από ακρετούς θεωρείται ως ο « πέμπτος κοινός χώρος» μετά το έδαφος, τη θάλασσα, τον αέρα και το διάστημα.

3.2 Επίπεδα Λειτουργίας του Κυβερνοχώρου

Πριν προχωρήσουμε στα χαρακτηριστικά γνωρίσματα του Κυβερνοχώρου , κρίνεται σκόπιμο να αναφέρουμε τα τρία επίπεδα στα οποία διαρθρώνεται το εικονικό αυτό πεδίο τα οποία είναι τα εξής: το φυσικό επίπεδο (physical layer), το συντακτικό επίπεδο (syntactic layer) και το σημασιολογικό επίπεδο (semantic layer) [57].

Το φυσικό επίπεδο αναφέρεται ουσιαστικά στο υλικό , στα μεταλλικά κουτιά, τα καλώδια, στις οθόνες, εκτυπωτές και τα scanners. Χωρίς αυτό κανένα πληροφοριακό σύστημα δεν μπορεί να υπάρξει. Να να επισημάνουμε ότι ένα δίκτυο είναι αδύνατον να εξαπατηθεί μόνο με τη φυσική καταστροφή των εξαρτημάτων του, μπορεί όμως να εξαπατηθεί με την υποκατάσταση ενός εξαρτήματος με κάποιο άλλο ώστε να μην λειτουργεί όπως το είχε σχεδιάσει ο κατασκευαστής του.

Το συντακτικό επίπεδο περιέχει τις οδηγίες και τις εντολές τις οποίες οι σχεδιαστές και οι χρήστες δίνουν στα μηχανήματα, καθώς και τα πρωτόκολλα με τα οποία οι μηχανές επικοινωνούν μεταξύ τους (: device recognition, packet framing, addressing, routin, database manipulation). Αυτό το σύνολο των οδηγιών είναι που στοχοποιούν οι hackers , οι οποίοι με άδολα μέσα και χωρίς κάποια άδεια επιθυμούν να επεμβαίνουν στο λογισμικό.

Το τρίτο επίπεδο το σημασιολογικό , περιλαμβάνει όλες τις πληροφορίες που περιέχουν τα μηχανήματα και των οποίων η επεξεργασία, η μεταφορά αλλά και η διαχείριση είναι υψίστης σημασίας. Το μεγαλύτερο ποσοστό των πληροφοριών αυτών είναι πληροφορίες που έχουν νόημα μόνο για τα ανθρώπινα όντα ως χρήστες ι των δικτύων και προορίζεται γι’ αυτά. Σε αυτό το επίπεδο ουσιαστικά ελέγχεται η εννοιλογική ορθότητα μιας εντολής, αν δηλαδή σύμφωνα με τον ανθρώπινο νου βγαίνει κάποιο νόημα. Η επίθεση σε αυτό το

[57] Libicki Martin C., «Cyberdeterrence and cyberwar», RAND Corporation, 2009,σελ.12-13

επίπεδο μπορεί να επιτευχθεί με την εισαγωγή μιας «ψευδούς» εντολής .[58] Για να καταφέρει κάποιος να επέμβει στο σημασιολογικό επίπεδο και να δώσει ψευδείς πληροφορίες θα πρέπει προηγουμένως να έχει διεισδύσει και στο συντακτικό.

3.3 Χαρακτηριστικά γνωρίσματα του Κυβερνοχώρου

α) Η απουσία γεωγραφικών συνόρων

Ένα από τα βασικότερα χαρακτηριστικά του Κυβερνοχώρου είναι ότι δεν προσδιορίζεται γεωγραφικά, δεν επιδέχεται οριοθετήσεις , διακρίνεται δηλαδή από την απουσία οποιουδήποτε γεωγραφικού συνόρου**.** Ενώ για την ύπαρξη οποιασδήποτε μορφής χώρου απαιτούνται σταθερά σημεία αναφοράς, ο κυβερνοχώρος στερείται διαστάσεων, σαφώς καθορισμένων ορίων και αμετακίνητων σημείων προσανατολισμού [59]. Η επιστημονική συγγραφέας Margaret Wertheim υποστηρίζει ότι το Διαδίκτυο μας παρέχει μια νέα έννοια του χώρου. «Διασκορπισμένος στο Διαδίκτυο», λέει η συγγραφέας, «ο χώρος μου δεν μπορεί πλέον να καθοριστεί με καθαρά φυσικά κριτήρια. Το πού ακριβώς βρίσκομαι όταν μπαίνω στο Διαδίκτυο είναι ένα ερώτημα προς διερεύνηση, αλλά σίγουρα η θέση μου δεν μπορεί να μετρηθεί μαθηματικά ή γεωγραφικά». Έτσι το μόνο που μπορούμε να επιβεβαιώσουμε για τη φύση του κυβερνοχώρου είναι ότι περιλαμβάνει μια μορφή ψηφιακής επικοινωνίας.[60]

Ωστόσο στο άρθρο 21 του Εγχειριδίου του Ταλίν αναφέρεται ότι οι επιχειρήσεις στον Κυβερνοχώρο υπόκεινται σε γεωγραφικούς περιορισμούς που επιβάλλονται από τις σχετικές διατάξεις του διεθνούς δικαίου, το οποίο εφαρμοζέται κατά τη διάρκεια μιας ένοπλης σύγκρουσης [61]. Ωστόσο υποστηρίζει η Ομάδα Εμπειρογνωμόνων ότι οι περιορισμοί με βάση τα

[58] Ο όρος 'ψευδής' αναφέρεται στην προκειμένη περίπτωση σε μία λογική τιμή που μπορεί να αποδοθεί σε μεταβλητές λογικού τύπου
[59] http://www.eeei.gr/interbiz/articles/cybspace.htm
[60] https://el.wikipedia.org/wiki/Κυβερνοχώρος
[61] «Cyber operations are subject to geographical limitations imposed by the relevant provisions of international law applicable during an armed conflict»

γεωγραφικά κριτήρια είναι ιδιαίτερα δύσκολο να εφαρμοστούν στο πλαίσιο του Κυβερνοπολέμου.

β) Η μεταβλητότητα

Μια από τις πλευρές του κυβερνοχώρου μπορεί να χαρακτηριστεί και ως πρωτεϊκή. Όπως ο Πρωτέας, ο θεός που μπορούσε να αλλάξει συνεχώς μορφές, έτσι και ο κυβερνοχώρος αλλάζει διαρκώς έκταση και βάθος.Σαν ανθρώπινο δημιούργημα είναι ατελές. Παλαιά στοιχεία διαγράφονται για να δώσουν τη θέση τους σε καινούργια, η ραγδαία τεχνολογική ανάπτυξη επιτρέπει την καταγραφή περισσότερων δεδομένων και καινούργιες ευκαιρίες δίδονται στους χρήστες για να γνωρίσουν τις άγνωστες πλευρές του κυβερνοχώρου.[62]

γ) Η ανωνυμία

Η ανωνυμία στην ελεύθερη έκφραση στο διαδίκτυο αποτελεί αναμφισβήτητα ένα δικαίωμα που προστατεύεται από τον νόμο ως επιμέρους έκφανση της Ελυθευρίας Έκφρασης[63]. Ωστόσο, η κατάχρηση της δοκιμάζει την ελευθεριότητα του κυβερνοχώρου και διευκολύνεται έτσι η διάπραξη εγκλημάτων υπό το πέπλο της ανωνυμίας με απότελσμα να καθίσταται ιδιαίτερα δυσχερής η εξιχνίαση τους. Η ανωνυμία του Κυβερνοχώρου οφείλεται στις τεχνικές που μπορεί να χρησιμοποιήσει ο κάθε χρήστης έτσι ώστε να μην αποκαλυφθεί. [64] Στην πραγματικότητα όμως αν εξαιρέσουμε ορισμένες ισχυρές τεχνολογίες κρυπτογράφησης που χρησιμοποιούνται για την εξασφάλιση της ανωνυμίας, η κατάσταση είναι λίγο διαφορετική. Από την στιγμή που κάθε υπολογιστής συνδέεται στο διαδίκτυο με μία διεύθυνση Πρωτοκόλλου

[62] http://www.eeei.gr/interbiz/articles/cybspace.htm
[63] Η ελευθερία έκφρασης κατοχυρώνεται στο Ελληνικό Σύνταγμα και στις διεθνείς συνθήκες προστασίας των ανθρωπίνων δικαιωμάτων (14 § 1 Σ, 10 § 1 ΕΣΔΑ, 19 § 2 ΔΣΑΠΔ)
[64] Clarke R and Knake R .K, “Cyberwar : The Next Threat to National Security And What To do about it, HarperCollins Publishers, New York, 2010, p.92

Διαδικτύου (Internet Protocol –IP) [65] , μέσω αυτής η διαδρομή που ακολουθεί κάθε χρήστης στον παγκόσμιο ιστό είναι ανιχνεύσιμη, ενώ μπορεί να ανευρεθεί από ποια θέση και σε ποια χρονική στιγμή πραγματοποιήθηκε οποιαδήποτε μεταφορά δεδομένων . Επιπρόσθετα να επισημάνουμε ότι η διεύθυνση IP είναι κατά κανόνα μοναδική, με αποτέλεσμα να επιτρέπει την αναγνώριση της ταυτότητας του χρήστη.[66]

δ) Η ταχύτητα και οι διαστάσεις

Η μεταφορά ψηφιακών δεδομένων μέσα στον Κυβερνοχώρο και μάλιστα από την μια πλευρά του Πλανήτη στην άλλη μπορεί να διεξαχθεί μέσα μόνο σε λίγα δευτερόλεπτα. Ο ταχέως αναπτυσσόμενος παγκόσμιος ιστός έχει οδηγήσει και στην ραγδαία αύξηση στην ταχύτητα ανταλλαγής πληροφοριών. Από την άλλη πλευρά οι διαστάσεις του Κυβερνοχώρου διαρκώς αυξάνονται λόγω της αύξησης των χρηστών του Διαδικτύου . Σύμφωνα με στοιχεία της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU) , στο τέλος του 1997 περίπου 70 εκατομμύρια άνθρωποι, ποσοστό που αντιστοιχούσε στο 1,7 % του παγκόσμιου πληθυσμού. Το 2009, μόνο δύο χρόνια αργότερα δηλαδή, ο αριθμός των χρηστών αυξήθηκε σε περίπου 1,9 δισεκατομμύρια ανθρώπους-δηλαδή στο 26 τοις εκατό του παγκόσμιου πληθυσμού. Κατά την πενταετία 2005-2010 ο αριθμός των χρηστών ανήλθε στα δύο δις.[67] Αυτή η αλματώδης αύξηση του αριθμού των χρηστών οφείλεται επίσης στο γεγονός ότι ο Κυβερνοχώρος είναι ένα πεδίο άμεσα προσβάσιμο από τον καθένα και με πολύ χαμηλό κόστος.

3.4 Το Διαδίκτυο , ως ειδικότερη μορφή του Κυβερνοχώρου

Οι προσπάθειες για τη δημιουργία ενός διαδικτύου ξεκίνησαν στις Η.Π.Α. κατάτη διάρκεια του ψυχρού πολέμου, στα πλαίσια εξεύρεσης λύσεων για την

[65] Το Πρωτοκόλλο Διαδικτύου (IP) αποτελεί το κύριο πρωτόκολλο επικοινωνίας για την μετάδοση πακέτων δεδομένων στο Διαδίκτυο και είναι αυτό πάνω στο οποίο είναι βασισμένο το Διαδίκτυο (https://el.wikipedia.org/wiki/Internet_Protocol)

[66] https://athens.indymedia.org/post/1472405/

[67] https://www.unric.org/el/index.php?option=com_content&view=article&id=26339&Itemid=18

προστασία των τηλεπικοινωνιών σε μια ενδεχόμενη πυρηνική επίθεση από την Σοβιετική Ένωση. Έτσι το 1969, η «Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων» (Advanced Research Projects Agency - ARPA) του υπουργείου Άμυνας των ΗΠΑ αποφάσισε τη δημιουργία ενός δικτύου τεσσάρων ηλεκτρονικών υπολογιστών (ARPANET) έτσι ώστε να εξασφαλίζεται η μεταξύ τους επικοινωνία, ακόμη και στην περίπτωση που ένας από αυτούς θα παρουσίαζε πρόβλημα στη λειτουργία του. Το Δίκτυο αυτό είχε καθαρά στρατιωτική προέλευση. Σχετικά με την δημιουργία του ARPANET διατυπώθηκαν δύο απόψεις. Σύμφωνα με την πρώτη, ο ανταγωνισμός μεταξύ ΗΠΑ και ΕΣΣΔ και η προσπάθεια υπεροχής και από τις δύο πλευρές στον Κυβερνοχώρο οδήγησε στην δημιουργία του ARPANET [68].

Σύμφωνα με την δέυτερη εκδοχή [69] η δημιουργία του είχε σκοπό την διασφάλιση της εθνικής ασφάλειας των ΗΠΑ στο ενδεχόμενο μιας πυρηνικής απειλής, μιας μόνιμης απειλής που επικρατούσε μετά τον Ψυχρό Πόλεμο.Έπρεπε να δημιουργηθεί ένα δίκτου ηλεκτρονικών υπολογιστών που και αν ακόμη ορισμένοι από αυτούς αδρανοποιούνταν σε περίπτωση πυρηνικής απειλής, το σύστημα επικοινωνιών για την εύρυθμη λειτουργία των στρατιωτικών επιχειρήσεων δεν θα επηρεαζόταν στο σύνολο του. Έτσι εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969, το ARPANET με τέσσερις κόμβους, μέσω των οποίων συνδέονταν τέσσερις υπερυπολογιστές, οι οποίοι τοποθετήθηκαν στο Πανεπιστήμιο της Καλιφόρνια (στη Σάντα Μπάρμπαρα και στο Λος Άντζελες), στο Πανεπιστήμιο SRI στο Στάνφορντ και στο Πανεπιστήμιο του Utah. Το 1971, οι κόμβοι αυξήθηκαν σε 15 και το 1972 ο αριθμός τους ανέρχονταν σε 37. Στο δεύτερο αυτό χρόνο λειτουργίας επινοήθηκε και το e-mail, ενώ σε σύντομο χρονικό διάστημα ανακαλύφθηκαν και οι Ταχυδρομικές Λίστες (Mailing Lists) οι οποίες στηρίχθηκαν στην τεχνική μετάδοσης των μηνυμάτων από κόμβο σε κόμβο, καθώς το ίδιο μήνυμα

[68] Η έκπληξη που δημιουργήθηκε στον Αμερικανό στρατιωτικό αλλά και επιστημονικό χώρο από την θέση σε τροχία του πρώτου δορυφόρου , του Sputnik, από την ΕΣΣΔ, οδήγησε στην Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων, Rid Th, - Hecker Marc, “War 2:0 Irregular Warfare in the Information Age, Preager Security International”, p.26

[69] Stevens Sh. “ Internet war crime tribunals and security in an interconnected world , Transnatioanl Law and Contemporary Problems “, 2009, p.3

μπορούσε να σταλεί ταυτόχρονα σ' όλα τα μέλη της λίστας κοινών ενδιαφερόντων (multicasting)[70].

Το πρωτόκολλο επικοινωνίας που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους ηλεκτρονικών υπολογιστών. Στις αρχές της δεκαετίας του '70 αναπτύχθηκε το πρωτόκολλο επικοινωνίας TCP (Transmission Control Protocol) , που αντικατέστησε το NCP. Λίγο αργότερα το TCP μετονομάστηκε σε TCP/IP (Transmission Control Protocol/ Internet Protocol). Το πρώτο (TCP) είναι υπεύθυνο για την διάσπαση της κάθε πληροφορίας σε περισσότερα «πακέτα» ενώ το δεύτερο για την πορεία που θα ακολουθήσουν αυτά τα «πακέτα» ώστε να φθάσουν στο σωστό προορισμό. Το σύστημα είχε ως αποστολή απλώς να μεταφέρει τα πακέτα έχοντας πλήρη άγνοια για το περιεχόμενο τους [71] Από το 1983 και μετά έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET. Το 1974 εγκαινιάστηκε το telnet , η πρώτη εμπορική εκδοχή του ARPANET. Το 1983 το ARPANET χωρίσθηκε σε δύο κομμάτια , το στρατιωτικό Milnet με αυστηρά ελεγχόμενη πρόσβαση και στο ακαδημαϊκό ARPANET στο οποίο είχε πρόσβαση ο καθένας [72]. Το 1984 το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ (National Science Foundation- NSF) δημιούργησε ένα νέο δίκτυο που ονομάστηκε NSFNet το οποίο όπως αποδείχτηκε αποτέλεσε την ραχοκοκαλία για το Διαδίκτυο [73]. Ένα δείγμα της δημοτικότητας του Internet μπορούν να αποτελέσουν τα σχετικά δημοσιεύματα σε διάφορα περιοδικά. Το Ανώτατο Δικαστήριο των ΗΠΑ δημοσιοποιεί τις αποφάσεις του και στο Διαδίκτυο [74].

Ορόσημο στο χώρο του Διαδικτύου αποτέλεσε η δημιουργία του παγκόσμιου ιστού (www – world wide web) [75] από τον Βρετανό Tim Berners – Lee το 1989

[70] http://hermes.di.uoa.gr/exe_activities/diadiktio/11_____.html
[71] Stevens Sh. : " Internet war crime tribunals and security in an interconnected world , Transnatioanl Law and Contemporary Problems ", 2009, p .4
[72] http://hermes.di.uoa.gr/exe_activities/diadiktio/11_____.html
[73] http://www.calvin.edu/academic/rit/webBook/chapter3/Introduction/ARPAgrows.htm
[74] http://hermes.di.uoa.gr/exe_activities/diadiktio/11_____.html
[75] Η τεχνική σχεδιασμού κειμένων που κάνουν χρήση υπερ-συνδέσμων (hyper-links) ονομάζεται 'υπερ-κείμενο' (hypertext), ενώ η γλώσσα που χρησιμοποιείται για την κατασκευή σελίδων του www ονομάζεται HTML (HyperText Markup Language). Για τη μεταφορά των σελίδων του www

που εκείνη την εποχή εργαζόταν στον Ευρωπαϊκό Οργανισμό Πυρηνικών Ερευνών (CERN) στην Γενεύη της Ελβετίας . Αυτό που οδήγησε τον Lee στην εφεύρεση του Παγκόσμιου ιστού ήταν το όραμά του για ένα κόσμο όπου ο καθένας θα μπορούσε να ανταλλάσσει πληροφορίες και ιδέες άμεσα προσβάσιμες από τους υπολοίπους. Στην ουσία πρόκειται για μια διασύνδεση πολλών μη ιεραρχημένων στοιχείων που παλαιότερα ήταν απομονωμένα. Τα στοιχεία αυτά μπορούν να πάρουν και άλλες μορφές πέραν της μορφής του γραπτού κειμένου, όπως εικόνας και ήχου.[76] Τέλος να επισημάνουμε ότι το Διαδίκτυο λειτουργεί σε μεγάλο βαθμό από κονδύλια του ιδωτικού τομέα και δεν διαθέτει κεντρική διεύθυνση – διοίκηση, παρά μόνο στις διευθύνσεις internet (internet protocol addresses) που απονέμονται και στις ονοματοδοσίες DNS από τον διεθνή μη- κερδοσκοπικό οργανισμό ICANN (Internet Corporation for Assigned Names and Numbers).

ΚΕΦΑΛΑΙΟ Β΄ Οι Επιθέσεις στον Κυβερνοχώρο

Ο συνεχώς αυξανόμενος αριθμός των χρηστών στο Διαδίκτυο και γενικότερα στον Κυβερνοχώρο με αντικρουόμενα συμφέροντα μεταξύ τους έχει μετατρέψει τον Κυβερνοχώρο σε πεδίο έντονης αντιπαράθεσης αποτελώντας εύφορο έδαφος για την τέλεση επιχειρήσεων με κακόβουλες αρκετές φορές προθέσεις και κίνητρα. Αυτό οφείλεται κυρίως στο γεγονός ότι στον Κυβερνοχώρο έχει άμεση και εύκολη πρόσβαση ο καθένας και στις ασύλληπτες τεχνολογικές δυνατότητες που προσφέρουν οι ηλεκτρονικοί υπολογιστές .

1.1 Ορισμός

Με τον όρο Κυβερνοεπίθεση νοείται κάθε δραστηριότητα που πραγματοποιείται στον Κυβερνοχώρο με εχθρική πρόθεση από την πλευρά

στο internet αναπτύχθηκε ένα ειδικό πρωτόκολλο επικοινωνίας η/υ και μεταφοράς πακέτων δεδομένων, το πρωτόκολλο HTTP (Hyper-Text Transmission Protocol). Για το λόγο αυτό όλες οι διευθύνσεις στον παγκόσμιο ιστό αρχίζουν με τη συντομογραφία *''http://'',* για να φαίνεται ότι το αρχείο στο οποίο παραπέμπουμε είναι μία σελίδα υπερ-κειμένου (hypertext page) και πρέπει να ανακτηθεί μέσω του πρωτοκόλλου http.

[76] https://el.wikipedia.org/wiki/%CE%A0%CE%B1%CE%B3%CE%BA%CF%8C%CF%83%CE%BC%CE%B9%CE%BF%CF%82_%CE%99%CF%83%CF%84%CF%8C%CF%82

ενός κρατικού δρώντα ή ενός ιδιώτη με σκοπό την διείσδυση στα δίκτυα ή στις ιστοσελίδες μιας άλλης χώρας και την πρόκληση ζημίας ή αναταραχής σε αυτά. Όταν αναφερόμαστε στην πρόκληση ζημίας δεν εννοούμε την υλική καταστροφή των ηλεκτρονικών υπολογιστών ή των δικτύων. Στόχος των κυβερνοεπιθέσεων αποτελεί η υποβάθμιση και η αδρανοποίηση της μαχητικής ικανότητας του αντιπάλου. Σύμφωνα με τον Libicki η παράνομη μεταφορά δεδομένων από τα δίκτυα ηλεκτρονικών υπολογιστών δεν αποτελεί κυβερνοεπίθεση [77]. Οι κυβερνοεπιθέσεις (cyber attacks) αποτελούν τμήμα μίας ευρύτερης κατηγορίας επιχειρήσεων οι οποίες είναι γνωστές ως πληροφοριακές επιχειρήσεις (information operations). Υποκατηγορία των πληροφοριακών επιχειρήσεων αποτελούν και οι επιχειρήσεις δικτύων ηλεκτρονικών υπολογιστών γνωστές και ως Computer Network Operations (CNO) . Οι επιχειρήσεις δικτύων, με τη σειρά τους, περιλαμβάνουν τις επιθέσεις σε δίκτυα ηλεκτρονικών υπολογιστών (Computer Network Attack - CNA), τις επιχειρήσεις για την άμυνα των δικτύων, καθώς και τις επιχειρήσεις εκμετάλλευσης των δικτύων (computer network exploitation – CNE) [78]. Οι τελευταίες αφορούν την συλλογή πληροφοριών (network mapping, Cybe Spying ή Espionage)[79] ή την παραποίηση αυτών με σκοπό την παραπλάνηση του αντιπάλου . Από τον συνδυασμό των άρθρων 20 και 30 του Εγχειριδίου του Ταλίν προκύπτει ότι ο όρος « επιχειρήσεις στον κυβερνοχώρο» περιλαμβάνει, αλλά δεν περιορίζεται αποκλειστικά σε « επιθέσεις στον κυβερνοχώρο ». Οι κυβερνοεπιθέσεις , όπως προκύπτει από το Εγχειρίδιο, είναι ένας όρος που αναφέρεται σε μια συγκεκριμένη κατηγορία επιχειρήσεων στον κυβερνοχώρο. Ορισμένες από αυτές, όπως εκείνες που επηρεάζουν την παροχή της ανθρωπιστικής βοήθειας διέπονται από το Δίκαιο των Ενόπλων Συρράξεων ακόμη και όταν οι ανωτέρω δεν έχουν την ένταση μιας «επίθεσης». Ομόφωνα τα μέλη της Διεθνούς Ομάδας Εμπειρογνωμόνων, όπως αναφέρεται στο άρθρο 20 του Εγχειριδίου συμφώνησαν ότι πρέπει να υπάρχει ένας σύνδεσμος μεταξύ της δραστηριότητας στον κυβερνοχώρο και της ένοπλης σύγκρουσης προκειμένου

[77] Libicki M. C, " Cyberdeterrence and Cyberwar (Rand Corporation, Santa Monica, CA, 2009, p. 23-24

[78] http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf (US Joint Publication -1-02, "DoD Dictionary of Military and Associated Terms"

[79] https://en.wikipedia.org/wiki/Cyber_spying

το Δίκαιο των Ενόπλων Συρράξεων να εφαρμοστεί στην εν λόγω δραστηριότητα [80]. Ωστόσο υπήρχε διχογνωμία ως προς την φύση του συνδέσμου. Κατά μια άποψη, το ΔΑΔ τυγχάνει εφαρμογής για κάθε δραστηριότητα στον κυβερνοχώρο που διεξάγεται από ένα συμβαλλόμενο μέρος της ένοπλης σύγκρουσης εναντίον του αντιπάλου του. Σύμφωνα με τη δεύτερη άποψη, η δραστηριότητα στον κυβερνοχώρο πρέπει να έχει αναληφθεί αποκλειστικά για την προώθηση των εχθροπραξιών, προκειμένου να συμβάλλει στη στρατιωτική προσπάθεια του επικεφαλή της όλης επιχείρησης [81].

Οι επιθέσεις σε δίκτυα (Computer Network Attack - CNA) οι οποιές πραγματοποιούνται με συγκεκριμένα «όπλα» - μεθόδους, είναι αυτές που θα αποτελέσουν το αντικείμενο μελέτης μας. Στόχος τους είναι η καταστροφή δεδομένων λειτουργίας του δικτύου με σκοπό την πρόκληση σύγχυσης σε αυτό ή η μετατροπή των δεδομένων που είναι αποθηκευμένα σε αυτό με απώτερο σκοπό το δίκτυο να προβεί σε λανθασμένες ενέργειες από αυτές που είχε προγραμματιστεί[82] και εν τέλει να επέλθει η πλήρης αδρανοποίηση του συστήματος ελέγχου του αντιπάλου και η πρόκληση σοβαρών ζημιών που ξεπερνούν την υλική καταστροφή των δικτύων. Σύμφωνα με το άρθρο 30 του Εγχειριδίου του Ταλίν μια επίθεση στον κυβερνοχώρο είναι μια λειτουργία του τελευταίου, είτε επιθετική ή αμυντική, που εύλογα αναμένεται να προκαλέσει τραυματισμό ή θάνατο σε πρόσωπα ή βλάβη ή καταστροφή σε αντικείμενα [83]. Για τους συντάκτες μάλιστα του εγχειριδίου , ο ορισμός αυτός ισχύει εξίσου σε διεθνείς αλλά και σε μη διεθνείς ένοπλες συγκρούσεις.

---

[80] «All members of the International Group of Experts agreed that there must be a nexus between the cyber activity and the armed conflict for the law of armed conflict to apply to the activity in question»

[81] «According to the second view, the cyber activity must have been undertaken in furtherance of the hostilities, that is, in order to contribute to the originator's military effort»

[82] Libicki M. " Conquest in Cyberspace: National Security and information Warfare" , Cambridge University Press, 2007,p. 76 -85

[83] Στο πρωτότυπο κείμενο «A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

1.2 Είδη των Κυβερνοεπιθέσεων

α) Κυβερνοκατασκοπεία

Ο όρος αυτός περιλαμβάνει όλες εκείνες τις ενέργειες που γίνονται με την βοήθεια του Διαδικτύου στον Κυβερνοχώρο , χωρίς άδεια ή κάποια εξουσιοδότηση και αποσκοπούν στην συλλογή πληροφοριών κυρίως απόρρητων,σχετικά με έναν κρατικό δρώντα , μια κυβέρνηση ή ακόμη και μια επιχείρηση [84]. Αυτές οι πληροφορίες μπορεί να είναι είτε προσωπικά στοιχεία, είτε διαβαθμισμένο υλικό και να αφορούν την εθνική ασφάλεια ενός κράτους , η γνωστοποίηση των οποίων μπορεί να οδηγήσει σε συγκριτικό πλεονέκτημα και υπεροχή σε σχέση με τον αντίπαλο του. Η Κυβερνοκατασκοπεία μπορεί να γίνει με οποιαδήποτε από τα «όπλα» των κυβερνοεπιθέσεων (π.χ κακόβουλο λογισμικό, ιούς, δούρειους ίππους) και πολλά άλλα τα οποία θα αναλύσουμε στην συνέχεια.

Η Κυβερνοκατασκοπεία αποτελεί την πιο δημοφιλή δραστηριότητα στον Κυβερνοχώρο[85]. Η Κίνα είναι η χώρα που κατέχει τα ηνία σε αυτό τον τομέα. Μια γνωστή περίπτωση κυβερνοσκοπείας είναι η υπόθεση « TITAN RAIN», είναι η ονομασία που δόθηκε από την Ομοσπονδιακή Κυβέρνηση των Ηνωμένων Πολιτειών σε μια σειρά συντονισμένων ενεργειών σε υπολογιστικά συστήματα του Υπουργείου Άμυνας από το 2003. Το αποτέλεσμα αυτής επιχείρησης ήταν να εκμαιεύσει η Κίνα πολύτιμες πληροφορίες και να αποσπάσει δεδομένα από το εσωτερικό δίκτυο του Υπουργείου Άμυνας της Αμερικής. Στις αρχές του Δεκεμβρίου του 2005 ο διευθυντής του SANS Institute, ενός ινστιτούτου ασφαλείας στις Ηνωμένες Πολιτείες, δήλωσε ότι οι επιθέσεις ήταν πιθανότατα αποτέλεσμα Κινέζων Στρατιωτικών Χάκερ οι οποίοι ήθελαν να συλλέξουν πληροφορίες σχετικά με τα αμερικανικά υπολογιστικά συστήματα[86] . Πέρα από τα τελευταία, στόχος των Κινέζων Χάκερ ήταν τα

[84] https://en.wikipedia.org/wiki/Cyber_spying
[85] Libicki , M. C., " Cyberdeterrence and Cyberwar ", Rand Corporation, Santa Monica, CA, 2009, p.26
[86] https://en.wikipedia.org/wiki/Titan_Rain

υπολογιστικάσυστήματα των Lockheed Martin 87, Sandia National Laboratories (εργαστήρια) [88] και της NASA.

Μια άλλη περίπτωση προερχόμενη πάλι από την Κίνα είναι η λεγόμενη "Ghostnet" . Είναι το όνομα που δόθηκε από ερευνητές της Information Warfare Monitor [89] σε μια μεγάλης κλίμακας επιχείρηση Κυβερνοκατασκοπείας, η οποία ανακαλύφθηκε τον Μάρτιο του 2009. Η διείσδυση που πραγματοποιήθηκε στα υπολογιστικά συστήματα με την χρήση κακόβουλου λογισμικού αφορούσε σε 103 χώρες του κόσμου. Οι μελέτες έδειξαν ότι το ένα τρίτο περίπου των στόχων που χτυπήθηκαν θεωρούνταν μεγάλης αξίας και περιλάμβαναν υπολογιστικά συστήματα που βρίσκονταν σε Πρεσβείες, Υπουργεία Εξωτερικών, Διεθνείς Οργανισμούς, Μέσα ενημέρωσης , ΜΚΟ και διάφορα κυβερνητικά γραφεία της Ινδίας, της Ταϋλάνδης , του Θιβέτ , του Λονδίνου, της Νέας Υόρκης [90]. Το πρόγραμμα αυτό με την χρήση κακόβουλου λογισμικού είχε την δυνατότητα να ενεργοποιεί κάμερες web και μικρόφωνα στους υπολογιστές [91] που είχαν «μολυνθεί» , έχοντας έτσι την δυνατότητα να καταγράφουν όλες τις συνομιλίες εντός εμβέλειας [92]. Όλες αυτές βέβαια οι ενέργειες δείχνουν την προσπάθεια της Κίνας να αποκτήσει πρωταρχική θέση και υπεροχή στο νέο αυτό πεδίο του Κυβερνοχώρου.

β) Κυβερνοτρομοκρατία (Cyber Terrorism)

Ο όρος αυτός περιλαμβάνει όλες τις δραστηριότητες και παράνομες ενέργειες τέτοιας έντασης, σε ηλεκτρονικούς υπολογιστές και δίκτυα με την βοήθεια

[87] https://en.wikipedia.org/wiki/Lockheed_Martin
[88] https://en.wikipedia.org/wiki/Sandia_National_Laboratories
[89] Πρόκειται για μια προηγμένη δραστηριότητα παρακολούθησης του Κυβερνοχώρου (https://en.wikipedia.org/wiki/Information_Warfare_Monitor)
[90] http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html
[91] Clarke R and Knake R .K, "Cyberwar : The Next Threat to National Security And What To do about it, HarperCollins Publishers, New York, 2010, p. 59-60
[92] http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html

κακόβουλου λογισμικού, ώστε να δημιουργήσουν ένα αίσθημα τρόμου και πανικού μέσα από τις ζημιές που προκαλούν στα υπολογιστικά συστήματα [93]. Θύματα μιας τέτοιας επίθεσης μπορεί να είναι μια κυβέρνηση ή ένας κρατικός φορέας ακόμη όμως και μια ιδωτική επιχείρηση. Συνήθως οι κυβερνοτρομοκράτες « χτυπούν» υποκινούμενοι από πολιτικά, ιδεολογικά ή θρησκευτικά κίνητρα [94]. Οι κυβερνοτρομοκράτες μπορεί είτε να ενεργούν ανεξάρτητα χωρίς κάποιον εργοδότη για δικούς τους ιδεολογικούς – προσωπικούς λόγους είτε να προσφέρουν τις υπηρεσίες τους με κάποιο αντάλλαγμα (χρηματικό συνήθως) λαμβάνοντες οδηγίες – κατευθύνσεις από τρίτους [95]. Σύμφωνα με την Αμερικανική Επιτροπή Υποδομών Ζωτικής Σημασίας στόχοι μιας τέτοιου είδους επίθεσης μπορεί να είναι υπολογιστικά συστήματα τραπεζών , στρατιωτικών εγκατάστασεων ακόμη και σταθμών παραγωγής ηλεκτρικής ενέργειας [96].

γ) <u>Κυβερνοέγκλημα</u>

Σύμφωνα με τον ορισμό που δίνεται από τον Michael Alex το Κυβερνοέγκλημα στην ουσία αποτελείται από Κυβερνοεπιθέσεις εναντίον ατόμων ή ιδιωτικών επιχειρήσεων με απώτερο σκοπό την απόκτηση χρηματικού οφέλους[97] . Οι δράστες του Κυβερνοεγκλήματος είναι συνήθως hackers, οι οποίοι δρουν ανεξάρτητα ή έχουν προσληφθεί από κάποιον εργοδότη με σκοπό είτε να βλάψουν το θύμα (μια κυβέρνηση, ένας ιδωτικός φορέας) είτε να αποκομίσουν οι ίδιοι οικονομικά οφέλη ή υποκινούμενοι πολλές φορές και από προσωπικά κίνητρα[98]. Σύμφωνα με τους Debarati Halder και Dr. K. Jaishankar τα κυβερνοεγκλήματα ορίζονται ως « Αδικήματα που διαπράττονται σε βάρος ατόμων ή ομάδων ατόμων με σκοπό να βλάψουν εσκεμμένα τη φήμη του θύματος ή να προκαλέσουν σωματική ή ψυχική βλάβη ή απώλεια, για το θύμα,

[93] Michael A., " Cyber Probling : The Politicisation of Virtual Attack", Defence Academy of the United Kingdom, p.1 (http://www.conflictstudies.org.uk/files/Cyber_Probing.pdf)
[94] https://en.wikipedia.org/wiki/Cyberterrorism
[95] Lech J. and Colarik A. , " Cyber Warfare and " Cyber Terrorism" , Information Science Reference, New York, 2008
[96] http://searchsecurity.techtarget.com/definition/cyberterrorism
[97] Michael A., " Cyber Probling : The Politicisation of Virtual Attack", Defence Academy of the United Kingdom, p.1 (http://www.conflictstudies.org.uk/files/Cyber_Probing.pdf)
[98] https://en.wikipedia.org/wiki/Computer_crime

άμεσα ή έμμεσα, με τη χρήση σύγχρονων δικτύων τηλεπικοινωνιών, όπως το Διαδίκτυο (chat rooms, e-mail) και τα κινητά τηλέφωνα (SMS / MMS) [99] .

Ένα παράδειγμα Κυβερνοεγκλήματος αποτελεί η περίπτωση του Gary McKinnon, από την Σκωτία, ο οποίος το 2002 κατηγορήθηκε ότι τέλεσε την μεγαλύτερη στρατιωτική κυβερνοεπίθεση όλων των εποχών. Ο ίδιος υποστήριξε πως έψαχνε για αποδείξεις ύπαρξης δραστηριοτήτων εξωγήνων (UFO) και άλλων τεχνολογιών χρήσιμων για την ανθρωπότητα[100]. Κατηγορήθηκε ότι «εισέβαλε» σε 97 στρατιωτικά υπολογιστικά συστήματα των Ηνωμένων Πολιτειών και της NASA από τον Φεβρουάριο του 2001 μέχρι τον Μάρτιο του 2002, στο σπίτι της θείας της φίλης του στο Λονδίνο χρησιμοποιώντας το όνομα «Solo». Σύμφωνα με τις αμερικανικές αρχές διεγράφησαν κρίσιμα αρχεία από τα λειτουργικά συστήματα, με αποτέλεσμα στην περιοχή της Ουάσιγκτον να τεθούν εκτός δικτύου για 24 ώρες 2.000 υπολογιστές που χρησιμοποιούνταν από τα στελέχη των Ενόπλων Δυνάμεων της συγκεκριμένης περιοχής. Ο McKinnon κατηγορήθηκε εσης για αντιγραφή δεδομένων, λογαριασμών και κωδικών πρόσβασης σε δικό του υπολογιστή. Σύμφωνα με εκτίμηση των αμερικανικών αρχών το κόστος της παρακολούθησης και τη διόρθωσης των προβλημάτων που προκάλεσε ήταν πάνω από 700.000 δολλάρια [101] .

δ) Κυβερνοακτιβισμός (Cyber Hactivism)

Ο όρος αυτός περιλαμβάνει κάθε δραστηριότητα που γίνεται στο πεδίο του Κυβερνοχώρου με στόχο την καταστροφή ιστοσελίδων , την πρόκληση βλάβης σε δίκτυα υποκινούμενη από πολιτικά κυρίως αλλά και οικονομικά κίνητρα . Η λέξη Hacktivism είναι μια αμφιλεγόμενη έννοια με πολλές σημασίες. Ως όρος επινοήθηκε το 1994 από την οργάνωση Cult of the Dead Cow Cult γνωστή και

[99] https://en.wikipedia.org/wiki/Computer_crime
[100] https://en.wikipedia.org/wiki/Gary_McKinnon
[101] http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm

ως CDC[102] . Η πιο γνωστή περίπτωση διαδικτυακών ακτιβιστών είναι οι επονομαζόμενοι « Anonymous» . Πρόκειται στην ουσία για μια ομάδα που ιδρύθηκε το 2003 και έγινε γνωστή εξαιτίας μιας πληθώρας επιδείξεων δημοσιότητας και επιθέσεων «άρνησης υπηρεσιών» που διενήργησαν κατά κυβερνήσεων , θρησκευτικών και εταιρικών ιστοσελίδων . Στο πρώιμο στάδιο της ξεκίνησε ως μια online community (εικονική κοινότητα) [103] που ενεργούσαν ανώνυμα και συντονισμένα έχοντας όμως αντισυμβατικές έως και αναρχικές αντιλήψεις. Στόχος της ομάδας αυτής έχουν αποτελέσει κυβερνητικές υπηρεσίες των ΗΠΑ, του Ισραήλ , της Τυνησίας, της Ουγκάντας, ιστοσελίδες παιδικής πορνογραφίας, οργανισμοί προστασίας των πνευματικών δικαιωμάτων, και εταιρείες όπως η PayPal, η MasterCard, η Visa και η Sony[104]. Τα μέλη της ομάδας διακρίνονται εύκολα μέσα στο κοινό εξαιτίας των μασκών Guy Fawkes που φορούν[105] . Ακολουθεί χαρακτηριστική είκονα με την συγκεκριμένη μάσκα.

Η κατηγοριοποίηση των Κυβερνοεπιθέσεων κρίνεται επιβεβλημένη, διότι ανάλογα με τα αποτελέσματα που επιφέρουν στο θύμα μπορούν να

[102]Η οργάνωση αυτή ιδρύθηκε το το 1984 στο Lubbock,στο Τέξας (https://en.wikipedia.org/wiki/Cult_of_the_Dead_Cow)

[103] Πρόκειται για κοινότητα της οποίας τα μέλη αλληλεπιδρούν μεταξύ τους κυρίως μέσω του Διαδικτύου (https://en.wikipedia.org/wiki/Online_community)

[104] https://en.wikipedia.org/wiki/Anonymous_(group)

[105] https://en.wikipedia.org/wiki/Guy_Fawkes_mask

αντιμετωπισθούν και από πλευρά διεθνούς δικαίου. Ανάλογα με την βαρύτητα της κάθε πράξης, αυτή μπορεί να αντιμετωπιστεί είτε σε εθνικό επίπεδο με την εφαρμογή της νομοθεσίας του κάθε κράτους είτε σε υπερεθνικό με την εφαρμογή άλλων νομικών κειμένων όπως την Ευρωπαϊκή Σύμβαση για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο από το Συμβούλιο της Ευρώπης [106], δίκαιο της χρήσης βίας , το δίκαιο του πολέμου με τις τρεις Συνθήκες της Γενεύης του 1949 και τα δύο Πρόσθετα Πρωτόκολλα 1977. Όταν διακινδυνεύεται όχι μόνο η εθνική αλλά και η διεθνής ασφάλεια και ειρήνη τότε πρέπει να ληφθούν τα αναγκαία μέτρα και να υπάρξει διεθνής συνεργασία σε διεθνές επίπεδο για την άμεση καταστολή των κυβερνοεπιθέσεων. Επίσης στην εργασία μελετάμε όλες τις κυβερνοεπιθέσεις ανεξάρτητα αν αυτές τελούνται από κρατικούς φορείς ή από μη κρατικούς δρώντες όπως για παράδειγμα τρομοκρατικές οργανώσεις ή μεμονωμένους hackers, οι οποίοι δρουν για προσωπικό όφελος (οικονομικά, πολιτικά κίνητρα).

1.3 "Όπλα " – Τεχνικές Κυβερνοεπιθέσεων

Τα πιο γνωστά όπλα σε μια επίθεση που μπορούν να χρησιμοποιηθούν είτε μεμονωμένα είτε συνδυαστικά μεταξύ τους είναι τα εξής:

1.3.1. Κακόβουλο Λογισμικό (malicious software / malware software) , στην ουσία πρόκειται για προγράμματα ή μακροεντολές που έχουν σχεδιαστεί για να διαγράψουν, να καταστρέψουν, να τροποποιήσουν, να μετατρέψουν αρχεία και πληροφορίες, προκαλώντας προβλήματα σε έναν υπολογιστή ή δίκτυο, διαταράσσοντας εν μέρει ή ολικώς την ομαλή του λειτουργία και αδυνατώντας τον να εκτελέσει τις λειτουργίες για τις οποίες κατασκευάστηκε αρχικά. Το κακόβουλο λογισμικό έχει την ικανότητα να δημιουργήσει « εισόδους», μέσω των οποίων κάποιος μπορεί να αναλάβει τον έλεγχο ενός υπολογιστή ή ενός δικτύου χωρίς να γίνει αυτό αντιληπτό από τον αρχικό του κάτοχο. Ο χαρακτηρισμός «κακόβουλο» αναφέρεται στην πρόθεση του δημιουργού του

[106] Λέγεται και Συνθήκη της Βουδαπέστης διότι υπογράφτηκε στην Βουδαπέστη στις 23 Νοεμβρίου του 2001 από 26 χώρες κράτη – μέλη του Συμβουλίου της Ευρώπης

λογισμικού, όταν δηλαδή βάσει των προθέσεων του ανωτέρω, το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα [107]. Η επίθεση με κακόβουλο λογισμικό μπορεί είτε άμεσα να αχρηστεύσει και να θέσει εκτός λειτουργίας έναν ηλεκρονικό υπολογιστή είτε μετά την παρέλευση ενός χρονικού διαστήματος από την στιγμή της αρχικής εγκατάστασης του κακόβουλου λογισμικού στον ηλεκρονικό υπολογιστή είτε αυτοματοποιημένα με τη διαβίβαση εντολής εκ του μακρόθεν. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες: Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες:σε αυτό που χρειάζεται ένα πρόγραμμα «ξενιστή» και σε αυτό που δεν χρειάζεται «ξενιστή» και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Επίσης μια άλλη διάκριση του κακόβουλου λογισμικού είναι σε ιομορφικό και μη ιομορφικό λογισμικό. Στην πρώτη κατηγορία ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους ενώ στην δεύτερη αυτά που δεν μπορούν να αναπαραχθούν χωρίς την ανθρώπινη επέμβαση [108]

Τα πιο γνωστά είδη κακόβουλου λογισμικού είναι οι ιοί (virus) , οι δούρειοι ίπποι (Trojan Horses) και τα ηλεκτρονικά σκουλήκια (Worms).

α) Ιός [109], πρόκειται για τμήμα του λογισμικού, στην πραγματικότητα για ένα πρόγραμμα το οποίο προσκολλάται σε άλλα προγράμματα ή αρχεία και μεταδίδεται από έναν ηλεκτρονικό υπολογιστή ή ένα δίκτυο σε ένα άλλο δημιουργώντας αντίγραφα του εαυτού του. Ενσωματώνει στην ουσία τον κώδικα του σε ένα πρόγραμμα ξενιστή. Στην απλούστερη μορφή τους επικαλύπτουν το αρχικό τμήμα του προγράμματος με τον δικό τους κώδικα ενώ στην πιο εξελιγμένη μορφή τους επισυνάπτουν δικό τους κώδικα στο τέλος του αρχείου με τις κατάλληλες εντολές σύνδεσης. Ο ιός έχει επίσης την δυνατότητα να εξαπλώνεται με μεγάλη ταχύτητα σε προγράμματα ξένου υπολογιστή χωρίς να γίνεται αντιληπτός. Αυτό οφείλεται στις τεχνικές απόκρυψεις που διαθέτει.

---

[107].https://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

[108] Karen P. , Kent K. and Nusbaum J. , “Guide to Malware Incident Prevention and Handling” , NIST, 2005 , p.121, available at (http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf)

[109] Ανήκει στην κατηγορία του ιομορφικού λογισμικού

Έχει την δυνατότητα απόκρυψης από λογισμικό προστασίας, ανιχνεύει διαδικασίες συστήματος δίνοντας λανθασμένες απαντήσεις με σκοπό την παραπλάνηση του χρήστη. Η μετάδοση του μπορεί να επιταχυνθεί με την βοήθεια κάποιας εξωτερικής συσκευής όπως μιας φορητή μνήμη USB ή ενός εξωτερικού σκληρού δίσκου. Τα αποτελέσματα ενός ιού μπορεί να είναι απλά η διαγραφή ορισμένων αρχείων και η τροποποίηση δεδομένων μέχρι όμως και η πλήρης διακοπή της λειτουργίας του υπολογιστικού συστήματος το οποίο έχει μολυνθεί από αυτόν.

Η ειδοποιός διαφορά ενός ιού συγκριτικά με τα υπόλοιπα προγράμματα είναι πως ο πρώτος μπορεί να μεταδοθεί οπουδήποτε έχει τη δυνατότητα. Εν κατακλείδι τα χαρακτηριστικά ενός ιού είναι τα ακόλουθα: α) η αναγνωρισιμότητα, η ικανότητα να γνωρίζει τον εαυτό του, β) η αναπαραγωγή, η ικανότητα να αντιγράφει τον ευατό του, γ) απόκρυψη, υπάρχουν ορισμένοι μέθοδοι που χρησιμοποιεί για να αποκρύψει την παρουσία του από τον χρήστη και τα αντιβιοτικά. Γενικά ο κύκλος ζωής του ιομορφικού λογισμικού στο οποίο ανήκει και ο ιός , έχει τις εξής φάσεις : α) την φάση επώασης στην οποία ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα και ενεργοποιείται από κάποιο γεγονός (π.χ. την παρουσία κάποιου αρχείου), β) την φάση αναπαραγωγής στην οποία πραγματοποιείται η δημιουργία αντιγράφων και ενδεχόμενη ενσωμάτωση σε ξενιστές και γ) την φάση ενεργοποίησης και εκτέλεσης , όπου εκτελείται μια σειρά ενεργειών (payload) με επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που «φιλοξενεί» το ιομορφικό λογισμικό. Ενδεικτικά θα αναφέρουμε διάφορα είδη ιών : παρασιτικοί, πολυμερείς, διαμένοντες στην κύρια μνήμη, κρυφοί, κρυπτογραφημένοι, πολυμορφικοί, ρετρό ιοί, μακρο- ιοί και ιοί που διαγράφουν τμήμα του ξενιστή [110]. Να τονίσουμε τέλος ότι ο ιός μπορεί να επιτίθεται , μπορεί και όχι. Σε κάθε περίπτωση όμως καταναλώνει πόρους του συστήματος που έχει μολύνει.

β) Δούρειος Ίππος (Trojan) , πρόκειται για ένα φαινομενικά χρήσιμο και μη βλαβερό πρόγραμμα το οποίο περιλαμβάνει κρυφές λειτουργίες οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα και να θέσουν σε κίνδυνο την ασφάλεια του υπολογιστικού

[110] http://www.ct.aegean.gr/people/kalloniatis/Security/Malicious_Software.pdf

συστήματος. Ανήκει στην κατηγορία του μη ιομορφικού λογισμικού. Το πρόγραμμα αυτό περιέχει μη εμφανή κακόβουλο λογισμικό, με αποτελέσμα ο χρήστης του να παραπλανάται θεωρώντας ότι χρησιμοποιεί ένα αβλαβές πρόγραμμα και ότι θα επέλθει το αποτέλεσμα που αποζητά, ενώ στην πραγματικότητα το ζημιογόνο αυτό λογισμικό μπορεί να οδηγήσει σε διαγραφή δεδομένων ακόμη και στην δημιουργία ηλεκτρονικών «κερκόπορτων»[111] στο σύστημα. Στόχος των δημιουργών αυτού του προγράμματος είναι κυρίως να αποκτήσουν τον πλήρη έλεγχο του συστήματος. Σε αντίθεση με τους ιούς και τα ηλεκτρονικά σκουλήκια που επιδιώκουν να μολύνουν ένα υπολογιστικό σύστημα, ο Δούρειος Ιππος δεν αναπαράγεται[112].

γ) «Ηλεκτρονικό «Σκουλήκι**»** (Worm) [113], πρόκειται για πρόγραμμα το οποίο διαδίδεται άμεσα με την βοήθεια κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα[114] ή το ηλεκτρονικό ταχυδρομείο (e- mail). Σε αντίθεση με τον ιό το «σκουλήκι» λειτουργεί χωρίς την ανθρώπινη επέμβαση ή να χρειαστεί να «τρέξει» προηγουμένως κάποιο πρόγραμμα. Το πιο ανησυχητικό αυτού του προγράμματος είναι το γεγονός ότι έχει την ικανότητα να αναπαράγεται αυτόματα μέσα στον υπολογιστή στον οποίο βρίσκεται έχοντας έτσι την δυνατότητα να αποστέλλει προσωπικά δεδομένα ή οποιαδήποτε πληροφορία στον δημιουργό του λογισμικού αυτού αποκτώντας έτσι ο τελευταίος τον πλήρη έλεγχο. Όλη αυτή η διαδικασία που ακολουθεί το «σκουλήκι» έχει ως αποτέλεσμα ένα μεγάλο μέρος της διαθέσιμης μνήμης να καταναλώνεται άσκοπα και να επιβαρύνεται έτσι το δίκτυο με «άχρηστες» πληροφορίες και δεδομένα καθιστώντας το λιγότερο λειτουργικό ως προς τους χρήστες του [115]. Το ηλεκτρονικό «σκουλήκι» εμφανίστηκε για πρώτη φορά στις 02 Νοεμβρίου

[111] Πρόκειται για σημεία εισόδου που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας τη συνηθισμένη διαδικασία ελέγχου πρόσβασης

[112] https://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

[113] Ο όρος αυτός εδώ χρησιμοποιείται από την φράση « Write Once Read Many”

[114] Το τοπικό δίκτυο (local area network) είναι ένα σύνολο συνδεδεμένων υπολογιστών που εκτείνονται σε περιορισμένη γεωγραφική περιοχή

[115] https://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

του 1988 στο MIT[116] από τον φοιτητή Robert Tappan Morris του Πανεπιστημίου Cornell [117], ο οποίος δήλωσε ότι το επινόησε για να υπολογίσει την χωρητικότητα και το μέγεθος του Διαδικτύου [118]

1.3.2. Η επόμενη τεχνική των Κυβερνοεπιθεσέων αποτελεί η άρνηση υπηρεσιών (Denial of Sevice (DoS) , η οποία έχει σκοπό όχι να καταστρέψει τον στόχο- δίκτυο αλλά να το υπερφορτώσει, ώστε να αδυνατεί να εξυπηρετήσει τους νόμιμους και εξουσιοδοτημένους χρήστες του, μη έχοντας οι τελευταίοι άμεση πρόσβαση σε πηγές πληροφοριών και δεδομένα, καθιστώντας το αναπόφευκτα αναξιόπιστο για ορισμένη χρονική περίοδο. Αυτό επιτυγχάνεται στην πράξη με την αποστολή σε πολύ σύντομο χρονικό διάστημα σχεδόν ταυτόχρονα, μεγάλου αριθμού αιτημάτων παροχής υπηρεσιών, όπως για παράδειγμα το να «διαβάζουν» μια ιστοσελίδα ταυτόχρονα εκατομμύρια χρήστες. Είναι προφανές ότι ο «βομβαρδισμός» ενός δικτύου με τόσα αιτήματα την ίδια στιγμή οδηγεί τον υπολογιστή σε αδυναμία εκτέλεσης του προγράμματος που του έχει ανατεθεί και ανάλογα με τον όγκο των αιτημάτων που δέχεται μπορεί να τεθεί και εκτός λειτουργίας [119]. Για παράδειγμα όταν πληκτρολογούμε μια διεύθυνση URL στο πρόγραμμα πλοήγησης μας, ουσιαστικά στέλνουμε ένα αίτημα στον server του υπολογιστή αυτής της τοποθεσίας για να εμφανιστεί η ζητούμενη ιστοσελίδα. Ο διακομιστής μπορεί να επεξεργαστεί μόνο έναν συγκεκριμένο αριθμό αιτημάτων ταυτόχρονα , οπότε αν ένας εισβολέας επιβαρύνει τον server με αιτήματα, δεν μπορεί να επεξεργαστεί το δικό μας αίτημά. Αυτή είναι μια "άρνηση υπηρεσίας" εφόσον δεν μπορούμε να αποκτήσουμε πρόσβαση στην ιστοσελία που ζητήσαμε .

Μια άλλη περίπτωση άρνησης υπηρεσιών είναι όταν ένας εισβολέας χρησιμοποιεί μηνύματα spam email για να επιχειρήσει παρόμοια επίθεση στο προσωπικό μας email. Σε κάθε email έχει δοθεί συγκεκριμένη ποσόστωση, η οποία περιορίζει την ποσότητα των δεδομένων που μπορούμε να έχουμε στο

[116] Massachusetts Institute of Technology (Τεχνολογικό Ινστιτούτο της Μασαχουσέτης)
[117] http://www.loundy.com/CASES/US_v_Morris2.html
[118] http://www.nato.int/docu/review/2013/Cyber/timeline/GR/index.htm
[119] https://www.cert.org/information-for/denial_of_service.cfm?

λογαριασμό μας μια δεδομένη χρονική στιγμή. Αν μας αποσταλούν ταυτόχρονα πολλά και υψηλής χωρητικότητας μηνύματα στον λογαριασμό μα , τότε λόγω της ποσόστωσης, δεν θα μπορούμε να λαμβάνουμε άλλα χρήσιμα μηνύματα [120]. Οι επιθέσεις άρνησης υπηρεσιών είναι από την φύση τους δύσκολο να ανιχνευθούν, διότι λόγω της συνεχώς μεταβαλλόμενης φύσεως του Διαδικτύου , οι εισβολείς χρησιμοποιούν παραποιημένες διευθύνσεις πηγής IP, έτσι ώστε να κρύψουν την ταυτότητα τους. Επιπλέον η δυσκολία αντιμετώπισης τους οφείλεται στο γεγονός ότι ο μεγάλος ρυθμός πακέτων που χρησιμοποιούνται για τη διεξαγωγή τους απαιτεί αρκετούς πόρους. Από την άλλη πλευρά, τα σύγχρονα υπολογιστικά συστήματα διαθέτουν περιορισμένους πόρους οι οποίοι δεν επαρκούν για τον εντοπισμό των συγκεκριμένων επιθέσεων.

1.3.3. Κατανεμημένη Άρνηση Υπηρεσιών (Distributed denial of service- DDOS)

Μια πιο εξελιγμένη μορφή της άρνησης υπηρεσιών αποτελεί η Κατανεμημένη Άρνηση Υπηρεσιών στην οποία χρησιμοποιούνται εκατομμύρια μολυσμένοι υπολογιστές, οι οποίοι χαρακτηρίζονται ως «zombies» [121] και επιτίθενται ταυτόχρονα σε ένα δίκτυο. Με την τεχνική αυτή καθίσταται εξαιρετικά δυσχερής η αναστολή μιας τέτοια επίθεσης, εφόσον υπάρχουν πολλές συντονισμένες πηγές οι οποίες «βομβαρδίζουν» τον στόχο, καλύπτωντας με αυτό τον τρόπο την πηγή συντονισμού της επίθεσης[122]. Ο αρχικά επιτιθέμενος ορίζει κάποιους υπολογιστές ως εκπαιδευτές για να ελέγξουν τους ενδιάμεσους υπολογιστές – πράκτορες ώστε να επιτεθούν τον στόχο – δίκτυο. Συνοπτικά μια επίθεση DDOS αποτελείται από τέσσερα στοιχεία: α) τον επιτιθέμενο, β) τους handles, πρόκειται για κόμβους που έχουν παραβιαστεί από τον επιτιθέμενο, γ) τους επιτιθέμενους - πράκτορες , στους οποίους «τρέχει» ένα πρόγραμμα και έχουν αναλάβει την παραγωγή μιας ροής πακέτων, δ) ο στόχος- δίκτυο. Ο εντοπισμός των διευθύνσεων IP (Internet Protocol Address) που χρησιμοποιούνται είναι σχεδόν ανέφικτος, εφόσον η επίθεση πραγματοποιείται από διαφορετικές τοποθεσίες και πηγές (υπολογιστές). Οι επιθέσεις αυτές, όπως γίνεται

[120] https://www.us-cert.gov/ncas/tips/ST04-015
[121] https://el.wikipedia.org/wiki/%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82_zombie
[122] http://www.icir.org/vern/papers/reflectors.CCR.01/node1.html

αντιληπτό είναι πολύ πιο αποτελεσματικές από τις απλές DOS επιθέσεις και λόγω των χαρακτηριστικών που διαθέτουν καθίστανται ιδιαίτερα επικίνδυνες. Τα συστήματα που αποτελούν τους πιο συχνούς στόχους είναι συνήθως συστήματα πανεπιστημιακών ιδρυμάτων ή οργανισμών παροχής δωρεάν πρόσβασης στο Διαδίκτυο.

Ορισμένα παραδείγματα τέτοιων επιθέσεων είναι [123] :

- Οι επιθέσεις που έγιναν σε μεγάλες εταιρείες όπως (eBay, Amazon.com, Yahoo, Bye.com, CNN) στις αρχές του 2000 με αποτέλεσμα να τεθούν εκτός λειτουργίας για ορισμένο χρονικό διάστημα. Οι συγκεκριμένες επιθέσεις αντιμετωπίστηκαν ως «έκτακτη κατάσταση» .

- Ο Βρετανικός παροχέας υπηρεσιών Cloud Nine τον Ιανουάριο του 2002 αναγκάστηκε να διακόψει την επιχειρηματική του δραστηριότητα

- Η απόπειρα επίθεσης εναντίον των Root Name Servers[124], η οποία απέτυχε λόγω υπερπάρκειας πόρων .

Τέλος η US –CERT (The United States Computer Emergency Readiness Team), η ομάδα ετοιμότητας και έκτακτης ανάγκης των ΗΠΑ , αναφέρει ορισμένα από τα συμπτώματα που μπορεί να παρουσιάσει ο υπολογιστής σε περίπτωση μιας επίθεσης DDOS : α) Η υπερβολικά αργή απόδοση του δικτύου, β) η αδυναμία πρόσβασης σε ορισμένες ιστοσελίδες, γ) μεγάλος αριθμός ληφθέντων spam – email στον προσωπικό μας λογαριασμό [125].

1.3.4 Λογικές Βόμβες (Logic Bombs)

[123] http://library.tee.gr/digital/m2142/m2142_koutepas.pdf
[124] Εξυπηρετητές Πυρήνα Ονομάτων (https://www.netnod.se/what-are-root-name-servers)
[125] https://www.us-cert.gov/ncas/tips/ST04-015

Πρόκειται για κώδικα κακόβουλου λογισμικού [126], το οποίο εισχωρεί σε ένα υπολογιστικό σύστημα και μπορεί να παραμείνει αδρανής μέχρι να πληρωθούν ορισμένες προϋποθέσει . Στην ουσία πρόκειται για προγράμματα τα οποία ενεργοποιούνται όταν πραγματοποιηθεί μια λογική συνθήκη (πχ όταν το όνομα του προγραμματιστή δε βρίσκεται στη μισθοδοσία της επιχείρησης) ή με την παρέλευση μιας προθεσμίας. Μόλις πληρωθεί η αίρεση που έχει τεθεί, το λογισμικό ξεκινά την δράση του διαγράφοντας αρχεία και δεδομένα ή ξεκινώντας μια επίθεση DOS ή DDOS [127].

1.3.5 IP Address spoofing (Παραπλάνηση)

Με την τεχνική αυτή δημιουργούνται πακέτα IP[128] με ψεύτικη διεύθυνση προέλευσης έτσι ώστε να μην αποκαλυφθεί η ταυτότητα του αποστολέα. Η επικεφαλίδα κάθε πακέτου IP διαθέτει εκτός από την αριθμητική προέλευση και τον προορισμό της διεύθυνσης του πακέτου. Ο επιτιθέμενος με την τεχνική αυτή μπορεί να τροποποιήσει την επικεφαλίδα ώστε το πακέτο να φαίνεται ότι εστάλη από διαφορετική διεύθυνση πηγής. Το IP spoofing χρησιμοποιείται σε denial-of-service επιθέσεις. Ο επιτιθέμενος παρουσιάζεται ως διαχειριστής διαφόρων νόμιμων και ακίνδυνων φαινομενικά ιστοσελίδων, παραπλανώντας έτσι τον χρήστη ενός υπολογιστή να επιλέξει μια συγκεκριμένη νόμιμη ,όπως νομίζει, σελίδα οδηγούμενος τελικά σε μια ιστοσελίδα παραποιημένη .η οποία δεν είναι τόσο ακίνδυνη. δίνοντας ίσως και προσωπικά του στοιχεία με ότι συνέπειες κάτι τέτοιο μπορεί να επιφέρει.

Για τα μέσα και τις μεθόδους που χρησιμοποιούνται κατά την διάρκεια των επιχειρήσεων στον Κυβερνοχώρο γίνεται ενδελεχής αναφορά στα **άρθρα 41-48** του Εγχειριδίου του Ταλίν. Συγκεριμένα στο άρθρο 41 γίνεται διάκριση μεταξύ

[126] Λέγεται αλλιώς και " slug code" (http://searchsecurity.techtarget.com/definition/logic-bomb)
[127] https://en.wikipedia.org/wiki/Logic_bomb
[128] Το Πρωτόκολλο Διαδικτύου (Internet Protocol Address) αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση πακέτων δεδομένων στο διαδίκτυο. Έχει ως αποστολή την παροχή δεδομένων από την πηγή υποδοχής τους στον τελικό προορισμό τους (https://en.wikipedia.org/wiki/Internet_Protocol)

των «όπλων» και των «μεθόδων» του Κυβερνοπολέμου. Ως μέσα νοούνται τα όπλα που χρησιμοποιούνται στις κυβερνοεπιθέσεις και τα υπολογιστικά συστήματα που συνδέονται με αυτά[129]. Από την άλλη πλευρά ως μέθοδοι του Κυβερνοπολέμου ορίζονται όλες οι τεχνικές, οι τακτικές και οι διαδικασίες με τις οποίες διεξάγονται οι επιθέσεις στον Κυβερνοχώρο . Οι δύο παραπάνω όροι είναι νομικοί και χρησιμοποιούνται και στο Δίκαιο των Ενόπλων Συρράξεων .Δεν θα πρέπει να συγχέονται με τον όρο «επιχειρήσεις στον Κυβερνοχώρο», ο οποίος δεν είναι νομικός αλλά αναφέρεται πολύ συχνά στο Εγχειριδίο του Ταλίν και υποδηλώνει μια δραστηριότητα στον Κυβερνοχώρο.

Οι δύο αυτοί όροι «μέσα¨και «μεθοδοι» ισχύουν τόσο στις διεθνείς όσο και σε μη διεθνείς ένοπλες συγκρούσεις. Για τους σκοπούς του παρόντος εγχειριδίου, τα όπλα του κυβερνοχώρου είναι τα μέσα που χρησιμοποιούνται, τα οποία είναι από το σχεδιασμό τους, τη χρήση ή τον επιδιώκομενο σκοπό τους ικανά να προκαλέσουν τραυματισμό ή θάνατο σε ανθρώπους και βλάβη ή καταστροφή σε αντικείμεν, επιφέροντας τις ίδιες συνέπειες που απαιτούνται για τον χαρακτηρισμό μιας πράξης στον κυβερνοχώρο ως επίθεση όπως αναφέρεται και στο άρθρο 30 του Εγχειριδίου. Ο όρος «μέσα» Κυβερνοπολέμου περιλαμβάνει τόσα τα όπλα που χρησιμοποιούνται όσο και τα οπλικά συστήματα . Το όπλο σαν έννοια γίνεται αντιληπτό ως μια πτυχή συστήματος που χρησιμοποιείται για να προκαλέσει βλάβη ή καταστροφή σε αντικείμενα ή τραυματισμό ή θάνατο σε ανθρώπους. Ως εκ τούτου, ο όρος «μέσα» Κυβερνοπολέμου περιλαμβάνει οποιαδήποτε συσκευή στον κυβερνοχώρο, εργαλείο, μηχανισμό, εξοπλισμό ή λογισμικό που χρησιμοποιείται και είναι σχεδιασμένα ή προορίζονται να χρησιμοποιηθούν για τη διεξαγωγή μιας κυβερνοεπίθεσης. Ο όρος «μεθοδοι» Κυβερνοπολέμου αναφέρεται στον τρόπο με τον οποίο οι επιχειρήσεις στον Κυβερνοχώρο έχουν ταξινομηθεί διακριτά από τα μέσα τα οποία χρησιμοποιούνται για την διεξαγωγή τους[130]. Ο όρος «οι τεχνικές, τακτικές και διαδικασίες» με τις οποίες διεξάγονται οι εχθροπραξίες, δεν περιλαμβάνει τις δραστηριότητες εκείνες στον Κυβερνοχώρο, οι οποίες περιλαμβάνουν επικοινωνίες μεταξύ φιλικών δυνάμεων. Από την άλλη πλευρά,

[129] «'means of cyber warfare' are cyber weapons and their associated cyber systems»
[130] The term "methods of warfare" refers to how cyber operations are mounted, as distinct from the instruments used to conduct them.

υπάρχει η πρόθεση να υποδηλώσει περισσότερες από εκείνες τις επιχειρήσεις οι οποίες δύνανται να θεωρηθούν ως επίθεση , όπως αναφέρεται και στο άρθρο 30 του Εγχειριδίου. Για παράδειγμα ένα ιδιαίτερο είδος επιχείρησης στον Κυβερνοχώρο που είναι σχεδιασμένη να επέμβει στην ικανότητα επικοινωνίας του εχθρού μπορεί να μην θεωρηθεί επίθεση με την έννοια που προβλέπει το άρθρο 30 του Εγχειριδίου του Ταλίν, αλλά σίγουρα θα αποτελούσε «μεθοδο» Κυβενροπολέμου. Το άρθρο 42 θέτει έναν περιορισμό στην χρήση των μέσων και των μεθόδων απαγορεύοντας να χρησιμοποιούνται μέσα ή μέθοδοι που από την φύση τους προκαλούν άσκοπο και υπερβολικό πόνο[131]. Με την διατύπωση αυτή θέλει το Εγχειρίδιο να αποτρέψει τις περιπτώσεις εκείνες όπου ένα όπλο ή μια ιδιαίτερη χρήση ενός όπλου επιδεινώνει τον πόνο χωρίς να προσφέρει κάποιο περεταίρω στρατιωτικό πλεονέκτημα στον δράστη. Η φράση «εκ φύσεως» επιβεβαιώνει ότι ένα μέσο ή μια μέθοδος Κυβερνοπολέμου παραβίαζει το άρθρο αυτό εάν προκαλέσει αναγκαστικά άσκοπο και υπερβολικό πόνο, ανεξάρτητα από το εάν ήταν σχεδιασμένο να το κάνει. Επίσης παραβίαση του κανόνα υπάρχει, όταν ένα μέσο ή μεθοδος είναι σχεδιασμένο ώστε άσκοπα και χωρίς να υπάρχει ανάγκη να επιδεινώνει τον πόνο.

Ένας ακόμη περιορισμός που τίθεται στο άρθρο 43 είναι η απογόρευση μέσων και μεθόδων τα οποίο είναι από την φύση τους δυσδιάκριτα. Αυτό συμβαίνει πρώτον, όταν αυτά δεν μπορούν να στραφούν σε ένα συγκεκριμένο στρατιωτικό στόχο και δεύτερον όταν περιορίζονται στα αποτελέσματα τους, διότι το επιτάσσει το Δίκαιο των Ενόπλων Συρράξεων και κατά συνέπεια από την φύση τους στρέφονται κατά στρατιωτικών και αστικών στόχων χωρίς διάκριση. Επίσης απαγορεύεται σύμφωνα με το άρθρο 45 η λιμοκτονία των πολιτών- αμάχων ως μέθοδος Κυβερνοπολέμου. Το άρθρο 47 ορίζει ότι σύμφωνα με το Πρόσθετο Πρωτόκολλο Ι απαγορέυεται τα συμβαλλόμενα μέρη να μετατρέπουν τον άμαχο πληθυσμό, τα πολιτιστικά αντικείμενα, τους τόπους λατρείας , τα αντικείμενα που είναι απαραίτητα για την επιβίωση του άμαχου πληθυσμού, το φυσικό περιβάλλον τα φράγματα , τα αναχώματα και τους σταθμούς παραγωγής ηλεκτρικής ενέργειας. Τέλος το άρθρο 48 αναφέρεται

[131] «It is prohibited to employ means or methods of cyber warfare that are of a nature to cause superfluous injury or unnecessary suffering»

στην υποχρέωση που έχουν όλα τα κράτη να εξασφαλίζουν τα μέσα Κυβερνοπολέμου που αποκτούν ή χρησιμοποιούν, να συμμορώνονται με τους κανόνες του ΔΑΔ, οι οποίοι δεσμεύουν το κάθε κράτος. Επιπλέον όλα τα κράτη που έχουν υπογράψει το Πρόσθετο Πρωτόκολλο Ι υποχρεούνταισε περίπτωση μελέτης ή υιοθέτησης ενός νέου μέσου ή μεθόδου πρέπει να λάβουν υπόψη τους εάν αυτά σε ορισμένες ή όλες τις περιπτώσεις θα παραβίαζαν το Πρόσθετο Πρωτόκολλο ή οποιοδήποτε άλλο κανόνα του Διεθνούς Δικαίου.

1.4 Στόχοι των Κυβερνοεπιθέσεων

Οι κυριότεροι στόχοι των Κυβερνοεπιθέσεων είναι οι βασικές κρατικές υποδομές. Με τον όρο βασικές αυτό αναφερόμαστε στις υποδομές εκείνες που αν αποτελέσουν στόχο και πληγούν, τότε διακυβεύεται η εθνική ασφάλεια ενός κράτους, αποσταθεροποιείται η οικονομία του και πιθανόν αυτό να οδηγηθεί σε αναπτυξιακό τέλμα. Οι στόχοι αυτοί, η προσβολή των οποίων επιφέρει αποφασιστικό αποτέλεσμα στην τελική έκβαση μιας σύγκρουσης, σχετίζονται με τις κρίσιμες υποδομές του κράτους που αποτελεί τον στόχο, στο μέτρο που αυτές είναι προσβάσιμες στους δράστες των Κυβερνοεπιθέσεων. Έτσι στο σύχρονο «ηλεκτρονικό» κόσμο, η προσβολή των κρίσιμων υποδομών μπορεί να παραλύσει ένα κράτος, χωρίς να είναι απαραίτητη η φυσική καταστροφή τους. Ενδιαφέρον παρουσιάζουν οι κρίσιμες υποδομές που συνδέονται με το διαδίκτυο με την βοήθεια των Συστημάτων Βιομηχανικού Ελέγχου ICS [132] (Industrial Control Systems), λόγω της εύκολης πρόσβασης τους. Αρχικά τα συστήματα ICS ήταν απομονωμένα από τα δίκτυα υπολογιστών, χρησιμοποιώντας δικά τους πρωτόκολλα για να επικοινωνήσουν με τον κεντρικό υπολογιστή. Το χαμηλό κόστος των συσκευών με ενσωματωμένες διεπαφές με το πρωτόκολλο διαδικτύου (Internet Protocol – IP) δημιούργησε καινοτομίες στον Κυβερνοχώρο καθιστώντας και τα συστήματα ICS στόχους των κυβερνοεπιθέσεων.

[132] Ο όρος ICS είναι μια γενική έννοια η οποία περιλαμβάνει διάφορους τύπους συστημάτων ελέγχου, όπως το σύστημα Επίβλεψης, Ελέγχου και Συλλογής Δεδομένων SCADA (Supervision, Control and Data Acquisition) και το σύστημα Κατανεμημένου Ελέγχου DCS (Distributed Control Systems) καθώς και άλλα μικρότερα συστήματα ελέγχου

Για να αποκτηθεί μια εικόνα των κρίσιμων υποδομών μιας χώρας, απαιτείται προηγουμένως η χαρτογράφησή τους. Δεν είναι όμως κάθε υποδομή εκμεταλλεύσιμη ούτε δύναται να υποβαθμιστεί με τον ίδιο τρόπο. Η προσβολή της εξαρτάται άμεσα από τα διαθέσιμα μέσα και την καταλληλότητά τους. Να επισημάνουμε ότι μια υποδομή η οποία δεν στηρίζεται ούτε εξαρτάται από κάποιο υπολογιστικό σύστημα τότε δεν παρουσιάζει ενδιαφέρον από πλευράς Κυβερνοπολέμου. Η ιεράρχηση των κρίσιμων υποδομών του αντιπάλου είναι μια δυναμική διαδικασία, η οποία εξαρτάται κάθε φορά από την συνολική εκτίμηση της καταστάσης και την αντίστοιχη φάση στην οποία βρίσκεται η σύγκρουση.

Κρίσιμες υποδομές ενός κράτους αποτελούν όλες οι εγκαταστάσεις παραγωγής και μεταφοράς ηλεκτρικής ενέργειας, παραγωγής και διανομής πετρελαίου και φυσικού αερίου, παροχής νερού, η γεωργία, τα δίκτυα τηλεπικοινωνιών, η δημόσια υγεία (νοσοκομεία), οι χρηματοοικονομικές υπηρεσίες, τραπεζικά δίκτυα, το δίκτυο μαζικής μεταφοράς (αεροδρόμια, σιδηροδρομικοί σταθμοί), πυρηνικά εργοστάσια, δορυφορικά συστήματα, το ναυτιλιακό σύστημα [133].

1.5 Παραδείγματα Κυβερνοεπιθέσεων

1.5.1 Η περίπτωση της Εσθονίας

Το κύμα των κυβερνοεπιθέσεων που ξέσπασε στην Εσθονία την Άνοιξη του 2007 οφειλόταν στην πολιτικοκοινωνική κατάσταση που επικρατούσε την περίοδο εκείνη στην χώρα, μετατρέποντας την σε αποδέκτη της πιο εκτεταμένης ηλεκτροβικής προσβολής. Συγκεκριμένα, αφορμή αποτέλεσε το νομοσχέδιο [134] που ήθελε να ψηφίσει η Εσθονική Βουλή σύμφωνα με το οποίο θα καταστρεφόταν οποιοδήποτε μνημείο που θεωρούνταν κατάλοιπο της

[133] https://en.wikipedia.org/wiki/Critical_infrastructure

[134] Clarke R and Knake R .K, “Cyberwar ,” The Next Threat to National Security And What To do about it” , Harper Collins Publishers, New York, 2010, p.11-12

κατοχής της χώρας από την Σοβιετική Ένωση. Έτσι αποφασίστηκε από τις Εσθονικές Αρχές να απομακρύνουν το χάλκινο άγαλμα του «Στρατιώτη του Ταλίν» [135], από κεντρικό σημείο της πρωτεύουσας της Εσθονίας το Ταλίν, όπου είχε τοποθετηθεί από τους Σοβιετικούς μετά το τέλος του Β΄ Παγκοσμίου Πολέμου , ώστε να μεταφερθεί σε διεθνές στρατιωτικό κοιμητήριο. Απέναντι στην ενέργεια αυτή υπήρξε μεγάλη αντίδραση τόσο από την Ρωσική Κυβέρνηση που θεώρησαν ότι προσβάλλεται με αυτό τον τρόπο η μνήμη ρων νεκρών – αγωνιστών , όσο και από την ρωσικής μειονότητας που ζούσε στην Εσθονία. Οι αντιδράσεις αυτές εκδηλώθηκαν με πορείες και διαδηλώσεις στους δρόμους και επιθέσεις έξω από την πρεσβεία της Εσθονίας στην Μόσχα[136]. Παρά την τεταμένη κατάσταση που επικρατούσε, το μνημείο τελικά απομακρύνθηκε από την θέση του την 27 Απριλίου του 2007 κάτι που οδήγησε σε έντονες αντιδράσεις από τους Ρώσους. Η Εσθονία [137] για τρεις εβδομάδες έγινε στόχος κυβερνοεπιθέσεων. Οι κυβερνοεπιθέσεις στο μεγαλύτερο μέρος τους ήταν τύπου DOS και DDOS εναντίον ιστοσελίδων Εσθονικών οργανισμών, του εσθονικού Κοινοβουλίου, των Υπουργείων, των τραπεζών[138], των νοσοκομείων, των ραδιοφωνικών σταθμών, των πανεπιστημίων, των τηλεοπτικών σταθμών, των δικτύων των εφημερίδων, των μέσων ενημέρωσης. Ακόμη και το γραφείο του Πρωθυπουργού έγινε στόχος κυβερνοεπιθέσεων. Επίσης πολλές από τις εσθονικές ιστοσελίδες παραβιάσθηκαν, επήλθαν αλλαγές στο περιεχόμενο τους χωρίς άδεια ή εξουσιοδότηση[139],ενώ κάποιες άλλες αντικαταστάθηκαν από

[135] Κάτω από το άγαλμα αυτό φυλάσσονταν τα οστά των στρατιωτών του Κόκκινου Στρατού που σκοτώθηκαν πολεμώντας τους ναζί αγωνιζόμενοι για την απελευθέρωση της Εσθονίας . Το μνημείο αρχικά είχε την ονομασία «Μνημείο στους ελευθερωτές του Ταλίν».Το μνημείο παρουσιάστηκε στις 22 Σεπτεμβρίου 1947 τρία χρόνια αφού ο «Κόκκινος Στρατός» έφτασε στο Ταλίν στις 22 Σεπτεμβρίου του 1944 κατά τον Β 'Παγκοσμίο Πόλεμο (https://en.wikipedia.org/wiki/Red_Army)

[136] http://news.in.gr/world/article/?aid=802799

[137] Η χώρα αυτή ήταν μια από τις πιο δικτυωμένες χώρες της Ευρώπης και σε μεγάλο βαθμό εξαρτημένη από την τεχνολογία και το Διαδίκτυο. Ήδη από την δεκαετία του 1990 η λειτουργία των εσθονικών τραπεζών στηρίζονταν στις ηλεκτρονικές υπηρεσίες και σύμφωνα με στοιχεία που δημοσιοποιήθηκαν το μεγαλύτερο μέρος των τραπεζικών συναλλαγών περίπου το 90% αυτών, το 2007 γινόταν δικτυακά, όπως και η δήλωση και πληρωμή των φόρων.Ακόμη και οι βουλευτικές εκλογές διεξάγονταν δικτυακά (Shackelford Sc. J., “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, Berkeley Journal of International Law, Vol. 27:1, 2009, p.192)

[139].Πρόκειται για την λεγόμενη web defacement (https://en.wikipedia.org/wiki/Website_defacement). Μια περίπτωση web defacement ήταν όταν

άλλες μεταδίδοντας μηνύματα προπαγανδιστικά εις βάρος της Εσθονικής Κυβέρνησης. Μια από τις τεχνικές των κυβερνοεπιθέσεων που χρησιμοποιήθηκε ήταν και το email- spamming[140], η συνεχής αποστολή ανεπιθύμητων μηνυμάτων στο ηλεκτρονικό ταχυδρομείο .

Οι τόσο έντονες και παρατεταμένες κυβερνοεπιθέσεις αποτέλεσαν ανεπανόρθωτο πλήγμα για την Εσθονία τόσο σε οικονομικό όσο και πολιτικοκοινωνικό επίπεδο δεδομένης της κατάστασης της χώρας. Οι εσθονοί είχαν συνηθίσει να πραγματοποιούν το σύνολο των συναλλαγών τους διαδικτυακά [141] και οι υποδομές της χώρας δεν ήταν προετοιμασμένες για μια τέτοιου βαθμού επίθεση. Μια άρρηκτα συνδεδεμένη με την τεχνολογία και το Διαδίκτυο χώρα που «βάλλεται» σε αυτούς τον τομείς, είναι λογικό να οδηγηθεί σε οικονομική παράλυση και να τεθούν εκτός λειτουργίας πολλοί από τους κρατικούς και ιδωτικούς τομείς για μεγάλο χρονικό διάστημα.

Η Εσθονία μην έχοντας το κατάλληλο νομοθετικό πλαίσιο για την αντιμετώπιση τέτοιων επιθέσεων, ως χώρα-μέλος του ΝΑΤΟ ζήτησε την συνδρομή της Συμμαχίας και την άμεση επέμβαση των «συμμάχων»[142], επιζητώντας να θεωρηθούν οι κυβερνοεπιθέσεις που δέχτηκε ως «ένοπλη επίθεση», προκειμένου να εφαρμοσθεί το άρθρο 5 της Ιδρυτικής Συνθήκης του ΝΑΤΟ. Σε αυτό προβλέπεται η δέσμευση των κρατών- μελών της Συμμαχίας να θεωρήσουν οποιαδήποτε «Ένοπλη Επίθεση» διεξάγεται προς ένα κράτος-μέλος ως επίθεση εναντίον όλων των υπόλοιπων μελών του και να πράξουν ανάλογα. Στην πραγματικότητα το Άρθρο 5 είναι η νομική βάση εμπλοκής του ΝΑΤΟ σε ένοπλες συγκρούσεις[143]. Σχετικά με το εάν μια επίθεση σε δίκτυα μπορεί να θεωρηθεί «ένοπλη» από την σκοπιά του διεθνούς δικαίου, ώστε να εφαρμοσθεί το άρθρο 51 του Χάρτη του ΟΗΕ, θα αναλυθεί στην συνέχεια της

---

hackers ανήρτησαν σε εσθονική ιστοσελίδα ψεύτικη απολογία του Πρωθυπουργού της χώρας σχετικά με την μεταφορά του χάλκινου αγάλαματος του «Στρατιώτη του Ταλίν». Το αξιωσημείωτο στηπροκειμένη περίπτωση είναι ότι η απολογία ήταν στα ρώσικα

[140] https://en.wikipedia.org/wiki/Spamming

[141] Σύμφωνα με τον Shackelford το 2002, 19 εκατομμύρια πολίτες είχαν την τεχνογνωσία για την διεξαγωγή κυβερνοεπιθέσεων

[142] Stevens Sh. ," Internet war crime tribunals and security in an interconnected world", Transational Law and Contemporary Problems, 2009, p.6

[143] http://www.strategyinternational.org/index.php/en/sectors/nato-transatl-relations/nato/74-5

εργασίας. Στην περίπτωση της Εσθονίας το ΝΑΤΟ έκρινε οι επιθέσεις δεν ήταν τέτοιας έντασης, ώστε να τύχει εφαρμογής το άρθρο 5 του Βορειοατλαντικού Συμφώνου και να ασκηθεί από την Εσθονία το δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας απέναντι σε «ένοπλη επίθεση»[144]. Απλά απέστειλε ειδικούς σε ζητήματα κυβερνοεπιθέσεων στην Εσθονία για να διεξάγουν εμπεριστατωμένη έρευνα, αλλά και για να παράσχουν τεχνική βοήθεια στους Εσθονούς, ώστε να αναπτύξουν καλύτερες αμυντικές τεχνικές στο πεδίο του Κυβερνοχώρου[145]. «Πρόκειται για ένα μείζον θέμα επιχειρησιακής ασφάλειας,το οποίο πρέπει να αντιμετωπιστεί με σοβαρότητα», δήλωσε αξιωματούχος του ΝΑΤΟ από το στρατηγείο της Συμμαχίας στις Βρυξέλλες [146]. Επίσης η Συμμαχία προέβη τον Απρίλιο του 2008 στην ίδρυση μιας διεθνούς στρατιωτικής οργάνωσης, με ονομασία Cooperative Cyber Defence Centre of Excellence (γνωστό ως CCDCOE). Στην ουσία πρόκειται για ένα κέντρο κυβερνοάμυνας με σκοπό να ενισχύσει τις αμυντικές ικανότητες στον Κυβερνοχώρο των χωρών-μελών του ΝΑΤΟ, βελτιώνοντας έτσι τη διαλειτουργικότητα της Συμμαχίας στον τομέα της Κυβερνοάμυνας[147]. Οι επιθέσεις στην Εσθονία προκάλεσαν αρκετές στρατιωτικές οργανώσεις σε διεθνές επίπεδο να αναθεωρήσουν και να επαναπροσδιορίσουν το ζήτημα της ασφάλειας των δικτύων στο σύγχρονο στρατιωτικό δόγμα.

---

[144] Το Βορειοατλαντικό Σύμφωνο υπογράφθηκε και τέθηκε σε ισχύ τον Απρίλιο του 1949 στην Washington. Σύμφωνα με το άρθρο 5 «Τα μέρη του ΝΑΤΟ συμφωνούν ότι μια ένοπλη επίθεση κατά ενός η περισσοτέρων μερών της Συμμαχίας, στην Ευρώπη ή στην Βόρειο Αμερική, θα θεωρηθεί ως επίθεση κατά όλων των μελών της Συμμαχίας. Επίσης συμφωνούν, ότι σε περίπτωση που υπάρξει μια τέτοια επίθεση, κάθε σύμμαχος, θα ασκήσει το αναγνωριζόμενο από το άρθρο 51 του Χάρτη του ΟΗΕ , το δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας , θα παρέχει στο μέρος ή στα μέρη που έχουν δεχθεί επίθεση, μονομερώς και σε συνεννόηση με τα άλλα μέρη, κάθε δυνατή ενέργεια την οποία θεωρεί απαραίτητη, συμπεριλαμβανομένου της χρήσης ένοπλης βίας, προκειμένου να αποκατασταθεί και να διατηρηθεί η ασφάλεια της ΒόρειοΑτλαντικήςπεριοχής»,(https://el.wikisource.org/wiki/%CE%A3%CF%85%CE%BD%CE%B8%CE%AE%CE%BA%CE%B7_%CE%A4%CE%BF%CF%85_%CE%92%CF%8C%CF%81%CE%B5%CE%B9%CE%BF%CF%85_%CE%91%CF%84%CE%BB%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%BF%CF%8D)

[145] Shackelford Sc. J., “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, Berkeley Journal of International Law, 2009, p.202-205

[146] https://athens.indymedia.org/post/705387/

[147] Το κέντρο ιδρύθηκε από επτά κράτη: την Εσθονία, τη Γερμανία, την Ιταλία, τη Λιθουανία, τη Λετονία και την Ισπανία (https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html)

Η Εσθονία υπέδειξε ως υπεύθυνη για τις κυβερνοεπιθέσεις την ρωσική κυβέρνηση υποστηρίζοντας πως αυτή βρισκόταν πίσω αυτές, χωρίς ωστόσο να καταφέρει να συλλέξει στοιχεία που να την ενοχοποιούν. Στις 06 Σεπτεμβρίου του 2007 ο Υπουργός Άμυνας της Εσθονίας Jaak Aaviksoo παραδέχτηκε ότι δεν είχε καμία απόδειξη που να συνδέει τις Κυβερνοεπιθέσεις της χώρας του με τις ρωσικές αρχές[148]. Η ρωσική πλευρά αρνήθηκε κατηγορηματικά οποιαδήποτε ανάμειξη στις Κυβερνοεπιθέσεις που σημειώθηκαν στην Εσθονία, θεωρώντας τις κατηγορίες εις βάρος της εντελώς αβάσιμες[149]. Μοναδική εξαίρεση αποτέλεσε ο Sergei Alexandrovich Markov ο οποίος στις 10 Μαρτίου του 2009 παραδέχτηκε την ανάμειξη του σε αυτές μαζί με τον βοηθό του Konstantin Goloskokov και τους Nashi [150]. Η μόνη σύλληψη που έγινε από τις εσθονικές αρχές ήταν του Dmitri Galushkevich, ενός φοιτητή ρωσικής καταγωγής που ζούσε στο Ταλίν, ο οποίος τον Ιανουάριο του 2008 κρίθηκε ένοχος για συμμετοχή σε επιθέσεις κατά ιστοσελίδων ενός εσθονικού μεταρρυθμιστικού κόμματος (Reform Party). Το πρόστιμο που του επιβλήθηκε ανήλθε στο ύψος των 17.500 κορώνων .

1.5.2 Η περίπτωση της Γεωργίας

Η Γεωργία είναι άλλη μια χώρα όπου πραγματοποιήθηκαν παρατεταμένες κυβερνοεπιθέσεις με αφορμή τις ένοπλες συγκρούσεις που ξέσπασαν μεταξύ της Γεωργίας από την μια πλευρά και της Ν. Οσετίας και Αμπχαζίας[151] από

[148] http://sputniknews.com/world/20070906/76959190.html

[149] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[150] Οι Nashi ήταν ένα πολιτικό κίνημα νεολαίας στην Ρωσία

[151] Μετά τη διάλυση της ΕΣΣΔ, η Γεωργία ανακήρυξε την ανεξαρτησία της ,το1991. Ενώ η Αμπχαζία και η Νότια Οσετία διεκδικούσαν την ανεξαρτησία τους τελικά και οι δύο περιοχές συμπεριλήφθηκαν στα διεθνώς αναγνωρισμένα σύνορα της Γεωργίας, με αποτέλεσμα να ανακηρύξουν de facto την ανεξαρτησία τους σχηματίζοντας μάλιστα και κυβερνήσεις. Οι πολεμικές συγκρούσεις που ξέσπασαν μεταξύ Γεωργίας- Ν. Οσετίας - Αμπχαζίας δεν άφησαν αμέτοχη την Ρωσία, η οποία είχε τοποθετήσει ειρηνευτικές δυνάμεις και στις δύο περιοχές (Αμπχαζία και ΝότιαΟσετία), οι οποίες λόγω της ρωσικής καταγωγής των κατοίκων τους ανέπτυξαν σχέσεις με τη Ρωσία, η οποία παραχώρησε και ρωσικά διαβατήρια στην πλειονότητα των πολιτών αυτών.

την άλλη, τον Αύγουστο του 2008. Η σημαντική γεωπολιτική θέση των δύο αυτών περιοχών οδήγησε σταδιακά σε μακροχρόνια στρατιωτική σύγκρουση τη Ρωσία και τη Γεωργία η οποία κλιμακώθηκε και οι σχέσεις των δύο χωρών οξύνθηκαν, όταν η πρώτη αποφάσισε να συνδράμει τις δύο αποσχισθείσες περιοχές της Γεωργίας, την Ν. Οσετία και την Αμπχαζία, τόσο στρατιωτικά όσο και διπλωματικά. Η Γεωργία στην προσπάθεια της να επαναφέρει την Ν. Οσετία υπό την κυριαρχία της, εισέβαλε στην πρωτεύουσα της τελευταίας, στο Τσχινβάλι, λίγο πριν την τελετή έναρξης των ολυμπιακών αγώνων στο Πεκίνο, στις 08 Αυγούστου του 2008 και λίγες ώρες μετά από συμφωνία εκεχειρίας, σκοτώνοντας τουλάχιστον δέκα Ρώσους στρατιώτες της ειρηνευτικής δύναμης που βρισκόταν, υπό την προεδρία του Γεωργιανού Μιχαήλ Σακασβίλι[152]. Το Τσχινβάλι, υπέστη σφοδρούς βομβαρδισμούς οι οποίοι επέφεραν τον θάνατο πολλών αμάχων «Παρά τις εκκλήσεις μας για ειρήνη και μονομερή κατάπαυση του πυρός, οι αυτονομιστές της Ν. Οσετίας συνέχισαν το βομβαρδισμό των γεωργιανών χωριών. Είμαστε υποχρεωμένοι να αποκαταστήσουμε τη συνταγματική τάξη σε όλη την περιοχή», δήλωσε ο Μαμούκα Κουρασβίλι, διοικητής των γεωργιανών δυνάμεων [153].

Η Ρωσία αντέδρασε άμεσα στην γεωργιανή αυτή επίθεση. Συγκεκριμένα ρωσικά στρατεύματα εισήλθαν στο έδαφος της Ν. Οσετίας, υποστηριζόμεναπό άρματα μάχης, ενώ ρωσικά αεροπλάνα βομβάρδισαν στρατιωτική βάση κοντά στην πρωτεύουσα της Γεωργίας . Ενίσχυσε επίσης τις «ειρηνευτικές» της δυνάμεις στην περιοχή, κατορθώνοντας να απομακρύνει τους Γεωργιανούς από την Ν. Οσετία[154]. Το όλο στρατιωτικό εγχείρημα έγινε υπό την επίβλεψη του πρωθυπουργού της Ρωσίας, Πούτιν. Παράλληλα ρωσικές δυνάμεις εισήλθαν στην Αμπχαζία κατορθώνοντας να εκδιώξουν τους Γεωργιανούς που βρίσκονταν στην περιοχή. Η σύγκρουση τερματίστηκε με την αποχώρηση των

[152] http://www.defencenet.gr/defence/o/22671
[153] https://el.wikipedia.org/wiki/%CE%A0%CF%8C%CE%BB%CE%B5%CE%BC%CE%BF%CF%82_%CF%84%CE%B7%CF%82_%CE%9D%CF%8C%CF%84%CE%B9%CE%B1%CF%82_%CE%9F%CF%83%CE%B5%CF%84%CE%AF%CE%B1%CF%82_2008
[154] http://geopolitics-gr.blogspot.gr/2008/08/blog-post_7278.html

γεωργιανών και ρωσικών δυνάμεων από την περιοχή και την αναγνώριση από τη Ρωσία της ανεξαρτησίας των δύο περιοχών [155]..

Το αξιωσημείωτο στην περίπτωση των κυβερνοεπιθέσεων στην Γεωργία είναι ότι αυτές έλαβαν χώρα πριν την έναρξη των στρατιωτικών επιχειρήσεων και την εισβολή της Γεωργίας στην Ν. Οσετία. Το πρώτο κύμα κυβερνοεπιθέσεων ξεκίνησε στις 19 Ιουλίου του 2008 με στόχο την την ιστοσελίδα του Μιχαήλ Σαακασβίλι, του Προέδρου της Γεωργίας, αρχικά[156] και στην συνέχεια του Υπουργείου Εξωτερικών και του Υπουργείου Άμυνας. Επρόκειτο για επιθέσεις τύπου DDos που αποσκοπούσαν στο να θέσουν εκτός λειτουργίας τις συγκεκριμένες ιστοσελίδες[157] . Επίσης χρησιμοποιήθηκε και η τεχνική της web defacement, όταν στις 11 Αυγούστου 2008 αναρτήθηκαν φωτογραφίες του Σαακασβίλι και του Χίτλερ σε μια προσπάθεια να παρομοιάσουν τον Πρόεδρο της Γεωργίας με τον Χίτλερ , στην ιστοσελίδα του Υπουργείου Εξωτερικών. Οι τεχνικές των Κυβερνοεπιθέσεων που χρησιμοποιήθηκαν ήταν σχεδόν ίδιες με αυτές στην Εσθονία (κατανεμημένη άρνηση υπηρεσίας, παραποίηση ιστοσελίδων - web defacement) και είχαν σκοπό να θέτουν εκτός λειτουργίας τις γεωργιανές ιστοσελίδες - στόχους. Ορισμένες ακόμη κυβερνοεπιθέσεις που καταγράφηκαν ήταν στις 10 Αυγούστου, όταν ιστοσελίδα πρακτορείου ειδήσεων της χώρας απενεργοποιήθηκε για κάποιες ώρες καθώς και η ιστοσελίδα του Γεωργιανού Κοινοβουλίου. Οι κυβερνοεπιθέσεις εστίσαν και σε εμπορικές ιστοσελίδες όπως και στην ιστοσελίδα της Εθνικής Τράπεζας της Γεωργίας με αποτέλεσμα να ανασταλεί η ομαλή λειτουργία του τραπεζικού συστήματος και να «παγώσουν» οι τραπεζικές συναλλαγές για περίπου 10 ημέρες με τεράστιο βέβαια οικονομικό αντίκτυπο για την χώρα [158]. Μια ακόμη τεχνική που χρησιμοποιήθηκε από τους hackers ήταν το email spamming αποστέλλοντας στις ηλεκτρονικές διευθύνσεις των πολιτικών , κακόβουλο λογισμικό. Όλες αυτές οι Κυβερνοεπιθέσεις έδρασαν αρνητικά στην ψυχολογία των Γωεργιανών

[155] https://el.wikipedia.org/wiki/%CE%A0%CF%8C%CE%BB%CE%B5%CE%BC%CE%BF%CF%82_%CF%84%CE%B7%CF%82_%CE%9D%CF%8C%CF%84%CE%B9%CE%B1%CF%82_%CE%9F%CF%83%CE%B5%CF%84%CE%AF%CE%B1%CF%82_2008

[156] Η επίθεση αυτή είχε ως αποτέλεσμα η ιστοσελίδα να τεθεί εκτός λειτουργίας για τουλάχιστον 24 ώρες

[157] Tikk E., Kaska K., Runnimeri K., Kert M., Taliharm A.-M., Vihul L., Cyber Attacks Against Georgia: Legal Lessons Identified, CCDCOE (NATO), November 2008, p.68-71

[158] http://www.nytimes.com/2008/08/13/technology/13cyber.html

,οι οποίοι δεν είχαν καθόλου πρόσβαση στις διεθνείς ιστοσελίδες, ώστε να ενημερώνονται για τις τρέχουσες εξελίξεις . Ωστόσο ο αντίκτυπος των Κυβερνοεπιθέσεων για την Γεωργία δεν ήταν τέτοιας έντασης όπως στην περίπτωση της Εσθονίας, διότι οι κρίσιμες υποδομές της χώρας δεν είχαν άμεση αλληλεξάρτηση από το Διαδίκτυο και την τεχνολογία γενικά.

Αν και οι Γεωργιανές αρχές θεωρούσαν πως για τις Κυβερνοεπιθέσεις αποκλειστικά υπεύθυνη είναι η Ρωσία και σε αυτή την περίπτωση όπως και στην Εσθονία, δεν αποδείχθηκε η ανάμειξη της. Στις 11 Αυγούστου σε δήλωση του ο Υπουργός Εξωτερικών της Γεωργίας ανέφερε: «Το κύμα των κυβερνοεπιθέσεων που έχουν ξεσπάσει από την Ρωσία με στόχο τις γεωργιανές ιστοσελίδες μεταξύ των οποίων και αυτή του ΥΠΕΞ αναστέλλουν την λειτουργία των τελευταίων», κατηγορώντας έτσι δημόσια την Ρωσία για όσα διαδραματίζονται στην χώρα του[159].

ΚΕΦΑΛΑΙΟ Γ΄ Νομική αντιμετώπιση του φαινομένου (Cyberwar) και προβληματισμοί που εγείρονται γύρω από αυτό

Η παγκόσμια κοινότητα αναγνωρίζοντας τη σπουδαιότητα της ασφάλειας του κυβερνοχώρου για την προώθηση των συμφερόντων της αλλά και τις κυβερνοαπειλές που υπάρχουν κατά της εθνικής ασφάλειας του κάθε προηγμένου τεχνολογικά κράτους, έχει πραγματοποιήσει τα πρώτα της βήματα προκειμένου να καθοριστούν οι κανόνες συμπεριφοράς εντός του κυβερνοχώρου σε εθνικό και παγκόσμιο επίπεδο. Πέρα όμως από τα μέτρα που καλούνται τα κράτη να λάβουν για να εξασφαλίσουν την δραστηριότητα τους στον Κυβερνοχώρο, υπάρχει έντονος προβληματισμός και εγείρονται ποικίλα ερωτήματα σχετικά με το ποιοι κανόνες δικαίου θα εφαρμοσθούν ώστε να αντιμετωπισθούν οι απειλές που δημιουργούνται . Κατά μια άποψη, προτείνεται η αναλογική εφαρμογή των ήδη ισχύοντων κανόνων του Διεθνούς Δικαίου (συμβατικού και εθιμικού) .Η άποψη αυτή αναλύεται ενδελεχώς στο Εγχειρίδιο του Ταλίν αποτελούμενο από 95 άρθρα , το οποίο συντάχθηκε το 2013 από μια

[159] http://www.telegraph.co.uk/news/worldnews/europe/georgia/2553058/Russia-continues-cyber-war-on-Georgia.html

Διεθνή Ομάδα Εμπειρογνωμόνων χωρίς όμως να αποτελεί νομικά δεσμευτικά κείμενο. Υπάρχει όμως και η αντικρουόμενη άποψη ότι λόγω της φύσεως και των ιδιαίτερων χαρακτηριστικών του Κυβερνοχώρου κρίνεται αναγκαία η θέσπιση νέων νομικών πλαισίων και νορμών τα οποία πρέπει να εφαρμόσουν οι χώρες, ώστε να αντιμετωπιστούν οι κίνδυνοι που ελλοχεύουν και να αυξηθούν τα επίπεδα ασφάλειας στον Κυβερνοχώρο[160]. Για αυτό απαιτείται αρμονική συνεργασία μεταξύ των κρατών, ώστε να υιοθετηθεί μια κοινή πολιτική για την αντιμετώπιση των Κυβερνοεπιθέσεων και να διασφαλιστεί μια κοινή τάξη δικαίου.

1. Αναλογική Εφαρμογή των ισχύοντων κανόνων Διεθνούς Δικαίου

1.1 Το δίκαιο της χρήσης βίας (jus ad bellum) [161]

Η χρήση της ένοπλης βίας μεταξύ των κρατών αποτελεί ένα φαινόμενο που έχει τις ρίζες του αρκετούς αιώνες πριν. Μέχρι το 1928 η προσφυγή στην χρήση βίας δεν απαγορευόταν , ακόμη και το Σύμφωνο της Κοινωνίας των Εθνών επέτρεπε την προσφυγή στον Πόλεμο υπό ορισμένες προϋποθέσεις. Ορόσημο για την εξέλιξη του δικαίου αποτέλεσε το Σύμφωνο των Παρισίων του 1928. Σύμφωνα με το άρθρο 1 του Συμφώνου απαγορευόταν η προσφυγή στον πόλεμο για την διευθέτηση των διεθνών διαφορών με μόνη εξαίρεση στην περίπτωση άσκησης του δικαιώματος άμυνας[162]. Το Σύμφωνο αυτό είχε ως συνέπεια να αποκρυσταλλωθεί ένας κανόνας εθιμικού δικαίου απαγόρευσης της χρήσης βίας [163] Το βασικό ρυθμιστικό πλαίσιο του δικαίου της χρήσης βίας διαμορφώθηκε με τον Χάρτη του ΟΗΕ, ο οποίος υπογράφτηκε μετά το τέλος

[160]Shackelford Scott J., “From Nuclear War to Net War: Analogizing Cyber Attacks inInternational Law” , Berkeley Journal of International Law, 2009, p. 248-250

[161] Το jus ad bellum είναι το Δίκαιο προ της ενόπλου συγκρούσεως και κατά τα πρώτα στάδια αυτής όπως αυτό καθορίζεται από το Σύμφωνο των Παρισίων 1928, τον Καταστατικό Χάρτη του ΟΗΕ και τις αποφάσεις του ΔΔΧ

[162] Η εξαίρεση αυτή δεν υπήρχε στο αρχικό κείμενο του Συμφώνου αλλά σε διακοίνωση του Υπουργείου Εξωτερικών των ΗΠΑ, Kellogg, η οποία έγινε δεκτή από τα κράτη (Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ. 481)

[163] Brownlie I., “The Rule of Law in International Affairs , International Law at the 50 th Anniversary of the United Nations, Kluwer Law International , 1998, p.194

του Β΄ Παγκοσμίου Πολέμου[164]. Η διεθνής κοινότητα έχοντας ως πρωταρχικό σκοπό, μετά το 1945 την ειρήνη, προσπάθησε να θέσει σε ισχύ ένα πλαίσιο δικαίου για την αρμονική διευθέτηση των διεθνών διαφορών και την διατήρηση της διεθνούς ειρήνης και ασφάλειας. Στην συνέχεια θα γίνει μνεία σε βασικά άρθρα του Χάρτη από τα οποία πηγάζουν ορισμένοι κανόνες σχετικά με την χρήση βία , το δικαίωμα ατομικής ή συλλογικής άμυνας και τις προϋποθέσεις άσκησης του, τον ρόλο του Συμβουλίου Ασφαλείας και τι συνιστά ένοπλη επίθεση κατά το Διεθνές Δίκαιο.

Ο κανόνας της απαγόρευση χρήσης βίας κατά το Διεθνές Δίκαιο

Σύμφωνα με το άρθρο 2 παράγραφο 4 του Χάρτη « Όλα τα μέλη στις διεθνείς τους σχέσεις θα απέχουν από την απειλή ή την χρήση βίας κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους είτε με οποιοδήποτε άλλο τρόπο ασυμβίβαστο με τους σκοπούς των Ηνωμένων Εθνών» [165]. Η υποχρέωση αυτή επεκτάθηκε σταδιακά σε όλα τα κράτη ως επακόλουθο της διαμόρφωσης ενός εθιμικού κανόνα απαγόρευσης της απειλής ή χρήσης βίας. Το ΔΔΧ στην Υπόθεση Νικαράγουα αναγνώρισε την αρχή αυτή προσδιορίζοντας ότι «έχει επίσης status εθιμικού δικαίου» [166]. Πρόκειται επίσης για κανόνα δογματικό, αναγκαστικού δικαίου (jus cogens), ο οποίος είναι δεσμευτικός για όλα τα κράτη**[167]**, δεν μπορεί να ανασταλεί με καμία διεθνή συνθήκη[168], δημιουργώντας υποχρεώσεις σε όλα τα μέλη της διεθνούς κοινότητας (erga omnes) [169]. Εν κατακλείδι τα κράτη είναι υποχρεωμένα bona

[164] Ο κυρωτικός αναγκαστικός νόμος για την χώρα μας ήταν ο Νόμος 585/1945(ΦΕΚ 242, Τεύχος Α΄/29-09-2015)

[165] Η πρωτότυπη διατύπωση :"[a]ll Members shall refrain in theirinternational relations from the threat or use of force against the territorial integrity orpolitical independence of any state, or in any other manner inconsistent with the Purposes of the United Nations"

[166] Όπως έκρινε το Διεθνές Δικαστήριο της Χάγης στην Υπόθεση Νικαράγουα (ICJ , Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.A.), 1986 ICJ Rep. 14, 187 – 190), το οποίο σύμφωνα με το άρθρο 38 παρ. 1 του Καταστατικού του εφαρμόζει και το διεθνές έθιμο, (Cassese A., " Διεθνές Δίκαιο", Gutenberg, 2012, σελ. 76)

[167] Σύμφωνα με το Άρθρο 4 του Χάρτη μόνο κράτη είναι δυνατόν να γίνουν μέλη των Ηνωμένων Εθνών, άρα και αυτή η απαγόρευση δεσμεύει μόνο κράτη ανεξάρτητα αν είναι μέλη του οργανισμού

[168] Άρθρο 53 της Σύμβασης της Βιέννης περί του Δικαίου των Διεθνών Συνθηκών (1969)

[169] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.482

fide να επιλύουν τις διαφορές τους με ειρηνικά μέσα (διαπραγματεύσεις, προσφυγή σε διαιτητικούς και δικαστικούς μηχανισμούς), χωρίς να δεσμεύονται να επιλέξουν συγκεκριμένο μέσο επίλυσης της διαφοράς τους. Γενικά ο κανόνας παραβιάζεται όταν ένα κράτος εκούσια ή mala fide αρνείται να προσφύγει σε διαπραγματεύσεις ή άλλα ειρηνικά μέσα για την επίλυση των διαφορών του[170]. Ο γενικός κανόνας της απαγόρευσης της χρήσης βίας επιδέχεται ορισμένες εξαιρέσεις τις οποίες θα μελετήσουμε στην συνέχεια.
Το κρίσιμο όμως ερώτημα που πρέπει να απαντηθεί είναι τι συνιστά χρήση βίας, τι ένοπλη επίθεση και κατά πόσο οι κυβερνοεπιθέσεις που διεξάγονται στο νέο αυτό πεδίο δράσης, τον Κυβερνοχώρο, υπάγονται στην παραπάνω κατηγορία. Αυτό που πρέπει να αναλογιστούμε είναι πως την περίοδο που συντάχθηκε ο Χάρτης του ΟΗΕ δεν υπήρχαν καν αυτοί οι όροι (Κυβερνοεπίθεση, Κυβερνοχώρος,κακόβουλο λογισμικό, ιοί), ώστε να ληφθούν υπόψη από τους συντάκτες του Χάρτη.

Για να απαντήσουμε στα παραπάνω ερωτήματα και να κατανοήσουμε καλύτερα το περιεχόμενο του άρθρου 2 παρ. 4, θα πρέπει να μελετήσουμε συνδυαστικά και κάποιες άλλες διατάξεις του Χάρτη. Το νόημα της απαγόρευσης της χρήσης βίας στις διεθνείς σχέσεις των κρατών δεν μπορεί να ερμηνευθεί αποκλειστικά από το άρθρο 2(4), αλλά σε συνδυασμό με τα άρθρα 39,41,42, 51 και 53 του Χάρτη. Καταρχήν το άρθρο 2(4) επιτάσσει τα κράτη να προσφεύγουν σε ειρηνικά μέσα επίλυσης των διεθνών διαφορών. Αυτός είναι και ο θεμελιώδης σκοπός των Ηνωμένων Εθνών, η ειρηνική διεύθετηση των διαφορών μεταξύ των κρατών. Ωστόσο απαγόρευση της χρήσης βίας δεν περιλαμβάνει οποιοδήποτε είδος χρήσης βίας (πολιτική ή οικονομική), αλλά σύμφωνα με την κρατούσα άποψη, περιορίζεται στην «ένοπλη» [171]. Αυτή η άποψη ενισχύεται και από τις προπαρασκευαστικές εργασίες του Χάρτη, όταν κατά την διεξαγωγή της ιδρυτικής Συνδιάσκεψης του ΟΗΕ στον Άγιο Φραγκίσκο η πρόταση της Βραζιλίας να συμπεριληφθούν και τα οικονομικά μέτρα στην απαγόρευση του άρθρου 2(4) απορρίφθηκε [172]. Επιπλέον και σε

[170] [170] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ. 77
[171] Dinstein Y. , "War, Aggression and Self-Defence", 3rd Edition , Cambridge University Press (Virtual Publishing) 2003, p. 81
[172] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.483

μεταγενέστερα κείμενα της Γενικής Συνέλευσης όπως η Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations[173] τον Οκτώβριο του 1970 και η Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations τον Νοέμβριο του 1987 [174] κατέστη σαφές ότι το άρθρο 2(4) αναφέρεται μόνο σε ένοπλη βία. Τα άλλα δύο είδη βίας (πολιτική και οικονομική) διέπονται από την αρχή της μη επέμβασης στις εσωτερικές και εξωτερικές υποθέσεις των κρατών [175], η οποία βέβαια δεν διατυπώνεται ρητά στον Χάρτη του ΟΗΕ. Σύμφωνα με την αρχή αυτή, ένα κράτος δεν επιτρέπεται να ασκήσει πίεση σε εθνικά όργανα (π.χ της νομοθετικής και εκτελεστικής εξουσίας) άλλου κράτους, ούτε και να παρέμβει στις σχέσεις μεταξύ των αρχών και των υπηκόων ξένων κρατών[176] .

Η διάταξη 2(4) του Χάρτη των Ηνωμένων Εθνών αναφέρεται στην αποχή από απειλή ή χρήση βίας κατά της εδαφικής ακεραιότητας ή πολιτικής ανεξαρτησίας ενός κράτους ή οποιοδήποτε άλλο τρόπο ασυμβίβαστο με τους σκοπούς των Ηνωμένων Εθνών. Ως παραβίαση της εδαφικής ακεραιότητας δεν νοείται μόνο η βίαιη πρόσκτηση εδάφους από ένα άλλο κράτος[177]. Να διευκρινιστεί ότι η κατάκτηση εδάφους δεν δημιουργεί νόμιμο τίτλο κυριαρχίας ακόμη και αν υπάρχει de facto κατοχή [178]. Επίσης οποιαδήποτε αναγνώριση εδαφικης επέκτασης είναι προϊόν χρήσης ή απειλής χρήσης βίας, είναι παράνομη [179]. Η παραβίαση της εδαφικής ακεραιότητας νοείται γενικά ως η παραβίαση της εδαφικής κυριαρχίας ενός κράτους[180] και η απαγόρευση της χρήσης βίας του άρθρου 2 (4) αφορά εκτός από την πρόσκτηση εδάφους με βία και το απαραβίαστο των συνόρων ενός κράτους ανεξάρτητα από τον απώτερο σκοπό

[173] http://www.un-documents.net/a25r2625.htm
[174] http://www.un.org/documents/ga/res/42/a42r022.htm
[175] Brownlie Ian, “International Law and the Use of Force by States”, 1963, p. 114-116
[176] Cassese A., Διεθνές Δίκαιο”, Gutenberg, 2012, σελ. 71
[177] Στην υπόθεση Legal Consequences of the Construction of a Wall το ΔΔΧ έκρινε ότι η απαγόρευση της πρόσκτησης εδαφών με χρήση βίας αποτελεί κανόνα εθιμικού δικαίου
[178] Cassese A., Διεθνές Δίκαιο”, Gutenberg, 2012, σελ. 75
[179] Cassese A., Διεθνές Δίκαιο”, Gutenberg, 2012, σελ.76
[180] Έτσι έκρινε το ΔΔΧ στην υπόθεση Νικαράγουα , ICJ Rep 1986

του κράτους που προσφεύγει στην χρήση βίας[181]. Από την άλλη πλευρά η χρήση βίας κατά της «πολιτικής ανεξαρτησίας» αφορά την ανατροπή της κυβέρνησης ενός κράτους ή τον περιορισμό στην άσκηση των λειτουργιών της, αναφορικά με την δικαστική, την εκτελεστική και την νομοθετική εξουσία[182]. Όπως αναφέρεται στο άρθρο 2 του Εγχειριδίου του Ταλίν , το ΔΔΧ στην Υπόθεση Νικαράγουα έκρινε ότι η αρχή της μη επέμβασης απαγορεύει σε όλα τα κράτη ή να παρεμβαίνουν άμεσα ή έμμεσα στις εσωτερικές ή εξωτερικές υποθέσεις των άλλων κρατών ». Βασιζόμενο στην θέση αυτή το Δικαστήριο έκρινε ότι η παροχή κεφαλαίων σε αντάρτες ήταν « αναμφισβήτητα μια πράξη παρέμβασης στις εσωτερικές υποθέσεις της Νικαράγουας , αν και δεν αποτελεί χρήση βίας».

Η έννοια της κυριαρχίας (Sovereignty) στον Κυβερνοχώρο δίνεται στο άρθρο 1 του Εγχειριδίου του Ταλίν σύμφωνα με το οποίο «Ένα κράτος μπορεί να ασκεί έλεγχο επί των υποδομών στον κυβερνοχώρο και των δραστηριοτήτων που διεξάγονται μέσα στο κυρίαρχο έδαφός του». Σκοπός του άρθρου είναι να τονίσει ότι παρόλο που κανένα κράτος δεν μπορεί να διεκδικήσει την κυριαρχία του κυβερνοχώρου, μπορει να ασκήσει τα κυριαρχικά του δικαιώματα σε οποιαδήποτε υποδομή στον κυβερνοχώρο που βρίσκεται στο έδαφός του , καθώς και στις δραστηριότητες που συνδέονται με την εν λόγω υποδομή στον κυβερνοχώρο[183]. Στη συνέχεια του άρθρου 1 (παράγραφος 6) ανφέρεται ότι «Μια επιχείρηση στον κυβερνοχώρο από ένα κράτος στρεφόμενη εναντίον υποδομών στον κυβερνοχώρο που βρίσκονται σε άλλο κράτος, μπορεί να αποτελεί παραβίαση της εδαφικής κυριαρχίας του τελευταίου. Το κάνει σίγουρα αν προκαλεί ζημία. Η Διεθνής Ομάδα Εμπειρογνωμόνων δεν συμφώνησε ομόφωνα ως προς το αν η τοποθέτηση κακόβουλου λογισμικού που δεν προκαλεί σωματική βλάβη (όπως και με το κακόβουλο λογισμικό που

[181] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.485

[182] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.484

[183] «This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure»

χρησιμοποιείται για την παρακολούθηση των δραστηριοτήτων) συνιστά παραβίαση της εθνικής κυριαρχίας».

Η Ομάδα Εμπειρογνωμόνων συνεχίζει στην παράγραφο 7 του άρθρου 1 : «Μια επιχείρηση στον Κυβερνοχώρο που αποσκοπεί στο να εξαναγκάσει την κυβέρνηση (και δεν επιτρέπεται βάσει των κανόνων του διεθνούς δικαίου) , ενδέχεται να συνιστά απαγορευμένη επέμβαση ή «χρήση βίας» που απαγορεύεται . Άρα για να θεωρηθεί ότι μια πράξη αποτελεί παραβίαση της εδαφικής ακεραιότητας ή επέμβαση στο εσωτερικό ενός κράτους απαραίτητη προϋπόθεση είναι το στοιχείο του εξαναγκασμού. Μια επιχείρηση στον κυβερνοχώρο που μπορεί να θεωρηθεί ως« ένοπλη επίθεση» ενεργοποιεί το δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας (ειδικότερα στο άρθρο 13). Πράξεις οι οποίες δεν αποτελούν ένοπλη επίθεση, αλλά συνιστούν, παραβίαση κάποιου κανόνα του διεθνούς δικαίου μπορεί να εξουσιοδοτήσουν το κράτος που έχει στοχοποιηθεί να καταφύγει σε αντίμετρα , τα οποία αναφέρονται ειδικότερα στο άρθρο 9 του Εγχειριδίου σύμφωνα με το οποίο: «Ένα κράτος το οποίο έγινε στόχοςμιας διεθνούς παράνομης πράξης μπορεί να καταφύγει σε αντίμετρα,συμπεριλαμβανομένων και των αντιμέτρων στον κυβερνοχώρο, κατά του υπεύθυνου κράτους». Αντιθέτως οι επιχειρήσεις στον Κυβερνοχώρο, οι οποίες τελούνται κατόπιν εξουσιοδότησης του Συμβουλίου Ασφαλείας στα πλαίσια του Κεφαλαίου VII του Χάρτη των Ηνωμένων Εθνών (άρθρο 18) δεν συνιστούν παραβίαση της εδαφικής κυριαρχίας του κράτους που στοχοποιείται. Αξίζει να αναφερθούμε και στην παράγραφο 10 του άρθρου 1 του Εγχειριδίου η οποία διευκρινίζει το νόημα της αρχής της κυριαρχίας στον Κυβερνοχώρο. Ειδικότερα αναφέρει τα εξής : «Στα πλαίσια του κυβερνοχώρου, η αρχή της κυριαρχίας επιτρέπει σε ένα κράτος, μεταξύ άλλων, να περιορίσει ή να προστατεύσει (εν μέρει ή ολικά) την πρόσβαση στο internet , με την επιφύλαξη των διατάξεων του ισχύοντος διεθνούς δικαίου, όπως είναι οι διατάξεις για τα ανθρώπινα δικαιώματα. Το γεγονός ότι κάποιες υποδομές στον κυβερνοχώρο που βρίσκονται στο έδαφος ενός συγκεκριμένου κράτους συνδέονται με το παγκόσμιο δίκτυο τηλεπικοινωνιών δεν μπορεί να ερμηνευθεί ως παραίτηση από τα κυριαρχικά του δικαιώματα επί της υποδομής αυτής». Συμπερασματικά το άρθρο 1 του Εγχειριδίου εξηγεί επαρκώς την έννοια της εδαφικής κυριαρχίας

ενός κράτους και σε ποιες περιπτώσεις υπάρχει παραβίαση αυτής (απαραίτητο το στοιχείο του εξαναγκασμού).

Σύμφωνα με το άρθρο 2(4) του Χάρτη του ΟΗΕ, η απαγόρευση της χρήσης ή απειλής χρήσης βίας, αναφέρεται στις διακρατικές σχέσεις. Κατά συνέπεια, τα κράτη μπορούν να καταφεύγουν στην χρήση βίας για την καταστολή εξεγέρσεων στο εσωτερικό τους ή για την αντιμετώπιση των απελευθερωτικών κινημάτων επιζητώντας την ανεξαρτησία τους σε περιοχές που βρίσκονται υπό αποικιοκρατικό καθεστώς και τις οποίες οι αποικιακές δυνάμεις θεωρούν ως αναπόσπαστο μέρος της επικράτειας τους [184]. Αντιθέτως απαγορεύεται η χρήση βίας από ένα κράτος για να στερήσει από ένα λαό το δικαίωμα στην αυτοδιάθεση [185]. Το άρθρο 2(4) δεν απαγορεύει μόνο την χρήση αλλά και την απειλή της χρήσης βίας . Σύμφωνα με την Γνωμοδότηση του ΔΔΧ για τα Πυρηνικά Όπλα , η απειλή της χρήσης βίας εάν δεν υπάγεται σε μια από τις εξαιρέσεις του κανόνα για μη χρήση βίας. Βέβαια η πρόθεση και πραγματική βούληση κάθε κράτους για την απειλή της χρήσης βίας κρίνεται κατά περίπτωση και εξαρτάται από τα πραγματικά περιστατικά κάθε φορά [186].

Στην περίπτωση των επιχειρήσεων στον Κυβερνοχώρο η απαγόρευση της απειλής ή χρήσης βίας διατυπώνεται ρητά στο άρθρο 10 του Εγχειριδίου του Ταλίν. Ειδικότερα αναφέρει ότι : «Μια επιχείρηση στον κυβερνοχώρο που αποτελεί απειλή ή χρήση βίας κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους ή ό,τι είναι με οποιοδήποτε άλλο τρόπο ασυμβίβαστο με τους σκοπούς των Ηνωμένων Εθνών , είναι παράνομη». Υπάρχουν δύο εξαιρέσεις στον κανόνα της απαγόρευση της χρήσης βίας , η πρώτη είναι η εξουσιοδότηση από το Συμβούλιο Ασφαλείας δυνάμει του κεφαλαίου VII (άρθρο 18 του Εγχειριδίου) και η δεύτερη η περίπτωση της αυτοάμυνας , σύμφωνα με το άρθρο 51 του Χάρτη του ΟΗΕ (άρθρο 13 του Εγχειριδίου), τις οποίες θα μελετήσουμε αναλυτικά στην συνέχεια της εργασίας . Η Διεθνής Ομάδα Εμπειρογνωμόνων δεν έλαβε θέση ως προς τη νομιμότητα

[184] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.74
[185] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.484
[186] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.484

των άλλων χρήσεων της βίας, όπως είναι η ανθρωπιστική παρέμβαση [187]. Επιπλέον, όπως αναφέρεται στο άρθρο 10 (6) : «Το γεγονός ότι μια επιχείρηση στον κυβερνοχώρο δεν συνιστά χρήση βίας δεν την καθιστά απαραίτητα νόμιμη σύμφωνα με το διεθνές δίκαιο. Συγκεκριμένα, μια πράξη του κυβερνοχώρου μπορεί να αποτελέσει παραβίαση της απαγόρευσης της παρέμβασης».

Σύμφωνα με το άρθρο 39 του Χάρτη, το Συμβούλιο Ασφαλείας είναι το αρμόδιο όργανο για να αποφαίνεται για την ύπαρξης απειλής κατά της ειρήνης, διατάραξης αυτής ή οποιασδήποτε επιθετικής πράξεως και να προβαίνει σε συστάσεις ή στη λήψη μέτρων, σύμφωνα με τα άρθρα 41 και 42 για την διατήρηση ή αποκατάσταση της διεθνούς ειρήνης και ασφάλειας. Οι εξουσίες που αποδίδονται στο Συμβούλιο Ασφαλείας από το Κεφάλαιο VII είναι αρκετά σημαντικές. Το άρθρο 39 αποτελεί μια καινοτομία, διότι δεν υποχρεώνει το Συμβούλιο Ασφαλείας να κάνει οριοθετήσεις για κάθε κατάσταση ή διαφορά που ενδέχεται να αποτελεί απειλή ή διατάραξη της ειρήνης ή επιθετική πράξη ούτε το υποχρεώνει να επιβάλει μέτρα –κυρώσεις.

Το Συμβούλιο Ασφαλείας, σύμφωνα με τα άρθρα 40-41 του Χάρτη , δύναται να λάβει προσωρινά, προληπτικά μέτρα , όταν αντιλαμβάνεται ότι μια κατάσταση πρόκειται να επιδεινωθεί, καλώντας τα μέλη των Ηνωμένων Εθνών να συνεργαστούν και να συμμορφωθούν με τα μέτρα αυτά. Αν τα προσωρινά μέτρα δεν τελεσφορήσουν, τότε το ΣΑ μπορεί να προβεί σε στρατιωτικές «κυρώσεις» , που δεν αποκλείουν ακόμη και τη χρήση ένοπλης βίας. Τα μέτρα των άρθρων 40-41 μπορεί να είναι οικονομικά ή εμπορικά σε βάρος ενός κράτους [188]. Υπάρχουν όμως και οι περιπτώσεις, όπου το ΣΑ έχει λάβει άλλου είδους μέτρα, όπως την διακοπή των διπλωματικών σχέσεων. Κάτι τέτοιο συνέβη στην περίπτωση της Νοτίου Αφρικής , η οποία είχε υιοθετήσει το

[187] «There re two widely awcknowledged exceptions to the prohibition on the use of force — uses of force authorized by the Security Council under Chapter VII (Rule 18) and self-defence pursuant to Article 51 and customary international law (Rule 13). The International Group of Experts did not take a position as to the lawfulness of other uses of force, such as humanitarian intervention»

[188] Στην περίπτωση της Ν. Αφρικής (1977-1994) το ΣΑ επέβαλλε εμπάργκο στην εισαγωγή όπλων και άλλου στρατιωτικού υλικού λόγω του apartheid. Ακολούθησαν οικονομικές κυρώσεις σε βάρος του Ιράκ με το ψήφισμα 661/1990 και της Σομαλία με το ψήφισμα 733/1992, βλ. Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.399

Apartheid (από την Αφρικάνικη λέξη που σημαίνει "διαχωρισμός"). Πρόκειται για έναν συστηματικό τρόπο θεσμοθέτησης φυλετικών διακρίσεων και διαχωρισμού που εφαρμόστηκε από την Κυβέρνηση της Νοτίου Αφρικής από το 1948 ως επίσημη πολιτική. Η Γενική Συνέλευση και το Συμβούλιο Ασφαλείας είχαν κηρύξει το apartheid ασυμβίβαστο με το Χάρτη των Ηνωμένων Εθνών. Με την πάροδο του χρόνου, είχε εδραιωθεί η πεποίθηση ότι η εξάλειψη του apartheid και η εγκαθίδρυση μιας αληθινά δημοκρατικής κοινωνίας απαιτούσε την επιβολή υποχρεωτικών κυρώσεων εναντίον της Νοτίου Αφρικής, στις οποίες προέβη τελικά το ΣΑ, όπως προαναφέραμε [189]. Να επισημάνουμε ότι χωρίς την ομόφωνη στήριξη της διεθνούς κοινότητας δεν μπορούν να τελεσφορήσουν τα μέτρα που λαμβάνει το ΣΑ.

Οι εξαιρέσεις στον κανόνα της απαγόρευσης της χρήσης βίας είναι τρεις. Η πρώτη είναι η περίπτωση άσκησης του δικαιώματος ατομικής και συλλογικής άμυνας σύμφωνα με το άρθρο 51 το οποίο προβλέπει ότι: « Καμία διάταξη του Χάρτη δεν θα εμποδίζει το φυσικό δικαίωμα της ατομικής ή συλλογικής αυτοάμυνας, σε περίπτωση που ένα μέλος των Ηνωμένων Εθνών δεχτεί επίθεση, μέχρι το Συμβούλιο Ασφαλείας να λάβει τα αναγκαία μέτρα για την διατήρηση της διεθνούς ειρήνης και ασφάλειας»[190].

Η δέυτερη περίπτωση είναι αυτή που προβλέπεται στο Κεφάλαιο VII του Χάρτη, όταν το ΣΑ εξουσιοδοτεί τα κράτη να προσφεύγουν στην χρήση βίας μετά από επιθετική πράξη κατά άλλου κράτους το οποίο είχε αντιδράσει στα πλαίσια της νόμιμης άμυνας[191] ή όταν κράτη εξουσιοδοτούνται από το ΣΑ να χρησιμοποιήσουν ένοπλη βία προκειμενου να αντιμετωπίσουν απειλές για την

[189] http://kypros.org/Human_Rights/index21a.html, βλέπε επίσης και Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.399

[190] Η πρωτότυπη διατύπωση : "[n]othing in the presentCharter shall impair the inherent right of individual or collective self-defence if anarmed attack occurs against a Member of the United Nations, until the Security Councilhas taken measures necessary to maintain international peace and security.."

191 Παραδείγματα τέτοιων περιπτώσεων έχουμε όταν το 1950 το ΣΑ εξουσιοδότησε τα κράτη-μέλη του Οργανισμού να βοηθήσουν την Νότια Κορέα να αντιμετωπίσει την επίθεση της Βόρειας επιτρέπωντας τους να χρησιμοποιήσουν την σημαία του ΟΗΕ κατά την διάρκεια των στρατιωτικών επιχειρήσεων (ψηφίσματα 82 και 83 του 84/1950). Επίσης το 1990 το ΣΑ εξουσιοδότησε τα κράτη- μέλη του Οργανισμού να προσφύγουν στην χρήση βίας για να απωθήσουν την Ιρακινή επίθεση κατά του Κουβέιτ (ψηφίσμα 678/1990) , Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.405

ειρήνη, κάτι που συμβαίνει κυρίως στις ανθρωπιστικές κρίσεις. Το ΣΑ έχει καταφέρει να διευρύνει την έννοια της απειλής για την ειρήνη που αναφέρεται στο άρθρο 39, περιλαμβάνοντας και τις ανθρωπιστικές κρίσεις που λαμβάνουν χώρα στο εσωτερικό ενός κράτους. Μια τέτοια περίπτωση συνέβη σε περιοχές της Βοσνίας και Ερζεγοβίνης όπου για να προστατευθούν, το ΣΑ εξέδωσε τα ψηφίσματα 836 και 844 /1993 με τα οποία εξουσιοδοτούσε τα κράτη- μέλη να αντιμετωπίσουν τις επιθέσεις σε βάρος των ασφαλών περιοχών με την χρήση αεροπορικών δυνάμεων [192] .

Οι δύο αυτές εξαιρέσεις στον κανόνα της απαγόρευσης της χρήσης βίας αναφέρονται στα άρθρα 10 (2), 13 και 18 του Εγχειριδίου του Ταλίν. Ειδικότερα στο άρθρο 13 γίνεται μνεία στο δικαίωμα της αυτοάμυνας. Σύμφωνα με αυτό: «Ένα κράτος που γίνεται στόχος μιας επιχείρησης στον κυβερνοχώρο, η οποία βρίσκεται στο επίπεδο της ένοπλης επίθεσης, μπορεί να ασκήσει το εγγενές δικαίωμα της αυτοάμυνας. Αν μια επιχείρηση στον κυβερνοχώρο αποτελεί ένοπλη επίθεση, αυτό εξαρτάται αποκλειστικά από την ένταση και τις επιπτώσεις της». Η Διεθνής Ομάδα Εμπειρογνωμόνων κατέληξε ομόφωνα στο συμπέρασμα ότι ορισμένες πράξεις στον κυβερνοχώρο μπορεί να έχουν τέτοια ένταση, ώστε να θεωρούνται « ένοπλη επίθεση » όπως αυτή συνάγεται σαν έννοια από τον Χάρτη του ΟΗΕ. Η άποψη αυτή έρχεται σε απόλυτη συμφωνία με την Απόφαση του ΔΔΧ για την Νομιμότητα των Πυρηνικών Όπλων, σύμφωνα με την οποία η επιλογή των μέσων μιας επιχείρησης δεν έχει καθοριστική σημασία, ώστε να θεωρηθεί αυτή ως ένοπλη επίθεση. Η θέση αυτή πυρρώνεται και από την πρακτική των Κρατών . Για παράδειγμα, είναι καθολικά αποδεκτό ότι οι χημικές, βιολογικές και ραδιολογικές επιθέσεις που έχουν την απαιτούμενη ένταση και τα αποτελέσματα, ώστε να αποτελούν ένοπλες επιθέσεις ενεργοποιούν το δικαίωμα της αυτοάμυνας. Αυτό συμβαίνει επειδή οι επακόλουθες συνέπειες μπορεί να περιλαμβάνουν πόνο ή ακόμη και το θάνατο. Παρόμοια συλλογιστική ισχύει και για τις επιχειρήσεις στον κυβερνοχώρο. Υπήρχε διχογνωμία στην Ομάδα Εμπειρογνωμόνων σχετικά με το αν στην έννοια «ένοπλη επίθεση », ο όρος «ένοπλη» περιλαμβάνει υποχρεωτικά την χρήση όπλων (άρθρο 41). Η πλεοψηφία υιοθέτησε την άποψη, ότι κάτι τέτοιο

[192] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.406

δεν ισχύει και πως καθοριστικός παράγοντας είναι, αν οι συνέπειες μιας πράξης στον κυβερνοχώρο, ανεξάρτητα από τα μέσα που χρησιμοποιήθηκαν για αυτήν, είναι ανάλογες και συγκρίσιμες με εκείνες που θα προέκυπταν από μια ενέργεια, η οποία θεωρείται κινητική ένοπλη επίθεση[193]. Το δικαίωμα της συλλογικής άμυνας αναφέρεται στο άρθρο 16 σύμφωνα με το οποίο : « Το δικαίωμα της αυτοάμυνας μπορεί να ασκηθεί και συλλογικά. Η συλλογική αυτοάμυνα εναντίον μιας επιχείρησης στον κυβερνοχώρο, η οποία ανέρχεται σε ένοπλη επίθεση μπορεί να ασκηθεί μόνο μετά από αίτημα του κράτους- θύματος και εντός του πεδίου εφαρμογής του αιτήματος [194].

Το άρθρο 18 του Εγχειριδίου του Ταλίν αναφέρεται στην δεύτερη εξαίρεση από τον κανόνα της απαγόρευσης της χρήσης βίας, ο οποίος σχετίζεται με την δράση του Συμβουλίου Ασφαλείας. Ειδικότερα όπως ορίζεται σε αυτό : «Το Συμβούλιο Ασφαλείας μπορεί να καθορίσει, εάν μια πράξη συνιστά απειλή για την ειρήνη, παραβίαση αυτής ή επιθετική πράξη , μπορεί να επιβάλλει ειρηνικά μέτρα συμπεριλαμβανομένων και των επιχειρήσεων που διεξάγονται στον κυβερνοχώρο. Αν το Συμβούλιο Ασφαλείας κρίνει ότι τα μέτρα αυτά δεν επαρκούν, τότε μπορεί να επιβάλλει πιο αυστηρά ακόμη και χρήση βίας, συμπεριλαμβανομένων και των μέτρων που αφορούν στον κυβερνοχώρο . Το παρόν άρθρο βασίζεται στο Κεφάλαιο VII του Χάρτη των Ηνωμένων Εθνών και ειδικότερα στα άρθρο 39, 41 και 42 του Χάρτη, τα οποία αναλύσαμε παραπάνω. Μέχρι σήμερα το ΣΑ δεν έχει ποτέ διαπιστώσει ότι μια επιχείρηση στον κυβερνοχώρο συνιστά απειλή για την ειρήνη, παραβίαση αυτής ή επιθετική ενέργεια . Ωστόσο, είναι αναμφισβήτητο γεγονός ότι έχει την εξουσία να το πράξει. Για παράδειγμα, ανήκει στην αρμοδιότητα του ΣΑ να καθορίσει εάν οι επιχειρήσεις στον κυβερνοχώρο που έχουν στόχο εθνικά τραπεζικά συστήματα

[193] «The International Group of Experts was divided as to whether the notion of armed attack, because of the term 'armed', necessarily involves the employment of 'weapons' (Rule 41). The majority took the position that it did not and that instead the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack»

[194] «The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim-State and within the scope of the request».

ή κρίσιμες εθνικές υποδομές συνιστούν απειλή για την ειρήνη, παραβίαση αυτής ή επιθετική ενέργεια[195].

Η τρίτη εξαίρεση στον κανόνα της απαγόρευσης της χρήσης βίας αποτελεί η πρόσκληση της κυβέρνησης ενός κράτους. Οι κυβερνητικές αρχές ενός κράτους έχουν το δικαίωμα, όταν στο εσωτερικό τους λαμβάνει χώρα μια ένοπλη εξέγερση για την καταστολή της, να ζητήσουν την στρατιωτική βοήθεια άλλου κράτους. Ωστόσο υπάρχουν τρεις περιπτώσεις όπου η πρόσκληση για στρατιωτική συνδρομή δεν είναι νόμιμη: α) εάν είναι απόρροια απειλής ή χρήσης βίας από το κράτος που την προσφέρει, β) εάν δεν προκύπτει με σαφήνεια αλλά εικάζεται, γ) εάν η πηγή προέλευσης του δεν είναι κυβερνητικός φορέας. Σύμφωνα μάλιστα με την κρίση του ΔΔΧ στην Υπόθεση Κονγκό κατά Ουγκάντας το κράτος που ζήτησε στρατιωτική βοήθεια μπορεί να την αποσύρει ανά πάσα στιγμή, με αποτέλεσμα η παραμονή των στρατιωτικών δυνάμεων του κράτους από το οποίο ζητήθηκε να συνδράμει, να συνιστά καταστρατήγηση του κανόνα της απαγόρευσης χρήσης βίας κατά το άρθρο 2(4)[196]. Και οι τρείς εξαιρέσεις έχουν γίνει αποδεκτές σε όλα τα μέλη της διεθνούς κοινότητας [197] .

Το επόμενο καίριο ερώτημα που πρέπει να απαντηθεί είναι πότε υπάρχει νόμιμη άμυνα, όπως αυτή αναφέρεται στο άρθρο 51 του Χάρτη, και πως συνδέεται ο ορισμός της επίθεσης με την συγκεκριμένη διάταξη. Καταρχήν για να κατανοήσουμε καλύτερα τις παραπάνω έννοιες θα αναφερθούμε προηγουμένως στην Υπόθεση Caroline[198] στην οποία αναγνωρίζεται το δικαίωμα άμυνας ως η μοναδική περίπτωση νόμιμης μονομερούς χρήσης βίας

[195] «The Security Council could equally decide that particular types of cyber operations amount to a threat to the peace, breach of the peace, or act of aggression in abstracto, that is, without reference to particular acts that have or are about to occur. For instance, it is within the authority of the Security Council to determine that cyber operations directed at national banking systems or critical national infrastructure qualify as such»

[196] [196] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.498

[197] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.484

[198] Το ιστορικό της υπόθεσης ξεκινάει από το 1837 με τη στρατολόγηση ορισμένων Αμερικανών στο καναδικό ναυτικό, με σκοπό τις επιθέσεις στα Βρετανικά πλοία που έπλεαν κοντά στις ακτές του Καναδά. Το συγκεκριμένο πλοίο Caroline ελλιμενίζονταν σε καναδικά λιμάνια, τα οποία αποτελούσαν ορμητήριο των Αμερικανών, οι οποίοι επιτίθονταν σε βρετανικά πλοία που περνούσαν κοντά στις καναδικές ακτές. Σε μία από αυτές τις επιθέσεις οι Βρετανοί συνέλαβαν

και με αφορμή αυτό το περιστατικό τέθηκαν οι προϋποθέσεις άσκησης του[199]. Για αρκετούς διεθνολόγους που ασχολήθηκαν με τη θεωρητική θεμελίωση του όρου της νόμιμης άμυνας η Υπόθεση Caroline αποτέλεσε ορόσημο. Σύμφωνα με το Άρθρο 51 του Χάρτη, νόμιμη άμυνα είναι το φυσικό (inherent) δικαίωμα ενός κράτους να αντιδράσει ως απάντηση σε μία ένοπλη επίθεση ενός άλλου κράτους.

Οι αρχές της νόμιμης άμυνας δεν αναφέρονται στο Χάρτη των ΗΕ αλλά εξάγονται από το Διεθνές Εθιμικό Δίκαιο. Είναι η αρχή της αμεσότητας, η αρχή της αναγκαιότητας και η αρχή της αναλογικότητας, όπως έκρινε και το ΔΔΧ στην Υπόθεση Caroline[200]. Θα προσπαθήσουμε να δώσουμε μια σύντομη ερμηνεία των αρχών αυτών, ώστε να γίνει αντιληπτό και κατανοητό το περιεχόμενο τους. Σύμφωνα με την αρχή της αναγκαιότητας, η χρήση βίας για λόγους νόμιμης άμυνας πρέπει να ασκείται μόνο στις περιπτώσεις που το θύμα της επίθεσης δεν μπορεί με άλλο μέσο να απωθήσει την επίθεση που δέχεται και κατά συνέπεια η ένοπλη βία κρίνεται επιτακτική και απαραίτητη. Ο όρος «ένοπλη επίθεση» αποτελεί την λέξη - κλειδί στον προσδιορισμό της «νόμιμης άμυνας», έτσι όπως αναφέρεται στο Άρθρο 51 του Χάρτη και η ερμηνεία αυτού καθορίζει κατά πόσο η μονομερής βία είναι επιτρεπτή. Μόνο η «ένοπλη επίθεση» μπορεί να «δικαιολογήσει» χρήση βίας στα πλαίσια την νόμιμης άμυνας. Το ΔΔΧ στην Υπόθεση Νικαράγουα κατά ΗΠΑ έκρινε ότι ένοπλη επίθεση αποτελεί η χρήση βίας, η οποία είναι τέτοιας έντασης και μεγέθους που ξεπερνά ένα απλό μεθοριακό επεισόδιο[201]. Το επόμενο ερώτημα που γεννάται είναι τι συνιστά ένοπλη επίθεση. Ο Χάρτης των Ηνωμένων Εθνών χρησιμοποιεί τους όρους επίθεση (aggression) και ένοπλη επίθεση (armed attack), χωρίς να τους οριοθετεί. Η παράνομη χρήση βίας για να θεωρηθεί ένοπλη επίθεση πρέπει να έχει τέτοια ένταση που να ξεπερνά ένα ελάχιστο «κατώφλι», σύμφωνα και με τον ορισμό της επίθεσης όπως

το προσωπικό, κατάσχεσαν το αμερικανικό πλοίο Caroline , το έκαψαν με αποτέλεσμα να σκοτωθούν δύο Αμερικανοί ναυτικοί. Ο Υπουργός Άμυνας της Βρετανίας απέστειλε επιστολή στις ΗΠΑ, σύμφωνα με την οποία ο βρετανικός στόλος βρισκόταν σε νόμιμη άμυνα , ICJ Rep. 1986, 14,347-348 $173

[200] ICJ Rep. 1986,14,103, $194

[201] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.488

αυτός υιοθετήθηκε από την Έκτη Επιτροπή τον Νοέμβριο του 1974 και στη συνέχεια από τη Γενική Συνέλευση τον Δεκέμβριο του 1974 με την Απόφαση 3314 (XXIX)[202]. Επιπλέον το ΔΔΧ στην Υπόθεση Νικαράγουα διαφοροποίησε, κάτι που επιβεβαίωσε και στην Υπόθεση Oil Platforms , την «ένοπλη επίθεση» από τις λιγότερο σοβαρές μορφές χρήσης βίας [203].

Στο Άρθρο 1 δίνεται ο γενικός ορισμός της επίθεσης σύμφωνα με τον οποίο «Επίθεση είναι η χρήση ένοπλης βίας από ένα κράτος κατά της κυριαρχίας, εδαφικής ακεραιότητας ή πολιτικής ανεξαρτησίας άλλου κράτους ή κατά οποιονδήποτε άλλο τρόπο ασυμβίβαστο με τον Χάρτη των Η.Ε. όπως θεσπίζεται στον παρόντα ορισμό».

Το Άρθρο 3 αναφέρεται στις πράξεις που αποτελούν επιθετικές ενέργειες και ορίζει ότι: «οι παρακάτω πράξεις, ανεξάρτητα από την κήρυξη πολέμου, θα χαρακτηρίζονται ως επιθετικές πράξεις, υπό τις προϋποθέσεις και τους ορισμούς του άρθρου 2». Οι πράξεις αυτές είναι α) η εισβολή ή η επίθεση από τις ένοπλες δυνάμεις ενός κράτους, του εδάφους ενός άλλου κράτους ή στρατιωτική κατοχή οποιασδήποτε μορφής καθώς και οποιαδήποτε προσάρτηση εδάφους ενός άλλου κράτους ή τμήματός του με τη χρήση βίας, β) ο βομβαρδισμός από τις ένοπλες δυνάμεις ενός κράτους κατά του εδάφους άλλου κράτους ή η χρήση όπλων κατά του εδάφους άλλου κράτους, γ) ο αποκλεισμός των λιμένων ή των ακτών ενός κράτους από τις ένοπλες δυνάμεις άλλου κράτους, δ) επίθεση από ένοπλες δυνάμεις ενός κράτους στις χερσαίες, θαλάσσιες ή εναέριες δυνάμεις ενός άλλου κράτους, ε) η χρήση των ενόπλων δυνάμεων ενός κράτους που βρίσκονται στο έδαφος ενός άλλου κράτους με την συναίνεση του τελευταίου κατά παράβαση των όρων που προβλέπονται σε σχετικές συμφωνίες ή η άρνηση απόσυρσης τους μετά την ανάκληση της συναίνεσης , στ) η άδεια ενός κράτους το οποίο έχει θέσει το έδαφός του στην διάθεση άλλου κράτους, ώστε αυτό να χρησιμοποιηθεί από το τελευταίο για την πραγματοποίηση επίθεσης κατά του τρίτου κράτους, ζ) η αποστολή στο έδαφος άλλου κράτους

[202] Twenty – Ninth Session, Supp. No 19 A/9619, Report of Special Committee, 11 Mar – 12 Apr 1974
[203] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.415

ενόπλων συμμοριών, ομάδων, ανταρτών ή μισθοφόρων, οι οποίοι διενεργούν κατά άλλου κράτους πράξεις ένοπλης βίας ανάλογες με τις προηγούμενες ή ουσιώδης ανάμειξη σε αυτές.

Η δεύτερη αρχή είναι η αρχή της αμεσότητας, σύμφωνα με την οποία η άσκηση ένοπλης αμυντικής δράσης από το κράτος που δέχεται την επίθεση πρέπει να γίνει άμεσα. Η αμεσότητα όμως είναι σχετική και κρίνεται κατά περίπτωση. Αναντίρρητα όμως η αντίδραση πρέπει να γίνεται αμέσως μόλις εκδηλωθεί η επίθεση και όχι μετά την παρέλευση μεγάλου, μη εύλογου, χρονικού διαστήματος. Άμεση λοιπόν είναι η νόμιμη άμυνα όταν η επίκληση του δικαιώματος άμυνας γίνεται άμεσα[204].

Τέλος η τρίτη αρχή εξαιρετικής σημασίας, είναι η αρχή της αναλογικότητας. Η έκταση της βίας που χρησιμοποιείται από το κράτος-θύμα πρέπει να είναι ανάλογη της δύναμης της πλευράς που επιτίθεται. Μπορεί να στρέφεται μόνο κατά στρατιωτικών στόχων σύμφωνα με τις αρχές του Ανθρωπιστικού Δικαίου[205]. Έτσι η ένταση, ο στόχος και το είδος της χρήσης βίας που χρησιμοποιείται στα πλαίσια της νόμιμης άμυνας πρέπει να είναι ανάλογα με αυτά της ένοπλης επίθεσης όπως έκρινε και το ΔΔΧ στην Υπόθεση Νικαράγουα, στην οποία έκρινε ότι τα μέτρα που είχαν λάβει οι ΗΠΑ κατά του Ιράν δεν πληρούσαν την αρχή της αναλογικότητας[206]. Διαφορετικά τα ληφθέντα μέτρα με το πρόσχημα της νόμιμης άμυνας μπορεί να θεωρηθούν αντίποινα.

Στη συνέχεια θα προσπαθήσουμε να απαντήσουμε σε ένα κρίσιμο ερώτημα που εγείρεται και αφορά τις προϋποθέσεις που πρέπει να ληφθούν υπόψη, ώστε να θεωρηθεί μια κυβερνοεπίθεση ως «ένοπλη επίθεση». Οι απόψεις σχετικά με αυτό το ζήτημα διαφοροποιούνται, ανάλογα με τα κριτήρια που θέτει κανείς, ώστε να υπαχθεί η κυβερνοεπίθεση στην κατηγορία της «ένοπλης επίθεσης» . Υποστηρίζεται από μια μερίδα αναλυτών, οι οποίοι υιοθετούν το κριτήριο του μέσου, ότι μια επίθεση που διεξάγεται στον Κυβερνοχώρο με την

[204] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.489
[205] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.416

χρήση ιών και γενικά κακόβουλου λογισμικού και προγραμμάτων σε καμία περίπτωση δεν μπορεί να θεωρηθεί «ένοπλη επίθεση», διότι οι μέθοδοι αυτοί είναι άυλης μορφής και δεν εμπίπτουν στην παραδοσιακή έννοια του όπλου[207]. Η αντικρουόμενη άποψη σε αυτή την θέση είναι ότι για να θεωρηθεί ένα αντικείμενο ή ένα σύστημα «όπλο» δεν λαμβάνεται υπόψη μόνο η κατασκευή του αλλά και ο στόχος που επιδιώκεται με την χρήση του σε συνδυασμό με τις συνέπειες που αυτό επιφέρει. Η άποψη αυτή ενισχύεται και από την Γνωμοδότηση του ΔΔΧ για τα Πυρηνικά Όπλα, το οποίο έκρινε ότι η εφαρμογή των άρθρων 2(4) και 51 του Χάρτη δεν περιορίζεται σε συγκεκριμένα όπλα αλλά ισχύει για κάθε είδους χρήσης βίας[208] . Το ΔΔΧ και στην Υπόθεση Νικαράγουα είπε ότι : «….the arming and training of the Contras as a weapon..»[209]. Την άποψη αυτή υιοθέτησε ομόφωνα και η Διεθνής Ομάδα Εμπειρογνωμόνων όπως διαφαίνεται και στο Εγχειρίδιο του Ταλίν, υποστηρίζοντας ότι το γεγονός και μόνον ότι ένας υπολογιστής (αντί για ένα πιο παραδοσιακό όπλο, οπλικό σύστημα ή πλατφόρμα) χρησιμοποιείται κατά τη διάρκεια μιας επιχείρησης στον Κυβερνοχώρο δεν έχει καμία σχέση με το εάν η πράξη αυτή συνιστά « χρήση βίας » . Στο άρθρο 13 του Εγχειριδίου αναφέρεται ότι η Διεθνής Ομάδα Εμπειρογνωμόνων κατέληξε ομόφωνα στο συμπέρασμα ότι ορισμένες πράξεις στον κυβερνοχώρο μπορεί να έχουν τέτοια ένταση, ώστε να θεωρούνται « ένοπλη επίθεση » όπως αυτή συνάγεται σαν έννοια από τον Χάρτη του ΟΗΕ. Ο κρίσιμος παράγοντας ,σύμφωνα με την πλειοψηφία της Ομάδας Εμπειρογνωμόνων, ώστε να θεωρηθεί μια επιχείρηση στον Κυβερνοχώρο ως «ένοπλη επίθεση» είναι η ένταση και τα αποτέλεσματα που αυτή επιφέρει , ανεξάρτητα από τα μέσα που χρησιμοποίηθηκαν , τα οποία πρέπει να είναι ανάλογα με αυτά που θα επέφερε μια κινητική ένοπλη επίθεση.

Σύμφωνα με το άρθρο 10 του Εγχειριδίου του Ταλίν «Μια επιχείρηση στον κυβερνοχώρο που αποτελεί απειλή ή χρήση βίας κατά της εδαφικής ακεραιότητας ή της πολιτικής ανεξαρτησίας οποιουδήποτε κράτους ή οτιδήποτε το οποίο είναι ασυμβίβαστο με τους σκοπούς των Ηνωμένων Εθνών , είναι

[207] Stevens Sh., “Internet war crime tribunals and security in an interconnected world , Transnatioanl Law and Contemporary Problems”, 2009, p.10
[208]ICJ Rep. 1996, 244 §39
[209] ICJ Rep. 1986, 118 §228

παράνομη». Οι έννοιες « χρήση βίας » και « απειλή χρήσης βίας » αναλύονται στα άρθρα 11 και 12 αντίστοιχα. Το γεγονός ότι μια επιχείρηση στον κυβερνοχώρο δεν συνιστά χρήση βίας δεν την καθιστά απαραίτητα νόμιμη σύμφωνα με το διεθνές δίκαιο. Συγκεκριμένα, μια επιχείρηση στον κυβερνοχώρο μπορεί να αποτελέσει καταστρατήγηση της αρχής της απαγόρευσης σχετικά με την παρέμβαση . Παρά το γεγονός ότι δεν ορίζεται ρητά στο Χάρτη των Ηνωμένων Εθνών, η απαγόρευση της παρέμβασης πηγάζει από την αρχή της κυρίαρχης ισότητας των μελών όπως προκύπτει στο άρθρο 2(1) του Χάρτη των Ηνωμένων Εθνών.

Εν συνεχεία κρίνεται σκόπιμο να αναφέρουμε τι συνιστά «χρήση βίας» στον Κυβερνοχώρο ,όπως προκύπτει από το άρθρο 11 του Εγχειριδίου. Σύμφωνα με αυτό : «Μια επιχείρηση στον Κυβερνοχώρο αποτελεί χρήση βίας, όταν έχει τέτοια ένταση και αποτελεσμάτα , συγκρίσιμα με άλλες πράξεις μη τελούμενες στον κυβερνοχώρο, οι οποίες αγγίζουν το επίπεδο της χρήσης βίας. Εξαιτίας της απουσίας συγκεριμένων κριτηρίων στον Χάρτη , σχετικά με το πότε μια πράξη συνιστά χρήση βίας, η Διεθνής Ομάδα Εμπειρογνωμόνων έλαβε υπόψη την απόφαση του ΔΔΧστην Υπόθεση της Νικαράγουας. Σε αυτή την περίπτωση, το ΔΔΧ έκρινε ότι για να διαπιστωθεί εάν οι συγκεκριμένες πράξεις ισοδυναμούν με « ένοπλη επίθεση » (άρθρο 13) λαμβάνεται υπόψη η ένταση και τα αποτελέσματα του. Με άλλα λόγια η Ομάδα Εμπειρογνωμόνων κατέληξε ότι για να καθοριστεί αν μια πράξη στον κυβερνοχώρο συνιστά χρήση βίας, λαμβάνονται υπόψη η ένταση και οι συνέπειες που αυτή επιφέρει. Αυτό είναι το καθοριστικής σημασίας κριτήριο. Στην παράγραφο 3 του άρθρου 11 αναφέρεται ένα παράδειγμα που δεν αποτελεί χρήση βίας. Ειδικότερα , μια επιχείρηση στον κυβερνοχώρο που δεν προκαλεί κάποια βλάβη και είναι ψυχολογικής φύσεως με αποκλειστικό σκοπό να υπονομεύσει την εμπιστοσύνη σε μια κυβέρνηση ή την οικονομία της δεν συνιστά χρήση βίας. Επιπλέον , το Διεθνές Δικαστήριο έκρινε στην υπόθεση Νικαράγουα ότι η παροχή οικονομικής βοήθειας στους αντάρτες εναντίον άλλου κράτους δεν αποτελεί χρήση βίας. Έτσι, για παράδειγμα, η χρηματοδότηση μια ομάδας ακτιβιστών για την διενέργεια επιχειρήσεων στον Κυβερνοχώρο στα πλάισια μιας εξέγερσης δεν συνιστά χρήση βίας.

Στο άρθρο 11 του Εγχειριδίου δίνεται ο ορισμός της απειλής της χρήσης βίας. Συγκεκριμένα αναφέρεται ότι : «Μια επιχείρηση στον κυβερνοχώρο ή μια επιχείρηση που επίκειται να συμβεί , συνιστά παράνομη απειλή χρήσης βίας , όταν η πράξη αυτή, εάν πραγματοποιηθεί, θα αποτελέσει παράνομη χρήση βίας». Η φράση «επιχείρηση στον κυβερνοχώρο ή μια επιχείρηση που επίκειται να συμβεί» του παρόντος άρθρου, εφαρμόζεται σε δύο περιπτώσεις. Η πρώτη είναι μια πράξη του κυβερνοχώρου που χρησιμοποιείται για να συνδεθεί η απειλή με την χρήση βίας. Αντιθέτως η δεύτερη είναι μια απειλή που μεταδίδεται με οποιοδήποτε μέσο (π.χ. δημόσιες διακηρύξεις) με σκοπό την διενέργεια πράξεων στον κυβερνοχώρο, οι οποίες θα χαρακτηριστούν ως χρήση βίας.

Επιπρόσθετα ,αν λάβει κανείς υπόψη του την ratio των διατάξεων του Χάρτη του ΟΗΕ και τις συνθήκες κάτω από τις οποίες αυτός συντάχθηκε, θα καταλάβει ότι οι συντάκτες του δεν αποσκοπούσαν στο να απαγορεύσουν τη χρήση συγκεκριμένων ειδών όπλων, αποκλείοντας κάποια άλλα. Ο σκοπός τους ήταν να διασφαλιστεί η διεθνής ειρήνη και ασφάλεια και να αποφευχθεί ένας ακόμη πόλεμος, αν αναλογιστούμε ότι μόλις είχε λήξει ο Β΄ Παγκόσμιος. Δεν εστίαζαν στο μέσο αλλά στα αποτελέσματα και τα συνέπειες που θα επέφερε η χρήση βίας, το οποίο είναι και το ζητούμενο μιας επίθεσης [210]. Επιπλέον ας αναλογιστούμε ότι την περίοδο που συντάχθηκε ο Χάρτης, οι όροι «Κυβερνοπόλεμος» και «Επιχειρήσεις στον Κυβερνοχώρο» δεν υπήρχαν καν σαν έννοιες, ώστε να συμπεριληφθούν σε αυτόν.

Σκοπός άλλωστε του άρθρου 51 είναι να παράσχει στα κράτη το δικαίωμα της αυτοάμυνας, μόνο στην περίπτωση που η επίθεση που δεχτούν έχει τέτοιο μέγεθος και ένταση, ώστε να μην αποτελεί ένα απλό μεθοριακό επεισόδιο (Υπόθεση Oil Platforms) αλλά να ξεπερνά ένα ελάχιστο «κατώφλι», σύμφωνα και με τον ορισμό της επίθεσης όπως δόθηκε από την ΓΣ με το Ψήφισμα 3314 (XXIX) και ενισχύθηκε με την Απόφαση του ΔΔΧ στην Υπόθεση Νικαράγουα ,

[210] Dinstein Y., “War, Aggression and Self-Defence”, 3rd Edition , Cambridge University Press 2003, p.103

χωρίς να δίνεται έτσι βαρύτητα στο μέσο ή τεχνική που χρησιμοποείται αλλά στις συνέπειες που τελικά επέρχονται.

Από την άλλη πλευρά, υπάρχουν ορισμένα χαρακτηριστικά των Κυβερνοεπιθέσεων, που δημιουργούν επιφυλάξεις για την υπαγωγή τους στην κατηγορία των ««ενόπλων επιθέσεων». Καταρχήν , όπως έχουμε αναφέρει και σε προηγούμενη ενότητα, είναι αρκετα δυσχερής ο εντοπισμός της πραγματικής πηγής προέλευσης μιας Κυβερνοεπίθεσης. Δεδομένου ότι ο δράστης έχει την δυνατότητα με ποικίλες τεχνικές να πράξει μια Κυβερνοεπίθεση χωρίς να αποκαλυφθεί άμεσα η ταυτότητα του(π.χ εάν είναι κρατικός φορέας ή μη κρατικός δρών), είναι δύσκολο να καταλογιστεί η ευθύνη σε συγκεκριμένο κράτος, απαραίτητη όμως προϋπόθεση για τις διατάξεις του Χάρτη που εφαρμόζονται μόνο σε διακρατικές σχέσεις [211].

Σχετικά με την δικαιοδοσία και τον καταλογισμό ευθύνης στον Κυβερνοχώρο, το άρθρο 2 του Εγχειριδίου του Ταλίν μας δίνει λύσεις και απαντά σε τυχόν ερωτήματα που εγείρονται. Σύμφωνα με αυτό : «Με την επιφύλαξη των υποχρεώσεων που απορρέουν από το Διεθνές Δίκαιο , ένα κράτος μπορεί να ασκήσει τη δικαιοδοσία του :
α) Σε πρόσωπα που διεξάγουν επιχειρήσεις στον κυβερνοχώρο στο έδαφός του (β) Σε υποδομές στον κυβερνοχώρο που βρίσκονται στο έδαφός του και γ) εκτός της επικράτειας του , σύμφωνα με το διεθνές δίκαιο. Με τον όρο « δικαιοδοσία» εννούμε την εξουσία ενός κράτους να καθορίζει, να επιβάλλει και να αποφαίνεται. Αυτή εκτείνεται σε όλα τα θέματα, συμπεριλαμβανομένων και εκείνων που είναι αστικής, ποινικής ή διοικητικής φύσεως[212]. Στη συνέχεια του άρθρου 2 αναφέρεται ότι : «Η κύρια βάση ώστε ένα κράτος να ασκήσει τη δικαιοδοσία του είναι η φυσική ή νομική παρουσία ενός προσώπου ή ενός αντικειμένου στο έδαφός του. Για παράδειγμα, σύμφωνα με την πρώτου είδους δικαιοδοσία ένα κράτος μπορεί να θεσπίζει νόμους και κανονισμούς που διέπουν τις δραστηριότητες στον κυβερνοχώρο των ατόμων, οι οποίες

[211]Ο χαρακτηρισμός του επιτιθέμενου και αν αυτός δρα ως εκπρόσωπος του κράτους ή αυτοπροσώπως ως μη κρατικός δρων και οι ευθύνες που καταλογίζονται κατά περίπτωση βλ. Stevens Sh., " Internet war crime tribunals and security in an interconnected world , Transnatioanl Law and Contemporary Problems", 2009, p.10

[212] «The term 'jurisdiction' encompasses the authority to prescribe, enforce, and adjudicate. It extends to all matters, including those that are civil, criminal, or administrative in nature».

διεξάγονται στο έδαφός του. Έχει επίσης την δυνατότητα να ρυθμίζει τις δραστηριότητες των ιδιωτικών οντοτήτων που έχουν καταχωρηθεί στη δικαιοδοσία του, αλλά που δραστηριοποιούνται στο εξωτερικό, όπως είναι οι πάροχοι των υπηρεσιών Διαδικτύου. Η φράση «Με την επιφύλαξη των υποχρεώσεων που απορρέουν από το Διεθνές Δίκαιο» περιλαμβάνει ορισμένες περιπτώσεις κατά τις οποίες το διεθνές δίκαιο μπορεί να περιορίσει αποτελεσματικά την άσκηση της δικαιοδοσίας ενός κράτους επί ορισμένων προσώπων ή αντικειμένων στο έδαφος του.

Σχετικά με την ευθύνη ενός κράτους γίνεται αναφορά στο άρθρο 6 του Εγχειριδίου. Σύμφωνα με αυτό : «Ένα κράτος φέρει διεθνή νομική ευθύνη για οποιαδήποτε επιχείρηση στον Κυβερνοχώρο που αποδίδεται σε αυτό και η οποία συνιστά παραβίαση μιας διεθνούς υποχρέωσης του» [213]. Το παρόν άρθρο βασίζεται στο εθιμικό διεθνές δίκαιο περί ευθύνης των κρατών, το οποίο σε μεγάλο βαθμό αντικατοπτρίζεται στα άρθρα της Διεθνούς Επιτροπής περί ευθύνης των κρατών. Στον τομέα του κυβερνοχώρου, μια διεθνώς παράνομη πράξη μπορεί να συνίσταται, μεταξύ άλλων, στην παραβίαση του Χάρτη των Ηνωμένων Εθνών (πχ. χρήση βίας με τεχνικές και μέσα που χρησιμοποιούνται στον κυβερνοχώρο) ή στην παραβίαση μιας υποχρέωσης που απορρέει από το Δίκαιο των Ενόπλων Συρράξεων (π.χ. μια επίθεση στον κυβερνοχώρο εναντίον αστικών στόχων), η οποία αποδίδεται στο κράτος. Η παραβίαση των κανόνων που ισχύουν σε περίοδο ειρήνης και όχι ένοπλης σύρραξης (π.χ. παραβίαση κάποιου κανόνα του Δικαίου της θάλασσας ή της αρχής της μη παρέμβασης) αποτελεί επίσης διεθνώς παράνομη πράξη και συνεπέγεται νομική ευθύνη για το κράτος στο οποίο η παράνομη πράξη θα καταλογιστεί, όπως συνάγεται από το άρθρο 6 του Εγχειριδίου. Στις περιπτώσεις όπου δράστης είναι μη κρατικός φορέας, η συμπεριφορά του μπορεί να αποδοθεί σε ένα κράτος και να δημιουργήσει διεθνή νομική ευθύνη. Το άρθρο 8 από τα Άρθρα περί κρατικής ευθύνης , η οποία επαναλαμβάνει το εθιμικό διεθνές δίκαιο, επισημαίνει ότι : « Η συμπεριφορά ενός προσώπου ή μιας ομάδας προσώπων θεωρείται πράξη ενός κράτους σύμφωνα με τους κανόνες του διεθνούς δικαίου, εάν το πρόσωπο

[213] «A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation»

ή ομάδα προσώπων στην πραγματικότητα ενεργεί σύμφωνα με τις οδηγίες του ή υπό την καθοδήγηση ή τον αποτελεσματικό έλεγχο του εν λόγω κράτους κατά την εκτέλεση της συμπεριφοράς του » . Αυτή η θέση υιοθετήθηκε και για το πεδίο του Κυβερνοχώρου. Για παράδειγμα, ένα κράτος μπορέι να συμβληθεί με μια ιδιωτική εταιρεία, ώστε η τελευταία να διεξάγει επιχειρήσεις στον κυβερνοχώρο ή με ιδιώτες προκειμένου να δράσουν εναντίον άλλων κρατών, γνωστοί ως «cyber volunteers» , όπως αναφέρεται στο Εγχειρίδιο του Ταλίν.

Στα πλαίσια των υποχρεώσεων που έχει ένα κράτος στον Κυβερνοχώρο, θα γίνει μνεία και στο άρθρο 5 του Εγχειριδίου σύμφωνα με το οποίο : «Ένα κράτος δεν θα πρέπει συνειδητά και εν γνώσει του να επιτρέπει οι υποδομές στον κυβερνοχώρο, που βρίσκονται στο έδαφός του ή υπό τον αποκλειστικό κυβερνητικό έλεγχο του, να χρησιμοποιούνται για πράξεις που δυσμενώς και παράνομα επηρεάζουν άλλα κράτη» [214]. Η αρχή της κυρίαρχης ισότητας συνεπάγεται την υποχρέωση κάθε κράτους να σέβεται την εδαφική κυριαρχία των άλλων κρατών. Όπως έκρινε και το Διεθνές Δικαστήριο , με την απόφαση του στην Υπόθεση της Νικαράγουας: « μεταξύ των ανεξάρτητων κρατών , ο σεβασμός της εδαφικής κυριαρχίας αποτελεί βασικό θεμέλιο στις διεθνείς σχέσεις». Ο κανόνας αυτός αντανακλάται και στην απόφαση του ΔΔΧ στην Υπόθεση για τα Στενά της Κέρκυρας (1949). Στην υπόθεση αυτή, το ΔΔΧ αποφάνθηκε αφενός για τον σεβασμό της εδαφικής κυριαρχίας ως θεμελιώδη βάση των διεθνών σχέσεων και αφετέρου ερμήνευσε τον σεβασμό αυτό ως την δυνατότητα που διαθέτει ένα κράτος να απαγορεύσει την άσκηση δικαιοδοσίας από τρίτο κράτος μέσα στο έδαφος του .

Σχετικά με το πόσο εφικτό είναι να καταλογιστεί ευθύνη σε ένα κράτος για επιχειρήσεις που διεξάγονται στον Κυβερνοχώρο, αναλύεται στα άρθρα 7 και 8 του Εγχειριδίου του Ταλίν. Συγκεκριμένα σύμφωνα με το άρθρο 7 : «Το γεγονός και μόνον ότι μια επιχείρηση στον κυβερνοχώρο έχει ξεκινήσει ή προέρχεται

[214] «A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States»

από υποδομές στον κυβερνοχώρο μιας κυβέρνησης δεν αποτελεί επαρκές αποδεικτικό στοιχείο, για να καταλογιστεί ευθύνη στο εν λόγω κράτος, αλλά αναμφισβήτητα είναι μια ένδειξη ότι το κράτος αυτό συνδέεται με τη συγκεκριμένη επιχείρηση . Να τονιστεί ότι ο κανόνας αυτός αφορά μόνο τις επιχειρήσεις που δρομολογούνται ή προέρχονται από κυβερνητικές υποδομές στον κυβερνοχώρο. Κατά συνέπεια το άρθρο αυτό δεν εφαρμόζεται για επιχειρήσεις στον κυβερνοχώρο που έχουν ξεκινήσει ή προέρχονται από υποδομές στον κυβερνοχώρο που δεν είναι κυβερνητικές, ακόμη και αν βρίσκονται στο έδαφος του κράτους . Εν κατακλείδι το άρθρο 7 επισημαίνει ότι το γεγονός πως μια επιχείρηση στον κυβερνοχώρο προέρχεται από τις υποδομές στον κυβερνοχώρο μιας κυβέρνησης αυτό αποτελεί απλά ένδειξη της ανάμειξης του εν λόγω κράτους σε αυτή.

Η ανωτέρω άποψη, που συνάγεται από το άρθρο 7, διατυπώνεται και στο άρθρο 8 του Εγχειριδίου σύμφωνα με το οποίο : «Το γεγονός ότι μια επιχείρηση στον κυβερνοχώρο έχει δρομολογηθεί μέσω μιας υποδομής του κυβερνοχώρου που βρίσκεται σε ένα κράτος δεν είναι επαρκές αποδεικτικό στοιχείο, ώστε να καταλογιστεί η ανωτέρω επιχείρηση στο εν λόγω κράτος». Το άρθρο αυτό αναφέρεται σε επιχειρήσεις στον κυβερνοχώρο που ξεκίνησαν από την υποδομή στον κυβερνοχώρο ενός κράτους και δρομολογούνται μέσω κυβερνητικών ή μη κυβερνητικών υποδομών στον κυβερνοχώρο ενός άλλου κράτους.

1.2 Το Δίκαιο των Ενόπλων Συρράξεων ή Το Δίκαιο του Πολέμου (Jus in Bello)

Το Δίκαιο των Ενόπλων Συρράξεων αποτελείται από ένα σύνολο κανόνων που έχουν είτε εθιμική προέλευση, αποτελούν δηλαδή διεθνές έθιμο (customary international law) , είτε συμβατική προέλευση , έχουν αποτυπωθεί δηλαδή σε διεθνείς συμβάσεις (treaty law) και ρυθμίζουν την συμπεριφορά των κρατών κατά την διάρκεια των ενόπλων συγκρούσεων. Το Δίκαιο των

Ενόπλων Συρράξεων αφορά τις ένοπλες διακρατικές συγκρούσεις, χωρίς να λαμβάνεται υποχρεωτικά υπόψη η τεχνική έννοια του όρου «πόλεμος» και χωρίς υποχρεωτικά το καθεστώς του πολέμου να αναγνωρίζεται από όλα τα κράτη που συμμετέχουν. Το Δίκαιο αυτό καλύπτει κάθε ένοπλη σύγκρουση, διεθνή και μη, ενώ σε περίπτωση κατοχής αυτό εφαρμόζεται μέχρι την ολοκλήρωση της [215]. Οι κανόνες του ΔΑΔ διαμορφώθηκαν ως αποτέλεσμα της εξισορρόπησης στρατιωτικών αναγκών και ανθρωπιστικών επιταγών και έχουν σκοπό κατά την διάρκεια μιας ένοπλης σύυραξης να προστατεύσουν τα άτομα που δεν λαμβάνουν μέρος στις εχθροπραξίες (άμαχοι) ή δεν μετέχουν πια σε αυτές (τραυματίες , ναυαγοί , ασθενείς και αιχμάλωτοι) [216]. Τα βασικά ρυθμιστικά κείμενα αποτελούν η Σύμβαση της Χάγης (1907), οι τέσσερις Συμβάσεις της Γενεύης (1949) και τα δύο Πρόσθετα σ' αυτές Πρωτόκολλα (1977). Σχετικά με την εφαρμογή του Δικαίου του Πολέμου, εφόσον αποτελεί διεθνές έθιμο, δεν έχει erga omnes χαρακτήρα συνεπώς δεν δεσμεύει όλα τα κράτη να το αποδεχθούν, εάν δεν το έχουν επικυρώσει. Η σχεδόν οικουμενική επικύρωση των τεσσάρων Συνθηκών (1949) και ο συνεχώς αυξανόμενος αριθμός των κρατών που επικυρώνουν τα Πρόσθετα Πρωτόκολλα, αποδεικνύουν την σχεδόν καθολική αποδοχή του Δικαίου σε διεθνές επίπεδο. Τέλος όλα τα κράτη μπορούν να απαιτήσουν από τα άλλα κράτη την τήρηση του εθιμικού Ανθρωπιστικού Δικαίου[217]. Το Δίκαιο των Ενοπλών Συρράξεων διακρίνεται από τρεις βασικές αρχές, την αρχή της αναλογικότητας, την αρχή της διάκρισης και την αρχή της αναγκαιότητας.

Τα μέρη στην σύρραξη δεν έχουν την απεριόριστη επιλογή στα μέρη και στις μεθόδους που θα χρησιμοποιήσουν, όπως προκύπτει και από το άρθρο 22 του Κανονισμού της Χάγης[218]. Σύμφωνα με την αρχή της αναγκαιότητας, οι στόχοι μιας επίθεσης κατά την διάρκεια μιας ένοπλης σύρραξης πρέπει βάσει της

---

[215] Χατζηκωνσταντίνου Κ , «Προσεγγίσεις στο Διεθνές Ανθρωπιστικό Δίκαιο»,Έκδ. Σιδέρης, 2010, σελ. 20

216 Μαρούδα Μ- Ντ, «Ανθρωπιστικό Δίκαιο των Ενόπλων Συρράξεων», Κεφάλαιο 17, σε συλλογικό τόμο των Κ.Μαγκλιβέρα, Κ.Αντωνόπουλου(επιμ.), Δίκαιο Διεθνούς Κοινωνίας,2011, Νομική Βιβλιοθήκη,σελ 731

[217] Χατζηκωνσταντίνου Κ, « Επτά + 1 προβλήματα για το Διεθνές Ανθρωπιστικό Δίκαιο», Εκδ. Σιδέρης, 2010, σελ. 22

[218] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ.554

φύσης τους (των εγγενών δηλαδή χαρακτηριστικών τους), της τοποθεσίας και του σκοπού που εξυπηρετούν να επιφέρουν με την ολική ή μερική καταστροφή ή εξουδετέρωση τους, ένα στρατιωτικό πλεονέκτημα [219]. Συνεπώς οι επιθέσεις σε στόχους που δεν πληρούν τις παραπάνω προϋποθέσεις δεν επιτρέπονται. Το πρόβλημα ανακύπτει, όταν αναφερόμαστε στους στόχους «διπλής χρησιμότητας», οι οποίοι εξυπηρετούν όχι μόνο στρατιωτικές αλλά και πολιτικές ανάγκες (π.χ ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας, γέφυρες). Οι στόχοι αυτοί είναι προτιμότερο λόγω της ιδιαιτερότητας τους, να μην καταστρέφονται αλλά να εξουδετερώνονται[220] . Στις κυβερνοεπιθέσεις ο στόχος δεν έχει τις περισσότερες φορές υλική μορφή, αποτελώντας συνήθως μια κρίσιμη κρατική υποδομή, η οποία στηρίζει την λειτουργία της σε ένα σύστημα δικτύου και αναμφισβήτητα αποτελεί στόχο «διπλής χρησιμότητας». Εάν η προσβολή της επιφέρει σημαντικό στρατιωτικό πλεονέκτημα, συμβάλλοντας θετικά στην τελική έκβαση μιας επίθεσης, τότε σε αυτή την περίπτωση τυγχάνει εφαρμογής η αρχή της αναγκαιότητας.

Η αρχή της διάκρισης αποτελεί μια θεμελιώδη και ουσιώδη αρχή του ΔΑΔ, σύμφωνα με το άρθρο 48 του Πρόσθετου Πρωτοκόλλου Ι του 1977 : «Προκειμένου να διασφαλιστεί ο σεβασμός και η προστασία του άμαχου πληθυσμού και των μη στρατιωτικών στόχων, τα μέρη μιας σύρραξης πρέπει να διακρίνουν μεταξύ μαχητών και άμαχου πληθυσμού και ανάμεσα στους στρατιωτικούς στόχους και αστικούς, όπως τα υλικά αγαθά που καλύπτουν τις ανάγκες των αμάχων. Επίσης οι στρατιωτικές επιχειρήσεις πρέπει να κατευθύνονται μόνο κατά στρατιωτικών στόχων [221]. Η έννοια του μαχητή προσδιορίζεται από τα Άρθρα 4 ΣΓ΄49 ΙΙΙ, 43 και 44 Π Ι΄ 77 και περιλαμβάνει τα μέλη των τακτικών Ενόπλων Δυνάμεων, οι οποίες είναι οργανωμένες δυνάμεις και μονάδες ενός μέρους σε ένοπλη σύγκρουση, οι οποίοι πρέπει να πληρούν τέσσερις προϋποθέσεις : α) να βρίσκονται υπό υπεύθυνη Διοίκηση, β)να φέρουν διακριτό έμβλημα αναγνωρίσιμο από απόσταση, γ) να φέρουν τα όπλα

[219] Χατζηκωνσταντίνου Κ :Προσεγγίσεις στο Διεθνές Ανθρωπιστικό Δίκαιο, Έκδ. Σιδέρης, Αθήνα, 1999, σελ.44
[220] Χατζηκωνσταντίνου Κ : Επτά + 1 προβλήματα για το Διεθνές Ανθρωπιστικό Δίκαιο, Έκδ. Σιδέρης, 2010, σελ.131-132
[221] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ. 545

τους φανερά , δ) να συμμορφώνονται κατά τις επιχειρήσεις τους με τους νόμους και τα έθιμα του πολέμου. Οι μαχητές κατά την σύλληψη τους αντιμετώπιζονται ως αιχμάλωτοι πολέμου, υπό την προϋπόθεση ότι δεν είναι υπήκοοι της Κατακρατούσας Δύναμης[222] , προστατεύονται από σχεδόν 100 διατάξεις και τυγχάνουν ανθρωπιστικής μεταχείρισης[223]. Από την άλλη πλευρά ο άμαχος απαγορεύεται να αποτελέσει στρατιωτικό στόχο, δεν μπορεί να λάβει μέρος στις εχθροπραξίες και αν το πράξει , χάνει την προστασία του.

Το άρθρο 20 του Εγχειριδίου του Ταλίν επεξηγεί πως οι πράξεις στον κυβερνοχώρο που πραγματοποιούνται υπό το πρίσμα μιας ένοπλης σύγκρουσης υπόκεινται στο Δίκαιο των Ενόπλων Συρράξεων, το οποίο εφαρμόζεται σε οποιαδήποτε επιχείρηση διενεργείται υπό την μορφή μιας ένοπλης σύγκρουσης. Παρά την καινοτομία των Κυβερνοπιχειρήσεων και των ιδιαίτερων χαρακτηριστικών τους, η Ομάδα Εμπειρογνωμόνων συμφώνησε ομόφωνα ότι το Δίκαιο των Ενόπλων Συρράξεων εφαρμόζεται και σε τέτοιες δραστηριότητες τόσο σε διεθνείς όσο και σε μη διεθνείς ένοπλες συγκρούσεις[224]. Ο όρος «ένοπλη σύγκρουση» στο Εγχειρίδιο αναφέρεται σε μία κατάσταση που περιλαμβάνει εχθροπραξίες, συμπεριλαμβανομένων και εκείνων που διεξάγονται με διάφορες κυβερνομεθόδους. Ο ορισμός της διεθνούς ένοπλης σύρραξης δίνεται στο άρθρο 22 του Εγχειριδίου σύμφωνα με το οποίο: «Μια διεθνής ένοπλη σύγκρουση υφίσταται, όταν υπάρχουν εχθροπραξίες, οι οποίες μπορεί να περιλαμβάνουν ή να περιορίζονται μόνο σε επιχειρήσεις στον κυβερνοχώρο μεταξύ δύο ή περισσοτέρων μερών».

Στα άρθρα 25 -29 γίνεται εκτενής αναφορά στην συμμετοχή στις ένοπλες συγκρούσεις. Ειδικότερα στο άρθρο 25 αναφέρεται ότι το Δίκαιο των Ενόπλων Συρράξεων δεν απαγορεύει σε οποιαδήποτε κατηγορία προσώπων τη συμμετοχή τους σε δραστηριότητες στον κυβερνοχώρο. Ωστόσο, οι έννομες συνέπειες της συμμετοχής διαφέρουν ανάλογα με τη φύση της ένοπλης

[222] Cassese A., Διεθνές Δίκαιο", Gutenberg, 2012, σελ.480
[223] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ. 542
[224] «The law of armed conflict applies to cyber operations as it would to any other operations undertaken in the context of an armed conflict. Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities in both international and non-international armed conflicts»

σύγκρουσης και την κατηγορία στην οποία ανήκει ένα άτομο [225]. Από τα παραπάνω συνάγεται ότι όσα ισχύουν για τους μαχητές σύμφωνα με το ΔΑΔ, ισχύουν και στον Κυβερνοπόλεμο. Πιο συγκεκριμένα στο άρθρο 26 εξηγείται πως αντιμετωπίζονται τα μέλη των Ενόπλων Δυνάμεων , τα οποία κατά την διάρκεια μιας διεθνούς ένοπλης σύγκρουσης και συγκεκριμένα όσο διεξάγονται δραστηριότητες στον Κυβερνοχώρο, δεν συμμορφώνονται με τις υποχρεώσεις που επιτάσσει το καθεστώς τους ως μαχητές. Σε αυτή την περίπτωση χάνουν την ασυλία τους και το δικαίωμα να αντιμετωπισθούν ως αιχμάλωτοι πολέμου κατά την σύλληψη τους [226]. Στην παράγραφο 4 του ανωτέρω άρθρου αναφέρεται ότι υπάρχουν δύο κατηγορίες μαχητών, αυτοί που αποτελούν μέλη των ενόπλων δυνάμεων ενός μέρους της σύγκρουσης καθώς και μέλη των παραστρατιωτικών ή εθελοντικών ομάδων σχηματίζοντας μέρος των ενόπλων δυνάμεων. Η κατηγορία αυτή περιλαμβάνει κυρίως τα μέλη των ενόπλων δυνάμεων ενός κράτους [227]. Η δεύτερη κατηγορία περιλαμβάνει τα μέλη των παραστρατιωτικών ομάδων και μέλη εθελοντικών σωμάτων, συμπεριλαμβανομένων και εκείνων των οργανωμένων κινημάτων αντίστασης , που ανήκουν σε ένα μέρος της σύγκρουσης . Η κατηγορία αυτή πρέπει να πληρεί τις τέσσερις προϋποθέσεις σύμφωνα με το άρθρο 4 της ΣΓ΄49 ΙΙΙ στο οποίο έχουμε ήδη αναφερθεί, για να θεωρούνται μαχητές. Μέλη ατάκτων δυνάμεων που πληρούν αυτές τις προϋποθέσεις και ανήκουν σε ένα μέρος της σύγκρουσης εξομοιώνονται με μαχητές και κατά την σύλληψη τους αντιμετωπίζονται ως αιχμάλωτοι πολέμου .

[225] «The law of armed conflict does not bar any category of person from participating in cyber operations. However, the legal consequences of participation differ based on the nature of the armed conflict and the category to which an individual belongs», άρθρο 25 του Εγχειριδίου του Ταλίν

[226] «In an international armed conflict, members of the armed forces of a Party to the conflict who, in the course of cyber operations, fail to comply with the requirements of combatant status lose their entitlement to combatant immunity and prisoner of war status», άρθρο 26 του Εγχειριδίου του Ταλίν

[227] «There are two categories of combatant. The first consists of “members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces”. This category primarily includes members of a State’s armed forces».

Εν συνεχεία στο άρθρο 26 προβλέπεται ότι «Σε μια διεθνή ένοπλη σύρραξη , οι κάτοικοι μιας περιοχής που δεν έχει καταληφθεί, οι οποίοι λαμβάνουν μέρος σε Κυβερνοεπιθέσεις ως μέλη levée en masse εξομοιώνονται με μαχητές και κατά την σύλληψη τους αντιμετωπίζονται ως αιχμάλωτοι πολέμου. Ως levée en masse χαρακτηρίζονται οι κάτοικοι μιας περιοχής που δεν έχει καταληφθεί, οι οποίοι στην θέα του εχθρού που πλησιάζει, παίρνουν αυθόρμητα τα όπλα για να αντισταθούν στους εισβολείς, χωρίς να έχουν τον χρόνο να σχηματίσουν τακτικές ένοπλες μονάδες. Ωστόσο η εφαρμογή της έννοιας αυτή στα πλαίσια του Κυβερνοχώρου είναι κάπως προβληματική . Ας υποθέσουμε ότι μέλη του πληθυσμού αυθόρμητα αρχίζουν να εξαπολύσουν επιχειρήσεις στον κυβερνοχώρο ως απάντηση σε μια εισβολή στην χώρας τους. Εάν οι επιχειρήσεις περιλαμβάνουν ένα μεγάλο τμήμα του πληθυσμού και εφόσον αφορούν τη δύναμη εισβολής , όσοι συμμετέχουν σε αυτές θα πληρούν τις προϋποθέσεις αναμφισβήτητα ως μέλη levée en masse. Ωστόσο, τα μέσα και οι ειδικές γνώσεις που απαιτούνται για να συμμετέχει κανείς αποτελεσματικά σε επιχειρήσεις στον κυβερνοχώρο μπορεί να είναι σχετικά περιορισμένα στον εν λόγω πληθυσμό. Αν υιοθετήσουμε την άποψη, ότι για να θεωρηθεί κάποιος μέλος levée en masse απαραίτητη προϋπόθεση είναι να υπάρχει φυσική εισβολή του εχθρού, τότε καταλήγουμε στο συμπέρασμα που αναφέρεται κ στο Εγχειρίδι, ότι ο όρος αυτός (levée en masse) δεν εφαρμόζεται στην περίπτωση του Κυβερνοπολέμου. Σύμφωνα με το άρθρο 28 του Εγχειριδίου οι μισθοφόροι που εμπλεκονται σε επιχειρήσεις στον κυβερνοχώρο δεν εξομοιώνονται με μαχητές και κατά την σύλληψη τους δεν αντιμετωπίζονται ως αιχμάλωτοι πολέμου [228]. Τέλος, στο άρθρο 29 γίνεται μνεία στους αμάχους και στην δυνατότητα που έχουν να συμμετέχουν στις Κυβερνοεπιχειρήσεις, χάνοντας όμως την προστασία τους για όσο χρονικό διάστημα συμμετέχουν σε αυτές [229].

Για την διάκριση στρατιωτικών – αστικών στόχων κρίνεται σκόπιμο να δώσουμε έναν ορισμό των στρατιωτικών στόχων. Σύμφωνα με το άρθρο 52 του Π Ι΄ 77 «στρατιωτικοί είναι οι στόχοι οι οποίοι από την φύση τους (στρατόπεδα,οχυρά), τοποθεσία, σκοπό (φορτηγό που μεταφέρει στρατιωτικό

[228] «Mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status»

[229] « Civilians are not prohibited from directly participating in cyber operations amounting to hostilities but forfeit their protection from attacks for such time as they so participate»

εξοπλισμό όπως όπλα, βόμβες) ή χρήση τους (σχολείο που χρησιμοποιείται για εκπαίδευση στρατιωτών) συμβάλλουν αποτελεσματικά στην στρατιωτική δράση και των οποίων η ολική ή μερική καταστροφή , κατάληψη ή εξουδετέρωση προσφέρει την δεδομένη χρονική στιγμή σημαντικό στρατιωτικό πλεονέκτημα[230]. Στο Κεφάλαιο ΙΙΙ του Πρόσθετου Πρωτοκόλλου Ι΄ του 1977 και συγκεκριμένα στο άρθρο 52 προβλέπεται ότι: « οι αστικοί στόχοι δεν γίνονται αντικείμενο επίθεσης ή αντιποίνων». Επιπλέον σύμφωνα με το άρθρο 52 παρ. 3 «σε περίπτωση αμφιβολίας κατά πόσο ένας στόχος ο οποίος λόγω φύσης και σκοπού δεν είναι προορισμένος να εξυπηρετεί στρατιωτικούς σκοπούς, χρησιμοποιηθεί για να ενισχύσει την στρατιωτική δράση, θεωρείται ότι δεν χρησιμοποιείται με αυτόν τον τρόπο» .

Στην περίπτωση των Κυβερνοεπιθέσεων η αναλογική εφαρμογή της αρχής της διάκρισης που ισχυεί στο ΔΑΔ συνάγεται ρητά από τα άρθρα 31 – 40 του Εγχειριδίου. Ο ορισμός των στρατιωτικών και αστικών στόχων δίνεται στο άρθρο 38 σύμφωνα με το οποίο : «Αστικοί στόχοι είναι όλα τα αντικείμενα που δεν αποτελούν στρατιωτικούς στόχους. Στρατιωτικοί είναι εκείνα τα αντικείμενα που από τη φύση τους, την τοποθεσία , το σκοπό ή τη χρήση τους, συμβάλλουν αποτελεσματικά στη στρατιωτική δράση και των οποίων η ολική ή μερική καταστροφή , κατάληψη ή εξουδετέρωση , υπό τις χρονικές περιστάσεις που ισχύουν, προσφέρει ένα σαφές στρατιωτικό πλεονέκτημα. Τέτοιοι στόχοι μπορεί να αποτελούν οι υπολογιστές, τα δίκτυα υπολογιστών και οι υποδομές στον κυβερνοχώρο». Ο όρος «στρατιωτικό πλεονέκτημα» αποσκοπεί στο να αποκλείσει το πλεονέκτημα που δεν είναι στρατιωτικής φύσεως και ειδικότερα ό,τι είναι αποκλειστικά οικονομικό, πολιτικό ή ψυχολογικό [231].

Στην πράξη όμως η εφαρμογή της αρχής αυτής παρουσιάζει δυσχέρειες, δεδομένου ότι αντικείμενο των κυβερνοεπιθέσεων αποτελούν ως επί το πλείστον οι κρίσιμες υποδομές που εντάσσονται στην κατηγορία των «στόχων διπλής χρησιμότητας», ικανοποιώντας ταυτόχρονα στρατιωτικές αλλά και αστικές ανάγκες. Για παράδειγμα ένα ενσύρματο ή ασύρματο δίκτυο

[230] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ. 551

[231] «The term 'military advantage' is meant to exclude advantage that is not military in nature. In particular, it would exclude advantage that is exclusively economic, political, or psychological»

επικοινωνίας κατά την διάρκεια μιας ένοπλης σύγκρουσης αποτελεί στρατιωτικό στόχο, εφόσον εξυπηρετεί τα μέλη του κάθε μέρους της σύρραξης να συντονίζονται μεταξύ τους, αλλά παράλληλα καλύπτει και την ανάγκη για επικοικωνία και ενημέρωση των πολιτών (μη στρατιωτική ανάγκη). Σύμφωνα με το άρθρο 39 του Εγχειριδίου «Ένα αντικείμενο που χρησιμοποιείται τόσο για πολιτικούς όσο και για στρατιωτικούς σκοπούς, συμπεριλαμβανομένων των ηλεκτρονικών των υπολογιστών, των δικτύων υπολογιστών, αποτελεί στρατιωτικό στόχο». Σκοπός αυτού του άρθρου είναι να αποσαφηνίσει το ζήτημα των αντικειμένων « διπλής χρήσης ». Οποιαδήποτε χρήση ή μελλοντική χρήση που συμβάλλει στην στρατιωτική δράση καθιστά ένα αντικείμενο στρατιωτικό στόχο. Η ιδιότητα ενός αντικειμένου ως στρατιωτικού και αστικού στόχου ταυτόχρονα δεν μπορεί να συνυπάρξει, είτε το ένα θα είναι είτε το άλλο. Αυτή η αρχή επιβεβαιώνει ότι όλα τα αντικείμενα « διπλής χρήσης» αποτελούν στρατιωτικούς στόχους σύμφωνα με το άρθρο 38 του Εγχειριδίου.

Η αρχή της αναλογικότητας διατυπώνεται με σαφήνεια στο άρθρο 51 του Πρόσθετου Πρωτοκόλλου Ι΄ του 77, σύμφωνα με το οποίο: «Απαγορεύεται μια επίθεση, η οποία αναμένεται ότι μπορεί να προκαλέσει απώλεια ζωής σε αμάχους, τραυματισμό, απώλεια στην περιουσία τους και γενικότερα απώλειες δυσανάλογα μεγαλύτερες σε σχέση με το άμεσο στρατιωτικό πλεονέκτημα που προσδοκάται.». Ωστόσο είναι αρκετά δύσκολος ο προσδιορισμός των όρων «δυσανάλογο» και «παράπλευρη απώλεια», αναφορικά με το αποτέλεσμα που επιδιώκεται [232] , διότι είναι αδύνατον να υπολογίσει κανείς εκ των προτέρων το ακριβές ύψος των ζημιών που θα προκληθούν από μια επίθεση. Αυτή η αδυναμία στάθμισης των απωλειών είναι πιο έντονη στον Κυβερνοπόλεμο, διότι όλα σχεδόν τα προγράμματα πλοήγησης εξυπηρετούν παράλληλα και ανάγκες πολιτών, δεν έχουν μόνο στρατιωτική χρήση και η στοχοποίηση τους θα στερήσει το δικαίωμα στην γνώση στους πολίτες- αμάχους. Επιπλέον πολλοί κρατικοί φορείς, νοσοκομεία και τράπεζες στηρίζουν την λειτουργία τους αποκλειστικά σε ηλεκτρονικά δίκτυα, συνεπώς οι απώλειες από μια κυβερνοεπίθεση με στόχο αυτά, θα είναι ζωτικής σημασίας .

[232] Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., Το Δίκαιο της Διεθνούς Κοινωνίας, Νομική Βιβλιοθήκη , 2011, σελ. 553

Η αρχή της αναλογικότητας διατυπώνεται στο άρθρο 51 του Εγχειριδίου του Ταλίν σύμφωνα με το οποίο «Μια επίθεση στον κυβερνοχώρο που αναμένεται να προκαλέσει απώλειες ζωών, τραυματισμό αμάχων, ζημία σε αντικείμενα ή συνδυασμό αυτών, τα οποία θα ήταν υπέρμετρα δυσανάλογα σε σχέση με το συγκεκριμένο και άμεσο στρατιωτικό πλεονέκτημα που προσδοκάται απαγορεύεται». Ένα παράδειγμα εφαρμογής αυτού του άρθρου είναι η περίπτωση μιας κυβερνοεπίθεσης στο Παγκόσμιο Σύστημα Εντοπισμού Θέσης, ο οποίος ως «διπλής χρήσης» αντικείμενο αποτελεί και στρατιωτικό στόχο. Ωστόσο στερώντας από τους χρήστες βασικές πληροφορίες, όπως δεδομένα πλοήγησης είναι πιθανό να προκληθεί βλάβη , για παράδειγμα , σε εμπορικά πλοία και αεροσκάφη της πολιτικής αεροπορίας που βασίζονται στο Παγκόσμιο Σύστημα Εντοπισμού Θέσης . Εάν αυτή η αναμενόμενη ζημία είναι υπέρμετρα δυσανάλογη σε σχέση με το αναμενόμενο στρατιωτικό πλεονέκτημα της επιχείρησης, η πράξη απαγορεύεται. Στην περίπτωση όμως του Κυβερνοπολέμου η δυνατότητα υπολογισμού των απωλειών που θα επιφέρει είναι αρκετά περιορισμένη, δεδομένης της ποιοτικής αλλά και ποσοτικής. αβεβαιότητας , ωστόσο πρέπει να καταβάλλεται κάθε δυνατή προσπάθεια για την εκτίμηση και πρόβλεψη των επιπτώσεων που θα επιφέρει μια Κυβερνοεπιθέση.

Συμπερασματικά και λαμβάνοντας υπόψη όλα τα παραπάνω, κρίνεται σκόπιμο να αναφερθούμε στους προβληματισμούς που εγείρονται σχετικά με την αναλογική εφαρμογή του Δικαίου των Ενόπλων Συρράξεων στον Κυβερνοπόλεμο. Δεδομένου ότι το ΔΑΔ εφαρμόζεται μόνο κατά την διάρκεια ενόπλων συγκρούσεων, θεωρούμε ότι και οι επιχειρήσεις στον Κυβερνοχώρο υπάγονται στην κατηγορία των ενόπλων συγκρούσεων. Αυτό αναφέρεται ρητά και στο άρθρο 20 του Εγχειριδίου σύμφωνα με το οποίο «Πράξεις στον κυβερνοχώρο που εκτελούνται στο πλαίσιο της ένοπλης σύγκρουσης υπόκεινται στο Δίκαιο των Ενοπλων Συγκρούσεων». Ένα βασικό ζήτημα που ανακύπτει, το οποίο αναφέραμε και σε προηγούμενη ενότητα, είναι η ταυτότητα του δράστη στον Κυβερνοπόλεμο, δεδομένης της ανωνυμίας που διακρίνει όσους συμμετέχουν σε αυτόν. Για την εφαρμογή του ΔΑΔ είναι απαραίτητο να

γνωρίζουμε τα μέρη που λαμβάνουν μέρος στις ένοπλες συρράξεις και καλούνται να το εφαρμόσουν. Κάτι τέτοιο όμως δεν είναι πρακτικά εφικτό στις Κυβερνοεπιθέσεις, όπου οι δράστες με ποικίλες τεχνικές και μεθόδους καταφέρνουν να καταστήσουν δύσκολο τον εντοπισμό τους. Ένα δεύτερο ζήτημα που ανακύπτει και έχουμε ήδη αναφέρει παραπάνω, είναι η διάκριση στρατιωτικών και αστικών στόχων και κατά πόσο αυτή μπορεί να εφαρμοστεί στην πράξη. Στο ΔΑΔ είναι εφικτή αυτή η διάκριση, εν αντιθέσει με τον Κυβερνοχώρο, όπου όλα τα δίκτυα ικανοποιούν κυρίως «υποδομές κοινής ωφελείας» (εργοστάσια παραγωής και μεταφορά ηλεκτρικής ενέργειας, δίκτυα μέσωνμεταφοράς, επικοικωνιακά και πληροφοριακά δίκτυα) με αποτέλεσμα να εξυπηρετούνται ταυτόχρονα όχι μόνο στρατιωτικοί σκοποί αλλά και βασικές ανάγκες των πολτιών.

2. Εγχειρίδιο του Ταλίν

Στο σημείο αυτό, έχοντας ήδη επικαλεστεί στην παρούσα εργασία αρκετά άρθρα του Εγχειριδίου του Ταλίν, κρίνεται σκόπιμο να αναφερθούμε εν συντομία στη νομική φύση αυτού του εγχειρήματος και στις συνθήκες κάτω από τις οποίες αυτό συντάχθηκε. Ειδικότερα, τον Μάρτιο του 2013, η University Press Cambridge δημοσίευσε το εν λόγω Εγχειρίδιο , το οποίο ουσιαστικά διερευνά τη δυνατότητα αναλογικής εφαρμογής του ισχύοντος διεθνούς δικαίου, του δικαίου της χρήσης βίας (jus ad bellum) και του ανθρωπιστικού δικαίου (jus in bello) στον Κυβερνοπόλεμο. Το εκπόνημα αυτό ήταν αποτέλεσμα συλλογικής εργασίας τριών ετών μιας ομάδας ειδικών με επικεφαλή τον καθηγητή Michael Schmitt από την Ναυτική Σχολή Πολέμου των Ηνωμένων Εθνών, το οποίο τους ανατέθηκε από το Κέντρο CCD-CoE (Cooperative Cyber Defense Center of Excellence) [233]. Δεν είναι νομικά δεσμευτικό κείμενο αλλά μια συνολική προσωπική αποτίμηση και απόρροια των ακαδημαϊκών γνώσεων μιας ομάδας ανεξάρτητων εμπειρογνωμόνων που ενεργούν μόνον υπό την προσωπική τους ιδιότητα [234]. Πρόκειται για ένα σύνολο 95 κανόνων, οι οποίοι προσπαθούν να

[233] https://ccdcoe.org/research.html

[234] https://ccdcoe.org/research.html

ρυθμίσουν όλες τις προβληματικές πτυχές του Κυβερνοπολέμου και τα ζητήματα Διεθνούς Δικαίου που ανακύπτουν από αυτόν.

3. Αντιμετώπιση του Κυβερνοεγκλήματος από τους Διεθνείς Οργανισμούς

3. 1 Συμβούλιο της Ευρώπης

Το Συμβούλιο της Ευρώπης δεδομένης της συνεχόμενης αύξησης των Κυβερνοεπιθέσεων σε διεθνές επίπεδο αφυπνίστηκε, συνάπτοντας στις 23/11/2001 Σύμβαση για το Κυβερνοέγκλημα [235]. Πρόκειται για την πρώτη διεθνής συνθήκη νομικά δεσμευτική για εγκλήματα που διαπράττονται μέσω του Διαδικτύου και γενικά στον Κυβερνοχώρο Η συγκεκριμένη Σύμβαση αποτελείται από διατάξεις με σκοπό την υιοθέτηση μιας κοινής εγκληματικής πολιτικής με σκοπό την προστασία της κοινωνίας και την επίτευξη αρμονικής διακρατικής συνεργασίας για την αντιμετώπιση των κινδύνων που ελλοχεύουν στον Κυβερνοχώρο. Αντικείμενο της συνθήκης αποτελούν τα εγκλήματα που ασχολούνται κυρίως με τις παραβιάσεις των δικαιωμάτων πνευματικής ιδιοκτησίας, απάτες σχετίζονται με ηλεκτρονικούς υπολογιστές, παιδική πορνογραφία και οι παραβιάσεις της ασφάλειας των δικτύων [236]. Για την αποτελσματικότερη εφαρμογή της συνθήκης απαιτείται αναμφίβολα καλή συνεργασία μεταξύ των κρατών, ώστε να εναρμονίζεται η εθνική έννομη τάξη κάθε κράτους με ομοιόφορφο τρόπο.

---

[235] Είναι γνωστή και ως Συνθήκη της Βουδαπέστης, διότι υπογράφτηκε στην πόλη αυτή από 26 χώρες κράτη- μέλη του Συμβουλίου της Ευρώπης (Αλβανία, Αρμενία, Αυστρία, Βέλγιο, Βουλγαρία, Γαλλία, Γερμανία Κροατία, Κύπρος, Εσθονία, Ελλάδα,Ελβετία,Ηνωμένο Βασίλειο, Ιταλία, Ισπανία,Ουγγαρία, Νορβγηία, Πολωνία, Πορτογαλία, Ρουμανία, Σουηδία, Ουκρανία, πρώην Γιουγκοσλαβική Μακεδονία της Δημοκρατίας, Φιλανδία και 4 χώρες παρατηρητές (ΗΠΑ, Ιαπωνία, Καναδάς, Νότιος Αφρική)

[236] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

3.2 Ευρωπαϊκή Ένωση

Σχεδόν όλες οι Ευρωπαϊκές χώρες στηρίζουν πλέον την ανάπτυξη τους στα ηλεκτρονικά συστήματα και δίκτυα. Η συνεχώς αυξανόμενη τεχνολογική ανάπτυξη είχε ως επακόλουθο την αύξηση των εγκληματικών κρουσμάτων στον Κυβερνοχώρο, με αποτέλεσμα η Ευρωπαϊκή Ένωση να προβεί στην λήψη προληπτικών και κατασταλτικών μέτρων. Συγκεκριμένα προχώρησε στην θέσπιση νομοθετικών πράξεων στα πλαίσια της στρατηγικής που υιοθέτησε για την ασφάλεια στον κυβερνοχώρο και την καταπολέμηση του κυβερνοεγκλήματος.

Τα είδη του κυβερνοεγκλήματος περιλαμβάνουν διάφορες εγκληματικές πράξεις, όπως οι επιθέσεις κατά των πληροφοριακών συστημάτων μέσω πλαστών ιστοσελίδων τραπεζών για να αποκτήσουν τους κωδικούς πρόσβασης σε τραπεζικούς λογαριασμούς των θυμάτων, η ηλεκτρονική απάτη και η πλαστογραφία[237]. Ορισμένες από τις νομοθετικές πράξεις της ΕΕ που συμβάλλουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι οι εξής: α) Το 2013 η οδηγία για τις επιθέσεις κατά των πληροφοριακών συστημάτων , η οποία έχει ως στόχο να αντιμετωπίσει μεγάλης κλίμακας κυβερνο-επιθέσεις, σε συνεργασία με τα κράτη μέλη τα οποία καλούνται να ενισχύσουν τις εθνικές τους νομοθεσίες για το έγκλημα στον κυβερνοχώρο και να εισαγάγουν αυστηρότερες ποινικές κυρώσεις[238], β) Το 2011 την οδηγία για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών στο διαδίκτυο και της παιδικής πορνογραφίας και της αποπλάνησης (παραβάτες που θέτουν τα παιδιά για να δελεάσουν ανηλίκους με σκοπό την σεξουαλική κακοποίηση)[239], γ) Το 2002 η Οδηγία προστασίας της ιδιωτικής ζωής, σύμφωνα με την οποία οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλουν να διασφαλίζουν την ασφάλεια των υπηρεσιών τους και να διατηρούν την

[237] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

[238] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

[239] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093

εμπιστευτικότητα των πληροφοριών των πελατών [240], δ) Το 2001 Απόφαση-πλαίσιο για την καταπολέμηση της απάτης και της πλαστογραφίας των μη μετρητών μέσων πληρωμής, η οποία καθορίζει τις δόλιες συμπεριφορές τις οποίες τα μέλη της ΕΕ χρειάζεται να αντιμετωπίσουν ως ποινικά αδικήματα που πρέπειι να τιμωρούνται [241].

Το Ευρωπαϊκό Κέντρο για εγκλήματα στον κυβερνοχώρο (EC3) άρχισε τις δραστηριότητές της τον Ιανουάριο του 2013. Η ίδρυση του Κέντρου πραγματοποιήθηκε στα πλαίσια της Στρατηγικής που υιοθέτησε η ΕΕ για την εσωτερική της ασφάλεια. Το EC3 τοποθετήθηκε εντός της Europol [242], διότι έτσι θα ήταν σε θέση να αντλήσει όχι μόνο από την υφιστάμενη ικανότητα επιβολής του νόμου της Europol , αλλά και να διευρύνει σημαντικά τις άλλες δυνατότητες, ιδίως την επιχειρησιακή και αναλυτική υποστήριξη στις έρευνες των κρατών μελών. Οι τομείς στους οποίους δραστηροποιείται το κέντρο είναι οι εξής [243]:

I) Εγκλήματα στον κυβερνοχώρο που διαπράττονται από οργανωμένες ομάδες, ιδιαίτερα όταν αυτά επιφέρουν μεγάλη κέρδη στους δράστες τους (π.χ ηλεκτρονική απάτη)

II) Εγκλήματα στον κυβερνοχώρο που προκαλούν σοβαρή βλάβη στο θύμα, όπως η σεξουαλική εκμετάλλευση των παιδιών

III) Εγκλήματα στον κυβερνοχώρο κατά των κρίσιμων υποδομών και των πληροφοριακών συστημάτων της Ε.Ε.

Ο ρόλος του EC3 στους παραπάνω τομείς είναι ο εξής:

I) Λειτουργεί ως κεντρικός κόμβος για ποινικές πληροφορίες και στοιχεία

II) Δημιουργεί μια ολοκληρωμένη λειτουργία προβολής συνδέοντας το έγκλημα στον κυβερνοχώρο αναφορικά με τις αρχές επιβολής του νόμου με τον ιδιωτικό τομέα και τα πανεπιστήμια

---

[240] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF
[241] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413
[242] Η Europol λειτουργεί μέσα σε ένα πλαίσιο αποτελούμενο από ομάδες ανάλυσης που ονομάζονται εστιακά σημεία (FP)
[243] https://www.europol.europa.eu/ec3

III) Υποστηρίζει την κατάρτιση και την ανάπτυξη ικανοτήτων , ιδίως για τις αρμόδιες αρχές των κρατών μελών

IV) Παρέχει εξαιρετικά εξειδικευμένη τεχνική και εγκληματολογική υποστήριξη ψηφιακών ικανοτήτων για την διεξαγωγή ερευνών και επιχειρήσεων

V) Παρέχει μια ποικιλία στρατηγικών προϊόντων ανάλυσης που επιτρέπουν τεκμηριωμένη λήψη αποφάσεων σε τακτικό και στρατηγικό επίπεδο, αναφορικά με την καταπολέμηση και την πρόληψη της εγκληματικότητας στον κυβερνοχώρο

VI) Εκπροσωπεί την Ευρωπαϊκή κοινότητα επιβολής του νόμου σε τομείς κοινού ενδιαφέροντος (π.χ Αναπτυξιακή Πολιτική και Διακυβέρνηση του Διαδικτύου).

Επιπλέον το EC3 παρέχει στα κράτη μέλη της ΕΕ υπηρεσίες λειτουργικής υποστήριξης και προηγμένης τεχνικής, αναλυτικής και ψηφιακής εξειδίκευσης σε θέματα ερευνών για εγκλήματα που τελούνται στον Κυβερνοχώρο. Στους διεθνείς εταίρους- συνεργάτες, όπως η Eurojust [244] και η Ιντερπόλ [245] και άλλες υπηρεσίες επιβολής του νόμου από χώρες εκτός της Ευρωπαϊκής Ένωσης, όπως το FBI [246] ή η Αμερικανική υπηρεσία μετανάστευσης και τελωνείων εκτέλεσης(ICE)[247]. Η συνεργασία αυτή έχει ως στόχο να αποφεύγεται η επικάλυψη των προσπαθειών μεταξύ εκείνων που εμπλέκονται στις έρευνες του εγκλήματος στον κυβερνοχώρο [248].

Για την ενίσχυση του αγώνα κατά των εγκλημάτων στον Κυβερνοχώρο, στον οποίο λόγω της απουσίας γεωγραφικών ορίων καθίσταται δυσχερέστερος ο εντοπισμός των δραστών και ανεξάρτητα από εθνικά σύνορα ή δικαιοδοσίες, η Ευρωπαϊκή Ένωση εγκαινίασε ένα καινούργιο εκπόνημα το J-CAT (Joint Cybercrime Action Taskforce) , την γνωστή ως Κοινή Δράση ειδικής ομάδας για το έγκλημα στον κυβερνοχώρο, η οποία φιλοξενείται στο EC3. Το έργο αυτό

[244] http://www.eurojust.europa.eu/Pages/home.aspx
[245] http://www.interpol.int
[246] Το FBI διερευνά εγκλήματα και υψηλής τεχνολογίας όπως η Κυβερνοκατασκοπεία, οι παράνομες εισβολές σε δίκτυα, οι απάτες στο Διαδίκτυο, συνεργαζόμενο με παγκόσμιους δημόσιους και ιδωτικούς οργανισμούς (https://www.fbi.gov/about-us/investigate/cyber)
[247] https://www.ice.gov/
[248] https://www.europol.europa.eu/ec3/cyber-operations

ξεκίνησε δοκιμαστικά για έξι μήνες και αποτελείται από αξιωματικούς που ασχολούνται με ζητήματα Κυβερνοεπιθέσεων προερχόμενοι από διάφορα κράτη μέλη της ΕΕ (Αυστρία, Γαλλία, Γερμανία, Ηνωμένο Βασίλειο , Ιταλία και Ισπανία) αλλά και άλλες χώρες εκτός Ε.Ε όπως η Κολομβία, Αυστραλία, ο Καναδάς και οι ΗΠΑ).

Στόχος του J-CAT είναι να συμβάλλει στην συντονισμένη δράση κατά του εγκλήματος στον κυβερνοχώρο και των υφιστάμενων απειλών. Το αντικείμενο στο οποίο δραστηριοποιείται είναι τα εγκλήματα υψηλής τεχνολογίας (όπως το κακόβουλο λογισμικό, τα botnets και η διείσδυση), το ξέπλυμα χρήματος, συμπεριλαμβανομένων και των εικονικών νομισμάτων, ηλεκτρονική απάτη (συστήματα online πληρωμών) και οι διάφορες πτυχές της σεξουαλικής εκμετάλλευσης και αποπλάνησης παιδιών στο χώρο του Διαδίκτυου. Για να είναι πιο αποτελεσματική επιλέγει και ιεραρχεί τις περιπτώσεις με τις οποίες θα ασχοληθεί. Τα μέλη της ειδικής ομάδας συλλέγουν τις απαραίτητες πληροφορίες μέχρι να αναπτύξουν το σχέδιο δράσης τους συνεργαζόμενοι και με δικαστικούς φορείς στο τέλος [249].

Το EC3 χαρακτηρίζεται από ένα ευρύ φάσμα δραστηριοτήτων, το οποίο περιλαμβάνει δελτία τύπου τα οποία εστιάζουν σε δραστηριότητες και τις συμφωνίες συνεργασίας [250], ενώ παρέχουν και οπτικοακουστικό υλικό σχετικά με το Κυβερνοέγκλημα και την πρόληψη του όσο αυτό είναι εφικτό [251] .

Η Ευρωπαϊκή Ένωση ίδρυσε το 2004 έναν οργανισμό με την ονομασία European Network in Information Security Agency – ENISA) - Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών, στην Κρήτη. Ο ENISA τέθηκε σε λειτουργία μετά την έκδοση του κανονισμού (ΕΚ) 460/2004[252] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαρτίου 2004. Ο νέος βασικός κανονισμός του ENISA είναι ο Κανονισμός (ΕΕ) 526/2013[253] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, ο οποίος κατήργησε τον κανονισμό (ΕΚ) 460/2004.

[249] https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat
[250] https://www.europol.europa.eu/category/press-release-category/ec3
[251] https://www.europol.europa.eu/content/page/crime-prevention-advices-129
[252] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
[253] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

Ο Οργανισμός αυτός αποτελεί την απάντηση της ΕΕ στα θέματα ασφάλειας στον Κυβερνοχώρο της Ευρωπαϊκής Ένωσης καθώς και ένα κέντρο εξειδικευμένης γνώσης. Τα λειτουργικά δίκτυα συμβάλλουν στην ομαλή λειτουργία της εσωτερικής αγοράς, και συγκεκριμένα επηρεάζουν την καθημερινή ζωή των πολιτών και των επιχειρήσεων, που χρησιμοποιούν ευρυζωνικές υπηρεσίες, ηλεκτρονικές τραπεζικές συναλλαγές, το ηλεκτρονικό εμπόριο. Στόχος του είναι η επίτευξη ενός υψηλού και αποτελεσματικού επιπέδου ασφάλειας δικτύων και πληροφοριών εντός της Ευρωπαϊκής Ένωσης. Σε συνεργασία με τα όργανα της ΕΕ και τα κράτη μέλη, ο Οργανισμός επιδιώκει να μεγιστοποιήσει την ασφάλεια των δικτύων και των πληροφοριών προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των οργανισμών του δημόσιου τομέα στην Ευρωπαϊκή Ένωση. Επιπλέον επικουρεί την Ευρωπαϊκή Επιτροπή στις τεχνικές προπαρασκευαστικές εργασίες ενημέρωσης και ανάπτυξης της κοινοτικής νομοθεσίας στον τομέα της ασφάλειας δικτύων και πληροφοριών. Επίσης βοηθάει τα κράτη- μέλη και την επιχειρηματική κοινότητα με την χρήση του διαλόγου στην πρόληψη αλλά και στην επίλυση προβλημάτων που σχετίζονται με την ασφάλεια σε προϊόντα λογισμικού και υλικού[254].

Αναφορικά με την δράση του Οργανισμού, οι δραστηριότητες του συνίστανται στην παροχή συμβουλών και συστάσεων, καθώς και στη στήριξη των δραστηριοτήτων ευαισθητοποίησης και συνεργασίας με τους φορείς της ΕΕ και των κρατών μελών. Επιπλέον είναι αρμόδιος για την συλλογή και την ανάλυση δεδομένων αναφορικά με περιστατικά ασφάλειας στην Ευρώπη και αναδυόμενους κινδύνους[255]. Με βάση τις εθνικές και τις κοινοτικές προσπάθειες, ο Οργανισμός αποτελεί Κέντρο Τεχνογνωσίας σε αυτόν τον τομέα. Ο ENISA επιπλέον προσπαθεί να ενισχύσει τη συνεργασία και αλληλεπίδραση μεταξύ των δρώντων τόσο του δημοσίου όσο και του ιδιωτικού τομέα. Μεταξύ άλλων, ο Οργανισμός ακολουθεί την ανάπτυξη των προτύπων, προωθεί δραστηριότητες εκτίμησης και διαχείρισης κινδύνων από τα κράτη

[254] https://www.enisa.europa.eu/about-enisa
[255] https://www.enisa.europa.eu/about-enisa/activities

μέλη και εκπονεί μελέτες για τα θέματα αυτά στο πλαίσιο των οργανισμών του δημόσιου και του ιδιωτικού τομέα [256].

3.3 NATO

Η Συμμαχία στα πλαίσια της αυξανόμενης τεχνολογικής ανάπτυξης και για να αντιμετωπίσει το ευρύ φάσμα απειλών και κινδύνων που ελλοχεύουν στον Κυβερνοχώρο, προχώρησε στην λήψη ορισμένων μέτρων. Το NATO υιοθέτησε για πρώτη φορά την αμυντική της πολιτική στον Κυβερνοχώρο, τον Ιανουάριο του 2008 μετά τις κυβερνοεπιθέσεις εναντίον της Εσθονίας [257] . Η ίδρυση του Κέντρου CCD-CoE (Cooperative Cyber Defense Center of Excellence) στο Ταλίν ήταν απόρροια των γεγονότων που συνέβησαν στην Εσθονία το 2007 και μια έκφανση της αμυντικής πολιτικής που προαναφέραμε. Η ιδέα για την δημιουργία του κέντρου προήλθε από την Εσθονία το 2004, μετά την ένταξη της στη Συμμαχία. Το 2006 η ιδέα εγκρίθηκε και το 2007 ξεκίνησαν οι διαπραγματεύσεις με αποτέλεσμα στις 28 Οκτωβρίου 2008 να ενεργοποιηθεί το κέντρο για πρώτη φορά στην Εσθονία, με απόφαση του Βορειοατλαντικού Συμβουλίου. Ιδρύθηκε από τα εξής κράτη: την Εσθονία, Σλοβακία, τη Λιθουανία, τη Λετονία, την Ισπανία, τη Γερμανία και την Ιταλία, οι οποίες υπέγραψαν το Μνημόνιο Συνεννόησης στις 14 Μαΐου 2008 με το Διοικητή του Allied Command Transformation (ACT), τον έναν από τους δύο Διοικητές του NATO. Πρόκειται για μια διαπιστευμένη διεθνή στρατιωτική οργάνωση, με σκοπό να ενισχύσει τις αμυντικές δυνατότητες των κρατών-μελών του NATO στον κυβερνοχώρο, βελτιώνοντας έτσι τη διαλειτουργικότητα της Συμμαχίας στον τομέα της άμυνας στον Κυβερνοχώρο [258]. Τα Centres of Excellence (COEs) είναι εθνικά ή πολυεθνικά χρηματοδοτούμενα ιδρύματα τα οποία εκπαιδεύουν τους ηγέτες και άλλους ειδικούς από χώρες – μέλη της Συμμαχίας. Προσφέρουν τεχνογνωσία και εμπειρία, ενισχύοντας με αυτό τον τρόπο το NATO στην άσκηση της αμυντικής πολτικής που έχει χαράξει τα τελευταία χρόνια.

Ερχόμενοι στην πιο πρόσφατη επικαιρότητα, το NATO σύναψε ένα Μνημόνιο Συμφωνίας για ζητήματα άμυνας στον Κυβερνοχώρο,τα ο οποίο υπογράφτηκε

[256] https://www.enisa.europa.eu/about-enisa/activities/mission
[257] http://www.nato.int/cps/en/natohq/topics_78170.htm
[258] https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html

στις 12 Οκτωβρίου 2015 μεταξύ της Συμμαχίας εκπροσωπούμενη από τον Βοηθό του Γενικού Γραμματέα και Πρέσβη Sorin Ducaru, ως Προέδρος του Cyber Defence Management Board (CDMB), και την Τσεχική Δημοκρατία, εκπροσωπούμενη από τον Μηχανικό Dušan Navrátil, τον διευθυντή της Τσεχικής Εθνικής Υπηρεσίας Ασφάλειας. Το μνημόνιο έχει ως στόχο να ενισχύσει την άμυνα στον Κυβερνοχώρο και την συνεργασία μεταξύ του ΝΑΤΟ και των εθνικών αρχών που ασχολούνται με ζητήματα Κυβερνοάμυνας. Ο Πρέσβης Ducaru δήλωσε ότι « είμαστε ευτυχείς που η Τσεχική Δημοκρατία έδρασε άμεσα, ώστε να ολοκληρωθεί το Μνημόνιο Συμφωνίας με το ΝΑΤΟ. Ένα τέτοιο εγχείρημα αποτελεί σημαντικό εργαλείο για την Συμμαχία και τα μέλη της προκειμένου να διασφαλιστεί καλύτερη προστασία των δικτύων " [259]. Εν κατακλείδι το Μνημόνιο αυτό Συμφωνίας που υπογράφτηκε, αντικατοπτρίζει την ενισχυμένη πολιτική του ΝΑΤΟ για την Κυβερνοάμυνα και το σχέδιο δράσης που έχει αναπτύξει, το οποίο εγκρίθηκε από τους Συμμάχους στη Σύνοδο Κορυφής της Ουαλίας το 2014.

Αναφορικά με την πολιτική του ΝΑΤΟ, αυτή αποτελεί μέρος του συνολικά επιδιωκόμενου έργου της Συμμαχίας για συλλογική άμυνα, επιβεβαιώνοντας ότι το Διεθνές Δίκαιο εφαρμόζεται και στον Κυβερνοχώρο. Αποστολή της πολιτικής αυτής είναι να ενισχύσει τη συνεργασία του ΝΑΤΟ με τον τομέα της βιομηχανίας ενώ περιλαμβάνει και θέματα όπως την ενσωμάτωση της Κυβερνοάμυνας στον επιχειρησιακό σχεδιασμό[260]. Τα μέλη της Συμμαχίας έχουν δεσμευθεί να προωθήσουν την ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή στην πρόληψη αλλά και καταστολή των Κυβερνοεπιθέσεων. Η νέα πολιτική συμπληρώνεται από ένα σχέδιο δράσης με συγκεκριμένους στόχους και χρονοδιαγράμματα υλοποίησης[261].

Το ΝΑΤΟ εκτός από την προστασία των συστημάτων επικοινωνιών και πληροφοριών (CIS), που ανήκουν και λειτουργούν από αυτό, προσπαθεί να προστατεύσει τις κρίσιμες εθνικές υποδομές και τα εθνικά δίκτυα των κρατών-μελών του, τα οποία χρησιμοποιούνται στις αποστολές της Συμμαχίας. Για το λόγο αυτό, συνεργάζεται με τις εθνικές αρχές για την ανάπτυξη των

[259] http://www.nato.int/cps/en/natohq/news_123857.htm
[260] http://www.nato.int/cps/en/natohq/topics_78170.htm

απαραίτητων μηχανισμών, με σκοπό την διασφάλιση ενός κατάλληλου επιπέδου άμυνας στον κυβερνοχώρο. Επιπλέον συνδράμει τις χώρες-μέλη του έτσι ώστε να προστατεύσουν τις δικές τους υποδομές ζωτικής σημασίας με την ανταλλαγή πληροφοριών και πρακτικών, καθώς και με τη διεξαγωγή αμυντικών ασκήσεων στον Κυβερνοχώρο, με σκοπό την ανάπτυξη της εθνικής εμπειρογνωμοσύνης[262].

Στα πλαίσια της ενίσχυσης της δυναμικότητας στην Κυβερνοάμυνα, δημιουργήθηκε το NATO Computer Incident Response Capability (NCIRC) – Κλιμάκιο Υπολογιστών του NATO για την αντιμετώπιση περιστατικών, το οποίο προστατεύει τα ηλεκτρονικά δίκτυα της Συμμαχίας με την αδιάλλειπτη παροχή κεντρικής υποστήριξης στην Κυβερνοάμυνα σε διάφορες τοποθεσίες του NATO. Επιπλέον οργανώνει την διεξαγωγή τακτικών ασκήσεων, όπως την ετήσια άσκηση γνωστή ως Cyber Coalition η οποία ενσωματώσει τα στοιχεία και τις εκτιμήσεις για την Κυβερνοάμυνα σε όλο το φάσμα των ασκήσεων της Συμμαχίας. Η ίδρυση της Σχολής του NATO για Συστήματα Επικοινωνιών και Πληροφοριών (NCISS) αποβλέπει στην άρτια κατάρτιση και εκπαίδευση του προσωπικού που ασχολείται τόσο με την Δομή και Διοίκηση του NATO (NATO Command Structure) όσο και με την Δομή και Δύναμη του NATO (NATO Force Structure), με σκοπό την αποτελσματικότερη και αποδοτικότερη διαχείριση και διοιίκηση των Συστημάτων Επικοινωνιών και Πληροφοριών (CIS)[263]. Επιπλέον η Σχολή του NATO στο Oberammergau της Γερμανίας, προσφέρει γνώσεις για την την καλύτερη κατανόηση της οργάνωσης, των αναγκών των Ειδικών Επιχειρήσεων και την ευρύτερη στρατηγική και πολιτική που ακολουθεί η Συμμαχία[264]. Όλα τα παραπάνω καθιστούν σαφές ότι τα ζητήματα ασφάλειας στην Κυβερνοάμυνα και οι υπάρχουσες απειλές στον Κυβερνοχώρο αποτελούν άμεση προτεραιότητα της Συμμαχίας.

4. Τρόποι Αντιμετώπισης του Φαινομένου από τις Ελληνικές Ένοπλές Δυνάμεις

[262] http://www.nato.int/cps/en/natohq/topics_78170.htm
[263] http://www.nciss.nato.int/mission.php
[264] http://www.natoschool.nato.int/

Η ραγδαία και συνεχώς μεταβαλλόμενη ανάπτυξη της τεχνολογίας έχει επηρεάσει και τον χώρο των Ενόπλων Δυνάμεων, οι οποίες όπως είναι φυσικό επιδιώκουν την επικράτηση στον Κυβερνοχώρο (cyber domain), ως κριτήριο πολεμικής ισχύος ενός κράτους. 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 έναντι των αντιπάλων του. Αυτή η μεταβολλόμενη κατάσταση στο τομέα της πληροφορικής και των επικοιωνιών προσφέρουν σημαντικές δυνατότητες στη βελτιστοποίηση της οργάνωσης και της λειτουργίας των Ενόπλων Δυνάμεων. Ωστόσο, η ολοένα αυξανόμενη εξάρτηση από την τεχνολογία δημιουργεί νέες απειλές και κινδύνους, για αυτό κρίνεται επιβεβλημένη η ορθή χρήση του Κυβερνοχώρου για την εθνική άμυνα κάθεκράτους.

Οι μεταβολές που επήλθαν εξαιτίας της ραγδαίας αύξησης των τεχνολογικών επιτευγμάτων και η χρήση αυτών στις στρατιωτικές επιχειρήσεις επέφερε την γνωστή «Επανάσταση στις Στρατιωτικές Επιχειρήσεις»- (Revolution in Military Affairs, RMA), ένα δόγμα όπως αυτό διαμορφώθηκε μετά τον Ψυχρό Πόλεμο. Στόχος της RMA είναι η βέλτιστη χρήση των τεχνολογιών πολέμου, ο εκσυγχρονισμός των οπλικών συστημάτων και η ελαχιστοποίηση των θυμάτων του επιτιθέμενου στρατού (risk free warfare)[265].

Στην Ελλάδα, το κυβερνητικό όργανο, το οποίο είναι αποκλειστικά αρμόδιο να καθορίζει την πολιτική σχετικά με ζητήματα εθνικής ασφάλειας είναι το Κυβερνητικό Συμβούλιο Εξωτερικών και Άμυνας (ΚΥΣΕΑ). Το Υπουργείο Εθνικής Άμυνας (ΥΕΘΑ) είναι ο αρμόδιος φορέας για την οργάνωση, τον σχεδιασμό και την διεξαγωγή Κυβερνοεπιθέσεων ,όταν χρειαστεί αλλά και για την διασφάλιση της άμυνας στον Κυβερνοχώρο. Άλλωστε οι Ένοπλες Δυνάμεις είναι υπεύθυνες για την λειτουργική και αποτελεσματική προστασία των κρίσιμων κρατικών υποδομών και την αδιάλειπτη λειτουργία των ανωτέρω, που αποτελούν τον βασικότερο στόχο των Κυβερνοεπιθέσεων, όπως αναλύσαμε σε

[265] http://www.theseis.com/index.php?option=com_content&task=view&id=1111&Itemid=29

προηγούμενη ενότητα. Επιπλέον αποστολή τους είναι η απρόσκοπτη λειτουργία των κρίσιμων Συστημάτων Επικοινωνιών και Πληροφορικής (Communication and Information Systems, CIS).

Το ΓΕΕΘΑ, σε συνεργασία με την Εθνική Υπηρεσία Πληροφοριών , εκδίδει τον Εθνικό Κανονισμό Ασφάλειας (ΕΚΑ) που αφορά στην ασφάλεια των διαβαθμισμένων πληροφριών, ο οποίος έχει συνταχθεί σύμφωνα με τους κανόνες του ΝΑΤΟ και εφαρμόζεται από τα Γενικά Επιτλεία των τριών κλάδων, στα οποία υπάρχουν τα αρμόδια τμήματα πληροφορικής. Επιπλέον από το 2000 συστάθηκε ως Τμήμα και από το 2004 λειτουργεί και δραστηριοποιείται ως Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ (ΓΕΕΘΑ/ΔΙΚΥΒ) με στόχο να αναβαθμιστεί σε Διοίκηση[266] . Η ΔΙΚΥΒ συντονίζει τα επιμέρους Επιτελεία των άλλων Κλάδων και δίνει κατευθυντήριες γραμμές για την υλοποίηση της Κυβερνοάμυνας. Η συγκεκριμένη Διεύθυνση έχει αναλάβει την υλοποίηση όλων των δράσεων για την καλύτερη δυνατή οργάνωσή τηςΚυβερνοάμυνας ενώ εκπροσωπεί τη χώρα με τη αποστολή στελεχών της σε διάφορες δραστηριότητες, τόσο σε ΝΑΤΟϊκό, όσο και σε Ευρωπαϊκό επίπεδο. Επιπλέον συμμετέχει στις ασκήσεις Κυβερνοάμυνας του ΝΑΤΟ ενώ διοργάνωσε την πρώτη εθνική άσκηση Κυβερνοάμυνας «ΠΑΝΟΠΤΗΣ»[267] τον Μάιο του 2010. Ακόμη συνεργάζεται με άλλες κρατικές υπηρεσίες, όπως η ΕΥΠ και η ΕΛΑΣ, οι οποίες μπορούν να συμβάλλουν στην αντιμετώπιση των αναδυόμενων στον Κυβερνοχώρο απειλών κατά της Εθνικής Ασφάλειας[268] . Μέσα στην ΔΙΚΥΒ λειτουργεί το Στρατιωτικό Κέντρο Αντιμετώπισης Κυβερνοπεριστατικών (ΣΚΑΚ) το οποίο διαθέτει συντονιστικό ρόλο σε ζητήματα Κυβερνοάμυνας . Το ΣΚΑΚ στελεχώνεται με προσωπικό από τα ΓΕ και αποτελεί το Στρατιωτικό CIRC (Computer Incident Response Capability) φροντίζοντας για τη εύρυθμη

[266] http://www.ekeo.gr/2011/02/%CE%B4%CE%B9%CE%BF%CE%AF%CE%BA%CE%B7%CF%83%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%80%CF%8C%CE%BB%CE%B5/

[267] Πρόκειται για προσωνύμιο δανεισμένο από την ελληνική μυθολογία και ήταν ένα από τα επίθετα με τα οποία χαρακτηριζόταν ο Δίας

[268] http://www.ekeo.gr/2011/02/%CE%B4%CE%B9%CE%BF%CE%AF%CE%BA%CE%B7%CF%83%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%80%CF%8C%CE%BB%CE%B5/

λειτουργία όλων των στρατιωτικών δικτύων, εντοπίζοντας κυβερνοεπιθέσεις, τις οποίες προσπαθεί να καταστείλει μεκάθε τρόπο. Η ΔΙΚΥΒ συνεργάζεται με τα Εθνικά Κέντρα αντιμετώπισης κυβερνοπεριστατικών, αλλά και με τα αντίστοιχα σε Διεθνές επίπεδο και ιδιαίτερα με αυτά του NATO (NCIRC) [269]. Ο βασικότερος στόχος της ΔΙΚΥΒ είναι ο εντοπισμός των κυβερνοεπιθέσεων και η αποτελεσματική αντιμετώπιση τους.

Ο σταθερά αυξανόμενος όγκος και η πολυπλοκότητα της κακόβουλης δραστηριότητας στον κυβερνοχώρο καθιστούν επιτακτική την ανάγκη κυρίως για πρόληψη (ανίχνευση και εντοπισμός) και λιγότερο για άμεση αντιμετώπιση. Για αυτό το λόγο πρωταρχική αποστολή του ΣΚΑΚ είναι ο συνεχής προληπτικός έλεγχος και ο εντοπισμός κακόβουλου λογισμικού στα δίκτυα των Ενόπλων Δυνάμεων, η συλλογή και επεξεργασία πληροφοριών σε περίοδο ειρήνης για ζητήματα κυβερνοάμυνας με σκοπό την έγκαιρη ενημέρωση και προειδοποίηση για υπάρχουσες απειλές στον Κυβερνοχώρο.

Για την επίτευξη των στόχων της Κυβερνοάμυνας απαιτούνται ορισμένες ενέργειες οι οποίες υλοποιούνται μέσω του ΚΑΚ και συντονίζονται από την ΔΙΚΥΒ. Οι βασικότερες από τις οποίες είναι οι εξής [270]:

Ι) Στα πλαίσια της σωστής προετοιμασίας και εκπαίδευσης του προσωπικού κρίνεται απαραίτητος ο προγραμματισμός και η τακτική διεξαγωγή εκπαιδευτικών ασκήσεων με αντικείμενο την αντιμετώπιση Κυβερνοεπιθέσεων.

ΙΙ) Διενέργεια σε όλα τα στρατιωτικά δίκτυα ελέγχου ασφαλείας (security audits), εκτιμήσεων τρωτοτήτων (vulnerability assessments) και ελέγχων διείσδυσης (penetration testing) από την ΓΕΕΘΑ/ΔΙΚΥΒ.

ΙΙΙ) Σε περίπτωση ανίχνευσης μιας ύποπτης δραστηριότητας στον Κυβερνοχώρο, εφόσον επιτευχθεί η αποτελεσματική αντιμετώπιση μιας κυβερνοεπίθεσης, πραγματοποιείται και πλήρης επαναφορά των δεδομένων από τους αρμόδιους διαχειριστές αυτού σε συνεργασία με το ΚΑΚ για την

[269] http://www.onalert.gr/stories/antimetwpish-kybernopei8esewn-sto-geetha/29352
[270] http://www.pentapostagma.gr/2014/02/%CE%B3%CE%B5%CE%B5%CE%B8%CE%B1-h-k%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1-%CF%84%CF%89%CE%BD-%CE%B5%CE%BD%CF%8C%CF%80%CE%BB%CF%89%CE%BD-%CE%B4%CF%85%CE%BD%CE%AC%CE%BC.html

πλήρη αποκατάσταση του συστήματος ή της υποδομής που στοχοποιήθηκε. Παράλληλα διενεργείται ενδελεχής καταγραφή όλων των ενεργειών που πραγματοποιήθηκαν και των δεδομένων που συλλέχθηκαν με σκοπό την ανάλυση της επίθεσης και την εξαγωγή συμπερασμάτων (lessons learned)

Όπως σε κάθε χώρα πρέπει να υπάρχουν οι Ομάδες Επείγουσας Παρέμβασης σε Υπολογιστές (Computer Emergency Response Teams -CERT) [271] για να δίνουν τις κατευθυντήριες γραμμές σε ζητήματα ασφάλειας στο Διαδίκτυο και αποσκοπώντας στη βελτίωση των συστημάτων ασφάλεια, το ίδιο ισχύει και στην Ελλάδα. Με το Νόμο 3646/ 2008, η Εθνική Υπηρεσία Πληροφοριών «ορίζεται ως η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και καθίσταται αρμόδια για την αντιμετώπιση και καταστολή ηλεκτρονικών επιθέσεων κατά δικτύων και πληροφιακών συστημάτων» αναλαμβάνοντας έτσι τον ρόλο ενός CERT.

5. Προτάσεις για την αντιμετώπιση των Κυβερνοεπιθέσεων μέσω της θέσπισης νέων κανόνων δικαίου και μέτρα που θα μπορούσαν να ληφθούν σε πολιτικό και στρατιωτικό επίπεδο

Παρά το γεγονός ότι έχουν θεσπιστεί διάφορες Συμβάσεις για το Κυβερνοέγκλημα και ενώ αρκετοί μελετητές ισχυρίζονται πως επαρκούν οι ήδη υπάρχοντες κανόνες Διεθνούς Δικαίου , η αναλογική εφαρμογή των οποίων θα μπορούσε να ρυθμίσει τα ζητήματα που ανακύπτουν λόγω του Κυβερνοπολέμου, σήμερα δεν υπάρχει κανένα διεθνές, νομικά δεσμευτικό, εργαλείο το οποίο να χαρακτηρίζει την Κυβερνοεπίθεση ως απειλή για την εθνική ασφάλεια μιας χώρας. Το Εγχειρίδιο του Ταλίν αποτελεί ένα σπουδαίο εγχείρημα, μη νομικά δεσμευτικό βέβαια κείμενο, το οποίο διερευνά τη δυνατότητα αναλογικής εφαρμογής του ισχύοντος διεθνούς δικαίου, του δικαίου της χρήσης βίας (jus ad bellum) και του ανθρωπιστικού δικαίου (jus in bello) στον Κυβερνοπόλεμο. Οι επιχειρήσεις στον Κυβερνοχώρο δεν απαγορέυονται μεν ρητά από κάποιον κανόνα, αλλά δεν υπάρχει μέχρι στιγμής και κανένα νομικά δεσμευτικό κείμενο, το οποίο να ρυθμίζει τις επιθέσεις αυτές,

[271] http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team

προβλέποντας τυχόν νομικούς περιορισμούς κατά την διεξαγωγή τους. Δεδομένου των ιδιαιτεροτήτων που παρουσιάζουν οι Κυβερνοεπιθέσεις, των μεθόδων που χρησιμοποιούνται και των ατόμων που μπορούν να τις υλοποιήσουν για την εκτέλεση τους, των στόχων τους (κρίσιμες υποδομές, συστήματα επικοινωνιών, κρίνεται απαραίτητη η άμεση σύναψη διεθνών συμφωνιών στα πλαίσια συνεργασίας όλων των κρατών, οι οποίες θα είναι πιο εξειδικευμένες και θα εξετάζουν την κάθε περίπτωση ξεχωριστά. Την άποψη αυτή ενστερνίζεται και ο Shackelfod, σύμφωνα με τον οποίο θα πρέπει να θεσπιστεί ένα νομικό πλαίσιο θα αντιμετωπίζει τις διάφορες κατηγορίες Κυβερνοεπιθέσεων με σκοπό την αύξηση της ασφάλειας στον Κυβρνοχώρο [272] .

Η Ρωσία ήταν από τις πρώτες χώρες που υποστήριζαν την ανωτέρω άποψη, ότι κρίνεται αναγκαία η θέσπιση νέων κανόνων και η σύναψη διεθνών συμφωνιών για την αντιμετώπιση του Κυβερνοπολέμου. Ήδη από το 1998 έθεσε επί τάπητος το ζήτημα της ασφάλειας στον Κυβερνοχώρο και συγκεκριμένα ο Ρώσος Υπουργός Εξωτερικών με επιστολή [273] ,που απέστειλε στις 23 Σεπτεμβρίου 1998 προς τον Γενικό Γραμματέα του ΟΗΕ, πρότεινε την έκδοση Ψηφίσματος σχετικά με την ασφάλεια στον Κυβερνοχώρο. Η ενέργεια αυτή κινητοποίησε τις ΗΠΑ με αποτέλεσμα να εκδοθεί Απόφαση της Γενικής Σύνελευσης τον Νοέμβριο του 2000 η οποία αναφερόταν στις απειλές που υπάρχουν και τους κινδύνους που ελλοχεύουν και καλούσε τα κράτη- μέλη να να λάβουν τα απαραίτητα μέτρα για την ασφάλεια των πληροφοριακών συστημάτων σε διεθνές επίπεδο [274].

Μια άλλη μερίδα αναλυτών υποστηρίζουν ότι θα ήταν σκόπιμη η υιοθέτηση οικουμενικής δικαιοδοσίας για την νομική αντιμετώπιση των Κυβερνοεπιθέσεων. Στα πλαίσια αυτής, κάθε εθνικό δικαστήριο θα έχει την δυνατότητα να εκδικάζει μια υπόθεση Κυβερνοεγκλήματος, ανεξάρτητα από τον τόπο τέλεσης του, την υπηκοότητα του θύτη ή του θύματος και τις συνθήκες κάτω από τις οποίες αυτό

[272] Shackelford S. J., “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, Berkeley Journal of International Law, 2009, p.246-248
[273] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/53/3&Lang=E
[274] U.N. G.A.Resolution 55/28, Developments in the field of information and telecommunications in the context of international security (November 20, 2000)

τελέστηκε. Ο Κυβερνοπόλεμος είναι ένα φαινόμενο το οποίο δεν σχετίζεται αποκλειστικά με τις Ένοπλες Δυνάμεις. Η επιτυχής διεξαγωγή των επιχειρήσεων στον Κυβενοχώρο προϋποθέτει θεμελιώδη αλλαγή νοοτροπίας, τόσο της πολιτικής όσο και της στρατιωτικής ηγεσίας και στενή συνεργασία όλων των εμπλεκόμενων φορέων με παράλληλη οργάνωση και εκπαίδευση του προσωπικού που εμπλέκεται και λαμβάνει μέρος στις συγκεκριμένες επιχειρήσεις και εργάζεται στον τομέα της Κυβερνοάμυνας. Πιο συγκεκριμένα σε πολτικό επίπεδο, κάθε τεχνολογικά αναπτυγμένο κράτος συμπεριλαμβανομένης και της Ελλάδος, πρέπει να προχωρήσει στην αναθεώρηση της ισχύουσας εθνικής νομοθεσίας και στην θέσπιση νέων κανόνων που να καθορίζουν το νομικό καθεστώς των Κυβερνοεπιθέσεων.

Επιπλέον κρίνεται σκόπιμη η συνεργασία κάθε κράτους με τον ΟΗΕ για την υιοθέτηση αρχών και κανόνων που θα είναι κοινά αποδεχτοί και μιας κοινής πολιτικής σχετικά με τα ζητήματα διεθνούς δικαίου που ανακύπτουν από τον Κυβερνοπόλεμο. Επιβεβλημένη κρίνεται η εισαγωγή στα εκπαιδευτικά ιδρύματα μαθημάτων με αντικείμενο την ασφάλεια στον Κυβερνοχώρο, δεδομένης της ευρείας και ολοένα αυξανόμενης χρήσης του Διαδικτύου από εφήβους, οι οποίοι έχουν άγνοια των κινδύνων που ελλοχεύουν.

Σε στρατηγικό επίπεδο πρέπει να ληφθούν ορισμένα μέτρα. Καταρχήν κρίνεται σκόπιμη η υιοθέτηση και μιας Εθνικής Πολιτικής και Στρατηγικής για ζητήματα Κυβερνοάμυνας και ασφάλειας στον Κυβερνοχώρο, έτσι ώστε να εξαλειφθεί κάθε είδους ασάφεια. Επιπλέον χρήσιμη θα ήταν η συμμετοχή κάθε κράτους σε ΝΑΤΟϊκές και διακρατικές ασκήσεις Κυβερνοπολέμου, με σκοπό την καλύτερη εκπαίδευση του προσωπικού και την προετοιμασία του σε περίπτωση πραγματικού Κυβερνοπολέμου. Σκόπιμη κρίνεται ακόμη από κάθε κράτος η μελέτη της τρωτότητας των συστημάτων επικοινωνιών και πληροφορικής που διαθέτει , όπως επίσης και των υποδομών που υποστηρίζονται από ανάλογα συστήματα και η οργάνωση της άμυνάς τους με βάση ένα μακροπρόθεσμο σχέδιο.

ΕΠΙΛΟΓΟΣ- ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφισβήτητα κατά την δεκαετία του 1990 και μετέπειτα η αλματώδης τεχνολογική ανάπτυξη και η εφαρμογή των ηλεκτρονικών υπολογιστών σε όλους τους τομείς της καθημερινότητας μας συνετέλεσε στον αυτοματισμό πολλών διαδικασιών και στην ταχύτητα διεξαγωγής αρκετών συναλλαγών. Στο χώρο των Ενόπλων Δυνάμεων η χρήση των τεχνολογικών επιτευγμάτων οδήγησε σταδιακά στην ανάπτυξη του δόγματος της «Επανάστασης στις Στρατιωτικές Υποθέσεις» (Revolution in Military Affairs, RMA) αλλάζοντας τα υπάρχοντα δεδομένα του παραδοσιακού πολέμου και τονίζοντας την άρρηκτη σχέση μεταξύ τεχνολογίας και πολέμου. Σύμφωνα με τον Clausewitz, «κάθε εποχή έχει το δικό της είδος πολέμου, τους δικούς της περιορισμούς και τις δικές της ιδιαίτερες προκαταλήψεις». Αρχικά, μόνο τα ανεπτυγμένα τεχνολογικά κράτη είχαν την δυνατότητα να συνδέονται στο Διαδίκτυο, σταδιακά όμως και κυρίως μετά το 1990 η πρόσβαση σε αυτό ήταν εφικτή από τον καθένα. Η ραγδαίως αυξανόμενη διάδοση και χρήση του Διαδικτύου δημιούργησε νέες έννοιες όπως Κυβερνοχώρος, Κυβερνοπόλεμος και Κυβερνοεπιθέσεις, δημιουργώντας και νέες ανάγκες

Ο Κυβερνοχώρος είναι το πεδίο διεξαγωγής αρκετών καθημερινών δραστηριοτήτων, όπως η μεταφορά ανταλλαγής δεδομένων και πληροφοριών αλλά και κυβερνοεγκλημάτων. Ένας εικονικός χώρος,όπου δραστηριοποιούνται όλοι οι δράστες των κυβερνοεπιθέσεων αλλά και πολλών στρατιωτικών επιχειρήσεων. Τα ιδιαίτερα χαρακτηριστικά αυτού, η έλλειψη γεωγραφικών συνόρων, η ανωνυμία, η μεταβλητότητα του, η εύκολη πρόσβαση με χαμηλό κόστος τον κάνουν να βρίσκεται πίσω από κάθε έκφανση της ανθρώπινης δραστηριότητας. Με απλά λόγια ο Κυβερνοχώρος βρίσκεται παντού. Η εικονική αυτή περιοχή γρήγορα μετατράπηκε από καθημερινό εργαλείο σε πεδίο έντονων συγκρούσεων ενώ διαθέτει ακρετά τρωτά σημεία, τα οποία από αρκετούς χρήστες αγνοούνται με αποτέλεσμα να μην υπάρχει η απαραίτητη

ασφάλεια. Οι αδυναμίες αυτές του Διαδικτύου αποτέλεσαν αντικείμενο εκμετάλλευσης με αποτέλεσμα να δημιουργηθούν κακόβουλα προγράμματα και να εισβάλλουν διάφοροι hackers σε υπολογιστικά συστήματα πραγματοποιώντας επιθέσεις σε δίκτυα γνωστές ως κυβερνοεπιθέσεις.

Ο Κυβερνοπόλεμος συνιστά όχι μόνο μια πραγματικότητα για όλα τα κράτη αλλά και μια νέα υπαρκτή και ιδιόμορφη απειλή ιδιάζουσας σημασίας, εξαιτιάς των ιδιαίτερων χαρακτηριστικών του, που καθιστούν αρκετά δύσκολη την διαχείριση του. Οι τεχνικές- μέθοδοι που χρησιμοποιούνται είναι διαθέσιμες παντού ενώ η μορφή τους εξελίσσεται συνεχώς με αποτέλεσμα να μην μπορούν να ανιχνευθούν εύκολα. Οι κυβερνοεπιθέσεις που διεξάγονται καθημερινά είναι χιλιάδες, ενώ βασικότεροι στόχοι αυτών αποτελούν οι κρίσιμες κρατικές υποδομές, όπως οι σταθμοί παραγωγής ηλεκτρικής ενέργειας, τα δίτκυα τηλεφωνικής επικοινωνίας, τα τραπεζικά συστήματα, τα συστήματα των Ενόπλων Δυνάμεων, η προσβολή των οποίων μπορεί να θέσει εκτός λειτουργίας πολλούς οργανισμούς και επιχειρήσεις, προκαλώντας μεγάλο οικονομικό και κοινωνικό κόστος.

Ο Κυβερνοπόλεμος, ως επιμέρους τμήμα του Πληροφοριακού Πολέμου, αποτελεί αναμφισβήτητα πυλώνα ισχύος ενός κράτους και για αυτό το λόγο θα πρέπει να αποτελεί μείζον ζήτημα για την Στρατηγική Πολιτική κάθε χώρας. Ωστόσο για την επιτυχή διεξαγωγή των επιχειρήσεων στον Κυβερνοχώρο απαιτείται να αλλάξει άρδην η νοοτροπία τόσο της πολιτικής όσο και της στρατιωτικής ηγεσίας. Επιπλέον η συνεχώς αυξανόμενη δραστηριότητα στον Κυβερνοχώρο και η αύξηση των κυβερνοεγκλημάτων υποδηλώνει την ανάγκη ανάπτυξης σε εθνικό επίπεδο ορθής αμυντικής πολιτικής, η οποία θα έγκειται στην παροχή καλύτερης εκπαίδευσης του προσωπικού που εργάζεται στον τομέα της κυβερνοάμυνας. Αναγκαία κρίνεται και η θέσπιση ενός νομικού ρυμθιστικού πλαισίου και η σύναχη διεθνών συνθηκών. Τα κράτη πρέπει να συνεργαστούν αρμονικά για την αντιμετώπιση της παγκόσμιας αυτής απειλής και των κινδύνων που ελλοχεύουν καθώς και την ανεύρεση μιας κοινώς αποδεκτής λύσης σε διεθνές επίπεδο με σκοπό την ασφάλεια στον Κυβερνοχώρο .

Είναι γεγονός, ότι ενώ το φαινόμενο του Κυβερνοπολέμου δεν εμφανίσθηκε την τελευταία δεκαετία, η επιμονή ορισμένων κρατών να αντιμετωπίζουν τις κυβερνοεπιθέσεις μόνο σε εθνικό επίπεδο και η έλλειψη συνεργασίας για την σύναψη μιας διεθνούς νομικά δεσμευτικής συμφωνίας, έχει προκαλέσει ποικίλα προβλήματα. Πέρα από τα μέτρα που καλούνται τα κράτη να λάβουν σε εθνικό επίπεδο για να εξασφαλίσουν την δραστηριότητα τους στον Κυβερνοχώρο, υπάρχει έντονος προβληματισμός και εγείρονται διάφορα ερωτήματα σχετικά με το ποιοι κανόνες δικαίου θα πρέπει να εφαρμοσθούν, ώστε να αντιμετωπισθούν οι απειλές που δημιουργούνται. Κατά μια άποψη, προτείνεται η αναλογική εφαρμογή των ήδη ισχύοντων κανόνων του Διεθνούς Δικαίου. Αρκετοί μελετητές υποστηρίζουν ότι τόσο το Δίκαιο της Χρήσης Βίας (jus ad bellum) όσο και το Δίκαιο των Ενόπλων Συρράξων ή του Πολέμου (jus in bello) επαρκούν για να αντιμετωπίσουν τις σύγχρονες αυτές μορφές βίας στις διεθνείς σχέσεις. Η άποψη αυτή στηρίζεται στο γεγονός ότι τα χαρακτηριστικά των κυβερνοεπιθέσεων και οι τεχνικές που χρησιμοποιούνται κατά την διάρκεια αυτών μπορούν να θεωρηθούν χρήση βίας και ένοπλη επίθεση σύμφωνα με τα άρθρα 2(4) και 51 του Χάρτη του ΟΗΕ, εφόσον οι συνέπειες και τα αποτελέσματα που προκαλούν ξεπερνούν ένα συγκεκριμένο «κατώφλι» βίας όπως λέγεται και ένα ελάχιστο επίπεδο έντασης όπως προβλέπεται στον ορισμό της επίθεσης. Το ζητούμενο των συντακτών του Χάρτη , σύμφωνα με αυτή την άποψη, δεν είναι τόσο το είδος του όπλου που χρησιμοποιείται αλλά το ύψος των συνεπειών που επιφέρει η χρήση του. Εν κατακλείδι, κατά την άποψη αυτή οι σχετικές διατάξεις του Χάρτη περί του δικαιώματος άμυνας αλλά και της απαγόρευσης χρήσης βίας όπως ορίζονται στον Καταστατικό Χάρτη του ΟΗΕ μπορούν να εφαρμοσθούν αναλογικά και να ρυθμίσουν αποτελεσματικά τα ζητήματα που ανακύπτουν κατά τις «ένοπλες επιθέσεις».

Από την άλλη πλευρά, υφίσταται ο αντίλογος ότι εξαιτίας των ιδιαιτεροτήτων που παρουσιάζουν οι Κυβερνοεπιθέσεις, των μεθόδων – όπλων με τις οποίες αυτές διεξάγονται αλλά και της ποικιλίας των δρώντων που μπορούν να τις υλοποιήσουν, κρίνεται απαραίτητη η σύναψη διεθνών συμφωνιών στα πλαίσια συνεργασίας όλων των κρατών, οι οποίες θα είναι πιο εξειδικευμένες και θα εξετάζουν την κάθε περίπτωση ξεχωριστά, αξιοποιώντας βέβαια και τους υπάρχοντες κανόνες Διεθνούς Δικαίου. Ορισμένοι μελετητές δεν ενστερνίζονται

απόλυτα την άποψη της επέκτασης του ρυθμιστικού πλαισίου, όπως αυτό ορίζεται στον Καταστατικό Χάρτη του ΟΗΕ για τα ζητήματα χρήσης βίας που ανακύπτουν στον Κυβερνοπόλεμο, θεωρώντας ότι απαιτείται η θέσπιση ενός νέου διεθνούς δεσμευτικά νομικού πλαισίου το οποίο πιθανόν να θέτει και ορισμένους περιορισμούς για τον τρόπο διεξαγωγής των Κυβερνοεπιθέσεων και γενικότερα των Κυβερνοεπιχειρήσεων. Σύμφωνα με τον Martin Libicki η συμβατική απαγόρευση της χρήσης βίας στον Κυβερνοχώρο είναι σχεδόν ανέφικτη [275]. Ωστόσο, συνεχίζει ο Libicki είναι εφικτή η σύναψη κανόνων δικαίου που θα θέτουν ορισμένα όρια στις διάφορες κατηγορίες κυβερνοεπιχειρήσεων.

Σημαντικό εγχείρημα ώστε να αποσαφηνιστούν αρκετά ζητήματα διεθνούς δικαίου που ανακύπτουν από τον Κυβερνοπόλεμο αποτέλεσε το Εγχειρίδιο του Ταλίν, ένα μη νομικά δεσμευτικά κείμενο ,το οποίο συντάχθηκε από μια Διεθνή Ομάδα Εμπειρογνωμόνων το 2013, η οποία μελέτησε την δυνατότητα αναλογικής εφαρμογής του δικαίου της χρήσης βίας και του ΔΑΔ στον Κυβερνοπόλεμο. Αναμφισβήτητα απαραίτητη προϋπόθεση για την σύναψη ενός ειδικού διεθνού καθεστώτος για την αντιμετώπιση του φαινομένου είναι η συνεργασία όλων των κρατών ώστε να υιοθετηθεί ένα σύνολο από κανόνες και διαδικάσίες με τις οποίες θα λαμβάνονται αποφάσεις σχετικά με τα ζητήματα και τις απειλές που πηγάζουν από τις κυβερνοεπιθέσεις. Επιπλέον προτείνεται όπως αναφέραμε στην προηγούμενη ενότητα, η υιοθέτηση μιας οικουμενικής δικαιοδοσίας για την νομική αντιμετώπιση των Κυβερνοεπιθέσεων. Στα πλαίσια αυτής, κάθε εθνικό δικαστήριο θα έχει την δυνατότητα να εκδικάζει οποιοδήποτε Κυβερνοέγκλημα, ανεξάρτητα από τον τόπο τέλεσης του, την υπηκοότητα του θύτη ή του θύματος και τις συνθήκες κάτω από τις οποίες αυτό τελέστηκε.

Λαμβάνοντας λοιπόν υπόψη όλα τα παραπάνω, γίνεται αντιληπτό ότι ο Κυβερνοπόλεμος είναι πλέον μια νέα υπαρκτή απειλή, εξαιτίας της οποίας τα κράτη οφείλουν να αφυπνιστούν άμεσα και να συνεργαστούν, ώστε να αντιμετωπιστεί αποτελσματικά το φαινόμενο αυτό και να βρεθεί μια κοινή και αποδεκτή από το σύνολο της διεθνούς κοινότητας, λύση. Διαφορετικά οι συνεχώς μεταβαλλόμενες τεχνολογικές εξελίξεις και η ραγδαία διάδοση του Διαδικτύου σε παγκόσμιο επίπεδο θα θέσουν σε κίνδυνο την διεθνή ασφάλεια

[275] Libicki M C., “Cyberdeterrence and cyberwar”, RAND Corporation, 2009, p. 199-201

αλλά και την εθνική κυριαρχία κάθε κράτους. Επιπλέον διαφαίνεται ότι ο Κυβερνοπόλεμος θα αποτελέσει στο μέλλον μια εναλλακτική για τα περισσότερα κράτη έναντι του παραδοσιακού πολέμου, εξαιτίας των ιδιαίτερων χαρακτηριστικών του. Για όλους αυτούς τους λόγους η διεθνής κοινότητα καλείται να βολιδοσκοπήσει την υπάρχουσα κατάσταση και να προβεί στην λήψη των αναγκαίων μέτρων και αποφάσεων με σκοπό την διατήρηση της διεθνούς ασφάλειας ιδίως στον Κυβερνοχώρο και της ειρήνης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Γάγγας Δ, «Εισαγωγή στο Διεθνές Δίκαιο των Ενόπλων Συρράξεων», Σιδέρης, Γ΄ Εκδοση, 2008
- Χατζηκωνσταντίνου Κ :Προσεγγίσεις στο Διεθνές Ανθρωπιστικό Δίκαιο, Έκδ Σιδέρης, 2009
- Αντωνόπουλος Κ. – Μαγκλιβέρας Κ., "Το Δίκαιο της Διεθνούς Κοινωνίας", Νομική Βιβλιοθήκη , 2011
- Κονδύλης Π., «Η Θεωρία του Πολέμου», Εκδ. Θεμέλιο, 1999
- Ιωάννου Κρ., "Δίκαιο Διεθνούς Ευθύνης, Εκδ. Εταιρείας Αξιοποίησης & Διαχείρισης Περιουσίας Δημοκρίτειου Πανεπιστημίου Θράκης" , Κομοτηνή , 2003
- Κολιόπουλος Κ., "Η Στρατηγική Σκέψη από την αρχαιότητα μέχρι σήμερα" , Εκδ. Ποιότητα, Αθήνα , 2008
- Χατζηκωνσταντίνου Κ , "Επτά + 1 προβλήματα για το Διεθνές Ανθρωπιστικό Δίκαιο", Έκδ. Σιδέρης, 2010
- Gray Christine, "International Law and the Use of Force", Oxford University Press, 2008 (repr. 2009)
- Dinstein Yoram, "War, Aggression and Self-Defence", 3rd ed., Cambridge University Press (Virtual Publishing), 2003
- Tikk E., Kaska K., Vihul L., "International Cyber Incidents – Legal Considerations" , Cooperative Cyber Defence Centre of Excellence (CCDCOE) – Estonia, 2010
- Tikk E., Kaska K., Runnimeri K., Kert M., Taliharm A.-M., Vihul L., "Cyber Attacks Against Georgia: Legal Lessons Identified" , CCDCOE (NATO), 2008

- Kamal Ahmad, “The Law of Cyber-Space – An Invitation to The Table of Negotiations”, United Nations Institute of Training and Research (UNITAR), 2005
- United States Air Force Law Review, Cyberlaw Edition, vol. 64, 2009
- Cassese A., Διεθνές Δίκαιο”, Gutenberg, 201274
- Libicki M., “Cyberdeterrence and cyberwar”, RAND Corporation, 2009
- Brownlie Ian, “International Law and the Use of Force by States”, 1963
- Clarke R and Knake R .K, “Cyberwar , “The Next Threat to National Security And What To do about it”, Harper Collins Publishers, New York, 2010
- Libicki M. “ Conquest in Cyberspace: National Security and information Warfare” , Cambridge University Press, 2007

ΑΡΘΡΟΓΡΑΦΙΑ

- Λιαρόπουλος Αν., “ Η γεωγραφία και η πληροφόρηση ως διαστάσεις της παγκόσμιας ασφάλειας. Ο Κυβερνοχώρος ως το νέο γεωπολιτικό παράδειγμα στην εποχή της πληροφόρησης ”, Πανελλήνιο Γεωγραφικό Συνέδριο , 2004
- Stevens Sh., “Internet war crime tribunals and security in an interconnected world”, Transnational Law and Contemporary problems, 2009
- Shackelford Scott J., “From Nuclear War to Net War: Analogizing Cyber Attacks inInternational Law”, Berkeley Journal of International Law, 2009
- Schmitt Michael N., Computer Network Attack and Use of Force in International Law : Thoughts on a Normative Framework, Columbia Journal of Transnational Law 37, (1998 – 1999),

- Lewis, James Timlin , Katrina, “ Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization”,CSIS
- Billo C. and Chang W. “Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations States”, Institute for security technology studies at Darmouth College, Hannover,2004

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

- http://www.isoc.org/
- https://en.wikipedia.org/wiki/Cyberspace
- https://el.wikipedia.org/wiki/TCP/IP
- http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings
- http://www.unidir.org/programmes/emerging-security-threats/international-law-and-state-behaviour-in-cyberspace-meeting-series
- http://www.cnas.org/blog/natural-security-news-7108#.VgmcjMvtmko
- http://www.globalsecurity.org/military/library/report/1999/WEBRES4.htm
- http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team
- http://www.ekeo.gr/2011/02/%CE%B4%CE%B9%CE%BF%CE%AF%CE%BA%CE%B7%CF%83%CE%B7-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%80%CF%8C%CE%BB%CE%B5/
- http://www.onalert.gr/stories/antimetwpish-kybernopei8esewn-sto-geetha/29352
- http://www.pentapostagma.gr/2014/02/%CE%B3%CE%B5%CE%B5%CE%B8%CE%B1-h-k%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AC%CE%BC%CF%85%CE%BD%CE%B1-%CF%84%CF%89%CE%BD-

%CE%B5%CE%BD%CF%8C%CF%80%CE%BB%CF%89%CE%BD-%CE%B4%CF%85%CE%BD%CE%AC%CE%BC.html

- http://www.wired.com/2011/10/virus-hits-drone-fleet/
- https://en.wikipedia.org/wiki/SCADA
- http://www.nato.int/cps/en/natohq/topics_78170.htm
- http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/53/3&Lang=E
- http://www.nato.int/cps/en/natohq/news_123857.htm
- http://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team
- https://www.europol.europa.eu/ec3/cyber-operations
- https://www.enisa.europa.eu/about-enisa/activities/mission
- https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html
- https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
- http://www.eurojust.europa.eu/about/background/Pages/History.aspx
- https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat
- https://www.europol.europa.eu/ec3/ec3-in-action
- http://www.theseis.com/index.php?option=com_content&task=view&id=1111&Itemid=29
- http://www.nciss.nato.int/mission.php
- http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF
- https://www.ice.gov/
- https://www.fbi.gov/about-us/investigate/cyber
- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413
- http://geopolitics-gr.blogspot.gr/2008/08/blog-post_7278.html
- http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&
- http://www.telegraph.co.uk/news/worldnews/europe/georgia/2553058/Russia-continues-cyber-war-on-Georgia.html

- http://www.un-documents.net/a25r2625.htm
- http://kypros.org/Human_Rights/index21a.html
- http://www.un.org/documents/ga/res/42/a42r022.htm
- https://athens.indymedia.org/post/705387/
- https://el.wikisource.org/wiki/%CE%A3%CF%85%CE%BD%CE%B8%CE%AE%CE%BA%CE%B7_%CE%A4%CE%BF%CF%85_%CE%92%CF%8C%CF%81%CE%B5%CE%B9%CE%BF%CF%85_%CE%91%CF%84%CE%BB%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CE%BF%CF%8D
- https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- http://sputniknews.com/world/20070906/76959190.html
- http://www.theregister.co.uk/2008/01/24/estonian_ddos_fine
- https://www.us-cert.gov/ncas/tips/ST04-015
- https://en.wikipedia.org/wiki/Logic_bomb
- https://en.wikipedia.org/wiki/Internet_Protocol
- https://en.wikipedia.org/wiki/Critical_infrastructure
- http://news.in.gr/world/article/?aid=802799
- http://library.tee.gr/digital/m2142/m2142_koutepas.pdf
- http://www.icir.org/vern/papers/reflectors.CCR.01/node1.html
- https://www.cert.org/information-for/denial_of_service.cfm
- http://www.loundy.com/CASES/US_v_Morris2.html
- http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
- http://www.ct.aegean.gr/people/kalloniatis/Security/Malicious_Software.pdf
- http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm
- http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
- https://en.wikipedia.org/wiki/Sandia_National_Laboratories
- https://en.wikipedia.org/wiki/Titan_Rain
- https://www.justsecurity.org/17729/time-u-s-international-strategy-cyberspace/
- https://ccdcoe.org/research.html