**Πανεπιστήμιο Μακεδονίας**
**ΔΕΣ – ΒΣΑΣ – ΑΔΙΣΠΟ**
**Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών**
***Διεθνείς Σχέσεις και Ασφάλεια***

# Διπλωματική εργασία με τίτλο: "Σύγχρονα τεχνολογικά μέσα και η έννοια της επίθεσης στο διεθνές δίκαιο. Ο Κυβερνοπόλεμος, υπό το πρίσμα του ΝΑΤΟ, της Ε.Ε. και των ελληνικών ενόπλων δυνάμεων του 21ου αιώνα"

Αβραάμ Καζαντζόγλου

Επιβλέπων: Νικόλαος Ζάικος

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

*Αβραάμ Καζαντζόγλου*

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

# 1. ΕΙΣΑΓΩΓΗ

> *…δεν υπάρχουν πλέον αυτοκίνητα, δεν υπάρχουν πλέον αεροπλάνα, δεν υπάρχουν πλέον ακουστικά βαρηκοΐας. Υπάρχουν υπολογιστές με τέσσερις τροχούς, υπολογιστές με φτερά και υπολογιστές που σε βοηθάνε να ακούς*[1]

Το επιχείρημα αυτό που ίσως σε κάποιους να ακούγεται ως υπεραπλουστευμένη προσέγγιση ενός πολύπλοκου θέματος, της διείσδυσης των υπολογιστών σε κάθε έκφανση της καθημερινότητας, αποτελεί προϊόν συζήτησης μεταξύ του πρωταγωνιστή της υπόθεσης (ορισμένοι το χαρακτήρισαν «σκάνδαλο») Wikileaks, Julian Assange και ορισμένων εκ των συνεργατών του. Είναι, πράγματι, εξαιρετικά δύσκολο να φανταστούμε τη ζωή μας χωρίς την παρουσία υπολογιστών. Με τον όρο «υπολογιστής», βέβαια, δεν περιοριζόμαστε μόνο στους επιτραπέζιους ή φορητούς ηλεκτρονικούς υπολογιστές. Αντίθετα, η αναφορά σχετίζεται με οποιαδήποτε ηλεκτρονική συσκευή έχει τη δυνατότητα να εκτελεί αυτόνομα υπολογισμούς, ανεξάρτητα εάν το αποτέλεσμα αυτών των υπολογισμών γίνεται άμεσα αντιληπτό ή όχι από τον άνθρωπο. Τα εξελιγμένα ακουστικά βαρηκοΐας, για παράδειγμα, εμπεριέχοντας κάποιες έξυπνες δυνατότητες (αυτόματη προσαρμογή στο επίπεδο του περιβάλλοντα θορύβου, προσαρμογή στις ιδιαιτερότητες του χρήστη κλπ.) αποτελούν αυτόνομη υπολογιστική μονάδα με πολύ συγκεκριμένο σκοπό.

Οι ψηφιακές φωτογραφικές μηχανές αποτελούν και αυτές αναμφίβολα μικρούς αλλά πανίσχυρους υπολογιστές με συγκεκριμένη δυνατότητα και σκοπό. Με τη διαρκή εξέλιξη της τεχνολογίας και την ενσωμάτωση στις φωτογραφικές μηχανές δέκτη GPS[2] και δυνατότητα ασύρματης δικτύωσης Wi-Fi, επιτρέπουν στον χρήστη να «ανεβάζει» στο διαδίκτυο φωτογραφίες αμέσως μετά τη λήψη τους (χωρίς μεσολάβηση οικιακού ή φορητού υπολογιστή), οι οποίες μάλιστα είναι και αυτόματα γεωτοποθετημένες[3]. Η σημερινή τεχνολογία παρέχει τη δυνατότητα (FluCard)[4] αυτή η διαδικασία να ολοκληρώνεται αυτόματα, χωρίς καμμιά επενέργεια από πλευράς του χρήστη ή ακόμη και εν αγνοία του.

Αξίζει να αναρωτηθεί κανείς εάν η υποδοχή USB[5] που σχεδόν όλα τα σημερινά αυτοκίνητα διαθέτουν με σκοπό την μεταφορά ψηφιακών αρχείων (κυρίως μουσικής) στο ηχητικό σύστημα του οχήματός μας μας παρέχει απόλυτη εξασφάλιση, έναντι δυνητικά κακόβουλων ενεργειών. Δηλαδή, εκτός από τα bits[6] της μουσικής,

---

[1] Julian Assange and others, *Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των Wikileaks* (Αθήνα: Ποιότητα, 2013)

[2] Global Positioning System (Σύστημα Εντοπισμού Θέσης)

[3] Geolocated, περιέχουν ψηφιακή πληροφορία της γεωγραφικής θέσης στην οποία λήφθηκαν.

[4] Alex Lu, "*Singapore: Closing the Next Deal*," World Policy Journal 28 (2011):29

[5] Universal Serial Bus, τεχνολογία διασύνδεσης περιφερειακών συσκευών ηλεκτρονικών υπολογιστών.

[6] Binary Digits, δυαδικά ψηφία. Ουσιαστικά χρησιμοποιείται, ως όρος, για να αναφερθούμε στην βασική μονάδα αποθήκευσης ψηφιακών δεδομένων.

είμαστε σε θέση να είμαστε απόλυτα βέβαιοι οτι δεν μεταφέρονται και άλλα ψηφιακά δεδομένα κάποιου κακόβουλου λογισμικού το οποίο έχει ως σκοπό την δημιουργία προβλημάτων σε κατάλληλο χρόνο στο ίδιο το όχημά μας ;

Στις 27 Δεκεμβρίου 2013, σύμφωνα με ηλεκτρονικό άρθρο του geostrategy.gr[7], δημοσιεύτηκε στο διαδίκτυο ένα μήνυμα των Anonymous Caucasus, που αυτοαποκαλούνται «Ηλεκτρονικός Στρατός του Εμιράτου του Καυκάσου» (Electronic Army of the Caucasus Emirate), με αποδέκτες τη Ρωσική κυβέρνηση και όλες τις ρωσικές επιχειρήσεις που συμμετείχαν και χρηματοδοτούσαν τους χειμερινούς Ολυμπιακούς Αγώνες. Το μήνυμα ανέφερε, μεταξύ άλλων, οτι οι Anonymous Caucasus ήταν αποφασισμένοι να στοχοποιήσουν με επιχειρήσεις κυβερνοπολέμου τη Ρωσική κυβέρνηση, ρωσικές τράπεζες και πολλά ρωσικά ιδρύματα. Ως γνωστό, στις αρχές Οκτωβρίου 2013, είχαν πραγματοποιηθεί μεγάλης κλίμακας κυβερνοεπιθέσεις στις ιστοσελίδες πολλών μεγάλων ρωσικών χρηματοπιστωτικών ιδρυμάτων όπως η κεντρική τράπεζα της Ρωσίας, η Alfa Bank και η Sberbank[8]. Συνέπεια όλων αυτών ήταν η εδραίωση κλίματος ανασφάλειας και αμφιβολίας περί του ασφαλούς της πραγματοποίησης των χειμερινών Ολυμπιακών αγώνων του Σότσι.

Σε μια άλλη περιοχή του πλανήτη, στο Ιράν, το 2010 συνέβη κάτι το οποίο θεωρείται οτι άλλαξε τα πάντα στο χώρο του διαδικτύου. Εάν το Internet πράγματι κάποτε υπήρξε ως μία ελεύθερη και ανοικτή κοινότητα, η εποχή εξαφανίστηκε για πάντα τον περασμένο χρόνο με την εξαπόλυση της κυβερνοεπίθεσης του worm Stuxnet[9]. Το worm[10] με το όνομα «Stuxnet» στοχοποίησε και επέφερε την καταστροφή σε έναν πολύ σημαντικό αριθμό συσκευών φυγοκέντρησης στις πυρηνικές εγκαταστάσεις του Ιράν. Μετά από αυτό έγινε πλήρως αντιληπτό και από τους πλέον δύσπιστους οτι τίποτε δεν μπορεί να θεωρείται άτρωτο στις κυβερνοεπιθέσεις αφού ακόμη και συστήματα που βασίζονται σε βιομηχανικού ενδιαφέροντος προγραμματιζόμενους λογικούς ελεγκτές στοχοποιήθηκαν και καταστράφηκαν και μάλιστα, σε εγκαταστάσεις ύψιστης ασφάλειας.

Λίγα χρόνια νωρίτερα, τον Μάιο του 2007, η Εσθονία αντιμετώπισε την πραγματικότητα του κυβερνοπολέμου. Σε μια ανώνυμη κυβερνοεπίθεση στοχοποιήθηκαν τόσο πολιτικά/ιδιωτικά όσο και κυβερνητικά υπολογιστικά συστήματα. Τα χτυπήματα σε ιστοσελίδες τραπεζών, υπουργείων, εφημερίδων και ραδιοτηλεοπτικών σταθμών άφησαν τη χώρα χωρίς κανένα τρόπο να ενημερώσει τους πολίτες για την κατάσταση στην οποία είχε περιέλθει και για την κυβερνοεπίθεση που εξελισσόταν.

Στην απέναντι πλευρά του Ατλαντικού, τις Η.Π.Α., σύμφωνα με αναδημοσίευση άρθρου της Wall Street Journal στην εφημερίδα Ναυτεμπορική την 21η Δεκεμβρίου 2015, Ιρανοί κυβερνοκατάσκοποι/χάκερ απέκτησαν πρόσβαση στο σύστημα ελέγχου ενός μικρού φράγματος σε απόσταση μικρότερη των 20 μιλίων από

---

[7] "*Τρομοκρατία και Χειμερινοί Ολυμπιακοί Αγώνες*," Geostrategy, http://www.geostrategy,gr/pdf/20140109 Winter Olympic Games 2014.html (accessed May 10, 2015).

[8] ο.π.

[9] Chris C. Demchak and Peter Dombrowski, "*Rise of a Cybered Westphalian Age*," Strategic Studies Quarterly (2011).

[10] Κατηγορία κακόβουλου λογισμικού.

τη Νέα Υόρκη πριν από δύο χρόνια, πυροδοτώντας προβληματισμούς οι οποίοι έφτασαν μέχρι τον Λευκό Οίκο. Η παραβίαση έλαβε χώρα, συνεχίζει το ίδιο άρθρο, εν μέσω επιθέσεων από χάκερ που συνδέονταν με την κυβέρνηση του Ιράν με στόχο τις ιστοσελίδες αμερικανικών τραπεζών, και λίγα χρόνια μετά την πρόκληση ζημιών σε ιρανικές πυρηνικές εγκαταστάσεις μέσω του διαβόητου κυβερνοόπλου Stuxnet, όπως αναφέρει το δημοσίευμα. Το ζήτημα της τρωτότητας υποδομών αποτελεί σημαντικό πονοκέφαλο για την αμερικανική κυβέρνηση, καθώς μεγάλο κομμάτι του αμερικανικού δικτύου είναι πρακτικά απροστάτευτο στο Ίντερνετ –και εν αντιθέσει με έναν κανονικό πόλεμο, με τις κυβερνοεπιθέσεις κάποιες φορές είναι δύσκολο να γνωρίζεις πού έχει χτυπήσει ο αντίπαλος[11]. Η δυσκολία ταυτοποίησης των δραστών είναι εμφανής στο συγκεκριμένο περιστατικό αφού τα στοιχεία της έρευνας έδειξαν, μεν, οτι η επίθεση φαίνεται να ξεκίνησε από υπολογιστές στην Τεχεράνη (μέσω της IP address τους) οι οποίοι διέσπειραν το κακόβουλο λογισμικό τύπου Δούρειου Ίππου με το όνομα «TinyZbot», ωστόσο η ομάδα των χάκερ άφησε ίχνη και σε άλλες χώρες, όπως η Ολλανδία, ο Καναδάς και το Ηνωμένο Βασίλειο[12].

Τη χρονιά που διανύουμε, «υπήρξαν αρκετές κυβερνοεπιθέσεις υψηλού προφίλ[13]» με στόχους εταιρείες τηλεπικοινωνιών, εταιρείες παιχνιδιών έως και κυβερνητικούς οργανισμούς. Πολύ πρόσφατα, στις 30 Νοεμβρίου και την 1η Δεκεμβρίου του τρέχοντος έτους, σύμφωνα με την αρχική αναφορά γεγονότων της Root Server Operators[14], πολλοί DNS servers δέχτηκαν υπερβολικά μεγάλη εισερχόμενη κυκλοφορία με αποτέλεσμα σε παγκόσμια κλίμακα πάρα πολλές ιστοσελίδες να μην είναι προσβάσιμες για μεγάλο χρονικό διάστημα. Το αξιοσημείωτο σε αυτήν την κυβερνοεπίθεση είναι οτι, παρά την επισταμένη διερεύνηση της πηγής αυτών των επιθέσεων, δεν κατέστη δυνατός ο εντοπισμός της.

Περιστατικά όπως τα παραπάνω συμβαίνουν καθημερινά σε όλο τον κόσμο και μάλιστα με τέτοιους ρυθμούς που, στον αμύητο, φαντάζουν ως σενάρια φαντασίας. Μια απλή επίσκεψη στον διαδικτυακό ιστότοπο της NORSE (http://map.norsecorp.com), όπου φαίνονται σε πραγματικό χρόνο και παγκόσμια κλίμακα οι επιχειρούμενες επιθέσεις σε υπολογιστικά συστήματα πάσης φύσεως, είναι αφοπλιστικά πειστική.

Σκοπός της εργασίας είναι να καταδειχτεί η σοβαρότητα των συνεπειών των κυβερνοεπιθέσεων αλλά κυρίως, να διαφανεί το αδιέξοδο της διεθνούς κοινότητας να αντιμετωπίσει συντεταγμένα το φαινόμενο του κυβερνοπολέμου (cyberwarfare). Βέβαια, η όποια αντιμετώπιση θα μπορούσε να είναι καταρχήν αποδεκτή μόνο ως αποτέλεσμα εφαρμογής κανόνων του διεθνούς δικαίου. Στο σημείο αυτό, αναδεικνύεται ο σκληρός πυρήνας του προβλήματος αφού δεν υπάρχει

---

[11] "*Ιρανοί χάκερ στόχευσαν φράγμα στη Νέα Υόρκη το 2013*," Η Ναυτεμπορική (αναδημοσίευση άρθρου της Wall Street Journal), sec. Τεχνολογία-Επιστήμη, 21 Δεκεμβρίου 2015

[12] Garance Burke and Jonathan Fahey, "*AP Investigation: US Power Grid Vulnerable to Foreign Hacks*," Associated Press (San Jose, California), 21 December 2015

[13] Jonathan Keane, "*Hacked in 2015: The Year in Cyber-Attacks*," Paste, 9 December, 2015, http://www.pastemagazine.com/articles/2015/12/hacked-in-2015-the-worst-cyber-attacks-of-the-year.html

[14] "*Events of 2015-11-30*," Root Server Operators, http://root-servers.org (accessed 12 December 2015).

συγκεκριμένη αντίληψη της μορφής της απειλής που συνιστά ο κυβερνοπόλεμος κατά το διεθνές δίκαιο, ούτε συγκλίνουσες προσεγγίσεις του πως θα πρέπει να ερμηνευτεί το υφιστάμενο δίκαιο των ενόπλων συρράξεων ή, ακόμη, εάν απαιτείται η τροποποίησή του, ώστε να ενταχθεί ο κυβερνοπόλεμος στην θέση που του αντιστοιχεί στο διεθνές δίκαιο.

Στο 2$^{ο}$ κεφάλαιο γίνεται προσπάθεια να καθορισθεί το πεδίο ορισμού του κυβερνοπολέμου και των λοιπών συναφών εννοιών, όπως κυβερνοέγκλημα, κυβερνοτρομοκρατία αλλά και εννοιών οι οποίες δευτερογενώς εμπλέκονται με την δραστηριότητα του κυβερνοπολέμου. Τέτοιες έννοιες είναι ο δικτυοκεντρικός πόλεμος (Network-centric warfare), ο υβριδικός πόλεμος και ο απεριόριστος πόλεμος. Ο διαχωρισμός των εννοιών αυτών, ενίοτε δύσκολη υπόθεση, έχει την αξία του και αποτελεί το γνωστικό υπόβαθρο για την εδραίωση της επιχειρηματολογίας που ακολουθεί.

Στο 3$^{ο}$ κεφάλαιο παρουσιάζεται η νομική οπτική του κυβερνοπολέμου και ειδικότερα το παρόν νομικό πλαίσιο καθώς και η διεθνής επιχειρηματολογία περί επάρκειας η μη του υφιστάμενου πλαισίου, οι διαφορετικές ερμηνευτικές προσεγγίσεις και οι προτάσεις νομικής αντιμετώπισης γενικά των σύγχρονων μορφών πολέμου και ειδικά του κυβερνοπολέμου.

Τα πιθανά οφέλη του κυβερνοπολέμου για τους διεθνείς δρώντες, είτε πρόκειται για κυρίαρχα κράτη, είτε για μη-κρατικές οντότητες προσεγγίζονται στο 4$^{ο}$ κεφάλαιο. Με άλλα λόγια, εξετάζεται η θετική συνδρομή των δράσεων που μπορούν να ενταχθούν στο πλαίσιο του κυβερνοπολέμου στους δρώντες του διεθνούς συστήματος που έχουν τόσο τη δυνατότητα όσο και τη βούληση να εμπλακούν σε τέτοιου είδους δράσεις. Παράλληλα, η προσκηνιακή κατακραυγή της διεθνούς κοινότητας έναντι των δράσεων του κυβερνοπολέμου συνιστά τροχοπέδη στην αλόγιστη και απροκάλυπτη χρήση κυβερνοεπιθέσεων από το σύνολο των δρώντων, περιορίζοντας, κατά κάποιο τρόπο, την έκταση των κυβερνοπεριστατικών σε παγκόσμιο επίπεδο. Σε τελική ανάλυση, ο κάθε δρών προβαίνει σε ή απέχει από δράσεις κυβερνοπολέμου όχι λόγω του αμφιβόλου της νομιμότητας ή της αήθους μορφής της πράξης αυτής καθαυτής, αλλά λόγω μιας καλομελετημένης ανάλυσης κόστους/οφέλους η οποία συνιστά, εφόσον μιλάμε για ορθολογικούς παίκτες, το αφετηριακό σημείο. Αν και οι ενδεχόμενοι δρώντες είναι δυνητικά πολλοί, για μεθοδολογικούς και μόνο σκοπούς γίνεται αναφορά σε κάποιους οι οποίοι έχουν εμπλακεί σε πρόσφατα περιστατικά, ως θύματα, ως φερόμενοι δράστες ή ακόμη ως συμμετέχοντες.

Από την σκοπιά των οντοτήτων που οφείλουν να οχυρωθούν έναντι του κυβερνοπολέμου αναμφισβήτητα, πέρα από τα κράτη, ιδιαίτερη αξία έχει η αμυντική προετοιμασία του ΝΑΤΟ αφού αυτό, καταστατικά, αποτελεί σύμφωνο αμυντικής μορφής. Ο κυβερνοπόλεμος δεν θα μπορούσε να αφήσει αδιάφορη την Βορειοατλαντική Συμμαχία η οποία άλλωστε έχει πολλάκις στοχοποιηθεί έως σήμερα. Ειδικά στην δεύτερη δεκαετία του αιώνα μας το ΝΑΤΟ έκανε σημαντικά βήματα θωράκισης απέναντι στον κυβερνοπόλεμο, τόσο σε τεχνολογικό επίπεδο όσο και σε δομικό και οργανωτικό.

Μπορεί μετά το τέλος του ψυχρού πολέμου το ΝΑΤΟ να επαναπροσδιόρισε την αποστολή του και την περιοχή ενδεχόμενης δράσης του, ωστόσο ο κυριότερος συμμετέχον σε αυτό, οι Η.Π.Α., έχοντας εκδηλώσει την πρόθεσή τους να τροποποιήσουν τις προτεραιότητές τους σχετικά με την σταδιακή απαγκίστρωσή

τους από το ευρωπαϊκό θέατρο και την ταυτόχρονη ενδυνάμωση της παρουσίας τους στην περιοχή του ειρηνικού, γνωστή και ως "Pacific Pivot[15]", οδήγησε τη γηραιά ήπειρο σε ανήσυχες σκέψεις για την επόμενη ημέρα. Οι επανερχόμενες απόψεις περί ίδρυσης ευρωστρατού ακούγονται σήμερα πιο έντονα και πιο συχνά από ποτέ. Έτσι, παρόλη την, προς το παρόν, ανυπαρξία ενόπλων δυνάμεων της Ευρωπαϊκής Ένωσης, επιχειρείται μια διερευνητική προσέγγιση της Ε.Ε. σχετικά με το θέμα του κυβερνοπολέμου ως αμυντική επιλογή.

Όπως είναι λογικά αναμενόμενο, η Ελλάδα ως χώρα, αποτελεί ξεχωριστό αντικείμενο ενδιαφέροντος σε σχέση με την απειλή του κυβερνοπολέμου. Τόσο ο χώρος των ενόπλων δυνάμεων με την στενή έννοια όσο και ο ιδιωτικός αλλά κυρίως ο δημόσιος τομέας και οι εθνικές υποδομές της χώρας, είναι τα επιμέρους σημεία που πραγματεύεται. Το ΝΑΤΟ, η ΕΕ και οι ελληνικές ένοπλες δυνάμεις, υπό τον φακό του κυβερνοπολέμου φωτίζονται στο 5$^{ο}$ κεφάλαιο.

Τέλος, ακολουθούν οι συμπερασματικές σκέψεις (6$^{ο}$ κεφάλαιο) για το σύνολο των σημείων προβληματισμού του θέματος της συγκεκριμένης εργασίας ενώ αντί επιλόγου παρατίθενται (ως 7$^{ο}$ κεφάλαιο) κάποιες απόψεις του γράφοντα που διεκδικούν, με αξιώσεις ελπίζω, το ρόλο της τροφής για περαιτέρω πνευματική διεργασία. Για τον αναγνώστη που το αντικείμενο του κυβερνοπολέμου και η νομική διάσταση που αυτό έχει σήμερα διεθνώς φαντάζει ως ένας ενδιαφέρον δρόμος να διαβεί, η βιβλιογραφία που χρησιμοποιήθηκε για την ολοκλήρωση της συγγραφής της εργασίας αυτής και που παρατίθεται ως 8$^{ο}$ κεφάλαιο μπορεί να τον απαλλάξει από τον κόπο της αρχικής αναζήτησης πηγών πληροφόρησης.

[15] U.S. Department of Defense, Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015* (Washington D.C., June 2015)

## 2. ΓΕΝΙΚΑ

> *…είναι ευτυχισμένος εκείνος που βρίσκει τον τρόπο να προσαρμόζεται με τις απαιτήσεις των καιρών και παρομοίως είναι δυστυχισμένος εκείνος που οι πράξεις του δεν συμφωνούν με τους καιρούς*[16]

### Διαδίκτυο (Internet)

Από την εμφάνιση του Διαδικτύου και έπειτα, άρχισαν να εμφανίζονται διάφοροι όροι με καταιγιστικό ρυθμό. Οι περισσότεροι από αυτούς έχουν τεχνική αφετηρία, σε μια προσπάθεια να ακολουθήσουν την εξέλιξη της ίδιας της τεχνολογίας των υπολογιστικών συστημάτων και των τεχνολογιών δικτύωσης. Όπως χαρακτηριστικά αναφέρει ο Jeremie Zimmermann, συνιδρυτής και εκπρόσωπος της ομάδας υποστήριξης πολιτών La Quadrature du Net[17], "όλα όσα έγιναν στο διαδίκτυο απλά εκτινάχθηκαν από εκεί που ήταν άγνωστα πριν λίγους μήνες ή λίγα χρόνια, άρα δεν μπορείς να προβλέψεις ποια θα είναι η επόμενη καινοτομία, και η εξέλιξη της καινοτομίας είναι τόσο γρήγορη, ώστε είναι πολύ πιο γρήγορη από τη διαδικασία δημιουργίας πολιτικής[18]". Το ίδιο το Διαδίκτυο αποτελεί κομβικής σημασία έννοια. Ως Διαδίκτυο νοείται κάθε συνένωση δύο ή περισσότερων δικτύων, όχι κατ' ανάγκη ίδιας τεχνολογίας, έτσι ώστε να επιτυγχάνεται η επικοινωνία μεταξύ τους και να λειτουργούν σε λογικό επίπεδο σαν ένα δίκτυο…Σήμερα με τον όρο διαδίκτυο εννοούμε το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων (net of nets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP, ενώ μπορεί να βρίσκονται εγκατεστημένοι σε κάθε γωνιά του πλανήτη[19].

### Κυβερνοχώρος (Cyberspace)

Κυβερνοχώρος ο [kivernoxóros] Ο18 : (πληροφ.) ένας εικονικός, πλασματικός χώρος που δημιουργείται με τη χρήση ηλεκτρονικού υπολογιστή και συνήθ. σε σύνδεση με το ίντερνετ. [λόγ. κυβερν(ητική) -ο- + χώρος μτφρδ. αγγλ. cyberspace (cyber < cybernetics, δες στο κυβερνητική)][20]

---

[16] Νικκολό Μακιαβέλλι, *Ο Ηγεμόνας*, (Αθήνα: Κάκτος, 2006), 187.

[17] La Quadrature du Net: http://laquadrature.net, ευρωπαϊκή οργάνωση που υπερασπίζεται τα δικαιώματα της ανωνυμίας στο διαδίκτυο.

[18] Julian Assange and others, *Cypherpunks, Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των WikiLeaks* (Βάρη: Ποιότητα, 2012).

[19] Γεώργιος Πάγκαλος και Ιωάννης Μαυρίδης, *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων* (Θεσσαλονίκη: Εκδόσεις Ανικούλα, 2002).

[20] "Λεξικό της κοινής νεοελληνικής," Κέντρο Ελληνικής Γλώσσας, http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=κυβερνχώρος&dq= (accessed 24 December, 2015).

Το διαδίκτυο έχει οδηγήσει σε μία έκρηξη της ποσότητας πληροφοριών που είναι διαθέσιμες στο κοινό-είναι απλά απίστευτη[21]. Οι πληροφορίες αυτές είναι, μαζί με την τεχνική υποδομή του διαδικτύου, τα βασικά συστατικά μέρη του λεγόμενου κυβερνοχώρου (cyberspace). Ο κυβερνοχώρος, σύμφωνα με τον Timothy Luke, είναι ο αποκλειστικός χώρος της ψηφιακής πληροφορίας[22]. Πρόκειται για ένα σύμπαν δεδομένων χωρίς όρια που διαπερνά κάθε φυσικό περιορισμό. Οι άνθρωποι μπορούν να επικοινωνούν και να αλληλοεπιδρούν ανεξάρτητα της ώρας και της τοποθεσίας τους[23]. Βέβαια, πρόκειται επίσης για έναν χώρο στον οποίο δεν υπάρχει καμιά υπέρτατη ρυθμιστική αρχή, εκτός ίσως από κάποιες αρχές με χαμηλού επιπέδου τεχνικές αρμοδιότητες. Υπό αυτή την έννοια, ο κυβερνοχώρος έχει αρκετά κοινά σημεία με την άναρχη κοινωνία του Hedley Bull: Το ποιος ελέγχει ποιόν, τι υπακούει σε ποιους κανόνες και που αρχίζουν και που τελειώνουν οι –όποιοι-κανόνες, παραμένει αναπάντητο ερωτηματικό. Σύμφωνα με τον Luke, "τα επιμέρους δίκτυα του Διαδικτύου βρίσκονται ταυτόχρονα παντού, πουθενά και κάπου αλλού[24]." Μια περισσότερο φιλοσοφική προσέγγιση της έννοιας του κυβερνοχώρου παρουσιάζεται από τον Stephen Carter, ο οποίος κάνει λόγο για "την άνοδο του κυβερνοχώρου η οποία συνιστά την αποθέωση της ιδέας της εξατομικευμένης εμπειρίας…η έλξη που ασκεί ο κυβερνοχώρος είναι αυτή ακριβώς η αυτονομία: μπορούμε να επιλέξουμε τη δική μας εμπειρία[25]."

Ο Κυβερνοχώρος αποτελείται από το σύνολο των παγκόσμιων δικτύων υπολογιστών (συμπεριλαμβανομένου και του Internet) και των περιφερειακών μηχανημάτων (εξυπηρετητές, δρομολογητές, μόντεμ, εκτυπωτές, ενσύρματες και ασύρματες γραμμές κλπ), τα οποία είναι συνδεδεμένα μεταξύ τους, προκειμένου να πραγματοποιείται η επεξεργασία, η αποθήκευση και η ροή των πληροφοριών (δεδομένων). Εκτός από το διαδίκτυο, ο κυβερνοχώρος περιλαμβάνει και το σύνολο των εσωτερικών δικτύων, τα οποία είναι εγκατεστημένα και λειτουργούν στο δημόσιο τομέα, στις τράπεζες, στους διάφορους οργανισμούς, στις ένοπλες δυνάμεις (εσωτερικά δίκτυα διοίκησης και ελέγχου, δίκτυα οπλικών συστημάτων όπως αρμάτων, αεροσκαφών, πολεμικών πλοίων, δορυφόρων κλπ) αλλά και το σύνολο των μεμονωμένων ηλεκτρονικών υπολογιστών που δεν είναι συνδεδεμένοι σε κανένα δίκτυο. Ο κυβερνοχώρος θα μπορούσε να χαρακτηρισθεί και ως ένας "προσβάσιμος παγκόσμιος ψηφιακός χώρος." Εξάλλου, αναφέρεται και ως ο "πέμπτος κοινός χώρος" μετά το έδαφος, τη θάλασσα, τον αέρα και το διάστημα[26]. Ο ορισμός αυτός πράγματι δίνει την έννοια του κυβερνοχώρου όχι ως κάτι παρόμοιο με το διαδίκτυο,

---

[21] Julian Assange and others, *Cypherpunks, Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των WikiLeaks* (Βάρη: Ποιότητα, 2012).

[22] Timothy W. Luke, "Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism," Alternatives: Global, Local, Political 26 (2001):122

[23] ο.π.

[24] Timothy W. Luke, "Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism," Alternatives: Global, Local, Political 26 (2001):131

[25] Stephen Carter, *Civility: Manners, Morals, and the Etiquette of Democracy* (New York: Basic Books, 1998), 193.

[26] Βασίλειος Γιαννακόπουλος, "Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή," GEOStrategy, http://www.geostrategy.gr/pdf/20110102%20Cyberwarfare.pdf (accessed 21 December, 2015).

αλλά ως μια έννοια πολύ ευρύτερη του Internet, το οποίο άλλωστε είναι ένα μόνο από τα στοιχεία του κυβερνοχώρου. Επίσης, η αλληλεξάρτηση και η αλληλεπίδραση τόσο πολλών και ενίοτε ετερόκλητων στοιχείων όπως οι τράπεζες και οι ένοπλες δυνάμεις, καταδεικνύουν ακριβώς την ιδιαίτερη υπόσταση του κυβερνοχώρου.

Για τον έλεγχο του κυβερνοχώρου, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, γίνεται μια μάχη διαρκείας. Η μάχη επικράτησης στον κυβερνοχώρο μπορεί να προσομοιαστεί με τις μάχες του παρελθόντος για τα νέα εδάφη ή, αργότερα, για τις μάχες επικράτησης και ελέγχου των πρώτων υλών ή, τέλος, τις μάχες για την εξασφάλιση φθηνού εργατικού δυναμικού[27]. Το μήλο της έριδος στην μάχη επικράτησης του κυβερνοχώρου είναι η πληροφορία. Αυτή ακριβώς η πληροφορία είναι που, συχνά, αποτελεί τον στόχο των κυβερνοεπιθέσεων.

## Κυβερνοέγκλημα (Cybercrime)

Η υιοθέτηση σύνθετων λέξεων με πρώτο συνθετικό το ”κυβερνό”, με σκοπό τον εμπλουτισμό του λεξιλογίου που αναφέρεται στον κυβερνοχώρο, πιθανόν να φαίνεται ως αναγκαστική λύση αφού πρόκειται για μια νέα πραγματικότητα. Είναι αλήθεια οτι για τον κυβερνοχώρο, όπως και για οποιαδήποτε άλλο νέο πεδίο θεωρητικής ή πρακτικής δράσης του ανθρώπου, το κενό των όρων που ήταν απαραίτητοι καλύπτεται από σύνθετες λέξεις. Λέξεις όπως “αυτοκίνητο”, “αερόστατο”, “ποδήλατο”, “πυροβόλο”, “αλεξίσφαιρο” και τόσες άλλες αποδεικνύουν οτι η η πρακτική χρήσης σύνθετων λέξεων είναι η εύκολη και γρήγορη λεξικολογική απάντηση στις αναδυόμενες ανάγκες που γεννιούνται από την πρόοδο και την εξέλιξη. Ωστόσο, η λύση αυτή έχει και ορισμένα μειονεκτήματα, όπως ενίοτε την αδυναμία σε συγκεκριμένη κατάσταση να αποδίδονται περισσότεροι του ενός, παρόμοιοι, όροι ή, κάποιος όρος να χρησιμοποιείται για να περιγράψει παρόμοιες αλλά όχι ακριβώς ίδιες καταστάσεις. Με μια γρήγορη αναζήτηση σε έντυπα ή ηλεκτρονικά λεξικά όρων που αναφέρονται στον κυβερνοχώρο καταδεικνύεται η εγκυρότητα της επιφύλλαξης της ορθότητας των λέξεων που, ευρέως, χρησιμοποιούνται για τον κυβερνοχώρο. Πέρα από την γλωσσική ασάφεια και τη δυσχέρεια στον διαχωρισμό των νοημάτων, προκύπτουν και ζητήματα που άπτονται της νομικής επιστήμης, όταν για παράδειγμα αναφερόμαστε σε “κυβερνοέγκλημα.” Ως κυβερνοέγκλημα (cybercrime) ορίζεται “οποιοδήποτε έγκλημα στο οποίο εμπλέκεται ηλεκτρονικός υπολογιστής και ένα δίκτυο[28]” και στη συνέχεια γίνεται επεξηγηματική αναφορά στο οτι ο υπολογιστής είτε μπορεί να έχει χρησιμοποιηθεί για την τέλεση του εγκλήματος είτε μπορεί να αποτελεί τον στόχο της εγκληματικής πράξης. Ένας από τους πολλούς ορισμούς του κυβερνοεγκλήματος μιλά για “αδικήματα κατά ατόμου ή ομάδας ατόμων με κίνητρο του εγκλήματος να βλάψει σκόπιμα την φήμη του θύματος ή να του προξενήσει ψυχική ή φυσική βλάβη, απώλεια, έμμεση ή άμεση, χρησιμοποιώντας σύγχρονα δίκτυα τηλεπικοινωνιών όπως το διαδίκτυο (chat rooms, e-mails, notice boards and groups) και κινητά

[27] Timothy W. Luke, “Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism,” Alternatives: Global, Local, Political 26 (2001):132

[28] Moore Robert, *Cybercrime: Investigating High-Technology Computer Crime* (Burlington: Anderson Publishing, 2011).

τηλέφωνα (SMS/MMS)[29].” Υπάρχει πληθώρα ορισμών, καλύπτοντας το φάσμα από πολύ απλούς (και, κατά συνέπεια ελλιπέστατους) ορισμούς έως και πολύ εξειδικευμένους, οι οποίοι μπορεί να αναφέρονται σε μία πολύ μικρή υποκατηγορία του κυβερνοεγκλήματος, όπως για παράδειγμα “κυβερνοέγκλημα εναντίων γυναικών[30].”

Στη γενικότερη μορφή του, ο Richard Clarke, πρώην σύμβουλος ασφαλείας στο Λευκό Οίκο, αναφέρει οτι "επιπλέον του κυβερνοπολέμου και της κυβερνοκατασκοπίας, υπάρχει και ένα τρίτο φαινόμενο, το κυβερνοέγκλημα, όπου οι άνθρωποι κερδίζουν δισεκατομμύρια δολάρια κάνοντας επιθέσεις σε τραπεζικούς λογαριασμούς και σε πιστωτικές κάρτες[31].” Στη συνέχεια, οι τραπεζικοί αυτοί λογαριασμοί ή τα στοιχεία των πιστωτικών καρτών είτε τυγχάνουν άμεσης εκμετάλλευσης από τους εγκληματίες είτε πωλούνται σε τρίτους για εκμετάλλευση σε μεταγενέστερο χρόνο. Το χαρακτηριστικό γνώρισμα, σύμφωνα με αυτή την προσέγγιση του κυβερνοεγκλήματος είναι το οικονομικό κέρδος. Σύμφωνα με το ειδησεογραφικό πρακτορείο Reuters, “η ετήσια ζημιά στην παγκόσμια οικονομία [από το κυβερνοέγκλημα] υπολογίζεται στα 445 δισεκατομμύρια δολάρια[32].” Περίπου 1,5 δισεκατομμύρια δολάρια χάθηκαν λόγω ηλεκτρονικής απάτης το 2012 στις Η.Π.Α.[33]

Ορισμένες προσεγγίσεις εντάσσουν κάτω από την κατηγορία του κυβερνοεγκλήματος την κυβερνοαπάτη (computer fraud), την κυβερνοτρομοκρατία (cyberterrorism), τον κυβερνοεκβιασμό (cyberextortion) ακόμη και τον κυβερνοπόλεμο (cyberwarfare), αναδεικνύοντας έτσι με τον καλύτερο τρόπο το αυθαίρετο της κατάταξης και του διαχωρισμού αυτών των συναφών, αλλά όχι ίδιων εννοιών. Από τις μεθοδικότερες προσεγγίσεις τόσο του όρου όσο και της έννοιας του κυβερνοεγκλήματος συναντάμε στην ανάλυση της Susan W. Brenner, στο άρθρο της με τίτλο “’At Light Speed’ :Attribution and Response to Cybercrime/Terrorism/ Warfare[34].”

Η ανάλυσή της ξεκινά με την παράθεση στοιχείων γύρω από την επίθεση που δέχτηκε το υπολογιστικό σύστημα του Γραφείου Βιομηχανίας και Ασφάλειας (BIS), τον Οκτώβριο του 2006. Η επίθεση αυτή ανάγκασε το BIS να αποσυνδέσει τους υπολογιστές του από το διαδίκτυο, κάτι το οποίο στέρησε από τους υπαλλήλους του τη δυνατότητα να συνεχίσουν την εργασία τους. Η επίθεση ανιχνεύτηκε οτι

---

[29] Halder, D., and Jaishankar, K., *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations* (Hershey:IGI Global, 2011).

[30] ο.π.

[31] Richard Clarke, ραδιοφωνική συνέντευξη με την Eleanor Hall (ABC Local Radio), 7 Δεκεμβρίου 2010.

[32] “Cyber crime costs global economy $445 billion a year: report,” Reuters (US edition), http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609 (accessed 24 December, 2015).

[33] “Cybercrime,” Wikipedia, https://en.wikipedia.org/wiki/Cybercrime#cite_note-igiglobal.com-3 (accessed 24 December, 2015).

[34] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 379-475.

προέρχονταν από ιστοσελίδες που φιλοξενούνταν σε κινεζικά υπολογιστικά συστήματα παροχής υπηρεσιών διαδικτύου, εντούτοις “οι υπεύθυνοι της επίθεσης ουδέποτε αναγνωρίστηκαν.” Το άρθρο αναφέρει στο σημείο αυτό:

> *Σκεφτείτε για λίγο αυτή την δήλωση: οι υπαίτιοι της επίθεσης ουδέποτε αναγνωρίστηκαν. Η δήλωση αυτή έχει πολλαπλές επιπτώσεις, με κυριότερη το οτι τα συγκεκριμένα άτομα που διέπραξαν την επίθεση δεν αναγνωρίστηκαν. Αυτό είναι εξαιρετικά αξιοσημείωτο. Με δεδομένες τις ευκαιρίες που ο κυβερνοχώρος δίνει για πραγματοποίηση παρόμοιων επιθέσεων από απομακρυσμένα σημεία και για ανωνυμία των δραστών, είναι κατά κανόνα αναμενόμενο οι κυβερνοεγκληματίες να μην εντοπίζονται και να μη συλλαμβάνονται*[35]

Και στη συνέχεια αναρωτιέται εαν πράγματι, με δεδομένο τον μη εντοπισμό των δραστών (παρόλο το δεδομένο της γεωγραφικής προέλευσης της επίθεσης, Κίνα) τι είδους απίθεση ήταν: Κυβερνοέγκλημα; (κινέζοι χάκερ εξαπέλυαν επαναστατικό χτύπημα σε κρατικούς υπολογιστές των Η.Π.Α.) Κυβερνοτρομακρατία; (αρχική προσπάθεια τρομοκρατών, όχι απαραίτητα κινεζικής καταγωγής, να καταρρεύσουν κρατικοί υπολογιστές των Η.Π.Α. με σκοπό την πραγματοποίηση των ιδεολογικών τους πεποιθήσεων) ή κυβερνοπόλεμος; (μία επιθετική ενέργεια των κινεζικών ενόπλων δυνάμεων). Πριν διαχωριστούν οι τρεις αυτές φαινομενικά παρόμοιες αλλά ουσιαστικά πολύ διαφορετικές έννοιες, πρέπει να ξεκαθαριστεί ο όρος κυβερνοαπειλή.

Σύμφωνα με την Susan Brenner, “Κυβερνοαπειλή (cyberthreat) γενικά είναι η χρήση της τεχνολογίας των υπολογιστών με σκοπό την εμπλοκή τους σε δραστηριότητες οι οποίες υποδαυλίζουν την ικανότητα της κοινωνίας να διατηρήσει την εσωτερική και την εξωτερική τάξη.” Η αναφορά σε εσωτερική και εξωτερική τάξη έλκει την προέλευσή της από τις πολιτικές επιστήμες. Σε ιστορική βάση, κάθε κοινωνία χρησιμοποιεί δύο στρατηγικές, απαραίτητες για τη διατήρηση της τάξης και την επιβίωση αλλά και την ευημερία της ίδιας της κοινωνίας. Η εσωτερική τάξη της κοινωνίας διατηρείται με την καθιέρωση και την εφαρμογή κανόνων, αυτό που στα σημερινά δεδομένα ονομάζεται ποινικό δίκαιο. Έτσι, τα μέλη που θα σκεφτόντουσαν να δράσουν κατά τρόπο διαφορετικό από αυτόν που οι κοινά θεσπισμένοι κανόνες επιτρέπουν (διάπραξη ληστείας, φόνου κλπ), αποθαρύνονται από το ποινικό δίκαιο και την σκέψη της τιμωρίας. Η εξωτερική τάξη, από την άλλη πλευρά, εξασφαλίζεται ουσιαστικά από τις ένοπλες δυνάμεις (πόλεμος, εαν χρειαστεί) και από τις διεθνείς συμφωνίες (σύμφωνα μη επίθεσης, συμμαχίες κλπ). Η συγγραφέας ονομάζει την διφυή αυτή κατάσταση “δυική κατάσταση εσωτερικής/εξωτερικής απειλής” ενώ την επιλογή μεταξύ αστυνομικής δύναμης και στρατού “δυναμική απόκρισης σε επίθεση[36].”

Η προσέγγιση αυτή βασίζεται στην υπόθεση οτι κάθε κοινωνία καταλαμβάνει ένα γεωγραφικά καθορισμένο σημείο για το οποίο οι έννοιες “κράτος/επικράτεια” και “κυριαρχία” είναι μη διαχωρίσιμες. Έτσι, οι απειλές για την κονωνική τάξη είναι εύκολα αναγνωρίσιμες είτε ως εσωτερικές (έγκλημα, τρομοκρατία) είτε ως

[35] ο.π. σ. 380
[36] ο.π. σ. 382

εξωτερικές (πόλεμος). Η εμπλοκή των υπολογιστών, των συστημάτων και των δικτύων αλλοιώνει την θεώρηση αυτή και καθιστά την δυαδική προσέγγιση (έσω/έξω απειλή) δυσδιάκριτη αφού εισάγεται μεγάλη αμφιβολία και σχετικότητα στην έννοια "κράτος/επικράτεια." Στον 21ο αιώνα, όποιος επιθυμεί να υποσκάψει την ικανότητα της κοινωνίας να διατηρήσει την τάξη, δεν έχει παρά να εξαπολύσει εικονικές επιθέσεις από οπουδήποτε στον κόσμο αφού τέτοιες επιθέσεις δεν μπορούν με ευκολία να ενταχθούν στην δυική κατάσταση εσωτερικής/εξωτερικής απειλής ούτε στην ιεραρχική ανάθεση (αστυνομική δράση ή ένοπλες δυνάμεις) που προκύπτει ως συνέπεια της προέλευσης της απειλής (εσωτερική, εξωτερική).

Με βάση τα παραπάνω, η Susan Brenner διαχωρίζει με ευθείες γραμμές τους τρείς κομβικούς όρους του κυβερνοεγκλήματος, της κυβερνοτρομοκρατίας και του κυβερνοπολέμου. Κυβερνοέγκλημα, σύμφωνα με το διαδικτυακά διαθέσιμο λεξικό Dictionary.com είναι "το έγκλημα που διαπράττεται σε ένα δίκτυο υπολογιστών." Σύμφωνα με την συγγραφέα του συγκεκριμένου άρθρου, "το βασικό πρόβλημα με αυτόν τον ορισμό του κυβερνοεγκλήματος είναι οτι οι Αμερικανοί νομικοί πρέπει να είναι σε θέση να εντάξουν την έννοια του κυβερνοεγκλήματος στο συγκεκριμένο νομικό πλαίσιο που χρησιμοποιείται στις Η.Π.Α. και γενικότερα, μέσα στο ευρύτερο πλαίσιο που συνδέει διάφορα δικαιικά συστήματα ανά τον κόσμο στον αγώνα εναντίον του κυβερνοεγκλήματος[37]." Έτσι, θα μπορούσε κανείς να αναρωτηθεί εαν το κυβερνοέγκλημα είναι διαφορετικό από το κοινό έγκλημα. Εαν ισχύει κάτι τέτοιο, τότε το επόμενο ερώτημα είναι ποιές είναι οι διαφορές τους. Εαν, πάλι, κυβερνοέγκλημα και κοινό έγκλημα δεν είναι διαφορετικές έννοιες, τότε το ερώτημα που προκύπτει είναι για ποιόν λόγο χρειάζεται να ορίσουμε (και μάλιστα με πολύ προσεκτικό τρόπο) το κυβερνοέγκλημα. Εαν και το νομικό πλαίσιο των εννοιών των δράσεων του κυβερνοχώρου αναπτύσσεται στο επόμενο κεφάλαιο, αξίζει να κάνουμε τις ορισμένες επισημάνσεις, αρχίζοντας από το οτι θα πρέπει να οριοθετηθεί τι είναι αλλά, κυρίως τι δεν είναι κυβερνοέγκλημα. Στη συνέχεια, θα γίνει ευκρινής η ανεπάρκεια του ορισμού που δίδεται στο κυβερνοέγκλημα στο διαδικτυακό λεξικό.

Στο ίδιο άρθρο του Journal of Criminal Law and Criminology, αναφέρεται οτι "στον ορισμό γίνεται η υπόθεση οτι κάθε κυβερνοέγκλημα συνιστά διάπραξη παραδοσιακού εγκλήματος και τίποτε περισσότερο, απλά με μη παραδοσιακούς τρόπους" δηλαδή, για παράδειγμα, αντί να χρησιμοποιηθεί ως εργαλείο του εγκλήματος ένα μαχαίρι, γίνεται χρήση του διαδικτύου. Η συγγραφέας επισημαίνει οτι αυτή η υπόθεση κατά κανόνα έχει βάση για όλα τα κυβερνοεγκλήματα που έχουμε δει ως τώρα. 'Ετσι, ουσιαστικά μιλάει για "παλιό κρασί σε νέα μπουκάλια[38]." Ισχυρίζεται, λοιπόν, οτι σχεδόν το σύνολο των εγκλημάτων σταδιακά θα μεταλαχτούν σε κυβερνοεγκλήματα εκτός, ίσως, από ορισμένα που αυτό δεν είναι εφικτό, όπως για παράδειγμα, τον βιασμό ή τη διγαμία. Καταλήγοντας, παρατηρεί οτι ενώ τα περισσότερα από τα κυβερνοεγκλήματα που έχουμε δει ως σήμερα είναι ουσιαστικά παραδοσιακά εγκλήματα που έχουν διαπραχτεί με σύγχρονα μέσα (δίκτυα υπολογιστών, διαδίκτυο κλπ), αυτό δεν είναι αληθές για το σύνολο των

[37] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 383.

[38] ο.π.

κυβερνοεγκλημάτων. Υπάρχει τουλάχιστον μια κατηγορία κυβερνοεγκλήματος που δεν αποτελεί την μοντέρνα έκδοση παραδοσιακού εγκλήματος[39]: η επίθεση άρνησης υπηρεσίας (Denial of Service attack[40], DoS ή Distributed DoS, DDoS). Στο διαδικτυακό λεξικό ορίζεται ως "το περιστατικό εκείνο κατά το οποίο ένας υπολογιστής ή ένα δίκτυο υπολογιστών καθίσταται ανενεργό διαταράσσοντας την πρόσβαση σε αυτό ή την λειτουργία του[41]." Ο σκοπός της επίθεσης αυτής είναι η υπερφόρτωση των εξυπηρετητών ώστε αυτοί να καθίστανται πρακτικά ανήμποροι να επιτελέσουν την φυσιολογική λειτουργία τους, με συνέπεια το δίκτυο να μην είναι πλεόν προσβάσιμο στους χρήστες του. Σε αυτή την κατηγορία επίθεσης κατατάσσονται όλα τα περιστατικά για τα οποία συχνά ακούμε ή διαβάζουμε και που οδηγούν σε αυτό που αναφέρεται στην ειδησεογραφία με τίτλους όπως "έπεσε η ιστοσελίδα του πενταγώνου," "έκλεισε το site του Amazon.com" κλπ. Συχνά οι επιθέσεις DDoS χρησιμοποιούνται με απώτερο σκοπό της εκβιασμό για οικονομικά οφέλη οπότε μπορεί να παραλληλιστεί με τον συνηθισμένο εκβιασμό για οικονομικούς λόγους του κοινού εγκλήματος. Ωστόσο, υπάρχουν και περιπτώσεις επιθέσεων DDoS, όπως αυτή εναντίον της ιστοσελίδας της Amazon το 2000, όπου δεν επρόκειτο ούτε για ηλεκτρονικό εκβιασμό ούτε για κάποια άλλη ηλεκτρονική μετεξέλιξη παλαιών μορφών εγκλήματος. "Αυτό είναι ένα παράδειγμα του νέου τύπου εγκλήματος: ένα καθαρό κυβερνοέγκλημα. Ως τέτοιο, απαιτεί να δημιουργήσουμε νέους νόμους οι οποίοι θα το κατατάσουν στα εγκλήματα (κυβερνοεγκλήματα).[42]"

Μετά από τα παραπάνω σημεία αιτιολογημένης διαφωνίας της συγγραφέα με τους διάφορους ορισμούς του κυβερνοεγκλήματος, η Susan Brenner προτείνει ως ορισμό του κυβερνοεγκλήματος τον εξής: "κυβερνοέγκλημα είναι η χρήση τεχνολογίας υπολογιστών για τη διάπραξη εγκλήματος, με τέτοια εμπλοκή που να απειλεί την ικανότητα της κοινωνίας να διατηρεί την εσωτερική της τάξη." Με αυτόν τον ορισμό, καλύπτεται η περίπτωση των παραδοσιακών εγκλημάτων που διαπράττονται με νέες τεχνολογίες όσο και η περίπτωση των νεοεμφανιζόμενων κυβερνοεγκλημάτων. Επιπλέον, γίνεται αναφορά σε οποιαδήποτε χρήση τεχνολογίας υπολογιστών και όχι μόνο χρήση τεχνολογίας υπολογιστικών δικτύων. Τέλος, πολύ σημαντική παρατήρηση είναι οτι ο ορισμός αυτός, εαν και νομικά πολύ βολικός, από μόνος τους δεν παρέχει την νομική αναγκαιότητα που απαιτείται, ως βάση, για την νόμιμη απόκριση σε περιστατικά κυβερνοεγκλήματος. Αυτό είναι κάτι που μας απασχολεί στο 3$^{ο}$ κεφάλαιο της εργασίας[43].

---

[39] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 384

[40] Ορισμένοι χρησιμοποιούν τον όρο "Buffer overflow attack."

[41] Dictionary.com, "*denial-of-service*," http://dictionary.reference.com/browse/denial-of-service?s=t (accessed 25 December, 2015).

[42] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 385

[43] ο.π., σ. 386.

## Κυβερνοτρομοκρατία (Cyberterrorism)

Σύμφωνα με το Dictionary.com, κυβερνοτρομοκρατία "είναι η επίθεση με βάση υπολογιστές που στοχεύει να καταστήσει ανενεργά ζωτικά υπολογιστικά συστήματα με σκοπό τον εκφοβισμό, τον εξαναγκασμό η την πρόκληση βλάβης στην κυβέρνηση ή σε τμήμα του πληθυσμού[44]." Η Wikipedia ορίζει την κυβερνοτρομοκρατία ως "μια τρομοκρατική πράξη που πραγματοποιείται μέσω της χρήσης του κυβερνοχώρου ή υπολογιστικών πόρων[45]" και αναφέρει επεξηγηματικά οτι "μια απλή πράξη προπαγάνδας στο διαδίκτυο, οτι θα υπάρξουν βομβιστικές επιθέσεις κατά τη διάρκεια των διακοπών μπορεί να θεωρηθεί κυβερνοτρομοκρατία. Επίσης, κυβερνοτρομοκρατία μπορούν να θεωρηθούν πράξεις από χάκερ εναντίον ατόμων ή οικογενειών οι οποίες έχουν οργανωθεί από ομάδες ανθρώπων μέσα σε δίκτυα και που έχουν την τάση να προκαλέσουν φόβο, να επιδείξουν δύναμη, να συλλέξουν πληροφορίες ικανές να καταστρέψουν τη ζωές άλλων ανθρώπων, ληστείες, εκβιασμοί κλπ.[46]" Στο βιβλίο με τίτλο "Terror on the Internet" ο Gabriel Weimann ορίζει την κυβερνοτρομοκρατία ως "τη χρήση δικτύων υπολογιστών για σαμποτάζ κρίσιμων εθνικών υποδομών[47]." Στο άρθρο της η Brenner αρχικά αναφέρεται σε έναν γενικό ορισμό που θεωρεί οτι "η κυβερνοτρομοκρατία συνίσταται στη χρήση τεχνολογίας υπολογιστών για τρομοκρατική δράση[48]." Ο ορισμός αυτός είναι όμοιος με τον ορισμό του κυβερνοεγκλήματος και κατά συνέπεια προκύπτει οτι οι κοινωνίες αντιμετωπίζουν το (κυβερνο)έγκλημα και την (κυβερνο)τρομοκρατία ως ένα και το αυτό. Ο λόγος που συμβαίνει αυτό είναι οτι τόσο το κυβερνοέγκλημα όσο και η κυβερνοτρομοκρατία απειλούν της εσωτερική τάξη της κοινωνίας και άρα η κοινωνία θεωρεί οτι και η αντιμετώπιση πρέπει να είναι ίδια. Παρόλη την σύγχυση αυτή, η συγγραφέας θεωρεί πως είναι απαραίτητη η διάκριση των δύο αυτών εννοιών, διότι "διαφέρουν κατά τρόπο που σχετίζεται με το πως οι κοινωνίες πρέπει να απαντήσουν σε αυτές[49]." Πέρα από αυτό, το έγκλημα είναι προσωπικό ενώ η τρομοκρατία έχει πολιτική χροιά. Η συγγραφέας προσθέτει οτι τα εγκλήματα διαπράττονται για προσωπικούς λόγους, όπως ίδιον όφελος και επιθυμία να κάνει κανείς κακό είτε με ψυχολογικό είτε με φυσικό τρόπο. Η τρομοκρατία, από την άλλη, συχνά έχει αποτέλεσμα, επίσης, την πρόκληση κακού όμως οι λόγοι που οδηγούν σε αυτό είναι πολύ διαφορετικοί. Αυτό είναι επαρκές για να διαφοροποιηθεί το έγκλημα από την τρομοκρατία.

---

[44] Dictionary.com, "cyberterrorism," http://dictionary.reference.com/browse/cyberterrorism?s=t (accessed 25 December, 2015).

[45] "Cybercrime," Wikipedia, https://en.wikipedia.org/wiki/Cybercrime (accessed 10 December, 2015.)

[46] ο.π.

[47] Gabriel (Weimann 2006)Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington D.C.: United States Institute of Peace, 2006), 148.

[48] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 386

[49] ο.π., σ.387.

Η τρομοκρατία συνήθως επιδιώκει να αποθαρρύνει τον πληθυσμό. Αυτό είναι, επίσης, επαρκής τεκμηρίωση διαφοροποίησης της τρομοκρατίας, η οποία έχει στόχο τον πολιτικό πληθυσμό, από τον πόλεμο, στον οποίο οι πολίτες υποτίθεται δεν πρέπει να στοχοποιούνται[50]. "Μέχρι σήμερα, δεν έχουν υπάρξει γνωστά περιστατικά κυβερνοτρομοκρατίας. Έχουν υπάρξει περιπτώσεις τις οποίες τα μέσα εσφαλμένα έχουν περιγράψει ως κυβερνοτρομοκρατία…αυτές οι περιπτώσεις, ωστόσο, εμπλέκουν κυβερνοέγκλημα, όχι κυβερνοτρομοκρατία…αφού σε όλες αυτές ο δράστης είχε προσωπικό κίνητρο και όχι κάποια ιδεολογία[51]." Για να γίνει ευκολότερα κατανοητό τι μπορεί να κάνει ή τι θα κάνει η κυβερνοτρομοκρατία, θα πρέπει να αναλυθεί ο τρόπος που οι τρομοκράτες χρησιμποιούν τους υπολογιστές και τα δίκτυα (συμπεριλαμβανομένου του Internet) με σκοπό να εξαχρειώσουν τον πληθυσμό και κατά συνέπεια να υποσκάψουν την ικανότητα της κοινωνίας να διαφυλάττει την εσωτερική τάξη[52]. Σε θεωρητικό επίπεδο, ο τρόπος χρήσης της τεχνολογίας των υπολογιστών για σκοπούς κυβερνοτρομοκρατίας, σύμφωνα με την εμπεριστατωμένη ανάλυση της Susan Brenner, εμπίπτει σε μία (ή συνδυαστικά, όπως προκύπτει σε περισσότερες) από τις παρακάτω περιπτώσεις:

### Όπλα Μαζικής Καταστροφής (Weapons of Mass Destruction)

Ευθύς εξαρχής ξεκαθαρίζει η αρθρογράφος[53] οτι η χρήση αυτή είναι θεωρητικής υφής αφού δεν συνιστά ρεαλιστική επιλογή. Η θεώρηση οτι η υπολογιστική τεχνολογία μπορεί να γίνει η ίδια όπλο μαζικής καταστροφής βασίζεται σε εσφαλμένη υπόθεση αφού, οι υπολογιστές από μόνοι τους δεν μπορούν να επιφέρουν φυσική βλάβη σε άτομα ή περιουσίες. Αυτή η δυνατότητα ανήκει στη δικαιοδοσία των καταστροφικών δράσεων του πραγματικού κόσμου. Εντούτοις, οι υπολογιστές *μπορούν* να κινητοποιήσουν δυνάμεις που παράγουν φυσική καταστροφή, τραυματισμό ή θάνατο ανθρώπων. Για παράδειγμα, αναφέρει το ίδιο άρθρο, "οι κυβερνοτρομοκράτες θα μπορούσαν να θέσουν εκτός ενεργείας τα συστήματα προστασίας και ελέγχου του πυρηνικού αντιδραστήρα σε κάποιο εργοστάσιο παραγωγής ηλεκτρικής ενέργειας, όπως αυτό του Chernobyl, το 1986. Αναλαμβάνοντας την ευθύνη για την καταστροφή, οι κυβερνοτρομοκράτες θα μπορούσαν να εκμεταλλευτούν τους τραυματισμούς, τους θανάτους και την ραδιολογική μόλυνση για να υπονομεύσουν την πίστη των πολιτών στις ικανότητες της κυβέρνησης να τους προστατέψει και να διατηρήσει την εσωτερική τάξη[54]." Μέχρι εδώ δεν φαίνεται να υπάρχει κάποια λογική ασυνέχεια του ισχυρισμού οτι πρόκειται περί κυβερνοτρομοκρατίας. Μπορεί το σενάριο αυτό να φαίνεται ως έγκυρο με την έννοια της τρομοκρατίας, ωστόσο δεν μπορεί να θεωρηθεί κυβερνοτρομοκρατία αφού, ενώ πράγματι η τεχνολογία υπολογιστών χρησιμοποιήθηκε για να δρομολογήσει την καταστροφική δυσλειτουργία στον

---

[50] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 388

[51] ο.π., σ. 389.

[52] ο.π.

[53] ο.π., σ. 390.

[54] ο.π., σ. 391.

πηρυνικό αντιδραστήρα του εργοστασίου, οι πολίτες θα αναφέρονται σε αυτό ως μια πυρηνική καταστροφή και όχι ως μια κυβερνοκαταστροφή. Καθίσταται προφανές οτι η συνεισφορά της χρήσης της τεχνολογίας υπολογιστών στο τελικό αποτέλεσμα είναι συμπτωματική, όσο αφορά στην ουσιαστική τρομοκρατική πράξη αλλά η ίδια δεν είναι τρομοκρατική πράξη. "Το να αποδεχτούμε αυτό το σενάριο ως κυβερνοτρομοκρατία είναι τόσο έγκυρο όσο έγκυρο θα ήταν να περιγραφεί η βομβιστική επίθεση της αμερικανικής πρεσβείας από μέλη της Al-Qaeda το 1998 ως 'αυτοκινητοτρομοκρατία', λόγω του οτι τα μέσα στα οποία ήταν τοποθετημένες οι βόμβες ήταν αυτοκίνητα[55]."

### Όπλα Μαζικού Περισπασμού (Weapons of Mass Distraction)

Αυτή η κυβερνοτρομοκρατική κατηγορία χρήσης τεχνολογίας υπολογιστών είναι τόσο θεωρητική όσο και πραγματική. Πρόκειται περί χρήσης τεχνολογίας υπολογιστών κομβικής σημασίας στην διάπραξη της τρομοκρατικής πράξης, μιάς πράξης που διαφέρει ουσιαστικά από κάποια τρομοκρατική πράξη με την παλαιά μορφή της. "Η χρήση της τεχνολογίας υπολογιστών έχει σκοπό να χειριστεί εντέχνως της ψυχολογία του πληθυσμού. Αυτός ο έντεχνος χειρισμός υποσκάπτει το ηθικό του πληθυσμού με το να υπονομεύει την πίστη των πολιτών στην κυβέρνησή τους. Ανάλογα με την περίπτωση, μπορεί ακόμη να έχει ως αποτέλεσμα τραυματισμό προσώπων, θάνατο πολιτών και καταστροφή περιουσίας[56]." Στη συνέχεια αναφέρεται ως παράδειγμα, τα γεγονότα της 11ης Σεπτεμβρίου 2001. Εκατομμύρια αμερικανών πολιτών έβλεπαν στις τηλεοράσεις τους τα γεγονότα να εξελίσσονται, ενώ αντίστοιχη ενημέρωση αντλούσαν και από το διαδίκτυο, κυρίως από τα μεγάλα διαδικτυακά ειδησεογραφικά κανάλια. Μάλιστα, ακριβώς λόγω της μεγάλης ζήτησης πληροφοριών από τη διαδικτυακή σελίδα του CNN, η πρόσβαση είχε μεγάλες καθυστερήσεις. "Τι θα συνέβαινε εάν όλοι αυτοί οι πολίτες, στην προσπάθεια να μάθουν τι συνέβαινε, αντί να οδηγηθούν στην επίσημη ιστοσελίδα του CNN, κατέληγαν να διαβάζουν τα 'νέα' από μια ιστοσελίδα που θα έλεγε: 'Παγκόσμιος πόλεμος-πυρηνικό ολοκαύτωμα στην Ευρώπη και την Αυστραλία, η Ιαπωνία ισοπεδώθηκε από επίθεση με χημικά'[57]." Η ανάρτηση τέτοιων χαλκευμένων ιστοσελίδων θα είχαν δράσει ως πολλαπλασιαστές τρόμου, επαυξάνοντας τα αποθαρρυντικά αποτελέσματα των πραγματικών τρομοκρατικών γεγονότων. Κεφαλαιώδους σημασίας είναι η διαπίστωση οτι σε αυτό το σενάριο, "δεν έγινε πραγματική χρήση όπλων[58] αλλά το οτι η τεχνολογία υπολογιστών συνιστά το εργαλείο της τρομοκρατικής πράξης[59]."

---

[55] ο.π., σ.391.

[56] ο.π.

[57] ο.π., σ. 392.

[58] Δεν αναφερόμαστε στις επιθέσεις με τα αεροσκάφη υπό αεροπειρατεία, αλλά στο σκέλος της σεναριακής εμπλοκής της τεχνολογίας υπολογιστών στην παροχή ψευδών ειδήσεων.

[59] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 393

### Όπλα Μαζικής Κοινωνικής Αναστάτωσης (Weapons of Mass Disruption)

Σε αυτή την κατηγορία ο στόχος των τρομοκρατών είναι να υποσκαφθεί η εμπιστοσύνη του πληθυσμού στην σταθερότητα και στην αξιοπιστία των απαραίτητων υποδομών, όπως μέσα μαζικών μετακινήσεων, δίκτυα και υπηρεσίες τροφοδοσίας, επικοινωνίες, χρηματοπιστωτικά ιδρύματα και υπηρεσίες παροχής υγείας. Εαν και μέχρι αυτό το σημείο ίσως να μη διαφαίνεται διαφορά μεταξύ των όπλων μαζικής αναστάτωσης και των όπλων μαζικού περισπασμού (αφού και τα δύο είδη στοχεύουν την πίστη των πολιτών έναντι των βασικών τομέων παροχών στην κοινωνία), αυτή (διαφορά) υπάρχει και σχετίζεται με το πως οι τεχνολογίες υπολογιστών χρησιμοποιούνται για να διαβρώσουν της εμπιστοσύνη του πληθυσμού στις κοινωνικές υπηρεσίες και υποδομές[60].

Στην περίπτωση εκδήλωσης τρομοκρατικής επίθεσης με στόχευση την ψυχολογική τρομοκράτηση, η χρήση της τεχνολογίας υπολογιστών ήταν για σκοπούς περισπασμού ώστε να υπονομευτεί η εμπιστοσύνη των πολιτών σε ένα ή περισσότερα συστήματα που είναι αναγκαία για την παροχή υπηρεσιών ή αγαθών. Αυτό το επιτυγχάνουν οι τρομοκράτες με το να κάνουν τους πολίτες να νομίζουν οτι ένα (ή περισσότερα) συστήματα έχουν τρωθεί και πλέον δεν λειτουργούν φυσιολογικά. Με τη διαφορά οτι οι τρομοκράτες ουδέποτε επηρρέασαν στην πραγματικότητα την λειτουργία αυτών των συστημάτων. Ο σκοπός είναι να επιτευχθεί ψυχολογική και όχι φυσική ζημιά.

Αντίθετα, στην περίπτωση που η τεχνολογία υπολογιστών χρησιμοποιείται ως μέσο μαζικής αναστάτωσης, ο στόχος των τρομοκρατών είναι πράγματι η επίτευξη ζημιάς σε ένα ή περισσότερα συστήματα. Ο τύπος πολύ συχνά κάνει αναφορές (όχι σπάνια, σεναριακού επιπέδου) για κυβερνοτρομοκράτες οι οποίοι πετυχαίνουν το κλείσιμο δικτύων ηλεκτρικής ενέργειας ή συστημάτων παροχής φυσικού αερίου ή πετρελαίου[61]. Αντίστοιχα με τη χρήση των τεχνολογιών υπολογιστών ως μέσα μαζικού περισπασμού, η χρήση τους ως μέσο μαζικής αναστάτωσης είναι τόσο θεωρητική όσο και ρεαλιστική. Η χρήση τεχνολογίας υπολογιστών είναι ανάλογη (λιγότερο ισοπεδωτική, ενδεχομένως) με την χρήση όπλων μαζικής καταστροφής στον πραγματικό κόσμο. Ο σκοπός, βέβαια, δεν είναι η πρόκληση καταστροφής του επιπέδου της 11ης Σεπτεμβρίου. Είναι πολύ πιό ύπουλος, αφού αποσκοπεί στην εξαχρείωση του πληθυσμού κάνοντας τους πολίτες να αμφισβητούν σοβαρά την ικανότητα της κυβέρνησης να διατηρεί την κατάσταση σε φυσιολογικά επίπεδα κανονικότητας και, συνεπώς να αποδομηθεί η ίδια η πολιτεία αφού δεν θα είναι σε θέση να εγγυηθεί την παροχή εκείνων των υπηρεσιών που είναι απόλυτα αναγκαίες στους πολίτες της. Ξεκάθαρα, ο στόχος αυτός είναι εξαιρετικά επικίνδυνος.

Παραδείγματος χάρη, η εξαπόλυση διαδοχικών, συγχρονισμένων επιθέσεων εναντίον μηχανών ATM[62] και άλλων συστημάτων οικονομικής υφής εύκολα εντάσσεται στη συγκεκριμένη κατηγορία. Καθώς θα προχωρά και θα εξαπλώνεται η

---

[60] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 393

[61] ο.π.

[62] Automatic Teller Machine, Αυτόματη Ταμειακή Μηχανή.

επίθεση, θα αρχίσει να γίνεται φανερή η τρομοκρατική προέλευση του προβλήματος. Επίσης, τόσο ως σενάριο όσο και ως αληθινό γεγονός, οι συνέπειες της διασποράς του κακόβουλου λογισμικού "Botnet[63]" στο νοσοκομείο Seattle's Northwest Hospital τον Ιανουάριο του 2005 εντάσσονται στην ίδια κατηγορία, παρόλο που το αρχικό κίνητρο του υπαίτιου της επίθεσης αυτής ήταν χρηματικό[64]. Σε κάθε περίπτωση, σύμφωνα με την ανακοίνωση τύπου του γραφείου του Γενικού Εισαγγελέα των Η.Π.Α., "…η διασπορά του botnet μόλυνε το δίκτυο υπολογιστών του νοσοκομείου…κάτι που οδήγησε σε αυξημένη κίνηση στο δίκτυο των υπολογιστών του νοσοκομείου…επηρεάζοντας τα συστήματα του νοσοκομείου με πολλούς τρόπους: πόρτες χειρουργείων δεν άνοιγαν, βομβητές κλήσης προσωπικού έπαψαν να λειτουργούν και υπολογιστές στην μονάδα εντατικής θεραπείας σταμάτησαν να λειτουργούν[65]."

Στο σημείο αυτό έχει ολοκληρωθεί μια προσπάθεια εννοιολογικού διαχωρισμού μεταξύ του τι συνιστά κυβερνοέγκλημα και τι κυβερνοτρομοκρατία. Εαν και συχνά τα όρια μεταξύ τους είναι δυσδιάκριτα, υπάρχουν εκείνα τα στοιχεία (μέρος των οποίων ήδη αναφέρθηκε) που επιτρέπουν την διάκριση μεταξύ των εννοιών αυτών. Ο στόχος και των δύο είναι η εσωτερική τάξη της ευνομούμενης και συνεταγμένης πολιτείας, απλά η χρήση των τεχνολογιών υπολογιστών γίνεται με διαφορετική μέθοδο και τεχνική. Η κατάσταση γίνεται περισσότερο περίπλοκη όταν εισαχθεί στην συζήτηση και μια τρίτη έννοια που εμπλέκει έγκλημα ή τρομοκρατική δράση προερχόμενη εκτός του έθνους-κράτους: τον κυβερνοπόλεμο.

## Κυβερνοπόλεμος (Cyberwarfare)

Οι Jarno και Rid θεωρούν οτι "ο κυβερνοπόλεμος είναι ένα μέρος της εξέλιξης του συμβατικού πολέμου, ο οποίος είναι άρρηκτα συνδεδεμένος με ευρύτερες κοινωνικές και πολιτικές αλλαγές[66]." Έτσι, δεν είναι πλέον εύκολο να φανταστεί κανείς κάποια σύρραξη η οποία δεν θα περιλαμβάνει κάποιο στοιχείο κυβερνοδραστηριότητας όπως η παρακολούθηση ή το σαμποτάζ. "Το να αναρωτιόματε εαν ο κυβερνοπόλεμος είναι αληθινός είναι λιγότερο σημαντικό από το να συγκεντρωνόμαστε στο πώς θα ανασχεθούν οι απειλές που προκύπτουν από τη χρήση της τεχνολογίας υπολογιστών. Άλλωστε, η κυβερνοεπίθεση δεν είναι απαραίτητο να σκοτώσει κάποιον ή να προξενήσει μεγάλη υλική ζημιά για να θεωρηθεί επικίνδυνη[67]." Ο Αντισμήναρχος της Πολεμικής Αεροπορίας των Η.Π.Α.

---

[63] http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/maxwellPlea.htm (accessed 26 December, 2015.)

[64] Τα ίδια ακριβώς αποτελέσματα θα είχε εάν πίσω από την συγκεκριμένη ενέργεια βρισκόταν αντί του δράστη κάποια τρομοκρατική ενέργεια. Μάλιστα, σε τέτοια περίπτωση η σφοδρότητα της επίθεσης θα ήταν μεγαλύτερη με σοβαρή πιθανότητα να υπήρχαν σοβαρότερες συνέπειες, όπως θάνατοι ασθενών, οι οποίοι θα αποδίδονταν σε ανεπάρκεια του νοσοκομείου (πολιτειακή ανεπάρκεια).

[65] http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/maxwellPlea.htm (accessed 26 December, 2015.)

[66] Jarno Limnell and Thomas Rid, "Is Cyberwar Real? Gauging the Threats," *Global Common Science & Technology*, April 2014.

[67] ο.π.

Gregory J. Rattray στο βιβλίο του "Strategic Warfare in Cyberspace[68]" ορίζει τον κυβερνοπόλεμο ως "στρατιωτικές επιχειρήσεις στον κυβερνοχώρο με σκοπό την επίθεση εναντίον του εχθρού και την προστασία των φίλιων κέντρων βάρους.[69]" Εναλλακτικοί ορισμοί αναφέρουν οτι ο κυβερνοπόλεμος είναι "κάθε ενέργεια που λαμβάνει χώρα στον κυβερνοχώρο και στοχεύει κατά της ισχύος μιάς χώρας ή κατά ενός μη κρατικού δρώντα (πρόσωπα, οργανισμούς, εταιρείες κλπ)[70]." Ο πρώην σύμβουλος ασφαλείας του Λευκού Οίκου, Richard Clarke, αναφέρει οτι "Ο κυβερνοπόλεμος είναι η καταστροφή, η αναστάτωση ή η πρόκληση ζημιάς σε συστήματα του πραγματικού κόσμου μέσω των επιθέσεων με συστήματα υπολογιστών, κάτι που συμβαίνει μόνο κατά τη διάρκεια κάποιου πολέμου ή, υποθέτω, κάποιας μυστικής δράσης. Άρα, πρόκειται να συμβεί όταν κράτη θα πάνε σε πόλεμο μεταξύ τους[71]." Ο Jonathan Kirshner θεωρεί οτι ο κυβερνοπόλεμος είναι αναπόσπαστο τμήμα της παγκοσμιοποίησης και οτι αποτελεί μια νέα στρατηγική απειλή[72].

"Ο κυβερνοπόλεμος δεν είναι απλά ένα νέο σύνολο από επιχειρησιακές τεχνικές. Είναι ένας αναδυόμενος, κατά την άποψή μας, νέος τρόπος πολέμου που θα απαιτήσει νέες προσεγγίσεις για τη σχεδίαση και τη δημιουργία πλάνων αντιμετώπισης καθώς και νέες μορφές δογμάτων και οργάνωσης[73]." Τέλος, ο Jeffrey M. Bale, ερευνητής και αναπληρωτής καθηγητής στο Monterey Terrorism Research and Education Program αναφέρει[74] τις δυσχέρειες που υπάρχουν λόγω των επικαλυπτόμενων όρων που χρησιμοποιούνται σε διάφορες προσπάθειες να δοθεί ορισμός στην έννοια του κυβερνοπολέμου. Συχνά η κυβερνοτρομοκρατία, το κυβερνοσαμποτάζ και ο κυβερνοπόλεμος συγχέονται σε επίπεδο ορισμού ενώ δεν

---

[68] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Mass: MIT Press, 2001)

[69] Κέντρο Βάρους, στην στρατηγική είναι, κατά τον Carl von Clausewitz, όλα εκείνα τα σημεία του εχθρού εναντίον των οποίων πρέπει να συγκεντρωθεί όλη η φίλια επίθεση. Σύμφωνα με την ανάλυση του Κωνσταντίνου Κολλιόπουλου στο βιβλίο του "Η Υψηλή Στρατηγική της Αρχαίας Σπάρτης", σ. 64, η έννοια του κέντρου βάρους μπορεί να πάρει διάφορες μορφές, είτε υλικές είτε ψυχολογικές. Παραδείγματα κέντρου βάρους διαφόρων πολεμικών προσπαθειών μπορεί να είναι οι ένοπλες δυνάμεις του αντιπάλου, η βιομηχανική του παραγωγή, μια σημαντική εδαφική περιοχή, η θέληση της ηγεσίας του να συνεχίσει τον πόλεμο, η ικανότητα της πολιτικής ηγεσίας του να εξασφαλίσει την υπακοή του λαού κλπ.

[70] Βασίλειος Γιαννακόπουλος, "Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή," Geostrategy, http://www.geostrategy.gr (accessed 15 March, 2015).

[71] Richard Clarke, *Former White House security advisor warns of cyber war*, The World Today with Eleanor Hall, http://www.abc.net.au/worldtoday/content/2010/s3086792.htm (accessed 10 December, 2015.)

[72] Jonathan Kirshner, Globalization, *American Power, and International Security*, Political Science Quarterly, Vol. 123, No. 3 (Fall 2008), p. 363-389

[73] John Arquilla and David Ronfeldt, Cyberwar is Coming!, Comparative Strategy, Vol. 12, No. 2 (Spring 1993), p. 141-165

[74] Jeffrey M. Bale, Deciphering Islamism and Terrorism: Review Article, Middle East Journal, Vol. 60, No. 4 (Autumn 2006), p. 777-788

είναι λίγες οι φορές που εμφανίζονται επιπλέον συναφείς όροι, όπως δικτυακός πόλεμος (netwar).

Το φθινόπωρο του 2006, η Πολεμική Αεροπορία των Η.Π.Α. υιοθέτησε νέα δήλωση της αποστολής της, σύμφωνα με την οποία θα πρέπει να είναι ικανή να "πολεμήσει στον αέρα, στο διάστημα και στον κυβερνοχώρο[75]." Η νέα αυτή δήλωση αναγνωρίζει αυτό που ήταν φανερό για ορισμένο καιρό: ο πόλεμος μπορεί και θα μεταναστεύσει προς τον κυβερνοπόλεμο[76]. Συνεχίζοντας, η Susan Brenner παραθέτει την δική της εκδοχή του ορισμού του κυβερνοπολέμου: "Κυβερνοπόλεμος είναι η πραγματοποίηση στρατιωτικών επιχειρήσεων με εικονικά μέσα. Συνίσταται στη χρήση του κυβερνοχώρου από τα κράτη ώστε αυτά να επιτύχουν το ίδιο αποτέλεσμα που επιδιώκουν μέσω της χρήσης συμβατικών στρατιωτικών δυνάμεων: να αποκτήσουν, δηλαδή, πλεονεκτήματα έναντι των ανταγωνιστικών κρατών ή να αποτρέψουν τα εχθρικά κράτη να αποκτήσουν πλεονεκτήματα έναντι αυτών των ιδίων[77]." Η αρθρογράφος επισημαίνει οτι αυτό είναι κάτι που ήδη συμβαίνει, υπό κάποια έννοια, αναφερόμενη σε αναφορές που φέρουν την Κίνα να εξαπολύει κυβερνοεπιθέσεις που στοχεύουν να σακατέψουν[78] τις υποδομές της Ταϊβάν και να παραλύσουν την κυβέρνηση και την οικονομία της. Σημείο προσοχής είναι οτι στον ορισμό αναφέρεται οτι ο κυβερνοπόλεμος είναι αγώνας μεταξύ κρατών. Όπως και στην τρομοκρατία, ο πόλεμος οδηγεί στην καταστροφή περιουσίας και στον τραυματισμό και στο θάνατο ανθρωπων. Αντίθετα με την τρομοκρατία όμως, ο πόλεμος είναι περιορισμένος σε συγκρούσεις μεταξύ συνόλων ανθρώπων, τους στρατούς οι οποίοι δρουν αντί του κράτους τους. Πράγματι συμβαίνει να σκοτώνονται και να τραυματίζονται πολίτες, όμως αυτό θεωρείται παράπλευρο γεγονός (συχνά ονομάζεται "παράπλευρες απώλειες".) Εντούτοις, το κυρίαρχο στοιχείο συγκέντρωσης της προσοχής και της προσπάθειας είναι ο θρίαμβος επί του στρατού του εχθρικού κράτους[79].

Στην πραγματικότητα, πάντα θα υπάρχει κάποια ασάφεια για το αν κάποιο γεγονός είναι έγκλημα η τρομοκρατική πράξη, ωστόσο η περίπτωση του πολέμου δεν επιδέχεται ασαφειών και είναι ξεκάθαρη. Αυτό συμβαίνει διότι ο πόλεμος είναι μοναδικός αφού μόνο κράτη έχουν τα μέσα και τους πόρους για να εξαπολύσουν πόλεμο στην ξηρά, στη θάλασσα ή στον αέρα εναντίον άλλου κράτους. Επίσης, όσοι εμπλέκονται ως εμπόλεμοι φορούν στολές, με διακριτικά που τους ταυτοποιούν ως μέλη των ενόπλων δυνάμεων συγκεκριμένου κράτους[80]. Και, ίσως το πιό σημαντικό, ο πόλεμος στον πραγματικό κόσμο έχει ως αναπόσπαστο χαρακτηριστικό του την παραβίαση εθνικών συνόρων αφού τα κράτη χαρακτηρίζονται από την επικράτεια

---

[75] Air Force Link-Welcome, http://www.af.mil/main/welcome.asp (accessed 21 April, 2007.)

[76] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 401

[77] ο.π.

[78] Αυτός είναι ο ακριβής όρος που χρησιμοποιείται στο πρωτότυπο.

[79] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 403

[80] ο.π.

που ελέγχουν. Αυτός ακριβώς είναι και ο λόγος που η απάντηση ενός κράτους σε κάποια εξωτερική απειλή είναι ο πόλεμος (εαν και αυτή δεν είναι πάντα η μόνη επιλογή.) Η απειλή για την κοινωνική τάξη προέρχεται όχι από κάποιους εσωτερικά στο κράτος αλλά από κάποιο άλλο κράτος, αναγκαστικά από το "εξωτερικό[81]." Στον πραγματικό κόσμο μπορεί να υπάρχει κάποια αβεβαιότητα για το εαν κάποιο γεγονός είναι έγκλημα η τρομοκρατία, κάτι που όμως έχει μικρή αξία αφού η απόκριση και για τα δύο είναι παρόμοια μιάς και τα δύο απειλούν την εσωτερική τάξη. Επιπλέον, η μονοπωλιακή έννοια του εδάφους αλλά και της στρατιωτικής δράσης από τα κράτη και μόνο από αυτά σημαίνει οτι στον πραγματικό κόσμο δεν θα είμαστε ποτέ αντιμέτωποι με την αβεβαιότητα του εαν αυτό που συμβαίνει είναι απειλή της εσωτερικής τάξης (έγκλημα ή τρομοκρατία) ή απειλή της ικανότητας του κράτους να διατηρήσει την εξωτερική τάξη (πόλεμος). Στον πραγματικό κόσμο, μόνο τα κράτη κάνουν πολέμους[82]. Έτσι, η δυική κατάσταση εσωτερικής/εξωτερικής απειλής που αναλύθηκε παραπάνω, στον πραγματικό κόσμο, διατηρείται στο ακέραιο.

Αντίθετα, η δυική κατάσταση εσωτερικής/εξωτερικής απειλής παύει να ισχύει όταν οι επιθέσεις συμβαίνουν στον εικονικό κόσμο. Δίνοντας σε μη κρατικούς δρώντες πρόσβαση σε μιά νέα, διάχυτη μορφή ισχύος, ο κυβερνοχώρος παύει το μονοπώλιο των κρατών στην ικανότητα να κάνουν πολέμους και ουσιαστικά ισοπεδώνει το πεδίο της αντιπαράθεσης ανάμεσα σε όλου τους δρώντες[83]. Από την οπτική των διεθνών σχέσεων, τα στεγανά του έθνους-κράτους παύουν να είναι αδιαπέραστα σε σημείο που να μπορεί να ισχυριστεί κάποιος οτι ο κυβερνοπόλεμος έθεσε τις βάσεις για το τέλος του έθνους κράτους, όπως το γνωρίζουμε για πολλούς αιώνες τώρα και σήμανε την απαρχή μιάς μετά-Βεστφαλιανής εποχής. Το πολύ σημαντικό αυτό ζήτημα αλλά κυρίως τις επακόλουθες δυσκολίες στην αντιμετώπιση του κυβερνοπολέμου το εξετάζουμε διεξοδικά στο 3$^{ο}$ κεφάλαιο. Στη συνέχεια θα επιχειρηθεί να οριοθετηθεί η έννοια του λεγόμενου Υβριδικού Πολέμου, ο οποίος έχει κάνει ήδη την εμφάνισή του στο προσκήνιο ορισμένων συρράξεων χαμηλού προφίλ και έτσι έχει δώσει στο θέμα του κυβερνοπολέμου μια διάσταση ρεαλιστικής παρουσίας.

## Υβριδικός Πόλεμος (Hybrid Warfare)

Ο Joseph Nye Jr., πρώην υφυπουργός Άμυνας των Η.Π.Α. και καθηγητής του πανεπιστημίου του Harvard, στο πλαίσιο ενός πάνελ (για το μέλλον του στρατού) κατά τη διάρκεια του Παγκόσμιου Οικονομικού Φόρουμ στο Νταβός, ερωτηθείς για το για ποιο είδος πολέμου πρέπει να ετοιμάζονται οι σημερινού στρατοί, μεταξύ άλλων απάντησε:

> *Ο πόλεμος τέταρτης γενιάς που διεξάγεται σήμερα δεν έχει καθορισμένα μέτωπα. Επικεντρώνεται στην κοινωνία του εχθρού,*

[81] Brenner, Susan W. 2007. *"At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare*. *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 404

[82] ο.π.

[83] ο.π.

*φθάνοντας βαθιά μέσα στην επικράτειά του για να καταστρέψει την πολιτική βούληση. Θα μπορούσαμε να προσθέσουμε και μια πέμπτη γενιά στην οποία η τεχνολογία, όπως τα μη επανδρωμένα αεροσκάφη και οι επιθετικές τακτικές στον κυβερνοχώρο, επιτρέπει στους στρατιώτες να παραμένουν πολύ μακριά από τους άμαχους στόχους τους*[84]

Και συμπλήρωσε αμέσως μετά, επεξηγώντας την αναφορά που έκανε για το διαχωρισμό του πολέμου σε γενιές, οτι:

*Αν και ο διαχωρισμός σε γενιές είναι λίγο αυθαίρετος, αντικατοπτρίζει μια σημαντική τάση: τη σύγχυση ανάμεσα στο στρατιωτικό μέτωπο και στα μετόπισθεν με τους αμάχους. Η στροφή αυτή επισπεύδεται λόγω του οτι ο πόλεμος μεταξύ κρατών αντικαθίσταται από ένοπλες συγκρούσεις μεταξύ μη κρατικών παικτών όπως αντάρτικες ομάδες, τρομοκρατικά δίκτυα, πολιτοφυλακές και εγκληματικές οργανώσεις. Η σύγχυση ενισχύεται από το γεγονός οτι οι ομάδες αυτές αλληλοεπικαλύπτονται ενώ ορισμένες υποστηρίζονται ακόμη και από κράτη. Οι Επαναστατικές Ενοπλες Δυνάμεις της Κολομβίας - η παλαιότερη αντάρτικη οργάνωση της Λατινικής Αμερικής - συμμάχησε με καρτέλ ναρκωτικών. Ορισμένες ομάδες Ταλιμπάν στο Αφγανιστάν και αλλού σύναψαν στενές σχέσεις με διεθνείς τρομοκράτες της Αλ Κάιντα. Οι αντάρτες της Ανατολικής Ουκρανίας πολεμούν δίπλα σε ρώσους στρατιώτες*[85]

Θα μπορούσε, βέβαια, κανείς να αναρωτηθεί εαν ο υβριδικός πόλεμος απαιτεί την ανάπτυξη νέων όπλων, τη χρήση καινοτόμων τεχνολογιών ή επιστημονικών ανακαλύψεων. Σε τέτοια περίπτωση, ένας πολύ μεγάλος αριθμός κρατικών ή μη-κρατικών δρώντων θα έμενε έξω από τη συμμετοχή σε υβριδικούς πολέμους αφού δεν θα είχε τα μέσα που η συγκεκριμένη υπόθεση θα απαιτούσε. Ωστόσο, αυτή η υπόθεση είναι εσφαλμένη, διότι

*Στους υβριδικούς αυτούς πολέμους χρησιμοποιούνται διάφορα όπλα - και δεν διαθέτουν όλα δύναμη πυρός. Με μια κάμερα σε κάθε κινητό - για να μην αναφερθούμε στην υπεροχή των κοινωνικών μέσων δικτύωσης - ο ανταγωνισμός της πληροφορίας έχει αναδειχθεί σε κρίσιμη πλευρά του σύγχρονου πολέμου. Στον υβριδικό πόλεμο, συμβατικές και μη συμβατικές δυνάμεις,*

[84] Joseph Nye Jr., "Ο πόλεμος στον 21ο αιώνα," Το Βήμα online, 10 Φεβρουαρίου 2015, http://www.tovima.gr/printarticle/?aid=675494
[85] ο.π.

*στρατιώτες και άμαχοι, καταστροφές και χειρισμός της πληροφορίας μπλέκονται μεταξύ τους*[86]

Τέλος, δίδοντας το στίγμα του ως ακαδημαϊκός αλλά και με την ιδιότητα του υφυπουργού των Η.Π.Α., διέγραψε τους ενδεχόμενους κινδύνους από την έλευση του υβριδικού πολέμου ενώ ταυτόχρονα παρέθεσε τα αναγκαία επόμενα βήματα για τους διεθνείς δρώντες υπό την οπτική της προετοιμασίας τους έναντι του υβριδικού πολέμου, λέγοντας

*Η απρόβλεπτη εξέλιξη του πολέμου αποτελεί σοβαρή πρόκληση. Σε ορισμένα αδύναμα κράτη, οι εσωτερικές απειλές παρέχουν σαφείς στόχους. Οι ΗΠΑ όμως πρέπει να συνδυάσουν τη συνέχιση της υποστήριξης των συμβατικών στρατιωτικών δυνάμεων, που αποτελούν σημαντικό αποτρεπτικό στην Ευρώπη και στην Ασία, με την επένδυση σε ένα ευρύ φάσμα εναλλακτικών ικανοτήτων, το οποίο απαιτούν οι συγκρούσεις στη Μέση Ανατολή. Σε εποχές αλλαγών άνευ προηγουμένου, οι ΗΠΑ - και άλλες μεγάλες δυνάμεις - πρέπει να είναι έτοιμες για όλα*[87]

Εκτός από τον Nye, στον ακαδημαϊκό χώρο από καιρό εμφανίστηκε η ιδέα του υβριδικού πολέμου. Ωστόσο δεν ήταν παρά τον Φεβρουάριο του 2014, στην Κριμαία όταν ο υβριδικός πόλεμος έκανε το παγκόσμιο ντεπούτο του, τουλάχιστον με την σύγχρονη μορφή του. Έτσι, στην προσπάθεια να οριοθετήσουμε την έννοια του υβριδικού πολέμου, μπορούμε να πούμε οτι ο σύγχρονος πόλεμος είναι χαοτικός απρόβλεπτος και άλυτος. Αυτό δεν είναι κάτι που μας είναι άγνωστο. Στις σημερινές απειλές, υφίστανται ως επιλογές (εκτός από τη μάχη), η χρησιμοποίηση των διπλωματικών μεθόδων, των σύγχρονων επικοινωνιών, της ψηφιακής διπλωματίας μέσω των κοινωνικών δικτύων και των διαμορφωτών της κοινής γνώμης. Αυτό το σύνολο μεθόδων, προσπαθειών, κινήσεων, είναι γνωστό ως υβριδικός πόλεμος. Αυτή είναι η συνειδητοποίηση της νέας πραγματικότητας του πολέμου. Γενικεύοντας υβριδικός πόλεμος είναι μια στρατιωτική στρατηγική που συνδυάζει συμβατικά μέσα, ασύμμετρες επιθέσεις και κυβερνοπόλεμο, όπως για παράδειγμα οικονομικές πιέσεις, στρατιώτες με υπερσύγχρονο εξοπλισμό που όμως δεν φορούν εθνόσημα, επιβολή κυρώσεων, προπαγάνδα, κυβερνοπόλεμος, κατασκοπεία. Αυτά είναι, όπως όλα δείχνουν, η νέα μορφή που έχουν οι συγκρούσεις σε μεγάλο μέρος του πλανήτη. Το ΝΑΤΟ ονομάζει αυτό το νέο φαινόμενο ”υβριδικό πόλεμο” και θεωρεί οτι κύριος εκφραστής αυτού του είδους πολέμου είναι η Ρωσία. Στη θεωρία του πολέμου, οι μορφές του υβριδικού πολέμου δεν είναι κάτι το καινούργιο. Ο μεγάλος Κινέζος θεωρητικός του πολέμου Σουν Τζου συμβούλευε πάντα τους μαθητές του να επιδιώκουν πολέμους που δεν θα χρειαστεί καν να κηρύξουν: αυτούς που κερδίζονται χωρίς μάχη. Αρκεί ένα κέντρο να συντονίζει μέτρα οικονομικής πολιτικής, κρατικής προπαγάνδας, πράξεων δολιοφθοράς και κυβερνοπολέμου σε μία μη

[86] Joseph Nye Jr., “Ο πόλεμος στον 21ο αιώνα,” Το Βήμα online, 10 Φεβρουαρίου 2015, http://www.tovima.gr/printarticle/?aid=675494
[87] ο.π.

γραμμική διαδικασία έτσι ώστε ουδέποτε να μπορεί να αποδειχθεί η πατρότητά τους[88].

Στην Κριμαία υπήρχε προετοιμασία, υπήρχαν στοιχεία εν υπνώσει. Αλλά υπήρχε και αιφνιδιασμός. Κανείς δεν περίμενε να βγουν 4.000.000 κόσμος κατά του Γιανούκοβιτς. Όλο αυτό αποκαλείται νέος πόλεμος (υβριδικός). Δεν περίμενε κανείς από ένα κράτος μεγάλο, σοβαρό και οργανωμένο όπως η Ρωσία να κάνει τέτοιο. Στον υβριδικό πόλεμο δεν μπορείς να πεις με βεβαιότητα ποιός τα κάνει όλα αυτά, άρα να έχεις και ένα συνομιλητή απέναντι σου. Κάποιοι λένε οι Ρώσοι, άλλοι οι Ουκρανοί ,άλλοι οι λεγόμενοι Warloards, άλλοι οι Τσετσένοι, άλλοι οτι ήταν άνθρωποι του Καντίρωφ (μισθοφόροι), οι λύκοι/hale angels, μοτοσικλετιστές κτλ. Επίσης υπάρχει η άποψη οτι ναι μεν το Κρεμλίνο υποστηρίζει αυτού του είδους τις επιχειρήσεις χωρίς όμως να τις ελέγχει πλήρως καθώς εμπλέκονται και οι μυστικές υπηρεσίες που καθιστά το περίπλοκο θέμα. Πως εξηγείται το γεγονός οτι απλοί άνθρωποι από τη μια μέρα στην άλλη πείσθηκαν να συμμετέχουν σε όλα αυτά; Για αυτό υποστηρίζεται οτι υπήρχαν έτοιμοι από καιρό οι θύλακες που ετοίμαζαν το έδαφος, σε βάθος χρόνου, έτσι ώστε όταν έρθουν οι κατάλληλες συνθήκες να κινητοποιήσουν σύντομα χιλιάδες ανθρώπους. Βέβαια αυτά μπορούν να γίνουν σε περιοχές με αποσχιστικές τάσεις και που συνορεύουν με χώρα που έχει βλέψεις. Παρά ταύτα όμως, η συμπεριφορά της Ρωσίας στην Ουκρανία αποτελεί μέρος μιας προσπάθειας να εξασφαλίσει εμμέσως τον έλεγχο του αποκαλούμενου «εγγύς εξωτερικού», που χάθηκε μετά την κατάρρευση της ΕΣΣΔ. Αυτή η συμπεριφορά δεν μελετήθηκε επαρκώς από τα Δυτικά κέντρα λήψεως αποφάσεων. Καθώς δεν δόθηκε από τους Δυτικούς η δέουσα προσοχή στο λεγόμενο «Δόγμα Μεντβέντεφ» του 2008, σύμφωνα με το οποίο η προστασία των δικαιωμάτων Ρώσων πολιτών (εκτός επικράτειας) αποτελεί υψίστη προτεραιότητα της ρωσικής εξωτερικής πολιτικής, ενώ η Δούμα, νομοθετώντας σχετικά από το 2009, επιτρέπει στις ρωσικές δυνάμεις να επεμβαίνουν στο εξωτερικό για την προστασία Ρώσων, με το Ρώσο πρόεδρο Πούτιν να αναφέρει μεταξύ άλλων πως η Ρωσία θα προασπίζεται, πάντα, ενεργά, τα δικαιώματα των Ρώσων και στο εξωτερικό με κάθε διαθέσιμο μέσο. Στην εξελεκτική πορεία του πολέμου με την σύγχρονη μορφή του, ολοένα και συχνότερα εμφανίζεται και μια συναφής με τον υβριδικό πόλεμο έννοια: ο απεριόριστος πόλεμος.

## Απεριόριστος Πόλεμος (Unlimited Warfare)

Ο Joseph Nye, αναφερόμενος στις νέες μορφές πολέμου, εξέφρασε την άποψη οτι με το πέρασμα του χρόνου οι περιορισμοί που θέτουν κάποια όρια στον πόλεμο θα εξασθενούν.

> *Στην Κίνα, για παράδειγμα, οι υπεύθυνοι του στρατού ανέπτυξαν μια στρατηγική «πολέμου χωρίς περιορισμούς» που συνδυάζει εργαλεία ηλεκτρονικά, διπλωματικά, του κυβερνοχώρου, τρομοκρατικά, οικονομικά και προπαγανδιστικά για να*

[88] Σημειώσεις του γράφοντος κατά τη διάρκεια παραδόσεων του μαθήματος με τίτλο "*Διεθνής Ασφάλεια και Σύγχρονες Απειλές*," Δρ. Καραγιάννης Εμμανουήλ, King's College & Πανεπιστήμιο Μακεδονίας (ΑΔΙΣΠΟ, 2015)

*εξαπατήσουν και να εξουθενώσουν τα αμερικανικά συστήματα. Οπως το έθεσε ένας κινέζος αξιωματούχος, 'ο πρώτος κανόνας του πολέμου χωρίς περιορισμούς είναι οτι δεν υπάρχουν κανόνες.' Οι τρομοκρατικές οργανώσεις, από την πλευρά τους, γνωρίζοντας οτι δεν μπορούν να κερδίσουν έναν συμβατικό στρατό πολεμώντας τον ευθέως, προσπαθούν να χρησιμοποιήσουν την ίδια τη δύναμη των κυβερνήσεων εναντίον τους. Με βίαια θεατρικό τρόπο, ο Οσάμα μπιν Λάντεν εξόργισε και προκάλεσε τις ΗΠΑ, ωθώντας τις να υπεραντιδράσουν με τρόπους που κατέστρεψαν την αξιοπιστία τους, αποδυνάμωσαν τις συμμαχίες τους στον μουσουλμανικό κόσμο και τελικά εξουθένωσαν τον στρατό τους - και, κατά κάποιον τρόπο, την κοινωνία τους*[89]

Η άποψη του Nye έχει ιδιαίτερη αξία αφού ο ίδιος του ομιλεί έχοντας υπάρξει κορυφαίο κυβερνητικό στέλεχος της κυβέρνησης των Η.Π.Α. αλλά και διακεκριμένος ακαδημαϊκός, κατά συνέπεια δεν είναι εύκολο κανείς να τον χαρακτηρίσει για τις μονόπλευρες απόψεις του, εκτός ίσως από το γεγονός οτι οι απόψεις αυτές κουβαλούν τον αμερικανικό τρόπο αντίληψης του παγκόσμιου γίγνεσθαι, κάτι που – ως bias- ισχύει γενικά για το σύνολο των ανθρώπων. Το ζήτημα του απεριόριστου πολέμου, εκτός από την εγγενή ασυμμετρία που τον χαρακτηρίζει και που δίνει χώρο για επιθέσεις κυβερνοπολέμου, έχει και ένα άλλο, πρωτόγνωρο χαρακτηριστικό: την απουσία κανόνων και ορίων, κάτι που αντανακλάται και στον όρο "απεριόριστος πόλεμος." Έτσι, υπάρχουν κάποια ερωτήματα που πρέπει να τεθούν και στη συνέχεια να απαντηθούν, με σημαντικότερο ίσως αυτό της "ηθικής." Ο Gaspar Biro, καθηγητής Διεθνών Σχέσεων στο Institute of Political Sciences of the Faculty of Law στο Πανεπιστήμιο της Βουδαπέστης, αναφέρει σχετικά:

*Άλλη ηθική νοείται στο κράτος ως την υψηλότερη συγκέντρωση πολιτικής και σε εκείνους που εκπροσωπούν το κράτος και άλλοι κανόνες αφορούν στις διαπροσωπικές σχέσεις. Η βία που χρησιμοποιείται από το κράτος υπόκειται σε διαφορετικό νομικό καθεστώς και ηθική κρίση από αυτή που ασκείται από ένα άτομο σ' ένα άλλο. Περί το τέλος του 17ου αιώνα και το πρώτο μέρος του επόμενου, οι δύο έννοιες είχαν πολλά κοινά σημεία, αν και ο πόλεμος συνέχισε να αποτελεί την ιδιαίτερη κατάσταση κατά την οποία ίσχυαν ειδικοί κανόνες. Στην Ευρώπη αναπτύχθηκε μια διεθνής γενική ηθική, η οποία καταστράφηκε τον 19ο αιώνα από τον εθνικιστικό οικουμενισμό. Κάποια έθνη είχαν μια αποστολή, ενώ τα μικρότερα μπορούσαν μοναχά να αναλογιστούν τη μοίρα τους. Με τον νέο τεχνολογικό πολιτισμό του 21ου αιώνα, βασισμένο στη γενετική, τη νανοτεχνολογία και τη ρομποτική, οι παλιοί κανόνες έχουν ολοένα και πιο περιορισμένη εφαρμογή. Σύμφωνα με*

[89] Joseph Nye Jr., "Ο πόλεμος στον 21ο αιώνα," Το Βήμα online, 10 Φεβρουαρίου 2015, http://www.tovima.gr/printarticle/?aid=675494

> *κάποιους, ο νέος κανόνας είναι οτι δεν υπάρχουν καθόλου κανόνες*[90]

Κλείνοντας το κεφάλαιο, ας σημειωθεί οτι η ηθική και το αίσθημα δικαίου σε συνθήκες πολεμικής αναμέτρησης ήταν πάντοτε έννοιες αντικρουόμενες και ενίοτε η χαλαρή ερμηνεία του τι συνιστά νόμιμο και τι ηθικό ήταν η διέξοδος των ισχυρών σε τέτοια νοητικά ψευδό-αδιέξοδα. Αδιάψευστος μάρτυρας αυτής της πραγματικότητας είναι ένα από τα συγκλονιστικότερα, από πλευράς "Realpolitik", αποσπάσματα του περιβόητου διαλόγου των Μηλίων, του Θουκυδίδη:

> *Νομίζουμε οτι και εμείς και εσείς πρέπει να επιδιώξουμε ότι πραγματικά θεωρούμε εφικτό, αφού ξέρουμε και ξέρετε πως κατά την ανθρώπινη λογική μπορούμε να μιλάμε για δίκαιο όταν τα δύο μέρη έχουν ίση ισχύ και οτι οι ισχυροί πράττουν ότι τους επιτρέπει η δύναμη τους και οι αδύναμοι υποχωρούν και το αποδέχονται*[91].

Το "ηθικόν" του θέματος του κυβερνοπολέμου είναι κάτι που αποτελεί πραγματική ερευνητική πρόκληση σε επίπεδο διεθνών σχέσεων, ωστόσο ξεφεύγει από τον σκοπό της παρούσας εργασίας. Το νομικό σκέλος ωστόσο, και ιδιαίτερα σε επίπεδο διεθνούς δικαίου, είναι το αντικείμενο με το οποίο θα ασχοληθούμε στο αμέσως επόμενο κεφάλαιο.

[90] Gaspar Biro, "*Ηθική και Διεθνείς Σχέσεις*," International Relations Quarterly, Vol. 4, No. 1, Spring 2001.
[91] Θουκυδίδης, *Ιστορία (Βιβλίο Ε 89)* (Αθήνα: Εκδόσεις ΠΟΛΙΣ, 2014), 779.

## 3. ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΚΑΙ ΥΦΙΣΤΑΜΕΝΟ ΔΙΕΘΝΕΣ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

> *Πρέπει λοιπόν να μάθετε οτι υπάρχουν δύο είδη αγώνα: ο ένας με τους νόμους, ο άλλος με τη δύναμη: ο πρώτος ταιριάζει στον άνθρωπο, ο δεύτερος στα θηρία: αλλά, επειδή ο πρώτος πολλές φορές δε φτάνει, χρειάζεται να καταφύγει κανείς στο δεύτερο*[92]

### Γενικά

Στην παραπάνω εισαγωγική φράση ο Μακιαβέλλι αναφέρεται στους νόμους με μια αφηρημένη έννοια, ωστόσο η σύγκριση με την άλλη εναλλακτική που παρουσιάζει, τη δύναμη, δείχνει την αντίληψη της εποχής περί αναγκαιότητας ύπαρξης κάποιου συνόλου κανόνων, μάλλον ευρείας αποδοχής, η συμπόρευση με τους οποίους χαρακτήριζε τους πολιτισμένους λαούς. Βέβαια, την εποχή που Μακιαβέλλι συνέγραψε το βιβλίο "ο Ηγεμόνας" το διεθνές δίκαιο δεν αποτελούσε καινοτομία αφού προϋπήρχε. Άλλωστε, όπως αναφέρει ο Βασίλης Περγαντής, "Σύμφωνα με μια πρώτη άποψη, το διεθνές δίκαιο υπάρχει από τη στιγμή που ήρθαν σε επαφή οργανωμένες κοινωνίες και δημιουργήθηκε ανάγκη ρύθμισης των μεταξύ τους σχέσεων[93]." Υπάρχουν και άλλες απόψεις σχετικά με την εμφάνιση του διεθνούς δικαίου, με τις "πλέον κρατούσες να τοποθετούν την εμφάνιση του διεθνούς δικαίου σε συγκεκριμένες γεωγραφικές ενότητες όπως Μεσοποταμία, την Ινδία ή την κλασσική Ελλάδα[94]." Για την εποχή της αρχαίας Ελλάδας αναφέρει ο Εμμανουήλ Ρούκουνας[95] οτι "η ελληνική κλασσική αρχαιότητα γνώρισε, πέρα από τον προαιώνιο θεσμό της συνθήκης, πολλούς ειδικούς θεσμούς που ερρύθμιζαν τις σχέσεις κυρίως μεταξύ των ελληνικών πόλεων: τα 'κοινά', τις συμμαχίες, τη διαλλαγή και τη μεσολάβηση, τις αμφικτυονίες, την προξενία, την πρεσβευτική ιδιότητα…" Παρόμοια είναι και η άποψη του Μιλτιάδη Σαρηγιαννίδη[96] ο οποίος καταρρίπτοντας την εσφαλμένη αντίληψη περί εμφάνισης του διεθνούς δικαίου στην Ευρώπη του 16ου αιώνα, αναφέρει "Αν και το διεθνές δίκαιο αναπτύχθηκε στην αρχαιότητα, έστω στοιχειωδώς, στη Μέση Ανατολή, την Ινδία και την Κίνα, συνιστά κοινή παραδοχή οτι ο ελληνικός και ο ρωμαϊκός πολιτισμός άσκησαν καθοριστική επιρροή στη μετέπειτα διαμόρφωση και συστηματοποίησή του." Η δομή της αρχαίας Ελλάδας, με τις πόλεις-κράτη ανά την επικράτεια δημιουργούσε την αναγκαιότητα να τυποποιηθούν κάποιοι κανόνες που θα σχηματοποιούσαν με συντεταγμένο τρόπο την αλληλεπίδραση (εμπορική, διπλωματική, πολιτιστική, αθλητική ή ακόμη και πολεμική) των πόλεων αυτών. Το περιεχόμενο των εννοιών "συνθήκη," "συμμαχία"

---

[92] Νικκολό Μακιαβέλλι, *Ο Ηγεμόνας*, (Αθήνα: Κάκτος, 2006), 133.

[93] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[94] ο.π.

[95] Εμμανουήλ Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (Αθήνα: Νομική Βιβλιοθήκη, 2015)

[96] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

και "συνομοσπονδία" εν πολλοίς καθορίσθηκε την εποχή των αρχαιοελληνικών πόλεων-κρατών. Δεν πρέπει να διαφύγει της προσοχή μας οτι την εποχή που μεσουρανούσε η ρωμαϊκή αυτοκρατορία "αναδείχθηκε η έννοια του δίκαιου πολέμου (bellum justum)[97]."

Στους αιώνες που ακολούθησαν, το διεθνές δίκαιο σχηματοποιήθηκε ανάλογα των απαιτήσεων της εποχής. Χαρακτηριστικά αναφέρεται[98] οτι την εποχή του Βυζαντίου "υιοθετήθηκε η πρακτική της σύναψης διεθνών συνθηκών…συνθηκών ειρήνης και εμπορίου." Επίσης, φάσεις όπως διαπραγμάτευση, υπογραφή και επικύρωση των συνθηκών είναι προϊόντα αυτής της περιόδου. Στην βυζαντινή επικράτεια είναι που συναντούμε για πρώτη φορά οργανωμένες υπηρεσίες αρμόδιες για την διεκπεραίωση των διεθνών σχέσεων. Την επόμενη ιστορική περίοδο, με κυρίαρχο τον "πολιτικό κατακερματισμό[99]," προέκυψε ένας ανομοιογενής χώρος με κυρίαρχη την εξουσία της Respublica Christiana. Εκεί, το θρησκευτικό στοιχείο ήταν αυτό που καθόριζε τις σχέσεις μεταξύ διαφορετικών "κρατών" και όχι σπάνια ο ορθός λόγος έμενε στη σκιά της θρησκευτικής επιταγής. Τα θέματα του πολέμου, της κυριαρχίας των νέων εδαφών, των θαλάσσιων επικονωνιών και η κυριαρχία των παράκτιων κρατών ήταν σημεία προβληματισμού και αφετηριακές αναζητήσεις που ώθησαν το διεθνές δίκαιο να εξελιχθεί περαιτέρω. "Η επόμενη σημαντική εξέλιξη σημειώθηκε με το έργο του Ολλανδού διπλωμάτη, συγγραφέα και ποιητή Hugo de Groot ή Grotius (1583-1645)[100]." Ο Grotius "εκπόνησε το 1625 την πρώτη ολοκληρωμένη και συστηματική μελέτη του διεθνούς δικαίου, το De Jure Belli ac Pacis (περί του Δικαίου στον Πόλεμο και στην Ειρήνη)[101]."

Επόμενο ορόσημο, τόσο για το διεθνές δίκαιο όσο και για την πολιτική επιστήμη γενικότερα ήταν η Συνθήκη της Βεστφαλίας, η οποία κατά τους Dailler και Pellet χαρακτηρίστηκε ως το πρώτο σύνταγμα της Ευρώπης. Εκεί, μεταξύ άλλων, αναγνωρίστηκε η ανεξαρτησία και η ισότητα των κρατών της Ευρώπης, θωρακίσθηκε η έννοια του κρατικού status quo, εισήχθη ο θεσμός της ουδετερότητας και θεμελιώθηκε ο διαχωρισμός ανάμεσα στις πνευματικές και κοσμικές αρμοδιότητες[102]. Όπως επισημαίνει ο Βασίλης Περγαντής, "η Συνθήκη της Βεστφαλίας θεωρείται χαρακτηριστικό δείγμα της αντίληψης περί του απαραβίαστου της αρχής της εθνικής κυριαρχίας[103]." Τέλος, είναι ιδιαίτερης αξίας το γεγονός οτι "…το σύστημα που εγκαθιδρύθηκε αποτέλεσε τη βάση για τη δημιουργία των εθνών-κρατών που θα συναντήσουμε στον 19ο αιώνα. Το σύστημα αυτό υπήρξε

[97] ο.π.
[98] ο.π.
[99] ο.π.
[100] Εμμανουήλ Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (Αθήνα: Νομική Βιβλιοθήκη, 2015)
[101] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)
[102] ο.π.
[103] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

αξιοσημείωτα σταθερό και κλονίστηκε μόνο από την Αμερικανική και τη Γαλλική επανάσταση[104].”

Στο επόμενο διάστημα, σημεία-σταθμοί στην εξελεκτική πορεία του διεθνούς δικαίου ήταν η Συνθήκη της Ουτρέχτης (1713) και το Συνέδριο της Βιέννης (1815) όπου “τέθηκαν οι βάσεις της μεταναπολεόντειας ευρωπαϊκής δημόσιας τάξης[105].” Έτσι, στην Τελική Πράξη του Συνεδρίου της Βιέννης έγινε μια σειρά από εξαιρετικές ρυθμίσεις, όπως οτι “καταδικάστηκε και απαγορεύτηκε ρητά το δουλεμπόριο… έγινε η διεθνοποίηση μεγάλων ποτάμιων οδών μέσα από την καθιέρωση της αρχής της ελεύθερης ναυσιπλοΐας…κωδικοποιήθηκαν σε μια πρώτη μορφή οι κανόνες για τη διπλωματική αντιπροσώπευση των κρατών…αναγνωρίστηκε η ουδετερότητα της Ελβετίας…και ξεκαθαρίστηκε οτι το σύστημα που εγκαθιδρύθηκε με το Συνέδριο της Βιέννης έδινε προτεραιότητα στη διατήρηση του status quo και στην κατάπνιξη με κάθε μέσο επαναστατικών κινήσεων για την ανατροπή των ευρωπαϊκών ηγεμόνων[106].” Την ίδια περίοδο “το διεθνές δίκαιο καθιερώθηκε ως αυτόνομο γνωστικό πεδίο στα προγράμματα σπουδών των πανεπιστημίων…και ιδρύθηκαν δύο σημαντικού επιστημονικοί φορείς…International Law Association και το Institut de Droit International. Λίγο αργότερα, οι δύο συνδιασκέψεις στη Χάγη το 1899 και το 1907 οριοθέτησαν μια ξεχωριστή περίοδο άνθησης για το διεθνές δίκαιο[107].”

Το επόμενο διάστημα τα θέματα που κυριάρχησαν ήταν ο αφοπλισμός και ο έλεγχος των εξοπλισμών ενώ τέθηκαν και οι πρώτοι κανόνες του μετέπειτα ανθρωπιστικού δικαίου. Εισήχθη “ο θεσμός της διεθνούς διαιτησίας με την ίδρυση του Διαρκούς Διαιτητικού Δικαστηρίου για την προσφυγή των κρατών για επίλυση των διαφορών τους…ενώ ένα αναντίρρητο επίτευγμα της Χάγης αποτέλεσε η ενσωμάτωση της ρήτρας Martens[108], κορωνίδα μέχρι τότε του δικαίου του πολέμου.” Οι βασικές προβλέψεις της στόχευαν στην προστασία τόσο των εμπολέμων όσο και των αμάχων αφού προέβλεπε οτι “η μεταχείριση των αμάχων και των εμπολέμων βασιζόταν τόσο στις αρχές και τα έθιμα του διεθνούς δικαίου όσο και ‘στην φιλανθρωπία και τις απαιτήσεις της δημόσιας συζήτησης’[109].”

Μετά την αποτυχία αποτροπής του Α’ παγκοσμίου πολέμου, η πρώτη “απόπειρα θεσμικής οργάνωσης σε οικουμενικό επίπεδο ήταν η ίδρυση της Κοινωνίας των Εθνών.[110]” Τόσο λόγω της σύνδεσής της με τη Συνθήκη των

---

[104] ο.π.

[105] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

[106] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[107] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

[108] ο.π.

[109] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[110] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

Βερσαλλιών (κάτι που της προσέδωσε το χαρακτήρα της δικαιοσύνης των νικητών) όσο και λόγω της μη επικύρωσής της από την Γερουσία των Η.Π.Α., η ΚτΕ δεν κατάφερε να αποδώσει στο διεθνή χώρο αυτό που ήταν αναμενόμενο. Η αποτυχία της φάνηκε με την είσοδο του κόσμου στον Β' Παγκόσμιο Πόλεμο.

Σύμφωνα με τον Βασίλη Περγαντή,

> *Ο Β' Παγκόσμιος Πόλεμος έχει αφήσει το αποτύπωμά του στο διεθνές δίκαιο και το διεθνές σύστημα. Η χρήση πυρηνικών όπλων, η ανάδυση του διεθνούς ποινικού δικαστηρίου μέσα από τις δίκες της Νυρεμβέργης και του Τόκυο, το Ολοκαύτωμα, και η μεταπολεμική θεσμική συγκρότηση της διεθνούς κοινωνίας με πιό σημαντικούς πυλώνες τον Οργανισμό Ηνωμένων Εθνών, το σύστημα Bretton Woods, και τη διαδικασία της ευρωπαϊκής ολοκλήρωσης, έχουν στη βάση τους την εμπειρία του μεσοπολέμου και του Β' Παγκοσμίου Πολέμου*[111]

Έτσι, πριν ακόμη το τέλος του Β' Π.Π., οι μεγάλες δυνάμεις με τις μεταξύ τους σχετικές συζητήσεις και συναντήσεις των ηγετών τους (Χάρτης του Ατλαντικού 1941, Διασυμμαχικό Συμβούλιο στο Λονδίνο 1941, Διακήρυξη των Ηνωμένων Εθνών 1942, Διακήρυξη της Μόσχας 1943 και της Τεχεράνης 1943 και Διάσκεψη στο Dumbarton Oaks 1944) είχαν προλειάνει το έδαφος για την μεταπολεμική πραγματικότητα σε επίπεδο παγκόσμιας συνεργασίας σε θέματα που σχετίζονται με την διατήρηση της ειρήνης. Τελικά, στο Σαν Φρανσίσκο στις 26 Ιουνίου του 1945 υπογράφηκε ο Χάρτης των Ηνωμένων Εθνών από πενήντα κράτη. Ο Χάρτης αποτελείται από 111 άρθρα με το πρώτο να καθορίζει τους σκοπούς του ΟΗΕ: διατήρηση της διεθνούς ειρήνης και ασφάλειας, ανάπτυξη φιλικών σχέσεων μεταξύ των κρατών και, με γενική έννοια, την επιδίωξη διεθνούς συνεργασίας. Το προοίμιό του, αναφερόμενο στους λαούς των Ηνωμένων Εθνών, "αναδεικνύει το υποκείμενο που συντάσσει τον χάρτη[112]" αν και όπως συμπληρώνει ο Μιλτ. Σαρηγιαννίδης, "οι λαοί των Ηνωμένων Εθνών δεν αποτελούν κάποιο νομικό πλάσμα."

Στις αρχές του οργανισμού συμπεριλαμβάνονται η κυρίαρχη ισότητα (όλα τα κράτη της διεθνούς κοινότητας είναι κυρίαρχα και ισότιμα), η καλόπιστη εκπλήρωση των υποχρεώσεων που προκύπτουν από τον Χάρτη (γενική αρχή του διεθνούς δικαίου, ελλείψει κεντρικής εξουσίας) και η ειρηνική επίλυση των διεθνών διαφορών (με πληθώρα επιλογών, όπως διαπραγμάτευση, έρευνα, μεσολάβηση, συνδιαλλαγή, διαιτησία και δικαστικό διακανονισμό.)

Κυρίαρχη αξία έχει το άρθρο 2 § 4, το οποίο απαγορεύει τη χρήση (ή την απειλή χρήσης) βίας. Επιπλέον, στην προηγούμενή του παράγραφο, αναφέρεται η υποχρέωση εξεύρεσης ειρηνικού τρόπου επίλυσης των διεθνών διαφορών των μελών του οργανισμού. Τέλος, στο άρθρο 33 παρέχονται οι πιθανοί τρόποι εξεύρεσης ειρηνικής λύσης, χωρίς η σειρά με την οποία αναφέρονται οι τρόποι αυτοί να συνιστά

---

[111] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[112] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

προτεραιοποίηση αυτών[113]. Ας σημειωθεί οτι η απαγόρευση χρήσης βίας δεν ήταν κάτι θεσπισμένο από παλαιά. Είναι προϊόν του Συμφώνου Briand-Kellogg toy 1928, όπου μεταξύ άλλων, τα συμβαλλόμενα κράτη παραιτούνταν από τον πόλεμο ως όργανο της εθνικής τους πολιτικής[114]. Έτσι τόσο η ρητή μορφή της απαγόρευσης των συγκεκριμένων άρθρων όσο και η παροχή πολλών επιλογών ειρηνικής προσπάθειας επίλυσης των διαφορών συγκροτεί με στιβαρό τρόπο την βούληση του ΟΗΕ να μην αποδέχεται καμμιά λύση πλην εκείνων που ανήκουν στο πεδίο της ειρηνικής προσέγγισης. Εντούτοις, σχετικά με την απαγόρευση της χρήσης βίας υπάρχει μια εξαίρεση, το άρθρο 51, σύμφωνα με το οποίο εαν ένα κράτος μέλος δεχθεί ένοπλη επίθεση έχει το εγγενές δικαίωμα να αμυνθεί, μεμονωμένα ή συλλογικά, μέχρι το συμβούλιο ασφαλείας να λάβει τα απαραίτητα εκείνα μέτρα για τη διατήρηση της διεθνούς ειρήνης και ασφάλειας. Στο σημείο αυτό δεν θα επιχειρηθεί να προσεγγιστούν οι διάφορες ερνμηνείες που έχει λάβει το περιεχόμενο του συγκεκριμένου άρθρου ούτε θα εισέρθουμε σε άσχετες με το αντικείμενο της παρούσας εργασίας πολιτικές ερμηνείες των επιλεκτικών επικλήσεων του συγκεκριμένου άρθρου στη διάρκεια της μέχρι τώρα ιστορίας του ΟΗΕ. Αντίθετα, θα αναφέρουμε ορισμένα σημεία που έχουν αξία στην προσέγγιση του ζητήματος του κυβερνοπολέμου, σε σχέση με το συγκεκριμένο άρθρο, ξεκινώντας από την έννοια της επίθεσης.

## Η έννοια της Επίθεσης (Aggression)

Σύμφωνα με την επικρατούσα ερμηνεία, "ο όρος επίθεση αφορά στις ενέργειες που μπορεί να προβεί ένα κράτος, το οποίο διαθέτει οργανωμένες στρατιωτικές δυνάμεις και δύναται να υποστηρίξει μια στρατιωτική επιχείρηση τέτοιου μεγέθους που θα απειλήσει την εδαφική κυριαρχία ή την πολιτική ανεξαρτησία ενός άλλου κράτους[115]." Τα σημεία ενδιαφέροντος είναι:

- Η ύπαρξη δύο τουλάχιστον εμπλεκομένων
- Οι εμπλεκόμενοι να είναι κράτη
- Η επιχείρηση να είναι στρατιωτική
- Το μέγεθος της επιχείρησης να είναι τέτοιο που να απειλεί την εδαφική κυριαρχία ή την πολιτική ανεξαρτησία του άλλου κράτους

[113] Εντούτοις, σύμφωνα με τον Εμμανουήλ Ρούκουνα, οι μέθοδοι δύναται να διακριθούν σε δύο κατηγορίες: τις "διπλωματικές" (διαπραγμάτευση, καλές υπηρεσίες, έρευνα, μεσολάβηση, συνδιαλλαγή) το αποτέλεσμα των οποίων δεν είναι δεσμευτικό για τα μέρη και τις "νομικές" (διαιτησία, δικαστικός διακανονισμός) που απολήγουν σε μια απόφαση δικαιοδοτικού οργάνου με βάση το δίκαιο η οποία είναι δεσμευτική για τα μέρη.

[114] Εμμανουήλ Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (Αθήνα: Νομική Βιβλιοθήκη, 2015)

[115] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

Τα παραπάνω απαιτείται να ισχύουν σωρευτικά, ώστε να μπορεί μια πράξη βίας να θεωρηθεί επίθεση και έτσι το κράτος που την υφίσταται να έχει το δικαίωμα στην άμυνα, μεμονωμένα ή συλλογικά, βάσει του άρθρου 51.

Βέβαια, υπάρχει πληθώρα στρατιωτικών δράσεων που ούτε προσχηματικά δεν προσεγγίζουν τις απαιτήσεις του άρθρου 51, όπως χαρακτηριστικά αναφέρονται η αμερικανική εισβολή στο Αφγανιστάν μετά την 11η Σεπτεμβρίου (με την επινόηση αντικατάστασης του όρου "κράτους" από "κράτος που υποθάλπει την τρομοκρατία"), την επέμβαση των ισραηλινών δυνάμεων για απελευθέρωση ομήρων στην Ουγκάντα (1976), την επέμβαση της Ρωσίας το 2008 στη Γεωργία και την ΝΑΤΟική επέμβαση στη Λιβύη το 2011[116]. Αλλά δεν είναι μόνο το άρθρο 51 που θέτει όρους.

Το Διεθνές Δικαστήριο Δικαιοσύνης (ΔΔΔ) "έχει εισάγει πρόσθετα κριτήρια, διαμορφώνοντας έτσι ένα αυστηρότερο πλαίσιο για τη νόμιμη άσκηση του δικαιώματος στην άμυνα[117]" και ειδικότερα έκρινε "οτι η νόμιμη άσκηση του δικαιώματος στην άμυνα εξαρτάται από την αναγκαιότητα (necessity) και την αναλογικότητα (proportionality) των μέτρων που λαμβάνει το αμυνόμενο κράτος[118]"

### Αναγκαιότητα (Necessity)

Η αναγκαιότητα, σύμφωνα με τον Κωνσταντίνο Αντωνόπουλο, "αφορά το γεγονός το οποίο καθιστά την ένοπλη αμυντική δράση επιτακτική. Το άρθρο 51 προβλέπει την ένοπλη επίθεση ως τέτοιο γεγονός, αλλά η πρακτική των κρατών πριν το 1945 δεν ήταν σαφής σχετικά με την έννοια της ενόπλου επιθέσεως….Το Δικαστήριο[119] έκρινε οτι ένοπλη επίθεση είναι μόνο εκείνη η (παράνομη) χρήση βίας η οποία χαρακτηρίζεται από μέγεθος και συνέπειες που υπερβαίνουν το μέγεθος ενός απλού μεθοριακού επεισοδίου.[120]" Έτσι, το μέγεθος αλλά και οι συνέπειες παίζουν καθοριστικό ρόλο στον χαρακτηρισμό (ή μη) της πράξης βίας ως "ένοπλης επίθεσης," αφήνοντας χώρο για ευέλικτες ερμηνευτικές προσεγγίσεις. Κάτι αντίστοιχο παρατηρείται και στην έννοια της αναλογικότητας.

### Αναλογικότητα (Proportionality)

Σύμφωνα με τον ίδιο, "η προϋπόθεση της αναλογικότητας είναι εξαιρετικά σημαντική" αφού "η ένταση και το είδος, ο στόχος και ο τόπος της αμυντικής δράσης πρέπει να είναι σε στενή σχέση αναλογίας με την ένοπλη επίθεση[121]." Και εδώ παρατηρείται απουσία δυνατότητας μονοσήμαντης ερμηνείας. Ειδικά για το ενδεχόμενο ένοπλης επίθεσης κυβερνοπολέμου, δεν είναι απόλυτα κατανοητό το 'ο τόπος της αμυντικής δράσης' αφού ο κυβερνοχώρος, ο τόπος πραγματοποίησης των

---

[116] ο.π.

[117] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

[118] ο.π.

[119] Υπόθεση Νικαράγουα κατά Η.Π.Α. (Ουσία)

[120] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[121] ο.π.

κυβερνοεπιθέσεων είναι εξ' ορισμού εικονικός. Αλλά δεν είναι μόνο αυτό. Το να θεωρηθεί κάποια δράση κυβερνοπολέμου (κυβερνοεπίθεση) ως "απαγορευμένη βία" απαιτεί ιδιαίτερα καλή νομική ικανότητα ερμηνευτικής διαστολής. Ωστόσο, πρέπει να επισημανθεί οτι "υφίσταται η άποψη ορισμένων συγγραφέων καθώς και η πρακτική ενός αριθμού κρατών (π.χ. Η.Π.Α.) και του ΝΑΤΟ, να θεωρείται απαγορευμένη 'βία' στα πλαίσια του άρθρου 2 (4), η οποία ενεργοποιεί το δικαίωμα άμυνας, η αποκαλούμενη 'διαδικτυακή επίθεση' (cyberattack), δηλαδή η μη-επιτρεπόμενη παρεμβολή σε εμπιστευτικά η προστατευμένα ηλεκτρονικά δίκτυα κρατικών υπηρεσιών ή οικονομικών ιδρυμάτων[122]." Η ερμηνεία αυτή αγγίζει μόνο τις περιπτώσεις που η κυβερνοεπίθεση επιφέρει αποτελέσματα παρόμοια με της λεγόμενης kinetic action, αφού σε οποιαδήποτε περίπτωση non-kinetic effects, τέτοια ερμηνεία θα αποτελούσε ερμηνεία εκτός πνεύματος του συγκεκριμένου άρθρου. Για το ίδιο ζήτημα, δηλαδή "το κατά πόσο η επίθεση που διεξάγεται με όρους ηλεκτρονικών επιθέσεων στο σύστημα της ηλεκτρονικής υποδομής της διακυβέρνησης ενός κράτους, αποτελεί ένοπλη επίθεση σύμφωνα με το άρθρο 51 του Χάρτη…η διεθνής κοινότητα έχει απασχοληθεί, όταν η Εσθονία δέχθηκε κυβερνοεπίθεση στις ηλεκτρονικές υποδομές της (2007), ενώ η Ρωσία εξαπέλυσε κυβερνο-επιθέσεις σε βάρος των ηλεκτρονικών συστημάτων της Γεωργίας για να προπαρασκευάσει τις στρατιωτικές επιχειρήσεις της κατά της Γεωργίας (2008). Το ζήτημα αυτό δεν έχει απασχολήσει το Συμβούλιο Ασφαλείας, ωστόσο τα κράτη δίνουν ιδιαίτερη έμφαση σε αυτό, ενώ και η επιστήμη επιχειρεί να το προσεγγίσει μέσα από τη λογική της επίθεσης και της άμυνας[123]." Το γεγονός οτι το Συμβούλιο Ασφαλείας δεν έχει ασχοληθεί σοβαρά με το ζήτημα του κυβερνοπολέμου και το εάν συνιστά ή όχι 'ενοπλη επίθεση δεν σημαίνει οτι δεν υπάρχει κινητικότητα σε άλλους χώρους. Όπως αναφέρει η Μαρία-Ντανιέλλα Μαρούδα, "σημαντική είναι και η ανεξάρτητη ακαδημαϊκή μελέτη κανόνων και αρχών που αφορούν το εφαρμοστικό διεθνές δίκαιο σε συρράξεις στον Κυβερνοχώρο που καταρτίσθηκε με πρωτοβουλία του Κέντρου Αριστείας του NATO Cooperative Cyber Defence, από διεθνείς εμπειρογνώμονες μετά από μελέτη 3 ετών και δημοσιεύθηκε τον Απρίλιο του 2013 ως εγχειρίδιο Tallinn για τον Κυβερνοπόλεμο. Περιλαμβάνει 95 κανόνες που ρυθμίζουν τέτοιες συρράξεις, καθώς και τον σχολιασμό τους[124]." Τέτοιες κινήσεις και μελέτες, μπορεί να μην γεννούν κανόνες διεθνούς δικαίου, ωστόσο αποτελούν τον σπόρο για προβληματισμό υψηλού ακαδημαϊκού υπόβαθρου και θα μπορούσαν να αποτελέσουν την αφετηριακή διαδικασία τροποποίησης του υφιστάμενου IHL. Με άλλα λόγια, τέτοιες πλήρως νομικά εμπεριστατωμένες μελέτες θα μπορούσαν, ως κάποιας μορφής soft law[125], να αποτελέσουν την αρχή της προσαρμογής του IHL στην πραγματικότητα του κυβερνοπολέμου.

---

[122] ο.π.

[123] Κώστας Θ. Χατζηκωνσταντίνου, Χαράλαμπος Ελ. Αποστολίδης και Μιλτιάδης Χ. Σαρηγιαννίδης, *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο*, (Αθήνα: Σάκκουλα, 2014)

[124] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[125] Σύμφωνα με τον Εμμανουήλ Ρούκουνα, "το Soft Law (στην ελληνική αποδίδεται ως άγουρο δίκαιο, μαλακό δίκαιο, ήπιο δίκαιο) δεν είναι θετικό δίκαιο, αλλά υποδηλώνει ρυθμίσεις που περιέχονται σε κείμενα νομικώς μη δεσμευτικά,

Όπως ξεκαθαρίζει ο Μιλτιάδης Σαρηγιαννίδης, "Συμπερασματικά, σε ότι έχει να κάνει με το δικαίωμα στην άμυνα, τόσο μέσα από τη συμβατική του αποτύπωση (Άρθρο 51) όσο και στην εθιμική του διάσταση, συνιστά την εξαίρεση στον κανόνα, δηλαδή την αρχή της απαγόρευσης χρήσης βίας. Επομένως, το δικαίωμα στην άμυνα πρέπει να ερμηνεύεται συσταλτικά και το περιεχόμενό του δεν υπερκαλύπτει σε καμία περίπτωση την απαγόρευση χρήσης βίας."

Σε επίπεδο εφαρμογής, όπως σημειώνει ο Εμμανουήλ Ρούκουνας, "το άρθρο 51 επικαλούνται τόσο τα κράτη που πράγματι δέχονται ένοπλη επίθεση και δικαιούνται να απαντήσουν ενόπλως, όσο και τα κράτη που παραβιάζουν κατάφωρα τον Χάρτη και πραγματοποιούν ένοπλες επιθέσεις κατά τρίτων κρατών[126]." Και συμπληρώνοντας, αναφέρει την ερμηνευτική διευκρίνηση του Διεθνούς Δικαστηρίου της Χάγης (ΔΔΧ) στην υπόθεση των στρατιωτικών και παραστρατιωτικών δραστηριοτήτων των Η.Π.Α. στη Νικαράγουα, οτι το συμβατικό και εθιμικό δίκαιο περί άμυνας ισχύουν εκ παραλλήλου (το εθιμικό δίκαιο συμπληρώνει το Άρθρο 51).

Περί της ερμηνείας του Άρθρου 51 υπήρξε (και εξακολουθεί να υπάρχει) διεθνής νομική κινητικότητα, όπως για παράδειγμα το ψήφισμα του Ινστιτιτούτου Διεθνούς Δικαίου στη σύνοδο της Χιλής. Έτσι, σύμφωνα με το ψήφισμα, "το Άρθρο 51 συμπληρώνεται από το εθιμικό δίκαιο και η ανάγκη και η αναλογικότητα αποτελούν τους καθοριστικότερους παράγοντες για την άσκηση του δικαιώματος της άμυνας" και "δεν υπάρχει νομική βάση για την θεωρία περί της λεγόμενης 'προληπτικής άμυνας'[127]. " Το θέμα της επίθεσης, όπως και με πληθώρα άλλων θεμάτων του διεθνούς δικαίου, επιδέχεται πολλών ερμηνειών. Η ερμηνεία των διεθνών συνθηκών, άλλωστε, είναι ένας χώρος που το ίδιο το διεθνές δίκαιο θεωρεί οτι δεν αποτελεί το ισχυρότερό του σημείο. Όπως άλλωστε ξεκαθαρίζει ο Αριστοτέλης Κωνσταντινίδης, "Οι συνθήκες, όπως εξάλλου και κάθε πράξη με νομική σημασία και αποτέλεσμα στο διεθνές δίκαιο, επιδέχονται και χρήζουν ερμηνείας…Στο διεθνές δίκαιο δεν ισχύει η γαλλικής προέλευσης θεωρία της 'σαφούς πράξης' (acte claire) που ισχύει, για παράδειγμα, στο κοινοτικό δίκαιο και θα είχε ως αποτέλεσμα να χρήζουν ερμηνείας μόνο όσες πράξεις δεν είναι σαφείς[128]." Εκτός από την έννοια της επίθεσης, στο ζήτημα του κυβερνοπολέμου έχει σημασία να σταθούμε σε δύο αρχές του διεθνούς δικαίου και ιδιαίτερα του διεθνούς ανθρωπιστικού δικαίου (International Humanitarean Law, IHL), της αρχή της Διάκρισης και την αρχή της Ουδετερότητας.

## Αρχή της Διάκρισης (Principle of Distinction)

ρυθμίσεις όμως που προοιωνίζονται αναβάθμιση σε νομικούς κανόνες, όταν και εφόσον συντρέξουν οι απαραίτητες για την εδραίωσή τους προϋποθέσεις," Δημόσιο Διεθνές Δίκαιο, (Αθήνα: Νομική Βιβλιοθήκη, 2015.)

[126] Εμμανουήλ Ρούκουνας, *Δημόσιο Διεθνές Δίκαιο*, (Αθήνα: Νομική Βιβλιοθήκη, 2015)

[127] ο.π.

[128] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

Σύμφωνα με το Διεθνές Ανθρωπιστικό Δίκαιο[129] (IHL) "Η επίθεση εναντίον οποιουδήποτε στόχου δεν επιτρέπεται. Προκειμένου να διασφαλισθεί η προστασία του άμαχου πληθυσμού και της περιουσίας του, τα μέρη στη σύρραξη υποχρεούνται να διακρίνουν σε όλες τις περιστάσεις, ανάμεσα στους στρατιωτικούς στόχους και την περιουσία των αμάχων και συνακόλουθα να κατευθύνουν τις στρατιωτικές τους επιχειρήσεις μόνο κατά στρατιωτικών στόχων.[130]" Η αρχή της διάκρισης γίνεται αποδεκτή ως κανόνας εθιμικού δικαίου[131], που σημαίνει οτι δεσμεύει το σύνολο των κρατών της διεθνούς κοινωνίας. Η συζήτηση περί στρατιωτικών στόχων στο πλαίσιο του κυβερνοπολέμου είναι ανοιχτή αφού, στην καλύτερη περίπτωση δεν είναι εύκολο και στην χειρότερη είναι πρακτικά αδύνατο να γνωρίζει ο επιτιθέμενος εαν οι συνέπειες της κυβερνοεπίθεσης που θα εξαπολύσει θα μπορέσουν να περιοριστούν μόνο σε στρατιωτικούς στόχους, λόγω της φύσης του κυβερνοχώρου και της μορφής δρομολόγησης της ψηφιακής πληροφορίας στο διαδίκτυο.

## Αρχή της Ουδετερότητας (Principle of Neutrality)

Όπως ήδη αναφέρθηκε παραπάνω, ο θεσμός της ουδετερότητας εισήχθη στην μεταβεστφαλιανή Ευρώπη[132], ο οποίος προέβλεπε τα δικαιώματα και τις υποχρεώσεις για την Ελβετία. Μέρος των υποχρεώσεων των εγγυητών ήταν "να μην προβούν σε πράξεις που θα ενέπλεκαν το ουδέτερο κράτος στις διαμάχες τους, αλλά και μια σειρά υποχρεώσεων αναφορικά με την απαγόρευση χρήσης βίας που βάρυναν το ουδέτερο κράτος[133]." Έκτοτε, ο θεσμός της ουδετερότητας επεκτεινόταν και σε άλλα κράτη, ορισμένα εκ των οποίων έβρισκαν καταφύγιο πίσω από την ουδετερότητα για την επίτευξη των εθνικά καθορισμένων στόχων τους, όπως η Τουρκία. Αντίστροφα, ακόμη και εάν η ουδετερότητα κάποιου κράτους ήταν υποδειγματικά παραλληλισμένη με το διεθνές πλαίσιο των υποχρεώσεων του ουδέτερου κράτους, δεν συνιστούσε προστασία έναντι κρατών με επεκτατική διάθεση, όπως η Γερμανία. Η ουδετερότητα εξακολουθεί να αποτελεί ισχυρή δέσμευση για τη διεθνή κοινωνία και σήμερα. Επιπλέον, εκτός από δέσμευση, αποτελεί άλλη μία αναφυόμενη αιτία πολυπλοκότητας στην αντιμετώπιση του κυβερνοπολέμου, υπό το πρίσμα του διεθνούς δικαίου, για λόγους που εξετάζονται παρακάτω.

---

[129] Ο όρος "Διεθνές Ανθρωπιστικό Δίκαιο" χρησιμοποιείται παράλληλα με τον όρο "Διεθνές Δίκαιο των Ενόπλων Συρράξεων" και τον όρο "Δίκαιο του Πολέμου" κατά ταυτόσημο τρόπο (Μαρία-Ντανιέλλα Μαρούδα)

[130] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

[131] Heike Spieker, *Civilian Immunity in Crimes of War*, (1999), 84.

[132] Στην τελική πράξη του Συνεδρίου της Βιέννης, τον Ιούνιο του 1815.

[133] Κωνσταντίνος Αντωνόπουλος και άλλοι, *Το Δίκαιο της Διεθνούς Κοινωνίας*, (Αθήνα: Νομική Βιβλιοθήκη, 2014)

> *"Οι υπολογιστές ελέγχουν μεγάλο μέρος της πολιτικής και στρατιωτικής υποδομής, συμπεριλαμβανομένων των επικοινωνιών, συστημάτων παροχής ενέργειας, αποχετευτικών συστημάτων και υπηρεσιών παροχής υγείας. Στις Η.Π.Α., οι ένοπλες δυνάμεις χρησιμοποιούν πάνω από δύο εκατομμύρια υπολογιστές και πάνω από δέκα χιλιάδες τοπικά δίκτυα. Επιπρόσθετα, το διαδίκτυο παρέχει διασυνδέσεις σε υπολογιστικά δίκτυα πολιτικής και στρατιωτικής χρήσης, χωρίς διάκριση μεταξύ τους. Σύμφωνα με μία καταμέτρηση, περίπου το 95% των τηλεπικοινωνιών του υπουργείου άμυνας δρομολογείται διαμέσου δημόσιου δικτύου…*[134]*"*

Αυτά τα στατιστικά στοιχεία προκαλούν έκπληξη, με δεδομένο οτι το διαδίκτυο ξεκίνησε ως πρόγραμμα της DARPA (ARPAnet), ενός αμερικανικού στρατιωτικού ερευνητικού οργανισμού. Όπως επισημαίνει ο Jeffrey T. G. Kelsey, "Λόγω της φύσης της διασύνδεσης των πολιτικών και στρατιωτικών δικτύων υπολογιστών, το διαδίκτυο μπορεί να δρομολογεί στρατιωτικά δεδομένα διαμέσου κόμβων των οποίων η φυσική τοποθεσία είναι στην επικράτεια μη φιλικών χωρών. Ακόμη σημαντικότερο, το διαδίκτυο μπορεί να δρομολογεί στρατιωτικές επικοινωνίες της μίας ή και των δύο πλευρών διαμέσου κόμβων μιας τρίτης χώρας κατά τη διάρκεια μιας ένοπλής σύρραξης μεταξύ των δύο πρώτων χωρών….το διαδίκτυο δεν μπορεί να κάνει διάκριση μεταξύ ενδεχόμενων συμμάχων, δυνητικών εχθρών ή ουδέτερων μερών.[135]"

Ο αρθρογράφος συνεχίζει λέγοντας οτι "κατά τη διάρκεια των στρατιωτικών επιχειρήσεων, οι εμπόλεμοι έχουν καθήκον με ιδιαίτερη προσοχή να ελαχιστοποιούν το μέγεθος των απωλειών των πολιτών θυμάτων καθώς και να περιορίζουν όσο γίνεται τη ζημιά στις περιουσίες των πολιτών. Οι διοικητές πρέπει να περιορίζουν τις επιθέσεις τους αυστηρά μόνο σε στρατιωτικούς στόχους." Οι στρατιωτικοί στόχοι ορίζονται ως εκείνοι οι οποίοι έχουν σημαντική συνεισφορά στην πολεμική προσπάθεια και των οποίων η καταστροφή (ολική ή μερική) προσφέρει ξεκάθαρο στρατιωτικό πλεονέκτημα στον επιυτιθέμενο. Ορισμένοι στόχοι εξυπηρετούν τόσο πολιτικό όσο και στρατιωτικό σκοπό. Η συγκεκριμένη αυτή κατηγορία στόχων ονομάζονται μικτοί στόχοι ή στόχοι διπλής χρήσης. Παραδείγματα τέτοιων στόχων είναι οδικές ή σιδηροδρομικές γέφυρες, λιμάνια, αυτοκινητόδρομοι, σταθμοί παραγωγής ηλεκτρικής ενέργειας κλπ. Σύμφωνα με τον Jeffrey Kelsey, "εάν τέτοιοι διπλής χρήσης στόχοι συνεισφέρουν καθοριστικά στην πολεμική προσπάθεια του

[134] Gregory F. Intoccia and Joe Wesley Moore, *Communications Technology, Warfare, and the Law: Is Network A Weapon System?*, (2006: Houston Journal of International Law)

[135] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

εχθρού, τότε στόχοι που μπορεί να φαίνονται πολιτικοί μετατρέπονται σε πλήρως νόμιμους στρατιωτικούς στόχους[136]."

Σε εφαρμογή της αρχής της διάκρισης, κατά την επιλογή των (κυβερνο)στόχων έχει εφαρμογή η ίδια συλλογιστική με τους στόχους του πραγματικού κόσμου. Έτσι, σε ορισμένες περιπτώσεις η κυβερνοεπίθεση είναι πλήρως εναρμονισμένη με την αρχή της διάκρισης αφού ο κυβερνοστόχος είναι αμιγώς στρατιωτικής χρήσης. Δεν είναι λίγοι εκείνοι που πιστεύους πως "κάθε στόχος που πληροί της προϋποθέσεις της αρχής της διάκρισης για χρήση συμβατικών όπλων, αυτόματα συμμορφώνεται με την ίδια αρχή για επίθεση με κυβερνοόπλα[137]." Με αυτή τη συλλογιστική, οι περιορισμοί του IHL[138] δεν συναρτώνται με το είδος του όπλου που θα χρησιμοποιηθεί παρά μόνο με τον στόχο. Τελικά, αυτό που προκύπτει από αυτή την θεώρηση είναι οτι ορισμένες περιπτώσεις χρήσης κυβερνοόπλων είναι αποδεκτές υπό την οπτική της αρχής της διάκρισης ενώ άλλες περιπτώσεις δεν είναι αποδεκτές, παραβιάζοντας την ίδια αρχή. Στο ένα άκρο του φάσματος είναι προφανώς οι ξεκάθαρα στρατιωτικοί στόχοι. Τέτοια περίπτωση, για παράδειγμα, θα μπορούσε να είναι κάποια συστοιχία βλημάτων εδάφους εδάφους η οποία για τη λειτουργία της στηρίζεται σε ένα στρατιωτικό δίκτυο υπολογιστών. Η κυβερνοεπίθεση εναντίον του στόχου αυτού δεν μπορεί να εγείρει ερωτήματα σχετικά με το εάν συμμορφώνεται με την αρχή της διάκρισης. Στο άλλο άκρο του φάσματος βρίσκονται όλες εκείνες οι περιπτώσεις που παρά την προσπάθεια για ελαχιστοποίηση των παράπλευρων απωλειών, η κυβερνοεπίθεση μπορεί να έχει ως αποτέλεσμα την άμεση και ηθελημένη πρόκληση θανάτου σε πολίτες, όπως για παράδειγμα η καταστροφή ενός συστήματος Radar της πολιτικής αεροπορίας που είναι απαράιτητο για την ασφαλή εκτέλεση των πτήσεων των πολιτικών αεροσκαφών. Προφανώς, αυτή η περίπτωση είναι ξεκάθαρα απαγορευτική, από την πλευρά του IHL. Με την μέχρι στιγμής ανάλυση "φαίνεται οτι και στα δύο άκρα του φάσματος η νομιμότητα της ενδεχόμενης κυβερνοεπίθεσης είναι ξεκάθαρη, με την πρώτη περίπτωση να επιτρέπεται και την δεύτερη να μην επιτρέπεται[139]." Για όλες τις περιπτώσεις που βρίσκονται σε ενδιάμεσα σημεία του φάσματος, η αρχή της διάκρισης είναι ένας μη-αποτελεσματικός οδηγός για τους στρατιωτικούς διοικητές. Εδώ ανήκει, άλλωστε, η μεγαλύτερη κατηγορία κυβερνοστόχων, στην λεγόμενη γκρίζα περιοχή, αφού η ίδια η δομή του διαδικτύου δεν παρέχει εξασφάλιση οτι δεν θα πληγούν και μη στρατιωτικά δίκτυα, ειδικά εάν αναφερόμαστε σε στόχους διπλής χρήσης. Στο σημείο αυτό ο αρθρογράφος κάνει μια εκπληκτικά προφητική διαπίστωση: "λόγω της εγγενούς φύσης των κυβερνοεπιθέσεων να είναι πολύ λιγότερο θανατηφόρες από τις συμβατικές επιθέσεις, οι εμπόλεμοι θα χρησιμοποιούν πολύ συχνότερα κυβερνοεπιθέσεις εναντίον στόχων που ίσως δεν χαρακτηρίζονται στρατιωτικοί η καταστροφή (προσωρινή ή μόνιμη) των οποίων θα έχει επιχειρησιακό όφελος για

---

[136] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

[137] ο.π.

[138] International Humanitarian Law

[139] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

τους επιτιθέμενους αφού χωρίς της απειλή απωλειών πολιτών δεν θα υπάρχει ορατή παραβίαση του σκοπού της αρχής της διάκρισης, ο οποίος δεν είναι άλλος από την προσπάθεια περιορισμού των απωλειών των αμάχων[140].” Κατά αυτό τον τρόπο, ο επιτιθέμενος έχει πολύ λιγότερες πιθανότητες να έρθει αντιμέτωπος με πολιτικές συνέπειες (απώλεια νομιμοποίησης, εσωτερικής ή εξωτερικής) αφού παρ’ όλη την παραβίαση της αρχής της διάκρισης, οι απώλειες αμάχων από την κυβερνοεπίθεση ίσως και να είναι ανύπαρκτες. Επιπλέον, ο κυβερνοπόλεμος εναντίον στόχων διπλής χρήσης ή καθαρά πολιτικού χαρακτήρα (απαγορευμένων, κατά το IHL), μπορεί να έχει ακόμη πιο ήπια δράση: να θέσει τους στόχους εκτός λειτουργίας (χωρίς να τους καταστρέψει, δηλαδή) μόνο για συγκεκριμένο χρονικό διάστημα, όσο απαιτείται ανάλογα το τακτικό πλάνο του επιτιθέμενου. Έτσι, μετά το πέρας της κυβερνοεπίθεσης, ο στόχος θα είναι και πάλι λειτουργικός.

Με αυτές τις δυνατότητες, στοιχειοθετείται το επιχείρημα του Jeffrey Kelsey “οτι με τον κυβερνοπόλεμο είναι πιθανότερο να έχουμε συχνότερα παραβίαση της αρχής της διάκρισης, όπως είναι διατυπωμένη στο διεθνές δίκαιο σήμερα, χωρίς όμως τις συνέπειες για τις οποίες έχει θεσπιστεί η αρχή της διάκρισης, τις απώλειες αμάχων.”

## Κυβερνοπόλεμος και η Αρχή της Ουδετερότητας

Από το 1815, η αρχή της ουδετερότητας εξυπηρετεί και “ρυθμίζει την συνύπαρξη του πολέμου και της ειρήνης, επιτρέποντας σε κράτη που δεν συμμετέχουν στη σύρραξη να διατηρούν σχέσεις με όλους τους εμπόλεμους[141].” Στην εποχή μας, η συνθήκη της Χάγης είναι η πρωτεύουσα πηγή κανόνων που διέπει την ουδετερότητα. Εκεί περιγράφονται τα δικαιώματα και τα καθήκοντα των εμπολέμων αλλά και των ουδέτερων κρατών που διατηρούν την ουδετερότητά τους κατά την ροή των γεγονότων μιάς σύρραξης. Σύμφωνα με τη συνθήκη, “η επικράτεια ενός ουδέτερου κράτους είναι απαραβίαστη. Οι εμπόλεμοι δεν μπορούν να μεταφέρουν στρατεύματα, όπλα ή άλλο πολεμικό υλικό μέσω της επικράτειας του ουδέτερου κράτους, ούτε είναι επιτρεπτό στρατιωτικά αεροσκάφη των εμπολέμων να εισέλθουν σε εναέριο χώρο δικαιοδοσίας του ουδέτερου κράτους. Οι συνθήκες απαιτούν από τα ουδέτερα κράτη να εμποδίσουν τους εμπόλεμους να περιπέσουν σε αυτές τις παραβάσεις της συνθήκη.” Η συνθήκη επίσης, στο άρθρο 8 του 1907 ορίζει μια περιορισμένη εξαίρεση για σκοπούς τηλεπικοινωνιών: “η ουδέτερη δύναμη δεν καλείται να απαγορέυσει ή να περιορίσει τα τηλεγραφικά ή τηλεφωνικά καλώδια ούτε και τον μηχανισμό ασύρματης τηλεγραφίας που ανήκει σε εμπόλεμους ή σε εταιρείες ή ιδιώτες, εφόσον το ουδέτερο κράτος αμερόληπτα επιτρέπει τη χρήση αυτών των υποδομών σε όλα τα εμπόλεμα μέρη[142].” Το σημείο αυτό της συγκεκριμένης συνθήκης είναι πολύ σημαντικό για τις προεκτάσεις αλλά και τις

[140] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

[141] ο.π. και Stephen C. Neff, *The Rights and Duties of Neutrals* (2000)

[142] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

νομικές υποχρεώσεις των, ουδέτερων κυρίως, κρατών, μεσούντος του κυβερνοπολέμου. Από την πλευρά τους, οι Η.Π.Α. επί αυτού είπαν[143] οτι "το συγκεκριμένο άρθρο της συνθήκης της Χάγης του 1907 έχει εφαρμογή στα εργαλεία των σύγχρονων επικοινωνιών: τους δορυφόρους και τις επίγειες υποστηρικτικές εγκαταστάσεις αυτών.[144]" Ωστόσο, όπως διευκρινιστικά αναφέρει ο Jeffrey Kelsey, "τίποτε στην συνθήκη της Χάγης του 1907 δεν υποδηλώνει οτι η εξαίρεση της συνθήκης που αναφέρεται στις επικοινωνίες μπορεί να κληρονομηθεί σε ψηφιακά συστήματα τα οποία εκτός από διαχείριση επικοινωνιών, παράγουν πληροφορία όπως οι κατασκοπευτικοί δορυφόροι που παρέχουν φωτογραφίες, μετεωρολογικοί δορυφόροι και δορυφόροι[145] ναυτιλιακών συστημάτων[146]." Σε τέτοια περίπτωση, η συνθήκη προβλέπει οτι "κάθε ουδέτερο κράτος που παρέχει τέτοια πληροφορία στον έναν εμπόλεμο θα επιτρέπει στον έτερο εμπόλεμο να δράσει εναντίον του ουδέτερου κράτους με σκοπό να εμποδίσει την ροή των πληροφοριών[147]." Και αυτή η πρόβλεψη είναι κεφαλαιώδους σημασίας για την νομική οπτική του κυβερνοπολέμου μέσω του διαδικτύου όπου, λόγω της μεθόδου δρομολόγησης των δεδομένων, είναι πρακτικά αδύνατο να γνωρίζει ο εκτελών κυβερνοεπίθεση τη διαδρομή που θα ακολουθήσουν τα ψηφιακά δεδομένα. Έτσι, η χρήση του διαδικτύου για κυβερνοπόλεμο διαμέσου των συνόρων των κρατών παραβιάζει την αρχή της ουδετερότητας αφού τα δεδομένα, κατά τη διαδρομή τους από το κράτος που εξαπολύει την κυβερνοεπίθεση έως το κράτος στόχο της κυβερνοεπίθεσης, θα διέλθουν από από πληθώρα άλλων κρατών και των τηλεπικοινωνιακών υποδομών τους. Έτσι, το εμπόλεμο κράτος που εξαπέλυσε την κυβερνοεπίθεση, αντίθετα με την άποψη ορισμένων ακαδημαϊκών, "παραβιάζει την αρχή τους ουδετερότητας[148]." Ορισμένοι ενδεχόμενα να αναρωτηθούν κατά πόσο το γεγονός οτι, στην ουσία δεν έχουμε φυσική εισχώρηση σε ουδέτερο κράτος (παρά μόνο διακίνηση δεδομένων μέσω των υποδομών του ουδέτερου κράτους), μπορούμε να μιλάμε για παραβίαση της ουδετερότητας. Όμως, η συνθήκη της Χάγης προβλέπει ρητά οτι "οι εμπόλεμοι απαγορεύεται να μεταφέρουν στρατεύματα, ή αυτοκινητοπομπές με πολεμοφόδια ή άλλες

[143] US Department of Defense General Counsel, *An Assessment of International Legal Issues in Information Operations*, (Montgomery, AL, Maxwell Air Force Base: 1999). Εκεί (Maxwell AFB) εδρέυει το κέντρο επιφόρφωσης των Judge Advocate Genera της πολεμικής αεροπορίας των Η.Π.Α. (USAF), η οποία έχει ιδιαίτερο ενδιαφέρον σε θέματα νομικής ερμηνείας των διεθνών συνθηκών αφού το σύνολο των στρατιωτικών δορυφόρων των Η.Π.Α. ανήκει στην Διοίκηση Διαστήματος της USAF.

[144] Έτσι, οι ΗΠΑ θέλησαν να προστατεύσουν τις στρατιωτικές δορυφορικές επικοινωνίες τους, προσδίδοντας άρωμα διεθνούς νομιμότητας, συνεπεία της δικής τους ερνηνείας του άρθρου 8.

[145] Αναφέρεται στο αμερικανικό δίκτυο ναυτιλιακών δορυφόρων NAVSTAR του συστήματος GPS, στο ρωσικό δίκτυο δορυφόρων του συστήματος GLONASS, το αντίστοιχο υπό ανάπτυξη σύστημα ευρωπαϊκών χωρών, Galileo κλπ.

[146] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

[147] ο.π.

[148] ο.π.

προμήθειες διαμέσου της επικράτειας της ουδέτερης δύναμης[149].” ‘Ετσι, σύμφωνα με τον Jeffrey Kelsey, “σε αντίθεση με την απλή μετάδοση σημάτων επικοινωνιών, η κυβερνοεπίθεση μεταφέρει όπλα [κυβερνοόπλα] μέσα από την επικράτεια μια ουδέτερης χώρας[150].” Η ίδια η πολεμική αεροπορία των Η.Π.Α. έχει δώσει στα “όπλα” τον ακόλουθο ορισμό[151]: “διατάξεις σχεδιασμένες να σκοτώνουν, τραυματίζουν ή να καθιστούν ανίκανους τους ανθρώπους ή να καταστρέφουν ιδιοκτησίες.” Προφανώς, λοιπόν, τα κυβερνοόπλα ταιριάζουν σε αυτόν τον ορισμό αφού οι κυβερνοεπιθέσεις “μπορούν να καταστρέψουν εξίσου στρατιωτικούς και πολιτικούς στόχους…επηρρεάζουν τους ανθρώπους περισσότερο έμμεσα παρά άμεσα. Κατά συνέπεια, τα κυβερνοόπλα έχουν πολλές ομοιότητες με τα όπλα του χθες[152].” Τελικά, ‘όπως καταλήγει και ο Davis Brown[153], “όταν πακέτα πληροφορίας που περιέχουν κακόβουλο κώδικα ταξιδεύουν μέσα από δίκτυα συστημάτων υπολογιστών τα οποία είναι στη δικαιοδοσία κάποιου ουδέτερου κράτους, η αυστηρή εφαρμογή της αρχής της ουδετερότητας έχει αποτέλεσμα το ουδέτερο κράτος να παραβιάζει την ουδετερότητα.” Έτσι, η συνθήκη της Χάγης απαγορεύοντας τη μεταφορά όπλων μέσα από την επικράτεια μια ουδέτερης δύναμης, δεν είναι δυνατόν να εξαιρεί όπλα στο μέγεθος των ηλεκτρονίων.

Σε συνέχεια αυτών, η κυβερνοεπίθεση, όπως κάθε άλλη επίθεση που πραγματοποιείται κατά μήκος της επικράτειας ουδέτερης χώρας, ενδέχεται να έχει ως αποτέλεσμα να παρασυρθεί η ουδέτερη χώρα στην σύρραξη, όπως τονίζει ο Jeffrey Kelsey. Έτσι, συνεχίζει, “η χρήση των κόμβων του διαδικτύου στο έδαφος της ουδέτερης χώρας θα μπορούσε να επιτρέψει στον εμπόλεμο που κάνει χρήση της υποδομής αυτής να αυξήσει το εύρος της επίθεσής του και ίσως, το αποτέλεσμα να είναι ευνοϊκότερο για αυτόν. Εάν η ουδέτερη χώρα δεν μπορεί ή δεν θέλει να δράσει σταματώντας την επίθεση [στο μέτρο που της αναλογεί, δηλαδή διαμέσου των κόμβων στην επικράτειά της], ο έτερος εμπόλεμος πιθανόν να επιλέξει να επιτεθεί με φυσικό τρόπο στο δίκτυο επικοινωνιών της ουδέτερης χώρας ώστε να περιορίσει ή να σταματήσει η κυβερνοεπίθεση[154].” Αυτό που φαίνεται εδώ είναι οτι, ακόμη και χωρίς την φυσική παραβίαση της επικράτειας της ουδέτερης χώρας, η κυβερνοεπίθεση ενδεχομένως να οδηγήσει την ουδέτερη χώρα να εμπλακεί, παρά τη θέλησή της, στην εξελισσόμενη σύρραξη. “Αυτή η ενδεχόμενη απώλεια του

[149] Συνθήκη της Χάγης V, 1907.

[150] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

[151] U.S. Department of the Air Force, *Policy Directive 51-4, Compliance with the Law of Armed Conflict* (1993)

[152] William J. Bayles, *The Ethics of Computer Network Attack,* Parameters (Spring 2001.)

[153] Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, Harvard International Law Journal, Vol. 47 (2006.)

[154] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

καθεστώτος του μη εμπόλεμου είναι το αποτέλεσμα που η αρχή της ουδετερότητας προσπαθεί να αποφύγει[155].”

Στο σημείο αυτό, και ειδικά όχι για την περίπτωση που η ουδέτερη χώρα έχει αντιληφθεί την χρήση της διαδικτυακής υποδομής της και επιλέγει να μην δράσει σταματώντας της εχθρική κυβερνοεπίθεση, αλλά κυρίως για την περίπτωση που η ουδέτερη χώρα έχει άγνοια για την εξελισσόμενη κυβερνοεπίθεση διαμέσου των κόμβων της, υπάρχουν μια σειρά από τεχνικές δυσκολίες που επιτείνουν το πρόβλημα. Η παρούσα δομή του διαδικτύου είναι ο βασικότερος λόγος αφού από σχεδιαστικής άποψης, δεν είναι φτιαγμένο για να ακολουθεί η πληροφορία (στην περίπτωση της κυβερνοεπίθεσης, το κακόβουλο λογισμικό) δεδομένη και αυστηρά προαποφασισμένη διαδρομή, από κόμβο σε κόμβο. Επιλέγεται ο αποδέκτης και τα υπόλοιπα αναλαμβάνονται από ειδικά προγράμματα (αλγόριθμοι δρομολόγησης) που επιλέγουν (με βάση τεχνικά κριτήρια που είναι δυναμικά) την κάλλιστη διαδρομή. Αυτή, η κάλλιστη διαδρομή (όχι απαραίτητα η συντομότερη ή η γρηγορότερη) μπορεί να περνάει από αριθμό δρομολογητών της ουδέτερης χώρας. Ειδικά για έξυπνες μορφές κυβερνοεπίθεσης, “Ακόμη και σήμερα, οι ουδέτερες χώρες δεν έχουν πρακτική μέθοδο εντοπισμού τέτοιων επιθέσεων.[156]” Ακόμη και εαν υπήρχε η δυνατότητα εντοπισμού αυτών των επιθέσεων, το μόνο που θα μπορούσε, ως απάντηση, να γίνει είναι να φιμωνόταν ολοκληρωτικά η ροή του διαδικτύου στο σύνολο (ή, σε μεγάλο τμήμα) της ουδέτερης χώρας, κάτι που είναι εξαιρετικά δύσκολο (ρεαλιστικά) να γίνει. Ωστόσο, το IHL απαιτεί η ουδέτερη χώρα να αναλάβει δράση για να αποτρέψει την κυβερνοεπίθεση, διατηρώντας έτσι την ουδετερότητά της. Στο σημείο αυτό δεν θα ήταν υπερβολικό κάποιος να θεωρήσει οτι με αυτήν την απόλυτη ερμηνεία του IHL, σχετικά με την υποχρέωση της ουδέτερης χώρας, η τελευταία βρίσκεται κυριολεκτικά στριμωγμένη στις δαγκάνες ενός μη ρεαλιστικού αδιεξόδου. Εναλλακτικά, μια άλλη ερμηνεία του IHL θα μπορούσε να προβλέπει της υποχρέωση, μεν, της ουδέτερης χώρας να εντοπίσει και στη συνέχεια να σταματήσει την διερχόμενη από τους κόμβους της επικράτειάς της κυβερνοεπίθεση, με την επισήμανση “στο μέτρο των υφιστάμενων δυνατοτήτων της[157].” Σε κάθε περίπτωση, επαναλαμβάνεται το δικαίωμα του εμπολέμου που δέχεται την κυβερνοεπίθεση, μέρος της οποίας διέρχεται από την επικράτεια της ουδέτερης χώρας, να απαντήσει ως μέτρο αυτοάμυνας, με μέσα της επιλογής του στοχοποιώντας την ουδέτερη χώρα, η οποία στη συνέχεια θα πρέπει να αμυνθεί και, τελικά, να έχουμε ως αποτέλεσμα της διεύρυνση της σύρραξης[158].

Οι εμπόλεμοι, από την πλευρά τους, μπορεί να έχουν σημαντικά κίνητρα να πραγματοποιήσουν κυβερνοεπίθεση με χρήση διαδικτυακής υποδομής κάποιας ουδέτερης χώρας, παραβιάζοντας με αυτόν τον τρόπο την αρχή της ουδετερότητας. “Παρόλη την παραβιάση της αρχής της ουδετερότητας, η εξαπόλυση κυβερνοεπιθέσεων διαμέσου του διαδικτύου επιτρέπει στις εμπόλεμες πλευρές να επιφέρουν ζημιές στον αντίπαλό τους χωρίς το κόστος που συνοδεύει τον συμβατικό

[155] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

[156] Newly Nasty, *Economist*, May 26, 2007, at 62,63

[157] ο.π.

[158] ο.π.

πόλεμο. Πράγματι, ο πόλεμος μέσω του διαδικτύου είναι δυνητικά φθηνότερος σε σχέση με τις συμβατικές επιχειρήσεις[159].”

Ένα άλλο σημαντικό κίνητρο για τους εμπόλεμους να καταφύγουν στην επιλογή του κυβερνοπολέμου, είναι και το γεγονός της “’έλλειψης απόδοσης ευθύνης” στους εξαπολύοντες κυβερνοεπιθέσεις. Για άλλη μια φορά, η δομή του διαδικτύου καθιστά την ανίχνευση και την απόδοση της ευθύνης με απόλυτη βεβαιότητα σε κάποιν φορέα εαν όχι αδύνατη, αλλά εξαιρετικά επισφαλή. Έχουμε δει οτι μέσω της ανάστροφης διερεύνσης των διευθύνσεων IP μπορεί να ανιχνευθεί η υποτιθέμενη προέλευση του επιτιθέμενου. Μόνο που αφενός τα ίχνη αυτά μπορούν πολύ εύκολα να καλυφθούν από τους δράστες πριν ακόμη η διερευνητική διαδικασία ξεκινήσει, αλλά υπάρχει και μια άλλη διάσταση της δυσχέρειας, πολύ πιο ενοχλητική: οι διευθύνσεις IP μπορούν εξίσου εύκολα να υποστούν (από τους ίδιους που εξαπολύουν την επίθεση) σκόπιμη αλλοίωση, ώστε να φαίνεται οτι η επίθεση ξεκίνησε από κάποιο άσχετο με το πραγματικό γεωγραφικό σημείο. Αυτό, εάν λαμβανόταν σοβαρά υπόψη κατά τη διαδικασία διερεύνησης της πηγής προέλευσης της επίθεσης, θα μπορούσε να εμπλέξει κράτη παντελώς άσχετα με την εξελισσόμενη σύρραξη, με ότι αυτό θα μπορούσε να σημαίνει.

[159] Jeffrey T. G. Kelsey, *Hacking into Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review, Vol. 106, No. 7 (May 2008), p. 1427-1451

## 4. Ο ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ ΩΣ ΣΥΓΧΡΟΝΗ ΜΟΡΦΗ ΠΟΛΕΜΟΥ

> *Στον κυβερνοχώρο οι άνθρωποι δρουν υπό το καθεστώς σχετικής ατιμωρησίας και υπό την προστασία της ανωνυμίας. Οι απειλές μπορούν, μεταξύ άλλων, να προέρχονται εξίσου από κράτη, εξτρεμιστικές ή τρομοκρατικές ομάδες, μεμονωμένους χάκερ ή από οργανωμένους εγκληματίες, οι οποίοι μπορούν να ασκήσουν ισχύ δυσανάλογα μεγαλύτερη από την αντίστοιχη που θα μπορούσαν να ασκήσουν στον πραγματικό κόσμο, με την ίδια προσπάθεια και τα ίδια μέσα*[160]

Η παραπάνω διαπίστωση είναι ενδεικτική του γεγονότος οτι ενέργειες στον κυβερνοχώρο και ιδιαίτερα εκείνες που εντάσσονται στο φάσμα του κυβερνοπολέμου μπορούν να προέρχονται από οποιαδήποτε πηγή, γεωγραφικά, πολιτισμικά ή πολιτικά. Εάν λάβουμε υπόψη και την συχνά συνεργατική σύμπραξη μεταξύ κάποιων από τις παραπάνω κατηγορίες με κίνητρο το πρόσκαιρα κοινό όφελος, εύκολα αντιλαμβανόμαστε την πολυπλοκότητα της εξεύρεσης της ενδεχόμενης απόφασης για λήψη μέτρων τόσο για την πρόληψη όσο και για την αντιμετώπιση του φαινομένου. Χαρακτηριστικό παράδειγμα συνεργατικής δράσης με κοινό παρονομαστή το οικονομικό συμφέρον ως κίνητρο παράλληλης δράσης δύο κατηγοριών με φαινομενικά διαφορετική αφετηρία είναι η ναρκοτρομοκρατία (narcoterrorism). Εδώ, ο αντικειμενικός σκοπός των κυκλωμάτων εμπορίας ναρκωτικών (η ασφαλής μεταφορά των ναρκωτικών από το χώρο παραγωγής/επεξεργασίας τους στους τόπους αρχικής διάθεσής τους) και ο αντικειμενικός σκοπός κάποιων τρομοκρατικών οργανώσεων (οικονομικό κέρδος για υποστήριξη της τρομοκρατικής τους δράσης, η οποία σχεδόν πάντα έχει κάποια υποστηρίζουσα ιδεολογική βάση) είναι σε πλήρη αρμονία, οδηγώντας στην αποδοχή μιας λύσης win-win για τα δύο μέρη: οι τρομοκράτες, παρέχοντας ένοπλη κάλυψη έναντι αμοιβής στις ομάδες εμπορίας ναρκωτικών, εξασφαλίζουν στο μέτρο του δυνατού την ασφάλεια της μεταφοράς του παράνομου εμπορεύματος, το οποίο ταξιδεύοντας με μεγαλύτερη ασφάλεια, φτάνει φθηνότερο στους τόπους διάθεσης και έτσι όλοι οι εμπλεκόμενοι είναι οικονομικά κερδισμένοι. Εαν και το παράδειγμα αυτό δεν αναδεικνύει το στοιχείο του κυβερνοπολέμου, δεν παύει να περιγράφει την σύμπραξη δύο ομάδων με φαινομενικά άσχετους σκοπούς δράσης για μεγιστοποίηση του κοινού κέρδους. Γενικεύοντας, σε περιπτώσεις που η απαραίτητη τεχνογνωσία εξαπόλυσης κυβερνοεπιθέσεων από κάποια οντότητα σε κάποια άλλη δεν είναι διαθέσιμη, δεν θα μπορούσε να αποκλειστεί η συνδρομή, κατόπιν πρόσκλησης και έναντι αμοιβής, κάποιας εξειδικευμένης ομάδας ανθρώπων οι οποίοι θα εξαπολύσουν τις δράσεις κυβερνοπολέμου εκ μέρους της πρώτης οντότητας εναντίον της δεύτερης (πχ κάποιου κράτους), διαμέσου του διαδικτύου και, άρα, διαμέσου των κόμβων περαιτέρω κρατών. Έτσι, η δυσχέρεια (συχνά στο όριο της αδυναμίας) εντοπισμού του εξαπολύοντος της επίθεση αυξάνεται ακόμη παραπάνω.

---

[160] Claire Yorke, Cybersecurity and Society: bigsociety.com, The World Today, December 2010, Vol. 66, No. 12, p.19

Οι κατηγορίες των πιθανών εμπλεκομένων σε περιστατικά κυβερνοπολέμου δεν είναι εύκολο να ταξινομηθούν με μαθηματική σαφήνεια, ωστόσο διακρίνονται σε δύο μεγάλες κατηγορίες. Η διάκριση αυτή φέρει το χαρακτηριστικό της μεταβεστφαλιανής εποχής αφού πρόκειται ουσιαστικά για τον διαχωρισμό των δρώντων (ή οντοτήτων) σε κρατικούς και σε μη κρατικούς. Στην περίπτωση των κρατικών δρώντων αναφερόμαστε ξεκάθαρα σε κυρίαρχα κράτη, τα οποία έχουν εντάξει τον κυβερνοπόλεμο ως μια επιλογή η οποία παραμένει διαθέσιμη για ενεργοποίηση ανάλογα των περιστάσεων. Βέβαια, όπως συνηθίζεται, πάντα γίνεται λόγος για κυβερνοάμυνα ή κυβερνοπροστασία και σχεδόν ποτέ για κυβερνοπόλεμο με την αρνητική διάσταση που αποκτά συχνά ο όρος αυτός. Το οτι όλοι αυτοί οι δρώντες είναι πλήρως έτοιμοι για να πραγματοποιήσουν το πρώτο χτύπημα κυβερνοπολέμου είναι μια ανομολόγητη πραγματικότητα.

Από την άλλη πλευρά υπάρχουν οντότητες που ενώ δεν είναι κράτη εντούτοις έχουν σοβαρές δυνατότητες κυβερνοπολέμου. Αυτό δεν είναι καινοφανές, αφού για παράδειγμα υπάρχουν εξτρεμιστικές ομάδες με σημαντική στρατιωτική εκπαίδευση, στελέχωση και εξοπλισμό. Η πρόσκτηση επιπλέον δυνατότητας πραγματοποίησης κυβερνοπολέμου δεν είναι κάτι ασύλληπτο. Αντίθετα μάλιστα, είναι ευκολότερο (και σημαντικά οικονομικότερο) για κάποια οργάνωση π.χ. όπως η Χεζμπολά, να αποκτήσει κυβερνοόπλα από το αποκτήσει σύγχρονα αντιαρματικά μέσα. Αυτές οι μη κρατικές οντότητες συνιστούν την έτερη μεγάλη ομάδα δρώντων στο πεδίο του κυβερνοπολέμου. Εαν ο εντοπισμός, η αξιολόγηση και η εκτίμηση των δυνατοτήτων για πραγματοποίηση κυβερνοπολέμου των οντοτήτων της δεύτερης κατηγορίας δρώντων φαίνεται να μην είναι απλή περίπτωση, δεν ισχύει το ίδιο για τους κρατικούς δρώντες αφού τα ίδια τα κράτη καταρτίζουν σχέδια κυβερνοπολέμου (κυβερνοάμυνας) στοιχεία των οποίων βλέπουν το φως της δημοσιότητας. Για μεθοδολογικούς σκοπούς παρακάτω παρουσιάζονται ορισμένοι μόνο από τους κρατικούς δρώντες, βάσει της επιλογής του γράφοντα με κριτήριο την όσο το δυνατό αντιπροσωπευτικότερη κάλυψη του παγκόσμιου συστήματος σε συνδυασμό με την ύπαρξη έγκυρων και αξιόπιστων διαθέσιμων στοιχείων.

## Κρατικοί Δρώντες

### ΗΠΑ

Σύμφωνα με την Jackie Northam, αμερικανίδα αρθρογράφο και ανάλυτρια, τον Απρίλιο του 2015 ο Πρόεδρος Ομπάμα εξέδωσε διάταγμα για την αντιμετώπιση του κυβερνοεγκλήματος. Το διάταγμα επιτρέπει στις Η.Π.Α. να παγώνουν τα περιουσιακά στοιχεία κυβερνοεγκληματιών και να μπλοκάρεται η οικονομική τους δραστηριότητα εντός των Η.Π.Α. Αυτό συνιστά την πρώτη συμπαγή νομοθέτηση στην προσπάθεια αντιμετώπισης του κυβερνοεγκλήματος[161]. Αν και η πρώτη ανάγνωση αυτής της κίνησης θα μπορούσε να εγείρει ερωτήματα περί της σχέσης της με τον κυβερνοπόλεμο, μια πιο διατρητική προσέγγιση φέρνει στην επιφάνεια την πραγματική πρόθεση της κυβέρνησης των Η.Π.Α.: καλύπτεται νομοθετικά η περίπτωση του κυβερνοεγκλήματος (χωρίς καμμία αναφορά στον κυβερνοπόλεμο), κάτι που είναι περισσότερο πολιτικά ορθό και που περνά ευκολότερα τους

[161] Jackie Northam, “U.S. Creates First Sanctions Program Against Cybercriminals”

σκοπέλους του αμερικανικού νομοθετικού συστήματος. Παραμένει σκόπιμα ασαφής, εν πολλοίς, η διαχωριστική γραμμή μεταξύ ερμηνείας του τι συνιστά κυβερνοέγκλημα και τι κυβερνοπόλεμο, το ποιος κατά περίπτωση θα δίνει την ερμηνεία αυτή αλλά και τελικά το έαν θα οφείλουν να λογοδοτούν ή όχι οι Η.Π.Α. (εντός και εκτός χώρας) για την λήψη κυβερνομέτρων στα οποία θα δίδεται ο χαρακτηρισμός "μέτρα κυβερνοπροστασίας" από το "κυβερνοέγκλημα." Η απόφαση της κυβέρνησης Ομπάμα δεν ήταν κάτι που λήφθηκε ξαφνικά ή αυτόματα. Αμέσως μετά την 11η Σεπτεμβρίου, σύμφωνα με σχετικό άρθρο της εφημερίδας New Yorker[162], είχε προταθεί από την κυβέρνηση Κλίντον να χρησιμοποιηθούν τεχνικές κυβερνοπολέμου[163] ώστε να "κλειδωθούν" ηλεκτρονικά οι τραπεζικοί λογαριασμοί που είχαν χρησιμοποιηυθεί από τον Οσάμα Μπιν Λάντεν και άλλους, προτάσεις που δεν έγιναν δεκτές από το υπουργείο οικονομικών, υπό το φόβο οτι στο άκουσμα και μόνο μιας τέτοιας κίνησης από πλευράς Η.Π.Α. θα υποβαθμιζόταν η πίστη στο παγκόσμιο τραπεζικό σύστημα, κάτι που θα ήταν εξαιρετικά δυσάρεστο και για τις ίδιες τις Η.Π.Α. Το σημαντικό από αυτήν την αναφορά είναι οτι η τεχνική δυνατότητα αυτής της τεχνικής κυβερνοπολέμου (και πληθώρας άλλων) υπήρχε, ωστόσο οι παράγοντες που δεν επέτρεψαν την ενεργοποίηση της συγκεκριμένης δράσης ήταν πολλοί και αρκετά πειστικοί ώστε να ακινητοποιήσουν την προταθείσα ενέργεια.

Στον ακαδημαϊκό χώρο οι απόψεις συγκλίνουν οτι οι Η.Π.Α. έχουν αποκτήσει (ή πρέπει να συνεχίσουν να αυξάνουν τις σχετικές ικανότητές τους) σοβαρές δυνατότητες κυβερνοπολέμου διότι βρίσκονται διαρκώς στο στόχαστρο κυβερνοεπιθέσεων ή στη μέση ενός ακήρυχτου και άγνωστης διάρκειας κυβερνοπολέμου. Ο πρώην διοικητής της κεντρικής υπηρεσίας πληροφοριών των Η.Π.Α. (C.I.A.), Leon Paneta είχε δηλώσει[164] ευθέως οτι το φάντασμα του κυβερνοπολέμου στοιχειώνει του αμερικανούς ηγέτες και οτι το επόμενο Περλ Χάρμπορ θα μπορούσε κάλλιστα να είναι μια κυβερνοεπίθεση, προτρέποντας με αυτόν τον τρόπο για λήψη περισσότερο ενεργών μέτρων από την κυβέρνηση. Ο Robert Gates σε αντίστοιχο άρθρο[165] του αναφέρει οτι με τόσους πολλούς δυνητικούς εχθρούς, από τρομοκράτες, κράτη παρίες έως αναπτυσσόμενες υπερδυνάμεις, οι οποίοι έχουν μάθει πως είναι πρακτικά ανέφικτο να αντιμετωπίσουν τις Η.Π.Α. ευθέως με συμβατικό τρόπο, θα πρέπει να αποτελεί σημείο προβληματισμού για τις ίδιες τις Η.Π.Α. το ενδεχόμενο ενός κυβερνοπολέμου από έναν ή περισσότερους από αυτούς τους εν δυνάμει εχθρούς της. Αναφερόμενος, μάλιστα, στην ιδιαιτερότητα του αναμενόμενου κυβερνοπολέμου, λέει πως θα είναι τέτοιας μορφής όπου "η Microsoft θα συνυπάρχει με τις ματσέτες και η τεχνολογία στελθ με τους βομβιστές αυτοκτονίας[166]." Έτσι, συνεχίζει, ενώ οι Η.Π.Α. είναι το

---

[162] Joe Klein, *Institutional Lassitude and Bureacratic Arrogance*, New Yorker, 1st October 2001.

[163] Ο αρθογράφος κάνει πολύ προσεκτικά χρήση της φράσης «τεχνικές κυβερνοπολέμου» αντί της ευθείας αναφοράς σε «κυβερνοπόλεμο,» κάτι που ενδέχεται να μην είναι διόλου τυχαίο.

[164] Thomas Rid, *The Empty Threat of Cyberwar*, Journal of Strategic Studies, February 2012

[165] Robert M. Gates, *A Balanced Strategy: Reprogramming the Pentagon for a New Age*, Forreign Affairs, January/February 2009, Vol. 88, No. 1, p.32

[166] ο.π.

δυνατότερο και το μεγαλύτερο κράτος στον κόσμο, υπάρχουν όρια στο τι μπορούν να πράξουν. Το ποιά ακριβώς είναι αυτά τα όρια συναρτάται με το είδος των προκλήσεων που αντιμετωπίζουν ή αναμένεται να αντιμετωπίσουν οι Η.Π.Α. στο μέλλον, κάτι που για τον κυβερνοπόλεμο –ως απειλή εναντίον τους- οι Η.Π.Α. το έχουν εντοπίσει αρκετά νωρίς.

Συγκεκριμένα, η Επιτροπή για την αναθεώρηση των προγραμμάτων και των σχεδίων περί των συστημάτων Διοίκησης Ελέγχου Επικοινωνιών Υπολογιστών και Πληροφοριών (Command Control Communications Computer & Intelligence, C4I) του αμερικανικού εθνικού συμβουλίου ερευνών, με έδρα την Washington D.C., σε μία εξαιρετικά λεπτομερή και πολυεπίπεδη μελέτη με τίτλο "Realizing the Potential of C4I: Fundamental Challenges[167]" αναλώνει μεγάλο τμήμα της ερευνητικής προσπάθειας περί των θεμελιωδών προκλήσεων των συστημάτων C4I σε θέματα γύρω από την ασφάλεια των πληροφοριακών συστημάτων. Καταγράφονται διαπιστώσεις όπως οτι η αυξανόμενη εξάρτηση των αμερικανικών ενόπλων δυνάμεων από υπολογιστικά συστήματα αυτομάτως αυξάνει την αξία των πληροφοριακών υποδομών και των πληροφοριακών συστημάτων ως στόχων. Επίσης, γίνεται αναφορά οτι η επίθεση εναντίον των στρατιωτικών πληροφοριακών αυτών υποδομών είναι συνήθης δραστηριότητα και όχι σπάνια οι επιθέσεις αυτές είναι πετυχημένες[168]. Έτσι, τα αμερικανικά συστήματα C4I με την αμφίβολη ικανότητα αυτοάμυνας έναντι κυβερνοεπιθέσεων, εγείρουν το ερώτημα του κατά πόσο θα είναι σε θέση να παρέξουν τις υπηρεσίες τους (οι οποίες, λόγω της διαρκώς αυξανόμενης εξάρτησης των ενόπλων δυνάμεων από αυτά, είναι καθοριστικής σημασίας) όταν θα έρθουν αντιμέτωπα με μία σοβαρή επίθεση προερχόμενη από έναν αποφασισμένο και έμπειρο αντίπαλο. Η επιτροπή επίσης εντοπίζει μέρος του προβλήματος στην ολοένα και αυξανόμενη αλληλοεξάρτηση στρατιωτικών και μη στρατιωτικών υποδομών, κάτι που καθιστά το ζήτημα της προστασίας των C4I μια πραγματική πρόκληση. Όπως είναι αναμενόμενο από την σύνθεση της επιτροπής[169] αλλά και από τον φορέα που την εξουσιοδότησε να πραγματοποιήσει την έρευνά της (Συμβούλιο Εθνικής Έρευνας των Η.Π.Α.), το παραμικρό εύρημα είναι πλήρως στοιχειοθετημένο και μάλιστα συχνά ποικιλοτρόπως. Έτσι, για να στοιχειοθετηθεί η ευπάθεια μιας τόσο ευαίσθητης κατηγορίας τεχνολογικού εξοπλισμού όπως τα συστήματα C4I, δεν αρκέστηκαν σε θεωρητικές προσεγγίσεις αλλά, αντίθετα, πραγματοποίησαν άσκηση με την επωνυμία "Eligible Receiver", μια άσκηση μεγάλης κλίμακας, *χωρίς προειδοποίηση*, υπό τον έλεγχο του Αρχηγού του ΓΕΕΘΑ των Η.Π.Α. Συνοπτικά, η άσκηση κατέδειξε τις ευπάθειες των υπολογιστικών υποδομών του υπουργείου Εθνικής Άμυνας των Η.Π.Α. καθώς και του ελλείμματος ικανότητας των Η.Π.Α. να απαντήσουν αποτελεσματικά σε μία συνδυασμένη επίθεση κατά των

[167] Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I Systems: Fundamental Challenges*, National Academy Press, Washington D.C.: 1999

[168] ο.π., σ. 131

[169] Στη βασική της σύνθεση βρίσκονται δεκαπέντε επιστήμονες εγνωσμένου κύρους και ακαδημαϊκής και πρακτικής υπερεπάρκειας, συνεπικουρούμενοι από επτά επιτελείς αλλά και άλλες δύο ανεξάρτητες υποεπιτροπές με ειδικότερο έργο και αντίστοιχη εξειδίκευση.

εθνικών υποδομών και των πληροφοριακών συστημάτων[170]. Όπως ήταν αναμενόμενο, το υπουργείο ακολουθώντας τις συστάσεις της επιτροπής[171], μπήκε σε τροχιά διαρκούς βελτίωσης και θωράκισης του συνόλου των στρατιωτικών υποδομών υπολογιστικών συστημάτων, σε συνδυασμό με αναθεώρηση του συνολικού τρόπου αντίληψης και σκέψης προ της απειλής κυβερνοπολέμου, κάτι που σταδιακά άρχισε να εμφανίζεται σε πληθώρα εγγράφων και κειμένων, επιπέδου συχνά πολύ υψηλού, όπως η Εθνική Στρατιωτική Στρατηγική των Η.Π.Α. του Ιουνίου του 2015. Άλλωστε, οποιαδήποτε τροποποίηση των υποδομών χωρίς παράλληλη προσαρμογή τρόπου σκέψης και αντιλήψεων του προσωπικού που βρίσκεται πίσω από αυτά τα συστήματα στα νέα δεδομένα, θα ήταν ανώφελη αλλά και επικίνδυνη προσπάθεια. Έτσι, όπως γράφει και ο στρατηγικός αναλυτής Michael Rubin[172], οι Η.Π.Α. αντί να προσανατολίζονται και να σχεδιάζουν μεγάλης κλίμακας στρατιωτικές επιχειρήσεις ή ακόμη και μικρής έκτασης πολέμους περιορισμένους σε συγκεκριμένα κράτη, το Πεντάγωνο πρέπει να αναπτύξει στρατηγικές για να εντοπίσει και να ανασχέσει τις μη συμβατικές απειλές τόσο από πλευράς κρατικών δρώντων όσο και εκείνες που προέρχονται από μη κρατικές οντότητες, οι οποίες θα επιχειρήσουν να επιτεθούν εναντίον των συμφερόντων των Η.Π.Α. Αυτό αποτελεί πραγματικότητα για τις Η.Π.Α. αφού, σύμφωνα με τον Jonathan Kirshner, οι Η.Π.Α. συμπεριλαμβάνονται στις πρώτες τρεις χώρες που συχνά αναφέρονται[173] ως εκείνες που αναπτύσσουν ταχύτερα ικανότητες κυβερνοπολέμου. Ωστόσο, συχνά η ανάδειξη των δρώντων εκείνων με τις καλύτερες δυνατότητες κυβερνοπολέμου ενέχει μεγάλο βαθμό υποκειμενικότητας.

Αυτό ακριβώς σχολιάζει ο Andrew F. Krepinevich Jr., γράφοντας[174] οτι ο ανταγωνισμός στον κυβερνοπόλεμο είναι τόσο πολύ καλυμμένος από μυστικότητα που είναι δύσκολο να διακρίνει το πραγματικό επίπεδο ευπάθειας των Η.Π.Α., κάτι που καθιστά το ενδεχόμενο να δεχθεί η χώρα κυβερνοεπίθεση υπό καθεστώς έκπληξης μια υπαρκτή πιθανότητα. Με αυτήν την άποψη ως βάση, εύκολα στοιχειοθετείται (και γίνεται ακόμη ευκολότερα αποδεκτό σε εσωτερικό επίπεδο) η αναγκαιότητα για ανάπτυξη όπλων, τεχνικών και δομών κυβερνοπολέμου ως αδήριτη ανάγκη λόγω της μη ασφαλούς δυνατότητας εκτίμησης του πραγματικού επιπέδου ευπάθειας. Επιπλέον, με αυτή τη συλλογιστική καλλιεργείται αργά αλλά σταθερά η πεποίθηση οτι στον κυβερνοπόλεμο το προληπτικό χτύπημα είναι η μόνη πραγματική δυνατότητα αποτροπής, κάτι που αντικατοπτρίζει την παρούσα σχολή σκέψης των Η.Π.Α.

Η παραπάνω συλλογιστική καθιστά ευκολότερη και την αποδέσμευση κονδυλίων για σκοπούς κυβερνοπολέμου, το μέγεθος των οποίων κυμαίνεται σε τάξη

---

[170] Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I Systems: Fundamental Challenges*, National Academy Press, Washington D.C.: 1999

[171] ο.π., σ.229

[172] Michael Rubin, *Assymetrical Threat Concept and its Reflections on International Security*, Strategic Research and Study Center (SAREM), 31st May, 2007

[173] Jonathan Kirshner, *Globalization, American Power, and International Security*, Political Science Quarterly (The Academy of Political Science), Vol. 123, No. 3, Fall 2008, p.378.

[174] Andrew F. Krepinevich Jr., *The Pentagon's Wasting Assets: The Eroding Foundations of American Power*, Forreign Affairs, Vol. 88, No. 4, July/August 2009, p.30-31

μεγέθους δισεκατομμυρίων δολαρίων, σύμφωνα με τον πρώην σύμβουλο ασφαλείας του Λευκού Οίκου, Richard Clarke[175]. Ο ίδιος χαρακτηριστικά αναφέρει οτι το Πεντάγωνο μόλις δημιούργησε τον νέο, 10$^{ο}$ στόλο, με την διαφορά οτι ο στόλος αυτός δεν έχει πλοία, είναι στον κυβερνοχώρο. Κατά συνέπεια, η κυβέρνηση των Η.Π.Α. πιστεύει οτι η απειλή κυβερνοπολέμου είναι κάτι παραπάνω από μια πραγματικότητα αφού ξοδεύει τεράστια ποσά για την ανάπτυξη επιθετικών δυνατοτήτων. Θεωρεί δε πως ενώ οι Η.Π.Α. έχουν επαρκή προετοιμασία για διεξαγωγή επιθετικών επιχειρήσεων κυβερνοπολέμου, το ίδιο δεν ισχύει για την πραγματοποίηση αμυντικών επιχειρήσεων. Η παραπάνω άποψη τεκμηριώνεται με οδηγό το επιχείρημα οτι στον κυβερνοπόλεμο η επιτιθέμενη πλευρά έχει πάντα το απόλυτο πλεονέκτημα και την πρωτοβουλία των κινήσεων[176], ωστόσο η επιχειρηματολογία αυτής της μορφής δεν παύει να συνιστά και μια πολύ βολική μέθοδο παρουσίασης της επιθετικής δράσης κυβερνοπολέμου ως την μόνη επιλογή, αμβλύνοντας έτσι τυχόν αντίλογο περί της μη νομιμότητας του προληπτικού χτυπήματος.

Ο κυβερνοπόλεμος για τις Η.Π.Α. είναι ένα από τα βασικά στοιχεία της λεγόμενης Επανάστασης στις Στρατιωτικές Υποθέσεις (Revolution in Military Affairs, R.M.A.) όπου μαζί με τα κατευθυνόμενα όπλα πολύ μεγάλης ακρίβειας[177], τα μη επανδρωμένα αεροχήματα[178] και τις επικοινωνίες δικτυοκεντρικού χαρακτήρα[179] σε πραγματικό χρόνο, αποτελούν το τετράπτυχο που, σύμφωνα με τον Michael Horowitz, έχει αλλάξει τον τρόπο που οι αμερικανικές ένοπλες δυνάμεις πραγματοποιούν τις επιχειρήσεις τους[180]. Λόγω του δυναμικού χαρακτήρα που οι εξελίξεις της τεχνολογίας προσδίδουν στον κυβερνοπόλεμο, ο Στρατηγός Martin Dempsey, Αρχηγός του αμερικανικού ΓΕΕΘΑ το 2013 εξέδωσε ένα white paper[181] μέσα στο οποίο ανέλυε το όραμά του για τις αμερικανικές ένοπλες δυνάμεις του 2020. Οι σχετικοί με τον κυβερνοπόλεμο όροι είναι παντού μέσα στο κείμενο αλλά αυτό που είναι αξιοπρόσεχτο είναι ο λιτός τρόπος που ο Στρατηγός περιγράφει την διαρκή επαγρύπνηση που απαιτείται από όλους, γράφοντας οτι η κυβερνοασφάλεια πρέπει να είναι εγγενές χαρακτηριστικό όλων των πράξεων, οραματιζόμενος τον κυβερνοπολεμιστή του 2020 να αντλεί όλες τους τις πληροφορίες κατά τη διάρκεια της μάχης από ένα θεωρητικό χώρο, το νέφος (cloud), σε όλο το εύρος διαβάθμισης των πληροφοριών, με οποιαδήποτε συσκευή, οποτεδήποτε και οπουδήποτε στον πλανήτη. Εάν το όραμα αυτό περιέχει μεγάλο βαθμό αισιόδοξης προσδοκίας είναι κάτι που θα φανεί στο κοντινό μέλλον, ωστόσο επί του παρόντος ο Gaspar Biro

[175] Eleanor Hall, *Former White House security advisor warns of cyber warfare*, interview on the The World Today, 7 December 2010.

[176] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, Vol. 89, No. 5, September/October 2010, p.99

[177] PGM, Precision Guidance Munition

[178] UAV/UCAV, Unmanned Aerial Vehicle/Unmanned Combat Aerial Vehicle

[179] Network-centric communications

[180] Michael C. Horowitz, *Review Article*, Perspective on Politics, Vol. 9, No. 3, September 2011, p.769

[181] General (US ARMY) Martin E. Dempsey (Chairman of the Joint Chiefs of Staff), *Joint Information Environment (White Paper),* 22 January 2013

αναφέρει[182] οτι ήδη από τον Μάρτιο του 2013 η Διοίκηση Κυβερνοχώρου των Η.Π.Α. (Cyber Command) ανακοίνωσε επίσημα τη δημιουργία επιθετικών ομάδων για κυβερνοπόλεμο, κάτι που είναι πλήρως ευθυγραμμισμένο και συνεπές με την εκπεφρασμένη βούληση των Η.Π.Α. να αποτελέσουν την πρωτοπόρα δύναμη και στον τομέα του κυβερνοπολέμου, κάτι που φαίνεται να συμβαίνει. Παρά το ιδιάζον του θέματος του κυβερνοπολέμου, για τις Η.Π.Α. και τις δυνατότητες των ενόπλων δυνάμεών της στο συγκεκριμένο πεδίο υπάρχει πληθώρα πηγών και άρθρων, κάτι που δεν ισχύει για τους λοιπούς κρατικούς δρώντες όπου οι επίσημες αναφορές είναι η εξαίρεση και όχι ο κανόνας.

### Ρωσία

Η Ρωσία έχει ήδη διαπράξει κυβερνοεπιθέσεις στο πρόσφατο παρελθόν κατά ολόκληρων κρατών, σύμφωνα με τους Wesley Clark και Peter Levin, οι οποίοι αναφέρονται[183] στην περίπτωση της Εσθονίας, την άνοιξη του 2007. Η συγκεκριμένη κυβερνοεπίθεση παρέλυσε, σύμφωνα με τους ίδιους, ιστοσελίδες αρκετών τραπεζών αλλά και την προσωπική ιστοσελίδα του πρωθυπουργού της χώρας. Τον επόμενο χρόνο, κατά τη διάρκεια του πολέμου στη Γεωργία, κυβερνητικά στελέχη της χώρας δήλωσαν πως ένας αριθμός από υπολογιστές της κυβέρνησης ελέγχονταν από Ρώσους χάκερ[184]. Η Ρωσία είναι επίσης (μαζί με τις Η.Π.Α., όπως ήδη αναφέρθηκε) μέσα στις τέσσερις χώρες που θεωρούνται ταχύτερα αναπτυσσόμενες στον τομέα του κυβερνοπολέμου[185] και της έχουν αποδοθεί επίσης κυβερνοεπιθέσεις εναντίον του Κυργιστάν το 2009, χωρίς ποτέ να έχει καταστεί δυνατό να τεκμηριωθούν αυτές οι "φήμες." Τη στιγμή της συγγραφής των γραμμών αυτών, σύμφωνα με την near real time απεικόνιση των σε εξέλιξη κυβερνοεπιθέσεων της NORSE[186], η Ρωσία φαίνεται να αποτελεί σταθερά χώρα προέλευσης κυβερνοεπιθέσεων μέσα στις πέντε πρώτες. Ασφαλώς και οι συγκεκριμένες δράσεις δεν είναι δυνατό να χαρακτηριστούν αυτόματα κυβερνοπόλεμος, ωστόσο δείχνουν το μέγεθος της δραστηριότητας στον κυβερνοχώρο με κακόβουλες προθέσεις. Ούτε, βέβαια, θεωρήθηκε αδιανόητο όταν μετά τις κυβερνοεπιθέσεις σε συστήματα διανομής ηλεκτρικής ενέργειας στις Η.Π.Α. παρουσιάστηκαν ενδείξεις[187] οτι πιθανόν πίσω από αυτά τα περιστατικά να υπήρχε Ρωσική εμπλοκή με συμμετοχή της κεντρικής κυβέρνησης. Για το ίδιο περιστατικό,

---

[182] Gaspar Biro, *Ηθική και Διεθνείς Σχέσεις* (Μετάφρασε η Αγγελική Νεβσεχιρλίογλου), International Relations Quarterly, Vol. 4, No. 1, Spring 2013, p.10

[183] Wesley K. Clark and Peter L. Levin, *Securing the Information Highway: How to Enhance the United States' Electronic Defenses*, Foreign Affairs, Vol. 88, No. 6, November/December 2009, p.3

[184] ο.π.

[185] Jonathan Kirshner, *Globalization, American Power, and International Security*, Political Science Quarterly (The Academy of Political Science), Vol. 123, No. 3, Fall 2008, p.378.

[186] http://map.norsecorp.com

[187] Garance Burke and Jonathan Fahey, *AP Investigation: US Power Grid Vulnerable to Foreign Hacks*, San Jose California, 21 December 2015.

άλλωστε, η Wall Street Journal περιέγραψε σε σχετικό άρθρο[188] της τον τρόπο με τον οποίο Ρώσοι (και Κινέζοι) κυβερνητικοί πράκτορες τοποθέτησαν το κακόβουλο λογισμικό στο δίκτυο διανομής ηλεκτρικής ενέργειας στις Η.Π.Α. Η Ρωσία ουδέποτε διέψευσε αυτές τις φήμες, κάτι που άλλωστε το συναντούμε σχεδόν στο σύνολο των περιπτώσεων απόδοσης χλιαρών κατηγοριών εναντίον κρατικών δρώντων μετά από την εκδήλωση κυβερνοεπιθέσεων κατά άλλου κρατικού δρώντα. Στην προερχόμενη από την ίδια την Ρωσία βιβλιογραφία και αρθογραφία δεν συναντούμε υποστηρικτικό υλικό για το τεχνολογικό υπόβαθρο των ενόπλων δυνάμεων της Ρωσικής Δημοκρατίας σε θέματα κυβερνοπολέμου, κάτι που είναι απόλυτα αναμενόμενο εάν αναλογιστεί κανείς την μακρά παράδοση που η προκάτοχος Σοβιετική Ένωση είχε στην απόκρυψη στον απόλυτο βαθμό οποιαδήποτε πληροφορίας ή ακόμη και φήμης σχετικά με πολλά υποσχόμενες και πρωτοπόρες ιδέες ή πρακτικές των ενόπλων δυνάμεων. Έτσι, ακόμη και στο επίσημο κείμενο της Ρωσικής Εθνικής Στρατιωτικής Στρατηγικής 2020 δεν συναντούμε κάποια ξεκάθαρη αναφορά σε θέματα κυβερνοπολέμου. Σχετιζόμενες αναφορές μπορεί να θεωρηθούν, για παράδειγμα, οτι ως αρνητική επίδραση στην διασφάλιση των Ρωσικών εθνικών συμφερόντων μπορεί να θεωρηθεί η παράνομη δράση στον κυβερνοχώρο, δήλωση που εκτός από γενική είναι και αυτονόητη ή το οτι σε παγκόσμιο επίπεδο αναμένεται να αυξηθεί ο αγώνας για την εξασφάλιση της πληροφορίας, κάτι επίσης αυτονόητο και γενικόλογο.

Σε ένα άλλο σημείο, αναφέρεται οτι στις προθέσεις της Ρωσίας είναι η επίτευξη ισότιμης και κοινά επωφελούς στρατηγικής συνεργασίας με τις Η.Π.Α. σε τομείς όπως ο έλεγχος των εξοπλισμών, η μη διάδοση των όπλων μαζικής καταστροφής, η αντιτρομοκρατική δράση και η ρύθμιση περιφερειακών συρράξεων, όμως ουδεμία αναφορά γίνεται για θέματα συνεργασίας του κυβερνοχώρου, κυβερνοπολέμου ή διαχείρισης πληροφοριών.

Το μόνο ίσως σημείο όπου κάποιος θα μπορούσε να εντοπίσει την δηλοποιημένη πρόθεση της Ρωσίας να αναπτύξει περαιτέρω τις ικανότητες στον κυβερνοπόλεμο είναι οι αναφορές στους τρόπους με τους οποίου προτίθεται να διασφαλίσει την εθνική ασφάλεια, όπου επεξηγηματικά στον όρο της Στρατηγικής Αποτροπής αναφέρεται η απαίτηση η χώρα να έχει υψηλή ικανότητα διαχείρισης των πληροφοριών. Τέλος, ως απειλές της στρατιωτικής ασφάλειας θεωρούνται οι πολιτικές ορισμένων ανεπτυγμένων ξένων χωρών που στοχεύουν στην ανάπτυξη, μεταξύ άλλων, υψηλής ακρίβειας μέσων να πραγματοποιούν τεχνολογικό ένοπλο αγώνα. Εδώ, δεν είναι δύσκολο να εξαχθεί το συμπέρασμα οτι η Ρωσία σχεδόν φωτογραφίζει και τον κυβερνοπόλεμο, εντάσσοντάς τον στις απειλές εναντίον της στρατιωτικής ασφάλειας της χώρας.

Η απουσία ρητής αναφοράς στον κυβερνοπόλεμο στο κείμενο της εθνικής στρατιωτικής στρατηγικής της Ρωσίας για το 2020 κάθε άλλο παρά τυχαία πρέπει να θεωρηθεί. Η Ε.Σ.Σ.Δ. παλαιότερα και η διάδοχος Ρωσική Δημοκρατία πρόσφατα, έχουν πολλές φορές αποδείξει οτι αυτό που αποκαλείται η τέχνη της Μασκιρόφκα είναι το βασικό modus operandi σε περιπτώσεις ενδεχόμενης στρατιωτικής δράσης. Εάν και ο όρος παραπλάνηση δεν αποδίδει της έννοια της Μασκιρόφκα, είναι πρόσφατη η περίπτωση της Κριμαίας όπου όλος ο δυτικός κόσμος κυριολεκτικά ήταν

[188] Ian Winkler, *Will There Be an Electronic Pearl Harbor?* PC World, http://www.pcworld.com/article/183436/electronic_pearl_harbor.html

απροετοίμαστος για αυτά που συνέβησαν εκεί με τον τρόπο που εξελισσόταν η κατάσταση, ενώ η ίδια η Ρωσία αφενός υλοποιούσε την υποστήριξη του σχεδιασμού της για προσάρτηση της Κριμαίας αφετέρου δήλωνε οτι δεν είναι ρωσικές οι δυνάμεις που επιχειρούν εκεί. Στην ίδια ακριβώς βάση, είναι περισσότερο από βεβαιο οτι η Ρωσία διαθέτει εξαιρετικά εξελιγμένες δυνατότητες κυβερνοπολέμου, τις οποίες προσεκτικά προστατεύει ενώ διατηρεί σε ετοιμότητα ολόκληρο μηχανισμό με σκοπό να τον κινητοποιήσει όταν κριθεί σκόπιμο και επωφελές, παραπλανώντας μέχρι την τελευταία στιγμή τους τυχόν ενδιαφερόμενους. Το πρόσφατο παρελθόν έδειξε, τελικά, οτι η τέχνη της Μασκιρόφκα επιβίωσε της μετάβασης από την εποχή του ψυχρού πολέμου στην σύγχρονη Ρωσία.

## Κίνα

> *Εαν γνωρίζατε πόσα πολλά μπορούμε να μάθουμε για εσάς από τον υπολογιστή σας, δεν θα χρησιμοποιούσατε ποτέ ξανά το διαδίκτυο στην Κίνα….μπορούμε να σπάσουμε σχεδόν κάθε κωδικό και να μπούμε στον τραπεζικό λογαριασμό σας, μπορούμε να διαβάσουμε τα e-mail σας ή να στείλουμε e-mail από τον υπολογιστή σας στο αφεντικό σας τόσο στα αγγλικά όσο και στα κινέζικα*[189]

Ο φυσικός χώρος δραστηριοποίησης της Κίνας στον χώρο του κυβερνοπολέμου δεν θα μπορουσε να είναι άλλος από την Ταϊβάν. Η επανένωση του νησιού με την μητέρα πατρίδα αποτελεί έναν από τους στόχους της Κίνας τα τελευταία χρόνια, κάτι που έχει φέρει τις Η.Π.Α. στο νησί σε ρόλο εξισορροπητή ώστε η Κίνα να αποτρέπεται από την εκδήλωση επιθετικών ενεργειών εναντίον της απροστάτευτης (σε διαφορετική περίπτωση) Ταϊβάν. Σύμφωνα με ένα σενάριο[190], η Ταϊβάν εξακολουθεί να απειλείται, παρά την ύπαρξη των αμερικανικών δυνάμεων εκεί, αφού η Κίνα χρησιμοποιώντας αρχικά κυβερνοπόλεμο θα θέσει εκτός λειτουργίας στόχους με επίπτωση στην πολιτική, οικονομική, κοινωνική και στρατιωτική δραστηριότητα στο νησί και έπειτα θα συνεχίσει την επίθεσή της με πιο συμβατικό τρόπο και μέσα. Το παραπάνω μάλλον θα παραμείνει σενάριο, ωστόσο έχει θεωρητική αξία αφού καταδεικνύει μια άλλη προσφορά του κυβερνοπολέμου ως το αρχικό βήμα σε μια κλιμακούμενη σύρραξη, νεκρώνοντας μέρος του δυναμικού του αντιπάλου και καθιστώντας την κύρια προσπάθεια ευκολότερη, γρηγορότερη και πιο ανώδυνη για τον επιτιθέμενο. Οι κινεζικές ένοπλες δυνάμεις, παρακολουθώντας και αναλύοντας τα δεδομένα από τον πρώτο πόλεμο του κόλπου, γρήγορα διαπίστωσαν το πόσο κρίσιμος μπορεί να είναι ο ρόλος του κυβερνοπολέμου. Από τότε και μετά, οι κινεζικές ένοπλες δυνάμεις έδωσαν ιδιαίτερη βαρύτητα στον τομέα αυτό. Λίγα χρόναι μετά, το 1995, έκανε την εμφάνισή του ένα άρθρο του ειδικού σε

[189] Michael Sheridan, *China's Net Warriors Take On West*, Sunday Times, 1 September 2002, p.24

[190] Gary D. Rawnsley, *Old Wine in new Bottles: China-Taiwan Computer-Based Information Warfare and Propaganda*, International Affairs, Vol. 81, No. 5, October 2005, p.1064

θέματα κυβερνοπολέμου Wang Pufeng με τίτλο "τοπικός πόλεμος σε συνθήκες υψηλής τεχνολογίας[191]", όπου ο συγγραφέας αναφέρει:

> *Στο κοντινό μέλλον ο πληροφοριακός πολέμος θα ελέγχει τη μορφή και την εξέλιξη του πολέμου. Αναγνωρίζουμε την εξελικτική αυτή τάση και την θεωρούμε ως την κινητήρια δύναμη προς την κατεύθυνση του εκμοντερνισμού και της αύξησης της ετοιμότητας των κινεζικών ενόπλων δυνάμεων. Η τάση αυτή θα είναι εξαιρετικά κρίσιμη στην επίτευξη της νίκης στους μελλοντικούς πολέμους.*

Έτσι θεωρείται πως ξεκίνησε η κινεζική έκδοση του Revolution in Military Affairs των Η.Π.Α. Η Κίνα φέρεται να έχει ιδρύσει κέντρο ανάπτυξης και εξομοίωσης κυβερνοπολέμου και να έχει πραγματοποιήσει ασκήσεις που είχαν ως μέρος τους τη διασπορά ιών σε υπολογιστικά συστήματα σε τοπικό επίπεδο (1997) αλλά και στο διαδίκτυο (2000). Η κινεζική στρατιωτική στρατηγική πλέον αναγνωρίζει την σπουδαιότητα της γνώσης ανάπτυξης και διασποράς ιών υπολογιστών, της διαδικασίας απόκτησης στοιχείων από υπολογιστές άλλων χωρών και της πραγματοποίησης ψυχολογικού πολέμου μέσω διαδικτύου[192]. Από τότε και μέχρι σήμερα τα περιστατικά κυβερνοεπιθέσεων μεταξύ των δύο χωρών είναι στην κυριολεξία αμέτρητα. Τη στιγμή που γράφονται αυτές οι γραμμές, βάσει της πληροφόρησης κακόβουλων επιθέσεων σε σχεδόν πραγματικό χρόνο από την NORSE[193], από την Κίνα φαίνεται να ξεκινούν οι περισσότερες κακόβουλες ενέργειες ενώ η Ταϊβάν τόσο ως χώρα θύμα όσο και ως χώρα αφετηρία κακόβουλων επιθέσεων είναι στην πέμπτη θέση, κατάσταση άκρως ενδεικτική της καθημερινότητας της περιοχής. Η Ταϊβάν από την πλευρά της, αναγνωρίζοντας την δυσχερή θέση στην οποία βρίσκεται υπό την διαρκή πίεση των κινεζικών κυβερνοεπιθέσεων, το 2003 δημιούργησε μια νέα μονάδα του υπουργείου εθνικής άμυνας με σκοπό την προστασία των υπολογιστικών συστημάτων του στρατού και ορισμένων μη στρατιωτικών δικτύων[194]. Βέβαια, η δραστηριότητα κυβερνοπολέμου της Κίνας δεν περιορίζεται μόνο κατά της Ταϊβάν.

Η Κίνα φέρεται να είναι πίσω από τις κυβερνοεπιθέσεις που έθεσαν εκτός λειτουργίας τα υπολογιστικά συστήματα στο αμερικανικό Πεντάγωνο αλλά και πίσω από κυβερνοεπιθέσεις εναντίον της Γαλλίας, της Γερμανίας και της Ηνωμένου Βασιλείου[195]. Για τις πρόσφατες επιθέσεις εναντίον του αμερικανικού δικτύου

---

[191] Wang Pufeng, *Informational Warfare and Military Revolution*, Bejing: Military Sciences Publication House, December 1995, p.144

[192] Gary D. Rawnsley, *Old Wine in new Bottles: China-Taiwan Computer-Based Information Warfare and Propaganda*, International Affairs, Vol. 81, No. 5, October 2005, p.1070

[193] http://map.norsecorp.com

[194] Gary D. Rawnsley, *Old Wine in new Bottles: China-Taiwan Computer-Based Information Warfare and Propaganda*, International Affairs, Vol. 81, No. 5, October 2005, p.1073

[195] Andrew F. Krepinevich Jr., *The Pentagon's Wasting Assets: The Eroding Foundations of American Power*, Forreign Affairs, Vol. 88, No. 4, July/August 2009, p.25

διανομής ηλεκτρικής ενέργειας φημολογείται[196] οτι και πάλι η Κίνα είχε ενεργή συμμετοχή σε αυτές. Η κινεζική κυβέρνηση έχει κατηγορηθεί από τις Η.Π.Α. ευθέως για τη συμμετοχή της σε αυτές τις δραστηριότητες, ωστόσο η κυβέρνηση της Κίνας το αρνείται κατηγορηματικά, περνώντας στην αντεπίθεση ισχυριζόμενη οτι, όχι μόνο δεν είναι ο δράστης αλλά οτι ουσιαστικά είναι και αυτή ένα από τα θύματα[197]. Πέρα από το επικοινωνιακό μέρος του παιχνιδιού, αναμφίβολα η Κίνα έχει κάνει αλματώδη πρόοδο στον κυβερνοπόλεμο, η οποία εάν συνδυαστεί με το σύνολο των λοιπών επιτευγμάτων της με στρατιωτικές προεκτάσεις, όπως το διαστημικό της πρόγραμμα, την τοποθετεί στους κορυφαίους σε παγκόσμιο επίπεδο δρώντες στον κυβερνοπόλεμο. Ο αρθρογράφος και αναλυτής William Lynn προβλέπει[198] οτι μέσα στα επόμενα 20 χρόνια πολλές χώρες, μεταξύ αυτών και η Κίνα, θα εκπαιδεύουν περισσότερους υψηλού επιπέδου επιστήμονες τεχνολογίας υπολογιστών από ότι οι Η.Π.Α., με όποια προέκταση αυτό μπορεί να πάρει στο θέμα του κυβερνοπολέμου.

Τέλος, ειδικά για την περίπτωση της Κίνας, η αλματώδης πρόοδος στον τομέα του κυβερνοπολέμου δεν πρέπει να αναλυθεί ως μεμονωμένος τομέας. Αντίθετα, σε επίπεδο ευρύτερης στρατηγικής σχεδίασης, ιδιαίτερη ανησυχία πρέπει να δημιουργεί η εμπέδωση της έννοιας του απεριόριστου πολέμου, πνευματική ιδιοκτησία των Qiao Liang και Wang Xiangsui οι οποίοι στο βιβλίο που δημοσίευσαν το 1999 μιλούν για μια νέα μορφή πολέμου όπου πρακτικά υπάρχει μόνο ένας κανόνας που λέει οτι δεν υπάρχουν κανόνες. Υπό αυτή την οπτική, ο κυβερνοπόλεμος θα ήταν μόνο ένα από τα διαθέσιμα εργαλεία ενός τέτοιου απεριόριστου πολέμου, χωρίς κανόνες και όρια.

### Άλλοι Κρατικοί Δρώντες

Όπως είναι φανερό οι κρατικοί δρώντες με δυνατότητα πραγματοποίησης κυβερνοπολέμου δεν είναι μόνο οι Η.Π.Α., η Ρωσία και η Κίνα. Υπάρχουν στο παγκόσμιο στερέωμα πολλές χώρες με αποδεδειγμένη δυνατότητα πραγματοποίησης κυβερνοπολέμου, τόσο μέσω περιστατικών που τους αποδίδεται με κάποια σχετική ασφάλεια η ευθύνη όσο και μέσω της συμμετοχής τους σε κάποιους συνομαδώσεις οι οποίες αποσκοπούν στην βελτιστοποίηση αντιμετώπισης του κυβερνοπολέμου και του επιμερισμού του κόστους της προσπάθειας.

Για παράδειγμα η Βόρεια Κορέα έχει αποδεδειγμένα δυνατότητα εκτέλεσης κυβερνοπολέμου. Μπορεί το περιστατικό με την κυβερνοεπίθεση σε γνωστή εταιρεία κατασκευής ηλεκτρονικών συσκευών να ήταν η περίπτωση με τη μεγαλύτερη δημοσιότητα, ωστόσο δεν ήταν η μοναδική. Η περίπτωση της συγκεκριμένης χώρας έχει ενδιαφέρον για πολλούς λόγους, με τον σημαντικότερο να είναι ο ολοκληρωτικός έλεγχος κάθε εισερχόμενης ή εξερχόμενης πληροφορίας από τους αρμόδιους κρατικούς φορείς. Το κράτος, έχοντας πλήρη έλεγχο ακόμη και στο υλικό (δρομολογητές, κόμβοι κλπ) του διαδικτύου εντός της χώρας, μπορεί ανά πάσα στιγμή να κλείσει πλήρως το διαδίκτυο στο σύνολο της επικράτειας. Όσο αυτό δε

[196] Garance Burke and Jonathan Fahey, *AP Investigation: US Power Grid Vulnerable to Foreign Hacks*, San Jose California, 21 December 2015.
[197] *Cyberwarfare in China*, Wikipedia, https://en.wikipedia.org/wiki/Cyberwarfare
[198] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, Vol. 89, No. 5, September/October 2010, p.106

συμβαίνει, οι ίδιοι λόγοι (ολοκληρωτικός κρατικός έλεγχος, μοναδικός πάροχος υπηρεσιών διαδικτύου κλπ) καθιστά την Βόρεια Κορέα ευάλωτη σε έξωθεν προερχόμενες κυβερνοεπιθέσεις.

Η Ινδία συγκαταλέγεται μεταξύ των χωρών που έχουν επίσης πολύ υψηλή ικανότητα εκτέλεσης κυβερνοεπιθέσεων[199] και γενικά με ιδιαίτερα αυξημένο αριθμό επιστημόνων υψηλού επιπέδου γνώσεων πληροφορικής. Σε επίπεδο κυβερνοπροστασίας, η Ινδία έχει υιοθετήσει κανόνες προστασίας από κυβερνοεπιθέσεις με τον τίτλο Πληροφοριακή Τεχνολογική Δράση 2000[200].

Σε αντίστοιχο επίπεδο είναι και το Πακιστάν, στο οποίο η κακόβουλη χρήση του διαδικτύου έχει σημειώσει μεγάλη αύξηση τελευταία, με έμφαση όμως στο κυβερνοέγκλημα. Ανεξάρτητα αυτού, λήφθηκαν σε κρατικό επίπεδο κάποια μέτρα με σκοπό την όσο γίνεται καλύτερη θωράκιση των χρηστών του διαδικτύου, με την ψήφιση του νομοσχεδίου προστασίας από το κυβερνοέγκλημα το 2007.

Το Ιράν είναι περισσότερο γνωστό με την υπόθεση του stuxnet ως χώρα θύμα κυβερνοπολέμου παρά ως χώρα με δυνατότητες πραγματοποίησης κυβερνοεπιθέσεων. Αυτό δεν σημαίνει οτι δεν έχει τέτοιες δυνατότητες, κάτι που θα φάνταζε εξωπραγματικό για μια χώρα με πυρηνική γνώση. Το γεγονός οτι δεν έχουμε καταγεγραμμένα υψηλού επιπέδου κρούσματα κυβερνοπολέμου[201] με επιβεβαιωμένη προέλευση το Ιράν δεν έχει απολύτως καμμιά σημασία. Το αντίθετο μάλιστα αφού, σύμφωνα με μια εκτίμηση του Cyber Threat News, το Ιράν θεωρείται από τις ανερχόμενες δυνάμεις στον τομέα του κυβερνοπολέμου.

Η περίπτωση του Ισραήλ έγινε παγκόσμια γνωστή σχετικά πρόσφατα με το κακόβουλο λογισμικό stuxnet και θύμα τις συσκευές φυγοκέντρισης σε εργοστάσιο εμπλουτισμού πυρηνικού καυσίμου στο Ιράν. Σύμφωνα με όλες τις ενδείξεις, σε μια προσπάθεια που από πολλούς χαρακτηρίστηκε ως κίνηση μη διασποράς των πυρηνικών όπλων[202], Ισραηλινοί χάκερ σχεδίασαν και εξαπέλυσαν την κυβερνοεπίθεση. Ειδικοί αναλυτές της εταιρείας Symantec και Sophos είπαν οτι λόγω της πολυπλοκότητας της επίθεσης η όλη σχεδίαση θα απαίτησε μήνες δουλειάς και προετοιμασίας[203]. Ο stuxnet φαίνεται να ήταν προϊόν μελέτης και ανάπτυξης της περιβόητης ομάδας 8200, η Ισραηλινή αντίστοιχη οντότητα της αμερικανικής NSA[204].

Εντός ευρωπαϊκού χώρου είναι σίγουρο οτι σχεδόν το σύνολο των μεγάλων χωρών της κεντρικής ευρώπης έχουν ανεπτυγμένη σοβαρή δυνατότητα κυβερνοπολέμου. Σε μικρότερη κλίμακα αντίστοιχες δυνατότητες αναμένεται να

---

[199] Jonathan Kirshner, *Globalization, American Power, and International Security*, Political Science Quarterly (The Academy of Political Science), Vol. 123, No. 3, Fall 2008, p.378.

[200] *Cyberwarfare in India*, Wikipedia, https://en.wikipedia.org/wiki/Cyberwarfare

[201] Σε προηγούμενο κεφάλαιο ήδη αναφέρθηκε η, σύμφωνα με όλα τα διαθέσιμα στοιχεία, εξαπόλυση κυβερνοεπίθεσης από την Τεχεράνη με στόχο το δίκτυο διανομής ηλεκτρικής ενέργειας στις Η.Π.Α.

[202] Ian Rutherford, *NATO's New Strategic Concept, Nuclear Weapons, and Global Zero*, International Journal, Vol. 66, No. 2, Spring 2011, p.480

[203] Middle East Institute, *Chronology: October 16, 2010-January 15, 2011*, Middle East Journal, Vol. 65, No. 2, Spring 2011, p.312

[204] Paula Margulies, *Israel: The Homeland of Start-Ups*, World Policy Journal, Vol. 28, No. 3, Fall 2011, p.31

υπάρχουν και στις λοιπές χώρες, κυρίως εστιασμένη σε κυβερνοάμυνα και ίσως σε κυβερνοεπίθεση. Αλλά δεν έχει κάποια προστιθέμενη αξία στην παρούσα εργασία η ενασχόληση με χώρες της ευρωπαϊκής ηπείρου ως κρατικοί δρώντες κυβερνοπολέμου. Αντίθετα, σύντομα θα δούμε κάποιους δρώντες κυβερνοπολέμου που δεν έχουν κρατική οντότητα.

## Μη-κρατικοί Δρώντες

> *Αλλά όταν μιλάμε για κυβερνοέγκλημα, βιολογικά όπλα και μια νέα γκάμα οπλισμού στην μεταβιομηχανική επανάσταση, όταν ζούμε σε έναν κόσμο όπου μια υποδοχή γραμμής τηλεφώνου ή ένα τηλεοπτικό πίατο σου δίνει ισχύ και κύρος, τότε δεν είναι μόνο τα μεγάλα κράτη που οφελούνται. Μη κρατικοί δρώντες που αισθάνονται φιμωμένοι μπορούν να μεγενθύνουν την ισχύ τους διαμέσου αυτής της νέας τεχνολογίας. Οι σχέσεις ισχύος θα είναι πολύ πολυπλοκότερες παρά ποτέ*[205]

### Ισλαμικό Κράτος

Ίσως λίγο καιρό πριν να μην μπορούσε κανείς να διανοηθεί οτι κάποιος μη κρατικός δρων θα μπορούσε να αποτελέσει κυβερνοαπειλή για υπολογιστικά συστήματα χωρών όπως για παράδειγμα των Η.Π.Α. Ωστόσο, η αίσθηση που έχουν οι ειδικοί μέσα στις Η.Π.Α. είναι οτι το Ισλαμικό Κράτος (Ι.Κ.) φαίνεται να έχει δυνατότητα να εξαπολύσει κυβερνοεπιθέσεις εναντίον στόχων εντός της επικράτειας των Η.Π.Α. Έτσι, ο υπεύθυνος για την κυβερνοασφάλεια του Λευκού Οίκου, Clifton Triplett, σε δηλώσεις[206] του δεν απέκλεισε το ενδεχόμενο κάποια από τις αναμενόμενες κυβερνοεπιθέσεις του Ι.Κ. να καταφέρει να διατρήσει τις προστασίες του υπολογιστικού συστήματος του Λευκού Οίκου. Συμπλήρωσε, μάλιστα, πως κατά τη γνώμη του πρέπει να αναμένει οτι σε κάποια χρονική στιγμή κάποια κυβερνοεπίθεση του Ι.Κ. θα είναι πετυχημένη. Μέχρι πρόσφατα οι συμπαθούντες το Ι.Κ. ουσιαστικά εκτελούσαν κυβερνοεπιθέσεις περισσότερο για επίδειξη δυνατοτήτων παρά για κατασκοπεία ή άλλους λόγους. Αργότερα, όμως, αυτό άρχισε να αλλάζει, με την αρχή να γίνεται νωρίς το 2015 με την λεγόμενη ομάδα κυβερνοχαλιφάτου που πέτυχε να αποκτήσει πρόσβαση και έλεγχο σε λογαριασμούς κοινωνικού δικτύου ή λίγο μετά (Απρίλιος 2015) που υποστηρικτές του Ι.Κ. κατάφεραν αρχικά να απενεργοποιήσουν το τηλεοπτικό δίκτυο TV5Monde για ώρες και στη συνέχεια αντικατέστησαν τα κανάλια της εταιρείας, τις ιστοσελίδες και τους λογαριασμούς κοινωνικής δικτύωσης με άλλα, με περιεχόμενο φιλικό προς το Ι.Κ[207].

---

[205] Robert Kaplan, *Mr. Order Meets Mr. Chaos*, Foreign Policy, No. 124, May-June 2001, p.58-59.

[206] Aliya Sternstein, *New OPM Cyber Czar Worried About an ISIS Hack*, Nextgov Newsletter, 14 December 2015

[207] ο.π.

Σύμφωνα με το ειδησεογραφικό πρακτορείο RT[208], επικαλούμενο πηγές μέσα από το αμερικανικό Πεντάγωνο, οι ένοπλες δυνάμεις των Η.Π.Α. πρόκειται να ανοίξουν ένα ψηφιακό μέτωπο με τους τρομοκράτες του Ι.Κ. με πεδίο αντιπαράθεσης τον κυβερνοχώρο. Η πρόθεση της αμερικανικής Διοίκησης Κυβερνοπολέμου είναι να χρησιμοποιήσει κακόβουλο λογισμικό για να προκαλέσει αναστάτωση και να διασπάσει την προπαγάνδα του Ι.Κ. και τις προσπάθειες στρατολόγησης που επιχειρούνται μέσα από το διαδίκτυο.

Και δεν είναι μόνο η προσπάθεια στρατολόγησης στο διαδίκτυο που έχει συνέπειες και κόστος για τον δυτικό κόσμο. Το Ι.Κ. μεταχειρίζεται σήμερα στρατηγικές αναμειγνύοντας ανηλεείς στρατιωτικές επιχειρήσεις με μια εμπρηστική εκστρατεία στα μέσα κοινωνικής δικτύωσης, προβάλλοντας φωτογραφίες και βίντεο από βάναυσες εκτελέσεις[209].

Καθίσταται σαφές οτι το Ι.Κ. αντιπαρατίθεται στον κυβερνοχώρο με πληθώρα αντιπάλων από δυσανάλογα ισχυρότερες δυνάμεις, κάτι που όμως στον κυβερνοπόλεμο δεν έχει μεγάλη αξία, όπως επιβεβαιώνεται και στην πράξη. Το Ι.Κ. δεν είναι ο πρώτος μη κρατικός δρων που εκμεταλλεύεται στο μέτρο που μπορεί τον κυβερνοπόλεμο.

### Χεζμπολά

Η Χεζμπολά είχε αρχίσει να αντιλαμβάνεται αρκετά πριν το Ι.Κ. το όφελος από την εκμετάλλευση των δομών του διαδικτύου κάτι μάλιστα που ταίριαζε ακριβώς στο προφίλ των επιχειρησιακών δράσεών της. Άλλωστε ήταν η συγκεκριμένη οργάνωση που το καλοκαίρι του 2006 αντιλήφθηκε πλήρως το όφελος πίσω από την –τότε-νεοαναδυόμενη έννοια του ασύμμετρου πολέμου[210] υπό συνθήκες υψηλής τεχνολογίας. Κατά την σύντομη διάρκειας σύγκρουση των 34 ημερών, η Χεζμπολά εκτόξευσε περίπου 4.000 ρουκέτες εναντίον του Ισραήλ η πλειονότητα των οποίων ήταν μικρής εμβέλειας ενώ το σύνολό τους ήταν μη κατευθυνόμενες. Εντούτοις, απαιτήθηκε να απομακρυνθούν από τα σπίτια τους με σχέδιο εκκένωσης περισσότεροι από 300.000 Ισραηλινοί πολίτες ενώ διυλιστήρια στην πόλη της Χάιφα άδειασαν προληπτικά τις δεξαμενές αποθήκευσης πετρελαίου ως προληπτικό μέτρο έναντι ενδεχόμενου χτυπήματος αριθμού ρουκετών εντός των εγκαταστάσεών του και, άρα, πιθανότητα καταστροφικών για όλη την περιοχή αλυσιδωτών εκρήξεων και πυρκαϊών. Η οικονομική επίπτωση της δράσης της Χεζμπολά ήταν σημαντική[211].

Ο κυβερνοπόλεμος αντίστοιχα, επιτρέπει σε μη κρατικούς δρώντες να επιφέρουν ή να επισείεται ο κίνδυνος να επιφέρουν αντίστοιχα χτυπήματα σε υποδομές κρατικών δρώντων με οικονομικές αλλά και ψυχολογικές συνέπειες τόσο στους εμπόλεμους όσο και στους αμάχους, εάν και όπως είδαμε στον κυβερνοπόλεμο η διάκριση αυτή δεν είναι ποτέ ευκρινής. Η πραγματική δυνατότητα

---

[208] RT USA, A Cyber Campaign: *Pentagon Ponders Fighting ISIS Online*, RT USA, http://www.rt.com/usa/326710-pentagon-isis-cyber-warfare/

[209] Joseph Nye, *Ο Πόλεμος στον 21ο Αιώνα*, Κόσμος, Το Βήμα online, http://www.tovima.gr/PrintArticle/?aid=675494

[210] Andrew F. Krepinevich Jr., *The Pentagon's Wasting Assets: The Eroding Foundations of American Power*, Forreign Affairs, Vol. 88, No. 4, July/August 2009, p.24

[211] ο.π.

της Χεζμπολά να εκτελεί υψηλής σημαντικότητας κυβερνοεπιθέσεις δεν είναι απόλυτα μετρήσιμη, ωστόσο η διαχρονική διασύνδεση της οργάνωσης με κύκλους στο Ιράν που την στηρίζουν οικονομικά, επιχειρησιακά και σε επίπεδο παροχής οπλικών μέσων συνεχίζει να μας δίνει το δικαίωμα να κατατάσσουμε την Χεζμπολά στην κορυφή των μη κρατικών δρώντων που έχουν δυνατότητα εκτέλεσης κυβερνοπολέμου. Είναι θέμα επιχειρησιακής ανάλυσης και προτεραιοποίησης των επιδιώξεών της το χρονικό σημείο στο οποίο η οργάνωση θα επιλέξει να δείξει τις δυνατότητές της και στον τομέα αυτό. Άλλωστε, όπως πολύ εύστοχα αναφέρει ο William Lynn, στον κυβερνοπόλεμο είναι η επίθεση που έχει το πάνω χέρι[212].

### Ανεξάρτητες οντότητες

Τελευταία υποκατηγορία μη κρατικών δρώντων είναι οι λεγόμενες ανεξάρτητες οντότητες. Συνηθέστερα πρόκειται για συνομαδώσεις ατόμων και σπανιότερα συναντούμε τα άτομα που δρουν ανεξάρτητα και μεμονωμένα. Στην πλειονότητα των περιπτώσεων η δράση των ανεξαρτήτων οντοτήτων δεν οδηγείται από κάποια υψηλού επιπέδου κινητήρια ιδεολογία, όπως η περίπτωση των κυβερνοπολεμιστών της Χεζμπολά, οι οποίοι υπηρετούν την ιδεολογία της κεντρικής οργάνωσης από το μετερίζι του κυβερνοχώρου. Εδώ συχνά η κυβερνοεπίθεση γίνεται για την κυβερνοεπίθεση ή για λόγους που είναι άμεσα συνδεδεμένοι με την ίδια την δομή του διαδικτύου. Θα μπορούσε απλουστευτικά να θεωρηθεί οτι στην υποκατηγορία αυτή εντάσσονται αυτομάτως όλοι οι χάκερ εαν και ο όρος είναι τόσο ευρείας χρήσης που ίσως η απλούστευση αυτή να αποτελεί παρακινδυνευμένη προσέγγιση. Ωστόσο, με την έννοια του χάκερ που δίδει ο Jeremie Zimmermann, φίλος και συνεργάτης του Julian Assange των Wikileaks, εύκολα ξεκαθαρίζεται οτι, πράγματι, οι χάκερ μπορεί να θεωρηθεί οτι εμπίπτουν σε αυτήν την κατηγορία δρώντων, τουλάχιστον στα αρχικά τους βήματα.

> *Ο χάκερ είναι ένας οπαδός της τεχνολογίας, κάποιος που του αρέσει να κατανοεί πώς δουλεύει, πώς λειτουργεί η τεχνολογία, όχι για να παγιδευτεί στην τεχνολογία, αλλά για να την κάνει να δουλέψει καλύτερα. Φαντάζομαι οτι όταν ήσασταν πέντε ή επτά χρονών είχατε ένα κατσαβίδι και προσπαθούσατε να ανοίξετε συσκευές για να καταλάβετε πώς ήταν από μέσα. Αυτό είναι το να είσαι χάκερ*[213].

Εαν και το κίνητρο, εφόσον πρόκειται πράγματι περί ειλικρινούς ενδιαφέροντος για την τεχνολογία, δείχνει (και μπορεί πράγματι) να είναι καλόηθες, αυτό δε σημαίνει οτι όλοι οι χάκερ παραμένουν σε αυτήν την κατάσταση, ούτε οτι οι πράξεις τους, οδηγούμενες από την τεχνολογική πρόκληση της απόκτησης επιπλέον γνώσης για κάποιο σύστημα, δεν θα εκληφθούν από κάποιους άλλους ως κακόβουλες ενέργειες. Και δεν θα μπορούσε να είναι διαφορετική η αντίδραση της πλευράς που δέχεται την διερευνητική από πλευράς κατανόησης τεχνολογίας παράνομη διείσδυση του χάκερ αφού δεν είναι σε θέση να γνωρίζει ποιός κάνει την επίθεση,

---

[212] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, Vol. 89, No. 5, September/October 2010, p.99

[213] Julian Assange and others, *Η Ελευθερία και το Μέλλον του Διαδικτύου: Η Ανάλυση του Εκδότη των Wikileaks* (Αθήνα: Ποιότητα, 2013)

για ποιούς λόγους και με τι σκοπούς. Για παράδειγμα, εαν το σύστημα-στόχος είναι το υπολογιστικό δίκτυο ελέγχου του συστήματος GPS στο Κολοράντο των Η.Π.Α. από έναν ή περισσότερους χάκερ (με την έννοια του παραπάνω ορισμού), τι θα πρέπει να κάνει η Διοίκηση Διαστήματος των Η.Π.Α.; Έτσι, μπορεί σε επίπεδο συζητήσεων το κίνητρο των χάκερ να είναι ή να δείχνει να είναι αγαθό, ωστόσο στον κυβερνοχώρο δεν χωράει διαφοροποίηση των δράσεων και των αντιδράσεων βάσει εκτίμησης των λόγων για τους οποίους επιχειρείται μια επίθεση. Σε τελικά ανάλυση, είναι λίγοι εκείνοι που παραμένουν απλοί εραστές της τεχνολογίας και, άρα, χάκερ με την ωραιοποιημένη μορφή αφού σε κάποια στιγμή θα οδηγηθούν στο επόμενο βήμα που είναι η κεφαλαιοποίηση της βαθύτερης γνώσης που έχουν αποκτήσει για οικονομικούς ή ιδεολογικούς λόγους. Έτσι, συμπερασματικά μπορούμε να πούμε οτι και αυτή η υποκατηγορία διαδραματίζει κάποιον ρόλο στον κυβερνοπόλεμο, ρόλο που σε καμμία περίπτωση δεν μπορεί να αγνοηθεί, λαμβάνοντας μάλιστα υπόψη και το επίπεδο της απόρρητης πληροφόρησης που κατάφερε τελικά να συλλέξει ο Julian Assange και οι συνεργάτες του, κάτι που αποκτά ιδιαίτερη αξία εάν αναλογιστεί κανείς και την ποιότητα των υπολογιστικών εκείνων συστημάτων τα οποία παραβιάστηκαν από την ομάδα των Wikileaks.

## 5. ΝΑΤΟ, ΕΥΡΩΠΑΪΚΗ ΕΝΩΣΗ, ΕΛΛΑΔΑ ΚΑΙ ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

Μετά την προσέγγιση του φαινομένου του κυβερνοπολέμου από την πλευρά των δρώντων, είτε πρόκειται για κρατικές είτε για μη κρατικές οντότητες, εύλογα θα μπορούσε να προκύψει το ερώτημα: στην έτσι κι' αλλιώς αφηρημένη αρένα του κυβερνοπολέμου, ισχύει άραγε οτι ο καθένας είναι εναντίων όλων ή έχουν ομαδοποιηθεί οι αμυντικές απαιτήσεις κάποιων δρώντων, οδηγώντας σε συμμαχικές δράσεις προσωρινού ή μονιμότερου χαρακτήρα; Η απάντηση κλίνει σαφώς προς την δεύτερη επιλογή, καθιστώντας την ανάπτυξη αμυντικών μηχανισμών στον κυβερνοπόλεμο ομαδοποιημένη δράση. Ωστόσο, λιγότερο ή περισσότερο, τα συμμαχούντα κράτη διατηρούν για τον εαυτό τους κάποιες επιλογές και τις αντίστοιχες δυνατότητες, τις οποίες δεν επιθυμούν να διαθέσουν σε κοινή χρήση. Παρόλο το νέο του χαρακτήρα της απειλής του κυβερνοπολέμου, δεν παρατηρήθηκε δημιουργία συμμαχιών με αποκλειστικό σκοπό την κοινή κυβερνοάμυνα. Αντίθετα, ο κυβερνοπόλεμος αντιμετωπίστηκε ως άλλη μια μορφή ένοπλης απειλής. Έτσι, ήδη υπάρχουσες συμμαχίες αναπροσάρμοσαν τους θεσμούς τους και τα μέσα τους στην νέα αυτή διάσταση, αφού για κάθε συμμαχία η έλευση του κυβερνοπολέμου δεν δημιούργησε από μόνη της νεους εχθρούς, απλά έδωσε στους ήδη χαρακτηρισμένους εχθρούς επιπλέον δυνατότητες. Το ΝΑΤΟ, ήδη στην έβδομη δεκαετία της ύπαρξής του και μετά από τις διαδοχικές αναπροσαρμογές του στην πραγματικότητα της γεωγραφικής περιοχής αρμοδιότητας του, αντιμετώπισε άλλη μία πρόκληση: τον κυβερνοχώρο. Σχετικά έγκαιρα αναγνώρισε τη σοβαρότητα της νέας αυτής μορφής απειλής και έκανε τις απαραίτητες προσαρμοστικές τροποποιήσεις στη δομή του ώστε να είναι προετοιμασμένο για κάθε ενδεχόμενο.

### ΝΑΤΟ

> *Απέναντι στο δεδομένο της ολοένα και αυξανόμενης εξάρτησης από την τεχνολογία και το διαδίκτυο, η Συμμαχία προωθεί τις προσπάθειές της για αντιμετώπιση της ευρείας κλίμακας κυβερνοαπειλών που στοχοποιούν τα δίκτυα του ΝΑΤΟ σε καθημερινή βάση. Η αυξανόμενη επιτήδευση αυτών των κυβερνοεπιθέσεων καθιστά την προστασία των επικοινωνιακών και πληροφοριακών συστημάτων της Συμμαχίας μια επείγουσα ανάγκη*[214].

### Χρονοδιάγραμμα[215]

Όπως είναι φυσικό, η Συμμαχία δεν αντιλήφθηκε ξαφνικά την απαίτηση προστασίας από τον κυβερνοπόλεμο ούτε και έφτασε στο σημερινό επίπεδο ικανοτήτων από τη μια στιγμή στην άλλη. Χρειάστηκε χρόνος, έρευνα, ανάλυση και γνώση (η οποία κάποιες φορές είχε το τίμημά της, όπως η περίπτωση της Εσθονίας) για να αποκρυσταλλωθεί η σημερινή πολιτική κυβερνοασφάλειας. Τα σημαντικότερα βήματα ήταν:

---

[214] ΝΑΤΟ, *Cyber Security*, http://www.nato.int/cps/en/natohq/topics_78170.htm
[215] ο.π.

*Σύνοδος Κορυφής της Πράγας, 2002*

Αν και το ΝΑΤΟ πάντα προστάτευε τα επικοινωνιακά και πληροφοριακά συστήματά του, η Σύνοδος Κορυφής της Πράγας το 2002 ανέδειξε την αναγκαιότητα για κυβερνοασφάλεια ως αντικείμενο της επίσημης ατζέντας.

*Σύνοδος Κορυφής της Ρίγα, 2006*

Οι ηγέτες των συμμαχικών χωρών μελών επαναβεβαίωσαν εκεί την ανάγκη παροχής επιπρόσθετης ααφάλειας στα επικοινωνιακά και πληροφοριακά συστήματα της συμμαχίας.

*Κυβερνοεπίθεση στην Εσθονία, 2007*

Αμέσως μετά την κυβερνοεπίθεση εναντίον δημόσιων και ιδιωτικών οργανισμών στην Εσθονία, τον Απρίλιο και τον Μάιο του 2007, οι υπουργοί άμυνας των μελών συμφώνησαν (Ιούνιος 2007) οτι απαιτείται επείγουσα δράση στον τομέα της κυβερνοάμυνας. Ως συνέπεια αυτού, το ΝΑΤΟ ενέκρινε την πρώτη Πολιτική Κυβερνοάμυνας, τον Ιανουάριο του 2008. Το καλοκαίρι του ίδιου έτους η σύρραξη μεταξύ Ρωσίας και Γεωργίας κατέδειξε οτι οι κυβερνοεπιθέσεις έχουν τη δυναμική να καταστούν μείζονα συστατικά του συμβατικού πολέμου.

*Σύνοδος Κορυφής της Λισαβόνας, 2010*

Στη Λισαβόνα, μεταξύ άλλων σημαντικών αποφάσεων για την μετεξέλιξη του ΝΑΤΟ, υιοθετήθηκε ένα νέο Στρατηγικό Σχέδιο, όπου δόθηκε ως έργο στην βορειοατλαντική επιτροπή να αναπτύξει μία σε βάθος πολιτική κυβερνοάμυνας και να προετοιμάσει το επιχειρησιακό πλάνο δράσης για εφαρμογή της πολιτικής αυτής. Έτσι, τον επόμενο έτος οι υπουργοί άμυνας του ΝΑΤΟ ενέκριναν την δεύτερη Πολιτική Κυβερνοάμυνας , η οποία έθεσε ως όραμα τις συνδυασμένες προσπάθειες κυβερνοάμυνας σε όλο το εύρος της συμμαχίας σε νέα βάση: αυτή ενός περιβάλοντος με ταχέως εξελισσόμενες απειλές και τεχνολογίες.

*Σύνοδος Κορυφής του Σικάγο, 2012*

Οι ηγέτες των χωρών επαναβεβαίωσαν την προσήλωση των χωρών τους στην βελτίωση της ικανότητας κυβερνοάμυνας της συμμαχίας και την τοποθέτηση όλων των δικτύων του ΝΑΤΟ κάτω από συγκεντρωτική προστασία. Έτσι, τον Ιούλιο του ίδιου έτους ιδρύθηκε η NCIA[216], ως μέρος την αναδόμησης του ΝΑΤΟ για το σκοπό αυτό. Τον Φεβρουάριο του 2014 τεκμηριώθηκε η αναγκαιότητα υιοθέτησης μιας νέας, αναθεωρημένης Πολιτικής Κυβερνοάμυνας η οποία (νέα Πολιτική) εγκρίθηκε για δοκιμαστική εφαρμογή τον Ιούνιο. Η νέα, τρίτη κατά σειρά Πολιτική Κυβερνοάμυνας του ΝΑΤΟ είναι αυτή που βρίσκεται σήμερα σε εφαρμογή.

*Σύνοδος Κορυφής της Ουαλίας, 2014*

Τον Σεπτέμβριο του 2014 στην Ουαλία η συμμαχία ενέκρινε ένα Σχέδιο Δράσης για την Κυβερνοάμυνα, το οποίο μαζί με την Πολιτική Κυβερνοάμυνας δίνει στο ΝΑΤΟ να επιτύχει την ευόδωση των βασικών επιδιώξεων της Συμμαχίας.

[216] **N**ATO **C**ommunication and **I**nformation **A**gency.

### Βασικές Κατευθύνσεις Κυβερνοάμυνας

Οι σημαντικότερες κατευθύνσεις που αποτελούν τα σημεία κλειδιά της Κυβερνοάμυνας του ΝΑΤΟ περιλαμβάνουν κατ' αρχάς την κοινή αντίληψη όλων των μελών οτι η Κυβερνοάμυνα είναι αναπόσπαστο τμήμα της βασικής υποχρέωσης των μελών στο πλαίσιο της συλλογικής άμυνας. Έτσι, η απαίτηση συμμετοχής όλων των μελών έναντι κυβερνοεπίθεσης σε ένα μέλος της συμμαχίας θωρακίζεται θεσμικά, κάτι που ως ένα βαθμό περιορίζει την δυνατότητα επιλεκτικής συμμετοχής (ή αποχής) κάποιου τρίτου κράτους μέλους στην συλλογική αμυντική αντίδραση εναντίον της κυβερνοεπίθεσης. Ωστόσο, λόγω της νεφελώδους έννοιας του κυβερνοχώρου, η δέσμευση για συλλογική κυβερνοάμυνα θα μπορούσε να θεωρηθεί μια χαλαρότερη έκδοση της πιο συγκεκριμένης συλλογικής συμβατικής άμυνας, η οποία αποτελεί μαζί με την διαχείριση κρίσεων και την συνεργατική ασφάλεια το τρίπτυχο των βασικών αρχών[217] του ΝΑΤΟ μετά τη Λισαβόνα.

Η έγκριση της πρώτης Πολιτικής Κυβερνοάμυνας το 2008 αναμφίβολα αποτελεί σημαντικό σταθμό αλλά και σημείο καμπής της συμμαχίας στο θέμα του Κυβερνοπολέμου. Το γεγονός οτι έπρεπε να προηγηθεί η κυβερνοεπίθεση στην Εσθονία ώστε το ΝΑΤΟ να κινητοποιηθεί είναι κάτι που δεν προσμετράται θετικά, ωστόσο τα αντανακλαστικά που ανέπτυξε η Συμμαχία μετά αμβλύνουν την αρνητική εικόνα της νωθρή εκκίνησης. Η εκάστοτε ισχύουσα Πολιτική Κυβερνοάμυνας θέτει το πλαίσιο και παρέχει κατευθύνσεις αμυντικής σχεδίασης στον τομέα της κυβερνοάμυνας και το γεγονός οτι ήδη βρισκόμαστε στην τρίτη κατά σειρά Πολιτική δείχνει τόσο τον ρυθμό εξέλιξης των δεδομένων στον κυβερνοχώρο όσο και την αποφασιστικότητα του ΝΑΤΟ να μην ακολουθεί αλλά τουλάχιστον να συμβαδίζει με την εποχή.

Καθίσταται σαφές οτι το ΝΑΤΟ είναι υπεύθυνο για την προστασία των δικών του επικοινωνιακών και πληροφοριακών υποδομών. Αντίθετα, το κάθε κράτος μέλος είναι υπεύθυνο για την προστασία των δικών του, εθνικών υποδομών πληροφορικής και επικοινωνιών. Επιπλέον, τα εθνικά αυτά συστήματα οφείλουν να είναι συμβατά με τα αντίστοιχα της Συμμαχίας για σκοπούς διαλειτουργικότητας.

Οι συμμαχικές χώρες δεσμεύονται να αυξήσουν την ροή πληροφόρησης και την αμοιβαία βοήθεια σε θέματα πρόληψης, αντιμετώπισης και επαναφοράς μετά από κυβερνοεπιθέσεις. Ειδικά στο θέμα της πρόληψης, υπάρχουν πολλά εθνικά στεγανά που καμμιά χώρα δεν θα δεχόταν να παραβιαστούν στον βωμό της συμμαχικότητας. Εάν και αυτό δεν καταγράφεται, είναι κοινά και σιωπηρά αποδεκτό στους κύκλους της συμμαχίας.

Αποτελεί διαρκή επιδίωξη του ΝΑΤΟ η ολοένα και μεγαλύτερη ενδυνάμωση των σχέσεων μεταξύ αυτού και του βιομηχανικού τομέα. Έτσι, θα επιτευχθεί θεσμική προσέγγιση σε έναν χώρο που με την διαρκώς αυξανόμενη αλληλεξάρτηση που η τεχνολογία επιβάλλει η προσέγγιση ήδη υφίσταται, αλλά με πιο άτυπο χαρακτήρα.

Τέλος, το ΝΑΤΟ στοχεύει στον εμπλουτισμό των δυνατοτήτων του στην κυβερνοάμυνα μέσω παροχής εκπαίδευσης του προσωπικού στο αντικείμενο, την καλλιέργεια παιδείας κυβερνοασφάλειας και την πραγματοποίηση ασκήσεων κυβερνοπολέμου. Το ΝΑΤΟ αναδεικνύει το τρίγωνο Άνθρωπος-Υπολογιστικό Σύστημα-Διαδικασία και θέτει ως στόχο την ενδυνάμωση και των τριών αυτών συντελεστών ως ανελαστική υποχρέωση στον αγώνα της κυβερνοάμυνας.

[217] Collective defence-Crisis management-Cooperative security

## Ευρωπαϊκή Ένωση

> *Η Ευρωπαϊκή Ένωση (ΕΕ) αποτελεί σήμερα ένα νέο πολιτικό σύστημα υπό διαμόρφωση. Στη δύσκολη, διακεκομμένη αλλά και εξαιρετικά ενδιαφέρουσα πορεία της από την οικονομική και νομισματική στην πολιτική ενοποίηση, η ΕΕ αντιμετώπισε τα αμείλικτα ζητήματα της ασφάλειας και της άμυνας, ζητήματα που εξακολουθούν να τίθενται με αμείωτη ένταση στο πεδίο των διεθνών σχέσεων. Τα ζητήματα αυτά υπογράμμισαν και την αναγκαιότητα της στρατιωτικής ισχύος, την οποία επιδιώκει να αποκτήσει σε όλο και μεγαλύτερο βαθμό η ΕΕ μέσω της ανάπτυξης της Ευρωπαϊκής Πολιτικής Ασφάλειας και Άμυνας (ΕΠΑΑ). Πρόκειται για το αποτέλεσμα μιάς μακρόχρονης πορείας που ουσιαστικά είχε ξεκινήσει από την επομένη του Β' Παγκόσμιου Πολέμου. Παράλληλα, πρόκειται για την αρχή μιας νέας προσπάθειας για μια σχετική, έστω, αυτοτέλεια της ΕΕ στον αμυντικό τομέα.*[218]

Η πρώτη ουσιαστική μεταπολεμική προσπάθεια των ευρωπαϊκών κρατών για τη δημιουργία μιάς αμυντικής συνεργασίας έγινε το 1948, με την υπογραφή της Συνθήκης των Βρυξελών[219]. Έκτοτε, πολλές προσπάθειες έχουν καταβληθεί για την απόκτηση πραγματικής αμυντικής δυνατότητας η οποία θα βασίζεται αποκλειστικά στα μέσα των χωρών μελών της ΕΕ. Η κίνηση που φάνηκε να είναι η πλέον ελπιδοφόρα προς την κατεύθυνση της αμυντικής ευρωπαϊκής ενοποίησης ήταν αναμφίβολα η δημιουργία της Δυτικοευρωπαϊκής Ένωσης (ΔΕΕ) η οποία όμως δεν κατάφερε να φανεί αντάξια των προσδοκιών των ευρωπαίων, ακόμη και μετά την Διακήρυξη της Ρώμης όπου φάνηκε οτι η ΔΕΕ μετά από ένα μεγάλο διάστημα αδράνειας θα έμπαινε σε τροχιά ουσιαστικής δράσης. Αντίστοιχες ήταν οι προσδοκίες αμέσως μετά την Συνθήκη του Μάαστριχτ όπου διεφάνη οτι η ΔΕΕ θα αποτελούσε τον αμυντικό μοχλό της ΕΕ. Ωστόσο, στη Συνθήκη του Άμστερνταμ εκφράστηκε η πρόθεση ενσωμάτωσης της ΔΕΕ στην ΕΕ κάτι που τελικά αποφασίστηκε στη σύνοδο κορυφής της ΕΕ στην Κολωνία το 1999, αφού μεταφέρθηκαν όλες οι επιχειρησιακές αρμοδιότητες της ΔΕΕ στην ΕΕ, στο πλαίσιο της Ευρωπαϊκής Πολιτικής Ασφάλειας και Άμυνας (ΕΠΑΑ)[220].

Η ΕΠΑΑ, σύμφωνα με τον Κώστα Λάβδα, συνιστά τον κύριο παράγοντα ισχύος της ΕΕ, με αντικειμενικό σκοπό την αντιμετώπιση των απειλών, όπως αυτές καθορίζονται στο κείμενο της Ευρωπαϊκής Στρατηγικής Ασφάλειας. Με τη Συνθήκη του Μάαστριχτ καθιερώθηκε η Κοινή Εξωτερική Πολιτική και Πολιτική Ασφάλειας

---

[218] Πρόλογος του Κώστα Λάβδα στο βιβλίο του Ιωάννη Παρίση *Η Ευρώπη της Άμυνας: Ευρωπαϊκή Πολιτική Ασφάλειας & Άμυνας*, Αθήνα: Εκδόσεις Έκφραση Πολιτισμού, 2010.

[219] Ιωάννης Παρίσης, *Η Ευρώπη της Άμυνας: Ευρωπαϊκή Πολιτική Ασφάλειας & Άμυνας*, Αθήνα: Εκδόσεις Έκφραση Πολιτισμού, 2010.

[220] Ιωάννης Παρίσης, *Η Ευρώπη της Άμυνας: Ευρωπαϊκή Πολιτική Ασφάλειας & Άμυνας*, Αθήνα: Εκδόσεις Έκφραση Πολιτισμού, 2010.

(ΚΕΠΠΑ), κάτι που συνιστά των δεύτερο πυλώνα της ΕΕ. Έτσι, η ΕΕ είχε πλέον ένα πλαίσιο εντός του οποίου μπορούσε να κινηθεί με σκοπό να ανταποκριθεί στις ελπίδες και τις προσδοκίες που δημιουργούσε το ρευστό περιβάλλον της ευρωπαϊκής ηπείρου, ειδικά με την κατάρρευση της Σοβιετικής Ένωσης, την διάλυση του Συμφώνου της Βαρσοβίας και το επακόλουθο κενό ισχύος που δημιουργήθηκε στην περιοχή. Με τις επακόλουθες τροποποιήσεις στην ΚΕΠΠΑ (Νίκαια, Λισαβόνα) η ΚΕΠΠΑ αποτέλεσε το θεσμικό πλαίσιο εντός του οποίου δημιουργήθηκε η ΕΠΑΑ[221]. Επίσης, μετά το Συμβούλιο της Θεσσαλονίκης[222] παρουσιάσθηκε το κείμενο της Ευρωπαϊκής Στρατηγικής Ασφάλειας (ΕΣΑ), που τέθηκε σε εφαρμογή στο τέλος του ίδιου έτους.

Η ΕΣΑ αποτελεί σημαντικό στοιχείο για την κατανόηση των αποστολών των στρατιωτικών δυνάμεων της ΕΕ και γενικότερα της ΕΠΑΑ[223]. Θεσμικά, το είδος των αποστολών αυτών περιγράφεται στην Διακήρυξη του Πίτερσμπεργκ και για αυτό συχνά ονομάζονται και αποστολές Πίτερσμπεργκ.

Ενώ με την μέχρι τώρα περιγραφή φαίνεται σε θεωρητικό επίπεδο να υπάρχει σημαντική δυνατότητα ανάληψης στρατιωτικών δράσεων από την ΕΕ, πρέπει να υπενθυμίσουμε οτι ακόμη και σήμερα, η ευρωπαϊκή ένωση δεν διαθέτει στρατό. Οι χώρες μέλη έχουν σε εθνικό επίπεδο σημαντικό επίπεδο στρατιωτικής ισχύος για τα παγκόσμια δεδομένα, αλλά πρόκειται για κάτι διαφορετικό. Υπάρχουν σχέδια, δομές και διαδικασίες για συγκρότηση ευρωπαϊκής δύναμης για ανάληψη δράσεων τύπου Πιτερσμπεργκ αλλά δεν υπάρχει ευρωπαϊκός στρατός. Ακόμη και η πολυσυζητημένη ευρωπαϊκή δύναμη ταχείας αντίδρασης είναι κάτι που παραμένει στη θεωρία. Έτσι, οι πραγματικές αμυντικές δυνατότητες της ΕΕ δεν μπορούν, τόσο ουσιαστικά όσο και δομικά, να συγκριθούν για παράδειγμα με τις αντίστοιχες ΝΑΤΟικές, παρόλο που τα συμμετέχεοντα κράτη και στους δύο οργανισμούς είναι περίπου τα ίδια, με το ΝΑΤΟ να περιλαμβάνει και μέλη εκτός ΕΕ. Κατά συνέπεια, δεν είναι δυνατό να μιλάμε σε επίπεδο ΕΕ και στρατού για πραγματικές δυνατότητες επιχειρήσεων πλην των δράσεων Πίτερσμπεργκ, στις οποίες δεν γίνεται καμμιά αναφορά για κυβερνοάμυνα.

Εκτός από την εγγενή αυτή αδυναμία, η ΕΠΑΑ δεν αναφέρεται σε κυβερνοπόλεμο και συναφείς δράσεις, ίσως γιατί ως κείμενο σχετικά υψηλού επιπέδου, καθορίζει το γενικό πλαίσιο αμυντικής δράσης. Σε αντιδιαστολή με το ΝΑΤΟ που την τελευταία δεκαετία η κυβερνοάμυνα έχει εξελιχθεί σε κομβικής σημασίας δράση, η ΕΕ φαίνεται να μην έχει φτάσει στο σημείο να αντιληφθεί το πόσο καταλυτική μπορεί να είναι η συνδρομή (θετική ή αρνητική) του κυβερνοπολέμου για την εξέλιξη των επιχειρήσεων. Δεν πρέπει να παραγνωρίζεται βέβαια οτι η ΕΠΑΑ και η αμυντική διάσταση της ΕΕ εν γένει δεν έχει ούτε τον βαθμό ωριμότητας του ΝΑΤΟ ούτε τις πραγματικές δυνάμεις μόνιμης στελέχωσης και άρα θα μπορούσε κανείς να ισχυριστεί οτι όταν γίνει πραγματικότητα ο ευρωστρατός τότε θα πρέπει να αρχίσει η ΕΠΑΑ να ασχολείται με θέματα κυβερνοπολέμου. Η προσωπική αντίληψη του γράφοντα είναι οτι ακριβώς λόγω των εγγενών αυτών μειονεκτημάτων της άμυνας στην ΕΕ και λόγω της γνώσης που ήδη υπάρχει σε εθνικό επίπεδο στις ένοπλες δυνάμεις των μελών της ΕΕ, θα πρέπει η ΕΠΑΑ να εκμεταλλεύεται τις δυνατότητες

[221] ο.π.

[222] Θεσσαλονίκη, 21 Ιουνίου 2003

[223] Ιωάννης Παρίσης, *Η Ευρώπη της Άμυνας: Ευρωπαϊκή Πολιτική Ασφάλειας & Άμυνας*, Αθήνα: Εκδόσεις Έκφραση Πολιτισμού, 2010.

που παρέχει ο κυβερνοπόλεμος σε ασθενείς ομάδες ώστε να αρχίσει να αναπτύσσεται τώρα η ευρωπαϊκή στρατηγική κουλτούρα, με αφετηριακό σημείο ακριβώς τον κυβερνοπόλεμεμο.

Ολοκληρώνοντας, εαν ανατρέξουμε στο Σχέδιο Δράσης Ανάπτυξης Στρατιωτικών Δυνατοτήτων που θεσπίστηκε ως συνέπεια του Helsinki Headline Goal, ενώ βλέπουμε οτι πράγματι η ΕΕ αναγνωρίζει το οτι έχει μεγάλες ελλείψεις σε πολλούς τομείς αμυντικής προετοιμασίας και συνέστησε 19 ομάδες εργασίας για την κάλυψη των ελλείψεων αυτών, δεν γίνεται καμμιά αναφορά σε ελλείψεις που να σχετίζονται με τις επιχειρήσεις στον κυβερνοχώρο. Έτσι, είναι ευκρινές πέρα από κάθε αμφιβολία οτι επί του παρόντος για την ΕΕ και την ΕΠΑΑ προέχει η κάλυψη των ελλείψεων αυτών που θεωρούνται άμεσης προτεραιότητας, με τον κυβερνοπόλεμπο να μην συμπεριλαμβάνεται σε αυτές.

## Ελλάδα

> *Από αυτά βγαίνει ένας γενικός κανόνας, ο οποίος ποτέ ή σπάνια σφάλλει: εκείνος που αφήνει κάποιον να γίνει ισχυρός καταστρέφεται. Γιατί αυτή την ισχύ τη δημιουργεί αυτός είτε με την εξυπνάδα του είτε με τη δύναμή του. Και η μία και η άλλη απ' αυτές τις δύο είναι ύποπτες για κείνον που έχει γίνει ισχυρός*[224]

Σύμφωνα με τον Βασίλειο Γιαννακόπουλο[225], οι ένοπλες δυνάμεις διεξάγουν επιχειρήσεις κυβερνοπολέμου, οι οποίες ανήκουν στην κατηγορία των επιχειρήσεων πληροφοριών (Information Operations - IO) και διαρκούν συγκεκριμένη χρονική περίοδο, προκειμένου να υποστηρίξουν άλλες μορφές στρατιωτικών επιχειρήσεων. Οι επιχειρήσεις αυτές αφορούν ενέργειες οι οποίες, εκτός λίγων εξαιρέσεων, δεν αποσκοπούν στη στοχοποίηση του προσωπικού ούτε στην καταστροφή των δικτύων, αλλά προσβλέπουν:

- Στην κυβερνοάμυνα (cyber-defense), δηλαδή στην προστασία των φίλιων πληροφοριακών συστημάτων από πιθανές κυβερνοεπιθέσεις
- Στην εκμετάλλευση των πληροφοριών (cyber-exploitation) του αντίπαλου δικτύου υπολογιστών, και
- Στην κυβερνοεπίθεση (cyber-attack) κατά του εχθρικού δικτύου

Οι ελληνικές ένοπλες δυνάμεις είναι εκπαιδευμένες και θεσμικά προετοιμασμένες για ανάληψη επιχειρήσεων κυβερνοάμυνας. Σε κάθε έκφανση της συνήθους καθημερινής δραστηριότητας οι αρχές της κυβερνοάμυνας είναι εμφανείς. Άλλωστε, δεν θα μπορούσε να είναι διαφορετικά αφού όπως σε όλους τους σύγχρονους στρατούς, έτσι και στις ελληνικές ένοπλές δυνάμεις, η διείσδυση της τεχνολογίας και η εξάρτηση των επιχειρήσεων από αυτή είναι δεδομένη. Η θετική

---

[224] Νικκολό Μακιαβέλλι, *Ο Ηγεμόνας*, (Αθήνα: Κάκτος, 2006), 38.

[225] Βασίλειος Γιαννακόπουλος, *Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή*, http://www.geostrategy.gr/pdf/20110102%20 Cyberwarfare.pdf (accessed 21 December, 2015).

πλευρά της τεχνολογίας δικτύων είναι οτι απλοποιεί και επιταχύνει σημαντική τις διαδικασίες λήψης αποφάσεων από τους διοικητές, παρέχοντάς τους πληρέστερη, ακριβέστερη και πιο έγκυρη πληροφόρηση όσο ποτέ άλλοτε. Σε όλα τα επίπεδα, από το τακτικό έως και το στρατηγικό, η δικτυοκεντρική δομή έχει ως επακόλουθο τις διαδαλώδεις διασυνδέσεις υπολογιστικών και επικοινωνιακών συστημάτων με πληθώρα τρόπων. Εδώ έγκειται, όπως είναι αναμενόμενο, η ενδεχόμενα αρνητική πλευρά της τεχνολογίας αφού όλα αυτά τα συστήματα απαιτούν γνώση της λειτουργίας τους, συντήρηση αλλά το κυριότερο, προστασία.

Η προστασία αυτή είναι φυσική και λογική. Η μεν πρώτη έχει σχέση με την διαφύλαξη από ζημιά (ακούσια ή εκούσια) ενώ η λογική έχει την έννοια που οι επιχειρήσεις κυβερνοπολέμου (κυβερνοεπιθέσεις) προσπαθούν να εκμεταλλευτούν. Οποιασδήποτε μορφής υπολογιστικό δίκτυο, συμπεριλαμβανομένου του διαδικτύου, γίνεται αγωγός ροής στρατιωτικών δεδομένων αποτελεί εξ' ορισμού ευάλωτο σημείο που πρέπει να προστατευθεί. Οι φίλιες αμυντικές επιχειρήσεις (κυβερνοάμυνα) έχουν ακριβώς αυτόν το σκοπό.

Στο σχετικό ελληνικό δόγμα, πράγματι αναλύονται ο ρόλος, ο τρόπος, τα μέσα και οι διαδικασίες τόσο των Αμυντικών Επιχειρήσεων Δικτύων Η/Υ όσο και των Επιθετικών Επιχειρήσεων Δικτύων Η/Υ. Επίσης, παρέχεται το σχετικό γνωστικό υπόβαθρο σχετικά με το εύρος των αναμενόμεων απειλών των φίλιων δικτύων Η/Υ, την προέλευσή τους, το αναμενόμενο επίπεδο έντασής τους και άλλες σχετικές πληροφορίες με σκοπό την απόκτηση σφαιρικότερης αντίληψης του συνόλου των κινδύνων και των ιδιαιτεροτήτων των συγκεκριμένων απειλών.

Λόγω της ευαισθησίας που έχει το θέμα του κυβερνοπολέμου και των προβλημάτων από πλευράς διεθνούς νομιμότητας όπως ήδη καλύφθηκε εκτενώς, ως κύριο όργανο αρμόδιο για τη λήψη αποφάσεων που οδηγούν στη διαμόρφωση και άσκηση της πολιτικής εθνικής άμυνας είναι το ΚΥΣΕΑ.

Τέλος, αξίζει να αναφερθεί οτι αναπόσπαστο μέρος της εγρήγορσης των ενόπλων δυνάμεων αλλά και με σκοπο την πληρέστερη εκπαίδευση των στελεχών, πραγματοποιούνται συχνά τόσο ασκήσεις κυβερνοπολέμου (αποκλειστικού ή μικτού χαρακτήρα) και προσομοιώσεις με σκοπό να αναδειχθούν οι ευπάθειες των συστημάτων. Ως συστήματα, από πλευράς εντοπισμού ευπαθών σημείων, λογίζεται τόσο το υλικό με τα δίκτυα που το εξυπηρετούν, όσο και το προσωπικό αλλά και οι θεσπισμένες διαδικασίες χρησιμοποίησης των υπολογιστικών συστημάτων. Συνήθως είναι ευκολότερο να εντοπιστούν και να διορθωθούν ανεπάρκειες στο υλικό σε σχέση με τις ευπάθειες που παρουσιάζουν τόσο οι διαδικασίες όσο και οι χρήστες των συστημάτων, δηλαδή οι άνθρωποι. Σε αυτό το σημείο, εστιάζει και η διαρκής εκπαίδευση αλλά και η διερεύνηση των τρωτοτήτων, τόσο μέσω των ασκήσεων όσο και μέσω των προσομοιώσεων. Ευτυχώς για τις ελληνικές ένοπλες δυνάμεις, αυτές οι δράσεις είναι εδραιωμένες θεσμικά. Ωστόσο, το οτι υπάρχουν διαδικασίες και τρόποι εντοπισμού των ευπαθειών πριν αυτές γίνουν αντικείμενο εκμετάλλευσης από την αντίπαλη πλευρά δεν σημαίνει οτι αυτόματα και άμεσα οι ευπάθειες εντοπίζονται και διορθώνονται. Έτσι, οι βασικές αρχές κυβερνοάμυνας είναι πάντα απαραίτητες όχι μόνο σε επίπεδο σχεδίασης των υπολογιστικών και επικοινωνιακών στρατιωτικών συστημάτων αλλά απαιτείται η πλήρης γνώση τους από το προσωπικό όλων των επιπέδων, ως το σημείο του χρήστη σε κατώτερο επίπεδο. Το ΓΕΕΘΑ έχοντας εντοπίσει αυτήν την αναγκαιότητα της διαρκούς επιμόρφωσης και εκπαίδευσης, έχει καταρτίσει προγράμματα για το σύνολο των εμπλεκομένων με τα συστήματα αυτά

και, στο μέτρο του εφικτού, παρέχει στοχευμένη εκπαίδευση για όλες τις περιπτώσεις.

Εάν και το μέγεθος των ελληνικών ενόπλων δυνάμεων δεν είναι συγκρίσιμο με των στρατών των μεγάλων κρατών των ιδιαίτερα ανεπτυγμένων χωρών, φαίνεται καθαρά οτι σε επίπεδο κυβερνοπολέμου η οργάνωση αλλά και η αντίληψη της ίδιας της αναγκαιότητας απόκτησης σοβαρών ικανοτήτων δεν υπολείπεται διόλου της σύγχρονης πραγματικότητας.

# 6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από την εμφάνιση του διαδικτύου και μέχρι σήμερα εμφανίστηκαν πολλοί όροι σε μια προσπάθεια να αποδωθούν οι έννοιες που ήταν συνακόλουθες των νέων τεχνολογιών και οι οποίες εμφανίζονταν με καταιγιστικό ρυθμό. Κυβερνοχώρος, κυβερνοάμυνα, κυβερνοεκβιασμός και πολλές άλλες που αν και ακούγονται παρόμοιες, αναφέρονται σε διαφορετικές έννοιες. Η κατάσταση αυτή ίσως να μην δημιουργεί προβλήματα σε εργασιακούς χώρους όπου η έννοια της κάθε λέξης μπορεί να μην είναι μονοσήμαντα ορισμένη. Ωστόσο, μιλώντας για διαφορά μεταξύ κυβερνοεγκλήματος, κυβερνοτρομοκρατίας και πολύ περισσότερο κυβερνοπολέμου, η κατάσταση είναι διαφορετική. Το κυβερνοέγκλημα ορίζεται ως χρήση της τεχνολογίας των υπολογιστών με σκοπό την εμπλοκή τους σε δραστηριότητες οι οποίες υποδαυλίζουν την ικανότητα της κοινωνίας να διατηρήσει την εσωτερική τάξη. Κάτι αντίστοιχο ισχύει για την κυβερνοτρομοκρατία, η οποία επίσης στοχεύει στην υποδαύλιση της διατήρησης της εσωτερικής τάξης, απλώς για λίγο διαφορετικούς λόγους από την περίπτωση του κυβερνοεγκλήματος. Έτσι, με αυτήν την εννοιολογική απόδοση, αυτόματα το κυβερνοέγκλημα και η κυβερνοτρομοκρατία, ως απειλές της εσωτερικής τάξης, διαφοροποιούνται ουσιαστικά από την τρίτη κομβική έννοια, τον κυβερνοπόλεμο.

Κυβερνοπόλεμος είναι η πραγματοποίηση στρατιωτικών επιχειρήσεων με εικονικά μέσα. Συνίσταται στη χρήση του κυβερνοχώρου από τα κράτη ώστε αυτά να επιτύχουν το ίδιο αποτέλεσμα που επιδιώκουν μέσω της χρήσης συμβατικών στρατιωτικών δυνάμεων: να αποκτήσουν πλεονέκτημα έναντι των ανταγωνιστικών κρατών ή να αποτρέψουν τα εχθρικά κράτη να αποκτήσουν πλεονέκτημα έναντι αυτών των ιδίων. Εδώ, το βασικό σημείο διαφοροποίησης σε σχέση με τις προηγούμενεςν έννοιες είναι οτι αυτό που βρίσκεται σε κίνδυνο δεν είναι η εσωτερική τάξη, αλλά η εξωτερική. Έτσι, τα κράτη έχουν να αντιμετωπίσουν απειλές που στρέφονται κατά των εθνικών συμφερόντων και που εκφράζονται ή προέρχονται από άλλα κράτη. Το τελευταίο, ωστόσο, δεν είναι απόλυτο αφού στον κυβερνοπόλεμο εκτός από κράτη υπάρχουν και άλλες οντότητες, μη-κρατικές, με δυνατότητες κυβερνοπολέμου.

Ενώ στον πραγματικό κόσμο μπορεί να υπάρχει κάποια αβεβαιότητα για το εάν κάποιο γεγονός είναι έγκλημα ή τρομοκρατία, αυτό στην πράξη έχει μικρή σημασία αφού και τα δύο είναι απειλές της εσωτερικής τάξης και η αντίδραση της κοινωνίας είναι παρόμοια. Αντίθετα, η μονοπωλιακή αντίληψη του εδάφους αλλά και του δικαιώματος χρήσης στρατιωτικής βίας από το κράτος και μόνο από αυτό, σημαίνει οτι στον πραγματικό κόσμο δεν θα είμαστε ποτέ αντιμέτωποι με την αβεβαιότητα του εάν αυτό που συμβαίνει είναι απειλή της εσωτερικής τάξης (έγκλημα, τρομοκρατία) ή απειλή της εξωτερικής τάξης και της κρατικής κυριαρχίας (πόλεμος). Στον πραγματικό κόσμο, μόνο τα κράτη κάνουν πολέμους, τουλάχιστον με την μορφή που έχει ο συμβατικός πόλεμος. Κατά συνέπεια, η ξεκάθαρη διαφοροποίηση αυτών των δύο καταστάσεων οδηγεί απροβλημάτιστα στην επιλογή της αντίδρασης και του φορέα που θα την υλοποιήσει (εσωτερική απειλή->αστυνομικές δυνάμεις, εξωτερική απειλή-> ένοπλες δυνάμεις). Εάν και με τις περιπτώσεις των ασύμμετρων απειλών αυτό δεν είναι απόλυτο, ωστόσο παραμένει ο κανόνας.

Η δυϊκή αυτή αντιστοίχιση παύει να είναι τόσο ευκρινής και συχνά καταργείται στην πράξη στον κυβερνοχώρο. Η απόκτηση από τους μη-κρατικούς δρώντες

δυνατότητας κυβερνοπολέμου, καταργεί την διαχωριστική γραμμή μεταξύ απειλής της εσωτερικής και της εξωτερικής τάξης και θολώνει το τοπίο αφού αντί κρατών, στο προσκήνιο βρίσκονται οντότητες οι οποίες συχνά στερούνται διεθνούς νομικής προσωπικότητας. Από την οπτική των διεθνών σχέσεων, τα στεγανά του κράτους πάυουν να είναι αδιαπέραστα σε σημείο που να μπορούμε να ισχυριστούμε οτι ο κυβερνοπόλεμος απειλεί τα θεμέλια του οικοδομήματος της έννοιας του κράτους, όπως ισχύει από την Συνθήκη της Βεστφαλίας και έπειτα.

Εκτός από τον κυβερνοπόλεμο που αλλάζει τις ισορροπίες ακόμη και σε επίπεδο κατανόησης περί του τι συμβαίνει, όπως στην περίπτωση της κυβερνοεπίθεσης στην Εσθονία, αναδεικνύεται και η έννοια του υβριδικού πολέμου. Έτσι, στους υβριδικούς πολέμους χρησιμοποιούνται διάφορα όπλα χωρίς απαραίτητα αυτά να διαθέτουν δύναμη πυρός με την κυριολεκτική σημασία. Για παράδειγμα, όπως αναφέρθηκε χαρακτηριστικά, με μια κάμερα σε κάθε κινητό και με την εξάπλωση των μέσων κοινωνικής δικτύωσης, ο ανταγωνισμός της πληροφορίας έχει αναδειχθεί σε κρίσιμη πλευρά του σύγχρονου πολέμου. Έτσι, συμβατικές και μη συμβατικές δυνάμεις, στρατιώτες και άμαχοι, καταστροφές και χειρισμός της πληροφορίας μπλέκονται μεταξύ τους. Η πιο πρόσφατη περίπτωση υβριδικού πολέμου θεωρείται ο πόλεμος στην Κριμαία, τον Φεβρουάριο του 2014. Εκεί, χρησιμοποιήθηκε ένα μίγμα από διπλωματικό αγώνα, δραστηριότητα σε επίπεδο διεθνούς δικαίου (lawfare), επιχειρήσεις κυβερνοπολέμου, οικονομικός πόλεμος, ψυχολογικές επιχειρήσεις, κινητοποίηση των αμάχων εντός της χώρας αλλά και χρήση ενόπλων τμημάτων χωρίς κανείς να μπορεί να πει από ποιές ένοπλες δυνάμεις προέρχονται. Αυτή είναι η νέα μορφή των πολεμικών συγκρούσεων που αναμένεται να κυριαρχήσει στον πλανήτη το επόμενο χρονικό διάστημα.

Μια άλλη παραλλαγή είναι ο λεγόμενος απεριόριστος πόλεμος, κάτι που ακόμη και σε ακαδημαϊκό επίπεδο είναι πολύ πρόσφατο αφού μόλις το 1999 εμφανίστηκε ως μελέτη στην Κίνα. Το ανησυχητικότερο πίσω από την ιδέα του πολέμου αυτού είναι η διακήρυξη οτι ο απεριόριστος πόλεμος υπακούει μόνο (ή κυρίως) στον κανόνα που λέει οτι δεν υπάρχουν κανόνες. Εκτός από ξεκάθαρη διάρρηξη των βασικών ηθικών αναχωμάτων, τίθεται και το ζήτημα της διεθνούς νομιμότητας αφού οι κανόνες του διεθνούς δικαίου των ενόπλων συγκρούσεων είναι το παγκόσμια αποδεκτό πλαίσιο συμπεριφοράς σε τέτοιες περιπτώσεις. Αν και προς το παρόν δεν μπορεί να αναφερθεί καμμιά περίπτωση σύγκρουσης που να παρατηρήθηκαν δράσεις οδηγούμενες από την ιδέα του απεριόριστου πολέμου, το γεγονός της αυξανόμενης έλξης που ασκεί η στρατηγική αυτή είναι σημείο ανησυχίας. Ομώς δεν είναι μόνο ο απεριόριστος πόλεμος που αντιμετωπίζει προβλήματα από την οπτική του διεθνούς δικαίου.

Επιστρέφοντας στον κυβερνοπόλεμο, τα δύο σημεία που υπάρχει σοβαρό ζήτημα σε σχέση με το διεθνές δίκαιο σχετίζονται με την αρχή της ουδετερότητας και την αρχή της διάκρισης. Το διεθνές ανθρωπιστικό δίκαιο ξεκαθαρίζει οτι η επίθεση εναντίον οποιουδήποτε στόχου απαγορεύεται. Η κινητήρια ιδέα πίσω από αυτή την αρχή είναι, ασφαλώς, η προστασία των αμάχων. Έτσι, τα εμπόλεμα μέρη υποχρεούνται να διακρίνουν ανάμεσα σε στρατιωτικούς και μη-στρατιωτικούς στόχους, με τους δεύτερους να ανήκουν στην περιοχή της απόλυτης απαγόρευσης στοχοποίησης. Αντίθετα, σε ότι έχει να κάνει με τους στρατιωτικούς στόχους, από πλευράς διεθνούς ανθρωπιστικού δικαίου πράγματι, όλοι αυτοί είναι έγκυροι και νόμιμοι στόχοι για τους εμπόλεμους. Αξίζει να σημειωθεί οτι η αρχή της διάκρισης

γίνεται αποδεκτή ως κανόνας εθιμικού δικαίου, δεσμεύοντας έτσι το σύνολο της διεθνούς κοινωνίας. Ο θεσμός της ουδετερότητας προβλέπει τα δικαιώματα και τις υποχρεώσεις εκείνων των κρατών που παραμένουν ουδέτερα κατά τη διάρκεια μια σύρραξης. Η ουδετερότητα μεταξύ άλλων προβλέπει για τους εμπόλεμους να μην προβαίνουν σε ενέργειες που θα μπορούσαν να εμπλέξουν το ουδέτερο κράτος στην μεταξύ τους διαμάχη ενώ για το ίδιο το ουδέτερο κράτος υπάρχει μια σειρά υποχρεώσεων που πρέπει να τις τηρεί, εφόσον επιθυμεί τη διατήρηση του status του ουδέτερου κράτους. Όπως είδαμε, ο κυβερνοπόλεμος αποτελεί εξαιρετική περίπτωση πρόκλησης και παραβίασης των δύο αυτών αρχών.

Στην περίπτωση του κυβερνοπολέμου και της αρχής της διάκρισης, κατά την επιλογή των κυβερνοστόχων έχει εφαρμογή η ίδια συλλογιστική με τους στόχους του συμβατικού πολέμου. Κάθε στόχος που πληροί τις προϋποθέσεις της αρχής της διάκρισης για χρήση συμβατικών όπλων αυτόματα συμμορφώνεται με την ίδια αρχή για επίθεση με κυβερνοόπλα. Έτσι, οι περιορισμοί του διεθνούς ανθρωπιστικού δικαίου δυν συναρτώνται με το είδος του όπλου που θα χρησιμοποιηθεί αλλά μόνο με τον στόχο. Κατά συνέπεια, ορισμένες περιπτώσεις χρήσης κυβερνοόπλων είναι αποδεκτές από την αρχή της διάκρισης ενώ κάποιες άλλες όχι. Στο ένα άκρο είναι οι ξεκάθαρα στρατιωτικοί στόχοι, οι οποίοι μπορούν να προσβληθούν τόσο με συμβατικά όσο και με κυβερνοόπλα. Στο άλλο άκρο είναι οι στόχοι που η προσβολή τους θα έχει ως αποτέλεσμα την άμεση και ηθελημένη πρόκληση θανάτου σε αμάχους και έτσι μιλάμε για απαγορευμένους στόχους. Έτσι, σύμφωνα με την αρχή της διάκρισης, είτε στην μία είτε στην άλλη περίπτωση η ερμηνεία της αρχής είναι ξεκάθαρη. Ωστόσο, γιο όλες τις ενδιάμεσες περιπτώσεις η αρχή της διάκρισης δεν δίνει ξεκάθαρα αποτελέσματα και, δυστυχώς, η πλειονότητα των κυβερνοστόχων εντάσσεται σε αυτήν την ενδιάμεση, γκρίζα περιοχή. Ο λόγος είναι η δομή του διαδικτύου η οποία δεν επιτρέπει εξασφάλιση οτι κατά την εξαπόλυση επίθεσης εναντίον ενός κυβερνοστόχου θα πληγούν μόνο στρατιωτικά δίκτυα, ειδικά εάν αναφερόμαστε στην περίπτωση των στόχων διπλής χρήσης. Έτσι, ή θα αποφασιστεί να τηρηθεί η αρχή της διάκρισης και οι κυβερνοστόχοι αυτοί να απορριφθούν, ή θα πληγούν, παραβιάζοντας την αρχή της διάκρισης. Εάν και αυτή η απόφαση συχνά υπακούει στην στρατιωτική αναγκαιότητα η οποία μπορεί να οδηγήσει στην παραβίαση της αρχής της διάκρισης, εάν συγκριθεί η κυβερνοεπίθεση με την επίθεση με συμβατικά όπλα εναντίον του ίδιου στόχου, φαίνεται η υπεροχή του κυβερνοπολέμου από το ενδεχόμενο αποτέλεσμα: ο κυβερνοπόλεμος ως λιγότερο θανατηφόρα αλλά εξίσου αποτελεσματική λύση συχνά αποτελεί λύση στην προσβολή στόχων διπλής χρήσης, παραβιάζοντας την αρχή της διάκρισης αλλά αποφεύγοντας τις απώλειες αμάχων ενώ ταυτόχρονα υλοποιείται η στρατιωτική αναγκαιότητα καταστροφής του εν λόγω στόχου. Έτσι, έχουμε το παράδοξο να πετυχαίνουμε τον σκοπό μας παραβιάζοντας την αρχή της διάκρισης με τρόπο που να εξασφαλίζει οτι θα πληρούνται οι προϋποθέσεις που οδήγησαν στην καθιέρωση της αρχής της διάκρισης: της αποφυγής απωλειών αμάχων. Τελικά, λαμβάνοντας υπόψη αυτούς τους προβληματισμούς δεν θα ήταν περίεργο στο μέλλον να έχουμε συχνότερες παραβιάσεις της αρχής της διάκρισης, με τη μορφή που είναι διατυπωμένη στο διεθνές δίκαιο σήμερα, χωρίς ωστόσο να έχουμε αύξηση των απωλειών αμάχων, και αυτό χάρη στον κυβερνοπόλεμο.

Από το 1815 η αρχή της ουδετερότητας ρυθμίζει την συνύπαρξη του πολέμου και της ειρήνης αφού επιτρέπει σε ουδέτερα κράτη να συνεχίζουν να έχουν σχέσεις με

τα εμπόλεμα. Η επικράτεια ενός ουδέτερου κράτους είναι απαραβίαστη. Οι εμπόλεμοι δεν μπορούν να μεταφέρουν στρατεύματα, όπλα ή άλλο πολεμικό υλικό μέσω της επικράτειας του ουδέτερου κράτους. Τα ουδέτερα κράτη οφείλουν να εμποδίζουν τους εμπόλεμους να παραβιάζουν την ουδετερότητά τους, κάνοντας κάτι από τα παραπάνω. Στον κυβερνοπόλεμο, όμως, είναι πρακτικά αδύνατο για το εμπόλεμο κράτος να γνωρίζει τη διαδρομή που θα ακολουθήσει το κακόβουλο λογισμικό το οποίο είναι το κυβερνοόπλο. Έτσι, η χρήση του διαδικτύου για κυβερνοπόλεμο παραβιάζει την αρχή της ουδετερότητας όλων εκείνων των κρατών από την επικράτεια των οποίων θα διέλθει το κυβερνοόπλο. Οι όποιες ενστάσεις που θεωρούν οτι δεν πρόκειται για παραβίαση εδάφους ούτε για διακίνηση όπλων διαμέσου των ουδέτερων χωρών έχουν καταρριφθεί αφού το κακόβουλο λογισμικό που οδεύει μέσα από την τηλεπικοινωνιακή δικτυακή υποδομή όλων των κρατών, από την στιγμή της εξαπόλυσής του ως τη στιγμή που θα πλήξει το υπολογιστικό σύστημα-στόχο σαφώς και είναι όπλο ενώ, οι κόμβοι των υποδομών διαμέσου των οποίων δρομολογείται το λογισμικό αυτό είναι, πέρα από κάθε αμφιβολία, μέσα στην περιοχή της απόλυτης κυριαρχίας αυτών των κρατών, μεταξύ των οποίων και πολλά ουδέτερα. Υπάρχει και ένα δεύτερο πρόβλημα στην αρχή της ουδετερότητας κατά τον κυβερνοπόλεμο, από την οπτική της απώλειας της ουδετερότητας των κρατών. Σύμφωνα με τις υποχρεώσεις της συνθήκης, τα ουδέτερα κράτη οφείλουν να εμποδίσουν την μεταφορά στρατευμάτων, όπλων (άρα και κυβερνοόπλων) από το έδαφός τους, κάτι που τεχνικά είναι σχεδόν αδύνατο να πραγματοποιηθεί. Έτσι, ενδέχεται ουδέτερο κράτος οι διαδικτυακοί κόμβοι του οποίου να χρησιμοποιήθηκαν ως μέρος της διαδρομής του κυβερνοόπλου από το επιτιθέμενο κράτος στο έτερο εμπόλεμο κράτος που δέχεται την επίθεση να χάσει το status της ουδετερότητας και σε ακραία περίπτωση να δεχθεί την ένοπλη απάντηση από το εμπόλεμο κράτος που υπέστη την κυβερνοεπίθεση. Τουλάχιστον για να καλυφθεί η περίπτωση όλων εκείνων των κρατών που από άγνοιά τους η επικράτειά τους γίνεται πεδίο διακίνησης κυβερνοόπλων, θα πρέπει να εξετάζεται με χαλαρότερα κριτήρια η αρχή της ουδετερότητας, λαμβάνοντας υπόψη όλα τα δεδομένα προτού αποφανθεί η διεθνής κοινότητα εάν πράγματι το ουδέτερο κράτος είχε ή όχι τη δυνατότητα να αντιληφθεί και να εμποδίσει την διακίνηση αυτή. Όπως και με την παραβίαση της αρχής της διάκρισης, έτσι και στην περίπτωση της αρχής της ουδετερότητας αναμένεται να αυξηθούν οι παραβιάσεις της αφού ο κυβερνοπόλεμος είναι φθηνότερη και πλέον αναίμακτη επιλογή συγκρινόμενος με οποιαδήποτε άλλη συμβατική μορφή πολέμου. Αυτή η διαπίστωση, σε συνδυασμό με την αδυναμία ουσιαστικής δυνατότητας απόδοσης ευθύνης στους εξαπολύοντες κυβερνοεπιθέσεις αναμένεται να οδηγήσει ολοένα και περισσότερα κράτη στην επιλογή του.

Ούτως ή άλλως, όπως είδαμε ο αριθμός των κρατών με δυνατότητες κυβερνοπολέμου είναι ήδη μεγάλος και αυξάνεται, όπως αυξάνονται και οι δυνατότητες και βελτιώνονται και τα μέσα που είναι διαθέσιμα. Νέες στρατηγικές αναπτύσσονται, δοκιμάζονται και τροποποιούνται αλλά και νέες οντότητες, όπως οι μη κρατικοί δρώντες εμφανίζονται να διεκδικούν μερίδιο στην αρένα του κυβερνοπολέμου. Ειδικά οι μη κρατικοί δρώντες, λόγω της ασαφούς διεθνούς τους υπόστασης και λόγω των γκρίζων περιοχών του κυβερνοπολέμου στο πεδίο του διεθνούς δικαίου, αποτελούν την πρόκληση των επόμενων ετών αφού ενώ οι ίδιοι τους έχουν την πολυτέλεια να δρουν σχεδόν χωρίς νομικούς περιορισμούς, τα κράτη που δέχονται τις κυβερνοεπιθέσεις τους (ορθά) περιορίζονται από τους κανόνες του

υφιστάμενου διεθνούς δικαίου. Αυτή η ετεροβαρής αντιμετώπιση δημιουργεί ένα δεύτερο επίπεδο ασυμμετρίας το οποίο περιπλέκει την κατάσταση.

Στον αγώνα του κυβερνοχώρου παρατηρούνται κινήσεις ομαδοποίησης κρατών με σκοπό την πληρέστερη αμυντική τους θωράκιση, κάτι που εκφράζεται με διακρατικές ή πολυμερείς αμυντικές συμφωνίας γενικού ή ειδικού σκοπού. Πατροπαράδοτες αμυντικές συμμαχίες, όπως το ΝΑΤΟ, έχουν ανάγει την κυβερνοάμυνα σε κομβικής σημασίας δράση τους, κάτι που φαίνεται από την καθημερινή πρακτική αλλά και από τις δομικές τροποποιήσεις που επέρχονται συχνά με σκοπό να θωρακισθεί θεσμικά η νέα αλλά πλήρως αναγκαία δυνατότητα, της κυβερνοάμυνας. Στον αντίποδα, στην ευρωπαϊκή γειτονιά η ΕΕ πορευόμενη επί μακρόν σε μια εξαιρετικά αργή διαδρομή ευρύτερης ολοκλήρωσης αν και αντιλαμβάνεται τις νέες τεχνολογίες τόσο ως εργαλείο όσο και ως επικίνδυνο όπλο στα λάθος χέρια, δεν έχει πράξει κάτι ουσιαστικό προς την κατεύθυνση της κυβερνοάμυνας. Άλλωστε, και στον χώρο της συμβατικής άμυνας η ΕΕ στερούμενη αυτόνομου και ικανού ευρωστρατού αντιπροσωπεύει μια οντότητα που έχει σοβαρότερα προβλήματα να αντιμετωπίσει από τον κυβερνοπόλεμο. Οι ελληνικές ένοπλες δυνάμεις, έχοντας παραμείνει προσδεδεμένες στην αλματώδη τεχνολογική πρόοδο και ακολουθώντας τα πρότυπα άλλων στρατών, έχουν οχυρωθεί επαρκώς στον πεδίο του κυβερνοχώρου. Αυτό από μόνο του δεν είναι αρκετό αφού όσο η τεχνολογία προοδεύει τόσο πρέπει να αυξάνει η επαγρύπνηση και η προετοιμασία για αντιμετώπιση κυβερνοεπιθέσεων είτε ως αυτόνομα περιστατικά είτε ως πρόδρομα βήματα μιας ευρύτερης επίθεσης. Ο ανθρώπινος παράγοντας, μαζί με τη διασφάλιση των δικτύων και την φυσική προστασία είναι τομείς αυξημένης προσοχής που δεν πρέπει να παραμελούνται ποτέ.

Το διεθνές δίκαιο διαχρονικά έχει επιδείξει την μακροζωία του και την προσαρμοστικότητά του στο διαρκώς εξελισσόμενο πεδίο των εμπόλεμων συγκρούσεων δείχνοντας με αυτόν τον τρόπο οτι ήρθε για να μείνει. Άλλωστε, ο αριθμός και μόνο των τροποποιήσεων του δικαίου της Χάγης δείχνει οτι όταν το ίδιο το δίκαιο, ως ανεπίσημος εκφραστής του κοινώς αποδεκτού "ορθού" τρόπου πολέμου αισθανθεί οτι μένει πίσω από τις εξελίξεις ανανεώνεται ανακάμπτοντας σταδιακά. Έτσι, για παράδειγμα συναντάμε στη Σύμβαση του Δουβλίνου το 2008 τις ρυθμίσεις εκείνες για την απαγόρευση των υποπυρομαχικών διασποράς τα οποία έκαναν της εμφάνισή τους πολλές δεκαετίες νωρίτερα. Μπορεί να χρειάστηκε σημαντικός χρόνος για να απαγορευτούν τα υποπυρομαχικά διασποράς, ωστόσο τελικά αυτό έγινε. Χωρίς να εμπεριέχεται ίχνος προφητικής διάθεσης, δεν θα ήταν παράλογο να ισχυριστεί κανείς οτι κάτι αντίστοιχο θα συμβεί και με το θέμα του κυβερνοπολέμου. Βήματα προετοιμασίας υπό τη μορφή soft law σαφώς και έχουν ήδη γίνει προς αυτήν την κατεύθυνση. Είναι ίσως πολύ νωρίς να απαιτούμε από το διεθνές δικαίο να λύσει τα νομικά προβλήματα στον τομέα του κυβερνοπολέμου τη στιγμή που η παγκόσμια κοινότητα δεν έχει ακόμη αποκρυσταλλωμένη άποψη για το τι είναι αλλά κυρίως τι δεν είναι ο κυβερνοπόλεμος.

# 7. ΑΝΤΙ ΕΠΙΛΟΓΟΥ

Η αλματώδης πρόοδος της τεχνολογίας όπως πολλές φορές ήδη αναφέρθηκε αποτελεί αναμφίβολα μεγάλη ευκαιρία για τις ανά τον κόσμο ένοπλες δυνάμεις να βελτιώνουν τη μαχητική τους ισχύ και να αυξάνουν της αποτελεσματικότητά τους. Συχνά, αφού αυτοί οι δύο στόχοι επιτευχθούν, η τεχνολογία βοηθάει και σε άλλους τομείς όπως εξοικονόμηση πόρων, βελτιστοποίηση τακτικών και διαδικασιών μη παραλείποντας να αναφέρουμε την μειώση του ρίσκου για απώλειες ανθρώπινου δυναμικού ή υλικού. Η αυτοματοποίηση, η δικτύωση και η μηχανογράφηση των στρατών σε όλο τον κόσμο επέφερε σημαντική εξοικονόμηση πόρων και προσέδωσε νέες δυνατότητες στους μαχητές που λίγα χρόνια πριν ήταν στην σφαίρα της φαντασίας. Τεχνολογίες όπως LASER, ηλεκτροπτικές εφαρμογές, μη επανδρωμένα αεροχήματα και δορυφορικές επικοινωνίες είναι μερικοί μόνο τομείς των βημάτων προόδου στην στρατιωτική τεχνολογία. Το ίδιο το διαδίκτυο (Intenet) δημιουργήθηκε στα εργαστήρια της DARPA ως απόλυτα στρατιωτική εφαρμογή (ARPAnet). Το σύστημα NAVSTAR που είναι το συνολικό σύστημα πίσω από το Παγκόσμιο Δορυφορικό Σύστημα Εντοπισμού Θέσης (GPS) που όλοι σχεδόν στον κόσμο απολαμβάνουν σήμερα είναι επίσης στρατιωτική εφαρμογή. Ποιός μπορούσε να φανταστεί πριν από 25 χρόνια οτι θα μπορεί να εκτελεί με το μαχητικό αεροσκάφος του χαμηλή ναυτιλία τη νύχτα μέσα σε εχθρικό έδαφος και τελικά θα εντοπίζει τον στόχο με ακρίβεια μέτρων; Έτσι, στην προ GPS εποχή αναπτύχθηκαν τρόποι και μέθοδοι λιγότερο εξαρτώμενες από την τεχνολογία της εποχής εκείνης που απαιτούσαν από τον άνθρωπο πολύπλευρες ικανότητες για να φέρει σε πέρας την αποστολή του. Δεν απέχει πολύ να πούμε οτι η ικανότητα να φέρει σε πέρας ο άνθρωπος μια πεπλεγμένη αποστολή είναι τόσο επιστήμη όσο και τέχνη και αυτό ισχύει γενικά για οποιαδήποτε διαδικασία πραγματοποιεί ο άνθρωπος. Το διαδίκτυο, τα συστήματα υπολογιστών και οι δορυφορικές επικοινωνίες έφεραν στον χώρο των ενόπλων δυνάμεων τόσες πολλές και τόσο σαρωτικές αλλαγές που μπορούμε να χρησιμοποιήσουμε τον όρο επανάσταση. Επανάσταση στον τρόπο που εκτελούμε τις επιχειρήσεις, επανάσταση στον τρόπο που αποκτούμε και εκμεταλλευόμαστε την πληροφορία και επανάσταση στον τρόπο που εκπαιδευόμαστε. Μόνο που στη σκιά της επανάστασης αυτής αρχίσαμε να χάνουμε σιγά σιγά την τέχνη της περισσότερο μηχανικής επίλυσης των προβλημάτων. Αυτό δεν είναι κατά ανάγκη μεμπτό, ωστόσο αποτελεί πεποίθηση του γράφοντα οτι πλησιάζουμε, ως κοινωνία και ως ένοπλες δυνάμεις, να είμαστε πλήρως εξαρτημένοι από τα δίκτυα υπολογιστών, τους δορυφόρους, το διαδίκτυο και τις δορυφορικές επικοινωνίες που στο απομακρυσμένο σενάριο να κληθούμε να επιχειρήσουμε ξαφνικά χωρίς αυτές τις δυνατότητες (είτε λόγω βλάβης των υποσυστημάτων τους είτε λόγω αποστέρησης των υπηρεσιών τους σε εμάς ως αποτέλεσμα εχθρικής ενέργειας) οι σκέψεις αποκτούν σκούρα απόχρωση. Με άλλα λόγια, μήπως ήρθε η ώρα να ξανααποκτήσουμε (έστω, ως εναλλακτική πρόταση) την χαμένη τέχνη της μη-αυτόματης επεξεργασίας ;

## 8. ΒΙΒΛΙΟΓΡΑΦΙΑ


Κολιόπουλος, Κωνσταντίνος. 2011. *Η Υψηλή Στρατηγική της Αρχαίας Σπάρτης (750-192 π.Χ.).* Βάρη, Αττική: Ποιότητα.

Κολοβός, Αλέξανδρος. 2003. *Διάστημα και εθνική ασφάλεια. Πολιτικές και στρατηγικές διαστάσεις.* Βάρη, Αττική: Ποιότητα.

Τσόμσκι, Νόαμ, and Αντρέ Βλιτσέκ. 2014. *Η Τρομοκρατία της Δύσης.* Αθήνα, Μακεδονία: Εκδόσεις Ψυχογιός.

Θουκυδίδης. 2011. *Ιστορία.* Edited by Ευτυχία Παναγιώτου. Translated by N. Μ. Σκουτερόπουλος. Αθήνα, Αττική: ΠΟΛΙΣ.

Ευθυμιόπουλος, Μάριος-Παναγιώτης. 2008. *Το ΝΑΤΟ στον 21° Αιώνα: Η ανάγκη για ένα νέο στρατηγικό πλάνο και η διεύρυνση των σχέσεων ΝΑΤΟ-Ρωσίας.* Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Βοσκόπουλος, Γιώργος. 2009. *Η Οικοδόμηση της Ευρώπης: Ειρήνη-Συμφιλίωση-Συνεργασία-Ολοκλήρωση.* Βάρη, Αττική: Ποιότητα.

Anderson, Jan Joel, and Thierry Tardy. 2015. "Hybrid: what's in a name ?" *Brief Issue*, October.

Arquilla, John, and David Ronfeldt. 1993. "Cyberwar is Coming !" *Comparative Strategy* (Taylor & Francis Inc.) 12 (2): 141-165.

Assange, Julian. 2012. *Cypherpunks: Η Ελευθερία και το Μέλλον του Διαδικτύου.* Αθήνα: Εκδόσεις Ποιότητα.

Au, Alex. 2011. "Singapore: Closing the Next Deal." *World Policy Journal* (World Policy Institute) 28 (3): 28-31.

Baldwin, David A. 1995. "Security Studies and the End of the Cold War." *World Politics* 48 (1): 117-141.

Bale, Jeffrey M. 2006. "Deciphering Islamism and Terrorism: Review Article." *Middle East Journal* (Middle East Institute) 60 (4): 777-788.

Biro, Gaspar. 2013. "Ηθική και Διεθνείς Σχέσεις." *Inetrnational Relations Quarterly* 4 (1).

Booth, Wayne C., G. Gregory Colomb, and M. Joseph Williams. 2003. *The Craft of Research.* Chicago, Illinois: The University of Chicago Press.

Brenner, Susan W. 2007. ""At Speed Light": Attribution and Response to Cybercrime/Terrorism/Warfare." *The Journal of Criminal Law and Criminology* (Northwestern University School of Law) 97 (2): 379-475. http://www.jstor.org/stable/40042831.

—. 2005. "Why the Law Enforcement Model Is a Problematic Strategy for Dealing with Terrorist Activity Online." *Proceedings of the Annual Meeting.* American Society of International Law. 108-111.

Burke, Garance, and Jonathan Fahey. 2015. "AP Investigation: US Power Grid Vulnerable to Foreign Hacks." *ABC News.* December 21. Accessed December 22, 2015. http://abcnews.go.com/US/wireStory/ap-investigation-us-power-grid-vulnerable-foreign-hacks-35882487.

Carter, Stephen. 1998. *Civility: Manners, Morals, and the Etiquette of Democracy.* New York, New York: Basic Books.

Clark, Wesley K., and Peter L. Levin. 2009. "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs* (Council on Foreign Affairs) 88 (6): 2-6, 8-10.

Clarke, Richard, interview by Eleanor Hall. 2010. "Former White House security advisor warns of cyber war." *The World Today with Eleanor Hall.* (December 7).

Clausewitz, Carl Von. 1999. *Περί του Πολέμου.* Edited by Νατάσα Ξεπούλια. Translated by Νατάσα Ξεπούλια. Αθήνα, Αττική: Εκδόσεις Βάνιας.

Computer Science and Telecommunications Board, National Research Council. 1999. *Realizing the Potential of C4I: Fundamental Challenges.* Washington D.C.: National Academy Press.

Demchak, Chris C., and Peter Dombrowski. 2011. "Rise of a Cyber Westphalian Age." *Strategic Studies Quarterly.*

Department of Homeland Security, U.S.A. 2011. "Cyber Storm III Final Report." *USA Document Handling System.* July. Accessed December 27, 2015. https://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf.

Dyner, Anna Maria. 2014. "Russia Demonstrates Its Strength in the East." *Swiss Federal Institute of Technology Zurich.* October 10. Accessed December 14, 2015. http://www.isn.ethz.ch/layout/set/print/content/view/full/24620?ing=en&id=184491.

Encyclopædia Britannica, Inc. n.d. *Encyclopædia Britannica, Inc.* Accessed December 12, 2015. http://www.britannica.com.

European Journal of International Law. n.d. *European Journal of International Law.* Accessed December 12, 2015. http://ejil.org.

European Union Institute for Security Studies. 2015. *On target? EU sanctions as security policy tools.* Edited by Iana Dreyer and José Luengo-Cabrera. September. Accessed December 17, 2015. http://www.iss.europa.eu/uploads/media/Report_25_EU_Sanctions.pdf.

—. 2015. *Towards an EU global strategy – Background, process, references.* Edited by Antonio Missiroli. September 25. Accessed December 17, 2015. http://www.iss.europa.eu/publications/detail/article/towards-an-eu-global-strategy-background-process-references/.

—. 2015. *Yearbook of European Security 2015.* April 15. Accessed December 1516, 2015. http://www.iss.europa.eu/uploads/media/YES_2015.pdf.

Evera, Stephen Van. 1997. *Guide to Methods for Students of Political Science.* Ithaca, New York: Cornell University Press.

Fritz, Jason. 2008. "How China will use cyber warfare to leapfrog in military competitiveness." *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* 8 (1): 28-80.

Galeotti, Mark, interview by Octavian Manea. 2015. *Hybrid War as a War on Governance* Swiss Federal Institute of Technology Zurich, (August 19).

Galula, David. 1964. *Counter-Insurgency Warfare: Theory and Practice.* New York, New York: Frederick A. Praeger, Inc.

Gates, Robert M. 2009. "A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* (Council of Foreign Relations) 88 (1): 28-40.

GEOStrategy. 2010. "Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή." *GeoStrategy.gr.* December 29. Accessed April 17, 2015. http://www.geostrategy.gr/pdf/20110102%20Cyberwarfare.pdf.

Grenier, John. 2003. "Strategic Warfare in Cyberspace: Review by John Grenier." *Technology and Culture* (Johns Hopkins University Press) 44 (1): 190-191.

Harvey, Frank P. 2003/2004. "Addicted to Security: Globalized Terrorism and the Inevitability of American Unilateralism." *International Journal* (Sage Publications, Ltd) 59 (1): 27-57.

Hoffman, Frank G. 2009. "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict." *Strategic Forum*, April.

Horowitz, Michael C. 2011. *Book Review of "Death by Moderation: The US Military's Quest for Useable Weapons" and "The Iraq Wars and America's Military Revolution".* Review, American Political Science Association.

Howard, Michael. 2009. *Ο Ρόλος του Πολέμου στη Νεότερη Ευρωπαϊκή Ιστορία.* Βάρη, Αττική: Ποιότητα.

Kasapoglu, Can. 2015. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control." *NATO Research Paper* (NATO Defense College) (121): 1-12.

Keane, Jonathan. 2015. *Hacked in 2015: The Year in Cyber-Attacks.* December 9. Accessed December 10, 2015. http://www.pastemagazine.com/articles/2015/12/hacked-in-2015-the-worst-cyber-attacks-of-the-year.html.

Kelsey, Jeffrey T. G. 2008. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." *Michigan Law Review* (The Michigan Law Review Association) 106 (7): 1427-1451.

Kirshner, Jonathan. 2008. "Globalization, American Power and International Security." *Political Science Quarterly* (The Academy of Political Science) 123 (3): 363-389.

Krepinevich Jr., Andrew F. 2009. "The Pentagon's Waisting Assets: The Eroding Foundations of American Power." *Foreign Affairs* (Council on Foreign Relations) 88 (4): 18-33.

Libicki, Martin. 1999-2000. "Rethinking War: The Mouse's New Roar ?" *Foreign Policy* (Washingtonpost Newsweek Interactive, LLC) 117: 30-32+34-43.

Limnell, Jarno, and Thomas Rid. 2014. "Is Cyberwar real ?" *Response*, March/April.

Luke, Timothy W. 2001. "Cyberspace as Meta-Nation: The Net Effects of Online E-Publicanism." *Alternatives: Global, Local, Political* (Sage Publications, Inc.) 26 (2): 113-142.

Lynn, William J. III. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (Council on Foreign Relations) 89 (5): 97-108.

Mazower, Mark. 2013. *Κυβερνώντας τον Κόσμο: Η Ιστορία μιας Ιδέας.* Αθήνα, Αττική: Εκδόσεις Αλεξάνδρεια.

—. 2009. *No Enchanted Palace: The End of Empire and the Ideological Origins of the United Nations.* New Jersey: Princeton University Press.

Mearsheimer, John J. 2011. *Η Τραγωδία της Πολιτικής των Μεγάλων Δυνάμεων.* Αθήνα: Εκδόσεις Ποιότητα.

NATO. 2015. *Centres of Excellence.* May 28. Accessed December 13, 2015. http://www.nato.int/cps/en/natohq/topics_68372.htm?selectedLocale=en#.

—. 2015. *Cyber Security.* November 25. Accessed December 13, 2015. http://www.nato.int/cps/en/natohq/topics_78170.htm.
—. 2015. *Cyber Security.* April 08. Accessed May 10, 2015. http://nato.int/cps/en/natohq/topics_78170.htm?electedlocal=en.
—. 2004. "Istanbul Summit Communiqué." *NATO Press Releases.* June 28. Accessed December 13, 2015. http://www.nato.int/docu/pr/2004/p04-096e.htm.
NATO Public Diplomacy Division. 2010. "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization ." *NATO.* November 20. Accessed December 3, 2015. http://www.nato.int.
—. 2012. "Briefing: Tackling New Security Challenges." *NATO.* September 23. Accessed November 21, 2015. http://www.nato.int.
—. 2011. "NATO after Lisbon." *NATO.* November 20. Accessed December 20, 2015. http://www.nato.int.
—. 2012. "What is NATO ? An introduction to the transatlantic Alliance." *NATO.* November 24. Accessed December 7, 2015. http://www.nato.int.
Neri, Filippo. 2001. *Introduction to Electronic Defense Systems.* 2nd. Norwood, MA: Artech House, Inc.
Nordstrom, Carolyn. 2011. "Extra-Legality: In the Middle." *Middle East Report: Illicit Crossings* (Middle East Research and Information Project (MERIP)) 261: 10-13.
Nye, Joseph. 2015. "Ο Πόλεμος στον 21ο Αιώνα." *Το Βήμα*, Φεβρουάριος 10.
Olson, Eric. 2015. "The New U.S. Military Recruit: 'A Ph.D Who Could Win a Bar Fight'." *The Wall Street Journal.* December 8. Accessed December 21, 2015. http://www.wsj.com/articles/the-new-u-s-military-recruit-a-ph-d-who-could-win-a-bar-fight-1449589994.
Parker, Charles F., and Eric K. Stern. 2002. "Blindsided? September 11 and the Origins of Strategic Surprise." *Political Psychology* (International Society of Political Psychology) 23 (3): 601-630.
Peterson, Ivars. 2001. "Sneaky Calculations." *Science News* (Society for Science & the Public) 160 (20): 318-319.
Raimes, Ann. 2008. *Keys for Writers.* Edited by Carrie Brandon. Boston, MA: Houghton Mifflin Company.
Raska, Michael. 2015. "Hybrid Warfare With Chinese Characteristics." *Swiss Federal Institute of Technology Zurich.* December 2. Accessed December 11, 2015. http://www.isn.ethz.ch/layout/set/print/content/view/full/24620?ing=en&id=195268.
Rasmussen, Anders Fogh. 2011. "NATO After Libya: The Atlantic Alliance in Austere Times." *Foreign Affairs* (Council of Foreign Relations) 90 (4): 2-6.
Rawnsley, Gary D. 2005. "Old Wine in New Bottles: China-Taiwan Computer-Based 'Information Warfare' and Propaganda." *International Affairs* (Royal Institute of International Affairs) 81 (5): 1061-1078.
Rid, Thomas. 2012. "The Empty Threat of Cyberwar." *The Wilson Quarterly* (Woodrow Wilson International Center for Scholars) 36 (1): 58-59.
Robb, John. 2006. "The Role of the Cities." *Global Guerrillas.* October 21. Accessed December 27, 2015.

http://globalguerrillas.typepad.com/globalguerrillas/2006/10/the_role_of_cit.html.
Root Server Operators. 2015. "Root-servers.org." *Root Servers.* December 4. Accessed December 12, 2015. http://root-servers.org/news/events-of-20151130.txt.
RT USA. 2015. "A cyber campaign: Pentagon ponders fighting ISIS online." *RT.* December 21. Accessed December 22, 2015. https://www.rt.com/usa/326710-pentagon-isis-cyber-warfare/.
Rubin, Michael. 2007. "Asymmetrical Threat Concept and its Reflections on International Security." *Strategic Research and Study Center* 1-13.
Russian Federation. 2009. "Russia's National Security Strategy to 2020." *Rustrans.* May 12. Accessed December 13, 2015. http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.
Rutherford, Ian P. 2011. "NATO's new strategic concept, nuclear weapons, and global zero." *International Journal* (Sage Publications, Ltd) 66 (2): 463-482.
Shaw, Malcolm N. 2008. *Inetrantional Law.* New York, New York: Cambridge University Press.
Sternstein, Aliya. 2015. "New OPM Cyber Czar Worried About an ISIS Hack." *Nextgov.* December 14. Accessed December 21, 2015. http://www.nextgov.com/cybersecurity/2015/12/new-opm-cyber-czar-says-he-fears-isis-hack/124479/?oref=ng-channelriver.
The American Society of International Law. n.d. *The American Society of International Law.* Accessed December 16, 2015. https://www.asil.org.
The Middle East Journal. 2011. "Chronology: October 16, 2010 - January 15, 2011." *The Middle East Journal* (Middle East Institute) 65 (2): 312.
The United Nations. 2015. *United Nations Treaty Collection.* Accessed December 13, 2015. https://treaties.un.org/Home.aspx.
Thiele, Ralph D. 2015. "The New Colour of War - Hybrid Warfare and Partnership." *Institut fur Strategie - Politik - Siecherheits - und Wirtschaftsberatung ISPSW.* October. Accessed December 16, 2015. http://www.ispsw.de.
Tse-tung, Mao. 1989. *On Guerrilla Warfare.* Translated by Samuel B. Griffith. Washington D.C., DC: Department of the Navy.
Tzu, Sun. 2008. *Η Τέχνη του Πολέμου.* Αθήνα, Αττική: Εκδόσεις Περίπλους.
UN International Court of Justice. n.d. *International Court of Justice.* Accessed December 28, 2015. http://www.icj-cij.org/homepage/index.php?lang=en.
United Nations Publication. 2004. *Charter of the United Nations and Statute of the International Court of Justice.* New York, New York: United Nations Publication.
United States Attorney's Office, Emily Langlie. 2006. "California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department." *United States Attorney's Office.* May 4. Accessed December 26, 2015. http://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/maxwellPlea.htm.
United States Joint Chief of Stuff. 2013. "Joint Chiefs of Staff Publications." *Joint Chiefs of Staff.* January 22. Accessed December 2, 2015. http://www.jcs.mil/portals/36/documents/publications/environmentalwhitepaper.pdf.

United States of America Department of Defence. 2015. "The National Military Strategy of the United States of America 2015." *Joint Chiefs of Staff, US DoD.* June 2. Accessed December 10, 2015. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

Verdier, Pierre-Hugues, and Erik Voeten. 2014. "Precedent, Compliance, and Change in Customary International Law: Explanatory Theory." *The American Journal of International Law* (American Society of International Law) 108 (3): 389-434.

Wall Street Journal. 2015. "WSJ: Ιρανοί χάκερ στόχευσαν φράγμα στη Νέα Υόρκη το 2013." *Η Ναυτεμπορική.* December 21. Accessed December 23, 2015. http://www.naftemporiki.gr/printStory/1045224.

Weimann, Gabriel. 2006. *Terror on the Internet: The New Arena, the New Challenges.* Washington D.C., D.C.: United States Institute of Peace.

Wikipedia. 2015. *Cybercrime.* December 8. Accessed December 10, 2015. https://en.wikipedia.org/wiki/Cybercrime.

—. 2015. *Cyberwarfare.* November 11. Accessed December 12, 2015. https://en.wikipedia.org/wiki/Cyberwarfare.

Winkler, Ira. 2012. "Will There Be an Electronic Pearl Harbor ?" *PC World.* December 12. Accessed December 12, 2015. http://www.pcworld.com/article/183436/electronic_pearl_harbor.html.

Woodrow Wilson International Center for Scholars. 2002. "While America Slept: A Survey of Recent Articles." *The Wilson Quarterly* (Woodrow Wilson International Center for Scholars) 26 (1): 81-82.

n.d. *World Digital Library.* Accessed December 11, 2015. http://www.wdl.org/en/.

Wright, Robert, and Robert Kaplan. 2001. "Mr. Order Meets Mr. Chaos." *Foreign Policy* (Washingtonpost Newsweek Interactive, LLC) 124: 50-60.

Yale Law School. 2008. *The Laws of War.* Accessed December 11, 2015. http://avalon.law.yale.edu/subject_menus/lawwar.asp.

Ying, Fu. 2015. "How China Sees Russia." *Foreign Affairs.* December 14. Accessed December 20, 2015. https://www.foreignaffairs.com/print/1116123.

Yorke, Claire. 2010. "Cybersecurity and Society." *The World Today* (Royal Institute of International Affairs) 66 (12): 19-21.

Παρίσης, Ιωάννης. 2010. *Η Ευρώπη της Άμυνας: Ευρωπαϊκή Πολιτική Ασφάλειας & Άμυνας.* Αθήνα, Αττική: Έκφραση Πολιτισμού.

Χατζηκωνσταντίνου, Κώστας Θ., Χαράλαμπος Ελ. Αποστολίδης, and Μιλτιάδης Χ. Σαρηγιαννίδης. 2014. *Θεμελιώδεις Έννοιες στο Διεθνές Δημόσιο Δίκαιο.* Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα Α.Ε.

Πάγκαλος, Γεώργιος, and Ιωάννης Μαυρίδης. 2002. *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.* Θεσσαλονίκη: Ανικούλα.

Πλατιάς, Αθανάσιος. 2010. *Διεθνείς Σχέσεις και Στρατηγική στον Θουκυδίδη.* Αθήνα, Αττική: Βιβλιοπωλείον της Εστίας.

Αντωνόπουλος, Κωνσταντίνος, and Κωνσταντίνος Μαγκλιβέρας. 2014. *Το Δίκαιο της Διεθνούς Κοινωνίας.* Αθήνα: Νομική Βιβλιοθήκη.

Αποστολίδης, Παύλος. 2014. *Μυστική Δράση: Υπηρεσίες Πληροφοριών στην Ελλάδα.* 2. Αθήνα, Αττική: Εκδόσεις Παπαζήση.

Γιαννακόπουλος, Βασίλης. 2014. "Τρομοκρατία και Χειμερινοί Ολυμπιακοί Αγώνες." *Geostrategy.* Ιανουάριος 9. Accessed Μάιος 10, 2015. http://www.geostrategy.gr/pdf/20140109%20Winter%20Olympic%20Games%202014.html.

Ρούκουνας, Εμμανουήλ. 2015. *Δημόσιο Διεθνές Δίκαιο.* Αθήνα: Νομική Βιβλιοθήκη.

Μακιαβέλλι, Νικκολό. 2006. *Ο Ηγεμόνας.* Αθήνα: Κάκτος.