ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Π.Μ.Σ ΤΜΗΜΑΤΟΣ ΔΙΕΘΝΩΝ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΕΙΔΙΚΕΥΣΗ: ΣΤΡΑΤΗΓΙΚΕΣ ΣΠΟΥΔΕΣ ΚΑΙ ΔΙΕΘΝΗΣ ΠΟΛΙΤΙΚΗ

Οι Θεωρήσεις των Διεθνών Σχέσεων και το Πληροφοριακό Περιβάλλον

Ο Κυβερνοχώρος ως Πεδίο Διεθνούς Ανταγωνισμού Ισχύος

Εισηγητής: Κωνσταντίνος Καλκετινίδης

Επιβλέπον Καθηγητής: Δρ. Κουσκουβέλης Ηλίας

Δεκέμβριος 2019

«Δηλώνω υπευθύνως ότι 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 ότι, όπως απαιτείται από αυτούς τους κανόνες, αναφέρομαι και παραπέμπω στις πηγές όλων των στοιχείων που χρησιμοποιώ και τα οποία δεν συνιστούν πρωτότυπη δημιουργία μου»

Κωνσταντίνος Καλκετινίδης

ΠΕΡΙΛΗΨΗ

Τα ψηφιακά επιτεύγματα των δύο πρώτων δεκαετιών του 21ου αιώνα έχουν αδιαμφισβήτητα διαμορφώσει τις προϋποθέσεις για ριζικές μεταβολές στον τρόπο οργάνωσης και λειτουργίας των σύγχρονων κοινωνιών τροχοδρομώντας μια αναπόφευκτη σύγκλιση στην ποικιλομορφία τους. Παραδόξως βέβαια, η σύγκλιση πραγματοποιείται με όχημα την πολυπολιτισμική χειραφέτηση, η οποία ωστόσο οδηγεί σε μια παγκόσμια κοινωνικοπολιτισμική ομογενοποίηση, ακολουθώντας τα βήματα της οικονομικής και πολιτικής παγκοσμιοποίησης.

Ωστόσο και το περιβάλλον, στο οποίο απαντώνται και ασκούνται οι διεθνείς σχέσεις, δηλαδή η «Κοινωνία» που απαρτίζεται από τους διεθνούς δρώντες της εποχής μας, είναι επίσης φορέας μεταβολών, που επιβάλλει η σύγχρονη πραγματικότητα στις συνθήκες ανταγωνισμού ισχύος αλλά και συνεργασίας μεταξύ των υπόψη δρώντων. Στο πλαίσιο αυτό, η εκούσια ή ακούσια διατάραξη της ισορροπίας των σχέσεων ισχύος, είτε με τις εκδηλώσεις του ανταγωνισμού μεταξύ της σχετικής ισχύος δύο ή περισσότερων διεθνών δρώντων είτε με τις εκδηλώσεις συνεργασίας – άθροισης της σχετικής ισχύος – αυτών, μοιραία επηρεάζεται από φαινόμενα που λαμβάνουν χώρα στον Κυβερνοχώρο ή εκδηλώνεται μέσα σε αυτόν.

Σκοπός του παρόντος πονήματος είναι η διερεύνηση των μεταβολών, των φαινομένων και των προκλήσεων που διαπιστώνονται ή ανακύπτουν εξαιτίας της νέας «κυβερνοπραγματικότητας», τόσο στο επίπεδο του θεωρητικού υπόβαθρου στο οποίο εδράζονται οι διεθνείς σχέσεις, όσο και στο επίπεδο της εφαρμοσμένης πολιτικής των διεθνών δρώντων για την κατανόηση – ερμηνεία και την εκμετάλλευση ή αντιμετώπισή τους κατά περίπτωση.

Αρχικά παρουσιάζονται οι κυριότερες θεωρητικές προσεγγίσεις αλλά και προβληματισμοί που προκύπτουν ως συνέπεια της επίδρασης της ψηφιακής τεχνολογίας στο διεθνοπολιτικό γίγνεσθαι. Στη συνέχεια, επιχειρείται η συνοπτική περιγραφή των βασικών ψηφιακών προκλήσεων ασφαλείας, οι οποίες ρυθμίζουν ή καθορίζουν την συμπεριφορά των διεθνών δρώντων. Στο τέλος γίνεται μια απολογιστική καταγραφή του βαθμού θεσμικής θωράκισης του υφιστάμενου διεθνούς νομικού πλαισίου, ώστε να εκτιμηθούν οι πιθανές προοπτικές διαμόρφωσης ενός κανονιστικού πλαισίου που θα δεσμεύει τους δρώντες, στο βαθμό που αυτό είναι εφικτό, λαμβάνοντας πάντα υπόψη τον άναρχο χαρακτήρα του διεθνούς συστήματος.

Συμπερασματικά, η παρούσα μελέτη αναδεικνύει την πολυπλοκότητα των επιδράσεων που παράγουν τα φαινόμενα που λαμβάνουν χώρα στον κυβερνοχώρο ή επηρεάζονται από την φύση του και τα οποία πλέον συμβάλλουν στη διαμόρφωση ή ακόμα και συνδιαμορφώνουν τις σχέσεις ισχύος στο διεθνοπολιτικό πεδίο. Στο πλαίσιο αυτό, το φαινόμενο του «κυβερνοπολέμου», ίσως το πιο εντυπωσιακό από τα φαινόμενα που σχετίζονται με τον κυβερνοχώρο, αποτελεί υπόδειγμα παράγωγου προϊόντος των ζυμώσεων ισχύος. Ο κυβερνοχώρος αποκαλύπτεται ως η παράμετρος, που διαπερνά τα τρία επίπεδα, κατά Waltz, μέσα στα οποία πλάθεται η αιτιοκρατική φύση της σύγκρουσης, ο

Άνθρωπος, το Κράτος και το Διεθνές Σύστημα. Κάθε δε προσπάθεια για τον περιορισμό – έλεγχο του κυβερνοχώρου, πόσο μάλλον για την εξουδετέρωσή των φαινομένων που λαμβάνουν χώρα σε αυτόν, φαντάζει ιδιαίτερα μεμακρυσμένη προοπτική, αν όχι ουτοπική, καθώς το επίπεδο μυστικότητας, που για λόγους αυτοσυντήρησης τα Κράτη είναι υποχρεωμένα να διατηρούν, συνιστά την ανατροφοδοτούμενη τροχοπέδη σε κάθε βήμα προς αποκατάσταση δίαυλων επικοινωνίας και συνεννόησης μεταξύ τους για τα ζητήματα ισχύος που σχετίζονται με τον χώρο αυτό.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΧΑΡΙΣΤΙΕΣ

Ίσως οι θερμότερες ευχαριστίες μου προς τους ανθρώπους, που συνέβαλλαν καθοριστικά για να μπορώ σήμερα να παρουσιάσω αυτό το πόνημα, δεν αρκούν για να εκφράσουν την ευγνωμοσύνη μου για την θετική επιρροή που άσκησαν προσφέροντας απλόχερα τις γνώσεις και τις εμπειρίες τους. Μπορώ ωστόσο να τους διαβεβαιώσω ότι πλέον είμαι φορέας των συμπτωμάτων της μάθησης που επήλθε, η οποία αφήνοντας ανεξίτηλη υπογραφή, έχει μεταβάλλει τη στάση και κυρίως την συμπεριφορά μου έναντι όλων των στοιχείων που ορίζουν ή σχετίζονται με τα δημόσια πράγματα και κυρίως αυτά που ερμηνεύουν τα φαινόμενα και τις συναλλαγές ισχύος που λαμβάνουν χώρα στο διεθνές πεδίο δράσης.

Ο Κοσμήτορας Σχολής Κοινωνικών, Ανθρωπιστικών Επιστημών και Τεχνών Καθηγητής Ηλίας Κουσκουβέλης, ο Καθηγητής Διεθνών Σχέσεων και Πολιτικής Γεώργιος Σπυρόπουλος, ο Αναπληρωτής Καθηγητής Θεωρίας των Διεθνών Σχέσεων Σπυρίδων Λίτσας, η Επίκουρη Καθηγήτρια Διεθνών Σχέσεων Φωτεινή Μπέλλου, η Επίκουρη Καθηγήτρια Διεθνούς Δικαίου Καλλιόπη Χαΐνογλου, διέθεσαν όλοι με υπομονή και πάθος την επιστημονική τους αυθεντία για να διαμορφώσουν και να βοηθήσουν να ωριμάσει η διεθνοπολιτική σκέψη επαγγελματιών που πιθανόν σύντομα θα κληθούν να ορίσουν την τύχη της χώρας, ο καθένας από το δικό του μετερίζι.

Η απλή και μόνο αναφορά των ονομάτων, των υπέροχων αυτών καθηγητών του Προγράμματος Μεταπτυχιακών Σπουδών του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών και συγκεκριμένα της κατεύθυνσης των Διεθνών Σπουδών με ειδίκευση τις Στρατηγικές Σπουδές και τη Διεθνή Πολιτική, αποτελεί κόσμημα για την διπλωματική μου εργασία και με τιμά ιδιαίτερα ως φιλομαθή πολίτη και ως αξιωματικό του Ελληνικού Στρατού.

Θα ήταν ωστόσο αμετροεπής παράλειψη να μην ευχαριστήσω μέσα από την ψυχή μου και τη σύζυγό μου Χριστίνα η οποία, σχεδόν τριάντα χρόνια τώρα, ακούραστα μου συμπαραστέκεται στον στρατιωτικό μου βίο και αδιάλειπτα με παρακινεί για επόμενα και υψηλότερα πνευματικά άλματα. Της αξίζει πολύ μεγαλύτερη τιμή από την απλή αφιέρωση αυτής της εργασίας.

Θεσσαλονίκη, Δεκέμβριος 2019

«Three years in cyberspace is like thirty years anyplace real[1]»

Bruce Sterling, science fiction author

1. Εισαγωγή… στις Διεθνείς «Κυβερνοσχέσεις»

Πλέον θεωρείται κοινοτυπία να αναφερόμαστε στην σύγχρονη πραγματικότητα και να χρησιμοποιούμε τον όρο «ψηφιακή εποχή[2]». Η ραγδαία τεχνολογική πρόοδος στον πληροφοριακό τομέα έχει ανατρέψει κάθε προηγούμενη αντίληψη περί χώρου, χρόνου και ταχύτητας επιτάσσοντας κατ΄ ελάχιστο τον επανασχεδιασμό τόσο των στοχεύσεων όσο και των μεθόδων σε στρατηγικό και τακτικό επίπεδο αντίστοιχα.

Ο επαναστατικός[3] χαρακτήρας της τεχνολογικής εξέλιξης σήμερα, όπως και κάθε προηγούμενή φορά κατά την ιστορική διαδρομή του ανθρώπου, φαίνεται ότι έχει πλέον υπερβεί το επιφανειακό επίπεδο των εποπτεύσιμων μεταβολών στην υφή των πραγμάτων. Το γεγονός αυτό επιβεβαιώνει την δραστικότητα των ψηφιακών επιτευγμάτων, η οποία διαμορφώνει τις προϋποθέσεις ριζικών αλλαγών στο πλαίσιο της οργάνωσης και λειτουργίας της κοινωνίας των ανθρώπων. Ωστόσο, από την οπτική των διεθνών σχέσεων, το βασικό ερώτημα που ενδιαφέρει είναι εάν τελικά η πίεση, που η ψηφιακή τεχνολογία μοιραία ασκεί στους ενδοκρατικούς θεσμούς και δομές, είναι ικανή να διαρρήξει το διηθητικό κέλυφος που διαχωρίζει το εσωτερικό των κύριων διεθνοπολιτικών δρώντων, δηλαδή των Κρατών, από τον άναρχο χώρο στον οποίο αυτά ανταγωνίζονται, στη βάση της υφιστάμενης κατανομής της ισχύος και των συμφερόντων τους, όπως αυτά διαμορφώνονται, όχι μόνο από την ποικιλότητα που εμφορείται ενδοκρατικά αλλά κυρίως από την ίδια την κατανομή της ισχύος και την θέση που αυτή επιφυλάσσει για το καθένα κράτος εντός του διεθνούς συστήματος. Το ζητούμενο βέβαια δεν είναι η διαπίστωση της «ψηφιακής» εισβολής στη διεθνή πολιτική αρένα, αλλά τι τελικά σημαίνει αυτή για τον χαρακτήρα, τη δομή και την ισορροπία του διεθνούς συστήματος και ποιες οι απορρέουσες προκλήσεις ασφαλείας που καλείται να αντιμετωπίσει το Κράτος τόσο στο πλαίσιο του διεθνούς ανταγωνισμού ισχύος, όσο και έναντι του ρόλου και των υποχρεώσεων του στο εσωτερικό του.

Το κυρίαρχο στοιχείο του τροποποιητικού χαρακτήρα της τεχνολογικής επανάστασης, που βιώνουν οι σημερινές ανθρώπινες γενεές, είναι το καθεστώς του «Ψηφιακού Πληροφοριακού Περιβάλλοντος» (Digital Information Environment). Στον καθημερινό λόγο βέβαια έχει επικρατήσει η έννοια του «Πληροφοριακού Περιβάλλοντος» χωρίς αναφορά στον ψηφιακό χαρακτήρα του, ο οποίος επισκίασε το γεγονός πως οι ρίζες του πληροφοριακού περιβάλλοντος χάνονται στο παρελθόν και αγγίζουν την εποχή που άνθρωπος πρωτοαναπαρήγαγε ιδεογράμματα για να εκφραστεί και να ανταλλάξει πληροφορίες με διαχρονικό σκοπό να συνεργαστεί, να διαφωνήσει, να καταναλώσει και να

---

[1] Bruce Sterling, “The Hacker Crackdown”, 1994, https://doc.lagout.org/security/Hacking-The%20Hacker%20Crackdown.pdf

[2] George Doukidis, Nikos Mylonopoulos, and Nancy Pouloudi , ‘’Social and Economic Transformation in the Digital Era’’, Athens, June 2003
Jill Shepherd, ‘’Chapter 1: What is the Digital Era?’’, University of Strathclyde, UK

[3] Bruce R. Guile (Editor), ‘’Information Technologies and Social Transformation’’, National Academy of Engineering; Melvin Kranzberg, ‘’The Information Age: Evolution or Revolution?’’, NATIONAL ACADEMY PRESS, Washington D.C. 1985, p.35 - 53

πολεμήσει[4]. Ενώ λοιπόν το πληροφοριακό περιβάλλον ήδη προϋπήρχε ως το φυσικό πεδίο ανταλλαγής πληροφοριών και επικοινωνίας, πολύ πριν από την εποχή της αρχαίας «αγοράς», ήταν σχετικά πρόσφατα, πριν περίπου ένα αιώνα, που ενσωμάτωσε την τεχνολογία των παλμών (συχνότητες) και των ημιαγωγών (ψηφιακή), με τελευταία εισαγωγή, μόλις πριν 40 χρόνια, την διασυνδεσιμότητα που προσφέρουν οι ηλεκτρονικοί υπολογιστές. Η κατανόηση της φύσης του πληροφοριακού περιβάλλοντος, όπως αυτό έχει εξελιχθεί και γίνεται αντιληπτό σήμερα, συμβάλει καθοριστικά στην αντίστοιχη κατανόηση των προκλήσεων ασφαλείας που το νεότευκτο αυτό «ψηφιακό» καθεστώς έχει επιβάλλει.

Συστατικό στοιχείο του Πληροφοριακού Περιβάλλοντος είναι η ψηφιοποίηση[5], ενώ το κυρίαρχο χαρακτηριστικό του είναι η άπειρη, χωρίς όρια φύση του. Η τεχνική δυνατότητα της ψηφιοποίησης είναι αυτή που επέτρεψε την σταδιακή αρχικά και ακολούθως συνεχώς επιταχυνόμενη ανάπτυξη ενός διασυνδεδεμένου και διαδραστικού συνόλου παγκόσμιων δικτύων υπολογιστών και συσκευών επικοινωνίας. Αυτό το «δίκτυο δικτύων» έχει εξελιχθεί σε μια παγκόσμια αρένα αλληλεπίδρασης για αμέτρητες δραστηριότητες διοχέτευσης – ροής πληροφοριών (raw data) και ιδεών (processed information) και αμοιβαίας ανταλλαγής αυτών μεταξύ των ανθρώπων και των μηχανών σε όλο τον κόσμο, ενώ το μέρος της ανθρωπότητας που δεν συμμετέχει σ΄ αυτό το πλέγμα δραστηριοτήτων συρρικνώνεται με νομοτελειακή τάση εξαφάνισης. Η «απειρότητα» του πληροφοριακού περιβάλλοντος γίνεται έμμεσα αντιληπτή από την φύσει παγκοσμιοποιημένη λειτουργικότητά του. Ο δε αγώνας όσων επιθυμούν τον περιορισμό και οριοθέτηση του πληροφοριακού περιβάλλοντος, είτε για λόγους συμφέροντος, όπως και αν αυτό ορίζεται, εδράζεται ή εκπηγάζει, είτε ωθούμενοι από ουτοπικά ελατήρια, μοιάζει απελπιστικά μάταιος μπροστά στα συνεχώς αυξανόμενα μεγέθη του διακινούμενου όγκου πληροφοριών και την αέναη εξάπλωση των πληροφοριακών «οδών», όπως και των «θυρών» διαφυγής κάθε φορά που εγείρονται φυσικά, διανοητικά[6], θεσμικά ή ψηφιακά εμπόδια.

Θα μπορούσαμε λοιπόν να νοηματοδοτήσουμε ως **«Πληροφοριακό Περιβάλλον»**, το υβριδικό πλέον περιβάλλον που συνδυάζει το πεδίο φυσικής δραστηριοποίησης των ανθρώπων και μηχανών με το ψηφιακό πεδίο και τα παράγωγα εικονικά καθεστώτα που δημιουργούνται μέσα σε αυτό, καθώς και τα παράγωγα αποτελέσματα (effects) που δημιουργούνται και επηρεάζουν τον φυσικό κόσμο. **«Κυβερνοχώρος»** δε, ορίζεται το ψηφιακό περιβάλλον που δημιουργείται συνδυαστικά από το σύνολο των ψηφιακών διασυνδέσεων μεταξύ ηλεκτρονικών υπολογιστών και συσκευών αμφίδρομης ή μονόδρομης επικοινωνίας με τις λεωφόρους ροών ανταλλαγής ψηφιακών μηνυμάτων[7] και τις ροές αυτές. Είναι ένας χώρος συνεχούς ροής και δεν μπορεί να περιγραφεί ούτε συσταλτικά, με αποκλειστικά μηχανιστικούς όρους, ούτε διασταλτικά με αμιγώς κοινωνιολογικούς[8]. Ο κυβερνοχώρος λοιπόν, αποτελεί πλέον τον πυρήνα του

---

[4] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.16

[5] David Burkett, ''DIGITISATION AND DIGITALISATION: WHAT MEANS WHAT?'' Dec 19, 2017 https://workingmouse.com.au/innovation/digitisation-digitalisation-digital-transformation

[6] Michael Fitzgerald, ''The Nine Obstacles to Digital Transformation'', https://sloanreview.mit.edu/article/the-nine-obstacles-to-digital-transformation/

[7] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: Executive Office of the President of the United States, 2009, p.1

[8] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.38

πληροφοριακού περιβάλλοντος, καθώς ενυπάρχει σε αυτό και ορίζει ανεπιστρεπτί την ύπαρξή του. Βέβαια, ο κυβερνοχώρος παραμένει μια μεταφορική έννοια[9], η οποία δεν πρέπει να συγχέεται με το «διαδίκτυο», το οποίο αποτελείται από πραγματικό υλικό: ένα παγκόσμιο δίκτυο υπολογιστών που χρησιμοποιούν καθορισμένα πρωτόκολλα επικοινωνιών μεταξύ τους, χωρίς να αποκλείεται η ταυτόχρονη ύπαρξη και άλλων παγκόσμιων δικτύων, που επικοινωνούν απλά με διαφορετικά πρωτόκολλα.

Η παγκόσμια συναντίληψη για την σημασία του κυβερνοχώρου ως κρίσιμου πεδίου δραστηριοποίησης αλλά και ανταγωνισμού σε κάθε τομέα της ανθρώπινης δράσης (πολιτικό, κοινωνικό, οικονομικό, στρατιωτικό, περιβαλλοντικό κλπ) καθιστά αναγκαία την μελέτη των φαινομένων που συσχετίζονται άμεσα ή έμμεσα με το πεδίο αυτό, προσελκύοντας ακόμα και την σκεπτικιστική προσοχή αυτών που αμφισβητούν σχεδόν αξιωματικά την μετασχηματιστική ισχύ του, είτε ενδοκρατικά / ενδοεταιρικά (στο πλαίσιο ενός οργανισμού), είτε διακρατικά / διεταιρικά (μεταξύ οργανισμών). Προς επίρρωση των ανωτέρω, σημαντικότατοι δημόσιοι και ιδιωτικοί πόροι διοχετεύονται κατάλληλα είτε για την ασφάλεια των δραστηριοτήτων στον κυβερνοχώρο (Cyber Security, Cyber Defence), είτε για εξασφάλιση μεριδίου αγοράς και επιρροής (Corporate Influence and Branding), είτε για την προώθηση της ίδιας της δραστηριοποίησης στο χώρο αυτό (Building Capacity) διαμορφώνοντας συνθήκες «κυβερνοπολιτικής» και ηλεκτρονικής διακυβέρνησης (Cyberpolitics[10] and e-Governance). Όπως διαπιστώνει ο Barlow, «ο κυβερνοχώρος, στην παρούσα κατάστασή του, έχει πολλά κοινά χαρακτηριστικά με τη Δύση του 19ου αιώνα. Είναι αχανής, αχαρτογράφητος, πολιτιστικά και νομικά αμφιλεγόμενος, λεκτικά υπερσυντετμημένος (εκτός αν τυχαίνει να είσαι δικαστικός στενογράφος), είναι δύσκολο να τον περιηγηθείς, να παίξεις μαζί του και να τον κερδίσεις. Μεγάλοι οργανισμοί ισχυρίζονται ότι τον κατέχουν ήδη, αλλά οι περισσότεροι από τους πραγματικούς «ιδιοκτήτες» είναι μοναχικοί και ανεξάρτητοι, μερικές φορές σε βαθμό κοινωνιοπάθειας[11]. Είναι, βέβαια, ένα τέλειο έδαφος αναπαραγωγής τόσο για τους απατεώνες όσο και για νέες ιδέες για την ελευθερία[12]».

Με την παρούσα εργασία επιχειρείται μια ψηλάφηση των προκλήσεων ασφαλείας που αναδύονται μέσα από την αναγκαία, συχνά βίαια, προσαρμογή των μέσων και των σκοπών, ώστε να αναζητηθεί αν και σε ποιο βαθμό η νέα αυτή κυβερνοπραγματικότητα (Cyber–reality[13]) επηρεάζει, τροποποιεί ή μεταλλάσσει τόσο την κατανόηση των θεωρητικών πυλώνων πάνω στους οποίους εδράζονται οι διεθνείς σχέσεις, όσο και την εφαρμοστική τέχνη της παραγωγής πολιτικής, είτε της πολιτικής ασφαλείας και άμυνας, είτε της εξωτερικής πολιτικής των κυβερνήσεων κρατών ή των κέντρων άσκησης αντίστοιχης εξουσίας, πολυμερών ή διεθνών οργανισμών.

---

[9] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.13

[10] Nazli Choucri, ''Cyberpolitics in International Relations'', The MIT Press, Cambridge, Massachusetts London, England, 2012

[11] Κοινωνιοπάθεια: Αντικοινωνική διαταραχή της προσωπικότητας https://www.onmed.gr/ygeia-psyhikh/story/331885/ta-simadia-pou-apokalyptoun-enan-koinoniopathi

[12] John Perry Barlow, Crime and Puzzlement (June 1990), https://www.eff.org/pages/crime-and-puzzlement

[13] Tim A.Scally, ''Cyber Reality: How the Security Industry Is Adjusting to the New Normal'', Security Distributing & Marketing, 02 Sep 2017 https://www.sdmmag.com/articles/94274-cyber-reality-how-the-security-industry-is-adjusting-to-the-new-normal

Αυτή η «Κυβερνοποίηση» (Cyberisation) των διεθνών σχέσεων αναφέρεται αφενός στην ήδη διενεργούμενη διείσδυση σε όλα τα διαφορετικά πεδία δραστηριότητας που σχετίζονται με τις διεθνείς σχέσεις, αφετέρου δε στην ολοένα αυξανόμενη εξάρτηση των υποκειμένων των διεθνών σχέσεων στις υποδομές, στα όργανα και μέσα – εργαλεία που μεταχειρίζεται ή προσφέρει ο κυβερνοχώρος[14]. Πίσω δε στη δεκαετία του 1990, ούτε οι Keohane και Nye δεν μπόρεσαν να διαβλέψουν ότι η πρόσβαση στο διαδίκτυο θα αποτελούσε έναν παγκόσμιο κανόνα, ένα θεμελιώδης αγαθό μόλις από τις αρχές της πρώτης δεκαετίας του 21ου αιώνα, μεταμορφώνοντας τελικά τις διεθνείς πολιτικές[15]. Πολιτικές, οι οποίες από προϊόντα μονοσήμαντων διμερών ή πολυμερών σχέσεων, ορίζονται πλέον από σχέσεις αλληλεξάρτησης παγκόσμιας κλίμακας.

Μετά το εισαγωγικό κεφάλαιο, με τον μάλλον προβοκατόρικο τίτλο «Εισαγωγή στις Διεθνείς Κυβερνοσχέσεις», όπου επιχειρείται μια μορφολογικής προσέγγισης - ελπίζω με αρκετή δόση αφαιρετικής διάθεσης - περιγραφή του περιβάλλοντος που συνιστά το ψηφιακό πεδίο δράσης, ακολουθεί το κεφάλαιο στο οποίο περιγράφεται σε αδρές γραμμές η σύνδεση της ψηφιακής πραγματικότητας με τις τρεις εικόνες του Kenneth Waltz[16]. Στη συνέχεια, στο 3ο Κεφάλαιο, αναφέρονται οι κυριότεροι προβληματισμοί που προκύπτουν από την διόπτευση των διεθνοπολιτικών ζητημάτων μέσα από τους φακούς των κυριότερων θεωρήσεων των διεθνών σχέσεων. Ζητήματα που αναφύονται μέσα από τις αλληλεπιδράσεις που ενυπάρχουν αλλά και παράγονται εξαιτίας της αποκάλυψης - θέσπισης της ψηφιακής διάστασης του κόσμου. Ακολούθως, στο 4ο Κεφάλαιο περιγράφονται οι απορρέουσες, «υλικής» υφής, προκλήσεις που ουσιαστικά αποτελούν τα παράγωγα προϊόντα της Κλαουζεβίτσιας τριβής που προκύπτουν από τις πολυποίκιλες και διαφορετικής έντασης σχέσεις που αναπτύσσονται μεταξύ των πρωταγωνιστών του διεθνούς συστήματος, κλασσικών και νεόκοπων, αδιαχώριστα.

Το πόνημα ολοκληρώνει τον λογικό του κύκλο με μάλλον ατελή συμπεράσματα που ουσιαστικά αναδεικνύουν τόσο τον δυναμικό χαρακτήρα του κυβερνοχώρου, ως χώρο διεθνοπολιτικού ανταγωνισμού, αλλά κυρίως την αποδοχή του γεγονότος ότι οι ζυμώσεις που προκαλεί ο ίδιος ο εξελισσόμενος χαρακτήρας του ψηφιακού κόσμου, δεν επιτρέπει, τουλάχιστον όχι ακόμα, την απόκτηση στέρεας θεωρητικής θεμελίωσης των φαινομένων που παρατηρούνται αλλά και βιώνονται μέσα σε αυτόν.

---

[14] Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges, Springel - Verlag Berlin Heidelberg, 2014, Preface, p.xi

[15] Robert O. Keohane and Joseph S. Nye, Jr. ‘’Power and interdependence in the information age’’, Foreign Affairs, 77(5), p. 81-94

[16] Kenneth Waltz, “Ο Άνθρωπος, το Κράτος και ο Πόλεμος: Μια θεωρητική ανάλυση”, Μετάφραση: Κ.Κολιόπουλος, Εισαγωγή στην Ελληνική έκδοση: Η.Κουσκουβέλης, Εκδόσεις Ποιότητα, Βάρη Αττικής, 2011

«When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole[17]»

Nikola Tesla, Serbian-American scientist

2. Ο Άνθρωπος, το Κράτος και το Διεθνές Σύστημα στην Ψηφιακή Εποχή

Λόγω της συνεχούς διεύρυνσης της δικτυακής διασυνδεσιμότητας και της αναπόφευκτης διείσδυσης του κυβερνοχώρου σε όλο το μήκος και πλάτος των κοινωνικοπολιτικών δραστηριοτήτων και εξελίξεων, καθώς και της επακόλουθης ανάπτυξης μιας ολοένα πιο συμπλεγματικής σχέσης με αυτές, οι οποίες με τη σειρά τους ανατροφοδοτούνται από τις δυνατότητες που προσφέρει ο κυβερνοχώρος, ήδη διαπιστώνεται ο βαθμός επιρροής που ασκεί το μοντέρνο αυτό πεδίο δράσης και παρουσίας στα γεγονότα που λαμβάνουν χώρα και στο πεδίο της διεθνούς πολιτικής. Προβάλλοντας τον πυρήνα της πολιτικής, όπως τον ορίζει ο Harold D. Lasswell[18] ως «Who Gets What, When and How» στο διεθνές επίπεδο, είναι αναμενόμενη η αυξανόμενη σημασία των σχέσεων, των γεγονότων και των εξελίξεων στον τομέα του κυβερνοχώρου για τη διεθνή ασφάλεια σε όλες τις εκφάνσεις της, λειτουργώντας δυνητικά μετασχηματιστικά[19].

Ο **Άνθρωπος** βρίσκεται στο επίκεντρο των ριζοσπαστικών, κοινωνιολογικής φύσης μεταβολών που εισηγείται η ψηφιακή, ημιυβριδική προς το παρόν, ψηφιακή πραγματικότητα, καθώς η τεχνητή νοημοσύνη έρχεται με γοργούς ρυθμούς για να γεμίσει τα κενά αυτής της υβριδικότητας ενός περιβάλλοντος όπου άνθρωπος και μηχανή θα συμβιώνουν άλλοτε ως ξεχωριστές και άλλοτε ως αδιαχώριστες οντότητες. Με ένα νεολογισμό θα μπορούσαμε να ορίσουμε τον σύγχρονο άνθρωπο ως «HOMO GOVERNUS», ο οποίος καλείται να επιβιώσει και δραστηριοποιηθεί επιτυχώς σε ένα νέο περιβάλλον, τα όρια του οποίου είναι μάλλον άπειρα, εντός του οποίου δοκιμάζονται τα όρια της νοητικής ικανότητάς του.

Ίσως η πλέον χαρακτηριστική αναλογία που περιγράφει τη μεταβολή στην αντίληψη της πραγματικότητας από τον άνθρωπο, αλλά και στον τρόπο διάδρασής του με το σύγχρονο ψηφιακό περιβάλλον, αποτελεί η μετεξέλιξη του νοήματος της ιδιότητας του «hacker», όπως αυτή αποδόθηκε αρχικά, στα τέλη της δεκαετίας του ’50, όταν περιέγραφε όσους συνέπαιρνε η τεχνολογική καινοτομία και το πάθος για την τεχνική δεξιοτεχνία και πώς κατέληξε σήμερα να αποτελεί, στην καλύτερη περίπτωση, συνώνυμο της διαδικτυακής απατεωνιάς ή, στη χειρότερη περίπτωση, το «σκοτεινό» και ανώνυμο άτομο που ασκεί

[17] Nicola Tesla, interview with John B. Kennedy, 1926
https://www.businessinsider.com/tesla-predicted-smartphones-in-1926-2015-7
[18] Harold D. Lasswell, ‘’Politics: Who Gets What, When, How’’, New York: Whittlesey House, 1936.
[19] Robert Reardon and Nazli Choucri, ‘’The Role of Cyberspace in International Relations: A View of the Literature’’, Department of Political Science, MIT, Paper Prepared for the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012, p.2

τρομοκρατία ή απεργάζεται ανατρεπτικά σχέδια ή απλά παρανομεί εργαλειοποιώντας τις δυνατότητες του κυβερνοχώρου[20].

Το **Κράτος**, το πρωτεύον δομικό στοιχείο του διεθνούς συστήματος δέχεται ισχυρή μετασχηματιστική πίεση στο εσωτερικό του, λόγω της φύσης του κυβερνοχώρου που αποκάλυψε η ψηφιακή τεχνολογία και η οποία, αφού διαπεράσει το κέλυφός που διαχωρίζει το ενδοκρατικό πολιτικό χώρο από αυτόν που καταλαμβάνει ο διεθνής πολιτικός χώρος, διαμορφώνει συνθήκες μεταβολής στις σχέσεις που διαμορφώνουν ή διαταράσσουν την ισορροπία του διεθνούς συστήματος. Το Βεστφαλιανό Κράτος αποκτά μια καινούρια υποχρέωση[21], ώστε να θεωρείται ότι εκπληρώνει το σκοπό της ύπαρξής του έναντι των υπηκόων του αλλά και της θέσης του στο διεθνές σύστημα: θα πρέπει να αντιμετωπίσει τις προκλήσεις ασφαλείας που διαμορφώνει και τις τρωτότητες που αποκαλύπτει η ψηφιακή διασυνδεσιμότητα που προσφέρει ο κυβερνοχώρος.

Το **Διεθνές Σύστημα** καλείται να συμπεριλάβει και να ενσωματώσει τις μετασχηματιστικές ιδιότητες του κυβερνοχώρου, ο οποίος λόγω της φύσης του εγείρει τέτοια ζητήματα ασφαλείας που είναι δυνατό, τόσο να διαταράξουν την ισορροπία ισχύος σε παγκόσμιο ή περιφερειακό επίπεδο, όσο και να διαμορφώσουν νέα πεδία διεθνούς συνεργασίας. Ο παγκοσμιοποιητικός χαρακτήρας του Κυβερνοχώρου σε συνδυασμό με τις φύσει άπειρες διαστάσεις του δεν αποκλείεται να αποτελέσουν μελλοντικά αιτίες για δομικές μεταβολές στο ίδιο το διεθνές σύστημα, οι οποίες αφορούν όχι μόνο την κατανομή της ισχύος και την πολικότητά του αλλά και την ίδια την ύπαρξη των δομικών του στοιχείων, όπως τα γνωρίσαμε μέχρι σήμερα.

Η αναφορά βέβαια στον Άνθρωπο, στο Κράτος και στο Διεθνές Σύστημα μόνο τυχαία δεν παραπέμπει στον Kenneth N.Waltz[22]. Το μεθοδολογικό υπόδειγμα με το οποίο προσεγγίζει το πολεμικό φαινόμενο αποτέλεσε το ιδανικό μοντέλο για να αναδειχθεί ο κυβερνοχώρος και η δραστηριότητα μέσα σε αυτόν, ως η πλέον νεόκοπη και δυναμική ως προς την μεταβλητότητά της παράμετρος, η οποία διαπερνά κάθετα τα τρία επίπεδα μέσα στα οποία πλάθεται η αιτιοκρατική φύση της σύγκρουσης.

Πραγματικά, η διάσταση του κυβερνοχώρου, είτε ως χώρος παρουσίας και εκδήλωσης της ανθρώπινης θέλησης είτε ως χώρος διαδραστικής αλληλεπίδρασης μεταξύ ανθρώπων, μεταξύ μηχανών και μεταξύ ανθρώπων και μηχανών, καθίσταται πεδίο συσχέτισης, σύγκρισης, ανταλλαγής μονάδων – στοιχείων ισχύος μεταξύ των δρώντων «εν αυτώ». Αναπόδραστα λοιπόν, η αντανάκλαση της κλιμάκωσης του βαθμού έντασης, στο πλαίσιο των παραπάνω συσχετισμών, καθίσταται αντιληπτή άλλοτε ως συνεργασία και άλλοτε ως σύγκρουση. Όταν στις προαναφερθείσες συνθήκες προστεθούν και τα θεσμικά παράγωγα της ανθρώπινης θέλησης, με τους ανάλογους βαθμούς ανεξαρτησίας θέλησης που τους αποδίδεται και απολαμβάνουν κατά περίπτωση, με κορυφαίο θέσπισμα το Κράτος και τη θέλησή του, τότε ο κυβερνοχώρος, ως παράγοντας σύγκρουσης ή συνεργασίας διαπερνά με την καταλυτική του δράση το δεύτερο επίπεδο του

[20] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.16 & 25

[21] US Department of Homeland Security ''2009 Cyberspace Policy Review'', https://www.dhs.gov/publication/2009-cyberspace-policy-review

[22] Kenneth Waltz, "Ο Άνθρωπος, το Κράτος και ο Πόλεμος: Μια θεωρητική ανάλυση", Μετάφραση: Κ.Κολιόπουλος, Εισαγωγή στην Ελληνική έκδοση: Η.Κουσκουβέλης, Εκδόσεις Ποιότητα, Βάρη Αττικής, 2011, σελ 7-10 (Εισαγωγή για την Ελληνική γλώσσα, από τον Καθηγητή, Ηλία Κουσκουβέλη)

μεθοδολογικού μοντέλου του Waltz και ακουμπά το τρίτο, το επίπεδο του Διεθνούς Συστήματος. Καθίσταται λοιπόν αυταπόδεικτα νομοτελειακή η μεταχείριση του κυβερνοχώρου ως παράμετρος επιρροής και συνδιαμόρφωσης του διεθνούς περιβάλλοντος ισχύος, καθώς λειτουργεί τόσο ως πεδίο διεθνικού ανταγωνισμού, όσο και ως φορέας στοιχειωδών μονάδων ισχύος.

Βεβαίως, μία παράμετρος από μόνη της δεν μπορεί, δεν διαθέτει την απαιτούμενη κρίσιμη μάζα, δεν εμπερικλείει το επαρκές αιτιολογικό υπόβαθρο για να αποτελέσει αιτία σύγκρουσης στον φυσικό κόσμο. Γι' αυτό άλλωστε χαρακτηρίζεται ως παράμετρος. Το καλύτερο ανάλογο αποτελεί το τροχαίο ατύχημα για το οποίο η συνδυαστική ενέργεια ή απουσία ενέργειας τουλάχιστον δύο παραγόντων – παραμέτρων αποτελεί αναγκαία προϋπόθεση για να λάβει χώρα. Συναφώς, ο συνδυασμός δύο ή περισσοτέρων παραμέτρων, δύναται να αποτελέσουν τη θρυαλλίδα συγκρουσιακών φαινομένων, τα οποία ωστόσο τελικά έλκουν την αναφορά τους είτε στους συσχετισμούς ισχύος και τον ανταγωνισμό που αυτοί παράγουν, είτε στον βαθμό αλληλεξάρτησης μεταξύ των διεθνών δρώντων, ανάλογα με την προκρινόμενη θεώρηση των πραγμάτων από τους μελετητές της θεωρίας των συγκρούσεων ή τους πολιτικούς που υλοποιούν μεθόδους εφαρμογής αυτών.

Οι τρεις «εικόνες», είτε ως κατηγορίες αιτιών πολέμου, όπως τις μεταχειρίστηκε ο Waltz για να αναδείξει στην πραγματικότητα τη φύση του Διεθνούς Συστήματος ως κυρίαρχο αίτιο παραγωγής πολέμου, πλέον των κλασικών μέχρι τότε προσεγγίσεων που περιλάμβανε αποκλειστικά το δίπολο ηγέτης (άνθρωπος) – έθνος (κράτος), είτε ως επίπεδα ανάλυσης, όπως τις χρησιμοποίησαν οι μετέπειτα μελετητές για την συστηματοποίηση των προσεγγίσεών τους στα διάφορα ζητήματα που επικεντρώνονται κάθε φορά, αποτελούν ορόσημα, κατά την παραμετροποίηση των συγκρούσεων. Μια παραμετροποίηση που αποσκοπεί, όχι τόσο για την επίτευξη μιας αναγκαίας θεωρητικοποίησης ή επιστημονικής κατηγοριοποίησης ή κάποιου άλλου αναγκαίου διαχωρισμού, αλλά για την ανάδειξη και κατάδειξη της διασύνδεσης και αλληλεπίδρασης των παραμέτρων μεταξύ τους, οι οποίες συνδυαστικά παράγουν, επηρεάζουν και διαμορφώνουν τις συγκρούσεις. Μια τέτοια παράμετρος είναι και ο κυβερνοχώρος, ο οποίος θα μπορούσε κανείς να ισχυριστεί, με αρκετή δόση σκωπτικής ουσίας, ότι αποτελεί πρακτικά μια καταλυτική προσθήκη - συνεισφορά της ψηφιακής εποχής στα διεθνή πράγματα.

Τελικά, σε μια απόπειρα κυβερνοκεντρικής θεώρησης των πραγμάτων, ο κυβερνοχώρος υπάρχει, νοηματοδοτείται και λαμβάνεται υπόψη από τη μία πλευρά ως διαμορφωτική παράμετρος επιρροής και επίδρασης στα τρία επίπεδα των αιτιών σύγκρουσης, είτε οριζόντια (ξεχωριστά για κάθε επίπεδο) και κάθετα (διασυνδετικά μεταξύ των επιπέδων) και από την άλλη πλευρά και παράλληλα, ως αντικείμενο εστιασμένης μελέτης στα αντίστοιχα τρία επίπεδα ανάλυσης.

«We've arranged a society based on science and technology, in which nobody understands anything about science technology. And this combustible mixture of ignorance and power, sooner or later, is going to blow up in our faces[23]»

Carl Sagan, cosmologist, astrophysicist - biologist, author and science communicator

3. Οι Θεωρήσεις των Διεθνών Σχέσεων Συναντούν τον Κυβερνοχώρο

3.1. Η Κυρίαρχη Θεματολογία

Σύμφωνα με τους Robert Reardon και Nazli Choucri[24] πέντε είναι τα κυρίαρχα ζητήματα – προσεγγίσεις στα οποία επικεντρώνεται το ενδιαφέρον της ακαδημαϊκής και πολιτικής βιβλιογραφίας και αρθρογραφίας σχετικά με το φαινόμενο του Κυβερνοχώρου:

- Ο Κυβερνοχώρος ως δομικό στοιχείο μιας Παγκόσμιας Κοινωνίας.
- Η οικονομική δραστηριότητα στον Κυβερνοχώρο και η παγκόσμια ανάπτυξη.
- Η διακυβέρνηση του Κυβερνοχώρου.
- Ο Κυβερνοχώρος και τα απολυταρχικά καθεστώτα.
- Ο Κυβερνοχώρος και η ασφάλεια:
  - Το Διεθνικό Έγκλημα.
  - Η Διεθνής Τρομοκρατία.

	Realism	Liberalism	Constructivism	No Dominant Paradigm
Global Civil Society			• Comor (2001) • Deibert (2003) • Murphy (2009)	
Security	• Goldman (2004) • Newmyer (2010)		• Dartnell (2003) • Der Derian (2003) • Hansen & Nissenbaum (2009)	• Eriksson & Giacomello (2006)
Authoritarian Regimes		• Corrales & Westhoff (2006)		
Development		• Alden (2003)		
Governance	• Drezner (2004)	• Newman (2008)	• Farrell (2003)	• Radu (2012)
General Theory			• Herrera (2003)	• Manjikian (2010) • Greathouse (2014)

ΠΙΝΑΚΑΣ 1: Ακαδημαϊκή αρθρογραφία (Academic Journals) και αρθρογραφία για την πολιτική του κυβερνοχώρου (Policy Journals)[25]

Ωστόσο, οι θεωρητικές προσεγγίσεις των φαινομένων, που σχετίζονται με τον ένα ή τον άλλο τρόπο με τον κυβερνοχώρο, δεν μπορούν περιοριστούν στις παραπάνω

[23] https://www.wired.com/2011/05/a-day-to-remember-carl-sagan/
https://www.youtube.com/watch?time_continue=7&v=jod7v-m573k (3:26 – 3:40)

[24] Robert Reardon and Nazli Choucri, ''The Role of Cyberspace in International Relations:
A View of the Literature'', Department of Political Science, MIT, Paper Prepared for the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012

[25] Robert Reardon and Nazli Choucri, ''The Role of Cyberspace in International Relations:
A View of the Literature'', Department of Political Science, MIT, Paper Prepared for the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012, p.6 & 7.

θεματικές, καθώς αυτές είναι προφανώς ευρύτερες, με παράγωγες επιδράσεις που δεν έχουν ακόμα αποσαφηνιστεί και των οποίων οι πιθανές συνέπειες ίσως δεν είναι ακόμα καν ανιχνεύσιμες. Βέβαια, η διαπιστωθείσα επιστημονική επικέντρωση εντάσσεται μάλλον σε μια προσπάθεια πρώιμης κατηγοριοποίησης που εξυπηρετεί την συστηματική μελέτη, ωστόσο παράλληλα αντανακλά πιθανότητα και το μάλλον συγκυριακό προβάδισμα συγκεκριμένων διεθνοπολιτικών θεωρητικών προσεγγίσεων, κυρίως στον αγγλοσαξονικό κόσμο, αναγκαστικά συμπεριλαμβανομένων και των πολιτικά συγγενών τους που γράφουν στην αγγλική.

Η Roxana Radu[26] προσεγγίζει την κατανόηση των επιπτώσεων που παράγει η διάσταση του κυβερνοχώρου πάνω στις διεθνείς σχέσεις, μέσω της μελέτης των τεχνικών επαναδιαμόρφωσης της παγκόσμιας διακυβέρνησης που προσφέρει η ψηφιακή τεχνολογία και τα μέσα εικονικής πραγματικότητας (digital and virtual mediums). Φωτίζοντας αυτή τη μεταβολή στην λογική της διακυβέρνησης καθίσταται ευχερής η διερεύνηση των φαινομένων που αφορούν στην ασφάλεια στον κυβερνοχώρο.

Στην αναζήτησή του, αν οι θεωρητικοί των διεθνών σχέσεων παραμένουν επίκαιροι και πολύτιμοι ως πηγή κατανόησης των φαινομένων του πολέμου και της σύγκρουσης στο πλαίσιο του κυβερνοχώρου ή όχι, ο Craig B. Greathouse[27] υποστηρίζει τη σημασία και τη συνεισφορά στην προσπάθεια επεξήγησης των επιπτώσεων του κυβερνοπολέμου και των ζητημάτων «κυβερνοασφάλειας» στη διεθνή πολιτική σκηνή τόσο των κλασσικών, όσο και των νεότερων μελετητών, όπως ο Douhet και ο Warden.

Άλλοι μελετητές, όπως η Hannah Samir Kassab[28] εστιάζουν στην πρακτική δυνατότητα ανάπτυξης μιας αξιόπιστης επιλογής κυβερνοαποτροπής και πώς το θεωρητικό υπόβαθρο της έννοιας της αποτροπής, όπως διαμορφώθηκε μέσα από τις συμπληγάδες του ψυχροπολεμικού τοπίου μπορεί να υποστηρίξει αυτή τη στρατηγική επιλογή στο πλαίσιο του ανταγωνισμού στον κυβερνοχώρο.

3.2. Ο Κυβερνοχώρος, το Πληροφοριακό Περιβάλλον και η Θεώρηση του Ρεαλισμού

Το ρεαλιστικό πρότυπο επικεντρώνεται στην κατανομή της ισχύος μεταξύ των κρατών ως κινητήρια δύναμη στις διεθνείς σχέσεις[29] οι οποίες είναι κατά βάση ανταγωνιστικές καθώς η παγκόσμια πολιτική ορίζεται ως ο αγώνας μεταξύ των κρατών υπό συνθήκες αναρχίας για να μεγιστοποιήσουν την ασφάλειά τους και να εξασφαλίσουν την επιβίωσή τους. Επειδή τα Κράτη δεν μπορούν να βασιστούν σε μια ανώτερη αρχή για να προστατευθούν, τελικά εξαρτώνται από τις δικές τους προσπάθειες προκειμένου να

[26] Roxana Radu, ‘’Power Technology and Powerful Technologies: Global Govermentality and Security in the Cyberspace’’ [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.3-20

[27] Craig B. Greathouse, ‘’Cyber War and Strategic Thought Do the Classic Theorists Still Matter’’, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.21-40

[28] Hanna Samir Kassab, ‘’In Search of Cyber Stability: International Relations,Mutually Assured Destruction and the Age of Cyber Warfare’’ [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.59-76

[29] Ηλίας Κουσκουβέλης, ‘’Εισαγωγή στις Διεθνείς Σχέσεις, Εκδόσεις Ποιότητα, Ε’ Έκδοση, 2007

εξασφαλιστούν από τις επιθετικές προκλήσεις των άλλων κρατών που ενεργούν κατά βάση ορθολογικά και με αντίστοιχες προθέσεις και ενέργειες. Ιδιαίτερα ο νεορεαλισμός, αν και αποδέχεται ότι η ενδοκρατική πολιτική αλλά και οι μη κρατικοί – διακρατικοί θεσμοί μπορούν να διαδραματίσουν ένα ρόλο στα διεθνή πράγματα και να επηρεάσουν την συμπεριφορά των κρατών σε διεθνές επίπεδο, οι δυνάμεις αυτές δεν μπορούν να αμφισβητήσουν την υπεροχή των κρατών και των κρατικών συμφερόντων στη διεθνή πολιτική.

Ο νεορεαλιστής, James Adams αντιλαμβάνεται το Διαδίκτυο ως άναρχο σύστημα και διατυπώνει τη θέση ότι «ο Κυβερνοχώρος έχει γίνει ένα νέο διεθνές πεδίο μάχης[30]» αντανακλώντας απόλυτα το ρεαλιστικό μοντέλο ασφάλειας, συμπεριλαμβάνοντας ταυτόχρονα κρατικούς και μη κρατικούς[31] δρώντες. Στο «εικονικό» αυτό πεδίο, κάθε δρών, μόνος του ή με τους συμμάχους – «φίλους» του, τους οποίους δεν μπορεί ποτέ να εμπιστεύεται πλήρως, προσπαθεί να σωρεύσει ψηφιακή ισχύ και επιρροή και ταυτόχρονα να προστατεύσει τους ψηφιακούς και ψηφιοποιημένους συντελεστές ισχύος που ο ίδιος διαθέτει, καθώς φοβάται την υφαρπαγή ή καταστροφή τους μετά από «κυβερνοεπιθετικές» ενέργειες των δυνητικών αντιπάλων του, εφόσον καταφέρουν να διασπάσουν την δική του «κυβερνοάμυνα». Ο δομικής φύσης ψηφιακός ή καλύτερα «ψηφιακογενής» φόβος και το παράγωγο αίσθημα ανασφάλειας ενισχύεται εκθετικά από το γεγονός ότι η απόδοση ευθύνης (attribution of responsibility) και ιδιαίτερα στο πλαίσιο της διεθνούς πολιτικής η απόδοση Διεθνούς Ευθύνης[32], μπορεί να στοιχειοθετηθεί πραγματικά πολύ δύσκολα.

Ωστόσο, το διαδίκτυο και ο κυβερνοχώρος, εκτός από την τάση να καταστεί πεδίο κλασσικού ανταγωνισμού ισχύος, αποτελεί παράλληλα φύσει ενισχυτής διεθνιστικών ιδεών, του κοσμοπολιτισμού και της παγκοσμιοποίησης[33], συμβάλλοντας ενεργά και σημαντικά στην σταδιακή επικράτηση ή κατά πολλούς στη επιβολή, με όρους ψυχολογίας μαζών, μιας μεταμοντέρνας ομογενοποιημένης κουλτούρας. Η ρεαλιστική θεώρηση, μπροστά στην απειλή ενδεχόμενης κατάλυσης της φυσικής αλλά και ουσιαστικής υπόστασης του κυρίαρχου διεθνοπολιτικού δρώντα, του Κράτους, στο πλαίσιο του μετασχηματισμού της διεθνούς τάξης, είτε προς σε ένα καθεστώς παγκόσμιας διακυβέρνησης, είτε προς μια παγκόσμια απουσία κρατικής διακυβέρνησης, όπου τα Κράτη ως πολιτική βιοποικιλότητα παύουν να υπάρχουν ή υφίστανται τύποις, έχει να απαντήσει με μια νομοτελειακή νόρμα της: το «δίλημμα ασφαλείας» ή καλύτερα το «δίλημμα ανασφάλειας». Το φαινόμενο αυτό μπορεί να απαντηθεί σε δύο επίπεδα και λειτουργεί κάτω από αυτές τις συνθήκες όπως ένα επώδυνο ερέθισμα που συνεγείρει ένα νευρικό σύστημα: Το πρώτο επίπεδο αναφέρεται στο κλασσικό πρότυπο, δηλαδή στο αίσθημα ανασφάλειας στο οποίο περιέρχεται το Κράτος, το οποίο με τη σειρά του κινητοποιεί το συνακόλουθο ένστικτο της αυτοσυντήρησης – επιβίωσης[34]. Το δεύτερο επίπεδο αναφέρεται στο δίλημμα ανασφάλειας στο οποίο περιέρχεται το ίδιο το Σύστημα, όταν αυτό απειλείται υπαρξιακά και αντιδρά

---

[30] Adams, James, "Virtual Defense" Foreign Affairs Vol. 80, No. 3 (May - Jun., 2001), pp. 98-112

[31] Johan Sigholm, ‘’NON-STATE ACTORS IN CYBERSPACE OPERATIONS’’ Captain, Ph.D. Swedish National Defence College

[32] Κ.Αντωνόπουλος, Κ.Μαγκλιβέρας, ‘’Το Δίκαιο της Διεθνούς Κοινωνίας’’, Εμμανουέλα Δούση, ‘’Η Διεθνής Ευθύνη των Κρατών’’ ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ,Αθήνα,2017, Κεφ 16, σ.487 – 516,

[33] Constantine J. Petallides, ‘’Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat, 2012, VOL. 4 NO. 03
http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat

[34] Measheimer John, ‘’The tragedy of great power politics, W.W Noston & Co, N.Y. – London, 2001, p.33

(βίαια) για να εξασφαλίσει την «ορθολογική» επιβίωσή του. Είναι η επιβίωση του Συστήματος που επιβάλλει ακόμα και την μεταβολή της ίδιας της πολικότητάς του, παρά την παρατηρούμενη φυσική τάση διατήρησης και διαιώνισης, που η φύση την αποδίδει στην δύναμη της αδράνειας (inertia).

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decisionmakers or innocent victims	Protests via web page defacements or DDoS attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

ΠΙΝΑΚΑΣ 2: Πίνακας μη κρατικών δρώντων στον κυβερνοχώρο[35]

3.2.1. Το Κλασσικό «Δίλημμα Ασφαλείας»

Τα Κράτη, οι αδιαμφισβήτητοι πρωταγωνιστές στο άναρχο διεθνές περιβάλλον, το καθένα ξεχωριστά, ενώπιον μιας συνεχώς αυξανόμενης πιθανότητας μιας

[35] Johan Sigholm - Non State Actors in Cyberspace Operations, p.11
https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations

ανατροφοδοτούμενης συνολικής καταστροφής της διεθνούς εμπιστοσύνης[36] και συνεργασίας και των παράγωγων διεθνών θεσμών που συστάθηκαν ακριβώς για να τις υπηρετούν και να τις επιζητούν, αργά και σταθερά στην αρχή, ταχέως και επιταχυνόμενα στη συνέχεια, θα περιέλθουν σε συνθήκες φόβου εξαιτίας των ήδη εξελισσόμενων ή επικείμενων, άγνωστης προέλευσης μαζικών κυβερνοεπιθέσεων. Μιας ακατάπαυστης ροής κυβερνοεπιθέσεων δυνητικά εκτοξευόμενων από δεδηλωμένους εχθρούς αλλά και υποτιθέμενους «φίλους», με επακόλουθη συνέπεια την περιχαράκωση και την αναζήτηση της αναγκαίας αντιστάθμισης ως ορθολογική επιλογή. Πλέον αντιπροσωπευτικό είναι το παράδειγμα των Βαλτικών χωρών[37].

Ο James Adams, υιοθετώντας αυτόν τον «ρεαλιστικό» φόβο, επισημαίνει ότι «η συντριπτική στρατιωτική υπεροχή και η πρωτοπορία στην τεχνολογία της πληροφορίας έχουν καταστήσει τις Ηνωμένες Πολιτείες την πιο ευάλωτη χώρα στις επιθέσεις στον κυβερνοχώρο.» Από της απαρχές της διαδικτυακής ιστορίας μέχρι την πρόσφατη εμπειρία καταδεικνύεται αυτός ο κίνδυνος αλλά και οι δυσκολίες πρόληψης. Ήδη από το 1998, μια ομάδα «hackers» χρησιμοποίησε εξελιγμένα εργαλεία ηλεκτρονικών υπολογιστών για να παραβιάσει εκατοντάδες βάσεις δεδομένων της αμερικανικής κυβέρνησης, συμπεριλαμβανομένης της NASA, του Πενταγώνου και άλλων οργανισμών. Αυτή η επίθεση που ονομάστηκε «Moonlight Maze» είχε ως αποτέλεσμα την κλοπή χιλιάδων διαβαθμισμένων εγγράφων, συμβάσεων, κρυπτογραφήσεων και άλλα ευαίσθητα στοιχεία. Η μακροχρόνια έρευνα απέδωσε ελάχιστες απαντήσεις, ωστόσο τελικά διαπιστώθηκε ότι οι επιθέσεις προέρχονταν από επτά ρωσικές ηλεκτρονικές διευθύνσεις IP[38]. Χωρίς τεχνική και θεσμική υποδομή για την διερεύνηση και τη διαπίστωση της ευθύνης τέτοιων επιθέσεων κάθε κυβέρνηση και στην προκειμένη περίπτωση η αμερικανική, δεν μπορεί να είναι σίγουρη για την αθωότητα της Ρωσίας ή αντίστοιχα άλλου δυνητικού ανταγωνιστή ή δεδηλωμένου αντιπάλου και εχθρού, με αποτέλεσμα περισσότερη δυσπιστία και υποψία. Το ζήτημα δε επιβολής κυρώσεων ανεβάζει το πρόβλημα σε άλλο επίπεδο.

Πιο πρόσφατα, το περίφημο «σκουλήκι» Stuxnet έδειξε ότι οι κυβερνήσεις εξακολουθούν να είναι ευάλωτες στις επιθέσεις στον κυβερνοχώρο. Το Stuxnet φαίνεται να έχει στοχεύσει κατά κύριο λόγο στις ιρανικές πυρηνικές εγκαταστάσεις και θεωρείται από πολλούς ως το πρώτο άμεσο παράδειγμα του κυβερνοπολέμου. Στο πλαίσιο της έρευνας σχετικά με τον ιό, η «Kaspersky Labs» έκρινε ότι «η επίθεση θα μπορούσε να διεξαχθεί μόνο με κρατική στήριξη». Το γεγονός αυτό καθίσταται διπλωματικός εφιάλτης καθώς αποδεικνύει ότι ένα κράτος είναι σε θέση να επιτεθεί σε ένα άλλο, απολαμβάνοντας καθεστώς ατιμωρησίας και χωρίς να αφήνει ίχνη που να αποδεικνύουν την προέλευση της κακόβουλης επίθεσης.

Ο πειραματισμός και η αντικειμενική καταγραφή της εμπειρίας αποτελούν κρίσιμα εργαλεία επαλήθευσης και πιστοποίησης της επιστημονικής θεμελίωσης μιας θεωρίας. Το

---

[36] James Adams, ‘’Virtual Defense’’, Foreign Affairs Vol. 80, No. 3 (May - Jun., 2001), p. 98-112

[37] Andrew Radin, Hybrid Warfare in the Baltics, Threats and Potential Responses, RAND Corporation, Santa Monica, Calif. 19 Oct 2015

[38] Chris Doman, ‘’ The First Cyber Espionage Attacks: How Operation Moonlight Maze made history’’, A Medium Corporation, Jul 7, 2016
https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7
https://securelist.com/penquins-moonlit-maze/77883/

ιστορικό παράδειγμα της κούρσας των εξοπλισμών κατά τη διάρκεια του Ψυχρού Πολέμου και του συνακόλουθου οδυνηρού αποτελέσματος για την ηττημένη πλευρά προέκρινε στρατηγικές εκμετάλλευσης των πλεονεκτημάτων που προσφέρει η κατάλληλη διαχείριση μιας παλέτας ασύμμετρων υβριδικών δυνατοτήτων (δόγμα Γερασίμωφ[39]), στην κατάλληλη κάθε φορά αναλογία, που εξασφαλίζουν στον χρήστη κυρίως οικονομία κλίμακας και σχεδόν ασυλία ή έστω σημαντική δυσχέρεια στη απόδοση ευθυνών (attribution). Κανείς δεν θα ήταν αρκετά ανόητος για να προσπαθήσει να ξεκινήσει έναν αγώνα εξοπλισμών για να ξεπεράσει τις ΗΠΑ στις αμυντικές δαπάνες, απεναντίας η ρεαλιστική θεώρηση, σύμφωνα με τον Adams, εκτιμά πως οι εχθρικές προς τις ΗΠΑ χώρες θα αρχίσουν ή θα εντείνουν τις προσπάθειές τους για την ανάπτυξη τέτοιων δυνατοτήτων που θα τους δώσουν ένα ασύμμετρο πλεονέκτημα και ενδεχομένως να διαμορφώσουν συνθήκες νίκης χωρίς να απαιτηθεί να πυροδοτήσουν έστω και ένα μόνο βλήμα. Προχωρώντας ακόμα ένα βήμα, για την αντιμετώπιση του νέου αυτού είδους απειλών, ο Adams καλεί το Αμερικανικό Υπουργείο Άμυνας να εξασφαλίσει τη θεσμική κατοχύρωση αλλά και τις τεχνικές δυνατότητες να παρακολουθεί το Διαδίκτυο σε βάρος ακόμα και ορισμένων πολιτικών ελευθεριών, στη βάση της διασφάλισης υπέρτερου αγαθού. Το «Moonlight Maze» αποτελεί «απλά μια γεύση από τους κινδύνους που έρχονται» μπροστά στο ενδεχόμενο να «μολυνθούν» αμυντικά συστήματα, δημόσιες υποδομές, εταιρικά και οικονομικά συστήματα και να εξαπλωθεί κυριολεκτικά το χάος.

3.2.2. Το Συστημικό «Δίλημμα Ασφαλείας»

Στο συστημικό επίπεδο, η απειλή κατάλυσης της δομικών συστατικών του διεθνούς συστήματος, δηλαδή των ίδιων των κρατών και της κατανομής ισχύος μέσα στην οποία ενυπάρχουν και ισορροπούν οι σχέσεις μεταξύ τους, ευαισθητοποιεί και κινητοποιεί τα ανακλαστικά επιβίωσης του ίδιου του συστήματος. Υφίσταται όμως τέτοιου είδους υπαρξιακή, συστημική απειλή; Πρακτικά, η ρεαλιστική θεώρηση και το ιστορικό προηγούμενο εισηγείται ως τέτοια απειλή την Παγκόσμια Ηγεμονία. Την μονοκρατορία. Μια παγκόσμια μορφή διακυβέρνησης, για την οποία τελικά δεν έχει σημασία, ούτε ενδιαφέρει το είδος, η μορφή ή το όνομά της αλλά το γεγονός ότι καταλύει ουσιαστικά το διεθνές σύστημα. Μπορεί να συσχετιστεί ο κυβερνοχώρος και τα φαινόμενα που λαμβάνουν χώρα μέσα σε αυτόν, αλλά και αυτά που συνδέονται έμμεσα με αυτόν, με αιτίες για τέτοιου επιπέδου δομικές ανατροπές;

Άραγε, πόσο μακριά βρίσκεται το διεθνές σύστημα από μία πραγματικότητα όπου η κατηγοριοποίηση των φορτίων ισχύος δεν θα αναφέρεται σε άυλα και υλικά, αλλά σε ψηφιακά και ψηφιοποιημένα; Μήπως οι χώρες που πρωτοπορούν στον τομέα της ψηφιακής τεχνολογίας δεν διαισθάνθηκαν πρώτες τον μυθολογικό φόβο της απώλειας που ένιωσαν οι αρχαίοι θεοί, όταν έπεσαν για πρώτη φορά θύματα των ανταγωνιστών «κυβερνο-Προμηθέων» (Hackers) που επιζητούσαν και σίγουρα στο προβλέψιμο μέλλον θα συνεχίζουν να επιζητούν πρόσβαση στα ψηφιακά «καυτά» μυστικά, σε μια προσπάθεια κατάλυσης ή αποτροπής μιας κρατικού χαρακτήρα μονοπωλιακής ψηφιακής ηγεμονίας; Ποιες πιθανότητες επιφυλάσσει το μέλλον του ανταγωνισμού στον κυβερνοχώρο στις

[39] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," In Moscow's Shadow (blog), July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

προσπάθειες τυχόν αυτονόμησης των σημερινών ή αυριανών mega-πολυεθνικών[40] εταιρειών που οδηγούν τις εξελίξεις στον τομέα της υψηλής – ψηφιακής τεχνολογίας, ώστε να καταστούν ανταγωνιστές ισχύος των εθνικών κρατών, αρχικά των πιο αδύναμων ή ευάλωτων, επιβάλλοντας τελικά την κυριαρχία τους, όπως το οραματίστηκε ο Γκίμπσον[41]. Αν αυτό θα μπορούσε να καταστεί δυνατό για διάφορους λόγους που προς το παρόν δεν είναι ίσως καν εφικτό να διατυπωθούν, γιατί τότε να μην καταστεί πιθανή και μια πιο μεσοπρόθεσμη υβριδική σύμπραξη μεταξύ οικονομικών τεχνολογικών κολοσσών με Κράτη εναντίων άλλων μεμονωμένων Κρατών ή Συνασπισμού / Συμμαχίας Κρατών ή άλλων υβριδικών συμπράξεων;

3.2.3. Αποτροπή στον Κυβερνοχώρο και Διάδοση Κυβερνοόπλων

Αναφερόμενοι ωστόσο σε ψηφιακά μυστικά, το ψυχροπολεμικό περιβάλλον της πυρηνικής ισορροπίας, την οποία κάποιοι την χαρακτήρισαν ισορροπία του «τρόπου», έρχεται να μας υπενθυμίσει τις θεωρίες πυρηνικής αποτροπής, οι οποίες για να λειτουργήσουν αποτελεσματικά δηλαδή εξισορροπητικά, αναπόφευκτα κατέληξαν σε μια βασική στρατηγική αναγκαιότητα: την απαγόρευση της διάδοσης των πυρηνικών όπλων. Εν πολλοίς, η θεωρία της αποτροπής ορίζει ότι όσο το κόστος της ανάληψης επιθετικής δράσης παραμένει υψηλό ενόσω το αντίστοιχο κόστος της ανάπτυξης ικανής αμυντικής διάταξης παραμένει χαμηλό, η ισορροπία διατηρείται. Επεκτείνοντας την επιχειρηματολογία στο κυβερνοχώρο, η Hannah Samir Kassab[42] υποστηρίζει ότι για τη διατήρηση της ασφάλειας της τεχνολογίας της πληροφορικής, θα πρέπει να αναπτυχθούν συστήματα κυβερνοάμυνας που να ανταποκρίνονται στις αρχές τις κλασσικής θεωρίας της αποτροπής. Οι κυβερνοεπιθέσεις είναι δυνατό να αποτραπούν εάν ένα κατάλληλο σύστημα, ένας «τοίχος» προστασίας από ψηφιακούς ιούς, εγκατασταθεί για να αντιμετωπίσει τις προσπάθειες ψηφιακής διείσδυσης στα αμυντικά συστήματα ενός κράτους, καθιστώντας ταυτόχρονα την υπόψη κυβερνοεπίθεση ιδιαίτερα κοστοβόρα γι' αυτόν που την αποφάσισε. Ακολουθώντας το παράδειγμα της στρατηγικής της Αμοιβαίας Εξασφαλισμένης Καταστροφής, το κόστος αυτό για να αποκτήσει χαρακτήρα αποτρεπτικό θα πρέπει η πιθανότητα εκδήλωσης μιας εχθρικής κυβερνοεπίθεσης να ανταπαντάται με μια, δεδηλωμένης ικανότητας, ανώτερη ποιοτικά και συντριπτική για τα εχθρικά ψηφιακά συστήματα, αντίδραση[43].

Μέχρι σήμερα, τα κυβερνοόπλα που αναπτύχθηκαν χρησιμοποιήθηκαν με τρόπο επιθετικό. Ήταν η επιλογή της Επίθεσης που κατεύθυνε στην πρόθεση ανάπτυξης των κυβερνοόπλων, καθώς ο εύκολος εντοπισμός των ψηφιακών κενών ασφαλείας των δυνητικών εχθρών σε συνδυασμό με το μικρό σχετικά κόστος κατασκευής, διατήρησης της μυστικότητας ύπαρξης, αλλά και απόκρυψης της ταυτότητας της πηγής – θέσης «βολής», αποτέλεσε και συνεχίζει να αποτελεί ετεροβαρής παράγοντας στους τακτικούς και

[40] Rob Boffard, ''Could An Evil Mega-Corporation Ever Exist In Real Life?'' https://io9.gizmodo.com/could-an-evil-mega-corporation-ever-exist-in-real-life-1630401831

[41] William Gibson, ''Neuromancer'', edited by Terry Carr, 1984

[42] Hannah Samir Kassab, "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare, [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.59-76

[43] Ηλίας Κουσκουβέλης, ''Θεωρία Διεθνών Σχέσεων στον Ψυχρό Πόλεμο, Αποτροπή και Πυρηνική Στρατηγική", Εκδόσεις Ποιότητα, Β' Έκδοση, Αθήνα, 2000, σελ 139-171

στρατηγικούς υπολογισμούς κόστους – οφέλους. Σύμφωνα με την Salma Shaheen[44], η πιθανότητα να αναπτύξουν κυβερνοόπλα όλο και περισσότερα κράτη συνεχώς μεγαλώνει. Άλλωστε, το θύμα μιας κυβερνοεπίθεσης με σχετική ευκολία μπορεί να χρησιμοποιήσει τα ίχνη του κυβερνοόπλου που το έπληξε για να αναπτύξει το δικό του, πιθανότατα πιο ισχυρό, αντίστοιχο όπλο, συμβάλλοντας ουσιαστικά στην διάδοση και εξέλιξη της δυνατότητας αυτής. Σε εφαρμογή της θεωρίας της ισορροπίας Επίθεσης – Άμυνας, χωρίς αντίστοιχη ανάπτυξη αμυντικού χαρακτήρα κυβερνοόπλων, ο υφιστάμενος επιθετικός χαρακτήρας τους λειτουργεί αποσταθεροποιητικά για τη διεθνή ασφάλεια. Σε συνδυασμό με μια κονστρουκτιβιστικού χαρακτήρα προσπάθεια περιορισμού της διάδοσης τους είναι δυνατό να περιοριστούν τουλάχιστον τα φαινόμενα ανεξέλεγκτης κλιμάκωσης των «κυβερνοσυγκρούσεων».

Θα μπορούσε να ισχυριστεί κανείς ότι είναι εντυπωσιακό το γεγονός ότι για ένα περιβάλλον τεχνολογικής αιχμής, όπως ο κυβερνοχώρος, εντοπίζονται στοιχεία αναλογικότητας με έννοιες που έχουν διερευνηθεί διεξοδικά στο πρόσφατο παρελθόν, όπως η πυρηνική αποτροπή, οι οποίες όμως βασίζονται σε κλασσικές θέσεις όπως αυτή του Κλαούζεβιτς περί της φύσης του πολέμου. Ο πόλεμος, κατά το Κλαούζεβιτς, είναι μια πράξη δύναμης με σκοπό τον εξαναγκασμό του αντιπάλου μας να εκπληρώσει την δική μας θέληση[45] (*War is [thus] an act of force to compel our enemy to do our will*). Μέσα στο υπόψη ορισμό εμπεριέχονται οι έννοιες της βίας («πράξη δύναμης»), ο επιτιθέμενος (του αντιπάλου «μας»), το θύμα (του «αντιπάλου» μας), το ζητούμενο (τον «εξαναγκασμό») και ο σκοπός («να εκπληρώσει τη δική μας θέληση»). Υπάρχει ακόμα ένα στοιχείο που συνάγεται και είναι ο λόγος, η αιτία της σύγκρουσης, δηλαδή η ύπαρξη μιας «διαφοράς» μεταξύ των αντιπάλων πλευρών, η οποία αντικειμενοποιείται από την «ανάγκη εξαναγκασμού για την επίλυσή της»[46]. Παρά το γεγονός ότι ο Κλαούζεβιτς δεν θα μπορούσε να είχε την παραμικρή ιδέα περί κυβεροπολέμου, ωστόσο ο αποστεωμένος ορισμός που εισηγείται για τον πόλεμο - αυτή ακριβώς είναι και η αξία του ορισμού του ως προϊόν της θεωρίας περί πολέμου – έχει εκπληκτική εφαρμογή για να ορίσει και να αποσυναρμολογήσει τα στοιχεία τα οποία συνθέτουν την έννοια του κυβερνοπόλεμου, στον πυρήνα του. Βέβαια, τα θεωρητικά αλλά και πρακτικά ζητήματα που εγείρονται κατά τη μελέτη του φαινομένου των κυβερνοσυγκρούσεων απέχουν από την υπεροχή της απλότητας με την οποία περιγράφεται η φύση του πολέμου, με σημαντικότερη ίσως δυσχέρεια την υπόδειξη ενός ορισμού, περί του τι αποτελεί πράξη πολέμου στον κυβερνοχώρο, ο οποίος παράλληλα θα απολαμβάνει καθολικής αποδοχής.

---

[44] Salma Shaheen, "Offence – Defense Balance in Cyber Warfare, [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.77-93

[45] Carl Von Clausevitz, "On War", Edited and Translated by M.Howard and P.Papet, Princeton University Press, New Jersey, 1989, p.75

[46] Sascha Knoepfel, "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War, [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.119

3.3. Ο Κυβερνοχώρος, το Πληροφοριακό Περιβάλλον και η Νεοφιλελεύθερη Θεώρηση

Στη νεορεαλιστική σχολή εντοπίζονται σχετικές αδυναμίες στην αντιμετώπιση των ζητημάτων ασφαλείας και τρομοκρατίας στον κυβερνοχώρο. Καθώς στο πεδίο μάχης του κυβερνοχώρου, οποιοσδήποτε είναι σε θέση να διεξάγει μια επίθεση, η αντικειμενική εξέταση των γεγονότων, που λαμβάνουν χώρα στο υπόψη περιβάλλον, αναγκαστικά συμπεριλαμβάνει την ανάλυση, αξιολόγηση, εξαγωγή συμπερασμάτων και τελικά απόδοση ευθύνης τόσο σε κρατικούς, όσο και σε μη κρατικούς δρώντες. Μπορεί, τουλάχιστον προς το παρόν, οι μη κρατικοί δρώντες να διαθέτουν σχετικά περιορισμένες δυνατότητες, οικονομικούς πόρους και τεχνολογική γνώση για να διεξάγουν κλασικούς συμβατικούς πολέμους, ωστόσο αυτό σε καμία περίπτωση δεν ισχύει στον τομέα του πληροφοριακού περιβάλλοντος και ιδιαίτερα στον κυβερνοχώρο. Ομοίως, η στρατηγική πρώτου – προληπτικού χτυπήματος που θα προδιαγράφει την συντριπτική ήττα του αντιπάλου τείνει να μην έχει καν νόημα στον κυβερνοχώρο, καθώς πρακτικά είναι αδύνατο να απαγορευθεί στον ή στους αντιπάλους να μην ανταποδώσουν με μια εξίσου μαζική αντεπίθεση.

Η αξία των καθεστώτων συνεργασίας στα θέματα που αφορούν στο περιβάλλον του κυβερνοχώρου τίθεται προς διερεύνηση από τους Eriksson και Giocomello[47]. Τονίζουν την αδυναμία των Κρατών να αντιμετωπίσουν κατά μόνας τα ζητήματα κυβερνοασφάλειας και την σημασία της συνεργασίας για τον περιορισμό της απειλής από τις κυβερνοεπιθέσεις. Ωστόσο, η πρακτική υλοποίηση της καθαρά ιδεαλιστικής αυτής άποψης προσκρούει στη δεινή πραγματικότητα. Τα Κράτη αρνούνται να συμπράξουν και να συνεργήσουν, καθώς προϋπόθεση μιας τέτοιας συνεργασίας αποτελεί καταρχήν η αποδοχή των μη κρατικών δρώντων στο ίδιο τραπέζι. Και αν αυτό φαντάζει εφικτό με βάση την ιστορική εμπειρία, η προϋπόθεση που κυριολεκτικά δοκιμάζει τα όρια ανοχής είναι το γεγονός ότι όλοι οι συνεργαζόμενοι δρώντες θα πρέπει να προσφέρουν και να αποκαλύψουν, προς χάριν του κοινού οφέλους, τις δυνατότητές τους, τις μεθόδους τους και εντέλει να παραχωρήσουν μέρος της κυριαρχίας τους, στο όνομα της αναγκαίας επιχειρησιακής διαφάνειας και της στρατηγικής εμπιστοσύνης μεταξύ όλων των συμβαλλόμενων μερών.

Παρά τις κοινά αποδεκτές δυσχέρειες που αντιμετωπίζει η διεθνής συνεργασία στα ζητήματα ασφάλειας στο κυβερνοχώρο, οι προσπάθειες για διεύρυνσή της, μέσω του τομέα της ασφάλειας των δικτύων[48], επικεντρώνονται στην προώθηση της ανάπτυξης της κοινής πολιτικής κυβερνοασφάλειας στο πλαίσιο διεθνών οργανισμών, όπως ο Οργανισμός για την Ανάπτυξη και Συνεργασία στην Ευρώπη (ΟΑΣΕ) και ο Διεθνής Οργανισμός Τηλεπικοινωνιών, οι οποίοι στον πυρήνα της δραστηριοποίησής τους, μεταξύ άλλων, είναι η από κοινού αντιμετώπιση των ζητημάτων που αποτελούν εμπόδια στη ροή ανθρώπων, πληροφοριών και κεφαλαίων μεταξύ των μελών τους. Σύμφωνα με τον Bajaj «η ασφάλεια στον κυβερνοχώρο δεν είναι ένα τεχνολογικό πρόβλημα που μπορεί να λυθεί. Είναι ένας κίνδυνος που πρέπει να τον διαχειριστεί ο συνδυασμός αμυντικής τεχνολογίας, έξυπνης

[47] Johan Eriksson and Giampiero Giacomello, “The Information Revolution, Security, and International Relations”, International Political Science Review / Revue internationale de science politique, Vol. 27, No. 3 (Jul., 2006), pp. 221-244

[48] S.D.McDowell et al., “Cooperative International Approaches to Network Security”, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.231-252

ανάλυσης, πληροφοριακού πολέμου και παραδοσιακής διπλωματίας»[49]. Μεταξύ των κρατών, το σημείο σύγκλισης των κινήτρων για ενίσχυση της κυβερνοασφάλειάς τους από κοινού, αποτελεί η αντιμετώπιση των απειλών που προέρχονται από μη κρατικούς δρώντες. Σύμμαχους στην προσπάθεια αυτή θα βρουν τις μεγάλες εμπορικές εταιρείες, καθώς το κόστος της επένδυσης για την ανάπτυξη και βελτίωση της τεχνολογικής υποδομής είναι πολύ υψηλό, είτε αφορά πιο ασφαλές και ανθεκτικό στις κυβερνοεπιθέσεις "hardware" είτε "software", ενώ το όφελος της συνεργασίας επιμερίζει την καταβολή της αναγκαίας προσπάθειας ανεξάρτητα αν αυτή αντιστοιχεί σε χρόνο, χρήμα ή ανθρώπινο δυναμικό. Η διεθνής συνεργασία μπορεί να ευδοκιμήσει σε πολλούς τομείς και ήδη υφίσταται σε διαφορετικό βαθμό στους παρακάτω[50]:

- Συνεργασίες και συμπράξεις πάνω στις επικοινωνιακές και πληροφοριακές υποδομές δημόσιου και ιδιωτικού τομέα στο πλαίσιο των εθνικών κέντρων διαχείρισης κόμβων.
- Συνεργασία των παγκόσμιων παρόχων διαδικτυακών υπηρεσιών όπως η Google, η Microsoft, το Twitter, το Yahoo και το Facebook με τις εκάστοτε κρατικές και διεθνείς αρχές επιβολής του νόμου.
- Συνεργασία των Ομάδων Απόκρισης Έκτακτης Ανάγκης (Computer Emergency Response Teams, CERT) για την ανταλλαγή δεδομένων με ανοιχτό τρόπο σχετικά με απειλές και τρωτότητες για τη δημιουργία ενός συστήματος παρακολούθησης και έγκαιρης προειδοποίησης.
- Συνεργασία στη διαχείριση περιστατικών κυβερνοεπιθέσεων και ανταλλαγή πληροφοριών με σκοπό την οικοδόμηση ενός διεθνούς συστήματος αντίδρασης σε τέτοια περιστατικά.
- Συνεργασία στην προστασία κρίσιμων υποδομών με τη δημιουργία διεθνούς φορέα πιστοποίησης του επιπέδου ασφάλειας των υποδομών ζωτικής σημασίας έναντι κυβερνοαπειλών.
- Συνεργασία στην ανταλλαγή και ανάπτυξη βέλτιστων πρακτικών για την ασφάλεια στον κυβερνοχώρο.
- Συνεργασία στη δημιουργία πνεύματος εγρήγορσης έναντι των κυβερνοαπειλών στο πλαίσιο συστήματος παρακολούθησης και έγκαιρης προειδοποίησης για κυβερνοεπιθέσεις.
- Συνεργασία για την εισαγωγή ενός κοινά αποδεκτού νομικού πλαισίου για την αντιμετώπιση εγκλημάτων στον κυβερνοχώρο, που αφορούν στην εδαφική αρμοδιότητα και στη διεθνή ευθύνη που εκπηγάζει από την άσκηση κυριαρχίας.

3.4. Ο Κυβερνοχώρος, το Πληροφοριακό Περιβάλλον και ο Κονστρουκτιβισμός

Η κονστρουκτιβιστική σχολή των διεθνών σχέσεων επικεντρώνεται στον ρόλο που παίζουν οι ιδέες, τα σύμβολα και τα διεθνή και περιφερειακά καθεστώτα στη διαμόρφωση των κρατικών προτεραιοτήτων και ακολούθως στην ίδια την συμπεριφορά των Κρατών. Στο

[49] Kamlesh Bajaj, "The Cybersecurity Agenda, Mobilizing for International Action, The EastWest Institute, New York, 2010, p.i - ii
https://www.eastwest.ngo/sites/default/files/ideas-files/Bajaj_Web.pdf

[50] Kamlesh Bajaj, "The Cybersecurity Agenda, Mobilizing for International Action, The EastWest Institute, New York, 2010, p.9.

πλαίσιο αυτό, έχει μάλλον καθιερωθεί ως θεμελιώδες αξίωμα της θεώρησης το γεγονός ότι το διαδίκτυο δεν αποτελεί απλά ένα μέσο διακίνησης πληροφοριών. Είναι ένας κοινωνικοπολιτικός εξισωτής (equalizer) που διαμορφώνει την ταυτότητά του από τους χρήστες του αλλά και διαμορφώνει την ταυτότητα αυτών με συνέπεια να επηρεάζει το χαρακτήρα του πληροφοριακού περιβάλλοντος και τον κόσμο των ιδεών που ενυπάρχει σε αυτό. Ο δε κυβερνοχώρος καθίσταται το καλύτερο πεδίο αποτύπωσης αλλά και το μέσο οπτικοποίησης της αέναης διάδρασης και αλληλεξάρτησης κρατικών και μη κρατικών δρώντων. Βέβαια, όχι και τόσο αναπάντεχα, ο ιδεαλισμός της κονστρουκτιβιστικής θεώρησης δεν δίνει πειστικές απαντήσεις στα εγειρόμενα διλήμματα ασφαλείας και κυρίως σε ότι αφορά τις κακόβουλες επιθέσεις που προέρχονται από μη κρατικούς δρώντες και οι οποίες στρέφονται εναντίων άλλων κρατικών ή μη κρατικών δρώντων αλλά και εναντίων ιδιωτών. Πέραν των ζητημάτων αντιμετώπισης της εγκληματικής και τρομοκρατικής δράσης είναι εμφανής η αδυναμία να προσφερθούν λύσεις και στην αντιμετώπιση εχθρικών διαθέσεων και ιδεών που μπορεί είτε να προκύψουν, είτε να επαναπροσδιοριστούν ενώ είχαν ήδη ιστορικά καταδικαστεί κατά την εξέλιξη του πολιτικού πολιτισμού και οι οποίες μπορούν να είναι εξίσου επιζήμιες (χιτλερικός εθνικοσοσιαλισμός, σταλινικός κομμουνισμός, κλπ).

Σε μια προσπάθεια να συλληφθεί εννοιολογικά και να ακτινογραφηθεί η δομή και ο χαρακτήρας του κυβερνοχώρου, η Katharina C.Below[51] εισηγείται ότι η δομή της ισχύος και η βία στον κυβερνοχώρο μπορεί αφαιρετικά να σκιαγραφηθεί διαχωρίζοντάς τον σε δύο μέρη, σε αντιστοιχία προς τις αντιλήψεις της Arendt περί ισχύος ως «δύναμη για να» και περί βίας «ως δύναμη πάνω σε». Ο κυβερνοχώρος λοιπόν στην ολότητά του είναι και τα δύο. Ένας μοντέρνος χώρος για να δηλώσει κανείς την παρουσία του, ένας χώρος πολιτικής ελευθερίας και ένα ανεξερεύνητο περιβάλλον ισχύος καθώς, επίσης ένας αντι-χώρος παρουσίας, ένας χώρος πλήρης από την «αρέντια» αντίληψη περί βίας, η οποία αρνείται την θετική απόδοση ευθύνης. Ενός χώρου όπου η παρουσία δεν δηλώνεται ή αποκρύπτεται όταν εφαρμόζονται φίλτρα και τεχνικές ελέγχου – απόκρυψης. Αξίζει να σημειωθεί ότι για την Arendt η ισχύς εκδηλώνεται – ευδοκιμεί (springs up) όταν οι άνθρωποι ενωθούν και ενεργήσουν από κοινού[52]. Ο χώρος αυτός δεν χρειάζεται θεσμικές δομές για να υλοποιηθεί, αλλά μια αυτόνομη δικτυακή συσχέτιση (networking association) ατόμων, ελεύθερων, ίσων και αυτοδιοικούμενων, που συμμετέχουν με ποικιλία απόψεων οι οποίες εκφράζονται με τα διαθέσιμα μέσα του λόγου.

Βέβαια, παρά την εξιδανικευμένη και εν πολλοίς ουτοπική προσέγγιση, ενός κόσμου συγκροτημένου περίπου ως σύνολο πόλεων – κρατών, όπου ίσοι πολίτες ενεργούν από κοινού ώστε να συζητήσουν και να διαπραγματευτούν ζητήματα πολιτικού σκοπού, το παράδειγμα τη Αραβικής Άνοιξης έδειξε ότι οι σχέσεις ισχύος, που δημιουργήθηκαν μέσα στον κυβερνοχώρο, μπορούν να μετεξελιχθούν σε βίαιες πράξεις στον μη ψηφιακό κόσμο. Φανταστείτε λοιπόν τι ενδεχομένως θα μπορούσε να δοκιμάσει ο πραγματικός κόσμος όταν στην διαδικτυακή «συζήτηση» ενταχθεί η τεχνητή νοημοσύνη με επιταχυνόμενη ικανότητά αυτοτροφοδοτούμενης ανάπτυξης της επιχειρηματολογίας, στο πλαίσιο μιας υβριδικής

[51] Katharina C. Below, "The Utility of Timeless Thoughts: Hannah Arendt's Conceptions of Power and Violence in the Age of Cyberization", [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.95-114

[52] Hannah Arendt, "On violence", New York, Harcourt Brace Javanovich, 1970, p.52

συζήτησης με την τετελεσμένης μαθησιακής ικανότητας ή έστω περιορισμένης ικανότητας συνειδητής επεξεργασίας δεδομένων του μέσου ανθρώπου.

«If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology[53]»

Bruce Schneier, cryptographer, computer security professional & writer

4. Ψηφιακές Προκλήσεις Ασφαλείας

4.1. Εκφάνσεις και Συνέπειες

4.1.1. Νομιμότητα και Τάξη vs Παρανομία και Αταξία

Τι είναι νόμιμο και τι παράνομο στον Κυβερνοχώρο. Τι είναι ανεκτό και τι όχι στον κυβερνοχώρο. Τι είναι τρομοκρατική και τι εγκληματική διαδικτυακή δράση. Τι είναι διαδικτυακό έγκλημα και τι διαμαρτυρία. Τι είναι κυβερνοπόλεμος και τι «κυβερνοειρήνη». Τελικά, αυτό που αποκτά αντικειμενική αξία είναι η διαπίστωση ότι το διαδίκτυο θολώνει ακόμα περισσότερο τα όρια και τις διαχωριστικές γραμμές των υφιστάμενων κονστρουκτιβιστικού[54] χαρακτήρα κοινωνικών, πολιτικών και ηθικών θεσπισμάτων. Είναι αυτό ακριβώς το σημείο από το οποίο εκπηγάζει ο φόβος που στοιχειοθετεί την απειλή και που τα Κράτη σπεύδουν να την αντιμετωπίσουν, να την περιορίσουν, να την κατανοήσουν, να την περιγράψουν και τελικά να την ελέγξουν. Στην επισκόπηση[55] της πολιτικής για τον κυβερνοχώρο του Αμερικανικού Υπουργείου Εσωτερικής Ασφάλειας για το έτος 2009 η αμερικανική κυβέρνηση διατυπώνει ξεκάθαρα τον φόβο της και την αίσθηση της απειλής: «*Ο κυβερνοχώρος αγγίζει σχεδόν τα πάντα και όλους. Παρέχει μια πλατφόρμα καινοτομίας και ευημερίας και τα μέσα για τη βελτίωση της γενικής ευημερίας σε ολόκληρο τον κόσμο. Αλλά με την ευρεία εμβέλεια μιας χαλαρής και ελαφρώς ρυθμιζόμενης ψηφιακής υποδομής, μεγάλοι κίνδυνοι απειλούν τα έθνη, τις ιδιωτικές επιχειρήσεις και τα ατομικά δικαιώματα*». Είναι δηλαδή το θολό τοπίο που διαμορφώνει η «χαλαρή» και η «ελαφρώς ρυθμιζόμενη ψηφιακή υποδομή» που σχηματοποιεί τους λόγους για τους οποίους το Κράτος αναγκάζεται να παρέμβει και να ασκήσει τη βασική υποχρέωση έναντι των υπηκόων του, αυτή της προστασίας.

Οι «*Anonymous*» είναι η πρώτη διαδικτυακή υπερσυνειδητότητα[56]. Τα μέλη δεν γνωρίζονται μεταξύ τους και πρακτικά καθίστανται μέλη μόνο όταν εργάζονται συλλογικά για την επίτευξη κάποιου στόχου. Αρχικά, η ομάδα ήταν υπεύθυνη για μικρές διαδικτυακές αψιμαχίες και την μόλυνση με ενοχλητικούς ιούς υπολογιστών, αλλά έκτοτε εξελίχθηκε σε έναν απρόσωπο υπερασπιστή της ουδετερότητας του δικτύου και της ελευθερίας της πληροφόρησης. Το φαινόμενο «*Anonymous*» καταδεικνύει πώς ένας μη κρατικός δρώντας

---

[53] Bruce Schneier, ''Secrets and Lies, DIGITAL SECURITY IN A NETWORKED WORLD", Wiley Publishing, Inc., Indianapolis, Indiana, 2004, p.xxii

[54] Anne-Marie Slaughter, Thomas Hale, ''International Relations, Principal Theories'', Published under the auspices of the Max Planck Foundation for International Peace and the Rule of Law under the direction of Rüdiger Wolfrum, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011
www.mpepil.com
http://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e722?rskey=ePM79E&result=1&prd=OPIL

[55] US Department of Homeland Security, ''2009 Cyberspace Policy Review'',
https://www.dhs.gov/publication/2009-cyberspace-policy-review

[56] Landers, Chris, "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)". Baltimore City Paper, 04 Apr 2008

μπορεί να προωθήσει και να αγωνιστεί για ένα ιδεώδες μέσω του Διαδικτύου και να έχει πραγματικό παγκόσμιο αντίκτυπο. Η διαδικτυακή αυτή οργάνωση έχει στο ενεργητικό της κυβερνοεπιθέσεις σε επίσημες ιστοσελίδες κοινοβουλίων (πχ Αυστραλία 2010), πολιτικές διαδικτυακές παρεμβάσεις τόσο εναντίων ηγετών δημοκρατικών χωρών όσο και αυταρχικών καθεστώτων (πχ διαμαρτυρίες του Κόμματος των Πράσινων στο Ιράν το 2009), παροχή ψηφιακών διευκολύνσεων για την παράκαμψη κρατικών περιορισμών πρόσβασης στο διαδίκτυο (εντολή διαδικτυακής λογοκρισίας από τον Ιρανό Πρόεδρο Αχμαντινετζάντ για να παρακωλύσει την ικανότητα διαδηλωτών να οργανωθούν), εξασφάλιση διαδικτυακής άμυνας για την προστασία διακομιστών και διαδικτυακών υπηρεσιών για τις οποίες κρατικοί φορείς εξασφάλισαν με δικαστικές εντολές την παύση τους (υπόθεση WIKILEAKS), δράσεις αντεκδίκησης για αποφάσεις που αφορούν στην επιχειρηματική πολιτική εμπορικών κολοσσών κλπ.

Η Αυστραλία και το Ιράν καταδίκασαν αμφότερες τις ενέργειες των «*Anonymous*» ως τρομοκρατία στον κυβερνοχώρο και προσπάθησαν να συλλάβουν τους εμπλεκόμενους, αλλά δεν μπόρεσαν να εντοπίσουν κανέναν ύποπτο. Χωρίς επίσημους ηγέτες, εκπροσώπους ή χώρους συνάντησης τέτοιες ομάδες διαδικτυακής δράσης είναι αδύνατο να αντιμετωπισθούν και να νικηθούν με συμβατικές μεθόδους και μέσα.

Η επαναστατική μετασχηματιστική δύναμη του διαδικτύου γίνεται αντιληπτή με τις τάσεις που ήδη τροχοδρομούν για να ορίσουν πολύ σύντομα την καθημερινότητα σε βαθμό απόλυτο. Ζούμε σε έναν καλωδιωμένο[57] κόσμο. Οι συνθήκες απόλυτης εξάρτησης είναι η μόνη ξεκάθαρη ιδέα μεταξύ του φυσικού κόσμου και του «κυβερνοκόσμου», όπου ο ψηφιακός κώδικας προγραμματισμού θολώνει την διαχωριστική γραμμή. Από τις χρηματοπιστωτικές συναλλαγές μέχρι τη διακίνηση στρατιωτικών δυνάμεων, από την ομαλή κατανομή της ηλεκτρικής ενέργειας μέχρι την παρακολούθηση της υποθαλάσσιας σεισμικής δραστηριότητας για την έγκαιρη προειδοποίηση επερχόμενων τσουνάμι, από την διαχείριση των αερομεταφορών μέχρι την ανάπτυξη της τέχνης και της τεχνολογίας η νέα κυβερνοπραγματικότητα ορίζει ήδη τον ανθρώπινο πολιτισμό.

Η ευημερία, η δημόσια ασφάλεια, η ελευθερία διακίνησης των αγαθών, των ανθρώπων και των ιδεών δεν αποτελούν αξίες για τις οποίες απαιτείται απλά ο επανασχεδιασμός της προστασίας τους, αλλά έννοιες που έχουν εισέλθει ήδη σε κοινωνιολογικό διάλογο επαναπροσδιορισμού με βάση τον νομοτελειακό μετασχηματισμό που επιβάλει ο νέος κόσμος διασυνδεδεμένων συστημάτων ψηφιακών δικτύων. Πρόσφατα, σε βρετανό στρατιώτη που επρόκειτο να αποσπασθεί για υπηρεσιακούς λόγους στη φρουρά των νησιών Φώκλαντ, ικανοποιήθηκε το αίτημά του για παροχή συνεχούς πρόσβασης στο διαδίκτυο καθ' όλη τη διάρκεια της υπηρεσίας του εκεί, κατόπιν θετικής εισήγησης των νομικών υπηρεσιών του Υπουργείου Άμυνας, με την αιτιολογία ότι η διευκόλυνση πρόσβασης[58] στο διαδίκτυο υπέχει θέση βασικού ανθρώπινου δικαιώματος[59].

---

[57] The Department of Defense Cyber Strategy, 17 Apr 2015, p.1

[58] Presented by Leigh Alexander with Matt Shore and produced by Matt Shore and Katie Callin ''Internet access is now a basic human right: part 1 – Chips with Everything tech podcast'', https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast

[59] United Nations, General Assembly, Human Rights Council, 32nd session, Agenda item 3, "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development", https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Σημείωση: Το ψήφισμα, το οποίο είναι μη δεσμευτικό, καταδικάζει τη σκόπιμη διακοπή της πρόσβασης στο Διαδίκτυο

Το δε άρθρο 5Α του Συντάγματος της Ελλάδας[60] αναφέρει ότι όλα τα άτομα έχουν δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας και ότι το κράτος έχει υποχρέωση να διευκολύνει την παραγωγή, ανταλλαγή, διάδοση και πρόσβαση σε ηλεκτρονικά μεταδιδόμενες πληροφορίες.

Το Νοέμβριο του 2014, πιθανότατα σε αντίποινα για τη σχεδιαζόμενη προβολή σατιρικής κινηματογραφικής ταινίας, η Βόρεια Κορέα πραγματοποίησε κυβερνοεπίθεση εναντίον της «Sony Pictures Entertainment», καθιστώντας χιλιάδες υπολογιστές μη λειτουργικούς και παραβιάζοντας τις εμπιστευτικές επιχειρηματικές πληροφορίες της εταιρείας. Εκτός από τα καταστρεπτικά αποτελέσματα των επιθέσεων, η Βόρεια Κορέα έκλεψε ψηφιακά αντίγραφα ορισμένων ταινιών που δεν είχαν κυκλοφορήσει, καθώς και χιλιάδες έγγραφα που περιέχουν ευαίσθητα δεδομένα σχετικά με διασημότητες, υπαλλήλους και επιχειρηματικές δραστηριότητες της εταιρείας Sony[61]. Αν η Β.Κορέα αντιλαμβάνεται ότι η υπόψη κινηματογραφική ταινία εντάσσεται στο πλαίσιο των ψυχολογικών επιχειρήσεων που διεξάγουν οι ΗΠΑ με σκοπό να πλήξουν την αφοσίωση του βορειοκορεατικού λαού στον ηγέτη τους ή να διαμορφώσουν αρνητική έως εχθρική άποψη εναντίον του βορειοκορεατικού καθεστώτος στο παγκόσμιο κοινό ή και τα δύο, τότε η δυνατότητα μιας κυβερνοεπίθεσης καθίσταται αποδεκτή ανταποδοτική ενέργεια στην αντίληψη όσων την αποφασίσουν με όμοιο τρόπο όπως καθίσταται αποδεκτή η απόφαση διεξαγωγής ψυχολογικών επιχειρήσεων στην αντίληψη όσων αντιμάχονται το καθεστώς.

4.1.2. Οι Σκοτεινές Πτυχές του Κυβερνοεγκλήματος

Τα όργανα. Οι νέοι ψηφιακοί εγκληματίες είναι, φυσικά, οι χάκερς[62]. Τον Ιούνιο του 2011, το BBC αναφέρει[63] ότι «στις πρώτες δεκαετίες του 21ου αιώνα η λέξη «χάκερ» έχει γίνει συνώνυμη με ανθρώπους που παραμονεύουν σε σκοτεινά δωμάτια, τρομοκρατώντας ανώνυμα το διαδίκτυο». Μια εικόνα που απέχει δραματικά από τους ιδεαλιστές ευφυείς φοιτητές, λάτρεις της τεχνολογίας, που διψούσαν για μάθηση και «σκότωναν» το χρόνο

από τις κυβερνήσεις. Η απόφαση επιβεβαίωσε ότι «τα ίδια δικαιώματα που έχουν τα άτομα εκτός σύνδεσης πρέπει επίσης να προστατεύονται ηλεκτρονικά».
Universal Declaration of Human Rights; ''Article 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers''.
http://www.un.org/en/universal-declaration-human-rights/
James Vincent, ''UN condemns internet access disruption as a human rights violation'' Jul 4, 2016,
https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access

[60] ''THE CONSTITUTION OF GREECE As revised by the parliamentary resolution of May 27th 2008 of the VIIIth Revisionary Parliament'', '' Article 5A, 1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19.
https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf

[61] The Department of Defense Cyber Strategy, 17 Apr 2015, p.2

[62] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.16 & 25

[63] Mark Ward, ''A brief history of hacking'' 09 Jun 2011,
https://www.bbc.com/news/technology-13686141

τους λύνοντας σύγχρονους γόρδιους δεσμούς εισβάλοντας στα πρώιμα συστήματα ηλεκτρονικών δικτύων. Υπάρχουν διάφορες τυπολογίες χάκερ, ωστόσο, η πιο βασική των οποίων τους διακρίνει με βάση τον χαρακτήρα της βούλησή τους[64]:

- Οι μη κακόβουλοι (τα επονομαζόμενα «λευκά καπέλα» ή αλλιώς «ηθικοί» χάκερς), οι οποίοι διερευνούν ένα σύστημα είτε ως προσωπική, ανιδιοτελής και δημιουργική ευχάριστη ενασχόληση είτε για εξέταση και δοκιμή της ασφάλειάς του επωφελεία των ιδιοκτητών του.
- Οι κακόβουλοι (τα «μαύρα καπέλα» ή αλλιώς «crackers»), οι οποίοι διεισδύουν «σπάζοντας» τις δικλείδες ασφαλείας - άμυνες ενός συστήματος για άλλους σκοπούς, όχι και τόσο αλτρουιστιστικούς. Αυτοί, οι άλλοι σκοποί, είναι το κλειδί για την περαιτέρω κατηγοριοποίηση των χάκερς, όπως τα «γκρίζα καπέλα», των οποίων οι δραστηριότητες εμπίπτουν στο φάσμα μεταξύ των δύο πόλων.

Ο κυβερνοχώρος διαθέτει αρκετό χώρο για επιτυχή δραστηριοποίηση πολλών υποκατηγοριών[65], όπως:

- Εγκληματίες του κυβερνοχώρου (cyber criminals). Συνιστούν τη μεγαλύτερη υποκατηγορία και είναι κοινοί κλέφτες που χρησιμοποιούν ποικίλες και μερικές φορές εξαιρετικά καινοτόμες τεχνικές για να υφαρπάξουν οτιδήποτε μπορεί να έχει αξία στην αγορά.
- Ομάδες «Κυβερνοαπειλών». Οι ειδικοί στον τομέα της ασφάλειας στον κυβερνοχώρο χαρακτηρίζουν ως ανώτερες ποιοτικά και επίμονες απειλές (Advanced Persistent Threat[66] - APT) τις καλά οργανωμένες και τεχνικά επιτηδευμένες ομάδες που «εξορμούν» υπό την προστασία μιας χώρας που λειτουργεί ως ασφαλής λιμένας και τους παρέχει το απαιτούμενο επίπεδο ανεκτικότητας ή και κάλυψης για να στοχοποιήσουν συγκεκριμένα ιδρύματα ή οργανισμούς - υπηρεσίες με σκοπό τη βιομηχανική κατασκοπεία και την κλοπή πνευματικής ιδιοκτησίας με μακροπρόθεσμη αξία.
- Ομάδες των «hacktivist». Είναι ακτιβιστικές ομάδες του διαδικτύου, όπως οι «Anonymous» και «LulzSec», οι οποίες δρουν – χακάρουν για διασκέδαση και χωρίς κάποια πλήρως μορφοποιημένη πεποίθηση, είτε αυτή είναι πολιτική, θρησκευτική, περιβαλλοντική ή προσωπική. Έχουν έρθει στο προσκήνιο μετά από μια σειρά από εντυπωσιακές επιθέσεις, συνήθως αλλοίωσης (Defacement) κάποιου ιστότοπου ή/και απαγόρευσης χρήσης μιας διαδικτυακής υπηρεσίας (Denial of Service[67] - DoS), αλλά και κλοπής δεδομένων (πχ αρχεία ηλεκτρονικού ταχυδρομείου, βάσεις δεδομένων πελατών κλπ) εμπορικών εταιρειών ή κρατικών θεσμών, διεθνών οργανισμών κλπ.

---

[64] Roger A. Grimes, ‘’Your guide to the seven types of malicious hackers’’, 08 Feb 2011
https://www.csoonline.com/article/2623407/your-guide-to-the-seven-types-of-malicious-hackers.html

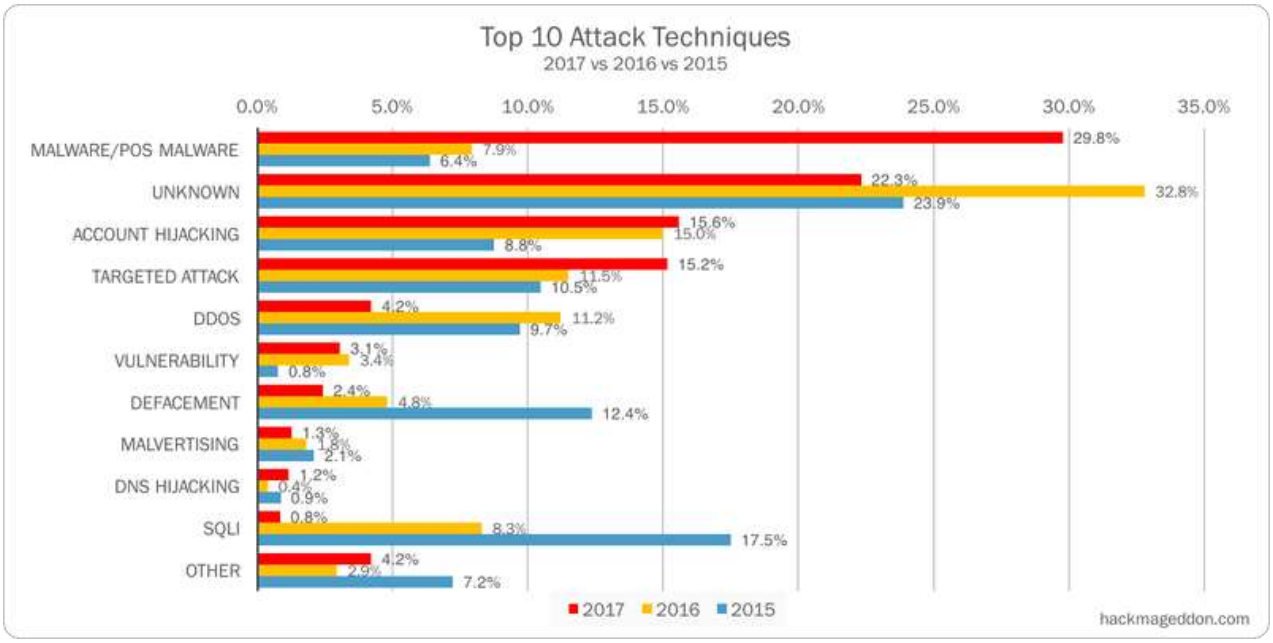
[65] D.J.Betz & T.Stevens, “CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER”, IISS, Arundel House, London, 2011, p.25 - 27

[66] What Is an Advanced Persistent Threat (APT)?
https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[67] What is a DDoS Attack? - DDoS Meaning
https://www.kaspersky.com/resource-center/threats/ddos-attacks

- «Μαχητές» του διαδικτύου (cyber-warriors[68]). Αυτοί είναι εξειδικευμένοι κρατικοί υπάλληλοι, ακόμα και ένστολοι, οι οποίοι ενεργούν είτε ως όργανα – πράκτορες APT είτε ως «κυβερνοκατάσκοποι» (cyber-spies) για να διεξάγουν επιθετικό ή αμυντικό κυβερνοπόλεμο.

Η κλίμακα του εγκλήματος στον κυβερνοχώρο. Μόνο το 2014 εκτιμάται ότι ένα δισεκατομμύριο ψηφιακά δεδομένα εκτέθηκαν διαδικτυακά παγκοσμίως κατόπιν κυβερνοεπιθέσεων με το εντυπωσιακό 47% των Αμερικανών να έχει κλεμμένα προσωπικά στοιχεία. Είναι πιθανό ότι είστε ήδη θύμα εγκλήματος στον κυβερνοχώρο, αλλά δεν είναι μόνο τα μεμονωμένα άτομα που διατρέχουν κίνδυνο. Το Υπουργείο Άμυνας των ΗΠΑ έχει να αντιμετωπίσει πάνω από 100.000 επιθέσεις ημερησίως και το 58% των εταιρικών υπολογιστών επηρεάζονται από μία ή περισσότερες μολύνσεις από κακόβουλο λογισμικό. Αυτή η παράνομη σάρωση των δεδομένων μπορεί να μετατραπεί σε τεράστια χρηματικά ποσά, με το έγκλημα στον κυβερνοχώρο να κοστίζει την παγκόσμια οικονομία έως και μισό τρισεκατομμύριο δολάρια κάθε χρόνο. Αυτό είναι το ίδιο με το σύνολο του παράνομου εμπορίου ναρκωτικών στον κόσμο.



ΔΙΑΓΡΑΜΜΑ 1: Στατιστικά στοιχεία κυβερνοεπιθέσεων έτους 2017[69]

Εξασφάλιση ασυλίας στις κυβερνοεπιθέσεις. Χιλιάδες άνθρωποι, επιχειρήσεις και κυβερνητικοί φορείς χρησιμοποιούν υπηρεσίες ασφαλούς διαχείρισης ιστοσελίδων (bulletproof web hosting services) για να βοηθήσουν στην αποτροπή της κατάργησης των ιστοτόπων τους από «κυβερνοεισβολείς» και στην ασφαλή αποθήκευση δεδομένων με εμπιστευτικότητα. Ωστόσο, τέτοιες υπηρεσίες εκμεταλλεύονται συχνά οι εγκληματίες του κυβερνοχώρου για την ανώνυμη χρήση και εκμετάλλευση κακόβουλου λογισμικού, «botnet», ανεπιθύμητων μηνυμάτων (spam) και αποθήκευσης - φιλοξενίας παράνομων δεδομένων. Ένας πάροχος τέτοιων υπηρεσιών, ο McColo[70], ήταν υπεύθυνος για τα δύο

[68] Jennifer J. Li, Lindsay Daugherty, ‘’Training Cyber Warriors. What Can Be Learned from Defense Language Training? https://www.rand.org/pubs/research_reports/RR476.html
[69] https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/
[70] Jaikumar Vijayan, ‘’McColo takedown: Internet vigilantism or online Neighborhood Watch?’’

τρίτα του συνόλου των ανεπιθύμητων μηνυμάτων στο διαδίκτυο πριν προκληθεί το κλείσιμο της διαδικτυακής του υπηρεσίας το 2008. Μια άλλη διαδικτυακή υπηρεσία, η «Russian Business Network[71]» απαιτούσε από τους πελάτες της να προβούν σε ενέργειες που συνιστούν διαδικτυακό έγκλημα προτού τους επιτραπεί να χρησιμοποιήσουν την υπηρεσία που επιθυμούσαν και τους πρόσφερε. Θεωρήθηκε ότι χρησιμοποιούσε το «σκουλήκι» (worm) «Storm[72]» που ευθύνεται για την μόλυνση έως και 50 εκατομμύριων υπολογιστών παγκοσμίως, δημιουργώντας έναν στρατό από «ζόμπι» υπολογιστές (botnet) υπό τον έλεγχό τους. Το 2007, αυτό το «botnet» ήταν τόσο ισχυρό που θα μπορούσε θεωρητικά να έχει θέσει μια χώρα ολόκληρη εκτός διαδικτυακής σύνδεσης υπερφορτώνοντας το δίκτυό της με κίνηση.

Ο πλέον καταζητούμενος στον κυβερνοχώρο. Ο Ευγένιος Μιχαΐλοβιτς Μπογκάτσεφ είναι ο πιο διάσημος «κυβερνοεγκληματίας» στον κόσμο, επικηρυγμένος από το FBI[73] για πληροφορίες που οδηγούν στη σύλληψή του με προσφερόμενη αμοιβή 3 εκατομμυρίων δολαρίων. Είναι γνωστός διαδικτυακά ως «lucky12345»' και η τεχνική του περιλαμβάνει την εξαπάτηση για την εγκατάσταση ενός προγράμματος «Trojan» με την ονομασία «Game over Zeus[74]». Το πρόγραμμα υποκλέπτει στοιχεία τραπεζικών λογαριασμών, κωδικούς πρόσβασης και άλλες προσωπικές πληροφορίες. Έχει μολύνει πάνω από 1 εκατομμύριο υπολογιστές και εξασφάλισε για τον «lucky12345» μια περιουσία 100 εκατομμυρίων δολαρίων. Έχει μάλιστα αναφερθεί ότι έχει εγκαταστήσει ένα κακόβουλο λογισμικό του τύπου «ransomware» στο αστυνομικό τμήμα της Μασαχουσέτης. Το υπόψη λογισμικό εμποδίζει τους χρήστες να έχουν πρόσβαση στα ηλεκτρονικά αρχεία τους απαιτώντας λύτρα. Έτσι λοιπόν, η αστυνομία έπρεπε να πληρώσει για να ξανακερδίσει πρόσβαση στη βάση δεδομένων με τις φωτογραφίες συλληφθέντων προσώπων (mugshots[75]). Ωστόσο, καθώς η Ρωσία δεν εκδίδει κατηγορούμενους εγκληματίες σε άλλες χώρες, είναι μάλλον απίθανο να συλληφθεί ο Μπογκάτσεφ.

Ένα Διαδίκτυο, πολλοί νόμοι. Περίπου το 70% του εγκλήματος στον κυβερνοχώρο δεν περιορίζεται από τα εθνικά σύνορα, γεγονός που καθιστά δύσκολη τη σύλληψη των δραστών. Αυτό που είναι παράνομο σε μια χώρα ενδέχεται να μην θεωρείται παράνομο αλλού. Σύμφωνα με έκθεση του ΟΗΕ, ο έλεγχος ή η αποστολή ανεπιθύμητων μηνυμάτων δεν αποτελεί ποινικό αδίκημα στο 63% των χωρών όπως η Ινδία, η Ρωσία και η Βραζιλία. Αυτό συμβαίνει παρά το γεγονός ότι τα ανεπιθύμητα μηνύματα μπορούν να μεταφέρουν κακόβουλο κώδικα, ο οποίος θα μπορούσε ενδεχομένως να παρακολουθεί έναν χρήστη, να υποκλέπτει δεδομένα ή να εγκαταστήσει κακόβουλα προγράμματα. Η έλλειψη συνεκτικής νομοθεσίας και διακρατικής συνεργασίας στα ζητήματα κυβερνοασφάλειας καθιστά

---

https://www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html

[71] Peter Warren, '' Hunt for Russia's web criminals'' Thu 15 Nov 2007
https://www.theguardian.com/technology/2007/nov/15/news.crime

[72] Dawn Kawamoto, ''Storm worm' rages across the globe'' April 13, 2007
https://www.cnet.com/news/storm-worm-rages-across-the-globe/

[73] https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

[74] Symantec Official Blog, ''International Takedown Wounds Gameover Zeus Cybercrime Network''
https://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

[75] Rhodri Marsden, ''Cyber Culture: Mugshots are forever (well, that;s what website blackmailers would like you to believe)'',INDEPENDENT, 9 Oct 2013
https://www.independent.co.uk/life-style/gadgets-and-tech/features/cyber-culture-mugshots-are-forever-well-thats-what-website-blackmailers-would-like-you-to-believe-8869808.html

δυσχερή τη διαδικασία απαγγελίας κατηγορίας και την σύλληψη και οδήγηση στη δικαιοσύνη των «spammers» ακόμα και σε χώρες όπως το Ηνωμένο Βασίλειο ή οι ΗΠΑ, όπου έχουν τεθεί σε εφαρμογή αυστηροί περιοριστικοί όροι στην αποστολή ανεπιθύμητων μηνυμάτων από το 2003.

«Πιάστε με αν μπορείτε». Παρά το γεγονός ότι είναι ο μεγαλύτερος διαμεσολαβητής της παράνομης διανομής αρχείων στον πλανήτη, η «Pirate Bay[76]» συνεχίζει να επιβιώνει διαδικτυακά. Αλλά πώς; Το 2006, μετά από επιδρομές στα γραφεία των ιδιοκτητών και την κατάσχεση των διακομιστών (servers), η ιστοσελίδα της υπόψη διαδικτυακής υπηρεσίας επέστρεψε εντός τριών ημερών, δημιουργώντας ένα εκτεταμένο δίκτυο εξυπηρετητών, έτσι ώστε η απώλεια οποιουδήποτε διακομιστή να μην επηρεάζει τη λειτουργία της ιστοσελίδας. Στη συνέχεια, το 2007, η «Pirate Bay» επιχείρησε, αλλά απέτυχε να αγοράσει την μικροχώρα «Sealand», ώστε να μπορέσει να δημιουργήσει το δικό της κράτος χωρίς νόμους περί πνευματικών δικαιωμάτων. Αντ' αυτού τελικά μετέφερε τις δραστηριότητές της στο «Cloud». Οι διακομιστές τους ‘’τρέχουν’’ σε πάνω από 20 εικονικές μηχανές ενώ οι πάροχοι δεν γνωρίζουν καν ότι φιλοξενούν την «Pirate Bay». Τούτο ουσιαστικά τους καθιστά απροσβλήτους από αστυνομικές εφόδους.

Απεριόριστη ελευθερία. Η διαδικτυακή ανωνυμία που προσφέρουν οι απρόσβλητοι στις κυβερνοεπιθέσεις διαδικτυακοί θύλακες (bulletproof holsters) μπορεί να χρησιμοποιηθεί από δημοσιογράφους για να αποφευχθεί η κρατική – κυβερνητική λογοκρισία. Η «wikileaks» έχει χρησιμοποιήσει τέτοιες υπηρεσίες, ενώ η ίδια ελευθερία μπορεί να αξιοποιηθεί από τρομοκράτες. Μία υπηρεσία, γνωστή ως «CloudFlare[77]», έχει χρησιμοποιηθεί από το ISIS για την προστασία των ιστοχώρων και των «chat rooms» που έχει δημιουργήσει η τρομοκρατική αυτή οργάνωση για την εξυπηρέτηση των σκοπών της. Σύμφωνα με τους «Anonymous», το ISIS χρησιμοποιεί τις υπόψη υπηρεσίες για να προστατεύσει 40 ιστοσελίδες αφιερωμένες στην προπαγάνδα και στην στρατολόγηση, την ανταλλαγή απόψεων και πληροφοριών και για την εκπαίδευση σε τεχνικές που μεταχειρίζεται η τρομοκρατική δράση.

Η πυρηνική επιλογή. Ενώ οι κυβερνήσεις συχνά προσπαθούν να καταπολεμήσουν το έγκλημα στον κυβερνοχώρο, πολλές από αυτές το χρησιμοποιούν επίσης προς όφελός τους μέσω της κατασκοπείας και του πολέμου. Ίσως το πιο διάσημο παράδειγμα ήταν ένα τμήμα κακόβουλου λογισμικού που ονομάζεται «Stuxnet», το οποίο εγκαταστάθηκε δολίως σε υπολογιστές του Ιράν και λειτουργούσε από διακομιστές στη Δανία και τη Μαλαισία. Αυτό το «σκουλήκι», το οποίο θεωρείται ότι έχει αναπτυχθεί από το Ισραήλ και τις ΗΠΑ, υπονόμευσε το πυρηνικό πρόγραμμα του Ιράν, ωστόσο το αποτέλεσμα της δράσης του ήταν κατάλληλα μεταμφιεσμένο ώστε να προσομοιάζει με μια σειρά ατυχημάτων. Το κυβερνοόπλο κατέστρεψε τελικά το 20% των διατάξεων φυγοκέντρισης του Ιράν

[76] Mary-Ann Russon, ‘’Pirate Bay loses hydra and .se domains, returning to original .org address following legal challenges’’ Updated May 23, 2016
https://www.ibtimes.co.uk/pirate-bay-loses-hydra-domains-returning-original-org-address-following-legal-challenges-1561515

[77] Testimony of Evan F. Kohlmann with Laith Alkhouri and Alexandra Kassirer Before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media” Charlie Hebdo and the Jihadi Online Network: Assessing the Role of American Commercial Social Media Platforms, January 27, 2015; 2:30pm, 2172 Rayburn House Office Building, Washington D.C.
https://docs.house.gov/meetings/FA/FA18/20150127/102855/HHRG-114-FA18-Wstate-KohlmannE-20150127.pdf

βλάπτοντας την ικανότητά τους να παράγουν αξιοποιήσιμα πυρηνικά υλικά. Όταν η κυβερνοεπίθεση συνδυαστεί με την δολοφονία πυρηνικών επιστημόνων, πως είναι δυνατό να μην εκτοξευτεί κατακόρυφα η ζήτηση για κατάταξη νεαρών επιστημόνων στον Ιρανικό «Κυβερνοστρατό»; Τα πράγματα όμως μπορεί να αποδειχθούν ακόμα χειρότερα όταν αυτός που επινοεί ένα «κυβερνουπερόπλο» (πολλοί χαρακτήρισαν τον stunxet ως το αντίστοιχο της ατομικής βόμβας στον κυβερνοχώρο) πέφτει ο ίδιος θύμα του όπλου που επινόησε, είτε από δικά του λάθη και παραλείψεις, είτε διότι απλά το υπερόπλο έπεσε σε λάθος χέρια.

Ο σκοτεινός ιστός (Dark Web[78]). Η μη ανιχνεύσιμη ανωνυμία του «Dark Web» έχει χρησιμοποιηθεί από εγκληματίες του κυβερνοχώρου για να κερδίσουν χρήματα. Εκτιμάται ότι το 9% όλων των διαδικτυακών συναλλαγών πρόκειται για απάτες. Τα κλεμμένα στοιχεία πιστωτικών ή χρεωστικών καρτών μπορούν πουληθούν για μόλις 5$, ενώ τα στοιχεία διαδικτυακής σύνδεσης σε έναν τραπεζικό λογαριασμό που διαθέτει πιστωμένα 20.000$ έχουν πωληθεί για μόλις 1.200$. Όμως, το παράνομο εμπόριο ναρκωτικών είναι ακόμη μεγαλύτερο, αντιπροσωπεύοντας πάνω από το 15% όλων των ιστοσελίδων του Dark Web. Μία από αυτές, η «Silk Road», επέφερε στον διαδικτυακό ιδιοκτήτη Ross Ulbright[79] κέρδη ύψους 80 εκατομμυρίων δολαρίων από προμήθειες τεράστιων πωλήσεων αξίας 1,2 δισεκατομμυρίων δολαρίων. Τερματίστηκε το 2013. Η διαδικτυακή μαύρη αγορά περιλαμβάνει πολλές άλλες υπηρεσίες μεταξύ αυτών οι πωλήσεις πυροβόλων όπλων, η μίσθωση μπράβων, χάκερ, ακόμη και διαδικτυακών ακόλουθων (followers) για την διαμόρφωση επιτυχημένου διαδικτυακού προφίλ.

«Carbanak[80]» - Η εξέλιξη του εγκλήματος στον κυβερνοχώρο. Πιθανότατα οι περισσότεροι άνθρωποι δεν έχουν ακούσει για τον Carbanak, αλλά είναι στην πραγματικότητα υπεύθυνος για την μεγαλύτερη μιμητική «κυβερνοπαραπλάνηση» στην ιστορία με λεία 1 δισεκατομμύριο δολάρια από περισσότερα από 100 χρηματοπιστωτικά ιδρύματα σε όλο τον κόσμο. Οι εγκέφαλοι της απάτης τα έκαναν όλα από τα πληκτρολόγια τους στη Ρωσία, την Ουκρανία και την Κίνα από το 2013 έως το 2015. Τα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν μολυνθεί από κακόβουλο λογισμικό «Carbanak and Cobalt[81]» επέτρεπαν τη συμμορία να καταγράψει τι συνέβη στις οθόνες του προσωπικού των τραπεζών. Μετά από μήνες μελέτης της συμπεριφοράς, μετέφεραν τα χρήματα στους δικούς τους λογαριασμούς ή έδιναν ηλεκτρονικές εντολές σε ATMs για να δώσουν μετρητά σε προκαθορισμένους χρόνους. Σε μια μόνο επιδρομή θα μπορούσαν να κλέψουν μέχρι και 10 εκατομμύρια δολάρια. Σηματοδότησε την αρχή ενός νέου τύπου εγκλήματος στον κυβερνοχώρο, το οποίο στοχοποιεί τις τράπεζες απευθείας, αντί να κλέβει από μεμονωμένους πελάτες - στόχους.

---

[78] Tarquin, ‘’How To Access Notorious Dark Web Anonymously (10 Step Guide)’’ Updated on 18 May 2018, https://darkwebnews.com/help-advice/access-dark-web/

[79] Donna Leinwand Leger, ‘’ How FBI brought down cyber-underworld site Silk Road’’, USA TODAY, Published Oct. 21, 2013, Updated May 15, 2014
https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

[80] David Meyer, ‘’ A Cyber Gang Stole $1 Billion by Hacking Banks and ATMs. Now Police Say They've Caught the Mastermind’’, FORTUNE, March 26, 2018
http://fortune.com/2018/03/26/carbanak-europol-arrest-spain-malware-banks/

[81] Lindsey O’Donnell, ‘’ ALLEGED MASTERMIND BEHIND CARBANAK CRIME GANG ARRESTED’’, threatpost.com, Mar 28,2018
https://threatpost.com/alleged-mastermind-behind-carbanak-crime-gang-arrested/130831/

Διαδικτυωμένες συσκευές (The Internet of Things – IoT[82]). Το έγκλημα στον κυβερνοχώρο σταδιακά περιορίστηκε σε μεγάλο βαθμό σε ότι αφορά τη μόλυνση των υπολογιστών και των κινητών τηλεφώνων, αλλά το διαδίκτυο των πραγμάτων αφήνει τα αντικείμενα καθημερινής χρήσης ευάλωτα στις κυβερνοαπειλές, όπως οι «έξυπνες» (smart) τηλεοράσεις ή τα έξυπνα αυτοκίνητα! Το διαδίκτυο των δυνητικά «κυβερνομολυσμένων» αγαθών: Για παράδειγμα, συσκευές παρακολούθησης βρεφών – μικρών παιδιών έχουν εκτεθεί, επιτρέποντας σε τρίτους να κατασκοπεύουν και μάλιστα να μιλούν σε μικρά παιδιά. Η χρήση διαδικτυωμένων συσκευών δημιουργεί πολλά νέα κανονιστικά - ρυθμιστικά και νομικά ζητήματα γύρω από τη χρήση του διαδικτύου και την ανάγκη ενίσχυσης των υφιστάμενων νομικών διατάξεων γύρω από αυτό. Τα ζητήματα έχουν ευρύ πεδίο εφαρμογής και ο ταχύς ρυθμός των αλλαγών στην τεχνολογία του Διαδικτύου υπερβαίνει συχνά την ικανότητα των σχετικών πολιτικών, νομικών και ρυθμιστικών πλαισίων για την προσαρμογή. Ένα σύνολο ζητημάτων αφορά τις διασυνοριακές ροές δεδομένων, οι οποίες συμβαίνουν όταν οι διαδικτυωμένες συσκευές συλλέγουν δεδομένα σχετικά με ανθρώπους που ανήκουν σε μία δικαιοδοσία και τη διαβιβάζουν σε άλλη με διαφορετικό πλαίσιο επεξεργασίας και προστασίας δεδομένων. Επιπλέον, τα δεδομένα που συλλέγονται είναι μερικές φορές ευάλωτα σε κατάχρηση, εγείροντας ενδεχομένως ζητήματα διακρίσεων και ανισότητας για ορισμένους χρήστες.

4.1.3. Η Κυβερνοασφάλεια, η Κυβερνοισχύς και η Δημοκρατία

Η ολοένα αυξανόμενη χρήση των κυβερνοεπιθέσεων ως πολιτικού μέσου αντικατοπτρίζει μια επικίνδυνη τάση στις διεθνείς σχέσεις, αναδεικνύοντας ταυτόχρονα το βαθμό αποδοχής της νέας πραγματικότητας από τους θεσμούς που ορίζουν το διεθνές σύστημα, με πρωταγωνιστές βεβαίως τα Κράτη. Η μελέτη του φαινομένου αναδεικνύει ορισμένα ενδιαφέροντα στοιχεία σχετικά με την διαφοροποιημένη συμπεριφορά των διεθνών δρώντων ως προς την επιλογή του κυβερνοχώρου ως χώρο ενεργητικής, επιθετικού χαρακτήρα, αντιπαράθεσης ή έστω αποδοχής της προοπτικής μιας τέτοιας στρατηγικής, έναντι μιας αμυντικού χαρακτήρα στρατηγικής που στοχεύει στην παθητική προστασία από κυβερνοαπειλές και κυβερνοεπιθέσεις.

Στον κυβερνοχώρο, δύο οποιοδήποτε δρώντες συνδέονται μεταξύ τους εντός ελάχιστων χιλιοστών του δευτερολέπτου, που είναι ο απαιτούμενος χρόνος για να ταξιδέψουν οι ψηφιακές πληροφορίες – εντολές από τον ένα στον άλλο, σχεδόν οπουδήποτε στον κόσμο. Αυτή η διαδικτυακή ταχύτητα, που αγγίζει την ταχύτητα του φωτός, απαλείφει τον παράγοντα χώρο, σε οτιδήποτε αναφέρεται σε προθέσεις και σκοπούς, κατά τρόπο ασύγκριτα πιο ριζοσπαστικό ακόμα και από την εμπειρία της βαλλιστικής τεχνολογίας σε συνδυασμό με αυτήν της πυρηνικής. Η αρχέγονη ανάγκη των στρατηγών να βρεθούν όσο πιο γρήγορα και όσο πιο κοντά στον εχθρό - στόχο τους κατέστη μια φευγαλέα πραγματικότητα μέσα στην οποία η πολιτική, που έχει το δικαίωμα και την υποχρέωση να λαμβάνει και να καθοδηγεί τις στρατηγικές αποφάσεις δεν διαθέτει τον επαρκή χωροχρόνο για να το πράξει[83]. Ο «κυβερνοχρόνος» γίνεται αντιληπτός μόνο

[82] Karen Rose, Scott Eldridge, Lyman Chapin ‘’The Internet of Things, An Overview Understanding the Issues and Challenges of a More Connected World’’, The Internet Society (ISOC), 2015

[83] Paul Virilio, ‘’SPEED AND POLITICS’’, Published by Semiotext(e), Wilshire Blvd, Suite 427, Los Angeles, 2007, p.62, 95, 151, 154

από τις καθυστερήσεις που προκαλούν οι αναγκαίες τεχνικές διασυνδέσεις και οι κόμβοι επικοινωνιών που μεσολαβούν μεταξύ των δρώντων. Αυτή η ταυτόχρονη εκδήλωση του αίτιου και του αιτιατού έχει προφανείς συνέπειες στην άσκηση ορισμένων μορφών εξουσίας. Ενέργειες που άρχισαν να εκδηλώνονται σε μία τοποθεσία μπορεί ακαριαία να έχουν αποτελέσματα σε μία άλλη, ανεξάρτητα από τον γεωγραφικό τους διαχωρισμό. Αν και αυτό επιτρέπει στους κρατικούς δρώντες την πρόσβαση σε ένα ευρύτερο φάσμα στόχων, κατανεμημένων σε παγκόσμια κλίμακα και εκτεθειμένων σε διάφορες μορφές πιθανού εξαναγκασμού, ταυτόχρονα διευκολύνει και την αντίστροφη δυναμική, κατά την οποία οι χωρικά απομακρυσμένοι δρώντες - ιδιαίτερα αυτοί εκτός της άμεσης δικαιοδοσίας του κράτους - μπορούν να ασκήσουν επιρροή και εξουσία ενάντια στις επιθυμίες ενός κράτους, με ελάχιστες ή μηδενικές πιθανότητες εντοπισμού ή παρεμπόδισης από το υπόψη κράτος. Μάλιστα, ο εξοβελισμός του χρόνου και του χώρου, που ουσιαστικά λαμβάνει χώρα κατά τις διαδικτυακές διαδράσεις, επιτρέπει την αύξηση του αριθμού των δρώντων που μπορεί να επηρεάζονται από μορφές εξουσίας, οι οποίες προηγουμένως ήταν κατά τεκμήριο περιορισμένες από το φυσικό και χρονικό διαχωρισμό. Αυτή η δυναμική επηρεάζει όλους τους δρώντες, ανεξάρτητα από τη σχετική ιστορική τους πρόσβαση στην εξουσία[84].

Οι σχετικά πιο αδύναμοι, με όρους διεθνοπολιτικής ισχύος, παίχτες, αλλά και οι λιγότερο προσηλωμένοι σε δημοκρατικές αρχές και παραδόσεις εμφανίζονται να είναι πιο πρόθυμοι να επιλέξουν ή να έχουν ήδη επιλέξει το πεδίο του κυβερνοχώρου ως ψηφιακό πεδίο αντιπαράθεσης, πιο πρόθυμοι να χρησιμοποιήσουν ή να αναπτύξουν, αν δεν χρησιμοποιούν ήδη τα κυβερνοόπλα που διαθέτουν και τέλος πιο πρόθυμοι να εκμεταλλευτούν τα αποτελέσματα κυβερνοεπιθέσεων που θα εκτοξεύσουν ή ήδη τα εκμεταλλεύονται οι ίδιοι ή εκπρόσωποί τους ή τρίτοι για να πλήξουν του ισχυρότερους ανταγωνιστές τους, καθιστώντας την αναγνωρισμένη αδυναμία τους και ασυμμετρία στην σχέση τους με τους ανταγωνιστές τους, σε πλεονέκτημα.

Οι δε ισχυρότεροι, καθώς και οι σχετικά πιο προσηλωμένοι σε δημοκρατικές αρχές και παραδόσεις διεθνοπολιτικοί δρώντες δείχνουν δυσκολία να αποδεχτούν την πρόκληση και να ανταπαντήσουν με όμοιο ή ανάλογο τρόπο. Η κατάσταση θυμίζει ως ένα βαθμό την μετάβαση από το ξίφος στο πυροβόλο όπλο, όπου οι παλαιοί, «ευγενικής» καταγωγής πολεμιστές των παραδοσιακά ισχυρών δυνάμεων αρνούνται να αποδεχθούν τα νέα πολεμικά ήθη που επιβάλλει η τεχνολογία στα χέρια των αναθεωρητικών, λαϊκών και ίσως λιγότερο συνεσταλμένων έναντι της ωμής βίας δυνάμεων. Η συζήτηση βέβαια έχει ήδη αρχίσει τόσο σε εθνικό – κρατικό επίπεδο, όσο και σε διεθνές – διασυμμαχικό. Η διαπιστωμένη πρόκληση ασφαλείας ανοίγει την ατζέντα και θέτει σε νέες βάσεις ζητήματα διεθνούς και συλλογικής ασφάλειας, τα οποία μέχρι χθες θα μπορούσαν να χαρακτηρισθούν και ως «βλασφημία»[85]. Είναι αυτή η δυσκολία που εξαναγκάζει σε προσαρμογές, όπως τις αντιλαμβάνεται ο Πλοίαρχος του Αμερικανικού Πολεμικού Ναυτικού Michael Widmann στο Κέντρο Συνεργατικής Κυβερνοάμυνας του NATO στην Εσθονία[86]:

---

[84] D.J.Betz & T.Stevens, “CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER”, IISS, Arundel House, London, 2011, p.39

[85] Council on Foreign Relations, ‘’Europe Slowly Starts to Talk Openly About Offensive Cyber Operations‘’, Nov 6, 2017 https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations

[86] Robin Emmott, ‘’ NATO mulls 'offensive defense' with cyber warfare rules’’, Reuters, Reuters, Reuters, Nov 30, 2017 https://www.reuters.com/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4

«Υπάρχει μια αλλαγή στη νοοτροπία (του NATO) για να αποδεχτούμε ότι οι ηλεκτρονικοί υπολογιστές, όπως τα αεροσκάφη και τα πλοία, έχουν επιθετική ικανότητα».

Σύμφωνα με τον ανεξάρτητο, μη κερδοσκοπικό οργανισμό και δεξαμενή σκέψης «Council on Foreign Relations (CFR)»[87], δεκαεννέα χώρες είναι ύποπτες για τη χρηματοδότηση «κυβερνοεπιχειρήσεων», συμπεριλαμβανομένων των Ηνωμένων Πολιτειών, ενώ τα κράτη έχουν αρχίσει να χρησιμοποιούν κυρώσεις και να συντάσσουν κατηγορητήρια για να τιμωρήσουν τον υποτιθέμενο εισβολέα τους και το κράτος που τον υποκινεί και υποστηρίζει. Τα πράγματα βέβαια περιπλέκονται και πρόκειται να καταστούν ακόμα πιο πολύπλοκα εφόσον ιδιωτικές εταιρείες καταστούν αυτόβουλες «κυβερνοδυνάμεις» και ανταλλάσσουν ψηφιακά πυρά όχι μόνο μεταξύ τους αλλά και εναντίων κρατών όχι για λογαριασμό άλλων κρατών αλλά για την εξυπηρέτηση των δικών τους διεθνών εταιρικών συμφερόντων.

Οι φιλελεύθερες ως προς το οικονομικό μοντέλο και δημοκρατικές ως προς την πολιτική διακυβέρνηση χώρες έχουν να αντιμετωπίσουν μια διπλή πρόκληση[88]**:**

- Από τη μία πλευρά να διαμορφώσουν ένα περιβάλλον που να διευκολύνει την ανοικτή διασύνδεση, να ευνοεί την οικονομική ευημερία και το ελεύθερο εμπόριο, να προωθεί την καινοτομία και να διασφαλίζει τη δημόσια ασφάλεια και τις πολιτικές ελευθερίες των πολιτών παράλληλα με την προστασία του ατόμου, της ιδιοκτησίας του και της ιδιωτικής του ζωής.

- Από την άλλη πλευρά τα κράτη δια των κυβερνήσεων τους πρέπει να προστατεύσουν τα δικαιώματα του ιδιωτικού – προσωπικού απορρήτου, την ισονομία, αμεροληψία και δικαιοσύνη κατά την επιβολή του νόμου, τις πηγές και τις μεθόδους συλλογής πληροφοριών και τις κυβερνητικές πληροφορίες που θα μπορούσαν να παρέχουν αθέμιτα ανταγωνιστικά πλεονεκτήματα.

Συμπερασματικά, θα μπορούσε να συνάγει κάποιος από την εμπειρική πρακτική τα ακόλουθα:

- Η πρακτική δυνατότητα του κυβερνοχώρου να δημιουργήσει σταθερές σχέσεις ισχύος παραμένει μάλλον εύθραυστη και αμφίβολη.

- Η πρόσβαση στο διαδίκτυο αποτελεί απαραίτητη προϋπόθεση για τη χρησιμοποίηση του κυβερνοχώρου ως χώρου παρουσίας με σκοπό την άσκηση ισχύος και την συμμετοχή στην πολιτική δράση.

- Η προσβασιμότητα και η συμμετοχή στην διαδικτυακή άσκηση επιρροής δεν εξασφαλίζει συνθήκες πολιτικής ελευθερίας σε ένα στεγανοποιημένο περιβάλλον από φαινόμενα κρατικής ή εταιρικής λογοκρισίας, από άσκηση συνειδητής παραπληροφόρησης προερχόμενη από επίσημους φορείς/θεσμούς και από ιδιώτες και από φυσική ή ψυχολογική βία.

---

[87] Cyber Operations Tracker
https://www.cfr.org/interactive/cyber-operations#Takeaways
https://www.cfr.org/about

[88] ‘’2009 Cyberspace Policy Review’’, Department of Homeland Security, p.iii

- Το διαδίκτυο έχει μάλλον ενισχύσει τους μη κρατικούς δρώντες περισσότερο σε σχέση με Κράτη[89], αλλά τα αποτελέσματα αυτής της επίδρασης δεν είναι συνεπή έναντι των διαφόρων πολιτικών περιβαλλόντων, καθώς περιορίζονται από τον τύπο των πολιτικών καθεστώτων και το είδος της ζητούμενης διαπραγμάτευσης.

Ακόμα και αν η ισχύς στον κυβερνοχώρο υφίσταται συνεχώς την απειλή της έκλυσης βίας, η απόλυτη νίκη της βίας πάνω στην ισχύ στον κυβερνοχώρο θα σήμαινε όχι μόνο την σιωπή της φωνής ενός λαού ή των ανθρώπων γενικά, αλλά και την παραίτηση από οποιαδήποτε προοπτική ενσωμάτωσης στο διεθνές σύστημα και στα οφέλη που προσφέρει αυτή[90].

Η παρουσία όλο και περισσότερων δρώντων στον κυβερνοχώρο σημαίνει ταυτόχρονα ότι και οι διαμεσολαβητές πολλαπλασιάζονται, οι οποίοι μπορεί να έχουν ή να μην έχουν οποιοδήποτε μερίδιο ισχύος ή έναν άμεσα αισθητό ρόλο στις λειτουργίες της κρατικής εξουσίας. Ένας τρόπος για να καταδείξουμε γιατί αυτό είναι προβληματικό, είναι να ανατρέξουμε στον φιλόσοφο Bertrand Russell, ο οποίος παρατηρεί ότι η ισχύς μπορεί να θεωρηθεί ως «παραγωγή επιδιωκόμενων αποτελεσμάτων»[91]. Αυτό παραμένει η επικρατούσα αντίληψη των στρατηγιστών, για τους οποίους η στρατηγική θεωρείται πως είναι η τέχνη του ξεκλειδώματος της εξουσίας, που είναι σύμφυτη προς τις εθνικές ικανότητες επηρεασμού των αποτελεσμάτων στο επίπεδο του εθνικού ενδιαφέροντος, σε ανταγωνισμό με άλλους στρατηγιστές που ενεργούν ομοίως σύμφωνα με τα δικά τους εθνικά συμφέροντα. Ο ισχυρισμός του Russell μπορεί να συμπλέει με πολλούς που βλέπουν την ισχύ μέσω των εστιακών φακών της άμεσης αιτίας και αποτελέσματος, ωστόσο αυτή η εικόνα είναι τόσο περίπλοκη εξαιτίας του χαρακτήρα του κυβερνοχώρου[92].

Η αλληλεξάρτηση και η διασυνδεσιμότητα των μαζικά δικτυωμένων χρηστών και συσκευών τροποποιούν αμετάκλητα τις παραδοσιακές δυναμικές της αιτίας και του αποτελέσματος. Αντί της μηχανιστικής ανίχνευσης της διάδοσης των ιδεών και των εικόνων μέσω των κόμβων και των συνδέσεων των παλαιότερης μορφής δικτυώσεων, στη σύγχρονη «μιντιακή οικολογία», «κανένας δεν γνωρίζει ποιοι θα είναι οι μάρτυρες ενός γεγονότος, πού και πότε θα το αντιληφθούν ή πώς θα το ερμηνεύσουν»[93]. Αυτό σημαίνει ότι τα αποτελέσματα της ισχύος στον κυβερνοχώρο μπορεί να είναι τόσο ακούσια όσο και εκούσια. Στην περίπτωση των μη κρατικών δρώντων, πολλοί από αυτούς μπορεί να καταστούν αθέλητα θύματα της κυβερνοισχύος αν, για παράδειγμα, ασκηθεί αυτή ανεύθυνα ή χωρίς να ληφθούν δεόντως υπόψη οι πιθανότητες της παραγωγής παράπλευρων

---

[89] Daniel W. Drezner "WEIGHING THE SCALES: THE INTERNET'S EFFECT ON STATE-SOCIETY RELATIONS", Brown Journal of World Affairs, Vol. 16, No. 2, p.31-44, Spring / Summer 2010, http://www.danieldrezner.com/research/scales.pdf

[90] Katharina C. Below, "The Utility of Timeless Thoughts: Hannah Arendt's Conceptions of Power and Violence in the Age of Cyberization", [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.111

[91] Betrand Russell, "Power: A new Social Analysis", G. Allen Unwin LTD, London, chapter III, p.35

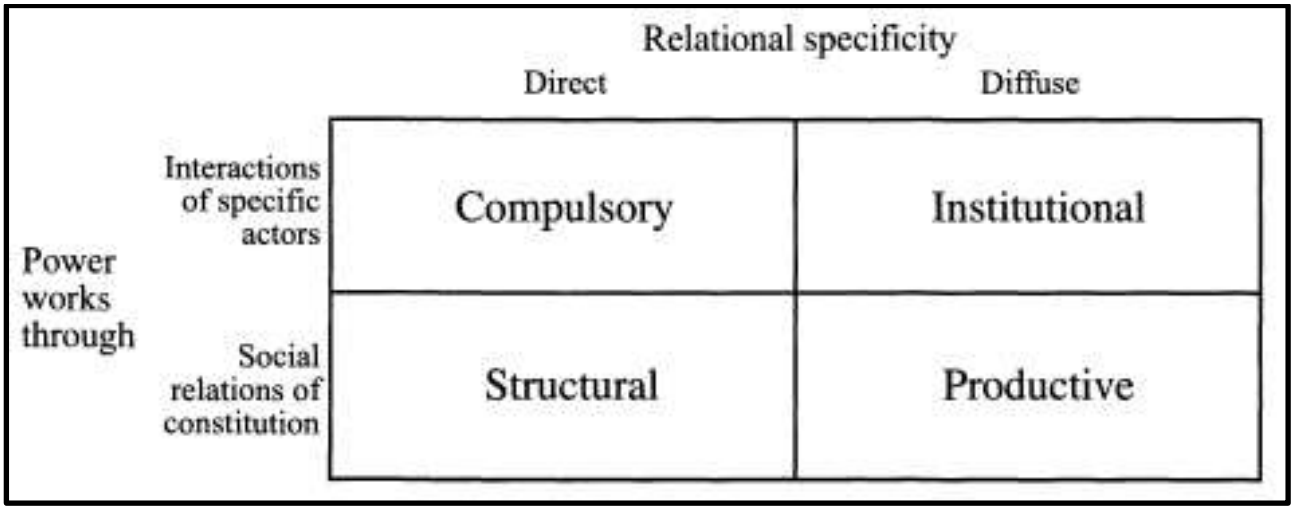
[92] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.40

[93] Andrew Hoskins & Ben O'Loughlin, "War and Media: The Emergence of Diffused War", Malden, MA, Cambridge: Polity, 2010, p.2.

απωλειών[94]. Πρακτικά, η ισχύς, με τα αποτελέσματα που επιφέρει και δια των οποίων εμμέσως γίνεται αντιληπτή, περιβάλλει ή διαπερνά και σε κάθε περίπτωση διαχέει την ουσία της εντός και εκτός του κυβερνοχώρου, καθώς οι σχέσεις, μέσω των οποίων ενεργοποιείται και δομείται. δεν ορίζονται αποκλειστικά από ή στον κυβερνοχώρο αλλά και σε αυτόν και από αυτόν, καθόσον η «αποκάλυψή» των εξωτικών του διαστάσεων διεύρυνε αντίστοιχα τα σύνορα του φυσικού χώρου.

Στο σημείο αυτό αξίζει να επισημανθεί ότι ο αγαπημένος, από τους σύγχρονους σχολιαστές ή και μελετητές, νεολογισμός της «κυβερνοισχύος» έχει στην πραγματικότητα υποκειμενική υφή, καθόσον ο προσδιορισμός «κυβερνό- » διατηρεί και εμπεριέχει τα τοπολογικά χαρακτηριστικά του περιβάλλοντος που αντιπροσωπεύει με τρόπο όμοιο προς τη χρησιμοποίηση των εννοιών της Θαλάσσιας Ισχύος ή της Αεροπορικής Ισχύος, εκφράζοντας έτσι την αντικειμενική δυνατότητα που διαθέτει κάποιος να κάνει[95] κάτι στο συγκεκριμένο περιβάλλον, είτε αναφέρεται στον αέρα είτε στη θάλασσα είτε στον κυβερνοχώρο! Η κυβερνοισχύς αντιπροσωπεύει τελικά την εκδήλωση της κλασσικής ισχύος στον κυβερνοχώρο και όχι μια νέα, διαφορετικής μορφής ή είδους ισχύος.

Σύμφωνα με τους M.Barnett & R.Duvall υφίστανται τέσσερις βασικές μορφές εκδήλωσης της ισχύος των οποίων τα αποτελέσματα μπορούν να γίνουν αντιληπτά στον κυβερνοχώρο.



ΔΙΑΓΡΑΜΜΑ 2: Ταξινόμηση της Ισχύος[96]

- **«Κυβερνοισχύς του Εξαναγκασμού».** Εκφράζει τη χρήση του άμεσου εξαναγκασμού από έναν δρώντα του κυβερνοχώρου στην προσπάθειά του να τροποποιήσει τη συμπεριφορά και τις συνθήκες ύπαρξης ενός άλλου. Το δε

[94] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.40

[95] William Mitchell, "Winged Defense: The Development and Possibilities of Modern Air Power – Economic and Military", Dover Publications, New York, 1988, p.xii.

[96] M.Barnett & R.Duvall –''Power in International Politics'', International Organization, Vol. 59, No. 1 (Winter, 2005), (pp. 39-75) Published by: Cambridge University Press on behalf of the International Organization Foundation, p.48 https://www.researchgate.net/publication/4854229_Power_in_International_Politics/link/5c49b5fc92851c22a38ccf51/download

υποκείμενο του εξαναγκασμού μπορεί να είναι ένας ηλεκτρονικός υπολογιστής ή ένα σύστημα – δίκτυο υπολογιστών ή ο χειριστής/ες αυτών ή το πρόσωπο ή ο θεσμός που επωφελείται πίσω από τους υπόψη χειριστές και ηλεκτρονικά δίκτυα. Ο περιορισμός των κινήτρων και των δυνατοτήτων ενός αντιπάλου ως επιθυμητό αποτέλεσμα της «κατανάλωσης» ισχύος εξαναγκασμού μπορεί να παραχθεί μόνον αν οι δρώντες – θύματα / δέκτες αντιληφθούν ή αναγνωρίσουν ότι πόροι που κατευθύνουν την ισχύ εναντίον τους έχουν δαπανηθεί ή θυσιαστεί και ταυτόχρονα έχουν πεισθεί για την αξιοπιστία των απειλών που στρέφονται εναντίον τους. Ως εκ τούτου, τόσο οι τύποι εκδήλωσης ισχύος εξαναγκασμού στον κυβερνοχώρο είναι δύσκολο να ασκηθούν - εφαρμοστούν, όσο και τα επιθυμητά αποτελέσματα είναι δύσκολο να παραχθούν – υλοποιηθούν.

- **«Θεσμική κυβερνοισχύς»[97].** Αναφέρεται στον έμμεσο έλεγχο ενός «κυβερνοδρώντα» από έναν άλλο διά της μεσολάβησης επίσημων ή ανεπίσημων θεσμών. Αν ο διαμεσολαβητικός θεσμός ενεργεί κάτω από τον απόλυτο έλεγχο ενός κρατικού δρώντα, τότε δεν μιλάμε για θεσμική κυβερνοισχύ, αλλά για ισχύ του «κυβερνοεξαναγκασμού». Η θεσμική ισχύς στο κυβερνοχώρο υφίσταται μόνον όταν ένας δρώντας είναι ικανός να επηρεάσει τους τρόπους με τους οποίους οι διαμεσολαβητικοί θεσμοί ενεργούν έτσι ώστε να «καθοδηγούν, να κατευθύνουν και να περιορίζουν τις ενέργειες ή την έλλειψη ενεργειών και τις συνθήκες ύπαρξης των άλλων. Στο κυβερνοχώρο, κρατικοί μηχανισμοί και μέσα μπορούν να χρησιμοποιηθούν για να ορίσουν «κανόνες και πρότυπα» για μια σειρά από θεσμούς που επιδρούν πάνω στην συμπεριφορά των χρηστών. Κλασσικά παραδείγματα τέτοιων προσπαθειών είναι η σύσταση από την πλευρά των ΗΠΑ του οργανισμού «Internet Corporation for Assigned Names and Numbers, ICANN», από την πλευρά της Ρωσίας του οργανισμού «International Telecommunication Union, ITU» και από της Κίνας του οργανισμού «Shanghai Cooperation Organisation, SCO).

- **«Δομική Κυβερνοισχύς».** Επενεργεί για τη διατήρηση των δομών μέσα στους οποίους εντοπίζονται όλοι οι δρώντες και σε μεγάλο βαθμό επιτρέπει ή περιορίζει τις ενέργειες που αυτοί επιθυμούν να υλοποιήσουν σε σχέση με τους άλλους με τους οποίους είναι άμεσα διασυνδεδεμένοι[98]. Σε αυτό το πλαίσιο, ενδιαφερόμαστε περισσότερο στο πώς ο κυβερνοχώρος βοηθά στον καθορισμό αυτών των δομικών θέσεων, παρά στο πώς οι δρώντες, που προέκυψαν μέσα σε αυτόν, διαμορφώνουν τον ίδιο τον κυβερνοχώρο. Αν και πιθανότατα δεν είναι δυνατό να συμπεράνουμε ότι ο κυβερνοχώρος κάνει κάτι που να συσχετίζεται άμεσα με την διεθνή τάξη, ωστόσο ένα αρχικό σημείο αναφοράς είναι να διερωτηθούμε αν ο κυβερνοχώρος διατηρεί τους υφιστάμενους δομικούς τύπους ή συμβάλλει στην δημιουργία νέων. Έτσι λοιπόν, πολλοί[99] ισχυρίζονται ότι η ιδέα της «πληροφοριακής

[97] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.47

[98] Barnett and Duvall, 'Power in International Politics', pp. 52–5.

[99] Fritz Machlup, "The Production and Distribution of Knowledge in the United States", Princeton, NJ: Princeton University Press, 1962.

Peter F. Drucker, "The Age of Discontinuity: Guidelines to Our Changing Society", London, Pan Books, 1971.

Daniel Bell, "The Coming of the Post-Industrial Society: A Venture in Social Forecasting", London, Heinemann Educational, 1974.

κοινωνίας (informational society)» είναι στενά συνδεδεμένη με τα ηλεκτρονικά δίκτυα που έχουν μετατρέψει τα δεδομένα, τις πληροφορίες και τις γνώσεις σε αγαθά. Άλλοι μελετητές έχουν συνδέσει την εμφάνιση και κυριάρχηση των δικτύων[100] με την παγκοσμιοποίηση του κεφαλαίου και την μεταμόρφωση του καπιταλισμού! Ίσως βέβαια να είναι πιο ακριβές, τουλάχιστον προς το παρόν, ότι ο τύπος οργάνωσης μιας καπιταλιστικής κοινωνίας μεταβάλλεται, αλλά όχι σε βαθμό που να μην είναι αναγνωρίσιμος. Οι τεχνολογίες της πληροφορίας έχουν επιβάλλει πολλές αλλαγές, αλλά δεν τα έχουν αλλάξει όλα[101]. Τουλάχιστον όχι ακόμα, αν και η επικείμενη εδραίωση της τεχνολογίας της τεχνητής νοημοσύνης μάλλον θα χαράξει ρότα σε αχαρτογράφητα κοινωνιολογικά και διεθνοπολιτικά νερά. Τα κοινωνικά και πολιτικά δίκτυα (social and civic networks), δομημένα γύρω από τα εργαλεία, τις ευκαιρίες και τα φόρα που προσφέρει ο κυβερνοχώρος, μπορούν πλέον να υπερκεράσουν και σε ορισμένες περιπτώσεις να αντικαταστήσουν τις ιεραρχικές δομές τις βιομηχανικής περιόδου. Τα γεγονότα, που σχετίζονται με αυτό που ονομάστηκε εμφατικά ως Αραβική Άνοιξη, αν μη τι άλλο κατέδειξαν αφενός την αντικειμενική δυνατότητα των διαδικτυακά διασυνδεδεμένων δικτύων να οργανώνουν και να κινητοποιούν ακτιβιστικές δραστηριότητες αντίστασης ή ομαδικής απείθειας φαινομενικά ή πραγματικά πέρα από τον θέληση των κρατών και τις αργόσυρτες γραφειοκρατικές τους νόρμες και συστήματα ελέγχου[102], αφετέρου τη σπουδή των κυβερνήσεων να καταστείλουν τέτοιες δράσεις[103]. Μπορεί ο ρόλος του διαδικτύου να υπερεκτιμάται από κάποιους ως προς τη δυνατότητα άσκησης σημαντικής επίδρασης κατά την προσπάθεια ανατροπής ενός καθεστώτος, ωστόσο σίγουρα συμβάλλει καθοριστικά στην δημοσιοποίηση και διεθνοποίηση ζητημάτων που απασχολούν ομάδες ενεργών ή ακόμα και μεμονωμένων ανήσυχων πολιτών κατά τρόπο που δεν θα ήταν δυνατό να γίνει γνωστός ο σκοπός του αγώνα τους αν δεν υπήρχε η πολλαπλασιαστική δύναμη που προσφέρει το διαδίκτυο, το οποίο λειτουργεί ως ενισχυτής ή μοχλός. Επιπλέον, από τα παραπάνω, εύκολα συνάγει κάποιος ότι η δομική κυβερνοισχύς μπορεί να ενεργεί τόσο με σκοπό τη διατήρηση της καθεστηκυίας τάξης όσο και για την ανατροπή του status quo ή έστω την παρενόχλησή του!

- **«Παραγωγική Κυβερνοισχύς».** Ο κυβερνοχώρος, ως πληροφοριακό περιβάλλον, είναι ένα ιδανικό πεδίο για την άσκηση και μετάδοση παραγωγικής κυβερνοισχύος. Αυτή συνίσταται στη διαμόρφωση κοινωνικών θεμάτων μέσω του διαλόγου που ενεργοποιείται και διευκολύνεται στον κυβερνοχώρο, ορίζοντας συνεπώς τα «πεδία της δυνατότητας» τα οποία περιορίζουν και διευκολύνουν την κοινωνική δράση[104]. Ο κυβερνοχώρος εξυπηρετεί στην «μιντιακή» αναπαραγωγή και

[100] Manuel Castells, "The Rise of the Network Society", Malden, MA and Oxford: Blackwell, 2000, p.21-31.
[101] Christian Fuchs, "Internet and Society: Social Theory in the Information Age", New York and Abingdon: Routledge, 2008.
[102] Manuel Castells, "The Internet Galaxy: Reflections on the Internet, Business, and Society", Oxford, Oxford University Press, 2001, p. 138.
[103] Hannah Roberts, "The Turkish Government reportedly blocked WhatsApp and other social media sites", Nov. 4, 2016, 10:43 AM
https://www.businessinsider.com/social-media-and-messaging-sites-blocked-in-turkey-2016-11
[104] Clarissa Rile Hayward, "De-Facing Power", Cambridge: Cambridge University Press, 2000, p. 30. Cited in Barnett and Duvall, 'Power in International Politics', p. 56.

ενίσχυση των υφιστάμενων συζητήσεων, καθώς και στην ανάπτυξη και διάδοση νέων. Με πολλούς τρόπους, η παραγωγική κυβερνοισχύς είναι το θεμέλιο για άλλες μορφές κυβερνοισχύος. Χωρίς τα κονστρουκτιβιστικής χροιάς υποκείμενα της κοινωνικής δικτύωσης, που «χτίζουν» το διαδικτυακό τους προφίλ, δεν υφίστανται οι παράγωγες κοινωνικές «κυβερνοσχέσεις» μέσω των οποίων εκδηλώνεται η ισχύς. Η παραγωγική κυβερνοισχύς συνδέει επίσης τον στρατιωτικό τομέα με την πολιτική σφαίρα όταν εκδηλώνεται το πολεμικό φαινόμενο, επιδιώκοντας να διαμορφώσει συνθήκες κυριαρχίας στον λόγο, στο προκρινόμενο αφήγημα, στην αντίληψη της «κοινής γνώμης» για την τρέχουσα πραγματικότητα ή για αυτή που πρόκειται ή επίκειται να διαμορφωθεί προς όφελος ενός στρατηγικού παίχτη[105]. Αυτό γίνεται ιδιαίτερα εμφανές κατά τη χρήση της «ήπιας» ισχύος με σκοπό να κερδίσει τις καρδιές και τα μυαλά, είτε κατά τη διάρκεια μιας σύγκρουσης ή πριν από αυτήν. Στην εποχή της «στρατηγικής επικοινωνίας» (strategic communications, STRATCOM) και της δημόσιας διπλωματίας (Public Diplomacy), η παραγωγική κυβερνοισχύς ίσως είναι η πιο σημαντική μορφή εκδήλωσης της κυβερνοισχύος[106]. Ο πλέον χαρακτηριστικός τρόπος με τον οποίο τα Κράτη επιδεικνύουν την παραγωγική τους κυβερνοισχύ είναι μέσω της κατασκευής φορέων απειλής στον κυβερνοχώρο. Με τον επίσημο χαρακτηρισμό ορισμένων δρώντων ως απειλές για την εθνική ασφάλεια, τα κράτη εξασφαλίζουν την επιθυμητή νομιμοποίηση ώστε να ακολουθήσουν πολιτικές και στρατηγικές που έχουν σχεδιαστεί για να αντιμετωπίζονται ως νόμιμοι στόχοι άλλων μορφών κρατικής εξουσίας.

Είναι ωστόσο σημαντικό να σημειωθεί ότι οι παραπάνω μορφές κυβερνοισχύος δεν λειτουργούν ανεξάρτητα και απομονωμένα μεταξύ τους. Κάτι τέτοιο θα μπορούσε να χαρακτηριστεί ως ιδιαίτερη εξαίρεση. Η Ισχύς μπορεί να θεωρηθεί ως μια «οικογένεια» σχετικών δυναμικών οι οποίες αν και διατηρούν την ιδιαιτερότητά τους, αλληλεπιδρούν για να σχηματίσουν μια συνισταμένη που περιγράφουμε γενικά ως «ισχύς».

4.2. Η Διεθνοπολιτικού Χαρακτήρα Βία στον Κυβερνοχώρο

4.2.1. Από της Ψηφιακές Επιθέσεις μέχρι τον Κυβερνοπόλεμο

Ο Cornish[107] εντοπίζει 4 τομείς για την κατηγοριοποίηση των πηγών των κυβερνοεπιθέσεων: επιθέσεις που προέρχονται και κατευθύνονται από τα κράτη (state-sponsored), από τον ιδεολογικό και πολιτικό εξτρεμισμό, από το οργανωμένο έγκλημα και από την ατομική εγκληματική δράση χαμηλού επιπέδου. Η Βρετανική Στρατηγική Ασφαλείας αναγνωρίζει 4 πηγές κυβερνοαπειλών, θεωρώντας ως αδιαίρετο τον τομέα της εγκληματικότητας στο διαδίκτυο, είτε αυτή αναφέρεται σε δραστηριότητες του οργανωμένου εγκλήματος, είτε σε μεμονωμένα εγκληματικά στοιχεία με μικρό σχετικά κύκλο εργασιών, αλλά διαχωρίζοντας τους τρομοκράτες και τα όργανά αυτών, τους «κυβερνοτρομοκράτες»

[105] Carsten F. Roennfeldt, 'Productive War: A Re-Conceptualisation of War', Journal of Strategic Studies, vol. 34, no. 1, 2011, pp. 39–62.

[106] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.51

[107] Cornish, et al. ''Cyberspace and the national security of the United Kingdom. Threats and responses'', Chatham House Report, London, 2009, p.3

από του διαδικτυακούς ακτιβιστές (hactivists). Τη λίστα συμπληρώνουν φυσικά, ως ενιαία πηγή οι υπηρεσίες πληροφοριών – ασφαλείας και οι στρατιωτικές υπηρεσίες των κρατών.

Οποιαδήποτε αναφορά σε σύγκρουση στον κυβερνοχώρο προϋποθέτει ψηφιακή ανταπόδοση σε μία ψηφιακή επίθεση, έστω και μοναδική, δηλαδή ψηφιακή αντεπίθεση σε μια κυβερνοεπίθεση που αποφάσισε να εξαπολύσει μία αντίπαλη πλευρά εναντίων των ψηφιακών ή ψηφιοποιημένων υποδομών, έστω και εναντίον ενός μεμονωμένου ηλεκτρονικού συστήματος – ηλεκτρονικού υπολογιστή ή εναντίον του συνόλου των ψηφιακών δικτύων που διαθέτει μία άλλη αντίπαλη πλευρά. Συνεκδοχικά, η αναφορά στην έννοια του κυβερνοπολέμου θα πρέπει να περιλαμβάνει σειρά ψηφιακών συγκρούσεων, δηλαδή την ανταλλαγή κυβερνοεπιθέσεων, όχι κατ΄ ανάγκη διατηρώντας χρονική ή χωρική συνέχεια, αλλά που εντάσσονται στο αυτό πλαίσιο εκδήλωσης ή κορύφωσης του ανταγωνισμού ισχύος. Φυσικά, ο ανταγωνισμός ισχύος εκδηλώνεται ποικιλοτρόπως και σίγουρα όχι αποκλειστικά με την ανταλλαγή ψηφιακών πυρών, ούτε όμως απαραίτητα η ανταλλαγή κυβερνοεπιθέσεων και η διεξαγωγή κυβερνοπολέμου προϋποθέτει αναγκαστικά την προσβολή και «υφαρπαγή των φορτίων ισχύος»[108] του αντιπάλου παράλληλα και με άλλα μέσα, τα οποία είναι δυνατό να μεταχειριστεί ένας δρών στο πλαίσιο του πολεμικού φαινομένου, όπως για παράδειγμα με την άσκηση βίας με τη χρήση συμβατικών ή πυρηνικών όπλων. Αυτό που γίνεται ολοένα πιο ξεκάθαρο είναι ότι ο πόλεμος στον κυβερνοχώρο είναι πόλεμος, η ένταση και τα αποτελέσματα του οποίου κλιμακώνονται, γεγονός που επηρεάζει τη σχέση της αναλογικότητας στην ανταπόδοση των επιθέσεων και όχι στη αντικειμενική φύση του ίδιου του πολεμικού φαινομένου.

Βεβαίως, παρά την αντικειμενική δυσκολία σαφούς διαχωρισμού, η ψηφιακή ανταπόδοση σε μία ψηφιακή επίθεση, μπορεί να λάβει είτε τη μορφή αντιμέτρων, όπως τα νοηματοδοτεί η διεθνής πρακτική[109], ώστε το κυρίαρχο κράτος που τα ενεργοποιεί να απολαμβάνει διεθνοπολιτική νομιμοποίηση των ενεργειών που αποσκοπούν στην άμυνά του, είτε με τη μορφή αντιποίνων, οπότε προσβάλλεται πρωτίστως η έννοια της αναλογικότητας[110] και επομένως η επίκληση στο δικαίωμα της «νόμιμης άμυνας» καθίσταται τουλάχιστον μαχητή.

Ο πυρήνας του σκοπού του κυβερνοπολέμου είναι η εξασφάλιση της δυνατότητας του ελέγχου από τη μία πλευρά και η αποφυγή του ελέγχου από την άλλη. Στο επίπεδο του διακρατικού ανταγωνισμού ή του ανταγωνισμού μεταξύ οργανισμών, διεθνών ή μη, εμπορικών ή μη, η ουσία του κυβερνοπολέμου έγκειται στην ταπεινή πρόθεση του εκβιασμού και εξαναγκασμού μεταβολής της συμπεριφοράς του Άλλου[111]. Κοντολογίς, στην απόκτηση και διατήρηση του ελέγχου της στάσης και συμπεριφοράς, άρα και των

---

[108] Σπ.Λίτσας, "Πόλεμος και Ορθολογισμός, Θεωρητικές προεκτάσεις και στρατηγικές εφαρμογές", Εκδόσεις ΠΟΙΟΤΗΤΑ, 2011, Βάρη Αττικής

Σημείωση: Λατρεμένη έκφραση, «κλεμμένη» από τον κ. Αναπληρωτή Καθηγητή Σπυρίδωνα Λίτσα κατά τις παραδόσεις του στη διάρκεια των Μεταπτυχιακών Σπουδών μου στο Τμήμα Διεθνών & Ευρωπαϊκών Σπουδών του Πανεπιστημίου Μακεδονίας).

[109] ICJ Rep.1996, 226, 245, 263, §§42-43, 96-97 [Κ.Αντωνόπουλος, Κ.Μαγκλιβέρας, ''Το Δίκαιο της Διεθνούς Κοινωνίας'', Αθήνα, Εκδ. Νομική Βιβλιοθήκη, 2017 (3η έκδοση), σελ.738

[110] Κ.Αντωνόπουλος, Κ.Μαγκλιβέρας, ''Το Δίκαιο της Διεθνούς Κοινωνίας'', Αθήνα, Εκδ. Νομική Βιβλιοθήκη, 2017 (3η έκδοση), σελ.738, υποσημείωση 46 [US reaction to ICJ Judgment in Iranian Oil Platforms Case, 2004]

[111] Hannah Samir Kassab, "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare, [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.75

αποφάσεων[112] που καθορίζουν κάθε φορά την εκδήλωση των δύο εννοιών, εξαιτίας της ροής ή της απουσίας των πληροφοριών που τελικά έχουμε στη διάθεσή μας ή λαμβάνουμε υπόψη κατά την επεξεργασία τους για την εξαγωγή συμπερασμάτων ή για την εκτίμηση του ρίσκου και του συμφέροντος, ώστε να ορισθεί η κλίση της πλάστιγγας. Έτσι, ο κυβερνοπόλεμος αποτελεί άλλη μια έκφραση της σχέσης ισχύος, όπως την ορίζει ο J.Rosenau ως σκόπιμου ελέγχου[113] (calculated control).

Όπως επεξηγεί ο Γ.Μ.Σπυρόπουλος[114], «στη σχέση ισχύος υπάρχουν δύο δρώντες, ο ελεγκτής και ο ελεγχόμενος, με τον δεύτερο να υπόκειται στην άσκηση ισχύος του πρώτου» και ότι «η ισχύς του ελεγκτή επηρεάζει την κυριαρχία του ελεγχόμενου», ενώ η ίδια η σχέση ισχύος «προϋποθέτει μια κυβέρνηση – ελεγχόμενη και ορθολογικά δρώσα, υπό την έννοια ότι διαθέτει την ικανότητα να προβαίνει σε σωστό υπολογισμό συμφερόντων». Η παραπάνω ιδέα θέτει τα θεμέλια του επιχειρήματος ότι η εκδήλωση κυβερνοεπίθεσης ενός κρατικού δρώντα που φιλοδοξεί να παίξει το ρόλο του ελεγκτή εναντίον ενός κρατικού δρώντα - ελεγχόμενου αποτελεί προσβολή της κυριαρχίας του δευτέρου και συνεπώς νομιμοποιείται στο πλαίσιο της διεθνούς έννομης τάξης όπως έχει θεσμοθετηθεί σήμερα, η άσκηση του δικαιώματος της νόμιμης άμυνας. Το πιο ισχυρό κίνητρο για μια «υπολογισμένη» κυβερνοεπίθεση, τουλάχιστον προς το παρόν, είναι σύμφωνα με τον Matsubara[115] ότι οι επιτιθέμενοι μπορούν να αποφύγουν τις διεθνείς κυρώσεις επειδή δεν υπάρχει επί του παρόντος διεθνής συναίνεση ως προς το τι στην πραγματικότητα συνιστά «ένοπλη επίθεση» ή «επικείμενη απειλή» στον κυβερνοχώρο (έτσι ώστε να μπορεί να επικαλεσθεί το κράτος – θύμα το δικαίωμα στην αυτοάμυνα δυνάμει του άρθρου 51 του Χάρτη των Ηνωμένων Εθνών). Έτσι λοιπόν, ενώ ορισμένες χώρες, συμπεριλαμβανομένων των Ηνωμένων Πολιτειών και της Ιαπωνίας, επιμένουν ότι ισχύουν οι αρχές του διεθνούς δικαίου στον τομέα του κυβερνοχώρου, άλλοι όπως η Κίνα ισχυρίζονται ότι οι επιθέσεις στον κυβερνοχώρο δεν απειλούν την εδαφική ακεραιότητα ή κυριαρχία.

Στο πλαίσιο του Δομικού Ρεαλισμού, ο κυβερνοπόλεμος δεν αποτελεί παρά μια ακόμα δυνατότητα που παρέχουν τα κυβερνοόπλα, όπως ακριβώς η χρησιμοποίηση συμβατικών ή πυρηνικών όπλων, όπως η χρησιμοποίηση των εργαλείων των ψυχολογικών επιχειρήσεων. Ένα ακόμα εξάρτημα στη δομή του Διεθνούς Συστήματος και της κατανομής των δυνατοτήτων και της ισχύος μέσα σε αυτό. Όσο διατηρεί συντριπτικά πλεονεκτήματα[116] δηλαδή παραμένει μια οικονομική και ευχερής επιλογή, που εμπεριέχει το στοιχείο του αιφνιδιασμού και που δύσκολα εντοπίζεται η πηγή εκπομπής των «κυβερνοπυρών» της (στοιχείο της αφάνειας) και ακόμα δυσκολότερα αποδίδεται η ευθύνη των αποτελεσμάτων της, οι ανταγωνιστές ισχύος θα την προτιμούν. «Είναι ο Ορθολογισμός, ηλίθιε», παραφράζοντας την γνωστή πολιτική ατάκα. Μέσα από τον πολιτικό ρεαλισμό και την

---

[112] Η.Κουσκουβέλης, ‘’Θεωρία Απόφασης στον Θουκυδίδη’’, Εκδ. Πανεπιστημίου Μακεδονίας, Θεσσαλονίκη, 2015 σελ.33

[113] J.Rosenau, ‘’The scientific Study of Foreign Policy’’, London, Collier-MacMillan, 1971, p.216

[114] Γ.Μ.Σπυρόπουλος, ‘’Διεθνείς Σχέσεις, Ρεαλιστική Προσέγγιση, Θεωρία και Πράξη’’, Αθήνα, Εκδόσεις Ποιότητα, 2010, σελ.100

[115] Mihoko Matsubara, ‘’A Stuxnet Future? Yes, Offensive Cyber-Warfare is Already Here’’, 2012, https://www.files.ethz.ch/isn/188327/ISN_154091_en.pdf

[116] Mihoko Matsubara, ‘’A Stuxnet Future? Yes, Offensive Cyber-Warfare is Already Here’’, 2012, https://www.files.ethz.ch/isn/188327/ISN_154091_en.pdf

σύνδεση με τη θεωρία πολέμου, ο Σπ.Λίτσας[117] εκλαμβάνει την επιλογή του πολέμου ως παράγωγο ορθολογισμού όταν «έχει να κάνει με την αποτελεσματική χρήση βίας, ώστε να επιτυγχάνονται οι στόχοι που θέτει ένα κράτος που καταφεύγει στον πόλεμο με όσο το δυνατόν μικρότερο φορτίο φθοράς και μέσα σε σχετικά σύντομο χρονικό διάστημα». Υπό το πρίσμα αυτό και σύμφωνα με τα βασικά κριτήρια για τον χαρακτηρισμό ενός πολέμου ως ορθολογικό[118] (ορθολογικό σχεδιασμό του πολέμου, ορθολογική αποτίμηση κόστους – οφέλους, ορθολογική παύση του πολέμου), η επιλογή του κυβερνοπολέμου μπορεί να αποτελέσει μια ορθολογική επιλογή των διεθνών δρώντων.

Σύμφωνα με τον Herbert S.Lin[119] οι εχθρικές ενέργειες - δραστηριότητες εναντίον ενός συστήματος ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών μπορεί να εμφανιστεί με δύο μορφές, μία με καταστρεπτική φύση και μία με μη καταστρεπτική. Ένα παράδειγμα καταστρεπτικής φύσης εχθρικής ενέργειας είναι η διαγραφή ψηφιακών δεδομένων από έναν ψηφιακό «ιό» που έχει «εγκατασταθεί» στο σκληρό δίσκο οποιουδήποτε μολυσμένου ηλεκτρονικού υπολογιστή.

- Μια καταστρεπτικού χαρακτήρα επίθεση στον κυβερνοχώρο, δηλαδή μια κυβερνοεπίθεση (Cyber-attack), αναφέρεται στη χρήση σκόπιμων ενεργειών και πράξεων, ίσως για μεγάλο χρονικό διάστημα, με σκοπό να αλλάξει, να διαταράξει, να εξαπατήσει, να υποβαθμίσει ή να καταστρέψει τα ηλεκτρονικά συστήματα του αντιπάλου ή τα δίκτυα ηλεκτρονικών υπολογιστών ή τις πληροφορίες και / ή τα προγράμματα που βρίσκονται εγκατεστημένα σε αυτά τα συστήματα και δίκτυα ή διακινούνται μέσω αυτών των συστημάτων ή δικτύων. Τέτοιες επιπτώσεις στα αντίπαλα ηλεκτρονικά συστήματα και δίκτυα ενδέχεται επίσης να έχουν έμμεσες επιπτώσεις στις οντότητες που συνδέονται ή εξαρτώνται από αυτά. Μια κυβερνοεπίθεση επιδιώκει να καταστήσει τα συστήματα ηλεκτρονικών υπολογιστών και τα δίκτυα του αντιπάλου μη διαθέσιμα ή μη αξιόπιστα και επομένως λιγότερο ή καθόλου χρήσιμα στον αντίπαλο.

- Η δεύτερη μορφή εχθρικής ενέργειας στον κυβερνοχώρο, η «κυβερνοεκμετάλλευση» (cyberexploitation) είναι μη καταστροφική. Ένα παράδειγμα είναι ένας ψηφιακός ιός που αναζητά τον σκληρό δίσκο οποιουδήποτε μολυσμένου υπολογιστή - θύμα και αποστέλλει μέσω ηλεκτρονικού ταχυδρομείου στην εχθρική πλευρά όλα τα αρχεία που περιέχουν αριθμό πιστωτικής κάρτας. Η κυβερνοεκμετάλλευση αναφέρεται στη χρήση ενεργειών και λειτουργιών, ίσως για μια εκτεταμένη χρονική περίοδο, με σκοπό την απόκτηση πληροφοριών που θα μπορούσαν διαφορετικά να διατηρούνται εμπιστευτικές και που βρίσκονται εγκατεστημένες σε αυτά τα συστήματα και δίκτυα ή διακινούνται μέσω αυτών των συστημάτων ή δικτύων. υπολογιστών του θύματος. Οι κυβερνοεκμεταλλεύσεις είναι συνήθως παράνομες και διεξάγονται με την όσο το δυνατόν μικρότερη παρέμβαση που να επιτρέπει την εξαγωγή των ζητουμένων πληροφοριών. Επιδιώκουν δε, να μην διαταράξουν την

[117] Σπυρίδων Ν. Λίτσας, ‘’Πόλεμος και Ορθολογισμός, Θεωρητικές Προεκτάσεις και Στρατηγικές Εφαρμογές’’, Εκδόσεις Ποιότητα, 2010, σελ.19.
[118] Σπυρίδων Ν. Λίτσας, ‘’Πόλεμος και Ορθολογισμός, Θεωρητικές Προεκτάσεις και Στρατηγικές Εφαρμογές’’, Εκδόσεις Ποιότητα, 2010, σελ.113.
[119] Herbert S. Lin, “Offensive Cyber Operations and the Use of Force”, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63], 2010, p.63

αντίληψη του θύματος, ως προς την κανονικότητα της λειτουργίας του συστήματος ή του δικτύου υπολογιστών που ελέγχει ή χρησιμοποιεί, καθώς η καλύτερη περίπτωση είναι το θύμα να μην αντιληφθεί ποτέ τίποτα. Η κυβερνοκατασκοπεία αποτελεί μια κρίσιμης σημασίας «κυβερνοδραστηριότητα». Η ίδια δεν περιλαμβάνει την καταστροφή ηλεκτρονικών συστημάτων ή δεδομένων, αλλά αποσκοπεί στην διείσδυση και παρακολούθηση της ηλεκτρονικής δραστηριότητας των ψηφιακών συστημάτων ή δικτύων ενός αντιπάλου για την απόκτηση πληροφοριών και την εξαγωγή εκτιμήσεων πληροφοριών, οι οποίες μεταξύ άλλων μπορούν ακολούθως να χρησιμοποιηθούν για την άσκηση καταστρεπτικού χαρακτήρα κυβερνοεπιθέσεων με τη χρήση επιθετικών κυβερνοόπλων.

4.2.2. Πράξη Πολέμου ή Μήπως Όχι

Γενικά, ο κυβερνοπόλεμος αναφέρεται σε επιθετικές και αμυντικές ενέργειες. Οι δε κυβερνοεπιθέσεις αφορούν 5 κύριους τύπους τακτικών ενεργειών[120]:

- Κατασκοπεία (espionage) / αναγνώριση (reconnaissance),
- Προπαγάνδα (propaganda),
- Άρνηση χρήσης των διαδικτυακών υπηρεσιών (denial of service - DoS),
- Τροποποίηση – αλλοίωση δεδομένων (data modification) και
- Χειραγώγηση υποδομών (infrastructure manipulation).

Κυρίαρχο ζήτημα σε κάθε αναφορά περί επιθετικής δράσης στον κυβερνοχώρο, εγείρει το θεμελιώδες ερώτημα αν μια τέτοια δραστηριότητα ή μια στιγμιαία καταλυτική προσβολή με κάποιο άγνωστο μέχρι σήμερα κυβερνοόπλο μπορεί να χαρακτηριστεί ως πράξη πολέμου και ως τέτοια να παράγει συγκεκριμένα νομικά πλάσματα στο πλαίσιο της διεθνούς νομολογίας και πρακτικής. Οποιαδήποτε βεβιασμένη υπόδειξη, ανάδειξη ή ανακήρυξη μιας επίθεσης με κακόβουλο λογισμικό ως πράξη πολεμική[121], κινδυνεύει να γίνει αιτία είτε υποβάθμισης των συνεπειών που αυτή επιφέρει άμεσα ή στο μέλλον στην περίπτωση που αποδειχθεί ότι δεν πληροί τις τυπικές προϋποθέσεις ώστε να δικαιολογείται αυτός ο χαρακτηρισμός, είτε να συνεισφέρει στην εκμαυλιστική συνήθεια της απάθειας μπροστά σε πραγματικές πράξεις πολέμου, προσφέροντας ερείσματα στην περιπτωσιολογία των εξαιρέσεων που φθείρουν τη διεθνή έννομη τάξη, όπως αυτή έχει καθιερωθεί μέχρι σήμερα. Μεταξύ όμως άλλων συνεπειών, οποιαδήποτε χρήση όρου που περιλαμβάνει τον επιθετικό προσδιορισμό «πολεμικός-ή», βασιζόμενη σε επισφαλή επιχειρήματα και θολές εκτιμήσεις, δημιουργεί μια πιθανώς πολύ επικίνδυνη κατάσταση κλιμάκωσης, η οποία προκαλείται από την υποκίνηση των θυμάτων μιας κυβερνοεπίθεσης να λάβουν ακόμα ισχυρότερα επιθετικά αντίμετρα εναντίον κάθε υποτιθέμενου

[120] Keneth Geers, “Cyberspace and the Changing Nature of Warfare”, Cooperative Cyber Defence Centre of Excellence (keynotes 1 & 3), Tallin

[121] Η έννοια της «Πολεμικής Πράξης» έχει το ίδιο περιεχόμενο με την έννοια «Πράξη Πολέμου» και χρησιμοποιούνται ως ισοδύναμα προς τους αγγλικούς όρους «Warfare» και «Act of war» αντίστοιχα.

«κυβερνοαντιπάλου», που παρουσιάζεται ή θα μπορούσε να είναι ο δράστης αυτής της «πολεμικής» πράξης[122].

Γενικά, υφίστανται τρεις[123], ανεξάρτητοι μεταξύ τους, τρόποι για να αποδοθεί σε μια πράξη ο προσδιορισμός «πολεμική», να αναγνωρισθεί και να ορισθεί ως τέτοια: διεθνώς, πολυμερώς και μονομερώς. Ειδικότερα:

- Κάθε κράτος διαθέτει τη φυσική ελευθερία, που του προσφέρει η άναρχη φύση του διεθνούς πολιτικού περιβάλλοντος, να ορίσει μονομερώς τι αποδέχεται ή να αναγνωρίζει ως πράξη πολέμου. Βέβαια η δυνατότητα ενός κράτους να επηρεάσει θετικά τα άλλα μέλη του διεθνούς συστήματος για τις αποφάσεις του, άρα και για το τι θεωρεί ως πράξη πολέμου και τι όχι, εξαρτάται πρωτίστως από την σχετική του θέση μέσα στο σύστημα, η οποία βέβαια είναι συνάρτηση της ισχύος του και του κύρους που διαθέτει συγκριτικά και έναντι των ανταγωνιστών και συμμάχων του. Στην περίπτωση που το κράτος που δέχτηκε την επίθεση απαντήσει, τότε, όσα κράτη είναι σκεπτικά ή δεν συμφωνούν με την θέση ότι η αρχική επίθεση ήταν πράξη πολέμου, υπάρχει ισχυρή πιθανότητα να το κατηγορήσουν και να το καταδικάσουν για άσκηση παράνομων αντιποίνων.

- Με τα Ηνωμένα Έθνη, ως διεθνή θεσμό αναγνωρισμένο και υπερισχυμένο από τα ίδια τα μέλη του με εξουσιοδότηση δεσμευτικής νομολογίας (Άρθρο 25 του Χάρτη του ΟΗΕ[124]), που παράγει πλάσματα με χαρακτήρα υποχρεωτικό όχι μόνο έναντι των μελών του, μία πράξη μπορεί να χαρακτηριστεί και να γίνει διεθνώς αποδεκτή ως «πολεμική» όταν έτσι την ορίσει ο υπόψη οργανισμός. Κάθε φορά που το Συμβούλιο Ασφαλείας αποδέχεται και αναγνωρίζει μία πράξη ως πολεμική, επεκτείνει ή συστέλλει το πλαίσιο το οποίο καθορίζει τη διατύπωση ενός διεθνώς αναγνωρισμένου ορισμού. Σε ότι αφορά τον κυβερνοπόλεμο δεν υφίσταται τέτοια απόφαση από τον ΟΗΕ, ούτε κάποια άλλη διεθνή συνθήκη ορίζει κάτι ανάλογο. Για το επιχείρημα ότι μια κυβερνοεπίθεση αποτελεί διαφορετική περίπτωση και ξεκάθαρα αποτελεί πράξη πολέμου, ο Libicki δεν αφήνει περιθώρια αμφισβήτησης: «αν δεν υφίσταται παγκόσμια συναίνεση ότι τέτοια αναλογία είναι σε ισχύ, μια κυβερνοεπίθεση δεν μπορεί να ορισθεί ως πράξη πολέμου».

- Η πιο κοντινή εκδοχή πολυμερούς αποδοχής ενός ορισμού, αποτελεί η κοινή αναγνώριση που απολαμβάνει μια δεδομένη κατάσταση ή πράξη στο πλαίσιο μιας συνθήκης μεταξύ κρατών, όπως το Βορειοατλαντικό Σύμφωνο. Χαρακτηριστική είναι η δήλωση του ΝΑΤΟ σχετικά με την κυβερνοεπίθεση που δέχτηκε η Εσθονία το 2007 ότι δεν αξίζει να επικαλεσθεί τη ρήτρα συλλογικής άμυνας[125]. Αυτό βέβαια δεν αποτελεί άρνηση ότι πρόκειται για πράξη του

[122] Sascha Knoepfel, "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War, [Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges'', Springel - Verlag Berlin Heidelberg, 2014] p.118

[123] Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Corporation, 2009, Appendix A, p.179

[124] Κ.Αντωνόπουλος, Κ.Μαγκλιβέρας, ''Το Δίκαιο της Διεθνούς Κοινωνίας'', Αθήνα, Εκδ. Νομική Βιβλιοθήκη, 2017 (3η έκδοση), σελ.184

[125] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", 17 May 2007 https://www.theguardian.com/world/2007/may/17/topstories3.russia

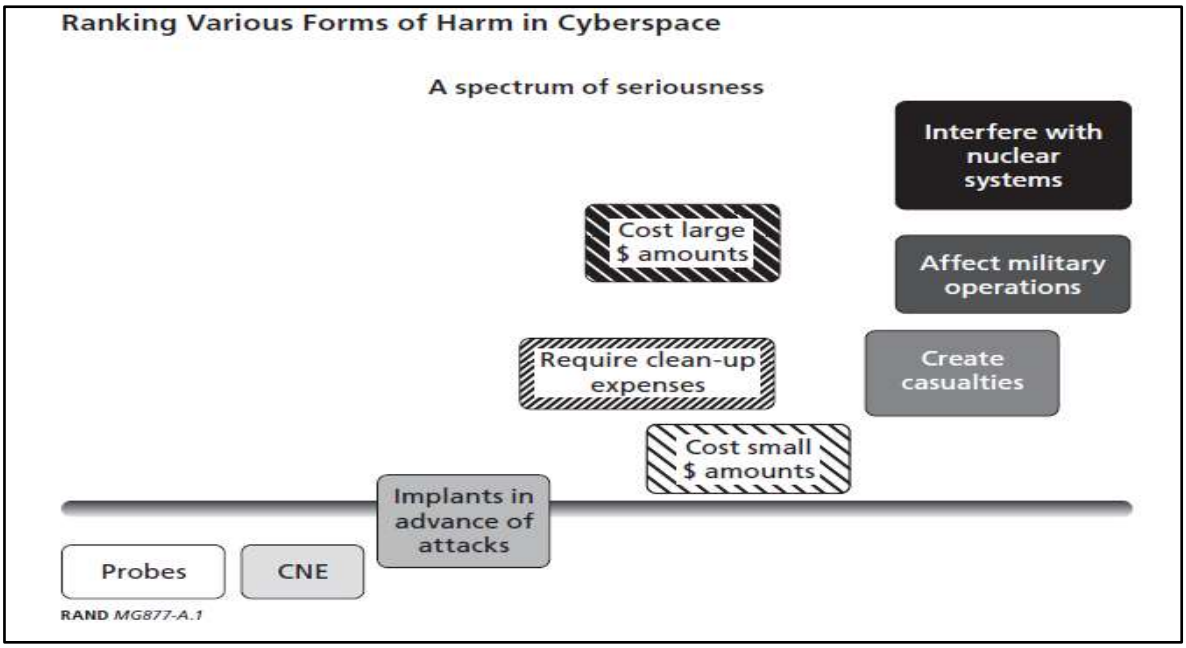
πολέμου, αλλά ούτε και ξεκάθαρη αποδοχή. Τα προβλήματα που εγείρονται στα ζητήματα απόδοσης της ευθύνης αλλά και το ρίσκο των συνεπειών μιας απόλυτης απόφασης προφανώς απέτρεψαν στην επίκληση στο άρθρο 5 της συνθήκης. Αν το ΝΑΤΟ είχε δηλώσει ότι η υπόψη κυβερνοεπίθεση επιδεχόταν δράση από την πλευρά της συμμαχίας, αυτό θα μπορούσε να λειτουργήσει ως προειδοποίηση προς το κράτος ή τα κράτη που ενδεχομένως είχαν επιτεθεί. Ωστόσο, το εάν θα θεωρούσαν ότι αυτό, που το ΝΑΤΟ όριζε ως πράξη πολέμου, αποτελούσε έναν νόμιμο ορισμό θα ήταν άλλο ζήτημα. Στην περίπτωση που το ΝΑΤΟ θα αντιδρούσε σε μία κυβερνοεπίθεση, όπως υποθετικά θα δήλωνε, τότε ο επιτιθέμενος θα αντιδρούσε στην αντίδραση του ΝΑΤΟ, όπως αυτός θα έκρινε καλύτερα προς το συμφέρον του. Συνεπώς, η διεθνής νομιμοποίηση μπορεί να διαδραματίσει κάποιο ρόλο αν ο επιτιθέμενος πείσει ότι δεν πίστευε ότι μία κυβερνοεπίθεση ήταν τόσο σοβαρό ζήτημα όσο μια πραγματική επίθεση και δεν επιθυμούσε η αντίδραση του ΝΑΤΟ να λειτουργήσει ως η τελευταία λέξη στο θέμα.

Όταν το Απρίλιο του 2007 οι Εσθονικές αρχές άρχισαν να αφαιρούν από ένα πάρκο ένα χάλκινο άγαλμα ενός σοβιετικού στρατιώτη της εποχής του Β 'Παγκοσμίου Πολέμου, περίμεναν βίαιες διαδηλώσεις από τους Εσθονούς ρωσικής καταγωγής. Γνώριζαν επίσης ότι αν υπάρχουν συγκρούσεις στο δρόμο, θα υπάρξουν μάχες και στο Διαδίκτυο. Μετά από αυτό που τελικά ακολουθήσε, που ορισμένοι ονόμασαν ως τον 1ο διαδικτυακό πόλεμο, ο υπουργός Άμυνας της Εσθονίας, σε συνέντευξή του, δήλωσε[126]: «Αποδείχθηκε ότι πρόκειται για κατάσταση εθνικής ασφάλειας. Μπορεί πραγματικά να συγκριθεί με όταν τα λιμάνια σας είναι κλειστά στη θάλασσα». Ωστόσο, ακόμη και αυτές οι οξείες εκτιμήσεις για τη δύναμη των κυβερνοεπιθέσεων και της ισχύος που αυτή εκλύει για να επιφέρει τέτοια επώδυνα αποτελέσματα, ξεπεράστηκαν από εκείνες του υπουργού Εξωτερικών της Εσθονίας, ο οποίος από την αρχή κατηγόρησε ευθέως τη διοίκηση του Πούτιν για άμεση εμπλοκή δηλώνοντας[127]: «Η Ευρωπαϊκή Ένωση είναι υπό επίθεση, επειδή η Ρωσία επιτίθεται στην Εσθονία», διεθνοποιώντας το ζήτημα και προσκαλώντας ουσιαστικά την ΕΕ να λάβει θέσεις μάχης, καθώς και της εκπροσώπου του Εσθονικού Κοινοβουλίου, η οποία δήλωσε: «Όταν κοιτάζω μια πυρηνική έκρηξη και την έκρηξη που συνέβη στη χώρα μας τον Μάιο, βλέπω το ίδιο πράγμα ... Όπως και η πυρηνική ακτινοβολία, ο κυβερνοπόλεμος δεν σας κάνει να αιμορραγείτε, αλλά μπορεί να καταστρέψει τα πάντα».

"At present, Nato does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country," said the Estonian defence minister, Jaak Aaviksoo.
"Not a single Nato defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future."

[126] Mark Landler & John Markoffmay, “Digital Fears Emerge After Data Siege in Estonia”, https://www.nytimes.com/2007/05/29/technology/29estonia.html

[127] JOSHUA DAVIS, “HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE” https://www.wired.com/2007/08/ff-estonia/



ΔΙΑΓΡΑΜΜΑ 3: Ταξινόμηση των Διάφορων Τύπων Βλαβών στον Κυβερνοχώρο με Βάση το Επίπεδο της Σοβαρότητας των Συνεπειών στον Πραγματικό Κόσμο[128]

Με μια πιο προσεκτική[129] και κυρίως ψύχραιμη ματιά, μπορεί κανείς να διαπιστώσει ότι τόσο στη Εσθονία, όσο και στην Γεωργία κατά τον Ρωσο-Γεωργιανό πόλεμο τον Αύγουστο του 2008, δεν υπήρξαν ανθρώπινες απώλειες, εδαφικές απώλειες, κρίσιμες καταστροφές στις υποδομές και σοβαρή αποδιοργάνωση ή διακοπή κρίσιμων υπηρεσιών εξαιτίας των κυβερνοεπιθέσεων που υπέστησαν οι δύο χώρες. Στην περίπτωση δε της Γεωργίας, οι Ρώσοι επέδειξαν ιδιαίτερα σημαντική συστολή, όχι και τόσο τυπική της σοβιετικής τους παράδοσης. Συστολή που αποτυπώθηκε τόσο στο επίπεδο της φυσικής κατάληψης της Τιφλίδας, καθώς αδιαμφισβήτητα θα μπορούσαν να υλοποιήσουν, όπως επέτρεψε η εξέλιξη της στρατιωτικής επιχείρησης, όσο και στο επίπεδο του κυβερνοχώρου, είτε γιατί επιθυμούσαν να διατηρήσουν μυστικά τα κυβερνοόπλα τους για μια μελλοντική σύγκρουση με το NATO, ώστε να αξίζει το τίμημα της αποκάλυψης των δυνατοτήτων τους, είτε γιατί αυτό ήταν το καλύτερο που μπορούσαν σύμφωνα με τις «κυβερνοεπιχειρησιακές» δυνατότητες που διέθεταν τότε.

Βέβαια, από την άλλη πλευρά, έχει περάσει κυλήσει πολύ νερό στον μύλο της κυβερνοπραγματικότητας. Με μία έμμεση προσέγγιση του ζητήματος, ήδη μεγάλες ασφαλιστικές εταιρείες όπως η «Zurich Insurance»[130] παίρνουν θέση στα χαρακώματα της διεθνούς νομολογίας, αποφασίζοντας ότι οι κυβερνοεπιθέσεις που είναι δυνατό να αποδοθούν ή θετικά αναγνωρίζονται ότι προέρχονται από άμεση ενέργεια ή ότι υποστηρίζονται τεχνικά από κάποιο κράτος, αποτελούν ουσιαστικά πράξη πολέμου και επομένως δεν θα καλύπτονται ασφαλιστικά! Επιπλέον, πρωτοπορώντας για άλλη μια φορά στη διεθνή πρακτική, το Ισραήλ με αεροπορική του επίθεση εναντίον εγκαταστάσεων της

[128] Martin C. Libicki, "Cyberdeterrence and Cyberwar", RAND Corporation, 2009, Appendix A, p.181

[129] D.J.Betz & T.Stevens, "CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER", IISS, Arundel House, London, 2011, p.31-32

[130] Matt Field, "Is cyberwarfare war? Insurers balk at paying for some cyberattacks" https://thebulletin.org/2019/04/is-cyberwarfare-war-insurers-balk-at-paying-for-some-cyberattacks/

τρομοκρατικής οργάνωσης «HAMAS» τον Ιούνιο του 2019[131], για πρώτη φορά συνέδεσε μια στρατιωτική ενέργεια στον πραγματικό κόσμο ως αντίδραση – απάντηση σε κυβερνοεπίθεση που δέχτηκε με πιστοποιημένη προέλευση από την περιοχή της Γάζας. Άμεση πρακτική συνέπεια βεβαίως είναι τα νέα όρια που θέτει η αποτρεπτική ισχύς του υπόψη κράτους και πόσο ανοίγει η βεντάλια των στρατηγικών επιλογών γενικότερα. Τα πράγματα γίνονται ακόμα πιο πολύπλοκα και σίγουρα πιο επικίνδυνα όταν η «κυβερνοτεχνολογία» καθιστά το κυνήγι των κινητών συστοιχιών πυρηνικών πυραύλων απίστευτα γρήγορο, πιο οικονομικό και ιδιαίτερα υψηλής ακρίβειας στον εντοπισμό τους[132]. Η ασύλληπτη, μόλις μερικά χρόνια πριν, εξασφάλιση της καταστροφής της σπονδυλικής στήλης των συστημάτων πυρηνικής αποτροπής, δηλαδή των κινητών συστοιχιών, με πυρηνικά ή ακόμα και με συμβατικά όπλα, υπονομεύει ανεπανόρθωτα την πυρηνική σταθερότητα. Οι συνέπειες αυτής της τεχνολογικής μεταβολής είναι πολλές:

- επαύξηση του οφέλους και του κινήτρου επιλογής του πλεονεκτήματος της πρώτης κρούσης,
- παραγωγή πιο «νευρικών» εκτιμήσεων πληροφοριών με χαρακτήρα «αντίδρασης», οι οποίες είναι φύσει πιο στενά συνδεδεμένες με επιθετικές δυνάμεις.
- βύθιση σε σπιράλ «κούρσας εξοπλισμών», κατά την διάρκεια της οποίας ο επιτιθέμενος και ο αμυνόμενος διέρχονται μέσα από αλλεπάλληλους κύκλους μέτρων και αντίμετρων.

Ο διαρκώς αυξανόμενος ρόλος του κυβερνοχώρου, ως πεδίο ανταγωνισμού ισχύος και των δραστηριοτήτων που σχετίζονται άμεσα ή έμμεσα με αυτόν, έχει καταστήσει πλέον φανερό ότι κάθε προσπάθεια να γίνει διάκριση μεταξύ της αποτροπής, όπως αυτή γίνεται αντιληπτή στον κυβερνοχώρο και της αποτροπής όπως αυτή γίνεται αντιληπτή στο κλασσικό, στρατηγικό επίπεδο, μοιάζει να είναι ολοένα και πιο μάταιη άσκηση. Είναι μάλλον αδύνατο να διατυπωθεί μια στρατηγική χωρίς να εξεταστεί και να ενσωματωθεί σε αυτή ο ρόλος του κυβερνοχώρου. Ενδεχομένως, η αποτροπή μπορεί να είναι μια ατελής προσέγγιση για την πρόληψη όλων των τύπων επιθέσεων στον κυβερνοχώρο, ωστόσο η στρατηγική αποτροπή επιβάλλεται να επιφυλάσσει ένα ρόλο για τον κυβερνοχώρο και για τα φαινόμενα που λαμβάνουν χώρα σε αυτόν[133].

4.2.3 Ο Κυβερνοχώρος και το Διεθνές Δίκαιο

Η εξέταση των φαινομένων που λαμβάνουν χώρα ή αφορούν στον κυβερνοχώρο και έλκουν το ενδιαφέρον της διεθνούς νομολογίας εστιάζει σε τρείς βασικούς τομείς[134]:

- Στον καθορισμό των περιστάσεων στο πλαίσιο του Νόμου που διέπει την προσφυγή στη βία μεταξύ κρατών **(jus ad bellum)**, εφόσον υφίστανται τέτοιες, υπό τις οποίες οι κυβερνοεπιχειρήσεις, δηλαδή οι δραστηριότητες στον κυβερνοχώρο που

[131] Kate Fazzini, “Israel says it bombed Hamas compound that committed cyberattacks” https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html

[132] Paul Bracken, “The Intersection of Cyber and Nuclear War” https://thestrategybridge.org/the-bridge/2017/1/17/the-intersection-of-cyber-and-nuclear-war

[133] Rosemary Tropeano, “Deterrence in Cyber, Cyber in Deterrence”, May 27, 2019 https://thestrategybridge.org/the-bridge/2019/5/27/deterrence-in-cyber-cyber-in-deterrence

[134] Nils Melzer, “Cyberwarfare and International Law”, UNIDIR Resources, Geneva, 2011, p.3

αναφέρονται στην εκμετάλλευση του υπόψη τομέα για την επίτευξη πολιτικοστρατιωτικών αντικειμενικών σκοπών σύμφωνα με τις επιταγές μιας σχεδιασμένης στρατηγικής στο πλαίσιο ανταγωνισμού ισχύος μεταξύ δύο ή περισσότερων πόλων, μπορούν να θεωρηθούν ως μια διεθνώς αναγνωρισμένη άδικη **απειλή χρήσης ή χρήση βίας**, ως **ένοπλη επίθεση** δικαιολογώντας την προσφυγή στην αναγκαία και αναλογική βία για λόγους αυτοάμυνας, ή ως **απειλή για την διεθνή ειρήνη και ασφάλεια ή διατάραξη της ειρήνης**, πράξη που υπόκειται στην δικαιοδοσία παρέμβασης του Συμβουλίου Ασφαλείας του ΟΗΕ.

- Στον καθορισμό της ευθύνης του κράτους, στο πλαίσιο του **κανόνα της ουδετερότητας**, που επιτρέπει σε χρήστες του κυβερνοχώρου οι οποίοι δεν είναι κρατικοί λειτουργοί, ρητά ή χωρίς την θέλησή του υπόψη κράτους, να χρησιμοποιούν τις τηλεπικοινωνιακές υποδομές του για να διεξάγουν κυβερνοεπιθέσεις εναντίον άλλων κρατών ή ακόμα και εναντίον οργανισμών, ιδιωτικών ή δημόσιων συμφερόντων, που έχουν έδρα σε έδαφος των υπόψη κρατών.

- Στον καθορισμό των ορίων, στο πλαίσιο του Νόμου των ενόπλων συρράξεων **(jus in bello)**, εντός των οποίων ορισμένα φαινόμενα του κυβερνοχώρου διέπονται από τους κανόνες του διεθνούς ανθρωπιστικού δικαίου (ΔΑΔ), ως εκφάνσεις του κυβερνοπολέμου, ενώ άλλα φαινόμενα δεν διέπονται, καθώς αποτελούν εκφάνσεις του κυβερνοεγκλήματος ή της κυβερνοτρομοκρατίας. Όπου δε, το ΔΑΔ έχει εφαρμογή, απαιτείται να διευκρινιστεί σε ποιό βαθμό οι κανόνες και αρχές, που έχουν σχεδιαστεί για να διέπουν τα παραδοσιακά μέσα και μεθόδους πολέμου, μπορούν να τεθούν σε ισχύ στον κυβερνοπόλεμο. Επισημαίνεται ότι, η εστίαση πραγματοποιείται πάνω στους κανόνες και τις αρχές του ΔΑΔ που διέπουν την διεξαγωγή των εχθροπραξιών και όχι σε εκείνες που διέπουν την προστασία και τη μεταχείριση των προσώπων που βρέθηκαν στα χέρια ενός από τα εμπλεκόμενα στην ένοπλή σύγκρουση μέρη, τομέας που είναι λιγότερο σχετικός με τον κυβερνοπόλεμο.

Πρακτικά ωστόσο, δεν υφίσταται, τουλάχιστον προς το παρόν, συναίνεση ως προς το ακριβές όριο στον κυβερνοχώρο, μετά το οποίο οι πράξεις θα πρέπει, κατά συνθήκη, να ισοδυναμούν με διεθνώς αδικαιολόγητη απειλή χρήσης ή χρήση βίας. Η αλήθεια είναι ότι ούτε όσοι συνέταξαν τον Χάρτη των Ηνωμένων Εθνών ούτε τη νομολογία σε εθνικό ή διεθνές επίπεδο μπορούσαν να προβλέψουν, ούτε αναμενόταν να μπορούν να παρέχουν σαφή κριτήρια που να ορίζουν το κατώφλι των δραστηριοτήτων στον κυβερνοχώρο που δεν προκαλούν θάνατο, τραυματισμό ή καταστροφή, μετά τη διέλευση του οποίου πρέπει να θεωρείται ότι απαγορεύεται από το άρθρο 2(4) του Χάρτη των Ηνωμένων Εθνών, καθώς οι κυβερνοεπιχειρήσεις σχεδόν πάντοτε πέφτουν στη γκρίζα ζώνη μεταξύ της παραδοσιακής άσκησης στρατιωτικής ισχύος και άλλων μορφών εξαναγκασμού[135].

Θα πρέπει βέβαια να επισημανθεί ότι μια κυβερνοεπιχείρηση δεν απαιτείται να ισοδυναμεί με «βία», στο πνεύμα της έννοιας του όρου του άρθρου 2(4) του Χάρτη των Ηνωμένων Εθνών, για να καθίσταται – θεωρείται διεθνώς ως αδίκημα, ούτε και ότι όλες κυβερνοεπιχειρήσεις που ισοδυναμούν με «βία» είναι αναγκαστικά παράνομες. Ο παράνομος χαρακτήρας μιας κυβερνοεπιχείρησης μπορεί να προκύψει από την παραβίαση

[135] Nils Melzer, "Cyberwarfare and International Law", UNIDIR Resources, Geneva, 2011, p.9

οποιασδήποτε υποχρέωσης δυνάμει της διεθνούς νομοθεσίας. Χαρακτηριστικό είναι το παράδειγμα της εκμετάλλευσης των διαδικτυακών υπηρεσιών από έναν κρατικό δρώντα για τη διεξαγωγή δραστηριοτήτων ηλεκτρονικής συλλογής πληροφοριών ή για την άσκηση ψυχολογικής επίδρασης ή τη διάδοση προπαγάνδας, δραστηριότητες που θα μπορούσαν κάθε μια να παραβιάσει την σφαίρα της κυριαρχίας του κράτους – θύματος και συνεπώς την εθιμική αρχή της μη-παρέμβασης παρά το γεγονός ότι δεν πιστοποιούνται ως πράξεις βίας[136]. Η διεθνής νομολογία μπορεί να συμπεριλάβει στο υφιστάμενο πλαίσιο που διέπει τις διπλωματικές[137] ή εμπορικές σχέσεις μεταξύ κρατών κάθε πράξη που λαμβάνει χώρα στον κυβερνοχώρο ή σχετίζεται με αυτόν και η οποία παραβιάζει ή περιορίζει διατάξεις του. Ομοίως, διασταλτικά μπορεί να συμπεριλάβει τις κυβερνοδράσεις που στρέφονται εναντίον ατομικών ελευθεριών ή παρεμποδίζουν ή επιτρέπουν την παρεμπόδιση της ελευθερίας έκφρασης[138].

Ωστόσο, η φύση του κυβερνοχώρου και ιδιαίτερα τα χαρακτηριστικά της πρακτικά ανεμπόδιστης προσβασιμότητας σε συνδυασμό με την εγγενή δυσχέρεια απόδοσης θετικής ευθύνης για κακόβουλες ενέργειες δημιουργεί μια ιδιάζουσα συνθήκη που λειτουργεί περιοριστικά ή έστω δημιουργεί προσκόμματα στην εφαρμογή της διεθνούς έννομης τάξης. Ενώ η ευθύνη της χρήση κυβερνοισχύος και «κυβερνοβίας» από de facto κρατικούς λειτουργούς - πράκτορες αποδίδεται άμεσα στο κράτος για λογαριασμό του οποίου ασκείται[139], κατά την «έμμεση» χρήση βίας, δηλαδή αυτή που ασκείται από μη κρατικούς λειτουργούς - φορείς[140] για λογαριασμό ενός κράτους, υποδηλώνεται μεν μια μορφή στήριξης αυτού του κράτους προς τους υπόψη μη κρατικούς φορείς με συνέπεια το κράτος να είναι διεθνώς υπεύθυνο για την «βοήθεια» που δέχτηκε, αλλά όχι για την βία που τελικά ασκήθηκε από τους μη κρατικούς δρώντες – οντότητες που συνέδραμαν με τις «υπηρεσίες» τους στο κράτος - πελάτη.

Η λήψη μέτρων για την αποτροπή ή απαγόρευση της κυβερνοβίας την οποία είναι δυνατό να μεταχειριστεί ένας μη κρατικός δρώντας, αποτελεί εσωτερικό ζήτημα για ένα κράτος και δεν αφορά την διεθνή έννομη τάξη όσο τα μέτρα περιορίζονται στον χώρο που το κράτος ασκεί νόμιμη κυριαρχία. Ωστόσο, η δράση μη κρατικών δρώντων στον κυβερνοχώρο μπορεί κατά περίπτωση να θεωρηθεί και ως απειλή για την διεθνή ειρήνη και ασφάλεια και συνεπώς να απαιτηθεί η απόφαση του Συμβουλίου Ασφαλείας για την κατάλληλη εξουσιοδότηση μιας κατάλληλης συλλογικής δύναμης για την επιβολή κατάλληλων μέτρων. Συνεπώς, πιθανή μονομερή απόφαση ενός κράτους να λάβει ένοπλη δράση κατά μη κρατικού δρώντα, που μεταχειρίζεται την κυβερνοισχύ εναντίον του από έδαφος στο οποίο ασκείται κυριαρχία από άλλο κράτος, καθίσταται έκνομη πράξη καθώς παραβιάζεται η κυριαρχία του υπόψη κράτους. Θα πρέπει ακόμα να επισημανθεί ότι ο ίδιος

---

[136] UN General Assembly resolution 36/103, "Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States", 9 December 1981, p.P78-80
https://treaties.un.org/doc/publication/ctc/uncharter.pdf

[137] Vienna Convention on Diplomatic Relations, arts. 24, 27 and 45(a)
http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

[138] Universal Declaration of Human Rights, article 19
https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

[139] UN General Assembly resolution A/RES/56/83 of 12 December 2001 and its annex
https://www.ilsa.org/Jessup/Jessup11/basicmats/StateResponsibility.pdf

[140] International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), merits, 1986, p.54-55 (§ 115), p.97-98 (§ 205), p.116-117 (§247)
https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

ο Χάρτης των ΗΕ διακρίνει την άσκηση βίας από την ένοπλη επίθεση [Άρθρο 2(4) και άρθρο 51 του Χάρτη των ΗΕ]. Αυτή η διάκριση υφίσταται και τον κυβερνοχώρο και δεν είναι δυνατό κάθε άσκηση κυβερνοβίας οποιαδήποτε μορφής να θεωρείται απαραίτητα κυβερνοεπίθεση. Αυτή η διάκριση εγείρει φυσικά ερωτήματα για τις συνθήκες κάτω από τις οποίες το κράτος – θύμα θα αξιολογήσει μια ενέργεια στον κυβερνοχώρο ως κυβερνοεπίθεση, αν θα αναζητήσει διεθνή στήριξη ή όχι σε αυτό, αν θα απαντήσει στο πλαίσιο που του επιτρέπει η διεθνής έννομη τάξη σύμφωνα με το θεσμό - αρχή της «νόμιμης άμυνας» ή «αυτοάμυνας», αν αυτοπεριορίζεται σύμφωνα με τις αρχές της αναγκαιότητας και της αναλογικότητας, αν επιλέξει να προβεί σε αντίποινα εκτιμώντας το ρίσκο έναντι της αποφασιστικότητας του Συμβουλίου Ασφαλείας να την χαρακτηρίσει παράνομη ενέργεια!

Αν και θα πρέπει να θεωρείται περίπου αυτονόητη η χρησιμοποίηση του κυβερνοχώρου από δύο ή περισσότερες, επίσημα αναγνωρισμένες ή de facto, εμπόλεμες πλευρές για την επίτευξη στρατιωτικών αντικειμενικών σκοπών μέσω «κυβερνοπληγμάτων», ωστόσο αυτό σε καμία περίπτωση δεν αποκλείει την χρήση οποιασδήποτε έντασης ή διάρκειας κυβερνοβίας και ανταλλαγής κυβερνοπληγμάτων μεταξύ δύο ή περισσότερων δρώντων, κρατικών και μη κρατικών κατά την περίοδο της ειρήνης ή τουλάχιστον κατά την περίοδο «μη θερμού» πολέμου οποιασδήποτε μορφής, επιτρέποντας τους υπόψη δρώντες να διεξάγουν κυβερνοπόλεμο μεταξύ τους χωρίς παράλληλα την εμπλοκή κλασσικών στρατιωτικών δυνάμεων ακόμα και ρομποτικών. Το γεγονός αυτό δημιουργεί διάφορα ζητήματα για την υφιστάμενη διεθνή νομολογία, ακόμα και στο επίπεδο της ταξινόμησης ή της ονοματοδοσίας των φαινομένων που αναφέρονται στον κυβερνοχώρο και αφορούν στην οργάνωση και προστασία της διεθνούς έννομης τάξης κατά την διεξαγωγή του πολέμου (Jus in Bello). Τελικά η νομική «τακτοποίηση» θα συνεχίσει να εκκρεμεί καθώς:

- δεν υφίσταται κοινός τόπος στην χρησιμοποίηση μιας κοινά αποδεκτής ορολογίας μεταξύ κρατών, διεθνών οργανισμών, συνασπισμών, συμμαχιών, μη κυβερνητικών οργανισμών, πολυεθνικών εταιρειών κλπ, ο οποίος να ορίζει και να περιγράφει τα φαινόμενα που λαμβάνουν χώρα στον κυβερνοχώρο[141],

- είναι αδύνατο τα φαινόμενα αυτά να διακριθούν ή να απομονωθούν χωροχρονικά μεταξύ τους, στο πλαίσιο ενός αναγκαίου συμβατισμού τον οποίο ο άνθρωπος μεταχειρίζεται και αντιλαμβάνεται στον φυσικό κόσμο (δηλαδή της κατάστασης της ειρήνης και του πολέμου, της ειρηνικής και της πολεμικής περιόδου) με αποτέλεσμα να μην έχει νόημα η αντίστοιχη οριοθέτηση μιας διαχωριστικής γραμμής βάσει της οποίας θα κατανεμηθούν τα φαινόμενα αυτά.

Ειδικό ενδιαφέρον για τη διεθνή έννομη τάξη έχει το ζήτημα της στοχοποίησης (targeting). Στον πυρήνα του διεθνούς ανθρωπιστικού δικαίου είναι η αρχή της διάκρισης[142]. Αυτή απαιτεί από τα εμπλεκόμενα μέρη μιας σύγκρουσης να εξασφαλίζουν πάντα την διακριτότητα μεταξύ των στρατιωτικών στόχων από την μία πλευρά και των ατόμων ή αντικειμένων που δικαιούνται ασυλίας έναντι κάθε επιθετικής προσβολής – ενέργειας από

[141] Nils Melzer, "Cyberwarfare and International Law", UNIDIR Resources, 2011, Geneva, Switzerland, p.22, § V.1.1

[142] Jean-Marie Henckaerts & Louise Doswald-Beck, "Customary International Humanitarian Law", Cambridge University Press, New York, 2005, Vol.I, Part I, Ch.1, Rule 1, p.3-8, https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf

την άλλη. Είναι παραπάνω από προφανές ότι η απλή μεταφορά των προβλέψεων του εθιμικού ανθρωπιστικού δικαίου, ακόμα και με τη γραπτή του πλέον εκδοχή, στο περιβάλλον του κυβερνοχώρου, ώστε να συμπεριλάβει τις δραστηριότητες και ενέργειες που λαμβάνουν χώρα σε αυτόν, είναι παραπάνω από δυσχερής. Οι προκλήσεις και οι αντίστοιχες διλημματικού χαρακτήρα αποφάσεις είναι πολλές:

- Με ποιον τρόπο παράγοντες που σχετίζονται με τη στοχοποίηση, όπως η «οργανωτική δομή» και η «ταυτότητα» μιας ομάδας ή η «ιδιότητα μέλους», θα πρέπει να ερμηνεύονται ή να αντιστοιχίζονται στον κυβερνοχώρο, όπου τα άτομα μπορούν να ενεργούν συλλογικά χωρίς απαραίτητα κάποια μακροχρόνια διασύνδεση ή συσχέτιση μεταξύ τους ή συγκρότηση ιεραρχικής δομής διοίκησης κα ελέγχου[143];

- Με ποιον τρόπο μπορεί να υλοποιηθεί η υποχρέωση των «κυβερνομαχητών» να καταστήσουν τον εαυτό τους διακριτό έναντι του άμαχου πληθυσμού και των λοιπών χρηστών του κυβερνοχώρου ενόσω εμπλέκονται σε μια κυβερνοεπίθεση ή συμμετέχουν στην προπαρασκευή αυτής[144];

- Απαιτείται οι «hackers» να φέρουν κάποιου είδους στολή για να θεωρούνται νόμιμοι μαχητές του κυβερνοχώρου ακόμα και όταν δεν βρίσκονται εντός του φυσικού πεδίου μάχης;

- Με ποια νομιμοποιητική αιτιολόγηση και ποια επιμέρους κριτήρια ένας διαδικτυακός κόμβος ή μια δέσμη υποβρύχιων οπτικών ινών μέσω των οποίων διακινούνται ταυτόχρονα ηλεκτρονικά δεδομένα πολιτικής και στρατιωτικής χρήσης μπορούν να καταστούν στόχος;

- Τα ηλεκτρονικά δεδομένα φέρουν ή όχι την ιδιότητα του «αντικειμένου» όπως αυτή γίνει αντιληπτή από την διεθνή νομολογία;

4.3. Οι Προοπτικές της Κυβερνοασφάλειας

4.3.1. Το Ζητούμενο της Κυβερνοασφάλειας

Η στρατηγική και το σχέδιο πρόληψης και αντιμετώπισης των κινδύνων που σχετίζονται με τον κυβερνοχώρο, καθώς και του μετριασμού των συνεπειών τους θα πρέπει να έχει χαρακτήρα ολιστικό. Θα πρέπει δηλαδή, να απευθύνεται και να αγκαλιάζει το υλικό και τις εγκαταστάσεις, το προσωπικό και τις υφιστάμενες διοικητικές δομές και τεχνικές διαδικασίες, καθώς και την πληροφορία που διακινείται και σωρεύεται. Εκτός από τις φυσικές καταστροφές, οι υποδομές θα πρέπει να είναι ανθεκτικές τόσο σε πιθανές ηλεκτρονικές επιθέσεις που στοχεύουν στην καταστροφή – κατάρρευση του λειτουργικού

[143] Michael Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", Naval War College International Law Studies, 2011, Vol 87, Ch.V, p. 98. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1077&context=ils

[144] ICRC - Additional Protocols to the Geneva Conventions of 12 Aug 1949, Art. 44(3), AP I. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

δικτύου διοίκησης και ελέγχου όσο και στην κακόβουλη – μη εξουσιοδοτημένη απόκτηση πρόσβασης σ΄ αυτό. Ειδικά για τις τεχνικές διαδικασίες, αυτές διακρίνονται στις ακόλουθες κύριες κατηγορίες και που αφορούν: τη λήψη αποφάσεων, τις αλυσίδες εφοδιασμού και παραγωγής, τις κατασκευές, μετασκευές και συντηρήσεις και την ασφάλεια και προστασία.

Προϋπόθεση για την προώθηση οποιαδήποτε πολιτικής ολιστικής αντιμετώπισης των ζητημάτων κυβερνοασφάλειας αποτελεί η υπέρβαση των φραγμών της επικοινωνίας μεταξύ των κοινά ενδιαφερόμενων ακαδημαϊκών, τεχνικών – τεχνολογικών και πολιτικών κοινοτήτων. Σύμφωνα με τον Matthew Crosston[145] οι υπόψη ομάδες δοκιμάζουν τις συνέπειες της πνευματικής απομόνωσης του κύκλου τους, σε ότι αφορά την κατανόηση του περιβάλλοντος του κυβερνοχώρου, την ανάπτυξη των θεμάτων που σχετίζονται με αυτόν και την εσωτερική και εξωτερική επικοινωνιακή λειτουργία του στο πλαίσιο των διεθνών σχέσεων. Η δε τάση των πολιτικών να επιδεικνύουν σχετική σπουδή προς τις τεχνοκρατικές προσεγγίσεις μάλλον πιο εύκολα συγκριτικά με τη φυσική αποστροφή τους προς την θεωρητική θεμελίωση των φαινομένων που αφορούν τις δυναμικές που αναπτύσσονται είτε στο εσωτερικό των κρατών – κοινωνιών, είτε στο διακρατικό - διεθνές επίπεδο, καθιστά υπαρκτό και συνεχώς διευρούμενο το ρήγμα, περιορίζοντας περαιτέρω το πεδίο και την προσβασιμότητα του θεωρητικού και του εμπειρικού έργου στον κυβερνοχώρο. Οι πνευματικοί, τεχνικοί και κυβερνητικοί κόσμοι χρειάζονται μια νέα γενιά ανθρώπινου δυναμικού που είναι έμπειρο στην οικοδόμηση γεφυρών μεταξύ αυτών των διαφορετικών αλλά και αλληλοσυνδεόμενων βάσεων γνώσης.

4.3.2. Πολιτική Κυβερνοασφάλειας: Προϋποθέσεις – Αξιώσεις – Γραμμή Εκκίνησης

Η συζήτηση στα ζητήματα ασφαλείας που έχουν επιβάλλει με εμπειρικό τρόπο οι ακολουθούμενες πρακτικές και στρατηγικές του διαπιστούμενου ανταγωνισμού στον κυβερνοχώρο έχει ως αφετηρία – βάση τις παρακάτω αξιώσεις:

- Οι προκλήσεις στα ζητήματα Ανθρώπινης Ασφάλειας, εκτός του γεγονότος ότι αλληλοσυνδέονται με όλα τα λοιπά ζητήματα ασφαλείας που επαναπροσδιορίζει ή παρθενικά εγείρει η νέα κυβερνοπραγματικότητα, καθιστούν την ανάγκη αντιμετώπισής τους άμεση, επιβάλλοντας μια ανθρωποκεντρική ατζέντα ασφαλείας σήμερα κιόλας.

- Το Κράτος δεν διαθέτει την φυσική ικανότητα να εξασφαλίσει την κυβερνοασφάλειά του μόνο του και σε συνθήκες διεθνούς απομόνωσης.

- Το υφιστάμενο διεθνές status quo δεν είναι πλέον ανεκτό, καθώς αποκαλύπτονται υφιστάμενες και νέες αδυναμίες, καθώς επίσης κενά ασφαλείας και κίνδυνοι που δεν είχαν αντιμετωπισθεί στο παρελθόν γιατί απλά δεν απαιτούνταν.

---

[145] Matthew Crosston, “Phreak the Speak: The Flawed Communications within Cyber Intelligentsia”, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.253- 267

Ως Γραμμή Εκκίνησης - Βάσης για τον καθορισμό της Πολιτικής Κυβερνοασφαλείας και των Γραμμών Επιχειρησιακής Δράσης για τη διασφάλιση τόσο της εσωτερικής κρατικής σταθερότητας, όσο και της σταθερότητας του διεθνούς συστήματος αποτελεί η κατανόηση των χαρακτηριστικών των περιστατικών κυβερνοεπιθέσεων, των πρωταγωνιστών που εμπλέκονται σε αυτές και των επιπτώσεων – επιδράσεων αυτών σε αρχές και θεσμούς. Οι Jan-Frederik Kremer και Benedict Muller[146] εισηγούνται ένα πλαίσιο μελέτης (SAM Framework) με το οποίο κατηγοριοποιούν τα υποκείμενα των κυβερνοδραστηριοτήτων, τις ίδιες τις δραστηριότητες στον κυβερνοχώρο και τις επιπτώσεις στις κυβερνήσεις διαχωρίζοντας τις απειλές που καλούνται αυτές να αντιμετωπίσουν σε άμεσες και έμμεσες (βλέπε Συνημμένο 3). Θα πρέπει ωστόσο να επισημάνουμε ότι οι δύο μελετητές δεν προσφέρουν ένα αντίστοιχο εργαλείο που να περιγράφει τις συνέπειες και επιδράσεις στο διεθνές σύστημα που πιθανόν έχουν αυτές οι ίδιες κυβερνοδραστηριότητες (cyber-activities) από αυτούς τους ίδιους πρωταγωνιστές (actors). Επίσης, όπως διαπιστώνει ο J.S.Nye Jr. ο διαχωρισμός των πρωταγωνιστών δεν είναι μπορεί να υπηρετήσει επαρκώς μια απόλυτη ταξινόμηση αλλά μια μάλλον γενική προσέγγιση[147].

4.3.3. Προοπτικές – Γραμμές Επιχειρησιακής Δράσης

Πολιτική Κατεύθυνση. Η επιβίωση του Κράτους, όχι απλά ως θεμελιώδη υποχρέωση προς τους υπηκόους του αλλά ως δομικό στοιχείο του ίδιου του Βεστφαλιανής καταγωγής Διεθνούς Συστήματος, σκιαγραφεί τον λόγο που είναι κρίσιμης σημασίας κρατική προτεραιότητα η διασφάλιση ότι ο κυβερνοχώρος είναι επαρκώς ανθεκτικός και αξιόπιστος για την υποστήριξη των στόχων για: βιώσιμη οικονομική ανάπτυξη, προστασία των πολιτικών ελευθεριών και της ιδιωτικής ζωής, θωράκιση της εθνικής / κρατικής ασφάλειας και για τη συνεχιζόμενη πρόοδο των δημοκρατικών θεσμών. Η εκπλήρωση αυτού του κρίσιμου και πολύπλοκου στην επίτευξή του στόχου καθίσταται εφικτή μόνο με την αντίστοιχη θεσμική αναθεώρηση και πολιτική κατοχύρωση, με την διοικητική - ηγετική εκπροσώπηση στα υψηλότερα επίπεδα κρατικής διακυβέρνησης, με την ενίσχυση της συμβουλευτικής διαδικασίας και της λογοδοσίας, με την συνέργεια όλων των διοικητικών βαθμίδων (ομάδες δράσης, τοπικές κοινότητες, δήμοι, περιφέρειες κλπ).

Οικοδόμηση της Ψηφιακής Ικανότητας (Digital Capacity Building)[148]. Λόγω της ψηφιακής τεχνολογίας, κάθε ανθρώπινη δραστηριότητα έχει ήδη περισσότερο ή λιγότερο επηρεαστεί και έχει υποστεί καθοριστικές μεταβολές[149]. Οι ίδιες οι τεχνολογικές προοπτικές ενισχύουν την άποψη ότι όλοι οι θεσμοί έχουν πλέον εισέλθει σε μία συνεχώς επιταχυνόμενη διαδικασία μετεξέλιξης με ρυθμό που πολύ σύντομα μάλλον θα ξεπεράσει τις δυνατότητες προσαρμογής τόσο του ανθρώπου ως υποκείμενο των θεσμών που το ίδιο έχει θεσπίσει, όσο και των ίδιων των θεσμών. Σε ένα τέτοιο περιβάλλον, η ανάγκη ενημέρωσης και ευαισθητοποίησης των πολιτών, τόσο για τις δυνατότητες που παρέχει η επέκταση της δραστηριοποίησής τους στον κυβερνοχώρο, δηλαδή η ενσωμάτωση της ψηφιακής διάστασης στην καθημερινότητά τους, όσο και για τους κινδύνους που

[146] Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014] p.41-58

[147] Joseph S. Nye, Jr, ‘’Cyber Power’’, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010

[148] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: Executive Office of the President of the United States, 2009, p.13

[149] Andy Budd, “How To Build Digital Capacity And Attracting Talent” https://www.smashingmagazine.com/2015/11/building-digital-capacity-attracting-talent/

ελλοχεύουν στο περιβάλλον αυτό, αποκτά ισότιμη τουλάχιστον αξία με την μέχρι σήμερα εκπαιδευτική διαδικασία που το σύγχρονο κράτος πολύ γρήγορα υιοθέτησε ως βασική προτεραιότητά του προκειμένου να εξυπηρετηθούν οι σκοποί για τους οποίους υπάρχει. Η οικοδόμηση αυτής της ικανότητας βασίζεται στους παρακάτω άξονες:

- Προώθηση την ευαισθητοποίησης των πολιτών του κράτους για τους κινδύνους του κυβερνοχώρου.

- Η δημιουργία ενός εκπαιδευτικού συστήματος που θα βελτιώσει την κατανόηση της ασφάλειας του κυβερνοχώρου και θα επιτρέπει την περαιτέρω ανάπτυξη της επιστήμης, της ψηφιακής τεχνολογίας, της τεχνολογίας της πληροφορίας και της αγοράς επωφελεία των σκοπών του κράτους, συμπεριλαμβανομένης της ευημερίας των πολιτών του.

- Την επανακατάρτιση του εργατικού δυναμικού και την προσέλκυση επιπλέον εξειδικευμένου προσωπικού στο υφιστάμενο δυναμικό του χώρου της πληροφορίας, ώστε το κράτος να διατηρεί ή να επεκτείνει τα συγκριτικά του ανταγωνιστικά πλεονεκτήματα.

- Αποκατάσταση περιβάλλοντος ασφαλείας στον κυβερνοχώρο και κατάλληλη ενίσχυση της επιχειρηματικότητας ώστε να συμπεριλάβει την έξυπνη διαχείριση των κινδύνων του κυβερνοχώρου στα επιχειρηματικά πλάνα της.

Σύμπραξη Δημόσιου (Κρατικού) και Ιδιωτικού Τομέα και κοινή ευθύνη για αποκατάσταση της κυβερνοασφάλειας[150]. Το Κράτος και η κεντρική κυβέρνηση δεν μπορούν παρά να συνειδητοποιήσουν ότι είναι αδύνατο να διασφαλισθούν πλήρως και απομονωμένα έναντι των προκλήσεων ασφαλείας στον κυβερνοχώρο, ακριβώς λόγω της φύσης του. Το γεγονός ότι στο χώρο αυτό το Κράτος καθίσταται ισότιμο με κάθε άλλο χρήστη αποτελεί καταλυτική συνθήκη που δηλοποιεί πριν από όλα ότι ο κυβερνοχώρος έχει τους δικούς του νόμους. Τα κρατικά, τα εταιρικά και τα ατομικά – ιδιωτικά συμφέροντα συμπλέκονται και η διασφάλιση του κυβερνοχώρου τα συνδέει άρρηκτα[151]. Η διαμόρφωση κοινών ή συμπλεόντων συμφερόντων επιβάλλουν και την κοινή ευθύνη για τη διασφάλιση αυτή η οποία εκφράζεται με την ανεμπόδιστη πρόσβαση σε αξιόπιστες υπηρεσίες και υποδομές. Ωστόσο, η εξυπηρέτηση των παραπάνω συμφερόντων δεν είναι δυνατό να περιοριστεί από τα παραδοσιακά γεωγραφικά σύνορα που αποτυπώνουν την κατανομή ισχύος μιας άλλης εποχής. Όπως προαναφέρθηκε, ο παγκοσμιοποιητικός χαρακτήρας του κυβερνοχώρου δεν αφήνει πολλά περιθώρια περιχαράκωσης. Συνέπεια των ανωτέρω και ως άμεσο επακολούθημα της παγκόσμιας διάχυσης των συμφερόντων, τόσο των σχετικά ισχυρών, όσο και των σχετικά αδυνάτων, είναι η επιδίωξη διεθνούς συνεργασίας για την

---

[150] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: Executive Office of the President of the United States, 2009, p.17

[151] Melissa Hathaway Questions, "Internet Security Alliance, Issue Area 3: Norms of Behavior", March 24, 2009, at 2, 4-7 https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20ISSUE%20AREA%203%20-%20NORMS%20OF%20BEHAVIOR---HATHAWAY%20QUESTIONS.pdf

Melissa Hathaway, "Getting beyond Norms: When Violating the Agreement Becomes Customary Practice", CIGI Paper No. 127, April 20, 2017
https://www.cigionline.org/publications/getting-beyond-norms-when-violating-agreement-becomes-customary-practice

διασφάλιση του κυβερνοχώρου. Η επίτευξη της συνεργασίας μεταξύ όλων των παραπάνω φορέων συμφερόντων διέρχεται μέσω:

- Της βελτίωσης της εταιρικής σχέσης μεταξύ του ιδιωτικού τομέα και της κυβέρνησης / κράτους. Βέβαια, η εταιρική σχέση μπορεί να λάβει πολλές μορφές, όχι πάντα αθώες. Είναι γνωστή η «κυβερνοαντεπίθεση» των Ιρανών στρεφόμενη κατά της «SAUDI ARAMCO» η οποία θα μπορούσε να ισχυριστεί κανείς ότι αποτελεί ιδιωτική εταιρεία που έχει στην ιδιοκτησία της ένα ολόκληρο κράτος, αλλά και εναντίον της «US BANK». Και τότε η αντίδραση του Προέδρου Ομπάμα ήταν λίγο ή πολύ η εξής: «leave the private sector to counter – attack». Η σύμπλευση συμφερόντων του Κράτους με Επιχειρηματικούς κολοσσούς δεν οδηγεί πάντα στον παράδεισο!

- Την αξιολόγηση και άρση των δυνητικών φραγμών που εμποδίζουν την εξέλιξη της σύμπραξης κράτους / δημόσιου και ιδιωτικού τομέα.

- Την αποκατάσταση αποτελεσματικής συνεργασίας του Κράτους με τη Διεθνή Κοινωνία στην πλέον διευρυμένη της εκδοχή της, η οποία συμπεριλαμβάνει άλλα Κράτη, Διεθνείς και Περιφερειακούς Οργανισμούς, Μη Κυβερνητικές Οργανώσεις (Διεθνείς και μη), εμπορικές εταιρείες (πολυεθνικές κα μη), ενώσεις ιδιωτών και ιδιώτες.

Διαμόρφωση αποτελεσματικού πλαισίου ανταλλαγής πληροφοριών και απόκρισης σε περιστατικά κυβερνοεπιθέσεων[152]. Στη διάσταση του Κυβερνοχώρου και του επιπέδου ασφαλείας που οι χρήστες του απολαμβάνουν, το ζήτημα της αντιμετώπισης των απειλών και της διάσπασης – κατάλυσης των μέτρων προστασίας σχετίζεται άμεσα με το επίπεδο συνεργασίας για την ανταλλαγή κρίσιμων και πολλές φορές διαβαθμισμένων πληροφοριών. Η πολιτική στο ζήτημα προϋποθέτει σαφήνεια, δέσμευση, συναίνεση και λογοδοσία τόσο για τον κυβερνητικό όσο και για τον ιδιωτικό τομέα και αναφέρεται:

- Στη δημιουργία πλαισίου δράσης – αντίδρασης με προσυμφωνημένες διαδικασίες ανταλλαγής πληροφοριών, προκαθορισμένες αρμοδιότητες και αποδεσμευμένες εξουσιοδοτήσεις δράσης στο κατάλληλο κάθε φορά διοικητικό επίπεδο.

- Στην ενίσχυση της από κοινού χρήσης και διαχείρισης πληροφοριών για τη βελτίωση των δυνατοτήτων απόκρισης στις κυβερνοεπιθέσεις. Μια πιθανή επιλογή θα μπορούσε να είναι η δημιουργία ενός μη κερδοσκοπικού μη κυβερνητικού οργανισμού που θα χρησιμεύσει ως αξιόπιστο τρίτο μέρος όπου ο δημόσιος – κρατικός και ο ιδιωτικός τομέας θα μπορούν να μοιραστούν πληροφορίες.

- Στη βελτίωση του επιπέδου παθητικής και ενεργητικής «κυβερνοπροστασίας» όλων των υποδομών. Ας μην ξεχνάμε ότι οι περισσότερες υποδομές κοινής ωφέλειας δεν κατασκευάστηκαν λαμβάνοντας υπόψη τις ιδιαίτερες ανάγκες κυβερνοπροστασίας που απαιτούν οι συνθήκες σήμερα. Αυτό συνεπάγεται κόστος αναβάθμισης και προσαρμογής και μάλιστα πάρα πολύ υψηλό.

---

[152] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: Executive Office of the President of the United States, 2009, p.23

Ενθάρρυνση της καινοτομίας. Ο τομέας των πληροφοριών και των επικοινωνιών συγκλίνει ταχύτατα προς μια ενιαία πλατφόρμα όπου οι εφαρμογές δεδομένων, φωνής και εικόνας θα μοιράζονται μια κοινή υποδομή. Ο αποκεντρωτικός χαρακτήρας του υφιστάμενου μοντέλου του Διαδικτύου επιτρέπει σε άτομα και επιχειρηματίες να αναπτύξουν και να υλοποιήσουν καινοτόμες εφαρμογές στα όρια του δικτύου χωρίς βέβαια να έχουν λάβει κάποια ειδική άδεια για αυτό. Η καινοτομία έχει προκαλέσει έκρηξη στη δημιουργία νέων επιχειρήσεων πολλών δισεκατομμυρίων δολαρίων που έχουν μεταβάλλει κατά τρόπο επαναστατικό τον τρόπο με τον οποίο οι χρήστες αλληλεπιδρούν με το δίκτυο και μεταξύ τους. Παρά το γεγονός πως η τεχνολογία γίνεται ολοένα και κρισιμότερη παράμετρος στην σχεδίαση και την διαμόρφωση περιβάλλοντος ασφαλείας, η διατήρηση της επιχειρηματικής αυτοπεποίθησης αλλά και της εμπιστοσύνης σε αυτή τη συνεχώς εξελισσόμενη τεχνολογική υποδομή είναι απαραίτητη. Πολλές λύσεις που αφορούν τεχνικά ζητήματα ή ζητήματα διαχείρισης δικτύων που βελτιώνουν σημαντικά την ασφάλεια, υπάρχουν ήδη στην αγορά, αλλά δεν χρησιμοποιούνται πάντοτε λόγω κόστους, πολυπλοκότητας, γραφειοκρατίας ή λόγω νομικών περιορισμών. Επιπλέον, οι υπάρχουσες λύσεις μπορούν να λειτουργήσουν θετικά, δεδομένου του υφιστάμενου σχεδιασμού της αρχιτεκτονικής του διαδικτύου. Μακροπρόθεσμα, η ανοιχτή συζήτηση και η καινοτομία θα συμβάλουν στη δημιουργία μιας ισχυρότερης υποδομής με διαφάνεια και λογοδοσία. Το Κράτος έχει κάθε συμφέρον να ενισχύσει την τεχνολογική καινοτομία στον ενιαίο τομέα της πληροφορίας και επικοινωνίας και να επωφεληθεί εξασφαλίζοντας τα κατάλληλα εργαλεία που θα ενισχύσουν την ασφάλειά του ως οντότητα στο διεθνές σύστημα αλλά και θα εξασφαλίσει και το κατάλληλο περιβάλλον ασφαλείας για την ανεμπόδιστη δραστηριοποίηση των υπηκόων του για τους οποίους υφίσταται. Αν δεν το κάνει, τότε ως μη ορθολογικός δρών θέτει την επιβίωσή του σε επισφάλεια εκθέτοντας τους υπηκόους του σε κινδύνους που με τη σειρά τους θα τους κινητοποιήσει είτε εναντίον του κράτους, είτε θα αναζητήσουν την αναγκαία προστασία σε άλλο πιο πετυχημένο φορέα κρατικής ισχύος.

Διαμόρφωση Διεθνούς Νομικού και Ρυθμιστικού Πλαισίου Δικαιωμάτων και Υποχρεώσεων[153]. Καταρχήν, το διεθνές νομικό πλαίσιο που αφορά τον κυβερνοχώρο χτίζεται εθιμικά.

- Ο ίδιος ο ΟΗΕ δεν έχει καθορισμένο ορισμό του τι αποτελεί κυβερνοπόλεμος, άλλωστε οι περισσότεροι εμπειρογνώμονες δεν μπορούν να συμφωνήσουν. Ούτε βέβαια προκαλεί έκπληξη ότι δεν υπάρχουν διεθνείς συμβάσεις που να διευθετούν οριστικά τα σχετικά με την χρησιμοποίηση του κυβερνοχώρου ζητήματα. Πρακτικά, ο κυβερνοχώρος διέρχεται μια εποχή εικονικής Άγριας Δύσης. Από το 2012, τουλάχιστον 11 έθνη έχουν επιθετικές δυνατότητες στον κυβερνοχώρο, ενώ τουλάχιστον 33 έχουν αμυντικές. Μεταξύ των χωρών με επιθετικές ικανότητες, οι Ηνωμένες Πολιτείες, η Κίνα και η Ρωσία ανακοίνωσαν δημοσίως την ύπαρξη μονάδων διεξαγωγής κυβερνοπολέμου στο πλαίσιο των στρατιωτικών τους δυνάμεων.

- Οι Ηνωμένες Πολιτείες τείνουν να μην δημοσιοποιούν τις δραστηριότητές τους στον κυβερνοχώρο. Αντίθετα, η Κίνα τείνει να είναι «πιο ομιλητική» σχετικά με τις προσπάθειές της στον κυβερνοχώρο και στην κυβερνοκατασκοπεία, οι επιθέσεις της γίνονται πιο γρήγορα γνωστές στο κοινό και γενικά προκαλούν

[153] Michael Beaver, ''THE UNITED NATIONS AND CYBERWARFARE'', Global Risk Advisors, Sep 28, 2016 https://globalriskadvisors.com/united-nations-cyber-warfare/

περισσότερες διαταραχές. Οι κινεζικές επιθέσεις τείνουν επίσης να επικεντρώνονται στην πληροφορία και με το βλέμμα προς την βιομηχανική κατασκοπεία. Για παράδειγμα, οι κινέζοι χάκερ έχουν υποκλέψει διαβαθμισμένες πληροφορίες σχετικά με το μαχητικό αεροσκάφος F-35, και το 2010 κατάφεραν να διεισδύσουν σε 34 μεγάλες εταιρείες, συμπεριλαμβανομένης της Google. Ενώ οι Κινέζοι χάκερ τείνουν να κάνουν πολύ θόρυβο όταν επιτίθενται, οι Ρώσοι χάκερ τείνουν να είναι πιο εκλεπτυσμένοι, όπως οι Αμερικανοί ομόλογοι τους. Πιο πρόσφατα, χάκερ που πιστεύεται ότι συνδέονται με τη ρωσική κυβέρνηση προσπάθησαν να πουλήσουν κλεμμένα κυβερνοόπλα της NSA στο Διαδίκτυο.

- Ο ΟΗΕ δεν ήταν στην πραγματικότητα ο πρώτος πολυεθνικός οργανισμός που πρότεινε κανόνες που να διέπουν τον κυβερνοχώρο. Η πρώτη σοβαρή απόπειρα προήλθε από τη Σύμβαση της Βουδαπέστης του 2001 για το έγκλημα στον κυβερνοχώρο. Η Σύμβαση, η οποία άρχισε να ισχύει το 2004, δεν αφορά το κυβερνοπόλεμο «per se», αλλά είναι η μόνη δεσμευτική διεθνής συνθήκη για το έγκλημα στον κυβερνοχώρο. Για όλες τις προθέσεις και σκοπούς, το έγκλημα στον κυβερνοχώρο μπορεί να θεωρηθεί ως ένα εξειδικευμένο είδος κυβερνοπολέμου. Για παράδειγμα, εάν οι Κινέζοι χάκερ κλέψουν πνευματική ιδιοκτησία από μια εταιρεία με έδρα τις ΗΠΑ, τότε αυτή η πράξη θα θεωρείται εγκληματικότητα στον κυβερνοχώρο. Ωστόσο, αυτό το έγκλημα μπορεί να ενταχθεί σε μια μεγαλύτερη εκστρατεία κυβερνοπολέμου για να υπονομεύσει την οικονομική δύναμη των ΗΠΑ. Θυμηθείτε: ο κυβερνοπόλεμος απαιτείται απαραίτητα να προκαλέσει σωματική βλάβη για να θεωρηθεί ως πράξη πολέμου[154]. Όσον αφορά τη Σύμβαση, δηλώνει ότι όλες οι κυβερνοεπιθέσεις ανεξάρτητα από το κίνητρο, είναι παράνομες και οι υπογράφοντες υποχρεούνται να εφαρμόσουν νόμους που να αντικατοπτρίζουν αυτήν την εντολή. Από το 2016, 49 χώρες έχουν επικυρώσει τη συνθήκη. Από αυτές, οι Ηνωμένες Πολιτείες έχουν υπογράψει και επικυρώσει (ως μη μέλος) και η Ρωσία δεν την έχει υπογράψει, ούτε επικυρώσει. Η Κίνα δεν ήταν συμβαλλόμενο μέρος της Συνθήκης, οπότε δεν έχει καμία υποχρέωση βάσει της Σύμβασης. Επομένως, βλέπουμε ότι υπάρχει ένα επισφαλές περιβάλλον στο οποίο οι Ηνωμένες Πολιτείες δεσμεύονται νομικά να μην εκτοξεύουν κυβερνοεπιθέσεις, ενώ η Ρωσία και η Κίνα ουσιαστικά παραβλέπουν την ίδια την ύπαρξη της Σύμβασης.

- Ο ΟΗΕ, τα τελευταία 15 χρόνια προσπαθεί να εφαρμόσει ουσιαστικές κατευθυντήριες γραμμές για τη διεθνή ασφάλεια στον κυβερνοχώρο. Υπήρξαν δύο εισηγήσεις ψηφισμάτων που εγκρίθηκαν το 2003 και το 2004. Η απόφαση 57/239 του 2003 απαιτεί μεγαλύτερη ευαισθητοποίηση και ευθύνη από ικανά κράτη για την πρόληψη, τον εντοπισμό και την αντιμετώπιση απειλών στον κυβερνοχώρο. Το ψήφισμα 58/199 του 2004 καλεί τα κράτη μέλη με εθνικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο να μοιραστούν και να βοηθήσουν άλλα έθνη-μέλη στις προσπάθειές τους να καταρτίσουν παρόμοιες στρατηγικές. Είναι αυτά τα ψηφίσματα ιδεαλιστικά και αισιόδοξα; Σίγουρα. Θα

[154] David E. Graham, ‘‘Cyber Threats and the Law of War’’, Journal of National Security Law & Policy, vol 4:87, 2010

μπορούσε κάποιος λογικός άνθρωπος να περιμένει από τις Ηνωμένες Πολιτείες, την Κίνα ή τη Ρωσία να βοηθήσουν αυτούς που θεωρούν ως εχθρούς τους στην ανάπτυξη της υποδομής τους στον κυβερνοχώρο; Πιθανώς όχι.

- Παρά τον ορθολογικό κατά τα άλλα κυνισμό, η έκθεση του 2010 της Ομάδας Κυβερνητικών Εμπειρογνωμόνων των Ηνωμένων Εθνών - που περιελάμβανε διπλωμάτες από τις Ηνωμένες Πολιτείες, την Κίνα και τη Ρωσία - διαπίστωσε ότι οι απειλές στον κυβερνοχώρο είναι από τις πιο σοβαρές προκλήσεις του 21ου αιώνα. Έτσι, ο ΟΗΕ έχει οδηγήσει τις πρόσφατες προσπάθειες για τη δημιουργία διαφάνειας και την οικοδόμηση εμπιστοσύνης μεταξύ των μελών του, ενώ το Ιούλιο του 2015 η Ομάδα Κυβερνητικών Εμπειρογνωμόνων εισηγείται επικαιροποιημένες «Αρχές και Κανόνες Υπεύθυνης Συμπεριφοράς στον Κυβερνοχώρο»[155]. Το πιο ελπιδοφόρο αποτέλεσμα ήταν η επιστολή του 2015 προς τον Γενικό Γραμματέα από την Κίνα, τη Ρωσία και άλλα μέλη του Οργανισμού Συνεργασίας της Σαγκάης ζητώντας συζητήσεις για την εκπόνηση πρότασης για την πρόληψη των μελών που χρησιμοποιούν το κυβερνοχώρο για πράξεις επιθετικότητας. Αν και η πρόταση έλαβε κάποιες σοβαρές επικρίσεις, συνέβαλε στην προώθηση του διαλόγου για τις διεθνείς σχέσεις στον κυβερνοχώρο.

4.4. Το Παρόν και το Μέλλον της Κυβερνοασφάλειας

4.4.1. Ευρωπαϊκή Ένωση και Κυβερνοασφάλεια[156]: Ένας Ανοιχτός, Ασφαλής και Προστατευμένος Κυβερνοχώρος

«Η στρατηγική για την ασφάλεια στον κυβερνοχώρο της Ευρωπαϊκής Επιτροπής και του Ύπατου Εκπροσώπου» που συντάχθηκε το 2013 ήταν το πρώτο ολοκληρωμένο έγγραφο πολιτικής της ΕΕ στον τομέα αυτό. Καλύπτει από την οπτική γωνία του κυβερνοχώρου τους τομείς της εσωτερικής αγοράς, της δικαιοσύνης, τις εσωτερικές υποθέσεις καθώς επίσης και την εξωτερική πολιτική της Ευρωπαϊκής Ένωσης.

Η στρατηγική συνοδεύεται από νομοθετική πρόταση για την ενίσχυση της ασφάλειας των συστημάτων πληροφοριών της ΕΕ. Αυτό θα ενθαρρύνει την οικονομική ανάπτυξη καθώς η εμπιστοσύνη στη χρήση του Διαδικτύου γενικά και ειδικότερα στη διαδικτυακή «online» αγορά μεγαλώνει.

Η στρατηγική καθιστά σαφείς τις προτεραιότητες της πολιτικής της ΕΕ στον κυβερνοχώρο[157]:

---

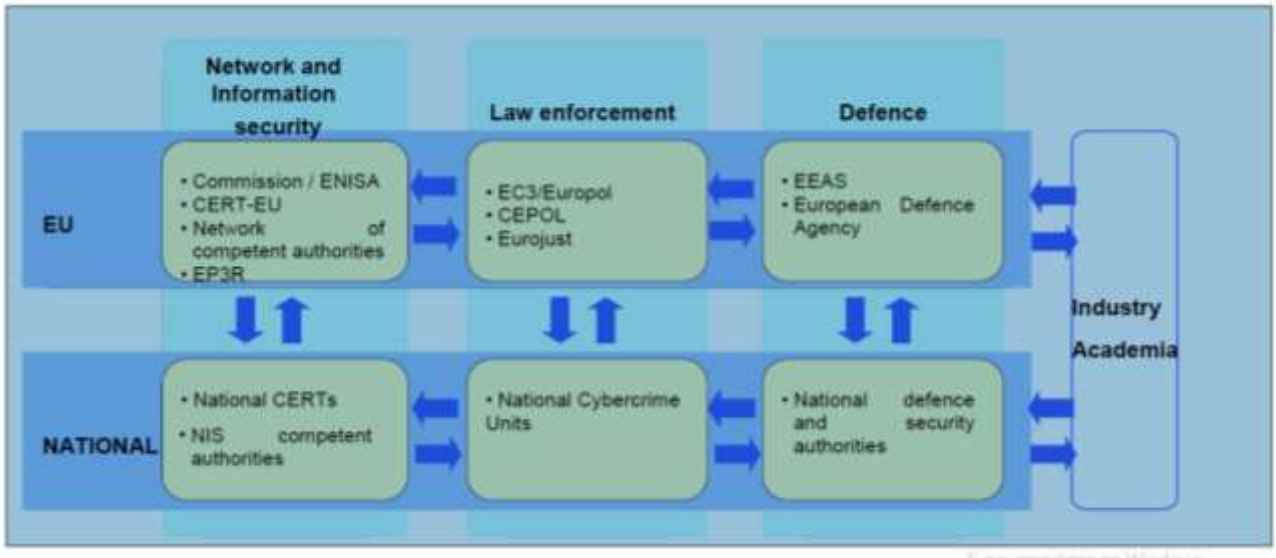
[155] United Nations A/70/174 General Assembly, 17th Session, Item 93 of the provisional agenda: ''Developments in the field of information and telecommunications in the context of international security'', Group of Governmental Experts on Developments, 22 July 2015
https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

[156] EU Commission, HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 7.2.2013.

[157] EU International Cyberspace Policy

- **Ελευθερία και ανοικτό πνεύμα:** η στρατηγική σκιαγραφεί το όραμα και τις αρχές για την εφαρμογή των βασικών αξιών της ΕΕ και των θεμελιωδών δικαιωμάτων στον κυβερνοχώρο.
- **Οι νόμοι, οι κανόνες και οι βασικές αξίες της ΕΕ ισχύουν τόσο στον κυβερνοχώρο όσο και στον φυσικό κόσμο:** η ευθύνη για έναν ασφαλέστερο κυβερνοχώρο έγκειται σε όλους τους παράγοντες της παγκόσμιας κοινωνίας της πληροφορίας, από τους πολίτες έως τις κυβερνήσεις.
- **Ανάπτυξη της δημιουργίας ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο:** η ΕΕ συνεργάζεται με διεθνείς εταίρους και οργανισμούς, τον ιδιωτικό τομέα και την κοινωνία των πολιτών για την υποστήριξη της παγκόσμιας ανάπτυξης ικανοτήτων σε τρίτες χώρες. Αυτό περιλαμβάνει τη βελτίωση της πρόσβασης σε πληροφορίες και ένα ανοιχτό διαδίκτυο και την πρόληψη των απειλών στον κυβερνοχώρο.
- **Προώθηση της διεθνούς συνεργασίας στον κυβερνοχώρο:** η διατήρηση ανοικτού, ελεύθερου και ασφαλούς κυβερνοχώρου αποτελεί παγκόσμια πρόκληση, την οποία η ΕΕ αντιμετωπίζει από κοινού με τους σχετικούς διεθνείς εταίρους και οργανισμούς, τον ιδιωτικό τομέα και την κοινωνία των πολιτών.

Για την αντιμετώπιση των ζητημάτων ασφάλειας στον κυβερνοχώρο, οι σχετικές δραστηριότητες θα πρέπει να καλύπτουν τρεις βασικούς πυλώνες: Τις Εθνικές Υπηρεσίες Πληροφοριών (National Intelligence Services, NIS), τις υπηρεσίες επιβολής του νόμου, και τις Αρχές Άμυνας και Ασφάλειας, θεσμοί οι οποίοι λειτουργούν επίσης εντός διαφορετικών νομικών πλαισίων.



ΔΙΑΓΡΑΜΜΑ 4: Πυλώνες των Δραστηριοτήτων Κυβερνοασφάλειας της ΕΕ[158].

Το Σεπτέμβριο του 2017, η ΕΕ επικαιροποίησε τη στρατηγική της για την ασφάλεια στον κυβερνοχώρο του 2013. Η νέα έκδοση έχει στόχο τη βελτίωση της προστασίας των κρίσιμων υποδομών της Ευρώπης και την ενίσχυση της ψηφιακής αυτοπεποίθησης της ΕΕ προς άλλες περιοχές του κόσμου. Ωστόσο, η αναθεωρημένη στρατηγική αφήνει ανοιχτά μια

https://eeas.europa.eu/topics/eu-international-cyberspace-policy/415/eu-international-cyberspace-policy_en

[158] EU Commission, HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Brussels, 7.2.2013, p.17

σειρά από ερωτήματα σχετικά με το πώς είναι δυνατό να υπερασπιστεί αξιόπιστα τον στόχο του «ανοιχτού, ασφαλούς και προστατευμένου κυβερνοχώρου», τόσο στο εσωτερικό όσο και στο εξωτερικό. Η ΕΕ δεν έχει ορίσει ικανοποιητικά ούτε τι σημαίνει γι' αυτή η έννοια της ανθεκτικότητας και της αποτροπής ούτε έχει καταστίσει επαρκώς σαφές πως έχει την πρόθεση να υπερβεί τον θεσμικό κατακερματισμό και την έλλειψη νόμιμης εξουσίας για λήψη αποφάσεων και δράση για τα θέματα κυβερνοασφάλειας. Επιπλέον, αμφιλεγόμενα θέματα, όπως η εναρμόνιση του ποινικού δικαίου ή η χρήση της ψηφιακής κρυπτογράφησης, έχουν παραλειφθεί πλήρως. Τα δε κράτη - μέλη θα πρέπει να εγκαταλείψουν τις αυτόνομες προσπάθειές τους και να επιταχύνουν τη νομική ρύθμιση της ασφάλειας του κυβερνοχώρου σε επίπεδο ΕΕ[159].

Ως προς τα ζητήματα κυβερνοάμυνας, ακόμα και η αναθεωρημένη στρατηγική της ΕΕ δεν προσθέτει οτιδήποτε νέο στην διεθνή πρακτική και σε κάθε περίπτωση το ΝΑΤΟ παραμένει το πρώτο και τελευταίο σημείο αναφοράς. Ήδη από το 2013, η Ευρωπαϊκή Επιτροπή είχε αποφασίσει να εντατικοποιήσει την συνεργασία ΕΕ - ΝΑΤΟ υιοθετώντας ένα χρόνο αργότερα κοινό το πλαίσιο πολιτικής της κυβερνοάμυνας (Cyber Defense Policy Framework).

Η πλέον πρόσφατη εξέλιξη αφορά στον καθορισμό του πλαισίου που επιτρέπει στην ΕΕ να επιβάλλει στοχευμένα περιοριστικά μέτρα που κρίνονται απαραίτητα για την επίτευξη των στόχων της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (ΚΕΠΠΑ) για την αποτροπή και αντιμετώπιση επιθέσεων στον κυβερνοχώρο που συνιστούν εξωτερική απειλή για την ΕΕ ή τα κράτη - μέλη της, συμπεριλαμβανομένων των κυβερνοεπιθέσεων κατά τρίτων κρατών ή διεθνών οργανισμών[160]. Στις 17 Μαΐου 2019, το Συμβούλιο της ΕΕ καθόρισε το πλαίσιο ενεργοποίησης κυρώσεων όταν επιθέσεις στον κυβερνοχώρο που εμπίπτουν στο πεδίο εφαρμογής αυτού του νέου καθεστώτος έχουν σημαντικό αντίκτυπο και οι οποίες:

- Προέρχονται ή διεξάγονται από το εξωτερικό της ΕΕ ή
- Χρησιμοποιούν υποδομές εκτός της ΕΕ ή
- Διεξάγονται από πρόσωπα και οντότητες που είναι εγκατεστημένες ή λειτουργούν εκτός της ΕΕ ή
- Διεξάγονται με την υποστήριξη ατόμων ή οντοτήτων που λειτουργούν εκτός της ΕΕ.

Πιο συγκεκριμένα, το εν λόγω πλαίσιο επιτρέπει στην ΕΕ να επιβάλει για πρώτη φορά κυρώσεις σε πρόσωπα ή οντότητες, που ευθύνονται τόσο για επιθέσεις όσο και για απόπειρες επιθέσεων στον κυβερνοχώρο, οι οποίοι παρέχουν οικονομική, τεχνική ή υλική υποστήριξη για τέτοιες επιθέσεις ή εμπλέκονται με άλλους τρόπους. Μπορούν επίσης να επιβάλλονται κυρώσεις σε πρόσωπα ή οντότητες που συνδέονται με αυτά τα πρόσωπα ή οντότητες. Τα περιοριστικά μέτρα περιλαμβάνουν την απαγόρευση της εισόδου στην ΕΕ σε πρόσωπα που ταξιδεύουν και το πάγωμα περιουσιακών στοιχείων προσώπων και

---

[159] Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges" (Translation by Tom Genrich), Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs, Berlin, 2017.

[160] Cyber-attacks: the Council of EU is now able to impose sanctions https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

οντοτήτων. Επιπλέον, απαγορεύεται σε πρόσωπα και οντότητες της ΕΕ να καθιστούν διαθέσιμα κεφάλαια προς όσους έχουν ενταχθεί στη λίστα των εγκεκριμένων κυρώσεων.

4.4.2. Κυβερνοάμυνα και ΝΑΤΟ: Η Πολιτική Δέσμευση[161]

Αν και η πλέον κρίσιμη στιγμή για την κυβερνοάμυνα του ΝΑΤΟ ήταν οι κυβερνοεπιθέσεις που υπέστη η Εσθονία το 2007, το ΝΑΤΟ άρχισε να αντιμετωπίζει τις απειλές στον κυβερνοχώρο πριν από αυτό το γεγονός. Κατά τη διάρκεια της επιχείρησης στο Κοσσυφοπέδιο το 1999, τα μέλη του ΝΑΤΟ και οι στρατιωτικές δυνάμεις αντιμετώπισαν σκληρές κυβερνοεπιθέσεις που αφορούσαν άρνηση παροχής υπηρεσιών (Denial of Services) και παραποίηση ιστοσελίδων (Defacements). Αν και τα περιστατικά αυτά δεν επηρέασαν τις επιχειρήσεις στο Κοσσυφοπέδιο, συνέβησαν σε μια εποχή όπου οι πολιτικές και στρατιωτικές ανησυχίες για την ασφάλεια του κυβερνοχώρου αυξάνονταν.

Το 2002, η σύνοδος κορυφής του ΝΑΤΟ στην Πράγα προσδιόρισε την ανάγκη ενίσχυσης των ικανοτήτων έναντι κυβερνοεπιθέσεων και την καθιέρωση του Προγράμματος Κυβερνοάμυνας (Cyber Defence Program). Από το πρόγραμμα προέκυψε το σύστημα αντιμετώπισης περιστατικών κυβερνοεπιθέσεων του ΝΑΤΟ (NATO Computer Incident Response Capability - NCIRC) προκειμένου να αποκτήσει η συμμαχία τη δυνατότητα να προλαμβάνει, να ανιχνεύει και να ανταποκρίνεται στις απειλές στον κυβερνοχώρο.

Το 2005, οι κυβερνοαπειλές συμπεριλήφθηκαν στο θεσμικό κείμενο της πολιτικής κατεύθυνσης της συμμαχίας (Comprehensive Political Guidance) και επισήμανε ξανά την ανάγκη προστασίας των συστημάτων πληροφοριών του ΝΑΤΟ, όπως διατυπώθηκε στη σύνοδο της Ρίγας, υποδεικνύοντας ότι το ενδιαφέρον του ΝΑΤΟ για την ασφάλεια στον κυβερνοχώρο αντικατόπτριζε τις ανησυχίες σχετικά με τις κοινωνικές, πολιτικές και στρατιωτικές τρωτότητες που δημιουργούσε η ολοένα και βαθύτερη εξάρτηση από τον κυβερνοχώρο. Παρόλο που το ΝΑΤΟ άρχισε να ανταποκρίνεται στις απειλές στον κυβερνοχώρο πολύ νωρίτερα από τις κυβερνοεπιθέσεις στην Εσθονία το 2007, αυτές αποκάλυψαν την συστημική ανεπάρκεια των δραστηριοτήτων του ΝΑΤΟ και πυροδότησαν μια σημαντική κλιμάκωση της πολιτικής δέσμευσης και των επιχειρησιακών δυνατοτήτων του ΝΑΤΟ στον τομέα αυτό. Οι απειλές στον κυβερνοχώρο παρουσίασαν προκλήσεις για την εικόνα και τη φήμη του ΝΑΤΟ, την ικανότητά του να εξασφαλίζει ασφαλείς επικοινωνίες υποστήριξης των στρατιωτικών επιχειρήσεων που διεξάγονται από τη Συμμαχία, τις ικανότητές του να λειτουργεί αποτελεσματικά καθώς ο κυβερνοχώρος αναδεικνύεται ως ένα νέο πεδίο μάχης ή πεδίο στρατιωτικών συγκρούσεων και την ικανότητα των μελών του ΝΑΤΟ να συνεισφέρουν στους στόχους και στις αποστολές της Συμμαχίας.

Η αυξημένη πολιτική δέσμευση μπορεί να διαπιστωθεί στο αποτέλεσμα της συνόδου κορυφής του Βουκουρεστίου το 2008, κατά την οποία τα μέλη του ΝΑΤΟ υπογράμμισαν την υιοθέτηση μιας Πολιτικής για την Άμυνα στον Κυβερνοχώρο (Policy on Cyber Defence), η οποία τόνισε την ανάγκη για το ΝΑΤΟ και τα κράτη – μέλη να προστατεύσουν τα βασικά πληροφοριακά συστήματα, να μοιράζονται μεταξύ τους βέλτιστες πρακτικές και να παρέχεται η δυνατότητα χορήγησης βοήθειας στα μέλη της συμμαχίας, κατόπιν αιτήματος,

[161] Fidler, David P.; Pregent, Richard; and Vandurme, Alex, "NATO, Cyber Defense, and International Law" (2013). Articles by Maurer, Faculty. Paper 1672.
http://www.repository.law.indiana.edu/facpub/1672

ώστε να αντιμετωπίσουν μια κυβερνοεπίθεση. Το ΝΑΤΟ συνέχισε να δίνει προτεραιότητα στην κυβερνοάμυνα στην «Στρατηγική Αντίληψη» (Strategic Concept) που υιοθετήθηκε στη Σύνοδο Κορυφής της Λισαβόνας (2010), την «Αντίληψη, την Πολιτική και το Σχέδιο Δράσης για την Κυβερνοάμυνα» (2011) και τη διακήρυξη της συνόδου κορυφής του Σικάγο (2012). Μέσα από αυτές τις πολιτικές εξελίξεις, το ΝΑΤΟ έχει δημιουργήσει ή ενθάρρυνε τη δημιουργία μηχανισμών υλοποίησης, με το NCIRC, τη στρατηγική για τη βελτίωση της κυβερνοάμυνας στο πλαίσιο της Συμμαχίας και στα μέλη του ΝΑΤΟ, συμπεριλαμβανομένων των εξής:

- Το Συμβούλιο Διεύθυνσης της Κυβερνοάμυνας (Cyber Defence Management Board - CDMB), το οποίο είναι το κύριο όργανο του ΝΑΤΟ που εποπτεύει τις δραστηριότητες του ΝΑΤΟ στον κυβερνοχώρο.

- Το Συνεργατικό Κέντρο Αριστείας Κυβερνοάμυνας (Cooperative Cyber Defence Centre of Excellence- CCDCOE) στο Ταλίν, στην Εσθονία, ως ερευνητικό και εκπαιδευτικό ίδρυμα που δεν αποτελεί επίσημα μέρος του ΝΑΤΟ, αλλά υποστηρίζεται από μέλη του ΝΑΤΟ που συνεργάζονται με το ΝΑΤΟ σε ζητήματα κυβερνοάμυνας.

- Συνεδριάσεις των Υπουργών Άμυνας του ΝΑΤΟ αφιερωμένες στην κυβερνοάμυνα.

- Διεξαγωγή ασκήσεων κυβερνοάμυνας με μέλη του ΝΑΤΟ.

Το ΝΑΤΟ ενσωμάτωσε επίσης την κυβερνοάμυνα στις υπάρχουσες διαδικασίες παραγωγής πολιτικής. Η έννοια της πολιτικής κυβερνοάμυνας και το σχέδιο δράσης του 2011 συνδέουν την προσπάθεια στην κυβερνοάμυνα που ελέγχεται από το CDMB με την Επιτροπή Άμυνας και Σχεδιασμού σε Ενισχυμένη Μορφή [Defence Policy and Planning Committee in Reinforced Format - DPPC (R)], η οποία ιδρύθηκε το 2010 και διαχειρίζεται τις διαδικασίες σχεδιασμού του ΝΑΤΟ. Το ΝΑΤΟ έχει επίσης καταστήσει πιο διαφανή τη διαδικασία μέσω της οποίας η συμμαχία θα λαμβάνει αποφάσεις σχετικά με απειλές στον κυβερνοχώρο που ενδέχεται να εμπλέκουν τη συλλογική άμυνα στο πλαίσιο της Βορειοατλαντικής Συνθήκης. Στην ουσία, το NCIRC (NATO Computer Incident Response Capability) θα ειδοποιήσει το CDMB για απειλές που έχει εντοπίσει, οι οποίες θα μπορούσαν να εγείρουν ανησυχίες συλλογικής άμυνας και ακολούθως το CDMB θα ενημερώσει και θα συνεργαστεί με το DPPC (R) εάν οι απειλές δικαιολογούν υψηλότερου επιπέδου συμμετοχή για λήψη αποφάσεων.

Μετά την υπουργική σύνοδο του Ιούνιου του 2016, κατά την οποία το ΝΑΤΟ αναγνώρισε τον κυβερνοχώρο ως έναν από τους επιχειρησιακούς τομείς, η συμμαχία ενέκρινε έναν οδικό χάρτη για τον κυβερνοχώρο στο πλαίσιο του οποίου[162]:

- ανακοίνωσε τη δημιουργία ενός νέου Κέντρου Επιχειρήσεων Κυβερνοχώρου (Cyberspace Operations Center - CyOC),

[162] https://www.nato.int/cps/en/natohq/topics_78170.htm

- δημιούργησε νέες επιτελικές λειτουργίες στις δύο στρατηγικές διοικήσεις [Allied Command Operations (ACO), Allied Command Transformation (ACT)],

- συμφώνησε σε ένα κοινό στρατιωτικό όραμα και μία στρατηγική για τον κυβερνοχώρο,

- προώθησε την συνεργασία με την Ευρωπαϊκή Ένωση, μεταξύ άλλων και στα ζητήματα κυβερνοασφάλειας, με έμφαση στην ανάλυση των κυβερνοαπειλών μεταξύ των ομάδων καταγραφής «κυβερνοσυμβάντων» και αντίδρασης – ανταπόκρισης σε αυτά, καθώς και στην ανταλλαγή εμπειριών βέλτιστης πρακτικής που αφορούν στην διαχείριση κρίσεων από την προοπτική του κυβερνοχώρου και των συνεπειών σε αυτόν.

Αυτά τα σημαντικά βήματα είναι ενδεικτικά των προκλήσεων που αντιμετωπίζει το ΝΑΤΟ, ιδιαίτερα δεδομένου του εύρους της συμμαχίας, της σχετικής ανωριμότητας του κυβερνοχώρου ως τομέα στρατιωτικών δραστηριοτήτων και την ποικιλομορφία των δυνατοτήτων και των εμπειριών μεταξύ των συμμάχων στον κυβερνοχώρο[163].

Τέλος, το Βορειοατλαντικό Συμβούλιο διατηρεί την εξουσία να δηλώνει εάν μια επίθεση στον κυβερνοχώρο συνιστά «ένοπλη επίθεση» στο πλαίσιο της Βορειοατλαντικής Συνθήκης.

4.4.3. ΟΗΕ: Προς μια Ψηφιακή Συνθήκη της Γενεύης

Στο πλαίσιο του Οργανισμού των Ηνωμένων Εθνών (ΟΗΕ) από το 1980 δραστηριοποιείται το Ινστιτούτο Ερευνών για τον Αφοπλισμό[164] (the United Nations Institute for Disarmament Research, UNIDIR), το οποίο ως αυτόνομο όργανο διεξάγει ανεξάρτητη έρευνα σχετικά με τον αφοπλισμό και συναφή προβλήματα, ιδίως διεθνή ζητήματα ασφάλειας. Με όραμα την διαμόρφωση ενός σταθερού και πιο ασφαλούς κόσμου στον οποίο τα κράτη και οι άνθρωποι προστατεύονται από απειλές βίας που σχετίζεται με τα όπλα, μεταξύ των σκοπών και των δραστηριοτήτων του ινστιτούτου εντάσσεται και η συνδρομή του στην υποστήριξη κρατών – μελών και ανθρώπων που προωθούν ιδέες και δράσεις που συμβάλλουν στη διαμόρφωση ενός πιο βιώσιμου και ειρηνικού κόσμου.

Με βάση την παραπάνω πρόθεση και αποστολή, το UNIDIR στοχεύει στην υλοποίηση της ανάπτυξης πολιτικών σε εθνικό, περιφερειακό και πολυμερές επίπεδο, καθώς και στη σχετική έρευνα και ανάλυση και εργάζεται για την ευαισθητοποίηση σχετικά με τις πρωτοβουλίες που αλληλεπιδρούν μεταξύ τους και σχετίζονται με τον κυβερνοχώρο προκειμένου να διασφαλιστεί η αρμονική ανάπτυξη και ανάπτυξη ενός σταθερού κυβερνοχώρου[165].

Τα έργα του ινστιτούτου που αναφέρονται στον κυβερνοχώρο και έχουν ολοκληρωθεί:

---

[163] Operationalizing Cyberspace as a Military Domain
https://www.rand.org/pubs/perspectives/PE329.html
[164] http://www.unidir.org/about/the-institute
[165] http://www.unidir.org/est-cyber

- Η έκδοση κείμενου συμπερασμάτων και εκτιμήσεων που αφορά στις «Εθνικές Δυνατότητες, Δόγμα, Οργάνωση και Οικοδόμηση Διαφάνειας και Εμπιστοσύνης για την Κυβερνοασφάλεια» (Απρίλιος 2012 - Οκτώβριος 2013). Η υπόψη μελέτη προσέφερε ένα στιγμιότυπο των τρεχουσών δραστηριοτήτων στον κυβερνοχώρο σε εθνικό, περιφερειακό και διεθνές επίπεδο, προκειμένου να βοηθήσει τους υπευθύνους χάραξης πολιτικής και τους διπλωμάτες να κατανοήσουν την πολυπλοκότητα της αρένας του κυβερνοχώρου. Αποτέλεσε δε το πρώτο εργαλείο του Οργανισμού για την περαιτέρω εμβάθυνση της κατανόησης του νέου «κυβερνοπεδίου» διεθνούς ανταγωνισμού[166].

- Η έκδοση μελέτης που αφορά στις «Προοπτικές για τον πόλεμο στον κυβερνοχώρο: Νομικά πλαίσια, διαφάνεια και οικοδόμηση εμπιστοσύνης»[167] (Φεβρουάριος 2012 – Φεβρουάριος 2012). Το έργο αυτό αύξησε την ευαισθητοποίηση των διπλωματών και των υπευθύνων για τη χάραξη πολιτικής σχετικά με το φάσμα του κυβερνοχώρου και την έναρξη πολυμερών συζητήσεων σχετικά με τον τρόπο πρόληψης και συγκράτησης τέτοιων συγκρούσεων.

- Η εκπόνηση ενός κώδικα («Cyber Index Tool»[168], Μάιος 2012 – Απρίλιος 2015), που περιγράφει την εξέλιξη των ζητημάτων που αφορούν στην ρύθμιση του πλαισίου δραστηριοποίησης στον κυβερνοχώρο σε κρατικό και υπερκρατικό επίπεδο.

Τα έργα του ινστιτούτου που αναφέρονται στον κυβερνοχώρο και βρίσκονται σε εξέλιξη είναι τα ακόλουθα:

- Σειρά σεμιναρίων σε θέματα διεθνούς ασφάλειας στον κυβερνοχώρο.

- Σειρά συνεδρίων σταθερότητας στον κυβερνοχώρο.

- Υποστήριξη των ομάδων κυβερνητικών εμπειρογνωμόνων (Groups of Governmental Experts, GGE) των Ηνωμένων Εθνών για τα θέματα κυβερνοχώρου.

- Σειρά Συσκέψεων για το Διεθνές Δίκαιο και τη Συμπεριφορά των Κρατών στον Κυβερνοχώρο.

Οι διεθνείς προσπάθειες για την αντιμετώπιση των απειλών στον κυβερνοχώρο είναι συγκριτικά πιο περιορισμένες ως προς τους διαθέσιμους πόρους με τις αντίστοιχες σε εθνικό επίπεδο. Οι περισσότεροι διεθνείς οργανισμοί που δραστηριοποιούνται ενεργά σήμερα στον κυβερνοχώρο είναι διακυβερνητικοί, ιδρύθηκαν και λειτουργούν υπό την επιρροή των κυβερνήσεων και βασίζονται σε πολυμερείς συνθήκες. Εξέχον παράδειγμα

[166] http://www.unidir.org/programmes/security-and-technology/national-capabilities-doctrine-organization-and-building-transparency-and-confidence-for-cyber-security-an-assessment
[167] http://www.unidir.org/programmes/security-and-technology/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building
[168] http://www.unidir.org/programmes/security-and-technology/the-cyber-index-tool
http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

είναι ασφαλώς τα Ηνωμένα Έθνη, τα οποία απολαμβάνουν την σχεδόν καθολική συμμετοχή του συνόλου των κρατών. Η Διεθνές Ένωση Τηλεπικοινωνιών (International Telecommunication Union, ITU) είναι ένα ακόμη σημαντικό διεθνές σώμα. Περιφερειακοί οργανισμοί όπως ο Οργανισμός Αμερικανικών Κρατών (OAS), το Περιφερειακό Φόρουμ (ARF) του Συνδέσμου των Χωρών της Νοτιοανατολικής Ασίας (Association of Southeast Asian Nations, ASEAN), ο Οργανισμός Οικονομικής Συνεργασίας Ασίας - Ειρηνικού και ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (Organization for Security and Co-operation in Europe, OSCE) παίζουν επίσης σημαντικούς ρόλους στον τομέα της κυβερνοασφάλειας[169].

Αποτελεί ιδεολογικού χαρακτήρα πεποίθηση μεταξύ των κύκλων του ΟΗΕ ότι είναι οι διεθνείς οργανισμοί που προσφέρουν την εγγενή δυνατότητα να οδηγούν τα κράτη στο τραπέζι των συζητήσεων παρά το γεγονός ότι το μεγαλύτερο μέρος του έργου που αφορά στα ζητήματα κυβερνοάμυνας οργανώνεται από τα κράτη. Οι πολυμερείς οργανισμοί[170], ως θεσπίσματα κρατικών και μη κρατικών οντοτήτων, μπορούν να συγκροτήσουν παράγωγους θεσμούς, όργανα, δομές που εξασφαλίζουν την δυνατότητα να συντονίζουν, να αναπτύσσουν προτάσεις, να ενισχύσουν στρατηγικές και γενικά να συνεισφέρουν στην κατανόηση των φαινομένων στον κυβερνοχώρο και στην αλληλοκατανόηση των «ανησυχιών» των διεθνών δρώντων στο νέο αυτό πεδίο ανταγωνισμού ισχύος. Αυτή η παλέτα δυνατοτήτων περιλαμβάνει την καθιέρωση / ενίσχυση κανόνων και αρχών για:

- την πρόληψη της κακόβουλης χρήση νέων κυβερνοτεχνολογιών,

- τη διαμεσολάβηση συμφωνιών για την εφαρμογή του διεθνούς δικαίου που αφορά στις ένοπλες συγκρούσεις,

- την προώθηση σε εθνικό επίπεδο:
    - της πρόληψης έναντι περιστατικών κυβερνοεπιθέσεων,
    - της προετοιμασίας για αντιμετώπιση περιστατικών κυβερνοεπιθέσεων,
    - της ανταπόκρισης σε περιστατικά κυβερνοεπιθέσεων,
    - της δυνατότητας ανάκτησης λειτουργιών και δεδομένων μετά από περιστατικά κυβερνοεπιθέσεων.

[169] United Nations Institute for Disarmament Research, “The Cyber Index, International Security Trends and Realities”, New York and Geneva, 2013, p.93

[170] United Nations Institute for Disarmament Research, “The Cyber Index, International Security Trends and Realities”, New York and Geneva, 2013, p.93

Συμπεράσματα

Ο Marshall McLuhan[171] πίσω στο όχι και τόσο μακρινό 1967 διατύπωσε τη σκέψη ότι «όποτε ένα νέο περιβάλλον γυρόφερνε ένα παλιό, υπήρχε πάντα μια καινούρια αίσθηση τρόμου». Ωστόσο, όπως παρατηρεί ο Sterling[172], για τον μέσο πολίτη της δεκαετίας του 1870, το τηλέφωνο ήταν μια πιο ζοφερή, πιο υψηλή και πιο δύσκολη στην κατανόησή της τεχνολογία από τα πιο απίθανα καμώματα των προηγμένων υπολογιστών της δεκαετίας του 1990! Παρά τα σύγχρονα τεχνολογικά «θαύματα» της ψηφιακής οπτικοακουστικής τεχνολογίας, της κυβερνοπραγματικότητας με τα πιο ευφάνταστα νέα είδη εγκλημάτων και αντίστοιχων νόμων για να τα καταδιώξουν, ο άνθρωπος, η κοινωνία των ανθρώπων και το διεθνές σύστημα έχει περάσει, όχι μια φορά, από παρόμοιες προκλήσεις και δεν τα πήγαν άσχημα.

Οι βασικές συνέπειες που επέβαλλε η τεχνολογική εξέλιξη στον τομέα της πληροφορίας και της επικοινωνίας με την αποκάλυψη ουσιαστικά μιας νέας διάστασης είναι:

- Η επικράτηση μιας νέας αντίληψης και η μεταβολή του θεσμικού - νομικού πλαισίου περί προστασίας προσωπικών δεδομένων και πολιτικών ελευθεριών (comprehensive review of perspectives and policies).

- Ο ρεαλιστικός κίνδυνος διάβρωσης της εμπιστοσύνης στο Κράτος ως θεσμός, στις υπηρεσίες που αυτό προσφέρει και στη χρησιμότητα μιας κυβέρνησης (Corrosion of State status and competiveness).

- Η συστημική απώλεια των οικονομικών αξιών (Systemic loss of economic value at state level).

- Το κόστος επανασχεδίασης και υλοποίησης μιας νέας αρχιτεκτονικής ασφαλείας που προϋποθέτει αντίστοιχη προσαρμογή των υφιστάμενων και νέων υποδομών.

Παράλληλα, ο κυβερνοχώρος αποκαλύπτεται ως η παράμετρος, που διαπερνά τα τρία επίπεδα, κατά Waltz, μέσα στα οποία πλάθεται η αιτιοκρατική φύση της σύγκρουσης: ο Άνθρωπος, το Κράτος και το Διεθνές Σύστημα. Κάθε προσπάθεια για τον περιορισμό – έλεγχο του κυβερνοχώρου, πόσο μάλλον για την εξουδετέρωσή των φαινομένων που λαμβάνουν χώρα σε αυτόν, φαντάζει ιδιαίτερα μεμακρυσμένη προοπτική, αν όχι ουτοπική, καθώς το επίπεδο μυστικότητας, που για λόγους αυτοσυντήρησης τα Κράτη είναι υποχρεωμένα να διατηρούν, συνιστά την ανατροφοδοτούμενη τροχοπέδη σε κάθε βήμα προς αποκατάσταση δίαυλων επικοινωνίας και συνεννόησης μεταξύ τους για τα ζητήματα ισχύος που σχετίζονται με τον χώρο αυτό.

---

[171] Canadian Broadcasting Corporation, 'Marshall McLuhan in Conversation with Norman Mailer', The Way It Is, broadcast 26 November 1967.
https://www.youtube.com/watch?v=PtzxWR-j1xY (4:32 – 4:35)

[172] Bruce Sterling, "The Hacker Crackdown", Bantam, New York, 1994, p.19-20.

Σε ότι αφορά τον κυβερνοπόλεμο[173], ήρθε για να μείνει και υπάρχουν 5 σημαντικοί λόγοι που κάνουν την τάση χρησιμοποίησής του να είναι αυξητική:

- Το διαδίκτυο είναι ευάλωτο στις κυβερνοεπιθέσεις.

- Υπάρχει πολύ θετικός λόγος οφέλους – κόστους, άλλωστε η νίκη στον κυβερνοχώρο μπορεί να μετατραπεί σε νίκη στο έδαφος ή να θεωρηθεί νίκη στο μυαλό των αντιπάλων ή στην ψυχή των φιλίων.

- Η ανεπάρκεια των υφιστάμενων υποδομών, μέσων και μεθόδων κυβερνοπροστασίας και κυβερνοάμυνας.

- Η ευχερής άρνηση της ευθύνης και η επακόλουθη εύλογη αδυναμία απόδοσης ευθυνών.

- Η δυνατότητα συμμετοχής στο φαινόμενο χωρίς περιορισμούς:

    - ως προς το ποιος συμμετέχει (Κράτη, μη κρατικοί οργανισμοί, ιδιώτες, εταιρείες κλπ),
    - πότε συμμετέχει,
    - πού συμμετέχει (από πού ξεκινά μια επίθεση και που απευθύνεται),
    - πώς συμμετέχει (μέσα, εύρος, κλιμάκωση, κλπ).

Απέναντι στην κυβερνοτρομοκρατία, ακόμα και αν αυτή υποθάλπεται από κρατικούς δρώντες θα μπορούσε να ισχυριστεί κανείς ότι η νεοφιλελεύθερη αρχή της διεθνούς συνεργασίας και της διαφάνειας φαίνεται ότι μπορεί να απαντήσει ικανοποιητικά στο αίτημα για περιορισμό, αν όχι εξάλειψη αυτής της απειλής[174]. Ωστόσο, η παραπάνω θεώρηση βασίζεται στην προϋπόθεση ότι τα Κράτη θα συναινέσουν σε μια κονστρουκτιβιστικής έμπνευσης συνεργασία, παρά το γεγονός ότι συνεχίζουν να διατρέχουν τον κίνδυνο της τυχόν αποσκίρτησης υπηρεσιακών παραγόντων που θα μπορούσαν να αποκαλύψουν πληροφορίες ασφαλείας σε πραγματικούς ή εν δυνάμει ανταγωνιστές τους, κάτι που πιθανότατα αποτελεί πιο επικίνδυνη απειλή από την αρχική απειλή από την οποία προσπαθούν να προστατευθούν, δηλαδή την τρομοκρατία μέσω του διαδικτύου. Άραγε μπορεί να έχει εφαρμογή αυτή η προϋπόθεση απέναντι στον κυβερνοπόλεμο που έχει κηρύξει ένα άλλο Κράτος ή ένας συνασπισμός Κρατών εναντίον ενός άλλου; Η εκτίμηση είναι πως όχι, καθώς τα κυβερνοόπλα έχουν πολλά κοινά χαρακτηριστικά με τα όπλα μαζικής καταστροφής και μάλλον η μελέτη του θεωρητικού υπόβαθρου και της πρακτικής της πυρηνικής αποτροπής μπορεί να προσφέρει τα πλέον στέρεα συμπεράσματα.

Σε ότι αφορά το διεθνές δίκαιο, το φαινόμενο του κυβερνοπολέμου δεν υφίσταται εντός πλήρους νομικού κενού, αλλά υπόκειται κατά βάση σε καθιερωμένους κανόνες και αρχές. Η μετάσταση αυτών των προϋπαρχόντων κανόνων και αρχών στο πεδίο του κυβερνοχώρου αντιμετωπίζει συγκεκριμένες δυσχέρειες και εγείρει αρκετά σημαντικά

---

[173] Kenneth Geers, ‘’Cyberspace and the Changing Nature of Warfare’’, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia

[174] Constantine J. Petallides, ‘’Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat’’, INQUIRIES Journal, 2012, VOL. 4 NO. 03, PG. 1/1 http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat

ερωτήματα, ορισμένα από τα οποία μπορούν να απαντηθούν μέσω της κλασσικής ερμηνείας των υφιστάμενων συνθηκών σε συνδυασμό με μια καλή δόση λογικής, ενώ άλλες απαιτούν ομόφωνη πολιτική απόφαση του διεθνούς νομοθέτη, δηλαδή της διεθνούς κοινωνίας των κρατών[175].

Αν και προς το παρόν ο κυβερνοπόλεμος δεν είχε δραματικές ανθρωπιστικές συνέπειες, ο δρόμος για την εδραίωση της ειρήνης στον κυβερνοχώρο, μόνο εύκολος δεν μπορεί να χαρακτηρισθεί. Η δυναμική πρόκλησης ανθρώπινων τραγωδιών είναι ήδη τεράστια και είναι πιθανό να αυξηθεί με την ολοένα αυξανόμενη εξάρτησή μας τόσο από τα κλασσικά πλέον ηλεκτρονικά συστήματα υπολογιστών όσο και από τα προηγμένα συστήματα τεχνητής νοημοσύνης που ελέγχουν και διατηρούν της επιθυμητές συνθήκες που έχουμε οι ίδιοι καθορίσει για την καθημερινότητα της ζωής μας.

Ο ΟΗΕ, προφανώς δεν έχει καταφέρει πολλά για να αποθαρρυνθούν οι κυβερνοεπιθέσεις, ενώ κατά ειρωνικό τρόπο, οι χειρότεροι παραβάτες είναι τα μόνιμα μέλη του Συμβουλίου Ασφαλείας του. Το επίπεδο μυστικότητας[176] που τα κράτη μπορούν να διατηρούν, ως προς τις δυνατότητές τους να αμυνθούν και να επιτεθούν στο πεδίο ανταγωνισμού που καλείται κυβερνοχώρος, αποτελεί πολύ σοβαρός ανασταλτικός παράγοντας προκειμένου να αποκατασταθούν δίαυλοι επικοινωνίας όπως αυτοί που ακόμα και η πυρηνική ισορροπία μπορούσε να ανεχθεί. Η πιθανότητα εξάλειψης του κυβερνοπολέμου συνολικά είναι μια μακρινή, μη ρεαλιστική, προοπτική, τουλάχιστον προς το παρόν, γι' αυτό το λόγο θα πρέπει ο κόσμος να μάθει να ζει με αυτό. Άλλωστε, υπάρχει το προηγούμενο των Όπλων Μαζικής Καταστροφής του 20ου αιώνα!

«We take interplanetary travel for granted today.
One day Man is going to do the same with interstellar travel.
And people will smile just looking at today's iPhones and iPads, so obsolete and so out-of-date toys the Humans had to deal with to communicate[177]».

[175] Nils Melzer, "Cyberwarfare and International Law", UNIDIR Resources, 2011, Geneva, Switzerland, p.36

[176] "Zero Days": A documentary focused on Stuxnet, a piece of self-replicating computer malware that the U.S. and Israel unleashed to destroy a key part of an Iranian nuclear facility, and which ultimately spread beyond its intended target. Zero Days is a 2016 American documentary film directed by Alex Gibney. It was selected to compete for the Golden Bear at the 66th Berlin International Film Festival.

[177] https://igotoffer.com/blog/how-powerful-was-the-apollo-11-computer

Συνημμένο 1:

Γενική Συνέλευση των Ηνωμένων Εθνών A/70/174, 17η Σύνοδος, Στοιχείο 93 της προσωρινής ημερήσιας διάταξης: «Εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας», Ομάδα των Κυβερνητικών εμπειρογνωμόνων για τις Εξελίξεις, 22 Ιουλίου 2015:

Λαμβάνοντας υπόψη τις υφιστάμενες και τις αναδυόμενες απειλές, τους κινδύνους και τα τρωτά σημεία και βασιζόμενη στις αξιολογήσεις και τις συστάσεις που περιέχονται στις εκθέσεις των προηγούμενων Ομάδων για το 2010 και το 2013, η παρούσα Ομάδα προτείνει τις ακόλουθες συστάσεις προς εξέταση από τα Κράτη για εθελοντικές, μη δεσμευτικές προδιαγραφές, κανόνες ή αρχές υπεύθυνης συμπεριφοράς των κρατών που αποσκοπούν στην προώθηση ανοικτού, ασφαλούς, σταθερού, προσιτού και ειρηνικού περιβάλλοντος Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ):

(α) Σύμφωνα με τους σκοπούς των Ηνωμένων Εθνών, συμπεριλαμβανομένης της διατήρησης της διεθνούς ειρήνης και ασφάλειας, τα κράτη πρέπει να συνεργάζονται για την ανάπτυξη και την εφαρμογή μέτρων για την αύξηση της σταθερότητας και της ασφάλειας στη χρήση των ΤΠΕ και για την πρόληψη των πρακτικών ΤΠΕ που αναγνωρίζονται ως επιβλαβείς που ενδέχεται να αποτελέσουν απειλή για τη διεθνή ειρήνη και ασφάλεια ·

(β) Σε περίπτωση συμβάντων ΤΠΕ, τα κράτη πρέπει να εξετάσουν όλες τις σχετικές πληροφορίες, συμπεριλαμβανομένου του ευρύτερου πλαισίου της εκδήλωσης, τις προκλήσεις της κατανομής στο περιβάλλον των ΤΠΕ και τη φύση και έκταση των συνεπειών.

(γ) τα κράτη δεν πρέπει να επιτρέπουν εν γνώσει τους την επικράτειά τους να χρησιμοποιούνται για διεθνώς παραβατικές πράξεις που χρησιμοποιούν ΤΠΕ.

(δ) Τα κράτη πρέπει να εξετάσουν τον καλύτερο τρόπο συνεργασίας για την ανταλλαγή πληροφοριών, την αμοιβαία συνδρομή, τη δίωξη τρομοκρατικών και εγκληματικών χρήσεων των ΤΠΕ και την εφαρμογή άλλων μέτρων συνεργασίας για την αντιμετώπιση τέτοιων απειλών. Ενδέχεται να χρειαστεί να εξετάσουν τα κράτη μέλη εάν πρέπει να αναπτυχθούν νέα μέτρα από την άποψη αυτή.

(ε) τα κράτη, προκειμένου να διασφαλίσουν την ασφαλή χρήση των ΤΠΕ, θα πρέπει να σέβονται τα ψηφίσματα 20/8 και 26/13 του Συμβουλίου Ανθρωπίνων Δικαιωμάτων σχετικά με την προώθηση, προστασία και απόλαυση των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο, καθώς και τα ψηφίσματα 68/167 και 69/166 σχετικά με το δικαίωμα στην ιδιωτική ζωή στην ψηφιακή εποχή, προκειμένου να διασφαλιστεί ο πλήρης σεβασμός των ανθρωπίνων δικαιωμάτων, συμπεριλαμβανομένου του δικαιώματος στην ελευθερία έκφρασης.

(στ) Κράτος δεν πρέπει να διεξάγει ή να υποστηρίζει εν γνώσει του δραστηριότητες ΤΠΕ σε αντίθεση με τις υποχρεώσεις του βάσει του διεθνούς δικαίου που βλάπτουν σκόπιμα τις ζωτικής σημασίας υποδομές ή αλλοιώνουν τη χρήση και λειτουργία των υποδομών ζωτικής σημασίας για την παροχή υπηρεσιών στο κοινό.

(ζ) Τα κράτη πρέπει να λάβουν τα κατάλληλα μέτρα για να προστατεύσουν την υποδομή ζωτικής σημασίας τους από απειλές ΤΠΕ, λαμβάνοντας υπόψη την απόφαση 58/199 της Γενικής Συνέλευσης για τη δημιουργία μιας παγκόσμιας κουλτούρας για την ασφάλεια του

κυβερνοχώρου και την προστασία των υποδομών ζωτικής σημασίας και άλλων σχετικών ψηφισμάτων.

(η) τα κράτη θα πρέπει να ανταποκρίνονται στις κατάλληλες αιτήσεις συνδρομής από άλλο κράτος, η κρίσιμη υποδομή του οποίου υπόκειται σε κακόβουλες πράξεις ΤΠΕ. Τα κράτη θα πρέπει επίσης να ανταποκρίνονται στις κατάλληλες αιτήσεις για την άμβλυνση των κακόβουλων δραστηριοτήτων ΤΠΕ που στοχεύουν στην υποδομή ζωτικής σημασίας ενός άλλου κράτους που προέρχεται από το έδαφός τους, λαμβάνοντας υπόψη τον σεβασμό της κυριαρχίας.

(θ) Τα κράτη πρέπει να λάβουν εύλογα μέτρα για να διασφαλίσουν την ακεραιότητα της αλυσίδας εφοδιασμού, ώστε οι τελικοί χρήστες να έχουν εμπιστοσύνη στην ασφάλεια των προϊόντων ΤΠΕ. Τα κράτη πρέπει να επιδιώξουν να αποτρέψουν τη διάδοση κακόβουλων εργαλείων και τεχνικών ΤΠΕ και τη χρήση επιβλαβών κρυφών λειτουργιών.

(ι) τα κράτη πρέπει να ενθαρρύνουν την υπεύθυνη αναφορά των τρωτών σημείων ΤΠΕ και να μοιράζονται τις σχετικές πληροφορίες σχετικά με τα διαθέσιμα μέσα αντιμετώπισης τέτοιων τρωτών σημείων προκειμένου να περιορίσουν και, ενδεχομένως, να εξαλείψουν τις πιθανές απειλές για τις ΤΠΕ και τις εξαρτώμενες υποδομές.

(ια) Τα κράτη δεν πρέπει να διεξάγουν ή να υποστηρίζουν εν γνώσει τους δραστηριότητες για τη βλάβη των συστημάτων πληροφόρησης των εξουσιοδοτημένων ομάδων αντιμετώπισης έκτακτων περιστατικών (ορισμένες φορές γνωστές ως ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης από υπολογιστή ή ομάδες αντίδρασης σε περιστατικά ασφάλειας του κυβερνοχώρου) άλλου κράτους. Ένα κράτος δεν πρέπει να χρησιμοποιεί εξουσιοδοτημένες ομάδες αντιμετώπισης καταστάσεων έκτακτης ανάγκης για να διεξάγει κακόβουλες διεθνείς δραστηριότητες.

Συνημμένο 2:

Cyber Operations Tracker[178]

2018
Indictment of officials from the Mabna Institute
Targeting of foreign ministries
Targeting of a European defense agency
Targeting of international sports federations
Targeting of global financial organizations and bitcoin users
Targeting of consulates and embassies in Eastern Europe
Targeting of individuals of interest to the government of Lebanon
Iron Tiger
Compromise of the Dukes
Compromise of computer networks associated with the 2018 Pyeongchang Winter Olympics
APT 37
Compromise of an air-gapped German government network

2017
NotPetya
JadeRAT
Bronze Butler
Indictment of APT 3 threat actors
APT 10
Compromise of Kaspersky Labs
APT 34
Targeting of the government of Belarus
Attempted compromise of email accounts associated with the UK Parliament
CopyKittens
Sowbug
Targeting of U.S. electric companies
Compromise of Qatari website, leading to diplomatic rift
Targeting of the citizen journalism website Bellingcat
WannaCry
Targeting of Ethiopian dissidents
Targeting of a Swiss federal agency
MuddyWater
Compromise of Far Eastern International Bank
Leviathan
Targeting of Marco Rubio's presidential campaign
Longhorn
Phishing campaign against Montenegro
Compromise of a Danish Ministry of Defense e-mail service
Compromise of the Czech foreign minister's computer
Targeting of French presidential candidate Emmanuel Macron's campaign
Magic Hound
WhiteBear
Compromise of the Italian Ministry of Foreign Affairs
Operation BugDrop
Targeting of employees of companies that operate U.S. nuclear power plants
Attempted compromise of Norwegian government networks
APT 33
Compromise of Israeli Defense Force personnel
Mexico accused of targeting journalists and civil society groups
Targeting North Korea's Reconnaissance General Bureau
Distributed denial of service against the government of Montenegro

[178] https://www.cfr.org/interactive/cyber-operations#Timeline

Compromise of cryptocurrency exchanges in South Korea
Compromise of Singapore's Ministry of Defense
Compromise of the International Association of Athletics Federations
Compromise the North Korean nuclear program

2016
Stealth Falcon
OilRig
Compromise of South Korean government computers (2016)
Mofang
RUAG espionage
Compromise of Ukrainian banks
Operation Mermaid
Compromise of the Democratic National Committee
Yahoo breach (2016)
Project Sauron
Compromise of entities involved in the China-Philippines territorial dispute
Targeting of the Islamic State group
A compromise causes a power outage in Kiev, Ukraine
Operation Sphinx
Compromise of computer networks associated with diplomats, journalists, and others in South Korea
Compromise of a mobile app used by Ukrainian artillery units
APT 16
Targeting of Kazakh dissidents
Compromise of the World Anti-Doping Agency
Yahoo breach (2014)
Lazarus Group
Attempted compromise of U.S. think tanks
Unnamed Actor
Shamoon 2.0
Prince of Persia
Compromise of Burmese government websites
Warning of impending incident on Russian banking network
Onion Dog
SWIFT-related bank heists

2015
Ocean Lotus
Duqu 2.0
APT 3
APT 17
Rocket Kitten
APT 30
Compromise of Anthem
Compromise of United Airlines
Targeting of Ukrainian law enforcement and government officials
Compromise of the Seoul subway system
Disruption of GitHub
Compromise of the Permanent Court of Arbitration's website
Compromise of unclassified White House networks
Emissary Panda
Compromise of South Korean government computers (2015)
Compromise of TV5 Monde
Blue Termite
Attempted compromise of the Dutch organization investigating the crash of flight MH17
Compromise of networks in the Saudi government ministries
Compromise of social media accounts of State Department officials
Compromise of the networks at the German parliament (Bundestag)
Network compromise at the Australian Bureau of Meteorology
Compromise of the Japanese pension system

Compromise of a power grid in eastern Ukraine
Equation Group
Compromise of a Pentagon legacy system
Compromise at the Office of Personnel Management
Hellsing
Compromise of an unclassified network associated with the U.S. Joint Chiefs of Staff

2014
APT 28
Black Energy
Newscaster
APT 18
Compromise of Community Health Systems
DragonOK
Compromise of U.S. Transportation Command Contractors
Turla
Moafee
Compromise of Canada's National Research Council
APT 12
Compromise of U.S. Investigations Services
Axiom
Careto
Fake Occupy Central apps
Snowglobe
Compromise of iCloud in China
Saffron Rose
Compromise of the U.S. State Department
Darkhotel
Compromise of the U.S. Postal Service
Regin
Putter Panda
Compromise of the U.S. National Oceanic and Atmospheric Administration
Operation Cleaver
Lotus Blossom
Attempted compromise of Ukrainian email accounts
Cloud Atlas
Crouching Yeti
Compromise of the Sands Casino
Indictment of PLA officers
Attack on a German steel plant
Compromise of Boeing
Machete
Compromise of Sony Pictures Entertainment

2013
The Dukes
Kimsuky
admin@338
Icefog
Deep Panda
Mirage
Red October
Compromise of EADS and ThyssenKrupp
PLA Unit 61398
Compromise of the Indian Defense Research and Development Organization
Team Spy Crew
Unresponsive computer networks in South Korea
Anchor Panda
Compromise of Australian government agencies
Patchwork

Compromise of unclassified U.S. Navy network
NetTraveler
Compromise of the Finnish Ministry of Foreign Affairs
Sykipot

2012
Denial of service attacks against U.S. banks in 2012–2013
Compromise of Coca-Cola
Lucky Cat
Flame
Madi
Compromise of Nortel
Gauss
Attempted compromise of the BBC Persian TV service
Sneaky Panda
SabPub
ITSecTeam
Compromise of Saudi Aramco and RasGas

2011
Compromise of a Taiwanese political party
Compromise of certificate issuer DigiNotar
Compromise at Mitsubishi Heavy Industries
Nitro attacks
Duqu
Interference with NASA satellite Landsat 7
Compromise of Canadian government departments
Interference with NASA satellite Terra (EOS AM-1)
Compromise of RSA SecureID tokens
Compromise of the U.S. Chamber of Commerce
Denial of service incident against South Korean and U.S. targets
Denial of service incident against a South Korean bank
Compromise of Oak Ridge National Laboratory
Shady RAT

2010
Compromise of the Indian Prime Minister's Office
Operation Aurora
Malware targets Vietnamese users
Night Dragon
Compromise of three Australian mining companies
Shadow Network
Stuxnet
Defacement of Baidu

2009
GhostNet
Compromise of the office of Senator Ben Nelson
Compromise of computers associated with the Joint Strike Fighter program
Fourth of July incident

2008
Compromise of Indian military computers
Offensive cyber campaign against Georgia
Compromise of U.S. presidential campaigns in 2008
Compromise at NASA Kennedy Space Center
Compromise of NASA network in Washington, DC
Agent.btz
Targeting of pro-Tibet activist groups

2007
Estonian denial of service incident
Compromise of National Defense University
Secretary of defense email incident
Compromise of German government networks
Compromise of French Defense Ministry website
Attempted compromise of Australian and New Zealand government computers
Compromise at the Department of Homeland Security
Attack on the Syrian Air Force
Compromise of Chinese government computers
Targeting of U.S. National Laboratories

2006
Compromise at the State Department
Compromise of the Pentagon's NIPRNet
Compromise at U.S. Naval War College

2005
Titan Rain

Download the Data

Συνημμένο 3:

"SAM Framework" Analysis[179]

Table 1 SAM-framework		
Stakeholder	Who?	Who is mandating, who is executing and who is affected?
Activities	What?	What activities have been carried out and what are the results in terms of defects?
Motives	Why?	Why have the activities been carried out, what are the underlying motivation and intentions?

Table 2 Stakeholders		
Name	**Description**	**Examples**
Individuals	Individual people	Comodohacker, Kevin Mitnick
Collectives, swarms	Temporary, cause-related pooling of individuals	4chan, anonymous
Groups	Structured and perpetual assemblage of individuals	Al-Qaeda, LulzSec
Organizations, enterprises	Constituted legal entities	Cisco, VW, GE, Exxon, Lockheed Martin
States, intergovernmental and supranational organizations		USA, UN, NATO, EU, Germany, China, Iran

Table 3 Actions			
	Example		**Physical impact**
Non-disruptive	To seal, to intercept To influence To manipulate, to control	Stealing of trade secrets Influencing public opinion Manipulation of financial services	Indirect Indirect Indirect, direct
Destructive	To disrupt, to destroy	Disruption of power supply	Direct

[179] Jan-Frederik Kremer, Benedict Muller (Editors) ''Cyberspace and International Relations, Theory, Prospects and Challenges, Springel - Verlag Berlin Heidelberg, 2014, p.46-55

Table 4 Motives		
Economic Psychological	Ideological Power-related	Political …

Table 5 Threats for governments	
Direct threats to authorities	**Indirect threats**
Government is directly affected	State (population, economy…) is affected, government might be responsible for protection
Disruption of government communications, stealing of state secrets, influencing of government decisions, attack of military infrastructure	Attacks on power grid, water supply, industrial espionage, disruption of major production facilities and communication networks, manipulation or disruption of financial transactions, …

Table 6 Relevance of threats: illustrative examples	
Low relevance for authorities (examples)	High relevance for authorities (examples)
Individual credit card fraud, hacking of an individual mail account, very limited stealing of insensitive corporate data, limited influencing attempts	Cyber-attack on government/military IT, disruption of stock market communication etc., attack on power grid, coordinated hacking of senior officials mail accounts, systematic and wide range stealing of sensitive industrial secrets

Table 7 Competence versus relevance		
	Low relevance	High relevance
Direct competences	Low threat level, low need for action by authorities, authorities are able to react— *non-critical situation*	High threat level, high need for actions by authorities, authorities are able to react— *critical, but solvable situation*
Indirect / no competences	Low threat level, low need for action by authorities, authorities are poorly to react—*partly critical situation*	High threat level, high need for action by authorities, authorities are poorly to react—*critical situation*

Πηγές

Βιβλιογραφία – Αρθρογραφία

1. George Doukidis, Nikos Mylonopoulos, and Nancy Pouloudi , ‘’Social and Economic Transformation in the Digital Era’’, Athens, June 2003
2. Bruce R. Guile (Editor), ‘’Information Technologies and Social Transformation’’, National Academy of Engineering; Melvin Kranzberg, ‘’The Information Age: Evolution or Revolution?’’, NATIONAL ACADEMY PRESS, Washington D.C. 1985
3. D.J.Betz & T.Stevens, “CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER”, IISS, Arundel House, London, 2011
4. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: Executive Office of the President of the United States, 2009
5. Nazli Choucri, ‘’Cyberpolitics in International Relations’’, The MIT Press, Cambridge, Massachusetts, London, England, 2012
6. Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges, Springel - Verlag Berlin Heidelberg, 2014
7. Robert O. Keohane and Joseph S. Nye, Jr. ‘’Power and interdependence in the information age’’, Foreign Affairs, 77(5)
8. Kenneth Waltz, “Ο Άνθρωπος, το Κράτος και ο Πόλεμος: Μια θεωρητική ανάλυση”, Μετάφραση: Κ.Κολιόπουλος, Εισαγωγή στην Ελληνική έκδοση: Η.Κουσκουβέλης, Εκδόσεις Ποιότητα, Βάρη Αττικής, 2011
9. Harold D. Lasswell, ‘’Politics: Who Gets What, When, How’’, New York: Whittlesey House, 1936
10. Robert Reardon and Nazli Choucri, ‘’The Role of Cyberspace in International Relations: A View of the Literature’’, Department of Political Science, MIT,Paper Prepared for the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012
11. Roxana Radu, ‘’Power Technology and Powerful Technologies: Global Govermentality and Security in the Cyberspace’’ [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]
12. Craig B. Greathouse, ‘’Cyber War and Strategic Thought Do the Classic Theorists Still Matter’’, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]
13. Hanna Samir Kassab, ‘’In Search of Cyber Stability: International Relations,Mutually Assured Destruction and the Age of Cyber Warfare’’ [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

14. Ηλίας Κουσκουβέλης, ‘’Εισαγωγή στις Διεθνείς Σχέσεις, Εκδόσεις Ποιότητα, Ε’ Έκδοση, 2007

15. Adams, James, "Virtual Defense" Foreign Affairs Vol. 80, No. 3 (May - Jun., 2001)

16. Johan Sigholm, ‘’NON-STATE ACTORS IN CYBERSPACE OPERATIONS’’ Captain, Ph.D. Swedish National Defence College

17. Κ.Αντωνόπουλος, Κ.Μαγκλιβέρας, ‘’Το Δίκαιο της Διεθνούς Κοινωνίας’’, Εμμανουέλα Δούση, ‘’Η Διεθνής Ευθύνη των Κρατών’’ ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, (3η έκδοση), Αθήνα, 2017

18. Measheimer John, ‘’The tragedy of great power politics, W.W Noston & Co, N.Y. – London, 2001

19. Andrew Radin, Hybrid Warfare in the Baltics, Threats and Potential Responses, RAND Corporation, Santa Monica, Calif. 19 Oct 2015

20. Hannah Samir Kassab, “In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

21. Ηλίας Κουσκουβέλης, ‘’Θεωρία Διεθνών Σχέσεων στον Ψυχρό Πόλεμο, Αποτροπή και Πυρηνική Στρατηγική”, Εκδόσεις Ποιότητα, Β’ Έκδοση, Αθήνα, 2000

22. Salma Shaheen, “Offence – Defense Balance in Cyber Warfare, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

23. Carl Von Clausevitz, “On War”, Edited and Translated by M.Howard and P.Papet, Princeton University Press, New Jersey, 1989

24. Sascha Knoepfel, “Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

25. Johan Eriksson and Giampiero Giacomello, “The Information Revolution, Security, and International Relations”, International Political Science Review / Revue internationale de science politique, Vol. 27, No. 3, Jul 2006

26. S.D.McDowell et al., “Cooperative International Approaches to Network Security”, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

27. Katharina C. Below, “The Utility of Timeless Thoughts: Hannah Arendt’s Conceptions of Power and Violence in the Age of Cyberization”, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

28. Hannah Arendt, “On violence”, New York, Harcourt Brace Javanovich, 1970

29. Bruce Schneier, ‘’Secrets and Lies, DIGITAL SECURITY IN A NETWORKED WORLD”, Wiley Publishing, Inc., Indianapolis, Indiana, 2004

30. Landers, Chris, "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)". Baltimore City Paper, 04 Apr 2008

31. The Department of Defense Cyber Strategy, 17 Apr 2015

32. D.J.Betz & T.Stevens, “CYBERSPACE AND THE STATE: TOWARD A STRATEGY FOR CYBER-POWER”, IISS, Arundel House, London, 2011

33. Karen Rose, Scott Eldridge, Lyman Chapin ‘’The Internet of Things, An Overview Understanding the Issues and Challenges of a More Connected World’’, The Internet Society (ISOC), 2015

34. Paul Virilio, ‘’SPEED AND POLITICS’’, Published by Semiotext(e), Wilshire Blvd, Suite 427, Los Angeles, 2007

35. Betrand Russell, “Power: A new Social Analysis”, G. Allen & Unwin LTD, London, 1938

36. Andrew Hoskins & Ben O’Loughlin, “War and Media: The Emergence of Diffused War”, Malden, MA, Cambridge: Polity, 2010

37. William Mitchell, “Winged Defense: The Development and Possibilities of Modern Air Power – Economic and Military”, Dover Publications, New York, 1988

38. Fritz Machlup, “The Production and Distribution of Knowledge in the United States”, Princeton, NJ: Princeton University Press, 1962

39. Peter F. Drucker, “The Age of Discontinuity: Guidelines to Our Changing Society”, London, Pan Books, 1971

40. Daniel Bell, “The Coming of the Post-Industrial Society: A Venture in Social Forecasting”, London, Heinemann Educational, 1974

41. Manuel Castells, “The Rise of the Network Society”, Malden, MA and Oxford: Blackwell, 2000

42. Christian Fuchs, “Internet and Society: Social Theory in the Information Age”, New York and Abingdon: Routledge, 2008

43. Manuel Castells, “The Internet Galaxy: Reflections on the Internet, Business, and Society”, Oxford, Oxford University Press, 2001

44. Clarissa Rile Hayward, “De-Facing Power”, Cambridge: Cambridge University Press, 2000, p. 30. Cited in Barnett and Duvall, ‘Power in International Politics’, p. 56.

45. Carsten F. Roennfeldt, ‘Productive War: A Re-Conceptualisation of War’, Journal of Strategic Studies, vol. 34, no. 1, 2011

46. Cornish, et al. ‘’Cyberspace and the national security of the United Kingdom. Threats and responses’’, Chatham House Report, London, 2009

47. Σπυρίδων Λίτσας, “Πόλεμος και Ορθολογισμός, Θεωρητικές Προεκτάσεις και Στρατηγικές Εφαρμογές”, Εκδόσεις ΠΟΙΟΤΗΤΑ, Βάρη Αττικής, 2011,

48. Ηλίας Κουσκουβέλης, ‘’Θεωρία Απόφασης στον Θουκυδίδη’’, Εκδ. Πανεπιστημίου Μακεδονίας, Θεσσαλονίκη, 2015

49. J.Rosenau, ‘’The scientific Study of Foreign Policy’’, London, Collier-MacMillan, 1971

50. Γ.Μ.Σπυρόπουλος, ‘’Διεθνείς Σχέσεις, Ρεαλιστική Προσέγγιση, Θεωρία και Πράξη’’, Αθήνα, Εκδόσεις Ποιότητα, 2010

51. Herbert S. Lin, “Offensive Cyber Operations and the Use of Force”, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Vol. 4:63], 2010

52. Keneth Geers, “Cyberspace and the Changing Nature of Warfare”, Cooperative Cyber Defence Centre of Excellence (keynotes 1 & 3), Tallin

53. Sascha Knoepfel, “Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

54. Martin C. Libicki, “Cyberdeterrence and Cyberwar”, RAND Corporation, 2009

55. Nils Melzer, “Cyberwarfare and International Law”, UNIDIR Resources, Geneva, 2011

56. Matthew Crosston, “Phreak the Speak: The Flawed Communications within Cyber Intelligentsia”, [Jan-Frederik Kremer, Benedict Muller (Editors) ‘’Cyberspace and International Relations, Theory, Prospects and Challenges’’, Springel - Verlag Berlin Heidelberg, 2014]

57. Joseph S. Nye, Jr, ‘’Cyber Power’’, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010

58. David E. Graham, ‘’Cyber Threats and the Law of War’’, Journal of National Security Law & Policy, vol 4:87, 2010

59. HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, Brussels, Feb 7, 2013

60. Annegret Bendiek, Raphael Bossong and Matthias Schulze, “The EU’s Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges” (Translation by Tom Genrich), Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs, Berlin, 2017

61. United Nations Institute for Disarmament Research, “The Cyber Index, International Security Trends and Realities”, New York and Geneva, 2013

62. Bruce Sterling, “The Hacker Crackdown”, Bantam, New York, 1994

Διαδίκτυο (websites – podcasts – multimedia)

1. Bruce Sterling, “The Hacker Crackdown”, 1994, https://doc.lagout.org/security/Hacking-The%20Hacker%20Crackdown.pdf
2. David Burkett, ‘’DIGITISATION AND DIGITALISATION: WHAT MEANS WHAT?’’ Dec 19, 2017, https://workingmouse.com.au/innovation/digitisation-digitalisation-digital-transformation
3. Michael Fitzgerald, ‘’The Nine Obstacles to Digital Transformation’’ https://sloanreview.mit.edu/article/the-nine-obstacles-to-digital-transformation/
4. Κοινωνιοπάθεια: Αντικοινωνική διαταραχή της προσωπικότητας https://www.onmed.gr/ygeia-psyhikh/story/331885/ta-simadia-pou-apokalyptoun-enan-koinoniopathi
5. John Perry Barlow, Crime and Puzzlement (June 1990), https://www.eff.org/pages/crime-and-puzzlement
6. Tim A.Scally, ‘’Cyber Reality: How the Security Industry Is Adjusting to the New Normal’’, Security Distributing & Marketing, 02 Sep 2017 https://www.sdmmag.com/articles/94274-cyber-reality-how-the-security-industry-is-adjusting-to-the-new-normal
7. Nicola Tesla, interview with John B. Kennedy, 1926 https://www.businessinsider.com/tesla-predicted-smartphones-in-1926-2015-7
8. Carl Sagan, cosmologist, https://www.wired.com/2011/05/a-day-to-remember-carl-sagan/ https://www.youtube.com/watch?time_continue=7&v=jod7v-m573k
9. Constantine J. Petallides, ‘’Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat”, INQUIRIES Journal, 2012, Vol.4 No.03 http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat
10. Johan Sigholm – “Non State Actors in Cyberspace Operations”, p.11 https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations
11. Chris Doman, ‘’The First Cyber Espionage Attacks: How Operation Moonlight Maze made history’’, A Medium Corporation, Jul 7, 2016 https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7 https://securelist.com/penguins-moonlit-maze/77883/
12. Mark Galeotti, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” In Moscow’s Shadow (blog), July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

13. Rob Boffard, ‘’Could An Evil Mega-Corporation Ever Exist In Real Life?’’ https://io9.gizmodo.com/could-an-evil-mega-corporation-ever-exist-in-real-life-1630401831

14. Kamlesh Bajaj, “The Cybersecurity Agenda, Mobilizing for International Action, The EastWest Institute, New York, 2010 https://www.eastwest.ngo/sites/default/files/ideas-files/Bajaj_Web.pdf

15. Anne-Marie Slaughter, Thomas Hale, ‘’International Relations, Principal Theories’’, Published under the auspices of the Max Planck Foundation for International Peace and the Rule of Law under the direction of Rüdiger Wolfrum, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011 www.mpepil.com http://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e722?rskey=ePM79E&result=1&prd=OPIL

16. US Department of Homeland Security ‘’2009 Cyberspace Policy Review’’, https://www.dhs.gov/publication/2009-cyberspace-policy-review

17. Presented by Leigh Alexander with Matt Shore and produced by Matt Shore and Katie Callin ‘’Internet access is now a basic human right: part 1 – Chips with Everything tech podcast’’, https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast

18. United Nations, General Assembly, Human Rights Council, 32nd session, Agenda item 3, “Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development”, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

19. Universal Declaration of Human Rights http://www.un.org/en/universal-declaration-human-rights/

20. James Vincent, ‘’UN condemns internet access disruption as a human rights violation’’ Jul 4, 2016, https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access

21. ‘’THE CONSTITUTION OF GREECE As revised by the parliamentary resolution of May 27th 2008 of the VIIIth Revisionary Parliament’’ https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf

22. Mark Ward, ‘’A brief history of hacking’’ 09 Jun 2011, https://www.bbc.com/news/technology-13686141

23. Roger A. Grimes, ‘’Your guide to the seven types of malicious hackers’’, 08 Feb 2011 https://www.csoonline.com/article/2623407/your-guide-to-the-seven-types-of-malicious-hackers.html

24. What Is an Advanced Persistent Threat (APT)?
https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

25. What is a DDoS Attack? - DDoS Meaning
https://www.kaspersky.com/resource-center/threats/ddos-attacks

26. Jennifer J. Li, Lindsay Daugherty, ‘’Training Cyber Warriors.What Can Be Learned from Defense Language Training?
https://www.rand.org/pubs/research_reports/RR476.html

27. https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

28. Jaikumar Vijayan, ‘’McColo takedown: Internet vigilantism or online Neighborhood Watch?’’
https://www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html

29. Peter Warren, ‘’ Hunt for Russia's web criminals’’ Thu 15 Nov 2007
https://www.theguardian.com/technology/2007/nov/15/news.crime

30. Dawn Kawamoto, ‘’Storm worm' rages across the globe’’ April 13, 2007
https://www.cnet.com/news/storm-worm-rages-across-the-globe/

31. https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

32. Symantec Official Blog, ‘’International Takedown Wounds Gameover Zeus Cybercrime Network’’
https://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

33. Rhodri Marsden, ‘’Cyber Culture: Mugshots are forever (well, that;s what website blackmailers would like you to believe)’’,INDEPENDENT, 9 Oct 2013
https://www.independent.co.uk/life-style/gadgets-and-tech/features/cyber-culture-mugshots-are-forever-well-thats-what-website-blackmailers-would-like-you-to-believe-8869808.html

34. Mary-Ann Russon, ‘’Pirate Bay loses hydra and .se domains, returning to original .org address following legal challenges’’ Updated May 23, 2016
https://www.ibtimes.co.uk/pirate-bay-loses-hydra-domains-returning-original-org-address-following-legal-challenges-1561515

35. Testimony of Evan F. Kohlmann with Laith Alkhouri and Alexandra Kassirer Before the House Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media” Charlie Hebdo and the Jihadi Online Network: Assessing the Role of American Commercial Social Media Platforms, January 27, 2015; 2:30pm, 2172 Rayburn House Office Building, Washington D.C.
https://docs.house.gov/meetings/FA/FA18/20150127/102855/HHRG-114-FA18-Wstate-KohlmannE-20150127.pdf

36. Tarquin, ‘’How To Access Notorious Dark Web Anonymously (10 Step Guide)’’ Updated on 18 May 2018, https://darkwebnews.com/help-advice/access-dark-web/

37. Donna Leinwand Leger, ‘’ How FBI brought down cyber-underworld site Silk Road’’, USA TODAY, Published Oct. 21, 2013, Updated May 15, 2014 https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

38. David Meyer, ‘’A Cyber Gang Stole $1 Billion by Hacking Banks and ATMs. Now Police Say They've Caught the Mastermind’’, FORTUNE, March 26, 2018 http://fortune.com/2018/03/26/carbanak-europol-arrest-spain-malware-banks/

39. Lindsey O’Donnell, ‘’ALLEGED MASTERMIND BEHIND CARBANAK CRIME GANG ARRESTED’’, threatpost.com, Mar 28,2018 https://threatpost.com/alleged-mastermind-behind-carbanak-crime-gang-arrested/130831/

40. Council on Foreign Relations, ‘’Europe Slowly Starts to Talk Openly About Offensive Cyber Operations‘’, Nov 6, 2017 https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations

41. Robin Emmott, ‘’NATO mulls 'offensive defense' with cyber warfare rules’’, Reuters, Reuters, Nov 30, 2017 https://www.reuters.com/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4

42. Cyber Operations Tracker https://www.cfr.org/interactive/cyber-operations#Takeaways

43. Daniel W. Drezner “WEIGHING THE SCALES: THE INTERNET’S EFFECT ON STATE-SOCIETY RELATIONS”, Brown Journal of World Affairs, Vol. 16, No. 2, p.31-44, Spring / Summer 2010 http://www.danieldrezner.com/research/scales.pdf

44. M.Barnett & R.Duvall, ‘’Power in International Politics’’, International Organization, Vol. 59, No. 1 (Winter, 2005), (pp. 39-75) Published by: Cambridge University Press on behalf of the International Organization Foundation, p.48 https://www.researchgate.net/publication/4854229_Power_in_International_Politics/link/5c49b5fc92851c22a38ccf51/download

45. Hannah Roberts, “The Turkish Government reportedly blocked WhatsApp and other social media sites”, Nov. 4, 2016, 10:43 AM https://www.businessinsider.com/social-media-and-messaging-sites-blocked-in-turkey-2016-11

46. Mihoko Matsubara, ‘’A Stuxnet Future? Yes, Offensive Cyber-Warfare is Already Here’’, 2012, https://www.files.ethz.ch/isn/188327/ISN_154091_en.pdf

47. Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia”, 17 May 2007
https://www.theguardian.com/world/2007/may/17/topstories3.russia

48. Mark Landler & John Markoffmay, “Digital Fears Emerge After Data Siege in Estonia”, May 29, 2007
https://www.nytimes.com/2007/05/29/technology/29estonia.html

49. Joshua Davis, “HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE” , Aug 21, 2007
https://www.wired.com/2007/08/ff-estonia/

50. Matt Field, “Is cyberwarfare war? Insurers balk at paying for some cyberattacks”, April 18, 2019
https://thebulletin.org/2019/04/is-cyberwarfare-war-insurers-balk-at-paying-for-some-cyberattacks/

51. Kate Fazzini, “Israel says it bombed Hamas compound that committed cyberattacks” May 6, 2019,
https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html

52. Paul Bracken, “The Intersection of Cyber and Nuclear War”, Jan 17, 2017
https://thestrategybridge.org/the-bridge/2017/1/17/the-intersection-of-cyber-and-nuclear-war

53. Rosemary Tropeano, “Deterrence in Cyber, Cyber in Deterrence”, May 27, 2019
https://thestrategybridge.org/the-bridge/2019/5/27/deterrence-in-cyber-cyber-in-deterrence

54. UN General Assembly resolution 36/103, “Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States”, Dec 9, 1981
https://treaties.un.org/doc/publication/ctc/uncharter.pdf

55. Vienna Convention on Diplomatic Relations
http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

56. Universal Declaration of Human Rights, article 19
https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

57. UN General Assembly resolution A/RES/56/83 of 12 December 2001 and its annex
https://www.ilsa.org/Jessup/Jessup11/basicmats/StateResponsibility.pdf

58. International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), merits, 1986
https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

59. Jean-Marie Henckaerts & Louise Doswald-Beck, “Customary International Humanitarian Law”, Cambridge University Press, New York, 2005,
https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf

60. Michael Schmitt, “Cyber Operations and the Jus in Bello: Key Issues”, Naval War College International Law Studies, 2011, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1077&context=ils

61. ICRC - Additional Protocols to the Geneva Conventions of 12 Aug 1949, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf

62. Andy Budd, “How To Build Digital Capacity And Attracting Talent” https://www.smashingmagazine.com/2015/11/building-digital-capacity-attracting-talent/

63. Melissa Hathaway Questions, “Internet Security Alliance, Issue Area 3: Norms of Behavior”, March 24, 2009, at 2, 4-7 https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20ISSUE%20AREA%203%20-%20NORMS%20OF%20BEHAVIOR---HATHAWAY%20QUESTIONS.pdf

64. Melissa Hathaway, “Getting beyond Norms: When Violating the Agreement Becomes Customary Practice”, CIGI Paper No. 127, April 20, 2017 https://www.cigionline.org/publications/getting-beyond-norms-when-violating-agreement-becomes-customary-practice

65. Michael Beaver, ‘’THE UNITED NATIONS AND CYBERWARFARE’’, Global Risk Advisors, Sep 28, 2016 https://globalriskadvisors.com/united-nations-cyber-warfare/

66. United Nations A/70/174 General Assembly, 17th Session, Item 93 of the provisional agenda: ‘’Developments in the field of information and telecommunications in the context of international security’’, Group of Governmental Experts on Developments, July 22, 2015 https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

67. EU International Cyberspace Policy https://eeas.europa.eu/topics/eu-international-cyberspace-policy/415/eu-international-cyberspace-policy_en

68. Cyber-attacks: the Council of EU is now able to impose sanctions https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

69. Fidler, David P.; Pregent, Richard; and Vandurme, Alex, "NATO, Cyber Defense, and International Law" (2013). Articles by Maurer, Faculty. Paper 1672. http://www.repository.law.indiana.edu/facpub/1672

70. NATO Cyber defence, https://www.nato.int/cps/en/natohq/topics_78170.htm

71. Operationalizing Cyberspace as a Military Domain https://www.rand.org/pubs/perspectives/PE329.html

72. United Nations Institute for Disarmament Research, The Institute http://www.unidir.org/about/the-institute

73. United Nations Institute for Disarmament Research, Cyber http://www.unidir.org/est-cyber

74. http://www.unidir.org/programmes/security-and-technology/national-capabilities-doctrine-organization-and-building-transparency-and-confidence-for-cyber-security-an-assessment

75. http://www.unidir.org/programmes/security-and-technology/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building

76. http://www.unidir.org/programmes/security-and-technology/the-cyber-index-tool

77. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

78. Canadian Broadcasting Corporation, 'Marshall McLuhan in Conversation with Norman Mailer', The Way It Is, broadcast 26 November 1967. https://www.youtube.com/watch?v=PtzxWR-j1xY (4:32 – 4:35)

79. https://igotoffer.com/blog/how-powerful-was-the-apollo-11-computer

Φιλμογραφία - Ντοκιμαντέρ

1. ''Neuromancer'',by William Gibson, edited by Terry Carr, 1984

2. "Web Warriors", by Jay Dahl, 2008

3. "Cyberwars: Invisible Warfare", by Antoine Vitkine, 2011

4. "Zero Days", by Alex Gibney, 2016

Ευρετήριο

Παράγωγες σύνθετες λέξεις με πρώτο συνθετικό το θέμα «κυβερν-» κατά σειρά όπως συναντώνται στο κείμενο την πρώτη φορά, εντός εισαγωγικών.