Όνομα Φοιτητή: Δημοσθένης Γεωργίου

Τμήμα: Κοινωνικών και Πολιτικών Επιστημών, Διεθνείς Σχέσεις 2ο

Μάθημα: Διπλωματική Εργασία Μάστερ, ΚΠΕ599 19

Επιβλέπον Καθηγητής: Παύλος Κοκτσίδης

Εαρινό Εξάμηνο 2023-2024

Παραβιάσεις (εδαφικής) κυριαρχίας στον Κυβερνοχώρο: Μια ισορροπία δυνάμεων μεταξύ ΗΠΑ και Ρωσίας / Κίνας

Περίληψη

Η εργασία παρουσιάζει την άποψη και την προσέγγιση των μεγάλων δυνάμεων των ΗΠΑ, Ρωσίας και Κίνας σχετικά με τον κυβερνοχώρο και την εδαφική κυριαρχία σε αυτόν. Η σημασία της ενεργού υπεράσπισης της κυριαρχίας των κρατών στον κυβερνοχώρο αναλύεται στην εργασία, αλλά εκφράζει επίσης τη δέσμευσή των δυνάμεων αυτών στη διεθνή συνεργασία και διακυβέρνηση βασισμένη σε δημοκρατικά και διαφανή κριτήρια. Οι χώρες αυτές έχουν θεσπίσει νόμους για την ασφάλεια του Διαδικτύου και την προστασία του κυβερνοχώρου, ενισχύοντας έτσι το νομικό πλαίσιο για την προστασία των ψηφιακών τους δραστηριοτήτων. Τέλος, προτείνονται πρωτοβουλίες για την ανάπτυξη και ασφάλεια του Διαδικτύου, περιλαμβανομένης της ενίσχυσης της διεθνούς συνεργασίας και του σεβασμού του κυβερνοχώρου ως βασικής αρχής. Συνολικά, η εργασία αναδεικνύει την προσπάθεια των μεγάλων δυνάμεων να παίξουν ενεργό ρόλο στη διαμόρφωση των διεθνών προτύπων και πολιτικών για τον κυβερνοχώρο, ενώ παράλληλα να εξασφαλίσουν την ασφάλεια και την κυριαρχία της σε αυτόν τον τομέα.

Πίνακας Περιεχομένων

1. Εισαγωγή

Ο κυβερνοχώρος σήμερα αναδεικνύεται ως νέο επιχειρησιακό πεδίο, όπου οι χώρες ανταγωνίζονται για την επιρροή, την ασφάλεια και την κυριαρχία. Ο κυβερνοχώρος έχει γίνει ένα θεμελιώδες χαρακτηριστικό του κόσμου στον οποίο ζούμε, επηρεάζοντας σχεδόν κάθε πτυχή της καθημερινότητάς μας. Η εμφάνιση του στην πολιτική σκηνή έχει μεταστρέψει τον κυβερνοχώρο από ένα θέμα "χαμηλής πολιτικής" σε ένα θέμα "υψηλής πολιτικής", με τις προκλήσεις και τις απειλές που παρουσιάζει να επηρεάζουν την εθνική ασφάλεια και να διαταράσσουν τη διεθνή τάξη. Ο κυβερνοχώρος ανατρέπει τις παραδοσιακές αντιλήψεις για τον χρόνο, τον χώρο, τη διείσδυση, την ρευστότητα, τη συμμετοχή, την αναγνώριση, και την ευθύνη, δημιουργώντας έναν νέο χώρο πολιτικής δράσης και αντιδράσεων. Η ανάλυση των προτύπων πρόσβασης και συμμετοχής, οι νέοι τύποι διεθνών συγκρούσεων και αντιπαραθέσεων, και οι εναλλακτικές προοπτικές για τον κυβερνοχώρο αποτελούν το νέο πεδίο έρευνας για την κατανόηση του. Με δεδομένο ότι οι παραδοσιακές προσεγγίσεις στη θεωρία και την έρευνα των διεθνών σχέσεων είναι κυρίως εστιασμένες στο κράτος και στη δυναμική της εξουσίας μεταξύ μεγάλων δυνάμεων, ουσιαστικά εξετάζουν την ανθρωποκεντρική προσέγγιση, κυρίως ορίζοντας τους όρους της αναμέτρησης βάσει κοινωνικών παραμέτρων. Ωστόσο, αυτή η παραδοσιακή προσέγγιση δεν έχει προσαρμοστεί ακόμα στον κυβερνοχώρο. Η θεωρία των διεθνών σχέσεων δεν έχει ακόμα αναγνωρίσει τις επιπτώσεις του κυβερνοχώρου στη διεξαγωγή των διεθνών σχέσεων, ιδίως όσον αφορά την επιδίωξη της "δύναμης και του πλούτου" (Choucri, 2012, σ. 3-5).

Οι τεχνολογίες διαδικτύου επιτρέπουν σε ένα κράτος να ελέγχει την πρόσβαση σε δεδομένα και πληροφορίες που αφορούν τους πολίτες του, τις επιχειρήσεις, και τις κρίσιμες υποδομές του. Η σημασία της εδαφικής κυριαρχίας ενός κράτους στον κυβερνοχώρο είναι κρίσιμη σε πολλά επίπεδα. Αν και η έννοια της εδαφικής κυριαρχίας πρωτίστως αφορά την κυριαρχία ενός κράτους στο έδαφός του, στον κυβερνοχώρο αντιμετωπίζουμε μια νέα διάσταση αυτής της έννοιας. Η εδαφική κυριαρχία στον κυβερνοχώρο είναι σημαντική για την ασφάλεια και την άμυνα ενάντια σε κυβερνοεπιθέσεις και παραβιάσεις των ψηφιακών συστημάτων, ενώ διαδραματίζει σημαντικό ρόλο στη δημιουργία ενός κλίματος εμπιστοσύνης και καινοτομίας στο διαδίκτυο, το οποίο είναι κρίσιμο για την ψηφιακή οικονομία (Adams, & Albakajai, 2016). Επιπλέον, η εδαφική κυριαρχία στον κυβερνοχώρο

επηρεάζει τις πολιτικές αποφάσεις και τη διπλωματική στρατηγική ενός κράτους σε διεθνές επίπεδο ενώ δίνει την δυνατότητα σε ένα κράτος να εφαρμόζει πολιτικές ελέγχου και προστασίας της ιδιωτικότητας των πολιτών του στον κυβερνοχώρο. Συνολικά, η εδαφική κυριαρχία στον κυβερνοχώρο αντιπροσωπεύει την ικανότητα ενός κράτους να προστατεύει, να διατηρεί την ασφάλεια και να διαχειρίζεται τις προκλήσεις που προκύπτουν στον ψηφιακό κόσμο (Assaf, κ.α., 2020).

Η Ρωσία, ήδη από το 1998, προσπάθησε να γίνει πρωτοπόρος όσον αφορά τις τεχνολογίες πληροφορικής (Information Technologies), που μόλις αναδύονταν την εποχή εκείνη, καθόσον αναγνώρισε την σημαντικότητα τους αρκετά νωρίς, και να παρουσιάσει τις ανησυχίες της ενώπιον των Ηνωμένων Εθνών. Παρά τα θετικά του διαδικτύου, φοβόταν για ένα ενδεχόμενο ανταγωνισμό μεταξύ των χωρών ‘’arms race’’ για την ανάπτυξη στρατιωτικών συστημάτων στο πλαίσιο του αναδυόμενου κυβερνοχώρου και ήλπιζε για την υπογραφή μιας Συνθήκης που θα απέτρεπε τους ‘’πληροφοριακούς πολέμους’’. Στην πραγματικότητα, ως ο ηττημένος του Ψυχρού Πολέμου ήταν αποφασισμένη να κατοχυρωθεί ξανά σαν υπερδύναμη, ενώ διέβλεπε ότι το διαδίκτυο θα μπορούσε να γεφυρώσει το χάσμα με τις ΗΠΑ που επιβεβαιώθηκε μερικά χρόνια νωρίτερα. Έκτοτε, σαν προέκταση του Ψυχρού Πολέμου, η Δύση και η Ρωσία με την Κίνα αλλά και ορισμένα άλλα αυταρχικά κράτη, προσπαθούν να επιβληθούν για τον καθορισμό είτε νόρμων, συμπεριφορών ή ακόμα και μιας Συνθήκης.

Στην παρούσα εργασία εξετάζεται η έννοια της εδαφικής κυριαρχίας στον κυβερνοχώρο και οι προκλήσεις που αντιμετωπίζονται σε αυτό το πλαίσιο. Η ανάλυση εστιάζεται στην ισορροπία δυνάμεων μεταξύ των Ηνωμένων Πολιτειών, της Ρωσίας και της Κίνας, καθώς αυτές οι χώρες αναδύονται ως κυρίαρχοι παίκτες στον κυβερνοχώρο. Επιπλέον, πραγματοποιείται μελέτη περιπτώσεων, όπου αναλύονται παραδείγματα παραβιάσεων εδαφικής κυριαρχίας στον κυβερνοχώρο από τις προαναφερθείσες χώρες. Η ανάλυση αυτή παρέχει μια ευκαιρία να κατανοήσουμε καλύτερα τις στρατηγικές, τις αντιδράσεις και τις επιπτώσεις αυτών των παραβιάσεων στον διεθνή χώρο. Τέλος, στα συμπεράσματα της εργασίας παρουσιάζονται τα κύρια ευρήματα και δίνεται μια συνολική αξιολόγηση της κατάστασης, καθώς και προτάσεις για τη διαχείριση των προκλήσεων που θα αντιμετωπίσουμε στο μέλλον.

1.1. Σκοπός και Σπουδαιότητα της Έρευνας, Ερευνητικά Ερωτήματα

Οι κυβερνοεπιθέσεις μπορούν να ανατρέψουν την παραδοσιακή έννοια της εθνικής ασφάλειας και να θέσουν σε αμφισβήτηση την κρατική κυριαρχία στον ψηφιακό χώρο. Επιπλέον, οι επιθέσεις στον κυβερνοχώρο μπορούν να επηρεάσουν τη λειτουργία κρίσιμων υποδομών, να παραβιάσουν ευαίσθητες πληροφορίες, να προκαλέσουν οικονομικές απώλειες και να απειλήσουν την ιδιωτικότητα των πολιτών. Η ανάπτυξη νέων τεχνολογιών και η αυξημένη συνδεσιμότητα των συσκευών και των υποδομών δημιουργούν νέες προκλήσεις για την κρατική ασφάλεια και κυριαρχία. Επομένως υπάρχει ανάγκη για την οριοθέτηση του Cyberspace, καθώς η απουσία κανόνων και διεθνών συμφωνιών μπορεί να οδηγήσει σε αυθαίρετες ενέργειες και επιθέσεις που απειλούν την ασφάλεια και την ελευθερία των πολιτών. Σε αντίθεση με τις παραδοσιακές θεωρίες Διεθνών Σχέσεων που εστιάζουν στην έννοια της κρατικής εξουσίας και του διεθνούς συστήματος, η αντιμετώπιση των υβριδικών απειλών στον κυβερνοχώρο απαιτεί νέες προσεγγίσεις. Αυτές περιλαμβάνουν τη συνεργασία μεταξύ των κρατών για την εφαρμογή κοινών κανόνων και προτύπων, τη δημιουργία πολυμερών συμφωνιών για την προστασία του κυβερνοχώρου και την ενίσχυση της διακυβέρνησης στον ψηφιακό χώρο.

Στην παρούσα έρευνα, εξετάζουμε πώς οι παραδοσιακές θεωρίες Διεθνών Σχέσεων, όπως ο ρεαλισμός και ο λειτουργικός ορθολογισμός, αντιμετωπίζουν το φαινόμενο του Cyberspace και πώς αυτές οι θεωρίες προσαρμόζονται για να αντιμετωπίσουν τις νέες προκλήσεις που παρουσιάζει ο ψηφιακός κόσμος. Το ερευνητικό ερώτημα που θα καθοδηγήσει την έρευνα είναι:

Ποια η σχέση μεταξύ Εδαφικής Κυριαρχίας και Κυβερνοχώρου; Παραβιάζεται η Εδαφική Κυριαρχία στον Ψηφιακό Χώρο; Ποιοι είναι οι μηχανισμοί παραβίασης και οι Δυνητικές Επιπτώσεις;

Αυτό το ερευνητικό ερώτημα επιτρέπει μια ευρύτερη εξέταση των επιπτώσεων του Cyberspace στην κρατική ασφάλεια και κυριαρχία και των δυνατοτήτων για προσαρμογή και αντίδραση βασιζόμενες σε παραδοσιακές θεωρίες Διεθνών Σχέσεων.

Ο σκοπός της μελέτης είναι να διερευνήσει την ισορροπία δυνάμεων μεταξύ των Ηνωμένων Πολιτειών, της Ρωσίας και της Κίνας στον Κυβερνοχώρο εστιάζοντας στις παραβιάσεις εδαφικής κυριαρχίας. Συγκεκριμένα, αφού πραγματοποιηθεί ανάλυση της έννοιας της εδαφικής κυριαρχίας στον κυβερνοχώρο και της σημασίας της στις διεθνής σχέσεις θα επιχειρηθεί η κατανόηση των προκλήσεων που σχετίζονται με τη διατήρηση της εδαφικής κυριαρχίας σε έναν ψηφιακό κόσμο και η ανάλυση της ισορροπίας δυνάμεων μεταξύ των κυριοτέρων παικτών, δηλαδή των ΗΠΑ, της Ρωσίας και της Κίνας. Για την ολιστική προσέγγιση του ζητήματος πραγματοποιείται εξέταση περιπτώσεων παραβιάσεων εδαφικής κυριαρχίας από αυτές τις χώρες και αξιολόγηση των επιπτώσεών τους. Τέλος γίνεται προβολή των συμπερασμάτων για τη βέλτιστη διαχείριση των προκλήσεων που προκύπτουν από τις παραβιάσεις εδαφικής κυριαρχίας στον κυβερνοχώρο και τη διασφάλιση ενός σταθερού και ασφαλούς διαδικτυακού περιβάλλοντος. Η μελέτη αποσκοπεί να προσφέρει κατανόηση, ανάλυση και διδάγματα για τη διαχείριση του κυβερνοχώρου στο πεδίο των διεθνών σχέσεων.

Οι παραβιάσεις εδαφικής κυριαρχίας στον κυβερνοχώρο απειλούν την εθνική ασφάλεια ενός κράτους, καθώς μπορούν να οδηγήσουν σε ανεπάρκεια πληροφοριών ή ακόμα και σε κυβερνοεπιθέσεις με στόχο την παραβίαση της εσωτερικής ασφάλειας. Επιπλέον, μπορούν να απειλήσουν την ιδιωτικότητα και την ατομική ασφάλεια των πολιτών, καθώς υπάρχει κίνδυνος διερρεύσης ευαίσθητων πληροφοριών. Επιπλέον, ο κυβερνοχώρος είναι αναπόσπαστο μέρος της σύγχρονης οικονομίας, και οι παραβιάσεις εδαφικής κυριαρχίας μπορούν να προκαλέσουν σοβαρές οικονομικές απώλειες, είτε μέσω της διακοπής λειτουργίας κρίσιμων υποδομών είτε μέσω της κλοπής εμπιστευτικών δεδομένων ενώ μπορούν να προκαλέσουν επίσης πολιτικές αντιδράσεις ανάμεσα σε κράτη, είτε μέσω διπλωματικών κινήσεων είτε μέσω ενδεχόμενων στρατιωτικών κινήσεων. Οι παραβιάσεις εδαφικής κυριαρχίας στον κυβερνοχώρο αναδεικνύουν τη σημασία των διεθνών σχέσεων και την συνεργασία μεταξύ κρατών για την αντιμετώπιση των κοινών κυβερνοπροκλήσεων. Η σπουδαιότητα της έρευνας έγκειται στην κατανόηση των νέων απειλών που εμφανίζονται στον κυβερνοχώρο και πώς αυτές μπορούν να επηρεάσουν την εθνική ασφάλεια και κυριαρχία. Η έρευνα παρέχει την βάση για την ανάπτυξη και εφαρμογή πολιτικών και στρατηγικών για την προστασία των κρατών από κυβερνοεπιθέσεις και τη διατήρηση της κυριαρχίας τους στον ψηφιακό χώρο. Οι εισηγήσεις προσφέρουν στη βελτίωση των μέτρων ασφαλείας στον

κυβερνοχώρο και στην ενίσχυση των ικανοτήτων ανίχνευσης, πρόληψης και αντίδρασης σε επιθέσεις. Επιπλέον, η έρευνα παρουσιάζει και αναλύει νέες προσεγγίσεις και θεωρίες στον τομέα των Διεθνών Σχέσεων για την αντιμετώπιση των προκλήσεων που προκύπτουν στον ψηφιακό κόσμο.

1.2 Μεθοδολογία

Η μεθοδολογία που χρησιμοποιείται είναι η Συγκριτική Μελέτη Περιπτώσεων η οποία αναλύει και συγκρίνει διαφορετικές περιπτώσεις ή παραδείγματα με σκοπό την κατανόηση των διαφορών και των ομοιοτήτων μεταξύ τους. Η μεθοδολογία της συγκριτικής μελέτης περιπτώσεων εστιάζει στη συλλογή και ανάλυση ποικίλων περιπτώσεων που αφορούν στο ίδιο ή σε συναφή θέματα, με στόχο την εξαγωγή γενικεύσεων και την κατανόηση των παραγόντων που επηρεάζουν τα αποτελέσματα. Εφαρμόζεται συνήθως όταν υπάρχει ανάγκη να γίνει σύγκριση διαφορετικών προσεγγίσεων ή καταστάσεων σε διαφορετικά πλαίσια όπως οι χώρες που εξετάζονται καθώς καθεμιά διέπεται από διαφορετικά οικονομικά, κοινωνικοπολιτικά και πολιτισμικά δεδομένα.

Συγκεκριμένα, στην παρούσα μελέτη, αναλύονται περιπτώσεις παραβιάσεων εδαφικής κυριαρχίας στον κυβερνοχώρο από τις Ηνωμένες Πολιτείες, τη Ρωσία και την Κίνα, αναλύοντας τα γεγονότα, τα κίνητρα, τις μεθόδους και τις επιπτώσεις της παραβίασης εδαφικής κυριαρχίας σε κάθε περίπτωση. Μετά την ανάλυση των περιπτώσεων, θα ακολουθήσει σύγκριση μεταξύ τους, στην οποία θα τονίζονται οι ομοιότητες και οι διαφορές στις προσεγγίσεις και τις αντιδράσεις των εν λόγω χωρών. Αυτή η σύγκριση θα επιτρέψει την αναγνώριση προτύπων και τάσεων στον τρόπο με τον οποίο οι χώρες αντιμετωπίζουν τα ζητήματα εδαφικής κυριαρχίας στον κυβερνοχώρο. Τέλος, με βάση τα ευρήματα της σύγκρισης, θα προταθούν πιθανές πολιτικές ή διπλωματικές προσεγγίσεις για τη διαχείριση των προκλήσεων που αντιμετωπίζονται στον τομέα της εδαφικής κυριαρχίας στον κυβερνοχώρο και την ενίσχυση της διεθνούς σταθερότητας και ασφάλειας.

Ειδικότερα, γίνεται σύγκριση των πολιτικών και των τεχνικών προσεγγίσεων των ΗΠΑ, της Ρωσίας και της Κίνας όσον αφορά στις προσπάθειές τους για ηλεκτρονική παρακολούθηση και κυβερνοεπιθέσεις σε άλλες χώρες που στόχο έχουν την παρενόχληση και την υπονόμευση δημοκρατικών διαδικασιών και θεσμών μέσω του διαδικτύου. Επιπλέον γίνεται ανάλυση των διαφόρων προσεγγίσεων των κρατών

για την προστασία των διαδικτυακών πόρων και των κρίσιμων υποδομών τους από κυβερνοεπιθέσεις και παραβιάσεις εδαφικής κυριαρχίας. Αυτές οι περιπτώσεις να παράσχουν μια πλούσια και ενδιαφέρουσα βάση για σύγκριση και ανάλυση των πολιτικών, τεχνικών και νομικών πτυχών που σχετίζονται με το θέμα της εδαφικής κυριαρχίας στον κυβερνοχώρο.

1.3 Κυβερνοχώρος, Εννοιολογικοί Ορισμοί, Τρωτότητα των Κρίσιμων Υποδομών, Ισορροπία Δυνάμεων

Ο ψηφιακός χώρος (cyberspace) έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο διεξάγονται οι διεθνείς σχέσεις καθώς έχει γίνει μια θεμελιώδης διάσταση του πραγματικού κόσμου, επηρεάζοντας τόσο την καθημερινή ζωή όσο και τη δυναμική των διεθνών σχέσεων. Ο ψηφιακός χώρος επιτρέπει τη διάδοση πληροφοριών, προπαγάνδας και επιρροής με ταχύτητα και εύρος που δεν είχε προηγουμένως συναντηθεί. Ειδικότερα, επιτρέπει την άμεση επικοινωνία μεταξύ ανθρώπων, οργανισμών και κρατών σε παγκόσμιο επίπεδο. Αυτό διευκολύνει τη διπλωματική επικοινωνία, τη διαπραγμάτευση και την ανταλλαγή πληροφοριών μεταξύ των χωρών. Το διαδικτυακό εμπόριο και οι ψηφιακές συναλλαγές επίσης έχουν καταλάβει κρίσιμο μέρος των διεθνών οικονομικών συστημάτων. Η παρουσία των ψηφιακών εταιρειών και πλατφορμών έχει σημαντικό αντίκτυπο στις διεθνείς οικονομικές σχέσεις και το εμπόριο. Επιπλέον, ο ψηφιακός χώρος έχει γίνει ένας τομέας στρατηγικής σημασίας για την εθνική ασφάλεια. Η προστασία από κυβερνοεπιθέσεις, η πρόληψη της κυβερνοεγκληματικότητας και η αντίδραση σε κυβερνοεπιθέσεις από άλλα κράτη αποτελούν σημαντικές πτυχές των διεθνών σχέσεων στον ψηφιακό χώρο.

Η επίδραση του ψηφιακού χώρου έχει επιταχύνει την αλληλεξάρτηση και αλληλεπίδραση μεταξύ των κρατών, επηρεάζοντας σημαντικά τη δυναμική των διεθνών σχέσεων καθώς παρέχει νέους τρόπους επικοινωνίας και διαπραγμάτευσης μεταξύ των κρατών. Οι διαπραγματεύσεις για παράδειγμα για διεθνή θέματα και συμφωνίες μπορούν πλέον, να λαμβάνουν χώρα διαδικτυακά, επιτρέποντας γρηγορότερη και πιο αποτελεσματική επικοινωνία.

Η μετάβαση του ψηφιακού χώρου από έναν τομέα χαμηλής πολιτικής σε πεδίο υψηλής πολιτικής αντικατοπτρίζει την εξέλιξη του ρόλου του στη διεθνή σκηνή και την αναγνώριση της σημασίας του από τα κράτη και τους διεθνείς φορείς.

Αρχικά, ο ψηφιακός χώρος θεωρούνταν κυρίως ένας τομέας με χαμηλή πολιτική σημασία, εστιάζοντας κυρίως σε θέματα ψυχαγωγίας, επικοινωνίας και εμπορίου. Ωστόσο, με την αύξηση της χρήσης του και τη διείσδυσή του σε περισσότερους τομείς της κοινωνίας, η πολιτική σημασία του αυξήθηκε δραματικά. Σήμερα, ο ψηφιακός χώρος αναγνωρίζεται ως ένα τμήμα με ιδιαίτερη πολιτική σημασία λόγω της σπουδαιότητας του για την εθνική ασφάλεια, την οικονομία και την κοινωνία. Κράτη και διεθνείς οργανισμοί αντιλαμβάνονται την ανάγκη να αντιμετωπίσουν τις προκλήσεις και τις απειλές που προκύπτουν, σε αυτόν και εξαιτίας αυτού, καθιστώντας τον έναν τομέα όπου η πολιτική δράση είναι αναγκαία. Η ανάγνωση του ψηφιακού χώρου στο πλαίσιο των διεθνών σχέσεων είναι σημαντική για να κατανοήσουμε τον τρόπο με τον οποίο αλληλεπιδρούν τα κράτη μεταξύ τους, εξετάζοντας τις διεθνείς διαπραγματεύσεις, τις συγκρούσεις και τις συμμαχίες, καθώς και τις προκλήσεις και τις ευκαιρίες που προκύπτουν από αυτόν. Επιπλέον, η ανάγνωση του ψηφιακού χώρου μας βοηθά να εξετάσουμε τις αλλαγές στη φύση της διεθνούς πολιτικής και να προβλέψουμε τις εξελίξεις.

Οι μεγάλες αλλαγές στη διεθνή πολιτική σκηνή οφείλονται σε τρεις παράγοντες, τις συγκρούσεις, την οικονομική μεταβολή των κρατών και την ανάπτυξη της τεχνολογίας. Η τεχνολογία της πληροφορικής και των επικοινωνιών (ICT) αλλάζει τη δυναμική των σχέσεων μεταξύ κρατών, αλλάζει την αρχιτεκτονική του διεθνούς συστήματος, ανατρέπει την οικονομία, το εμπόριο και τα ευαίσθητα δεδομένα που συλλέγουν οι υπηρεσίες πληροφοριών, ενώ είναι πηγή νέων προβλημάτων για την εξωτερική πολιτική παράλληλα, αλλάζει και επιταχύνει την αντίληψη των σημαντικών γεγονότων που σχετίζονται με την ασφάλεια. Επιπλέον, ο κυβερνοχώρος διαθέτει εκπληκτικά χαρακτηριστικά, είναι φθηνός, προστατεύει την ανωνυμία, επιτρέπει επιθέσεις από μακρινές αποστάσεις, από παντού και με απίστευτη ταχύτητα και το εύρος του ενισχύεται συνεχώς από την εμφάνιση νέων χρηστών του Διαδικτύου. Η τεχνολογία αποτελεί τον κύριο άξονα για την κατανόηση των διεθνών σχέσεων και της αλλαγής της εξουσίας. Στον παγκοσμιοποιημένο κόσμο και στην εποχή του κυβερνοχώρου, εκείνοι που είναι πιο τεχνολογικά προηγμένοι θα επικρατούν, όπως συνέβη τον 19ο αιώνα όταν η Αγγλία κυριαρχούσε στις θάλασσες και τον 20ο αιώνα όταν οι ΗΠΑ είχαν την αεροπορική κυριαρχία και την καλύτερη προβολή δύναμης.

Για την κατανόηση του ρόλου των πληροφορικών τεχνολογιών στη σύγχρονη κοινωνία και την παγκόσμια διακυβέρνηση αναδείχθηκαν κάποιες κυρίαρχες

θεωρητικές προσεγγίσεις, όπως αυτή των ρεαλιστών, των ντετερμινιστών και αυτή των κοινωνικών κονστρουκτιβιστών (social constructivists). Οι ρεαλιστές υποστηρίζουν την άποψη ότι ο κυβερνοχώρος αποτελεί έναν ακόμα τομέα όπου ισχύουν οι κλασικές αρχές του ρεαλισμού. Σύμφωνα με το ρεαλιστικό προσεγγιστικό πλαίσιο, ο κυβερνοχώρος είναι ένας χώρος όπου τα κράτη δρουν με βάση τον εθνικό τους συμφέρον για την επιβίωση τους. Η δυναμική των διεθνών σχέσεων στον κυβερνοχώρο για τους ρεαλιστές ακολουθεί την ίδια λογική με τη δυναμική σε άλλους τομείς, όπως οι παραδοσιακές στρατηγικές συγκρούσεις και οι οικονομικές διαπραγματεύσεις. Η εξουσία, η επιρροή και ο ανταγωνισμός παίζουν κεντρικό ρόλο στον κυβερνοχώρο, όπως και στους άλλους τομείς των διεθνών σχέσεων. Επιπλέον, κατά τον ρεαλισμό η ανάπτυξη της κυβερνοασφάλειας και η εφαρμογή κυβερνοεπιθέσεων αποτελούν μέρος μιας ευρύτερης στρατηγικής εξουσίας και επιρροής στο διεθνές πεδίο. Οι κυβερνοεπιθέσεις μπορούν να χρησιμοποιηθούν για την επίτευξη γεωπολιτικών και οικονομικών στόχων, καθώς και για την προστασία των εθνικών συμφερόντων. Τέλος, στον ρεαλισμό υπογραμμίζεται η σημασία της στρατηγικής ισορροπίας δυνάμεων στον κυβερνοχώρο, παρόμοια με εκείνη που ισχύει για τα κράτη στο διεθνές πεδίο. Η ισχύς στον κυβερνοχώρο σύμφωνα με τους ρεαλιστές είναι ένα σημαντικό μέσο για την επίτευξη γεωπολιτικών στόχων και για τη διατήρηση της εθνικής ασφάλειας και του ανταγωνισμού (Nye & S, 2004 σ. 21-33), (Craig & Valeriano, 2018).

Η Ντετερμινιστική Προσέγγιση (Deterministic Approach) στον κυβερνοχώρο βασίζεται στην ιδέα ότι ο κυβερνοχώρος είναι μια εξελισσόμενη αλλά προβλέψιμη περιοχή, όπου οι διεθνείς σχέσεις μπορούν να πραγματοποιηθούν μέσω καθορισμένων και αποτελεσματικών μεθόδων. Σύμφωνα με τις Ντετερμινιστικές θεωρήσεις οι ενέργειες και οι αντιδράσεις σε διάφορες κυβερνοεπιθέσεις μπορούν να προβλεφθούν με βάση συγκεκριμένους κανόνες, πρωτόκολλα και διαδικασίες. Σύμφωνα με αυτήν την προσέγγιση, οι κυβερνοεπιθέσεις και οι αντιδράσεις σε αυτές μπορούν να διαχειριστούν μέσω αναλυτικών μοντέλων και αλγορίθμων. Ωστόσο, η προσέγγιση αυτή ενδέχεται να μην λαμβάνει επαρκώς υπόψη της τις πτυχές της αβεβαιότητας και της πολυπλοκότητας που χαρακτηρίζουν τον κυβερνοχώρο (Higle & Sen, 1991), (Sahinidis, 2004). Αυτό επιβεβαιώνει τη σημασία ενός πιο σύγχρονου πλαισίου που λαμβάνει υπόψη τις πολυδιάστατες και δυναμικές πτυχές του κυβερνοχώρου όπως ο ρεαλισμός .

Οι κοινωνικοί κονστρουκτιβιστές (social constructivists) θεωρούν ότι η πραγματικότητα και η αλήθεια δημιουργούνται μέσα από τις κοινωνικές διαδικασίες και τις αλληλεπιδράσεις μεταξύ των ανθρώπων. Στο πλαίσιο των διεθνών σχέσεων, εστιάζουν στον τρόπο με τον οποίο τα κράτη, οι οργανώσεις και άλλοι διεθνείς παράγοντες κατασκευάζουν και ερμηνεύουν τις κοινές αντιλήψεις, τις κοινωνικές αξίες και τους πολιτικούς στόχους. Ουσιαστικά, οι πολιτικές, οι συμπεριφορές και οι αλληλεπιδράσεις στον διεθνή χώρο καθορίζονται από τις κοινωνικές πρακτικές και τις αντιλήψεις των διακρατικών παραγόντων, και όχι από δομές ή δυνάμεις. Βάσει αυτής της θεωρίας, η έννοια της δύναμης, της ασφάλειας και της ταυτότητας του κράτους δεν είναι αντικειμενικά ορισμένες, αλλά κατασκευάζονται και αλλάζουν μέσα από τις κοινωνικές διαδικασίες. Ο ρόλος των ιδεολογιών, των πολιτισμικών παραγόντων και της διπλωματίας στην προσέγγιση αυτή αποκτά σημασία για τη διαμόρφωση των διεθνών σχέσεων (Ciolan, 2014).

Επιπλέον, έχουν εισχωρήσει στο πεδίο των Διεθνών Σχέσεων, νέες έννοιες και θεωρητικές προσεγγίσεις με έμφαση στην ασφάλεια και τις μεταβαλλόμενες μορφές εποπτείας όπως η έννοια της κυβερνητικότητας (governmentality) που έχει λάβει πολλές ερμηνείες και έχει εφαρμοστεί σε διάφορα επίπεδα εξουσίας. Η προσέγγιση του governmentality έχει επεκταθεί στον ψηφιακό χώρο, ως απόρροια της επίδρασης των τεχνολογιών πληροφορικής και επικοινωνιών και αφορά την επιδίωξη και την άσκηση εξουσίας και ελέγχου στον κυβερνοχώρο. Αυτό περιλαμβάνει πρακτικές και πολιτικές που εφαρμόζονται από κυβερνήσεις, οργανισμούς και άλλες εξουσιαστικές οντότητες για τον έλεγχο, την παρακολούθηση και την επιβολή κανόνων στον διαδικτυακό χώρο. Ο εκφραστής της έννοιας του governmentality στον κυβερνοχώρο είναι ο Michel Foucault, ένας Γάλλος φιλόσοφος και κοινωνιολόγος. Ο Foucault ασχολήθηκε εκτενώς με τη φύση της εξουσίας και των μηχανισμών ελέγχου στη σύγχρονη κοινωνία, και η έννοια του governmentality αποτελεί ένα κεντρικό στοιχείο του έργου του. Αλλά αν και η εργασία του Foucault δεν εστίαζε στις σύγχρονες τεχνολογίες, αναγνώριζε τη σημασία τους στην άσκηση της εξουσίας (Radu, 2013).

Η κυβερνητικότητα αντιπροσωπεύει τη δυναμική της διαμόρφωσης των πρακτικών εξουσίας, και συνδέεται με την εκμετάλλευση των τεχνολογιών για την επίτευξη συγκεκριμένων στόχων. Η δυναμική φύση όμως της κυβερνητικότητας, η οποία περιλαμβάνει την "ηλεκτρονική κυβερνητικότητα" ή την τεχνική "διακυβέρνησης από απόσταση" οδήγησε στην ανάπτυξη αντίθετων απόψεων που περιλαμβάνουν αντιλήψεις όπως η μείωση της εξουσίας των κρατών στην εποχή των

ψηφιακών τεχνολογιών. Επιπλέον, η παγκοσμιοποίηση της κυβερνητικότητας, προκάλεσε την αύξηση της επιρροής των διεθνών οργανισμών, όπως η Παγκόσμια Τράπεζα, το Διεθνές Νομισματικό Ταμείο και άλλοι, στη διαμόρφωση των πολιτικών και πρακτικών κυβέρνησης σε επίπεδο κρατών. Μέσω της παγκοσμιοποίησης της κυβερνητικότητας, οι διεθνείς οργανισμοί επηρεάζουν τις πρακτικές κυβέρνησης των κρατών μέσω της παροχής χρηματοοικονομικής στήριξης και της επιβολής οικονομικών περιορισμών. Αυτό μπορεί να οδηγήσει σε μια παγκόσμια εναρμόνιση των πολιτικών και των πρακτικών κυβέρνησης, καθώς και σε μια μείωση της εθνικής κυριαρχίας σε ορισμένους τομείς και σε επιπτώσεις στη διαμόρφωση της πολιτικής και της οικονομικής πραγματικότητας σε παγκόσμιο επίπεδο (Burchell et al., 1991).

1.3.1 Η Ασφάλεια στον Κυβερνοχώρο

Η έννοια της ασφάλειας στον κυβερνοχώρο για την αντιμετώπιση των κινδύνων που προκαλεί ένα πανταχού παρόν εικονικό περιβάλλον, έχει εξελιχθεί σημαντικά με την πάροδο του χρόνου, καθώς οι τεχνολογικές εξελίξεις και η αυξημένη ψηφιοποίηση των διαδικασιών έχουν δημιουργήσει νέους κινδύνους και προκλήσεις στον κυβερνοχώρο. Εστιάζοντας στο πλαίσιο του ΟΗΕ, η αντίληψη της κυβερνοασφάλειας έχει εξελιχθεί για να αντιμετωπίσει αυτούς τους κινδύνους και να προσαρμοστεί στην αλλαγή του τοπίου της ασφάλειας. Αρχικά, η ασφάλεια στον κυβερνοχώρο εστιάστηκε κυρίως στην προστασία των δικτύων και των υπολογιστών από κυβερνοεπιθέσεις και κυβερνοεγκλήματα. Ωστόσο, με την πάροδο του χρόνου, η έννοια της κυβερνοασφάλειας έχει επεκταθεί για να περιλαμβάνει επίσης την προστασία των πληροφοριών, των δεδομένων και των ψηφιακών υποδομών. Η αντίληψη της κυβερνοασφάλειας εξελίχθηκε περαιτέρω για να περιλάβει την προστασία από τις διαδικτυακές απειλές που μπορούν να επηρεάσουν την πολιτική σταθερότητα, την οικονομική ασφάλεια και τη δημόσια υγεία. Αυτό περιλαμβάνει την αντιμετώπιση των κυβερνοεπιθέσεων που μπορούν να προκαλέσουν διαταραχές στη λειτουργία των κρίσιμων υποδομών και υπηρεσιών. Η εξέλιξη αυτή περιλαμβάνει την ανάλυση και την αντιμετώπιση των κινδύνων από διάφορες πηγές. Η ολοκληρωμένη προσέγγιση της κυβερνοασφάλειας επιδιώκει την προαγωγή της σταθερότητας, της ασφάλειας και της ανθεκτικότητας στον κυβερνοχώρο (Bing, 2009).

Οι αποφάσεις για την ασφάλεια στον κυβερνοχώρο στο πλαίσιο του ΟΗΕ καθορίζονται μέσω διαφόρων μηχανισμών και οργάνων που ασχολούνται με το θέμα

της κυβερνοασφάλειας σε συνεργασία μεταξύ των κρατών μελών του ΟΗΕ και άλλων διεθνών οργανισμών μέσω διαπραγματεύσεων και συμφωνιών. Η συμμετοχή στη διακυβέρνηση για την κυβερνοασφάλεια επηρεάζεται από την δυναμική της παγκόσμιας διακυβέρνησης και τις εξελίξεις στον τομέα της τεχνολογίας και των επικοινωνιών. Φορείς όπως τα κράτη, οι διεθνείς οργανισμοί, οι επιχειρήσεις και η κοινωνία των πολιτών μπορούν να έχουν διαφορετικό βαθμό συμμετοχής ανάλογα με τον ρόλο και τα συμφέροντά τους στον τομέα της κυβερνοασφάλειας. Η παγκόσμια διακυβέρνηση στον τομέα της κυβερνοασφάλειας επηρεάζεται επίσης από τις γεωπολιτικές σχέσεις και τις οικονομικές δυνάμεις. Οι αποφάσεις που λαμβάνονται σε αυτό το πλαίσιο μπορεί να έχουν επιπτώσεις στον τρόπο με τον οποίο διαμορφώνονται οι πολιτικές και οι στρατηγικές σε εθνικό και διεθνές επίπεδο για την ασφάλεια στον κυβερνοχώρο.

Ουσιαστικά όμως υπάρχει σαφής έλλειψη μιας ακριβής οριοθέτησης του όρου "κυβερνοασφάλεια" σε ψηφίσματα του ΟΗΕ, παρά το γεγονός ότι ο όρος αυτός έχει χρησιμοποιηθεί σε αρκετά έγγραφα. Παραταύτα, έχει σημειωθεί αξιοσημείωτη εξέλιξη των ψηφισμάτων του ΟΗΕ σχετικά με την κυβερνοασφάλεια και τις πρακτικές αντιμετώπισης των κυβερνοαπειλών. Οι αναφορές σε ασφαλείς πληροφορίες και κρίσιμες πληροφοριακές υποδομές έχουν εισαχθεί στα ψηφίσματα του ΟΗΕ από το 2003, παρουσιάζοντας τη σημασία της προστασίας των υποδομών αυτών για τη διασφάλιση της κυβερνοασφάλειας. Επιπλέον, παρατηρούνται αντιφάσεις στις δράσεις των κυβερνήσεων των κρατών για την αντιμετώπιση της κυβερνοανασφάλειας. Ενώ υπάρχει μια τάση για μεγαλύτερη διεθνή συνεργασία για την προστασία των κρίσιμων υποδομών, παρατηρείται παράλληλα μια αύξηση των εθνικών μέτρων που περιορίζουν τις πιθανότητες παγκόσμιας συνδεσιμότητας μέσω φίλτρων, αποκλεισμού περιεχομένου, παρακολούθησης κ.λπ. Αυτές οι αντιφάσεις αποτυπώνουν την πολυπλοκότητα της κυβερνοασφάλειας ως έννοιας και την πρόκληση για την επίτευξη της σε διεθνές και εθνικό επίπεδο (Barry, 1996).

Ουσιαστικά υπάρχουν δυναμικές σχετικά με την επιθυμία ορισμένων κρατών να διατηρήσουν ή να αποκτήσουν κεντρικό ρόλο στη λήψη αποφάσεων σχετικά με την κυβερνοασφάλεια, ενώ παράλληλα με αυτόν τον τρόπο εξασφαλίζουν την ελευθερία δράσης για την προστασία των εθνικών κρίσιμων πληροφοριακών υποδομών τους. Αυτό αποτυπώνει τη διαμάχη για την εξουσία και την επιρροή μεταξύ οργανισμών και κρατών στη διαμόρφωση των πολιτικών για την κυβερνοασφάλεια. Σε περιπτώσεις διαπραγματεύσεων που οδηγούνται από τα

"Ηνωμένα Έθνη" σχετικά με την ασφάλεια στον κυβερνοχώρο αποκαλύπτονται πρακτικές για τον έλεγχο των σύγχρονων κοινωνιών που γίνονται άμεσα αντιληπτές και βρίσκονται σε συμφωνία με την κεντρική ιδέα του Foucault για την κυβερνητικότητα όπου αναλύονται διάφορες στρατηγικές, πρακτικές και αλληλεπιδράσεις που αποτελούν μορφές ελέγχου επί των πληθυσμών. Η διακυβέρνηση σε παγκόσμιο επίπεδο εφαρμόζει την ίδια λογική για την άσκηση ελέγχου πάνω στα κράτη από διεθνείς οργανισμούς. Ουσιαστικά αναδεικνύεται η πολυπλοκότητα και η διαρκή διαμάχη γύρω από την κυβερνοασφάλεια, καθώς και η σημασία της εξέλιξής της σε έναν ευρύτερο διεθνή διάλογο. Αναδεικνύεται επομένως η ανάγκη για μια από την αρχή κατασκευή των αρχών και των κανόνων της κυβερνοασφάλειας σε διεθνές επίπεδο, καθώς και για μια ευρύτερη συζήτηση που θα περιλαμβάνει εκτός από τους παραδοσιακούς φορείς, προτάσεις και από τις τοπικές κοινότητες και την ακαδημαϊκή κοινότητα (Kremer & Müller, 2013).

Ένα άλλο κύριο χαρακτηριστικό της κυβερνοασφάλειας αποτελεί η δυσκολία να αναδειχθεί ποιος είναι ο υπεύθυνος για κυβερνοεπιθέσεις και να αποδειχθεί προκαλώντας μια διαμάχη σχετικά με το ποιοι είναι οι κύριοι φορείς στη διακυβέρνηση της κυβερνοασφάλειας και πώς αντιλαμβάνονται τις ευθύνες τους. Οι παράγοντες που δυσκολεύουν την ανάδειξη της ευθύνης στον κυβερνοχώρο είναι η ποικιλία των κυβερνο-όπλων, τα οποία εύκολα κρύβονται και μεταφέρονται στο διαδίκτυο ενώ παράλληλα δυσκολεύουν την ανίχνευση των επιτιθεμένων. Επιπλέον, παρατηρείται δυσκολία απόδοσης ευθύνης σε κυβερνοεπιθέσεις λόγω έλλειψης ενσωματωμένων δεδομένων αναγνώρισης ενώ και η απόσταση μεταξύ επιτιθέμενου και θύματος δεν αποτελεί πρόβλημα στον κυβερνοχώρο. Τέλος, η τεχνολογία των κυβερνο-όπλων είναι παρόμοια με αυτή της κυβερνοκατασκοπίας, δυσκολεύοντας τη διάκριση μεταξύ επιθέσεων και κατασκοπείας. Παρά τις δυσκολίες αυτές, η ανάδειξη της ευθύνης για κυβερνο-επιθέσεις είναι δυνατή με τη χρήση στοιχειώδους αποδεικτικού υλικού και την εφαρμογή τεχνικών διαχείρισης δεδομένων (Law & Bijker, 1992).

1.3.2 Ισορροπία Δυνάμεων

Η παραδοσιακή ισορροπία δυνάμεων βασίζεται στην κυριαρχία των κρατών ως των πραγματικών παραγόντων σε ένα διεθνές σύστημα που χαρακτηρίζεται από

αναρχία. Η ισορροπία της δύναμης αποτελεί την προσπάθεια των αδυνάτων να περιορίσουν τους ισχυρούς. Κάθε αδύναμο κράτος αντισταθμίζει την αδυναμία του με τη δημιουργία συμμαχιών ή άλλων μέσων ισορροπίας, προκειμένου να αποφευχθεί η εμφάνιση ηγεμονικών δυνάμεων. Ωστόσο, στη νέα παγκόσμια πραγματικότητα, όπου η εκτίμηση της δύναμης δεν βασίζεται μόνο σε παραδοσιακή στρατιωτική ισχύ και όπου η κυριαρχία των κρατών είναι παρελθόν, είναι απαραίτητο να αναζητηθούν διαφορετικά ερμηνευτικά μοντέλα. Τα κράτη δεν εγκαταλείπουν τη στρατιωτική τους δύναμη, αλλά όλο και περισσότερο βασίζονται στη μαλακή και την έξυπνη τους ισχύ. Ο κυβερνοχώρος, είναι το μοναδικό περιβάλλον που δημιούργησε εξολοκλήρου ο άνθρωπος και είναι προσαρμόσιμο σε αυτόν. Σε αντίθεση με την εποχή του Ψυχρού Πολέμου, όπου οι πόλεμοι εκτελούνταν από πληρεξούσια κράτη, ο κυβερνοχώρος προσφέρει την επιλογή της άμεσης σύγκρουσης.

Το ισοζύγιο εξουσίας στον κυβερνοχώρο διαφέρει από αυτό στον παραδοσιακό κόσμο, καθώς δεν είναι εύκολο να επιτευχθεί λόγω πολλών παραγόντων. Στην εποχή του κυβερνοχώρου, οι προϋποθέσεις της ισορροπίας της δύναμης που λαμβάνουν υπόψη τα κράτη και εξηγούν τη δύναμη ως στρατιωτική ισχύ δεν αντιστοιχούν πλέον στην πραγματικότητα. Υπάρχουν πολλοί βασικοί παράγοντες στον κυβερνοχώρο και η δύναμη έχει διαφορετικά χαρακτηριστικά. Είναι απαραίτητο να εγκαταλειφθεί η ρεαλιστική και νεορεαλιστική παράδοση των Morgenthau και Waltz και να δοθεί έμφαση στη νεοφιλελεύθερη σχολή των Keohane και Nye, που επισημαίνει τις διακρατικές σχέσεις όπου η στρατιωτική ισχύς δεν μπορεί να λειτουργήσει ως παράγοντας σταθεροποίησης του διεθνούς συστήματος καθώς μπορεί να αντιμετωπιστεί από αισθητά αδύνατους αντιπάλους σε σχέση με την στρατιωτική τους ισχύ. Αυτό σημαίνει ότι θα πρέπει να υπάρχει ένα άλλο σχετικό μέγεθος για την μέτρηση της ισχύος κάθε κράτους. Με την έννοια της "αντιληπτής δύναμης" επιχειρείται να αντιμετωπιστεί η δυσκολία κατάταξης των κρατών ανάλογα με την ισχύ τους. Με την συγκεκριμένη έννοια η δύναμη ενός κράτους υπολογίζεται με βάση διάφορους παράγοντες, συμπεριλαμβανομένων των διαστάσεων της χώρας, της στρατιωτικής δομής και της οικονομικής και βιομηχανικής δυναμικής της και αναφέρεται στην αξιολόγηση της δύναμης ενός κράτους με βάση διάφορους παράγοντες που επηρεάζουν την αντίληψη των άλλων κρατών σχετικά με τη δυνατότητά του να ασκήσει επιρροή και να αντιμετωπίσει προκλήσεις. Αυτοί οι παράγοντες αξιολογούνται με βάση το επίπεδο της στρατηγικής (S) και την προθυμία (W) της χώρας να χρησιμοποιήσει τη δύναμή της για να επιτύχει τους στρατηγικούς

της στόχους. Αυτοί οι δύο παράγοντες όμως είναι δύσκολο να ποσοτικοποιηθούν ακριβώς. Η αντιληπτή δύναμη ουσιαστικά, προσπαθεί να αξιολογήσει την ισχύ ενός κράτους όχι μόνο με βάση τα μετρήσιμα στοιχεία, αλλά και με βάση τον τρόπο με τον οποίο αυτή η ισχύς ερμηνεύεται και αντιλαμβάνεται από άλλα κράτη.

Οι λειτουργίες των κρατών γίνονται όλο και περισσότερο "εικονικές", ενώ οι επενδύσεις σε γνώση και καινοτομία αποτελούν την κύρια πηγή εξουσίας. Αυτό σημαίνει μια επανάσταση στις διπλωματικές υποθέσεις, η οποία θα βασίζεται όλο και περισσότερο στη μαλακή ισχύ και σε εργαλεία που είναι όλο και λιγότερο φυσικά. Η παγκοσμιοποίηση προκαλεί πολυπλοκότητα και αυξανόμενη αλληλεξάρτηση, η οποία δεν έχει πάντα θετικά αποτελέσματα. Οι συγκρούσεις εντός των κρατών και οι εξουσιοδοτημένες συγκρούσεις είναι πιο πιθανό να συμβούν, σύμφωνα με ορισμένες υπηρεσίες πληροφοριών. Συνεπώς, η εξέλιξη της τεχνολογίας και η ανάδυση του κυβερνοχώρου επηρεάζουν βαθιά την δυναμική των διεθνών σχέσεων και των συγκρούσεων, ενθαρρύνοντας τη χρήση νέων στρατηγικών και εργαλείων και διαπραγματεύσεις βασισμένες σε δεδομένα. Η Δυτική προσέγγιση για την ισορροπία των δυνάμεων επικεντρώνεται στη χρήση της δύναμης και την επίτευξη συγκεκριμένων στόχων μέσω της άμεσης επίθεσης, ενώ η Ανατολική προσέγγιση, εμπνευσμένη από τον Sun Tzu, εστιάζει στη χρήση της νοημοσύνης και της απάτης για την επίτευξη νίκης χωρίς τη χρήση στρατιωτικής δύναμης. Η Δυτική προσέγγιση θεωρείται κατάλληλη για συγκρούσεις με παραδοσιακά όπλα, ενώ η Ανατολική προσέγγιση θεωρείται καλύτερα προσαρμοσμένη σε συγκρούσεις μη-κινητικού χαρακτήρα, όπως εκείνες που συμβαίνουν στον κυβερνοχώρο. Η Ανατολική προσέγγιση, έχει ως αποτέλεσμα την ενίσχυση της ανθεκτικότητας του συστήματος, εστιάζοντας στην αξιοποίηση της φυσικής τάσης των πραγμάτων και την προετοιμασία για την αλλαγή του παιχνιδιού. Συνολικά, η επίτευξη ισορροπίας εξουσίας στον κυβερνοχώρο είναι αμφίβολη λόγω της πολυπλοκότητας του περιβάλλοντος και της ανατροφοδότησης που προκύπτει από τις επιθέσεις και τις αντιδράσεις τους. Το συμπέρασμα εάν η ισορροπία εξουσίας στην εποχή του κυβερνοχώρου είναι εφικτή είναι "όχι", με την τεχνολογία να αποδεικνύεται για μια ακόμη φορά το κρίσιμο στοιχείο για τη διαμόρφωση της παγκόσμιας εξουσίας.(Gori, 2018).

1.3.2 Κυβερνοπόλεμος και Κυβερνοεπιθέσεις

Ο κυβερνοπόλεμος (cyber war) αναφέρεται στη χρήση δικτυακών δυνατοτήτων ενός κράτους ή μη-κρατικού φορέα για να διαταράξει, υποβαθμίσει, διαμορφώσει ή καταστρέψει πληροφορίες που βρίσκονται σε υπολογιστές ή δίκτυα υπολογιστών ή τους ίδιους τους υπολογιστές ή τα δίκτυα ενός άλλου φορέα. Η επίθεση μπορεί να εκτελεστεί από κράτος ή μη-κρατικό φορέα και μπορεί να στοχεύει σε οργανισμούς, εταιρείες, διεθνείς οργανισμούς ή άλλους φορείς. Παρόλα αυτά όμως δεν υπάρχει ομοφωνία ως προς το τι αποτελεί πράξη πολέμου στον κυβερνοχώρο και υπάρχει εγγενής δυσκολία στον καθορισμό του κυβερνοπολέμου λόγω της σύνθετης φύσης των δικτύων υπολογιστών και των εξελισσόμενων σχεδίων και λειτουργιών των κυβερνοεπιθέσεων. Ο ορισμός της πράξης πολέμου με βάση τον Carl von Clausewitz, ο οποίος ορίζει τον πόλεμο ως μια πράξη βίας με σκοπό την αναγκαστική κάμψη της θέλησης του εχθρού φαίνεται να είναι εφαρμόσιμη στον κυβερνοχώρο και θα μπορούσε να γίνει αποδεκτή από πολλές χώρες, καθώς η έννοια του πολέμου όπως την περιέγραψε ο Clausewitz είναι ευρέως αποδεκτή στη διεθνή κοινότητα (Carr, 2012).

Η έννοια του πολέμου έχει εξελιχθεί και διαφοροποιηθεί με την πάροδο του χρόνου. Ο πόλεμος δεν είναι μια σταθερή έννοια αλλά μια σταθερή παρουσία στη διεθνή πολιτική που διαφέρει σε συχνότητα, διάρκεια, σοβαρότητα, αιτίες, συνέπειες και άλλες διαστάσεις. Ο τύπος και η φύση του πολέμου έχει μεταβληθεί μέσω των αιώνων αλλά και λόγω της επίδρασης που έχει η τεχνολογική πρόοδος και οι αλλαγές στις κοινωνίες και τις πολιτικές οργανώσεις. Πολλές προσπάθειες έχουν γίνει για την εννοιολογική κατανόηση του πολέμου από διάφορους συγγραφείς και αναλυτές, περιλαμβανομένων των Cicero (Atkins, 2023), Grotius (Bull, 2017), Wright (Wright, 1983), Malinowski (Malinowski, 1941), Clausewitz (Von Clausewitz, 2022), και άλλων. Σημαντικό όμως ρόλο διαδραμάτισε ο Clausewitz στην εννοιολογική κατανόηση του πολέμου ο οποίος θεωρεί τον πόλεμο ως συνέχεια της πολιτικής δράσης με άλλα μέσα και επισημαίνει τρεις κύριες μεταβλητές που διαμορφώνουν οποιονδήποτε πόλεμο, την πολιτική φύση του, τον σκοπό του και την νομιμοποίηση της βίας. Η δυναμική φύση του κυβερνοπολέμου όμως διαφέρει σε αρκετά σημεία από την φύση του συμβατικού πολέμου και επακόλουθα η στρατηγική σκέψη απαιτείται να προσαρμοστεί ανάλογα ενώ η συνεχή έρευνα και ανάπτυξη νέων

κυβερνοεπιθέσεων, αυξάνει τις ανησυχίες των κρατών για τη διασφάλιση της ασφάλειας στον κυβερνοχώρο (Kumar & Castells, 1997).

Ο κυβερνοπόλεμος για να θεωρηθεί ως ενέργεια πολέμου σύμφωνα με τις έννοιες του Κλάουζβιτς για τη φύση του πολέμου αρχικά, θα πρέπει να έχει πολιτική φύση, καθώς ο πόλεμος είναι ένα φαινόμενο που συμβαίνει μόνο μεταξύ πολιτικών κοινοτήτων με στρατιωτικό ανταγωνισμό. Συνεπώς, για να θεωρηθεί μια ενέργεια ως πόλεμος, πρέπει να συμβαίνει μεταξύ πολιτικών οντοτήτων και να περιέχει μια μορφή κοινωνικο-πολιτικής οργάνωσης. Ο πόλεμος όμως δεν είναι μόνο πολιτικός, αλλά είναι επίσης και μια οργανωμένη δραστηριότητα, συλλογική και κοινωνική, και όχι ατομική. Συνεπώς, οι κυβερνοεπιθέσεις που πραγματοποιούνται από άτομα ή ομάδες χωρίς καμία στρατιωτική συμμετοχή υπάγονται στους κυβερνοεγκληματίες ή τους κυβερνοκατασκοόπους. Όσον αφορά τον κυβερνοπόλεμο, πρέπει να έχει πολιτικό σκοπό και να εκτελείται σε στρατιωτικό πλαίσιο. Οι κυβερνοεπιθέσεις με ιδιωτικά συμφέροντα, όπως η υπονόμευση και η κλοπή γνώσεων, ανήκουν σε κυβερνοεγκληματικές ενέργειες. Οι κυβερνοεπιθέσεις που στοχεύουν σε πολιτικούς σκοπούς, όπως αυτές στις περιπτώσεις της Εσθονίας της Γεωργίας της Ουκρανίας ή της περίπτωσης του Stuxnet, είναι παραδείγματα αυτού του είδους.

Επιπλέον απαιτείται ως έναν ορισμένο βαθμό στρατιωτική δράση για να θεωρηθεί μια ενέργεια ως πόλεμος. Σύμφωνα με τον Κλάουζβιτς, ο πόλεμος είναι ένα φαινόμενο που συνοδεύεται από βία. Ο Κλάουζβιτς υποστήριξε ότι ο πόλεμος μπορεί να έχει όλους τους βαθμούς έντασης σε ό,τι αφορά τη βία, και ότι δεν υπάρχει λογικό όριο για την εφαρμογή αυτής της βίας. Αυτή η βία δεν είναι τυχαία, αλλά εφαρμόζεται με κανόνες και έθιμα και ο βαθμός της μπορεί να διαφέρει. Οι κυβερνοεπιθέσεις ενδέχεται να μην προκαλούν θάνατο και μπορεί να μην είναι τόσο θανατηφόρες όσο οι συμβατικές επιθέσεις και μπορεί να μην είναι συγκρίσιμες με εκείνες του παραδοσιακού πολέμου, στο μέλλον οι κυβερνοεπιθέσεις θα είναι σε θέση να προκαλέσουν μεγάλη ζημία, όπως κατέδειξαν ήδη μερικά περιστατικά όπως το Stuxnet. Η ικανότητα των κυβερνοεπιθέσεων να προκαλέσουν καταστροφές και βίαιες ενέργειες φαίνεται από τα παραδείγματα των κυβερνοεπιθέσεων που έχουν πραγματοποιηθεί. Συγκεκριμένα οι σύγχρονες κυβερνοεπιθέσεις περιλαμβάνουν επιθέσεις σε κρίσιμες υποδομές, όπως το ρεύμα και τα δίκτυα νερού, καθώς και την χρήση κυβερνοπόλεμου ως κυρίαρχης μεθόδου για την πρόοδο κάποιων φάσεων μιας συγκρούσεως, όπως ήταν η περίπτωση των πολέμων της Γεωργίας και της Ουκρανίας με την Ρωσία.

Μέσω της μελέτης των κλασικών θεωριών του πολέμου μπορούμε να κατανοήσουμε τους γενικούς κανόνες και τους κανονισμούς πίσω από οποιονδήποτε πόλεμο και επίσης να αποκτήσουμε σαφή εικόνα του κυβερνοπόλεμου. Η θεωρία του Clausewitz, συνεχίζει να συμβάλλει στη γνώση μας για τον πόλεμο και είναι πρωτοπόρος όσον αφορά την εννοιολογική ανάλυση του κυβερνοπολεμου (Clausewitz 1989). Με βάση τις αντιλήψεις του Clausewitz, κάθε κυβερνοεπίθεση μπορεί να θεωρηθεί ως ενέργεια πολέμου μόνο αν πληροί αυτά τα χαρακτηριστικά. Σύμφωνα με αυτό, ο ορισμός της κυβερνοπολέμου ακολουθεί αυτά τα χαρακτηριστικά με σκοπό την εννοιολογική αποσαφήνιση. Συνεπώς, ορίζεται ο κυβερνοπόλεμος ως μια σύγκρουση με βάση ένα μοντέλο πολέμου υψηλής τεχνολογίας, ο οποίος περιλαμβάνει ή περιορίζεται στον κυβερνοπολέμο, μεταξύ εξειδικευμένων ομάδων που προκαλούν, βλάβες και καταστροφή με κύριο σκοπό την επίτευξη των στόχων που έχουν ορίσει οι πολιτικές ομάδες. Επιπλέον, επισημαίνεται ότι η κυβερνοπόλεμος μπορεί να χρησιμοποιηθεί παράλληλα με τα συμβατικά μέσα πολέμου ή αποκλειστικά μόνο στον κυβερνοχώρο. Ωστόσο, οι στόχοι του κυβερνοπόλεμου είναι οι ίδιοι με αυτούς του παραδοσιακού πολέμου. Η βία μπορεί να διαφέρει σε βαθμό, και η δυνατότητα πολέμου χωρίς θανατηφόρα αποτελέσματα είναι δυνατή με βάση την θεωρία του Clausewitz (J.-F. Kremer & Muller, 2013).

Παρόλα αυτά διαπιστώνονται ορισμένα τεχνικά προβλήματα στον κυβερνοπόλεμο και στον τρόπο που επηρεάζουν την εφαρμογή των εννοιών του Κλάουζεβιτς για τη φύση του πολέμου. Πρώτον, είναι συχνά δύσκολο να εντοπιστούν οι υπεύθυνοι για μια κυβερνοεπίθεση και αυτό μπορεί να οδηγήσει σε αβεβαιότητα σχετικά με το ποιος φέρει την ευθύνη για αυτήν. Δεύτερον, οι κυβερνοεπιθέσεις συχνά στρέφονται εναντίον ιδιωτικών εταιρειών και όχι τόσο εναντίον κυβερνήσεων, ιδιαίτερα στην περίπτωση κρίσιμης υποδομής που ανήκει και λειτουργεί κυρίως από τον ιδιωτικό τομέα. Ωστόσο, αυτά τα τεχνικά προβλήματα μπορούν να επιλυθούν με την αξιολόγηση του θέματος ως ένα ζήτημα ασφαλείας. Συμπερασματικά, παρά τα προβλήματα αυτά, η πολιτική φύση του πολέμου μπορεί να εφαρμοστεί στον κυβερνοπόλεμο εφόσον υλοποιείται από οργανωμένες ένοπλες ομάδες.

Η κυβερνοεπίθεση μπορεί να στοχεύει πολλούς φορείς, συμπεριλαμβανομένων κυβερνήσεων, επιχειρήσεων ή διεθνών οργανισμών ενώ μπορεί να προκαλέσει σημαντικές αλλαγές στην κοινωνία ή σε μια ομάδα ατόμων μετά από μια μεγάλη κυβερνοεπίθεση. Η προέλευση μιας κυβερνοεπίθεσης είναι δύσκολο να προσδιοριστεί και να αποδειχθεί, κυρίως λόγω της ευκολίας παραποίησης

των δεδομένων. Μη-κρατικοί φορείς, όπως οι "hacktivists" ή άλλες ομάδες, μπορούν να εμπλακούν σε κυβερνοεπιθέσεις που εκπορεύονται από κρατικές οντότητες, κάνοντας την αναγνώριση του υπεύθυνου ακόμα πιο δύσκολη. Συνήθως σε αυτές τις περιπτώσεις και να βρεθούν οι υπεύθυνοι των επιθέσεων δεν είναι δυνατόν να συνδεθούν με τον κύριο φορέα που διέταξε την επίθεση.

Οι κυβερνοεπιθέσεις θεωρούνται ένα νέο μέσο με το οποίο τα κράτη αγωνίζονται για την επιρροή και την εξουσία στη διεθνή σκηνή καθώς μπορούν να μειώσουν τη δύναμη του κράτους και να το θέσουν υπό τον έλεγχο τους μια άλλη οντότητα. Αυτό σημαίνει ότι η εξουσία δεν είναι πλέον κεντρική στο κράτος ή φυσική, αλλά μπορεί να είναι και τεχνολογική. Οι κυβερνοεπιθέσεις επηρεάζουν επίσης την σχετική δύναμη των κρατών στο διεθνές σύστημα. Αρκετές προηγμένες τεχνολογικά χώρες συμπεριλαμβανομένης και της χώρας μας έχουν σχηματίσει δομές για την κυβερνοάμυνα τους. Οι περισσότερες από αυτές έχουν συμπεριλάβει αυτές τις δομές στα υπουργεία άμυνας θεωρώντας τον κυβερνοχώρο ως ουσιαστικό στοιχείο της εθνικής τους ασφάλειας και προβαίνοντας σε συγκεκριμένα βήματα για την προστασία τους. Ειδικότερα, οι ΗΠΑ έχουν δημιουργήσει την Υπηρεσία Κυβερνοασφάλειας των Ηνωμένων Πολιτειών (USCYBERCOM) με σκοπό να διεξαγάγουν επιχειρήσεις σε όλα τα επίπεδα του κυβερνοχώρου, για τη διασφάλιση της πρόσβασης σε δίκτυα πληροφοριών του Υπουργείου Άμυνας, την προετοιμασία για πιθανές επιχειρήσεις, καθώς και για την αποτροπή αντίστοιχων επιθέσεων.

Επιπλέον οι επιθέσεις εξαρτώνται περισσότερο από την ποιότητα της άμυνας παρά από την επίθεση, η πλειονότητα των των επιθέσεων προέρχεται από πολιτικά δίκτυα ή από ουδέτερες και φιλικές χώρες, και υπάρχει κίνδυνος παρερμηνείας λόγω της δυσκολίας στον εντοπισμό των στόχων μιας επίθεσης. Τα κυβερνο-όπλα είναι φθηνά και εύχρηστα, αλλά μπορούν επίσης να εξουδετερωθούν αν οι ευπάθειες εντοπιστούν και επιδιορθωθούν. Επίσης, οι επιπτώσεις των κυβερνο-επιθέσεων μπορεί να είναι άμεσες ή καθυστερημένες, επιδεινώνοντας ή ανατρέποντας τις παραδοσιακές αντιδράσεις. Επιπλέον, οι κυβερνο-επιθέσεις μπορούν να απειλήσουν όχι μόνο την ασφάλεια του στόχου, αλλά καμιά φορά και την ασφάλεια άλλων φορέων με τις ίδιες ευπάθειες.

Theft	Passwords, sensitive data through guessing, theft or compromised computer system
Bugs/back doors	Incorrect coding, difficult to find in prog ram resulting in system failure.
Authentication failure	Sign-in mechanism failure due to interference, server compromised
Protocol failures	Denial of use of application due to faulty protocol
Information leakage	Computer espionage
Exponential attacks	Use of Viruses and Worms that rapidly spread and cause harm to computer systems
Denial of service attacks	Overuse and straining of hardware to shut down or degrade service
Botnets	Espionage, Trojan horses and worms
Active attacks	Intruder who modifies, deletes and sends own data

Πίνακας 1: *Κατηγορίες Κυβερνοεπιθέσεων (Πηγή: J.-F. Kremer & Muller, 2013)*

2. Εδαφική Κυριαρχία στον Κυβερνοχώρο: Έννοια και Προκλήσεις

2.1 Εξέλιξη της έννοιας της εδαφικής κυριαρχίας στον ψηφιακό κόσμο

Η έννοια της εδαφικής κυριαρχίας στον ψηφιακό κόσμο έχει εξελιχθεί με την εμφάνιση του Διαδικτύου και των ψηφιακών τεχνολογιών. Αρχικά, η έννοια της εδαφικής κυριαρχίας συνδέονταν κυρίως με τα σύνορα των κρατών, αλλά με την ανάπτυξη του Διαδικτύου, οι διαδικτυακές δραστηριότητες έκαναν ομιχλώδες το τοπίο σχετικά με αυτά τα φυσικά σύνορα και δημιουργήθηκαν νέες μορφές κυριαρχίας και εξουσίας. Στον ψηφιακό κόσμο, η εδαφική κυριαρχία συνδέεται με την ανάπτυξη του Διαδικτύου και των διαδικτυακών υποδομών, καθώς και με τις ψηφιακές πλατφόρμες και τις ψηφιακές υπηρεσίες που υπάρχουν σε αυτόν τον χώρο. Συνεπώς, η έννοια της εδαφικής κυριαρχίας στον ψηφιακό κόσμο έχει εξελιχθεί για να λάβει υπόψη και τις ψηφιακές δραστηριότητες που διαμορφώνουν τον τρόπο με τον οποίο η εξουσία και η κυριαρχία ασκούνται και αντιλαμβάνονται σε αυτόν τον χώρο.

Η εξέλιξη του Διαδικτύου και η δημιουργία του μοντέλου multi-stakeholder για τη διακυβέρνησή του αποτελούν μια σημαντική διαδικασία που αντικατοπτρίζει την πολυπλοκότητα και την ποικιλομορφία του διαδικτυακού περιβάλλοντος. Αρχικά, το Διαδίκτυο ξεκίνησε ως ένα ερευνητικό εγχείρημα στα πλαίσια της ακαδημαϊκής κοινότητας και της στρατιωτικής έρευνας στις ΗΠΑ. Αρχικά, η διαχείρισή του ήταν αποκλειστικά κρατική, με τον ρόλο της κυβέρνησης των ΗΠΑ να είναι κεντρικός σε αυτήν τη διαδικασία. Καθώς το Διαδίκτυο αναπτυσσόταν και επεκτεινόταν παγκοσμίως, έγινε φανερό ότι η κεντρική διακυβέρνηση από μια κυβέρνηση ή οργανισμό δεν θα μπορούσε να ανταποκριθεί επαρκώς στις ανάγκες και τις προκλήσεις που παρουσίαζε το Διαδίκτυο. Αυτό οδήγησε στην έννοια του μοντέλου multi-stakeholder το οποίο αναγνωρίζει ότι η διακυβέρνηση του Διαδικτύου πρέπει να είναι πολυμερής, δηλαδή να συμμετέχουν πολλαπλά μέρη από διαφορετικούς τομείς της κοινωνίας. Αυτά τα μέρη περιλαμβάνουν κυβερνήσεις, τον ιδιωτικό τομέα, την κοινωνία των πολιτών, την ακαδημαϊκή κοινότητα, και άλλους ενδιαφερόμενους φορείς.

Η έννοια του μοντέλου αποτελεί μια απάντηση στην ανάγκη για πιο ανοιχτή, συμμετοχική και δημοκρατική διακυβέρνηση του Διαδικτύου. Κατά τη διαδικασία αυτή, οι συμμετέχοντες φορείς εργάζονται από κοινού για την ανάπτυξη κοινών αρχών, κανόνων, και προγραμμάτων που θα διαμορφώσουν την εξέλιξη και τη χρήση του Διαδικτύου. Καίτοι το μοντέλο multi-stakeholder έχει εξελιχθεί ως η βέλτιστη πρακτική για τη διακυβέρνηση του Διαδικτύου, εξακολουθούν να υπάρχουν προκλήσεις και διαφωνίες ως προς τον τρόπο λειτουργίας και την κατανομή της εξουσίας ανάμεσα στους διάφορους φορείς. Παρ' όλα αυτά, το μοντέλο συνεχίζει να είναι η κύρια προσέγγιση για τη διακυβέρνηση του Διαδικτύου, με συνεχείς προσπάθειες για τη βελτίωση και την προσαρμογή του στις αλλαγές και τις ανάγκες του σύγχρονου διαδικτυακού περιβάλλοντος.

Οι Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ) επέδειξαν αρχικά ηγετικό ρόλο στη δημιουργία και τη διαχείριση του Διαδικτύου καθώς η αρχική ιδέα και ανάπτυξη του Διαδικτύου προήλθε από τις ΗΠΑ. Αρχικά, το Διαδίκτυο λειτουργούσε υπό την αιγίδα του αμερικανικού στρατού, προτού να μεταφερθεί στο Εθνικό Ίδρυμα Επιστημών των ΗΠΑ. Από την αρχή λοιπόν, οι ΗΠΑ διαμόρφωσαν τις αρχές και τα πρότυπα του Διαδικτύου με βάση τη δική τους οπτική και τα συμφέροντα. Στη συνέχεια, η διαχείριση του Διαδικτύου μεταφέρθηκε σε ιδιωτικές οργανώσεις, όπως η Internet Corporation for Assigned Names and Numbers (ICANN) (Internet corporation for assigned names and numbers (ICANN), n.d.), η οποία ιδρύθηκε το 1998. Η ICANN ανέλαβε την ευθύνη για τη διαχείριση των διευθύνσεων IP και των ονομάτων τομέων και είναι επικεφαλής στη διαδικασία διαχείρισης του Διαδικτύου. Αν και η ICANN είναι μια ανεξάρτητη οργάνωση, οι ΗΠΑ διατήρησαν σημαντική επιρροή σε αυτήν. Για παράδειγμα, η κυβέρνηση των ΗΠΑ εξακολουθεί να έχει δικαίωμα έγκρισης ή απόρριψης των αποφάσεών της και να ασκεί επιρροή στην κατεύθυνση της πολιτικής της. Με αυτόν τον τρόπο, οι ΗΠΑ ασκούσαν και εξακολουθούν να ασκούν σημαντική επιρροή στην ανάπτυξη και τη λειτουργία του Διαδικτύου, ακόμα και αφού μεταφέρθηκε η διαχείρισή του σε ιδιωτικούς φορείς όπως η ICANN. Επιπλέον, πολλές από τις σημαντικές εταιρείες του Διαδικτύου που συμμετέχουν στην ICANN και σε άλλα φόρα έχουν έδρα στις ΗΠΑ, όπως η Google, η Facebook, η Amazon και η Apple. Αυτό σημαίνει ότι οι ΗΠΑ διατηρούν σημαντική επιρροή μέσω αυτών των εταιρειών.

2.2 Ορισμός της εδαφικής κυριαρχίας στον κυβερνοχώρο

Η θεμελιώδης αρχή της κρατικής κυριαρχίας στο δημόσιο διεθνές δίκαιο, θεσπίστηκε μετά τη Συνθήκη της Βεστφαλίας. Αυτή η αρχή κατοχυρώνεται στον Χάρτη των Ηνωμένων Εθνών και αποτελεί τη βάση της διεθνούς έννομης τάξης μετά τον Β' Παγκόσμιο Πόλεμο. Μετά την ανάπτυξη του Κυβερνοχώρου δημιουργήθηκε η ανάγκη για την εξέλιξη του διεθνούς δικαίου να ληφθούν υπόψη οι τεχνολογικές εξελίξεις, ιδιαίτερα η άνοδος των τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) και κατ΄ επέκταση η δημιουργία του κυβερνοχώρου. Αυτές οι τεχνολογίες έχουν αλλάξει ριζικά τον τρόπο αλληλεπίδρασης των κρατών, θολώνοντας τα παραδοσιακά όρια και αμφισβητώντας τα υπάρχοντα νομικά πλαίσια.

Ορισμένοι υποστηρίζουν ότι η κυριαρχία των κρατών θα πρέπει να εφαρμοστεί και στον ψηφιακό χώρο. Παρά το γεγονός ότι η κυριαρχία είναι ένα βασικό στοιχείο του διεθνούς συστήματος, η εφαρμογή της στον ψηφιακό χώρο μέχρι σήμερα είναι ανεφάρμοστη και απειλεί τις υπάρχουσες διακρατικές θεσμικές δομές στον ιδιωτικό τομέα. Επιπλέον, προβάλλει η άποψη ότι μια κυρίαρχη ψηφιακή κυβέρνηση είναι αντίθετη προς την ελεύθερη πληροφόρηση και επικοινωνία. Αντ' αυτού, προτείνεται η έννοια του ψηφιακού χώρου ως ένα παγκόσμιο αγαθό. Παρόλο που ορισμένοι αμφισβητούν αυτήν την προσέγγιση, οι πιθανές συνέπειές της και πώς μπορεί να επηρεάσει τη διακυβέρνηση του ψηφιακού χώρου απαιτεί περαιτέρω έρευνα και ανάπτυξη των εννοιών του ψηφιακού χώρου, της κυριαρχίας και του κοινού κεκτημένου, καθώς και των επιπτώσεών τους στις διεθνείς σχέσεις και τη διακυβέρνηση του Διαδικτύου. Η δυτική βεστφαλική κυριαρχία βασίζεται στην αρχή ότι τα κράτη είναι ταυτόσημα με συγκεκριμένα φυσικά εδάφη και φυσικά σύνορα, εντός των οποίων οι εγχώριες πολιτικές αρχές είναι η μοναδική νόμιμη πηγή θεσμικής οργάνωσης και πολιτικής. Συνεπώς, η κυρίαρχη άποψη για την εδαφική κυριαρχία είναι η απαγόρευση των εξωτερικών παρεμβάσεων στις εσωτερικές υποθέσεις άλλων κρατών.

Μετά από την μακροχρόνια συζήτηση σχετικά με το εάν ισχύουν οι υφιστάμενοι κανόνες και αρχές του διεθνούς δικαίου στον κυβερνοχώρο ή εάν απαιτούνται νέοι κανόνες, η ακαδημαϊκή κοινότητα, οδηγήθηκε στην συναίνεση ότι οι αρχές του διεθνούς δικαίου, συμπεριλαμβανομένης της κυριαρχίας, ισχύουν και στον κυβερνοχώρο. Αυτή η συναίνεση ενισχύεται από δηλώσεις νομικών

εμπειρογνωμόνων όπως ο Harold Koh και το έργο διεθνών φορέων όπως η Ομάδα Κυβερνητικών Εμπειρογνωμόνων των Ηνωμένων Εθνών (Kapustin, 2023). Τα κράτη που διεξάγουν δραστηριότητες στον κυβερνοχώρο πρέπει να σέβονται την κυριαρχία άλλων κρατών. Αυτό σημαίνει ότι οι ενέργειες στον κυβερνοχώρο δεν πρέπει να παραβιάζουν την εδαφική ακεραιότητα ή την πολιτική ανεξαρτησία άλλων κρατών. Παρόλα αυτά διαπιστώθηκε η ανάγκη προσαρμογής των διεθνών νομικών πλαισίων για την αντιμετώπιση των προκλήσεων που θέτει ο κυβερνοχώρος, επιβεβαιώνοντας παράλληλα τις διαρκείς αρχές της κρατικής κυριαρχίας και της κυριαρχικής ισότητας (Van Den Berg, 2020, σ.77).

Τα περίπλοκα νομικά ζητήματα όμως, που αφορούν την έννοια της εδαφικής κυριαρχίας στον κυβερνοχώρο δημιουργούν ερωτήματα σχετικά με το εάν ορισμένες κυβερνοεπιθέσεις, οι οποίες δεν φθάνουν στο επίπεδο της χρήσης βίας ή της επέμβασης σε εσωτερικές υποθέσεις, αλλά απαγορεύονται από το διεθνές δίκαιο λόγω υποχρέωσης σεβασμού του κυρίαρχου κράτους. Αυτό το ζήτημα είναι ιδιαίτερα αμφιλεγόμενο επειδή η απουσία συγκεκριμένων απαγορευτικών κανόνων μπορεί να αφήσει τα κράτη με ελευθερία να διεξάγουν τέτοιες κυβερνοεπιχειρήσεις. Το Εγχειρίδιο του Ταλίν, το οποίο είναι μια ακαδημαϊκή προσπάθεια για την οριοθέτηση των κανόνων που ισχύουν για τη συμπεριφορά του κράτους στον κυβερνοχώρο. Ο κανόνας 4 του Εγχειριδίου του Ταλίν ορίζει ότι ένα κράτος δεν πρέπει να διεξάγει κυβερνοεπιχειρήσεις που παραβιάζουν την κυριαρχία άλλου κράτους. Το Εγχειρίδιο χρησιμοποιεί μια προσέγγιση που βασίζεται σε αποτελέσματα για να προσδιορίσει πότε συμβαίνουν τέτοιες παραβιάσεις, εστιάζοντας στην παραβίαση της εδαφικής ακεραιότητας ενός κράτους και στην παρέμβαση σε εγγενώς κυβερνητικές λειτουργίες. Η προσέγγιση που βασίζεται στα αποτελέσματα του Εγχειριδίου του Ταλίν στις παραβιάσεις της εδαφικής κυριαρχίας έρχεται σε αντίθεση με την παραδοσιακή κατανόηση της κυριαρχίας που υποστηρίζεται από διεθνή δικαστήρια, όπως το Μόνιμο Δικαστήριο Διεθνούς Δικαιοσύνης (PCIJ) και το Διεθνές Δικαστήριο Δικαιοσύνης (ICJ). Σύμφωνα με αυτή την προσέγγιση, οποιαδήποτε μη εξουσιοδοτημένη παρουσία ή πράξη ξένης κρατικής εξουσίας παραβιάζει την κυριαρχία, ανεξάρτητα από το αν υπάρχει σωματική βλάβη.

Μια εναλλακτική προσέγγιση που βασίζεται σε εισβολές για τις παραβιάσεις της εδαφικής κυριαρχίας στον κυβερνοχώρο συνδέει την παραβίαση της κυριαρχίας με παραβιάσεις της ασφάλειας των πληροφοριών, ιδιαίτερα της ακεραιότητας των στοχευμένων συστημάτων ΤΠΕ. Εστιάζοντας στις τεχνικές πτυχές των εισβολών

στον κυβερνοχώρο, αυτή η προσέγγιση στοχεύει να παρέχει έναν ακριβέστερο προσδιορισμό των επιτρεπτών και των μη επιτρεπτών πράξεων στον κυβερνοχώρο, μειώνοντας έτσι τις νομικές αβεβαιότητες. Η έννοια της εδαφικής κυριαρχίας στον κυβερνοχώρο περιβάλλεται από διαφορετικές απόψεις σχετικά με την ύπαρξή της ως ξεχωριστό κανόνα στο διεθνές δίκαιο. Ο Κανόνας 4 του Εγχειριδίου 2.0 του Ταλίν, βεβαιώνει ότι τα κράτη δεν πρέπει να διεξάγουν επιχειρήσεις στον κυβερνοχώρο που παραβιάζουν την κυριαρχία άλλων κρατών. Αυτός ο κανόνας βασίζεται στην υπόθεση ότι υπάρχει ξεχωριστός κανόνας στη διεθνή έννομη τάξη που απαιτεί σεβασμό της εδαφικής κυριαρχίας άλλων κρατών (J. Wright, 2018).

Πρόσφατες δηλώσεις αξιωματούχων από το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες αμφισβητούν την ύπαρξη ενός συγκεκριμένου κανόνα εδαφικής κυριαρχίας στον κυβερνοχώρο. Ο γενικός εισαγγελέας του Ηνωμένου Βασιλείου εξέφρασε αμφιβολίες σχετικά με την προέκταση ενός συγκεκριμένου κανόνα εδαφικής κυριαρχίας πέρα από τη γενική αρχή της κυριαρχίας. Ομοίως, ο πρώην νομικός σύμβουλος του Υπουργείου Εξωτερικών των ΗΠΑ πρότεινε ότι οι επιχειρήσεις στον κυβερνοχώρο που διεξάγονται σε έδαφος άλλου κράτους ενδέχεται να μην παραβιάζουν απαραίτητα το διεθνές δίκαιο, ειδικά εάν έχουν ελάχιστα ή καθόλου αποτελέσματα. Ένα υπόμνημα που εκδόθηκε από τον απερχόμενο γενικό σύμβουλο του Υπουργείου Άμυνας των ΗΠΑ τον Ιανουάριο του 2017, φέρεται να ανέφερε ότι η κυριαρχία δεν είναι κανόνας αλλά «βασική αρχή» που διέπει άλλους δεσμευτικούς κανόνες του διεθνούς δικαίου. Αυτή η θέση υποστηρίζεται από ορισμένους Αμερικανούς συγγραφείς, συμπεριλαμβανομένων εκείνων που σχετίζονται με την αμερικανική κυβερνητική διοίκηση (Corn & Taylor, 2017).

Έχουν αναπτυχθεί δύο επιχειρήματα κατά της ύπαρξης κανόνα εδαφικής κυριαρχίας στον κυβερνοχώρο. Το ένα επιχείρημα υποστηρίζει ότι δεν υπάρχει επαρκής κρατική πρακτική και νομική υποχρέωση για τη θέσπιση κανόνα εδαφικής κυριαρχίας στο εθιμικό διεθνές δίκαιο. Η έλλειψη συγκεκριμένου κανόνα που να απαγορεύει ορισμένες δραστηριότητες στον κυβερνοχώρο στην επικράτεια άλλου κράτους υποδηλώνει ότι τα κράτη είναι ελεύθερα να ενεργούν εντός του κυβερνοχώρου χωρίς τέτοιους περιορισμούς. Επιπλέον, επισημαίνει ότι οι επιχειρήσεις κατασκοπείας διεξάγονται εντός της επικράτειας άλλων κρατών χωρίς απαγόρευση βάσει του διεθνούς δικαίου (C. (retired) G. Corn & Jensen, 2018). Το άλλο επιχείρημα υποστηρίζει ότι η φύση του κυβερνοχώρου, που χαρακτηρίζεται από την εδαφικότητα και την παγκόσμια εμβέλειά του, περιπλέκει την εφαρμογή των

αρχών εδαφικής κυριαρχίας. Υποδηλώνει ότι οι παραδοσιακές εδαφικές έννοιες δεν μεταφέρονται εύκολα στον κυβερνοχώρο, όπου οι επιχειρήσεις μπορούν να προέρχονται από διάφορες διάσπαρτες τοποθεσίες σε όλο τον κόσμο. Η επιβολή περιορισμών που βασίζονται στην κυριαρχία θα μπορούσε να εμποδίσει την ικανότητα των κρατών να αντιμετωπίσουν αποτελεσματικά τις απειλές στον κυβερνοχώρο, καθώς πρέπει να υπερασπιστούν την υποδομή τους στον κυβερνοχώρο ανεξάρτητα από τη γεωγραφική θέση του εισβολέα (Corn & Taylor, 2017). Πέρα όμως από αυτά τα δύο επιχειρήματα, υπάρχει και η άποψη ότι ουσιαστικά παρερμηνεύουν το δόγμα του Lotus[1], το οποίο δεν παρέχει στα κράτη απεριόριστη ελευθερία δράσης, αλλά μάλλον αναγνωρίζει την απουσία ενός συγκεκριμένου απαγορευτικού κανόνα του διεθνούς δικαίου (Hertogen, 2014).

Η κρατική κυριαρχία περιλαμβάνει τόσο εσωτερικές όσο και εξωτερικές πτυχές. Η εσωτερική κυριαρχία αναφέρεται στην εξουσία ενός κράτους να κυβερνά εντός της επικράτειάς του, ενώ η εξωτερική κυριαρχία αφορά τα δικαιώματα και τις υποχρεώσεις ενός κράτους στις αλληλεπιδράσεις του με άλλα κράτη. Το διεθνές δίκαιο επιβάλλει έναν θεμελιώδη περιορισμό στην κρατική εξουσία, απαγορεύοντας σε ένα κράτος να ασκεί την εξουσία του στην επικράτεια άλλου κράτους χωρίς άδεια, εκτός εάν επιτρέπεται από διεθνή έθιμα ή σύμβαση. Η εδαφική κυριαρχία δεν είναι απλώς μια αρχή, αλλά λειτουργεί και ως απαγορευτικός κανόνας του διεθνούς δικαίου, που απαιτεί σεβασμό της ανώτατης αρχής ενός κράτους στην επικράτειά του. Η εδαφική κυριαρχία ως «βασικός κανόνας» που προέρχεται από το γενικό διεθνές δίκαιο, είναι απαραίτητος για τη διατήρηση της συνύπαρξης ανεξάρτητων κρατών και την επίτευξη κοινών στόχων. Οι νομικές αρχές και η νομολογία υποστηρίζουν την ύπαρξη κανόνα εδαφικής κυριαρχίας στο διεθνές δίκαιο, επιβεβαιώνοντας τη

[1] Η υπόθεση "S.S. Lotus (Γαλλία εναντίον Τουρκίας)" αφορούσε ένα περιστατικό ναυτικής σύγκρουσης που συνέβη το 1926 στο Αιγαίο Πέλαγος μεταξύ ενός γαλλικού πλοίου με την ονομασία "S.S. Lotus" και ενός τουρκικού πλοίου με την ονομασία "Boz-Kourt". Κατά τη σύγκρουση, ένας Τούρκος υπήκοος έχασε τη ζωή του και η γαλλική κυβέρνηση προέβη σε δικαστικές ενέργειες κατά του κυβερνήτη και του πλοιοκτήτη του τουρκικού πλοίου. Η Γαλλία υποστήριζε ότι η δίωξη κατά του κυβερνήτη και του πλοιοκτήτη του τουρκικού πλοίου ήταν νόμιμη σύμφωνα με το δίκαιο της θαλάσσας και τους κανόνες που διέπουν την εφαρμογή της δικαιοδοσίας από τα κράτη σε περιπτώσεις ναυτικών ατυχημάτων. Αντίθετα, η Τουρκία υποστήριζε ότι η Γαλλία δεν είχε δικαίωμα να διώκει τους Τούρκους υπηκόους για ένα ατύχημα που συνέβη στην ελεύθερη θάλασσα, επειδή δεν υπήρχε κανένας διεθνής κανόνας που να απαιτεί την άσκηση νομικών διώξεων σε τέτοιες περιπτώσεις. Το Δικαστήριο αποφάνθη ότι η Γαλλία είχε δικαίωμα να εφαρμόσει το δίκαιο της και να διώξει τους Τούρκους υπηκόους, αφού το ατύχημα συνέβη κατά τη διάρκεια ενός ταξιδιού που είχε αρχικά το πλοίο αποπλεύσε από τον λιμένα της Σμύρνης στην Τουρκία, ο οποίος υπαγόταν στην εφαρμογή του νόμου της Γαλλίας. Ως εκ τούτου, η δίωξη των Τούρκων υπηκόων ήταν νόμιμη σύμφωνα με το δίκαιο της θάλασσας και τη διεθνή ναυτική νομοθεσία.

σημασία του στη διακυβέρνηση της κρατικής συμπεριφοράς, συμπεριλαμβανομένου του πεδίου του κυβερνοχώρου.

Από την άλλη πλευρά, το επιχείρημα κατά της αντίληψης ότι ένας κανόνας εδαφικής κυριαρχίας δεν εφαρμόζεται στον κυβερνοχώρο, επί του παρόντος επειδή υπάρχει έλλειψη ομοιομορφίας στην κρατική πρακτική σχετικά με την εφαρμογή της εδαφικής κυριαρχίας στον κυβερνοχώρο. Οι θέσεις του Ηνωμένου Βασιλείου και ορισμένων Αμερικανών συγγραφέων, αμφιβάλλουν για την ύπαρξη ενός τέτοιου κανόνα, ενώ απόψεις άλλων χωρών όπως η Γερμανία και η Γαλλία, που υποστηρίζουν την εφαρμογή του. Διαφορετικές χώρες ερμηνεύουν και εφαρμόζουν διαφορετικά τις αρχές της κυριαρχίας στον κυβερνοχώρο. Για παράδειγμα, ενώ το Ηνωμένο Βασίλειο υποστηρίζει την ύπαρξη κανόνα εδαφικής κυριαρχίας, η Γερμανία και η Γαλλία ισχυρίζονται ότι η κυριαρχία και οι διεθνείς κανόνες ισχύουν για τη συμπεριφορά του κράτους στον κυβερνοχώρο. Τα κράτη διεκδικούν τακτικά δικαιοδοσία για δραστηριότητες εντός της υποδομής τους στον κυβερνοχώρο, αντιμετωπίζοντας τες σαν να εμπίπτουν στα εδαφικά όρια της κυριαρχίας τους. Για παράδειγμα, νομικές ενέργειες, όπως κατηγορίες που κατατέθηκαν από τον Ειδικό Εισαγγελέα των ΗΠΑ κατά ξένων παραγόντων, αποδεικνύουν την πρακτική εφαρμογή των αρχών της εδαφικής κυριαρχίας.

Οι προκλήσεις που τίθενται από τα μοναδικά χαρακτηριστικά του κυβερνοχώρου, όπως η εδαφική φύση του και η ευκολία πρόσβασης από κακόβουλους παράγοντες υποδηλώνει ότι το διεθνές νομικό καθεστώς χρειάζεται να προσαρμοστεί σε αυτές τις προκλήσεις, ενώ εξακολουθεί να αναγνωρίζει τον βασικό κανόνα της εδαφικής κυριαρχίας. Αν και αναγνωρίζεται η ανάγκη προσαρμογών, υπάρχουν διαθέσιμα νομικά μέσα όπως τα αντίμετρα και το δόγμα της ανάγκης για την αντιμετώπιση απειλών στον κυβερνοχώρο εντός του υπάρχοντος νομικού πλαισίου. Τέλος, οποιοδήποτε επιχείρημα κατά της ύπαρξης εδαφικής κυριαρχίας στον κυβερνοχώρο θα πρέπει να αποδείξει την καθολική κρατική πρακτική και την άποψη της δικαιοσύνης που υποστηρίζει μια τέτοια εξαίρεση, και όχι το αντίστροφο. Ουσιαστικά η πολυπλοκότητα του ζητήματος και η συνεχιζόμενη συζήτηση γύρω από την εφαρμογή των αρχών εδαφικής κυριαρχίας στον κυβερνοχώρο, τονίζει τη σημασία της εξέτασης διαφορετικών εθνικών προοπτικών και ένδικων μέσων εντός του υπάρχοντος νομικού πλαισίου (Schmitt & Vihul, 2016, σσ.111 - 141).

2.3.1 Προκλήσεις και παράγοντες που επηρεάζουν την εδαφική κυριαρχία στον κυβερνοχώρο

Η ψηφιακή επίθεση κατά μιας χώρας από κράτος ή ομάδα κρατών αποτελεί παραβίαση της δυτικής βεστφαλικής κυριαρχίας. Αυτές οι επιθέσεις μπορούν να είναι είτε στρατιωτικές ενέργειες σε κατάσταση πολέμου είτε μορφές κυβερνοπόλεμου ή κυβερνοκατασκοπείας. Η συνεργασία μεταξύ των κρατών για την καταπολέμηση του κυβερνοεγκλήματος μπορεί να περιλαμβάνει παραβίαση της εδαφικής κυριαρχίας, αλλά αυτή η εξαίρεση επιτρέπεται και προωθείται επειδή θεωρείται επωφελής για τα κράτη που συμμετέχουν. Οι παραβιάσεις της κυριαρχίας μπορεί να είναι θετικές για όλα τα εμπλεκόμενα μέρη, αλλά παράλληλα παρουσιάζονται ανισότητες και ανεπάρκειες των διεθνών συμφωνιών και συνεργασιών στον ψηφιακό χώρο. Υφίσταται το ενδεχόμενο οι παραβιάσεις της κυριαρχίας να κανονικοποιηθούν στο μέλλον, καθώς η ανάπτυξη συστημάτων "ενεργής άμυνας" στον ψηφιακό χώρο ουσιαστικά εξασφαλίζουν ότι αυτές οι παραβιάσεις θα γίνονται αυτόματα και θα θεσμοθετούνται ως πολιτική ασφαλείας και άμυνας. Αυτά τα συστήματα έχουν την εξουσία να ανταποκρίνονται σε επιθέσεις και παραβιάσεις των φιλικών δικτύων με αντίστοιχες ενέργειες ανταπόδοσης στη μορφή πακέτων δεδομένων εναντίον περιουσιακών στοιχείων που συχνά βρίσκονται έξω από τα σύνορα της χώρας που εκτελούνται οι επιθέσεις.

Καθώς όλο και περισσότερες κυβερνητικές υπηρεσίες χρησιμοποιούν αυτά τα συστήματα ενεργής άμυνας, το επίπεδο παραβιάσεων της κυριαρχίας αυξάνεται παγκοσμίως, και τείνει να γίνει η κατάσταση αυτή ο κανόνας. Ωστόσο, οι παραβιάσεις της κυριαρχίας μπορεί να είναι είτε η κανονική κατάσταση είτε η εξαίρεση, ανάλογα με την οπτική γωνία και τις πολιτικές ανάγκες της εποχής. Επομένως, οι κανόνες ανταπόδοσης των επιθέσεων στον ψηφιακό χώρο προωθούνται από τις χώρες όχι μόνο ως μέσο αποτροπής, αλλά και για να δείξουν τι είναι αποδεκτό και τι όχι μεταξύ των κρατών που συμφωνούν να τους ακολουθήσουν.

Η έννοια της εγχώριας κυριαρχίας αφορά τους τρόπους με τους οποίους διεξάγονται οι εσωτερικές υποθέσεις των κρατών, συγκεκριμένα πώς είναι οργανωμένη η αρχή εντός του κράτους και πόσο αποτελεσματικός είναι ο βαθμός ελέγχου που ασκούν αυτές οι πολιτικές δομές. Οι προσπάθειες των κρατών να ρυθμίσουν τη χρήση του ψηφιακού χώρου εντός των συνόρων τους και από τους

πολίτες τους, γίνεται με τη θέσπιση πολλαπλών νομοθετικών πράξεων και την ίδρυση νέων δομών που σχεδιάστηκαν για να διαχειριστούν τον ψηφιακό χώρο και τις σχετικές τους κανονιστικές διατάξεις. Ο τρόπος με τον οποίο ο ψηφιακός χώρος έχει επηρεάσει τόσο την αρχή όσο και τον έλεγχο εντός των κρατών, και πώς οι πολιτικές απαντήσεις στον ψηφιακό χώρο διαφέρουν ανάλογα με τις πολιτικές μορφές των κρατών φαίνεται στα παραδείγματα όπως το Ηνωμένο Βασίλειο, όπου η Στρατηγική Κυβερνοασφάλειας του 2009 ίδρυσε το Γραφείο Κυβερνοασφάλειας (OCSIA) για να παρέχει "στρατηγική ηγεσία σε θέματα κυβερνο-ασφάλειας". Από την δημιουργία αυτή προέκυψε η συνεργασία μεταξύ δημόσιων και ιδιωτικών φορέων για την επίτευξη πολιτικών στόχων και την στήριξη της OCSIA ως κύριο εργαλείο για την ανάπτυξη και επέκταση της εξουσίας στον έλεγχο του κυβερνοχώρου, τις επιχειρήσεις και τη ρύθμιση των δραστηριοτήτων στον ψηφιακό χώρο που επηρεάζουν τα συμφέροντα του Ηνωμένου Βασιλείου στην εσωτερική και εξωτερική επικράτεια. Γενικότερα παρατηρείται η τάση ορισμένων κρατών να ελέγχουν την πρόσβαση των πολιτών τους σε πληροφορίες στο διαδίκτυο, με τη δικαιολογία ότι ορισμένοι τύποι "περιεχομένου" και δραστηριοτήτων αποτελούν απειλές για την εσωτερική τάξη και την αρχή, καθώς και για τις καθιερωμένες οικονομικές πρακτικές.

Οι κυβερνήσεις, τόσο στο δυτικό όσο και στο ανατολικό κόσμο, χρησιμοποιούν διάφορες μορφές ελέγχου στον ψηφιακό χώρο προκειμένου να αντιμετωπίσουν απειλές εναντίον της εγχώριας κυριαρχίας. Ειδικότερα, στοχεύουν στο να αποτρέψουν την πρόσβαση των χρηστών σε συγκεκριμένους ιστότοπους ή πηγές πληροφοριών μέσω της ρύθμισης της κυκλοφορίας διαδικτύου σε διάφορα επίπεδα. Άλλη μορφή ελέγχου αποτελεί ο συνδυασμός νομικών, και τεχνικών μέτρων που επιτρέπουν στα κράτη να αποκλείουν την πρόσβαση σε πληροφορίες με βάση την εκάστοτε ανάγκη τους. Τέλος μια τρίτη μορφή ελέγχου δεν στοχεύει στον φυσικό έλεγχο του χώρου, αλλά στην επίτευξη γνωστικών αλλαγών μέσω ενημερωτικών και προπαγανδιστικών καμπανιών, στηριζόμενες σε παρακολούθηση και εξόρυξη δεδομένων που επιτρέπουν στα κράτη να ανταγωνίζονται τους πολίτες τους στον ψηφιακό χώρο. Οι προσπάθειες αυτές, ελέγχου των δραστηριοτήτων των πολιτών μέσω του ψηφιακού χώρου έχουν αντιμετωπίσει αντίσταση από τους πολίτες ενώ συχνά προκαλούν και την αντίδραση τους. Οι έλεγχοι αυτοί διαφέρουν ανάλογα με την πολιτική μορφή του κάθε κράτους, αλλά πολλά δημοκρατικά κράτη έχουν

εφαρμόσει παρόμοια μέτρα υπό το πρίσμα της αντιμετώπισης της τρομοκρατίας (Goldsmith & Eggers, 2005).

Μια άλλη μορφή κυριαρχίας είναι αυτή της κυριαρχίας της αλληλεξάρτησης (interdependence sovereignty). Η κυριαρχία της αλληλεξάρτησης περιλαμβάνει τον έλεγχο των ροών "αγαθών, ατόμων, ρύπων, ασθενειών και ιδεών πέρα από τα εδαφικά σύνορα" και είναι η πιο συχνά αναφερόμενη μορφή κυριαρχίας. Το παγκόσμιο διαδίκτυο έχει ευημερήσει ακριβώς λόγω της μη περιορισμένης ροής πληροφοριών πέρα από εθνικά σύνορα, μια κατάσταση που αντιβαίνει στην κατάσταση της διατήρησης των εδαφικών δικαιωμάτων στον κυβερνοχώρο. Αυτό συνοψίζεται από το διάσημο αξίωμα του Διαδικτύου ότι "τα εθνικοί σύνορα δεν είναι εμπόδια στον δρόμο του πληροφοριών". Η λογική κατάληξη μιας κατάστασης όπου οι εθνικές ανησυχίες για την ασφάλεια υπερισχύουν είναι ένα σε βάθος ρυθμιζόμενο διαδικτυακό περιβάλλον, όπου οι εθνικοί κυβερνοχώροι αντιστοιχούν στα εθνικά φυσικά σύνορα και αντανακλούν εθνικά πρότυπα. Επιπλέον,πολλές προσπάθειες για τον έλεγχο του Διαδικτύου προκειμένου να ανακτηθεί η αλληλεξάρτηση της κυριαρχίας έχουν ένα παράδοξο αποτέλεσμα, καθώς οι κυβερνήσεις θέλουν να προάγουν το Διαδίκτυο ως πηγή οικονομικής ανάπτυξης και εκδημοκρατισμού, αλλά ταυτόχρονα επιχειρούν να ελέγξουν τις ίδιες τις ροές πληροφοριών για πολιτικούς σκοπούς, εκφρασμένες σε έννοιες εθνικής ασφάλειας. Τέλος, παρά τις τάσεις στις λειτουργίες του κυβερνοχώρου και των χρηστών του, τόσο κρατικών όσο και μη κρατικών, για να προκαλέσουν την κυριαρχία σε διάφορες μορφές της, όπως αναφέρει ο Stephen Krasner, η κυριαρχία «διατηρείται».(Betz & Stevens, 2011)

Το μοντέλο για τη διακυβέρνηση του Διαδικτύου περιλαμβάνει μια ποικιλία οργανισμών και ενδιαφερόμενων φορέων που συνεργάζονται για τη λήψη αποφάσεων και την εκπόνηση πολιτικών που αφορούν το Διαδίκτυο. Ορισμένοι από αυτούς τους φορείς είναι, η ICANN (Internet Corporation for Assigned Names and Numbers) είναι μια μη κερδοσκοπική εταιρεία που είναι υπεύθυνη για τη διαχείριση του καθολικού τομέα των ονομάτων του Διαδικτύου (DNS), συμπεριλαμβανομένων των καταχωρητών ονομάτων και αριθμών IP. Η IANA (Internet Assigned Numbers Authority) (N.d., Iana.org), η οποία είναι υπεύθυνη για την ανάθεση παγκοσμίως μοναδικών πόρων, όπως τους αριθμούς IP και τα πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Η ISOC (Internet Society) (Build, promote, and defend the Internet, 2017), η οποία είναι μια παγκόσμια οργάνωση με στόχο την προώθηση της ανάπτυξης και της χρήσης του Διαδικτύου σε όλο τον κόσμο. Η IETF (Internet

Engineering Task Force), (IETF, Home, n.d.) μια παγκόσμια ομάδα εθελοντών που ασχολείται με την ανάπτυξη προτύπων Διαδικτύου. Η IRTF (Internet Research Task Force) μια ομάδα που εργάζεται πάνω σε επιστημονική έρευνα που αφορά το Διαδίκτυο. Η IESG (Internet Engineering Steering Group) είναι η ομάδα που διοικεί τη λειτουργία της IETF. Το IAB (Internet Architecture Board) (n.d., IAB)που είναι υπεύθυνο για την προώθηση της ανάπτυξης της αρχιτεκτονικής του Διαδικτύου. Οι RIR (Regional Internet Registries) που είναι οι οργανισμοί που χορηγούν διευθύνσεις IP και αναλύουν την κατανομή τους σε περιφερειακό επίπεδο (Mueller, 2009).

Σε παγκόσμιο επίπεδο, οι παραπάνω οργανισμοί συνεργάζονται με διεθνείς οργανισμούς, κυβερνήσεις και ενδιαφερόμενους φορείς για τη διαμόρφωση πολιτικών και προτύπων που αφορούν το Διαδίκτυο. Επιπλέον, επιχειρήσεις όπως η Amazon, η Apple, η AT&T, η Cisco, η Dell και η EMC συχνά συμμετέχουν στο μοντέλο multi-stakeholder μέσω εμπλοκής σε διάφορους οργανισμούς και ομάδες εργασίας που ασχολούνται με θέματα διαδικτύου. Η συμμετοχή τους συμβάλλει με την εμπορική εμπειρία και τους πόρους που είναι απαραίτητοι για την ανάπτυξη και την εφαρμογή αποτελεσματικών πολιτικών και τεχνικών λύσεων για το διαδίκτυο.

Το μοντέλο διακυβέρνησης που επικρατεί στον κυβερνοχώρο, όπου ισχυρές χώρες που διαθέτουν σημαντικό βάρος στο Διαδίκτυο λαμβάνουν τις αποφάσεις προκαλεί αντιδράσεις από άλλες χώρες που θεωρούν ότι δεν έχουν επαρκή εκπροσώπηση. Χώρες όπως η Κίνα και η Ρωσία έχουν αρχίσει να αντιλαμβάνονται τη σημασία του κυβερνοχώρου για την εθνική τους ασφάλεια και αναζητούν τρόπους να διασφαλίσουν την ανεξαρτησία τους σε αυτόν τον τομέα. Η εισαγωγή της έννοιας του κυβερνοχώρου προκαλεί αναθεώρηση του τρόπου με τον οποίο οι χώρες συμμετέχουν στη διακυβέρνηση του διαδικτύου και αναζητούν τρόπους να προστατεύσουν τα συμφέροντά τους σε αυτόν τον τομέα. Οι προκλήσεις και οι αλλαγές που συμβαίνουν στον κυβερνοχώρο και τη διακυβέρνηση του Διαδικτύου λόγω της κυριαρχίας και των προσπαθειών των χωρών να προστατεύσουν τα δικά τους συμφέροντα καθιστούν το διαδίκτυο ως πηγή αντιπαραθέσεων μεταξύ των χωρών που επιθυμούν να επιβάλουν την κυριαρχία τους και αυτών που αγωνίζονται για πιο ισορροπημένες δομές διακυβέρνησης που λαμβάνουν υπόψη τα συμφέροντα όλων των εμπλεκομένων. Επιπλέον, οι χώρες επιδιώκουν να αποκτήσουν ελεγκτικά μέσα στον κυβερνοχώρο προκειμένου να προστατεύσουν την εθνική τους ασφάλεια και να εξασφαλίσουν ότι τα δεδομένα και οι επικοινωνίες που διέρχονται από το Διαδίκτυο δεν είναι υπό τον έλεγχό αλλοδαπών δυνάμεων ενώ παράλληλα

αντιμετωπίζουν την πρόκληση να συνεργαστούν διεθνώς για την ανάπτυξη διεθνών κανόνων και προτύπων για τη διακυβέρνηση του διαδικτύου, παρά τις διαφορετικές προσεγγίσεις και τα συμφέροντα των διαφόρων κρατών. Η ανάπτυξη νομοθεσίας και μέτρων προστασίας της ιδιωτικότητας και των δικαιωμάτων των πολιτών στον κυβερνοχώρο αποτελεί προτεραιότητα για πολλές χώρες, καθώς οι πολίτες τους ανησυχούν για την προστασία των δεδομένων τους και την αποφυγή παραβιάσεων από εξωτερικές δυνάμεις. Αυτές οι προκλήσεις απαιτούν στρατηγικές που θα εξισορροπούν την ασφάλεια, την ιδιωτικότητα, την ελευθερία και τη διαφάνεια στον κυβερνοχώρο, ενώ παράλληλα θα επιτρέπουν την καινοτομία και την ανάπτυξη του Διαδικτύου ως παγκόσμιου δικτύου επικοινωνίας και πληροφοριών (Mathiason, 2008).

2.3.2 Προκλήσεις σε νομικό πλαίσιο

Η νομική πρόκληση που αντιμετωπίζουν πολλές χώρες αφορά την εφαρμογή του Διεθνούς Δικαίου του Εμπολέμου (ΔΔΕ) στον κυβερνοχώρο. Η έλλειψη διεθνούς συναίνεσης για τον τρόπο ρύθμισης των εισβολών στον κυβερνοχώρο οδηγεί σε σύγχυση. Οι προκλήσεις που προκύπτουν στην κατασκευή μιας πολυμερούς συνθήκης για τον κυβερνοχώρο είναι αρχικά πώς μια συνθήκη επιβιώνει σε περίοδο συγκρούσεων, επιπλέον οι κυβερνοεπιθέσεις μπορούν να προκαλέσουν ανεπιθύμητες επιπτώσεις που είναι δύσκολο να αξιολογηθούν ή να ποσοτικοποιηθούν. Η αντικειμενικότητα μιας συνθήκης κυβερνοπολέμου θα πρέπει να είναι η ρύθμιση αυτής της μορφής πολέμου και των συνεπειών της. Η πιθανότητα ενός μεγάλου κυβερνο-πολέμου είναι πραγματική, δεδομένου του αριθμού των χωρών που επί του παρόντος δεσμεύονται να εφαρμόσουν επιθετικές ικανότητες στον κυβερνοχώρο.

Κάποιες από τις κύριες αρχές του Διεθνούς Δικαίου των Ένοπλων Συγκρούσεων (ΔΔΕΣ) που θα μπορούσαν να χρησιμοποιηθούν για να καθοδηγήσουν τις μελλοντικές συζητήσεις για τις συνθήκες κυβερνο-πολέμου. Ένα από τα σημαντικά ζητήματα είναι πώς να καθοριστεί η διάκριση μεταξύ στρατιωτικών και μη στρατιωτικών συστημάτων και περιουσιών στον κυβερνοχώρο. Στην παραδοσιακή μάχη, υπάρχει συνήθως ένας καθαρός διαχωρισμός μεταξύ πολιτικών και στρατιωτικών περιουσιών, αλλά στον κυβερνοχώρο η γραμμή είναι λιγότερο σαφής. Αυτό προκαλεί δυσκολίες στην εφαρμογή της αρχής της στρατιωτικής αναγκαιότητας και απαιτεί μεγαλύτερη συνεργασία μεταξύ διεθνών νομικών εμπειρογνωμόνων,

στρατιωτικών και ηλεκτρονικών μηχανικών. Η αρχή της διάκρισης σχεδιάστηκε για να ορίζει τους μαχητές από τους μη-μαχητές. Σύμφωνα με την τρέχουσα εφαρμογή του Διεθνούς Δικαίου των Ένοπλων Συγκρούσεων (ΔΔΕΣ), μόνο οι στρατιώτες των κανονικών ένοπλων δυνάμεων επιτρέπεται να χρησιμοποιούν δύναμη κατά του εχθρού. Σε πραγματική σύγκρουση, οι μαχητές πρέπει να διακρίνονται από τους μη-μαχητές. Δεν πρέπει να χρησιμοποιούνται οι μη-μαχητές ή περιουσία για να αποφευχθεί κάποια επίθεση. Εάν νόμιμοι μαχητές αιχμαλωτιστούν από τον εχθρό, δεν μπορούν να τιμωρηθούν για τις πράξεις τους, εφόσον συμμορφώνονται με το Διεθνές Δίκαιο του Πολέμου. Οι νόμιμοι μαχητές πρέπει επίσης να χειρίζονται με ανθρωπιστικό τρόπο σύμφωνα με τα συμφωνημένα πρότυπα για τη μεταχείριση των πολεμιστών και πρέπει να απελευθερώνονται άμεσα με τον τερματισμό των εχθροπραξιών (Dinstein, 2012).

Η εφαρμογή αυτής της αρχής στον κυβερνο-πόλεμο του εικοστού πρώτου αιώνα είναι ιδιαίτερα δύσκολη επειδή πολλές διαδικτυακές επιθέσεις εκτελούνται μακριά από οποιαδήποτε τοποθεσία υπάρχει εχθρός. Εάν μια κυβερνο-επίθεση εκτελείται από χιλιόμετρα μακριά από μια ανώνυμη ή μυστική δύναμη, δεν υπάρχει αξιόπιστος τρόπος εφαρμογής αυτής της αρχής. Η εφαρμογή της αρχής αντιμετωπίζει επιπλέον προκλήσεις εάν οι επιτιθέμενοι είναι μη στρατιωτικό προσωπικό, πόσο μάλλον αν είναι πολίτες. Από τον Πρώτο Παγκόσμιο Πόλεμο και έπειτα, οι εθνικές κυβερνήσεις έχουν συνεργαστεί μέσω του ΔΔΕΣ για να απαγορεύσουν τη χρήση ορισμένων όπλων με δυνατότητα να προκαλέσουν σοβαρές ζημιές πέρα από τους αρχικούς τους στόχους. Παραδείγματα απαγορευμένων όπλων είναι το δηλητηριώδες αέριο και οι λέιζερ. Και τα δύο αυτά όπλα, ένα παλαιό και ένα νέο, είχαν τη δυνατότητα να προκαλέσουν μαζικούς τραυματισμούς και ζημιές πέρα από τους στόχους τους. Έτσι, οι στρατιωτικές δυνάμεις που χρησιμοποιούν το δημόσιο Διαδίκτυο για τη διανομή κακόβουλου κώδικα ή κακόβουλου λογισμικού θα μπορούσαν να θεωρηθούν ότι παραβιάζουν την αρχή των απαγορευμένων όπλων. Για παράδειγμα, εάν μια κυβερνο-δύναμη ενσωματώσει κακόβουλο κώδικα σε ένα δημόσιο ιστότοπο που μολύνει πολύ περισσότερα μη-μαχητικά συστήματα από μαχητικά, η πράξη θα μπορούσε να θεωρηθεί ως παράβαση της συγκεκριμένης αρχής. Και πάλι, επειδή δεν υπάρχει συναίνεση για το τι αποτελεί κυβερνο-όπλο, είναι δύσκολο να εφαρμοστεί αυτή η αρχή. Έτσι, πιθανώς θα χρειαστεί ένα μεγάλο πραγματικό γεγονός κυβερνο-πολέμου για να μειωθεί η ασάφεια περί της αρχής αυτής.

Σύμφωνα με το ΔΔΕΣ, η αρχή της προδοσίας σχεδιάζεται για να ρυθμίσει την κατευθυνόμενη καταστροφή ορισμένων εγκαταστάσεων που θεωρούνται ιστορικά νόμιμα καταφύγια κατά τη διάρκεια του πολέμου, παραδείγματα είναι όλοι οι εργαζόμενοι σε ιατρικές δομές και οι εγκαταστάσεις και τα καταφύγια. Συνήθως, αυτού του είδους οι εγκαταστάσεις είναι σαφώς σηματοδοτούμενες με διεθνώς αναγνωρισμένα σύμβολα (π.χ. Ο Ερυθρός Σταυρός ή η Ερυθρά Ημισέληνος) (International Committee of the Red Cross, 2021). Σύμφωνα με το ΔΔΕΣ, οι στρατιωτικοί διοικητές ή το προσωπικό έχουν απαγορευθεί να μετατρέπουν νόμιμα στρατιωτικούς στόχους σε ψευδή καταφύγια χρησιμοποιώντας λανθασμένα σύμβολα. Στον κυβερνοχώρο, η αρχή της προδοσίας μπορεί να ισχύει εάν τοποθετηθούν ψευδή σήματα καταφύγιων σε διαδικτυακά συστήματα που χρησιμοποιούνται για στρατιωτικούς σκοπούς. Για παράδειγμα, η χρήση ενός ακαδημαϊκού δικτύου όπως το UK JANET από τον στρατό για να διευκολύνει τη μεταφορά εντολών ελέγχου και ελέγχου σε πραγματικό χρόνο θα θεωρείτο παράβαση της προδοσίας. Αντίστοιχα, τα κρίσιμα συστήματα πληροφοριών που εξυπηρετούν νοσοκομεία ή σχολεία θα πρέπει να είναι σαφώς ταυτοποιημένα στον κυβερνοχώρο για να αποτραπεί η επίθεση αυτών των δομών με εχθρικές κυβερνο-επιθέσεις. Τα θέματα αναγνώρισης και ταυτοποίησης είναι δύσκολα στον κυβερνοχώρο, κάνοντας σχεδόν οποιαδήποτε επίθεση μια επιχείρηση υψηλού κινδύνου.

Επιπλέον, η αρχή της ουδετερότητας, που ιστορικά καθιερώθηκε για τη διατήρηση της ειρήνης μεταξύ των χωρών κατά τη διάρκεια ανοιχτών εχθροπραξιών, αντιμετωπίζει σημαντικές προκλήσεις στο πλαίσιο του κυβερνοπολέμου. Η ουδετερότητα παραδοσιακά περιλαμβάνει την αποχή από την υποστήριξη οποιασδήποτε πλευράς σε μια σύγκρουση για την αναζήτηση ασυλίας από επίθεση. Ωστόσο, η εφαρμογή αυτής της αρχής στον κυβερνοχώρο είναι πολύπλοκη λόγω της φύσης των σύγχρονων δικτύων επικοινωνίας και της φύσης του διαδικτύου χωρίς σύνορα. Στον παραδοσιακό πόλεμο, οι ουδέτερες χώρες αναμένεται να απέχουν από την παροχή υποστήριξης, όπως όπλα, προσωπικό ή έδαφος, σε οποιοδήποτε εμπόλεμο μέρος. Σε αντάλλαγμα, οι εμπόλεμοι συμφωνούν να μην επιτεθούν στην ουδέτερη χώρα. Ωστόσο, στον κυβερνοχώρο, η διάκριση μεταξύ ουδέτερων και μη ουδέτερων εδαφών είναι πρόκληση, επειδή οι κυβερνοεπιθέσεις συχνά πραγματοποιούνται στις υποδομές δικτύου πολλών χωρών. Για παράδειγμα, μια κυβερνοεπίθεση που εξαπολύθηκε από το Ισραήλ ή τη Νότια Κορέα μπορεί να περάσει από δρομολογητές που βρίσκονται τόσο σε συμμαχικές όσο και σε ουδέτερες

χώρες, θολώνοντας τα όρια ουδετερότητας. Επιπλέον, η έννοια της ουδετερότητας στον κυβερνοχώρο αντιμετωπίζει πρόσθετες πολυπλοκότητες λόγω της παγκοσμιοποιημένης και διασυνδεδεμένης φύσης του Διαδικτύου. Οι συντονισμένες επιθέσεις στον κυβερνοχώρο, όπως αυτές στην Εσθονία το 2007, μπορούν να περιλαμβάνουν υπολογιστές από πολλές χώρες, με πολλές από τις επηρεαζόμενες υπηρεσίες να βρίσκονται σε ουδέτερες χώρες, συχνά εν αγνοία των ιδιοκτητών. Αυτή η πρόκληση υπογραμμίζει την ανάγκη για ενημερωμένα πλαίσια και συμφωνίες για την αποτελεσματική αντιμετώπιση της ουδετερότητας στον κυβερνοχώρο. Καθώς η διακυβέρνηση του κυβερνοχώρου συνεχίζει να εξελίσσεται, οι υπεύθυνοι χάραξης πολιτικής και οι στοχαστές πρέπει να αντιμετωπίσουν αυτές τις πολυπλοκότητες για να διατηρήσουν μια ειρηνική και λειτουργική παγκόσμια δικτυωμένη κοινωνία. Η συνεχιζόμενη ανάπτυξη και η πολυπλοκότητα των απειλών στον κυβερνοχώρο υπογραμμίζουν τη σημασία της προληπτικής αντιμετώπισης αυτών των προκλήσεων (Hughes, 2010).

2.4 Προσεγγίσεις των χωρών σε Διεθνές Πλαίσιο

Από το 2000, οι αναφερθείσες κρατικά υποστηριζόμενες κυβερνοεισβολές έχουν επεκταθεί από επιθέσεις σε κυβερνητικές ιστοσελίδες έως και τις κρίσιμες υποδομές. Για παράδειγμα, το 2000, Ισραηλινοί πράκτορες απενεργοποίησαν τις δημόσιες ιστοσελίδες της Χεζμπολάχ και της Παλαιστινιακής Εθνικής Αρχής, με αποτέλεσμα να προκαλέσουν έναν "κυβερνοθρησκευτικό πόλεμο". Το 2001, μια διαμάχη στη Νότια Θάλασσα της Κίνας οδήγησε την Κίνα να εκτελέσει κυβερνοεπίθεση εναντίον μιας ηλεκτρικής εγκατάστασης στην Καλιφόρνια, προκαλώντας σχεδόν την παύση της λειτουργίας του δικτύου. Περιστατικά κυβερνοεπιθέσεων παρατηρήθηκαν επίσης από μη κρατικούς παράγοντες, όπως οι επιθέσεις σε δίκτυα στην Εσθονία το 2007 και στη Γεωργία το 2008. Η απάντηση σε αυτές τις απειλές και επιθέσεις περιλαμβάνει τη δημιουργία νέων πολιτικών και πρωτοβουλιών για την κυβερνοασφάλεια, όπως η αντιμετώπιση της κυβερνοεπίθεσης ως κοινή υποχρέωση άμυνας, όπως ανακοίνωσε το ΝΑΤΟ κατά τη διάρκεια της Συνόδου Κορυφής το 2008. Η κυβερνοασφάλεια αντιμετωπίζεται τόσο ως ζήτημα εσωτερικής επιβολής του νόμου όσο και ως στρατιωτικό ζήτημα άμυνας, και η διαχωριστική γραμμή μεταξύ των δύο αυτών προσεγγίσεων είναι ασαφής.

Πολλές κυβερνήσεις είναι έτοιμες να αναπτύξουν δυνατότητες που εναντίον των διαδικτυακών αντιπάλων τους. Οι πρωτοβουλίες αυτές περιλαμβάνουν την ανάπτυξη εθνικών στρατηγικών για την κυβερνοασφάλεια, τη σύσταση νέων οργάνων και κέντρων λήψης αποφάσεων, καθώς και την ενίσχυση των στρατιωτικών τους ικανοτήτων στον κυβερνοχώρο. Συγκεκριμένα, το Ηνωμένο Βασίλειο, ανακοίνωσε το 2009 το πρόγραμμά του για την κυβερνοασφάλεια, με τη δημιουργία δύο νέων οργάνων - του Γραφείου Κυβερνοασφάλειας (Office of Cyber-Security) και του Κέντρου Λειτουργιών Κυβερνοασφάλειας (Cyber-Security Operations Centre). Επίσης, ο ηγέτης του Συντηρητικού Κόμματος, David Cameron, δήλωσε το 2010 ότι η κυβερνοασφάλεια είναι σημαντικό μέρος της εθνικής στρατηγικής ασφάλειας του κόμματός του. Αυτές οι ενέργειες καθιστούν το Ηνωμένο Βασίλειο το πρώτο κράτος μέλος της ΕΕ που ανακοινώνει ένα πλαίσιο δράσης για την αντιμετώπιση εθνικών διαδικτυακών απειλών (Singer & Friedman, 2014).

Μερικές από τις πρωτοβουλίες και δράσεις που έχουν αναληφθεί από διάφορες χώρες για την αντιμετώπιση των κυβερνοαπειλών και την ενίσχυση των δυνατοτήτων τους στον κυβερνοχώρο αφορούν για παράδειγμα την Νότια Κορέα η οποία ανακοίνωσε το 2010 την προετοιμασία ενός στρατιωτικού κυβερνοπόλεμου για την αποτροπή επιθέσεων από τη Βόρεια Κορέα και άλλες χώρες καθώς ισχυρίζεται ότι η Κίνα χρησιμοποίησε ιούς για να κλέψει πληροφορίες από τα κυβερνητικά του συστήματα το 2004. Επιπλέον το 2008 ο Ινδικός στόλος ξεκίνησε προετοιμασίες για μάχες στον ψηφιακό χώρο. Επίσης, ανακοίνωσε την ανάγκη για ελέγχους κυβερνοασφάλειας που θα πραγματοποιούνται περιοδικά από το Ινδικό Κέντρο Κυβερνοασφάλειας. Έχει ξεκινήσει επίσης την ανάπτυξη μιας διακήρυξης κυβερνοπολέμου βασισμένη στη πυρηνική στρατηγική της.Το Ισραήλ επίσης για την προστασία των δικτύων των Ενόπλων Δυνάμεων του μέσω του Matzob, το οποίο λειτουργεί υπό το Σώμα C41 και είναι υπεύθυνο για τα δίκτυα Ασφαλείας του Ισραήλ και της Mossad, καθώς και για τα κύρια συστήματα των εθνικών επιχειρήσεων που είναι υπεύθυνα για τα δίκτυα ηλεκτρικής ενέργειας και ύδρευσης. Το Matzob τακτικά ελέγχει κρυπτογραφήσεις και τείχη ασφάλειας. Οι ηγέτες της άμυνας είναι περήφανοι για την κυβερνο-ικανότητα των πολιτών του Ισραήλ και για την τεχνολογική τους εξειδίκευση που τους καθιστά ανεξάρτητους από ξένη βοήθεια ή τεχνολογία. Αυτές οι ενέργειες αναδεικνύουν τη σοβαρότητα των κυβερνοεπιθέσεων και τη σημασία που δίνουν πολλές χώρες στην ανάπτυξη και ενίσχυση των δυνατοτήτων τους για την αντιμετώπισή τους (Subrahmanian et al., 2019).

2.4.1 Η άποψη της Ρωσίας

Η θέση της Ρωσίας σχετικά με την εδαφική κυριαρχία στον κυβερνοχώρο υποστηρίζει ότι η κυριαρχία υφίσταται και στον κυβερνοχώρο, όπως και στον φυσικό κόσμο. Αυτό σημαίνει ότι κάθε κράτος έχει το δικαίωμα να ασκεί ελεύθερα την εσωτερική του κυριαρχία στον κυβερνοχώρο του, χωρίς εξωτερικές παρεμβάσεις ή επιθέσεις από άλλα κράτη. Επιπλέον, πιστεύει ότι η επίλυση των προβλημάτων ασφάλειας στον κυβερνοχώρο πρέπει να γίνει με διεθνή συνεργασία και υιοθέτηση κοινών μεθόδων ενώ, πρέπει να εφαρμοστούν οι κανονισμοί του διεθνούς δικαίου για να αποφευχθούν συγκρούσεις λόγω της χρήσης της τεχνολογίας πληροφοριών και επικοινωνιών. Η Ρωσία επίσης επιμένει στο ότι οι υποθέσεις ενός κράτους στον κυβερνοχώρο πρέπει να παραμείνουν ανεξάρτητες από εξωτερικές παρεμβάσεις. Άλλα κράτη δεν πρέπει να παρεμβαίνουν στις εσωτερικές υποθέσεις ενός κράτους μέσω του κυβερνοχώρου ενώ, δηλώνει ότι το Άρθρο 51 του Χάρτη των Ηνωμένων Εθνών, που αναφέρεται στο δικαίωμα αυτοάμυνας για τα κράτη, δεν μπορεί να εφαρμοστεί άμεσα στον κυβερνοχώρο. Αυτό σημαίνει ότι η αυτοάμυνα ενός κράτους σε περίπτωση κυβερνοεπιθέσεων πρέπει να εξετάζεται με διαφορετικό τρόπο από την αυτοάμυνα σε παραδοσιακές συγκρούσεις.

Παρά τις κατηγορίες για επιθέσεις κατά της Εσθονίας και της Γεωργίας, η ρωσική κυβέρνηση έχει αρνηθεί κάθε ευθύνη. Η συμπεριφορά της Ρωσίας στη διεθνή διπλωματία, εστιάζεται στις προσπάθειες για αναγνώριση του καθεστώτος της στη διεθνή σκηνή και την επιρροή της στον κυβερνοχώρο. Η Ρωσία έχει την ανάγκη αναγνώρισης της ως αναπόσπαστου κομματιού της διεθνούς τάξης και προσπαθεί να επιτύχει αυτόν τον στόχο μέσω της διπλωματικής προσπάθειας και της στρατηγικής επικοινωνίας. Οι συγκρούσεις μεταξύ της Ρωσίας και των δυτικών χωρών σχετικά με το μοντέλο διακυβέρνησης του Διαδικτύου επαναφέρουν τη Ρωσία στα επίπεδα των διεθνών αλληλεπιδράσεων, και τοποθετούν τη χώρα σε μια κατάσταση που θυμίζει τα διπλωματικά έθιμα του Ψυχρού Πολέμου. Η πληροφοριακή ασφάλεια, για την Ρωσία είναι θεμελιώδης για την κατανόηση της κυβερνοπολιτικής της, καθώς και η περιφερειακή προσπάθεια για την κωδικοποίηση της, η οποία αυξάνεται σταδιακά σε παγκόσμιο επίπεδο. Η στάση της Ρωσίας στην κυβερνοδιπλωματία, αποτελεί εκδήλωση μιας ιδεολογικής πάλης που οι επιχειρηματίες φιλελεύθερων κυβερνο-

κανονιστικών πλαισίων δεν μπορούν απλώς να απαξιώσουν ή να αγνοήσουν. Το ερώτημα που προκύπτει είναι το πώς θα προσφέρει μια ελκυστική εναλλακτική λύση.

Το 2018 ήταν ένα σημείο καμπής στο ζήτημα της παγκόσμιας διακυβέρνησης του Διαδικτύου, με την υιοθέτηση δύο ανταγωνιστικών ψηφισμάτων. Το πρώτο ήταν μια επαναβεβαίωση της ομάδας Εμπειρογνωμόνων του ΟΗΕ για την κυβερνοπολιτική (UN GGE) που υποστηρίχθηκε από τις Ηνωμένες Πολιτείες, ενώ το δεύτερο ψήφισμα ξεκίνησε την Διακοινοβουλευτική Ομάδα εργασίας (OEWG), το οποίο υποστηρίχθηκε από τη Ρωσία. Η Ρωσία είδε τα ψηφίσματα αυτά ως θετική εξέλιξη στην κυβερνοδιπλωματία της, μετά την πάροδο 20 ετών από το 1998, όταν κατέθεσε το πρώτο της σχέδιο ψηφίσματος σχετικά με την Πληροφορική και Τεχνολογία Επικοινωνίας στην Πρώτη Επιτροπή Εκστρατείας και Διεθνούς Ασφάλειας του Γενικού Συμβουλίου του ΟΗΕ. Η Ρωσία πρότεινε επίσης ένα ψήφισμα για το κυβερνοέγκλημα με στόχο τη δημιουργία ενός ξεχωριστού μονοπατιού στον ΟΗΕ, ως εναλλακτική της Συνθήκης της Βουδαπέστης για το Κυβερνοεγκλημα, η οποία αντιτίθεται από τη Ρωσία λόγω της διασυνοριακής πρόσβασης σε δεδομένα από τις υπηρεσίες πληροφοριών. Οι προτεραιότητες της κυβερνοδιπλωματίας της Ρωσίας είναι αρχικά η επιθυμία της, τόσο περιφερειακά όσο και παγκοσμίως, να χρησιμοποιήσει το διαδύκτιο ως μέσο για την αποκατάσταση του σεβασμού της Ρωσίας σε διεθνές επίπεδο ως μια υπερδύναμη. Επιπλέον, η μακροχρόνια προτεραιότητα της ρωσικής κυβερνοδιπλωματίας, είναι "η δημιουργία συνθηκών για την προώθηση διεθνώς της πρωτοβουλίας για την ανάπτυξη και υιοθέτηση Σύμβασης για τη Διεθνή Πληροφοριακή Ασφάλεια από τα Κράτη Μέλη του ΟΗΕ". Η Ρωσία προσπαθεί να προετοιμάσει το έδαφος για τη θέσπιση ενός νομικού πλαισίου για τον κυβερνοχώρο, παρά το γεγονός ότι η επίτευξη μιας Σύμβασης για την Πληροφοριακή Ασφάλεια στον κυβερνοχώρο είναι ακόμα ανέφικτη. Η Ρωσία προωθεί την ιδέα μιας διεθνούς Σύμβασης για να αντιμετωπίσει την υποτιθέμενη υπεροχή του δυτικού συστήματος και να επιβάλει μια εναλλακτική θεώρηση των διεθνών σχέσεων.

Η Ρωσία ουσιαστικά ακολουθεί μια διπλή στρατηγική στην κυβερνοδιπλωματία. Αφενός, επιδιώκει την εντατικοποίηση της "ασφάλειας" του κυβερνοχώρου, παρουσιάζοντας όλα τα "κυβερνο" ή ψηφιακά συμβάντα ως σοβαρή απειλή για την ασφάλεια. Αφετέρου, αναλαμβάνει το ρόλο της μεγάλης δύναμης που μπορεί να εξασφαλίσει την αντιμετώπιση αυτής της απειλής. Με αυτήν τη θέση, η Ρωσία δρα ταυτόχρονα και ως αναθεωρητική αλλά και ως συντηρητική δύναμη. Αυτή

η θέση προσφέρει διακριτές ανταμοιβές, καθώς παρέχει την δυνατότητα να παρουσιάζεται η Ρωσία ως ανήσυχος, αλλά και ικανός ηγέτης στον κυβερνοχώρο για το μη-δυτικό, κόσμο. Συνεπώς, η Ρωσία επιστρέφει στο παγκόσμιο παιχνίδι της διεθνούς τάξης. Στην ουσία, η Ρωσία παρουσιάζει τον κυβερνοχώρο ως έναν τόπο εξίσου επικίνδυνο με τον πυρηνικό κατά τη γεωπολιτική της προβολή. Αυτό προκαλεί ανησυχίες σχετικά με την ασφάλεια και προωθεί την ιδέα της ανάγκης για παγκόσμια ρύθμιση του διαδικτύου. Επιπλέον, η Ρωσία εκμεταλλεύεται την αυξανόμενη παγκόσμια αντίληψη κατά των ΗΠΑ και των δυτικών χωρών για να ενισχύσει την προβολή της ως υπεύθυνη δύναμη. Χρησιμοποιεί επίσης, τον κυβερνοχώρο ως πλατφόρμα για την επιστράτευση των περιφερειακών της προσπαθειών εναντίον της δυτικής τάξης του κόσμου. Οι συχνές κυβερνοεπιθέσεις και σκάνδαλα, όπως εκείνα των αποκαλύψεων του Snowden[2] και του Cambridge Analytica[3], ενισχύουν τον ισχυρισμό της Ρωσίας για την επικινδυνότητα του κυβερνοχώρου και την ανάγκη για κανόνες. Η αυξανόμενη λαϊκιστική αίσθηση σε παγκόσμιο επίπεδο εξυπηρετεί επίσης τα συμφέροντα του Κρεμλίνου, το οποίο έχει τους ιδεολογικούς και λειτουργικούς πόρους για να εκμεταλλευτεί αυτήν την αίσθηση ως νέα δομική δύναμη στη διεθνή πολιτική.

Για το κενό στον διάλογο για τον ρόλο του διεθνούς δικαίου στον κυβερνοχώρο, αν και υπάρχει συναίνεση ότι ισχύει, η ρωσική ερμηνεία είναι ότι αποτελεί το σύνολο των κανόνων και συμφωνιών που διέπουν τις σχέσεις μεταξύ των μεγάλων δυνάμεων, με έμφαση στην κυριαρχία και απόρριψη της ιδέας του ατόμου ως υποκειμένου του διεθνούς δικαίου. Η ρωσική ερμηνεία βασίζεται στην κλασική κατανόηση της κυριαρχίας και με απόλυτη απόρριψη της έννοιας του ατόμου ως υποκειμένου του διεθνούς δικαίου. Από την άλλη πλευρά, οι φιλελεύθεροι θεωρούν το διεθνές δίκαιο ως μέσο για τη διατήρηση μιας συναίνεσης, ιδιαίτερα σε σχέση με ένα ανοιχτό και ελεύθερο διαδίκτυο που ανήκει στο φιλελεύθερο όραμα της διεθνούς

[2] Το 2013, ο Edward Snowden, πρώην υπάλληλος της Εθνικής Υπηρεσίας Ασφαλείας (NSA) των Ηνωμένων Πολιτειών, διέρρευσε εκατομμύρια εμπιστευτικά έγγραφα που αφορούσαν την παρακολούθηση των επικοινωνιών από τις αμερικανικές υπηρεσίες πληροφοριών. Οι αποκαλύψεις αυτές ανέδειξαν τις μαζικές παρακολουθήσεις και παρεμβάσεις στις διαδικτυακές επικοινωνίες παγκοσμίως, προκαλώντας έντονη αντίδραση και θέτοντας σε αμφισβήτηση την ιδιωτικότητα και την ελευθερία στο Διαδίκτυο.

[3] Το 2018, έγινε γνωστό ότι η Cambridge Analytica, μια εταιρεία ανάλυσης δεδομένων, είχε συγκεντρώσει προσωπικά δεδομένα από εκατομμύρια χρήστες του Facebook χωρίς τη συγκατάθεσή τους. Αυτά τα δεδομένα χρησιμοποιήθηκαν στη συνέχεια για την προσαρμογή και την κατεύθυνση πολιτικών εκστρατειών, συμπεριλαμβανομένων των εκλογών, με στόχο την επιρροή των αποτελεσμάτων. Αυτό το σκάνδαλο ανέδειξε τους κινδύνους που συνδέονται με την εκμετάλλευση των προσωπικών δεδομένων στον κυβερνοχώρο και τις επιπτώσεις στην πολιτική διαδικασία.

τάξης. Η δυτική ερμηνεία δηλαδή του διεθνούς δικαίου, μετατοπίζεται προς τις υπερεθνικές, αντί για τις κρατικές, λύσεις.

Η Ρωσία προωθεί την έννοια της "δημοκρατικοποίησης" των διεθνών σχέσεων, αλλά στην πραγματικότητα αυτή η ατζέντα εξυπηρετεί την πολυπολικότητα της Ρωσίας, παρά την πραγματική δημοκρατικοποίηση της λήψης αποφάσεων στο διεθνές σύστημα. Το διεθνές δίκαιο και οι διεθνείς κανόνες είναι ζωτικής σημασίας για τη διατήρηση του διεθνούς συστήματος, και γι' αυτό η Ρωσία δεσμεύεται απολύτως σε αυτά. Ωστόσο, αντίθετα από το πως εννοούνται στο φιλελεύθερο κόσμο, η Ρωσία ερμηνεύει το διεθνές δίκαιο διαδικαστικά. Μια νομική διευθέτηση στον κυβερνοχώρο, κατά την ρώσικη προσέγγιση, προορίζεται να στοχεύσει το τρέχον "χαλαρό" κυβερνοχώρο που βασίζεται στη λογική του "κοινού δικαίου", η οποία επιτρέπει και αναπαράγει τη φιλελεύθερη προοπτική. Επίσης, οι διεθνείς κανόνες, ειδικά αυτοί που αφορούν την κυβερνοασφάλεια, είναι σημαντικοί στον ρωσικό διπλωματικό διάλογο, καθώς βοηθούν τη Ρωσία να διατηρήσει το καθεστώς της ως μεγάλη δύναμη και στον κυβερνοχώρο. Στη ρωσική προσέγγιση, οι κανόνες υπάρχουν για να ρυθμίζουν τη συμπεριφορά μεταξύ κρατών με διαφορετικές κανονιστικές διατάξεις, και, για να είναι αποτελεσματικοί, πρέπει να είναι δεσμευτικοί (Plotkin, 2020).

2.4.2 Η άποψη των ΗΠΑ

Οι Ηνωμένες Πολιτείες έχουν ισχυρή επιρροή στον κυβερνοχώρο λόγω της τεχνολογικής τους πρωτοπορίας και της μεγάλης τους οικονομικής και στρατιωτικής ισχύος. Η δημιουργία της πρώτης Αμερικανικής κυβερνοδύναμης (USCYBERCOM) φανερώνει την αυξανόμενη σημασία του κυβερνοχώρου στη στρατηγική των Ηνωμένων Πολιτειών (Dziwisz & Romaniuk, 2023). Ως εκ τούτου, η θέση τους σχετικά με την εδαφική κυριαρχία στον κυβερνοχώρο έχει σημαντικές επιπτώσεις στο διεθνές πεδίο της ασφάλειας στον κυβερνοχώρο. Οι Ηνωμένες Πολιτείες επισημαίνουν τη σημασία της προστασίας των κρίσιμων υποδομών, όπως τα μέσα μεταφοράς, και υπογραμμίζουν την ύπαρξη της κυβερνοκυριαρχίας, αλλά ταυτόχρονα αναγνωρίζουν την ανάγκη για τη συμμόρφωση με τις διεθνείς υποχρεώσεις και τον σεβασμό των δικαιωμάτων του ανθρώπου. Οι ΗΠΑ έχουν προσπαθήσει να ορίσουν τον κυβερνοχώρο μέσω διαφόρων εγγράφων και πολιτικών δηλώσεων. Ο

κυβερνοχώρος αναφέρεται ως ένα διαδίκτυο πληροφοριακών υποδομών, συμπεριλαμβανομένων των δικτύων τηλεπικοινωνιών, των υπολογιστικών συστημάτων και των ενσωματωμένων επεξεργαστών και ελεγκτών. Θεωρούν επίσης, τον κυβερνοχώρο ως στρατηγικό τομέα και νευραλγικό σύστημα ελέγχου του κράτους. Τονίζουν τη σημασία του για τη λειτουργία των κρίσιμων υποδομών και των κρατικών επιχειρήσεων, ενώ θεωρούν την προστασία του κυβερνοχώρου ως θέμα εθνικής ασφάλειας και έχουν θεσπίσει εθνικές στρατηγικές και διατάγματα για την ενίσχυση της κυβερνοασφάλειας.

Επιπλέον, οι ΗΠΑ προτείνουν τη δημιουργία διεθνών μηχανισμών και οργανισμών για την αντιμετώπιση των κυβερνοαπειλών και την προώθηση της κυβερνοασφάλειας σε παγκόσμιο επίπεδο. Η προσπάθεια κυριαρχίας στον κυβερνοχώρο δεν ανήκει όμως μόνο στις ΗΠΑ, αλλά και σε άλλες χώρες όπως η Κίνα, η Ινδία και η Ρωσία. Ουσιαστικά απαιτείται η συνεννόηση μεταξύ των χωρών για την δημιουργία ενός πολυμερούς καθεστώτος για τη διακυβέρνηση του κυβερνο-πολέμου σε παγκόσμιο επίπεδο αλλά και να εξετασθεί ο ρόλος που μπορεί να διαδραματίσει μια συνθήκη κυβερνο-πολέμου ή "Συνθήκη για τον Κυβερνοχώρο" στον περιορισμό των δυσμενών επιπτώσεων των διακυβερνητικών συγκρούσεων στον κυβερνοχώρο. Οι ΗΠΑ εκφράζουν, την προθυμία τους να βοηθήσουν τις αναπτυσσόμενες χώρες στην ενίσχυση της ικανότητάς τους στην κυβερνοασφάλεια, παρέχοντας τεχνική γνώση και υποστήριξη για τη βελτίωση των νομικών πλαισίων και των εθνικών πολιτικών τους. Τέλος, επισημαίνουν τη σημασία της εκπαίδευσης και της ενημέρωσης του κοινού σχετικά με τους κίνδυνους και τα μέτρα προστασίας στον κυβερνοχώρο.

Από νομικής πλευράς το 2001 εκδόθηκε από τις ΗΠΑ ο"Νόμος Patriot". Ο σκοπός αυτού του νόμου είναι να εμποδίσει ή να αντιμετωπίσει τις τρομοκρατικές δραστηριότητες. Ο Νόμος επιτρέπει στην κυβέρνηση να λαμβάνει προσωπικές πληροφορίες, συμπεριλαμβανομένων τηλεφωνικών, ηλεκτρονικών, ιατρικών, οικονομικών και άλλων εγγραφών, ανά πάσα στιγμή χωρίς την επίβλεψη και την άδεια του δικαστή. Αυτό επιτρέπει στην πράξη την ελεύθερη παρακολούθηση οποιουδήποτε. Επιπλέον, ο νόμος αυτός διευρύνει τον ορισμό της τρομοκρατίας και επεκτείνει το πεδίο δραστηριοτήτων που διαχειρίζονται από την αστυνομία (United States Senate et al., 2020).

2.4.3 Η άποψη της Κίνας

Η Κίνα υποστηρίζει την αρχή της ενεργού υπεράσπισης της κυριαρχίας στον κυβερνοχώρο, αλλά παραδέχεται παράλληλα ότι η κυριότητα των stakeholders είναι η κυρίαρχη πρακτική στον κυβερνοχώρο. Για να προσαρμοστεί στην υφιστάμενη κατάσταση, η Κίνα έχει αποδεχθεί ένα μοντέλο συνύπαρξης που λαμβάνει υπόψη του τόσο την κυριαρχία των κρατών όσο και τον ρόλο των stakeholders. Οι βασικές αρχές αυτού του μοντέλου περιλαμβάνουν την υιοθέτηση του μοντέλου κυριαρχίας συν-διακυβέρνησης για θέματα δημόσιας πολιτικής που σχετίζονται με τον κυβερνοχώρο, ενώ στους τεχνικούς και οικονομικούς τομείς υιοθετείται το μοντέλο που καθοδηγείται από τους stakeholders. Η βασική στρατηγική για το μοντέλο συνύπαρξης περιλαμβάνει τη λήψη αποφάσεων σχετικά με το πού μπορούν να γίνουν συμβιβασμοί και πού όχι. Για παράδειγμα, δεν μπορούν να γίνουν συμβιβασμοί όταν πρόκειται για θέματα όπως ο έλεγχος των δικτύων στην επικράτεια μιας χώρας ή η διαχείριση του ορίου του κυβερνοχώρου. Από την άλλη πλευρά, μπορούν να γίνουν συμβιβασμοί σε θέματα που αφορούν τεχνικά ή οικονομικά θέματα, όπου οι stakeholders έχουν εξειδικευμένες γνώσεις και εμπειρία (M. L. Mueller, 2010).

Υπάρχουν ενδείξεις ότι ο Λαϊκός Απελευθερωτικός Στρατός της Κίνας επιθυμεί να προκαλέσει την κυριαρχία των ΗΠΑ στο ηλεκτρομαγνητικό φάσμα σε περίπτωση διμερούς στρατιωτικής αντιπαράθεσης. Η ετήσια αναφορά της Επιτροπής Οικονομικής και Ασφάλειας των ΗΠΑ προς το Κογκρέσο δείχνει αυξημένη επιθετική ικανότητα από την κυβέρνηση της Κίνας. Η Κίνα έχει εκφράσει την θέση της για την κυριαρχία στον κυβερνοχώρο μέσω διαφόρων ομιλιών και δηλώσεων του Προέδρου Ξι Τζινπίνγκ και άλλων αξιωματούχων. Κεντρικό στοιχείο αυτής της θέσης είναι η έννοια του κυβερνοχώρου, υποστηρίζει ότι οι κυβερνήσεις έχουν το δικαίωμα και την ευθύνη να λαμβάνουν αποφάσεις και να ρυθμίζουν τις δραστηριότητες στον κυβερνοχώρο εντός των συνόρων τους, σύμφωνα με τα εθνικά τους συμφέροντα και την κυριαρχία τους.

Συγκεκριμένα, η Κίνα υποστηρίζει ότι ο κυβερνοχώρος είναι ένας τομέας όπου ισχύουν οι κυριαρχικές αρχές των κρατών, και κάθε κράτος έχει το δικαίωμα να καθορίζει την πολιτική του για τον κυβερνοχώρο και να επιβάλλει την κυριαρχία του εκεί. Η Κίνα αντιτίθεται σε οποιαδήποτε παρέμβαση κράτους στην κυβερνητική τους πολιτική στον κυβερνοχώρο, ιδίως όταν αυτή η παρέμβαση θίγει τα εθνικά τους

συμφέροντα και την κυριαρχία τους, ενώ προωθεί τη διεθνή συνεργασία για τη δημιουργία ενός συστήματος διεθνούς διακυβέρνησης του κυβερνοχώρου που θα βασίζεται σε πολυμερή, δημοκρατικά και διαφανή κριτήρια. Αυτές οι θέσεις αποτελούν ένα μέρος της προσπάθειας της Κίνας να αναδείξει τον ρόλο της ως σημαντικό παράγοντα στη διαμόρφωση των διεθνών κανόνων και της πολιτικής για τον κυβερνοχώρο (Shen, 2016).

Η πρόταση της Κίνας σχετικά με τις πρωτοβουλίες που πρέπει να αναληφθούν για την ανάπτυξη και την ασφάλεια του Διαδικτύου εκφράστηκαν από τον Λιου Γιουνσάν και τον Μα Κάι, δύο αξιωματούχους της Κίνας. Σύμφωνα με αυτούς προτείνεται η ενίσχυση της διεθνούς συνεργασίας για τη βελτίωση των κανόνων διακυβέρνησης του Διαδικτύου, με στόχο την προώθηση ενός συστήματος βασισμένου στην πολυμερή, δημοκρατική και διαφανή διακυβέρνηση. Παράλληλα τονίζεται η ανάγκη σεβασμού του κυβερνοχώρου ως βασικής αρχής για την προώθηση της καινοτομίας και της οικονομικής ανάπτυξης, η ενίσχυση της εκπροσώπησης και της φωνής των αναδυόμενων αγορών και των αναπτυσσόμενων χωρών και η ανάγκη για συνεργασία μεταξύ των χωρών σε τομείς όπως η έρευνα και ανάπτυξη τεχνολογίας, το διασυνοριακό ηλεκτρονικό εμπόριο και η καινοτομία στα ΜΜΕ. Τονίζεται επίσης, από τους δυο αξιωματούχους, η σημασία της διασποράς των πολιτισμών μέσω του Διαδικτύου και η ανάγκη για ανταλλαγή πολιτισμικών ιδεών και επικοινωνίας μεταξύ των χωρών αλλά και η ανάγκη για εφαρμογή μέτρων που θα προστατεύουν τον κυβερνοχώρο, τα δεδομένα και τα δίκτυα από κυβερνοεπιθέσεις και άλλες απειλές (Assembly, 2015).

Οι νόμοι που έχουν θεσπιστεί για την ασφάλεια του Διαδικτύου και την προστασία του κυβερνοχώρου στην Κίνα περιλαμβάνουν α) τον νόμο Εθνικής Ασφάλειας, που εγκρίθηκε το 2015, και θεσπίζει ένα σύστημα ασφαλείας πληροφοριών ενώ, ενισχύει τις προσπάθειες για την πρόληψη, τη διακοπή και την τιμωρία κυβερνο-επιθέσεων, την αποτροπή παραβιάσεων της κυβερνοασφάλειας και την προστασία του κυβερνοχώρου από τέτοιες επιθέσεις, β) τους νόμους ασφάλειας Δικτύου, που εγκρίθηκαν το 2016 και το 2017 και προβλέπουν μέτρα για την προστασία των νόμιμων δικαιωμάτων και συμφερόντων πολιτών, επιχειρήσεων και άλλων οργανισμών στον κυβερνοχώρο, ενώ καθορίζουν περαιτέρω το πεδίο εφαρμογής των κρίσιμων πληροφοριακών υποδομών για τη διατήρηση της κυβερνοχώρου. Προστατεύουν επίσης την ασφάλεια δεδομένων και πληροφοριών στο Διαδίκτυο και θέτουν κανόνες για τις δραστηριότητες σε διάφορα δίκτυα και

πλατφόρμες στο Διαδίκτυο. Οι νόμοι αυτοί ουσιαστικά θεσπίζουν τα θεμέλια για την ασφάλεια του Διαδικτύου και την προστασία του κυβερνοχώρου στην Κίνα, και παρέχουν νομικό πλαίσιο για την εποπτεία, την εφαρμογή του νόμου και την επίλυση διαφορών στον κυβερνοχώρο (Daricili & Burak, 2018).

3. Μελέτη Περιπτώσεων: Παραβιάσεις Εδαφικής Κυριαρχίας στον Κυβερνοχώρο

3.1 Περιστατικά κυβερνοεπιθέσεων στις ΗΠΑ

Υπάρχουν αρκετά παραδείγματα που αναδεικνύουν τη σοβαρότητα των κυβερνοεπιθέσεων που αποσκοπούν στην παραβίαση της εδαφικής κυριαρχίας των ΗΠΑ στον κυβερνοχώρο και την ανάγκη για αποτελεσματικά μέτρα ασφαλείας και προστασίας. Το 2015, εκδηλώθηκε μια μαζική παραβίαση δεδομένων στο Office of Personnel Management (OPM), μια κυβερνητική υπηρεσία που υπεύθυνη για τη διαχείριση των προσωπικών δεδομένων των υπαλλήλων της κυβέρνησης των ΗΠΑ. Οι δράστες, πιθανότατα υποστηριζόμενοι από κρατικό φορέα, απέκτησαν πρόσβαση σε εκατομμύρια προσωπικά δεδομένα υπαλλήλων της κυβέρνησης συμπεριλαμβανομένων δεδομένων ασφαλείας και πληροφοριών ασφαλιστικών δικαιωμάτων. Η παραβίαση επηρέασε εκατομμύρια ατομικά δεδομένα υπαλλήλων της κυβέρνησης, συμπεριλαμβανομένων πιθανώς προσωπικών πληροφοριών και ευαίσθητων λεπτομερειών. Η παραβίαση αυτή αποτελεί μια από τις μεγαλύτερες και πλέον σοβαρές παραβιάσεις προσωπικών δεδομένων που έχουν καταγραφεί στην ιστορία των Ηνωμένων Πολιτειών. Η παραβίαση προκάλεσε σοβαρές ανησυχίες σχετικά με την ασφάλεια των πληροφοριών και την ικανότητα των αντιμέτρων για την προστασία τους. Επίσης, έθεσε το ζήτημα της κυβερνοασφάλειας υψηλά στην ατζέντα της κυβέρνησης των ΗΠΑ και προκάλεσε ευρεία συζήτηση για το πώς θα πρέπει να προστατεύονται τα προσωπικά δεδομένα στην ψηφιακή εποχή (Fruhlinger, 2020).

Το 2020, παραβιάστηκαν οι υποδομές του Αμερικάνικού Υπουργείου της Εθνικής Περιουσίας (U.S. National Treasury) από κυβερνοεπιθέσεις, με στόχο την υπονόμευση της οικονομίας και του χρηματοπιστωτικού συστήματος των ΗΠΑ. Η κυβερνοεπίθεση αναδεικνύει την αυξανόμενη απειλή που αντιμετωπίζει η οικονομία και το χρηματοπιστωτικό σύστημα των ΗΠΑ από κυβερνοεπιθέσεις. Η παραβίαση των υποδομών της Αμερικάνικης κυβέρνησης δεν απειλεί μόνο τη λειτουργία του τραπεζικού συστήματος αλλά και την οικονομική σταθερότητα των ΗΠΑ και κατ' επέκταση, την παγκόσμια οικονομία. Οι κυβερνοεπιθέσεις αυτού του είδους στρέφονται συχνά κατά κρίσιμων υποδομών και οργανισμών που αποτελούν πυλώνες της οικονομίας ενός κράτους. Η συγκεκριμένη μπορεί να είχε καταστροφικές

συνέπειες, συμπεριλαμβανομένης της κλοπής ευαίσθητων χρηματοοικονομικών δεδομένων, της υπονόμευσης της εμπιστοσύνης των πολιτών στο χρηματοπιστωτικό σύστημα και της απώλειας χρηματοπιστωτικής σταθερότητας. Η αντιμετώπιση τέτοιων κυβερνοεπιθέσεων απαιτεί τη στενή συνεργασία μεταξύ των κυβερνητικών αρχών, των κρίσιμων υποδομών και των εταιρειών ασφαλείας πληροφοριών. Επιπλέον, είναι σημαντικό να ενισχυθούν τα μέτρα ασφαλείας και να αναπτυχθούν στρατηγικές αντίδρασης για την αντιμετώπιση τέτοιων επιθέσεων στο μέλλον (Sanger, 2020).

3.2 Περιστατικά κυβερνοεπιθέσεων στην Κίνα

Το 2017, η Κίνα κατηγορήθηκε για την επίθεση στην Equifax, μια μεγάλη εταιρεία πιστωτικής αξιολόγησης στις Ηνωμένες Πολιτείες. Κατά τη διάρκεια αυτής της επίθεσης, περίπου 145 εκατομμύρια Αμερικανοί πολίτες εκτέθηκαν σε κλοπή ταυτότητας και προσωπικών πληροφοριών συμπεριλαμβανομένων ονομάτων, διευθύνσεων, αριθμών κοινωνικής ασφάλισης και αριθμών πιστωτικών καρτών. Η παραβίαση αυτή είχε σοβαρές επιπτώσεις για τους εν λόγω αμερικανούς πολίτες, καθώς έθετε τις προσωπικές τους πληροφορίες σε κίνδυνο κατάχρησης και απάτης. Η επίθεση κατά της Equifax αναδεικνύει τη σοβαρότητα των κυβερνοεπιθέσεων και την ανάγκη για ενίσχυση των μέτρων ασφαλείας στον κυβερνοχώρο. Επιπλέον, η αντιμετώπιση τέτοιων επιθέσεων απαιτεί συνεργασία μεταξύ των κρατικών αρχών, των εταιρειών και των άλλων ενδιαφερόμενων φορέων για την αντιμετώπιση των κυβερνοαπειλών και τη διασφάλιση της ασφάλειας των πολιτών και των επιχειρήσεων (Equifax data breach settlement, 2019).

Κατά τους Ολυμπιακούς Αγώνες του 2008 στο Πεκίνο, η Κίνα κατηγορήθηκε για επιθέσεις κατά αθλητικών οργανισμών διάφορων χωρών, συμπεριλαμβανομένων των ΗΠΑ, που στόχευαν στην παραβίαση των συστημάτων τους και την κλοπή ευαίσθητων πληροφοριών. Οι λεπτομέρειες σχετικά με την εκτέλεση και την έκταση αυτών των επιθέσεων δεν είναι πλήρως γνωστές, αλλά υπήρξαν αναφορές για επιδράσεις σε συστήματα πληροφορικής πολλών οργανισμών, συμπεριλαμβανομένων αθλητικών φορέων. Αυτή η επίθεση αναδεικνύει την ικανότητα των κρατών ή άλλων εχθρικών οντοτήτων να χρησιμοποιούν τις κυβερνοεπιθέσεις ως μέσο για την

επίτευξη γεωπολιτικών ή γεωστρατηγικών στόχων. Επιπλέον, επισημαίνει τη σημασία της διατήρησης ισχυρών μέτρων ασφαλείας στους ψηφιακούς χώρους, ιδίως κατά μεγάλων και κρίσιμων εκδηλώσεων, όπως οι Ολυμπιακοί Αγώνες (Heath, 2008).

3.3 Περιστατικά κυβερνοεπιθέσεων στην Ρωσία

Κατά τις προεδρικές εκλογές του 2016 στις Ηνωμένες Πολιτείες, η Ρωσία κατηγορήθηκε για παρέμβαση στις εκλογικές διαδικασίες μέσω κυβερνοεπιθέσεων και διαδικτυακής παρέμβασης με σκοπό τον επηρεασμό των αποτελεσμάτων. Η ρωσική παρέμβαση περιελάμβανε τη χρήση κυβερνοεπιθέσεων για την παραβίαση των συστημάτων εκλογικής πληροφόρησης, την απόπειρα εξάπλωσης παραπλανητικών πληροφοριών μέσω κοινωνικών μέσων και διαδικτυακών πλατφορμών, καθώς και τη διαρροή ευαίσθητων δεδομένων με σκοπό να υπονομεύσει την εμπιστοσύνη στη διαδικασία εκλογών και να δημιουργήσει αναταραχή. Οι αναφορές για τη ρωσική παρέμβαση προκάλεσαν έντονο πολιτικό αντίκτυπο και επισημάνθηκαν ως ένα παράδειγμα του πώς οι κυβερνοεπιθέσεις μπορούν να χρησιμοποιηθούν για την παρέμβαση στις εσωτερικές πολιτικές διαδικασίες και τη δημιουργία αναταραχής σε δημοκρατικές διαδικασίες (Nussbaum & Turcotte, 2020).

Επιπλέον, το 2015, ανακοινώθηκε ότι υπήρχε ρωσικός δάκτυλος πίσω από το περιστατικό που είχε ως στόχο την παραβίαση του δικτύου του γερμανικού Κοινοβουλίου. Αρκετές αναφορές υπήρχαν για κυβερνοεπιθέσεις κατά διάφορων οργανισμών του NATO, μερικές από τις οποίες καταγράφηκαν ως εκτεταμένες και σοβαρές παραβιάσεις των δικτύων ασφαλείας.

Τέλος η Ρωσία κατηγορήθηκε για επιθέσεις και παρεμβάσεις στον κυβερνοχώρο της Ουκρανίας τόσο κατά τη διάρκεια της κρίσης στην ανατολική Ουκρανία και της κατάληψης της Κριμαίας το 2014 όσο και κατά την εισβολή της το 2022. Αυτές οι κυβερνοεπιθέσεις είχαν ως στόχο την αποσταθεροποίηση της Ουκρανίας και την ενίσχυση των ρωσικών συμφερόντων στην περιοχή. Οι επιθέσεις περιλάμβαναν διάφορες μορφές κυβερνοεπιθέσεων, όπως διακοπή των υποδομών δικτύων επικοινωνίας, κατάρρευση των συστημάτων πληροφορικής και παρεμβάσεις στις εκλογικές διαδικασίες. Οι κυβερνοεπιθέσεις αντιμετωπίστηκαν ως μέρος της ευρύτερης στρατηγικής παραβίασης της ασφάλειας της Ουκρανίας από την

επιτιθέμενη Ρωσία αλλά και ως μέρος της προετοιμασίας για την εισβολή της στην περιοχή και ενέτειναν τις διεθνείς εντάσεις μεταξύ Ρωσίας και Ουκρανίας, καθώς και μεταξύ της Ρωσίας και των δυτικών χωρών. ΑΑξιολόγηση των επιπτώσεων και των πιθανών μελλοντικών εξελίξεων (Bateman, 2022).

3.4 Η Ισορροπία Δυνάμεων μεταξύ ΗΠΑ, Ρωσίας και Κίνας στον Κυβερνοχώρο

Το διαδίκτυο διαχειρίζεται από ενδιαφερόμενα μέρη από την κοινωνία των πολιτών, τον ιδιωτικό τομέα και, σε μικρότερο βαθμό, από τις κυβερνήσεις. Ωστόσο, οι κυβερνήσεις αυξάνουν ολοένα και περισσότερο τον ρόλο τους στον κυβερνοχώρο, οδηγώντας σε μια αναδιανομή της εξουσίας όπου τα κράτη δεν ανταγωνίζονται μόνο με άλλα ενδιαφερόμενα μέρη, αλλά και μεταξύ τους. Έτσι, όλοι οι χρήστες του κυβερνοχώρου αντιμετωπίζουν μια μάχη για την εξουσία μεταξύ των κρατών που επηρεάζει τον ιδιωτικό τομέα και την κοινωνία των πολιτών, την πολυμερή προσέγγιση για τη διαχείριση των πόρων του Διαδικτύου και, συνεπώς, τον ευρύτερο κυβερνοχώρο.

Η παραδοσιακή κατανόηση της ισορροπίας της εξουσίας, όπου τα κράτη επιδιώκουν την επιβίωση ως ανεξάρτητες οντότητες σε ένα άναρχο παγκόσμιο σύστημα, φαίνεται να προκαλεί ιδιαίτερες προκλήσεις όταν μετεξελίσσεται σύμφωνα με την έννοια της κυβερνοεξουσίας. Σε ένα σύγχρονο κόσμο η περιορισμένη χρήση της στρατιωτικής παρέμβασης για ισορροπία απαιτεί τη διεύρυνση της παραδοσιακής στρατιωτικής αντίληψης για να συμπεριλάβει ένα ευρύτερο φάσμα μέσων - συμπεριλαμβανομένων όχι μόνο οικονομικών αλλά και παραγόντων "μαλακής εξουσίας". Η πρόκληση είναι ότι στον κυβερνοχώρο πολλά (αλλά όχι όλα) από τα παραδοσιακά ρεαλιστικά μέτρα εξουσίας του κράτους δεν φαίνεται να αντέχουν, και είναι, επομένως, απαραίτητο να αναθεωρήσουμε τι σημαίνει η εξουσία στον κυβερνοχώρο.

Η ισορροπία των δυνάμεων και η στρατιωτική ισορροπία της εξουσίας στον κυβερνοχώρο περιπλέκεται περαιτέρω από χαρακτηριστικά που είναι μοναδικά καθώς η επιτυχία μιας επίθεσης αντικατοπτρίζει περισσότερο τη συνολική ποιότητα της άμυνας παρά την ποιότητα της επίθεσης. Οι επιθετικές ικανότητες είναι πολύ φθηνότερες και πιο εύκολο να αναπτυχθούν και να εφαρμοστούν από το άθροισμα των απαραίτητων μέτρων άμυνας. Επιπλέον, η διαφορά μεταξύ αμέσου

προετοιμασίας για επίθεση και απλής κατασκοπείας μπορεί να είναι δύσκολο να διακριθεί για τον αμυνόμενο, κάτι που κάνει δύσκολη την ερμηνεία της πρόθεσης. Αντίθετα από τα συμβατικά όπλα, τα "κυβερνο-όπλα" μπορούν να επαναχρησιμοποιηθούν αλλά μπορεί να καταστούν άχρηστα μόλις επιλυθεί η ευπάθεια. Μπορούν επίσης να επαναχρησιμοποιηθούν από το θύμα ή από άλλο μέρος που έχει πρόσβαση στην τεχνολογία. Επιπλέον, δεν υπονομεύουν μόνο την ασφάλεια του στόχου, αλλά και θέτουν σε κίνδυνο την ασφάλεια άλλων φορέων που χρησιμοποιούν συστήματα με τις ίδιες ευπάθειες. Αυτά τα εργαλεία είναι συγκεκριμένα - τα αποτελέσματα εξαρτώνται από το δίκτυο του θύματος - και μπορεί να είναι άμεσα ή μετά από χρονική καθυστέρηση.

Η συμβολή του Οργανισμού Ηνωμένων Εθνών σε αυτό το πλαίσιο αποτελεί την συγκρότηση της πρώτης επιτροπής της Γενικής Συνέλευσης του ΟΗΕ, η οποία ασχολείται με θέματα εξοπλισμών και διεθνούς ασφάλειας, και τη συμβολή των κρατών σε αυτήν τη διαδικασία. Πιο συγκεκριμένα, οι προσπάθειες των κρατών στο πλαίσιο του ΟΗΕ απαιτούν την εμπλοκή και άλλων ενδιαφερομένων φορέων, όπως ο ιδιωτικός τομέας, οι ακαδημαϊκοί και οι οργανώσεις της κοινωνίας των πολιτών, στις διαδικασίες που αφορούν τις διεθνείς στρατηγικές ασφάλειας στον κυβερνοχώρο. Τρεις σημαντικές προσπάθειες στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών στοχεύουν στην ανάπτυξη διεθνών κανόνων και συνεργασίας για την ασφάλεια στον κυβερνοχώρο.Ειδικότερα η Ομάδα Κυβερνητικών Εμπειρογνωμόνων του ΟΗΕ (GGE) και η Ανοιχτή Ομάδα Εργασίας (OEWG) η οποίες ιδρύθηκαν το 2010 και έχουν συνεδριάσει πέντε φορές, εκδίδοντας τρεις αναφορές συναίνεσης οι οποίες προτείνουν κανόνες, μέτρα εμπιστοσύνης και πρωτοβουλίες για τη μείωση του κινδύνου παρερμηνείας στον κυβερνοχώρο. Η Ομάδα προτείνει επίσης την εφαρμογή του διεθνούς δικαίου στις κυβερνοεπιθέσεις. Επιπλέον, τα κράτη μέλη της Οργάνωσης Συνεργασίας της Σανγκάης (SCO)έχουν κυκλοφορήσει ένα προσχέδιο διεθνούς κώδικα συμπεριφοράς για την ασφάλεια των πληροφοριών στη Γενική Συνέλευση του ΟΗΕ. Ο κώδικας προτείνει την εθελοντική αποχή από τη χρήση των ΤΠΕ για δραστηριότητες που αντίκεινται στη διατήρηση της διεθνούς ειρήνης και ασφάλειας. Το 2003, η Γενική Συνέλευση ενέκρινε μια ψήφιση που καλεί τα κράτη να δημιουργήσουν μια κουλτούρα κυβερνοασφάλειας με την ευαισθητοποίηση των εγχώριων ενδιαφερομένων και τη λήψη μέτρων για την αντιμετώπιση των κυβερνοαπειλών. Αυτές οι πρωτοβουλίες στοχεύουν στην ενίσχυση της διεθνούς

συνεργασίας και στην εξέλιξη κανόνων και προτύπων για τη διαχείριση των κυβερνοαπειλών και την προώθηση της ασφάλειας στον κυβερνοχώρο.

Οι προσπάθειες των διεθνών οργανισμών και των περιφερειακών οργανισμών να βελτιώσουν τη διεθνή ασφάλεια και σταθερότητα στον κυβερνοχώρο περιλαμβάνει επίσης τον Οργανισμό για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (OSCE) ο οποίος εργάζεται για την ανάπτυξη μέτρων εμπιστοσύνης σε περιφερειακό επίπεδο για την ασφάλεια των πληροφοριών το Φόρουμ Ασφάλειας της Νοτιοανατολικής Ασίας (ARF) το οποίο εργάζεται πάνω σε παρόμοια μέτρα εμπιστοσύνης για την ασφάλεια των πληροφοριών, η συμφωνία Wassenaar η οποία προσπαθεί να ρυθμίσει την εξαγωγή και τον έλεγχο εξοπλισμού και λογισμικού. Παρά τις προσπάθειες αυτές, η ανάπτυξη κοινών κανόνων και νομικών ερμηνειών για την διεθνή ασφάλεια και σταθερότητα στον κυβερνοχώρο παρουσιάζει δυσκολίες. Η εφαρμογή ενός πλαισίου ισορροπίας της δύναμης θα μπορούσε να είναι μέσω του πεδίου του ελέγχου των εξοπλισμών, αλλά αυτό θα ήταν εξαιρετικά δύσκολο να επιτευχθεί λόγω των διαφορών στην κατανόηση των κυβερνοαπειλών και των διαφορών στην ερμηνεία του διεθνούς δικαίου μεταξύ των κρατών.

4. Συμπεράσματα

4.1 Ανασκόπηση των βασικών ευρημάτων

Το Διαδίκτυο αποτελεί ένα κλασικό παράδειγμα κυριαρχίας, ενώ οι πληροφορίες ρέουν ελεύθερα πέρα από τα εθνικά σύνορα χωρίς σημαντικούς περιορισμούς. Αυτό δημιουργεί προκλήσεις στον τρόπο που οι κυβερνήσεις ασκούν την εξουσία τους στον κυβερνοχώρο και προκαλεί συγκρούσεις μεταξύ των εθνικών και διεθνών συμφερόντων. Οι προσπάθειες ελέγχου του Διαδικτύου από μεμονωμένα κράτη προκαλούν συχνά αντιδράσεις και αντιφάσεις, καθώς προσπαθούν να εξασφαλίσουν την ασφάλεια και την επιρροή τους στον κυβερνοχώρο ενώ ταυτόχρονα επιδιώκουν να επωφεληθούν από την ελεύθερη ροή πληροφοριών για οικονομικούς και κοινωνικούς σκοπούς. Το μοντέλο διακυβέρνησης του Διαδικτύου περιλαμβάνει πολλούς οργανισμούς και ενδιαφερόμενους φορείς που συνεργάζονται για την λήψη αποφάσεων. Αυτοί οι φορείς συνεργάζονται με διεθνείς οργανισμούς και κυβερνήσεις για τη διαμόρφωση διεθνών προτύπων και κανόνων που αφορούν το Διαδίκτυο. Παράλληλα, οι προκλήσεις που αντιμετωπίζονται στον κυβερνοχώρο απαιτούν στρατηγικές που εξισορροπούν την ασφάλεια, την ιδιωτικότητα, την ελευθερία και τη διαφάνεια, προκειμένου να διατηρηθεί η λειτουργία και η ανάπτυξη του Διαδικτύου ως παγκόσμιου δικτύου επικοινωνίας και πληροφοριών. Αυτή η διαδικασία αναπόφευκτα εμπεριέχει διαπραγματεύσεις και συμβιβασμούς μεταξύ διαφορετικών ενδιαφερόμενων μερών και απαιτεί συνεργασία τόσο εντός όσο και εκτός εθνικών συνόρων.

Η φύση των κυβερνοεπιθέσεων καθιστά δύσκολη την εφαρμογή αρχών όπως η προδοσία και η ουδετερότητα. Καθώς οι επιθέσεις μπορούν να προέρχονται από ανώνυμους ή μυστικούς επιτιθέμενους και να διεξάγονται μέσω υποδομών που διασχίζουν πολλές χώρες. Σημαντικά ζητήματα για επίλυση αποτελούν η ανάγκη για διεθνή συνεργασία και συμφωνίες για την αντιμετώπιση των κυβερνοεπιθέσεων, καθώς και η ανάγκη για ενημερωμένα πλαίσια και συμφωνίες που να αντιμετωπίζουν την πολυπλοκότητα της ουδετερότητας στον κυβερνοχώρο. Η άποψη των Ηνωμένων Πολιτειών ως προς τον κυβερνοχώρο είναι ιδιαίτερα σημαντική λόγω της τεχνολογικής τους πρωτοπορίας και της οικονομικής και στρατιωτικής τους ισχύος. Οι ΗΠΑ έχουν επισημάνει τη σημασία της προστασίας κρίσιμων υποδομών, όπως τα μέσα μεταφοράς, και την ύπαρξη κυβερνοκυριαρχίας, ενώ παράλληλα αναγνωρίζουν

την ανάγκη συμμόρφωσης με διεθνείς υποχρεώσεις και σεβασμό των δικαιωμάτων του ανθρώπου. Επίσης, προτείνουν τη δημιουργία διεθνών μηχανισμών για την αντιμετώπιση κυβερνοαπειλών και την προώθηση της κυβερνοασφάλειας σε παγκόσμιο επίπεδο. Συνολικά, οι ΗΠΑ παίζουν κρίσιμο ρόλο στον κυβερνοχώρο τόσο από πολιτικής όσο και από τεχνολογικής πλευράς, επηρεάζοντας την διεθνή κυβερνοασφάλεια και προωθώντας πρωτοβουλίες για τη δημιουργία πολυμερών μηχανισμών και την ενίσχυση τους παγκοσμίως.

Για την Ρωσία η κυβερνοδιπλωματία έχει γίνει ένας τρόπος επαναδιεκδίκησης και αναβάθμισης του παγκόσμιου ρόλου της Ρωσίας, η οποία προανήγγειλε μια πιο ενεργή διεθνή πολιτική από το Κρεμλίνο. Ο τομέας της παγκόσμιας διακυβέρνησης του Διαδικτύου παρέχει ένα νέο έδαφος νομιμοποίησης. Η Ρωσία φαίνεται να ακολουθεί μια διπλή στρατηγική, που συνδυάζει την επιδίωξη της κυβερνοασφάλειας με το ρόλο της ως μεγάλης δύναμης στον κυβερνοχώρο. Η Ρωσία επιχειρεί να αυξήσει την επίπτωση των κυβερνοαπειλών, προβάλλοντας τα ψηφιακά γεγονότα ως σοβαρές απειλές για την ασφάλεια. Συγχρόνως, διαδραματίζει τον ρόλο της ως δύναμη που μπορεί να αντιμετωπίσει αυτές τις απειλές, ενισχύοντας έτσι την εικόνα της ως ηγέτιδα δύναμη στον κυβερνοχώρο. Επιπλέον, η Ρωσία εκμεταλλεύεται την ανησυχία για την ασφάλεια στον κυβερνοχώρο προκειμένου να προωθήσει την ιδέα της παγκόσμιας ρύθμισης του διαδικτύου. Η προσέγγιση αυτή αποσκοπεί στην αποτροπή της υποτιθέμενης υπεροχής του δυτικού συστήματος και στην ενίσχυση της διεθνούς επιρροής της Ρωσίας. Τέλος, η Ρωσία προωθεί μια ερμηνεία του διεθνούς δικαίου που εξυπηρετεί τα συμφέροντά της ως μεγάλης δύναμης στον κυβερνοχώρο. Αυτή η ερμηνεία επικεντρώνεται στην κυριαρχία των κρατών και απορρίπτει την έννοια του ατόμου ως υποκειμένου του διεθνούς δικαίου.

Η Κίνα από την άλλη υιοθετεί μια προσέγγιση στον κυβερνοχώρο που συνδυάζει την έννοια της κυριαρχίας των κρατών με τον ρόλο των stakeholders. Αυτό περιλαμβάνει την αναγνώριση της σημασίας της ενεργού υπεράσπισης της κυριαρχίας στον κυβερνοχώρο από μέρους της Κίνας, αλλά και την προσπάθεια για συνεργασία και διεθνή διακυβέρνηση με βάση δημοκρατικά και διαφανή κριτήρια. Συγκεκριμένα, η Κίνα εκφράζει την άποψη ότι ο κυβερνοχώρος είναι ένας τομέας όπου επικρατούν οι κυριαρχικές αρχές των κρατών, και κάθε κράτος έχει το δικαίωμα να καθορίζει την πολιτική του για τον κυβερνοχώρο εντός των συνόρων του. Ταυτόχρονα, υποστηρίζει την ανάγκη για διεθνή συνεργασία και διακυβέρνηση βασισμένη σε πολυμερή και δημοκρατικά κριτήρια. Η πρόταση της Κίνας για την ανάπτυξη και ασφάλεια του

Διαδικτύου περιλαμβάνει ενίσχυση της διεθνούς συνεργασίας, τον σεβασμό του κυβερνοχώρου ως βασικής αρχής, την προστασία των δεδομένων και των δικτύων από κυβερνοεπιθέσεις, καθώς και τη διάδοση των πολιτισμών μέσω του Διαδικτύου. Τέλος, η Κίνα έχει θεσπίσει νόμους για την ασφάλεια του Διαδικτύου και την προστασία του κυβερνοχώρου, που θέτουν τα θεμέλια για τη νομική προστασία και εποπτεία του κυβερνοχώρου στη χώρα.

4.2 Προτάσεις για τη διαχείριση των προκλήσεων στο μέλλον

Προκειμένου να αντιμετωπιστούν οι προκλήσεις που συνδέονται με τον ψηφιακό χώρο και να δημιουργηθούν νέα θεωρητικά πλαίσια για την κατανόηση και ανάλυσή του, υπάρχει η ανάγκη για πιο αποτελεσματικούς μηχανισμούς διακυβέρνησης του Διαδικτύου προκειμένου να αντιμετωπιστούν οι προκλήσεις που σχετίζονται με την ασφάλεια, την ιδιωτικότητα και την προστασία των δεδομένων. Η αποτελεσματική χρήση και διαχείριση του ψηφιακού χώρου, προκειμένου να επιτευχθεί παγκόσμια συνεργασία και κατανόηση απαιτεί διαπολιτισμική προσέγγιση για την κατανόηση των διαφορετικών πολιτισμών και αντιλήψεων. Επιπλέον, υφίσταται η ανάγκη για προστασία των ανθρωπίνων δικαιωμάτων στον ψηφιακό χώρο, συμπεριλαμβανομένης της ελευθερίας του λόγου, της ιδιωτικότητας και της προστασίας από την κυβερνο-παρακολούθηση. Τέλος, απαιτείται συνεργασία και κοινοποίηση πληροφοριών μεταξύ κρατών και διεθνών οργανισμών για την αντιμετώπιση κοινών απειλών και προκλήσεων στον ψηφιακό χώρο.

Μια προσέγγιση βασισμένη σε εισβολές για την αξιολόγηση των παραβιάσεων της εδαφικής κυριαρχίας στον κυβερνοχώρο παρέχει ένα σαφέστερο και πιο προβλέψιμο πλαίσιο για τη λειτουργία των κρατών. Διαπιστώνεται η ανάγκη για ένα σαφές και λειτουργικό κριτήριο για την αξιολόγηση των παραβιάσεων της εδαφικής κυριαρχίας στον κυβερνοχώρο. Η προσέγγιση που βασίζεται στην εισβολή, που εστιάζει σε τεχνικές πτυχές και όχι σε φυσικά αποτελέσματα, μπορεί να χαρακτηριστεί ως πιο βιώσιμο εργαλείο για την επίτευξη σαφήνειας και προβλεψιμότητας. Το κριτήριο της εισβολής ευθυγραμμίζεται με την ουσία της εδαφικής κυριαρχίας, η οποία αφορά τη ρύθμιση της πρόσβασης στην επικράτεια και τη διατήρηση της αποκλειστικότητας της κρατικής εξουσίας εντός των συνόρων της. Εστιάζοντας στην εισβολή, η προσέγγιση είναι ανεξάρτητη από την πρόθεση του

επιτιθέμενου κράτους και τις συνέπειες των πράξεών του. Η βάση της αξιολόγησης των παραβιάσεων της εδαφικής κυριαρχίας στην εισβολή επιτρέπει στα κράτη στόχους να απαιτούν παύση και να θεσπίσουν αντίμετρα πριν πραγματοποιηθούν οι επιβλαβείς συνέπειες των επιχειρήσεων στον κυβερνοχώρο. Αυτή η έγκαιρη ένδικη προσφυγή θεωρείται σημαντικό πλεονέκτημα της προτεινόμενης προσέγγισης. Η προσέγγιση που βασίζεται στην εισβολή αντιστοιχεί με μεγαλύτερη ακρίβεια στην τεχνική πλευρά των επιχειρήσεων στον κυβερνοχώρο. Εστιάζοντας στην ίδια την πράξη της εισβολής και όχι στα αποτελέσματά της, η προσέγγιση θεωρείται ότι αντικατοπτρίζει περισσότερο την πραγματικότητα των δραστηριοτήτων στον κυβερνοχώρο. Ουσιαστικά θα πρέπει να ενθαρρύνεται η συνεχή εξερεύνηση και συζήτηση νέων ιδεών σχετικά με την ερμηνεία και την εφαρμογή του διεθνούς δικαίου στον κυβερνοχώρο. Φόρουμ όπως η Ομάδα Κυβερνητικών Εμπειρογνωμόνων και η Ανοιχτή Ομάδα Εργασίας είναι κατάλληλες πλατφόρμες για τέτοιες συζητήσεις.

Βιβλιογραφία

Adams, J., & Albakajai, M. (2016). Cyberspace: A new threat to the sovereignty of the state. *Management Studies*, *4*(6). https://doi.org/10.17265/2328-2185/2016.06.003

Assaf, A., Moshnikov, D., Assaf, A., Moshnikov, D., & 'International Law in the Digital Age' Research and Study Group. (2020). Contesting sovereignty in cyberspace. *International Cybersecurity Law Review*, *1*(1–2), 115–124. https://doi.org/10.1365/s43439-020-00004-5

Assembly, U. G. (2015). Developments in the field of information and telecommunications in the context of international security. *United Nations General Assembly*.

Atkins, J. W. (2023). Cicero on the Justice of War. Power and Persuasion in Cicero's. *Philosophy*, 170–204.

Barry, A. (1996). Lines of communication and spaces of rule. In A. Barry, T. Osborne, & N. Rose (Eds.), *Foucault and political reason: Liberalism, neoliberalism, and rationalities of government*. University of Chicago Press.

Bateman, J. (2022, December 16). *Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

Betz, D. J., & Stevens, T. (2011). Chapter two: Cyberspace and sovereignty. *Adelphi Series*, *51*(424), 55–74. https://doi.org/10.1080/19445571.2011.636955

Bing, J. (2009). Building cyberspace: a brief history of Internet. In *Internet Governance* (pp. 8–47). Oxford University Press.

Build, promote, and defend the Internet. (2017, May 16). Internet Society. https://www.internetsociety.org/

Bull, H. (2017). The importance of Grotius in the study of international relations. In *Grotius and Law* (pp. 317–345).

Burchell, G., Gordon, C., & Miller, P. (1991). *The Foucault effect: Studies in governmentality*.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*.

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. *Revista de Administratie Publica Si Politici Sociale*, *12*(1).

Corn, C. (retired) G., & Jensen, E. (2018, June 8). *The technicolor zone of cyberspace, part 2*. Just Security. https://www.justsecurity.org/57545/technicolor-zone-cyberspa

Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. *AJIL Unbound*, *111*, 207–212. https://doi.org/10.1017/aju.2017.57

Craig, A. J., & Valeriano, B. (2018). Realism and cyber conflict: Security in the digital age. *Realism in Practice*, *85*.

Cyber-Interference in the 2016 U.S. Presidential Election: A Crisis Analysis Case Study. (n.d.).

Cyberpolitics in international relations. (2013). *Choice (Chicago, Ill.)*, *50*(12), 50-6993-50–6993. https://doi.org/10.5860/choice.50-6993

Daricili, A., & Burak, B. (2018). Analysis of the cyber security strategies of people's republic of china. *Güvenlik Stratejileri Dergisi*, *14*, 1–35.

Dinstein, Y. (2012). The principle of distinction and cyber war in international armed conflicts. *Journal of Conflict and Security Law*, *17*(2), 261–277. https://doi.org/10.1093/jcsl/krs015

Dziwisz, D., & Romaniuk, S. N. (2023). *The Handbook of Homeland Security*. CRC Press.

Equifax data breach settlement. (2019, July 11). Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Fruhlinger, J. (2020, February 12). *The OPM hack explained: Bad security practices meet China's Captain America*. CSO Online. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Goldsmith, S., & Eggers, W. D. (2005). *Governing by network: The new shape of the public sector*. Rowman & Littlefield.

Gori, U. (2018). The Balance of Power in Cyberspace. In *Confronting an axis of cyber?: China, Iran* (pp. 143–160). North Korea.

Heath, N. (2008, October 31). *How hackers were thwarted at the Beijing Olympics*. ZDNET. https://www.zdnet.com/article/how-hackers-were-thwarted-at-the-beijing-olympics-5000245439/

Hertogen, A. (2014). Letting lotus bloom. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2629681

Higle, J. L., & Sen, S. (1991). Stochastic Decomposition: An Algorithm for Two-Stage Linear Programs with Recourse. *Operations Research*, *39*(6), 946–955.

Home. (n.d.). IETF. Retrieved April 28, 2024, from https://www.ietf.org/

Hughes, R. (2010). A treaty for cyberspace. *International Affairs*, *86*(2), 523–541. https://doi.org/10.1111/j.1468-2346.2010.00894.x

International Committee of the Red Cross. (2021, February 25). *Cyber Warfare: does International Humanitarian Law apply?* International Committee of the Red Cross. https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law

Internet corporation for assigned names and numbers (ICANN). (n.d.). Icann.org. Retrieved April 28, 2024, from https://www.icann.org/en

Kapustin, A. (2023). State sovereignty in cyberspace: International legal dimension. *Journal of Foreign Legislation and Comparative Law*, *18*(6), 1–1. https://doi.org/10.12737/jflcl.2022.079

Kremer, J. F., & Müller, B. (Eds.). (2013). *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media.

Kremer, J.-F., & Muller, B. (Eds.). (2013). *Cyberspace and International Relations: Theory, Prospects and Challenges* (2014th ed.). Springer.

Kumar, K., & Castells, M. (1997). The information age: Economy, society and culture. Volume I. the rise of the network society. *The British Journal of Sociology*, *48*(3), 524. https://doi.org/10.2307/591145

Law, J., & Bijker, W. E. (1992). Postscript: Technology, stability, and social theory. In W. E. Bijker & J. Law (Eds.), *Shaping technology/building Society: Studies in sociotechnical change* (pp. 290–308). MIT Press.

Malinowski, B. (1941). An anthropological analysis of war. *American Journal of Sociology*, *46*(4), 521–550.

Mathiason, J. (2008). *Internet governance: The new frontier of global institutions*. Routledge.

Mueller, M. (2009). Internet governance: Infrastructure and institutions. *Journal of the American Society for Information Science and Technology*, *61*(7), 1511–1512. https://doi.org/10.1002/asi.21289

Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. Mit Press.

Nussbaum, B., & Turcotte, B. (2020). Cyber-Interference in the 2016 US Presidential Election: A Crisis Analysis Case Study. In *Oxford Research Encyclopedia of Politics*.

Nye, J. S., Jr, & S, N. J., Jr. (2004). *Power in the Global Information Age*. Routledge.

Plotkin, R. (2020). *Privacy, security, and cyberspace*. Chelsea House Publications.

Radu, R. (2013). Power technology and powerful technologies: global governmentality and security in the cyberspace. In *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 3–20). Springer.

Sahinidis, N. V. (2004). Optimization Under Uncertainty: State-of-the-Art and Opportunities. *Computers & Chemical Engineering*, *28*(6–7), 971–983.

Sanger, D. E. (2020, December 13). Russian hackers broke into federal agencies, U.s. officials suspect. *The New York Times*. https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Schmitt, M. N., & Vihul, L. (2016). Respect for sovereignty in cyberspace. *Tex. L. Rev*, *95*.

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324. https://doi.org/10.1080/17544750.2016.1206028

Singer, P. W., & Friedman, A. (2014). Cybersecurity: What everyone needs to know. *Oup Usa*.

Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, A. (2019). *The global cyber-vulnerability report the global cyber-vulnerability report*. Springer International Publishing.

United States Senate, Select Committee on Intelligen (senate), & United States Congress. (2020). *USA PATRIOT Act*. Independently Published.

Van Den Berg, B. (Ed.). (2020). *Governing cyberspace: Behavior, power and diplomacy*. Rowman & Littlefield Publishers.

Von Clausewitz, C. (2022). *On war*. Svarog Books.

Wright, J. (2018). Cyber and international law in the 21st century. *Chatham House*, *23*.

Wright, Q. (1983). *A Study of War*. University of Chicago Press.

(N.d.-a). Iana.org. Retrieved April 28, 2024, from http://www.iana.org/about/informational-booklet.pdf

(N.d.-b). Iab.Org. Retrieved April 28, 2024, from https://www.iab.org/