ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΙΣ ΔΙΕΘΝΕΙΣ ΚΑΙ ΕΥΡΩΠΑΪΚΕΣ ΣΠΟΥΔΕΣ

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ:

«Τα ανθρώπινα δικαιώματα στον κυβερνοχώρο υπό το πρίσμα του διεθνούς δικαίου»

Διονυσία Γούργαρη

Α.Μ. 16005

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:

ΑΝΔΡΕΑΣ ΛΙΑΡΟΠΟΥΛΟΣ

ΣΕΠΤΕΜΒΡΙΟΣ 2021

Το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος. / the intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

(υπογραφή)

Αφιερωμένη στους γονείς και τα αδέλφια μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κύριο Ανδρέα Λιαρόπουλο για την πολύτιμη καθοδήγηση, βοήθεια και υπομονή του σε όλες τις δυσκολίες που αντιμετώπισα κατά τη διάρκεια της πορείας εκπόνησης της διπλωματικής μου εργασίας, για το σημαντικό βιβλιογραφικό υλικό που μου υπέδειξε καθώς και για την άμεση ανταπόκρισή του σε κάθε επικοινωνία που είχαμε. Στο σημείο αυτό, θα ήθελα να ευχαριστήσω θερμά και τους υπόλοιπους καθηγητές και καθηγήτριες του μεταπτυχιακού μου προγράμματος για την παροχή σημαντικών επιστημονικών γνώσεων και πληροφοριών μέσω των οποίων διεύρυνα τους πνευματικούς μου ορίζοντες και απέκτησα μία διαφορετική οπτική γωνία του σημερινού γίγνεσθαι.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Τα τελευταία χρόνια η καθημερινότητα του σύγχρονου ανθρώπου είναι άμεσα συνδεδεμένη με την καθιέρωση και επέκταση της χρήσης του Διαδικτύου στους περισσότερους-αν όχι σε όλους- τομείς της ζωής του. Το Διαδίκτυο ή αλλιώς Internet προσφέρει με το πάτημα απλά ενός κουμπιού όλες τις απαραίτητες πληροφορίες που χρειάζονται οι πολίτες των χωρών που έχουν πρόσβαση σε αυτό προκειμένου να διαμορφώσουν την κοινωνική, οικονομική, πολιτική, πολιτισμική και ακαδημαϊκή πτυχή του τρόπου ζωής τους καθώς και να ενημερώνονται ελεύθερα, καθημερινά και άμεσα για ο,τιδήποτε οι ίδιοι επιθυμούν ανεξαρτήτως του χρόνου και του χώρου στον οποίο βρίσκονται.

Η ψηφιακή εποχή πρόσφερε στους χρήστες του Διαδικτύου την απαραίτητη ελευθερία αναζήτησης και διαθεσιμότητας πληθώρας γνώσεων και πληροφοριών απαραίτητων για την εξέλιξη και αναβάθμιση της ποιότητας της καθημερινότητας τους ενισχύοντας την ανάπτυξη συνεργασίας και επικοινωνίας ανάμεσα τόσο σε πολίτες όσο και χώρες σε ολόκληρη την υφήλιο. Ωστόσο, κατά την διάρκεια των δύο τελευταίων δεκαετιών παρατηρείται σε έντονο βαθμό η διαπίστωση ότι ο τρόπος με τον οποίο πραγματοποιείται η αντιμετώπιση και χρήση των εκτεταμένων υπηρεσιών του Διαδικτύου είναι διαφορετικής νοοτροπίας και στοχοθεσίας σε ένα Δημοκρατικό πολίτευμα από ένα πιο αυταρχικό – πιο ολοκληρωτικό- καθεστώς άλλης χώρας. (Sharp Gary Walter)

Πιο συγκεκριμένα, το Διαδίκτυο ενίσχυσε τα ατομικά δικαιώματα όπως την αίσθηση της ελευθερίας των πολιτών των δημοκρατικών χωρών για ενημέρωση, μόρφωση, ελεύθερη επικοινωνία, έκφραση και δημοσίευση των προσωπικών τους ιδεολογιών και απόψεων στον κυβερνοχώρο προσδίδοντάς τους περισσότερες ικανότητες και δύναμη για δράση, ελεύθερη κριτική ικανότητα και επιλογή. Αντιθέτως, οι πολιτικοί ηγέτες των χωρών οι οποίες κυβερνούνται από αυταρχικά – ολοκληρωτικά καθεστώτα χρησιμοποίησαν με διαφορετικό τρόπο το Διαδίκτυο με σκοπό να μετατρέψουν την ελεύθερη διακίνηση ιδεών και γνώσεων σε μετάδοση ψευδών ειδήσεων και

προπαγανδιστικών νοοτροπιών και απόψεων έχοντας ως απώτερο σκοπό την περαιτέρω εγκαθίδρυση του πολιτικού τους συστήματος, τον έλεγχο του πληθυσμού των χωρών τους σε γνωστικό και λειτουργικό επίπεδο καθώς και τον αποκλεισμό τους από το δικαίωμα για εξέφραση των ιδεών τους σε δημόσιο επίπεδο σε ιστοσελίδες του Κυβερνοχώρου.

Η συγκεκριμένη διαπίστωση μας οδηγεί στην έννοια του Ψηφιακού Αυταρχισμού - θα την αναλύσουμε εκτενέστερα στη συνέχεια - ο οποίος ορίζει ουσιαστικά τον αποπροσανατολισμό από τα αληθή γεγονότα και τη λογοκρισία και επιτήρηση που ασκούν πολλά μη δημοκρατικά πολιτεύματα τα οποία επιθυμούν να εγκλωβίσουν στα σύνορά τους το Διαδίκτυο μετατρέποντάς το από παγκόσμιο σε εθνικό, τον έλεγχο του οποίου εναποθέτουν αποκλειστικά στο κυβερνητικό κόμμα και καθεστώς τους.

Ο ψηφιακός αυταρχισμός (Heintschel von Heinegg Wolff) μετατρέπει σε «πιόνια» τους πολίτες περιορίζοντας ή ακόμα και ακυρώνοντας τα ατομικά δικαιώματα τους με πληθώρα διαφορετικών μέσων και τακτικών απειλώντας αντίστοιχα και το πνεύμα και την ιδεολογία της ίδιας της Δημοκρατίας παγκοσμίως. Επιπρόσθετα, το Διαδίκτυο λόγω της ελευθερίας που προσφέρει και -στην οποία μάλιστα βασίστηκε αρχικά η δημιουργία του- και στην ελεύθερη πρόσβαση οδήγησε στην εκμετάλλευσή του ως τρωτού στοιχείου για ορισμένα άτομα ακόμα και χώρες και πολιτικά κόμματα τα οποία διαρκώς προσπαθούν να υποκλέψουν προσωπικά δεδομένα πολιτών ,επιχειρήσεων ακόμα και υπουργικών δομών προκειμένου να χρησιμοποιήσουν τις πληροφορίες και τις γνώσεις παρασκηνιακά για προσωπικό τους όφελος σε οικονομικό πολιτικό και τεχνολογικό επίπεδο.

Οι γνωστές, λοιπόν, κυβερνοεπιθέσεις ή με άλλα λόγια ο κυβερνοπόλεμος μεταξύ των χρηστών και των χωρών γενικότερα στο πλαίσιο του Διαδικτύου θέτουν μία προβληματική πραγματικότητα και ένα κρίσιμο, αλληλοσυσχετιζόμενο και αλληλοαναιρούμενο δίπολο μεταξύ ελευθερίας και ασφάλειας καθώς όσο αυξάνεται η ελευθερία των πολιτών στο Διαδίκτυο τόσο

μειώνεται η ουσιαστική τους ασφάλεια ενώ όσο αυξάνεται η ασφάλεια τους τόσο περισσότερο περιορίζονται και επιβλέπονται οι κινήσεις και οι δράσεις τους με αποτέλεσμα να μειώνεται η ελευθερία τους, να πλήττονται τα ατομικά τους δικαιώματα και να υπονομεύονται οι πρωταρχικές αξίες της δημοκρατίας απειλώντας την μέσω της ενίσχυσης της προπαγάνδας των αυταρχικών καθεστώτων. Μάλιστα, ο Ψηφιακός Αυταρχισμός έχει λάβει τη μορφή τείχους προστασίας από τις πιθανές κυβερνοεπιθέσεις καλύπτοντας με τον τρόπο αυτό τους πραγματικούς λόγους άσκησης του εις βάρος των πολιτών που ζουν εντός των συνόρων των αυταρχικών καθεστώτων.

Τέλος, τα παραπάνω χαρακτηριστικά στοιχεία και γεγονότα θα αναλυθούν σε βάθος μέσω της μελέτης αντίστοιχων περιπτώσεων όπως είναι οι ΗΠΑ και η Κίνα οι οποίες θα μας οδηγήσουν σε συγκεκριμένα συμπεράσματα και προτάσεις αντιμετώπισης των παραπάνω προβληματικών καταστάσεων της σύγχρονης ψηφιακής εποχής.

ΚΕΦΑΛΑΙΟ 1. ΚΥΒΕΡΝΟΧΩΡΟΣ

1.1. ΟΡΙΣΜΟΣ

Ως Κυβερνοχώρος ορίζεται το περιβάλλον που αποτελείται και διαμορφώνεται από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές. «Όπως διατύπωσε η Λενιώ Μυριβήλη (Λενιώ Μυριβήλη 2020) «*ο κυβερνοχώρος αναφέρεται ως ψηφιακός τόπος της τεχνοεπιστήμης, για άλλους είναι ένας ιδιαίτερος χώρος διεπαφής υποκειμένων, πρακτικών και τεχνολογιών. Μερικές φορές ο κυβερνοχώρος παρουσιάζεται ως χώρος διαφυγής απ΄ την «πραγματικότητα», αφού σε αυτόν μπορούμε να μεταμορφωνόμαστε κατά βούληση. Άλλες φορές πάλι φαντάζει ως υβριδικός χώρος μέσα στον οποίο συμφιλιώνονται και μετουσιώνονται πολιτισμικοί πόλοι».*

Προκειμένου να αναλύσουμε με περισσότερη ακρίβεια τον ορισμό του Κυβερνοχώρου μπορούμε να αναφερθούμε στην ετυμηγορία της ίδιας της λέξης. Σε αυτήν πρωταρχικό ρόλο διαδραματίζει η ελληνική γλώσσα σύμφωνα με την οποία «Κυβερνήτης» είναι ο καπετάνιος, αυτός που διοικεί και ελέγχει ένα πλοίο ενώ «χώρος» είναι στη συγκεκριμένη περίπτωση η θάλασσα και τα χαρακτηριστικά και οι εκάστοτε συνθήκες που τη συνοδεύουν. Ο Κυβερνοχώρος σε αντιστοιχία με τη σύγχρονή του έννοια αναφέρεται στην ικανότητα ενός ατόμου να χειρίζεται, να κατευθύνει και να ελέγχει με δική του πρωτοβουλία και χρησιμοποιώντας απλά τα χέρια του τον ηλεκτρονικό υπολογιστή ο οποίος είναι το μέσο της δημιουργίας της εικονικής πραγματικότητας η οποία αντιπροσωπεύεται από τον ίδιο τον Κυβερνοχώρο.

Ο ορισμός του Κυβερνοχώρου ως λέξη και ως έννοια ,ωστόσο, έλαβε διαφορετικούς εννοιολογικούς σχηματισμούς σε ποικίλους χώρους και χρόνους και από διαφορετικά άτομα. Επικρατέστερος για την απαρχή του ως λέξη ήταν αυτός του συγγραφέα επιστημονικής φαντασίας William Gibson ο οποίος γράφοντας το μυθιστορηματικό του έργο «Νευρομάντης» το 1984 παρέθεσε τον όρο του Κυβερνοχώρου ως εξής στο παρακάτω απόσπασμα (WikiPedia 2021): *«Μία ομόφωνη παραίσθηση που βιώνεται καθημερινά από*

δισεκατομμύρια νόμιμους χρήστες, σε κάθε χώρα ,από παιδιά που μαθαίνουν μαθηματικές αρχές…Μία γραφική απεικόνιση δεδομένων απομονωμένων από κάθε υπολογιστή στο ανθρώπινο σύστημα. Αδιανόητη περιπλοκότητα. Γραμμές φωτός εκτείνονται στο μη -χώρο της διανόησης, ομάδες και αστερισμοί πληροφοριών .Όπως τα φώτα μιας πόλης υποχωρούν…». Πιο συγκεκριμένα έκανε λόγο για ένα φανταστικό σενάριο στο οποίο υπήρχαν οι λεγόμενοι καουμπόη της κονσόλας «- σε αντιστοιχία με τους χάκερ της σύγχρονης εικονικής πραγματικότητας του Διαδικτύου οι οποίοι εισέρχονταν με τα κράνη τους σε τρισδιάστατα εικονικά περιβάλλοντα οπτικοποιώντας ένα παγκόσμιο ψηφιακό δίκτυο πληροφοριών- το σημερινό δηλαδή Internet».

Στον Κυβερνοχώρο οι άνθρωποι ανταλλάσσουν δεδομένα και πληροφορίες και συνδέονται με άλλους υπολογιστές μέσω ενός ευρύτερου και παγκόσμιου Δικτύου δικτύων γνωστού ως Διαδίκτυο ή Internet -για το οποίο θα πραγματοποιηθεί εκτενέστερη ανάλυση στη συνέχεια της έρευνας. Επιπλέον, στον Κυβερνοχώρο -μέσα στον οποίο συμπεριλαμβάνεται η χρήση του Διαδικτύου- πραγματοποιούνται καθημερινά και παγκόσμια καταχωρίσεις δεδομένων και πληροφοριών από όλους τους χρήστες που διαθέτουν ηλεκτρονικό υπολογιστή και πρόσβαση στο Διαδίκτυο. Τράπεζες, δημόσιες και ιδιωτικές επιχειρήσεις, εταιρείες, υπουργεία και φορείς διοικητικών και πολιτικών αρχών, πανεπιστήμια, τηλεπικοινωνίες, στρατιωτικές εγκαταστάσεις και μέσα μεταφοράς καθώς και οι ίδιοι οι άνθρωποι ως μονάδες και όλων των ειδών οι φορείς του σύγχρονης πραγματικότητας αλληλοεπιδρούν και ανταλλάσσουν δεδομένα στο πλαίσιο και την έκταση που προσφέρει με το πάτημα ενός απλά κουμπιού ο Κυβερνοχώρος καθιστώντας διαθέσιμες νέες δυνατότητες και προοπτικές σε ένα ψηφιακό γίγνεσθαι εικονικής πραγματικότητας.(Wikipedia)

1.2. ΜΕΓΕΘΟΣ-ΔΙΑΣΤΑΣΕΙΣ

Αξιοσημείωτο χαρακτηριστικό της έννοιας του Κυβερνοχώρου αποτελεί η διαπίστωση ότι εκπροσωπείται και ορίζεται από το κοινό δίκτυο που συνθέτουν

εκατομμύρια ηλεκτρονικοί υπολογιστές και εκατομμύρια διαφορετικές ιστοσελίδες με ηλεκτρονικό και εικονικό περιεχόμενο το οποίο ανανεώνεται και εμπλουτίζεται καθημερινά από εκατομμύρια χρήστες του Διαδικτύου παγκοσμίως. Σύμφωνα μάλιστα με την έρευνα από το Internet World Stats οι "διαστάσεις" του κυβερνοχώρου αυξάνονται με συστηματικά ραγδαίους ρυθμούς. Πιο συγκεκριμένα, οι χρήστες του Διαδικτύου στις 31 Μαρτίου του 2021 σε παγκόσμιο επίπεδο ανέρχονταν στους 5,168,780,607 (Internet World Stats).Ο Κυβερνοχώρος και το Διαδίκτυο αποτελούν εικονική πραγματικότητα και ο μόνος τρόπος να μετρηθούν ποσοτικά είναι μέσω της μέτρησης των ψηφιακών δεδομένων που ανταλλάσσουν μεταξύ τους οι χρήστες του ανά τον κόσμο καθώς και οι εγκαταστάσεις και υλικοτεχνικές υποδομές που εμπλουτίζονται από τις εταιρίες τηλεπικοινωνιών που κάνουν διαθέσιμη την παροχή και πρόσβαση στο Διαδίκτυο δημιουργώντας τις απαραίτητες τεχνικές συνθήκες για να καθίσταται λειτουργική η χρήση του. Όπως γίνεται κατανοητό το μέγεθος του και η έκταση της εμβέλειας του Κυβερνοχώρου όχι μόνο είναι δύσκολο να συλληφθεί αλλά αυξάνεται με ραγδαίους και ανοδικούς ρυθμούς σε καθημερινή βάση καθώς είναι ευρέως αντιληπτή η άμεση διασύνδεση του ρυθμού της ζωής του σύγχρονου ανθρώπου με την τεχνολογία.

1.3. ΕΛΛΕΙΨΗ ΣΥΝΟΡΩΝ-ΑΝΩΝΥΜΙΑ-ΙΣΧΥΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Είναι αδύνατον να μην προσθέσουμε στα πιο βασικά και σημαντικά χαρακτηριστικά γνωρίσματα του Κυβερνοχώρου το γεγονός ότι δεν διαθέτει φυσικά όρια, ούτε συνοριακούς περιορισμούς καθώς αποτελεί παγκόσμιο φαινόμενο εικονικής πραγματικότητας και είναι διαθέσιμο προς όλους τους πολίτες ανεξαρτήτως έθνους και εθνικότητας, θρησκείας, ηλικίας, χώρου και χρόνου. Επιπρόσθετα, η ελευθερία ακριβώς που προσφέρει δεν αφορά μόνο την απεριόριστη πρόσβαση σε αυτόν και τις υπηρεσίες του αλλά ταυτόχρονα και το γεγονός ότι αποτελεί και ένα απρόσωπο και ανώνυμο μέσο καταχώρησης και ανταλλαγής δεδομένων και πληροφοριών (Gervais Michael, 2005).

Αυτό, λοιπόν, σε συνδυασμό με τη διαπίστωση ότι δεν υπάρχει καμία εξουσιαστική ή ανώτερη αρχή που να λειτουργεί ως ρυθμιστική ισχύς και να επιβάλλει νόμους ή κανόνες ομαλής και αρμονικής λειτουργίας του Κυβερνοχώρου και των πολλαπλών υπηρεσιών του δημιουργεί τις ευνοϊκές συνθήκες για όσους επιθυμούν να αποπροσανατολίσουν, ζημιώσουν και να βλάψουν με διάφορες κακοπροαίρετες ενέργειες άλλους συμπολίτες τους στο πλαίσιο της εικονικής και ενιαίας κοινωνίας του Κυβερνοχώρου με απώτερο σκοπό την ικανοποίηση προσωπικού τους -ή και μη-οφέλους.

Χαρακτηριστικά παραδείγματα αποτελούν τα ζητήματα Κυβερνοασφάλειας που προκύπτουν τις τελευταίες ,κυρίως ,δεκαετίες εξαιτίας των κυβερνοεπίθεσεων που διαδραματίζονται όλο και σε συχνότερο και σοβαρότερο επίπεδο παγκοσμίως μεταξύ πολιτών ατομικά αλλά και κρατών γενικότερα- στοιχεία στα οποία θα γίνει εκτενέστερη αναφορά στη συνέχεια της έρευνας.

ΚΕΦΑΛΑΙΟ 2-ΔΙΑΔΙΚΤΥΟ

2.1. ΟΡΙΣΜΌΣ

Χρησιμοποιώντας τον όρο Διαδίκτυο αναφερόμαστε σε ένα δίκτυο δικτύων το οποίο βασίζεται στη διασύνδεση των υπολογιστών-που έχουν πρόσβαση σε αυτόν-μεταξύ τους. Μέσω του Διαδικτύου οι άνθρωποι μπορούν να μοιραστούν πληροφορίες και δεδομένα καθώς και να επικοινωνήσουν μεταξύ τους από οποιοδήποτε σημείο του κόσμου. Σύμφωνα με την ορολογία των σχολικών βιβλίων της Πληροφορικής: *«Το όνομα Διαδίκτυο είναι μία σύνθετη λέξη που παράγεται από τις λέξεις Διασύνδεση Δικτύων. Στα αγγλικά ο όρος Internet γεννήθηκε από τη συνένωση των λέξεων International Network (Διεθνές Δίκτυο Υπολογιστών).» (Αράπογλου Α. et al., 2017)*

Σύμφωνα με απόσπασμα από την εφημερίδα το Βήμα γίνεται αναφορά για το Διαδίκτυο ως εξής: «Στα μέσα της δεκαετίας του ’80 οι άνθρωποι άρχισαν να βλέπουν τη συλλογή των επί μέρους δικτύων που συναποτελούσαν το ARPANET, το NSFNET και άλλα δίκτυα ως ένα Διαδίκτυο (internetwork) και σύντομα άρχισαν να μιλούν για το Διαδίκτυο (Internet). Δεν υπήρξε κάποια επίσημη τελετή ονοματοδοσίας αλλά ο όρος παραμένει ως σήμερα σε ευρεία χρήση.»

Ένας επιπλέον ορισμός για το Διαδίκτυο εντοπίζεται στην ιστοσελίδα της Βικιπαίδεια ο οποίος προσδιορίζει το βασικό περιεχόμενο της παραπάνω έννοιας σύμφωνα με τα παρακάτω*: «Το Διαδίκτυο (αγγλικά:Internet) είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών , οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται TCP/IP (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί δισεκατομμύρια χρήστες καθημερινά σε ολόκληρο*

τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται Διαδίκτυο.» (Wikipedia, Διαδίκτυο 2021).

2.2. ΑΠΑΡΧΈΣ ΚΑΙ ΙΣΤΟΡΙΚΉ ΕΞΈΛΙΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Στα τέλη της δεκαετίας του 1960 οι σχέσεις μεταξύ Η.Π.Α. και Σοβιετικής Ένωσης που εντείνονταν με μία σειρά γεγονότων κατά τη διάρκεια της χρονικής περιόδου γνωστής ως Ψυχρός Πόλεμος βρίσκονταν σε κρίσιμο σημείο. Με αφορμή την αποστολή στο Διάστημα του δορυφόρου Σπούτνικ 1 από τη Σοβιετική Ένωση, οι Η.Π.Α. αποφάσισαν την έναρξη της διεξαγωγής επιστημονικών ερευνών στις πανεπιστημιακές δομές με σκοπό τη δημιουργία και οργάνωση ενός δικτύου το οποίο θα επέτρεπε την ομαλή και ασφαλή επικοινωνία μεταξύ των στρατιωτικών, πολεμικών καθώς και πολιτικών εγκαταστάσεων -γενικότερα- αλλά κυρίως σε πιθανό ενδεχόμενο πυρηνικής επίθεσης από την Σοβιετική Ένωση.

Το δίκτυο που αποτέλεσε τον βασικό ‘‘πρόγονο’’ του σημερινού Διαδικτύου ονομάστηκε ARPANET και αποτελεί το ακρωνύμιο των παρακάτω λέξεων της αγγλικής γλώσσας: Advanced Research Projects Agency Network. Το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών της Αμερικής το οποίο και χρηματοδότησε για την διεξαγωγή της συγκεκριμένης έρευνας απέκτησε το 1969 την πρόσβαση στο δίκτυο ARPANET.Πιο συγκεκριμένα, η σύνθεση της ιδέας του δικτύου ARPANET βασίστηκε σε 3 διαδοχικές θεωρίες. Όπως αναφέρεται στο σύνδεσμο της Βικιπαίδεια με τον όρο Διαδίκτυο : «*Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ.Λικλάιντερ (J.C.R. Licklider) που ανέφερε σε συγγράμματά του το "γαλαξιακό δίκτυο". Η θεωρία αυτή υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν*

*αποκεντρωμένο έτσι ώστε ακόμη κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Τη λύση σε αυτό έδωσε ο Πολ Μπαράν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλάινροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο.» (*Wikipedia, Διαδίκτυο 2021)

Σε πρώτο στάδιο συνέδεε τέσσερις (4) διαφορετικούς υπολογιστές οι οποίοι ήταν στα παρακάτω συγκεκριμένα κομβικά σημεία: Στο πανεπιστήμιο της Καλιφόρνια στη Σάντα Μπάρμπαρα, στο πανεπιστήμιο της Καλιφόρνια στο Λος Άντζελες, στο SRI στο Στάνφορντ και ,τέλος, στο πανεπιστήμιο της Γιούτα. Με σταδιακό ρυθμό και αυξανόμενες τάσεις το μέγεθος και η μορφή του μεταβλήθηκε στο πέρασμα των χρόνων.Το 1974 πλήθος υπολογιστών αποκτούν πρόσβαση στο ARPANET το οποίο με σκοπό να αποφορτιστεί αποφασίζεται να διαχωριστεί το 1983 σε δύο τμήματα: στο MILNET το οποίο προοριζόταν για επικοινωνίες στρατιωτικού περιεχομένου και στο νέο ARPANET το οποίο απευθυνόταν στην ακαδημαϊκή κοινότητα με κύριο στόχο και μέλημα τη συνέχιση της έρευνας για την εξέλιξη και βελτίωση του δικτύου.

Πολλές χώρες ξεκινούν τις έρευνες για τη δημιουργία άλλων δικτύων ωστόσο το πιο σημαντικό βήμα για την καθιέρωση του Διαδικτύου με τη σημερινή του διαδεδομένη μορφή έγινε από τον Βρετανό Τιμ Μπέρνερς Λη το 1989 στο ερευνητικό ίδρυμα με την ονομασία Ευρωπαϊκός Οργανισμός Πυρηνικών Ερευνών -γνωστό και με την αγγλική ονομασία «CERN». Δημιουργείται και διαδίδεται στον Κυβερνοχώρο και σε όλους τους υπολογιστές που διαθέτουν πρόσβαση στο Διαδίκτυο ο Παγκόσμιος ιστός (αγγλικά: World Wide Web ή www),ο οποίος ορίζεται ως «*ένα ανοιχτό σύστημα διασυνδεδεμένων πληροφοριών και πολυμεσικού περιεχομένου, που επιτρέπει στους χρήστες του Διαδικτύου να αναζητήσουν πληροφορίες μεταβαίνοντας από ένα έγγραφο στο άλλο.»*

Για έναν πληρέστερο ορισμό αλλά και κατανόηση της έννοιας του Παγκόσμιου Ιστού αλλά και της ιδιαίτερης βαρύτητας που η πρόσβαση σε αυτό είχε για την εξέλιξη του Διαδικτύου καλό θα ήταν να παρατεθεί το παρακάτω απόσπασμα σύμφωνα με το οποίο: *«Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το World Wide Web (WWW) (Παγκόσμιο Ιστό)που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC και modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς.»*

2.3. ΜΈΓΕΘΟΣ ΔΙΑΔΙΚΤΎΟΥ

Αν και στο αρχικό του στάδιο το Διαδίκτυο απευθυνόταν σε περιορισμένο κοινό και η λειτουργία του βασίστηκε σε συγκεκριμένους σκοπούς τα οφέλη της χρήσης του για τη διάδοση και μεταφορά πληροφοριών αλλά και ελεύθερης επικοινωνίας μεταξύ των ανθρώπων ακόμα και σε διαφορετικά μέρη σε παγκόσμιο επίπεδο πυροδότησε μία πρωτοφανή έκρηξη της ανάγκης και της εκδήλωσης του ενδιαφέροντος για πρόσβαση σε αυτόν από πλήθος ηλεκτρονικών υπολογιστών. Σύμφωνα με την εφημερίδα «Το Βήμα» : «*Το μέγεθος του δικτύου αυξήθηκε εκρηκτικά. Το 1990 το Διαδίκτυο περιείχε 3.000 δίκτυα και 200.000 υπολογιστές. Το 1992 συνδέθηκε ο πρώτος εκατομμυριοστός υπολογιστής στο δίκτυο. Το 1995 υπήρχαν πολλαπλά κεντρικά δίκτυα-ραχοκοκαλιές (backbones), εκατοντάδες γεωγραφικά δίκτυα όπως το ελληνικό GRnet, δεκάδες χιλιάδες τοπικά δίκτυα, εκατομμύρια*

υπολογιστές και δεκάδες εκατομμύρια χρήστες, με το μέγεθος να διπλασιάζεται περίπου κάθε χρόνο.»

Αντίστοιχα στη σημερινή εποχή του 21ου αιώνα το Διαδίκτυο και οι υπηρεσίες καθώς και οι ιστοσελίδες που περιλαμβάνονται σε αυτόν είναι πραγματικά δύσκολο να συλληφθούν με φυσικούς αριθμούς. Σύμφωνα με απόσπασμα έρευνας που παρατίθεται στο διεπιστημονικό περιοδικό «Interdisciplinary Science Topics" : «*θα χρειαζόταν να κοπούν το 2% των δέντρων στο δάσος του Αμαζονίου, για να τυπωθεί όλος ο Παγκόσμιος Ιστός (Web). Η εκτίμηση αυτή βασίσθηκε στον υπολογισμό ότι για την εκτύπωση μιας μέσης ιστοσελίδας χρειάζονται 30 σελίδες χαρτιού Α4. Αν αυτό έχει κάποια δόση αλήθειας, τότε όλο το Ίντερνετ* θα *χρειαζόταν περίπου 1,36X10^11 σελίδες χαρτιού για να τυπωθεί σε τόμους. Σύμφωνα με μια εναλλακτική εκτίμηση, όλο το Ίντερνετ μπορεί να τυπωθεί σε 305,5 δισεκατομμύρια σελίδες.»(NewSpot 2016)*

ΚΕΦΑΛΑΙΟ 3 – ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

3.1. ΟΡΙΣΜΟΣ

Στη σημερινή εποχή η οντότητά μας ως φυσικές παρουσίες διακρίνονται σε ατομικό και συλλογικό επίπεδο και ανάλογα με το θέμα στο οποίο αναφερόμαστε διακρινόμαστε για την κοινωνική, πολιτική ,θρησκευτική ,επαγγελματική ,πολιτική ταυτότητα μας καθώς και πολλές άλλες. Σε αυτές ,λοιπόν, προστίθεται και η ψηφιακή μας ταυτότητα η οποία είναι μοναδική και ξεχωριστή για κάθε άνθρωπο όπως ακριβώς και για κάθε ηλεκτρονικό υπολογιστή ο οποίος διαθέτει συγκεκριμένη και ξεχωριστή ηλεκτρονική διεύθυνση-γνωστή ως IP address.Η απόλυτη ελευθερία της πρόσβασης του Διαδικτύου εκτός από τα προτερήματα έχει και τα αντίστοιχα μειονεκτήματα της γεγονός από το οποίο απορρέει η ανάγκη προσαρμογής, καθιέρωσης και

υιοθέτησης των ανθρώπινων δικαιωμάτων στο πλαίσιο του Κυβερνοχώρου όπου και ο όρος τους μετατρέπεται σε ψηφιακά δικαιώματα καθώς και υποχρεώσεις των χρηστών του Διαδικτύου (Margulies Peter, 2013).

Στις 16 Ιουνίου 1945 με αφορμή το τέλος των δύο Παγκοσμίων πολέμων και τις τραγικές συνέπειες τους στην ανθρωπότητα αποφασίστηκε στο τέλος των συνδιασκέψεων για τη Διεθνή Οργάνωση, η ανάγκη σύστασης και υπογραφής από τα συμβαλλόμενα κράτη του Χάρτη των Ηνωμένων Εθνών στον Άγιο Φραγκίσκο. Συγκεκριμένα, η ισχύς του περιεχομένου του ξεκίνησε στις 24 Οκτωβρίου 1945.Η πορεία για την διεθνή προστασία των ανθρωπίνων δικαιωμάτων περιλάμβανε πολλές τροποποιήσεις και διαφορετικά κεφάλαια και άρθρα στα οποία αναφέρονται ρητά τα είδη των κυρίαρχων ανθρωπίνων δικαιωμάτων που κάθε άνθρωπος διαθέτει στην κατοχή του ήδη από τη γέννησή του ως ξεχωριστή οντότητα χωρία καμία διάκριση ως προς τη φυλή ,το φύλο, τη γλώσσα ή τη θρησκεία. Προστατεύοντας τον κάθε πολίτη ξεχωριστά τα κράτη με σκοπό να βελτιώσουν ατομικά τη συνείδηση των ανθρώπων υπέρ του αλληλοσεβασμού και της αξιοπρέπειας και προστασίας των δικαιωμάτων τους ,ταυτόχρονα, σκόπευαν και σε μία συλλογική και αρμονική συνεργασία , ομαλή επικοινωνία και επίλυση πολιτικών ,οικονομικών και εδαφικών διαφορών μεταξύ τους υπό το πρίσμα του Διεθνούς Δικαίου. Ορισμένα βασικά θεμελιώδη δικαιώματα αποτελούν η ισότητα όλων των ανθρώπων για ίσες ευκαιρίες και δικαιώματα και ίση αντιμετώπιση, το δικαίωμα της ζωής, την απαγόρευση της δουλείας, το δικαίωμα για απαλλαγή από βασανιστήρια καθώς και το δικαίωμα για δίκαιη δίκη.

3.2. ΨΗΦΙΑΚΑ ΔΙΚΑΙΩΜΑΤΑ

Τα ανθρώπινα δικαιώματα ως γενική έννοια προσαρμόστηκαν και στο επίπεδο της τεχνολογίας καθώς δημιουργήθηκε η ανάγκη να ρυθμιστούν με κανόνες, κώδικες συμπεριφοράς, δικαιώματα και υποχρεώσεις οι συμμετέχοντες στην παγκόσμια ψηφιακή κοινότητα με σκοπό την ομαλή τους συνύπαρξη και επικοινωνία.

Όταν αναφερόμαστε στον όρο ψηφιακά δικαιώματα (Lubell, Noam, 2010) ουσιαστικά αναφερόμαστε στην προέκταση και προσαρμογή των θεμελιωδών ανθρωπίνων δικαιωμάτων του Διεθνούς Δικαίου που σχετίζονται με τη χρήση των ηλεκτρονικών υπολογιστών και των δικτύων επικοινωνίας της σύγχρονης πραγματικότητας δηλαδή κατά κύριο λόγο για τους ηλεκτρονικούς υπολογιστές και την πρόσβαση στο δίκτυο των Δικτύων-το Διαδίκτυο.

Τα ψηφιακά δικαιώματα τα οποία αφορούν τον κάθε άνθρωπο ξεχωριστά είναι πολυάριθμα και αποτελούν ουσιαστικά την προέκταση των ήδη κατοχυρωμένων ανθρώπινων δικαιωμάτων όπως έχουν διατυπωθεί στην Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου καθώς και στο Διεθνές Δίκαιο. Για παράδειγμα, μπορούμε να αναφέρουμε το δικαίωμα για εργασία, για ελεύθερη κρίση και άσκηση του εκλογικού δικαιώματος, το δικαίωμα στην παροχή δημόσιας υγείας και πολλά ακόμα ανάλογα με το θέμα και τον εκάστοτε τομέα που μας αφορά. Τα πιο σημαντικά ,ωστόσο, ανθρώπινα δικαιώματα που συναντάμε στη σύγχρονη ψηφιακή εποχή σχετίζονται με το δικαίωμα των χρηστών του Διαδικτύου για ελεύθερη πρόσβαση και χρήση των πληροφοριών και του περιεχομένου που διατίθενται στον Κυβερνοχώρο και στο δικαίωμα για προστασία της προσωπικής και ιδιωτικής ζωής και ταυτότητας των ατόμων, προστασία των προσωπικών τους δεδομένων και το δικαίωμα προστασίας της πνευματικής ιδιοκτησίας των ατόμων που αλληλοεπιδρούν και συμμετέχουν με οποιοδήποτε τρόπο στο Διαδίκτυο και τα μέσα που αυτό προσφέρει.

Με την πάροδο του χρόνου και την εξέλιξη της τεχνολογίας η καθημερινότητα των ανθρώπων επεκτείνεται σε όλο και περισσότερες δραστηριότητες στο Διαδίκτυο και είναι αναμενόμενο να δημιουργείται όλο και μεγαλύτερη ανάγκη προστασίας και κατοχύρωσης των ψηφιακών -στην προκειμένη περίπτωση- ανθρωπίνων δικαιωμάτων. Τεχνολογικές εφαρμογές, διαδικτυακοί ιστότοποι , ιστοσελίδες και μέσα κοινωνικής δικτύωσης περιέχουν τα προσωπικά στοιχεία της ταυτότητας των ατόμων που τα χρησιμοποιούν ενώ

το συγκεκριμένο γεγονός αφορά αντίστοιχα και δεδομένα κυβερνητικών θεσμών και υπουργείων των χωρών με αποτέλεσμα το Διαδίκτυο να αποτελεί ένα μέσο διάθεσης σημαντικών ατομικών και συλλογικών στοιχείων πολιτών και χωρών.

Με βάση τα παραπάνω στοιχεία κατανοούμε ότι ο Κυβερνοχώρος μετέβαλλε ριζικά το ρυθμό και τις δυνατότητες της οργάνωσης των καθημερινών μας δραστηριοτήτων τόσο θετικά όσο και αρνητικά. Όλα είναι πιο εύκολα και άμεσα προσβάσιμα , ελεύθερα για όλους όμως ταυτόχρονα όλες οι κινήσεις βρίσκονται εκτεθειμένες και ανεξέλεγκτες καθώς η ισχύς στον Κυβερνοχώρο αποτελεί ουτοπία εφόσον δεν υφίσταται κανένα άτομο ή κράτος υπεύθυνο να λογοδοτήσει ή να ελέγξει όσα διαδραματίζονται στον ηλεκτρονικό τομέα του Διαδικτύου.

ΚΕΦΑΛΑΙΟ 4 – ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

4.1. ΟΡΙΣΜΟΣ

Σύμφωνα με το άρθρο του κ. Ανδρέα Λιαρόπουλου Ζητήματα ασφαλείας στον Κυβερνοχώρο: «*Ο κυβερνοχώρος είναι η ραχοκοκαλιά της σύγχρονης κοινωνίας και αποτελεί παγκόσμιο ιστό διασυνδεδεμένων επικοινωνιακών και πληροφοριακών δικτύων, στα οποία είναι αποθηκευμένες πληροφορίες που σχετίζονται με κρίσιμες υποδομές, όπως η υγεία, οι μεταφορές, η ενέργεια και ο χρηματοπιστωτικός τομέας. Οι σύγχρονες κοινωνίες στηρίζονται στα πληροφοριακά και επικοινωνιακά δίκτυα για τη λειτουργία των υποδομών τους και ο υψηλός βαθμός εξάρτησής τους από αυτές τις καθιστά ευάλωτες στις κυβερνοεπιθέσεις. Ο κυβερνοχώρος έχει δημιουργήσει νέο πεδίο δράσης για τα κράτη, τους τρομοκράτες, τους εγκληματίες και τις κοινωνίες και συνεπώς νέο αντικείμενο ασφάλειας».*

Η Κυβερνοασφάλεια τα τελευταία χρόνια με την έξαρση της χρήσης του Διαδικτύου σε όλες τις εκφάνσεις της ζωής μας αποτελεί ξεχωριστό και ανεξάρτητο κεφάλαιο όχι μόνο για τα ίδια τα άτομα ως ιδιωτικοί χρήστες του για προσωπικούς σκοπούς αλλά και για ολόκληρα τα κράτη, τις πολιτικές παρατάξεις, τους διεθνείς οργανισμούς και πολλούς άλλους πολιτικούς και μη θεσμούς σε συλλογικό επίπεδο. Έχουν διατυπωθεί διάφοροι εννοιολογικοί όροι για την περιγραφή της έννοιας της Κυβερνοασφάλειας ανάλογα με τον εκάστοτε φορέα ο οποίος ασχολείται και αναφέρεται σε αυτήν. Σύμφωνα με το Ευρωπαϊκό Ελεγκτικό Συνέδριο: *«Η κυβερνοασφάλεια καλύπτει την πρόληψη και την ανίχνευση κυβερνοπεριστατικών, την αντίδραση σε αυτά και την ανάκαμψη από αυτά. Τα περιστατικά μπορεί να είναι εσκεμμένα ή μη και κυμαίνονται, ενδεικτικά, από την τυχαία κοινολόγηση πληροφοριών έως επιθέσεις κατά επιχειρήσεων και υποδομών ζωτικής σημασίας και την κλοπή δεδομένων προσωπικού χαρακτήρα, ή ακόμη και έως την παρέμβαση σε δημοκρατικές διαδικασίες. Όλα αυτά τα συμβάντα μπορούν να έχουν πολυποίκιλες επιζήμιες επιδράσεις σε πρόσωπα, οργανισμούς και κοινότητες.»*

Τα προτερήματα των υπηρεσιών του Διαδικτύου στον Κυβερνοχώρο κατέστησαν αναγκαία και άμεση τη μέριμνα των κρατών παγκοσμίως για ασφαλή πρόσβαση σε αυτόν καθώς η ελευθερία της σύστασής του αυτομάτως συνδέεται με την έλλειψη προστασίας και με την έκθεση των πληροφοριών και δεδομένων των φορέων του σε μεγάλο ποσοστό. Αποτέλεσμα των παραπάνω είναι η κακόβουλη προσπάθεια επίθεσης από την πλευρά πολλών ιδιωτών - που ασχολούνται επαγγελματικά ή μη με τους ηλεκτρονικούς υπολογιστές- ή ακόμα και ολόκληρων τεχνολογικών και μυστικών υπηρεσιών των ίδιων των κρατών ή πολιτικών παρατάξεων με σκοπό την εξασφάλιση οικονομικού ή πολιτικού ή προσωπικού κέρδους εις βάρος άλλων ατόμων ή κρατών που επιθυμούν να βλάψουν με ποικίλους τρόπους, η παράθεση των οποίων έπεται στη συνέχεια. Συχνά ο όρος Κυβερνοασφάλεια χρησιμοποιείται συμπληρωματικά και με άλλους όπως οι παρακάτω: Κυβερνοέγκλημα, Κυβερνοαπειλή, Κυβερνοπόλεμος, Κυβερνοεπίθεση (Bzostek Rachel).

4.2. ΑΙΤΙΕΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗΣ

Πιο συγκεκριμένα, μία αιτία μπορεί να αποτελεί η προσωπική διαφωνία ή εμπάθεια που ίσως νιώθει κάποιος για ένα συμπολίτη του και επιθυμεί να του υποκλέψει, δημοσιεύσει ή καταστρέψει προσωπικά δεδομένα και στοιχεία που πιθανόν να διαθέτει στον προσωπικό του υπολογιστή. Επιπρόσθετα , ένα ακόμα κίνητρο για μία κυβερνοεπίθεση είναι το κέρδος, τακτική την οποία συνήθως ακολουθούν ιδιωτικές εταιρίες προκειμένου να υποκλέψουν ερευνητικά στοιχεία από τον ανταγωνιστή τους ή να του προκαλέσουν οικονομική ζημιά προσβάλλοντας τις σημαντικές πληροφορίες που διατίθενται στο δίκτυο των υπολογιστών του. Μπορούμε να προσθέσουμε και ένα ακόμα σύνηθες, σοβαρό και μεγάλης εμβέλειας κίνητρο κυβερνοεπίθεσης το οποίο σχετίζεται με πολιτικούς λόγους και διεξάγεται εναντίον χωρών, κρατικών υποδομών και κυβερνητικών οργανισμών και παίρνει τη μορφή της κατασκοπείας και της τρομοκρατίας εις βάρος του αντιπάλου κυρίως για οικονομικούς αλλά και για ιδεολογικούς ακόμα και θρησκευτικούς λόγους (Clayton Mark).

4.3. ΤΥΠΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

Υπάρχουν συγκεκριμένοι τρόποι με τους οποίους μπορούν οι επιτιθέμενοι να αποκτήσουν πρόσβαση σε ένα συγκεκριμένο ηλεκτρονικό υπολογιστή ή σε ένα δίκτυο διασυνδεδεμένων υπολογιστών που μπορεί να ανήκουν σε κάποια επιχείρηση, σε τραπεζικούς φορείς ,στρατιωτικές εγκαταστάσεις ή και πολιτικούς φορείς και υποδομές όπως είναι διάφοροι διεθνείς και δημόσιοι οργανισμοί. Ο στόχος της επίθεσης είναι άμεσα συνδεδεμένος και με την αιτία πρόκλησής της και τα κίνητρα που είναι επιθυμητό από τον επιτιθέμενο να ικανοποιηθούν (Hathaway A. Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia). Σύμφωνα με το Φουτρή Παρασκευά στο περιεχόμενο της διπλωματικής του εργασίας υπάρχουν συγκεκριμένοι τρόποι παραβίασης των διαδικτυακών συνδέσεων και δεδομένων ενός ηλεκτρονικού υπολογιστή και επομένως μίας πράξης κυβερνοεπίθεσης - κυβερνοεγκλήματος ορισμένοι από τους οποίους είναι (Gervais Michael 2012):

- Επίθεση στις ιστοσελίδες
- Επίθεση στην υπηρεσία ονοματολογίας (DNS-Domain Name System)
- Επίθεση με Δούρειους Ίππους(Trojan Horses)
- Επίθεση στο ηλεκτρονικό ταχυδρομείο
- Επίθεση με ιούς
- Επίθεση με πλαστογράφηση
- Επίθεση από εύρεση των κωδικών πρόσβασης

4.4. ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

Η τεχνολογία διαρκώς αυξάνεται και εξελίσσεται σε όλους τους τομείς της καθημερινότητάς μας και το Διαδίκτυο έχει πλέον κυριαρχήσει στον Κυβερνοχώρο. Η πολιτική και στρατιωτική ηγεσία όλων των χωρών παγκοσμίως επενδύουν συστηματικά σε χώρο, χρόνο και χρήμα προκειμένου

να εκσυγχρονίσουν και να βελτιώσουν τις τεχνολογικές τους υποδομές και ταυτόχρονα την άμεση και επιτυχή συνεργασία, επαφή αλλά και ανταγωνισμό με τις υπόλοιπες χώρες του παγκοσμίου χάρτη με τις οποίες αλληλοεπιδρούν για πολιτικούς ,οικονομικούς, στρατιωτικούς αλλά και επιστημονικούς λόγους σε καθημερινό επίπεδο. Το τεχνολογικό κομμάτι αποτελεί πλέον ένα από τα σημαντικότερα κεφάλαια στην ατζέντα αυτών των χωρών προς επένδυση (Lin S. Herbert).

Στην έννοια και τον ορισμό του Κυβερνοπολέμου συμπεριλαμβάνονται οι κυβερνοεπιθέσεις και η κατασκοπεία (Iglezakis Ioannis). Μετά τη ξηρά, τον αέρα και τη θάλασσα το ΝΑΤΟ αναγνωρίζει ως επιπλέον πεδίου πολέμου και άμυνας τον Κυβερνοχώρο και καλεί τα κράτη του να αναπτύξουν τεχνικές και μεθόδους για προστασία των δεδομένων και των τεχνολογικών τους υποδομών από πιθανές κυβερνοεπιθέσεις αντίπαλων πολιτικών παρατάξεων αλλά και αντίπαλων καθεστώτων και κυβερνήσεων άλλων χωρών (Geiss Robin).Είναι αξιοσημείωτο ότι τα σύγχρονα κράτη προσπαθούν από τη μία πλευρά να προστατευθούν από πιθανές επιθέσεις που θα μπορούσαν να βλάψουν, να υποκλέψουν ή και να απορρυθμίσουν τα συστήματα και σημαντικά δεδομένα του ενιαίου εγχώριου συστήματος των ηλεκτρονικών υπολογιστών και από την άλλη εκπαιδεύουν και ωθούν το πολιτικό, διοικητικό ,επιστημονικό και στρατιωτικό δυναμικό τους στην εξοικείωση και την εφεύρεση λειτουργικών μεθόδων μέσω των οποίων θα μπορούσαν να επιτεθούν στον πιθανό τους αντίπαλο με ποικίλους τρόπους (Checka Terence).

Οι κυβερνοεπιθέσεις -που διεξάγονται κυρίως μεταξύ κρατών και μάλιστα ως μέσο επίθεσης ή αντεπίθεσης μεταξύ των αντίπαλων ενόπλων δυνάμεων- είναι σε θέση να προκαλέσουν συγκεκριμένες βλάβες ανάλογα με το στόχο τον οποίο αναλαμβάνουν να φέρουν εις πέρας (Dev R. Priyanka). Όπως γνωρίζουμε, καθώς ζούμε στην εποχή της Πληροφορίας και της Επικοινωνίας μέσω της Επανάστασης της Τεχνολογίας και με τη χρήση των ηλεκτρονικών υπολογιστών καθώς και της κατασκοπείας δημιουργείται ο τέλειος συνδυασμός για παρακολούθηση και συγκέντρωση κρίσιμων δεδομένων του αντιπάλου με

ελάχιστο χρόνο, άμεσο και έγκυρο τρόπο και αποφυγή σπατάλης στρατιωτικών εφοδίων καθώς και με ελάχιστο ανθρώπινο δυναμικό (Biggio Giacomo) .

Τα αντίπαλα κράτη ενισχύουν και επενδύουν στην ανάπτυξη γνώσεων, τεχνικών και βελτίωσης των τεχνολογικών δυνατοτήτων τους κυρίως όσον αφορά τη χρήση των δικτύων του συστήματος των ηλεκτρικών υπολογιστών τους. Απώτερος στόχος τους είναι η προστασία τους αλλά και η εναλλακτική επίθεσή τους αντί της χρήσης ένοπλης βίας ή της κήρυξης πολέμου ή απειλής χρήσης των πυρηνικών τους υποδομών (Heintschel von Heinegg Wolff). Ωστόσο, αν και μία από τις συχνότερες τακτικές των κρατών για επίθεση είναι η κατασκοπεία των ηλεκτρονικών και διαδικτυακών συστημάτων και η υποκλοπή σημαντικών δεδομένων για πολιτικούς ή στρατιωτικούς ή ακόμα και επιστημονικούς σκοπούς - προσπαθώντας να εξοικονομήσουν χρόνο και χρήμα που θα απαιτούσε η διεξαγωγή μίας επιστημονικής έρευνας για καινοτομία στη χώρα τους-υπάρχουν και ορισμένες επιθέσεις που θέτουν σε κίνδυνο τα θεμελιώδη ανθρώπινα δικαιώματα αλλά και τις ίδιες τις ζωές των πολιτών (Augustine P. Zachary).

Μία κυβερνοεπίθεση είναι σε θέση να επηρεάσει ή και να απορρυθμίσει πλήρως το σύστημα της εναέριας κυκλοφορίας μία χώρας ή ακόμα και των συγκοινωνιών της θέτοντας σε κίνδυνο την ασφάλεια και ομαλή τους λειτουργία και σκορπίζοντας πραγματικό πανικό λόγω των άμεσων και σοβαρών συνεπειών που μπορεί μία τέτοιου είδους επίθεση να προκαλέσει (Handler Gosnell Stephenie).Επικίνδυνες κυβερνοεπιθέσεις αποτελούν ,επίσης, και η παρέμβαση στα συστήματα ροής αγωγών πετρελαίου καθώς και ο κίνδυνος σε πιθανή εμπλοκή με τα συστήματα των ηλεκτρονικών υπολογιστών που σχετίζονται με τα πυρηνικά όπλα.

Κατά τη διάρκεια των τελευταίων δεκαετιών έχουν σημειωθεί πολυάριθμές κυβερνοεπιθέσεις στο Διαδίκτυο και η σοβαρότητά τους έγκειται στο γεγονός ότι απειλούν όχι μόνο τα ατομικά δικαιώματα των πολιτών αλλά και ολόκληρων

χωρών προσβάλλοντας τις βασικές αρχές και κανόνες του Διεθνούς Δικαίου που σχετίζονται με την κυριαρχία και ανεξαρτησία τους (DeLuca D. Christopher). Υπάρχουν ,ωστόσο, ορισμένες οργανωμένες επιθέσεις οι οποίες είχαν μεγάλο αντίκτυπο σε παγκόσμιο επίπεδο και έγιναν ευρέως γνωστές οι οποίες αναφέρονται στη συνέχεια:

⇒ Εσθονία :Το Φεβρουάριο του 2007 η κυβέρνηση της Εσθονίας προχώρησε στην επικύρωση του νομοσχεδίου 'Forbidden Structures Law'' σύμφωνα με το οποίο θα καταστρέφονταν ορισμένα μνημεία που σχετίζονταν με την ''κατοχή'' της χώρας από την ΕΣΣΔ. Πιο συγκεκριμένα, στην πλατεία Ταλίν της χώρας βρισκόταν το άγαλμα του Στρατιώτη του Κόκκινου Στρατού το οποίο επρόκειτο να μετακινηθεί σε άλλη κατεύθυνση καθώς είχε τοποθετηθεί στην πλατεία από τους Σοβιετικούς μετά το τέλος του Β΄ Παγκοσμίου Πολέμου. Το παραπάνω γεγονός προκάλεσε την αντίδραση των Ρώσων πολιτών της Εσθονίας καθώς και της Ρωσικής Κυβέρνησης καθώς το άγαλμα αυτό υμνούσε τους Ρώσους στρατιώτες που πάλεψαν για την απελευθέρωση της Εσθονίας από τους Γερμανούς με αποτέλεσμα να προκύψουν έντονες συγκρούσεις ανάμεσα στις εθνικιστικές ομάδες της Εσθονίας που επιθυμούσαν τη μετακίνηση του αγάλματος και των Ρώσων πολιτών της Εσθονίας που αρνούνταν κατηγορηματικά το παραπάνω ενδεχόμενο. Ωστόσο, παρά τις έντονες αντιδράσεις και διαμάχες που ξέσπασαν η Κυβέρνηση της Εσθονίας πράγματι μετακίνησε το συγκεκριμένο άγαλμα από την πλατεία Ταλίν. Το αντίκτυπο της πράξης αυτής είχε ,ωστόσο, τραγικές συνέπειες για το κράτος της Εσθονίας.

Η τεχνολογία της Πληροφορικής και των τεχνολογιών στο εσθονικό κράτος είχε ήδη αρχίσει να γίνεται έντονα αισθητή από τη δεκαετία του 1990 καθώς και τα επόμενα χρόνια όπου τόσο οι τράπεζες και οι κρατικές υπηρεσίες δημιούργησαν ηλεκτρονικές βάσεις δεδομένων στηριζόμενες στα οφέλη και τις υπηρεσίες του Διαδικτύου. Οι κυβερνοεπιθέσεις τις οποίες δέχτηκε με διαφορετικές χρονικές περιόδους η Εσθονία είχαν ποικίλους στόχους υψίστης λειτουργικής σημασίας όπως επιθέσεις σε πολιτικές, κυβερνητικές και

τραπεζικές ιστοσελίδες και εταιρείες αναφορικά με την παροχή και πρόσβαση στο Διαδίκτυο και στην κινητή τηλεφωνία.

Το παραπάνω γεγονός είχε ως αποτέλεσμα τεράστιες οικονομικές απώλειες καθώς ολόκληρη η λειτουργία της χώρας ήταν άμεσα συνδεδεμένη με την ασφαλή και ομαλή λειτουργία του Διαδικτύου ενώ πολλές ιστοσελίδες αναγκάστηκαν να κλείσουν τελείως μέχρι οι βάσεις δεδομένων να ανακτηθούν ή να αποκατασταθούν σε περίπτωση που είχαν υποστεί απώλεια ή διαστρέβλωση εξαιτίας των επιτιθέμενων. Επιπρόσθετα, η χώρα σε γενικό επίπεδο αναγκάστηκε να αποσυνδεθεί από τον Παγκόσμιο Ιστό και να επωμιστεί πλήρως τα έξοδα και τις λύσεις καθώς και την απώλεια χρόνου για την αποκατάσταση των πολλαπλών προβλημάτων που προέκυψαν στη λειτουργία των κρατικών, δημόσιων και ιδιωτικών φορέων που βασίζονταν σε μεγάλο βαθμό στο Διαδίκτυο.

⇒ Γεωργία: Οι σχέσεις ανάμεσα στη Ρωσία και τη Γεωργία ήταν ιδιαίτερα τεταμένες όταν η Ρωσία φάνηκε να υποστηρίζει ενεργά την απόσχιση της Αμπχαζίας και της Ν.Οσσετίας. Η ένταση κορυφώθηκε και οι ένοπλες συγκρούσεις ανάμεσα στις δυνάμεις της Ρωσίας που υποστήριζαν της παραπάνω χώρες και της Γεωργίας που αντιστέκονταν στην προσπάθεια απόσχισης τους είχαν σαν αποτέλεσμα να δυσχεράνει το κλίμα μεταξύ τους. Πέρα από τις ένοπλες διαμάχες, ωστόσο, πραγματοποιήθηκαν και κυβερνοεπιθέσεις εις βάρος της Γεωργίας με κυριότερους στόχους τις ιστοσελίδες του Πρόεδρου της χώρας και της Κυβέρνησης γενικότερα, των ειδησεογραφικών πρακτορείων καθώς και της σημαντικότερης τράπεζας της, της λεγόμενης TBC. Τα παραπάνω στοιχεία είχαν ως αποτέλεσμα να απενεργοποιηθεί πλήρως η λειτουργία των ιστοσελίδων καθώς και οι τραπεζικές συναλλαγές της χώρας ,σε γενικότερο βαθμό, προκαλώντας την πλήρη απορρύθμιση της λειτουργίας του κράτους σε ιδιωτικό και δημόσιο επίπεδο καθώς και της πρόσβασής του στις ηλεκτρονικές υπηρεσίες του Διαδικτύου με σκοπό να αποκλείσουν τους πολίτες και τους πολιτικούς φορείς από την πληροφόρηση και την πρόσβαση στην ενημέρωση σχετικά με την

εξέλιξη των γεγονότων καθώς και την αποστολή μηνυμάτων και την επικοινωνία με άλλες χώρες στο εξωτερικό.

Στα παραπάνω χαρακτηριστικά στοιχεία μπορούμε να προσθέσουμε και την ευρέως διαδεδομένη περίπτωση υποκλοπής σημαντικών πληροφοριών με τεχνολογικά μέσα από την πλευρά του NSA (NATIONAL SECURITY AGENCY) όπως αποκάλυψε ο Edward Snowden.

Τον Ιούνιο του 2013, έχοντας καταφέρει τη συγκέντρωση σημαντικού όγκου απόρρητων αρχείων των Ηνωμένων Πολιτειών της Αμερικής, κατέδειξε μέσα από τη δημοσίευση μίας σειράς εκθέσεων στην εφημερίδα «Guardian» ότι οι Η.Π.Α. παρακολουθούσαν τόσο Αμερικανούς όσο και ξένους πολίτες καθώς και κυβερνήτες άλλων χωρών καταγράφοντας τις προσωπικές τους συνομιλίες και συλλέγοντας προσωπικά δεδομένα με παράνομο τρόπο καταπατώντας τα ατομικά και πρωταρχικά ανθρώπινα δικαιώματα που αναγνωρίζονται μέσω του Διεθνούς Δικαίου. Το συγκεκριμένο γεγονός αποτέλεσε ένα από τα μεγαλύτερα πλήγματα που δέχθηκαν οι μυστικές υπηρεσίες και οι υπηρεσίες συλλογής πληροφοριών της Αμερικής καταδεικνύοντας τη λεπτή γραμμή ισορροπίας ανάμεσα στην εθνική ασφάλεια και την προστασία της ιδιωτικής ζωής και πυροδοτώντας πλήθος συζητήσεων και προβληματισμών για προγράμματα μαζικής παρακολούθησης (Halberstam Manny).

ΚΕΦΑΛΑΙΟ 5-ΕΙΔΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Πλέον η καθημερινότητα μας, οι αγορές μας ,οι τραπεζικές μας συναλλαγές ο τρόπος διασκέδασης και αναψυχής με διάφορα τεχνολογικά μέσα οπτικοακουστικού υλικού, η επικοινωνία και η ανταλλαγή μηνυμάτων καθώς και η ενημέρωση των πολιτών σε όλες τις χώρες που έχουν πρόσβαση στο Διαδίκτυο πραγματοποιούνται μέσω αυτού και οι πολίτες είναι άμεσα συνδεδεμένοι και εξαρτημένοι από την ομαλή λειτουργία του. Επομένως, οι κυβερνήσεις των χωρών σε παγκόσμιο επίπεδο επενδύουν όλο και περισσότερο στη διασύνδεση και ανάπτυξη των διαδικτυακών τους υπηρεσιών και στην επένδυση όσον αφορά την τεχνολογική τους ανάπτυξη. Η δυναμική των χωρών μετατίθεται από τα όπλα μαζικής καταστροφής και τον πόλεμο σε μία άτυπη μορφή ανταγωνισμού με σκοπό να αναδειχθεί η καθεμία από αυτές βασικότερη δύναμη στον παγκόσμιο Χάρτη μέσω της συλλογής πληροφοριών με σκοπό την τεχνολογική, επιστημονική και γενικότερη εξέλιξη σε διαφορετικούς τομείς και αντικείμενα αναφοράς (Jensen Talbot Eric.)

Από την μία πλευρά το Διαδίκτυο προσφέρει όλα τα θετικά χαρακτηριστικά που αναφέραμε προηγουμένως ενώ από την άλλη πλευρά εγκυμονεί κινδύνους θέτοντας σε επικίνδυνη έκθεση τα πρωταρχικά ανθρώπινα δικαιώματα καθώς και τα κατοχυρωμένα διεθνή δικαιώματα των χωρών μέσω της συλλογής -τυπικά ή άτυπα- προσωπικών δεδομένων αλλά και πληροφοριών είτε αυτές περιλαμβάνουν ιδιωτικό, επιστημονικό, πολιτικό ή και τεχνολογικό περιεχόμενο.

Όσον αφορά τους σκοπούς συλλογής των παραπάνω πληροφοριών στη σύγχρονη πολιτική τάξη και διαχωρισμό των χωρών σημαντικό ρόλο διαδραματίζει το πολιτικό σύστημα κάθε χώρας και συγκεκριμένα το γεγονός ότι μία χώρα μπορεί να έχει δημοκρατικό τρόπο διακυβέρνησης ενώ μία άλλη να διοικείται από κάποιο αυταρχικό- απολυταρχικό καθεστώς και διοίκηση και να διέπεται από συγκεκριμένους νόμους και κανόνες. Επομένως, η ελευθερία

και ο τρόπος χρήσης του Διαδικτύου στα δημοκρατικά πολιτεύματα δεν συναντάται με παρόμοιο τρόπο στα αυταρχικά καθεστώτα άλλων χωρών καθώς τα πολιτικά συστήματα και ο τρόπος διακυβέρνησης μέσω των δημοκρατικών και των αντίστοιχων αυταρχικών-απολυταρχικών καθεστώτων είναι σχεδόν αντίθετης κατεύθυνσης κυρίως όσον αφορά τα ατομικά ανθρώπινα δικαιώματα των πολιτών και -στην προκειμένη περίπτωση- των χρηστών του Διαδικτύου (Gaul Allison).

Στη συνέχεια, θα αναφερθούμε σε αναλυτικό βαθμό στον τρόπο με τον οποίο πραγματοποιείται σε ένα πρότυπο δημοκρατικό πολίτευμα η συλλογή ατομικών και συλλογικών δεδομένων και πληροφοριών που προκύπτουν από την ευρεία και καθημερινή χρήση του Διαδικτύου και το βαθμό με τον οποίο μπορούν να συλλεχθούν και να χρησιμοποιηθούν εποικοδομητικά προκειμένου να βελτιωθούν η ποιότητα και τα είδη των διαφόρων υπηρεσιών που προσφέρονται στο πλαίσιο του Κυβερνοχώρου και ταυτόχρονα με σκοπό την αντιμετώπιση επερχόμενων απειλών Κυβερνοεγκλήματος ή Κυβερνοεπιθέσεων που καθημερινά διαδραματίζονται.

Στον αντίποδα ,αντίστοιχα , βρίσκεται ο τρόπος με τον οποίο ένα αυταρχικό καθεστώς περιορίζει και ελέγχει την ελευθερία των πολιτών για πρόσβαση στο Διαδίκτυο με την προσωπική τους βούληση και πρωτοβουλία και η διαρκής παρέμβαση με συγκεκριμένα τεχνολογικά συστήματα προκειμένου να ασκήσουν αυστηρή επιτήρηση και λογοκρισία υπό την υποτιθέμενη ασπίδα της προστασίας της χώρας και του πολιτεύματος από εξωτερικές απειλές Κυβερνοεπιθέσεων που θα έβλαπταν τους ίδιους τους πολίτες. Με σκοπό την περαιτέρω ανάλυση των συγκεκριμένων στοιχείων θα εξετάσουμε δύο χαρακτηριστικές μελέτες περιπτώσεων δημοκρατικού από τη μία πλευρά και αυταρχικού-απολυταρχικού καθεστώτος από την άλλη πλευρά: τις Ηνωμένες Πολιτείες της Αμερικής και την Κίνα.

5.1. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ – ΚΙΝΑ

Η Κίνα αποτελεί τη δεύτερη μεγαλύτερη οικονομία του κόσμου μετά τις Η.Π.Α. και τη μεγαλύτερη χώρα σε εξαγωγή αγαθών. Στη διακυβέρνηση της κυριαρχεί το Κομμουνιστικό κόμμα της Κίνας με βασικό εκπρόσωπο τον Σι Τζινπίνγκ του οποίου κύρια στρατηγική αποτελεί η υπεροχή της Κίνας έναντι των υπόλοιπων χωρών ως οικονομική, τεχνολογική και πολιτική υπερδύναμη και κατ' επέκταση ως κομμουνιστική νοοτροπία που ανταγωνίζεται την αντίστοιχη πολιτική της Δημοκρατίας των δυτικών αντίπαλων χωρών μέσω της επέκτασης των τεχνολογικών της εφευρέσεων και υποδομών στον Κυβερνοχώρο από τη μία και τον απόλυτο έλεγχο και περιορισμό των πολιτών της στο αυστηρά επιτηρούμενο στα πλαίσια των συνόρων της Διαδίκτυο (Desmond Ball).

Για την Κίνα βασική πολιτική και τακτική για την ανασυγκρότηση της ιεραρχίας των χωρών και για την ανάπτυξη της ίδιας ως μεγάλης δύναμης αποτελεί η ενδυνάμωση των τεχνολογικών εγκαταστάσεων καθώς θεωρούν ότι μπορούν να αμυνθούν αλλά και να προκαλέσουν πλήγμα σε πιθανό αντίπαλο όχι τόσο με συμβατικό πόλεμο αλλά κυρίως με τεχνολογικό τρόπο ή με διάφορες κυβερνοεπιθέσεις γεγονός στο οποίο συμβάλλει το ότι εξασφαλίζεται η μείωση στο ελάχιστο σε χρόνο ,χρήμα, υλικοτεχνικά εφόδια καθώς και ανωνυμία της επίθεσης με αποτέλεσμα να είναι και περισσότερο αποτελεσματική για το κράτος. Η έννοια της κυβερνοασφάλειας είναι δυναμική και άμεσα εξαρτώμενη από τον βαθμό διείσδυσης του κυβερνοχώρου στις σύγχρονες κοινωνίες (Margulies Peter) . Το φάσμα των κυβερνοεπιθέσεων μπορεί να περιλαμβάνει: μηχανές αναζήτησης, κοινωνικά δίκτυα, δημόσιες διοικήσεις, ηλεκτρονικές πλατφόρμες πληρωμής, διαδικτυακούς τόπους ηλεκτρονικού εμπορίου, εθνικές υποδομές, αλλά και το προσωπικό ηλεκτρονικό ταχυδρομείο μας. Μια κυβερνοεπίθεση μπορεί να αποσκοπεί στη δυσλειτουργία ενός συστήματος, αλλά και στην υποκλοπή δεδομένων. Οι στόχοι είναι οι κυβερνήσεις, ο ιδιωτικός τομέας αλλά και η κοινωνία (Adam Segal).

Κύριος ανταγωνιστής για το κράτος της Κίνας αποτελούν οι Η.Π.Α. καθώς προσπαθεί να υπερισχύσει η μία έναντι της άλλης σε οικονομικό ,πολιτικό και τεχνολογικό επίπεδο με κύριο σημείο δράσης τις υπηρεσίες του Κυβερνοχώρου. Σύμφωνα με την έκθεση IISS η τεχνολογία της Κίνας βρίσκεται 10 χρόνια πίσω σε σχέση με τις Η.Π.Α οι οποίες ,ωστόσο, δεν πρέπει να εφησυχάζονται καθώς η αναπτυσσόμενη βιομηχανική δραστηριότητα και επένδυση της Κίνας στον Κυβερνοχώρο αποτελούν άμεση απειλή.

Η πολιτική ασφαλείας της Κίνας στον Κυβερνοχώρο περιλαμβάνει όχι μόνο την τεχνολογική και οικονομική της ανάπτυξη αλλά και την υπερίσχυση του πολιτικού της καθεστώτος ως αυταρχικού κράτους έναντι της δημοκρατίας και προκειμένου να το επιτύχει προσπαθεί να επιβάλλει τους πολιτικούς της κανόνες όχι μόνο στο εσωτερικό της χώρας και των πολιτών της αλλά και στο εξωτερικό συνεργαζόμενη με άλλα αυταρχικά καθεστώτα όπως η Ρωσία και πουλώντας τεχνολογικά εφόδια κινέζικης παραγωγής σε άλλες χώρες επεκτείνοντας την νοοτροπία της εις βάρος των χωρών της δυτικής κουλτούρας και διακυβέρνησης.

5.2. ΨΗΦΙΑΚΌΣ ΑΥΤΑΡΧΙΣΜΌΣ

5.2.1. ΟΡΙΣΜΌΣ

Όταν ιδρύθηκε το Διαδίκτυο σηματοδότησε την δυνατότητα των χωρών και των πολιτών να επικοινωνούν αμεσότερα και με περισσότερες λειτουργικές δυνατότητες σε κάθε γωνιά του κόσμου ενισχύοντας το αίσθημα της ελευθερίας και της πρωτοβουλίας για δράση – ατομική ή συλλογική. Ωστόσο, για την Κίνα το Διαδίκτυο αποτελεί και αυτό ένα μέσο -οικονομικό και πολιτικό – για επέκταση και ενίσχυση της πρωτοκαθεδρίας του αυταρχικού καθεστώτος τόσο στο εσωτερικό της ίδιας της χώρας όσο και στο εξωτερικό. Ο ψηφιακός αυταρχισμός είναι η πολιτική της Κίνας να ασκεί τον απόλυτο έλεγχο στις

δραστηριότητες, τη ροή και τη χρήση των πληροφοριών που διακινούνται μέσω των διάφορων εφαρμογών του Διαδικτύου (Council on Foreign Relations). Σύμμαχος της είναι η συνεχής επιτήρηση και λογοκρισία που ασκεί σε όσα λέγονται ή γράφονται ενώ ταυτόχρονα προσπαθεί να μεταβάλλει ή τροποποιήσει ή και να αποκρύψει από τους χρήστες του σημαντικές πληροφορίες και δεδομένα οδηγώντας τους πολίτες της στην προπαγάνδα και τον αποπροσανατολισμό με σκοπό να προστατέψει από οποιαδήποτε αρνητική πολιτική ,οικονομική ή κοινωνική επιρροή το αυταρχικό της καθεστώς. Σύμφωνα με τον ορισμό του David Lyon ***ως επιτήρηση ορίζεται η συλλογή και χρήση προσωπικών δεδομένων με σκοπό την επιρροή ή των αποπροσανατολισμό αυτών στους οποίους ανήκουν.***

Η επιτήρηση ως ολική διαδικασία διεξάγεται από ένα οργανωμένο σύστημα αποτελούμενο από υπεύθυνους ασφαλείας, επιχειρήσεις διοικούμενες από το κράτος καθώς και ιδιωτικές εταιρείες που επιθυμούν να αποκτήσουν ή να αυξήσουν τα κέρδη τους μέσω της πρακτικής της παρακολούθησης - επιτήρησης. Μέσω του ψηφιακού αυταρχισμού η Κίνα καταπατά τα ανθρώπινα δικαιώματα των πολιτών της για ελευθερία της έκφρασης του λόγου, της προσωπικής επιλογής και πρωτοβουλίας για προσωπική δράση ή ακόμα και της διαμαρτυρίας, της αντίδρασης και της κριτικής εναντίον του πολιτεύματος της και των κυβερνώντων της. Ουσιαστικά, για το αυταρχικό καθεστώς της Κίνας το Διαδίκτυο και η τακτική του Ψηφιακού Αυταρχισμού αποτελεί το νέο υπερόπλο μέσω του οποίου θα επιβληθεί, θα ελέγξει και θα χειραγωγήσει την ανθρώπινη βούληση των πολιτών της και μέσω της οικονομικής και τεχνολογικής της ανάπτυξης και πώλησης των προϊόντων της στον Κυβερνοχώρο και σε άλλες χώρες θα καταφέρει να υποβαθμίσει τις Η.Π.Α., να απειλήσει και να διεκδικήσει την πρωτοκαθεδρία της καθώς και την ίδια τη δημοκρατία ως πολίτευμα.

Βέβαια, για την επίσημη πολιτική γραμμή επιβολής του ο Ψηφιακός Αυταρχισμός αποτελεί και την πολιτική ασφαλείας της Κίνας έναντι των

πιθανών εχθροπραξιών και επιθέσεων στον Κυβερνοχώρο γεγονός το οποίο ενισχύει τη δυσκολία διάκρισης ανάμεσα στην ελευθερία του Διαδικτύου από τη μία και την ανάγκη διασφάλισης των ατομικών δικαιωμάτων που μπορούν να καταπατηθούν από την απόλυτη αυτή ελευθερία εξαιτίας της ύπαρξης πράξεων Κυβερνοεγκλήματος από την άλλη.

5.2.2. ΤΟ ΜΕΓΑΛΟ ΤΕΙΧΟΣ – «THE GREAT FIREWALL»

Το μεγάλο τείχος προστασίας της Κίνας αποτελεί το σύνολο των νομοθετικών ενεργειών και τεχνολογικών ρυθμίσεων που επιβάλλει η κυβέρνηση της Λαϊκής δημοκρατίας της Κίνας για τη λειτουργία και τους όρους χρήσης του Διαδικτύου στο εσωτερικό της χώρας. Από το 1996 -όπου ήταν και τα πρώτα χρόνια συμμετοχής της Κίνας στο Διαδίκτυο- η κυβέρνηση της ανακοίνωσε σαφέστατα ότι το Διαδίκτυο θα βρισκόταν υπό τον πλήρη έλεγχο και την καθοδήγηση από τις επίσημες αρχές εξουσίας.

Ειδικότερα, από το 2013 και έπειτα όλες οι δραστηριότητες και η ροή δεδομένων και πληροφοριών ελέγχονται και λειτουργούν με βάση τους ρυθμιστικούς κανόνες και την έγκριση ή μη του Υπουργείου Κυβερνοασφάλειας της Κίνας το οποίο βρίσκεται σε άμεση επικοινωνία με το κυβερνών κόμμα. Ο βασικός μηχανισμός του Μεγάλου τείχους έγκειται στο γεγονός ότι αποκλείει ή περιορίζει επιλεκτικά την πρόσβαση των χρηστών της χώρας σε ξένους ιστότοπους και ιστοσελίδες καθώς και σε εφαρμογές κινητών με το πρόσχημα της προστασίας και της διασφάλισης της ομαλής λειτουργίας του Διαδικτύου από ξένες απειλές στα πλαίσιο των συνόρων της (Hong shen).

Πιο συγκεκριμένα, σκοπός της κυβέρνησης της Κίνας είναι να απεξαρτηθεί πλήρως σε βάθος χρόνου από την τεχνολογική πρωτοκαθεδρία των αμερικανικών κολοσσών ενημέρωσης και ροής πληροφοριών και ψυχαγωγίας στο Διαδίκτυο και να τις αντικαταστήσει με δικές της τις οποίες θα καταφέρει να πουλήσει και σε άλλες χώρες ενισχύοντας την οικονομική της ανάπτυξη και πολιτική της επιρροή ως μεγάλη δύναμη αλλά και ως αυταρχικό καθεστώς.

Χαρακτηριστικό των παραπάνω στοιχείων αποτελεί το γεγονός της κριτικής ή και αποκλεισμού κατά καιρούς στα κινέζικά σύνορα της πρόσβασης των πολιτών της ή του επιμέρους περιεχομένου των ιστοσελίδων της YAHOO!SEARCH , MICROSOFT LIVE SEARCH GOOGLE SEARCH CHINA. Επιπρόσθετα, εφαρμογές όπως το FACEBOOK, TWITTER, INSTAGRAM έχουν αποκλειστεί και απαγορευτεί στην Κίνα και τείνουν να αντικατασταθούν από τις αντίστοιχες κινέζικες εφαρμογές όπως είναι το WeChat και το Weibo οι οποίες είναι αυστηρά ελεγχόμενες και αρνητικά διακείμενες προς οποιαδήποτε ανεπιθύμητη κριτική σχετικά με την πολιτική και τις κυβερνητικές πρωτοβουλίες της χώρας. Η επιτήρηση, η λογοκρισία και η αυστηρότητα σχετικά με το βαθμό πρόσβασης και τον τρόπο χρήσης των διαδικτυακών εφαρμογών αποδεικνύονται στο γεγονός ότι το 2019 -μάλιστα στις τρεις πρώτες εβδομάδες του έτους- η κυβέρνηση της Κίνας κατάργησε πάνω από 700 ιστοσελίδες και 9.000 εφαρμογές κινητού.

Εκτός από την διαδικτυακή δραστηριότητα ο ψηφιακός αυταρχισμός της Κίνας επεκτάθηκε μέσω ενός προγράμματος με το όνομα Skynet και σε ολόκληρο το Πεκίνο καλύπτοντας το με τουλάχιστον 800.000 κάμερες ενώ μέχρι το 2015 ολόκληρη η πόλη είχε καλυφθεί πλήρως με κάμερες. Βασική φιλοδοξία αποτελεί ένα επιπλέον τεχνολογικό πρόγραμμα γνωστό ως «Κοφτερά Μάτια» ή «Sharp Eyes» μέσω του οποίου η επιτήρηση των κινήσεων και της συμπεριφοράς των πολιτών θα επεκταθεί στη διασύνδεση των καμερών με τα κινητά καθώς και με τις τηλεοράσεις των πολιτών. Μέσω της ανάπτυξης της τεχνολογικής νοημοσύνης και της τοποθέτησης χιλιάδων καμερών ακόμα και σε ολόκληρη τη χώρα- όσο είναι εφικτό- η κυβέρνηση φιλοδοξεί την διαρκή παρατήρηση των κινήσεων των πολιτών σε όλους τους δημόσιους χώρους μέσω των καμερών ,των τηλεοράσεων και των κινητών τους χωρίς να απαιτείται η πρόσβαση στο Διαδίκτυο.

Όλοι οι πολίτες θα βρίσκονται υπό καθημερινή και ασταμάτητη επίβλεψη από το κράτος επιτήρησης της Κίνας και με υψηλή ανάλυση αναγνώρισης

προσώπου θα είναι δυνατόν να εντοπίζεται και να συλλαμβάνεται οποιοδήποτε είδος παρανομίας ή αντικοινωνικής για το νόμο συμπεριφοράς.

Σε συνδυασμό με την εγχώρια τοποθέτηση και την υψηλή τεχνολογία ανάλυσης καμερών το κυβερνών κόμμα έθεσε γνωστή την εγκατάσταση ειδικού εθνικού προγράμματος και λογισμικών γνωστών ως Κοινωνικό Πιστωτικό Σύστημα της Κίνας έως το 2020 σύμφωνα με το οποίο θα συγκεντρώνονται οι χρηματοπιστωτικές αγορές και οι οικονομικές και κοινωνικές συναλλαγές και τάσεις συμπεριφοράς των πολιτών καθώς και τα προσωπικά τους δεδομένα και με ειδικές αναλύσεις θα καταγράφεται το αντίστοιχο ποσοστό αξιοπιστίας και πιστοληπτικής ικανότητας που αναλογεί στον κάθε πολίτη ξεχωριστά. Από τις παραπάνω καταμετρήσεις το αποτέλεσμα που θα προκύπτει θα κρίνει αν το άτομο θα κερδίσει ένα είδος ανταμοιβής για τη νόμιμη συμπεριφορά του ή κάποια τιμωρία σε περίπτωση που εντοπιστεί παράνομη ή μη έγκυρη συμπεριφορά σύμφωνα με τη νομοθεσία και τους κανονισμούς του αυταρχικού καθεστώτος της Κίνας.

Πίσω από την οργάνωση του παραπάνω εγχειρήματος βρίσκονται τόσο ιδιωτικές όσο και δημόσιες ομάδες συμφερόντων ελεγχόμενες από την κρατική εξουσία και το κυβερνών Κόμμα οι οποίες αναλαμβάνουν την επιτήρηση και το διακανονισμό του ελέγχου των κινήσεων που διαδραματίζονται από τους πολίτες στον οικονομικό, πολιτικό και κοινωνικό τομέα επηρεάζοντας ,ταυτόχρονα, τα μέσα μαζικής επικοινωνίας και τον τρόπο κατανομής των πληροφοριών στο Διαδίκτυο ανάλογα με τα ενδιαφέροντα του κάθε πολίτη και την κατεύθυνση στην οποία επιθυμεί το κράτος να τον προσανατολίσει παραβιάζοντας το ατομικό δικαίωμα της ελευθερίας και της ιδιωτικής του ζωής.

Μέσω των προγραμμάτων υψηλής τεχνολογίας που χρησιμοποιούνται στην επίτευξη του Κοινωνικού Πιστωτικού Συστήματος πραγματοποιείται συλλογή πληροφοριών όπως τα προσωπικά- ατομικά στοιχεία ταυτοποίησης του κάθε πολίτη, οικονομικές συναλλαγές ή οφειλές όπως φόροι και δάνεια, ταξίδια και τρόποι ψυχαγωγίας καθώς και τάσεις στα μέσα κοινωνικής δικτύωσης.

Με τους παραπάνω τρόπους η κυβέρνηση της Κίνας από την μία πλευρά καταφέρνει να χρησιμοποιήσει το Διαδίκτυο ως τεχνολογικό εργαλείο ανάπτυξης και ως οικονομική επένδυση στη χώρα της αλλά και στο εξωτερικό-συνεργαζόμενη με αυταρχικά κυρίως καθεστώτα όπως η Ρωσία στα οποία προωθεί τα απαραίτητα λογισμικά και τις εφαρμογές για επιτήρηση του Διαδικτύου και ,επομένως, συντήρηση της πολιτικής σταθερότητας και του πολιτεύματος- ενώ από την άλλη πλευρά μέσω της στενής επιτήρησης, του αποκλεισμού ιστοσελίδων , της περιορισμένης πρόσβασης των πολιτών σε μη εγχώριες ηλεκτρονικές και διαδικτυακές εφαρμογές και του οργανωμένου και στοχευμένου φιλτραρίσματος της ροής και του είδους των πληροφοριών που αναμεταδίδονται καταφέρνει να προστατεύει, να αποτρέπει και να διασφαλίζει τις σημαντικές πληροφορίες και ηλεκτρονικές και τεχνολογικές της υπηρεσίες και δομές από τις αρνητικές συνέπειες των κυβερνοεπιθέσεων (Melzer Nils).

Επίσης, προστατεύει σε σημαντικό βαθμό τους πολίτες από εγκληματικές και παράνομες πράξεις καθώς λόγω της αυξημένης λογοκρισίας και επίβλεψης τους με τα τεχνολογικά μέσα που έχει εφεύρει το κράτος καθώς και με τους αυστηρούς κανόνες και τις βαρύτατες ποινές που χαρακτηρίζουν το αυταρχικό καθεστώς της Κίνας τέτοιου είδους ανεπιθύμητες και προβληματικές καταστάσεις τείνουν να μειώνουν σημαντικά την εμφάνισή τους προσφέροντας ,ταυτόχρονα, πολιτική σταθερότητα και συνοχή.

Ταυτόχρονα, για ένα αυταρχικό καθεστώς η μεγαλύτερη απειλή είναι η ελευθερία της έκφρασης και ,κυρίως, η ελευθερία του Τύπου και των Μέσων Μαζικής Ενημέρωσης είτε μέσω των εφημερίδων είτε μέσω των ηλεκτρονικών μορφών όπως η τηλεόραση και οι διάφορες ιστοσελίδες ενημέρωσης του Διαδικτύου. Προκειμένου να διατηρήσει το Κόμμα την εξουσία του έχει άμεση ανάγκη να ελέγχει, να διαστρεβλώνει ή και να απαγορεύει την οποιαδήποτε είδηση επιχειρήσει κάποιος να διαδώσει εις βάρος του ενώ ,σε πολλές

περιπτώσεις, το Κόμμα επιθυμεί να χειραγωγήσει το πλήθος των πολιτών με τη διάδοση και αναμετάδοση ψευδών ειδήσεων.

Ήδη από το Νοέμβριο του 2012 -έχοντας αναλάβει επικεφαλής της διοίκησης του Κόμματος- ο Xi Jinping κατέστησε σαφές στις εφημερίδες και τα περιοδικά τον πλήρη έλεγχο τους με τη μορφή απαγόρευσης συγκεκριμένων λέξεων ενώ πλήθος δημοσιογράφων και διευθυντών απολύθηκαν ή κατέληξαν στη φυλακή.

Η προπαγάνδα και ο τρόπος διαχείρισης της γλώσσας καθώς και η επανάληψη συγκεκριμένων λέξεων από το κυβερνών κόμμα αποτελούν βασική μορφή άσκησης επιρροής στο πλήθος των πολιτών της χώρας καθώς το όραμά του είναι να ομοιογενοποιηθεί υπέρ της Κυβέρνησης και των αξιών του αυταρχικού – ολοκληρωτικού καθεστώτος ο τρόπος σκέψης τους. Σε αυτό σημαντικό ρόλο θα διαδραμάτιζε η εξάπλωση του Διαδικτύου και της αναμετάδοσης πληροφοριών και ροής ειδήσεων μέσω αυτού με σκοπό την εξυπηρέτηση των πολιτικών, κοινωνικών και οικονομικών συμφερόντων της χώρας της Κίνας έναντι των δυτικών – δημοκρατικά κυβερνώμενων – χωρών.

Σε όλες τις ειδήσεις μεταδίδεται πληθώρα θετικών αντιδράσεων ή θετικά διακείμενων εκφράσεων υπέρ των πράξεων και ενεργειών της Κυβέρνησης αλλά και διαστρέβλωση και παραποίηση των γεγονότων ώστε κανείς να μην έχει τη δυνατότητα να αμφισβητήσει ή να προβάλλει αντίσταση στην εξουσία και τον πλήρη έλεγχο του ολοκληρωτικού καθεστώτος.

Η λογοκρισία είναι άμεσα συνδεδεμένη με την πολιτική κουλτούρα της Κίνας όπου τα ανθρώπινα δικαιώματα όπως αυτό της ελεύθερης έκφρασης καταπατώνται άμεσα ή έμμεσα. Χαρακτηριστική τακτική της αυταρχικής κυβέρνησης είναι η διαστρέβλωση της πραγματικότητας προκειμένου να

καταπολεμηθούν οι αντιφρονούντες ή αυτοί που αρνούνται γενικά να υποταχθούν στην απόλυτη καταπίεση που αυτή επιβάλλει στους πολίτες της.

Το 2017 ο Liu Xiaobo αποτέλεσε τον πρώτο βραβευμένο νικητή Νόμπελ Ειρήνης που απεβίωσε μέσα στη φυλακή μετά τον Γερμανό ειρηνιστή Καρλ φον Οσιέτσκι-που είχε πεθάνει το 1938 στο νοσοκομείο όντως κρατούμενος των ναζί-καθώς είχε βρεθεί σε αυτήν ήδη από το 2010 όταν κρίθηκε ένοχος ως εγκληματίας σύμφωνα με τις επίσημες πάντα δηλώσεις που είχαν ανακοινωθεί. Η πραγματική αλήθεια ,όμως, είναι διαφορετική καθώς ο ίδιος για σχεδόν μία δεκαετία ήταν και από τους πιο γνωστούς πολέμιους και επικριτές του τρόπου διακυβέρνησης του κόμματος.

Για την κυβέρνηση της Κίνας όσοι διαφωνούν δημόσια με τις πρακτικές του κράτους είναι γνωστοί ως αντιφρονούντες και ,επομένως, ως εγκληματίες καθώς η εναντίωση στην εξουσία του κόμματος ισοδυναμεί στην Κίνα με διάπραξη -ίσως και του σημαντικότερου- εγκλήματος.

Οι πολίτες που παρουσιάζουν τον εαυτό τους ως εχθρικά διακείμενο ιδιαίτερα στις μέρες μας μέσω του Διαδικτύου και του πλαισίου του Κυβερνοχώρου τείνουν να αποτελούν απειλή και να τιμωρούνται παραδειγματικά μέσω της λογοκρισίας που έχει πλέον επιβληθεί από το Κόμμα καταπατώντας ολοκληρωτικά το δικαίωμα της ελευθερίας του λόγου με οποιοδήποτε τεχνολογικό ή μη μέσο.

Παρόμοια περίπτωση παραβίασης του δικαιώματος για ελευθερία της έκφρασης στο πλαίσιο του Κυβερνοχώρου από την Κίνα αποτελεί ο σύγχρονος ακτιβιστής Ai Weiwei ο οποίος χρησιμοποιώντας το Twitter άσκησε κριτική με δηλώσεις του για την αρνητική στάση του Κόμματος της Κίνας έναντι της Δημοκρατίας και των ανθρώπινων δικαιωμάτων.

Το Twitter έχει απαγορευθεί ως μέσο κοινωνικής δικτύωσης στην Κίνα και οι δηλώσεις τόσο του ίδιου όσο και άλλων αντιφρονούντων δεν δημοσιεύονται και στα αντίστοιχα μέσα κοινωνικής δικτύωσης της Κίνας εντός των συνόρων της. Η παραπάνω ενέργεια, λοιπόν, καταδικάστηκε από την Κυβέρνηση της Κίνας και ο Ai Weiwei πέρασε 3 μήνες στη φυλακή όταν και συνελήφθη στο Πεκίνο το 2011 για ΄οικονομικά εγκλήματα'' και αργότερα αφέθηκε ελεύθερος καθώς δεν υπήρχε καμία ουσιαστική απόδειξη για την υποτιθέμενη ενοχή του.

Ήδη από το 2009 στην Κίνα το Facebook και το Twitter είχαν απαγορευθεί ως δυτικά πρότυπα κοινωνικής δικτύωσης και είχαν αντικατασταθεί από το τοπικό Weibo, το WeChat και το Baidu Tieba σε μία από τις επιχειρήσεις οικονομικού ανταγωνισμού στο πλαίσιο του Κυβερνοχώρου ανάμεσα στην Κίνα και τις Η.Π.Α. Βέβαια, η δημιουργία κινέζικων κοινωνικών δικτύων υπό το πρίσμα της δημιουργίας του Μεγάλου Τείχους αποτελούσε και την ασφάλεια και ασπίδα της χώρας έναντι των κακόβουλων λογισμικών και των ενδεχόμενων Κυβερνοεπιθέσεων που επιτυγχάνεται μέσω του διαρκή ελέγχου και της επιτήρησης από το κυβερνών Κόμμα. Στα τέσσερα χρόνια έως το 2013- όπου και έγιναν οι πρώτες ριζικές απαγορεύσεις και περιορισμοί στο Διαδίκτυο της Κίνας- οι πολίτες είχαν καταφέρει να δημιουργήσουν κοινότητες στην ιστοσελίδα Weibo μέσω των οποίων μπορούσαν να ασκούν κριτική, να ανταλλάσσουν μηνύματα και να εκφράζουν τις απόψεις τους ενώ διάσημα πρόσωπα όπως τραγουδιστές ή ηθοποιοί λόγω του τεράστιου πλήθους ακολούθων τους στο Διαδίκτυο και μέσω της δημιουργίας διάφορων blogs ασκούσαν έντονη επιρροή στον τρόπο σκέψης και δράσης του κοινωνικού συνόλου της Κίνας.

Ο Murong Huecun – ο οποίος αποτελεί μία από τις πιο ενεργείς προσωπικότητες του Weibo- και επιπλέον 350 εκατομμύρια χρήστες του μπορούσαν πλέον να έχουν πρόσβαση σε σημαντικές πληροφορίες σχετικά με τη χώρα τους για ζητήματα όπως η ατμοσφαιρική ρύπανση, διατροφικά σκάνδαλα , αστυνομική βία και υπεξέρεση της εξουσίας. Με παρόμοιους τρόπους για πρώτη φορά μετά από πολλά χρόνια το κοινωνικό σύνολο της

Κίνας είχε πρόσβαση σε «ευαίσθητες» για το κυβερνών αυταρχικό καθεστώς πληροφορίες.

Το συγκεκριμένο μέσο κοινωνικής δικτύωσης αν και αποτέλεσε το μεγαλύτερο όπλο για τους επαναστάτες και τους αντιφρονούντες του ολοκληρωτικού κόμματος έγινε ταυτόχρονα και ο σημαντικότερος στόχος για την κυβέρνηση της Κίνας. Κυρίως από τον Νοέμβριο του 2013 ξεκίνησαν οι αυστηρές και παραδειγματικές τιμωρίες υπό την διοίκηση του Xi Jinping ο οποίος κατέστησε σαφές το ενδεχόμενο φυλάκισης έως και τρία χρόνια σε οποιονδήποτε τολμούσε να δημοσιεύσει αρνητικά σχόλια ή επικριτικές γνώμες στο Weibo σχετικά με την διοίκηση και σοβαρά θέματα που αφορούν τη χώρα συνολικά.

Όπως ήταν αναμενόμενο, οι πολίτες συνειδητοποίησαν ότι ο εκφοβισμός, η λογοκρισία και η επιτήρηση που ίσχυαν ανέκαθεν στο πολιτικό καθεστώς της Κίνας είχαν επιστρέψει δυναμικά με σκοπό να εμποδίσουν το επαναστατικό κύμα που είχαν καταφέρει -μέσω της διάδοσης και επέκτασης του Διαδικτύου- να οργανώσουν και εν τέλει να κατασταλούν οποιεσδήποτε αντιδράσεις ή απαγορευμένες συζητήσεις – ιδιωτικές ή δημόσιες – σχετικά με πολιτικά, οικονομικά και πολιτικά θέματα υψίστης για το κράτος βαρύτητας. Πολλοί ενεργοί στα μέσα κοινωνικοί δικτύωσης «bloggers» , επιχειρηματίες και διάσημες προσωπικότητες αναγκάστηκαν να διαγράψουν τους δημόσιους λογαριασμούς τους και τους χιλιάδες ακόλουθους τους όντας εκφοβισμένοι από τη στάση και τις έμμεσες απειλές του αυταρχικού καθεστώτος της χώρας.

Αξιοσημείωτο χαρακτηριστικό αποτελεί το γεγονός ότι η κυβέρνηση της Κίνας δε σταμάτησε ως προς σε αυτό μόνο την καταπάτηση των ανθρωπίνων δικαιωμάτων των πολιτών της χώρας της στον κυβερνοχώρο αλλά προχώρησε στο να χρησιμοποιήσει προς όφελος της την ισχύ και την επιρροή του Weibo και των μέσων κοινωνικής δικτύωσης κατακλύζοντας το με πλήθος

δημοσιεύσεων σχετικά με τη μόδα, τα μέσα ψυχαγωγίας και διάσημα πρόσωπα τα οποία αποθεώνουν και υποστηρίζουν το κόμμα με θετική για αυτό παραπληροφόρηση και προπαγάνδα εις βάρος των πραγματικών γεγονότων και της αλήθειας την οποία σκόπιμα αποκρύπτουν από το κοινωνικό σύνολο.

Επιπρόσθετα, η Κίνα ,αν και ,αρχικά, στηρίχτηκε στις μεγάλες εταιρείες της Αμερικής για την επέκταση των τηλεπικοινωνιών και των μέσων διαδικτυακής οργάνωσης και πρόσβασης στον Κυβερνοχώρο ,στη συνέχεια, ένας από τους κυριότερους στόχους της εξωτερικής της πολιτικής για την προστασία της χώρας της από κυβερνοκατασκοπείες και κυβερνοεπιθέσεις ήταν να ανεξαρτητοποιηθούν πλήρως από αυτές και να ιδρύσουν αντίστοιχες και αποκλειστικά δικές τους αποβλέποντας ταυτόχρονα και έμμεσα στην οικονομική τους ανάπτυξη πωλώντας τον τεχνολογικό τους εξοπλισμό και τις εφαρμογές για έλεγχο του Διαδικτύου της χώρας τους και στο εξωτερικό σε άλλες χώρες με αυταρχικά καθεστώτα διαιωνίζοντας την καταπάτηση της ελευθερίας κρίσης και βούλησης καθώς και του ίδιου του δημοκρατικού πολιτεύματος (Jason Fritz).

Το συγκεκριμένο γεγονός είχε ως αποτέλεσμα η Κίνα να προχωρήσει στη ψήφιση του Νόμου για τον Κυβερνοχώρο σύμφωνα με τον οποίο όλες οι εταιρείες και οργανώσεις τηλεπικοινωνιών και Διαδικτύου που λειτουργούν εντός της Κίνας οφείλουν να δρουν σύμφωνα με τη νομοθεσία, τον κανονισμό και τους περιορισμούς που ορίζει ο νόμος της χώρας σχετικά με τη διαχείριση του περιεχομένου και των πληροφοριών που κυκλοφορούν και μεταδίδονται μέσω της πρόσβασης του Διαδικτύου (David Lyon) .

Οι εταιρείες ,δηλαδή, που δραστηριοποιούνται στην Κίνα και πολλές από αυτές ανήκουν στη Δύση και σε πολιτεύματα δημοκρατικού τύπου -με τις αντίστοιχες ελευθερίες όσον αφορά τον τρόπο έκφρασης και την ελευθερία για προστασία των προσωπικών δεδομένων- καλούνται στην Κίνα να λογοδοτούν ως προς την πρόσβαση των χρηστών τους και ως προς τα προσωπικά τους δεδομένα καθώς και να εγκαταστήσουν ξεχωριστές διόδους επικοινωνίας στο

λογισμικό τους ώστε να μπορεί η διοίκηση της Κίνας που ασχολείται με τον έλεγχο των κινήσεων στο Διαδίκτυο να έχει ανά πάσα στιγμή πλήρη έλεγχο και εποπτεία στο περιεχόμενο τους.

Το Υπουργείο Κυβερνοασφάλειας της Κίνας έχει πλήρη δικαιοδοσία υπό την επιτήρηση του Xi Jinping να υποχρεώνει σύμφωνα με την παραπάνω νομοθεσία τις ξένες εταιρείες να προλαμβάνουν και να αποτρέπουν τη δημοσίευση ακατάλληλου και ευαίσθητου πολιτικού υλικού καθώς και να μην δημοσιεύουν ή αποθηκεύουν τα προσωπικά δεδομένα των χρηστών της χώρας εκτός Κίνας. Μία χαρακτηριστική περίπτωση αποτελεί το γεγονός ότι σε συνδυασμό με τους κανόνες και τους όρους του Μεγάλου Τείχους η Κίνα υποχρέωσε την αμερικάνικη εταιρεία της Apple να διαγράψει πολλές από τις εφαρμογές της από το App store στο τοπικό της δίκτυο γεγονός το οποίο αποδεικνύει για άλλη μία φορά το μέγεθος της καταπάτησης των ανθρωπίνων δικαιωμάτων τόσο σε μεμονωμένο επίπεδο όσο και σε συλλογικό στον τομέα των επιχειρήσεων μέσω της μορφής της λογοκρισίας και της επιτήρησης άνευ ορίων.

Τα παραπάνω στοιχεία αποτελούν μία μικρή ένδειξη του ψηφιακού αυταρχισμού της Κίνας ως αυταρχικού καθεστώτος στο πλαίσιο του Κυβερνοχώρου και των τεχνολογικών εξελίξεων και εφαρμογών. Μέσω της εξάπλωσης της πολιτικής της στο Διαδίκτυο και σε άλλα απολυταρχικά καθεστώτα η δημοκρατία και τα ανθρώπινα δικαιώματα αντιμετωπίζουν σοβαρό κίνδυνο επικράτησης και αυτοπροστασίας της ισχύς τους στο σύγχρονο παγκόσμιο τεχνολογικό σύστημα. Τα τελευταία χρόνια και κυρίως από το 2018 και έπειτα η Κίνα αποτέλεσε τη χώρα με τη μεγαλύτερη παραβίαση της ελευθερίας στο Διαδίκτυο (Andrew Liaropoulos).

5.3. ΠΕΡΙΠΤΩΣΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ: ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΤΗΣ ΑΜΕΡΙΚΗΣ (Η.Π.Α.)

Προκειμένου να κατανοήσουμε την πολιτική νοοτροπία αντιμετώπισης του Διαδικτύου για τις Η.Π.Α. αρκεί να αναφερθούμε σε όσα ειπώθηκαν κατά καιρούς από σημαντικούς πολιτικούς εκπροσώπους της χώρας όπως ο Barack Obama και η Hillary Clinton.Συγκεκριμένα, αναφέρουμε ως ορόσημο την πολιτική των Η.Π.Α. καθώς όχι μόνο πρωτοστάτησαν στην τεχνολογική εφεύρεση και εξάπλωση των λειτουργικών δομών και τηλεπικοινωνιών του Διαδικτύου σε παγκόσμιο επίπεδο αλλά και διότι αποτελούν την εκπροσώπηση και απάντηση της Δύσης, του δυτικού τρόπου ζωής και ,κυρίως, του δημοκρατικού πολιτεύματος, των αρχών και αξιών έναντι των αυταρχικών καθεστώτων της Ανατολής.

Βασική γραμμή της πολιτικής των Η.Π.Α. αποτελεί ανέκαθεν η απελευθέρωση της λειτουργίας και των υπηρεσιών του Διαδικτύου στο πλαίσιο του Κυβερνοχώρου. Το Διαδίκτυο για τα δημοκρατικά πολιτεύματα προσφέρει την ελευθερία της επιλογής και έκφρασης των πολιτών καθώς και τη δυνατότητα για άμεση, ουσιαστική και εποικοδομητική επικοινωνία μέσω της ανταλλαγής πληροφοριών, απόψεων και ιδεών. Ο,τιδήποτε συμβαίνει στην άλλη άκρη της Γης αναμεταδίδεται με ήχο και εικόνα σε όλους τους χρήστες που διαθέτουν πρόσβαση στο Διαδίκτυο καθώς τα μέσα μαζικής επικοινωνίας αποτελούν αναπόσπαστο κομμάτι του δυτικού τρόπου ζωής (Mudrinich M. Major Erik).

Για τις Η.Π.Α. -που διαθέτουν έως και σήμερα την πρωτοκαθεδρία στην εξάπλωση της πρόσβασης στο Διαδίκτυο έναντι της Κίνας που προσπαθεί -και ίσως και καταφέρει -να την υπερβεί στις επόμενες δεκαετίες, τα ψηφιακά δικαιώματα αποτελούν προέκταση των πρωταρχικών ανθρωπίνων δικαιωμάτων του δημοκρατικού πολιτεύματος.

Ωστόσο, στη σύγχρονη ψηφιακή εποχή εκτός από τα θετικά χαρακτηριστικά στοιχεία που διαθέτει και προσφέρει στους χρήστες του το Διαδίκτυο και οι τεχνολογικές εφαρμογές ελλοχεύουν ορισμένες προβληματικές καταστάσεις από την απεριόριστη ελευθερία της πρόσβασης και χρήσης αυτών (Kesan P. Jay, Hayes M. Carol) . Καθώς το Διαδίκτυο είναι άναρχο και δεν ελέγχεται από κάποια υπηρεσία ή κρατική δομή στις δημοκρατικές χώρες, οι πολίτες βρίσκονται εκτεθειμένοι σε οποιοδήποτε περιεχόμενο και είδος πληροφοριών τυχόν διακινείται και το οποίο τυγχάνει να είναι συχνά μη έγκυρο, παραπλανητικό ή ανακριβές (Grosswald Levi).

Η πιθανότητα έκθεσης της ίδιας της χώρας και των πολιτών της σε πιθανές κυβερνοεπιθέσεις αυξάνονται καθώς η απουσία ελέγχου δυσκολεύει δραματικά τον εντοπισμό των επιτιθέμενων στον Κυβερνοχώρο (Jupillat Nicolas). Επίσης, σε αντίθεση με την πολιτική των αυταρχικών καθεστώτων όπως το αντίστοιχο της Κίνας, μέσω της πρόσβασης του Διαδικτύου πολλές και διαφορετικές κοινωνικές και πολιτικές ομάδες αντιφρονούντων δημιουργούν εντάσεις μεταξύ τους εξαπλώνοντας και σε άλλες χώρες τις αντίθετες με το δημοκρατικό πολίτευμα απόψεις τους προκαλώντας συχνά κρίσεις και εντάσεις που διαταράσσουν την ομαλή λειτουργία του συστήματος της χώρας.

Οι Η.Π.Α. – καθώς και οι υπόλοιπες δημοκρατικές χώρες που εκπροσωπούνται από αυτές- από τη μία πλευρά προσπαθούν να προστατεύσουν την κυριαρχία της δημοκρατίας των ανθρώπινων δικαιωμάτων, της ελευθερίας του λόγου και της πρόσβασης στην αντικειμενική και αμερόληπτη πληροφόρηση σε παγκόσμιο επίπεδο και από την άλλη πλευρά καλούνται να προστατεύσουν την έκθεση των προσωπικών τους ατομικών δεδομένων τα οποία εκτίθενται καθημερινά σε όλο το μήκος των τεχνολογικών εφαρμογών του Διαδικτύου τα οποία χρησιμοποιούν και μετατρέπονται σε εύκολα προσβάσιμο και εκμεταλλεύσιμο υλικό για αντίπαλες ομάδες - πολιτικές ή κοινωνικές- καθώς και ολόκληρες χώρες (Condron M. Sean). Τα σύγχρονα μέσα και δίκτυα πληροφοριών και τεχνολογίας εμπεριέχουν διττό τρόπο

αντιμετώπισης τους- θετικό ή αρνητικό- αναλόγως τους στόχους και τις προοπτικές των ατόμων ή χωρών και του τρόπου με τον οποίου πρεσβεύουν ότι τα χρησιμοποιούν (Jensen Talbot Eric).
Το Διαδίκτυο περιλαμβάνει πάντα μία σκοτεινή πλευρά η οποία αποτελεί μεγάλη πρόκληση για τη σύσταση του δημοκρατικού πολιτεύματος καθώς καλείται να ελεγχθεί ως προς τις λειτουργίες και τις υπηρεσίες που προσφέρει χωρίς ,ωστόσο, να περιοριστούν ή παραβιαστούν τα ανθρώπινα δικαιώματα και η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής.

Οι Η.Π.Α. αναγνωρίζουν τη βαρύτητα της ευθύνης τους απέναντι στην αντιμετώπιση του ψηφιακού αυταρχισμού και της παραβίασης των ψηφιακών ατομικών δικαιωμάτων καθώς όχι μόνο ιδρύθηκε το ίδιο το Διαδίκτυο στη δική τους επικράτεια αλλά και επειδή αποτελούνται από πολίτες διαφορετικών χωρών γεγονός που σηματοδοτεί την ανάγκη χρήσης και εξάπλωσης των τεχνολογικών εφαρμογών με θετικά διακείμενους τρόπους για συνεργασία και ομαλή συνύπαρξη και επικοινωνία μεταξύ των χωρών σεβόμενες τη διαφορετικότητα ως προς τη θρησκεία, το πολίτευμα, τα ήθη και τις αξίες καθεμίας εξ' αυτών (Crook R. John).

Κατά τη διάρκεια των τελευταίων ετών παρατηρείται μία όλο και αυξανόμενη τάση οργάνωσης και προγραμματισμού συγκεκριμένων πολιτικών και οικονομικών ενεργειών προς την παραπάνω κατεύθυνση. Σε συνεργασία με οργανισμούς, εταιρείες που ανήκουν στον τομέα της τεχνολογίας, ιδρύματα καθώς και κυβερνήσεις άλλων χωρών, οι Η.Π.Α. χρηματοδοτούν προγράμματα που υποστηρίζουν την ελευθερία και την προστασία των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο όπως το Bureau of Democracy και το Open Technology Fund. Μέσω των εκδηλώσεων και των μέσων μαζικής ενημέρωσης επιδιώκεται η θετική επιρροή του κοινωνικού συνόλου υπέρ των προτερημάτων ενός ελεύθερου άνευ ορίων και συνόρων Διαδικτύου (Daugirdas Kristina, Mortenson Davis Julian).

Επιπλέον, έμπρακτη και οργανωμένη προσπάθεια για την διασφάλιση των ψηφιακών δικαιωμάτων και των προσωπικών δεδομένων των πολιτών πραγματοποιείται από την εταιρεία Microsoft καθώς και από την Google, οι οποίες προσπαθούν μέσω της μεγάλης εμβέλειας και επιρροής που διαθέτουν - ως εταιρείες ορόσημο στο κυβερνοχώρο – να έρθουν σε επαφή με σημαντικές ομάδες συμφερόντων που προωθούν την ασφάλεια του Διαδικτύου και του απόρρητου των προσωπικών δεδομένων καθώς και να δημιουργήσουν τις κατάλληλες υποδομές για περαιτέρω επιστημονικές έρευνες και τεχνολογικές εφευρέσεις που θα ενισχύσουν τους παραπάνω σκοπούς.

Στην παραπάνω στοχοθεσία συμβάλλουν σε σημαντικό βαθμό και οι ακαδημαϊκές μελέτες μέσω των οποίων προτείνονται πρακτικές λύσεις και τεχνολογικά προγράμματα με τη μορφή ειδικών λογισμικών και πρωτοκόλλων σχεδιασμένων για την ομαλή λειτουργία και προστασία του Διαδικτύου. Ορισμένα χαρακτηριστικά προγράμματα που **προκύπτουν** από τη δράση του ακαδημαϊκού τομέα των Η.Π.Α. συμπεριλαμβάνουν το Media Lab και το Oxford Internet Institute.

Απαραίτητη για την κυβερνητική πολιτική των Η.Π.Α. είναι η δημιουργία νέων εργαλείων και προγραμμάτων από τους ειδικούς τεχνικούς που ανήκουν στο τομέα έρευνας και καινοτομίας του Κυβερνοχώρου καθώς και η οικονομική τους ενίσχυση για την εφεύρεση και δημιουργία των κατάλληλων τεχνικών και λειτουργικών υποδομών που θα είναι σε θέση να αντιμετωπίσουν το επικίνδυνο κύμα εξάπλωσης του ψηφιακού αυταρχισμού προστατεύοντας την αυτοκυριαρχία των χωρών μέσω της διασφάλισης των προσωπικών δεδομένων και της ροής των πληροφοριών με ελευθερία πρόσβασης στο Διαδίκτυο (Schmitt N. Michael (ed)).

5.4. ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΟ ΜΕΛΛΟΝ

Για την Κυβέρνηση

Τόσο οι Η.Π.Α όσο και οι υπόλοιπες χώρες που υποστηρίζουν την ελευθερία του Διαδικτύου οφείλουν να εναποθέτουν στους κατάλληλους κυβερνητικούς υπαλλήλους την δικαιοδοσία οριοθέτησης των επιμέρους νομοθετικών ρυθμίσεων σχετικά με το βαθμό και τον τρόπο πρόσβασης ,χρήσης και συλλογής των προσωπικών δεδομένων των πολιτών από οργανισμούς, εταιρείες ή δημόσιες υπηρεσίες (Melzer Nils) . Επίσης, οι πολίτες θα ήταν ωφέλιμο να έχουν τη δυνατότητα πρόσβασης ή και διαγραφής των ατομικών τους κινήσεων στο Διαδίκτυο και να υπάρξουν συγκεκριμένες νομοθετικές ρυθμίσεις που θα επιτρέπουν σε ορισμένες επείγουσες περιπτώσεις την πρόσβαση στα ψηφιακά δεδομένα των πολιτών από τρίτα πρόσωπα.

Προκειμένου να επιτευχθεί η ασφάλεια και η ελευθερία του Διαδικτύου σε παγκόσμιο επίπεδο ένα σημαντικό βήμα αποτελεί και η προσπάθεια άσκησης οικονομικών αποκλεισμών ή κυρώσεων σε τεχνολογικές εταιρείες που προωθούν σε αυταρχικά καθεστώτα - όπως η Κίνα -ειδικά λογισμικά προγράμματα επιτήρησης και λογοκρισίας πλήττοντας την διαφάνεια των προσωπικών ελευθεριών των πολιτών στο πλαίσιο του Κυβερνοχώρου.

Για τον ιδιωτικό τομέα

Οι ιδιωτικές εταιρείες και επιχειρήσεις θα μπορούσαν να καθοδηγήσουν την πολιτική τους με βάση τους ρυθμιστικούς κανόνες των Ηνωμένων Εθνών για τις επιχειρήσεις και τα ψηφιακά δικαιώματα προστατεύοντας το δικαίωμα απόκρυψης ή μη χρήσης και συλλογής των προσωπικών τους πληροφοριών χωρίς την αντίστοιχη ενημέρωση ή συγκατάθεσή τους.

Επιπρόσθετα, θα είναι σημαντική και η ενημέρωση και εκπαίδευση των εργαζομένων των ιδιωτικών εταιρειών ώστε να είναι σε θέση να αντιμετωπίσουν ενδεχόμενα υποκλοπής προσωπικών δεδομένων πελατών τους από πιθανές κυβερνοεπιθέσεις που θα σκόπευαν στην παραβίαση των ατομικών τους δικαιωμάτων.

ΕΠΙΛΟΓΟΣ

Η σύγχρονη ψηφιακή εποχή αποτελεί δραματική αλλαγή για τους ρυθμούς και τα δεδομένα της πολιτικής, οικονομικής και κοινωνικής ζωής τόσο σε συλλογικό επίπεδο μέσω των χωρών όσο και σε ατομικό επίπεδο μέσω των χρηστών του Διαδικτύου. Τα θετικά χαρακτηριστικά του Διαδικτύου μέσω των πολλαπλών τεχνολογικών δυνατοτήτων που προσφέρει είναι ταυτόχρονα σε θέση να μετατραπούν σε αρνητικά ανάλογα με τους σκοπούς και τις βλέψεις των εκάστοτε χωρών, κυβερνήσεων ή ατόμων που έχουν πρόσβαση στις υπηρεσίες του (International Law Association Study Group on the Conduct of Hostilities in the 21st Century).

Η αρχική του δημιουργία και σύσταση απέβλεπε στην ιδεολογική γραμμή της χώρας προέλευσης του – των Η.Π.Α.- η οποία αποσκοπεί στην ένωση των διαφορετικών χωρών του Παγκόσμιου Χάρτη σε ένα ενιαίο πολυδιάστατο τηλεπικοινωνιακό και διαδικτυακό ιστότοπο που θα ενισχύσει την άμεση και εποικοδομητική επικοινωνία και αρμονική ανταλλαγή ιδεών και πληροφοριών υπό το πρίσμα του Διεθνούς Δικαίου για την ομαλή συμβίωση των διάφορων κρατών στο πλαίσιο της ψηφιακής -πλέον- κοινότητας.

Ωστόσο, το Διαδίκτυο καλείται πλέον να προσαρμοστεί σε μία διαφορετική πραγματικότητα οριοθέτησης της ελεύθερης πρόσβασης σε αυτό από τους χρήστες του αποκλείοντας ταυτόχρονα την καταπάτηση των ατομικών τους δικαιωμάτων για ελευθερία έκφρασης, προστασίας της ιδιωτικής ζωής και των προσωπικών τους δεδομένων (Li Sheng) . Βασικό τροχοπέδη στην επίτευξη των παραπάνω στόχων αποτελεί ο αυστηρά ελεγχόμενος, περιοριστικός και διακατεχόμενος από λογοκρισία, επιτήρηση και απολυταρχικό έλεγχο τρόπος πρόσβασης των πολιτών στο Διαδίκτυο από αυταρχικά καθεστώτα.

Ως αποτέλεσμα- όπως είδαμε χαρακτηριστικά στην περίπτωση της ψηφιακής πολιτικής της Κίνας- το Διαδίκτυο απειλείται από διαχωρισμό της κοινότητας του στη Δύση και την Ανατολή, στη δημοκρατία και τα απολυταρχικά καθεστώτα καθώς και στην ελευθερία και την απαγόρευση, τον αποπροσανατολισμό και

την προπαγάνδα .Είναι επιτακτική , επομένως, η ανάγκη προστασίας των ψηφιακών δικαιωμάτων και κατ' επέκταση των ατομικών ανθρώπινων δικαιωμάτων καθώς και του δημοκρατικού πολιτεύματος ενάντια στην έμμεση επεκτατική οικονομική και πολιτική απειλή της Κίνας και αντίστοιχων αυταρχικών καθεστώτων στο πλαίσιο του Κυβερνοχώρου (Wingfield C. Thomas).

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Augustine P. Zachary, 'Cyber Neutrality: A Textual Analysis of Traditional Jus in. Bello Neutrality Rules through a Purpose - Based Lens' (2014) 71 A.F.L. Rev. 69
2. Biggio Giacomo, 'Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects' (2017) 15 Can. J. L. & Tech. 41
3. Bzostek Rachel, Why Not Preempt?: Security, Law, Norms and Anticipatory Military Activities (Ashgate Publishing 2008)
4. Checka Terence, 'Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach' (2015) 63 Clev. St. L. Rev. 495
5. Clayton Mark, 'Stuxnet Attack on Iran Nuclear Program Came About a Year Ago, Report Says' (2011) The Christian Science Monitor http://www.csmonitor.com/USA/2011/0103/Stuxnet-attack-on-Iran-nuclear-program-came-about-a-year-ago-re port-says"
6. Condron M. Sean, 'Getting it Right: Protecting American Critical Infrastructure in Cyberspace' (2007) 20 Harvard J.L. & Tech. 403
7. Crook R. John (ed), 'State Department Legal Adviser Addresses International Law in Cyberspace' (2013) 107 Am. J. Int'l L. 243
8. Daugirdas Kristina, Mortenson Davis Julian (eds) 'Contemporary Practice of the United States Relating to International Law' (2015) 109 Am. J. Int'l L. 873
9. DeLuca D. Christopher, 'The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors' (2013) 3 No. 9 Pace Int'l L. Rev. Online Companion 278 74
10. Dev R. Priyanka, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response' (2015) 50 Tex Int'l L.J.381
11. Gaul Allison, 'Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare' (2013) Syracuse J. Sci. & Tech. L. Rep. 51

12. Geiss Robin, ‘Cyber Warfare: Implications for Non-International Armed Conflicts’ (2013) Int’l L. Stud. |627
13. Gervais Michael, ‘Cyber Attacks and the Laws of War’ (2012) Berkeley J. Int'l Law 525
14. Grosswald Levi, ‘Cyberattack Attribution Matters Under Article 51 of the U.N. Charter’ (2011) 36 Brook. J. Int’l L. 1151
15. Halberstam Manny, ‘Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks’ (2013) 46 Geo. Wash. Int’l L. Rev. 199
16. Handler Gosnell Stephenie, ‘The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare’ (2012) 48 Stan. J. Int'l L. 209
17. Hathaway A. Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, ‘The Law of Cyber-Attack’ (2012) 100 Calif. L. Rev.817
18. Heintschel von Heinegg Wolff, ‘Territorial Sovereignty and Neutrality in Cyberspace’ (2013) 89 Int'l L. Stud. 123
19. Hoisington Matthew, ‘Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense’ (2009) 32 B.C. Int'l & Comp. L. Rev. 439
20. Iglezakis Ioannis , The Legal Regulation of Cyber Attacks (Kluwer Law International 2016)
21. International Law Association Study Group on the Conduct of Hostilities in the 21st Century, ‘The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare’ (2017) 93 Int’l L. Stud. 322
22. Internet World Stats, https://internetworldstats.com/
23. Jensen Talbot Eric, ‘Cyber Warfare and Precautions Against the Effects of Attacks’ (2010) 88 Tex. L. Rev. 1533
24. Jensen Talbot Eric, ‘Sovereignty and Neutrality in Cyber Conflict’ (2012) 35 Fordham Int'l L.J. 815
25. Jupillat Nicolas, ‘Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility’ (2015) 92 U. Det. Mercy L. Rev. 115
26. Kesan P. Jay, Hayes M. Carol, ‘Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace’ (2012) 25 Harv. J.L. & Tech. 429

27. Li Sheng, ‘When Does Internet Denial Trigger the Right of Armed Self-Defense?’ (2013) 38 Yale J. Int’l L. 179
28. Lin S. Herbert, ‘Offensive Cyber Operations and the Use of Force’ (2010) 4 J. Nat'l Sec. L. & Pol'y [i] 63
29. Lubell, Noam ‘Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?’ (2013) 89 Int’l L. Stud. 252
30. Margulies Peter, ‘Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility’ (2013) 14 Melb. J. Int'l L. 496
31. Melzer Nils, Cyberwarfare and International Law (United Nations Institute for Disarmament Research 2011)
32. Melzer Nils, International Humanitarian Law: A Comprehensive Introduction
33. Mudrinich M. Major Erik, ‘Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem’ (2012) Air Force Law Review 68 A.F. L. Rev. 167
34. David Lyon, Surveillance Society: Monitoring Everyday Life. By David Lyon, Buckingham: Open University Press, 2001. 189 pp.
35. Schmitt N. Michael (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017)
36. Wikipedia, Διαδίκτυο (2021), https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF
37. Schmitt N. Michael (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (1st edn, Cambridge University Press 2013)
38. Sharp Gary Walter, Sr, Cyberspace and the Use of Force (Aegis esearch Corporation 1999)
39. Tikk Eneken, Kaska Kadri, Vihul Liis, International Cyber Incidents: Legal Considerations (Cooperative Cyber Defense Centre of Excellence 2010)
40. Wingfield C. Thomas, The Law of Information Conflict: National Security Law in Cyberspace (Aegis Research Corp 2000)
41. WikiPedia Κυβερνοχώρος, https://el.wikipedia.org/wiki/%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%82#cite_note-3

42. Οικονομίδης Κωνσταντίνος, Δούση Εμμανουέλα, Το Δίκαιο της Ευθύνης των Κρατών για Διεθνείς Αδικοπραξίες (1η εκδ, Ι. Σιδέρης 2007)
43. Λενιώ Μυριβήλη (PHP), https://web.archive.org/web/20041030194259/http://www.aegean.gr/culturaltec/myrivili/cyberculture/default.htm
44. Αράπογλου Α., Μαβόγλου Χ., Οικονομάκος Η., Φύτρος Κ.., Βιβλιο Γυμνασίου Α,Β,Γ Πληροφορικής, ΠΑΙΔΑΓΩΓΙΚΟ ΙΝΣΤΙΤΟΥΤΟ, http://ebooks.edu.gr/ebooks/v/html/8547/2759/Pliroforiki_A-B-G-Gymnasiou_html-empl/indexA_4_1.html
45. NewSpot , «Τι μέγεθος έχει το Ίντερνετ - Πόσο γρήγορα μεγαλώνει», https://newpost.gr/tech/5c125c6256dccb7e13e3233c/ti-megethos-exei-to-internet-poso-grhgora-megalwnei (2016)
46. ΑΝΔΡΕΑΣ Ν. ΛΙΑΡΟΠΟΥΛΟΣ, Καθημερινή, 2016, https://www.kathimerini.gr/society/886704/apopsi-zitimata-asfaleias-ston-kyvernochoro/
47. Hong shen, Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative , International Journal of Communication December 2018, pages 2688-89. Ibid, page 2864.
48. "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism", Council on Foreign Relations,26 September 2019,online at:https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political
49. Andrew Liaropoulos, Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and TerrorismVolume 6 - Issue 2 , April-June 2016
50. Adam Segal, What's the Future of Chinese Hacking?, July 2016 https://motherboard.vice.com/en_us/article/ezpa5w/future-of-chinese-hacking
51. Desmond Ball, China's Cyber Warfare Capabilities , ANU Research Publications,2011
52. Jason Fritz,How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness, Culture Mandala, Vol. 8, No. 1, October 2008
53. Miguel Alberto Gomez,AWAKEN THE CYBER DRAGON: CHINA'S CYBER STRATEGY AND ITS IMPACT ON ASEAN https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_I mpact_on_ASEAN
54. Shirley Hung,, The Chinese INTEPNET: Control Through the Layers, October 30, 2012