ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Δ.Π.Μ.Σ.)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ ΚΑΙ ΤΜΗΜΑΤΟΣ ΝΟΜΙΚΗΣ ΔΗΜΟΚΡΙΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΡΑΚΗΣ

Διπλωματική Εργασία στο μάθημα «Ηλεκτρονικό Έγκλημα»

Τίτλος εργασίας : "Κυβερνοτρομοκρατία"

Επιβλέπων Καθηγητής: κ. Θεοχάρης Δαλακούρας

Email: theodalak@yahoo.gr

Ονοματεπώνυμο: Παρασκευή Διαβάτη

e-mail: mli20003@uom.edu.gr **Θεσσαλονίκη 10/12/2021**

Περιεχόμενα

Ευχαριστίες

Η παρούσα διπλωματική εργασία πραγματοποιήθηκε στο Πανεπιστήμιο Μακεδονίας , στο τμήμα εφαρμοσμένης πληροφορικής το 2022.

Η ολοκλήρωση της συγκεκριμένης μεταπτυχιακής διπλωματικής δεν θα ήταν δυνατή χωρίς την πολύτιμη συμβολή και εμπνευστή μου κατά την διάρκεια των μαθημάτων μας , του καθηγητή μου κ. Θεοχάρη Δαλακούρα.

Ένα μεγάλο ευχαριστώ πάει στην οικογένεια μου για την αμέριστη συμπαράσταση τους και την ανιδιοτελή αγάπη τους. Ιδιαίτερες δε ευχαριστίες στον πατέρα μου Αθανάσιο Διαβάτη,σ.δικηγόρο, για τις ατελείωτες ώρες συζήτησης αλλά και βοήθειας επι νομικών θεμάτων και απορριών μου.

Οι βαθύτερες όμως ευχαριστίες μου πάνε στον φίλο μου Λάμπρο Στέφου, αντισυνταγματάρχη των ενόπλων δυνάμεων ,για την συνεχή παρότρυνση του, την συνεχη στήριξη του και βοήθεια του κατά την διάρκεια και όχι μόνο αυτού του μεταπτυχιακού.

Σεπτέμβριος 2022

Εισαγωγή

Η εποχή που διανύουμε χαρακτηρίζεται από την αλματώδη εξέλιξη της τεχνολογίας. Δεν είναι τυχαίο ότι το ίδια άλματα παρατηρούσαμε επί δεκαετίες και πολύ πιθανόν να συναντήσουμε μεγαλύτερα άλματα στο μέλλον. Ο παράγοντας τεχνολογία είναι ένα έργο σε συνεχή εξέλιξη που δεν συναντά τροχοπέδη και έχει αποδείξει στο πέρασμα του χρόνου την ενεργητική του δράση στην ζωή του ανθρώπου. Έχει διευκολύνει την ζωή του ανθρώπου, έχει εξασφαλίσει την ποιότητα του βιοτικού επιπέδου του με περισσότερες αυτοματοποιημένες διαδικασίες και λιγότερες ανησυχίες για τα προβλήματα της καθημερινότητας του. Αρχικά ο άνθρωπος την χρησιμοποίησε για να μετατρέψει τις πρώτες ύλες σε χρήσιμα για αυτόν εργαλεία. Σήμερα χρησιμοποιεί την τεχνολογία αδιαλείπτως αφού έχει κατακλύσει την ζωή του παρέχοντας του τη δυνατότητα να την βελτιώνει σε πολλούς τομείς όπως η υγεία, η βιομηχανία, οι μεταφορές, οι πληροφορίες, η επικοινωνία κλπ. Ο ηλεκτρονικός υπολογιστής και το διαδίκτυο, δύο από τα πιο σπουδαία επιτεύγματα της τεχνολογίας, και γενικότερα η ανάπτυξη του τομέα της πληροφορίας είναι τα στοιχεία που συνέβαλαν κατά κύριο λόγο στη βελτίωση της ποιότητας της καθημερινής ζωής του ανθρώπου και γενικά της κοινωνικής και οικονομικής ευημερίας.

Η δε εποχή της πανδημίας μπορεί να έφερε την Ελλάδα αντιμέτωπη με τον υφιστάμενο τεχνολογικό αναλφαβητισμό αλλά μέσα σε ελάχιστο χρονικό διάστημα κατάφερε να ανακτήσει έδαφος και να φέρει την ψηφιακή ανάπτυξη όχι μόνο στην καθημερινή ζωή των ανθρώπων, σε τομείς όπως είναι η εκπαίδευση, η επικοινωνία, η επιστήμη κ.α., αλλά και στις κοινωνικές, πολιτικές και οικονομικές συνθήκες διαβίωσης. Αποτέλεσμα αυτού είναι να προσφέρεται η δυνατότητα να πραγματοποιούνται συναλλαγές σε πραγματικό χρόνο πλέον καθημερινά, διευκολύνοντας τόσο τη ζωή των πολιτών όσο και την οικονομική ζωή της χώρας. Οι συναλλαγές με το Δημόσιο ή τους ιδιώτες διεκπεραιώνονται μέσω των ηλεκτρονικών συστημάτων των τραπεζών (e-banking), συνταγογραφήσεις γίνονται άυλα και χωρίς την ταλαιπωρία των πολιτών με αναμονές και σπατάλη πολύτιμου χρόνου. Βεβαίως η προαναφερθείσα εξέλιξη

της τεχνολογίας υποστηρίζεται από πολλά επιχειρήματα, άλλα υπέρ και άλλα κατά αλλά είναι άδικο να ποινικοποιούμε την τεχνολογία για τον τρόπο που οι άνθρωποι την εκμεταλλεύονται.

Ο κόσμος του διαδικτύου δίνει πρόσβαση σε μια τεράστια ποσότητα πληροφοριών. (Κακαβούλης, 2018) (License, 2022) Οι πληροφορίες που αντλούνται από το διαδίκτυο σε συνδυασμό με την τεχνική υποδομή του διαδικτύου αποτελούν τον λεγόμενο κυβερνοχώρο (cyberspace). Πρόκειται για έναν κόσμο που ξεπερνά κάθε φυσικό περιορισμό. Αυτό σημαίνει ότι είναι ένας «άναρχος κόσμος» όπως έχει πει και ο Hedley Bull: " Το ποιος ελέγχει ποιόν, τι υπακούει σε ποιους κανόνες και που αρχίζουν και που τελειώνουν οι εν λόγω κανόνες, παραμένει ένα αναπάντητο ερωτηματικό". Στην πραγματικότητα, ο κυβερνοχώρος μπορεί να θεωρηθεί ως η διασύνδεση των ανθρώπων μέσω υπολογιστών και τηλεπικοινωνιών, ανεξάρτητα από τη φυσική γεωγραφία.

Ο Κυβερνοχώρος αποτελείται από το σύνολο των παγκόσμιων δικτύων και των περιφερειακών τους μηχανημάτων, όπως δρομολογητές, ρούτερ, εκτυπωτές, μέσω της σύνδεσης των οποίων πραγματοποιείται η επεξεργασία και η ροή των πληροφοριών. Επίσης στον κυβερνοχώρο περιλαμβάνεται και το σύνολο των εσωτερικών δικτύων, τα οποία είναι εγκατεστημένα στο δημόσιο τομέα, στις τράπεζες, σε διάφορους οργανισμούς, στις ένοπλες δυνάμεις (εσωτερικά δίκτυα διοίκησης και ελέγχου, δίκτυα οπλικών συστημάτων όπως αρμάτων, αεροσκαφών, πολεμικών πλοίων, δορυφόρων κλπ). Ορθά λοιπόν έχει χαρακτηριστεί ως ένας «παγκόσμιος προσβάσιμος ψηφιακός χώρος».

Η μεγάλη μάχη στον κυβερνοχώρο δίδεται για την πληροφορία η οποία είναι η αιτία και ο στόχος συχνών πλέον κυβερνοεπιθέσεων. Τα πληροφοριακά συστήματα τα οποία εξυπηρετούν την καθημερινότητα των χρηστών, βοηθώντας τους να εκμεταλλευτούν όλες τις παρεχόμενες δυνατότητες των ηλεκτρονικών υπολογιστών, δεν είναι άτρωτα. Υπάρχουν πληροφορίες που εκμεταλλεύονται κακόβουλοι χρήστες και γνώστες της τεχνολογίας όπως κωδικοί πρόσβασης που πληκτρολογούνται, φωτογραφίες που αναρτώνται στα κοινωνικά μέσα δικτύωσης, διευθύνσεις κατοικίας ή εργασίας κ.α., με την

κατάλληλη επεξεργασία των οποίων πραγματοποιούνται αξιόποινες πράξεις εναντίον των καλόπιστων και αφελών χρηστών των ηλεκτρονικών υπολογιστών. Εύκολα συμπεραίνει κανείς ότι το μέσο που βελτιώνει σημαντικά την καθημερινότητα των χρηστών τους κάνει ευάλωτους και τους θυματοποιεί. Έτσι λοιπόν, λόγω της συνεχούς δικτύωσης των ηλεκτρονικών υπολογιστών τα νομικά ζητήματα που ανακύπτουν για την αντιμετώπιση των κυβερνοεγκλημάτων έγιναν πολυπλοκότερα και η ανάγκη της νομικής αντιμετώπισης των συνεχώς νεοεμφανιζόμενων εγκληματικών συμπεριφορών πιο επιτακτική.

Η συγκεκριμένη λοιπόν εργασία θα ασχοληθεί με τα εγκλήματα στον κυβερνοχώρο και κυριότερα με την κυβερνοτρομοκρατία. Όπως προαναφέρθηκε η τεχνολογία και δη το διαδίκτυο αποτελεί ίσως το κύριο και το πιο αποτελεσματικό μέσο δραστηριοποίησης της τρομοκρατίας. Έτσι λοιπόν όσο αναπτύσσονται τα κράτη τόσο μεγαλύτερη είναι η εξάρτηση τους από υψηλής κλίμακας τεχνολογικές εφαρμογές ή διαδικασίες συνδεδεμένες με εθνικές υποδομές. Διάφορα και πολύπλοκα εθνικής εμβέλειας συστήματα τεχνολογίας, παρουσιάζονται ως πιθανοί στόχοι, και με μεγάλο κίνδυνο να υποστούν επιθέσεις με καταστροφικά αποτελέσματα. Όπως θα αναλυθεί παρακάτω οι επιθέσεις αυτές μπορεί να πραγματοποιηθούν είτε με τη χρήση υπολογιστών π.χ. κατάρρευση των συστημάτων ελέγχου μιας σημαντικής κρατικής δομής για παράδειγμα ενός αεροδρομίου, είτε με την χρήση εκρηκτικών υλών η οποία αποτελεί και την «παραδοσιακότερη μορφή άσκησης βίας».

Κεφάλαιο 1

Γενικές έννοιες

1.1. Κυβερνοέγκλημα

Ως κυβερνοέγκλημα ορίζεται «οποιοδήποτε έγκλημα στο οποίο εμπλέκεται ηλεκτρονικός υπολογιστής και ένα δίκτυο». Το Βικιλεξικό αναφέρεται στο κυβερνόεγκλημα ως «ηλεκτρονικό έγκλημα που διαπράττεται με χρήση δικτύων υπολογιστών και κυρίως μέσω του διαδικτύου». Ο

υπολογιστής χρησιμοποιείται είτε για την τέλεση του εγκλήματος είτε ως στόχος της εγκληματικής πράξης. Άλλος ορισμός του κυβερνοεγκλήματος αναφέρεται σε αδικήματα κατά του ατόμου ή ομάδα ατόμων με σκοπό την βλάβη της υπόληψης του θύματος προκαλώντας του ψυχική, φυσική βλάβη, έμμεση ή άμεση απώλεια, χρησιμοποιώντας είτε το διαδίκτυο είτε κινητό τηλεφώνο (sms/mms). Άρα ως κυβερνοέγκλημα μπορούν να οριστούν οι παράνομες ψηφιακές ενέργειες που σκοπό έχουν να προκαλέσουν βλάβη σε επιχειρήσεις ή φυσικά πρόσωπα. Γίνεται όμως αντιληπτό ότι στην κατηγορία του κυβερνοεγκλήματος εντάσσονται κι άλλες έννοιες όπως η κυβερνοαπάτη, η κυβερνοτρομοκρατία, ο κυβερνοεκβιασμός και ο κυβερνοπόλεμος, έννοιες συναφείς με το κυβερνοέγκλημα αλλά όχι ίδιες.

Το βασικότερο αίτιο του εγκλήματος στον κυβερνοχώρο, εντοπίζεται στον ευάλωτο χαρακτήρα των συστημάτων πληροφοριών. Η ευάλωτη φύση των εν λόγω συστημάτων συνίσταται από το τεράστιο πλήθος πληροφοριών στο διαδίκτυο, γεγονός που τα καθιστά αντικείμενο άμεσης επίθεσης και παρεμβολής. Διαπιστώνεται πως η προσπάθεια προστασίας τους με την θέσπιση νομικού πλαισίου είναι ανεπαρκής. Άλλωστε για να υπάρχει αποτέλεσμα στην καταστολή των εγκλημάτων που τελούνται στο διαδίκτυο πρέπει να καταργηθούν τα σύνορα και τα εδαφικά όρια και να υπάρξει διεθνής δράση. Ας μην ξεχνάμε ότι ο κυβερνοχώρος από πολλούς χαρακτηρίζεται ως ο πέμπτος χώρος (μετά το έδαφος ,την θάλασσα, τον αέρα και το διάστημα) ή η Πέμπτη εικονική διάσταση η οποία δεν χαρακτηρίζεται από γεωγραφικά, εθνικά ή χρονικά όρια και δεν υπάρχουν ιδιοκτησίες και νόμοι.

Τα κύρια λοιπόν χαρακτηριστικά του κυβερνοεγκλήματος τα οποία καθιστούν την ποινική του δίωξη δυσχερή είναι :

1. Η Ταχύτητα – Η διάπραξη των σχετικών πράξεων λαμβάνει χώρα σε ελάχιστο χρόνο και συχνά δεν γίνεται αντιληπτή από το θύμα.

2. Η Ευκολία – Η διάπραξη των σχετικών πράξεων είναι εύκολη και γίνεται από τον ηλεκτρονικό υπολογιστή και τον οικείο χώρο του δράστη.

3. Η Ανωνυμία – Η διάπραξη κυβερνοεγκλημάτων εκμεταλλεύεται την σχετική ανωνυμία, που προσφέρουν οι τεχνολογικές υποδομές του διαδικτύου.

4. Ο Διασυνοριακός Χαρακτήρας – Οι προπαρασκευαστικές ενέργειες, οι πράξεις αλλά και τα αποτελέσματα του κυβερνοεγκλήματος συνήθως λαμβάνουν χώρα ταυτοχρόνως σε πολλές χώρες.

5. Η Δυσχέρεια στην Διερεύνηση – Ο διασυνοριακός χαρακτήρας αλλά και τα ψηφιακά ίχνη του κυβερνοεγκλήματος δυσχεραίνουν τη διερεύνηση και εξιχνίασή του.

6. Η Διακρατική Συνεργασία – Ο διασυνοριακός χαρακτήρας του κυβερνοεγκλήματος απαιτεί την διακρατική συνεργασία των διωκτικών αρχών.

7. Η Έλλειψη Επαρκούς Καταγραφής – Το μέγεθος των τελούμενων κυβερνοεγκλημάτων είναι δυσανάλογα μεγαλύτερο των καταγραφόμενων περιστατικών. (Broumas, 2015)

Το κυβερνοέγκλημα, από μία εγκληματολογική σκοπιά, διαθέτει μοναδικά χαρακτηριστικά, καθότι σε καμία περίπτωση δεν μπορεί να θεωρηθεί ότι ανήκει στην κατηγορία των εγκλημάτων βίας. Βασικό στοιχείο της τέλεσης των κυβερνοεγκλημάτων, τουλάχιστον υπό μία ευρύτερη έννοια, είναι ο διασυνδεδεμένος ηλεκτρονικός υπολογιστής σε σύστημα πληροφοριών, είτε ως στόχος επίθεσης, είτε ως το βασικό όργανο της επίθεσης, είτε ως ένα βοηθητικό εργαλείο για τη διάπραξη της επίθεσης.

1.2 Κυβερνοεπιθέσεις

Οι κυβερνοεπιθέσεις αποτελούν παράνομη προσπάθεια πρόσβασης στις πληροφορίες ενός οργανισμού και στόχο έχουν την διατάραξη της ομαλής λειτουργίας του. Είναι γεγονός ότι καταγράφονται καθημερινά εκατομμύρια επιθέσεις καθημερινά σε επιχειρήσεις και οργανισμούς. Το κίνητρο μπορεί να διαφέρει, η επίθεση μπορεί να σχετίζεται με εγκληματική πράξη, κατασκοπία, πολιτικούς αντιπάλους ή απλώς με ερασιτέχνη χάκερ. Μια γρήγορη αναζήτηση στο διαδίκτυο δείχνει την συχνότητα που λαμβάνουν μέρος σε διάφορα σημεία του πλανήτη. Οι κυβερνοεπιθέσεις γίνονται με την χρήση του διαδικτύου σε σύστημα υπολογιστών με σκοπό την πρόκληση βλάβης ή δυσλειτουργίας.

Ο τρόπος μιας κυβερνοεπίθεσης μπορεί να έχει διάφορες μορφές:

1. **Phishing**

Το ηλεκτρονικό "ψάρεμα" είναι μια μορφή ψηφιακών επιθέσεων κατά την οποία οι εγκληματίες μιμούνται μια αξιόπιστη ή νόμιμη πηγή, ζητώντας συνήθως ευαίσθητες και προσωπικές πληροφορίες όπως κωδικούς πρόσβασης ή / και στοιχεία λογαριασμού του θύματος. Οι απάτες ηλεκτρονικού "ψαρέματος" απευθύνονται συνήθως στα θύματά τους μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μια προσπάθεια την προσέλκυση ατόμων ή ομάδων να επισκεφθούν μια ιστοσελίδα, να συμπληρώσουν ένα ψεύτικο έντυπο ή να κατεβάσουν ένα συνημμένο αρχείο.

2. Malware

Το malware περιγράφει γενικά αυτό που λέμε "κακόβουλο λογισμικό". Περιλαμβάνει κάθε μορφή κακόβουλου κώδικα που έχει σχεδιαστεί ειδικά για να διεισδύσει σε υπολογιστή ή συσκευή χωρίς εξουσιοδότηση. Αυτός ο όρος χρησιμοποιείται για να συμπεριλάβει όλους τους διάφορους τύπους κακόβουλου λογισμικού, από ιούς υπολογιστών έως ιούς τύπου Trojan horse, ανεξάρτητα από τον τρόπο με τον οποίο προσβάλλει τα θύματα, τον τρόπο συμπεριφοράς ή τις ζημιές που προκαλεί. Αν και το malware δεν προκαλεί ζημιά σε επίπεδο hardware, μπορεί να κλέψει, να διαγράψει και να καταλάβει τα δεδομένα του θύματος, ενώ κατασκοπεύει τη δραστηριότητά του χωρίς να το θύμα να το γνωρίζει.

3. Spam

Το spam είναι μια ψηφιακή έκδοση του ανεπιθύμητου ηλεκτρονικού ταχυδρομείου. Περιγράφεται ως οποιαδήποτε μορφή ανεπιθύμητης επικοινωνίας που αποστέλλεται μαζικά (Unsolicited Bulk Email, ή UBE) η πιο κοινή μορφή του οποίου είναι ένα εμπορικό email (Unsolicited Commercial Email, UCE). Αυτά τα emails αποστέλλονται από μια ανώνυμη πηγή σε έναν μεγάλο αριθμό διευθύνσεων, ώστε ακόμα και αν λίγοι άνθρωποι ανταποκριθούν, ο αποστολέας να βγαίνει και πάλι κερδισμένος. Ωστόσο, το spam αποστέλλεται ακόμα και μέσω υπηρεσιών άμεσων μηνυμάτων, είτε ως απλό κείμενο, είτε μέσω των καναλιών επικοινωνίας των κοινωνικών δικτύων.

4. Trojan Horse

Ένας Δούρειος Ίππος είναι μια μορφή κακόβουλου λογισμικού που χρησιμοποιεί μεταμφίεση για να κρύψει τον πραγματικό σκοπό του, προκειμένου να διεισδύσει σε μια συσκευή ή ένα σύστημα ασφαλείας. Τα Trojan μιμούνται νόμιμο λογισμικό για να κερδίσουν την εμπιστοσύνη των θυμάτων τους και κατόπιν δίνουν πρόσβαση σε κυβερνοεγκληματίες επιτρέποντάς τους να κλέψουν, να διαγράψουν, να μπλοκάρουν, να αντιγράψουν ή να τροποποιήσουν ευαίσθητα δεδομένα.

5. **Υποκλοπή Ταυτότητας χρήστη (identity theft)**

Η υποκλοπή ταυτότητας είναι ένα έγκλημα στο οποίο ένας εισβολέας χρησιμοποιεί εξαπάτηση για να αποκτήσει ευαίσθητες πληροφορίες από ένα θύμα και στη συνέχεια να καταχραστεί τα δεδομένα αυτά ενεργώντας στο όνομα του θύματος. Οι δράστες συνήθως υποκινούνται από παράνομους σκοπούς, όπως αιτήσεις για έκδοση πιστωτικών καρτών ή δανείων, πραγματοποίηση ηλεκτρονικών αγορών ή προκειμένου να αποκτήσουν πρόσβαση σε προσωπικά και οικονομικά στοιχεία. Οι εγκληματίες συχνά χρησιμοποιούν μεθόδους ηλεκτρονικού "ψαρέματος" (phishing) και άλλες τεχνικές κοινωνικής μηχανικής και ενίοτε εκμεταλλεύονται την πρόσβαση σε δημόσια προφίλ κοινωνικών δικτύων ώστε να μιμηθούν τα θύματά τους.

6. **Επιθέσεις σε διαδικτυακές εφαρμογές (web application attacks)**

Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.

7. **Παραβιάσεις προσωπικών δεδομένων**

Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.

8. **Εσωτερικές απειλές (insider threat)**

Απειλές που προέρχονται από στελέχη Φορέων που εργάζονται ή εργάζονταν σε έναν Οργανισμό, καθώς και εξωτερικών συνεργατών, οι οποίοι κατέχουν εσωτερική πληροφόρηση σχετικά με τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων που περιγράφονται στην παρούσα ενότητα, συνήθως με πολύ μεγάλο αντίκτυπο για τον Φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή/και αντιμετωπισθούν.

9. Botnets

Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.

10. Φυσικές απειλές

Απειλές που στοχεύουν στην καταστροφή ή αλλοίωση ή κλοπή εξοπλισμού, με απώτερο στόχο την διαρροή ή/και καταστροφή δεδομένων ή την άρνηση υπηρεσίας.

11. Διαρροή δεδομένων

Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.

12. Cryptojacking

Τεχνικές που χρησιμοποιούν την υπολογιστική ισχύ του υπολογιστή του χρήστη με σκοπό την άντληση (mining) κρυπτονομισμάτων (bitcoins).

13. Επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS attacks)

Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την

πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας). (ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ, 2020)

14. Ransomware

Είναι ένας τύπος κακόβουλου λογισμικού που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει το περιεχόμενό της, εμποδίζοντας τον χρήστη από την πρόσβαση στα προσωπικά του αρχεία με σκοπό την καταβολή λύτρων. Σε αντάλλαγμα, οι εγκληματίες υπόσχονται - βεβαίως, χωρίς εγγυήσεις - να αποκαταστήσουν την πρόσβαση στο μολυσμένο μηχάνημα ή τα δεδομένα. Το Ransomware μπορεί να εμφανίζεται με πολλές διαφορετικές μορφές. Η πιο συχνή μορφή είναι ένα αναδυόμενο παράθυρο στο desktop του υπολογιστή, όπου οι χρήστες πρέπει να είναι ιδιαίτερα προσεκτικοί για ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που θα μπορούσαν να τους εξαπατήσουν και να παρασυρθούν σε επικίνδυνους ιστότοπους ή συνδέσμους λήψης. (eset.com, 2001)

Το ransomware θεωρείται ως η μάστιγα του διαδικτύου. Η έννοια ransomware έγινε γνωστή σε μεγάλη μερίδα του πλανήτη μετά την επίθεση που δέχθηκε το Βρετανικό σύστημα υγείας NHS το 2017, μια επίθεση που δεν στόχευε το σύστημα υγείας αλλά προκάλεσε ένα ντόμινο προβλημάτων σε 150 χώρες και προκαλώντας ζημιά σε περίπου 250.000 μηχανήματα παγκοσμίως. Πολλές οργανωμένες εγκληματικές συμμορίες προσπαθούν συνεχώς να αποκτήσουν πρόσβαση σε δίκτυα υπολογιστών για να τους κρατήσουν όμηρους. Η στατιστική επιθέσεων μπορεί να δίνει υψηλό δείκτη δράσης, αλλά μπορεί να χρειαστεί πολύς χρόνος και προσπάθεια από τους εγκληματίες για να χτυπήσουν με επιτυχία το σύστημα υπολογιστή ενός θύματος.

Τον Ιούλιο στις Ηνωμένες Πολιτείες της Αμερικής χάκαραν παράλληλα 200 εταιρείες εφοδιασμού, στο οποίο οι χάκερς έδειξαν ότι ακολουθώντας τον προμηθευτή λογισμικού πολλαπλών οργανισμών μπορούν να έχουν δεκάδες, ίσως εκατοντάδες θύματα με μία κίνηση. Έχουμε δει αλυσιδωτές επιθέσεις στο παρελθόν, αλλά αυτό ίσως είναι το μεγαλύτερο περιστατικό που αφορά το ransomware γεγονός που αποδεικνύει ότι οι συμμορίες ransomware σκέφτονται δημιουργικά για να προκαλέσουν τον μεγαλύτερο αντίκτυπο και να ζητήσουν τα περισσότερα λύτρα. Το συνολικό παγκόσμιο κέρδος που

αποκομίζουν οι συμμορίες ηλεκτρονικού εγκλήματος εκτιμάται σε 1,3 τρισεκατομμύρια τον χρόνο. Οι ειδικοί που ασχολούνται με την κυβερνοασφάλεια συμβουλεύουν την μη διαπραγμάτευση και μη καταβολή των λύτρων. Πάραυτα το 45% των επιχειρήσεων/ οργανισμών που θα πέσουν θύματα επιθέσεων θα καταβάλουν τα λύτρα με το μεγαλύτερο ποσοστό αυτών να χάνουν και τα χρήματα τους αλλά και τα δεδομένα τους. (Γιάννης Γορανίτης, 2021)

Μια πολύ σημαντική επίθεση η οποία καταγράφηκε μέσα στο 2021 ήταν αυτή της εταιρείας Colonial Pipeline. Οι εκβιαστές λοιπόν χρησιμοποίησαν το κακόβουλο λογισμικό της DarkSide για να κρυπτογραφήσουν τα υπολογιστικά συστήματα της εταιρείας και να την υποχρεώσουν να καταβάλει περίπου 5 εκατ. δολάρια για να ανακτήσει και πάλι τον έλεγχο των συστημάτων της. Η κλίμακα της συγκεκριμένης επίθεσης στον αγωγό πετρελαίου και η απειλή που δημιουργήθηκε για την ενεργειακή αυτονομία της χώρας σήμανε συναγερμό στις αμερικάνικες αρχές. Γι’ αυτό λοιπόν το Υπουργείο Δικαιοσύνης των Ηνωμένων Πολιτειών ζήτησε να αποκτήσει η αντιμετώπιση της εν λόγω μορφής κυβερνοεπιθέσεων ισάξια προτεραιότητα με την καταπολέμηση της τρομοκρατίας. (Γιάννης Γορανίτης, 2021).

1.3 Τρομοκρατία

Δυστυχώς τα τελευταία 30 χρόνια δεν είναι δυνατή η ομοφωνία διεθνώς ενάντια στην τρομοκρατία. Στην δεκαετία του ’80 δόθηκαν δυο από τους τρεις ορισμούς που αφορούν την Τρομοκρατία και που θεωρούνται αποδεκτοί από πολλές πλευρές.

1. Ο πρώτος ορισμός (1983), δόθηκε από το Στέιτ Ντιπάρτμεντ των ΗΠΑ στο "Title 22 of the United States Code, Section 2656(d)", ως ακολούθως: «μια προσχεδιασμένη βίαιη ενέργεια, στρεφόμενη ενάντια σε άμαχους στόχους, που πραγματοποιείται από υποεθνικές ή μυστικές ομάδες με πολιτικά κίνητρα, οι οποίες συχνά επιθυμούν να ασκήσουν επιρροή σε ένα ακροατήριο - στόχο.»

2. Ο δεύτερος (1988) προέρχεται από τους επιστήμονες Άλεξ Σμιντ (Alex P. Schmid) και Άλμπερτ Γιόνγκμαν (Albert J. Jongman) και είναι ο παρακάτω:

«Η τρομοκρατία είναι μια μέθοδος επαναλαμβανόμενων πράξεων βίας, στην οποία εμπλέκονται σχετικά κρυφά άτομα, ομάδες ή κρατικοί δρώντες, λόγω ιδιοσυγκρασίας, εγκληματικών ή πολιτικών λόγων, και όπου, σε αντίθεση με τη δολοφονία, οι άμεσοι στόχοι της βίας δεν αποτελούν και τον απώτερο σκοπό αυτής. Τα δε άμεσα θύματα επιλέγονται τυχαία ή μέσω συμβολικής στοχοποίησης, ως μέρος ενός ευρύτερου πληθυσμού-στόχου στον οποίο αποσκοπεί η πράξη, λειτουργώντας ως μήνυμα προς αυτόν. Έτσι, διαμέσου του θύματος, αποκαθίσταται μια επικοινωνία μεταξύ των δρώντων και του ακροατηρίου-στόχου, μέσω της επιδίωξης τρομοκράτησης, της προβολής απαιτήσεων ή της έλκυσης προσοχής, ανάλογα με την τελική στόχευση, που μπορεί να είναι ο εκφοβισμός, ο πειθαναγκασμός ή η προπαγάνδα.»

3. Ο τρίτος ορισμός (1997), υιοθετήθηκε από τη Γενική Συνέλευση του Οργανισμού Ηνωμένων Εθνών (Resolution 51/210) και ορίζει ως Τρομοκρατία: «...τις εγκληματικές ενέργειες που αποσκοπούν στην πρόκληση φόβου, είτε στο σύνολο της κοινωνίας είτε σε μια ομάδα ατόμων είτε σε μεμονωμένα άτομα, έχοντας ως κίνητρο πολιτικές στοχεύσεις. Οι πράξεις αυτές είναι σε κάθε περίπτωση μη δικαιολογημένες, άσχετα από τη φύση των εθνικών, θρησκευτικών, φιλοσοφικών, ιδεολογικών, πολιτικών, φυλετικών, θρησκευτικών κινήτρων που επικαλούνται οι δράστες» (Βικιπαίδεια, 2021).

Κεφάλαιο 2

Ιστορική Αναδρομή

Το φαινόμενο της τρομοκρατίας έκανε την εμφάνιση του τον 11ο περίπου αιώνα με τους Ασσασίνους, μια αποσχισμένη από τους Σιίτες μουσουλμανική ομάδα, η οποία είχε διακριτά όλα τα χαρακτηριστικά μιας τρομοκρατικής ομάδας όπως την ξέρουμε σήμερα. Οι Ασσασίνοι είχαν υιοθετήσει την πρακτική της δολοφονίας των εχθρικών ηγετών επειδή η λατρεία τους δεν επέτρεπε την ανοιχτή σύγκρουση.

Παρά το γεγονός ότι οι Ασσασίνοι και οι Ζηλωτές ενήργησαν αιώνες πριν, παρατηρούμε ότι οι δράσεις και οι μεθοδεύσεις τους είναι ίδιες με τις σημερινές τρομοκρατικές πρακτικές. Μάλιστα θεωρούνται πρωτεργάτες της σύγχρονης τρομοκρατίας ως προς την επιλογή στόχων, σκοπών αλλά και την

οργάνωση. Παρά το γεγονός ότι οι ενέργειες τους δεν είχαν επιτυχία, θα έλεγε κανείς ότι έχουν παραμείνει γνωστοί στην ιστορία για την τεράστια ψυχολογική βία που άσκησαν οι πρακτικές τους.

Η τρομοκρατία αποτέλεσε και συνεχίζει να αποτελεί όπλο του αδυνάτου και του καταπιεσμένου απέναντι σε μια μεγαλύτερη δύναμη. Ο τρόμος υπήρξε μια από τις βασικότερες πρακτικές στις στρατιωτικές επιχειρήσεις. Επί αιώνες, πολέμαρχοι προσέφευγαν στην πρακτική του τρόμου, με παραδειγματικές πράξεις σκληρότητας και βιαιότητας για να καταφέρουν να κάμψουν την θέληση του αντιπάλου τους. (βλ. οθωμανικός στρατός). Η τρομοκρατία έχει χρησιμοποιηθεί πολλές φορές και από κυβερνητικές υπηρεσίες ή κυβερνητικούς παράγοντες - φορείς δημιουργώντας την έννοια της κρατικής τρομοκρατίας που παρατηρείται ιστορικά από την αρχαιότητα και διαιωνίζεται μέχρι σήμερα. Μια αρκετά κοινή, στην σύγχρονη ζωή, μορφή τρομοκρατίας είναι αυτή των Μέσων Μαζικής Ενημέρωσης τα οποία στην προσπάθεια τους να επιτύχουν μεγάλα νούμερα τηλεθέασης αναπαράγουν και δίνουν φωνή σε εξτρεμιστικές οργανώσεις.

Τα βασικά χαρακτηριστικά της τρομοκρατίας είναι η ανωνυμία των μελών (όχι όμως και των οργανώσεων), οι δολοφονίες, οι βομβιστικές επιθέσεις, οι αεροπειρατείες κ.α. Όλες αυτές οι ενέργειες βασίζονται στα στοιχεία του αιφνιδιασμού και του φανατισμού είτε αυτός είναι ιδεολογικός είτε είναι θρησκευτικός. Η βασική επιδίωξη των τρομοκρατικών πλέον χτυπημάτων, στην σημερινή εποχή είναι να πλήξουν όσο το δυνατόν μεγαλύτερο αριθμό αμάχων και ανυποψίαστων πολιτών.

Ένα από τα βασικότερα όπλα της τρομοκρατίας είναι η πρόκληση οικονομικών πληγμάτων σύμφωνα με το οποίο η χώρα που δέχεται το πλήγμα εμφανίζεται αδύναμη, ανίκανη να αντιμετωπίσει την δράση της (της τρομοκρατίας), λίγοτερο αξιόπιστη για τα οικονομικά συμφέροντα των ξένων επενδυτών και συνεπώς επικίνδυνη για τους ξένους επισκέπτες. Με αυτό τον τρόπο επηρεάζει την οικονομία μια χώρας - στόχου σε καίριους τομείς όπως ο τουρισμός. Επιπρόσθετα μια τρομοκρατική επίθεση δύναται να κατευθυνθεί σε στόχους - σύμβολα όπως για παράδειγμα το Παγκόσμιο Κέντρο Εμπορίου της

Νέας Υόρκης (2001) ώστε να επιφέρει σημαντικό πλήγμα με μια μόνο ενέργεια. (Πάπυρος Larousse Britannica, 2006).

Το χτύπημα στους Δίδυμους πύργους στο παγκόσμιο κέντρο εμπορίου άλλαξε την παγκόσμια αντίληψη της τρομοκρατίας. Οι απώλειες εκείνη την ημέρα στη Νέα Υόρκη και το Πεντάγωνο ανήλθαν στις 6.000 ανθρώπους. Παρά το μέγεθος των απωλειών στο εν λόγω χτύπημα, έρευνες αποδεικνύουν ότι οι απώλειες από την καθημερινή βία είναι πολύ μεγαλύτερες.

Δεν είναι δύσκολο να αντιληφθεί κανείς τον τρόμο που προκάλεσαν οι μαζικές τρομοκρατικές επιθέσεις στην αρχή του 21ου αιώνα. Τα ΜΜΕ παγκοσμίως έπαιξαν τεράστιο ρόλο στην διαμόρφωση της κοινής γνώμης. Οι τρομοκράτες σήμερα «γνωρίζουν πλέον πως η κατοχή του απαραίτητου υλικοτεχνικού εξοπλισμού συνδυαστικά με τη δημιουργία εκείνων των εικόνων που είναι σε θέση να εγγυηθούν τη μέγιστη προσέλκυση των μέσων στο κατάλληλο χρόνο, αποτελεί δικλείδα ασφαλείας για την επιτυχία». (Μαρία Κουτσανδριά, 2020)

Αντιλαμβανόμαστε λοιπόν ότι τα Μέσα ενημέρωσης έχουν αναμφίβολα ψυχολογικό αντίκτυπο στις κοινωνίες βάζοντας σε δεύτερη μοίρα τα πολιτικά, ιδεολογικά ή και θρησκευτικά κίνητρα του τρομοκράτη. Με την λέξη «τρομοκρατία» έχουν περιγραφεί μέσα στην πάροδο των χρόνων, μια σειρά από βίαιες πράξεις όπως ενδοκρατικές φιλονικίες, βία συμμοριών μέχρι και προσχεδιασμένη ανθρωποκτονία. Με το χτύπημα στο Παγκόσμιο Κέντρο Εμπορίου προβλήθηκε έντονα η έννοια της τρομοκρατικής βίας. Ο στόχος του συγκεκριμένου χτυπήματος ήταν τα πολυάριθμα θύματα αμάχων πολιτών. Ο σκοπός των επιθέσεων αυτών την 11 Σεπτεμβρίου ήταν να πιέσουν την κυβέρνηση των Η.Π.Α. να αλλάξουν την πολιτική απέναντι στην Μέση Ανατολή, κάτι που βεβαίως είχε το αντίθετο αποτέλεσμα με συνέπεια την έναρξη του πολέμου στο Ιράκ προκαλώντας την «πτώση» του Σαντάμ Χουσεΐν και αργότερα την εκτέλεση του αρχηγού (Μπιν Λάντεν) της τρομοκρατικής οργάνωσης Αλ Κάιντα.

Ο άμεσος στόχος ενός τρομοκρατικού χτυπήματος είναι απλά το εξιλαστήριο θύμα, δηλαδή μέσα από την βία και τον τρόμο που προκαλεί, επιχειρεί να στείλει ένα καλά σχεδιασμένο μήνυμα σε ένα μεγαλύτερο κοινό. Η

τρομοκρατία βασίζεται στη γέννηση αισθήματος κινδύνου και ανησυχίας που προκαλείται στην κοινωνία (έμμεσος στόχος), πέρα από το θύμα που δέχεται την επίθεση(άμεσος στόχος).

Παρατηρώντας την εξέλιξη των τρομοκρατικών επιθέσεων διαπιστώνεται ότι η τρομοκρατία και ο τρόπος διεξαγωγής των χτυπημάτων μεταλλάσσεται. Πάραυτα συνεχίζει να καταγράφονται ολοένα και περισσότερες επιθέσεις από εξτρεμιστές που στοχεύουν όσο το δυνατόν σε μεγαλύτερους φυσικούς στόχους (αθλητικά δρώμενα, εμπορικά καταστήματα, συναυλίες, θέατρα κ.α.), και παράλληλα εξελίσσεται η δυναμική της τρομοκρατίας με τη χρήση της τεχνολογίας. Η εν λόγω δυναμική εντοπίζεται κυρίως στο διαδίκτυο, εξελίσσεται και εξαπλώνεται σε ταχύτατους ρυθμούς προκαλώντας παγκόσμιο πανικό.

Κεφάλαιο 3

Ειδικότεροι ορισμοί

3.1 Κυβερνοχώρος

Το διαδίκτυο λοιπόν ενώ αποτελεί την μεγαλύτερη πηγή πληροφοριών, τον μεγαλύτερο τρόπο επικοινωνίας και πλέον είναι καθημερινότητα για το μεγαλύτερο κομμάτι του πληθυσμού της γης, παρόλα αυτά δεν αποτελεί τεχνολογικό παράδεισο και χρειάζεται μεγάλη προσοχή και επεξεργασία των πληροφοριών που βρίσκουμε σε αυτό.

Έρευνες έχουν δείξει ότι τρομοκρατικές οργανώσεις πλέον χρησιμοποιούν τον κυβερνοχώρο για στρατολόγηση νέων μελών ή για να βρουν χρηματοδότηση για τον σκοπό τους. Η ίδια έρευνα έδειξε ότι οι τρομοκράτες στοχεύουν νέους ανθρώπους και εκμεταλλεύονται «νέα μέσα» όπως το Facebook, το Twitter, το Instagram, το Tik Tok, το Youtube κ.α.

Οι πλατφόρμες κοινωνικής δικτύωσης είναι το τέλειο μέσο για να αποκτήσει επιρροή και να στρατολογήσει κανείς υποστηρικτές για τις ιδέες του. Με αυτόν τον τρόπο αντί να ακρωτηριάζουν το κρατικό σύστημα πληροφορικής του έθνους, οι τρομοκρατικές ομάδες είναι πολύ πιο επικίνδυνες στρατολογώντας και κερδίζοντας υποστήριξη μέσω των μέσων κοινωνικής

δικτύωσης. Οι τρομοκράτες αναγνώρισαν γρήγορα την ευκαιρία που τους προσφέρει ο κυβερνοχώρος δηλαδή τα κενά ασφαλείας, την εύκολη πρόσβαση των χρηστών, την ανωνυμία που κερδίζουν και συνολικά την ευκαιρία να προσεγγίσουν ένα ευρύτερο κοινό. Έρευνες δείχνουν ότι έχει παρατηρηθεί, οι νέοι άνθρωποι να είναι πιο ευάλωτοι, ευμετάβλητοι και πιο εύκολο να επηρεαστούν (Subrahmanian, 2015)εξαιτίας της ανώριμης συμπεριφοράς τους, του νεαρού της ηλικίας τους, της έλλειψης εμπειρίας και παιδείας πάνω στην κυβερνοασφάλεια.

3.2 Κυβερνοαπειλή

Στον σύγχρονο κόσμο είναι αδύνατο κάποιος να αγνοήσει την εξάρτησή του ανθρώπου από την τεχνολογία. Ένας από τους κύριους παράγοντες της παγκόσμιας πολιτικής είναι ότι ακόμη και τα κράτη εξαρτώνται σε μεγάλο βαθμό από την τεχνολογία για να διατηρήσουν τους κρίσιμους τομείς τους όπως η άμυνα, η διακυβέρνηση, η οικονομία και η ενέργεια. Η Myriam Dunn Cavelty[1] το 2010 τόνισε ότι η απειλή στον κυβερνοχώρο πάντα συσχετίζεται με την εθνική ασφάλεια. Ως εκ τούτου, η προστασία της εθνικής ασφάλειας στον κυβερνοχώρο είναι απαραίτητη για τη διατήρηση της πολιτικής, κοινωνικής και οικονομικής σταθερότητας.

Το 2013, η Pricewaterhouse Cooper διεξήγαγε μια έρευνα στην οποία αναλυόταν το ποσοστό αύξησης των κυβερνοεπιθέσεων στα επόμενα χρόνια και ήδη την χρονιά της διεξαγωγής της έρευνας το ποσοστό αύξησης ήταν 23%. Ένα αρκετά καλό χτύπημα προς τις Ηνωμένες Πολιτείες της Αμερικής έγινε το 2015, όπου χάκερς που συνδέονταν με το χαλιφάτο του ISIS (Ισλαμικό Κράτος του Ιράκ και Συρία) χάκαραν και έκλεψαν στρατιωτικά αμυντικά συστήματα. Η απειλή λοιπόν στον κυβερνοχώρο δεν είναι μπλόφα ούτε μύθος αλλά αποτελεί

[1] Η Myriam Dunn Cavelty είναι Αναπληρώτρια Έρευνας και Διδασκαλία στο Κέντρο Σπουδών Ασφάλειας (CSS) και Ανώτερη Λέκτορας Πολιτικής Ασφάλειας στο ETH Zurich. Η έρευνά της επικεντρώνεται στην πολιτική του κινδύνου και της αβεβαιότητας στις πολιτικές ασφάλειας και στις αλλαγές των αντιλήψεων για τη (δι)εθνική ασφάλεια λόγω ζητημάτων στον κυβερνοχώρο (κυβερνοασφάλεια, κυβερνοπόλεμος, προστασία κρίσιμων υποδομών).
Εκτός από τις διδακτικές, ερευνητικές και εκδοτικές της δραστηριότητες, συμβουλεύει κυβερνήσεις, διεθνείς οργανισμούς και εταιρείες στους τομείς της ασφάλειας στον κυβερνοχώρο, του κυβερνοπολέμου, της προστασίας των κρίσιμων υποδομών, της ανάλυσης κινδύνου και της στρατηγικής προοπτικής. (http://www.myriamdunn.com/index/Welcome.html)

μια πραγματικότητα η οποία κλιμακώνεται και μεγαλώνει συνέχεια ως συνέπεια της τεχνολογικής εξέλιξης. Αυτό στο οποίο στοχεύουν οι κυβερνοτρομοκράτες πλέον, είναι να εκμεταλευτούν κάποια ευπάθεια στην ραχοκοκαλιά της κρατικής διαδικτυακής υποδομής (όπως για παράδειγμα ο χρηματοπιστωτικός και τραπεζικός τομέας).

Οι τυπολογίες κυβερνοαπειλής προέρχονται από διαφορετικούς τύπους. Για παράδειγμα, η Myriam Dunn Cavelty χωρίζει τις κυβερνοαπειλές σε τρεις τυπολογίες:

1. Έγκλημα στον κυβερνοχώρο

Το έγκλημα στον κυβερνοχώρο βασίζεται στην ικανότητα μιας εγκληματικής οργάνωσης να αξιοποιεί και να καλύπτει την εγκληματική της δραστηριότητα χρησιμοποιώντας την τεχνολογική πολυπλοκότητα

2. Κυβερνοπόλεμος

Αποτελεί μια ψηφιακή έκδοση του κλασσικού πολέμου, όπου η τεχνολογία ειδικεύεται στον σύγχρονο πόλεμο

3. Κυβερνοτρομοκρατία

Προκαλείται από τρομοκρατικές ομάδες που εκμεταλλεύονται το τεχνολογικό πλεονέκτημα τους έναντι του ακροατηρίου-στόχου με σκοπό τη διάδοση του φόβου για πολιτικούς σκοπούς και με βασικό σκοπό την αποσταθεροποίηση της εθνικής ασφάλειας. (Ramadhan, 2020)

3.3 Κυβερνοτρομοκρατία

Η κυβερνοτρομοκρατία είναι ένα νέο είδος τρομοκρατικής επίθεσης. Ο Μπάρυ Κόλλιν, ανώτερο στέλεχος του Ινστιτούτου Ασφάλειας και Πληροφοριών των Η.Π.Α, σε δημοσίευσή του για το Διεθνές Συμπόσιο Ποινικής Δικαιοσύνης το 1997 είπε : «Το πρόσωπο της διεθνούς τρομοκρατίας αλλάζει. Μπορεί οι στόχοι και τα κίνητρά της να παραμένουν ίδια, πλέον όμως χρησιμοποιεί νέα και ασυνήθιστα όπλα. Οι υπάρχοντες αμυντικοί μηχανισμοί δεν είναι έτοιμοι για αυτή τη νέα απειλή. Είμαστε ανίσχυροι ενάντια σε αυτό το καταστροφικό, πρωτόγνωρο όπλο. Γιατί αυτή την φορά ο εχθρός δεν θα μας επιτεθεί με φορτία εκρηκτικών, ούτε με δοχεία γεμάτα θανατηφόρα χημικά, ούτε

με δυναμίτες ζωσμένους γύρω από τα σώματα φανατικών. Αυτή τη φορά ο εχθρός θα μας επιτεθεί με μηδενικά και άσσους σε έναν χώρο που είμαστε πιο τρωτοί: στο σημείο που ο φυσικός κόσμος συνδέεται με τον εικονικό. Η σύγχρονη τρομοκρατία πέρασε σε μια νέα εποχή. Μια εποχή που ο κυβερνοτρομοκράτης δρα ανενόχλητος και αόρατος από το σαλόνι του σπιτιού του και προκαλεί χάος και καταστροφή στην άλλη άκρη της γης.» (Βίκυ Καρυστινού, 2016). Το Ομοσπονδιακό Γραφείο Ερευνών (FBI), θεωρεί ότι η κυβερνοτρομοκρατία είναι «οποιαδήποτε προμελετημένη επίθεση με πολιτικά κίνητρα εναντίον πληροφοριών, συστημάτων υπολογιστών ή προγραμμάτων υπολογιστών και δεδομένων που οδηγεί σε βία κατά μη μαχητών στόχων από υποεθνικές ομάδες ή μυστικούς πράκτορες». Το ΝΑΤΟ από την άλλη χαρακτηρίζει την κυβερνοτρομοκρατία ως «κυβερνοεπίθεση που χρησιμοποιεί ή εκμεταλλεύεται δίκτυα υπολογιστών ή επικοινωνιών για να προκαλέσει επαρκή καταστροφή ή διακοπή για να δημιουργήσει φόβο ή να εκφοβίσει μια κοινωνία σε έναν ιδεολογικό στόχο» (Marco Marsili, 2019).

Ένας άλλος τρόπος με τον οποίο μπορούμε να περιγράψουμε την κυβερνοτρομοκρατία-ηλεκτρονική τρομοκρατία είναι η «χρήση των υπολογιστών ή και των τηλεπικοινωνιακών δικτύων τόσο σαν όπλο όσο και σαν στόχο (φυσική καταστροφή), παρακινούμενη από θρησκευτικές και πολιτικές πεποιθήσεις ή μυστικούς πράκτορες, προκειμένου να εξασκήσουν βία σε άμαχο πληθυσμό προκαλώντας ανθρώπινες απώλειες ή και φυσικές καταστροφές με σκοπό να επηρεάσουν την κοινή γνώμη ή και τις κυβερνήσεις» (ΑΔΗΩΤΟΣ, 2019).

Ο όρος «Κυβερνοτρομοκρατία» χρησιμοποιήθηκε για να χαρακτηριστούν οι τρομοκρατικές επιθέσεις που πραγματοποιούνται είτε με χρήση υψηλής τεχνολογίας είτε για να χτυπηθούν εγκαταστάσεις που χρησιμοποιούν υψηλή τεχνολογία. Ο Dan Verton (¨the invisible threat of Cyber-Terrorism¨) δίνει την εξής έννοια στην λέξη κυβερνοτρομοκρατία : « η εκτέλεση μίας ξαφνικής επίθεσης από εθνική ή διεθνή τρομοκρατική ομάδα ή μεμονωμένες τοπικές εγκληματικές ομάδες με πολιτική ατζέντα, χρησιμοποιώντας τεχνολογία υπολογιστών και internet, προκειμένου να ακρωτηριαστούν ή να απενεργοποιηθούν οι εθνικές ηλεκτρονικές και φυσικές υποδομές, δημιουργώντας με αυτόν τον τρόπο απώλεια σε βασικές υπηρεσίες,

όπως η παροχή ηλεκτρικής ενέργειας, τα συστήματα άμεσης βοήθειας, υπηρεσίες τηλεπικοινωνιών, τραπεζικά συστήματα, το διαδίκτυο και πλήθος άλλων ».Η κυβερνοτρομοκρατία λοιπόν αφορά μια επίθεση που γίνεται στον άυλο κόσμο του διαδικτύου εκεί όπου οι πληροφορίες ρέουν με ταχύτητα μεγαλύτερη από αυτή του φωτός.

Όπως αναφέραμε λοιπόν σε προηγούμενο κεφάλαιο τα μέσα τέλεσης του εγκλήματος της κυβερνοτρομοκρατίας είναι η χρήση ηλεκτρονικού υπολογιστή, το διαδίκτυο και η τεχνολογία πληροφοριών. Σε ολόκληρο τον κόσμο η τεχνολογία πληροφοριών χρησιμοποιείται πλέον ευρέως και η εξάρτηση των κρατών από αυτήν είναι τεράστια, πράγμα που καθιστά ευάλωτες τις εκάστοτε χώρες σε κυβερνοεπιθέσεις. Το 2005 στις Βρυξέλλες πραγματοποιήθηκε από την Ευρωπαϊκή Κομισιόν, μια παρουσίαση με θέμα το Ευρωπαϊκό πρόγραμμα για την προστασία των κρίσιμων υποδομών (European programme for critical infrastructure protection). Στην παρουσίαση αυτή έγινε ένας καθορισμός των κρίσιμων υποδομών, ως φυσικές πηγές, υπηρεσίες, τεχνολογικές και επικοινωνιακές εγκαταστάσεις, δίκτυα και υποδομές, οι οποίες αν διακοπούν ή καταστραφούν, θα έχουν σοβαρό αντίκτυπο στην υγεία, την ασφάλεια την οικονομία και την ευημερία ενός κράτους .Οι κρίσιμες υποδομές είναι σημαντικές για την εύρυθμη και ομαλή λειτουργία του κρατικού μηχανισμού και θα πρέπει να θεωρείται ως πρώτη προτεραιότητα η διασφάλισή τους και η μη διακοπή της λειτουργίας τους. Οι κρίσιμες υποδομές λοιπόν, αποτελούν κατά βάση το στόχο των κυβερνοτρομοκρατικών επιθέσεων (Παναγιώτη Κικίλια, 2008).

Ο Clay Wilson ειδικός σε θέματα τεχνολογίας και ειδικής ασφάλειας του Υπουργείου Άμυνας των ΗΠΑ αναφέρει τα είδη των επιθέσεων της κυβερνοτρομοκρατίας που δύνανται να εκτελεστούν με τους παρακάτω τρόπους:

1. Φυσική Επίθεση: με χρήση συμβατικών όπλων εναντίον εγκαταστάσεων υψηλής τεχνολογίας (όπως για παράδειγμα πραγματοποιήθηκε την 11 Σεπτεμβρίου του 2001 στο Παγκόσμιο Κέντρο Εμπορίου και το Υπουργείο Εθνικής Άμυνας των Ηνωμένων Πολιτειών της Αμερικής όπου οι παραπάνω επιθέσεις προκάλεσαν σοβαρά προβλήματα στην

ομαλή λειτουργία του κράτους των ΗΠΑ). Οι φυσικές επιθέσεις κοινώς δεν αποτελούν καινούργια προσθήκη στο προσκήνιο της τρομοκρατίας και μέχρι πρόσφατα αποτελούσαν τον βασικό τρόπο χτυπήματος των τρομοκρατικών οργανώσεων.

2. Δικτυακή Επίθεση: εδώ αναφέρεται σε κακόβουλα λογισμικά ή αλλιώς ιούς μέσα στα πληροφοριακά συστήματα ενός κράτους. Υποστηρίζεται δε ότι οι δικτυακές επιθέσεις είναι οι επιθέσεις του μέλλοντος όπως και οι όροι κυβερνοτρομοκρατία και κυβερνοεπιθέσεις. Όσο μεγαλύτερη είναι η εξάρτηση των κοινωνιών από τα πληροφοριακά συστήματα και την δικτύωση, τόσο μεγαλύτερη είναι η αύξηση του κινδύνου για κάποια επίθεση. Είναι δεδομένο ότι πλέον τα περισσότερα αν όχι όλα τα κράτη είναι πλήρως εξαρτημένα από το διαδίκτυο και τα πληροφοριακά συστήματα. Ας σκεφτούμε για παράδειγμα την εγκατάσταση ενός κακόβουλου λογισμικού στον υπολογιστή ενός διαγνωστικού κέντρου, η παράλυση του συστήματος δύναται να έχει αντίκτυπο σε μερικές χιλιάδες ανθρώπων. Αν η εγκατάσταση του κακόβουλου λογισμικού γίνει στο κεντρικό σύστημα ύδρευσης ή φυσικού αερίου σε κάποια πόλη, η παράλυση του συγκεκριμένου δικτύου θα έχει αντίκτυπο σε εκατοντάδες χιλιάδες ίσως και εκατομμύρια κόσμου. Συμπερασματικά όλες οι κοινωνίες του πλανήτη είναι ευάλωτες έναντι μιας επίθεσης κυβερνοτρομοκρατίας. Οι δικτυακές επιθέσεις λοιπόν, είναι ένα βασικό στοιχείο της κυβερνοτρομοκρατίας, και αναμένεται στο μέλλον να χρησιμοποιούνται από ακόμα μεγαλύτερο αριθμό τρομοκρατικών οργανώσεων, ενώ η προστασία των κρατικών υποδομών ενάντια σε αυτές, προβληματίζει ιδιαίτερα τις κυβερνήσεις, καθώς υπάρχει η διαπίστωση σήμερα ότι υπάρχουν αρκετά τρωτά σημεία σε αυτές (Παναγιώτη Κικίλια, 2008) .

3. Ηλεκτρομαγνητική επίθεση (EMP): χρήση δηλαδή ηλεκτρομαγνητικών παλμών για καταστροφή ηλεκτρονικών συστημάτων. Ο ηλεκτρομαγνητικός παλμός είναι ένα ισχυρό κύμα στο οποίο μεταφέρεται ηλεκτρομαγνητική ενέργεια. Μια EMP επίθεση μπορεί να καταστρέψει σε ακτίνα 1,8 χιλιομέτρων ότι ηλεκτρονικό και πληροφοριακό σύστημα υπάρχει. Είναι αλήθεια ότι μια EMP επίθεση μπορεί να προκαλέσει τεράστια ζημιά και λόγω της ευρείας πληροφόρησης που υπάρχει στο διαδίκτυο για το πως να κατασκευαστεί μια EMP βόμβα, αναμένεται να αποτελέσει ένα αρκετά συνηθισμένο φαινόμενο στο μέλλον .

3.4 Προσηλυτισμός

Προσηλυτισμός εν γένει σημαίνει προσεταιρισμός, ρυμούλκηση ενός ατόμου στις απόψεις άλλου με τη διδασκαλία και τη πειθώ. Είναι η πνευματική και πρακτική λειτουργία που αποβλέπει στην επιρροή συνείδησης, κυρίως ως προς το θρησκευτικό της περιεχόμενο. Σήμερα ο όρος «προσηλυτισμός» χρησιμοποιείται για να περιγράψει αποκλειστικά αποδοκιμαζόμενες μορφές κοινωνικής συμπεριφοράς. Σηματοδοτεί τη δόλια και μεθοδευμένη προσπάθεια διείσδυσης στη θρησκευτική συνείδηση του ατόμου. Έτσι λοιπόν, προσηλυτισμός θεωρείται η πνευματική και πρακτική εκείνη λειτουργία, που αποβλέπει στην επιρροή της θρησκευτικής συνείδησης με απατηλά και δόλια μέσα . Στην Ελλάδα ο προσηλυτισμός απαγορεύεται ρητά από το Σύνταγμα (άρθρο 13 §2 του Συντάγματος). Με το διαδίκτυο και γενικότερα με την τεχνολογία ο προσηλυτισμός είναι κάτι το οποίο δεν μπορεί να ελεγχθεί. Σελίδες του διαδικτύου που φαίνονται αντικειμενικά ακίνδυνες, μπορεί να ενέχουν σοβαρούς κινδύνους και για αυτό το λόγο είναι επιτακτική η εκπαίδευση των ανθρώπων πάνω στα νέα δεδομένα της τεχνολογικής ανάπτυξης.

Μια τρομοκρατική ομάδα λοιπόν μέσω των μέσων κοινωνικής δικτύωσης μπορεί να στρατολογήσει νέα μέλη, να αντλήσει χρήματα για τον σκοπό της ακόμα και να κάνει τον σκοπό της ελκυστικό στον κόσμο. Μπορούμε λοιπόν με ασφάλεια να πούμε ότι η τεχνολογία και ιδίως τα μέσα κοινωνικής δικτύωσης αποτελούν το τέλειο μέσο για την διάδοση και την εξάπλωση της τρομοκρατικής ιδεολογίας. Είναι ευρύτερα γνωστό ότι οργανώσεις όπως ο ISIS, χρησιμοποιούν διάφορες πλατφόρμες όπως το Facebook, Instagram, Twitter και το Youtube για να προσηλυτίσουν, να πείσουν να ενταχθούν στην οργάνωση τους νέα μέλη και να ασπαστούν την θρησκεία του Ισλάμ.

Οι άνθρωποι στις μέρες μας νιώθουν εξοικειωμένοι στην χρήση διάφορων εφαρμογών συνομιλίας είτε αυτό είναι το Viber, το telegram, το Signal, το what’s app και το προσωπικό ηλεκτρονικό ταχυδρομείο, εφαρμογές που πλέον είναι ενσωματωμένες στα κινητά τους τηλέφωνα και η πρόσβαση σε αυτά είναι πάρα πολύ απλή. Το προνόμιο - όφελος όλων αυτών των εφαρμογών στους απλούς πολίτες είναι η ευελιξία στον τρόπο χρήσης τους και

η ασφάλεια που προσφέρουν, αφού οι εταιρείες έχουν αναβαθμίσει το λογισμικό τους και παρέχουν σε αυτές κρυπτογράφηση.

Ενώ ο μέσος χρήστης αποζητά την ασφάλεια του διαδικτύου, δεν το προαναφερθέν προνόμιο να ευνοεί και τις εγκληματικές οργανώσεις στην δράση τους. Για παράδειγμα βοηθάει τις τρομοκρατικές ομάδες να υλοποιήσουν αποστολές και να έχουν την ευκαιρία να κινητοποιηθούν από τη μια χώρα στην άλλη, να επικοινωνούν ανώνυμα και πολλές φορές μάλιστα σε δημόσια forum με τον δικό τους κώδικα επικοινωνίας και λόγω της ανωνυμίας – προστασίας αυτών των πλατφορμών, δεν διστάζουν να δρουν χωρίς το φόβο υποκλοπής των συνομιλιών τους.

Ο σκοπός της ανωνυμίας του διαδικτύου είναι η διασφάλιση του απορρήτου για τον χρήστη όταν αυτός συνδέεται στο internet ή πρόκειται να επικοινωνήσει μέσω διαδικτύου. Αυτό αποτελεί προνόμιο που απολαμβάνουν και οι εγκληματικές-τρομοκρατικές οργανώσεις. Σε έρευνα του ο Στίβεν Αϊνταχόσα παραθέτει στοιχεία όπου δείχνουν ότι η Αλ Κάιντα ήταν η πρώτη τρομοκρατική ομάδα η οποία χρησιμοποίησε το διαδίκτυο για να συντονίσει τις δραστηριότητες της. Στην έρευνα αναφέρεται ότι η συγκεκριμένη ομάδα συντονίστηκε επιτυχώς και απαρατήρητα σχεδόν με τους «πράκτορές της» που ήταν σε αδράνεια, οι λεγόμενοι sleeping cells και συντόνισαν την τραγική επίθεση της 11ης Σεπτεμβρίου που συγκλόνισε και άλλαξε το ρου ολόκληρου του κόσμου. Για να προετοιμάσει μια τέτοιου μεγέθους επίθεση σε τέτοιο βεληνεκές, εκπαίδευσε τους «πράκτορές» της στην σχεδίαση και κατασκευή μιας βόμβας που θα χρησιμοποιούνταν εναντίον του εχθρού. Δημιούργησαν έναν ιστότοπο για το Παγκόσμιο Ισλαμικό Μέτωπο Μέσων (Global Islamic Media Front) και συντονίστηκαν με τους πράκτορές τους παρέχοντας τους βασική εκπαίδευση για το πως να σχεδιάσουν, να κατασκευάσουν μια βόμβα, ώστε να διαδώσουν την ριζοσπαστική ιδεολογία τους για να κερδίσουν υποστήριξη από τις μουσουλμανικές χώρες. Σκοπός τους ήταν να αποσταθεροποιήσουν τις δυτικές χώρες και να σκορπίσουν τον τρόμο στην καρδιά της κοινωνίας (IDAHOSA Stephen Osaherumwen, 2017). Η δε κρυπτογράφηση που χρησιμοποιείται από τα περισσότερα λογισμικά των διάφορων ελεύθερων εφαρμογών, έχει κάνει την επικοινωνία των τρομοκρατών

πιο μυστική, δυσκολότερη στην ανίχνευση της, με συνέπεια οι οργανώσεις να καθίστανται πιο ευέλικτες στον συντονισμό τους.

Τρομοκρατικές οργανώσεις όπως ο ISIS, η Αλ Κάιντα, η Χεζμπολά για παράδειγμα, στοχεύουν στην γενιά των millennials διότι δείχνουν τεράστιο ενδιαφέρον για τα μέσα κοινωνικής δικτύωσης. Η τραγική αλήθεια είναι ότι τα ερεθίσματα της γενιάς των millennials προέρχονται κατά βάση από τα μέσα της τεχνολογίας και αυτό φέρει ως αποτέλεσμα το smartphone να είναι επέκταση του χεριού τους. Επιπλέον το γεγονός ότι δεν προσφέρεται βασική εκπαίδευση στην ασφαλή πλοήγηση στο διαδίκτυο, τους καθιστά υπερβολικά ευάλωτους στους κινδύνους τους διαδικτύου και δη στον προσηλυτισμό, την εκμετάλλευση διάφορων επικίνδυνων οργανισμών και ανθρώπων.

Άρθρο Ισλαμικού Κράτους με τίτλο ¨A New Age of Terrorist Recruitment: Target Perceptions of the Dabiq Magazine¨, αναφέρει ότι τρομοκρατικές ομάδες όπως η ISIS τείνουν να στρατολογούν νεαρά μέλη ηλικίας από 18 ως 25. Υποστηρίζεται μάλιστα ότι οι τρομοκρατικές οργανώσεις στρατολογούν μέλη με τριτοβάθμια εκπαίδευση και άτομα που προέρχονται από την μεσαία τάξη. Έρευνες δείχνουν επίσης ότι άτομα των παραπάνω ηλικιών (18-25) βρίσκονται ακόμα σε φάση αναζήτησης της ταυτότητας τους και ως εκ τούτου καθίστανται πιο ευάλωτοι, πιο ευκολόπιστοι και αποτελούν ευκολότερα θύματα χειραγώγησης από τρομοκρατικές οργανώσεις.

Η Cavelty σε άρθρο της το 2014 δήλωσε ότι η τρομοκρατία έχει καταστροφικές επιπτώσεις στη σύγχρονη κοινωνία και τόνισε ότι το αντικείμενο αναφοράς στο πλαίσιο του προσηλυτισμού είναι η ίδια η κοινωνία. Ως εκ τούτου, η απειλή προέρχεται από τον κοινωνικό τομέα. Μια τρομοκρατική ομάδα χρειάζεται νέα μέλη για να διατηρήσει τον αγώνα της. Με την τεχνολογία σύμμαχο τους δίνεται η ευκαιρία προσέγγισης ενός ευρύτερου κοινού. Τα μέσα κοινωνικής δικτύωσης είναι πλατφόρμες όπου οι τρομοκρατικές ομάδες μπορούν να επηρεάσουν τους ανθρώπους, ειδικά τη νεότερη γενιά, να ενταχθεί στη λεγόμενη «επανάστασή» τους. Η στόχευση ανθρώπων νεαρότερων ηλικιών, όπως προαναφέραμε, γίνεται γιατί θεωρούνται αυτές οι ηλικίες πιο ευάλωτες λόγω της ασταθούς ψυχολογίας , της αδυναμίας κρίσεως απέναντι στην τρομοκρατική ιδεολογία καθώς και του ανυπέρβλητου ενθουσιασμού ως

προς την επανάσταση κατά του κατεστημένου και κατά της εκάστοτε κρατικής καταπίεσης.

Τα μέσα κοινωνικής δικτύωσης μπορούν πολύ εύκολα να εργαλειοποιηθούν για την κυβερνοτρομοκρατία, ειδικά με τον προσηλυτισμό, επειδή επηρεάζει και αλλάζει την ανθρώπινη ψυχολογία. Το παιχνίδι με την αμοιβαία ταυτότητα, την κοινή θρησκεία και το μαινόμενο μίσος προς τη δυτική κουλτούρα είναι χρήσιμο για τις τρομοκρατικές ομάδες να στρατολογούν νέα μέλη από την οικονομία της μεσαίας τάξης.

Ο προσηλυτισμός έχει σοβαρό αντίκτυπο παγκοσμίως. Οι τρομοκρατικές ομάδες χρησιμοποιούν δύο τύπους επιρροής:

1. Η επίσημη προπαγάνδα. Διαδίδουν την ιδεολογία τους δημιουργώντας έναν επίσημο ιστότοπο ή λογαριασμό σε πολλά μέσα κοινωνικής δικτύωσης. Μέσω του λογαριασμού στα μέσα κοινωνικής δικτύωσης, τρομοκρατικές ομάδες όπως η ISIS πείθουν τους ανθρώπους να ενταχθούν στον σκοπό τους, να γίνουν τακτικά μέλη ή να τους υποστηρίξουν.
2. Η ανεπίσημη προπαγάνδα. Είναι μια μέθοδος όπου η ιδεολογία ενός τρομοκράτη εξαπλώνεται μέσω των «εκπροσώπων» τους (μέσω ανθρώπων που υποστηρίζουν τον σκοπό της οργάνωσης) Αν και δεν είναι άμεση προπαγάνδα, αυτή η μέθοδος είναι εξίσου καταστροφική. Πλατφόρμες μέσων κοινωνικής δικτύωσης όπως το Facebook ή το Twitter αναδεικνύονται ως ο τέλειος διανομέας για τη διάδοση της ριζοσπαστικής ιδεολογίας. Στο τέλος οι πληροφορίες μπορούν να φτάσουν σε μεγαλύτερο κοινό και να αποκτήσουν επιρροή. Το Facebook, το Twitter και το Youtube είναι οι πιο αποτελεσματικές πλατφόρμες μέσων κοινωνικής δικτύωσης ως ριζοσπαστικό μέσο και τα τρία αυτά μέσα έχουν σημαντικό αντίκτυπο στον προσηλυτισμό των ανθρώπων. (Iqbal Ramadhan, 2020)

Κεφάλαιο 4

Δικαιώματα στο διαδίκτυο

4.1 Ψηφιακά Δικαιώματα

Τα ψηφιακά δικαιώματα είναι τα ανθρώπινα δικαιώματα που επιτρέπουν την πρόσβαση των ατόμων και τη δυνατότητά τους να χρησιμοποιήσουν και να επεξεργαστούν ψηφιακά μέσα επικοινωνίας ή να έχουν πρόσβαση και δυνατότητα χρήσης υπολογιστών, άλλων ηλεκτρονικών συσκευών και δικτύων επικοινωνίας. Το σημαντικότερο και πιο γνωστό από αυτά τα δίκτυα επικοινωνίας είναι το Διαδίκτυο, το οποίο όπως λέει και το όνομά του, αποτελεί το «δίκτυο των δικτύων»

Τα ψηφιακά δικαιώματα είναι όλα τα ανθρώπινα δικαιώματα που σχετίζονται με τις παραπάνω δραστηριότητες στην ψηφιακή εποχή, στην οποία ζούμε. Ενδεικτικά κάποια από τα κυριότερα ψηφιακά δικαιώματα είναι:

- το δικαίωμα στην ιδιωτική ζωή,
- η προστασία των προσωπικών δεδομένων,
- η ελευθερία της έκφρασης,
- η ελευθερία πληροφόρησης,
- το δικαίωμα στην ιδιοκτησία –υλική και πνευματική,
- το δικαίωμα στη δικαστική προσφυγή και
- η απαγόρευση των διακρίσεων.

Είναι σχεδόν βέβαιο ότι με την συνεχή εξέλιξη της τεχνολογίας και την αντίστοιχη επέκταση των ανθρωπίνων δραστηριοτήτων θα δημιουργηθούν νέα ψηφιακά δικαιώματα.

Καθημερινά επιδιδόμαστε σε δραστηριότητες μέσω του διαδικτύου και ηλεκτρονικών συσκευών: κάνουμε αγορές, επικοινωνούμε, ανταλλάσσουμε απόψεις και πληροφορίες, ενημερωνόμαστε. Δεν είναι υπερβολή λοιπόν να πούμε ότι πλέον ταυτόχρονα με τον πραγματικό κόσμο, ζούμε και δραστηριοποιούμαστε και σε έναν ψηφιακό. Για αυτό λοιπόν τον λόγο όπως ο πραγματικός μας εαυτός έχει ανάγκη προστασίας, την ίδια ακριβώς ανάγκη προστασίας έχει και ο ψηφιακός.

Τα ψηφιακά δικαιώματα δεν είναι τίποτα άλλο από προέκταση των ήδη κατοχυρωμένων δικαιωμάτων στην Οικουμενική Διακήρυξη των Δικαιωμάτων

του Ανθρώπου, στο διεθνές και ευρωπαϊκό δίκαιο, αλλά και στο Σύνταγμα της Ελλάδας. Με την ανάπτυξη της τεχνολογίας και την είσοδο στην ψηφιακή εποχή δημιουργήθηκε ένας νέος ψηφιακός κόσμος, παράλληλος με τον πραγματικό. Τα ήδη κατοχυρωμένα δικαιώματα πήραν και μία νέα διάσταση, ώστε να καλύψουν το νέο χώρο ανθρώπινης δραστηριότητας που δημιουργήθηκε.

Τα ψηφιακά δικαιώματα χρήζουν της ίδιας προστασίας με τα ήδη κατοχυρωμένα δικαιώματα, αφού αποτελούν προέκταση των κατοχυρωμένων θεμελιωδών ανθρωπίνων δικαιωμάτων. Είναι βέβαιο δε ότι είναι απολύτως απαραίτητη η θεσμοθέτηση νέας νομοθεσίας, ώστε να ρυθμίσει ενδελεχώς τις όποιες ιδιαιτερότητες της νέας κατάστασης.

Για να μπορέσουμε να προστατέψουμε τα ψηφιακά μας δικαιώματα όμως, πρέπει πρώτα να ενημερωθούμε για αυτά. Πρέπει να μάθουμε πώς τα προσωπικά μας δεδομένα χρησιμοποιούνται από εταιρείες, κράτη και άλλα άτομα. Πρέπει να μάθουμε πού αρχίζει και πού τελειώνει η ελευθερία της έκφρασής μας στο διαδίκτυο. Πρέπει να μάθουμε πώς να προστατεύουμε τις διαδικτυακές μας συναλλαγές. Πρέπει να μάθουμε πού και πότε επιτρέπεται η παρακολούθηση των δραστηριοτήτων μας με κάμερες και πού όχι. Με λίγα λόγια χρειάζεται εκπαίδευση στις μικρές ηλικίες πλέον και εκπαιδευτικά σεμινάρια σε ενηλίκους για να αντιληφθούμε καλύτερα τα οφέλη αλλά και τους κινδύνους και να μπορέσουμε να υπερασπιστούμε σωστά τους εαυτούς μας.

Τα ψηφιακά δικαιώματα είναι κομμάτι της καθημερινότητάς μας. Όπως ενδιαφερόμαστε για την προστασία των δικαιωμάτων και των ελευθεριών μας στον πραγματικό κόσμο, πρέπει να αρχίσουμε να ενδιαφερόμαστε για την προστασία τους και στον ψηφιακό κόσμο (Κακαβούλης, 2018).

4.2 Λογοκρισία

Δυστυχώς όμως ενώ το διαδίκτυο αποτελεί πηγή πληροφόρησης και έκφρασης , όπως αναφέρθηκε , υπάρχουν χώρες όπως η Κίνα , η Τουρκία, τα Ηνωμένα Αραβικά Εμιράτα , το Ιράν , το Βιετνάμ και η Αίγυπτος που έχουν τους

περισσότερους περιορισμούς στο διαδίκτυο καθώς και την μεγαλύτερη λογοκρισία.

Η λογοκρισία του διαδικτύου είναι ο έλεγχος ή περιορισμός της πρόσβασης και του περιεχομένου που μπορεί να δημοσιευθεί ή να προβληθεί στο Διαδίκτυο, όπως έχει τεθεί σε ισχύ από τις ρυθμιστικές αρχές ή από ιδιωτική πρωτοβουλία. Μεμονωμένα άτομα και οργανώσεις μπορούν να ασκήσουν πολιτική αυτολογοκρισίας για ηθικούς, θρησκευτικούς, ή για επαγγελματικούς λόγους, να συμμορφώνονται με τα κοινωνικά πρότυπα, λόγω εκφοβισμού ή από φόβο για τις νομικές ή άλλες συνέπειες.

Η έκταση της λογοκρισίας στο Διαδίκτυο διαφέρει από χώρα σε χώρα. Ενώ οι περισσότερες δημοκρατικές χώρες έχουν μέτρια λογοκρισία στο Διαδίκτυο, άλλες χώρες φτάνουν στο σημείο του να περιορίζουν την πρόσβαση σε πληροφορίες, όπως τις ειδήσεις, και να απαγορεύουν τις συζητήσεις μεταξύ των πολιτών. Ένα παράδειγμα ήταν η αυξημένη λογοκρισία όσο διήρκεσε η Αραβική Άνοιξη. Άλλα θέματα της λογοκρισίας είναι τα πνευματικά δικαιώματα, η συκοφαντική δυσφήμιση, η παρενόχληση και το άσεμνο υλικό.

Οι κρατικές υπηρεσίες διαθέτουν εργαλεία για την εφαρμογή περιορισμών, αλλά οι υποστηρικτές της ελευθερίας του διαδικτύου προσπαθούν να ξεπεράσουν αυτά τα εμπόδια και τα φίλτρα. Οι ιστοσελίδες περιορισμένης πρόσβασης προστατεύονται αποτελεσματικά με εντοπισμό και φραγή αιτημάτων DNS[2], αλλά εταιρείες όπως οι Cloudflare, Mozilla και Google αλλάζουν το DNS σε επίπεδο TLS[3] καθιστώντας την αναχαίτιση δύσκολη.

Όπως είναι φυσικό υπάρχουν υποστηρικτές αλλά και πολέμioi της λογοκρισίας του διαδικτύου. Έρευνα που έγινε το 2012 για την Διαδικτυακή Κοινότητα έδειξε ότι το 71% των ερωτηθέντων συμφώνησαν ότι «πρέπει να υπάρχει λογοκρισία κάποιας μορφής στο Διαδίκτυο». Στην ίδια έρευνα, το 83% συμφώνησε ότι «η πρόσβαση στο Διαδίκτυο θα πρέπει να θεωρείται βασικό ανθρώπινο δικαίωμα» και το 86% συμφώνησε ότι «η ελευθερία της έκφρασης πρέπει να είναι

[2] DNS= Domain Name System (ο « τηλεφωνικός κατάλογος» του διαδικτύου)

[3] TLS= Transport Layer Security (στην ουσία κρυπτογραφεί δεδομένα που αποστέλλονται μέσω του Διαδικτύου για να διασφαλίσει χάκερ και τρολς δεν μπορούν να δουν τι μεταδίδετε. Κάτι που είναι ιδιαίτερα χρήσιμο για ιδιωτικές και ευαίσθητες πληροφορίες, όπως για παράδειγμα κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών και προσωπική αλληλογραφία).

εγγυημένη στο Διαδίκτυο». Η αντίληψη της λογοκρισίας στο διαδίκτυο στις ΗΠΑ βασίζεται ως επί το πλείστον στην Πρώτη Τροπολογία και το δικαίωμα για επεκτατική ελευθερία του λόγου και πρόσβαση στο περιεχόμενο χωρίς να ληφθούν υπόψη οι συνέπειες. Σύμφωνα με την GlobalWebIndex, πάνω από 400 εκατομμύρια άνθρωποι χρησιμοποιούν εικονικά ιδιωτικά δίκτυα για να παρακάμψουν τη λογοκρισία ή για την αύξηση της ιδιωτικότητας του χρήστη.

Η φραγή και το φιλτράρισμα μπορεί να βασίζονται σε σχετικά στατικές μαύρες λίστες ή να καθορίζεται πιο δυναμικά βάσει εξέτασης των πληροφοριών που ανταλλάσσονται σε πραγματικό χρόνο. Οι μαύρες λίστες μπορεί να έχουν παραχθεί αυτόματα ή μη, και συνήθως δεν διατίθενται πάρα μόνο σε χρήστες λογισμικών φραγής. Η φραγή ή το φιλτράρισμα μπορεί να γίνονται σε συγκεντρωτικό εθνικό επίπεδο, σε ένα αποκεντρωμένο υποεθνικό επίπεδο, ή σε επίπεδο ιδρύματος, για παράδειγμα σε βιβλιοθήκες, πανεπιστήμια ή Ίντερνετ καφέ. Η φραγή και το φιλτράρισμα μπορεί επίσης να διαφέρουν μεταξύ των διαφορετικών ISP[4] μιας χώρας. Οι χώρες μπορούν να φιλτράρουν το απόρρητο περιεχόμενο σε συνεχή βάση και/ή να εφαρμόζουν προσωρινό φιλτράρισμα κατά τη διάρκεια συγκεκριμένων περιόδων, όπως στις εκλογές. Σε ορισμένες περιπτώσεις, οι λογοκριτικές αρχές ενδέχεται να μπλοκάρουν κρυφά περιεχόμενο ώστε να παραπλανηθεί το κοινό και να πιστέψει ότι δεν έχει εφαρμοστεί λογοκρισία. Αυτό επιτυγχάνεται με την εμφάνιση του μηνύματος λάθους «Δεν Βρέθηκε», κατόπιν της προσπάθειας πρόσβασης σε μια κλειδωμένη ιστοσελίδα. Εκτός και αν ο ελεγκτής έχει πλήρη έλεγχο σε όλους τους υπολογιστές που είναι συνδεδεμένοι στο Ίντερνετ, όπως στη Βόρεια Κορέα (όπου πρόσβαση στο ενδοδίκτυο έχουν μόνο οι προνομιούχοι πολίτες), ή στην Κούβα, όπου η ολοκληρωτική λογοκρισία των πληροφοριών είναι έως και ανέφικτη λόγω της υποκείμενης κατανεμημένης τεχνολογίας του Διαδικτύου. Οι ψευδωνυμίες και τα καταφύγια δεδομένων (όπως το Freenet) προστατεύουν την ελευθερία του λόγου χρησιμοποιώντας τεχνολογίες που εγγυώνται ότι δεν μπορεί να αφαιρεθεί υλικό και εμποδίζει την αναγνώριση των δημιουργών. Οι τεχνολογικά έμπειροι χρήστες συχνά βρίσκουν τρόπους να

[4] ISP= Internet Service Provider (Ένας πάροχος υπηρεσιών διαδικτύου (ISP) είναι μια εταιρεία που παρέχει σε άτομα και οργανισμούς πρόσβαση στο Διαδίκτυο και σε άλλες συναφείς υπηρεσίες. Ένας ISP διαθέτει τον εξοπλισμό και την πρόσβαση στην τηλεπικοινωνιακή γραμμή που απαιτείται για να έχει ένα σημείο παρουσίας στο διαδίκτυο για τη γεωγραφική περιοχή που εξυπηρετείται.)

αποκτήσουν πρόσβαση σε φραγμένο περιεχόμενο. Παρ'όλα αυτά, η φραγή παραμένει μία αποτελεσματική μέθοδος για τον περιορισμό της πρόσβασης σε απόρρητες πληροφορίες στους περισσότερους χρήστες όταν οι λογοκριτές, όπως στην Κίνα, βρίσκονται σε θέση να διαθέσουν σημαντικούς πόρους για την οικοδόμηση και τη διατήρηση ενός ολοκληρωμένου συστήματος λογοκρισίας.

Χρησιμοποιούνται διαφορετικές μέθοδοι για τον αποκλεισμό συγκεκριμένων ιστότοπων ή σελίδων, όπως DNS δηλητηρίαση, φραγή της πρόσβασης σε ορισμένες διευθύνσεις IP[5], ανάλυση και φιλτράρισμα διευθύνσεων URL[6], επιθεώρηση των πακέτων φίλτρων και επαναφορά των συνδέσεων.

Υπάρχουν διάφορες προσεγγίσεις λογοκρισίας στο περιεχόμενο του διαδικτύου:

- **Φραγή διευθύνσεων IP:** Το αίτημα πρόσβασης από μια συγκεκριμένη διεύθυνση IP απορρίπτεται. Αν ο ιστότοπος προορισμού φιλοξενείται σε έναν κοινόχρηστο διακομιστή φιλοξενίας, θα αποκλειστούν όλοι οι ιστότοποι του ίδιου διακομιστή. Μερικές μεγάλες ιστοσελίδες όπως η Google έχουν διαθέσει πρόσθετες διευθύνσεις IP για να παρακάμψουν τις φραγές, αλλά αργότερα οι φραγές επεκτάθηκαν ώστε να καλύψουν τις νέες διευθύνσεις. Λόγω των προκλήσεων του γεωεντοπισμού, οι γεω-φραγές συνήθως υλοποιούνται μέσω φραγής διευθύνσεων IP.
- **Φιλτράρισμα και ανακατεύθυνση του Συστήματος Ονομάτων Τομέων (DNS):** Τα αποκλεισμένα ονόματα τομέα δεν επιλύονται, ή μια εσφαλμένη διεύθυνση IP επιστρέφεται μέσω πειρατείας DNS ή με άλλα μέσα [7].

[5] IP = Internet Protocol. (το οποίο είναι το σύνολο κανόνων που διέπουν τη μορφή των δεδομένων που αποστέλλονται μέσω του Διαδικτύου ή του τοπικού δικτύου). Μια διεύθυνση IP είναι μια μοναδική διεύθυνση που προσδιορίζει μια συσκευή στο Διαδίκτυο ή σε ένα τοπικό δίκτυο.

[6] URL= Uniform Resource Locator (είναι ένα μοναδικό αναγνωριστικό που χρησιμοποιείται για τον εντοπισμό ενός πόρου στο Διαδίκτυο. Αναφέρεται επίσης ως διεύθυνση web. Οι διευθύνσεις URL αποτελούνται από πολλά μέρη -- συμπεριλαμβανομένου ενός πρωτοκόλλου και ενός ονόματος τομέα -- που λένε σε ένα πρόγραμμα περιήγησης ιστού πώς και πού να ανακτήσει έναν πόρο.)

[7] Αυτό επηρεάζει όλα τα βασισμένα σε IP πρωτόκολλα όπως τα HTTP, FTP και POP. Μία τυπική μέθοδος παράκαμψης είναι να βρεθεί ένας εναλλακτικός DNS αναλυτής που να επιλύει τα ονόματα τομέων σωστά, αλλά και οι διακομιστές ονομάτων τομέων υπόκεινται σε αποκλεισμό, ιδιαίτερα μέσω φραγής διευθύνσεων IP. Ένας άλλος ελιγμός είναι η παράκαμψη του DNS που επιτρέπεται εάν η διεύθυνση IP παρέχεται από άλλες πηγές και δεν είναι φραγμένη η ίδια. Για παραδείγματα αναφέρονται η δυνατότητα τροποποίησης του αρχείου Hosts ή πληκτρολόγηση της διεύθυνσης IP

- **Φιλτράρισμα του Ενιαίου Εντοπιστή Πόρων (URL):** Οι συμβολοσειρές των URL σαρώνονται για συγκεκριμένες λέξεις-κλειδιά ανεξάρτητα από το όνομα τομέα που προσδιορίζεται στη διεύθυνση URL. Αυτό επηρεάζει το πρωτόκολλο HTTP[8]. Μία τυπική μέθοδος παράκαμψης είναι η χρήση χαρακτήρων διαφυγής στο URL, ή η χρήση κρυπτογραφημένων πρωτόκολλων όπως τα VPN[9] και TLS/SSL.
- **Φιλτράρισμα πακέτων:** Τερματισμός στη μετάδοση των πακέτων ενός πρωτόκολλου TCP όταν έχει εντοπιστεί ορισμένος αριθμός αντιφατικών λέξεων-κλειδιών. Μία τυπική μέθοδος παράκαμψης είναι η χρήση κρυπτογραφημένων συνδέσεων – όπως με VPN και TLS/SSL[10].
- **Επαναφορά της σύνδεσης:** Αν μια προηγούμενη σύνδεση TCP[11] είναι αποκλεισμένη από το φίλτρο, οι μετέπειτα προσπάθειες σύνδεσης από αμφότερες τις πλευρές μπορούν επίσης να αποκλειστούν για κάποιο μεταβλητό χρονικό διάστημα. Ανάλογα με τη θέση του αποκλεισμού, και άλλοι χρήστες ή ιστοσελίδες μπορούν επίσης να αποκλειστούν, αν η επικοινωνία είναι δρομολογημένη μέσω της αποκλεισμένης θέσης. Μια μέθοδος παράκαμψης είναι να αγνοηθεί το πακέτο επαναφοράς που αποστέλλεται από τον τοίχο προστασίας.
- **Αποσύνδεση δικτύου:** Μία τεχνικά απλούστερη μέθοδος για την λογοκρισία του Διαδικτύου είναι η ολοκληρωτική διακοπή της λειτουργίας όλων των δρομολογητών, είτε με χρήση λογισμικού ή με μηχανική

[8]Hypertext Transfer Protocol (Το HTTP (Πρωτόκολλο μεταφοράς υπερκειμένου) είναι το σύνολο κανόνων για τη μεταφορά αρχείων -- όπως κείμενο, εικόνες, ήχος, βίντεο και άλλα αρχεία πολυμέσων -- μέσω του ιστού. Μόλις ένας χρήστης ανοίξει το πρόγραμμα περιήγησής του, χρησιμοποιεί έμμεσα το HTTP.)

[9] VPN= virtual private network (Ένα VPN (εικονικό ιδιωτικό δίκτυο) είναι ο ευκολότερος και πιο αποτελεσματικός τρόπος για τους ανθρώπους να προστατεύσουν την επισκεψιμότητά τους στο Διαδίκτυο και να διατηρήσουν την ταυτότητά τους ιδιωτική στο διαδίκτυο. Καθώς συνδέονται σε έναν ασφαλή διακομιστή VPN, η κυκλοφορία τους στο Διαδίκτυο διέρχεται από μια κρυπτογραφημένη σήραγγα στην οποία κανείς δεν μπορεί να δει, συμπεριλαμβανομένων των χάκερ, των κυβερνήσεων και του παρόχου υπηρεσιών διαδικτύου σας.

[10] SSL =Secure Sockets Layer (είναι μια τυπική τεχνολογία ασφαλείας για τη δημιουργία κρυπτογραφημένης σύνδεσης μεταξύ ενός διακομιστή και ενός προγράμματος-πελάτη—συνήθως ενός διακομιστή web (ιστότοπος) και ενός προγράμματος περιήγησης ή ενός διακομιστή αλληλογραφίας και ενός προγράμματος-πελάτη αλληλογραφίας (π.χ. Outlook).)

[11] TCP= Transmission Control Protocol (Το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP) είναι ένα πρότυπο που ορίζει τον τρόπο δημιουργίας και διατήρησης μιας συνομιλίας δικτύου μέσω της οποίας οι εφαρμογές μπορούν να ανταλλάσσουν δεδομένα.Το TCP λειτουργεί με το Πρωτόκολλο Διαδικτύου (IP), το οποίο καθορίζει τον τρόπο με τον οποίο οι υπολογιστές στέλνουν πακέτα δεδομένων ο ένας στον άλλο. Μαζί, TCP και IP είναι οι βασικοί κανόνες που ορίζουν το διαδίκτυο

επέμβαση στον εξοπλισμό (απενεργοποίηση μηχανών, τράβηγμα των καλωδίων)[12] .

- **Λογοκρισία Πύλης και απόκρυψη των αποτελεσμάτων αναζήτησης:** Οι μεγάλες πύλες, με συμπεριλαμβανόμενες τις μηχανές αναζήτησης, μπορούν να αποκλείσουν ορισμένους ιστότοπους που κανονικά θα περιλάμβαναν. Τοιουτοτρόπως ένας ιστότοπος καθίσταται αόρατος για τους ανθρώπους που δεν γνωρίζουν την ακριβή διευθυνσή του. Η εν λόγω ενέργεια σε μια μεγάλη πύλη έχει παρόμοιο αποτέλεσμα με τη λογοκρισία. Μερικές φορές αυτή η εξαίρεση γίνεται για να ικανοποιήσει μια νομική ή άλλου τύπου απαίτηση, άλλες φορές οφείλεται καθαρά στην διακριτικότητα της πύλης. Για παράδειγμα, οι Google.de και Google.fr κατάργησαν τον όρο Νεο-Ναζί και άλλες καταχωρήσεις όπως όριζε η γερμανική και η γαλλική νομοθεσία.
- **Επιθέσεις Δικτύων Υπολογιστών:** Οι επιθέσεις άρνησης υπηρεσιών και οι επιθέσεις που υπονομεύουν τις αντίπαλες ιστοσελίδες μπορεί να έχουν το ίδιο αποτέλεσμα με άλλες τεχνικές αποκλεισμού, παρεμποδίζοντας ή περιορίζοντας την πρόσβαση σε ορισμένες ιστοσελίδες ή άλλες ηλεκτρονικές υπηρεσίες, έστω και για μόνο για ένα περιορισμένο χρονικό διάστημα. Η τεχνική αυτή μπορεί να χρησιμοποιηθεί κατά τη διάρκεια μίας προεκλογικής περιόδου ή άλλης κρίσιμης περίστασης. Χρησιμοποιείται συχνότερα από μη κρατικούς φορείς που επιδιώκουν να διαταράξουν τις υπηρεσίες.

Οι παραπάνω προσεγγίσεις λογοκρισίας ενέχουν κινδύνους του υπέρμετρου και ανεπαρκούς αποκλεισμού. Το ζήτημα στις εφαρμογές που φράζονται και αποκλείονται είναι η δυσκολία στο να αποκλειστεί με ακρίβεια το περιεχόμενο του στόχαστρου χωρίς να αποκλείονται μαζί και επιτρεπτές πληροφορίες. Για

[12] Φαίνεται πως αυτό συνέβη στις 27 και 28 Ιανουαρίου 2011,κατά τη διάρκεια των Αιγυπτιακών διαδηλώσεων του 2011, σε ό,τι έχει περιγραφεί ευρέως ως ένας «άνευπροηγουμένου» αποκλεισμός του διαδικτύου.Περίπου 3.500 διαδρομές Πρωτόκολλων Εξωτερικής Δρομολόγησης(BGP) στα Αιγυπτιακά δίκτυα έκλεισαν κατά το χρονικό διάστημα 22:10-22:35 την 27 Ιανουαρίου. Αυτός ο πλήρης αποκλεισμός υλοποιήθηκε χωρίς να διακοπούν οι μεγάλες διηπειρωτικές συνδέσεις οπτικών ινών, με την εταιρεία Renesys να δηλώνει την 27 Ιανουαρίου, «Οι σημαντικές διαδρομές οπτικών ινών Ευρώπης-Ασίας που διέρχονται μέσω της Αιγύπτου φαίνεται πως παρέμειναν ανεπηρέαστες». Πλήρεις αποκλεισμοί σημειώθηκαν επίσης το 2007 στη Μιανμάρ/Βιρμανία, το 2011 στη Λιβύη, και στη Συρία κατά τη διάρκεια του Συριακού εμφυλίου πολέμου. Μια μέθοδος παράκαμψης είναι η χρήση δορυφορικής υπηρεσίας παροχής Ίντερνετ για πρόσβαση στο Διαδίκτυο.

παράδειγμα έστω ότι γίνεται φραγή σε μια διεύθυνση IP ενός διακομιστή που φιλοξενεί πολλαπλές ιστοσελίδες, τότε θα αποτραπεί η πρόσβαση σε όλες τις ιστοσελίδες του και όχι μόνο σε εκείνες που περιέχουν περιεχόμενο που κρίνεται προσβλητικό.

Οργανώσεις όπως το Global Network Initiative, το Electronic Frontier Foundation, η Διεθνής Αμνηστία, και η Αμερικανική Ένωση για τις Πολιτικές Ελευθερίες έχουν με επιτυχία ασκήσει πιέσεις σε ορισμένους προμηθευτές, όπως την Websense, για να κάνουν αλλαγές στο λογισμικό τους, να αποφεύγουν τις συνεργασίες με καταπιεστικές κυβερνήσεις, και να επιμορφώσουν τα σχολεία που άνευ προθέσεως έχουν ρυθμίσει τις παραμέτρους των λογισμικών φιλτραρίσματος πολύ αυστηρά. Παρ ' όλα αυτά, οι κανονισμοί και η ανάληψη ευθυνών σχετικά με τη χρήση των εμπορικών φίλτρων και υπηρεσιών είναι συχνά ανύπαρκτα, και υπάρχει σχετικά ελάχιστη πρόνοια από την κοινωνία των πολιτών ή άλλες ανεξάρτητες ομάδες. Οι πωλητές συχνά θεωρούν τις πληροφορίες για το ποιες τοποθεσίες και περιεχόμενο έχουν αποκλειστεί ως πολύτιμη πνευματική ιδιοκτησία που δεν είναι διαθέσιμη εκτός της εταιρείας, και μερικές φορές ούτε καν στους οργανισμούς που αγοράζουν τα φίλτρα. Συνεπώς, βασισμένοι σε έτοιμα-για-χρήση συστήματα φιλτραρίσματος, το λεπτομερές καθήκον της απόφασης του τι είναι και τι δεν είναι αποδεκτός λόγος μπορεί να εναποτεθεί μόνο στους εμπορικούς προμηθευτές (wikipedia, n.d.)

Ανάμεσα στις χώρες που έχουν περιορισμούς στο διαδίκτυο είναι και η γειτονική Τουρκία η οποία είναι γνωστό ότι προσπαθεί επι πολλά χρόνια να εισαχθεί στην «αγκαλιά» της Ευρωπαϊκής Ένωσης.

Τον Απρίλιο του 2015 η Τουρκία απαγορεύει την πρόσβαση σε όλα τα κοινωνικά δίκτυα το οποίο βεβαίως αποκαταστάθηκε πολύ γρήγορα διότι τα μέσα κοινωνικής δικτύωσης συμμορφώθηκαν άμεσα με τις απαιτήσεις της Τούρκικης κυβέρνησης. Η νομική μηχανή της Τουρκίας έδωσε εντολή να αποσύρει τα εν λόγω κατακριτέα για την ίδια κείμενα και φωτογραφίες και η google υπό την απειλή ότι θα απαγορευόταν στην χώρα η πρόσβαση στην εν λόγω μηχανή αναζήτησης. Αυτό βέβαια προκάλεσε την οργή των τούρκων

χρηστών του Διαδικτύου, της αντιπολίτευσης και των μη κυβερνητικών οργανώσεων προάσπισης της ελευθερία της έκφρασης. (Ανανιάδης, n.d.)

Τον Αύγουστο δε του 2019 το δικαστήριο της Άγκυρας διέταξε τον αποκλεισμό στην πρόσβαση σε 136 ιστότοπους ή λογαριασμούς σε ιστότοπους κοινωνικής δικτύωσης χρηστών που επικρίνουν την κυβέρνηση, συμπεριλαμβανομένων μελών της τουρκικής αντιπολίτευσης, κρίνοντας ότι απειλούν «την εθνική ασφάλεια» της Τουρκίας .

Ο νόμος στην Τουρκία ορίζει ότι μπορεί να αποκλείεται η πρόσβαση σε ιστότοπους για την υπεράσπιση της εθνικής ασφάλειας και της δημόσιας τάξης. Το δικαστήριο βεβαίως δεν διευκρίνισε στην απόφαση του , ποιο ακριβώς είναι το περιεχόμενο που κρίθηκε ότι «απειλεί» την εθνική ασφάλεια και για πιο λόγο επέβαλε τον αποκλεισμό της πρόσβασης. (enallaktikos.gr, 2019)

Κεφάλαιο 5

Περιπτωσιολογικές μελέτες

5.1 Περιπτώσεις κυβερνοτρομοκρατίας

Οι τρομοκράτες χρησιμοποιούν τον κυβερνοχώρο για να προκαλέσουν αβεβαιότητα. Για τους δικούς τους λόγους, αγωνίζονται ενάντια στις κρατικές αρχές και τις κυβερνήσεις και χρησιμοποιούν όλα τα διαθέσιμα μέσα για να επιτύχουν το δικό τους στόχο. Οι επιθέσεις στον κυβερνοχώρο εμφανίζονται σε δύο μορφές, η μία επιτίθεται στις πληροφορίες-δεδομένα και η άλλη επικεντρώνεται στα συστήματα ελέγχου. Η κλοπή δεδομένων και η καταστροφή οδηγούν σε σαμποτάζ υπηρεσιών και αυτή είναι η πιο κοινή μορφή επιθέσεων στο Διαδίκτυο και σε υπολογιστές. Οι επιθέσεις που επικεντρώνονται στον έλεγχο συστημάτων χρησιμοποιούνται για την απενεργοποίηση ή τον χειρισμό της φυσικής υποδομής. Για παράδειγμα, μπορεί να εκτελεστεί απομακρυσμένος έλεγχος σε δίκτυα παροχής ηλεκτρικού ρεύματος, σιδηροδρόμων ή υπηρεσιών παροχής ύδατος, προκειμένου να δημιουργηθεί σύγχυση και πανικός στο εσωτερικό μιας κοινωνίας. Αυτό επιτυγχάνεται με την αποστολή δεδομένων μέσω του διαδικτύου ή διεισδυτικών συστημάτων ασφαλείας. Τέτοια αδύναμα σημεία στο σύστημα

χρησιμοποιήθηκαν στο περιστατικό στην Αυστραλία που συνέβη τον Μάρτιο του 2000, όπου ένας δυσαρεστημένος υπάλληλος (ο οποίος δεν προσλήφθηκε με πλήρη απασχόληση) χρησιμοποίησε το Διαδίκτυο για να απελευθερώσει ένα εκατομμύριο λίτρα μη επεξεργασμένων λυμάτων στον ποταμό και σε παράκτια ύδατα στο Κουίνσλαντ. Στην πραγματικότητα, μετά από 44 ανεπιτυχείς απόπειρες, η 45η ήταν επιτυχής. Οι πρώτες 44 δοκιμές δεν ανιχνεύθηκαν καθόλου.

Το 1988, μια τρομοκρατική οργάνωση, μέσα σε δύο εβδομάδες, προσέβαλλε - πλημμύρισε διάφορες πρεσβείες της Σρι Λάνκα με 800 e-mail την ημέρα. Το μήνυμα που εμφανιζόταν ήταν «Είμαστε οι Internet Black Tigers και το κάνουμε αυτό για να διακόψουμε τις επικοινωνίες σας." Η Υπηρεσία Πληροφοριών χαρακτήρισε την επίθεση ως την πρώτη γνωστή τρομοκρατική επίθεση σε κυβερνητικά συστήματα υπολογιστών.

Το 1998 διαδικτυακοί σαμποτέρ επιτέθηκαν στον ιστότοπο του Ινδικού Κέντρου Ατομικών Ερευνών Bhabba και έκλεψαν μηνύματα ηλεκτρονικού ταχυδρομείου. Οι τρεις ανώνυμοι σαμποτέρ μέσω διαδικτυακής συνέντευξης ισχυρίστηκαν ότι διαμαρτύρονταν για τις πρόσφατες πυρηνικές εκρήξεις στην Ινδία.

Τον Ιούλιο του 1997, ο αρχηγός της Κινεζικής ομάδας χάκερ (Chinese hacker group) ισχυρίστηκε ότι προσωρινά απενεργοποίησε τον κινεζικό δορυφόρο και ανακοίνωσε ότι οι χάκερ δημιούργησαν έναν νέο παγκόσμιο οργανισμό για να διαμαρτυρηθούν και να αποτραπούν οι επενδύσεις από δυτικές χώρες στην Κίνα.

Τον Σεπτέμβριο του 1998, την παραμονή των κοινοβουλευτικών εκλογών στη Σουηδία, σαμποτέρ επιτίθενται στον ιστότοπο του δεξιού πολιτικού κόμματος στη Σουηδία και δημιούργησαν έναν σύνδεσμο από έναν ιστότοπο του αριστερού πολιτικού κόμματος προς πορνογραφικούς ιστότοπους. Τον ίδιο μήνα, σαμποτέρ επιτέθηκαν στον ιστότοπο της κυβέρνησης του Μεξικού σε διαμαρτυρία ενάντια στην κυβερνητική διαφθορά και λογοκρισία.

Κατά τη διάρκεια της σύγκρουσης στο Κοσσυφοπέδιο, οι χάκερ του Βελιγραδίου πραγματοποίησαν επίθεση άρνησης υπηρεσίας (DoS) στους

διακομιστές του ΝΑΤΟ. «Παρακολούθησαν» διακομιστές του ΝΑΤΟ με μηνύματα ICMP Ping, οι οποίοι συνήθως χρησιμοποιούνταν για διαγνωστικούς σκοπούς ή σκοπούς ελέγχου σε σφάλματα λειτουργιών IP.

Κατά τη διάρκεια του Παλαιστινιακού-Ισραηλινού κυβερνοπολέμου το 2000 χρησιμοποιήθηκε παρόμοια επίθεση. Παλαιστίνιοι χάκερς χρησιμοποίησαν εργαλεία DoS για να επιτεθούν στον ISP του Ισραήλ (Internet Service Provider), Netvision. Αν και η επίθεση ήταν αρχικά επιτυχής, η Netvision κατάφερε να αντισταθεί στις συνεχείς επιθέσεις αυξάνοντας την ασφάλειά του.

Τον Απρίλιο του 2007, πολλές δημοσιογραφικές οργανώσεις που συνδέονται με το «Associated Press» ανέφεραν ότι οι επιθέσεις στον κυβερνοχώρο σε υποδομές κρίσιμων πληροφοριών στην Εσθονία διενεργούνταν από διακομιστές υπολογιστών που βρίσκονται στη Ρωσία, αν και αργότερα διαπιστώθηκε ότι είναι μια επίθεση κατανεμημένων DoS που πραγματοποιείται από διαφορετικές τοποθεσίες σε όλο τον κόσμο (ΗΠΑ, Καναδάς, Βραζιλία, Βιετνάμ και άλλες τοποθεσίες). Φυσικά, οι τοποθεσίες των υπολογιστών που εμπλέκονται σε μια τέτοιου είδους επίθεση δεν δείχνει πάντα τη θέση των άμεσων συμμετεχόντων στην επίθεση. Στην πραγματικότητα είναι η θέση των λεγόμενων μηχανών «ζόμπι» που λειτουργούν ως μεσάζοντες κατά τη διάρκεια της επίθεσης, χωρίς τη γνώση τους ή χωρίς καμία γνώση των άμεσων επιτιθέμενων. Η επίθεση απενεργοποίησε εντελώς τη λειτουργία των ιστότοπων πολλών κυβερνητικών ιδρυμάτων, μέσων μαζικής ενημέρωσης και χρηματοπιστωτικών ιδρυμάτων και οδήγησε σε διπλωματικές συνομιλίες που ήταν ένας λόγος για την εξέταση της πιθανότητας της δημιουργίας ενός ερευνητικού κέντρου που υποστηρίζεται από το ΝΑΤΟ, ικανό να προσδιορίσει την πηγή των κυβερνοεπιθέσεων. Τον Αύγουστο του 2008, μια παρόμοια επίθεση πραγματοποιήθηκε κατά της Γεωργίας. Η πρώτη εκτίμηση συμπέραινε ότι η επίθεση έγινε από Ρώσους χάκερ.

Τον Οκτώβριο του 2007, χάκερ επιτέθηκαν στον ιστότοπο του προέδρου της Ουκρανίας Βίκτορ Γιούσενκο. Την ευθύνη για αυτήν την επίθεση ανέλαβε η ριζοσπαστική ρωσική εθνικιστική ομάδα νέων, το Ευρασιατικό Κίνημα Νέων.

Η Κεντρική Υπηρεσία Πληροφοριών των ΗΠΑ (CIA) αποκάλυψε δημόσια ότι τον Ιανουάριο του 2008, χάκερ σταμάτησαν με επιτυχία τα δίκτυα τροφοδοσίας σε πολλές πόλεις των Η.Π.Α. Τον Νοέμβριο του 2008, το Πεντάγωνο αντιμετώπισε πρόβλημα με κυβερνοεπιθέσεις από ιό, ωθώντας το Υπουργείο Άμυνας (DoD) να λάβει για πρώτη φορά μέτρα απαγόρευσης της χρήσης εξωτερικών συσκευών αποθήκευσης δεδομένων, όπως συσκευές flash drives και DVD.

Ένα από τα παραδείγματα που προκάλεσαν παγκόσμιο πανικό σημειώθηκε στα τέλη του 2008, όταν ομάδα χάκερ που ονομάζεται «Greek Security Team», εισέβαλε ηλεκτρονικά σε συστήματα υπολογιστών CERN (Ευρωπαϊκό Κέντρο Πυρηνικής Έρευνας) τόσο βαθιά, που ήταν πολύ κοντά στον έλεγχο ενός από τους ανιχνευτές στο LHC (Large Hadron Collider), τον μεγαλύτερο επιταχυντή σωματιδίων. Οι χάκερ εισέβαλαν στο σύστημα την πρώτη ημέρα του πειράματος και τοποθέτησαν μια ψεύτικη σελίδα στον ιστότοπο του CERN, του οποίου στόχος ήταν να δυσφημίσει τους εμπειρογνώμονες που είναι υπεύθυνοι για το ηλεκτρονικό σύστημα, αποκαλώντας τους «μια ομάδα μαθητών». Οι υπάλληλοι του CERN δήλωσαν ότι δεν προκάλεσε ζημιά.

Την άνοιξη του 2017 μια ομάδα χάκερ που ονομάζονται «Shadow Brokers» διέρρευσε το EternalBlue[13] σε έναν σκοτεινό ιστότοπο. Οι χάκερ αν και δεν είχαν στοχοποιήσει το Βρετανικό σύστημα υγείας (NHS), ανέδειξαν τρωτά σημεία ασφάλειας και αυτό είχε ως αποτέλεσμα την ακύρωση χιλιάδων ραντεβού και λειτουργιών, μαζί με την ξέφρενη μετεγκατάσταση ασθενών έκτακτης ανάγκης από πληγέντα κέντρα έκτακτης ανάγκης. Το προσωπικό αναγκάστηκε επίσης να επιστρέψει στο στυλό και το χαρτί και να χρησιμοποιήσει τα δικά του κινητά αφού η επίθεση επηρέασε βασικά συστήματα, συμπεριλαμβανομένων των τηλεφώνων. Έτσι λοιπόν Το WannaCry ransomware εξέθεσε μια συγκεκριμένη ευπάθεια των Microsoft

[13] το Eternalblue, το όνομα που δόθηκε στην ευπάθεια λογισμικού στο λειτουργικό σύστημα Windows της Microsoft, και λειτουργεί με την εκμετάλλευση του Microsoft Server Message Block 1.0. Το Μπλοκ μηνυμάτων διακομιστή (SMB) είναι ένα πρωτόκολλο κοινής χρήσης αρχείων δικτύου και «επιτρέπει στις εφαρμογές σε υπολογιστή να διαβάζουν και να γράφουν σε αρχεία και να ζητούν υπηρεσίες» που βρίσκονται στο ίδιο δίκτυο. Κατά ειρωνικό τρόπο, φέρεται να αναπτύχθηκε ως εκμετάλλευση κυβερνοεπίθεσης από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ. Αν και αναφέρθηκε ότι γνώριζαν τα τρωτά σημεία του εργαλείου, η NSA δεν το έφερε στην προσοχή της Microsoft.

Windows, όχι μια επίθεση σε μη υποστηριζόμενο λογισμικό. Οι περισσότερες από τις συσκευές NHS που είχαν μολυνθεί με το ransomware, βρέθηκε ότι εκτελούσαν το υποστηριζόμενο, αλλά μη επιδιορθωμένο, λειτουργικό σύστημα Microsoft Windows 7, εξ ου και τα άκρα της κυβερνοεπίθεσης. Το ransomware εξαπλώθηκε επίσης μέσω του Διαδικτύου, συμπεριλαμβανομένου του δικτύου N3 (το ευρυζωνικό δίκτυο που συνδέει όλους τους ιστότοπους του NHS στην Αγγλία), αλλά ευτυχώς, δεν υπήρξαν περιπτώσεις εξάπλωσης του ransomware μέσω NHSmail (το σύστημα email του NHS)[14]. Αποτέλεσμα της συγκεκριμένης επίθεσης ήταν να επηρεαστούν περίπου 250 χιλιάδες μηχανήματα σε περισσότερες από 150 χώρες. Η συγκεκριμένη επίθεση θεωρείται ίσως η μεγαλύτερη επίθεση ransomware που έγινε ποτέ και επηρέασε μια ποικιλία εταιρειών και φορέων, ανάμεσα τους και το Βρετανικό σύστημα υγείας (NHS), την Telefonica με έδρα την Ισπανία, τη FedEx της Αμερικής, τη γερμανική σιδηροδρομική εταιρεία Deutsche Bahn και τη LATAM Airlines. (AcronisCyber Protect, 2020).

Αξιοσημείωτη υπήρξε και η επίθεση στην Colonial Pipeline το 2020. Η συγκεκριμένη επίθεση θεωρείται μια από τις σημαντικότερες εναντίον κρίσιμων υποδομών στην ιστορία, δεδομένου ότι μεταφέρουν περίπου το ήμισυ των προμηθειών καυσίμου της Ανατολικής Ακτής των ΗΠΑ και οι τιμές επηρεάζονται από την επάρκεια του καυσίμου. Το FBI αναφέρει πως πίσω από την επίθεση ήταν η DarkSide, μια σχετικά νέα αλλά αρκετά δραστήρια ομάδα ransomware που θεωρούνταν ότι έδρευε στη Ρωσία. Πιστεύεται δε ότι πρόσβαση στα συστήματα της Colonial αποκτήθηκε μέσω κάποιου e mail, που μπορεί να στάλθηκε στο διοικητικό προσωπικό της εταιρείας, το άνοιγμα του οποίου οδήγησε στο κατέβασμα κάποιου ιού / malware. Αυτό που τονίζεται δε είναι ότι πριν την εξαπόλυση της επίθεσης ransomware είναι πολύ πιθανόν οι χάκερ να βρίσκονταν στα συστήματα της Colonial Pipeline για μήνες (naftemporiki, 2021). Το αποτέλεσμα της συγκεκριμένης επίθεσης, ήταν η εταιρεία να πληρώσει 5 εκατομμύρια δολάρια σε κρυπτονόμισμα τις πρώτες

[14] Το NHS της Αγγλίας ανέφερε ότι τουλάχιστον 80 από τα 236 καταπιστεύματα επηρεάστηκαν επιπλέον 603 πρωτοβάθμιας περίθαλψης και άλλους οργανισμούς του NHS, συμπεριλαμβανομένων 595 ιατρείων GP. Το Υπουργείο, το NHS Αγγλίας και η Εθνική Υπηρεσία Εγκλήματος ανέφεραν ότι κανένας οργανισμός του NHS δεν πλήρωσε τα λύτρα, αλλά το Υπουργείο δεν γνωρίζει πόσο κόστισε το NHS η διακοπή των υπηρεσιών, αν και υπολογίζεται ότι συνολικά ανέρχονται σε 92 εκατομμύρια λίρες

ώρες της επίθεσης, λόγω των μεγάλων προβλημάτων που δημιουργήθηκαν από το χακάρισμα στην παροχή καυσίμων και πετρελαίου στην ανατολική ακτή των ΗΠΑ[15] (insider, 2021)

5.2 Περίπτωση της Εσθονίας

Η Εσθονία αποτελεί ένα λαμπρό παράδειγμα στον τομέα της ηλεκτρονικής διακυβέρνησης. Μέσα σε λίγα μόλις χρόνια έγινε η πρώτη χώρα παγκοσμίως που οι πολίτες της μπορούν να διεκπεραιώσουν τα πάντα με ηλεκτρονικό τρόπο. Ενώ στην δεκαετία του ’90 οι πολίτες της Εσθονίας δεν είχαν καν πρόσβαση σε ηλεκτρονικούς υπολογιστές, η κυβέρνηση τους με επικεφαλή τον Toomas Hendrik Ilves αποφασίζει να επενδύσει στην πληροφοριακή υποδομή της χώρας. Ενδεικτικά αναφέρεται ότι το 1997 θεσπίστηκε το σύστημα της ηλεκτρονικής διακυβέρνησης και το 2000 εισήχθη στην Εσθονία το σύστημα ηλεκτρονικής φορολόγησης. Το 2002 οι Εσθονοί πολίτες απέκτησαν ψηφιακές ταυτότητες, οι οποίες παρείχαν νομικά δεσμευτικές ψηφιακές υπογραφές και το 2005 ξεκίνησε η ηλεκτρονική ψηφοφορία στις δημοτικές εκλογές της Εσθονίας. Σήμερα, το 99% των δημόσιων υπηρεσιών παρέχονται ηλεκτρονικά και το 99% των τραπεζικών συναλλαγών διεξάγονται ηλεκτρονικά (Δέσποινα Βλάχου, Μαρία Ζαμπατή και Χριστίνα Κοντραφούρη , 2020). Αυτό βέβαια έχει σαν αποτέλεσμα την πλήρη εξάρτηση μιας ολόκληρης χώρας από το διαδίκτυο.

Τον Απρίλιο του 2007 η κυβέρνηση της Εσθονίας απομάκρυνε από το κέντρο του Ταλίν το άγαλμα του «Χάλκινου Στρατιώτη» στο στρατιωτικό νεκροταφείο. Το συγκεκριμένο μνημείο ήταν αφιερωμένο στην μνήμη των στρατιωτών του Κόκκινου Στρατού που σκοτώθηκαν πολεμώντας τους νεοναζί. Το άγαλμα λοιπόν για την ρώσικη μειονότητα μνημόνευε την απελευθέρωση της Εσθονίας αλλά για τους Εσθονούς συμβόλιζε την σοβιετική καταπίεση. Με την μετακίνηση λοιπόν του μνημείου προκλήθηκαν ταραχές από την ρωσική

[15] Με την ολοκλήρωση της πληρωμής, οι χάκερς έδωσαν στην εταιρεία ένα εργαλείο αποκωδικοποίησης για να αποκτήσουν και πάλι πρόσβαση στο δίκτυο, αλλά το ίδιο εργαλείο προχωρούσε αργά την αποκατάσταση του δικτύου και η Colonial συνέχισε μόνης της τις εργασίες για την αποκατάσταση του προβλήματος.

μειονότητα γιατί θεώρησαν την μετεγκατάσταση του ως μεγαλύτερη περιθωριοποίηση της εθνικής του ταυτότητας.

Την επόμενη μέρα από τα γεγονότα ξεκίνησαν μια σειρά από κυβερνοεπιθέσεις οι οποίες διήρκησαν για αρκετές βδομάδες και έπληξαν τους δικτυακούς τόπους της κυβέρνησης και πολλών επιχειρήσεων της χώρας. Οι βασικοί στόχοι των επιθέσεων ήταν υπουργεία, το κοινοβούλιο, δημόσιες υπηρεσίες, πολιτικά κόμματα και τα έξι μεγαλύτερα Χρηματοπιστωτικά ιδρύματα της χώρας. Οι άγνωστοι μέχρι σήμερα χάκερ[16] χρησιμοποίησαν μερικές εκατοντάδες χιλιάδες botnets (υπολογιστές "ζόμπι"), δηλαδή χρησιμοποίησαν υπολογιστές ανυποψίαστων χρηστών σε όλο τον πλανήτη οι οποίοι είχαν ήδη μολυνθεί με κακόβουλο λογισμικό (ίσως με άνοιγμα κάποιου email αφού στάλθηκαν εκατομμύρια ανεπιθύμητα mail) με σκοπό να μετατρέψουν τους απλούς χρήστες σε «πιόνια». Η επίθεση στην Εσθονία ήταν μια πρωτοφανής Distributed Denial Of Service Attack. Οι πολίτες της Εσθονίας βρέθηκαν να μην έχουν πρόσβαση σε επίσημες ιστοσελίδες της κυβέρνησης, των δημόσιων υπηρεσιών αλλά και στους τραπεζικούς τους λογαριασμούς. Το αποτέλεσμα αυτών τον επιθέσεων κατέστησε αντιληπτό παγκοσμίως ότι όσο πιο εξαρτημένη είναι μια χώρα από το διαδίκτυο τόσο πιο ευάλωτη είναι και χρειάζεται να επενδύσει περισσότερο στην κυβερνοασφάλεια της. Έτσι λοιπόν μετά την μαζική αυτή επίθεση στην Εσθονία δημιουργήθηκε και εφαρμόστηκε ένα πανίσχυρο παγκοσμίου επιπέδου σύστημα ασφάλειας στον κυβερνοχώρο.

5.3 The Ardit Ferizi case

Τον Σεπτέμβριο του 2015 συλλαμβάνεται στην Μαλαισία ο Ardit Ferizi[17] από το Κόσοβο, ο οποίος κατηγορείται ότι υπέκλεψε δεδομένα και πληροφορίες που ανήκαν σε στρατιωτικούς και σε άλλους κυβερνητικούς αξιωματούχους και τα έδωσε σε μέλη της εγκληματικής οργάνωσης ISIS για να βοηθήσει τις επιθέσεις της οργάνωσης κατά της Δύσης.

Η υπόθεση αυτή είναι σημείο σταθμός για την καταπολέμηση της κυβερνοτρομοκρατίας γιατί είναι η πρώτη φορά που οι Ηνωμένες Πολιτείες της

[16] Η κυβέρνηση της Εσθονίας κατηγόρησε την Ρωσία για τις επιθέσεις , αφού η πηγή πολλών επιθέσεων εντοπίστηκε σε ρωσικά IP , αλλά η Ρωσία δεν ανέλαβε ΠΟΤΕ την ευθύνη.

[17] χρησιμοποιούσε το ψευδώνυμο «Th3Dir3ctorY»

Αμερικής απήγγειλαν κατηγορίες αυτοτελώς και ατομικά σε κάποιο πρόσωπο, ως κυβερνοτρομοκράτη.

Πιο συγκεκριμένα ο Ferizi φαίνεται να υπέκλεψε από περίπου 1300 στρατιωτικούς και άλλους κυβερνητικούς αξιωματούχους, ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, κωδικούς πρόσβασης, τοποθεσίες και αριθμούς τηλεφώνων. Σκοπός του με αυτήν του την πράξη ήταν να προσφέρει βοήθεια σε μέλη του ISIS να εντοπίσουν και να επιτεθούν στους Αμερικάνους στρατιώτες. Φαίνεται ότι όλα αυτά τα στοιχεία προωθήθηκαν σε συγκεκριμένο μέλος του ISIS τον Junaid Hussain (ο οποίος σκοτώθηκε τον Αύγουστο του 2015 σε επίθεση που έγινε από την πλευρά των Η.Π.Α κατά της Συρίας) ο οποίος το αποκάλυψε και στο Twitter. Πιο συγκεκριμένα ανέβασε ένα αρχείο το οποίο αποτελούταν από 30 σελίδες και το οποίο περιείχε ευαίσθητα προσωπικά δεδομένα και συνοδευόταν από το εξής μήνυμα[18] « *είμαστε μέσα στα ηλεκτρονικά ταχυδρομεία και στα πληροφοριακά συστήματα σας, παρακολουθούμε και καταγράφουμε την κάθε σας κίνηση, έχουμε τα ονόματα και τις διευθύνσεις σας, είμαστε στα ηλεκτρονικά ταχυδρομεία, στους λογαριασμούς κοινωνικής σας δικτύωσης, εξάγουμε ευαίσθητα δεδομένα και μοιράζουμε τις προσωπικές σας πληροφορίες στους στρατιώτες του χαλιφάτου, οι οποίοι σύντομα με την άδεια του Αλάχ θα επιτεθούν στα εδάφη σας*.!»

Ο Ferizi ήταν μέλος μιας ομάδας χάκερ του Κοσόβου, η οποία όπως ο ίδιος δήλωσε είχε δημιουργηθεί για να πολεμήσει ηλεκτρονικά στον κυβερνοπόλεμο την Σερβία. Είχε δηλώσει συγκεκριμένα ότι «*Ο λαός του Κοσσυφοπεδίου εκδιώχθηκε από την Δημοκρατία της Σερβίας. Ένας πόλεμος που πυροδοτήθηκε το 1999. Σκότωσαν περίπου 20.000 κόσμο και βίασαν πάνω από 30.000 γυναίκες. Η KHS (Kosova Hacker's Security) δημιουργήθηκε για να πολεμήσει την Σερβία στον Κυβερνοκόσμο*».[19] Οι επιθέσεις της KHS βεβαίως δεν παρέμειναν μόνο στην χώρα της Σερβίας αλλά πραγματοποίησαν πλήθος επιθέσεων εναντίον διεθνών οργανισμών, ιστοσελίδων και υπολογιστών

[18] "we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the [caliphate], who soon with the permission of Allah will strike at your necks in your own lands!".

[19] «Kosovo people were violated from the Republic of Serbia. A war sparked between Serbia and Kosovo in 1999. They killed about more than 20, 000 people and raped more than 30, 000 women. Kosova Hacker's Security was created to fight the Serbian country in the Cyber World".

διάφορων κυβερνήσεων όπως Ουκρανία, Ισραήλ, και οργανισμών όπως η Ιντερπόλ κλπ.

Πριν την ψήφιση του αντιτρομοκρατικού νόμου στην Αμερική , “USA Patriot Act”[20],ο οποίος ψηφίστηκε από το Κογκρέσο των Ηνωμένων Πολιτειών ως απάντηση στις επιθέσεις της 11ης Σεπτεμβρίου 2001, ο Feriz θα ήταν αδύνατον να συλληφθεί αλλά και να του απαγγελθούν οποιεσδήποτε κατηγορίες και αυτό γιατί τα εγκλήματα που διέπραξε στρέφονταν κατά υπολογιστών και πληροφοριακών συστημάτων και με το προϋπάρχον νομικό σύστημα των Ηνωμένων Πολιτειών δεν θα μπορούσε να στοιχειοθετηθεί η κατηγορία για διάπραξη τρομοκρατικών ενεργειών.

Στο άρθρο 18 U.S.C. §2332(b) του παραπάνω νόμου και με τίτλο “Κυβερνητικές πράξεις που διαπερνούν τα εθνικά σύνορα” (acts of terrorism transcending national boundaries) δίνεται ένας ορισμός σε μια σειρά τρομοκρατικών ενεργειών αλλά το συγκεκριμένο άρθρο δεν περιλαμβάνει όλα τα εγκλήματα κατά των πληροφοριακών συστημάτων και υπολογιστών[21]. Στο άρθρο 18 U.S.C. περιγράφονται μόνο τα εγκλήματα της κατασκοπείας και της κυβερνοτρομοκρατίας. Αυτό που παρατηρούμε να περιγράφεται στον συγκεκριμένο νόμο είναι ότι μια ενέργεια για να θεωρηθεί τρομοκρατική και η οποία αφορά σε ηλεκτρονικό υπολογιστή θα πρέπει η πράξη που διαπράττεται να χαρακτηρίζεται από την παραδοχή αυτής και θα πρέπει να υπάρχει πρόθεση πρόκλησης ζημιάς στα πληροφοριακά συστήματα.

Κεφάλαιο 6

Διεθνείς Στρατηγικές Αντιμετώπισης Κυβερνοτρομοκρατίας

6.1 Ευρωπαϊκή Ένωση

[20] Πλήρης τίτλος:Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”

[21] Έρχεται όμως με τον νόμο Computer Fraud and Abuse Act και συμπληρώνει το παραπάνω άρθρο του νόμου USA Patriot Act

Η Ευρωπαϊκή Επιτροπή ενέκρινε μια διάταξη που απαιτεί από όλα τα μέλη της Ευρωπαϊκής Ένωσης να επιβάλλουν ποινές σε όλες τις δραστηριότητες που χαρακτηρίζονται ως «επίθεση μέσω παρεμβολής σε πληροφοριακά συστήματα ως τρομοκρατική πράξη, εάν ο στόχος τους είναι «σοβαρή αλλοίωση ή καταστροφή πολιτικών, οικονομικών ή κοινωνικών δομών ». Η Γαλλία επέκτεινε την αστυνόμευση επί του θέματος στον έλεγχο ιδιωτικών ιδιοκτησιών χωρίς εντάλματα.

Η Ισπανία, παρόμοια με τη βρετανική νομοθεσία, περιορίζει τις δραστηριότητες οποιουδήποτε οργανισμού που σχετίζεται άμεσα ή έμμεσα με την ΕΤΑ (Euskadi Ta Askatasuna) – μια ένοπλη αυτονομιστική ομάδα για τη βασκική πατρίδα και την ελευθερία.

Η κυβέρνηση της Γερμανίας μειώνει τα όρια σχετικά με την παρακολούθηση τηλεφωνικών κλήσεων και την παρακολούθηση ηλεκτρονικών μηνυμάτων και τραπεζικών λογαριασμών και αποκαθιστά την προηγουμένως περιορισμένη επικοινωνία μεταξύ της μυστικής υπηρεσίας και της αστυνομίας.

Τον Ιούνιο του 2002, το Ηνωμένο Βασίλειο, με το πρόσχημα της αντιτρομοκρατίας, προσπάθησε να θεσπίσει κανονισμούς που θα εξουσιοδοτούσαν σχεδόν όλες τις τοπικές και εθνικές κυβερνητικές υπηρεσίες να έχουν πρόσβαση στην κυκλοφορία επικοινωνιών δεδομένων χωρίς την ανάγκη εντάλματος.

Η Αυστραλία εισήγαγε νόμο για τους τρομοκράτες προκειμένου να υποκλέψει το ηλεκτρονικό ταχυδρομείο (εξουσιοδοτώντας τον κύριο Αυστραλιανό Οργανισμό Πληροφοριών Ασφαλείας) και να δημιουργήσει μια επίθεση που να στρέφεται κατά της προετοιμασίας και του σχεδιασμού τρομοκρατικών ενεργειών. Αυτός ο νόμος επιτρέπει στην κυβέρνηση να «παγώσει» ή να αφαιρέσει την ιδιοκτησία ενός τρομοκράτη. Η Νέα Ζηλανδία έχει θεσπίσει παρόμοια νομοθεσία προκειμένου να συμμορφωθεί με τη διμερή συμφωνία για τη νομική εναρμόνιση μεταξύ αυτών των δύο χωρών.

Η Ινδία θέσπισε επίσης το δικό της διάταγμα για την προστασία από την τρομοκρατία, επιτρέποντας στις αρχές να συλλαμβάνουν τον ύποπτο χωρίς δίκη, για την παρακολούθηση και κατάσχεση χρημάτων και περιουσιών

ύποπτων τρομοκρατών, και σε ορισμένες περιπτώσεις για την επιβολή της θανατικής ποινής.

Ορισμένες πολιτείες, όπως στην περίπτωση των ΗΠΑ και της Αυστραλίας, συνέστησαν τη ρύθμιση ενός κέντρου λειτουργίας δικτύου στον κυβερνοχώρο, το οποίο θα περιλαμβάνει παρόχους υπηρεσιών Διαδικτύου και προγραμματιστές υλικού και λογισμικού υπολογιστών. Καθήκον τους είναι να αναπτύξουν ασφαλή τεχνολογία, ως έξυπνο λογισμικό ανάλυσης, που θα μπορεί να αναλύει υπάρχοντα δεδομένα, δημόσια και ιδιωτικά, προκειμένου να ανιχνεύει ύποπτες δραστηριότητες.

6.2 ΝΑΤΟ

Ξεκινά ένα νέο πρόγραμμα για την τρομοκρατία στον κυβερνοχώρο του ΝΑΤΟ, το οποίο περιλαμβάνει διάφορους φορείς του ΝΑΤΟ:

1. Η Υπηρεσία Επικοινωνιών και Πληροφοριών του ΝΑΤΟ (NCSA) ως η «πρώτη γραμμή άμυνας κατά της τρομοκρατίας στον κυβερνοχώρο»
2. Το Τεχνικό Κέντρο Ασφάλειας πληροφοριών (NITC), υπεύθυνο για τις επικοινωνίες και την ασφάλεια των υπολογιστών.
3. Κέντρο Επιχειρήσεων Διασφάλισης Πληροφοριών του ΝΑΤΟ (NIAOC), υπεύθυνο για τη διαχείριση και το συντονισμό του κρυπτογραφικού εξοπλισμού για την ετοιμότητα απόκρισης σε επίθεση στον κυβερνοχώρο εναντίον του ΝΑΤΟ.
4. Μηχανισμός - Ικανότητα Απόκρισης περιστατικών Υπολογιστών του ΝΑΤΟ (NCIRC) του οποίου στόχος είναι να προστατεύει τα κρυπτογραφημένα επικοινωνιακά συστήματα του ΝΑΤΟ.

Μετά την κυβερνοεπίθεση κατά της Εσθονίας τον Απρίλιο και τον Μάιο του 2007, οι υπουργοί του ΝΑΤΟ συμφώνησαν στο περίγραμμα της ιδέας της κυβερνοάμυνας του ΝΑΤΟ, η οποία παρουσιάστηκε στο Nordwijk, τον Οκτώβριο του 2008. Αυτή η ιδέα στις αρχές του 2008 αναπτύχθηκε σε Πολιτική του ΝΑΤΟ για την Κυβερνοασφάλεια.

Μετά τη Σύνοδο Κορυφής του Βουκουρεστίου τον Απρίλιο 2008, το ΝΑΤΟ ίδρυσε την Αρχή Διαχείρισης Κυβερνητικής Άμυνας (CDMA), προκειμένου να συγκεντρώσει όλους τους βασικούς δρώντες στις

δραστηριότητες του ΝΑΤΟ που σχετίζονται με την άμυνα στο κυβερνοχώρο και να διαχειριστεί με τον καλύτερο τρόπο την υποστήριξη στην κυβερνοάμυνα σε οποιοδήποτε μέλος της συμμαχίας κατά της επίθεσης στον κυβερνοχώρο, κατόπιν αιτήματος. Ταυτόχρονα, οι ηγέτες του ΝΑΤΟ συμφώνησαν με την επίσημη ίδρυση του Συνεργατικού Κέντρου Αριστείας Κυβερνοάμυνας του ΝΑΤΟ (CCD-CoE), το οποίο λειτουργεί πιστοποιημένα από το 2008. «Η αποστολή και το όραμα» του CCD-CoE περιγράφονται ως εξής: «ενίσχυση της ικανότητας, της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ του ΝΑΤΟ, των κρατών του ΝΑΤΟ και των εταίρων στην άμυνα στον κυβερνοχώρο μέσω της εκπαίδευσης, της έρευνας και της ανάπτυξης, των διδαγμάτων και της διαβούλευσης» και να είναι «η κύρια πηγή εμπειρογνωμοσύνης στον τομέα της συνεργατικής άμυνας στον κυβερνοχώρο με τη συσσώρευση, τη δημιουργία και τη διάδοση γνώσεων σε σχετικά θέματα εντός του ΝΑΤΟ, των κρατών του ΝΑΤΟ και των εταίρων». Η τρέχουσα οργάνωση έχει πολλούς «χορηγούς εθνών»: Εσθονία, Γερμανία, Ουγγαρία, Ιταλία, Λετονία, Λιθουανία, Ολλανδία, Πολωνία, Σλοβακία, Ισπανία και ΗΠΑ. Η σημασία του εν λόγω κέντρου το οποίο έχει έδρα στο Ταλίν διαφάνηκε κατά τη διάρκεια της επίθεσης στην Εσθονίας το 2007.

6.3 Ηνωμένα Έθνη

Στο σύστημα των Ηνωμένων Εθνών, η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) έχει την ευθύνη για τις πρακτικές και εφαρμογές της διεθνούς ασφάλειας στον κυβερνοχώρο. Η αποστολή του ITU καθορίζει το ζήτημα της ασφάλειας στον κυβερνοχώρο με συγκεκριμένους όρους.

Ο σκοπός του οργανισμού είναι να αναπτύξει ασφάλεια στη χρήση του κυβερνοχώρου μέσω ανάπτυξης βελτιωμένης ασφάλειας στο διαδίκτυο. Η επίτευξη της ασφάλειας στον κυβερνοχώρο και της ειρήνης στον κυβερνοχώρο είναι μερικές από τις πιο κρίσιμες ανησυχίες για την ανάπτυξη των Τεχνολογιών Επικοινωνιών και πληροφοριών (ICT), και η ITU λαμβάνει συγκεκριμένα μέτρα μέσω του Παγκόσμιου Προγράμματος Δράσης για την ασφάλεια στον κυβερνοχώρο (GCA) .

6.4 ΟΟΣΑ

Το 2002 εκδόθηκαν από τη Διεύθυνση Επιστήμης, Τεχνολογίας και Βιομηχανίας του ΟΟΣΑ, οι οδηγίες για την ασφάλεια των συστημάτων πληροφοριών και των δικτύων οι οποίες αποτελούν πρότυπο σημείο αναφοράς για εθνικές και διεθνείς πρωτοβουλίες επί της ασφάλειας στον κυβερνοχώρο.

Οι οδηγίες βασίζονται σε εννέα συμπληρωματικές αρχές που οργανώνουν μια ενιαία κατεύθυνση ασφάλειας:

1. Ευαισθητοποίηση (η ανάγκη ασφάλειας των συστημάτων πληροφοριών και δικτύων) .

2. Ευθύνη (όλοι οι συμμετέχοντες είναι υπεύθυνοι για την ασφάλεια των συστημάτων πληροφοριών και δικτύων) .

3. Απόκριση (οι συμμετέχοντες θα πρέπει να ενεργούν για περιστατικά ασφαλείας έγκαιρα και συνεργατικά) .

4. Δεοντολογία (σεβασμός των νόμιμων συμφερόντων άλλων χρηστών και προώθηση βέλτιστων πρακτικών) .

5. Δημοκρατία (τα μέτρα ασφαλείας πρέπει να είναι συμβατά με τις βασικές αξίες μιας δημοκρατικής κοινωνίας) .

6. Εκτίμηση κινδύνου (ευρεία εκτίμηση απειλών και αδυναμιών ως βάση για τη διαχείριση κινδύνων) .

7. Σχεδιασμός ασφαλείας (τα μέτρα ασφαλείας πρέπει να αποτελούν βασικό χαρακτηριστικό των συστημάτων πληροφοριών και των δικτύων) .

8. Διαχείριση ασφάλειας (ολοκληρωμένη προσέγγιση με τη συμμετοχή όλων των ενδιαφερομένων σε όλα τα επίπεδα, αντιμετώπιση απειλών όπως εμφανίζονται) .

9. Επανεκτίμηση (συνεχής επανεξέταση, αναθεώρηση και τροποποίηση των μέτρων ασφαλείας καθώς εξελίσσονται οι κίνδυνοι).

6.5 ΟΑΣΕ

Ο Οργανισμός ζήτησε από τις συμμετέχουσες χώρες να παρακολουθούν στενά τις ιστοσελίδες των τρομοκρατών και των εξτρεμιστικών

οργανώσεων και να ανταλλάσσουν πληροφορίες με άλλες κυβερνήσεις στο εσωτερικό του ΟΑΣΕ και άλλα σχετικά φόρουμ. Επιπλέον ζήτησε «πιο ενεργή συμμετοχή των κυβερνητικών ιδρυμάτων και του ιδιωτικού τομέα στην πρόληψη και την αντιμετώπιση της χρήσης του Διαδικτύου για τρομοκρατικούς σκοπούς.

Το φόρουμ συνεργασίας του ΟΑΣΕ για την ασφάλεια (FSC) συνέβαλε επίσης στην συμμετοχή του οργανισμού στον τομέα της ασφάλειας στον κυβερνοχώρο. Αν και το έργο του FSC έχει επικεντρωθεί σε μεγάλο βαθμό στον έλεγχο των όπλων, στον αφοπλισμό και στην οικοδόμηση μέτρων εμπιστοσύνης, τελευταία το φόρουμ άρχισε να ενδιαφέρεται περισσότερο για την ασφάλεια στον κυβερνοχώρο. Τον Μάρτιο του 2009, συγκλήθηκε σεμινάριο από τον ΟΑΣΕ για μια ολοκληρωμένη προσέγγιση για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Τέλος, ο ΟΑΣΕ υποστηρίζει τις εθνικές προσπάθειες, όπως τις Αρμενικές Ένοπλες Δυνάμεις επί της αντιμετώπισης του κυβερνοεγκλήματος και της κυβερνοασφαλείας.

6.6 Συμβούλιο της Ευρώπης (ΣτΕ)

Η συμβολή του ΣτΕ στη διεθνή πολιτική ασφάλειας στον κυβερνοχώρο γίνεται κυρίως μέσω της Σύμβασης για το έγκλημα στον κυβερνοχώρο, η οποία άνοιξε προς υπογραφή τον Νοέμβριο του 2001 και τέθηκε σε ισχύ τον Ιούλιο του 2004. Είναι σημαντικό να σημειωθεί ότι, αν και η Σύμβαση υπογράφηκε από πολλές χώρες, συμπεριλαμβανομένου του Καναδά, της Ιαπωνίας, της Νότιας Αφρικής και των ΗΠΑ, μέχρι σήμερα έχει επικυρωθεί από μόνο 26 χώρες, συμπεριλαμβανομένης της Βόρειας Μακεδονίας, της Αλβανίας, της Κροατίας, της Εσθονίας, της Ουγγαρίας, της Λιθουανίας, της Ρουμανίας και της Σλοβενίας. 11 κράτη της ΕΕ δεν έχουν ακόμη επικυρώσει τη Σύμβαση και πέντε κράτη μέλη του ΣτΕ δεν έχουν καν υπογράψει (συμπεριλαμβανομένης της Ρωσίας). Η Σύμβαση υπεγράφη και επικυρώθηκε από χώρες που δεν είναι μέλη του ΣτΕ (Καναδάς, Ιαπωνία, Νότια Αφρική και ΗΠΑ). Δεκαέξι άλλες χώρες που δεν είναι μέλη του Συμβουλίου της Ευρώπης αναφέρονται με τον τίτλο «χρησιμοποιούμενες τη Σύμβαση ως κατευθυντήρια γραμμή για την εθνική τους νομοθεσία» (συμπεριλαμβανομένης της Βραζιλίας και της Ινδίας).

Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο είναι σημαντική από πολλές πτυχές.

1. Η Σύμβαση αντιμετωπίζει τις παράνομες δραστηριότητες και πρακτικές που εμφανίζονται σε όλο το φάσμα των απειλών για την ασφάλεια στον κυβερνοχώρο.
2. Η Σύμβαση θεσπίζει κοινά πρότυπα και διαδικασίες που είναι νομικά δεσμευτικές για τους υπογράφοντες της.
3. Η Σύμβαση είναι ανοιχτή στα κράτη μέλη του Συμβουλίου και σε άλλα, γεγονός που αυξάνει την εξουσία της ως διεθνές μέσο.
4. Τέλος, η Σύμβαση εισήγαγε απαιτήσεις για το χειρισμό δεδομένων και την πρόσβαση που οδήγησαν σε ανησυχίες σχετικά με τη νομοθεσία περί απορρήτου και τις πολιτικές ελευθερίες.

6.7 G8

Η κύρια συμβολή του G8 στη διεθνή πολιτική ασφάλειας στον κυβερνοχώρο είναι η Υποομάδα Εγκλήματος υψηλής τεχνολογίας, που δημιουργήθηκε ως υποσύνολο του Ομίλου της Λυών το 1996 για την καταπολέμηση του διεθνούς οργανωμένου εγκλήματος. Ο σκοπός αυτής της υποομάδας ήταν «να ενισχύσει την ικανότητα των χωρών της G8 να προστατεύουν, να διερευνούν και να διώκουν εγκλήματα που διαπράττονται χρησιμοποιώντας υπολογιστές, επικοινωνίες δικτύου και άλλες νέες τεχνολογίες». Η αποστολή της υπομονάδας επεκτάθηκε με σκοπό να συμπεριλάβει τη χρήση του Διαδικτύου από τρομοκράτες και την προστασία της υποδομής πληροφοριών ζωτικής σημασίας. Η υποομάδα προσπαθεί να αντιμετωπίσει το έγκλημα στον κυβερνοχώρο όχι μόνο εντός της δικαιοδοσίας των χωρών της G8, αλλά και να δημιουργήσει κατευθυντήριες γραμμές που θα μπορούσαν να υιοθετήσουν και να εφαρμόσουν άλλες χώρες. Η υποομάδα έχει δημιουργήσει δίκτυο επαφής 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα για το έγκλημα υψηλής τεχνολογίας και την ενημέρωση του διεθνή καταλόγου για την προστασία της υποδομής κρίσιμων πληροφοριών (CCIP). Η υποομάδα έχει δημοσιεύσει τα έγγραφα βέλτιστων πρακτικών και τις κατευθυντήριες γραμμές για την αξιολόγηση των απειλών για την ασφάλεια των υπολογιστών και των

δικτύων και έχει οργανώσει διεθνή εκπαιδευτικά συνέδρια για υπηρεσίες εγκληματικότητας στον κυβερνοχώρο.

Κεφάλαιο 7

Νομικό πλαίσιο

7.1 Συνθήκη της Βουδαπέστης

Το συμβούλιο της Ευρώπης αναγνωρίζοντας την σπουδαιότητα των εγκλημάτων στον κυβερνοχώρο το 2001 φέρνει προς υπογραφή στα κράτη -μέλη του , μια Σύμβαση που αφορά το Κυβερνοέγκλημα. Η σύμβαση αυτή θα γίνει γνωστή με το όνομα Συνθήκη της Βουδαπέστης και η οποία τίθεται σε ισχύ από την 1η Ιουλίου του 2004[22].

Στόχος της Συνθήκης της Βουδαπέστης είναι να εναρμονιστεί η ποινική νομοθεσία των κρατών -μελών με την ποινικοποίηση ορισμένων παράνομων ενεργειών που λαμβάνουν χώρα στον κυβερνοχώρο. Η Σύμβαση λοιπόν περιέχει βασικά διατάξεις ουσιαστικού ποινικού δικαίου, οι οποίες ρυθμίζουν αδικήματα που αφορούν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που έχουν αποθηκευτεί σε υπολογιστικά συστήματα και σε συστήματα Ηλεκτρονικών Υπολογιστών.

Η εν λόγω Συνθήκη ξεκαθαρίζει και την έννοια της κυβερνοεγκληματικότητας, δηλαδή διακρίνονται τρία βασικά κριτήρια που είναι ο πυρήνας του κυβερνοεγκλήματος:

1. Η παράνομη πρόσβαση σε πληροφοριακό σύστημα
2. η παράνομη παρέμβαση σε πληροφοριακό σύστημα
3. η παράνομη παρέμβαση σε δεδομένα.

Αφού λοιπόν οριοθετείται η έννοια του κυβερνοεγκλήματος, η Σύμβαση προσδιορίζει επιμέρους ποινικά αδικήματα και επιβάλλει στα κράτη -μέλη που συμμετέχουν να χαρακτηρίσουν τις πράξεις, που από πρόθεση προκαλούν βλάβη στα δίκτυα, στην ακεραιότητα, στην διαθεσιμότητα των δεδομένων ή των συστημάτων πληροφορικής, ως αξιόποινες. Η Συνθήκη της Βουδαπέστης στα

[22] Η Ελλάδα είναι συμβαλλόμενο κράτος στην εν λόγω διεθνή σύμβαση, ωστόσο μέχρι και σήμερα δεν την έχει κυρώσει και ενσωματώσει στην Ελληνική έννομη τάξη.

άρθρα της, απαγορεύει την κατασκευή, κατοχή, διανομή και διάθεση προγραμμάτων υπολογιστών τύπου, όπως είναι γνωστά στην γλώσσα της πληροφορικής, ιών (viruses,virus), worms (σκουλήκια), Trojan Horses (Δούρειοι Ίπποι), και την διακίνηση συνθηματικών και κωδικών πρόσβασης και άλλα παρόμοια μέσα που μπορούν να στοιχειοθετήσουν την διάπραξη κάποιας αξιόποινης πράξης. Η Σύμβαση επίσης επιβάλλει στα συμβαλλόμενα κράτη - μέλη της να προβλέψουν στο ποινικό τους δίκαιο αδικήματα που τελούνται με υπολογιστές για παράδειγμα απάτη με Η/Υ, κατοχή και διεθνής διανομή παιδικής πορνογραφίας, πλαστογραφία και αδικήματα που αφορούν στην πνευματική ιδιοκτησία και την παραβίαση αυτής. Με αυτό τον τρόπο δίνεται η δυνατότητα στα συμβαλλόμενα κράτη-μέλη να διατηρήσουν την ιδιαιτερότητα της εσωτερικής τους έννομης τάξης αλλά παράλληλα να υιοθετήσουν και έννοιες «μη απόλυτες» δίνοντας έτσι την δυνατότητα στα κράτη - μέλη να διατυπώσουν τις επιφυλάξεις που δύνανται να έχουν προς την εφαρμογή ορισμένων διατάξεων αλλά και να τις προσαρμόσουν όπως αρμόζει στην εκάστοτε έννομη τάξη τους.

Η σύμβαση της Βουδαπέστης είχε ως σκοπό να θωρακίσει τις ποινικές δικονομικές διατάξεις των κρατών-μελών της οι οποίες είναι απολύτως απαραίτητες. Έτσι θεσπίστηκαν αναγκαίες διαδικασίες οι οποίες λειτουργούν αποτελεσματικά σε ότι αφορά την έρευνα, την συλλογή αποδεικτικών στοιχείων σε ηλεκτρονική μορφή σε πραγματικό χρόνο, την δίωξη και την εκδίκαση των εγκλημάτων που τελούνται, σε συστήματα πληροφοριών ή υπολογιστών αλλά και σε εγκλήματα που τελούνται στον κυβερνοχώρο ώστε να υπάρχει δυνατότητα αντιμετώπισης των διάφορων εμποδίων που προκαλούνται από τον διασυνοριακό χαρακτήρα των συγκεκριμένων εγκλημάτων. Έτσι λοιπόν οι διατάξεις του ποινικού δικονομικού δικαίου στοχεύουν στην έρευνα και κατάσχεση αποθηκευμένων αρχείων σε ηλεκτρονικό υπολογιστή, διαφύλαξη και γνωστοποίηση διακινούμενων δεδομένων, αντιμετώπιση υποκλοπής περιεχομένου δεδομένων σε πραγματικό χρόνο και διαφύλαξης αποθηκευμένων δεδομένων σε σύστημα ηλεκτρονικού υπολογιστή. Οι διατάξεις αυτές έχουν ως μοναδικό στόχο να δώσουν στις αρχές τον απαραίτητο χώρο αλλά και το σωστό νομοθετικό πλαίσιο ώστε να διεξάγονται οι απαραίτητες έρευνες και παράλληλα να παρεμποδίζεται η εξαφάνιση ή

απάλειψη δεδομένων, τα οποία είναι απαραίτητα για να καταστεί μια έρευνα, επείγουσα ή μη, σύννομη.

Γι' αυτό λοιπόν η Σύμβαση της Βουδαπέστης επιβάλλει στα κράτη - μέλη της την υποχρέωση να λάβουν μέτρα για την ορθή διαχείριση από τους παρόχους που αποθηκεύουν όλων των ειδών δεδομένων και να γίνεται σωστή κίνηση επαρκών δεδομένων ώστε να μπορεί να εντοπιστεί η διαδρομή κάποιας αξιόποινης πράξης και να είναι δυνατόν να παραδοθεί η συγκεκριμένη δρομολόγηση (της παραπάνω ενέργειας) στις Αρμόδιες Αρχές. Επίσης η σύμβαση προβλέπει την υποχρέωση των κρατών μελών να διατάσσουν πρόσωπα που βρίσκονται εντός της επικράτειας τους να παραδώσουν δεδομένα που είναι αποθηκευμένα είτε σε κάποιο πληροφοριακό σύστημα είτε σε κάποιο υπολογιστή τους, αλλά και στους παρόχους των υπηρεσιών αυτών των πληροφοριακών συστημάτων, ώστε να συνδράμουν όπως μπορούν παρέχοντας τις απαραίτητες πληροφορίες στις Αρμόδιες Αρχές.

Στο άρθρο 22 της Σύμβασης της Βουδαπέστης υπάρχει ειδική ρύθμιση για την δικαιοδοσία. Ειδικότερα, κάθε συμβαλλόμενο μέρος έχει δικαιοδοσία αν η παράβαση έλαβε χώρα

1. εντός της επικράτειάς του
2. επί ενός πλοίου που φέρει την σημαία του εν λόγω Συμβαλλόμενου Μέρους
3. επί ενός αεροσκάφους που είναι καταχωρημένο σύμφωνα με τους νόμους του εν λόγω Συμβαλλόμενου Μέρους
4. από ένα πολίτη του, εάν το έγκλημα τιμωρείται από το ποινικό δίκαιο στον τόπο που διαπράχθηκε ή εάν το έγκλημα διαπράχθηκε εκτός της εδαφικής δικαιοδοσίας ενός κράτους[23]

Η διάταξη όμως δεν αποκλείει την δυνατότητα στο Κράτος-μέλος να ασκήσει ποινική δίωξη σύμφωνα με το εγχώριο δίκαιο του, χωρίς αυτό να αποτελεί παραβίαση της δικαιοδοσίας. Αν τώρα υπάρχει διεκδίκηση από πολλά Κράτη μέλη που έχουν δικαιοδοσία επί ενός εγκλήματος, τότε η Σύμβαση δίνει

[23] Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο , Άρθρο 22

την δυνατότητα διαβούλευσης των Κρατών για να βρεθεί η καταλληλότερη δικαιοδοσία για να ασκηθεί η δίωξη.

Η Οδηγία 2013/40/ΕΕ και συγκεκριμένα το άρθρο 12 ξεκαθαρίζει ότι «τα κράτη μέλη θεμελιώνουν τη δικαιοδοσία τους, εφόσον το αδίκημα έχει διαπραχθεί:

1. εν όλω ή εν μέρει στο έδαφος τους· ή
2. από υπήκοό τους, τουλάχιστον σε περιπτώσεις κατά τις οποίες η πράξη θεωρείται αδίκημα στον τόπο όπου έχει διαπραχθεί.

Τα κράτη-μέλη εξασφαλίζουν ότι διαθέτουν δικαιοδοσία, αν:

1. ο δράστης διέπραξε το αδίκημα, όταν βρισκόταν στο έδαφός τους, ανεξάρτητα από το εάν το αδίκημα στρεφόταν κατά συστήματος πληροφοριών στο έδαφός τους

2. το αδίκημα στρέφεται κατά συστήματος πληροφοριών στο έδαφός τους ανεξάρτητα από το εάν όταν ο δράστης διέπραξε το αδίκημα βρισκόταν στο έδαφός τους. Αν τώρα το κράτος μέλος θέλει να θεμελιώσει δικαιοδοσία για κάποιο αδίκημα που διαπράττεται εκτός συνόρων του πρέπει εν πρώτης να ενημερώσει την Επιτροπή και μπορεί να διεκδικήσει την δικαιοδοσία εφόσον, μεταξύ άλλων, : α) ο δράστης του αδικήματος έχει τη συνήθη κατοικία του στο έδαφος του, ή β) το αδίκημα διαπράττεται προς όφελος νομικού προσώπου εγκατεστημένου στο έδαφος του[24]»

Η Σύμβαση της Βουδαπέστης έθεσε σε πρωταγωνιστικό ρόλο διατάξεις διεθνούς δικαστικής συνεργασίας, που προσδιορίζουν και εξασφαλίζουν στο σύστημα των υπολογιστών

1. την διαφύλαξη αποθηκευμένων δεδομένων τους ,
2. την παροχή πληροφοριών ,
3. την αμοιβαία συνδρομή ,
4. την έκδοση
5. την γνωστοποίηση των διαφυλαγμένων δεδομένων που διακινούνται.

[24] ΟΔΗΓΙΑ 2013/40/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ, της 12ης Αυγούστου 2013, για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, άρθρο 12

Κατ΄ αυτόν τον τρόπο εισήγαγε κανόνες διεθνούς συνεργασίας και επικοινωνίας και επικεντρώθηκε στην ανάγκη της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του κυβερνοεγκλήματος. Πρόβλεψε και επέκτεινε την συνεργασία με όλα τα κράτη (και ιδιαιτέρως με τα κράτη εκτός Ευρώπης, που δεν έχουν ακόμη προσχωρήσει στην Σύμβαση) προβλέποντας την απαραίτητη νομοθετική κάλυψη. Ειδικότερα πρόβλεψε την θέσπιση κανόνων για τα αδικήματα στα οποία επικεντρώνει η Σύμβαση το ενδιαφέρον της και την επιβολή ποινών φυλακίσεως το ελάχιστο ενός χρόνου. Ακόμη καθιέρωσε γενικές αρχές που ρυθμίζουν την αμοιβαία συνδρομή και τους τρόπους με τους οποίους θα παρέχεται αυτή ,ιδίως όσον αφορά κράτη που δεν υπάρχει η σχετική Σύμβαση, απλοποιώντας τις διαδικασίες που τις διέπουν και περιορίζοντας τους λόγους αρνήσεως παροχής της συνδρομής

Επιπρόσθετα :

1. Διαμόρφωσε κανόνες που επιδιώκουν την απλοποίηση της αυθόρμητης παροχής πληροφοριών που αφορούν κυρίως δεδομένα προσωπικού χαρακτήρα μεταξύ των κρατών που συνδέονται με την παροχή συνδρομής ,
2. Επέκτεινε την παραπάνω δυνατότητα ιδίως για τα κράτη που δεν διαθέτουν νομοθεσία προστασίας προσωπικών δεδομένων
3. Ρύθμισε (δικονομικά) τα θέματα της διατήρησης δεδομένων, της αποκάλυψής τους, των κατασχέσεων κατόπιν ερευνών τυχόν αποθηκευμένων δεδομένων και της υποκλοπής δεδομένων κινήσεως και περιεχομένου.
4. Προέβλεψε σχετικά με το ζήτημα της δικαιοδοσίας κάθε μέρος που συμβάλλεται να έχει δικαιοδοσία εφόσον μέσα στην επικράτειά του διαπράττεται το αδίκημα, αλλά να έχει επίσης δικαιοδοσία και όταν το αδίκημα – παράβαση- έγκλημα διαπράττεται σε άλλη χώρα από υπήκοο του , ή ακόμη και εκτός της εδαφικής δικαιοδοσίας κάποιου κράτους.

7.2 Ελληνικό νομικό πλαίσιο

Η κυβερνοτρομοκρατία δεν τυποποιείται αυτοτελώς σαν έγκλημα ούτε στον Ποινικό Κώδικα ούτε σε διεθνή νομοθετικά κείμενα, γεγονός που σημαίνει ότι δεν τιμωρείται. Έτσι λοιπόν παρατηρούμε ότι ως κυβερνοτρομοκρατία μπορούμε να ορίσουμε την τέλεση ενός οποιουδήποτε τυποποιημένου στον ποινικό κώδικα κυβερνοεγκλήματος, υπό στενή έννοια με τρόπο ή σε έκταση ή

υπό συνθήκες που είναι δυνατό να βλάψει σοβαρά μια χώρα ή έναν διεθνή οργανισμό και με σκοπό (του δράστη) :

1. Να εκφοβίσει σοβαρά έναν πληθυσμό .
2. Να εξαναγκάσει παρανόμως δημόσια αρχή.
3. Να εξαναγκάσει διεθνή οργανισμό να εκτελέσει οποιαδήποτε πράξη .
4. Να βλάψει σοβαρά ή να καταστρέψει τις θεμελιώδεις συνταγματικές, πολιτικές, οικονομικές δομές μιας χώρας ή ενός διεθνούς οργανισμού.

Ο όρος “κυβερνοέγκλημα υπό ευρεία έννοια” από την άποψη του ουσιαστικού ποινικού δικαίου χρησιμοποιείται καταχρηστικά, αφενός γιατί με την εξέλιξη και τη χρήση των μέσων που προσφέρει η τεχνολογία όλα τα εγκλήματα στην πραγματικότητα είναι δυνητικά κυβερνοεγκλήματα, αφού μεσολαβεί η χρήση δικτύων ή συστημάτων πληροφοριών σε κάποιο στάδιο της εκτέλεσής τους και αφετέρου διότι πρόκειται για την ίδια πράξη η οποία τελείται με τη χρήση νέων μέσων και εργαλείων.

Η χρήση του όρου «κυβερνοέγκλημα υπό στενή έννοια» έγινε αναγκαία λόγω της Σύμβασης της Βουδαπέστης, η οποία εισήχθη στην ελληνική έννομη τάξη με τον ν.4411/2016, και εκεί για πρώτη φορά θεσπίστηκαν τα παραπάνω εγκλήματα. Τα κυβερνοεγκλήματα παρουσιάζουν ιδιαιτερότητα αφού η διάπραξη αυτών αλλά και η επέλευση των αποτελεσμάτων αυτών των πράξεων συναντάται καθαρά στον ψηφιακό κόσμο, τουτέστιν στον κυβερνοχώρο. Στα εν λόγω εγκλήματα, που εισήχθησαν στην ελληνική ποινική έννομη τάξη με τον ν. 4411/2016, παρατηρείται ότι εκτός ότι τελούνται στον κυβερνοχώρο, ο δράστης χρησιμοποιεί τις δυνατότητες που του παρέχει ο κυβερνοχώρος για να στραφεί είτε κατά των ίδιων των δομικών στοιχείων του κυβερνοχώρου (πληροφοριακά συστήματα , βάσεις δεδομένων κλπ) είτε (ο δράστης) κατά της ακεραιότητας, της διαθεσιμότητας των δεδομένων, είτε απλά για να αποκτήσει παράνομη πρόσβαση σε συστήματα, να υποκλέψει και να δημιουργήσει παρεμβολές σε δεδομένα και πληροφοριακά συστήματα.

Η έννοια της «πράξης» στο κυβερνοέγκλημα αποκτά τελείως διαφορετικό περιεχόμενο αφού το προσβαλλόμενο έννομο αγαθό, το υποκείμενο, ο χώρος και ο χρόνος τέλεσης τους εγκλήματος βρίσκονται σε ψηφιακή διάσταση. Πράγμα που σημαίνει ότι στο άρθρο 14 ΠΚ δεν έχουμε μεταβολή μόνο

κάποιων στοιχείων της πράξης, αλλά έχουμε αλλαγή του πλαισίου αναφοράς της πράξης αφού το έγκλημα αφορά τον υλικό κόσμο, ενώ το κυβερνοέγκλημα τον ψηφιακό.

Το κυβερνοέγκλημα μπορεί να κατηγοριοποιηθεί ως εξης:

1. Εάν το άμεσα προσβαλλόμενο αντικείμενο που εξειδικεύει το προσβαλλόμενο έννομο αγαθό είναι υλικό ή ψηφιακό.

2. Το περιβάλλον διενέργειας της πράξης απαιτείται να είναι de facto εν όλω ψηφιακό.

3. Το αποτέλεσμα της πράξης δεν νοείται να μην επιφέρει συγκεκριμένα αποτελέσματα στον ψηφιακό κόσμο

4. Είναι απαραίτητο να διαχωριστεί η τρομοκρατία από τα υπόλοιπα εγκλήματα, άρα και στην ηλεκτρονική τους μορφή ,και να ληφθεί υπόψη το κίνητρο των πράξεων και οι απώτερες άμεσες ή έμμεσες συνέπειες τους[25].

Η επικύρωση της Σύμβασης της Βουδαπέστης με τον ν.4411/2016 επέφερε σημαντικές αλλαγές στον Ποινικό Κώδικα προσθέτοντας και αλλάζοντας διάφορα άρθρα. Ενδεικτικά αναφέρονται οι επιπρόσθετες περιπτώσεις στ και ζ στο άρθρο 13 ΠΚ (όπως τροποποιήθηκε με τον ν. 4619) , όπου εξηγεί τις έννοιες του πληροφοριακού συστήματος και των ψηφιακών δεδομένων . Συγκεκριμμένα ορίζεται ότι " **Πληροφοριακό σύστημα**" είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών εκ των οποίων μία ή περισσότερες εκτελούν σύμφωνα με ένα πρόγραμμα αυτόματη επεξεργασία ψηφιακών δεδομένων , καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται αποτελούν αντικείμενο επεξεργασίας , ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση , την προστασία και τη συντήρηση των συσκευών αυτών ΄΄ Και περαιτέρω "**Ψηφιακά δεδομένα**" είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα,

[25] Στην περίπτωση δηλαδή της τρομοκρατίας, «ο σοβαρός εκφοβισμός ενός πληθυσμού ή ο παράνομος εξαναγκασμός δημόσιας αρχής ή διεθνούς οργανισμού να εκτελέσει οποιαδήποτε πράξη ή να απόσχει από αυτήν ή η πρόκληση σοβαρής βλάβης ή και καταστροφής των θεμελιωδών συνταγματικών, πολιτικών, οικονομικών δομών μιας χώρας ή ενός διεθνούς οργανισμού» σύμφωνα με το ελληνικό δίκαιο, ή ο αντίστοιχος παράγων που σε κάθε περίπτωση διαφοροποιεί την τρομοκρατία από το κοινό έγκλημα σε άλλα δικαιϊκά συστήματα ή πολιτικές θεωρίες.

συμπεριλαμβανομένου προγράμματος που παρέχει την δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μία λειτουργία΄΄.-, Με τους ανωτέρω ορισμούς αποσαφηνίστηκαν κατά τρόπο αναμφισβήτητο οι έννοιες των ΄΄πληροφοριακών συστημάτων΄΄ και των΄΄ ψηφιακών δεδομένων΄΄ και έχει καταστεί δυνατή η αντιμετώπιση των παραβατικών επεμβάσεων και των παρανομιών που διαπράττονται σχετικά με ό,τι αφορά τα θέματα που ανάγονται στις έννοιες αυτές.-

Περαιτέρω προστέθηκαν στις διατάξεις του ΠΚ τα άρθρα 292Β και 292Γ , τα οποία αναφέρονατι στην ΄΄παρακώλυση λειτουργίας πληροφοριακών συστημάτων΄΄

. Με το ανωτέρω άρθρο 292Β αποσαφηνίστηκε πλέον κατά αναλυτικό τρόπο η έννοια της παρακωλύσεως και προβλέφθηκαν σημαντικές ποινές για την παραβίαση των σχετικών διατάξεων των Αποσαφηνίστηκε ,λοιπόν , και προβλέφθηκε ότι ΄΄ 1.-΄Οποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή η διακόπτυει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή , διαβίβαση , διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα μέσα αυτά , τιμωρείται με φυλάκιση και χρηματική ποινή. 2.-Η πράξη της πρώτης παραγράφου τιμωτείται α) με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή , αν τελέσθηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημα΄των πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών , οικονομική ζημία ιδιαόιτερα μεγάλης αξίας ή σημαντική απώλεια δεδομεών , β) με φυλάκιση τουλάχιστον δύο ετών και χηματική ποινή αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών , οικονομική ζημία ιδιαιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομεών και γ) με φυλάκιση τουλάχιστον τρρειώβ ετών και χρηματική ποιμνή , αν τελέστηκε κατά συστημα΄των πληροφοριών που αποτελοπύν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες .Ως

ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα , η υγεία , οι συγκοινωνίες . οι μεταφορές και η ενέργεια.-΄΄

Ενώ περαιτέρω με το άρθρο 292 Γ ορίσθεκε : ΄΄ Μ εφυλάκιση έως δύο έτη ή χρηματική ποινή τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί ,προμηθεύεται προς χρήση , εισάγει , κατέχει , διανέμει ή με άλλο τρόπο διακινεί α) συσκευές ή προγράμματα υπολογιστή σχεδιασμένα ή προσαρμοσμένα κυρίως για τον σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β , β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με την χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος του πληρφοριακού συστήματος.΄΄

Ακόμη αντικαταστάθηκε το άρθρο 370Γ ,που αφορούσε σε παράνομη πρόσβαση σε πληροφοριακό σύστημα και αποσαφηνίσθηκε ότι ΄΄1.- ΄Οποιος αθέμιτα αντιγράφει , αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών , τα οποία συνιστούν κρατικά , επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχος τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα ,ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. , 2.-Ασν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων , καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. ΄΄

Και ακόμη προστέθηκε το άρθρο 370 Δ το οποίο κάνει λόγο για την αθέμιτη χρήση τεχνικών μέσων και αποσαφηνίζει και προβλέπει και ρυθμίζει ότι ΄΄ 1.- όποοιος χωρίες δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών , τιμωρείαι με χρηματική ποινή ή παροχή κοινωφελούς υπηρεσίας , 2.- ΄Οποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών , παραβιάζοντας απαγορεύσεις ή κ,έτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του τιμωρείται με

φυλάκιση. 3.- Αν ο δράστης είναι στη υπηρεσία του νομίμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων , η πράξη της προηγούμενης παραγράφου τιμωρείται μόνον αν απαγορεύεατι ρητά από εσωτερικό κανονισμό από έγγραφη απόφαση του κατόχου ή αρμόδιθου υπαλλήλου.- ΄΄

Σημαντική επίσης είναι η αντικατάσταση των διατάξεων του άρθρου 386Α ΠΚ , το οποίο αναλύει την απάτη με υπολογιστή και προβλέπει ότι ΄΄ 1.- ΄Οποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος , βλάπτει ξένη περιουσία επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή , β) με τη χωρίς δικαίωμα παρέμβαση στη λειτουργία προγράμματος ή συστήματος υπολογιστή , γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή , ιδίως δεδομένων αναγνώρισης της ταυτότητας , δ) με τη χωρίς δικαίωμα εισαγωγή , αλλοίωση , διαγραφή ή εξάλειψη δεδομένων υπολογιστή , ιδίως δεδομένων αναγνώρισης της ταυτότητας ή ε) με την χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για την μετακίνηση χρημάτων , τιμωρείται με φυλάκιση και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το πο΄σον των εκατόν είκοσί χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή. . 2.- ΄Οιποιος κατασκευάζει , διαθέτει η κατέχει πρόγραμμα ή σύστημα υπολογιστή που προορίζεται για διάπραξη εγκλήματος της παραγράφου 1 τιμωρείται με φυλάκιση έως δύο έτη και χρηματική ποινή . Απαλλάσσεται από κάθε ποινή όποιος καταστρέφει με δική του θέληση το παραπάνω πρόγραμμα ή σύστημα υπολογιστή πριν το χρησιμοποιήσει για την διάπραξη του εγκλήματος της παραγράφου 1. 3.- Αν η απάτη με υπολογιστή στρέφεται άμεσα κατά του νομικού προσώπου , του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζηνία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες.Η πράξη αυτή παραγράφεται μετά είκοσι έτη. ΄΄ .

Αυτά είναι μερικά από τα άρθρα που αντικαθίστανται με τον ν. 4411/2016 στην έννομη ελληνική ποινική νομοθεσία , όπως αυτά τροποποιήθηκαν με τον ν. 4619/2019.-

Η Ευρωπαϊκή Ένωση εξέδωσε την Οδηγία (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου του 2017 με σκοπό την καταπολέμηση της τρομοκρατίας (την αντικατάσταση της απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου) και την προσαρμογή της νομοθεσίας των Κρατών Μελών της για την καταπολέμηση της τρομοκρατίας λαμβάνοντας υπόψη τον διεθνή χαρακτήρα της τρομοκρατίας. Η παραπάνω οδηγία θεσπίζει κανόνες σχετικά με τον ορισμό των αδικημάτων και των σχετικών ποινών στον τομέα της τρομοκρατίας και προβλέπει έναν εξαντλητικό κατάλογο σοβαρών αδικημάτων τα οποία οι χώρες της ΕΕ στην εθνική τους νομοθεσία πρέπει να ταξινομούν ως τρομοκρατικά αδικήματα όταν διαπράττονται ή υπάρχει απειλή διάπραξής τους για συγκεκριμένο τρομοκρατικό σκοπό. Παρατηρούμε ότι η Οδηγία προβλέπει και την λήψη μέτρων για την άμεση αφαίρεση και το κλείδωμα τρομοκρατικού διαδικτυακού περιεχομένου που φιλοξενείται στην επικράτειά τους και την επίτευξη της αφαίρεσης του περιεχομένου αυτού από ιστοσελίδες εκτός της επικράτειάς τους. Τονίζεται επίσης η ανάγκη, με την τροποποίηση της απόφασης 2005/671/ΔΕΥ, της ανταλλαγής πληροφοριών και της συνεργασίας όσον αφορά τα τρομοκρατικά αδικήματα. Συνίσταται δε η συλλογή πληροφοριών και διαβίβασης τους στην Europol ή την EuroJust.

Κεφάλαιο 8

Προτάσεις αντιμετώπισης Κυβερνοεπιθέσεων.

8.1.Εκπαίδευση των πολιτών.

Το πρώτο βήμα για τη στήριξη της κυβερνοάμυνας του ευρύτερου κοινού είναι η εκπαίδευση. Βλέπουμε ότι η εκπαίδευση είναι ένας σημαντικός παράγοντας—οι χώρες με ισχυρά εκπαιδευτικά συστήματα, είναι λιγότερο ευάλωτες σε κυβερνοεπιθέσεις. Πολλές χώρες προσφέρουν ιστότοπους και μαθήματα όπου οι πολίτες τους μπορούν να μάθουν περισσότερα για τις πρακτικές ασφάλειας στον κυβερνοχώρο .

Θα ήταν λοιπόν πολύ πρακτικό αν :

1. Οι χώρες σε παγκόσμιο επίπεδο μπορούν να δημιουργήσουν εκπαιδευτικό υλικό προσαρμοσμένο στις ανάγκες της κάθε χώρας και να το φιλοξενούν τόσο σε εθνικούς διακομιστές όσο και σε δημοφιλείς ιστοσελίδες, έτσι ώστε όλοι να μπορούν να αξιοποιήσουν αυτήν την επένδυση ως κοινόχρηστο πόρο. Το εκπαιδευτικό υλικό μπορεί να περιλαμβάνει (αλλά σίγουρα δεν πρέπει να περιορίζεται) σε Βίντεο κλιπ 5 λεπτών ή λιγότερο το οποίο θα δημοσιεύεται στο κανάλι YouTube του εκάστοτε κράτους αλλά και σε παρόμοιους ιστότοπους. Ηχητικές μηνύματα μπορούν να παίζονται ως ανακοινώσεις σε δημόσιες υπηρεσίες σε περιοδικά διαστήματα και σε κατάλληλους ραδιοφωνικούς σταθμούς.

2. Τα σχολεία είναι απαραίτητο να έχουν υποχρεωτικό μάθημα την ασφάλεια στον κυβερνοχώρο μια φορά το χρόνο. Όπως έχουν επιλεγεί συγκεκριμένες μέρες στις οποίες τα παιδιά διδάσκονται για την ανακύκλωση, την υγιεινή, την σεξουαλική διαπαιδαγώγηση, είναι αναγκαίο να δημιουργηθούν αντίστοιχες μέρες εκμάθησης κυβερνοασφάλειας. Κατά τις εν λόγω ημέρες όλα τα σχολεία θα υποχρεούνται να διδάσκουν βασικές αρχές κυβερνοασφάλειας στους μαθητές. Οι δοκιμές παραβίασης της ασφάλειας στον κυβερνοχώρο είναι επιτακτικό να αποτελούν μέρος των προγραμμάτων σπουδών των μαθητών, ώστε οι μαθητές να προσέχουν τι διατυπώνεται κατά τη διάρκεια των διαλέξεων για την κυβερνοασφάλεια και να μπορούν να το αφομοιώνουν πιο αποτελεσματικά.

3. Οι κυβερνητικοί οργανισμοί και εταιρείες είναι αναγκαίο να περιλαμβάνουν τουλάχιστον 1-2 ώρες κυβερνοασφάλειας ως μέρος των προγραμμάτων εκπαίδευσης του προσωπικού τους, τόσο για νέους υπαλλήλους όσο και ως μέρος προγραμμάτων επανεκπαίδευσης και εκτεταμένης μάθησης.

8.2 Οικοδόμηση Εθνικής Ικανότητας Κυβερνοάμυνας

Το πρώτο βήμα που χρειάζεται να κάνουν παγκοσμίως οι χώρες για να χτίσουν την άμυνα τους κατά των κυβερνοεπιθέσεων είναι η ανίχνευση. Έρευνες δείχνουν ότι όταν δημοσιευθούν τα τρωτά σημεία κάποιας εταιρείας ή ενός οργανισμού (κυβερνητικού ή μη) ο όγκος των επιθέσεων αυξάνεται κατά

πέντε φορές. Οι χώρες λοιπόν, πρέπει να είναι εξαιρετικά προσεκτικές στην παρακολούθηση των εγχώριων δικτύων τους και πρέπει να βρίσκονται σε συνεχή επαγρύπνηση για αναφορές νέων ευπαθειών στον κυβερνοχώρο. Όλα αυτά απαιτούν ισχυρές δομικές αλλαγές στην εδραίωση της κυβερνοασφάλειας, όπως την δημιουργία μιας ομάδας επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο. Η οικοδόμηση μιας τέτοιας βασικής ομάδας κορυφαίων επαγγελματιών στον τομέα της κυβερνοασφάλειας, η οποία θα εργάζεται για τις κυβερνήσεις αποτελεί μεγάλη πρόκληση, αφού οι κορυφαίοι ειδικοί στον συγκεκριμένο τομέα τείνουν να εργάζονται για εταιρείες του ιδιωτικού τομέα όπου τα οικονομικά κίνητρα είναι μεγαλύτερα από τα αντίστοιχα του δημόσιου τομέα.

Οι ενέργειες που θα μπορούσαν να αναληφθούν σε εθνικό επίπεδο είναι οι παρακάτω:

1. Παροχή οικονομικών κινήτρων σε πανεπιστήμια και κοινοτικά κολέγια για να περιλαμβάνουν στην διδακτική ύλη μαθήματα κυβερνοασφάλειας.
2. Παροχή οικονομικών κινήτρων (π.χ. δίδακτρα πανεπιστημίου ή σε μεταπτυχιακούς τίτλους ή πιστώσεις για δίδακτρα κολεγίου) σε φοιτητές για να υιοθετήσουν σταδιοδρομία στον τομέα της κυβερνοασφάλειας με υποχρέωση την υπηρεσία σε κρατικό φορέα επί συγκεκριμένου χρονικού διαστήματος (15 χρόνια).
3. Παροχή ανταγωνιστικών αμοιβών στους δημόσιους υπαλλήλους που εργάζονται στον τομέα της κυβερνοασφάλειας.
4. Προσφορά υποτροφιών ερευνητικών προγραμμάτων σε πανεπιστήμια που αναπτύσσουν αλγόριθμους για τον εντοπισμό σε πραγματικό χρόνο της απειλής στον κυβερνοχώρο, καθώς και για τον μετριασμό του κινδύνου.
5. Να δημιουργηθούν εθνικές Ομάδες Αντιμετώπισης Έκτακτης Ανάγκης Υπολογιστών (CERT) με πρότυπο το CERT των ΗΠΑ που ασχολείται με την παρακολούθηση και τον εντοπισμό απειλών στον κυβερνοχώρο σε πραγματικό χρόνο.
6. Να δοθούν οικονομικά κίνητρα που εκτείνονται και στο προσωπικό που συμμετέχει στις εν λόγω εταιρείες (π.χ. ευνοϊκή φορολογική μεταχείριση) οι οποίες ενθαρρύνουν την συνεργασία και συνεισφέρουν ενεργά στις εθνικές

Ομάδες Αντιμετώπισης Έκτακτης Ανάγκης Υπολογιστών (CERT). Επίσης τα οικονομικά κίνητρα να αφορούν και την εκπαίδευση του προσωπικού των εταιρειών σε θέματα κυβερνοασφάλειας.

8.3 Έγκαιρη Οικοδόμηση Νομοθετικού Πλαισίου για την κυβερνοασφάλεια.

Εγκληματίες θα υπάρχουν πάντα, ειδικά όταν είναι δυνατό να επωφεληθούν από τα κενά τόσο των νόμων των μεμονωμένων εθνών, όσο και από τα κενά που υπάρχουν πέρα από τα εθνικά σύνορα, τα οποία μπορούν να επιδεινωθούν περαιτέρω από τα εθνικά και πολιτικά συμφέροντα.

Κάθε χώρα όχι μόνο χρειάζεται ένα ισχυρό σύνολο νόμων που αφορούν την ασφάλεια στον κυβερνοχώρο, αλλά, ίσως το πιο σημαντικό, έναν μηχανισμό και έναν φορέα για την επιβολή, την ερμηνεία και την προσαρμογή αυτών των νόμων στον ταχέως εξελισσόμενο τομέα της πληροφορικής. Ειδικότερα:

1. Οι χώρες κρίνεται αναγκαίο να ιδρύσουν μια Εθνική Αρχή Κυβερνοασφάλειας επιφορτισμένη με το έργο της ρύθμισης της κυβερνοσφαίρας, μέσω της ερμηνείας των κατάλληλων νόμων που υπάρχουν ήδη στα βιβλία για νέες συμπεριφορές στον κυβερνοχώρο. Ρόλος της εν λόγω αρχής θα είναι να παρακολουθεί στενά την εκκολαπτόμενη τεχνολογία, ώστε οι νέοι νόμοι να μπορούν να εγκριθούν αμέσως μετά τη διάθεση της νέας τεχνολογίας στην αγορά, και όχι αρκετά χρόνια αργότερα.
2. Οι χώρες κρίνεται αναγκαίο να καθορίσουν μια εθνική διαδικασία η οποία θα δύναται να καταπολεμήσει αποτελεσματικά οποιαδήποτε αναδυόμενη τεχνολογία που μπορεί να χρησιμοποιηθεί για την πραγματοποίηση επιθέσεων στον κυβερνοχώρο. Ορισμένες χώρες μπορεί να αντιμετωπίζουν μια τέτοια νέα τεχνολογία όπως η τεχνολογία όπλων που χρειάζεται προσεκτική παρακολούθηση και ρύθμιση, ενώ άλλες μπορεί να επιλέξουν λιγότερους κανονισμούς.
3. Οι χώρες κρίνεται αναγκαίο να διασφαλίσουν την θέσπιση ισχυρών νόμων, και την ίδρυση επαρκών αρχών επιβολής αυτών, για τη δίωξη ατόμων που διαπράτουν εγκλήματα στον κυβερνοχώρο, ακόμη κι αν αυτά τα εγκλήματα διαπράχθηκαν εκτός των συνόρων της χώρας τους.

8.4 Διεθνής Συνεργασία Κυβερνοασφάλειας.

Απαιτείται συντονισμός μεταξύ των χωρών για την ρύθμιση του εγκλήματος στον κυβερνοχώρο. Η Interpol και η Europol συμβάλλουν σημαντικά στη διαμόρφωση ποινικών ερευνών σε όλο τον κόσμο. Στη Χάγη, το Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο έχει αναπτύξει μεθόδους για την ενσωμάτωση διασυνοριακών ερευνών για εγκλήματα στον κυβερνοχώρο. Υφίσταται όμως μεγαλύτερη ανάγκη για την ίδρυση μιας διεθνούς υπηρεσίας επιφορτισμένης με τη σύναψη πολυμερών συμφωνιών κυβερνοασφάλειας και τη διαμεσολάβηση διαφορών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο μεταξύ των εθνών.

Συγκεκριμένα προτείνεται η δημιουργία:

1. Ενός ενιαίου οργανισμού επιφορτισμένου με το έργο της ασφάλειας στον κυβερνοχώρο, όπως η σύνθεση του G-20, μεταξύ των πιο έμπειρων χωρών στον κυβερνοχώρο, ο οποίος είναι αρκετά ισχυρός ώστε να περιλαμβάνει μεγάλες ανεπτυγμένες οικονομίες καθώς και μεγάλες αναπτυσσόμενες οικονομίες.
2. Ενός Διεθνή Οργανισμού Κυβερνοασφάλειας, παρόμοιου με τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU), που θα συνδράμει στη διαμόρφωση πολυεθνικών συμφωνιών γύρω από την ασφάλεια στον κυβερνοχώρο και θα παρέχει ένα μέσο για την επιβολή τους. Συγκεκριμένα, ένας τέτοιος οργανισμός θα μπορούσε να ασκήσει πίεση στα κράτη μέλη ώστε να τηρούν έναν υπεύθυνο κώδικα με νόμους για το κυβερνοέγκλημα και επιβολής αυτών εγχώρια.
3. Ενός οργανισμού που θα παρέχει εκπαιδευτικά προγράμματα σε χώρες με χαμηλότερο κατά κεφαλήν ΑΕΠ, αφού έρευνες δείχνουν ότι αυτές οι χώρες έχουν χαμηλότερο δείκτη ασφάλειας στον κυβερνοχώρο. Για τον λόγο αυτό υπάρχει μεγαλύτερη ανάγκη να βοηθηθούν αυτές οι χώρες να αναπτύξουν καλύτερα τις ικανότητές τους στον τομέα της κυβερνοασφάλειας.

Κεφάλαιο 9

Συμπεράσματα

Η ραγδαία εξέλιξη της τεχνολογίας ενώ έχει λύσει τα χέρια της ανθρωπότητας και προσφέρει ένα πολύ καλύτερο και ανώτερο βιωτικό επίπεδο στην καθημερινότητα των ανθρώπων, δεν παύει να εγκυμονεί νέες προκλήσεις και κινδύνους. Το κυβερνοέγκλημα και κατ' επέκταση η κυβερνοτρομοκρατία αποτελούν ενδεικτικά κάποιους από τους προαναφερθέντες κινδύνους. Η κυβερνοτρομοκρατία δε επειδή δεν τυποποιείται ως έγκλημα ούτε στο Ελληνικό αλλά ούτε και σε διεθνές επίπεδο είναι ένα έγκλημα που δεν τιμωρείται. Για τον λόγο αυτό έχει αποτελέσει σημαντικό θέμα συζήτησης σε διεθνές επίπεδο.

Το πρώτο πράγμα λοιπόν που κρίνεται απαραίτητο είναι να καθοριστεί και να αναγνωριστεί από την διεθνή κοινότητα η έννοια της κυβερνοτρομοκρατίας. Ο ορισμός πρέπει να είναι ακριβής και στενός ώστε να επιτρέπει τη νόμιμη δίωξη εγκληματικών πράξεων. Απαιτείται ένας νομικός κανόνας για να εκτιμηθεί εάν μια συμπεριφορά είναι νόμιμη ή όχι.

Αυτή η μελέτη επικεντρώθηκε στη δυναμική των κυβερνοεπιθέσεων και της τρομοκρατίας στον κυβερνοχώρο και υπογράμμισε την ολοένα αυξανόμενη πιθανότητα του πολέμου στον κυβερνοχώρο τα τελευταία χρόνια. Με την ανθρώπινη φυλή να εξαρτάται όλο και περισσότερο από την τεχνολογία και τους υπολογιστές να κατακλύζουν τη ζωή των ανθρώπων, το πεδίο εκμετάλλευσης του κυβερνοχώρου αυξάνεται ραγδαία για να θέσει σε κίνδυνο την ασφάλεια ενός οργανισμού ή ενός ολόκληρου έθνους.

Η κοινωνία είναι το αντικείμενο αναφοράς και οι άνθρωποι της μεσαίας οικονομίας είναι οι πιο ευάλωτοι. Τα κράτη μπορούν να αρχίσουν να φιλτράρουν λογαριασμούς στα μέσα κοινωνικής δικτύωσης που έχουν οποιαδήποτε σχέση με τρομοκρατικές ομάδες. Ωστόσο, τα μέσα κοινωνικής δικτύωσης είναι ένα τέλειο μέσο για τη διάδοση της βίαιης ριζοσπαστικής ιδεολογίας για τη στρατολόγηση νέων μελών. Οι πληροφορίες στα μέσα κοινωνικής δικτύωσης είναι μαζικές και μπορούν να επηρεάσουν ένα ευρύτερο

κοινό. Οι κυβέρνησεις πρέπει να δαπανήσουν κονδύλια από τον προϋπολογισμό τους στην ασφάλεια του διαδικτύου αλλά και για να φιλτράρουν και να προβλέψουν την απειλή της κυβερνοτρομοκρατίας, που επηρεάζει τις κοινωνίες τους. Επιπλέον, είναι επιτακτική ανάγκη τα κράτη να επενδύσουν στην ανάπτυξη των πληροφοριακών τους συστημάτων και στην εκπαίδευση του ανθρώπινου δυναμικού τους.

Τα κράτη μπορούν να αναπτύξουν ένα εποικοδομητικό και ολιστικό πρόγραμμα δημιουργώντας νομικά πλαίσια και συνδυάζοντας όλους τους τομείς, μεταξύ άλλων άμυνα, πληροφοριακά συστήματα, ακόμη και εκπαίδευση. Το αποτέλεσμα ενός τέτοιου νομικού πλαισίου θα είναι ένα εθνικό στρατηγικό σχέδιο για αντιμετώπιση οποιασδήποτε απειλής από τρομοκράτες. Η εφαρμογή ενός τέτοιου είδους προγράμματος δύναται να ενισχύσει την ευαισθητοποίηση, ειδικά για την αντιμετώπιση οποιωνδήποτε προσπαθειών εξτρεμισμού και είναι επιτακτική ανάγκη να υιοθετηθεί παγκοσμίως.

Είναι αλήθεια ότι δεν υπήρξε ποτέ καμία επίθεση στον κυβερνοχώρο που να έχει οδηγήσει σε σημαντική διακοπή των υπηρεσιών ή ακόμη και σε απώλεια ανθρώπινων ζωών, αλλά αυτό σίγουρα δεν δικαιολογεί εφησυχασμό. Οι κυβερνοεπιθέσεις που έχουν συμβεί πρόσφατα και αναφέρονται σε αυτήν τη μελέτη θα φαινόταν πιθανές μόνο σε μυθοπλασία μόλις λίγες δεκαετίες πριν, αλλά τώρα θεωρούνται ως ήσσονος σημασίας ή μέτριες πράξεις διακοπής ή κατασκοπείας. Ο ρυθμός της τεχνολογικής προόδου καθιστά σαφές ότι οι κυβερνοτρομοκρατικές επιθέσεις θα αυξηθούν τα επόμενα χρόνια, εάν δεν ληφθούν κατάλληλα αντίμετρα. Κάποιοι θα υποστήριζαν ότι ο αδικαιολόγητος φόβος γύρω από υποθετικές κυβερνοτρομοκρατίες έχει οδηγήσει σε μεγαλύτερη αναστάτωση και αύξηση της περιττής ανασφάλειας μεταξύ των μαζών που είναι αντιπαραγωγική για την ανάπτυξη. Αν και αυτό ισχύει σε κάποιο βαθμό, πρέπει επίσης να γίνει κατανοητό ότι καθώς η τεχνολογία βελτιώνει σημαντικά την ποιότητα ζωής και ελέγχει όλο και περισσότερες πτυχές της επιβίωσης του ανθρώπου, η ανταλλαγή πρέπει να είναι εξίσου σημαντική. Εάν η τεχνολογία μπορεί να μας οδηγήσει στο φεγγάρι, μια καταστροφή ή ένας συμβιβασμός θα διασφαλίσει ότι θα μείνουμε εκεί για πάντα και δεν θα επιστρέψουμε ποτέ. Στην ουσία, όταν τα κέρδη είναι τεράστια, οι

απώλειες μπορεί να είναι εξίσου μεγάλες και μια διορατική ματιά θα αναζητούσε μια πιο αναζωογονητική και ισχυρή πολιτική ασφάλειας στον κυβερνοχώρο.

Κατόπιν των παραπάνω διαπιστώνεται η ανάγκη καθιέρωσης ενός κοινού οργανισμού – θεσμού – ιδρύματος το οποίο θα αναλάβει την εποπτεία – διαιτησία και καταστολή κυβερνοεγκλημάτων και κατ' επέκταση της κυβερνοτρομοκρατίας. Το επίπεδο στο οποίο κρίνεται αποτελεσματικό να εξεταστεί η θέσπιση ενός τέτοιου οργανισμού είναι τα Ηνωμένα Έθνη για τους παρακάτω λόγους:

1. Η αντιμετώπιση της κυβερνοτρομοκρατίας σε πιο ευρεία κλίμακα (μεγάλο πλήθος συμμετεχόντων κρατών στον Οργανισμός Ηνωμένων Εθνών)
2. Η παροχή τεχνογνωσίας σε κράτη [που δεν έχουν θεσπίσει μηχανισμούς για την αντιμετώπιση της κυβερνοτρομοκρατίας
3. Παγκόσμια καθιέρωση νομικής υπόστασης και απαιτήσεων αντιμετώπισης κυβερνοτρομοκρατίας γεγονός που θα δημιουργήσει κοινούς μηχανισμούς καταστολής του φαινομένου.
4. Το μέγεθος του οργανισμού θα προσδώσει μεγαλύτερη σοβαρότητα στην αντιμετώπιση της κυβερνοτρομοκρατίας και πιθανόν να παρέξει την απαιτούμενη χρηματοδότηση για την πάταξη της εν λόγω τρομοκρατίας.
5. Ο Οργανισμός των Η.Ε. δύναται να χρησιμοποιήσει ιδρυθέντες – υπάρχοντες μηχανισμούς καταστολής υπολοίπων κοινοπραξιών ή παγκόσμιων συμφώνων συνεργασίας όπως ΝΑΤΟ , ΟΑΣΕ , ΟΟΣΑ κτλ.

Τέλος ένας από τους περιορισμούς που προκύπτουν κατά την λήψη διαφόρων μέτρων ασφάλειας στον κυβερνοχώρο είναι η ισορροπία που απαιτείται μεταξύ των μέτρων ασφαλείας και των πολιτικών ελευθεριών. Είναι βασικό να εξασφαλιστούν τα ατομικά και άρα και τα ψηφιακά δικαιώματα των πολιτών παγκοσμίως όταν χρησιμοποιούν το διαδίκτυο. Είναι απαραίτητο να εξασφαλιστεί η ελευθερία της έκφρασης και να περιοριστεί η λογοκρισία του διαδικτύου σε σημαντικά γεγονότα της καθημερινότητας των πολιτών. Η παράβαση των ατομικών δικαιωμάτων συνιστά απειλή για την ελευθερία των πολιτών, ιδίως στα δημοκρατικά πολιτεύματα του κόσμου. Απολύτως απαραίτητη είναι όμως και η ισορροπία μεταξύ της παροχής συγκεκριμένων προνομίων σε έναν συγκεκριμένο οργανισμό ή κυβέρνηση, και των

γενικότερων απαιτήσεων προς όφελος όλων των νόμιμων χρηστών για να διαμορφωθεί ένα διεθνές περιβάλλον επικοινωνίας και τεχνολογίας που θα είναι μη φιλικός στις φιλοδοξίες τρομοκρατών και εξτρεμιστών και γενικά εγκληματιών στο κυβερνοχώρο.

Βιβλιογραφία

Βικιπαίδεια. (2021, Αυγουστος). *Βικιπαίδεια η ελεύθερη εγκυκλοπαίδεια* . Ανάκτηση από Βικιπαίδεια η ελεύθερη εγκυκλοπαίδεια : https://el.wikipedia.org/wiki/%CE%A4%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%AF%CE%B1

Βίκυ Καρυστινού. (2016, Ιούνιος). *http://www.menoeuropi.gr/.* Ανάκτηση από http://www.menoeuropi.gr/: http://www.menoeuropi.gr/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%84%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%AF%CE%B1-%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%B1%CF%80%CE%B5%CE%B9/

AcronisCyber Protect. (2020). *The NHS cyber attack.* AcronisCyber Protect.

Broumas, A. (2015). *CyberInsuranceGreece.com*. Ανάκτηση από https://www.cyberinsurancegreece.com/kyvernoegklima-asfaleia/: https://www.cyberinsurancegreece.com/kyvernoegklima-asfaleia/

enallaktikos.gr. (2019, Αυγουστος). Ανάκτηση από https://enallaktikos.gr/toyrkia-apagoreytike-i-prosvasi-se-136-i/: https://enallaktikos.gr/toyrkia-apagoreytike-i-prosvasi-se-136-i/

eset.com. (2001). *https://www.eset.com/gr*. Ανάκτηση από https://www.eset.com/gr: https://www.eset.com/gr/types-of-cyber-threats/

IDAHOSA Stephen Osaherumwen. (2017). *International Terrorism: The Influence of Social Media in Perspective.* World Wide Journal of Multidisciplinary Research and Development.

insider. (2021, Μάιος). *insider.gr.* Ανάκτηση από https://www.insider.gr/epiheiriseis/172264/colonial-pipeline-plirose-5-ekat-dolaria-stoys-haker-tis-kybernoepithesis: https://www.insider.gr/epiheiriseis/172264/colonial-pipeline-plirose-5-ekat-dolaria-stoys-haker-tis-kybernoepithesis

Iqbal Ramadhan. (2020, Δεκέμβριος). Cyber-Terrorism in the Context of Proselytizing,Coordination, Security, and Mobility. *Islamic World and Politics*.

License, C. C.-S. (2022, Ιούλιος). *Wikipedia*. Ανάκτηση από https://el.wikipedia.org/wiki/%CE%9B%CE%BF%CE%B3%CE%BF%CE%BA%CF%81%CE%B9%CF%83%CE%AF%CE%B1_%CF%84%CE%BF%CF%85_%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85

Marco Marsili. (2019). The War on Cyberterrorism. *Democracy and Security*.

naftemporiki. (2021, Ιουλιος Σαββατο). *naftemporiki.gr*. Ανάκτηση από naftemporiki.gr: https://www.naftemporiki.gr/finance/story/1745358/ti-krubei-i-kubernoepithesi-se-200-etaireies-ton-ipa

Ramadhan, I. (2020). *Cyber-Terrorism in the Context of Proselytizing,.* Islamic World and Politics,Vol. 4, No. 2,.

Subrahmanian, V. (2015). *The global cyber vulnerability report.* Springer.

wikipedia. (χ.χ.). Ανάκτηση από https://el.wikipedia.org/wiki : https://el.wikipedia.org/wiki

wikipedia. (χ.χ.). *https://el.wikipedia.org*. Ανάκτηση από wikipedia: https://el.wikipedia.org/wiki/%CE%9B%CE%BF%CE%B3%CE%BF%CE%BA%CF%81%CE%B9%CF%83%CE%AF%CE%B1_%CF%84%CE%BF%CF%85_%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85

ΑΔΗΩΤΟΣ. (2019). Κυβερνοτρομοκρατία.

Ανανιάδης, Κ. (χ.χ.). *Techgear*. Ανάκτηση από https://www.techgear.gr/turkey-bans-social-networks-9194 : https://www.techgear.gr/turkey-bans-social-networks-9194

Γιάννης Γορανίτης. (2021, Ιούνιος Πεμπτη). *Το Βήμα*. Ανάκτηση από https://www.tovima.gr: https://www.tovima.gr/2021/06/24/society/kyvernoepitheseis-pos-droun-oi-ekviastes-tou-diadiktyou-ti-symvainei-stin-ellada-ti-systinoun-oi-eidikoi/

Δέσποινα Βλάχου, Μαρία Ζαμπατή και Χριστίνα Κοντραφούρη . (2020). *Η επίδραση των κυβερνοεπιθέσεων στη μετεξέλιξη της κυβερνοασφάλειας:Η περιπτωσιολογική μελέτη της Εσθονίας.* Πειραιάς : Πανεπιστήμιο Πειραιώς, Εργαστήρι Πληροφόρησης και Κυβερνοασφάλειας .

Καζαντζόγλου, Α. (2016). *Συγχρονα τεχνολογικά μέσα και η έννοια της επίθεσης στο διεθνές δίκαιο. Ο Κυβερνοπόλεμος , υπό το πρίσμα του ΝΑΤΟ , της Ε.Ε και των ελληνικών ενόπλων δυνάμεων του 21ου αιώνα.* Θεσσαλονίκη : Πανεπιστήμιο Μακεδονίας.

Κακαβούλης, Κ. (2018, Ιούνιος). *https://www.homodigitalis.gr/posts/1857*. Ανάκτηση από https://www.homodigitalis.gr: https://www.homodigitalis.gr/posts/1857

Μαρία Κουτσανδριά. (2020, Μαιος). *offlinepost.gr*. Ανάκτηση από offlinepost.gr: https://www.offlinepost.gr

Ναυτεμπορική. (2021). *Colonial Pipeline: Πώς έγινε η πρωτοφανής κυβερνοεπίθεση.* Ανάκτηση από naftemporiki.gr: https://www.naftemporiki.gr/story/1724632/colonial-pipelinepos-egine-i-protofanis-kubernoepithesi

Παναγιώτη Κικίλια. (2008, Ιούλιος). Κυβερνοτρομοκρατία και εφαρμογή νέων τεχνολογιών στην τρομοκρατία. *it security PROFESSIONAL*, σ. IT issue 5.

Πάπυρος Larousse Britannica. (2006). *Εγκυκλοπαίδεια .* Αθήνα : Πάπυρος.

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ. (2020). *ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025.* ΑΘΗΝΑ: ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ.