ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΟΛΙΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ
ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ: ΤΥΠΟΛΟΓΙΕΣ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΣΤΗΝ Ε.Ε. ΚΑΙ ΣΤΗΝ ΕΛΛΑΔΑ

ΜΕΤΑΞΑ ΒΑΣΙΛΙΚΗ

Α.Μ. 3652
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΒΥΖΙΡΓΙΑΝΝΑΚΗΣ ΔΗΜΗΤΡΙΟΣ
ΡΕΘΥΜΝΟ 2021

Ευχαριστίες

Η εκπόνηση μιας πτυχιακής εργασίας είναι κατά βάση μια μοναχική διαδικασία, όπως μου είχε αναφέρει, ο καθηγητής μου και επιβλέπων για αυτήν την εργασία, ο κ. Δημήτριος Βυζιργιαννάκης. Ωστόσο, χωρίς την πολύτιμη βοήθειά του και τις συμβουλές του δεν θα μπορούσα να ολοκληρώσω αυτό το έργο και για αυτό θα ήθελα να τον ευχαριστήσω, που παρόλο των συνθηκών (εξ αποστάσεως εκπαίδευση και πανδημία), καταφέραμε να έχουμε μια τόσο καλή επικοινωνία και συνεργασία. Δεν μπορώ να ξεχάσω την οικογένεια μου, που έπαιξε τόσο μεγάλο ρόλο στο να καταφέρω να τελειώσω με επιτυχία τις σπουδές μου στο Πανεπιστήμιο Κρήτης, και φυσικά, τους συμφοιτητές μου και συναδέλφους μου Άννα, Κατερίνα, Μαρία και Πάνο, που ήταν το στήριγμά μου σε όλη την πορεία των φοιτητικών μου χρόνων...

Περιεχόμενα

Εισαγωγή

Το «ηλεκτρονικό έγκλημα» ή αλλιώς «κυβερνοέγκλημα» αποτελεί ένα αρκετά ενδιαφέρον φαινόμενο προς μελέτη, λόγω το ότι ζούμε στην εποχή της Πληροφορίας. Η ψηφιακή εξέλιξη και η ανάπτυξη της τεχνολογίας, πέρα από τα θετικά αποτελέσματα που δημιουργεί (όπως η άμεση πρόσβαση στην γνώση,), γεννά παράλληλα και αρνητικά, δηλαδή την εμφάνιση νέων μορφών εγκληματικότητας και κινδύνων για τον χρήστη του διαδικτύου. Αρχικά, είναι σημαντικό να οροθετηθούν κάποιες βασικές έννοιες όπως το έγκλημα, το ηλεκτρονικό έγκλημα, το Κυβερνοέγκλημα, το διαδίκτυο αλλά και να επισημανθεί η ιστορική εξέλιξη του Cybercrime. Στην συνέχεια, θα προχωρήσουμε στην αναφορά της διάκρισης του ηλεκτρονικού εγκλήματος, των χαρακτηριστικών που εμφανίζει κάθε φαινόμενο και των μορφών κυβερνοεγκλήματος, δηλαδή:

- παιδική πορνογραφία
- απάτες στο διαδίκτυο (π.χ. κλοπή προσωπικών δεδομένων)
- διαδικτυακή πειρατεία
- hacking
- εγκλήματα στα chat rooms
- σωματεμπορία
- παραβίαση πνευματικών δικαιωμάτων
- διαδικτυακή τρομοκρατία (και cyberbullying)
- κακόβουλο λογισμικό
- προπαγάνδα και επηρεασμός κοινωνικού συνόλου (διαμόρφωση κοινής γνώμης)

Όλα τα παραπάνω, μπορούν να επηρεάσουν σε προσωπικό (άτομο) και σε συλλογικό επίπεδο (κοινωνία), δημιουργώντας πολιτικές, οικονομικές και κοινωνικές μεταβολές. Ποιοι δρώντες μπορούν να λειτουργήσουν ως αρωγοί για την μείωση, αν όχι εξάλειψη, του ηλεκτρονικού εγκλήματος; Με ποιους τρόπους προσπαθούν να εξασφαλίσουν ασφάλεια στους χρήστες του διαδικτύου και των social media; Το

νομικό πλαίσιο και ο ποινικός κώδικας είναι άρρηκτα συνδεδεμένα με την προστασία του πολίτη από τον διαδικτυακό κίνδυνο και την τιμωρία των δραστών. Διάφορα study cases θα προσμετρηθούν, ειδικότερα γεγονότα για κάθε μορφή κυβερνοεγκλήματος και κάποια σχετικά με τα social media (facebook, instagram κλπ.), και το πως αυτά είναι ικανά να ενισχύσουν τις κατάλληλες συνθήκες ώστε να οδηγηθεί ο δράστης στην παράνομη πράξη.

Στο 1ο Κεφάλαιο με τίτλο «Σχετικά με το Κυβερνοέγκλημα» θα εξετάσουμε τον όρο του «Κυβερνοεγκλήματος», αλλά και συναφείς έννοιες του εγκλήματος και του διαδικτύου που θα βοηθήσουν στην εμβάθυνση του θέματος. Στην συνέχεια θα αναφερθούμε στα πιο σημαντικά ιστορικά γεγονότα που εξελίχθηκαν στον Κυβερνοχώρο και στο Διαδίκτυο και θα καταλήξουμε στο τι ζητήματα και προκλήσεις δημιουργεί αυτό το τόσο σύγχρονο και μεταβαλλόμενο φαινόμενο. Στο 2ο Κεφάλαιο: «Τυπολογική Ταξινόμηση Κυβερνοεγκλήματος» θα διακρίνουμε τους τύπους Κυβερνοεγκλήματος αλλά και τα χαρακτηριστικά που διαθέτουν ξεχωριστά. Πιο συγκεκριμένα, για κάθε μορφή που μπορεί να λάβει το έγκλημα στον Κυβερνοχώρο θα παρατίθεται και μία αντίστοιχη μελέτη περίπτωσης.

Στο 3ο Κεφάλαιο: «Αντίκτυπος Κυβερνοεγκλήματος», παρουσιάζονται οι πολιτικές, οικονομικές και κοινωνικές επιπτώσεις του Κυβερνοεγκλήματος σε ευρωπαϊκό και ελληνικό επίπεδο, δηλαδή πως επηρεάζονται τα άτομα αλλά και η κοινωνία. Στο Κεφάλαιο 4 με τίτλο «Πολιτικές Αντιμετώπισης Κυβερνοεγκλήματος» καλύπτεται το περιεχόμενο της ασφάλειας, της πρόληψης και τα προγράμματα που δημιουργεί η Ευρωπαϊκή Ένωση - και η Ελλάδα σε συνεργασία μαζί της- για την επίλυση του προβλήματος, καθώς η ζημιά που προκαλεί η χρήση υπολογιστών από τους πολίτες μπορεί να γίνει ανεπανόρθωτη. Οι πολιτικές ασφάλειας έχουν ως στόχο να αποτρέψουν μια επίθεση πριν την εμφάνισή της, ή να μειώσουν τις αρνητικές επιπτώσεις μετά την εκδήλωσή της. Εν τέλει, θα καταλήξουμε σε συμπερασματικές παρατηρήσεις και προτάσεις ώστε να ολοκληρωθεί το ερευνητικό πεδίο.

Η ταχεία τεχνολογική ανάπτυξη συνεχίζεται και θα συνεχίσει να φέρνει νέες προκλήσεις. Η αυξανόμενη δημοτικότητα του Διαδικτύου επιτρέπει σε πολλούς

χρήστες να συνδέσουν τους υπολογιστές τους σε αυτό, καθιστώντας τους πιο ευάλωτους σε εξωτερικές επιθέσεις, γεγονός που επιβαρύνεται από τη διάδοση «έξυπνων οικιακών συσκευών με αυξημένες δυνατότητες συνδεσιμότητας. Οι αντιλήψεις μας για το έγκλημα στον κυβερνοχώρο ενημερώνονται και επηρεάζονται ταυτόχρονα από πολιτικές συζητήσεις και συζητήσεις στα μέσα ενημέρωσης για το πρόβλημα (Yar & Steinmetz, 2019). Το ηλεκτρονικό έγκλημα είναι ένας συγκριτικά νέος τομέας έρευνας και παραθέτοντας τις συνιστώσες, τους θεσμούς, τις επιπτώσεις του εγκλήματος στον κυβερνοχώρο και διάφορους παράγοντες που εμπλέκονται στο ζήτημα αυτό, η εργασία αυτή έχει ως σκοπό την κατανόηση και ανάλυση του ραγδαία μεταβαλλόμενου φαινομένου, δηλαδή του εγκλήματος στον κυβερνοχώρο.

Κεφάλαιο 1: Σχετικά με το Κυβερνοέγκλημα

1.1 Τι είναι το Κυβερνοέγκλημα;

Αρχικά, ο όρος Κυβερνοέγκλημα (Cybercrime) προέρχεται από τις λέξεις «κυβερνήτης» και «έγκλημα». Η λέξη «κυβερνήτης» αναφέρθηκε πρώτη φορά από τον Nobert Wiener (μαθηματικός και φιλόσοφος), ο οποίος έβαλε τις βάσεις για την κατανόηση του φαινομένου του κυβερνοεγκλήματος, επισημαίνοντας τις αλληλεπιδράσεις των υπολογιστικών μηχανών με τον άνθρωπο. Το φαινόμενο του κυβερνοεγκλήματος σίγουρα αποτελεί ένα πολυπαραγοντικό και πολυδιάστατο θέμα προς ανάλυση, λόγω της εκτεταμένης πλέον διάδοσης των ψηφιακών τεχνολογιών σε κάθε πτυχή της καθημερινότητας. Ειδικότερα, συνδέεται άμεσα με το διαδίκτυο και τον κυβερνοχώρο, έννοιες οι οποίες θα αναλυθούν και θα εξηγηθούν στην επόμενη ενότητα. Μια από τις πολλές προσπάθειες καθορισμού της έννοιας είναι εκείνη του McQuade III (2009), αναφέροντας πως, το έγκλημα στον κυβερνοχώρο δεν είναι ένα νέο, αλλά μάλλον ένα εξελισσόμενο φαινόμενο όσον αφορά την υιοθέτηση της τεχνολογίας των πληροφοριών (Information Technology) για καταχρηστικούς και εγκληματικούς σκοπούς.

Η διαχείριση του φαινομένου αποτελεί μια νέα πρόκληση για την κοινωνία σε παγκόσμιο επίπεδο. Η ευρεία χρήση ηλεκτρονικών συσκευών στην καθημερινότητα των ανθρώπων, και γενικότερα των Ψηφιακών Προσωπικών Βοηθών (Digital Personal Assistants), ταυτόχρονα αναδεικνύει το όλο και περισσότερο αυξανόμενο αριθμό διασυνδεδεμένων υπολογιστών στο διαδίκτυο. Για να κατανοήσουμε την κατάσταση αυτή, οφείλουμε να εμβαθύνουμε και στον όρο του «εγκλήματος». Όπως αναφέρεται από τους Yar & Steinmetz (2019), ο ορισμός του Thomas and Loader περιέχει μια σημαντική διάκριση που δικαιολογεί περαιτέρω προβληματισμό, δηλαδή ότι μεταξύ του *εγκλήματος* (πράξεις που απαγορεύονται ρητά από το νόμο, και ως εκ τούτου παράνομες) και της *απόκλισης* (πράξεις που παραβιάζουν άτυπους κοινωνικούς κανόνες και νόμους και, ως εκ τούτου, θεωρούνται ανεπιθύμητες ή απαράδεκτες) υπάρχει αξιοσημείωτη διαφορά σε σχέση με το επίπεδο παραβατικότητας και της εγκληματικής πράξης. Ωστόσο, το έγκλημα και η

αποκλίνουσα συμπεριφορά δεν μπορούν πάντα να διαχωρίζονται αυστηρά στην εγκληματολογική έρευνα (Yar & Steinmetz, 2019). Αυτό αιτιολογείται από το γεγονός ότι υπάρχουν γενικές αντιλήψεις του πληθυσμού σχετικά με το τι θεωρούν αποκλίνουσα συμπεριφορά. Μπορεί, δηλαδή, να παρερμηνευθεί μια πράξη, η οποία στην συνέχεια μέσω της δημιουργίας νόμων να καταδικαστεί ως εγκληματική. Εφόσον, το εγκληματικό φαινόμενο είναι διαπραγματεύσιμο καταλήγουμε και στο συμπέρασμα, πως κινείται στην ίδια κατεύθυνση και εξέλιξη με εκείνη του διαδικτύου και της κοινωνίας.

Εξ ορισμού, το έγκλημα στον κυβερνοχώρο είναι ένα έγκλημα που σχετίζεται με την τεχνολογία, τους υπολογιστές και το Διαδίκτυο (Schell & Martin, 2004). Από την δεκαετία του 1980 άρχισε να αλλάζει όλο και περισσότερο η φύση του εγκλήματος, αλλά και να λαμβάνει νέα διάσταση, πιο τεχνολογική. Μέσω των εφευρέσεων και των καινοτομιών, όπως η δημιουργία του Παγκόσμιου Διαδικτύου (1993) και η ανάπτυξη διαφόρων εφαρμογών λογισμικού, κατέστησαν αναπόφευκτη την εμφάνιση του εγκλήματος στον κυβερνοχώρο (McQuade, 2009). Ιδιαίτερα στην Δύση παρατηρείται η επέκταση της χρήσης του Διαδικτύου, το οποίο επιτρέπει την ανταλλαγή δεδομένων και πληροφοριών. Η αυξανόμενη εξάρτησή μας από τους υπολογιστές και τα ψηφιακά δίκτυα καθιστά την ίδια την τεχνολογία δελεαστικό στόχο, είτε για την απόκτηση πληροφοριών, είτε ως μέσο πρόκλησης αναστάτωσης και ζημίας (Clough, 2010). Ουσιαστικά, η διαφορά ανάμεσα στο κυβερνοέγκλημα και στο έγκλημα είναι ο τόπος που διαπράττεται, σύμφωνα με τον Brenner (2010) και ενώ, οι περισσότεροι ανησυχούν για τους εγκληματίες στην πραγματική ζωή, που χρησιμοποιούν φυσικά μέσα (πχ όπλα), εμφανίζονται τώρα οι εγκληματίες στον κυβερνοχώρο με την χρήση τεχνολογιών των υπολογιστών.

Καθώς έχουμε υπόψη μας, πως ο όρος «κυβερνοέγκλημα» έχει μια ευρεία διάσταση, μπορούμε να κατανοήσουμε και τα περιθώρια που αφήνονται ως προς την εξήγησή του. Πρώτη φορά που αναφέρθηκε αυτό το φαινόμενο ήταν με τις εξής ορολογίες: «έγκλημα στον υπολογιστή», «έγκλημα που σχετίζεται με υπολογιστές» ή «έγκλημα μέσω υπολογιστή». Το «κυβερνοέγκλημα» και το «εικονικό έγκλημα», από την άλλη, εμφανίστηκαν μαζί με το διαδίκτυο. Μέσα από την έρευνα γενικότερα,

διαπιστώνεται πως υπάρχει μια πληθώρα ορολογιών σχετικά με το κυβερνοέγκλημα, που είτε μερικές στοχεύουν στην σχέση του εγκλήματος με το διαδίκτυο, είτε στην σχέση του με τους υπολογιστές. Πολλοί διεθνείς οργανισμοί, όπως τα Ηνωμένα Έθνη, η Interpol, ο Ο.Ο.Σ.Α. (Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης) και το Συμβούλιο της Ευρώπης έχουν αναγνωρίσει τις προκλήσεις που δημιουργεί το φαινόμενο και προσπαθούν να ευαισθητοποιήσουν τον κόσμο για την σοβαρότητα επί του θέματος. Η πληθώρα στις ερμηνευτικές προσεγγίσεις βοηθά και στην περαιτέρω κατανόηση της κατάστασης. Το υποκεφάλαιο αυτό ωστόσο, έχει στόχο να παρουσιάσει βασικές πληροφορίες σχετικά με το τι είναι το κυβερνοέγκλημα. Περισσότερες λεπτομέρειες παρουσιάζονται σταδιακά με κάθε κεφάλαιο.

Τέλος, μέσα από την φύση του κυβερνοεγκλήματος μπορούμε να διακρίνουμε πως διέπεται από κάποια συγκεκριμένα χαρακτηριστικά και σύμφωνα με την Παπανικολάου (2009) είναι πέντε:

(1) Ταχύτητα και Ανωνυμία: οι δράστες λειτουργούν ως ψηφιακοί νομάδες (nomads), μπορούν ανώνυμα και στιγμιαία να εγκληματίσουν και δεν χρειάζεται η φυσική μετακίνησή τους.

(2) Απειλή για όλους: όλοι είναι υποψήφια θύματα στο διαδίκτυο, είτε πρόκειται για μεμονωμένα άτομα, είτε για κρατικές υπηρεσίες και ιδιωτικές επιχειρήσεις.

(3) Δυσκολία εντοπισμού: λόγω του διασυνοριακού χαρακτήρα είναι δύσκολο, τεχνικά και νομικά, να βρεθεί ο δράστης και τα αποδεικτικά στοιχεία.

(4) Εξειδικευμένο προσωπικό για την διερεύνηση: για την σωστή έρευνα επιβάλλεται και ανάλογο εκπαιδευμένο δυναμικό, ακόμη και η συνεργασία ανάμεσα στις αρμόδιες αρχές και τα κράτη.

(5) Μη επαρκείς πληροφορίες: τα στοιχεία που έχουν συλλεχθεί και συλλέγονται δεν αποτυπώνουν την πραγματικότητα. Δεν καταγγέλλονται όλα τα περιστατικά κυβερνοεγκλήματος, που συμβάλλει και αυτό στην δυσκολία εξιχνίασης των εγκλημάτων.

Αν έχουμε κατά νου όλα τα παραπάνω, καταλήγουμε στο συμπέρασμα πως το φαινόμενο του εγκλήματος στον κυβερνοχώρο εγείρει ζητήματα ασφάλειας και ιδιωτικότητας. Μέσω των πληροφοριών που δημοσιεύει κάθε άτομο στον κυβερνοχώρο ή και στο διαδίκτυο, αυτόματα καθίσταται περισσότερο ευάλωτο στους κινδύνους. Για αυτό, ο κυβερνοχώρος ενδυναμώνει τους εγκληματίες με νέους τρόπους (Brenner, 2010), και όσο αυξάνεται η χρήση των νέων τεχνολογιών και του διαδικτύου, είναι αδιαμφισβήτητο πώς οι κίνδυνοι δεν θα εξαφανιστούν ούτε θα μειωθούν. Ο εφησυχασμός είναι ικανός να προκαλέσει σημαντικές και ενίοτε ανεπανόρθωτες ζημιές σε προσωπικό και συλλογικό επίπεδο.

1.2 Διασαφήνιση βασικών εννοιών

Παρακάτω, γίνεται μια παράθεση ορισμού σημαντικών εννοιών, που θα βοηθήσουν τον/την αναγνώστη/-τρια να κατανοήσουν καλύτερα το ερευνητικό περιεχόμενο γύρω από το φαινόμενο του Κυβερνοεγκλήματος.

Αντεγκληματική Πολιτική: σε μια εισήγηση στο Συμβούλιο της Ευρώπης ορίστηκε ως «το σύνολο των μέτρων που τείνουν στην προστασία της κοινωνίας από την εγκληματικότητα, στη φροντίδα για την μελλοντική εξέλιξη του εγκληματία και τη διασφάλιση των δικαιωμάτων του θύματος». Γενικότερα, πρόκειται για μια πολυπαραγοντική έννοια που μεταβάλλεται παράλληλα με το αντίστοιχο κοινωνικό, οικονομικό και πολιτικό πλαίσιο.

APRANET (Advanced Research Project Agency Network): στα τέλη της δεκαετίας του 1960 υπό τον J.C.R. Licklider, ερευνητές και επιστήμονες στις Ηνωμένες Πολιτείες με εντολή από το Υπουργείο Άμυνας δημιούργησαν έναν τρόπο για τους ανθρώπους που χωρίζονται σε μεγάλες αποστάσεις να επικοινωνούν με τη χρήση υπολογιστών, δηλαδή το *δίκτυο υπολογιστών*. Ενεργοποιήθηκε αρχικά το 1969 συνδέοντας τους κεντρικούς υπολογιστές του Ερευνητικού Ινστιτούτου του Στάνφορντ, του Πανεπιστημίου της Καλιφόρνιας-Σάντα Μπάρμπαρα, του Πανεπιστημίου της Καλιφόρνιας-Λος Άντζελες (UCLA) και του Πανεπιστημίου της Γιούτα. Μέσα σε δύο χρόνια, άλλα δεκαπέντε πανεπιστήμια και ερευνητικά ιδρύματα σε όλες τις Ηνωμένες Πολιτείες είχαν επίσης συνδεθεί με τους υπολογιστές του άλλου

χρησιμοποιώντας ARPANET. Το ARPANET σηματοδότησε μια μετάβαση στον υπολογισμό από αυτόνομα μηχανήματα ικανά για πολύπλοκους μαθηματικούς υπολογισμούς σε συσκευές που επέτρεψαν επίσης την επικοινωνία μεταξύ μεμονωμένων χρηστών υπολογιστών και των οργανισμών στους οποίο συνεργάστηκαν. Το εξής δίκτυο διαλύθηκε το 1990, αλλά το τεχνολογικό του σύστημα εντάχθηκε σε νέα δίκτυα, τα οποία κατέστησαν δυνατές τις επικοινωνίες στο Διαδίκτυο για εμπορικούς σκοπούς (McQuade, III, 2009: 7-8).

Bot: είναι ένα διαδικτυακό πρόγραμμα (Internet bot) που εκτελεί αυτοματοποιημένες εργασίες μέσω του ίντερνετ. Ονομάζεται επίσης και *web bot, web robot, WWW robot* ή απλά *bot*. Στις περισσότερες περιπτώσεις τα bots εκτελούν σχετικά απλές λειτουργίες που θα πρέπει να επαναληφθούν εκατοντάδες ή χιλιάδες φορές. Μία κλασσική εφαρμογή των bots είναι οι αράχνες του διαδικτύου (web spiders), οι οποίες περιφέρονται από ιστοσελίδα σε ιστοσελίδα και χρησιμοποιούνται για την ανάλυσή της σε ρυθμό πολλαπλάσιο απ' ότι θα μπορούσε ένας άνθρωπος. Η Google και όλες οι άλλες μηχανές αναζήτησης χρησιμοποιούν τέτοιες αράχνες για την ανάλυση και ταξινόμηση των ιστοσελίδων με λέξεις-κλειδιά, ούτως ώστε στην συνέχεια να μπορούν να παρουσιάσουν στον χρήστη τα αποτελέσματα της αναζήτησης σε πολύ μικρό χρονικό διάστημα. Ωστόσο, αρκετές φορές χρησιμοποιούνται και για κακόβουλο σκοπό από hackers (paramarketing.gr, 2021). Γενικότερα, ένα bot είναι ένα πρόγραμμα που μολύνει ένα στοχευμένο υπολογιστή και του επιτρέπει να ελέγχεται εξ αποστάσεως. Ο εισβολέας εκμεταλλεύεται αδυναμίες ασφαλείας, γενικά σε έναν υπολογιστή συνδεδεμένο στο Internet, για να τοποθετήσει μικρά προγράμματα που ονομάζονται δαίμονες και εκτελούνται στο παρασκήνιο του κεντρικού υπολογιστή, χωρίς να το γνωρίζει ο χρήστης. Αυτοί οι υπολογιστές συχνά αναφέρονται ως «ζόμπι» ή «bots» και ελέγχονται εξ αποστάσεως (Clough, 2010: 35). Επίσης, έχουν γίνει ένα από τα κύρια εργαλεία της εγκληματικής δραστηριότητας που χρησιμοποιείται στο Διαδίκτυο, και συχνά βασικό κίνητρο χρήσης τους είναι η επιθυμία των εγκληματιών του κυβερνοχώρου να βγάλουν λεφτά (McQuade, III, 2009: 12). Τα chatbots έχουν προγραμματιστεί να αλληλεπιδρούν με τους χρήστες διαδικτύου σε πραγματικό χρόνο για την παροχή πληροφοριών. Από την

άλλη, τα gamebots ενεργούν ως παίκτες σε multiplayer online παιχνίδια για να γίνουν πιο διασκεδαστικά. Αλλά υπάρχουν επίσης, και κακά bots, και ο αριθμός τους αυξάνεται καθημερινά. Το 2019, τα κακά bots αντιπροσώπευαν το 24,1% της όλης κίνησης στο διαδίκτυο, σύμφωνα με την Impervar's Bad Bot Report. Τα κακά bots διαδίδουν μηνύματα spam και κακόβουλο λογισμικό, κλέβουν διαπιστευτήρια σύνδεσης και ευαίσθητα δεδομένα, διεξάγουν επιθέσεις άρνησης υπηρεσίας και διαδίδουν παραπληροφόρηση στα μέσα κοινωνικής δικτύωσης, μεταξύ άλλων. Επιπλέον, το γεγονός ότι διεισδύουν στα κοινωνικά δίκτυα, έχει διεγείρει πολλές ανησυχίες τα τελευταία χρόνια, καθώς συμμετείχαν σε κοινωνικές και πολιτικές συζητήσεις. Συνήθως στο χώρο των μέσων ενημέρωσης και των social media χρησιμοποιούνται, αυτά τα bots, για τη δημιουργία πλαστών προφίλ και για να προσθέσουν (ψεύτικα) likes και οπαδούς. Ωστόσο, γίνονται πραγματικά επικίνδυνα όταν μιμούνται τη συμπεριφορά των πραγματικών χρηστών και συμμετέχουν ενεργά στο δημόσιο λόγο. Κύριο παράδειγμα του κινδύνου, που θέτουν αυτά τα bots, αποτελούν οι προεδρικές εκλογές του 2016 στις ΗΠΑ. Με το σκάνδαλο της Cambridge Analytica, οι περισσότεροι χρήστες των μέσων κοινωνικής δικτύωσης συνειδητοποίησαν πως οι πολιτικά κομματικές ομάδες μπορούν να χρησιμοποιήσουν τα μέσα κοινωνικής δικτύωσης για να διαδώσουν παραπληροφόρηση και fake news (ψεύτικα νέα). Τα bots διαδραματίζουν σημαντικό ρόλο στην εξάπλωση της παραπληροφόρησης. Το Twitter προσδιόρισε 2.752 bot λογαριασμούς που συνδέονται με τη Ρωσική Υπηρεσία Έρευνας στο Διαδίκτυο, ένας από τους κύριους παράγοντες στην εκστρατεία παραπληροφόρησης του 2016, καθώς και 36.000 ρωσικά bots, σύμφωνα με μια έκθεση του Talos Intelligence (Plutis, 2020).

Διαδίκτυο: ως αντικείμενο έρευνας έχει προβληματίσει αρκετά την παγκόσμια ερευνητική και επιστημονική κοινότητα, όχι μόνο για το ότι όλο και περισσότερο επεκτείνεται η χρήση του, αλλά και λόγω της συνεχούς ανάπτυξης και εξέλιξής του ως προς την λειτουργική του ικανότητα και δυνατότητα. Γι' αυτό και υπάρχουν άλλωστε, πολλές προσπάθειες ορισμού του διαδικτύου. Σύμφωνα με τον Chadwick (2006:5-12), το Διαδίκτυο είναι ένα δίκτυο δικτύων το οποίο ενσωματώνει τεχνολογίες επικοινωνιών καθορισμένες από ανοικτά αλλά σαφώς ορισμένα πρότυπα

και πρωτόκολλα που επιτρέπουν την επικοινωνία ενός προς πολλούς, πολλών προς πολλούς και πολλών προς έναν, σε τοπικό, εθνικό και παγκόσμιο επίπεδο με σχετικά χαμηλό επίπεδο φραγμών εισόδου. Ένας ακόμη ορισμός, αναφέρεται στο διαδίκτυο ως Διαδίκτυο των Πραγμάτων (Internet of Things). Ο όρος "Διαδίκτυο των Πραγμάτων", η αλλιώς IoT, χρησιμοποιείται για τη σύνδεση των αντικειμένων που χρησιμοποιούν οι άνθρωποι στην καθημερινότητα τους με το Διαδίκτυο και τον υπολογιστή. Τέτοιες συνδέσεις αποσκοπούν τόσο στο να αλληλεπιδρούν μεταξύ τους, όσο και να ελέγχονται από τους ανθρώπους οι συσκευές που βρίσκονται σε απομακρυσμένες περιοχές, αλλά και να παρέχουν οι επιχειρήσεις υπηρεσίες στους πελάτες τους (Holler, 2014). Γενικότερα, συνδέει εκατοντάδες εκατομμύρια συσκευές. Η διαφορά μεταξύ των 2 αυτών ορισμών είναι ότι του Chadwick τονίζει περισσότερο την χαοτικότητα των λειτουργιών το διαδικτύου και το γεγονός ότι αποτελεί μια πηγή παραγωγής με πολλούς αποδέκτες μέσω πολλών δικτύων, ενώ στου Holler απουσιάζει ο ανθρώπινος ρόλος, πιο συγκεκριμένα, οι συσκευές πραγματοποιούν το μεγαλύτερο μέρος της εργασίας χωρίς την ανθρώπινη παρέμβαση, παρόλο που οι άνθρωποι μπορούν να αλληλεπιδρούν με τις συσκευές. Το διαδίκτυο χρησιμοποιείται ως μέσο για την εξυπηρέτηση του κόσμου και έχει δημιουργηθεί με σκοπό την συγκέντρωση και διαχείριση τεράστιου όγκου δεδομένων/πληροφοριών. Συγκροτείται ως συλλογικότητα άλλων οντοτήτων και ταυτόχρονα περιέχει όλες τις μορφές και τις κατευθύνσεις ατομικής και μαζικής επικοινωνίας.

Κυβερνοχώρος: οι Yar & Steinmetz (2019) ορίζουν τον Κυβερνοχώρο ως χώρο αλληλεπίδρασης ή το περιβάλλον που δημιουργείται συνδέοντας υπολογιστές σε ένα δίκτυο επικοινωνίας. Τα εγκλήματα σε αυτόν τον χώρο συγκεντρώνουν τους παραβάτες, τα θύματα και τους στόχους, τα οποία πολλές φορές βρίσκονται σε διαφορετικές χώρες και ηπείρους, και έτσι το αδίκημα εκτείνεται σε πολλά εθνικά εδάφη και ξεπερνά τα σύνορα. Επιπλέον, η λέξη αυτή διαδόθηκε από τον συγγραφέα Γουίλιαμ Γκίμπσον το 1984. Σύμφωνα με εκείνον, αποτελούσε μια πλήρως καθηλωτική εικονική πραγματικότητα μέσω της οποίας οι χρήστες των δικτύων υπολογιστών από όλο τον κόσμο θα μπορούσαν να επικοινωνήσουν και να αλληλεπιδράσουν μεταξύ τους. Επιπροσθέτως, είναι μια άμορφη σφαίρα μέσα και

μέσα από την οποία οι άνθρωποι αλληλεπιδρούν χρησιμοποιώντας υπολογιστές και άλλες συσκευές πληροφορικής που είναι συνδεδεμένες με το Διαδίκτυο. Από τον Ιανουάριο του 2021, υπήρχαν 4,783,503,852 (4.7+ δισεκατομμύρια) άνθρωποι που έχουν πρόσβαση στο Διαδίκτυο (Άλγκρεν, 2021), και ο κυβερνοχώρος συνεχίζει να επεκτείνεται από την άποψη των χρηστών, του περιεχομένου, των δυνατοτήτων και των τεχνολογικών περιπλοκών του (McQuade, 2009: 52). Το μέγεθος του κυβερνοχώρου είναι εξαιρετικά τεράστιο, αυξάνεται εκθετικά και ταυτόχρονα διαθέτει όλα τα χαρακτηριστικά μιας επιρρεπούς σε έγκλημα "γειτονιά" (Kshetri, 2010: 227-247). Ο κυβερνοχώρος γίνεται το εργαλείο που χρησιμοποιούν οι εγκληματίες για να διαπράξουν παλιά εγκλήματα με νέους τρόπους (Brenner, 2010:10). Δεδομένου ότι η φύση του κυβερνοχώρου εξακολουθεί να είναι μια πολύ ευέλικτη και τρέχουσα ανησυχία, ο όρος στερείται μια ορισμένη ιδιαιτερότητα στη λαϊκή γλώσσα και αυτό αποδεικνύεται από το γεγονός ότι στην ακαδημαϊκή κοινότητα είναι ακόμη υπό συζήτηση η διασαφήνιση του ορισμού. Ωστόσο, από προσπάθειες ορισμού της έννοιας παρατηρείται ότι εμφανίζονται δύο σημαντικές πτυχές του κυβερνοχώρου, οι οποίες είναι οι χωρικές και οι κοινωνικές (Slaughter, 2021). Πιο συγκεκριμένα, δεν πρόκειται για έναν πραγματικό "χώρο", αλλά για έναν εικονικό και ότι "ο κυβερνοχώρος επηρεάζεται από τις αξίες, τους πολιτισμούς, τα συστήματα ισχύος και τις θεσμικές τάξεις μέσα στις οποίες ενσωματώνεται" (Sassen, 2002 οπ. αναφ. Slaughter). Πολλά υποδίκτυα υπολογιστών, δηλαδή, που ανταλλάσσουν δεδομένα με κύριο στόχο την διαδικτυακή επικοινωνία και αλληλεπίδραση. Ο κυβερνοχώρος ως "μαζική συναινετική ψευδαίσθηση", όπως αναφέρει ο Γκίμπσον, ουσιαστικά απεικονίζει την ανθρώπινη κοινωνία, όχι μόνο μέσα από τις δραστηριότητες και ενέργειες που υλοποιεί κάθε χρήστης μέσα στον χώρο αυτό, αλλά και μέσα από τον λόγο που επέλεξε ο καθένας να υλοποιήσει μια συγκεκριμένη ενέργεια ή δραστηριότητα.

Οργανωμένο έγκλημα: σύμφωνα με τους Μπόση & Βασιλειάδη (2016) θεωρείται μία παράνομη δραστηριότητα που πραγματοποιείται από ομάδες ατόμων οι οποίες είναι οργανωμένες σε συγκεκριμένο ιεραρχικό πλαίσιο με διακριτούς ρόλους και κατανομή αρμοδιοτήτων μεταξύ των μελών τους, δραστηριοποιούνται για μη

προκαθορισμένο χρονικό διάστημα, χρησιμοποιούν βία ή την απειλή χρήσης βίας ως κύριο μέσο για την επίτευξη των επιμέρους στόχων τους, έχουν ως βασικό σκοπό της δράσης τους την επίτευξη σημαντικού υλικού οφέλους για τα μέλη τους και διαπράττουν παράνομες πράξεις μεγάλης βαρύτητας προκειμένου να αποκομίσουν αυτό το υλικό όφελος.

1.3 Χρονοδιάγραμμα εγκλήματος στον Κυβερνοχώρο

1940-50: το 1943, το υπολογιστικό σύστημα ENIAC δημιουργήθηκε από του John Mauchly και J. Presper Eckert. Αποτελούσε έναν πολύ εξελιγμένο υπολογιστή σε σχέση με την δημιουργία των πρώτων δύο δεκαετίες νωρίτερα όπως π.χ. The Complex Number Calculator. Σε αυτές τις πρώιμες υπολογιστικές μηχανές δεν είχαν εντοπιστεί συμβάντα που θα μπορούσαν να χαρακτηριστούν με τη σύγχρονη ορολογία ως «κυβερνοεπιθέσεις». Μόνο ο John von Neumann είκασε ότι τα προγράμματα υπολογιστών θα μπορούσαν να αναπαραχθούν (ένα πρόγραμμα να δημιουργεί αντίγραφα του εαυτού του με ή χωρίς παραλλαγές) και μόλις το 1949 ανέπτυξε μια θεωρία βασισμένη σε ιούς υπολογιστών (Chadd, 2020). Επίσης, ο Alan Turing, ένας από τους πρωτοπόρους θεωρητικούς της επιστήμης των υπολογιστών και ο Gordon Welchman εξέλιξαν μια μηχανή αποκρυπτογράφησης κώδικα που ονομάστηκε «The Bombe» η οποία είχε αναπτυχθεί αρχικά από Πολωνούς μαθηματικούς για την αποκρυπτογράφηση κρυπτογραφημένων μηνυμάτων Γερμανικής συσκευής κρυπτογράφησης Enigma κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου. Υπό την έννοια αυτή είναι η πρώτη καταγεγραμμένη προσπάθεια αξιοποίησης υπολογιστικών μηχανών για μη επιτρεπτή πρόσβαση σε πληροφορίες.

1950-60: τέλη της δεκαετίας του ‘50, εμφανίστηκε το «phreaking του τηλεφώνου». Τα άτομα, που έκαναν «phreak», εκτός από το γεγονός ότι είχαν ιδιαίτερο ενδιαφέρον για το πως λειτουργούν τα τηλεφωνικά δίκτυα, χρησιμοποίησαν αυτή την μέθοδο για να παραβιάσουν τα πρωτόκολλα που επιτρέπουν στους μηχανικούς τηλεπικοινωνιών να εργάζονται στο δίκτυο εξ αποστάσεως ώστε να πραγματοποιούν δωρεάν κλήσεις και να αποφεύγουν τα τέλη κλήσεων μεγάλων αποστάσεων. Όσον αφορά τις τηλεφωνικές εταιρείες, δεν υπήρχε τρόπος να σταματήσουν το φαινόμενο του

«phreaking», αν και η πρακτική τελικά εξαφανίστηκε στη δεκαετία του '80 (Chadd, 2020). Από του πιο γνωστούς phreaks αποτελούσαν ακόμη και οι ιδρυτές της Apple, ο Steve Wozniak και ο Steve Jobs.

1960-70: οι περισσότεροι υπολογιστές αποτελούσαν τεράστιες υπολογιστικές μηχανές, με καλύτερη ταχύτητα, κλειδωμένοι σε ασφαλή δωμάτια ελεγχόμενης θερμοκρασίας. Αυτά τα μηχανήματα ήταν πολύ δαπανηρά, επομένως η πρόσβαση - ακόμη και σε προγραμματιστές - παρέμεινε περιορισμένη (Chadd, 2020). Όταν οι υπολογιστές άρχισαν να μειώνουν το μέγεθος και το κόστος, πολλές μεγάλες εταιρείες επένδυσαν σε τεχνολογίες για την αποθήκευση και διαχείριση δεδομένων και συστημάτων. Η αποθήκευσή τους με κλειδαριά έγινε περιττή αφού άρχισαν να χρησιμοποιούνται κωδικοί πρόσβασης.

1970-80: η ασφάλεια των υπολογιστών γεννήθηκε το 1972 με το ερευνητικό έργο στο APRANET αλλά και λόγω της ανάπτυξης του ενδιαφέροντος από την ακαδημαϊκή κοινότητα. Ο Bob Thomas και ο Rey Tomlinson δημιούργησαν τα προγράμματα, Creeper και Reaper αντίστοιχα, τα οποία μπορούσαν να μετακινηθούν ελεύθερα στο δίκτυο. Το πρόγραμμα Reaper όμως, είχε ως στόχο να βρίσκει και να διαγράφει το Creeper εντελώς από το δίκτυο. Έτσι αποτέλεσε το πρώτο λογισμικό προστασίας από τους ιούς αλλά το πρώτο computer worm, καθώς ήταν αυτό αντιγραφόμενο πρόγραμμα. Η δημιουργία πρώιμης ασφάλειας υπολογιστών έγινε από την ESD και την ARPA με την Πολεμική Αεροπορία των ΗΠΑ και άλλους οργανισμούς που συνεργάστηκαν για να αναπτύξουν ένα σχέδιο για το τμήμα του λειτουργικού συστήματος που παρέχει πρόσβαση σε χρήστες (security kernel) για το σύστημα υπολογιστών Honeywell Multics. Η UCLA και το Ινστιτούτο Έρευνας του Στάνφορντ εργάστηκαν σε παρόμοια έργα (Chadd, 2020). Επιπλέον, το έργο Ανάλυσης Προστασίας της ARPA διερεύνησε την ασφάλεια του λειτουργικού συστήματος αναγνωρίζοντας αυτοματοποιημένες τεχνικές για την ανίχνευση τρωτών σημείων στο λογισμικό. Το 1976, το Operating System Structures για την υποστήριξη ασφάλειας και αξιόπιστου λογισμικού δήλωσε: «η ασφάλεια έχει γίνει ένας σημαντικός και προκλητικός στόχος στο σχεδιασμό συστημάτων υπολογιστών», γεγονός που σηματοδοτεί την αλλαγή στην κυβερνοασφάλεια και την ανάδειξη της καθολικής

ανάγκης για την προστασία των δεδομένων. Τρία χρόνια αργότερα Kevin Mitnick (16 χρονών) χάκαρε το Ark (υπολογιστή της Digital Equipment Corporation για την ανάπτυξη λειτουργικών συστημάτων) και έφτιαξε αντίγραφα του λογισμικού αργότερα όμως συνελήφθη και φυλακίστηκε. Αυτή η πράξη αποτέλεσε τη πρώτη από τις πολλές επιθέσεις στον κυβερνοχώρο που θα υπάρξουν μέσα στις επόμενες δεκαετίες.

1980-90: αυτή η δεκαετία σηματοδοτεί την μετάβαση από το δίκτυο του APRANET στο Internet (Διαδίκτυο). Το 1981 ο Ian Murphy, γνωστός και ως «Captain Zap», εισβάλλει στο δίκτυο AT&T και αλλάζει το εσωτερικό ρολόι για να χρεώνει τιμές εκτός ωρών σε ώρες αιχμής. Επιπλέον, κατέστη ο πρώτος που καταδικάστηκε για έγκλημα στον κυβερνοχώρο. Από την άλλη μεριά, ο πρώτος ιός υπολογιστών, ο Elk Cloner, δημιουργήθηκε ως φάρσα από έναν 15χρονο μαθητή γυμνασίου και ο ιός αυτός μόλυνε τους υπολογιστές Apple II μέσω δισκέτας το 1982. Επιπλέον, την περίοδο του Ψυχρού Πολέμου, η απειλή της ασφάλειας στον κυβερνοχώρο αυξήθηκε λόγω του φαινομένου της κατασκοπείας ανάμεσα στις ΗΠΑ και την Σοβιετική Ένωση. Το 1986, ο Γερμανός χάκερ Marcus Hess χρησιμοποίησε μια πύλη διαδικτύου στο Berkley της Καλιφόρνια, για να εισέρθει το ARPANET. Παραβίασε 400 στρατιωτικούς υπολογιστές, συμπεριλαμβανομένων μεγάλων συστημάτων υπολογιστών όπως στο Πεντάγωνο, σκοπεύοντας να κλέψει και να πουλήσει στρατιωτικές πληροφορίες, κωδικούς πρόσβασης και άλλα δεδομένα στις Σοβιετικές Μυστικές Υπηρεσίες (KGB). Ο Clifford Stoll παρατήρησε αυτή την παρατυπία και χρησιμοποίησε τη τακτική «honeypot», με βάση την οποία, ενώ γίνεται αντιληπτή η παραβίαση, η παράτυπη πρόσβαση ενθαρρύνεται, με σκοπό τη συλλογή όσο το δυνατόν περισσότερων δεδομένων για τον εισβολέα. Τελικός στόχος αυτής της πρακτικής είναι πρώτον, η όσο το δυνατόν πληρέστερη εκτίμηση της βλάβης που έχει προκληθεί, δεύτερον η αποτροπή μελλοντικών παρόμοιων συμβάντων και τρίτον, η τελική ανακάλυψη και ιδανικά σύλληψη του δράστη. Με την εισβολή στο Berkley ακολούθησε η ανακάλυψη του ιού worm (σκουληκιών) «Morris», που δημιουργήθηκε από τον Robert Morris, φοιτητή του Πανεπιστημίου Cornell. Αυτό το σκουλήκι κατέστρεψε περισσότερους από 6.000 υπολογιστές και είχε ως αποτέλεσμα ζημίες

ύψους 98 εκατομμυρίων $. Μολυσμένοι υπολογιστές βρέθηκαν στη NASA, το Πεντάγωνο και τα πανεπιστήμια, των MIT, Berkley και Stanford. Το 1987 ήταν το έτος γέννησης των εμπορικών προγραμμάτων προστασίας από ιούς. Ο Andreas Lüning και ο Kai Figge κυκλοφόρησαν το πρώτο τους λογισμικό προστασίας από ιούς. Τρεις Τσεχοσλοβάκοι δημιούργησαν την πρώτη έκδοση του antivirus NOD, ενώ στις ΗΠΑ, ο John McAfee ίδρυσε το McAfee (Chadd, 2020). Μία από τις πρώτες καταστροφές ιών έγινε από τον Γερμανό Bernd Fix όταν εξουδετέρωσε τον περίφημο «ιό της Βιέννης» (1987), δηλαδή ένα κακόβουλο λογισμικό που διαδόθηκε και κατέστρεψε αρχεία. Μέχρι το 1988, πολλές εταιρείες προστασίας από ιούς είχαν συσταθεί σε όλο τον κόσμο, καθώς οι τελικοί χρήστες άρχισαν να ενημερώνονται και να μαθαίνουν περισσότερα για τους ιούς των ηλεκτρονικών υπολογιστών. Η δεκαετία έκλεισε με περισσότερες προσθήκες στην αγορά ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των F-Prot, ThunderBYTE και Norman Virus Control (Chadd, 2020). Η πρώτη περίπτωση μεγάλης κλίμακας ransomware διαδόθηκε μέσω δισκέτας. Το κακόβουλο λογισμικό διανεμήθηκε σε 20.000 συμμετέχοντες στο συνέδριο του Παγκόσμιου Οργανισμού Υγείας για το AIDS. Μετά τη λήψη του, το ransomware κρυπτογραφεί κάποια αρχεία μετά την επανεκκίνηση του υπολογιστή για ορισμένες φορές. Για να ξεκλειδωθεί ο υπολογιστής, οι χρήστες πρέπει να στείλουν 189$ με «χρέωση αδειοδότησης» στην PC Cyborg Corporation με αντάλλαγμα ένα κλειδί αποκρυπτογράφησης.

1990-00: αυτή την περίοδο τα πιο σημαντικά γεγονότα ήταν ότι α) οι πρώτοι πολυμορφικοί ιοί δημιουργήθηκαν (κωδικός που μεταλλάσσεται διατηρώντας τον αρχικό αλγόριθμο ανέπαφο για να αποφευχθεί η ανίχνευση), β) το βρετανικό περιοδικό «Computer PC Today» κυκλοφόρησε μια έκδοση με δωρεάν δίσκο που "κατά λάθος" περιείχε τον ιό DiskKiller, μολύνοντας δεκάδες χιλιάδες υπολογιστές και γ) ιδρύθηκε το EICAR (Ευρωπαϊκό Ινστιτούτο Έρευνας κατά των ιών Υπολογιστών) (Chadd, 2020). Μέχρι το 1996, πολλοί ιοί χρησιμοποίησαν νέες τεχνικές και μεθόδους, όπως ο πολυμορφισμός και οι «μακροί ιοί», θέτοντας ένα νέο σύνολο προκλήσεων για παρόχους προστασίας από ιούς που έπρεπε να αναπτύξουν νέες δυνατότητες εντοπισμού και αφαίρεσης. Νέοι αριθμοί ιών και κακόβουλων

προγραμμάτων εκτοξεύθηκαν τη δεκαετία του 1990, από δεκάδες χιλιάδες στις αρχές της δεκαετίας που αυξάνονταν σε 5 εκατομμύρια ανά χρόνο μέχρι το 2007 (Chadd, 2020). Μέχρι τα μέσα της δεκαετίας του '90, ήταν σαφές ότι η ασφάλεια στον κυβερνοχώρο έπρεπε να επεκταθεί και αναπτυχθεί για την προστασία του κοινού. Ένας ερευνητής της NASA ανέπτυξε το πρώτο πρόγραμμα τείχους προστασίας, φτιάχνοντάς το στις φυσικές δομές που εμποδίζουν την εξάπλωση πραγματικών πυρκαγιών σε κτήρια. Πιο συγκεκριμένα, χρησιμοποιώντας δρομολογητές διαχωρίζουν τα δίκτυα σε μικρότερα δίκτυα, προσπαθώντας τα τείχη προστασίας να εμποδίσουν την επίθεση ενός ιού ή κακόβουλων λογισμικών, η οποία έχει σκοπό να μολύνει όλους τους υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο ταυτόχρονα (Radware.com, 2021). Προς το τέλος της δεκαετίας του 1990, η χρήση του ηλεκτρονικού ταχυδρομείου διαδόθηκε ευρέως και έμελλε να αλλάξει και να εκσυγχρονίσει την επικοινωνία, , ωστόσο, άνοιξε μία νέα πύλη εισόδου για ιούς. Το 1999, ο ιός «Mellisa» (δημιουργός του ο David Smith) εξαπλώθηκε και εισερχόταν στον υπολογιστή του χρήστη μέσω ενός εγγράφου του Word και έπειτα έστελνε αντίγραφά του στις 50 πρώτες διευθύνσεις ηλεκτρονικού ταχυδρομείου στο Microsoft Outlook. Παραμένει ένας από τους ταχύτερα διαδεδομένους ιούς και η ζημιά κόστισε περίπου 80 εκατομμύρια δολάρια.

2000-10: την δεκαετία αυτή, οι απειλές στον κυβερνοχώρο αρχίζουν να διαφοροποιούνται και να πολλαπλασιάζονται. Με το Διαδίκτυο διαθέσιμο σε περισσότερα σπίτια και γραφεία σε όλο τον κόσμο, οι εγκληματίες στον κυβερνοχώρο είχαν περισσότερες ευκαιρίες για εκμετάλλευση από ποτέ (Chadd, 2020). Το 2001, εμφανίστηκε μια νέα τεχνική μόλυνσης: οι χρήστες δεν χρειάζονται πλέον να κατεβάσουν αρχεία. Απλά αρκούσε μια επίσκεψη σε έναν μολυσμένο ιστότοπο, καθώς οι κακοί δρώντες αντικατέστησαν καθαρές σελίδες με μολυσμένες ή έκρυβαν κακόβουλο λογισμικό σε νόμιμες ιστοσελίδες (Chadd, 2020). Οι υπηρεσίες ανταλλαγής άμεσων μηνυμάτων (chats) άρχισαν επίσης να δέχονται επίθεση. Ορισμένες εγκληματικές οργανώσεις άρχισαν να χρηματοδοτούν σε μεγάλο βαθμό επαγγελματικές επιθέσεις στον κυβερνοχώρο και για αυτό οι πάροχοι προστασίας κατέβαλαν ακόμη περισσότερες προσπάθειες για να αντιμετωπίσουν αυτές τις

απειλές. Το 2000 διατέθηκε ο πρώτος μηχανισμός προστασίας από ιούς το OpenAntivirus. Ενώ, το 2001 κυκλοφορεί το ClamAV, ο πρώτος μηχανισμός προστασίας από ιούς ανοιχτού κώδικα και η Avast δημιούργησε δωρεάν λογισμικό προστασίας από ιούς. Μια βασική πρόκληση του antivirus είναι ότι μπορεί συχνά να επιβραδύνει την απόδοση ενός υπολογιστή. Μια άλλη καινοτομία αυτή τη δεκαετία ήταν η ασφάλεια λειτουργικών συστημάτων. Αυτό συχνά περιλαμβάνει την εκτέλεση τακτικών ενημερώσεων ενημερωμένων εκδόσεων λειτουργικού συστήματος, την εγκατάσταση ενημερωμένων μηχανών και λογισμικού προστασίας από ιούς, τείχους προστασίας και ασφαλών λογαριασμών με διαχείριση χρηστών (Chadd, 2020). Με τον πολλαπλασιασμό των smartphone, αναπτύχθηκε επίσης λογισμικό προστασίας από ιούς για αυτά. Επίσης, το 2005 παρατηρείται το φαινόμενο πειρατείας από νέους ιδιαίτερα ανθρώπους για να καταφέρουν να έχουν πρόσβαση software, μουσική και ταινίες, ενώ το 2007 αυξάνονται τα περιστατικά παιδικής πορνογραφίας.

2010-20: στην δεκαετία του 2010 εμφανίζονται και καταγράφονται πολλές παραβιάσεις και επιθέσεις υψηλού επιπέδου που άρχισαν να επηρεάζουν την εθνική ασφάλεια των χωρών και κόστισαν εκατομμύρια χρήματα σε αρκετές επιχειρήσεις. Από τα πιο σημαντικά κυβερνοεγκλήματα είναι (Chadd, 2020):

· 2012: Ο Σαουδάραβας χάκερ 0XOMAR δημοσιεύει τις λεπτομέρειες περισσότερων από 400.000 πιστωτικών καρτών στο διαδίκτυο

· 2013: Πρώην υπάλληλος της CIA για την κυβέρνηση των ΗΠΑ Edward Snowden αντιγράφει και διέρρευσε διαβαθμισμένες πληροφορίες από την Εθνική Υπηρεσία Ασφαλείας (NSA)

· 2013-2014: Κακόβουλοι χάκερ εισέβαλαν στο Yahoo, θέτοντας σε κίνδυνο τους λογαριασμούς και τα προσωπικά στοιχεία των 3 δισεκατομμυρίων χρηστών του. Στη συνέχεια, το Yahoo επιβλήθηκε πρόστιμο 35 εκατομμυρίων δολαρίων επειδή δεν αποκάλυψε τις ειδήσεις

· 2017: WannaCry ransomware μόλυνε 230.000 υπολογιστές σε μια μέρα και αποτελεί το πρώτο γνωστό παράδειγμα ransomware που λειτουργεί μέσω ενός worm (λογισμικό ιών που αναπαράγεται και διανέμεται).

· 2019: Πολλές επιθέσεις DDoS (επίθεση άρνησης υπηρεσιών) ανάγκασαν το χρηματιστήριο της Νέας Ζηλανδίας να κλείσει προσωρινά.

Η αυξανόμενη χρήση του διαδικτύου και η εξέλιξη των τεχνολογικών συσκευών στην καθημερινότητά μας, έδωσαν το χώρο στους κυβερνοεγκληματίες για νέες ευκαιρίες εκμετάλλευσης. Το γεγονός αυτό μπορεί να αποδειχθεί από τα δεδομένα που έχει δημοσιεύσει ο Άλγκρεν (2021):

· Το κόστος των ζημιών στον κυβερνοχώρο θα κοστίσει έως και 6 τρισεκατομμύρια δολάρια ετησίως έως το 2021.

· 1 στα 131 μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν επικίνδυνα κακόβουλα προγράμματα όπως ransomware και επιθέσεις ηλεκτρονικού ψαρέματος (phishing).

· Το πιο παραβιασμένο CMS είναι WordPress, αποτελώντας πάνω από το 90% όλων των προσπαθειών εισβολής.

· Πάνω από το 40% του εγκλήματος στον κυβερνοχώρο οι επιθέσεις στοχεύουν μικρές επιχειρήσεις.

· Η μεγαλύτερη παραβίαση των δεδομένων συνέβη το 2013 όταν 3 δισεκατομμύρια χρήστες του Yahoo οι αριθμοί τηλεφώνου, οι ημερομηνίες γέννησης και οι ερωτήσεις ασφαλείας, έχουν καταστραφεί.

· Σε παγκόσμιο επίπεδο, το έγκλημα στον κυβερνοχώρο είναι το δεύτερο πιο αναφερόμενο έγκλημα σχετικά με την κυβερνοασφάλεια.

· 93% των παραβιάσεων δεδομένων συμβαίνει μέσα σε λίγα λεπτά και το 83% δεν ανακαλύπτεται για εβδομάδες.

· Οι αδύναμοι ή κλεμμένοι κωδικοί πρόσβασης είναι η πιο κοινή τακτική μεταξύ των εγκληματιών στον κυβερνοχώρο. Το 81% των επιθέσεων στον κυβερνοχώρο βασίζονται σε αδύναμους ή κλεμμένους κωδικούς πρόσβασης.

1.4 Βαρύτητα προβλήματος και προκλήσεις

Το μέγεθος του κυβερνοχώρου είναι εξαιρετικά μεγάλο και αυξάνεται εκθετικά (Kshetri, 2010: 227), γεγονός που συντέλεσε στο να ανέβει ως προτεραιότητα στην κυβερνητική ατζέντα πολλών κρατών το έγκλημα στον κυβερνοχώρο. Αυτό επιβεβαιώνεται άλλωστε από τα εξής στοιχεία: 1) περίπου το 40% του παγκόσμιου πληθυσμού είχε σύνδεση στο Internet το 2018. Το 1995, ήταν λιγότερο από 1% και 2) από τις 2 Ιανουαρίου 2021 υπήρχαν ήταν 4,783,503,852 (4.7+ δισεκατομμύρια) σε όλο τον κόσμο, ενώ στο τέλος του 2016 καταγράφηκαν 3.42 δισεκατομμύρια χρήστες (Άλγκρεν, 2021). Η σημαντική ανάπτυξη του κυβερνοχώρου, η ύπαρξη πολλών μικρών παικτών και η έλλειψη/μείωση των «φυσικών» διαπροσωπικών σχέσεων σημαίνει ότι η εμφάνιση ευκαιριών είναι πιο πιθανό να προκύψουν στον κυβερνοχώρο παρά στο φυσικό κόσμο (Kshetri, 2010: 228). Οι ευκαιρίες που προσφέρονται προς το οργανωμένο έγκλημα αλλά και τους μεμονωμένους εγκληματίες θα έχει ως αποτέλεσμα την περαιτέρω εξέλιξη και διάδοση του φαινομένου καθώς η ψηφιακή τεχνολογία θα διαδίδεται όλο και περισσότερο.

Εφόσον μιλάμε για εξέλιξη ως προς το φαινόμενο, εννοούμε και την ανάδυση νέων μορφών κυβερνοεγκλήματος αλλά και την μετατροπή και προσαρμογή των ήδη υπαρχουσών στο ψηφιακό περιβάλλον. Αν μη τι άλλο, αυτό δίνει παράλληλα το κίνητρο σε αρκετές εταιρείες τεχνολογιών και πληροφορικής να εμβαθύνουν στο τομέα της ασφάλειας, διασφαλίζοντας έτσι σε πολλούς χρήστες την προστασία μέσα στο χώρο του Διαδικτύου. Ακόμη και διάφοροι οργανισμοί και κυβερνητικές υπηρεσίες έχουν αρχίσει να προωθούν και να εφαρμόζουν νέες πολιτικές ώστε να αποθαρρύνουν αποκλίνουσες και παραβατικές συμπεριφορές στον κυβερνοχώρο με σκοπό πάντα την μεγιστοποίηση της ασφάλειας. Με την πάροδο του χρόνου, σίγουρα θα υπάρξουν περισσότερο πυκνά και εκτεταμένα δίκτυα θεσμών, φορέων, νόμων και κανόνων που θα αναπτυχθούν για την καταπολέμηση των εγκλημάτων στον

κυβερνοχώρο (Kshetri, 2010: 228). Άρα, περισσότερα προβλήματα προκύπτουν όταν υπάρχουν περιορισμένοι πόροι και ανεπαρκής τεχνογνωσία.

Είναι ευρέως γνωστό ότι το ψηφιακό περιβάλλον έχει βαθιά επίδραση στον τρόπο που μπορούν να πραγματοποιηθούν οι κοινωνικές αλληλεπιδράσεις (τόσο νόμιμες όσο και παράνομες), και αλλάζει έτσι το πιθανό πεδίο και κλίμακα προσβολής, τροποποιώντας τις σχέσεις μεταξύ παραβατών και θυμάτων και τη δυνατότητα για συστήματα ποινικής δικαιοσύνης προσφέρουν ικανοποιητικές λύσεις θεραπείας ή πρόληψης (Capeller, 2001 οπ. Αναφ. οι Yar & Steinmetz, 2019). Μπορούμε να συμφωνήσουμε λοιπόν με τους Yar & Steinmetz (2019) ότι τα νέα κοινωνικά αλληλεπιδραστικά χαρακτηριστικά του περιβάλλοντος στον κυβερνοχώρο (κυρίως η κατάρρευση των φραγμών χωροχρόνου, η συνδεσιμότητα πολλών χρηστών, η ανωνυμία και η ευκολία αλλαγής της διαδικτυακής ταυτότητας) καθιστούν δυνατή την δημιουργία νέων μορφών και μοτίβων παράνομης δραστηριότητας.

Η αυξανόμενη εξάρτηση της κοινωνίας από τα δίκτυα της τεχνολογίας υπολογιστών μας καθιστά όλο και πιο ευάλωτους στην αποτυχία και εκμετάλλευση αυτών των συστημάτων (Yar & Steinmetz, 2019). Ειδικότερα, σε αυτή την νέα κατάσταση πραγμάτων που ζούμε αυτή την περίοδο, της πανδημίας, η εξάρτηση έχει μεγαλώσει πολύ περισσότερο, αφού η τηλεργασία έχει αυξηθεί. Σχετικό παράδειγμα μπορεί να αποτελέσει και η περίπτωση των πανεπιστημίων όπου εδώ και 1,5 χρόνο όλη η εκπαίδευση των φοιτητών στηρίζεται και πραγματοποιείται μέσα από διαδικτυακές πλατφόρμες με εικονικές αίθουσες (π.χ. Zoom, Webex). Σύμφωνα, λοιπόν, με τον Clough (2010: 5-8) οι βασικές προκλήσεις για το κυβερνοεγκλήματος, προκύπτουν και αναφύονται από τα χαρακτηριστικά της ψηφιακής τεχνολογίας, δηλαδή:

- **Κλίμακα:** το Διαδίκτυο επιτρέπει χρήστες να επικοινωνούν με πολλά άτομα, χωρίς μεγάλο κόστος και εύκολα. Οι άνθρωποι στο Διαδίκτυο παρέχουν μια άνευ προηγουμένου δεξαμενή με παραβάτες και θύματα. Αυτό λειτουργεί ως «πολλαπλασιαστής δύναμης», επιτρέποντας την παραβατικότητα σε κλίμακα που δεν θα μπορούσε να επιτευχθεί στο φυσικό περιβάλλον.

- **Προσβασιμότητα:** Αρχικά, οι υπολογιστές αποτελούσαν μεγάλες, δυσκίνητες συσκευές και χρησιμοποιούνταν κυρίως από κυβερνητικά, ερευνητικά και χρηματοπιστωτικά ιδρύματα, έτσι, η ικανότητα διάπραξης κυβερνοεγκλημάτων περιορίστηκε σε μεγάλο βαθμό σε άτομα με πρόσβαση και εξειδίκευση. Σήμερα, η τεχνολογία είναι πανταχού παρούσα και όλο και πιο εύκολη χρήση, διασφαλίζοντας τη διαθεσιμότητά του τόσο στους παραβάτες όσο και στα θύματα. Το να έχεις πρόσβαση πλέον στο Διαδίκτυο είναι το πιο εύκολο πράγμα. Ακόμη και μικρά παιδιά μπορούν να χρησιμοποιήσουν και να κατανοήσουν τις βασικές λειτουργίες ενός κινητού τηλεφώνου ή tablet.
- **Ανωνυμία:** Η ανωνυμία είναι ένα προφανές πλεονέκτημα για έναν δράστη και η ψηφιακή τεχνολογία το διευκολύνει με πολλούς τρόπους. Οι παραβάτες μπορεί σκόπιμα απόκρυψη της ταυτότητάς τους στο Διαδίκτυο με χρήση διακομιστών μεσολάβησης, πλαστογραφημένου email ή Διευθύνσεις IP.
- **Φορητότητα και δυνατότητα μεταφοράς:** Κεντρικό στοιχείο της δύναμης της ψηφιακής τεχνολογίας είναι η ικανότητα αποθήκευσης τεράστιων ποσότητες δεδομένων. Έγγραφα, εικόνες ή ήχος μπορούν να μεταδοθούν απλά και με αμελητέο κόστος σε εκατομμύρια παραλήπτες.
- **Παγκόσμια εμβέλεια:** Το ποινικό δίκαιο παραδοσιακά θεωρείται τοπικό, περιορισμένο στην εδαφική δικαιοδοσία στην οποία συνέβη το αδίκημα. Τα σύγχρονα δίκτυα υπολογιστών αμφισβήτησαν αυτό το παράδειγμα. Είτε πρόκειται για επίθεση άρνησης πρόσβασης (Denial of Service – DoS) ή διανομή παιδικής πορνογραφίας, δεν υπάρχει ανάγκη οι παραβάτες και τα θύματα να βρίσκονται στην ίδια περιοχή. Αυτό όχι μόνο παρέχει, κυριολεκτικά, έναν κόσμο ευκαιριών για τους παραβάτες, παρουσιάζει τεράστιες προκλήσεις για την επιβολή του νόμου.

- **Απουσία ικανής προστασίας:** Η φύση των ηλεκτρονικών δεδομένων απαιτεί εξελιγμένες εγκληματολογικές τεχνικές για να διασφαλιστεί προστασία. Ακόμα και όταν εμπλέκονται επίσημοι θεσμοί, η διαφύλαξη δεδομένων

μπορεί να είναι περιορισμένη ή ανύπαρκτη. Όπως και στο φυσικό περιβάλλον , δεν είναι ούτε πρακτικό ούτε επιθυμητό η αστυνομία να είναι παντού. Ο ρόλος του «προστάτη», λοιπόν, πρέπει να μοιραστεί με άλλους σε ολόκληρη την κοινότητα, είτε πρόκειται για γονείς που παρακολουθούν τα παιδιά τους χρήση του Διαδικτύου, χρηματοπιστωτικών ιδρυμάτων που αναζητούν ύποπτες συναλλαγές ή διαχειριστές συστήματος που εντοπίζουν εισβολές σε κάποιο δίκτυο. Όλα πρέπει να παίζουν ένα σημαντικό ρόλο «κηδεμονίας», ειδικότερα οι κυβερνητικές ρυθμιστικές αρχές. Οι πάροχοι υπηρεσιών Διαδικτύου είναι ιδιαίτερα σημαντικοί, αποτελώντας ουσιαστικά τους φύλακες δεδομένων στο Διαδίκτυο. Η αποτελεσματική ρύθμιση απαιτεί έρευνα ως προς τον τρόπο πρόληψης και εφαρμογή κανόνων ποινικού δικαίου, ώστε παράλληλα να οριστικοποιηθεί ποια είναι η αποδεκτή συμπεριφορά μέσα στο διαδικτυακό περιβάλλον.

Όπως είπαμε οι νέες τεχνικές επίθεσης οδηγούν και στην εμφάνιση νέων φαινομένων. Υπάρχουν τρεις δυνάμεις που οδηγούν αυτό το νέο κύμα επιθέσεων: οργανωμένες συμμορίες εγκλήματος στον κυβερνοχώρο, κινήματα «hacktivist» και χάκερς εθνικών κρατών (White, 2020: 7). Ο προσδιορισμός της εγκληματικής δραστηριότητας στην ψηφιακή εποχή απαιτεί πιο ασφαλή συστήματα, εκπαίδευση χρηστών, νέα νομοθεσία, νέες μεθόδους επιβολής και διεθνείς συμφωνίες που αντιμετωπίζουν τη διακρατική φύση του εγκλήματος στον κυβερνοχώρο (jjay.cuny.edu, 2021). Η κατανόηση του τρόπου που οι νέες τεχνολογίες μπορούν να αξιοποιηθούν από εγκληματίες είναι απαραίτητη γι’ αυτούς που χαράζουν εθνική πολιτική, για τα Σώματα Ασφαλείας και για τις εταιρείες τεχνολογίας και πληροφορικής. Κάποιες από τις σημερινές απειλές είναι οι παρακάτω (Καούλλας, 2021):

- **Οπτικο-ακουστική Πλαστοπροσωπία**: πλαστοπροσωπία ήχου και βίντεο για εκβιασμό ή εξαπάτηση θυμάτων.
- **«Ψάρεμα» πληροφοριών:** ή «phishing» είναι από τα παλαιότερα κυβερνοεγκλήματα. Είναι μια επίθεση «κοινωνικής μηχανικής» («social engineering»), όπου ο θύτης καταφέρνει, αφού συλλέξει αρκετές

προσωπικές και επαγγελματικές πληροφορίες για το θύμα, μέσα από ηλεκτρονική συζήτηση ή αλληλογραφία μαζί του να αποσπάσει στοιχεία πρόσβασης σε τραπεζικούς ή άλλους λογαριασμούς.

- **Διατάραξη νόμιμων συστημάτων Τεχνητής Νοημοσύνης(ΤΝ):** εφόσον τα συστήματα ΤΝ καθίστανται ολοένα και πιο απαραίτητα για την κυβέρνηση, υπηρεσίες κοινής ωφέλειας, το εμπόριο και τη λειτουργία οικιακών συσκευών, οι ευκαιρίες για επιθέσεις θα αυξηθούν, οδηγώντας σε πολλά πιθανά σενάρια εγκληματικότητας και τρομοκρατίας που θα προκύψουν από στοχευμένη διακοπή αυτών των συστημάτων.
- **Εκβιασμός μεγάλης κλίμακας:** στον παραδοσιακό εκβιασμό («blackmail») ο θύτης απειλεί το θύμα πως θα αποκαλύψει εγκληματική ή παραβατική συμπεριφορά ή ενοχλητικά προσωπικά μυστικά και πληροφορίες που θα τον εκθέσουν ή/και εξευτελίσουν. Η ΤΝ μεταλλάσσει αυτό το έγκλημα διότι μπορεί να συλλέγει αυτόματα έναν τεράστιο όγκο προσωπικών πληροφοριών από μέσα κοινωνικής δικτύωσης, αρχείων e-mail και προγραμμάτων περιήγησης. Μέσα από αυτά μπορούν να εντοπιστούν μεγάλοι αριθμοί ευπαθών ατόμων και πιθανών στόχων.
- **Διασπορά «Fake News»:** παραπληροφόρηση και προπαγάνδα.
- **Μέτριας ανησυχίας εγκλήματα:** κάποια από αυτά είναι η πώληση ψεύτικων υπηρεσιών («snake oil») μέσα από αυτοματοποιημένα μηνύματα και διαφημίσεις που θα δημιουργούν συστήματα ΤΝ, η «δηλητηρίαση δεδομένων» («data poisoning») μέσα από τη διοχέτευση πληροφοριών για τη χειραγώγηση νόμιμων συστημάτων ΤΝ και ο αυτόματος εντοπισμός τρωτών σημείων τους.
- **Ανταλλαγή εγκληματικής τεχνογνωσίας:** τα κυβερνοεγκλήματα στον ψηφιακό χώρο μπορούν εύκολα να κοινοποιηθούν και να επαναληφθούν ή και να πωληθούν, επιτρέποντας έτσι η διακίνηση και η εμπορία εγκληματικής τεχνογνωσίας να παρέχεται ως υπηρεσία.

Κεφάλαιο 2: Τυπολογική ταξινόμηση Κυβερνοεγκλήματος

2.1. Διάκριση και μορφές Κυβερνοεγκλήματος

Όπως αναφέρθηκε και προηγουμένως, στο πλαίσιο και περιεχόμενο αυτής της εργασίας, είναι απολύτως φανερό και ευδιάκριτο το πόσο έχει εισέλθει στην καθημερινότητά μας η τεχνολογία, το διαδίκτυο ακόμη και οι υπολογιστές προσωπικής χρήσης. Όσο μεγαλώνει διάρκεια χρήσης τους, αλλά και οι λειτουργίες που βοηθούν τον άνθρωπο στην εργασία και γενικότερα δραστηριότητες και ενέργειες που επιθυμεί να εκτελέσει, τόσο περισσότερο αυξάνονται οι πιθανότητες να εκτεθεί σε κίνδυνο. Σήμερα, η έκθεση στον κίνδυνο, δηλαδή, επηρεάζεται ιδιαίτερα από τον τρόπο που προσαρμόζεται ένα κράτος, μια επιχείρηση ή μεμονωμένα το άτομο στην πανδημία του COVID-19.

Σύμφωνα, λοιπόν, με τη Δίωξη Ηλεκτρονικού Εγκλήματος, ως ηλεκτρονικό έγκλημα «θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία» (lawspot.gr, 2021). Αυτές οι εγκληματικές μπορούν να λάβουν διαφορετικές μορφές, τις οποίες και θα αναλύσουμε στα επόμενα κεφάλαια, υποδεικνύοντας και αρκετές μελέτες περίπτωσης.

Μια αρχική διάκριση του ηλεκτρονικού εγκλήματος είναι **α)** με την χρήση του ηλεκτρονικού υπολογιστή ως **εργαλείου** και **β)** όσα εγκλήματα γίνονται μέσω Διαδικτύου, που έχουν, δηλαδή, ως **στόχο** τον ηλεκτρονικό υπολογιστή. Σύμφωνα με τον Berasategui (2021), η πρώτη κατηγορία εμπεριέχει πολύ λιγότερο τεχνικά ανεπεξέργαστα εγκλήματα, καθιστώντας τα έτσι πιο συνηθισμένα, στα οποία ο εισβολέας βασίζεται σε ανθρώπινες αδυναμίες για εκμετάλλευση. Τα εγκλήματα αυτά περιλαμβάνουν κλοπές, απάτες και παρενοχλήσεις που υπάρχουν εδώ και αιώνες, πολύ πριν ξεκινήσει η ανάπτυξη της επιστήμης των υπολογιστών. Η δεύτερη κατηγορία, από την άλλη πλευρά, απαιτεί πολύ υψηλότερη εμπειρία από τους δράστες

και συνήθως διαπράττεται από οργανωμένη ομάδα και όχι ένα άτομο. Δεδομένης της σχετικής τεχνογνωσίας που απαιτείται για την εκτέλεση και της καινοτομίας αυτών των ειδών εγκλημάτων, αυτά είναι αυτά που η κοινωνία είναι πιο απροετοίμαστη να αντιμετωπίσει. Αυτά τα εγκλήματα συνήθως εξαρτώνται από ιούς υπολογιστών, κακόβουλο λογισμικό και επιθέσεις άρνησης υπηρεσίας.

Τα πιο συνηθισμένα κυβερνοεγκλήματα που παρατηρούνται στην Ελλάδα σύμφωνα με το lawspot.gr (2021) είναι:

- οι απάτες μέσω Διαδικτύου
- η παιδική πορνογραφία
- το cracking και το hacking
- η διακίνηση-πειρατεία λογισμικού
- τα εγκλήματα σχετικά με πιστωτικές κάρτες
- η διακίνηση ναρκωτικών και
- τα εγκλήματα στα chat rooms.

Αντίστοιχα στην Ευρώπη παρατηρείται ιδιαίτερη ανησυχία από το 2015 στα εξής (European Commission, 2015):

- κλοπή ταυτότητας
- απάτη σε email
- διαδικτυακή απάτη
- προσβλητικό περιεχόμενο και παιδική πορνογραφία
- παράνομη πρόσβαση σε διαδικτυακές υπηρεσίες
- χακάρισμα σε λογαριασμούς email
- απάτη σε διαδικτυακές τραπεζικές συναλλαγές
- εκβιασμός στον κυβερνοχώρο
- κακόβουλο λογισμικό

Πέρα από την απλή αυτή διάκριση, υπάρχουν και άλλες που έχουν αναπτύξει και ορίσει διάφοροι μελετητές ανά τα χρόνια. Μία από αυτές είναι η διάκριση ανάμεσα

στις στοχευμένες επιθέσεις και τις ευκαιριακές σύμφωνα με τον Kshetri (2010: 11-13). Στις **στοχευμένες επιθέσεις** χρησιμοποιούνται συγκεκριμένα εργαλεία έναντι συγκεκριμένων στόχων στον κυβερνοχώρο και πραγματοποιούνται από εξειδικευμένους χάκερ με εμπειρία για να κάνουν σοβαρές ζημιές, ορισμένα από τα οποία υποκινούνται από οικονομικά κέρδη. Συνήθως ξεκινούν από τρομοκράτες, αντίπαλες εταιρείες, ιδεολογικούς χάκερ ή κυβερνητικές υπηρεσίες. Για παράδειγμα, τον Αύγουστο του 2004, έξι χάκερ καταδικάστηκαν από ένα δικαστήριο της Καλιφόρνιας για τη συμμετοχή τους σε επιθέσεις DoS εναντίον επιχειρηματικών αντιπάλων (Leyden, 2004 οπ. αν. ο Kshetri, 2010: 11-13). Οι **ευκαιριακές επιθέσεις** συνεπάγονται με την «απελευθέρωση» σκουληκιών και ιών που εξαπλώνονται αδιακρίτως σε όλο το Διαδίκτυο. Οι ευκαιριακές επιθέσεις είναι λιγότερο επικίνδυνες από τις στοχευμένες επιθέσεις και έχουν μικρότερες οικονομικές επιπτώσεις.

Τα εγκλήματα στον κυβερνοχώρο μπορούν. επίσης. να ομαδοποιηθούν σε δύο τύπους: **εγκλήματα αρπακτικών** με σκοπό το κέρδος (predatory crimes) και **εγκλήματα** στον κυβερνοχώρο **που βασίζονται στην αγορά** (Naylor, 2005 οπ. αν. ο Kshetri, 2010: 13). Τα εγκλήματα αρπακτικών στον κυβερνοχώρο μπορούν να οριστούν ως παράνομες πράξεις στον κυβερνοχώρο στις οποίες «κάποιος παίρνει ή βλάπτει σίγουρα ή σκόπιμα το άτομο ή την περιουσία ενός άλλου» (Glaser, 1971: 4 οπ. αν. ο Kshetri, 2010: 13). Παραδείγματα περιλαμβάνουν την κλοπή χρημάτων από τον τραπεζικό λογαριασμό κάποιου και την παραβίαση πνευματικής ιδιοκτησίας. Τα εγκλήματα στον κυβερνοχώρο που βασίζονται στην αγορά, από την άλλη πλευρά, δημιουργούν νέα εισοδήματα αντί να αναδιανέμουν τον υφιστάμενο πλούτο όπως κάνουν τα εγκλήματα αρπακτικών (Naylor, 2005 οπ. αν. ο Kshetri, 2010: 13). Τέτοια εγκλήματα συμβαίνουν, για παράδειγμα, στις πωλήσεις κλεμμένων πληροφοριών ή πιστωτικών καρτών και παράνομων ναρκωτικών στο διαδίκτυο.

Σύμφωνα με τους Schell & Martin (2004: 30) εγκλήματα στον κυβερνοχώρο, επιπλέον, μπορούν να οδηγήσουν είτε σε **βλάβη στα άτομα** είτε σε **βλάβη ιδιοκτησίας**. Εγκλήματα που προκαλούν βλάβη στα άτομα μπορεί να περιλαμβάνει το Cyberstalking (εμμονική παρακολούθηση), δηλαδή χρήση του κυβερνοχώρου για έλεγχο, παρενόχληση ή τρομοκράτηση ενός ατόμου μέχρι το σημείο που φοβάται για

σωματική βλάβη ή θάνατο, αλλά και Cyberpornography (Κυβερνοπορνογραφία) όπου κάποιος μπορεί να κατέχει, δημιουργεί, εισάγει, εμφανίζει, δημοσιεύει ή διανέμει πορνογραφία (ειδικά παιδική πορνογραφία) ή άλλα άσεμνα υλικά. Από την άλλη, το έγκλημα στον κυβερνοχώρο που οδηγεί σε βλάβη περιουσίας εκτελείται γενικά χρησιμοποιώντας τεχνικές «σπασίματος» και περιλαμβάνει τέτοιες κοινές παραλλαγές όπως είναι: 1) Flooding (τεχνική με την οποία «πλημμυρίζεται» ένας πάροχος υπηρεσίας με εικονικά αιτήματα με αποτέλεσμα την ανικανότητα εξυπηρέτησης των νόμιμων χρηστών): μια μορφή βανδαλισμού με στόχο την άρνηση υπηρεσίας (DoS) σε εξουσιοδοτημένους χρήστες ενός ιστότοπου ή συστήματος, 2) Παραγωγή και απελευθέρωση ιών και σκουληκιών: μια μορφή βανδαλισμού που προκαλεί διαφθορά και πιθανώς διαγραφή δεδομένων, 3) Spoofing (Πλαστογράφηση): η πίστωση στον κυβερνοχώρο μιας αυθεντικής ταυτότητας ενός χρήστη από μη αυθεντικούς χρήστες, προκαλώντας απάτη ή απόπειρα απάτης σε ορισμένες περιπτώσεις, ακόμη και κρίσιμη βλάβη υποδομών, 4) Phreaking: μορφή κλοπής ή/και απάτης στον κυβερνοχώρο που αποτελείται από τη χρήση τεχνολογίας για τη δωρεάν χρήση τηλεφωνικών κλήσεων, 5) Παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας και πνευματικών δικαιωμάτων: μια μορφή κλοπής που περιλαμβάνει την αντιγραφή πληροφοριών ή λογισμικού χωρίς συγκατάθεση.

Τέλος, ας μην ξεχνάμε ότι σε περιόδους κρίσης τα ήδη υπάρχοντα προβλήματα οξύνονται και υπάρχει μεγάλη ανάγκη για την καταπολέμηση αυτών των κινδύνων. Έτσι, εμφανίζεται οι **τεχνικές μη παραβάσεις** (Technical Nonoffenses). Αποτελούν πολιτικά παρακινούμενες, αμφιλεγόμενες και τεχνικές μη παραβιάσεις στον κόσμο του εγκλήματος στον κυβερνοχώρο που περιλαμβάνουν: 1. Hacktivism: ακτιβιστές χάκερ ή hacktivists, που ταιριάζουν τα ενδιαφέροντα του ακτιβισμού τους με τις ικανότητες των χάκερ ωστέ να προωθήσουν τις πλατφόρμες τους και τις αποστολές τους και 2. Cybervigilantism: γίνεται μια σύγκλιση του κυβερνοχώρου και της επαγρύπνηση (Schell & Martin, 2004: 31). Επομένως, αυτού του είδους «παραβιάσεις» είναι κοινωνικά αποδεκτές, εφόσον δεν αποσκοπούν σε συμφέροντα κατά του δημοσίου καλού ή αποτελούν τρομοκρατικές επιθέσεις.

2.2 Απάτη

Η χρήση του Διαδικτύου σημαίνει βίωση όλων των ειδών από κόλπα και σχέδια που έχουν δημιουργηθεί για να εξαπατούν τους ανθρώπους ως προς τα χρήματά τους ή άλλα περιουσιακά στοιχεία, συμπεριλαμβανομένων και των προσωπικών τους δεδομένων (McQuade III, 2009: 73). Η «απάτη» («fraud») μπορεί να λάβει διαφορετικές μορφές ως κυβερνοέγκλημα και το κίνητρο του δράστη αντίστοιχα διαφοροποιείται. Η απάτη, όμως, που παρατηρείται να διαπράττεται πιο συχνά είναι εκείνη με οικονομικό κίνητρο και περιεχόμενο.

Όπως αναφέρει ο McQuade (2009: 73), «*μια βασική διαφορά, φυσικά, είναι ότι όταν συμβαίνουν εγκλήματα στον κυβερνοχώρο που περιλαμβάνουν απάτη και κλοπή, συχνά παραμένουν αόρατα στους υπεραστικούς δρόμους του Διαδικτύου και μπορούν να επηρεάσουν αρνητικά εκατοντάδες, χιλιάδες ή ακόμα και εκατομμύρια ανθρώπους σε όλο τον κόσμο σε πολύ σύντομο χρονικό διάστημα ακόμη και ταυτόχρονα. Επιπλέον, οι εγκληματίες στον κυβερνοχώρο μπορούν να ξεκινήσουν τα σχέδιά τους από οπουδήποτε στον κόσμο προσφέρεται σύνδεση στο Διαδίκτυο. Κατά συνέπεια, και σε αντίθεση με τις παραδοσιακές απάτες και κλοπές, σχεδόν πάντα θα παραμείνουν άγνωστες, κρυμμένες μέσα τα φαινομενικά απεριόριστα όρια του κυβερνοχώρου, ακόμη και πολύ καιρό μετά αφού τα εγκλήματά τους έχουν διαπραχθεί*».

Από τα παραπάνω μπορούμε να καταλάβουμε την μεγάλη έκταση που μπορεί να λάβει μια «απάτη με πιστωτικές κάρτες», «απάτη με κλοπή ταυτότητας», ακόμη και το «phishing» («μέθοδος ψαρέματος»). Πιο συγκεκριμένα, το 2018, το Παγκόσμιο Οικονομικό Φόρουμ σημείωσε ότι η απάτη και το οικονομικό έγκλημα ήταν μια βιομηχανία τρισεκατομμυρίων δολαρίων, αναφέροντας ότι οι ιδιωτικές εταιρείες ξόδεψαν περίπου 8,2 δισεκατομμύρια δολάρια για τους ελέγχους κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, μόνο το 2017. Τα ίδια τα εγκλήματα, που εντοπίστηκαν και δεν ανιχνεύθηκαν γίνονται πιο πολυάριθμα και δαπανηρά από ποτέ. Σε μια ευρέως αναφερθείσα εκτίμηση, για κάθε δολάριο απάτης τα ιδρύματα χάνουν σχεδόν τρία δολάρια, μόλις προστεθούν οι σχετικές δαπάνες στην ίδια την απώλεια απάτης (Hasham, Joshi & Mikkelsen, 2019).

Η απάτη μπορεί να οριστεί ως γενικά ένα πλήθος εγκλημάτων, όπως πλαστογραφία, πιστωτικές απάτες και απειλές εμπιστευτικότητας, που περιλαμβάνουν εξαπάτηση οικονομικού προσωπικού ή υπηρεσιών για διάπραξη κλοπής (Hasham, Joshi & Mikkelsen, 2019). Από την άλλη πλευρά, η απάτη με πιστωτικές κάρτες συμβαίνει συνήθως στο Διαδίκτυο μετά από την δημιουργία ή διαφορετικά μετά από απόκτηση πρόσβασης σε έναν οικονομικό λογαριασμό από τους κυβερνοεγκληματίες. Στη συνέχεια, ενώ χρησιμοποιείται ψευδή αναγνώριση ή ο δράστης προσποιείται ότι είναι κάποιος άλλος, θα κάνει αγορές αγαθών και υπηρεσιών στο όνομα του άλλου άτομο που μπορεί να υπάρχει ή όχι (McQuade III, 2009: 73).

Μια άλλη μέθοδος απάτης αποτελεί η «κλοπή ταυτότητας» («identity theft»). Ο Clough (2010: 189-190) αναφέρει ότι μέσα την ικανότητά μας να αναγνωρίζουμε τον εαυτό μας, είμαστε σε θέση να συμμετέχουμε πλήρως στο κοινότητα. Κατά συνέπεια, εάν δεν μπορέσουμε να επιβεβαιώσουμε την ταυτότητά μας, ενδέχεται να μην έχουμε πρόσβαση τα δικαιώματά μας. Ομοίως, εάν κάποιος παριστάνει κάποιον άλλον, μπορεί να έχει πρόσβαση σε κάποια πράγματα που δεν δικαιούται. Πώς μπορεί να διαπραχθεί, λοιπόν, η «κλοπή ταυτότητας»; Η διαδικτυακή εισβολή και εξόρυξη δεδομένων κειμένου σε chat rooms ή ιστότοπους κοινωνικής δικτύωσης, κλοπή ταχυδρομικής αλληλογραφίας ή μη τεμαχισμένα έντυπα έγγραφα, «dumpster diving» για χαρτογραφικά αρχεία ή σκληρούς δίσκους που δεν έχουν καταστραφεί από παλιούς υπολογιστές και δεν έχουν ανακυκλωθεί σωστά, μαζί με διαδικτυακό έλεγχο δημόσιων αρχείων ή προειδοποιητικών ειδοποιήσεων, ακόμη και ένας περίπατος σε ένα νεκροταφείο ώστε να συγκρίνει κανείς πληροφορίες από τις ταφόπλακες με δημόσια αρχεία των αποθανόντων ατόμων, είναι όλα τα μέσα με τα οποία γίνονται υποθέσεις ή κατασκευάζονται οι ψευδείς ταυτότητες (McQuade III, 2009: 75). Συμπληρωματικά, μόλις ένα άτομο ταυτοποιηθεί και οι αντίστοιχες πληροφορίες χρηματοοικονομικού λογαριασμού έχουν ληφθεί, η διαδικτυακή απάτη μπορεί να είναι μόνο λίγα πλήκτρα μακριά από το να γίνει πραγματικότητα.

Επόμενη μέθοδος προς ανάλυση είναι το «phishing» («ψάρεμα»). Το ηλεκτρονικό «ψάρεμα» περιλαμβάνει τη μαζική διανομή μηνυμάτων ηλεκτρονικού ταχυδρομείου, «ρίχνοντας δίχτυα» για τη λήψη πιθανών θυμάτων. Ενώ το ηλεκτρονικό ψάρεμα

μπορεί να είναι χρησιμοποιείται για μια ποικιλία από απάτες, είναι ίσως το πιο συναφές με απάτες που υποτίθεται ότι προέρχονται από τράπεζες, εταιρείες πιστωτικών καρτών και ηλεκτρονικούς πωλητές που προσπαθούν να εξαπατήσουν θύματα στην παράδοση ευαίσθητων πληροφοριών όπως κωδικοί πρόσβασης, ονόματα χρηστών, αριθμοί κοινωνικής ασφάλισης κ.λπ. (James, 2005 οπ. αναφ. από Yar & Steinmetz, 2019). Επιπλέον, οι «ψαράδες» τώρα εμπλέκονται σε οργανωμένα δίκτυα εγκληματιών και συνεργάζονται ώστε να ξεπλύνουν χρήματα στέλνοντας μηνύματα μέσω ηλεκτρονικού ταχυδρομείου, δηλαδή κάνοντας «spam», και ανταλλάσσοντας άμεσα μηνύματα, το οποίο ονομάζεται «spim». Αυτό συμβαίνει όλο και περισσότερο με δίκτυα bot που επιτρέπουν στους κυβερνοεγκληματίες να έχουν απομακρυσμένη πρόσβαση και έλεγχο σε υπολογιστές διασκορπισμένους ευρέως σε όλο τον κόσμο, αλλά ταυτόχρονα να είναι συνδεδεμένοι στενά με τον Διαδικτυακό Ιστό. Οι εγκληματίες του κυβερνοχώρου μπορούν έτσι να στέλνουν πάρα πολλά email και στιγμιαία μηνύματα που μερικές φορές έχουν τη μορφή διαφημίσεων. Αυτά χρησιμεύουν ως έξυπνοι και πολύ παραπλανητικοί τρόποι να προσελκύσουν τους χρήστες συσκευών τεχνολογίας πληροφοριών (IT) και να κάνουν κλικ σε συνδέσμους Ιστού που τους οδηγούν σε Ιστότοπους με ενσωματωμένη ημιαυτόματη εξόρυξη δεδομένων σε επιχειρήσεις που διευθύνονται από κυβερνοεγκληματίες (McQuade III, 2009: 75).

Το «spoofing», ως μια άλλη τεχνική, αποτελεί δόλια πρακτική δημιουργίας αντίγραφων νόμιμων ιστότοπων, μέσω των οποίων μπορούν να κατευθύνονται τα θύματα και εν τέλει να παραδώσουν εν αγνοία τους ευαίσθητες πληροφορίες όπως τραπεζικά στοιχεία, αριθμοί πιστωτικών καρτών και κωδικοί πρόσβασης λογαριασμών (Yar & Steinmetz, 2019). Ουσιαστικά, η ενσωμάτωση πλαστογραφημένων ιστοσελίδων, τα ηλεκτρονικά μηνύματα «ψαρέματος» ενεργούν ως μέσο για την παράδοση κακόβουλου λογισμικού σε υπολογιστές, εξαπατώντας το άτομο κατά τη λήψη ενός κακόβουλου συνημμένου, μεταμφιεσμένο ως κάτι τόσο αβλαβές, όπως ένα έγγραφο ή αρχείο φωτογραφίας.

Με την έλευση της ψηφιοποίησης και της αυτοματοποίησης των χρηματοπιστωτικών συστημάτων, αυτά τα εγκλήματα έχουν γίνετε περισσότερο

ηλεκτρονικά εξελιγμένα και απρόσωπα (Hasham, Joshi & Mikkelsen, 2019). Ένα από τα πιο γνωστά εγκλήματα απάτης στον κυβερνοχώρο, λοιπόν, αποτελεί η απάτη «Nigerian» μέσω ηλεκτρονικού ταχυδρομείου. Η έλευση του Διαδικτύου επέτρεψε στους παραβάτες να προσεγγίσουν εκατομμύρια πιθανά θύματα χωρίς μεγάλο κόστος. Όσο περισσότεροι άνθρωποι γίνεται να μπορούν να υπάρξουν υποψήφια θύματα, τόσο μεγαλύτερη είναι η πιθανότητα «να πέσει κάποιος στα δίχτυα» της απάτης. Τα είδη απάτης που μπορεί να διαπραχθούν στο Διαδίκτυο είναι πάρα πολλά και ήδη έχουμε αναφερθεί στα πιο σημαντικά. Ας δούμε τώρα τι προέκυψε με την απάτη «Nigerian».

Οι «Νιγηριανές Απάτες», ή αλλιώς «Απάτες 419», αποτελούν μία διαφορετική μορφή διακίνησης μηνύματος με απατηλό περιεχόμενο. Ως ένα σύστημα προκαταβολών πήρε το όνομά του από το ίδιο το τμήμα του ποινικού κώδικα της Νιγηρίας, που απαγορεύει την απάτη. Σύμφωνα με το FBI, οι απάτες επιστολών της Νιγηρίας συνδυάζουν την απειλή της απάτης πλαστοπροσωπίας με μια παραλλαγή ενός συστήματος προκαταβολών, στο οποίο μια επιστολή που αποστέλλεται με αλληλογραφία ή μέσω ηλεκτρονικού ταχυδρομείου από τη Νιγηρία προσφέρει στον παραλήπτη την «ευκαιρία» να μοιραστεί με ποσοστό εκατομμυρίων δολαρίων, ό,τι ο συντάκτης - αυτοαποκαλούμενος κυβερνητικός αξιωματούχος - προσπαθεί να μεταφέρει παράνομα από τη Νιγηρία. Ο παραλήπτης ενθαρρύνεται να στείλει πληροφορίες στον συντάκτη, όπως κενά χαρτιά επιστολόχαρτου, όνομα τράπεζας και αριθμούς λογαριασμού και άλλες πληροφορίες αναγνώρισης χρησιμοποιώντας έναν αριθμό φαξ που αναφέρεται στην επιστολή ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου επιστροφής που παρέχεται στο μήνυμα. Επιπλέον, περισσότεροι από 14.600 άνθρωποι ανέφεραν ότι πέφτουν θύματα από προωθητικές απάτες το 2019. Συλλογικά, έχασαν 100,6 εκατομμύρια δολάρια ή περίπου 6.800 δολάρια το καθένα. Ουσιαστικά, ο απατεώνας ισχυρίζεται συνήθως ότι είναι μέλος μιας πλούσιας Νιγηριανής ή άλλης Δυτικής Αφρικής οικογένειας, επικοινωνώντας προσωπικά με κάποιο άτομο μετά το θάνατο ενός αγαπημένου προσώπου. Επιδιώκουν να μεταφέρουν μια μεγάλη περιουσία από τη χώρα για λόγους φύλαξης και στον τραπεζικό λογαριασμό του θύματος. Ποια είναι η παγίδα; Το γεγονός ότι πρέπει να

υποβληθούν μικρές πληρωμές με χρέωση από τα θύματα ώστε για αντάλλαγμα να δοθεί ένα μεγάλο ποσό από τα κρυμμένα χρήματα των απατεώνων (Deutsch, 2021).

Μια τυπική Νιγηριανή απάτη, λοιπόν, μπορεί περιλαμβάνει ένα συναισθηματικό email, γράμμα, μήνυμα κειμένου ή μήνυμα κοινωνικής δικτύωσης (Rijnetu, 2019), που ως τρόποι επικοινωνίας είναι αρκετά εύκολο να πραγματοποιηθούν λόγω του σχεδόν μηδενικού κόστους. Ας μην ξεχνάμε, πως ο παράγοντας της πανδημίας έχει συμβάλλει στην αύξηση χρήσης του Διαδικτύου και των τεχνολογικών συσκευών. Άρα, αυτό σημαίνει πως υπάρχουν περισσότερα περιστατικά από scammers που προσπαθούν να «αρπάξουν» κάθε ευκαιρία εξαπάτησης για προσωπικό όφελος. Σύμφωνα με την Deutsch (2021), οι συνήθεις τύποι απάτης COVID-19 περιλαμβάνουν:

· Ψεύτικες οργανώσεις υγείας: οι απατεώνες θέτουν ως υγειονομικές αρχές όπως ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) και τα Κέντρα Ελέγχου Νόσων των ΗΠΑ (CDC) για να προσφέρουν θεραπείες, δοκιμές ή άλλες πληροφορίες COVID-19.

· Ιστότοποι που πωλούν πλαστά προϊόντα: κάποιοι ιστότοποι προσφέρουν μάσκες προσώπου, απολυμαντικό χεριών, απολυμαντικά μαντηλάκια και άλλα προϊόντα υψηλής ζήτησης που δεν φτάνουν ποτέ στον πελάτη.

· Ψεύτικες κυβερνητικές πηγές: ορισμένοι απατεώνες ισχυρίζονται ότι εκδίδουν ενημερώσεις και πληρωμές για λογαριασμό της Υπηρεσίας Εσωτερικών Εσόδων (IRS) ή της τοπικής φορολογικής αρχής.

· Ψευδείς οικονομικές προσφορές: οι απατεώνες ενδέχεται να παρουσιάζονται ως τράπεζες, συλλέκτες χρεών ή επενδυτές με προσφορές που έχουν σχεδιαστεί για να κλέψουν τα οικονομικά στοιχεία πολλών ανθρώπων.

· Ψεύτικα αιτήματα δωρεάς για ΜΚΟ: αρκετοί άνθρωποι επιθυμούν να κάνουν δωρεές σε φιλανθρωπικούς σκοπούς για να βοηθήσουν στην αντιμετώπιση καταστροφών. Αυτό παρέχει μια εξαιρετική ευκαιρία για τους απατεώνες να δημιουργήσουν ψεύτικους μη κερδοσκοπικούς οργανισμούς, νοσοκομεία και άλλους οργανισμούς για τη συλλογή χρημάτων.

2.3 Διαδικτυακή Τρομοκρατία

Όπως και κάθε άλλη μορφή εγκληματικότητας, που συνέβαινε (και συνεχίζει να συμβαίνει) στον φυσικό κόσμο, κατάφερε να εμφανιστεί στον Κυβερνοχώρο, έτσι έγινε και με την τρομοκρατία. Ακόμη και πριν τη τρομοκρατική επίθεση κατά των ΗΠΑ στις 11 Σεπτεμβρίου 2001, οι ειδικοί εξέφραζαν ανησυχίες ως προς το επίπεδο ασφάλειας στον Κυβερνοχώρο. Γι' αυτό τον λόγο αυτή η μέρα αποτέλεσε ορόσημο για την έρευνα πάνω σε αυτό το πεδίο, αλλά και την εφαρμογή πρακτικών που θα βοηθούσαν στην μεγιστοποίηση της ασφάλειας. Το 1997, μάλιστα, ο Mark Pollitt συνδύασε έναν ορισμό του κυβερνοχώρου με τον ορισμό της «τρομοκρατίας» από το Υπουργείο των ΗΠΑ για να προσφέρει τον ακόλουθο ορισμό της κυβερνοτρομοκρατίας: «*Προμελετημένη, πολιτικά υποκινούμενη επίθεση κατά πληροφοριών, συστημάτων υπολογιστών, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που οδηγούν σε βία κατά μη μαχόμενους στόχους από υποεθνικές ομάδες ή μυστικούς πράκτορες*». Ένας παρόμοιος ορισμός προσφέρθηκε σε μια έκθεση του Κογκρέσου του 2003 που αναφέρεται στην κυβερνοτρομοκρατία ως «*η πολιτικά υποκινούμενη χρήση υπολογιστών ως όπλων ή ως στόχων, από υποεθνικές ομάδες ή μυστικούς πράκτορες που προτίθενται στη βία, για να επηρεάσουν ένα ακροατήριο ή να προκαλέσουν μια κυβέρνηση να αλλάξει τις πολιτικές της*» (όπως αναφ. ο McQuade, 2009: 55).

Είναι σημαντικό να σημειωθεί ότι οι «νέοι» εγκληματίες δεν αποτελούν απομονωμένα άτομα που εργάζονται σε οικιακούς υπολογιστές. Όπως προαναφέραμε, οι εγκληματίες του κυβερνοχώρου μοιάζουν με εγκληματίες στον συμβατικό κόσμο (Kshetri, 2010: 14). Μια έρευνα που διεξήχθη μεταξύ των μελών της Συνομοσπονδίας Βρετανικών Βιομηχανιών έδειξε ότι οι επιτιθέμενοι στα πιο σοβαρά εγκλήματα στον κυβερνοχώρο το 2000 ήταν χάκερ (44,8%), πρώην εργαζόμενοι (13,4%), οργανωμένες εγκληματικές ομάδες (12,8%), νυν εργαζόμενοι (11,5%), πελάτες (7,9%), ανταγωνιστές (5,8%), πολιτικές ομάδες και ομάδες διαμαρτυρίας (2,6%), και τρομοκράτες (1,4%) (Ειδήσεις BBC, 2001 όπως αναφ. ο Kshetri, 2010: 14). Επομένως, σύμφωνα με τα παραπάνω προφίλ που μπορεί να έχει κάποιος κυβερνοτρομοκράτης ή ένας εν δυνάμει κυβερνοτρομοκράτης, η παραβατική του

συμπεριφορά μπορεί να οφείλεται σε ψυχολογικούς λόγους (π.χ. εκδίκηση), οικονομικούς (ως μέσο για παραγωγή εισοδήματος) είτε λόγω ενδιαφέροντος.

Σύμφωνα με τον Clough (2010: 11) τέτοιες επιθέσεις έχουν τη δυνατότητα να προκαλέσουν σημαντική βλάβη, διαταράσσοντας ενδεχομένως βασικές υπηρεσίες όπως η ύδρευση, η ενέργεια, τα νοσοκομεία, τα χρηματοπιστωτικά συστήματα, οι υπηρεσίες έκτακτης ανάγκης, ο έλεγχος των αεροπορικών/θαλάσσιων μεταφορών κλπ.. Επιπλέον, αν και, μέχρι σήμερα, η απειλή ήταν περισσότερο δυνητική παρά πραγματική, μελέτες δείχνουν ότι έχει αυξηθεί ο αριθμός των κυβερνοεπιθέσεων κατά των υποδομών ζωτικής σημασίας, συμπεριλαμβανομένων των συστημάτων εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA), δηλαδή των συστημάτων υπολογιστών στα οποία βασίζεται η αυτόματη παρακολούθηση και προσαρμογή των υποδομών ζωτικής σημασίας.

Αυτό που πρέπει να κατανοηθεί είναι το γεγονός ότι η τεχνολογία χρησιμοποιείται για τη διευκόλυνση των δραστηριοτήτων των τρομοκρατών. Για παράδειγμα, οι επιθέσεις DoS (άρνηση λειτουργίας υπηρεσίας) μπορούν να χρησιμοποιηθούν εναντίον κυβερνητικών ιστότοπων ή διακομιστών, ανώνυμοι λογαριασμοί ηλεκτρονικού ταχυδρομείου και κρυπτογράφηση μπορούν να χρησιμοποιηθούν για την απόκρυψη τρομοκρατικών επικοινωνιών και ιστότοποι μπορούν να χρησιμοποιηθούν για τη διάδοση προπαγάνδας (Clough, 2010: 12). Το Διαδίκτυο μπορεί επίσης να χρησιμοποιηθεί ως τρόπος συλλογής πληροφοριών ή οδηγιών σχετικά με την εκπαίδευση σε όπλα, ενώ η τεχνολογία χρησιμοποιείται για τη συγκέντρωση χρηματοδότησης, για παράδειγμα μέσω εγκλημάτων ταυτότητας ή ως όχημα για ξέπλυμα χρήματος. Υπό την έννοια αυτή, η «κυβερνοτρομοκρατία» απλώς αποδίδει κίνητρο για άλλες μορφές εγκλήματος στον κυβερνοχώρο (Clough, 2010: 12).

Επιπροσθέτως, η κυβερνοτρομοκρατία υπό τη στενότερη έννοια της αποτελεί τη «*χρήση εργαλείων δικτύου υπολογιστών για τη βλάβη ή τον τερματισμό κρίσιμων εθνικών υποδομών (όπως η ενέργεια, οι μεταφορές, οι κυβερνητικές επιχειρήσεις)*». Μια τέτοια άποψη θεωρεί την κυβερνοτρομοκρατία ως τρομοκρατία, με τη στενότερη

νομική έννοια, τη πραγματικής ή απειλούμενη βλάβη σε πρόσωπα, περιουσιακά στοιχεία ή βασικές υπηρεσίες, συνήθως με πολιτικό, θρησκευτικό ή ιδεολογικό κίνητρο, με σκοπό τον εκφοβισμό του κοινού και /ή τον επηρεασμό της κυβερνητικής δράσης (Clough, 2010: 12). Γι' αυτό και ο νόμος περί τρομοκρατίας του 2000 περιλαμβάνει δράσεις που «*έχουν σχεδιαστεί σοβαρά για να παρεμβαίνουν ή να διαταράσσουν σοβαρά ένα ηλεκτρονικό σύστημα*» και σύμφωνα με την Έρευνα Εγκλημάτων υπολογιστών και Ασφάλειας του CSI/FBI το 2008, μόνο το 27 τοις εκατό των περιστατικών αναφέρθηκαν στις αρχές επιβολής του νόμου, με το 23,9% των περιστατικών να μην έχουν αναφερθεί καθόλου (Clough, 2010: 14).

Η Dorothy Dening, μια εμπειρογνώμονας στον κυβερνοχώρο, υπολόγισε ότι θα χρειάζονταν 6-10 χρόνια για να φτάσει μια τρομοκρατική ομάδα σε ένα σύνθετο, συντονισμένο επίπεδο στο οποίο θα μπορούσαν να δημιουργήσουν εξελιγμένα εργαλεία πειρατείας και να προκαλέσουν ουσιαστικά προβλήματα έναντι σε ολοκληρωμένες, ετερογενείς άμυνες σε δίκτυα υπολογιστών. Η έκθεση κατέληξε στο συμπέρασμα, ότι για έναν τρομοκράτη, η χρήση της τεχνολογίας θα είχε κάποια πλεονεκτήματα έναντι των φυσικών μεθόδων. Θα μπορούσε, δηλαδή, να διεξαχθεί εξ αποστάσεως και ανώνυμα η επίθεση, και δεν θα απαιτούσε χειρισμό εκρηκτικών ή κάποια αποστολή αυτοκτονίας. Επιπλέον, η τρομοκρατία στον κυβερνοχώρο μπορεί να γίνει εξαιρετικά ελκυστική ακριβώς λόγω της τεράστιας προσοχής που δίνεται από την κυβέρνηση και τα μέσα ενημέρωσης (Schell & Martin, 2004: 13).

Οι κρίσιμες υποδομές ενός κράτους αποτελούν κατά βάση στόχο των κυβερνοτρομοκρατικών επιθέσεων, επιχειρώντας να δημιουργήσουν με αυτόν τον τρόπο απώλεια σε βασικές υπηρεσίες, όπως η παροχή ηλεκτρικής ενέργειας, τα συστήματα άμεσης βοήθειας, οι υπηρεσίες τηλεπικοινωνιών, τα τραπεζικά συστήματα και άλλες κρίσιμες για τη λειτουργία ενός κράτους εγκαταστάσεις (Κικίλιας, 2008). Αυτές οι επιθέσεις, πλέον αποτελούν απειλή όχι μόνο για μια χώρα, αλλά για όλες στον κόσμο. Και τελικά, τον Ιούνιο του 2010 εμφανίστηκε το κακόβουλο λογισμικό «Stuxnet», κάτι σαν μια «ψηφιακή βόμβα διάτρησης» που επετέθη εναντίον του Ιρανικού πυρηνικού προγράμματος (NATO, 2021). Μέσω ενός απλού USB-stick που συνδέθηκε σε έναν στρατιωτικό φορητό υπολογιστή σε μια στρατιωτική βάση στην

Μέση Ανατολή, διασπάρθηκε κατασκοπευτικό λογισμικό που δεν εντοπίστηκε σε τόσο απόρρητα όσο και αδιαβάθμητα συστήματα, και έτσι το σκουλήκι Stuxnet κατάφερε να εξαπλωθεί. Αν και η αποτίμηση των ζημιών παραμένει ακόμη ασαφής, αυτό δείχνει τον πιθανό κίνδυνο του κακόβουλου λογισμικού που επηρεάζει κρίσιμα συστήματα υπολογιστών που διαχειρίζονται τις ενεργειακές προμήθειες ή τα δίκτυα κυκλοφορίας (NATO, 2021).

Ο τρόπος που λειτουργούσε ήταν ο εξής (Παρθενοπούλου, 2018): «*Το σπουδαίο με αυτόν τον ιό είναι ότι δεν άφηνε ίχνη, και άρα ήταν δύσκολο στον εντοπισμό του. Το Stuxnet όταν προσβάλλει έναν υπολογιστή, ελέγχει αρχικά αν αυτός ο υπολογιστής είναι συνδεδεμένος με συγκεκριμένα μοντέλα PLC(Programmable Logic Controller) που κατασκευάζονται από την Siemens. Τα μοντέλα PLC ελέγχουν σταθμούς παραγωγής ηλεκτρικής ενέργειας. Ο ιός σταματάει τον προγραμματισμό του PLC με αποτέλεσμα οι φυγοκεντρητές να στροβιλίζονται πιο γρήγορα σε σύγκριση με αυτό που έχει προγραμματιστεί, προκαλώντας κατ' αυτόν τον τρόπο ζημία και ενδεχομένως την καταστροφή τους. Σημαντικό είναι να σημειωθεί ότι το Stuxnet έστελνε μήνυμα στους υπολογιστές του πυρηνικού εργοστασίου τα δεδομένα της προηγούμενης φυσιολογικής δραστηριότητας που είχε καταγράψει και όχι τα δεδομένα της πραγματικής. Αυτό είχε ως αποτέλεσμα οι φυγοκεντρητές να καταστρέφονται, αλλά οι μηχανικοί να μην γνωρίζουν την αιτία. Μπορεί το Stuxnet να ήταν μια λιγότερο αναίμακτη λύση σε σύγκριση με την επιλογή στρατιωτικής εισβολής στο Ιράν, ωστόσο αυτό δεν σημαίνει ότι η λύση αυτή δεν ενείχε σοβαρούς κινδύνους και συνέπειες.*»

Το θέμα της κυβερνοτρομοκρατίας απασχολεί το σύνολο των Υπηρεσιών Δίωξης και Ασφάλειας όλου του κόσμου, αφού όσο η εξάρτηση των κρατών από τα πληροφοριακά συστήματα αυξάνει, τόσο μεγαλύτερες θα είναι οι συνέπειες από τα κυβερνοτρομοκρατικά χτυπήματα. Ειδικά οι Υπηρεσίες Πληροφοριών και Δίωξης των Η.Π.Α. προβληματίζονται ιδιαίτερα με την κυβερνοτρομοκρατική απειλή και υποστηρίζουν ότι σταδιακά οι τρομοκρατικές επιθέσεις θα πραγματοποιούνται είτε αποκλειστικά είτε συνδυαστικά με τη χρήση υψηλής τεχνολογίας (Κικίλιας, 2008).

Τέλος, σύμφωνα με τον Mike Morell, τον πρώην αναπληρωτή διευθυντή της CIA, η ικανότητα των τρομοκρατών να επικοινωνούν μέσω κρυπτογραφημένων καναλιών αποτελεί τεράστιο πρόβλημα λέγοντας στο CBS: «*Πιστεύω ότι θα ξεκινήσει ένας καινούργιος δημόσιος διάλογος σχετικά με την ισορροπία ασφάλειας και προσωπικών δεδομένων*», ενώ τον τελευταίο χρόνο, οι Ευρωπαϊκές κυβερνήσεις πιέζουν τους τεχνολογικούς κολοσσούς, όπως Google, Facebook και Twitter, να δημιουργήσουν «πίσω πόρτες» στα συστήματά τους, από τις οποίες θα έχουν πρόσβαση στα κρυπτογραφημένα εργαλεία τους αν και, κάτι τέτοιο θα αποδυναμώσει την ασφάλεια της κρυπτογράφησης και θα υπονομεύσει την εμπιστοσύνη στο Internet, προειδοποιούν οι ειδικοί (Αγγελέτου, 2015).

2.4 Παιδική Πορνογραφία

Η «πορνογραφία» είναι ένας ευρύς όρος που γενικά αναφέρεται σε κάποιου είδους σεξουαλικό περιεχόμενο, ωστόσο, το Διαδίκτυο περιλαμβάνει εκατομμύρια ιστοσελίδες που περιγράφουν ή δείχνουν ανθρώπους που εμπλέκονται με σεξουαλικές δραστηριότητες και μεγάλο μέρος αυτής της «ψυχαγωγίας ενηλίκων» μπορεί να το αγοράσει οποιοσδήποτε μέσω εμπορικών ιστοσελίδων ή να έχει σε αυτό το υλικό εύκολη πρόσβαση χωρίς χρέωση (McQuade, 2009: 23). Σύμφωνα με τον McQuade (2009: 24), η παιδική πορνογραφία περιλαμβάνει σεξουαλικά άσεμνες ή προκλητικές εικόνες μη ενηλίκων. Πιο συγκεκριμένα, φωτογραφίες ή ταινίες που περιέχουν γυμνές εικόνες αγοριών ή κοριτσιών και εμπλέκονται σε σεξουαλική δραστηριότητα μεταξύ τους ή με ενήλικες είναι παιδική πορνογραφία. Πολλοί άνθρωποι που εμπλέκονται σε εγκλήματα παιδικής πορνογραφίας είναι παιδεραστές - ενήλικες σεξουαλικοί παραβάτες - που αναζητούν ακατάλληλες σωματικές αλληλεπιδράσεις με παιδιά και το σημερινό προφίλ παιδεραστών έχει ελάχιστα, ακόμη και καθόλου κοινωνικοοικονομικά όρια, δηλαδή μπορούν να εμφανιστούν από όλα τα κοινωνικά στρώματα. Δεδομένου του διεθνούς χαρακτήρα του εμπορίου παιδικής πορνογραφίας, αυτό παρουσιάζει σημαντικές προκλήσεις για την επιβολή του νόμου, καθώς το υλικό που είναι παράνομο σε μια δικαιοδοσία μπορεί να είναι νόμιμο σε μια άλλη (Clough, 2010: 255).

Όπως αναφέρει ο Keshtri (2010: 47): *«υποστηρίζεται ότι η διαδικτυακή παιδική πορνογραφία «μειώνει το κοινωνικό στίγμα» καθώς δεν υπάρχει φυσική παρουσία, γεγονός που εξαλείφει την πιθανότητα συνάντησης με άλλους εγκληματίες που ασχολούνται με την παιδική πορνογραφία (Shelley, 1998). Η έρευνα για τα εγκλήματα στον συμβατικό κόσμο έχει δείξει ότι οι κοινωνικοπολιτισμικές πρακτικές και τα πολιτικά και οικονομικά συστήματα συνδέονται στενά με τα εγκλήματα. Υποθέτουμε, λοιπόν, ότι το αίσθημα ενοχής δεν είναι εξίσου διαδεδομένο στον κάθε δράστη, αφού ο καθένας έχει διαφορετικό κοινωνικοπολιτιστικό υπόβαθρο. Με άλλα λόγια, το ψυχολογικό κόστος ενός εγκλήματος στον κυβερνοχώρο είναι μια συνάρτηση του κοινωνικοπολιτισμικού υπόβαθρου ενός εγκληματία στον κυβερνοχώρο.»*

Αξίζει επίσης να σημειωθεί τι είναι γνωστό για τα θύματα (εκείνα που κακοποιήθηκαν και απεικονίστηκαν) παιδικής πορνογραφίας (οπ. αναφ. οι Yar & Steinmetz, 2019), δηλαδή εκτιμάται ότι τα κορίτσια είναι πιο πιθανό να είναι θύματα παιδικής πορνογραφίας (INHOPE, 2016: 8; IWF, 2017: 4; Seto et κ.λπ., 2018: 20, 22) και ότι η πλειονότητα των παιδιών που εμφανίζονται σε τέτοιο διαδικτυακό υλικό είναι καυκάσιας ή ασιατικής καταγωγής, με πολύ λίγες εικόνες μαύρων παιδιών (INTERPOL, 2018: 40; Seto et al., 2018: 22; Taylor et al., 2001: 96). Μερικές από τις πιο ακραίες παραλλαγές που έχουν προκύψει περιλαμβάνει την παραγωγή και διανομή της πορνογραφίας «βιντεοκασέτας» (ιδίως στο darkweb) που περιλαμβάνει βίαιες πράξεις όπως βασανιστήρια, σεξουαλική επίθεση, βιασμός, ακόμη και δολοφονία που προκαλείται σε άτομα, συμπεριλαμβανομένων παιδιά (Ormsby, 2018: 257–280, οπ. αναφ. Yar & Steinmetz, 2019). Βρήκαν επίσης άλλες μελέτες ότι τα παιδιά είναι πιο πιθανό να κακοποιηθούν από κάποιον που ξέρουν από την οικογένεια ή γνωστούς (Gewirtz-Meydan et al., 2018: 242; Mitchell and Jones, 2013; Seto et al., 2018: 23). Επιπλέον, εξετάζοντας τη σοβαρότητα και το μέγεθος της ψυχολογικής πίεσης που μπορεί να υποστούν τα θύματα, αξίζει να σημειωθούν οι συνέπειες της πορνογραφικής σεξουαλικής εκμετάλλευσης. Τα παιδιά μπορεί να βιώσουν μια σειρά από πολλές αρνητικές συνέπειες ως αποτέλεσμα της σεξουαλικής κακοποίησης, συμπεριλαμβανομένων των διαρκών συναισθημάτων ντροπής, ταπείνωσης, ενοχής και θυμού, πέρα από τα προβλήματα ψυχικής υγείας όπως «διαταραχή

μετατραυματικού στρες, κατάθλιψη, άγχος, επιθετικότητα και κατάχρηση ουσιών», αν και δεν υποφέρουν όλοι από τέτοια μακροπρόθεσμα αποτελέσματα (Domhardt et al., 2015: 476, οπ. αναφ οι Yar & Steinmetz, 2019).

Η χρήση του κυβερνοχώρο, σε αυτή την κατηγορία που εξετάζουμε, πραγματοποιείται για κατοχή, δημιουργία, εισαγωγή, εμφάνιση, δημοσίευση ή διανομή πορνογραφίας (ειδικά παιδική πορνογραφία) ή άλλα άσεμνα υλικά (Schell & Martin, 2004: 30). Τουλάχιστον το 80% αυτών που αγοράζουν παιδική πορνογραφία είναι ενεργά κακοποιητές παιδιών. Επιπλέον, βρέθηκε 36% από παραγωγούς παιδικής πορνογραφίας που χρησιμοποίησαν το αμερικανικό ταχυδρομείο για να εκμεταλλευτούν ένα παιδί να είναι πραγματικοί παιδικοί κακοποιητές. Όσοι δημιουργούν περιεχόμενο παιδικής πορνογραφίας κυμαίνονται στην ηλικία από 10 έως 65 και η παιδική πορνογραφία είναι μια βιομηχανία που μπορεί να φτάσει 2–3 δισεκατομμύρια δολάρια ετησίως (Posey, 2003, οπ. αναφ. οι Schell & Martin, 2004: 40). Ο νόμος ορίζει την παιδική πορνογραφία ως οποιαδήποτε οπτική απεικόνιση σεξουαλικής συμπεριφοράς που αφορά ανήλικο, δηλαδή άτομα κάτω των 18 ετών.

Καθώς η ψηφιακή τεχνολογία έχει γίνει ευρύτερα διαθέσιμη, και το Διαδίκτυο πιο διαδεδομένο, έχει σημειωθεί αντίστοιχη αύξηση στον αριθμό των διώξεων για αδικήματα παιδικής πορνογραφίας. Ενώ αυτό εξηγείται εν μέρει από την αλλαγή των προτεραιοτήτων των υπηρεσιών επιβολής του νόμου, αυτή είναι αναμφίβολα μια απάντηση στη διάδοση της παιδικής πορνογραφίας στο Διαδίκτυο (Clough, 2010: 247). Η ικανότητα παραγωγής παιδικής πορνογραφίας ενισχύεται σημαντικά από το γεγονός ότι οι ψηφιακές εικόνες μπορούν να παραχθούν φθηνά χωρίς την ανάγκη εξωτερικής επεξεργασίας και να αναπαραχθούν χωρίς μείωση της ποιότητας. Οι εικόνες κακοποίησης παιδιών μπορούν επίσης να μεταδοθούν σε πραγματικό χρόνο μέσω της χρήσης webcams ή άμεσων μηνυμάτων, μερικές φορές κατόπιν αιτήματος και καθοδήγησης των πελατών που πληρώνουν (Clough, 2010: 249). Το παγκόσμιο εμπόριο παιδικής πορνογραφίας μπορεί επίσης να είναι πολύ επικερδές, οδηγώντας στη συμμετοχή ομάδων οργανωμένου εγκλήματος τόσο στην παραγωγή όσο και στη διανομή, πιο συγκεκριμένα, το 2006, εκτιμήθηκε ότι υπήρχαν περισσότεροι από 100.000 ιστότοποι που προσφέρουν παιδική πορνογραφία (Clough, 2010: 250).

Σύμφωνα με το thorn.org (2021) Όσοι επιδιώκουν ή συμμετέχουν επί του παρόντος στην εκμετάλλευση παιδιών μπορούν να συνδεθούν σε δίκτυα και φόρουμ του Διαδικτύου για να πουλήσουν, να μοιραστούν και να ανταλλάξουν υλικό και αυτές οι αλληλεπιδράσεις διευκολύνονται μέσω διαφόρων μορφών τεχνολογίας διαδικτύου, συμπεριλαμβανομένων ιστότοπων, ηλεκτρονικού ταχυδρομείου, άμεσων μηνυμάτων, συνομιλίας αναμετάδοσης Διαδικτύου, ομάδων συζήτησης, δικτύων peer-to-peer, ιστότοπων διαδικτυακών τυχερών παιχνιδιών, ιστότοπων κοινωνικής δικτύωσης και ανωνυμοποιημένων δικτύων.

Επίσης, το κυβερνοέγκλημα αυξήθηκε κατά την διάρκεια της πανδημίας. Η επικεφαλής της Europol, Καθρίν ντε Μπολ, ανακοίνωσε ότι η αύξηση στις δραστηριότητες παιδόφιλων καταγγέλθηκε από τις εθνικές αρχές επιβολής του νόμου των 27 χωρών της ΕΕ που διαπίστωσαν μεγαλύτερη πρόσβαση σε παράνομες ιστοσελίδες και έκλεισαν περισσότερες διαδικτυακές πλατφόρμες για την ανταλλαγή υλικού σεξουαλικού περιεχομένου με παιδιά και επιπλέον, οι αξιωματούχοι της Europol κατάφεραν να εντοπίσουν πολλούς, οι οποίοι αναζητούσαν τρόπους να συνομιλήσουν με ανήλικους στον αποκαλούμενο «σκοτεινό ιστό» (dark web), που χρησιμοποιείται ευρέως για παράνομες δραστηριότητες (CNN Greece, 2020). Όσοι εργάζονται για την καταπολέμηση αυτού του είδους κακοποίησης έχουν αρχίσει να χρησιμοποιούν τον όρο "υλικό σεξουαλικής κακοποίησης παιδιών" (CSAM=child sexual abuse material), ο οποίος μεταφέρει με μεγαλύτερη ακρίβεια το περιεχόμενο και συνδέεται ρητά με την πηγή του προβλήματος. Το Καναδικό Κέντρο Παιδικής Προστασίας διαπίστωσε ότι τα παιδιά κάτω των 12 ετών απεικονίζονταν στο 78,30% των εικόνων και των βίντεο που αξιολογήθηκαν από την ομάδα τους και το 63,40% αυτών των παιδιών ήταν κάτω των 8 ετών. Μεταξύ του ίδιου υλικού, διαπίστωσαν ότι το 80,42% των παιδιών ήταν κορίτσια, ενώ το 19,58% ήταν αγόρια (thorn.org, 2021).

«*Τον Μάιο του 2017, το FBI σε συνεργασία με πολλές ευρωπαϊκές αστυνομίες, εξάρθρωσε ένα από τα μεγαλύτερα κυκλώματα οργανωμένης παιδικής πορνογραφίας στο διαδίκτυο μετά από πολύχρονη έρευνα. Συνελήφθησαν οι υπεύθυνοι του ιστότοπου Playpen που λειτουργούσε στο σκοτεινό διαδίκτυο (Dark Web) με περισσότερους από 150.000 χρήστες ανά τον κόσμο. Οι διαχειριστές του ιστότοπου καταδικάστηκαν σε*

ποινές κάθειρξης, ενώ σε διάφορες ευρωπαϊκές χώρες συνελήφθησαν συνολικά 368 ύποπτοι. Ο ιστότοπος Playpen ήταν τεχνικά δομημένος με τέτοιο τρόπο ώστε επέτρεπε στους χρήστες του να έχουν εύκολη πρόσβαση σε ένα ευρύ φάσμα υλικού παιδικής πορνογραφίας και σεξουαλικής κακοποίησης παιδιών. Ένα τμήμα του επικεντρώνονταν αποκλειστικά σε νήπια, ένα άλλο στην αιμομιξία και πολλά άλλα σε διάφορα φετίχ με παιδιά» (Europol, "Major online child sexual abuse operation", Media Release, 5.5.2017, οπ. αναφέρει ο Δρ. Στεργιούλης, 2020).

Τέλος, οι Yar & Steinmetz (2019) συμπεραίνουν ότι: «Ενώ η παιδική πορνογραφία δεν είναι ένα φαινόμενο μοναδικό στο διαδίκτυο, η εμφάνισή της στο διαδίκτυο εντείνει τα ρυθμιστικά προβλήματα, καθώς το διαδίκτυο επιτρέπει την κυκλοφορία τέτοιων αναπαραστάσεων που εκτείνονται σε εδαφικά και πολιτιστικά πλαίσια, με τις διαφορετικές ηθικές τους αρχές σχετικά με τις αποδεκτές και απαράδεκτες επικοινωνίες. Τα προβλήματα με τον εντοπισμό προσβλητικού υλικού, κρυμμένα πίσω από προστατευτικά τείχη προστασίας και κωδικούς πρόσβασης, αυξάνουν την πρόκληση για τις υπηρεσίες επιβολής του νόμου. Έχουν σημειωθεί σημαντικές πρόοδοι προς τη διεθνή εναρμόνιση και συνεργασία σε σχέση με την αντιμετώπιση της παιδικής πορνογραφίας, αντανακλώντας τον αυξανόμενο βαθμό παγκόσμιας ηθικής συναίνεσης επί του θέματος. Ωστόσο, εξακολουθούν να υπάρχουν σημαντικές διαφορές σε θέματα όπως αυτό που μετράει ως «άσεμνη» ή «απρεπής» εικόνα ενός παιδιού, το οποίο μετράει ως «παιδί», αν αντικείμενα όπως εικόνες που δημιουργούνται από υπολογιστή, ψευδοφωτογραφίες και κινούμενα σχέδια θα πρέπει να περιλαμβάνονται στους νόμους κατά της πορνογραφίας και τι είδους κυρώσεις πρέπει να ισχύουν για όσους παράγουν, διαδίδουν ή κατέχουν απαγορευμένες εικόνες.»

2.5 Παραβίαση πνευματικών δικαιωμάτων

Η αυτολεξεί αντιγραφή κειμένου κάποιου άλλου χωρίς την προσθήκη εισαγωγικών και μιας παραπομπής σε κείμενο για την επίδειξη ιδιοκτησίας είναι παραβίαση πνευματικών δικαιωμάτων καθώς και λογοκλοπή, και η παράφραση (δηλαδή η έκφραση των ιδεών των άλλων με δικά του λόγια) χωρίς να δίνει κανείς εύσημα σε

έναν συγγραφέα για τις αρχικές του ιδέες με παραπομπή σε κείμενο συνιστά επίσης λογοκλοπή και παραβίαση πνευματικών δικαιωμάτων (McQuade, 2009: 1). Πιο συγκεκριμένα, Η παραβίαση πνευματικών δικαιωμάτων συμβαίνει όταν ένα άτομο εκτός από τον ιδιοκτήτη της πνευματικής ιδιοκτησίας χρησιμοποιεί ένα έργο, όπως από ένα άρθρο, κείμενο σε ένα βιβλίο, μια εικόνα, πληροφορίες, λογισμικό ή μουσική από το Διαδίκτυο, με τρόπο που δεν δίνει πίστωση ή δεν καταβάλλει δικαιώματα στον δημιουργό (McQuade, 2009: 31).

Ωστόσο, υπάρχουν μερικοί πιστεύουν ότι τα πάντα στον Παγκόσμιο Ιστό είναι δημόσια και είναι ελεύθερα να χρησιμοποιηθούν με οποιονδήποτε τρόπο αποφασίζει ένα άτομο. Η ευρεία διάδοση και χρήση του Διαδικτύου έχει ως αποτέλεσμα την εκθετική αύξηση του διαθέσιμου περιεχομένου και ως εκ τούτου είναι πολύ εύκολο για κάποιον άλλο εκτός από τον ιδιοκτήτη-δημιουργό να αντιγράψει και να επικολλήσει κείμενο, εικόνες και άλλο υλικό για περαιτέρω χρήση. Παρ' όλα αυτά, οι νόμοι και οι οδηγίες παραβίασης πνευματικών δικαιωμάτων ισχύουν για πόρους στο Internet, όπως συμβαίνει σε ένα βιβλίο, άρθρο, βίντεο ή μουσική (McQuade, 2009: 32). Αν και δεν είναι «απάτη» κυριολεκτικά, , η παραβίαση ποινικών δικαιωμάτων πνευματικής ιδιοκτησίας μπορεί να θεωρηθεί συναφές αδίκημα, το οποίο προκύπτει από τη μη εξουσιοδοτημένη παρέμβαση στα δικαιώματα ιδιοκτησίας άλλου (Clough, 2010: 221). Ένα από τα σύγχρονα εργαλεία που έχουν κατασκευαστεί για αυτό τον λόγο είναι και το Turnitin. Το εργαλείο αυτό, βασίζεται στο Web και παίρνει μια φοιτητική εργασία που αποστέλλεται στη βάση δεδομένων της, δημιουργεί έναν ψηφιοποιημένο αλγόριθμο του χαρτιού και τα web-bots το κυκλοφορούν στο Διαδίκτυο για να ελέγξουν για ακριβείς αντιστοιχίσεις κειμένου, στην συνέχεια δημιουργείται μια αναφορά που εμφανίζει μια λίστα πηγών από ιστοσελίδες, από τις θέσεις όπου βρέθηκαν οι πληροφορίες, παρέχοντας συνδέσεις που μπορούν να ελεγχθούν για τυχόν περιπτώσεις πιθανής παραβίασης πνευματικών δικαιωμάτων (McQuade, 2009: 2).

Ο McQuade (2009: 129) παρακάτω περιγράφει πως μια μεγάλη επιχείρηση σαν το Napster ουσιαστικά παραβίασε τους κανόνες πνευματικών δικαιωμάτων. Το αρχικό Napster ήταν ένα πρόγραμμα κοινής χρήσης αρχείων που αναπτύχθηκε από τον

Shawn Fanning ενώ φοιτούσε στο Βορειοανατολικό Πανεπιστήμιο της Βοστώνης. Ο Fanning ήθελε μια ευκολότερη μέθοδο λήψης μουσικής από την αναζήτηση φόρουμ συνομιλίας αναμετάδοσης Διαδικτύου (IRC). Μετά τη δημιουργία του Napster, ο Fanning αποφάσισε να το ξεκινήσει ως επιχείρηση και ίδρυσε ένα γραφείο και μια εκτελεστική ομάδα στο San Mateo της Καλιφόρνια, τον Σεπτέμβριο του 1999. Η επιχείρηση ήταν εξαιρετικά επιτυχημένη και, στο αποκορύφωμά της, η Napster είχε 80 εκατομμύρια εγγεγραμμένους χρήστες. Το Napster θεωρείται ευρέως ως ένα από τα πρώτα ομότιμα (p2p) συστήματα διαμοιρασμού αρχείων που διατίθενται στο Διαδίκτυο. Το Napster ασχολήθηκε αποκλειστικά με τη μουσική και επέτρεψε στους χρήστες να αναζητούν αρχεία μουσικής MP3 που είναι αποθηκευμένα στους υπολογιστές άλλων ανθρώπων που βρίσκονται οπουδήποτε στον κόσμο. Η τεχνολογία p2p επέτρεψε τη μεταφορά ακριβών αντιγράφων των περιεχομένων των ψηφιακών αρχείων μουσικής μεταξύ των χρηστών χωρίς να τηρούν τις αξιώσεις πνευματικών δικαιωμάτων. Ωστόσο, όταν δισκογραφικές εταιρείες και μουσικοί καλλιτέχνες όπως ο Dr. Dre και οι Metallica ανακάλυψαν ότι οι χρήστες διανέμουν τη μουσική τους πάνω από το Napster χωρίς να πληρώνουν δικαιώματα που οφείλονται ξεκίνησε δικαστικός αγώνας. Το 2000, η A&M Records και αρκετές άλλες εταιρείες ηχογράφησης συμμετείχαν στην έναρξη αγωγής κατά της Napster για παραβίαση πνευματικών δικαιωμάτων (βλ. A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004, 9th Cir. [2001], οπ. αναφ. ο McQuade, 2009: 129).

Παραδοσιακά η προστασία της πνευματικής ιδιοκτησίας στο διεθνές και στο κοινοτικό δίκαιο πνευματικής ιδιοκτησίας διακρίνεται από αυτήν των συγγενικών δικαιωμάτων. Ενώ η πνευματική ιδιοκτησία αφορά τα πρωτότυπα έργα του πνεύματος (όπως έργα λογοτεχνικά, καλλιτεχνικά κ.α.) και χορηγείται στους δημιουργούς αυτών, η προστασία των συγγενικών δικαιωμάτων αφορά στις συμβολές προσώπων που συνεισφέρουν στη διάδοση των έργων, όπως οργανωτικής, επιχειρηματικής, οικονομικής ή τεχνικής φύσεως συμβολές και τέλος δικαιούχος πνευματικών δικαιωμάτων είναι ο δημιουργός ή ο δικαιούχος αποκλειστικής άδειας των δικαιωμάτων (Europa EU, 2021). Στην Ελλάδα μάλιστα για την αντιμετώπιση της online προσβολής Δικαιωμάτων Πνευματικής Ιδιοκτησίας μόλις στις 3 Σεπτεμβρίου

2018 η Επιτροπή για τη Διαδικτυακή Προσβολή Δικαιωμάτων Πνευματικής Ιδιοκτησίας ξεκίνησε να λειτουργεί και να δέχεται αιτήσεις για προστασία πνευματικών έργων και συγγενικών δικαιωμάτων από διαδικτυακές προσβολές (lawspot.gr, 2018).

Η αυξανόμενη σημασία του Διαδικτύου (όπως έχουμε ήδη αναφέρει πολλές φορές λόγω της μεγάλης επίδρασης σε πολλούς τομείς στο Παγκόσμιο Ιστό) έχει δημιουργήσει νέα εμπόδια για τους κατόχους δικαιωμάτων πνευματικής ιδιοκτησίας και είναι ευκολότερο από ποτέ να έχουν πρόσβαση σε υλικό που προστατεύεται από πνευματικά δικαιώματα από εταιρείες σε όλο τον κόσμο και η δημιουργία νέων τεχνολογιών έχει ξεπεράσει την ικανότητα του ρυθμιστικού περιβάλλοντος να διασφαλίζει ότι τα πνευματικά δικαιώματα ισχύουν για νέες μορφές (Kenton, 2020). Υπάρχουν πολλοί τύποι και μορφές παραβίασης πνευματικών δικαιωμάτων και παρακάτω είναι μερικά παραδείγματα δραστηριοτήτων που θα συνιστούσαν παραβίαση πνευματικών δικαιωμάτων εάν τις πραγματοποιήσετε χωρίς πρώτα να λάβετε άδεια από τον κάτοχο, τον δημιουργό ή τον κάτοχο του υλικού που προστατεύεται από πνευματικά δικαιώματα (Layton, 2021):

- Εγγραφή ταινίας σε κινηματογράφο.
- Δημοσίευση βίντεο το οποίο διαθέτει λέξεις ή τραγούδια που προστατεύονται από πνευματικά δικαιώματα.
- Χρήση εικόνων που προστατεύονται από πνευματικά δικαιώματα.
- Χρήση τραγουδιών που προστατεύονται από πνευματικά δικαιώματα μιας μουσικής ομάδας
- Τροποποίηση εικόνας και, στη συνέχεια, δημοσίευσή της χωρίς αναφορά στην πρωτότυπη πηγή
- Δημιουργία εμπορευμάτων προς πώληση που διαθέτουν λέξεις ή εικόνες που προστατεύονται από πνευματικά δικαιώματα .
- Λήψη μουσικής ή ταινιών χωρίς πληρωμή για τη χρήση τους.
- Αντιγραφή οποιουδήποτε λογοτεχνικού ή καλλιτεχνικού έργου χωρίς άδεια ή γραπτή συμφωνία.

Τα πιο σημαντικά στοιχεία, λοιπόν, που πρέπει να δοθεί έμφαση σχετικά με την παραβίαση πνευματικών δικαιωμάτων αποτελούν τα εξής (Kenton, 2020):

- Παραβίαση πνευματικών δικαιωμάτων είναι η χρήση ή η παραγωγή υλικού που προστατεύεται από πνευματικά δικαιώματα χωρίς την άδεια του κατόχου των πνευματικών δικαιωμάτων.
- Τα άτομα και οι εταιρείες που αναπτύσσουν νέα έργα εγγράφονται για την προστασία των πνευματικών δικαιωμάτων για να διασφαλίσουν ότι μπορούν να επωφεληθούν από τις προσπάθειές τους.

- Σε άλλα μέρη μπορεί να χορηγηθεί άδεια χρήσης των έργων αυτών μέσω ρυθμίσεων αδειοδότησης ή αγοράς των έργων από τον κάτοχο των πνευματικών δικαιωμάτων.

Με άλλα λόγια, η πνευματική ιδιοκτησία και η παραβίαση πνευματικών δικαιωμάτων είναι κλοπή - λαμβάνοντας ό, τι δεν ανήκει στον δράστη της παράκαμψης κρυπτογράφησης, στερώντας έτσι από τους κατόχους πνευματικών δικαιωμάτων δικαιώματα για την πώληση των προϊόντων τους (Schell & Martin, 2004: 72)

2.6 Πειρατεία

Πειρατεία αποτελεί αντιγραφή προστατευμένου λογισμικού χωρίς εξουσιοδότηση (Schell & Martin, 2004: 3). Η πρακτική της δημιουργίας αντιγράφων τέτοιων προστατευόμενων από το δικαίωμα του δημιουργού έργων αναφέρεται ως «πειρατεία» και συνήθως διαπράττεται από τους πολίτες προκειμένου να αποφευχθεί η καταβολή χρημάτων στον δημιουργό και τον εκδότη ή τον διανομέα υλικού που προστατεύεται από πνευματικά δικαιώματα (McQuade, 2009: 108). Στην ουσία, η πειρατεία ισοδυναμεί με ακριβώς μια τέτοια παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας. Στις τρέχουσες χρήσεις, η πειρατεία αναφέρεται στη μη εξουσιοδοτημένη αντιγραφή και διανομή (μερικές φορές, αν και όχι απαραίτητα, για εμπορικό όφελος) περιεχομένου που προστατεύεται από πνευματικά δικαιώματα (Yar & Steinmetz, 2019).

Ένας σημαντικός παράγοντας για την εξήγηση αυτής της αύξησης της πειρατείας στο διαδίκτυο είναι η ταχεία επέκταση του ίδιου του διαδικτύου (Yar & Steinmetz, 2019). Επιπλέον, η πειρατεία είναι άμεσα συνδεδεμένη με την παραβίαση πνευματικών δικαιωμάτων, όπως αναλύσαμε στην προηγούμενη ενότητα. Πιο συγκεκριμένα, σύμφωνα με τον McQuade (2009: 143), *η ψηφιακή πειρατεία, που μερικές φορές αναφέρεται ως «λαθρεμπόριο», είναι μια μορφή παραβίασης των δικαιωμάτων πνευματικής ιδιοκτησίας και μια μέθοδος παράνομης απόκτησης και διανομής λογισμικού, παιχνιδιών, βίντεο, μουσικής και άλλων μέσων ενημέρωσης μέσω της χρήσης υπολογιστικών και τηλεπικοινωνιακών συσκευών. Αυτό περιλαμβάνει την αναπαραγωγή και διανομή υλικού που προστατεύεται από πνευματικά δικαιώματα σε οποιαδήποτε μορφή χωρίς τη συγκατάθεση του κατόχου των πνευματικών δικαιωμάτων. Αυτό το υλικό μοιράζεται συχνά μέσω του Διαδικτύου μέσω δικτύων κοινής χρήσης αρχείων ή /και μέσω ομότιμων δικτύων (p2p), καθώς και σε πειρατικούς διακομιστές. Κάθε αρχείο που παρέχεται από διακομιστές που φιλοξενούνται μπορεί να οδηγήσει σε εκατομμύρια λήψεις. Η ψηφιακή πειρατεία λαμβάνει χώρα και εκτός του Διαδικτύου. Για παράδειγμα, τα φυσικά αντίγραφα πειρατικών DVD πωλούνται παράνομα σε πολλές πόλεις. Η ψηφιακή πειρατεία έχει καταστεί ένα αρκετά σημαντικό πρόβλημα.*

Σήμερα, μερικές από τις κορυφαίες βιομηχανίες του κόσμου ισχυρίζονται ότι χάνουν δισεκατομμύρια δολάρια κάθε χρόνο λόγω της κλοπής της πνευματικής ιδιοκτησίας τους μέσω του διαδικτύου (Yar & Steinmetz, 2019):

- Μια έκθεση εκτιμά ότι μέχρι το 2022 η ψηφιακή πειρατεία θα περιλαμβάνει έως και 856 δισεκατομμύρια δολάρια της συνολικής αξίας (Frontier Economics, 2017: 8). Οι κύριοι τομείς που επηρεάζονται είναι εκείνοι που παράγουν λογισμικό ηλεκτρονικών υπολογιστών, μουσική, κινηματογραφικές ταινίες και, πιο πρόσφατα, τα βιβλία
- Μεταξύ 2004 και 2009, 30 δισεκατομμύρια τραγούδια μεταφορτώθηκαν παράνομα από το διαδίκτυο και ότι μόνο το 37 τοις εκατό της μουσικής που καταναλώνεται από τους Αμερικανούς πληρώνεται στην πραγματικότητα (RIAA, 2012 οπ. αναφ. οι Yar & Steinmetz, 2019).

- Η βιομηχανία λογισμικού υπολογιστών διεκδικεί τις μεγαλύτερες οικονομικές απώλειες στην πειρατεία. Σε μια πρόσφατη έκθεση, η Business Software Alliance (BSA) ισχυρίστηκε ότι περισσότερο από το ήμισυ του συνόλου του λογισμικού που εγκαταστάθηκε και χρησιμοποιήθηκε σε συστήματα παγκοσμίως δεν είχε άδεια. Υπολόγισαν ότι η αξία αυτού του λογισμικού χωρίς άδεια ήταν 52,24 δισεκατομμύρια δολάρια (BSA, 2016: 6-7 οπ. αναφ. οι Yar & Steinmetz, 2019).

- Το 2005, η Ένωση Κινηματογραφικών Ταινιών της Αμερικής (MPAA), μια εμπορική ομάδα για κινηματογραφικά στούντιο, υπολόγισε ότι έχασε 2,3 δισεκατομμύρια δολάρια παγκοσμίως από την πειρατεία στο Διαδίκτυο (MPAA, 2005 οπ. αναφ. ο McQuade 2009: 143).

Σήμερα, η ευαισθητοποίηση του κοινού για την προστασία της πνευματικής ιδιοκτησίας έχει αυξηθεί και εν ολίγοις, τα κανονιστικά και γνωστικά ιδρύματα κατά του εγκλήματος στον κυβερνοχώρο είναι πιθανό να είναι ισχυρότερα σε μια κοινωνία που έχει πιο έμπειρους καταναλωτές και επιχειρήσεις από ό, τι σε μια κοινωνία με λιγότερο έμπειρους καταναλωτές και επιχειρήσεις (Kshetri, 2010: 111).

Ένα από τα πρώτα παραδείγματα ψηφιακής πειρατείας, που παρουσιάζουν οι Yar & Steinmetz (2019), περιλάμβανε μια μικρή ομάδα ενθουσιωδών υπολογιστών που ονομάζονταν Homebrew Computer Club (HBCC) τη δεκαετία του 1970 (Levy, 1984. Βόζνιακ, 2006): *Αυτή η ομάδα γοητεύτηκε με τους πρώτους υπολογιστές μικροεπεξεργαστών όπως το Altair 8800. Κατά τη διάρκεια αυτής της περιόδου, ο Bill Gates και δύο συνάδελφοί του ανέπτυξαν έναν βασικό διερμηνέα (λογισμικό που επιτρέπει τη χρήση μιας γλώσσας προγραμματισμού σε ένα σύστημα) για το 8800 και δέχτηκαν προπαραγγελίες για να βοηθήσουν στη χρηματοδότηση του έργου. Η κυκλοφορία του διερμηνέα στην αγορά ήταν γεμάτη καθυστερήσεις, οι οποίες απογοήτευσαν τη καταναλωτική βάση του. Ένα αντίγραφο του λογισμικού που διέρρευσε τελικά έφτασε στα μέλη της HBCC που έφτιαχναν με ανυπομονησία αντίγραφα ο ένας για τον άλλον (Levy, 1984). Όταν ο Gates άκουσε για αυτό, έγραψε μια έντονα διατυπωμένη ανοιχτή επιστολή που δημοσιεύθηκε στο ενημερωτικό δελτίο*

της HBCC και καταδίκασε αυτά τα αντίγραφα, χαρακτηρίζοντάς τους πειρατές. Τα μέλη της HBCC δεν έβλεπαν την κατάσταση με τον ίδιο τρόπο, δηλαδή το είχαν ως πράξη απλής ανταλλαγής πληροφοριών, μια ένταση που θα συνέχιζε μεταξύ ιδιοκτητών περιεχομένου και πειρατών κατά τη διάρκεια των επόμενων δεκαετιών.

Ένα από τα πιο αξιοσημείωτα χαρακτηριστικά της πειρατείας στο διαδίκτυο είναι η προφανής πανταχού παρουσία της, δηλαδή αντί να περιορίζεται σε μια μικρή κατηγορία «επαγγελματιών εγκληματιών», η δραστηριότητα πειρατείας φαίνεται να είναι κοινωνικά διαδεδομένη και να αναλαμβάνεται σε τακτική βάση από άτομα που διαφορετικά θα θεωρούσαν τους εαυτούς τους "νομοταγείς πολίτες" (Yar & Steinmetz, 2019). Η συμμετοχή στην παράνομη τηλεφόρτωση υλικού που προστατεύεται από πνευματικά δικαιώματα φαίνεται να καλύπτει άτομα από διάφορες κοινωνικές τάξεις και κοινωνικά στρώματα, οπότε είναι σημαντική η προφανής αντίστροφη σχέση μεταξύ ηλικίας και τάσης διάπραξης αδικημάτων πνευματικής ιδιοκτησίας: όσο μικρότερη είναι η ηλικιακή ομάδα, τόσο πιο πιθανή είναι η συμμετοχή τους (Yar & Steinmetz, 2019).

Στην Ελλάδα μόλις το 2020, με το άρθρο 25 του Νόμου 4708/2020 θεμελιώθηκε η δυνατότητα του dynamic blocking injunction, ενός δυναμικού εργαλείου στην καταπολέμηση της διαδικτυακής πειρατείας (lawspot.gr, 2020). Με τη δημοτικότητα του Διαδικτύου και της τεχνολογίας να εξελίσσεται γρήγορα, όλο και περισσότεροι άνθρωποι χρησιμοποιούν το διαδίκτυο και συχνά οι ιστότοποι πειρατών διαθέτουν διαφημίσεις για να δώσουν στον ιστότοπο μια όψη νομιμότητας, αλλά το πιο σημαντικό για τους εγκληματίες είναι ότι τους δημιουργεί προσοδοφόρα έσοδα (Fact-uk.org, 2021).

Η πειρατεία επηρεάζει αρνητικά κάθε άτομο που εργάζεται σε βιομηχανίες που προαναφέρθηκαν αφού υπάρχουν λιγότερα χρήματα για να επενδυθούν σε νέο λογισμικό, αναπτύσσοντας μουσικούς καλλιτέχνες και ταινίες, και υπάρχει λιγότερη δουλειά για προγραμματιστές, δοκιμαστές, μηχανικούς ήχου και εικόνας, ηθοποιούς, σεναριογράφους, μουσικούς, βοηθούς, σχεδιαστές συνόλων, φύλακες ασφαλείας, καταστήματα, πωλητές, προγραμματιστές ιστότοπων και κάθε άλλο τύπο ατόμου που

συμμετέχει στη δημιουργία, τη συσκευασία, τη διαφήμιση, τη διανομή, την υποστήριξη, την προώθηση ή την αναθεώρηση διάφορων προϊόντων και υπηρεσιών (Webroot, 2021). Ένα προφανές πρόβλημα με αυτό είναι ότι τα επίπεδα πειρατείας που εντοπίζονται, και αντίστοιχα ο αριθμός των ποινικών υποθέσεων και των καταδικαστικών αποφάσεων, εξαρτώνται από το επίπεδο της δραστηριότητας των αρχών επιβολής της σχετικής νομοθεσίας. Ως εκ τούτου, οι εμφανείς αυξήσεις των επιπέδων πειρατείας μπορεί, στην πραγματικότητα, να είναι αποτέλεσμα πιο εντατικοποιημένων μέτρων επιβολής, καθώς η μεγαλύτερη προσοχή από τις αρχές θα οδηγήσει αναπόφευκτα στην αποκάλυψη μεγαλύτερου ποσοστού αδικημάτων. Τέλος, η εμφάνιση της πειρατείας στο διαδίκτυο ως πρόβλημα εγκληματικότητας εξαρτάται με θεμελιώδη τρόπο από τον ισχυρισμό ότι οι άνθρωποι μπορούν και πρέπει να έχουν δικαιώματα ιδιοκτησίας σε σχέση με την έκφραση ιδεών (Yar & Steinmetz, 2019).

2.7 Σωματεμπορία

Εδώ και σχεδόν 30 χρόνια, το ζήτημα της εμπορίας ανθρώπων, το οποίο χαρακτηρίζεται συνήθως ως κατεξοχήν διασυνοριακό έγκλημα, έχει διερευνηθεί και παρατηρηθεί από πολλούς, αναμφισβήτητα με αμφίβολη επιτυχία (Segrave & Vitis, 2017: 28). Μεταξύ άλλων, η Sznitka (2021) εξηγεί: «*Με την ανάπτυξη της τεχνολογίας και τη χρήση των μέσων κοινωνικής δικτύωσης, η αγορά και πώληση ανθρώπων έχει γίνει τόσο εύκολη όσο ένα απλό "κλικ" σε ένα πληκτρολόγιο. Σε ιστότοπους όπως backpage.com, άνδρες, γυναίκες και παιδιά ήταν διαθέσιμοι για "αγορά" με σεξουαλικές πράξεις ως "προϊόν" τους για πώληση. Αυτοί οι ιστότοποι διευκόλυναν περισσότερο από ποτέ τους διακινητές να βρουν θύματα και έχουν καταστήσει τις μορφές πληρωμής σχεδόν μη ανιχνεύσιμες. Αυτό προκαλεί τεράστια ανησυχία, διότι τα θύματα διακινούνται χωρίς τρόπο εντοπισμού εκείνων που πληρώνουν για τις υπηρεσίες τους, γεγονός που καθιστά ακόμη πιο δύσκολο για τις αρχές επιβολής του νόμου να κατηγορήσουν αυτούς τους εγκληματίες. Επιπλέον, οι διακινητές είναι σε θέση να στείλουν ένα "αίτημα φιλίας" και να "follow" σε πιθανά θύματα μέσω διαφόρων εφαρμογών όπως facebook, instagram, twitter κ.λπ.*». Η εμπορία ανθρώπων αναδιαμορφώνεται μέσω των τεχνολογικών εξελίξεων, δια του οποίου, οι τεχνολογίες των πληροφοριών καθιστούν «πολλές πτυχές της εμπορίας ανθρώπων πιο ορατές και

πιο ανιχνεύσιμες, προς το καλύτερο και προς το χειρότερο» (boyd et al. 2011, p.1; see also Musto and boyd 2014; Perer 2012; Sarkar 2015; Vanderschaaf 2013, οπ. αναφ. Segrave & Vitis, 2017: 29).

Το internetsafety101.org (2021) αναφέρει, ότι οι διακινητές χρησιμοποιούν το Διαδίκτυο ως τρόπο στόχευσης ανυποψίαστων και ευάλωτων νέων για δικό τους προσωπικό οικονομικό όφελος, καθώς οι «στόχοι» δεν θεωρούνται ανθρώπινα όντα αλλά απλώς πηγή προσόδου. Σύμφωνα με το F.B.I., η σωματεμπορία είναι η 2η ταχύτερα αναπτυσσόμενη εγκληματική βιομηχανία - ακριβώς πίσω από τη διακίνηση ναρκωτικών. Είναι ένας εύκολος, χαμηλού κινδύνου (πολλοί διακινητές εξακολουθούν να πιστεύουν ότι το υψηλό περιθώριο κέρδους αξίζει τον κίνδυνο ανίχνευσης) και κερδοφόρα βιομηχανία λόγω της τεράστιας καταναλωτικής ζήτησης. Η σωματεμπορία είναι μια μορφή σύγχρονης δουλείας και οι εγκληματίες σεξουαλικής διακίνησης χρησιμοποιούν βία, απειλές, ψέματα, χρήματα, ναρκωτικά και άλλες μορφές εξαναγκασμού για να εξαναγκάσουν ή να αναγκάσουν παιδιά και ενήλικες να συμμετάσχουν σε ανεπιθύμητες σεξουαλικές πράξεις παρά τη θέλησή τους, με αποτέλεσμα οι καταστάσεις που αντιμετωπίζουν τα θύματα σεξουαλικής διακίνησης να ποικίλλουν δραματικά (Sznitka, 2021). Το Craigslist θεωρείται το μεγαλύτερο online site που προσφέρει σεξουαλικές υπηρεσίες γυναικών χωρίς τη θέλησή τους αφού διαθέτει και τομέα ερωτικών υπηρεσιών με διαφημίσεις που έχουν εμπλέξει το site με την πορνεία, την παιδική πορνογραφία και ο «τομέας ερωτικών υπηρεσιών» έχει αλλάξει σε «τομέα για ενήλικες» (Χατζηβασιλείου, 2020).

Οι σωματέμποροι πολλές φορές παράγουν και πορνογραφικό υλικό, το οποίο διακινούν μέσω διαδικτύου, το οποίο έχει ως συνέπεια τα κακόβουλα λογισμικά να πλήττουν servers, οι οποίοι δεν έχουν ασφάλεια και να εγκαθιστούν πορνογραφικό υλικό, διαδίδοντάς το σε άλλους servers, χωρίς να το γνωρίζει καν ο κάτοχος του υπολογιστή και με το πάτημα ενός κουμπιού του ηλεκτρονικού υπολογιστή γίνεται προώθηση εκατομμυρίων αρχείων με υλικό σωματεμπορίας και εμπορίας ανθρώπων (Χατζηβασιλείου, 2020). Τα άτομα που μοιράζονται προσωπικές πληροφορίες σε διαδικτυακές πλατφόρμες είναι εκείνα τα οποία είναι πιο πιθανό να γίνουν στόχος τέτοιων εγκληματιών, ειδικά αν γίνει αντιληπτό ότι αντιμετωπίζουν προβλήματα όπως

«οικονομικές δυσκολίες, χαμηλή αυτοεκτίμηση ή οικογενειακά τους προβλήματα» (Ehc, 2020). Στην συνέχεια, οι διακινητές χρησιμοποιούν τις ιστορίες των στόχων τους ως βάση για καλά προγραμματισμένες επιθέσεις μέσω του Internet, πείθοντάς τους ότι θέλουν να είναι χρήσιμοι ή ότι ενδιαφέρονται για μια σχέση, ωστόσο, τα θύματά τους θα εξαναγκαστούν αργότερα σε σεξουαλική εργασία ή καταναγκαστική εργασία, αφού οι διακινητές καταφέρουν να δημιουργήσουν μια ψευδή αίσθηση εμπιστοσύνης και τους πείσουν να συναντηθούν αυτοπροσώπως (Ehc, 2020).

Κάποια σημαντικά στατιστικά αποτελούν τα παρακάτω (Sznitka, 2021):

- Από το 2007, το National Human Trafficking Hotline, έχει λάβει αναφορές για 22.191 υποθέσεις σεξουαλικής διακίνησης εντός των Ηνωμένων Πολιτειών.
- Το 2016, το Εθνικό Κέντρο αγνοουμένων και κακοποιημένων παιδιών εκτίμησε ότι 1 στους 6 απειλούμενους φυγάδες ήταν πιθανά θύματα σεξουαλικής διακίνησης.
- Ο Διεθνής Οργανισμός Εργασίας εκτιμά ότι υπάρχουν 4,5 εκατομμύρια άνθρωποι παγιδευμένοι σε αναγκαστική σεξουαλική εκμετάλλευση σε όλο τον κόσμο.
- Η σωματεμπορία είναι μια επικερδής βιομηχανία που βγάζει περίπου 99 δισεκατομμύρια δολάρια το χρόνο.
- Περίπου 2 εκατομμύρια παιδιά πέφτουν θύματα εκμετάλλευσης κάθε χρόνο στο παγκόσμιο εμπόριο σεξ.

Όταν ξεκίνησε η ευαισθητοποίηση σχετικά με την εμπορία ανθρώπων και την τεχνολογία, μια σημαντική συνιστώσα της διεθνούς καταπολέμησης της εμπορίας ανθρώπων θεμελιώθηκε στο γεγονός ότι γυναίκες και παιδιά είναι ίσοι απέναντι στον κίνδυνο της σεξουαλικής εκμετάλλευσης (Segrave & Vitis, 2017: 30). Η πιο συχνή μορφή της εμπορίας ανθρώπων που καταλαμβάνει το 79% είναι η γενετήσια εκμετάλλευση (Χατζηβασιλείου, 2020). Η διαιώνιση της ιδέας ότι το διαδίκτυο επιτρέπει στην εμπορία ανθρώπων να παραβεί τα γεωγραφικά σύνορα δημιουργεί την ψευδαίσθηση μιας παντοδύναμης απειλής που τίθεται κυρίως σε ανθρώπους

(γυναίκες) στον Παγκόσμιο Νότο των οποίων η πρόσβαση σε ευκαιρίες μετανάστευσης είναι περιορισμένη (Segrave & Vitis, 2017: 34). Ωστόσο, στο πλαίσιο της διακίνησης της εμπορίας ως τεχνολογικού προβλήματος, οι δρώντες κατά της εμπορίας ανθρώπων έχουν συνδυάσει επιτυχώς την καταπολέμηση της πορνείας, της μετανάστευσης και της ατζέντας για την έννομη τάξη (Segrave & Vitis, 2017: 34). Συμπερασματικά, θα λέγαμε ότι υπάρχει αδήριτη ανάγκη για τη θέσπιση μιας παγκόσμιας νομοθεσίας που να αφορά την σωματεμπορία μέσω διαδικτύου, καθώς τα terabytes του dark web ολοένα και αυξάνονται (Χατζηβασιλείου, 2020).

2.8 Κακόβουλο λογισμικό

Σύμφωνα με τον McQuade (2009:121) το κακόβουλο λογισμικό (Malware) είναι ένας γενικός όρος για μια ποικιλία επιβλαβούς λογισμικού που έχει σχεδιαστεί ειδικά για να επιτίθεται σε συστήματα υπολογιστών, δίκτυα ή δεδομένα και προήλθε από το συνδυασμό των λέξεων στα αγγλικά «malicious» και «software», που χρησιμοποιείται για να περιγράψει ιούς υπολογιστών, σκουλήκια Διαδικτύου, προγράμματα καταγραφής πληκτρολόγησης, rootkits, λογισμικό υποκλοπής spyware, botnets. Παρόλο που υπάρχουν πολλοί διαφορετικοί τύποι κακόβουλου λογισμικού, όλα τα κακόβουλα προγράμματα έχουν ένα κοινό κοινό: για τον τελικό χρήστη ή τον ιδιοκτήτη του συστήματος υπολογιστή που εκτελεί το κακόβουλο λογισμικό, η ύπαρξη του κακόβουλου λογισμικού είναι ανεπιθύμητη, άγνωστη ή επιβλαβής. Οι περισσότερες μορφές κακόβουλου λογισμικού εγκαθίστανται σε συστήματα υπολογιστών. Οι ιοί, το λογισμικό υποκλοπής spyware και τα rootkit μπορούν να βλάψουν τους υπολογιστές ανοίγοντας μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου ή συνημμένα ηλεκτρονικού ταχυδρομείου ή από υπολογιστές χρηστών που επισκέπτονται ψεύτικους ιστότοπους που προσποιούνται ότι είναι νόμιμοι ιστότοποι χωρίς κακόβουλη πρόθεση (McQuade, 2009:121).

Ουσιαστικά, πρόκειται για λογισμικό που έχει σχεδιαστεί για να διεισδύει ή / και να καταστρέφει έναν υπολογιστή χωρίς τη συγκατάθεση του κατόχου και ενώ υπάρχουν πολλοί τύποι κακόβουλου λογισμικού, οι περισσότεροι άνθρωποι γνωρίζουν μόνο δύο: ιούς και σκουλήκια (Brenner, 2010: 20). Στη δεκαετία του 1990

και στις αρχές της δεκαετίας του 2000, το κακόβουλο λογισμικό έτεινε να γράφεται από εφήβους ή μετα-εφήβους χάκερ που είχαν την τάση να κάνουν «κακή» ή να χτίσουν τη φήμη τους ως συγγραφείς κώδικα. Μέχρι το 2007, το φαινόμενο «Willie Sutton» ήταν σε πλήρη εξέλιξη, δηλαδή: Το κακόβουλο λογισμικό είχε γίνει το κυριότερο εργαλείο των επαγγελματιών που το χρησιμοποιούν για να βγάζουν χρήματα κλέβοντας ιδιόκτητες πληροφορίες και άλλους πόρους από τα θύματα, αποσπώντας χρημάτων συνήθως από επιχειρήσεις και κρυπτογράφοντας δεδομένα κρατώντας το για λύτρα (Brenner, 2010: 35). Η διάδοση κακόβουλου λογισμικού μπορεί επίσης να παρομοιαστεί με ένα παραδοσιακό πραγματικό έγκλημα: τον βανδαλισμό και οι νόμοι σχετικά με τον βανδαλισμό, καθιστούν έγκλημα την σκόπιμη καταστροφή «πραγματικής ή προσωπικής ιδιοκτησίας άλλου» χωρίς τη συγκατάθεση του ιδιοκτήτη (Brenner, 2010: 40).

Τα κύριες μορφές κακόβουλου λογισμικού είναι τέσσερις (4), (Bitdefender.gr, 2021):

- **Ransomware:** το Ransomware είναι ένας μικρός ιός υπολογιστών που κρυπτογραφεί όλα τα αρχεία σε έναν μολυσμένο υπολογιστή. Μόλις κρυπτογραφηθεί, ο υπολογιστής είναι άχρηστος επειδή δεν είναι δυνατή η πρόσβαση σε κανένα από τα δεδομένα που είναι αποθηκευμένα σε αυτόν. Εάν ένας υπολογιστής έχει παραβιαστεί από ransomware, τότε ένα μήνυμα θα εμφανιστεί στην οθόνη που θα ζητάει το κλειδί αποκρυπτογράφησης και θα ξεκλειδώσει τα αρχεία του υπολογιστή. Η παγίδα είναι ότι πρέπει να καταβληθεί κάποιο χρηματικό ποσό για να αποκτηθεί το κλειδί. Η πληρωμή λύτρων δεν είναι συνήθως καλή ιδέα, καθώς δεν υπάρχει εγγύηση ότι ο εισβολέας θα δώσει το κλειδί αποκρυπτογράφησης. Αντ ‘αυτού, πρέπει να είναι διασφαλισμένη η δημιουργία ενός αντιγράφου ασφαλείας των αρχείων.
- **Trojans:** πήρε το όνομά του από τον ελληνικό μύθο του Δούρειου Ίππου (Trojan Horse) και είναι μια μορφή κακόβουλου λογισμικού που γλιστρά στον υπολογιστή του θύματος. Μόλις εγκατασταθεί, το trojan δεν κάνει σχεδόν τίποτα μέχρι να ενεργοποιηθεί. Ακριβώς όπως οι στρατιώτες που

κρύβονται στο ξύλινο άλογο, το trojan γλιστρά πίσω από τις άμυνες του υπολογιστή και στη συνέχεια ξεκινά μια επίθεση από μέσα. Αυτή η μορφή κακόβουλου λογισμικού μπορεί να διαγράψει ή να καταστρέψει δεδομένα ή απλώς να λειτουργήσει ως πόρτα, επιτρέποντας στους χάκερ να έχουν πρόσβαση και να χρησιμοποιούν έναν υπολογιστή όταν το επιλέξουν.

- **Spyware:** τα σύγχρονα συστήματα που έχουν σχεδιαστεί για την προστασία των κωδικών πρόσβασης είναι πολύ αποτελεσματικά. Εάν οι χάκερ εισέλθουν σε δίκτυο και κλέψουν μια βάση δεδομένων, οι περισσότεροι από τους κωδικούς πρόσβασης δεν μπορούν να χρησιμοποιηθούν επειδή είναι κρυπτογραφημένοι. Το λογισμικό υποκλοπής spyware έχει σχεδιαστεί για να τους βοηθά να τους αποκρυπτογραφήσουν. Μόλις εγκατασταθεί, το λογισμικό υποκλοπής spyware ξεκινά τη συλλογή και καταγραφή όλων των ειδών πληροφοριών, συμπεριλαμβανομένων των ιστότοπων που μπορεί να έχει επισκεφτεί ένας χρήστης. Το spyware στη συνέχεια στέλνει σταδιακά αυτές τις πληροφορίες στον εγκληματία που τις ελέγχει. Αυτά τα δεδομένα επιτρέπουν στον εισβολέα να διαβάσει τους κωδικούς πρόσβασής του θύματος και να τους χρησιμοποιήσει για να εισέλθει στους διαδικτυακούς λογαριασμούς του.

- **Worms:** το worm είναι ένας τύπος ιού υπολογιστή που έχει σχεδιαστεί για να αντιγράφεται σε έναν μολυσμένο υπολογιστή και, στη συνέχεια, να μεταδίδει τη μόλυνση σε άλλους υπολογιστές στο ίδιο δίκτυο. Αυτό σημαίνει ότι μια μόλυνση σε κάποιον οικιακό υπολογιστή μπορεί να εξαπλωθεί γρήγορα στον φορητό υπολογιστή (και σε οποιοδήποτε άλλο σύστημα είναι συνδεδεμένο στο ίδιο δίκτυο). Ένα worm μπορεί επίσης να χρησιμοποιήσει την ηλεκτρονική ατζέντα κάποιου χρήστη για να στείλει email στις επαφές του, ενδεχομένως για να μολύνει και τους υπολογιστές τους. Η μόλυνση μπορεί να μην προκαλέσει απαραίτητα βλάβη ή διαγραφή αρχείων, αλλά μπορεί να προκαλέσει επιβράδυνση του υπολογιστή και του δικτύου.

Κάθε τύπος κακόβουλου λογισμικού έχει τον δικό του μοναδικό τρόπο πρόκλησης καταστροφών και τα περισσότερα στηρίζονται σε κάποια ενέργεια από τους χρήστες. Ορισμένα στελέχη παραδίδονται μέσω email μέσω συνδέσμου ή εκτελέσιμου αρχείου, ενώ άλλοι παραδίδονται μέσω άμεσων μηνυμάτων ή κοινωνικών μέσων, ακόμα και τα κινητά τηλέφωνα είναι ευάλωτα σε επιθέσεις (Forcepoint.com, 2021). Επιπλέον, σύμφωνα με το lawspot.gr (2017) περίπου το 80% των επιχειρήσεων στην Ευρώπη έχουν βιώσει τουλάχιστον ένα περιστατικό παραβίασης της ασφάλειας στον κυβερνοχώρο και πολλά από αυτά τα περιστατικά δεν ανιχνεύονται ή δεν αναφέρονται στις αρχές. Οι ευρωβουλευτές έχουν κάνει επίσης αναφορά στην παγκόσμια κυβερνοεπίθεση του ransomware «WannaCry», η οποία έπληξε χιλιάδες ηλεκτρονικούς υπολογιστές σε περίπου 100 χώρες και πολλές οργανώσεις, συμπεριλαμβανομένης της Εθνικής Υπηρεσίας Υγείας του Ηνωμένου Βασιλείου.

Όσον αφορά το Ransomware, σύμφωνα με την Europol (2021), είναι μία κατηγορία κακόβουλου λογισμικού που εμποδίζει ή περιορίζει την πρόσβαση των χρηστών στα συστήματα ή τις συσκευές τους, απαιτώντας να πληρώσουν λύτρα, χρησιμοποιώντας συγκεκριμένους διαδικτυακούς τρόπους πληρωμής και εντός καθορισμένης προθεσμίας, προκειμένου να ανακτήσουν τον έλεγχο των δεδομένων τους. Το Crypto ransomware, από την άλλη, είναι ένας τύπος κακόβουλου λογισμικού που κρυπτογραφεί δεδομένα χρηστών και απαιτεί λύτρα, συνήθως πληρωτέα με Bitcoin cryptocurrency, για την αποκρυπτογράφηση των δεδομένων. Πιο συγκεκριμένα, το WannaCry είναι μια παραλλαγή crypto ransomware που έχει εξαπλωθεί μαζικά σε όλο τον κόσμο από τις 12 Μαΐου 2017. Είναι επίσης γνωστή ως WannaCrypt, WanaCrypt0r, WRrypt και WCRY. Άρα, έχει δύο βασικά χαρακτηριστικά: 1) αποτελεί έναν ιό σκουλήκι (worm) που έχει τη δυνατότητα να εξαπλωθεί μέσα σε δίκτυα χωρίς αλληλεπίδραση με τον χρήστη και 2) μια παραλλαγή ransomware που κρυπτογραφεί αρχεία χρηστών και στη συνέχεια ζητά χρήματα για την αποκρυπτογράφηση των αρχείων.

Οι κακόβουλες επιθέσεις δεν περιορίζονται μόνο σε εγκληματικές ομάδες αλλά επεκτείνεται και σε επίπεδο κρατών. Οι πυρηνικές εγκαταστάσεις του Ιράν έγιναν στόχος κυβερνοεπίθεσης με το σκουλήκι Stuxnet. Ο στόχος του Stuxnet είναι να

«καταστρέψει» τον πυρηνικό φυγοκεντρητή του Ιράν επηρεάζοντας συγκεκριμένες εντολές για τον έλεγχο της ταχύτητας των οργανων ελέγχου. Με αυτόν τον τρόπο, οι Ηνωμένες Πολιτείες είχαν ελπίδες να αποτρέψουν πιθανές στρατιωτικές επιθέσεις από το Ισραήλ. Πιο συγκεκριμένα, οι κωδικοί υπολογιστών προκάλεσαν σοβαρή ζημιά παρεμβαίνοντας στους ελεγκτές φυγοκέντρησης για να τους βγάλουν εκτός ελέγχου (και ακόμη και να μεταδώσουν ψευδή μηνύματα πίσω σε εκείνους που τους παρακολουθούσαν, ώστε να μην ανησυχούν μέχρι να είναι πολύ αργά) και το αποτέλεσμα ήταν αυτό που ακούστηκε σαν έκρηξη αργής κίνησης καθώς φυγοκεντρητές συγκρούστηκαν μεταξύ τους (Corera, 2021). Η πυρηνική σύμβαση επιτρέπει στο Ιράν να παράγει και να αποθηκεύει περιορισμένη ποσότητα ουρανίου εμπλουτισμένη σε 3,67%. Το ουράνιο εμπλουτισμένο έως 90% ή περισσότερο μπορεί να χρησιμοποιηθεί για την κατασκευή πυρηνικών όπλων. Από τότε που ο Τραμπ αποχώρησε από τη συμφωνία, το Ιράν έχει εντείνει τις παραβιάσεις του για να αυξήσει την πίεση στις Ηνωμένες Πολιτείες. Έχουν συμπεριλάβει τη λειτουργία προηγμένων φυγοκεντρωτών για τον εμπλουτισμό του ουρανίου, τη συνέχιση του εμπλουτισμού σε 20% συγκέντρωση του πιο σχάσιμου ισότοπου U-235 και την κατασκευή ενός αποθέματος αυτού του υλικού (BBC News, 2021).

Όπως αναφέραμε, το κακόβουλο λογισμικό είναι μία κατηγορία προγραμμάτων Η/Υ που έχουν σχεδιαστεί για να διαταράσσουν ή να παρεμβαίνουν στην κανονική λειτουργία ενός υπολογιστή (Yar & Steinmetz, 2019). Ενώ, παραδοσιακά χρησιμοποιείται για την πρόκληση μη εξουσιοδοτημένης τροποποίησης και εξασθένισης δεδομένων, το κακόβουλο λογισμικό χρησιμοποιείται όλο και περισσότερο για την πρόσβαση σε εμπιστευτικές πληροφορίες για τη διευκόλυνση της απάτης και άλλων αδικημάτων, όπως οι λεγόμενες «μικτές απειλές», για παράδειγμα η απόκτηση πρόσβασης σε εμπιστευτικά δεδομένα και επικοινωνίες, η δημιουργία ψευδών λογαριασμών ή η απόκτηση πλαστών εγγράφων ταυτοποίησης (Clough, 2010: 32). Η επιχείρηση κακόβουλου λογισμικού — η "διαδικτυακή παραοικονομία του κακόβουλου λογισμικού", όπως την περιέγραψε ένας αναλυτής - εκτιμάται ότι παράγει περισσότερα από 100 δισεκατομμύρια δολάρια σε έσοδα κάθε χρόνο (Brenner, 2010: 63). Το κακόβουλο λογισμικό στο διάστημα δεν είναι πιθανό να γίνει

σημαντικό πρόβλημα, αλλά δείχνει πόσο ευάλωτα είναι τα συστήματά μας σε αυτή την ταχέως εξελισσόμενη απειλή (Brenner, 2010: 36).

2.9 Hacking

Ο ορισμός του «χάκερ» ήταν διαφορετικός και ανά δεκαετίες αλλάζει. Ουσιαστικά, ο όρος αναφέρεται σε ένα άτομο που μπορεί να έχει πρόσβαση σε συστήματα πληροφοριών συμπεριλαμβανομένων των δικτύων υπολογιστών χωρίς άδεια. Η καταστροφή ενός συστήματος υπολογιστή ή η υπέρβαση της εξουσίας του δικτύου θεωρείται μια μορφή ηλεκτρονικής εισβολής. Σύμφωνα με τον ορισμό των ομοσπονδιακών και πολλών νόμων περί εγκλήματος στον κυβερνοχώρο, η παραβίαση των υπολογιστών έχει πλέον επεκταθεί σε άτομα πέραν των εξουσιοδοτημένων δικαιωμάτων τους σε ένα δεδομένο δίκτυο υπολογιστών (McQuade, 2009: 87). Ο όρος «hacker» και πολλά ακόμη πράγματα από την κουλτούρα των χάκερς, προέκυψαν από το Εργαστήριο Τεχνητής Νοημοσύνης του Ινστιτούτου Τεχνολογίας της Μασαχουσέτης στα τέλη του 1950 (Brenner, 2010: 14). Οι βασικές μορφές συμπεριφοράς που ενδέχεται να εμπίπτουν σε αυτήν την κατηγορία εγκλήματος («hacking») δεν είναι αμοιβαία αποκλειόμενες ούτε καθολικά ορισμένες. Μία από τις κύριες προκλήσεις της νομοθεσίας για το έγκλημα στον κυβερνοχώρο είναι να διασφαλιστεί ότι μπορούν να προσαρμοστούν σε διάφορες αλληλεπικαλυπτόμενες και εξελισσόμενες απειλές. Ωστόσο, οι τρεις κύριες κατηγορίες συμπεριφοράς είναι: 1. Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή ή σύστημα υπολογιστή 2. κακόβουλο λογισμικό 3. Επιθέσεις άρνησης υπηρεσίας (Clough, 2010: 28).

Σύμφωνα με τους Yar & Steinmetz (2019) για πολλούς ανθρώπους το έγκλημα στον κυβερνοχώρο και το hacking έχουν γίνει συνώνυμα. Ο δημόσιος λόγος για το χάκερ φαίνεται να προκαλεί φόβο και γοητεία σε ίσο βαθμό. Η προέλευση αυτής της έντονης αντιπαράθεσης μπορεί να γίνει κατανοητή με διάφορους τρόπους. Η πιο απλή εξήγηση των κοινωνικών ευαισθησιών στο hacking τονίζει τον βαθμό απειλής ή κινδύνου που φέρει η δραστηριότητα. Το hacking ξεκίνησε όπως αναφέρει και ο Rioux (White, 2020: 18) από το «building hacking» ένας όρος που προήλθε από την ιδέα να ανεβείς σε στέγες, να εξερευνείς και να ανακαλύπτεις νέα μέρη σε κτήρια ή

και τόπους. Αυτού του είδους η συμπεριφορά ήταν διερευνητική και άνοιγε το μυαλό των ανθρώπων ότι υπήρχαν πράγματα που μπορούσες να κάνεις και μέρη που μπορούσες να πας που οι άνθρωποι δεν περίμεναν ότι υπήρχαν. Από εκεί ξεκίνησε η κουλτούρα. Οι επιθέσεις hacking μπορεί μερικές φορές να φαίνονται σαν το έργο τεράτων από το ψηφιακό βάθος (digital deep?), δηλαδή αναδύονται και, καταπίνουν προσωπικά δεδομένα, αρπάζουν αριθμούς πιστωτικών καρτών, συντρίβουν δίκτυα υπολογιστών και σπέρνουν παραπληροφόρηση, πριν εξαφανιστούν πίσω στο σκοτάδι, αφήνοντας τον πληθυσμό τρομοκρατημένο και αβέβαιο πού θα χτυπήσουν στη συνέχεια (White, 2020: 306). Αυτό έχει δημιουργήσει γόνιμο έδαφος για την αναπτυσσόμενη βιομηχανία κυβερνοασφάλειας, η οποία ισχυρίζεται ότι προσφέρει προστασία από τις επιθέσεις αυτών των τεχνο-τεράτων.

«Επί του παρόντος, πολλές δραστηριότητες που χαρακτηρίζονται ως hacking είναι εξαιρετικά κακόβουλες, με πολλούς σύγχρονους «χάκερ» να έχουν πρόσβαση σε συστήματα πληροφοριών για οικονομικό όφελος ή καταστροφικούς σκοπούς. Οι χάκερ που συμμετέχουν σε παράνομες δραστηριότητες είναι κοινώς γνωστοί ως «χάκερ μαύρου καπέλου», ενώ εκείνοι που χρησιμοποιούν τις δεξιότητές τους για αυτό που πιστεύουν ότι είναι ηθικοί και κατάλληλοι σκοποί είναι γνωστοί ως «χάκερ λευκών καπελών». Ωστόσο, αυτή η διάκριση συχνά ορίζεται κάπως άσχημα και η χρήση του όρου «χάκερ γκρι καπέλων» έχει γίνει όλο και πιο συχνή για να αντικατοπτρίζει τις συχνά θολές ηθικές και νομικές γραμμές που διασχίζονται στη διαδικασία του hacking» (McQuade, 2009: 88). Ο Derek Manky, ερευνητής ασφαλείας στο Fortinet, σημείωσε: «Το hacking έχει κλιμακωθεί από καταστροφικό χαρακτήρα σε οικονομικό κέρδος μέσω ηλεκτρονικού "ψαρέματος", στοχεύοντας ανθρώπους για στοιχεία τραπεζικών λογαριασμών και κλέβοντας λογαριασμούς από εκεί» (πρβλ. Fong, 2008 οπ. αναφ. ο Kshetri, 2010: 23).

Το οργανωμένο έγκλημα υπάρχει σχεδόν από τις πρώτες ημέρες της παραβίασης υπολογιστών και έχει γίνει πλέον πιο συχνό φαινόμενο, καθώς τα μέλη του έχουν συνειδητοποιήσει πόσο πιο ασφαλές είναι να ληστεύουν ανθρώπους και θεσμούς σχεδόν, παρά αυτοπροσώπως (White, 2020: 7). Ίσως το πιο ανησυχητικό από όλα είναι, ότι τα εθνικά κράτη έχουν αρχίσει να επενδύουν αρκετά στο πεδίο παραβίασης

υπολογιστών, προσθέτοντας ομάδες hacking στο οπλοστάσιο των όπλων που διατίθενται στις στρατιωτικές εγκαταστάσεις και τις εγκαταστάσεις πληροφοριών τους (White, 2020: 8). Η φύση της τεχνολογίας και των κοινοτήτων hacking και των ομάδων οργανωμένου εγκλήματος έχουν μειώσει σημαντικά την πολυπλοκότητα της τεχνογνωσίας και της τεχνολογίας του εγκλήματος στον κυβερνοχώρο και τα περισσότερα εργαλεία hacking είναι ευρέως διαθέσιμα στο διαδίκτυο και απαιτούν ελάχιστη ή καθόλου εμπειρία (Kshetri, 2010: 85). Ταυτόχρονα, οι τεχνολογίες hacking βελτιώνονται με ανησυχητικό ρυθμό και οι κυβερνοεγκληματίες ενορχηστρώνουν νέες παραλλαγές της κοινωνικής μηχανικής (Kshetri, 2010: 247).

Σύμφωνα με την Brenner (2010: 55): «*η πειρατεία στον κυβερνοχώρο μπορεί να προκλήθηκε από απλή περιέργεια, ανάλογη με αυτό που παρακίνησε τους αρχικούς χάκερ κεντρικού υπολογιστή. Αλλά η περιέργεια έχει γίνει ένα καθαρά ιδιοσυγκρασιακό φαινόμενο. Οποιοσδήποτε είναι περίεργος για ένα άτομο ή ένα ζήτημα και έχει ορισμένες δεξιότητες υπολογιστών μπορεί να χακάρει υπολογιστές που μπορεί να περιέχουν την απάντηση. Το κίνητρο τώρα είναι καθαρά εγωιστικό. Και επειδή οι υπολογιστές πιθανότατα ανήκουν σε κάποιον άλλο, οι παραβιάσεις - σε αντίθεση με τις παραβιάσεις του κεντρικού υπολογιστή - παραβιάζουν τα δικαιώματα ιδιοκτησίας, αλλά και τα δικαιώματα των διαφόρων ιδιοκτητών υπολογιστών να αποκλείουν άλλους από τα συστήματά τους».* Επιπλέον, κοινότητα hacking χαρακτηρίζεται επίσης από υψηλό βαθμό ανταλλαγής πληροφοριών και τα μέλη της κοινότητας είναι πρόθυμα να βοηθήσουν τους συναδέλφους χάκερ να λύσουν προβλήματα όπως η πρόσβαση σε ένα δρομολογητή και η διέλευση από ένα τείχος προστασίας (Bednarz, 2004 οπ. αναφ. ο Kshetri, 2010: 68). Συνήθως, η ανταλλαγή και η κοινή χρήση εργαλείων και μυστικών hacking πραγματοποιούνται σε κλειστά chat rooms (Acohido & Swartz, 2005 οπ. αναφ. ο Kshetri, 2010: 68).

Το hacking και το έγκλημα στον κυβερνοχώρο περνούν από μια ταχεία μεταβατική φάση και τις τελευταίες δύο δεκαετίες, οι περισσότερες βιομηχανικές χώρες έχουν θεσπίσει πολλούς νόμους για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και έχουν αναπτύξει άλλες ρυθμιστικές υποδομές (Kshetri, 2010: 110). Το hacking είναι ένας όρος με δύο διακριτικές έννοιες. Πρώτον, η πράξη της δημιουργικής

επίλυσης προβλημάτων όταν αντιμετωπίζει σύνθετα τεχνικά προβλήματα και, δεύτερον, παράνομες και συνήθως παράνομες δραστηριότητες που σχετίζονται με μη εξουσιοδοτημένη πρόσβαση ή παρέμβαση σε συστήματα υπολογιστών (Yar & Steinmetz, 2019). Ως εκ τούτου, οι συζητήσεις σχετικά με το hacking αποτελούν παράδειγμα του τι κάνουν οι εγκληματολόγοι και οι κοινωνιολόγοι στη «διαδικασία επισήμανσης» και την «κοινωνική οικοδόμηση της απόκλισης», καθώς υπάρχει ένα ευρύ φάσμα δραστηριοτήτων hacking είναι εμφανές στο διαδίκτυο σήμερα, που κυμαίνονται από την εισβολή υπολογιστών και τη διανομή ιών, μέχρι την καταστροφή του ιστότοπου και την άρνηση υπηρεσίας (Yar & Steinmetz, 2019). Οι κώδικες, οι πολιτικές, οι αρχές, τα πρότυπα και οι διαδικασίες κατά του εγκλήματος στον κυβερνοχώρο είναι πιθανό να αναπτυχθούν με την πάροδο του χρόνου και το παράδειγμα του hacking βοηθά στην εξήγηση των διαδικασιών που στηρίζουν τη σταδιακή ανάπτυξη των γνωστικών ιδρυμάτων κατά του εγκλήματος (Yar & Steinmetz, 2019).

2.10 Προπαγάνδα και χειραγώγηση κοινής γνώμης

Η προπαγάνδα δεν αποτελεί νέο φαινόμενο. Έχει παρατηρηθεί εδώ και αιώνες. Η βασική μορφή στο Διαδίκτυο που λαμβάνει είναι οι ψεύτικες ειδήσεις. Οι ψεύτικες ειδήσεις, λοιπόν, μια μορφή κίτρινου τύπου ή αλλιώς προπαγάνδας με στόχο την παραπληροφόρηση ή και την φάρσα μέσω του παραδοσιακού Τύπου, των ΜΜΕ ή και των social media. Η μέθοδος διάδοσης των fake news έχει αναπτυχθεί τόσο πολύ τον 21ο αιώνα που ακόμη και οι κλασικοί Τύποι, όπως εφημερίδα, περιοδικά και ειδησεογραφικά γραφεία έχουν δημιουργήσει δικούς τους ιστότοπους ενημέρωσης. Επιπλέον, αποτελεί μια τακτική η προπαγάνδα, με την οποία μέσω διάδοσης ψεύτικων δεδομένων και παραπληροφόρησης, πετυχαίνει στόχους ώστε να επηρεάσει τη κοινή γνώμη, δημιουργώντας έτσι μεγάλο πολιτικό ζήτημα. Οι bad actors (κακοί δρώντες) παίζουν τον κυρίαρχο ρόλο εξάπλωσης των fake news.

Το τρίγωνο των ψεύτικων ειδήσεων απεικονίζει τους 3 παράγοντες που βοηθούν στην διάδοση των fake news, δηλαδή (Trend Micro, 2017):

1. Εργαλεία και υπηρεσίες: Στόχος τους είναι να εξαπλωθεί στα social media η πληροφορία, η οποία έχει πουληθεί σε πολλές διαδικτυακές κοινότητες. Τα πιο γνωστά εργαλεία είναι τα paid likes/ followers. Τα πιο ασυνήθιστα αποτελούν κάποιες υπηρεσίες που υπόσχονται να συμπληρώνουν οι ίδιες διάφορα online polls και κάποιοι άλλοι (συνήθως χρηματοδότες) αναγκάζουν τους ιδιοκτήτες ιστοσελίδων να κατεβάσουν ιστορίες. Ένα ακόμη εργαλείο, είναι οι τεχνικές από spammers για να προσελκύσουν χρήστες στο να βλέπουν τις ειδήσεις τους.

2. Κοινωνικά δίκτυα: Η μελέτη των social media βοηθά στην διαμόρφωση μιας εικόνας της σχέσης μεταξύ των bots και αποδεκτών. Μέσα στα κοινωνικά δίκτυα γίνεται η προώθηση μιας εκστρατείας και τα ίδια γνωρίζουν το πεδίο της αλλά και το πως οργανώνεται για να χειραγωγήσει την κοινή γνώμη.

3. Κίνητρο: Γιατί γίνονται όμως, όλα αυτά; Υπάρχουν πάρα πολλοί λόγοι για να απαντήσει κανείς σε αυτήν την ερώτηση, αλλά οι κυριότεροι είναι:

α. η επιθυμία χρηματικού/ κέρδους μέσω διαφήμισης

β. η εγκληματική πράξη

γ. πολιτικός λόγος

Όπως η φωτιά χρειάζεται το οξυγόνο, την θερμότητα και το καύσιμο για να υπάρξει, έτσι και τα fake news, χωρίς τα 3 στοιχεία που προαναφέρθηκαν, δεν μπορούν να διαδοθούν στο κοινό (Trend Micro, 2017). Πιο συγκεκριμένα, μπορεί να αποτύχει η χειραγώγηση μιας συγκεκριμένης ομάδας χρηστών, την οποία έχει στο στόχαστρο είτε ένας ιδιοκτήτης ιστοσελίδας, είτε κάποιος που χρηματοδοτεί μια ιστοσελίδα για να παρουσιάσει ψεύτικα δεδομένα. Ανεξάρτητα βέβαια από τον κίνητρο, η επιτυχία της εκστρατείας κρύβεται στο πόσο θα επηρεάσει τον κόσμο (Trend Micro, 2017).

Οι ψεύτικες ειδήσεις του διαδικτύου κυκλοφορούν στα social media, στους ιστότοπους και στα feeds των χρηστών και στη συνέχεια εισάγονται στον «Θάλαμο Ήχου» (Echo Chamber). Πρόκειται για έναν θάλαμο όπου μοιράζονται δεδομένα με εκθετικό τρόπο μεταξύ χρηστών και φίλων των χρηστών. Μια κατάσταση, δηλαδή,

στην οποία οι πεποιθήσεις ενισχύονται ή ενισχύονται από την επικοινωνία και την επανάληψη μέσα από ένα κλειστό σύστημα και τις μονώνει από τον αντίλογο.Μέσα στον θάλαμο ο ήχος αντηχεί, σε αυτήν την περίπτωση αντηχεί η πληροφορία. Γι' αυτό, λοιπόν, τα fake news κυκλοφορούν μέσω ιδιωτικών ροών σε λογαριασμούς κοινωνικών δικτύων. «*Οι ιδέες και απόψεις μέσα στον θάλαμο αντηχούν, έτσι ώστε οι άνθρωποι μέσα σε αυτόν να αρχίσουν να πιστεύουν, ότι αποτελούν την επικρατέστερη παγκόσμια άποψη ακόμη και αν οι ίδιοι βρίσκονται στο περιθώριο, ενώ ο αντίλογος και οι αντίθετες απόψεις ποτέ δεν τα καταφέρνουν στον θάλαμο ή αγνοούνται προκαλώντας τον «θάνατό» τους*» (Repath, 2018).

Η ίδια η Ε.Ε. συναντά πολλά εμπόδια και προβλήματα με το φαινόμενο των ψεύτικων ειδήσεων και αυτό φαίνεται από τα εξής ευρήματα (Gr Times, 2018):

- 83% των πολιτών Ευρώπης και 87% των Ελλήνων θεωρούν τα fake news κίνδυνο για την δημοκρατία.
- 55% των Ελλήνων και 37% των Ευρωπαίων απαντά κάθε μέρα στο ερώτημα «πόσο συχνά συναντάτε ειδήσεις ή πληροφορίες που πιστεύετε ότι παραποιούν την πραγματικότητα ή είναι ψευδείς;».
- Οι ψευδείς ειδήσεις έχουν 70% μεγαλύτερες πιθανότητες να εξαπλωθούν σε σχέση με τις αληθινές, στο twitter. (έρευνα του Media Lab MIT).
- Μια αληθινή είδηση κάνει 6 φορές περισσότερο χρόνο για να φτάσει σε 1.500 άτομα/χρήστες. Η ταχύτητα οφείλεται στην πρωτοτυπία και τα bots που τις διαδίδουν σαν πραγματικοί λογαριασμοί.

Αυτά είναι μερικά από τα στοιχεία που παρουσίασε η Μαρία Σπυράκη (ευρωβουλευτής του ΕΛΚ) στην συζήτηση «Fake News: Πραγματικότητα ή Παραπληροφόρηση;».

Είναι ένα διαδικτυακό ρομπότ (internet bot) που προγραμματίζει και εκτελεί αυτοματοποιημένες εργασίες μέσω του ίντερνετ. Ονομάζεται επίσης και web bot, web robot, WWW robot ή απλά bot (Διβράμης, 2020). Στις περισσότερες περιπτώσεις, τα

ρομπότ εκτελούν σχετικά απλές λειτουργίες που πρέπει να επαναληφθούν εκατοντάδες ή χιλιάδες φορές. Μια κλασική εφαρμογή ρομπότ είναι οι αράχνες ιστού, οι οποίες περιφέρονται μεταξύ ιστότοπων και χρησιμοποιούνται για την ανάλυσή τους πολλές φορές γρηγορότερα από τους ανθρώπους. Η Google και όλες οι άλλες μηχανές αναζήτησης χρησιμοποιούν τέτοια προγράμματα αράχνης για την ανάλυση και κατάταξη ιστοσελίδων με λέξεις - κλειδιά, ώστε να μπορούν να παρουσιάζουν αποτελέσματα αναζήτησης στους χρήστες σε σύντομο χρονικό διάστημα. Τέλος, διάφοροι διακομιστές ιστού μπορούν να δημιουργήσουν ένα απλό αρχείο κειμένου που ονομάζεται «robots.txt» που περιέχει τους κανόνες που πρέπει να ακολουθούν τα ρομπότ που επισκέπτονται τη σελίδα (Διβράμης, 2020). Ωστόσο, ορισμένα ρομπότ μπορεί να αγνοήσουν αυτούς τους κανόνες.

Υπάρχει έντονη σκέψη για επιβολή κυρώσεων και τιμωριών σε ιστότοπους που δημιουργούν παραπληροφόρηση, από την Ε.Ε. η οποία έχει σπαταλήσει 1.000.000€ για την καταπολέμηση του φαινομένου. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) έχει άλλωστε ως στόχο την προστασία και ασφάλεια. Η Ε.Ε. ανέπτυξε τον Κώδικα Ορθής Πρακτικής, τον οποίο κάθε ιστοσελίδα πρέπει να παρουσιάσει και όποιος τον παραβιάζει να έχει κυρώσεις. Μέσω του κώδικα εξασφαλίζεται διαφάνεια για το ποιος χρηματοδοτεί τις πλατφόρμες στο διαδίκτυο. Ο χρηματοδότης οφείλει να γράφει το όνομά του και τα στοιχεία του στην πλατφόρμα. Δεύτερον εξηγεί από που προέρχονται οι πόροι και τέλος ποιος είναι ο σκοπός του. Εισάγεται έτσι, μια διαδικασία εντοπισμού πλαστών λογαριασμών και κινήσεων. Το douple check συγκροτεί ένα ανεξάρτητο δίκτυο φορέων εξακρίβωσης στοιχείων για να υπάρχει διασταύρωση αυτών 2 φορές πριν ανέβει μια είδηση σε μια πλατφόρμα.

Το 2016 στο λεξικό της Οξφόρδης κυριάρχησε η έκφραση post-truth, δηλαδή οι ψευδείς ειδήσεις δημιουργούν εναλλασσόμενες πραγματικότητες ή μια πραγματικότητα που δεν υπάρχει για να εξυπηρετηθούν συμφέροντα (Gr Times, 2018). Υποδηλώνει τις συνθήκες σύμφωνα με τις οποίες τα αληθινά γεγονότα έχουν μικρότερη επιρροή στην διαμόρφωση της κοινής γνώμης γιατί κυριαρχούν πληροφορίες που απευθύνονται στο θυμικό, την συγκίνηση και στις προσωπικές πεποιθήσεις του κάθε ατόμου (Gr Times, 2018). Πιο συγκεκριμένα η Μαρία Σπυράκη

εξηγεί πως: «Μας λένε αυτό που θέλουμε να ακούσουμε διαμορφωμένο σε σχέση με την προτίμηση εκείνου που έχει το συμφέρον. Είναι μια κατασκευασμένη αλήθεια και δεν έχει καμία σχέση με την πραγματικότητα που γνωρίζουμε».

Ένα από τα βασικότερα προβλήματα που δημιουργείται, εξαιτίας των fake news είναι νομικής φύσης. Πιο συγκεκριμένα, η προσβολή των δικαιωμάτων στην πληροφόρηση και στην έκφραση, τα οποία δικαιώματα είναι κατοχυρωμένα στην ΕΣΔΑ στο άρθρο 10 και στην Ελλάδα συνταγματικά κατοχυρωμένα στα άρθρα 5Α και 14 (Ντόκος, 2019). Σύμφωνα με αυτά μπορεί ο καθένας να εκφραστεί και να πληροφορηθεί χωρίς περιορισμούς, πλην εξαιρέσεων. Οι εξαιρέσεις λοιπόν, είναι τα fake news αφού είναι συνταγματικά απαγορευμένη η διάδοσή τους.

Επίσης, σημαντικό είναι να αναφερθεί ότι η προπαγάνδα εξυπηρετεί συγκεκριμένες σκοπιμότητες:

· πολιτικές

· οικονομικές

· κοινωνικές

· ανθρωπιστικές

· τρομοκρατικές

Η επιρροή του αποδέκτη μπορεί να οδηγήσει στην χειραγώγηση, τρομοκράτηση, προκατάληψη και περιθωριοποίησή του (Ντόκος, 2019). Η προπαγάνδα αποτελεί απειλή καθώς μπορεί να οδηγήσει στο χαθεί η εμπιστοσύνη στους θεσμούς της δημοκρατίας, ενισχύεται η πόλωση, δημιουργείται ανισορροπία και έτσι η επιβίωση της κοινωνίας βρίσκεται σε κίνδυνο (Νικόλαος Παναγιώτου, οπ. αναφ. το Gr Times, 2018). Ο πιο κοινός στόχος που προκαλεί πρόβλημα είναι ο πολιτικός. Γίνεται, δηλαδή, χειραγώγηση των ψηφοφόρων στις εκλογές και στα δημοψηφίσματα μέσω εξάπλωσης ψεύτικων ιστοριών (weaponised fake news). Παράλληλα, μολύνεται ο δημόσιος διάλογος και ο τρόπος λήψης αποφάσεων. Είναι γνωστό το σκάνδαλο της Cambridge Analytica με τον τότε Αμερικανό Πρόεδρο Donald Trump και το

Facebook. Περίπου το 2010-2016, συλλέχθηκαν προσωπικά δεδομένα από 87 εκατομμύρια χρήστες του Facebook χωρίς τη συγκατάθεση τους, τα οποία χρησιμοποιήθηκαν κυρίως για πολιτική διαφήμιση, πιο συγκεκριμένα για την προεδρική εκστρατεία του 2016. Το σκάνδαλο πυροδότησε ένα αυξανόμενο ενδιαφέρον του κοινού για την ιδιωτικότητα και την επιρροή των κοινωνικών μέσων στην πολιτική.

Αρχικά, από όλα αυτά μπορούμε να συμπεράνουμε ότι η προπαγάνδα και τα fake news είναι εφικτό να προκαλέσουν μεγαλύτερη καταστροφή και αρνητικές επιπτώσεις όταν διαδίδονται μέσω του ίντερνετ. Η λύση σε αυτό το πρόβλημα είναι η χρήση της κριτικής σκέψης. Οι εξής ερωτήσεις μπορούν να βοηθήσουν στην αναγνώριση κάποιας αναληθούς πληροφορίας (Ντόκος, 2019):

-Ποια είναι η πηγή της είδησης;

-Ποιος είναι ο δημιουργός της;

-Είναι αξιόπιστη;

-Πότε δημοσιεύθηκε η είδηση;

-Δημοσιεύθηκε σε περισσότερα μέσα/ από διαφορετικές πηγές;

-Είναι το περιεχόμενο αντικειμενικό ή υποκειμενικό/προκατειλημμένο;

Πρώτο βήμα για την πρόληψη στο φαινόμενο αυτό είναι η επίγνωσή του από τους χρήστες, ώστε να προφυλάσσονται από ειδήσεις με παραπλανητικό και κακόβουλο περιεχόμενο. Η δημιουργία μιας υπηρεσίας κοινωνικής δικτύωσης όπου θα υπάρχει η δυνατότητα στους χρήστες να αναφέρουν ψεύτικα δεδομένα και το προσωπικό αυτής της υπηρεσίας να ελέγχει και να ερευνά τις αναφορές αυτές, είναι αναγκαία. Αν και τα social media έχουν την μεγαλύτερη ευθύνη για την διαμόρφωση της κοινής γνώμης, κάνουν προσπάθειες για να καταπολεμήσουν την εξάπλωση των fake news και τις παραπλανητικές πολιτικές διαφημίσεις. Ανεξάρτητα από το γεγονός ότι δέχονται πιέσεις από τις κυβερνήσεις ή φοβούνται μήπως αλλοιωθεί η εικόνα τους.

Η αύξηση του χρόνου χρήσης των users των κοινωνικών δικτύων έχει κάνει ακόμη πιο εύκολο το έργο των εκστρατειών παραπληροφόρησης σε διάφορα ζητήματα. Το να αναρτήσει κανείς ή να διαμοιράσει απλά μια προπαγάνδα, όμως, έχει διαφορά από το να αλλάξεις κάτι για να στοχοποιηθεί ένα συγκεκριμένο κοινό (Trend Micro, 2017). Τα social media δημιουργήθηκαν με σκοπό να διατηρήσουν την επικοινωνία μεταξύ των ανθρώπων αλλά έχουν καταλήξει ως ένα μέσο πηγής πληροφοριών και προκαλεί μεγάλη δυσκολία στους χρήστες στο να διακρίνουν την αλήθεια των γεγονότων ή τα νέα από την προπαγάνδα (Brooks, 2020). Ο Sir Brian Leverson QC (Βρετανός δικαστής) το 2011 ανέφερε πως: «Ο Τύπος παρέχει έναν απαραίτητο έλεγχο σε όλες τις πτυχές της δημόσιας ζωής. Γι' αυτό όποια αποτυχία στα Μέσα Ενημέρωσης μας επηρεάζει όλους.» (οπ. αναφ. η Napley, 2017). Η προπαγάνδα σίγουρα δεν αποτελεί ένα αθώο πολιτικά φαινόμενο. Οι κακόβουλες επιθέσεις με πολιτική σκοπιμότητα μπορούν να οδηγήσουν σε αρνητικές επιπτώσεις εκλογές ή και διάφορα κοινωνικά ζητήματα. Η πρόληψη στον τεχνικό τομέα (προγράμματα επαλήθευσης των fake news, αλγόριθμοι) και η ενίσχυση της κριτικής σκέψης των ατόμων μπορούν να καταφέρουν την μείωση του φαινομένου αν όχι την εξάλειψή του, παρά το γεγονός ότι η παραπληροφόρηση είναι αρκετά πιο ανταγωνιστική από την αλήθεια (Gr Times, 2018).

2.11 Διαδικτυακός ρατσισμός και βία

Σύμφωνα με τους Yar και Steinmetz (2019) η βία στον Κυβερνοχώρο είναι ψυχολογική βλάβη ή υποκίνηση σωματικής βλάβης σε άλλους, παραβιάζοντας έτσι νόμους σχετικά με την προστασία του ατόμου, π.χ. ρητορική μίσους, παρακολούθηση. Το πρόβλημα, φυσικά, είναι ότι πολλές μορφές παραδοσιακού εγκλήματος, συμπεριλαμβανομένων εκείνων που έχουν ως αποτέλεσμα υλικές ζημιές και βία, διαπράττονται όλο και περισσότερο με τη βοήθεια υπολογιστών, φορητών ηλεκτρονικών συσκευών και του Διαδικτύου (McQuade, 2009: 62).

Τις τελευταίες δεκαετίες, εμφανίστηκε ο όρος «ρητορική μίσους» (hate speech), αρχικά ως απάντηση στις ανησυχίες των ανθρώπων ότι η χρήση ρατσιστικής γλώσσας ενθαρρύνει τις διακρίσεις και υποκινεί μίσος και βία κατά ομάδων και ατόμων

εθνοτικών μειονοτήτων (Yar και Steinmetz, 2019). Σε ορισμένες χώρες με διαφορετικό ιστορικό και πολιτικό υπόβαθρο, έχουν προκύψει ανησυχίες για τις κοινωνικές συνέπειες αυτής της γλώσσας. Η ρητορική μίσους μπορεί να γίνει καλύτερα κατανοητή ως ο λόγος που συκοφαντεί άτομα ή ομάδες με βάση τη φυλή, το χρώμα, το δόγμα, την εθνικότητα, τον σεξουαλικό προσανατολισμό, τη θρησκεία, την εθνικότητα, τη μετανάστευση, την αναπηρία ή παρόμοια χαρακτηριστικά για την προώθηση της βίας ή με άλλο τρόπο δημιουργώντας ένα εχθρικό περιβάλλον (Yar και Steinmetz, 2019).

Ο διαδικτυακός εκφοβισμός και η διαδικτυακή ρητορική μίσους κατά των γυναικών είναι βία με βάση το φύλο και μέρος ενός συνεχόμενου κύκλου βίας κατά των γυναικών που ξεκινά εκτός σύνδεσης και έχει απήχηση στο διαδίκτυο και αντίστροφα. Ο μισογυνισμός στο Διαδίκτυο (όπως ο ρατσισμός και η ομοφοβία στο Διαδίκτυο) είναι αποτέλεσμα ενός ευρύτερου μοτίβου υποταγής και βίας. Ακριβώς όπως στην πραγματική ζωή, οι γυναίκες, ειδικά εκείνες με «αδυναμίες», βιώνουν μια σειρά συνεχών επιθέσεων από ανεπιθύμητη σεξουαλική πρόκληση, σεξισμό ή/και ρατσισμό. Ακόμη και συχνές προσβολές, τρομακτικές , και μερικές φορές απειλητικές για τη ζωή τους. Η προώθηση της πραγματικής αλλαγής με την οποία οι άντρες και οι γυναίκες δεν αποδέχονται καμία μορφή βίας κατά των γυναικών και η ισότητα των φύλων πραγματοποιείται στην πολιτική, την εργασία, την οικονομία και την κοινωνία – αυτές είναι οι πραγματικές αλλαγές που απαιτούνται (Segrave & Vitis, 2017: 121).

Το Zoombombing αναφέρεται σε ανεπιθύμητες και ενοχλητικές εισβολές που συνήθως από εισβολείς στο Διαδίκτυο σε τηλεδιάσκεψη. Ένα Zoombomb συνοδεύεται από άσεμνο, ρατσιστικό, ομοφοβικό, ισλαμοφοβικό ή αντισημιτικό υλικό, το οποίο συνήθως οδηγεί στο τέλος της συνάντησης. Το FBI έχει λάβει πολλαπλές αναφορές για συνέδρια που διαταράσσονται από πορνογραφικές ή/και εικόνες μίσους και απειλητική γλώσσα. Εντός της περιοχής ευθύνης του Τμήματος της Βοστώνης του FBI (AOR), η οποία περιλαμβάνει το Μέιν, τη Μασαχουσέτη, το Νιου Χάμσαϊρ και το Ρόουντ Άιλαντ, δύο σχολεία στη Μασαχουσέτη ανέφεραν τα ακόλουθα περιστατικά (Boston FBI, 2020):

· Στα τέλη Μαρτίου του 2020, ένα γυμνάσιο με έδρα τη Μασαχουσέτη ανέφερε ότι ενώ ένας δάσκαλος πραγματοποιούσε μια διαδικτυακή τάξη χρησιμοποιώντας το λογισμικό τηλεδιάσκεψης Zoom, ένα άτομο που δεν είχε ταυτότητα κάλεσε στην τάξη. Αυτό το άτομο φώναξε βωμολοχίες και στη συνέχεια φώναξε τη διεύθυνση του σπιτιού του δασκάλου στη μέση της διδασκαλίας.

· Ένα δεύτερο σχολείο με έδρα τη Μασαχουσέτη ανέφερε ότι σε μια συνάντηση ζουμ είχε πρόσβαση ένα άγνωστο άτομο. Σε αυτό το περιστατικό, το άτομο ήταν ορατό στην βιντεοκάμερα και εμφάνιζε τατουάζ σβάστικας.

Η εξέταση του τι συνιστά έμφυλη και σεξουαλική βία συζητείται, διερευνάται και αμφισβητείται όλο και περισσότερο σε διαδικτυακούς χώρους, αλλά και είναι σημαντικό ότι οι συζητήσεις σχετικά με το «τι πρέπει να γίνει» και τι «γίνεται» σχετικά με το φύλο, τη βία και την τεχνολογία διεξάγονται τώρα σε διάφορους δικτυωμένους χώρους, σε ορισμένες περιπτώσεις εμποτισμένοι με φεμινιστικό λόγο (Segrave & Vitis, 2017: 123). Η λέξη ρατσισμός κυριολεκτικά σημαίνει μίσος ή φόβος για άτομα άλλων φυλών, δηλαδή υποδηλώνει μια εχθρική στάση απέναντί τους, περιορίζοντας και διακρίνοντας αυτά τα άτομα από το κοινωνικό σύνολο. Το πρόβλημα είναι ότι λόγω της εύκολης ανωνυμίας που μπορεί να έχει κάποιος χρήστης στο Διαδίκτυο, το φαινόμενο του ρατσισμού μπορεί να λάβει μεγαλύτερες διαστάσεις και να έχει χειρότερες επιπτώσεις - ψυχολογικές κυρίως - στο άτομο.

Κεφάλαιο 3: Αντίκτυπος Κυβερνοεγκλήματος

3.1 Πολιτικές επιπτώσεις Κυβερνοεγκλήματος

Σύμφωνα με τον McQuade (2009: 166) οι εγκληματολόγοι, αξιωματούχοι επιβολής του νόμου, κυβερνητικοί αξιωματούχοι, ασφαλιστικοί πράκτορες και άλλα μέλη της κοινωνίας που ασχολούνται με τον κοινωνικό και οικονομικό αντίκτυπο του εγκλήματος στον κυβερνοχώρο προσπαθούν τακτικά να μετρούν τη διάδοση ή/και την επίπτωση του εγκλήματος στον κυβερνοχώρο και τον αντίκτυπό τους σε εκείνους που επηρεάζονται. Αυτό επιτυγχάνεται συνήθως μέσω εξειδικευμένης έρευνας, συμπεριλαμβανομένων ερευνών για τα θύματα εγκλημάτων ή συστηματικής ανάλυσης αναφορών αστυνομικής έρευνας, οι οποίες μπορούν να συνδυαστούν με μελέτες οικονομικών επιπτώσεων. Μια έρευνα που διεξήχθη από το Κέντρο Rozsa του Πανεπιστημίου του Κάλγκαρι συμπέρανε πως ο μέσος πολίτης είναι πιο πιθανό να είναι θύμα ηλεκτρονικού εγκλήματος από αυτό ενός φυσικού εγκλήματος (Zickefoose, 2008 οπ. αναφ. ο Kshetri, 2010: 6).

Για παράδειγμα, οι κοινωνίες που έχουν αδύναμους ή καθόλου νόμους για το έγκλημα στον κυβερνοχώρο και όπου οι κοινωνικοπολιτιστικές πρακτικές παρέχουν κάποιο βαθμό νομιμότητας σε τέτοια εγκλήματα, είναι πιθανό να υπάρχει γόνιμο έδαφος για αυτά τα εγκλήματα (Kshetri, 2010: 156). Από την άλλη, όταν οι υπηρεσίες επιβολής του νόμου στις αναπτυσσόμενες οικονομίες ασχολούνται πραγματικά με την καταπολέμηση των δραστηριοτήτων ηλεκτρονικού εγκλήματος, η πιθανότητα να ελέγχουν τέτοιες δραστηριότητες είναι πολύ μεγαλύτερη από ό,τι όταν μια κυβέρνηση απλώς τις επιβάλλει για να το κάνει. Επιπροσθέτως, ο αντίκτυπος στους θεσμούς διακυβέρνησης και τη συμμετοχή των πολιτών θεωρείται ιδιαίτερα σημαντικός. Η δομή του Διαδικτύου και η διάδοση των ηλεκτρονικών κοινωνικών δικτύων επιτρέπουν σε όλους να εκφράσουν τις απόψεις τους και αυτές μπορούν να ακουστούν ελεύθερα παντού. Ουσιαστικά, θεωρείται ότι οι Τεχνολογίες Πληροφοριών και Επικοινωνίας (ΤΠΕ) προωθούν την ισότητα, το οποίο αποτελεί βασικό δημοκρατικό δικαίωμα, πράγμα που σημαίνει ότι κάθε πολίτης μπορεί να μιλήσει ισότιμα και ελεύθερα. Ωστόσο, η δημοσιότητα δεν εξασφαλίζει απαραίτητα

διαφάνεια, και απαιτείται ουσιαστικός έλεγχος της πληροφορίας και των δεδομένων που διατίθενται, κάτι το οποίο οι ΤΠΕ δεν μπορούν να παρέχουν διαρκώς.

3.2 Οικονομικές επιπτώσεις Κυβερνοεγκλήματος

Η ταχεία διάδοση και ψηφιοποίηση των οικονομικών δραστηριοτήτων από το Διαδίκτυο έχει οδηγήσει στην εμφάνιση μιας νέας γενιάς εγκληματιών και οι οικονομικές, πολιτικές και κοινωνικές επιπτώσεις των δραστηριοτήτων αυτών των κυβερνοεγκληματιών έχουν λάβει σημαντική προσοχή τα τελευταία χρόνια, επομένως τα άτομα, οι επιχειρήσεις και οι κυβερνήσεις δικαίως ανησυχούν για την ασφάλεια των συστημάτων, των δικτύων και των υποδομών πληροφορικής τους (Kshetri, 2010). Τα εγκλήματα στον κυβερνοχώρο γίνονται όλο και πιο διαδεδομένα και εξελίσσονται και φαίνεται να έχουν πιο σοβαρές οικονομικές επιπτώσεις από τα περισσότερα συμβατικά εγκλήματα (Kshetri, 2010: 35). Οι επιπτώσεις του εγκλήματος στον κυβερνοχώρο εμφανίζονται συχνότερα στις πλούσιες οικονομίες, στις μεγάλες εταιρείες και στα άτομα υψηλού εισοδήματος. Ένας από τους λόγους είναι ότι οι μεγάλες εταιρείες έχουν μεγαλύτερα δίκτυα, τα οποία προσφέρουν περισσότερους στόχους στους χάκερ.

Τα τελευταία χρόνια, όλες οι εταιρείες επενδύουν σε τεχνικά μέτρα ασφαλείας για την πρόληψη επιθέσεων στον κυβερνοχώρο και προσπαθούν να προστατεύσουν τα «όριά τους» δημιουργώντας ένα προστατευμένο εσωτερικό περιβάλλον πληροφοριών για την ασφαλή αποθήκευση και επεξεργασία ευαίσθητων δεδομένων του οργανισμού και των πελατών του (Κολλιδάς, 2020). Μια έρευνα της Riptech έδειξε ότι οι εγκληματικές ομάδες ή μεμονωμένα άτομα είναι πιο πιθανό να ξεκινήσουν στοχευμένες επιθέσεις εναντίον μεγαλύτερων εταιρειών παρά μικρότερων (Kshetri, 2010: 155). Μια δημοφιλής άποψη είναι ότι τα εγκλήματα στον κυβερνοχώρο έχουν πιο σοβαρές οικονομικές επιπτώσεις από τα περισσότερα συμβατικά εγκλήματα και σύμφωνα με τη παγκόσμια έρευνα οικονομικού εγκλήματος της PricewaterhouseCoopers το 2007, πάνω από το 43% των εταιρειών που ερωτήθηκαν ανέφεραν ότι υπέστησαν ένα ή περισσότερα σημαντικά οικονομικά εγκλήματα (Kshetri, 2010: 4). Η πανδημία έχει επίσης αυξήσει την «περιοχή επίθεσης» για τους

εγκληματίες στον κυβερνοχώρο, καθώς δημόσιοι και ιδιωτικοί οργανισμοί έχουν ψηφιοποιήσει τους περισσότερους τομείς δραστηριοτήτων τους και γι' αυτό υπάρχει ανάγκη επαναπροσδιορισμού των κανόνων και του τρόπου με τον οποίο εφαρμόζονται τα μέτρα προστασίας (Κολλιδάς, 2020). Η νέα οικονομία του σήμερα βασίζεται αρκετά στις ΤΠΕ και παρουσιάζει μεγάλες δυνατότητες ανάπτυξης, συμπεριλαμβανομένων πολλών δραστηριοτήτων. Φαίνεται πως ο πιο δυναμικός κλάδος της νέας αυτής οικονομίας αποτελεί το ηλεκτρονικό εμπόριο, στο οποίο μπορεί να συναντήσει κανείς πολλούς κινδύνους όπως είναι η απάτη.

Εκτιμάται ότι το κόστος της διαδικτυακής απάτης και του εγκλήματος στον κυβερνοχώρο υπερβαίνει τα 5 τρισεκατομμύρια δολάρια και το 2020, είχε ξεπεράσει το σωρευτικό κόστος της διακίνησης ναρκωτικών (Κολλιδάς, 2020). Αξίζει να σημειωθεί ότι σε μια μελέτη, για πρώτη φορά στη λίστα των πιο κοινών μορφών οικονομικού εγκλήματος μετά την κλοπή, ήταν η απάτη που σχετίζεται με συμβάσεις προμηθειών και σύμφωνα με τους συμμετέχοντες, η απάτη στις συμβάσεις προμηθειών αποτελεί «διπλή απειλή» για τις εταιρείες, διότι διαβρώνει τη διαδικασία απόκτησης προϊόντων και υπηρεσιών και ταυτόχρονα υπονομεύει τις προσπάθειές τους να βρουν νέες ευκαιρίες (AccountacyGreece, 2020). Ένα είναι σίγουρο σύμφωνα με την Κατσούλη (2016) ότι «το οργανωμένο έγκλημα, που εστιάζει αποκλειστικά στο οικονομικό όφελος γίνεται μέσω πληθώρας μηχανισμών όπως το «ηλεκτρονικό ψάρεμα» (phishing) ή η πώληση κλεμμένων εταιρικών δεδομένων». Άλλες μορφές οικονομικού εγκλήματος αποτελούν η δωροδοκία και η διαφθορά, λογιστική απάτη, νομιμοποίηση εσόδων από παράνομες δραστηριότητες, κλοπή προσωπικών δεδομένων και πνευματικών δικαιωμάτων και η φορολογική αδιαφάνεια (AccountacyGreece, 2020).

3.3 Κοινωνικές επιπτώσεις Κυβερνοεγκλήματος

Η φύση του εγκλήματος και οι επιπτώσεις του στην κοινωνία αλλάζουν στον βαθμό που το Διαδίκτυο και άλλα συστήματα πληροφοριών, μαζί με υπολογιστές και άλλους τύπους πληροφορικής, όπως τα κινητά τηλέφωνα πολλαπλών χρήσεων χρησιμοποιούνται για παράνομους σκοπούς (McQuade, 2009: 166). Κάθε χρόνο

εκατομμύρια άνθρωποι σε όλο τον κόσμο που ζουν, εργάζονται ή ακόμη νέοι και παιδιά που χρησιμοποιούν αυτούς και άλλους τύπους συσκευών τεχνολογίας πληροφοριών (IT) πέφτουν θύματα ενός ή περισσότερων τύπων εγκλήματος στον κυβερνοχώρο ή διαδικτυακής κατάχρησης, όπως η πειρατεία υπολογιστών, ο εντοπισμός κλοπής, διαδικτυακών απειλών και παρενόχλησης και η κλοπή ή καταστροφή δεδομένων. Ορισμένα θύματα κυβερνοεγκλήματος βιώνουν την καταστροφή, χειραγώγηση ή άρνηση πρόσβασης σε πολύτιμα δεδομένα. Άλλοι υφίστανται απώλεια χρόνου, χρημάτων, εξοπλισμού υπολογιστών ή/και άλλων πόρων, ενώ άλλοι φοβούνται ότι τα συστήματά τους θα επιτεθούν ξανά ή θα βιώσουν κάποια μορφή συναισθηματικής βλάβης (McQuade, 2009: 166). Οι τρέχουσες εκτιμήσεις των κοινωνικών και οικονομικών επιπτώσεων του εγκλήματος στον κυβερνοχώρο ποικίλλουν σημαντικά ανάλογα με το είδος του εγκλήματος στον κυβερνοχώρο και τον πληθυσμό των θυμάτων που μελετήθηκαν, τη χρονική περίοδο και την αξία που αποδίδεται στις απώλειες που βιώνουν τα θύματα (McQuade, 2009: 167).

Όλες οι μορφές βλάβης που αντιμετωπίζουν τα θύματα εγκλήματος, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο, μπορούν να χαρακτηριστούν και να κατανοηθούν ως προς τον κοινωνικό και οικονομικό τους αντίκτυπο. Ο κοινωνικός αντίκτυπος αναφέρεται στις αρνητικές συνέπειες που βιώνουν οι άνθρωποι σε προσωπικό επίπεδο, όπως ο φόβος ή οι αρνητικές επιπτώσεις στις διαπροσωπικές σχέσεις τους, ενώ οι οικονομικές επιπτώσεις αναφέρονται στις οικονομικές απώλειες που βιώνουν τα μέλη της κοινωνίας ή των οργανισμών (McQuade, 2009: 166). Θεωρητικά, οι κοινωνικές και οικονομικές συνέπειες είναι αδιαχώριστες, διότι παρόλο που η οικονομική αξία μπορεί να σχετίζεται με προσωπικό τραυματισμό και ταλαιπωρία, η απώλεια χρημάτων ή άλλων χρηματοοικονομικών περιουσιακών στοιχείων (συμπεριλαμβανομένων πολύτιμων δεδομένων) μπορεί να οδηγήσει σε παραβιάσεις της ιδιωτικής ζωής, οικογενειακές συγκρούσεις, ακόμη και απώλεια της απασχόλησης και της θέσης εργασίας (McQuade, 2009: 166).

Ο αρνητικός κοινωνικός αντίκτυπος του εγκλήματος στον κυβερνοχώρο γίνεται αισθητός σε όλα τα κοινωνικά και ηλικιακά φάσματα. Μια εκτίμηση ανέφερε ότι το 20-25% των νέων έχουν πέσει θύματα κυβερνοεκφοβισμού (nasuwt.org 2009, οπ. αναφ. ο Kshetri, 2010: 5) και το WiredSafety.org, περισσότεροι από τους μισούς 9-13 ετών «είτε έχουν εκφοβιστεί στον κυβερνοχώρο είτε έχουν εκφοβιστεί στον κυβερνοχώρο, είτε είχαν έναν στενό φίλο που ήταν» (Saroyan, 2005 οπ. αναφ. ο Kshetri, 2010: 5). Για εκατομμύρια νέους, οι χώροι του κυβερνοχώρου γίνονται πιο σημαντικοί από τους φυσικούς χώρους που παραδοσιακά έχει δημιουργήσει η κοινωνία για να φιλοξενήσει την ψυχαγωγία των νέων και τις ψυχαγωγικές ανάγκες, δηλαδή μπορεί να προτιμούν να συναντιούνται ιδιωτικά ή δημόσια αλλά στο διαδίκτυο παρά αυτοπροσώπως (McQuade, 2009: 65). Πιο συγκεκριμένα, η ψηφιακή κουλτούρα της νεολαίας επεκτείνει τις σύνθετες κοινωνικές αλληλεπιδράσεις στον πραγματικό κόσμο, με άλλα λόγια, υπάρχει διάκριση μεταξύ του να είναι συνδεδεμένοι στο Διαδίκτυο ή εκτός σύνδεσης επειδή ζουν ταυτόχρονα μέσα στη σφαίρα των κυβερνοχώρου και των φυσικών χώρων, το οποίο έχει περιπλέξει την παραδοσιακή κοινωνική δυναμική και αμφισβητούνται οι έννοιες για το τι μπορεί να θεωρηθεί φυσιολογικές έναντι αποκλίνουσες συμπεριφορές, ηθικές ή ανήθικες συμπεριφορές (McQuade, 2009: 65).

Οι νέοι που έχουν μεγαλώσει με υπολογιστές ή άλλες συσκευές πληροφορικής και το Διαδίκτυο μπορεί να αναπτύσσουν διαφορετικά πρότυπα όσον αφορά τον τρόπο συμπεριφοράς στο διαδίκτυο σε αντίθεση με όταν δεν χρησιμοποιούν το Διαδίκτυο, επειδή αλληλεπιδρούν όλο και περισσότερο μέσω του κυβερνοχώρου όπου οι κοινωνικές κυρώσεις δεν ορίζονται σαφώς ή δεν επιβάλλονται με συνέπεια όπως γίνεται στον πραγματικό κόσμο (McQuade, 2009: 65). Για παράδειγμα, μια «κακή συμπεριφορά» στον κυβερνοχώρο δεν θα επιφέρει πιθανότατα το ίδιο επίπεδο καταγγελίας ή τιμωρίας που θα το έκανε αυτό στο σπίτι, στο σχολείο ή σε ένα περιβάλλον εργασίας. Εν κατακλείδι, ο ψηφιακός κόσμος έχει επηρεάσει τον τρόπο με τον οποίο οι νέοι συμπεριφέρονται και αλληλεπιδρούν, δηλαδή έχει δημιουργήσει νέους τρόπους δημιουργίας κοινωνικών ομάδων και διασυνδέσεων μεταξύ των μελών τους, ενώ από την άλλη πλευρά οι κοινωνικές αλληλεπιδράσεις, ξεκινώντας από τη

σωματική επαφή, δεν αποτελούν πλέον απαραίτητο καθοριστικό σημείο φιλίας (McQuade, 2009: 66). Στον ψηφιακό κόσμο, οι άνθρωποι πρέπει απλώς να αναζητήσουν ένα κοινό συμφέρον ή ενδιαφέρον σε ένα κοινωνικό δίκτυο και να ζητήσουν να προστεθούν ως φίλοι, ωστόσο, λόγω της μεγάλης έκθεσης των νέων στο Διαδίκτυο, οι ίδιοι κατακλύζονται από διαδικτυακές δραστηριότητες που μπορεί να περιλαμβάνουν ελάχιστη ή καθόλου επίβλεψη ενηλίκων / γονέων (McQuade, 2009: 66).

Ο εθισμός συνήθως ορίζεται από τη σχέση μεταξύ του ατόμου και των ορατών συμπεριφορών του και η σοβαρότητά του μπορεί συνήθως να καθοριστεί από τον αντίκτυπό του σε διάφορους τομείς της ζωής ενός ατόμου, συμπεριλαμβανομένης της υγείας, των οικονομικών, της καριέρας και των σχέσεων με την οικογένεια, τους φίλους και την κοινωνία (McQuade, 2009: 2-3). Μια πρόσθετη πρόκληση είναι η αναδυόμενη «κυβερνοψυχοπαθητική» εκείνων που σχεδιάζουν και απελευθερώνουν ιούς ή άλλους καταστροφικούς μηχανισμούς κατά της παγκόσμιας οικογένειας χρηστών υπολογιστών. Αυτοί «οι κυβερνοψυχοπαθητικοί» προκαλούν σημαντική βλάβη σε απληροφόρητους χρήστες μολύνοντας υπολογιστές και προσπαθώντας να χειριστούν ή να καταστρέψουν δεδομένα που είναι αποθηκευμένα σε διάφορα παγκόσμια συστήματα πληροφοριών. Μπορεί πολλές φορές να υποκινούνται από πολιτικές, οικονομικές, εταιρικές ή προσωπικές προσπάθειες για να αποκτήσουν ένα αντιληπτό πλεονέκτημα εις βάρος των άλλων (McQuade, 2009: 97-98).

Εν ολίγοις, οι παράγοντες που προκαλούν έγκλημα λέγεται ότι επηρεάζουν τόσο τους άνδρες όσο και τις γυναίκες, αλλά, τα χαρακτηριστικά του φύλου στην κοινωνία, μας επιτρέπουν να καταλάβουμε ότι οι άνδρες ενεργούν περισσότερο εγκληματικά ως απάντηση σε στους αιτιολογικούς παράγοντες σε σχέση με τις γυναίκες (Yar & Steinmetz, 2019). Σύμφωνα με τον Καρατράντο (2020) οι παράγοντες που εντείνουν το φαινόμενο της εγκληματικότητας στον Κυβερνοχώρο είναι οι εξής: η ευελιξία στο modus operandi (τρόπος δράσης) των εγκληματικών οργανώσεων, η αύξηση της καθημερινής δραστηριότητας στο διαδίκτυο, η ζήτηση ή έλλειψη συγκεκριμένων προϊόντων, οι πληρωμές και οικονομικές συναλλαγές μέσω του διαδικτύου, η διείσδυση των εγκληματικών ομάδων στη νόμιμη οικονομική δραστηριότητα, η

υποχρεωτική παραμονή και συμβίωση στο σπίτι για μεγάλο χρονικό διάστημα, η πίεση, το στρες και η αίσθηση του αδιεξόδου, η οικονομική ύφεση και επιπτώσεις στον εργασιακό τομέα, η άρνηση της πανδημίας και η υιοθέτηση θεωριών συνωμοσίας.

Παρακάτω παρουσιάζονται κάποια στοιχεία από την Έκθεση Κυβερνοασφάλειας τον Φεβρουάριο το 2015 της Ευρωπαϊκής Επιτροπής, η οποία εξέτασε την εμπειρία και τις αντιλήψεις των πολιτών της ΕΕ σχετικά με ζητήματα ασφάλειας στον κυβερνοχώρο και πως έχουν αλλάξει από την προηγούμενη έρευνα του Μαΐου-Ιουνίου 2013. Σε σύγκριση με το 2013, οι Ευρωπαίοι πολίτες έχουν ελαφρώς υψηλότερο επίπεδο κατανόησης των κινδύνων του εγκλήματος στον κυβερνοχώρο και οι περισσότεροι χρήστες του Διαδικτύου πιστεύουν ότι μπορούν να προστατευτούν επαρκώς από το έγκλημα στον κυβερνοχώρο. Ωστόσο, εξακολουθούν να υπάρχουν πολλοί άνθρωποι που αισθάνονται ότι αγνοούν την κατάσταση και δεν μπορούν να προστατευθούν καθόλου:

- Οι χρήστες του Διαδικτύου είναι πιο πιθανό να έχουν αλλάξει τη συμπεριφορά τους στο διαδίκτυο λόγω ανησυχιών για την ασφάλεια από το 2013 (European Commission, 2015: 30).

- Οι ενέργειες που είναι πιο πιθανό να κάνουν οι ερωτηθέντες είναι η εγκατάσταση λογισμικού προστασίας από ιούς (61%) και να μην ανοίγουν μηνύματα ηλεκτρονικού ταχυδρομείου από άτομα που δεν γνωρίζουν (49%). Άλλες αλλαγές περιλαμβάνουν τη δυνατότητα παροχής προσωπικών πληροφοριών σε ιστότοπους (38%), χρησιμοποιώντας μόνο τον δικό τους υπολογιστή (38%) επισκέπτονται μόνο ιστότοπους που γνωρίζουν και εμπιστεύονται (36%), χρησιμοποιώντας διαφορετικούς κωδικούς πρόσβασης για διαφορετικούς ιστότοπους (31%) και αλλάζουν τακτικά τους κωδικούς πρόσβασής τους (27%) (European Commission, 2015: 30).

- Η συντριπτική πλειοψηφία των χρηστών του Διαδικτύου συμφωνούν ότι αποφεύγουν να αποκαλύπτουν προσωπικές πληροφορίες στο διαδίκτυο (89%), ενώ το 85% συμφωνεί ότι ο κίνδυνος να πέσει θύμα εγκλήματος στον κυβερνοχώρο

αυξάνεται. Μόνο μικρά ποσοστά ερωτηθέντων διαφωνούν με αυτές τις δηλώσεις (10% και 12% αντίστοιχα) (European Commission, 2015: 45).

- Σε όλες τις χώρες της ΕΕ, τουλάχιστον το 70% των χρηστών του Διαδικτύου συμφωνούν ότι ο κίνδυνος να πέσουν θύματα εγκλήματος στον κυβερνοχώρο αυξάνεται. Τα υψηλότερα ποσοστά παρατηρούνται στη Φινλανδία (94%), στην Κροατία (92%) και η Σουηδία (92%), στο Λουξεμβούργο (62%) και η Σουηδία (61%), οι μεγάλες αναλογίες «συμφωνούν απολύτως» (European Commission, 2015: 48)

- Υπάρχει διαφοροποίηση μεταξύ των κρατών μελών όσον αφορά το ποσοστό των χρηστών του Διαδικτύου που συμφωνούν ότι ανησυχούν ότι τα διαδικτυακά προσωπικά τους στοιχεία δεν διατηρούνται ασφαλή από ιστότοπους. Ερωτηθέντες στην Ισπανία (91%), την Πορτογαλία (85%) και η Ελλάδα (84%) είναι πιο πιθανό να συμφωνήσουν, και στην Ελλάδα περισσότεροι από τους μισούς ερωτηθέντες «συμφωνούν απόλυτα» (57%) (European Commission, 2015: 49).

- Όταν ερωτώνται πόσο ανησυχούν για την εμπειρία ή το γεγονός ότι είναι θύματα διαφορετικών τύπων εγκλήματος στον κυβερνοχώρο, οι χρήστες του Διαδικτύου είναι πιο πιθανό να πουν ότι ανησυχούν για την αναγνώριση κλοπής (το 68% ανησυχεί για αυτό) και την ανακάλυψη κακόβουλου λογισμικού στη συσκευή τους (66%). Οι χρήστες του Διαδικτύου εκφράζουν επίσης ανησυχία για το γεγονός ότι έπεσαν θύματα απάτης με τραπεζικές κάρτες ή ηλεκτρονικές τραπεζικές συναλλαγές (63%) και σχετικά με την παραβίαση των μέσων κοινωνικής δικτύωσης ή του λογαριασμού ηλεκτρονικού ταχυδρομείου τους (60%) (European Commission, 2015: 54)

- Οι δύο πιο συνηθισμένες καταστάσεις που βιώνουν οι ερωτηθέντες είναι η ανακάλυψη κακόβουλου λογισμικού στη συσκευή τους (47%) και λαμβάνουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα τηλεφώνημα ζητώντας δόλια πρόσβαση στον υπολογιστή, τις συνδέσεις ή τα προσωπικά τους στοιχεία (31%). Σε κάθε περίπτωση, το 7% των χρηστών του Διαδικτύου λένε ότι αυτό τους έχει συμβεί συχνά (European Commission, 2015: 56).

•Κλοπή Ταυτότητας

Σε ολόκληρη την ΕΕ συνολικά, το 68% των χρηστών του Διαδικτύου δηλώνουν ότι ανησυχούν πολύ ή δίκαια για την κλοπή ταυτότητας. Τα υψηλότερα επίπεδα ανησυχίας παρατηρούνται στη Γαλλία (όσον αφορά το 80%) και στην Ισπανία (79%). Οι ερωτηθέντες στην Εσθονία και τις Κάτω Χώρες (48% σε κάθε χώρα) είναι λιγότερο πιθανό να ανησυχούν για κλοπή ταυτότητας. (European Commission, 2015: 57)

•Απάτες σε emails και τηλεφωνικές κλήσεις

Το επίπεδο ανησυχίας σχετικά με τα μηνύματα ηλεκτρονικού ταχυδρομείου ή τις τηλεφωνικές κλήσεις που ζητούν δόλια πρόσβαση στον υπολογιστή ή άλλες λεπτομέρειες είναι γενικά συνεπές σε ολόκληρη την ΕΕ, αν και οι ερωτηθέντες στην Ιρλανδία (72%) είναι πιο πιθανό από εκείνους σε άλλες χώρες να πουν ότι ανησυχούν, και αυτό περιλαμβάνει το 44% που είναι "πολύ ανήσυχοι". Υψηλά επίπεδα ανησυχίας παρατηρούνται επίσης στην Ισπανία (67% αφορά), στην Ελλάδα (66%) και η Πορτογαλία (66%) (European Commission, 2015: 59)

•Διαδικτυακή Απάτη

Κατά μέσο όρο, το 56% των χρηστών του Διαδικτύου σε ολόκληρη την ΕΕ δηλώνουν ότι ανησυχούν πολύ ή δίκαια για την απάτη στο διαδίκτυο. Οι ερωτηθέντες στην Ισπανία (71%) και η Ιρλανδία (70%) είναι πολύ πιθανό να πουν ότι ανησυχούν, με ένα υψηλό ποσοστό ερωτηθέντων στην Ιρλανδία να δηλώνουν ότι «ανησυχούν πολύ» (39%). Οι ερωτηθέντες στη Σουηδία (30%) και οι Κάτω Χώρες (35%) είναι λιγότερο πιθανό να πουν ότι ανησυχούν για διαδικτυακή απάτη (European Commission, 2015: 61).

•Προσβλητικό υλικό και Παιδική Πορνογραφία

Οι ερωτηθέντες στην Ισπανία είναι πολύ πιο πιθανό από εκείνους σε άλλες χώρες να πουν ότι ανησυχούν πολύ ή δίκαια για την τυχαία αντιμετώπιση παιδικής πορνογραφίας στο διαδίκτυο (79%). Οι ερωτηθέντες στη Σουηδία (19%) και οι Κάτω

Χώρες (25%) για άλλη μια φορά εκφράζουν τα χαμηλότερα επίπεδα ανησυχίας (European Commission, 2015: 63).

•Πρόσβαση σε Διαδικτυακές υπηρεσίες

Τα υψηλότερα επίπεδα ανησυχίας σχετικά με τη μη πρόσβαση σε επιγραμμικές υπηρεσίες λόγω κυβερνοεπιθέσεων παρατηρούνται στη Λετονία (69% πολύ ή αρκετά ενδιαφερόμενο), στην Ιρλανδία (66%) και την Τσεχική Δημοκρατία (65%). Οι ερωτηθέντες στη Σουηδία (33%) και η Φινλανδία (36%) είναι λιγότερο πιθανό να ανησυχούν για αυτό το είδος προβλήματος (European Commission, 2015: 67).

•Χακάρισμα Λογαριασμών Email

Κατά μέσο όρο, το 60% των χρηστών του Διαδικτύου σε ολόκληρη την ΕΕ δηλώνουν ότι ανησυχούν πολύ ή δίκαια για την παραβίαση των μέσων κοινωνικής δικτύωσης ή του λογαριασμού ηλεκτρονικού ταχυδρομείου τους. Οι ερωτηθέντες στην Ισπανία (74%), την Πορτογαλία (72%), τη Μάλτα (71%) και η Κροατία (70%) είναι πολύ πιθανό να πουν ότι ανησυχούν. Οι ερωτηθέντες στη Σουηδία (37%) είναι λιγότερο πιθανό να πουν ότι ανησυχούν για την παραβίαση ενός λογαριασμού, ενώ χαμηλά ποσοστά μπορούν επίσης να παρατηρηθούν στην Εσθονία (44%) και τις Κάτω Χώρες (46%) (European Commission, 2015: 69).

•Διαδικτυακή Τραπεζική Απάτη

Συνολικά, το 63% των χρηστών του Διαδικτύου στην ΕΕ ανησυχούν πολύ ή δίκαια για την απάτη με τραπεζικές κάρτες ή ηλεκτρονικές τραπεζικές συναλλαγές. Τα υψηλότερα επίπεδα ανησυχίας παρατηρούνται στη Λετονία (79%), στη Γαλλία (76%) και την Ισπανία (75%). Ερωτηθέντες στη Γερμανία (46%), τη Σουηδία (48%) και η Εσθονία (49%) είναι λιγότερο πιθανό από εκείνες σε άλλες χώρες να ανησυχούν για τραπεζική κάρτα ή απάτη μέσω ηλεκτρονικής τραπεζικής (European Commission, 2015: 71).

•Εκβιασμοί στον Κυβερνοχώρο

Οι ερωτηθέντες στην Ισπανία (68% ανησυχούν πολύ ή δίκαια), την Ιρλανδία (61%), την Τσεχική Δημοκρατία (60%) και η Λετονία (60%) είναι πιο πιθανό από εκείνους σε άλλες χώρες να πουν ότι ανησυχούν για το γεγονός ότι τους ζητείται μια πληρωμή σε αντάλλαγμα για να πάρουν πίσω τον έλεγχο της συσκευής τους (European Commission, 2015: 73).

•Κακόβουλο λογισμικό

Κατά μέσο όρο, το 66% των χρηστών του Διαδικτύου σε ολόκληρη την ΕΕ δηλώνουν ότι ανησυχούν πολύ ή δίκαια για την ανακάλυψη κακόβουλου λογισμικού στη συσκευή τους. Παρόμοιος αριθμός παρατηρείται στα περισσότερα επιμέρους κράτη μέλη. Οι ερωτηθέντες στην Ελλάδα (76%) και η Μάλτα (76%) είναι πιο πιθανό να πουν ότι ανησυχούν για αυτό, ενώ οι ερωτηθέντες στη Σουηδία (41%) είναι μακράν οι λιγότερο πιθανό να πουν ότι ανησυχούν για την ανακάλυψη κακόβουλου λογισμικού (European Commission, 2015: 75).

Πιο πρόσφατα δεδομένα δείχνουν ότι οι ψηφιακές απειλές εξελίσσονται ραγδαία και το κοινό θεωρεί ότι το έγκλημα στον κυβερνοχώρο είναι η κύρια απειλή, ειδικότερα, η έρευνα δείχνει ότι οι επιθέσεις εξαργύρωσης έχουν αυξηθεί κατά 300% από το 2015 και ο οικονομικός αντίκτυπος του εγκλήματος στον κυβερνοχώρο έχει αυξηθεί από το 2013 στο 2017 πέντε φορές και ενδέχεται αυξηθεί περαιτέρω, τετραπλασιασμός έως το 2019, ενώ, το 87% των Ευρωπαίων πιστεύουν ότι το έγκλημα στον κυβερνοχώρο είναι η κύρια πρόκληση για την εσωτερική ασφάλεια της ΕΕ (Europa EU, 2017). Σύμφωνα με αναφορές από ευρωπαϊκά ιδρύματα και διεθνείς οργανισμούς, καθώς και έρευνες από ερευνητικά ιδρύματα, η πρώτη περίοδος περιοριστικών μέτρων που εφαρμόστηκαν από χώρες για τη διαχείριση της πανδημίας COVID-19 είχε επίσης αντίκτυπο στην κατάσταση του εγκλήματος στην Ευρωπαϊκή Ένωση, καθώς οι οργανωμένες εγκληματικές ομάδες έδειξαν ευελιξία και υιοθέτησαν γρήγορα διαφορετικό modus operandi, δηλαδή νέες εγκληματικές μεθόδους (Καρατράντος, 2020).

Κεφάλαιο 4: Πολιτικές Αντιμετώπισης του Κυβερνοεγκλήματος

4.1 Επιβολή Νόμου

Η κύρια πρόκληση που αντιμετωπίζουν οι υπηρεσίες επιβολής του νόμου και άλλες ρυθμιστικοί φορείς είναι οι διεθνικές πτυχές του εγκλήματος στον κυβερνοχώρο και ο κοινωνικός, οικονομικός και προσωπικός αντίκτυπός του (McQuade, 2009: 97). Όπως αναφέρει πιο συγκεριμένα ο McQuade (2009: 137): «Σε αντίθεση με τα παραδοσιακά εγκλήματα όπως η δολοφονία, η επίθεση, η ληστεία και η διάρρηξη, στα οποία οι αρχές επιβολής του νόμου συνήθως απολαμβάνουν υψηλά ποσοστά επιλύσεων και επιτυχίας της δίωξης, τα σύνθετα εγκλήματα στον κυβερνοχώρο απαιτούν περισσότερες τεχνικές δεξιότητες και γνώσεις από ερευνητές και εισαγγελείς. Οι οργανωμένοι εγκληματίες του κυβερνοχώρου τείνουν να είναι πολύ διανοούμενοι, πειθαρχημένοι και επικεντρωμένοι στη βελτίωση των μεθόδων υψηλής τεχνολογίας, καθιστώντας τη διερεύνηση των δραστηριοτήτων τους τόσο κουραστική όσο και περίπλοκη, ενώ οι αμερικανικές και διεθνείς υπηρεσίες επιβολής του νόμου, όπως η Ιντερπόλ, αμφισβητούνται όλο και περισσότερο από την κλίμακα, την πολυπλοκότητα και τον όγκο των οργανωμένων υποθέσεων ηλεκτρονικού εγκλήματος».

Μερικοί υποστηρίζουν ότι η επιβολή του νόμου χάνει τη μάχη ενάντια στους κυβερνοεγκληματίες (Zeller, 2005 οπ. αναφ. ο Kshetri, 2010: 25). Πολλές κυβερνήσεις έχουν υποτιμήσει τον πιθανό αντίκτυπο του εγκλήματος στον κυβερνοχώρο και έχουν παραμελήσει να δώσουν ιδιαίτερη προσοχή στην καταπολέμηση αυτού του νέου τύπου εγκλήματος (Kshetri, 2010: 25). Από τη σκοπιά των υπηρεσιών επιβολής του νόμου, η δυνατότητα χρήσης ανωνυμίας, μεταμφιέσεως και κρυπτογράφησης αποτελεί σοβαρό εμπόδιο για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Yar & Steinmetz, 2019). Το έγκλημα στον κυβερνοχώρο θέτει πολλές προκλήσεις για την επιβολή του νόμου (Brenner, 2010: 135).

Όταν τα εγκλήματα στον κυβερνοχώρο αφορούν θύματα σε μια χώρα και δράστες σε άλλη χώρα, η αστυνομία δεν μπορεί να βασιστεί στις διαδικασίες που συνήθως χρησιμοποιεί για να βρει αποδεικτικά στοιχεία ή / και να συλλάβει εγχώριους δράστες. Επιπλέον, αντιμετωπίζουν δύο προκλήσεις. Η μία πρόκληση είναι η συλλογή αποδεικτικών στοιχείων από το εξωτερικό και η άλλη πρόκληση είναι η κράτηση υπόπτων στο εξωτερικό (Brenner, 2010: 141). Οι κοινωνίες πρέπει να διατηρήσουν την τάξη, τόσο εσωτερικά όσο και εξωτερικά γι' αυτό τον λόγο η επιβολή του νόμου είναι ευθύνη των κρατών αλλά και συνάρτηση του ενδιαφέροντος ενός έθνους-κράτους για τη διατήρηση της τάξης εντός της επικράτειας που ελέγχει (Brenner, 2010: 172). Ωστόσο, όλο το έγκλημα στον κυβερνοχώρο είναι ένα νέο έγκλημα επειδή φέρνει πρωτοφανείς προκλήσεις στις υπηρεσίες επιβολής του νόμου και η φύση αυτών των προκλήσεων καθιστά δύσκολο για τις υπηρεσίες επιβολής του νόμου να ξεπεράσουν αυτές τις προκλήσεις (Brenner, 2010: 207). Η δυσκολία να συμβαδίζει με αυτό που κάνουν οι εγκληματίες στον κυβερνοχώρο επιδεινώνεται από την αφάνεια του περιβάλλοντος τους (Brenner, 2010: 220).

Η κυβέρνηση πρέπει να δαπανήσει χρήματα και πόρους για την πρόληψη και την επιβολή του νόμου (Clough, 2010: 200). Ωστόσο, υπάρχουν ακόμη κενά στις εθνικές και ευρωπαϊκές στρατηγικές για την ασφάλεια στον κυβερνοχώρο, όπως η έλλειψη των απαραίτητων δυνατοτήτων για την άμυνα ενάντια σε νέες προκλήσεις στον κυβερνοχώρο, η έλλειψη δεξιοτήτων ασφάλειας στον κυβερνοχώρο και η έλλειψη εμπορικών και οικονομικών κενών, ειδικά στο στάδιο της ανάπτυξης. Με την καθοδήγηση της κρίσης COVID-19, ο ψηφιακός μετασχηματισμός της κοινωνίας έχει επεκτείνει το πεδίο των απειλών και έφερε νέες προκλήσεις, απαιτώντας προσαρμοστικά και καινοτόμα μέτρα αντιμετώπισης. Ο αριθμός των επιθέσεων στον κυβερνοχώρο συνεχίζει να αυξάνεται και οι επιθέσεις από διάφορες πηγές εντός και εκτός της ΕΕ γίνονται όλο και πιο περίπλοκες. Επομένως, η ΕΕ πρέπει να πρωτοστατήσει στην ασφαλή ψηφιοποίηση.

4.2 Πολιτικές Αντιμετώπισης στην Ε.Ε.

Η Europol δημιούργησε το Ευρωπαϊκό Κέντρο Εγκλήματος (EC3) στον κυβερνοχώρο το 2013 για να ενισχύσει την αποδοχή επιβολής του νόμου στο έγκλημα στον κυβερνοχώρο της ΕΕ, συμβάλλοντας έτσι στην προστασία των ευρωπαίων πολιτών, επιχειρήσεων και κυβερνήσεων από το έγκλημα στον κυβερνοχώρο. Η επιτροπή προγράμματος EC3 παρέχει καθοδήγηση στο EC3 σχετικά με τον τρόπο επίτευξης των στόχων του και την εκπλήρωση των επίσημων καθηκόντων του με βάση την εταιρική σχέση, τον καταμερισμό ευθυνών και τη συνεργασία με όλα τα μέλη της επιτροπής διαχείρισης (Europol, 2021). Πιο συγκεκριμένα, το EC3 ακολουθεί μια τρισδιάστατη προσέγγιση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο: εγκληματολογία, στρατηγική και επιχειρήσεις.

Διαθέτει δύο ομάδες εγκληματολογίας, 1) την ψηφιακή εγκληματολογία και 2) την εγκληματολογία εγγράφων, καθεμία από τις οποίες επικεντρώνεται στην επιχειρησιακή υποστήριξη και στην έρευνα και ανάπτυξη, και υπάρχουν δύο ομάδες στρατηγικής: α) αυτή που ασχολείται με την πρόληψη και διαχείριση ενδιαφερομένων, η οποία καθιερώνει εταιρικές σχέσεις, διασφαλίζει την ανάπτυξη τυποποιημένης εκπαίδευσης και συντονίζει μέτρα πρόληψης και ευαισθητοποίησης και β) στρατηγική και ανάπτυξη, η οποία είναι υπεύθυνη για την στρατηγική ανάλυση, τη χάραξη πολιτικών και νομοθετικών μέτρων και τη Διακυβέρνηση Διαδικτύου (Europol, 2021). Όσον αφορά το επίπεδο επιχειρήσεων, το EC3 επικεντρώνεται στους εξής τύπους εγκλημάτων στον κυβερνοχώρο: Cyber-dependent έγκλημα, σεξουαλική εκμετάλλευση παιδιών στο διαδίκτυο και απάτη πληρωμών (Europol, 2021).

Η Ευρωπαϊκή Επιτροπή και ο Ύπατος Εκπρόσωπος της ΕΕ για την εξωτερική πολιτική και την πολιτική ασφάλειας υπέβαλαν μια νέα στρατηγική της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο στα τέλη του 2020 (European Commision, 2020). Καλύπτει την ασφάλεια του συνεχώς αυξανόμενου αριθμού συνδεδεμένων αντικειμένων στα σπίτια, τα γραφεία και τα εργοστάσια, δημιουργεί συλλογικές ευκαιρίες να ανταποκριθούν τα κράτη σε μεγάλες κυβερνοεπιθέσεις και αναπτύσσεται σχέση αμοιβαίας βοήθειας με συνεργάτες σε όλο τον κόσμο για να διασφαλίσει την ασφάλεια και τη σταθερότητα του διεθνούς δικτύου. Η στρατηγική περιγράφει πώς

ένας γενικός τομέας στον κυβερνοχώρο μπορεί να χρησιμοποιήσει τους συλλογικούς πόρους και την εμπειρογνωμοσύνη της ΕΕ και των κρατών μελών για να εξασφαλίσει την πιο αποτελεσματική απάντηση στις απειλές στον κυβερνοχώρο (European Commision, 2020).

Με την επιταχυνόμενη ανάπτυξη του ψηφιακού μετασχηματισμού σε παγκόσμια κλίμακα και όλο και πιο διαδραστική φιλοξενία στο Διαδίκτυο, οι πολίτες, οι εταιρείες και οι κυβερνήσεις εκτίθενται όλο και περισσότερο σε απειλές στον κυβερνοχώρο και σε ψηφιακά εγκλήματα (European Commision, 2020). Η ΕΕ υποστηρίζει επίσης την ανάγκη συντονισμένης προσέγγισης για τον μετριασμό των κινδύνων στον κυβερνοχώρο, διότι το Συμβούλιο της Ευρωπαϊκής Ένωσης τόνισε τη σημασία της ασφάλειας στον κυβερνοχώρο ως «βασικό στοιχείο της ψηφιακής ενιαίας αγοράς, διότι διασφαλίζει την εμπιστοσύνη στην ψηφιακή τεχνολογία και τη διαδικασία ψηφιακού μετασχηματισμού» (European Commision, 2020). Η ΕΕ διαθέτει ένα ισχυρό ακαδημαϊκό ερευνητικό ίδρυμα στην ασφάλεια στον κυβερνοχώρο, την βιομηχανική έρευνα, ανάπτυξη προϊόντων και σχετικές δραστηριότητες.

Η κύρια πρόκληση για την Ευρώπη είναι το γεγονός, ότι η βιομηχανία ασφάλειας στον κυβερνοχώρο είναι πιο ανεπτυγμένη σε μη ευρωπαϊκούς παίκτες και πάροχους υπηρεσιών, όπως και έχει διαπιστωθεί σε διάφορες μελέτες. Ο στόχος της νέας στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο που έχει προταθεί ως μέρος του «Σχεδίου Ανάκαμψης 2020» είναι να: 1) ενισχύσει περαιτέρω τη συνεργασία, τη γνώση και την ικανότητα σε επίπεδο ΕΕ, 2) να ενισχύσει στην ΕΕ τις βιομηχανικές δυνατότητες και εταιρικές σχέσεις, 3) ενθάρρυνση της εμφάνισης ΜΜΕ στον τομέα και 4) προστασία ως κρίσιμη υποδομή (European Commision, 2020).

Αρχικά, ο ENISA αποτελεί έναν οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο («Οργανισμός Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών») και παρέχει υποστήριξη σε κράτη μέλη, θεσμικά όργανα και επιχειρήσεις της ΕΕ σε βασικούς τομείς, συμπεριλαμβανομένης της εφαρμογής του NIS Directive. Ο ευρωπαϊκός νόμος για την ασφάλεια στον κυβερνοχώρο τέθηκε σε

ισχύ τον Ιούνιο του 2019 και καθιέρωσε ένα κοινοτικό πλαίσιο για την πιστοποίηση της κυβερνοασφάλειας, ενισχύοντας έτσι την ασφάλεια στον κυβερνοχώρο των διαδικτυακών υπηρεσιών και των καταναλωτικών συσκευών. Προκειμένου να υποστηρίξει καλύτερα τα κράτη μέλη στην αντιμετώπιση απειλών και επιθέσεων στον κυβερνοχώρο, ο ENISA υποχρεούται να βελτιώσει τις δυνατότητες της κυβερνοασφάλειας σε επίπεδο ΕΕ και να συνεργαστεί στενά με τα κράτη μέλη για την υποστήριξη της ανάπτυξης ικανοτήτων και των προετοιμασιών. Η Ευρωπαϊκή Επιτροπή έχει δεσμευτεί να δημιουργήσει ένα ευρωπαϊκό κέντρο ικανότητας για τη βιομηχανία δικτύων, την τεχνολογία και την έρευνα, ένα δίκτυο εθνικών κέντρων συντονισμού και μια κοινότητα αρμοδιοτήτων ασφάλειας δικτύου. Η πρόταση στοχεύει στην ενίσχυση των δυνατοτήτων ασφάλειας στον κυβερνοχώρο της ενθαρρύνοντας τα ευρωπαϊκά οικοσυστήματα τεχνολογίας και βιομηχανικής ασφάλειας στον κυβερνοχώρο, καθώς και συντονίζοντας και συγκεντρώνοντας σχετικούς πόρους.

Το στρατηγικό φόρουμ για σημαντικά έργα κοινού ευρωπαϊκού ενδιαφέροντος (IPCEI) ανέπτυξε ένα κοινό όραμα για την «Ασφάλεια στον κυβερνοχώρο στην Ευρώπη έως το 2030», χρησιμεύοντας ως οδηγός για τη διαμόρφωση, την ιεράρχηση και τον συντονισμό συστάσεων για δράσεις (European Commision, 2020). Αυτό το όραμα στοχεύει στη διασφάλιση της ανταγωνιστικότητας του κλάδου της ασφάλειας στον κυβερνοχώρο της ΕΕ στην παγκόσμια αγορά ασφάλειας στον κυβερνοχώρο και στην αύξηση των επιπέδων προστασίας με την κατάλληλη λύση στην κυβερνοασφάλεια. Η ΕΕ, έτσι, θα αυξήσει επίσης την αυτονομία και την τεχνολογική της κυριαρχία στην ασφάλεια στον κυβερνοχώρο και θα επιτύχει παγκόσμια βιομηχανική ηγεσία. Οι προτεινόμενες συντονισμένες επενδύσεις είναι οι εξής, σύμφωνα με την Ευρωπαϊκή Κομισιόν:

1. Ασφαλές 5G για καινοτομία και υπηρεσίες στον κυβερνοασφάλεια

2. Κοινοποίηση και εκμετάλλευση πληροφοριών σχετικά με απειλές, ευπάθεια και περιστατικά

3. Εξασφάλιση εξαιρετικά κρίσιμων εφαρμογών και βασικών υπηρεσιών: ηλεκτρική ενέργεια, φυσικό αέριο, νερό, οχήματα

4. Ανάπτυξη και προώθηση λύσεων προστασίας δεδομένων από άκρο σε άκρο χρησιμοποιώντας προηγμένη κρυπτογραφία

5. Ευρωπαϊκός χώρος δεδομένων: δημιουργία πλαισίου και υποδομής για ασφαλή επικοινωνία, αποθήκευση και διαχείριση δεδομένων

Ο Παγκόσμιος Δείκτης Cybersecurity (GCI) αποτυπώνει τη δέσμευση των χωρών για την κυβερνοασφάλεια σε παγκόσμιο επίπεδο και για την ευαισθητοποίηση σχετικά με τη σημασία και τις διαφορετικές διαστάσεις του ζητήματος. Καθώς η ασφάλεια στον κυβερνοχώρο έχει ένα ευρύ πεδίο εφαρμογής, καλύπτοντας πολλές βιομηχανίες και διάφορους τομείς, το επίπεδο ανάπτυξης ή εμπλοκής κάθε χώρας αξιολογείται σε πέντε πυλώνες, δηλαδή, σε νομικά, τεχνικά, οργανωτικά μέτρα, την ανάπτυξη ικανοτήτων και τη συνεργασία (European Commision, 2020). Σύμφωνα με αυτό τον δείκτη, υπάρχει ένα μεγάλο κενό στη δέσμευση στον κυβερνοχώρο σε όλο τον κόσμο. Στις πιο αφοσιωμένες χώρες της ΕΕ, βρίσκουμε τη Γαλλία, τη Λιθουανία, την Εσθονία και την Ισπανία.

Ο Εθνικός Δείκτης Ασφάλειας στον κυβερνοχώρο μετρά τις αξιολογήσεις ασφάλειας στον κυβερνοχώρο χωρών στον κόσμο. Σύμφωνα με αυτήν τη διαφορετική μέτρηση, οι δέκα κορυφαίες χώρες που είναι καλύτερα προετοιμασμένες για επιθέσεις στον κυβερνοχώρο είναι η Ελλάδα, η Τσεχία και η Εσθονία, η Λιθουανία, η Ισπανία, η Κροατία, η Γαλλία, η Φινλανδία, η Δανία και οι Κάτω Χώρες. Στην ΕΕ οι χώρες με το υψηλότερο μερίδιο επαγγελματιών με ειδικές τεχνολογικές δεξιότητες στη κυβερνοασφάλεια περιλαμβάνει το Λουξεμβούργο, την Κύπρο, Ισπανία, Γαλλία, Ιρλανδία, Ιταλία και Εσθονία. Το 86% των επαγγελματιών με δεξιότητες ασφάλειας στον κυβερνοχώρο είναι άντρες που δείχνουν σε μεγάλο βαθμό το χάσμα των φύλων στον τομέα. Χώρες όπου το χάσμα είναι σχετικά μικρότερο και απασχολούνται περισσότερες γυναίκες είναι η Ιταλία, η Ρουμανία και η Ιρλανδία (European Commision, 2020).

Υπάρχουν διάφορα κενά στις εθνικές και ευρωπαϊκές στρατηγικές ασφάλειας στον κυβερνοχώρο που εμποδίζουν την ανάπτυξη μιας ισχυρότερης βιομηχανίας στον κυβερνοασφάλεια. Ορισμένα κράτη μέλη δεν διαθέτουν τις απαραίτητες δυνατότητες για να υπερασπιστούν τις αναδυόμενες τάσεις που καθιστούν την ευρωπαϊκή αρχιτεκτονική στον κυβερνοχώρο πιο ευάλωτη σε πιθανές επιθέσεις. Για να αναπτύξουν μια ισχυρή ευρωπαϊκή βιομηχανία στον τομέα της ασφάλειας στον κυβερνοχώρο, οι εταιρείες θα χρειαστούν επίσης περισσότερες επιχειρηματικές δεξιότητες προκειμένου να αξιοποιήσουν την τεχνολογία αιχμής. Ωστόσο, όλα τα κράτη μέλη της ΕΕ έχουν τις δικές τους εθνικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο, οι οποίες αποτελούν μια συλλογή προγραμματισμένων δράσεων για τη βελτίωση της ασφάλειας και της ανθεκτικότητας των εθνικών υποδομών και υπηρεσιών (European Commision, 2020).

4.3 Πολιτικές Αντιμετώπισης στην Ελλάδα

Με το Π.Δ. 178/2014 προβλέφθηκε η ίδρυση και η διάρθρωση της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και βασικός σκοπός της ήταν η πρόληψη, η έρευνα και η καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος αποτελεί μια αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας και σύμφωνα με την Ελληνική Αστυνομία και το Υπουργείο Προστασίας του Πολίτη στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών,

β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής,

γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων,

δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και

ε. Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων

Το Μάρτιο του 2018, κατόπιν εισήγησης της Εθνικής Αρχής Κυβερνοασφάλειας, εκδόθηκε η 3η Αναθεώρηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Στην εν λόγω στρατηγική προσδιορίσθηκαν ως γενικές αρχές (Υπ. Ψηφιακής Διακυβέρνησης, 2020):

1. Η ανάπτυξη και εδραίωση ενός ασφαλούς και ανθεκτικού κυβερνοχώρου.

2. Η συνεχής βελτίωση των δυνατοτήτων μας στην προστασία από κυβερνοεπιθέσεις με έμφαση στις κρίσιμες υποδομές και η διασφάλιση της επιχειρησιακής συνέχειας.

3. Η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.

4. Η ανάπτυξη ισχυρής κουλτούρας ασφάλειας των πολιτών, του δημόσιου και ιδιωτικού τομέα, αξιοποιώντας τις σχετικές δυνατότητες της ακαδημαϊκής κοινότητας και εν γένει των φορέων του δημόσιου και ιδιωτικού τομέα.

Όσον αφορά το τρέχον στρατηγικό σχέδιο ασφάλειας στον κυβερνοχώρο, η Ελλάδα έχει υιοθετήσει ευρωπαϊκά πρότυπα και μεθόδους για τη διαμόρφωση αυτού του σχεδίου και των στόχων της.

Λαμβάνοντας υπόψη τα συμπεράσματα της ανάλυσης αποκλίσεων (gap analysis), η οποία πραγματοποιήθηκε από την Εθνική Αρχή Κυβερνοασφάλειας, οι τομείς στρατηγικού ενδιαφέροντος για την 4η Αναθεώρηση εκτείνονται σε έξι (6) διαστάσεις: στο σχεδιασμό έκτακτης ανάγκης, αναφορές περιστατικών (Incident reporting), ασφάλεια και προστασία της ιδιωτικότητας, έρευνα και ανάπτυξη, Συμπράξεις Δημοσίου – Ιδιωτικού Τομέα (ΣΔΙΤ) και στις επενδύσεις στα μέτρα ασφάλειας (Υπ. Ψηφιακής Διακυβέρνησης, 2020). Επιπλέον, οι στρατηγικοί στόχοι έχουν την ίδια κατευθυντήρια γραμμή με τους στόχους του ENISA για όλα τα κράτη-μέλη, δηλαδή: 1. ένα λειτουργικό σύστημα διακυβέρνησης, 2. θωράκιση κρίσιμων

υποδομών, ασφάλεια και νέες τεχνολογίες, 3. βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας, 4. ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης και 5. ανάπτυξη ικανοτήτων (capacity building) και προαγωγή της ενημέρωσης και ευαισθητοποίησης

Η οργάνωση των Υπηρεσιών της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), καθόρισε τις αρμοδιότητες της Διεύθυνσης Κυβερνοχώρου της Ε.Υ.Π., στις οποίες περιλαμβάνονται (Υπ. Ψηφιακής Διακυβέρνησης, 2020):

α) τεχνικής φύσεως θέματα ασφάλειας πληροφοριών (Εθνική Αρχή INFOSEC) και ειδικότερα για την ασφάλεια των εθνικών επικοινωνιών, των συστημάτων τεχνολογίας πληροφοριών, καθώς και για την αξιολόγηση και πιστοποίηση των διαβαθμισμένων συσκευών και συστημάτων ασφάλειας επικοινωνιών και πληροφορικής

β) η αξιολόγηση και πιστοποίηση κρυπτοσυστημάτων, καθώς και την υποστήριξη των Ενόπλων Δυνάμεων (Ε.Δ.) και των υπηρεσιών του δημοσίου τομέα σε θέματα κρυπτασφάλειας (Εθνική Αρχή CRYPTO),

γ) η εξασφάλιση των εθνικών ηλεκτρονικών συσκευών τηλεπικοινωνιών από διαρροές λόγω ανεπιθύμητων, ηλεκτρομαγνητικών και μη μεταδόσεων (Εθνική Αρχή TEMPEST),

δ) οι αρμοδιότητες Ομάδας Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT), εντός του εθνικού πλέγματος Κυβερνοασφάλειας που καθορίζει η Εθνική Αρχή Κυβερνοασφάλειας, για τις κυβερνοεπιθέσεις εναντίον των δημοσίων φορέων της χώρας, που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του Γ.Ε.ΕΘ.Α. (CSIRT). Ειδικότερα, το Εθνικό CERT της Ε.Υ.Π. υποστηρίζει την Προεδρία της Κυβέρνησης και τα Υπουργεία, με εξαίρεση το Υπουργείο Εθνικής Άμυνας, για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων, εναντίον τους.

Γενικότερα, ο στόχος είναι να δημιουργηθεί ένα σύγχρονο ψηφιακό περιβάλλον που θα επιτρέπει τη συνεχή εισροή και ανάπτυξη νέων τεχνολογιών και καινοτομιών στην ψηφιακή εποχή με κύριο γνώμονα την προστασία.

Κεφάλαιο 5: Συμπεράσματα

Στην πραγματικότητα, υπάρχουν πολλές και περίπλοκες συζητήσεις σχετικά με το έγκλημα στον κυβερνοχώρο. Το έγκλημα στον κυβερνοχώρο – παρόμοιο με κάθε έγκλημα – περιλαμβάνει μια «μάχη μεταξύ καλού και κακού», δηλαδή μεταξύ των δυνάμεων της τάξης και των δυνάμεων της αταξίας (Brenner, 2010: 207). Διαφορετικές ομάδες που μπορεί να μην συμμετείχαν σε παραδοσιακές εγκληματικές δραστηριότητες πριν από πολλά χρόνια άρχισαν να προσελκύονται από το έγκλημα στον κυβερνοχώρο, επειδή υπάρχουν πολλά κενά στον ηλεκτρονικό κόσμο και είναι σχετικά εύκολο να αξιοποιηθούν. Σε σύγκριση με πολλά παραδοσιακά εγκλήματα, το έγκλημα στον κυβερνοχώρο είναι πιο βολικό αφού στην πραγματικότητα, οι παραβάτες μπορούν να μένουν στο σπίτι και να πίνουν μπύρα ενώ διαπράττουν έγκλημα (Preatoni, 2003 οπ. αναφ. οι Schell & Martin, 2004: 104), ενώ στο παρελθόν, οι εγκληματίες έπρεπε να βγουν έξω για να κλέψουν, να επιτεθούν ή να τσακωθούν. Εάν οι χώρες θέλουν να βελτιώσουν την ικανότητά τους να προλαμβάνουν και να ελέγχουν το έγκλημα στον κυβερνοχώρο, θα πρέπει: 1) να τροποποιήσουν το τρέχον μοντέλο επιβολής του νόμου, ώστε να μπορούν να ανταποκριθούν αποτελεσματικά στο διεθνοποιημένο έγκλημα στον κυβερνοχώρο ή/και 2) να αναπτύξουν νέες προσεγγίσεις για το έγκλημα στον κυβερνοχώρο (Brenner, 2010: 208).

Αρχικά, πολιτική αντιμετώπισης του εγκλήματος είναι το σύνολο των κατασταλτικών διαδικασιών μέσω των οποίων το κράτος αντιδρά στο έγκλημα (Fauerbach, 1803). Επιπλέον, σε μια εισήγηση στο Συμβούλιο της Ευρώπης, η αντεγκληματική πολιτική ορίστηκε ως «το σύνολο των μέτρων που τείνουν στην προστασία της κοινωνίας από την εγκληματικότητα, στη φροντίδα για την μελλοντική εξέλιξη του εγκληματία και τη διασφάλιση των δικαιωμάτων του θύματος». Γενικότερα, πρόκειται για μια πολυπαραγοντική έννοια που μεταβάλλεται ταυτόχρονα με την κοινωνία. Είναι σημαντικό να προσθέσουμε πως η αντεγκληματική πολιτική εμφανίζει τις εξής σύγχρονες τάσεις, σύμφωνα με την Κωνσταντίνου (2018):

Α)Κοινωνική Αντεγκληματική Πολιτική

1. Μηδενική Ανοχή: Βασικοί στόχοι είναι η μείωση της εγκληματικότητας και η αποκατάσταση της τάξης και της ασφάλειας. Κατά το 1980 αναπτύχθηκε αυτή

η θεωρία στις ΗΠΑ και τέθηκε σε εφαρμογή πρώτη φορά στην Νέα Υόρκη το 1933. Θεμελιωτές της θεωρίας είναι ο Wilson και ο Kelling μέσα από ένα πείραμα από τον καθηγητή ψυχολογίας, Zimbardo. Το πείραμα αυτό έδειξε πως οι βανδαλισμοί και οι εγκληματικές πράξεις μπορούν να γίνουν οπουδήποτε, εφόσον δεν υπάρξει έλεγχος της παραβατικής συμπεριφοράς και γενικότερα, όταν υπάρχει ένα κλίμα απαξίωσης προς τέτοιου είδους συμπεριφορές, η αταξία μπορεί να αυξηθεί και ταυτόχρονα η αρχή της αμοιβαιότητας των σχέσεων μέσα στην κοινωνία να υποβαθμιστεί ("κανένας δεν νοιάζεται"). Μια περιοχή με σημάδια παραμέλησης έχει περισσότερες πιθανότητες να οδηγήσει τα άτομα σε παραβατική συμπεριφορά. Η στρατηγική της μηδενικής ανοχής έχει ως στόχο την καταπολέμηση οργανωμένων και βίαιων εγκλημάτων με εξειδικευμένες δράσεις αντιμετώπισης. Οι επικριτές, ωστόσο, θεωρούν πως μπορεί να οδηγήσει σε κατάχρηση εξουσίας από την αστυνομία και στην διατάραξη της σχέσης του πολίτη με την αστυνομία.

2. Κοινοτική πρόληψη: Ο όρος community crime prevention είναι εμπνευσμένος από τον αγγλοσαξονικό χώρο. Η κοινοτική πρόληψη μαζί με την παιδαγωγική πρόληψη συμπεριλαμβάνονται στο πακέτο κοινωνικής πρόληψης της αντεγκληματικής πολιτικής, το οποίο παραπέμπει στο συναινετικό μοντέλο αξιών και σε μία κοινότητα, τα μέλη της οποίας ενώνονται για να αντιμετωπίσουν μαζί έναν κοινό στόχο, δηλαδή την μείωση της εγκληματικότητας στη γειτονιά-κοινότητά τους. Η πρόληψη αυτή βρίσκει αντίκτυπο και δράση μέσω κοινωνικών φορέων, κυρίως, όμως, μέσω αστυνομίας. Εφαρμόστηκε πρώτα στις ΗΠΑ και στην Γαλλία και ύστερα ακολούθησαν Αγγλία, Ολλανδία, Βέλγιο, Ισπανία, Γερμανία και Ελλάδα. Κατά το 1980 οι ΗΠΑ χρησιμοποίησαν στρατηγικές όπως neighborhood watch (επιτήρηση γειτονιάς), footpatrol (πεζές περιπολίες) και storefront (αστυνομικοί σταθμοί) ενώ η Γαλλία εστίασε την καταπολέμηση μέσω της εκπαίδευσης και της κοινωνικής δράσης.

Β) Επανορθωτική - Αποκαταστατική Αντεγκληματική Πολιτική Ποινική Διαμεσολάβηση

Η επανορθωτική/αποκαταστατική δικαιοσύνη θεμελιώθηκε από τον Englash το 1977 και ουσιαστικά αποτελεί μια έννοια "ομπρέλα", που περιλαμβάνει αφ' ενός ένα αξιακό για την δικαιοσύνη πλαίσιο και αφ' ετέρου μια ευρύτητα και ποικιλομορφία πρακτικών, όπως είναι η διαμεσολάβηση και οι συνεδρίες σε κύκλους στο πλαίσιο τοπικών κοινωνιών. Κρίνεται απαραίτητη ωστόσο, όταν πρόκειται για ποινική διαμεσολάβηση, η επιθυμία για συμμετοχή και των δύο πλευρών δράστη και θύματος" (Shapland, 2006).

Βασικοί στόχοι:

1) Η δικαιοσύνη επιβάλλει την αποκατάσταση αυτών που επλήγησαν.

2) Τα μέρη που ενεπλάκησαν και επηρεάστηκαν από το έγκλημα πρέπει να έχουν την ευκαιρία να συμμετέχουν πλήρως στην διαδικασία απονομής δικαιοσύνης εάν το επιθυμούν.

3) Ο ρόλος των τοπικών κοινοτήτων πρέπει να είναι ενδυναμωμένος, με στόχο την επίτευξη και διατήρηση της κοινωνικής ειρήνης.

Επίσης, δημιουργήθηκαν 2 τάσεις σε αυτήν την δικαιοσύνη:

a) Μαξιμαλιστική= ριζική αλλαγή του συστήματος απονομής ποινικής δικαιοσύνης και αντικατάστασής του από το σύστημα αξιών-προτάσεών της. (Ν. Ζηλανδία, Αυστραλία)

b) Μινιμαλιστική= λειτουργεί συμπληρωματικά ή εναλλακτικά μόνο στις περιπτώσεις πλημμελημάτων. (Καναδάς, Πολιτείες Β. Αμερικής, χώρες της Β. Ευρώπης, Μ. Βρετανία)

Εφόσον, κατανοήσαμε την αντεγκληματική πολιτική ως έννοια, θα προχωρήσουμε τώρα στην ανάλυση του κυβερνοεγκλήματος και των υπηρεσιών που προσπαθούν να το καταπολεμήσουν. Πρώτον, το έγκλημα μπορεί να εμφανιστεί και σε εθνικό επίπεδο και σε διεθνικό επίπεδο κάτι στο οποίο έχει συμβάλλει η παγκοσμιοποίηση. Μια δεύτερη διάκριση του εγκλήματος είναι η εξής:

1. Πταίσμα: τιμωρείται με πρόστιμο (από 29 έως 590 ευρώ) ή κράτηση (1 ημέρα έως 1 μήνα)
2. Πλημμέλημα: τιμωρείται με χρηματική ποινή (από 150 έως 150.000 ευρώ) ή με φυλάκιση (10 ημέρες έως 5 χρόνια)

3. Κακούργημα: τιμωρείται με κάθειρξη ισόβια ή πρόσκαιρη (5 έως 20 χρόνια) (lawspot.gr, 2017)

Στην Ελλάδα ωστόσο, με νόμο που εκδόθηκε το 2019 το πταίσμα σαν αδίκημα καταργήθηκε και κάποιες πράξεις που ήταν πταίσματα δεν θα τιμωρούνται καν και κάποιες άλλες έγιναν πλημμελήματα.

Η Ελληνική Αστυνομία είναι μια Υπηρεσία Επιβολής του Νόμου σύμφωνα με τον Νόμο αρ. 2800/2000 και η αποστολή της είναι: 1) να διασφαλίσει την ειρήνη και την τάξη καθώς και την απρόσκοπτη κοινωνική ανάπτυξη των πολιτών και 2) την πρόληψη και απαγόρευση του εγκλήματος καθώς και για την προστασία του κράτους. Με Προεδρικό Διάταγμα 178/2014 έχουμε την ίδρυση ενός νέου κλάδου, της Διεύθυνσης Εγκλήματος στον κυβερνοχώρο. Η υπακοή στους νόμους όπως και η υποστήριξη και αποδοχή των θεσμών απονομής της ποινικής δικαιοσύνης (Αστυνομία και Δικαστήρια) εξαρτώνται καθαρά από το επίπεδο της εμπιστοσύνης και της νομιμοποίησης οι θεσμοί αυτοί θα απολαύουν από την ίδια την κοινωνία (Τσιγκανού, 2016). Αυτό το επιβεβαιώνουν και τα εξής ευρήματα:

- Πριν την έλευση της κρίσης εμφανίζεται μια παγιωμένη κρίση δυσπιστίας των Ελλήνων πολιτών στο σύστημα πολιτικής αντιπροσώπευσης που συμπαρασύρει και την παράμετρο της κρίσης εμπιστοσύνης στα Δικαστήρια και την Αστυνομία.
- Το 2010 τα ευρήματα υποδεικνύουν ένα συνεχώς διογκούμενο αίσθημα ανασφάλειας και ‘απειλής’ που διαπερνά τόσο τις διαπροσωπικές σχέσεις όσο και τη στάση του κοινωνικού σώματος απέναντι στους θεσμούς.
- Μόλις το ½ δηλώνει ότι η Αστυνομία αντιμετωπίζει τους ανθρώπους στην Ελλάδα με σεβασμό.
- Κατά τα 2/3 το κοινωνικό σώμα διακατέχεται επίσης από την πεποίθηση ότι η αστυνομία επιδεικνύει ρατσιστική συμπεριφορά καθώς «συμπεριφέρεται χειρότερα σε θύματα εγκληματικών ενεργειών που ανήκουν σε διαφορετική φυλή ή εθνική ομάδα απ’ ότι οι περισσότεροι Έλληνες» (οπ. αναφ. Τσιγκανου, 2016)

Σύμφωνα με την Αθανασία Συκιώτου (2018) - αναπληρώτρια Καθηγήτρια Εγκληματολογίας της Νομικής Σχολής του Δημοκρίτειου Παν/μίου Θράκης και

Συντονίστρια του Εργαστηρίου Εγκληματολογικών Επιστημών - η νέα τάση στην αντεγκληματική πολιτική εστιάζει περισσότερο στην «τεχνολογική εξουδετέρωση» του εγκληματικού κινδύνου. Είναι αυτή που χαρακτηρίζεται ως «διαχειριστική» (managerial), υπογραμμίζοντας την ασφαλιστική και αναλογιστική (actuarial) λογική της, τόσο στον έλεγχο του εγκλήματος, όσο και στον τρόπο απονομής της δικαιοσύνης. Στόχος της τάσης αυτής δεν είναι η βελτίωση ή επανένταξη εγκληματιών, αλλά η μεθοδολογική εξουδετέρωση της επικινδυνότητας των πράξεών τους. Οι ποινές οδηγούνται περισσότερο από την ιδέα της ασφάλειας της κοινωνίας παρά από αυτή της επανένταξης του εγκληματία, γιατί απλά θεωρούμε ότι αυτός είναι καλύτερα να εξουδετερωθεί για τη δική μας ασφάλεια. Στην έκθεση της Ευρωπαϊκής Επιτροπής για την Κυβερνοασφάλεια συγκεκριμένα αναφέρεται ότι «οι χρήστες του Διαδικτύου εκφράζουν υψηλά επίπεδα ανησυχίας για το έγκλημα στον κυβερνοχώρο. Η πλειοψηφία συμφωνεί ότι ο κίνδυνος να πέσει θύμα εγκλήματος στον κυβερνοχώρο αυξάνεται και ανησυχούν ότι τα διαδικτυακά προσωπικά τους στοιχεία δεν διατηρούνται ασφαλή από ιστότοπους ή από δημόσιες αρχές» (European Commision, 2015: 94).

Η Αντεγκληματική Πολιτική σήμερα δέχεται όλο και περισσότερο υπερεθνικές πιέσεις και όσο προχωρά ραγδαία η παγκοσμιοποίηση, τόσο ολισθαίνει το φιλελεύθερο και δημοκρατικό μοντέλο της Αντεγκληματικής πολιτικής (Συκιώτου, 2018). Μέσω της παγκοσμιοποίησης επηρεάζεται η οικονομία, ο πολιτισμός και η πολιτική και η ίδια επιθυμεί να εμφανίσει ως μια απλή ιδέα την διεθνοποίηση του δικαίου. Για αυτό τον λόγο πλέον, ο εθνικός νομοθέτης δεν μπορεί να παρέμβει και να ελέγξει με την ίδια ευκολία πριν μερικά χρόνια. Ιδιαίτερα όταν μια χώρα εντάσσεται σε κάποιον Διεθνή Οργανισμό, η υπακοή στις κατευθυντήριες γραμμές που ορίζει πρέπει να ακολουθούνται από όλες τις χώρες ώστε να επιτευχθεί η αντιμετώπιση των κυβερνοεγκλημάτων. Επιπλέον, η διεθνής συνεργασία, εντός και εκτός του πλαισίου των διεθνών θεσμών, οφείλει να αντιλαμβάνεται ότι αντιμετωπίζει αποτελεσματικά το έγκλημα όταν στρέφει τις δυνάμεις της στην ενίσχυση των κρατών στα οποία αυτό εκδηλώνεται πιο έντονα, και όχι απλά στην καθιέρωση πλήθους ρυθμίσεων που δεν πρόκειται να εφαρμοστούν σε πλήρη έκταση και με επαρκή συνέπεια από τα εμπλεκόμενα κράτη (Μπόση & Βασιλειάδης, 2016). Είναι προφανές ότι το

οργανωμένο έγκλημα με τις δράσεις του, οι σημαντικότερες εκ των οποίων περιλαμβάνουν το εμπόριο ναρκωτικών, την παράνομη διακίνηση ανθρώπων, το εμπόριο όπλων και το ξέπλυμα μαύρου χρήματος, αποτελεί ένα φαινόμενο που υποσκάπτει την ομαλή λειτουργία των κρατών, απειλεί την κοινωνική τους συνοχή και τελικά μπορεί να θίξει την ασφάλειά τους τόσο στο εσωτερικό όσο και στις εξωτερικές τους σχέσεις (Μπόση & Βασιλειάδης, 2016). Ο Ruggiero αιτιολογεί το έγκλημα στην παράδοση, την απουσία κράτους, την παθολογία, την έλλειψη ελέγχου, τη σχετική φτώχεια, τις παρεμβατικές υποκουλτούρες και από μια ανεπάρκεια είτε για έλεγχο, είτε λογικότητας (χαμηλός αυτοέλεγχος) (οπ. αν. Λαμπροπούλου, 2003).

Μέσω του Διαδικτύου, δημιουργήθηκε ένας παγκόσμια προσβάσιμος και διακρατικός εικονικός κόσμος, με αποτέλεσμα να ρυθμίζεται σε μεγάλο βαθμό με ad hoc τρόπο, καθιστώντας το ένα περιβάλλον για εγκληματικές ενέργειες και καθώς διαφέρει σημαντικά από τον φυσικό-πραγματικό κόσμο, τα κράτη εμφανίστηκαν ανέτοιμα για τον έλεγχο και ρύθμισή του (Alkaabi, Ali and Mohay, George and McCullagh, Adrian J. and Chantler, Alan, 2010). Ο ίδιος ο White (2020: 311) αναφέρει πως ο σύγχρονος και πλούσιος σε δεδομένα κόσμος μας είναι πολύ γεμάτος από όλο και πιο σύνθετες, αλληλένδετες τεχνολογίες και κενά ασφαλείας για να αποτρέψει τους χάκερ να περάσουν. Η πανταχού παρουσία του κυβερνοχώρου, η ύπαρξη πολλών μικρών παικτών και η έλλειψη προσωπικής αλληλεπίδρασης σημαίνει ότι ο οπορτουνισμός είναι πιο πιθανό να συμβεί στον κυβερνοχώρο παρά στον φυσικό κόσμο (Kshetri, 2010: 228). Σε σύγκριση με οποιοδήποτε άλλο έγκλημα, το έγκλημα στον κυβερνοχώρο φαίνεται να απαιτεί περισσότερη διεθνή συνεργασία και ανταλλαγή πληροφοριών ως προς τον τρόπο διαχείρισής του.

Γενικότερα, η αποκλίνουσα συμπεριφορά οφείλεται σε προβλήματα και ελλείψεις. Προβλήματα, τα οποία οφείλει το κράτος να λύσει μέσω των δημόσιων κοινωνικών πολιτικών. Επίσης, το κυβερνοέγκλημα δημιουργεί μια παράνομη οικονομία, που «συμβιώνει» στο ίδιο πλαίσιο, ταυτόχρονα με τη νόμιμη. Η μορφολογία, η κοινωνική οργάνωση και το modus operandi (=τρόπος δράσης) των εγκληματικών οργανώσεων καθορίζονται από το ευρύτερο οικονομικό και κοινωνικό πλαίσιο και από τις σχέσεις εξουσίας. Επομένως, η εκάστοτε ποινική αντίδραση απέναντι στο οργανωμένο έγκλημα θα είναι αναποτελεσματική, εάν δεν πλαισιώνεται και από την ανάπτυξη

δράσεων κοινωνικής πρόληψης του οργανωμένου εγκλήματος, όπως κοινωνικές πολιτικές για τη ρύθμιση και τη μείωση της φτώχειας και την ελάττωση των κοινωνικών ανισοτήτων καθώς και στρατηγικές παρέμβασης για τους νέους με στόχο τη διεύρυνση των ευκαιριών εργασίας (Σταμούλη, 2016). Η Ελλάδα φαίνεται να εστιάζει περισσότερο στις ποινές και την ενίσχυση του αστυνομικού σώματος ακολουθώντας τις κατευθυντήριες γραμμές της Ε.Ε, η οποία λειτουργεί ως συντονιστικό όργανο. Αυτό που οφείλει σίγουρα κάθε χώρα είναι να εστιάσει περισσότερο στην εκπαιδευτική πολιτική και στις κοινωνικές δράσεις, ώστε να μειωθούν οι παραβατικές συμπεριφορές και οι ανισότητες. Για να ξεκινήσεις να λύνεις το πρόβλημα πρέπει να γνωρίζεις από που ξεκινάει (τις αιτίες) και όχι απλά να προσπαθείς να το απομονώνεις για πάντα (δηλαδή, φυλακές). Έτσι, πρέπει να λάβουμε υπόψιν μας τα λόγια του Vikrant Parsai, συγκεκριμένα ότι «η κοινωνία προσκαλεί το έγκλημα, και οι εγκληματίες αποδέχονται την πρόσκληση». Χωρίς την μέριμνα και πρόληψη του κράτους η ασφάλεια των ατόμων τίθεται σε κίνδυνο. Όπως αναφέρουν και οι Schell & Martin (2004: 44), ο μόνος τρόπος για να προστατευτούμε ως κοινωνία είναι να έχουμε καλή γνώση του εγκλήματος στον κυβερνοχώρο και να τηρούμε τις προειδοποιήσεις των ειδικών.

Βιβλιογραφία

Brenner, S. W. (2010). *Cybercrime : criminal threats from cyberspace*. Santa Barbara, California: ABC-CLIO, LLC.

Clough, J. (2010). *Principles of Cybercrime*. New York: Cambridge University Press.

Kshetri, N. (2010). *The Global Cybercrime Industry (Economic, Institutional and Strategic Perspectives)*. Berlin Heidelberg: Springer.

McQuade, S. C. (2009). *ENCYCLOPEDIA OF CYBERCRIME*. Westport, Connecticut: Greenwood Press.

Schell, B. H., & Martin, C. (2004). *Cybercrime : a reference handbook (Contemporary world issues)*. Santa Barbara, California: ABC-CLIO.

Segrave, M. & Vitis, L. (2017). *Gender, Technology and Violence*. New York : Routledge.

White, G. (2020). *CRIMEDOTCOM FROM VIRUSES TO VOTE RIGGING, HOW HACKING WENT GLOBAL*. Reaktion Books Ltd.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3d ed.). UK: SAGE Publications Ltd.

Ηλεκτρονική Βιβλιογραφία

Αγγελέτου, Β. (2015). *Στον κυβερνοχώρο μεταφέρεται η τρομοκρατία.* Insider.gr. Retrieved 24 March 2021, from https://www.insider.gr/eidiseis/kosmos/1587/ston-kyvernohoro-metaferetai-i-tromokratia.

Άλγκρεν, Μ. (2021). *100+ Στατιστικές και γεγονότα Διαδικτύου (2021) που πρέπει να γνωρίζετε.* Retrieved 25 January 2021, from https://www.websitehostingrating.com/el/internet-statistics-facts/

Διβράμης, Γ. (2020). *Το 61.5% της κίνησης στο ίντερνετ είναι bot!*. Paramarketing.gr. Retrieved 5 September 2021, from https://paramarketing.gr/%CF%84%CE%BF-61-5-%CF%84%CE%B7%CF%82-%CE%BA%CE%AF%CE%BD%CE%B7%CF%83%CE%B7%CF%82-%CF%83%CF%84%CE%BF-%CE%AF%CE%BD%CF%84%CE%B5%CF%81%CE%BD%CE%B5%CF%84-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-bot-135/

Ευρωπαϊκή Επιτροπή. (2020). *ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ σχετικά με την στρατηγική της ΕΕ για την Ένωση Ασφάλειας.* Βρυξέλλες.

Ελληνική Αστυνομία και Υπ. Προστασίας Πολίτη. (2021). *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.* Retrieved 13 May 2021, from http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=819

Καούλλας, Λ. (2021). *Τεχνητή Νοημοσύνη και εγκλήματα του μέλλοντος*. Simerini. Retrieved 17 February 2021, from

https://simerini.sigmalive.com/article/2021/1/11/tekhnete-noemosune-kai-egklemata-tou-mellontos/.

Καραντράντος, Τ. (2020). COVID 19: *Lockdown και επιπτώσεις στην εγκληματικότητα στην Ε.Ε.*. ΕΛΙΑΜΕΠ. Retrieved 12 July 2021, from https://www.eliamep.gr/publication/covid-19-lockdown-%CE%BA%CE%B1%CE%B9-%CE%B5%CF%80%CE%B9%CF%80%CF%84%CF%8E%CF%83%CE%B5%CE%B9%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%84%CE%B9%CE%BA%CF%8C%CF%84/.

Κατσούλη, Έ. (2016). *Κυβερνοέγκλημα: Το τέλος της αθωότητας;*. KPMG. Retrieved 12 July 2021, from https://home.kpmg/gr/el/home/insights/2016/07/cyber-security-the-end-of-innocence.html.

Κικίλιας, Π. (2008). *Κυβερνοτρομοκρατία και εφαρμογή νέων τεχνολογιών στην τρομοκρατία.* IT SECURITY PRO. Retrieved 24 March 2021, from https://www.itsecuritypro.gr/kyvernotromokratia-ke-efarmogi-neon-technologion-stin-tromokratia/.

Κολλιδάς, Γ. (2020). *Άποψη: «Σκοτεινό Διαδίκτυο» και κυβερνοέγκλημα.* Η ΚΑΘΗΜΕΡΙΝΗ. Kathimerini.gr. Retrieved 12 July 2021, from https://www.kathimerini.gr/economy/561084904/apopsi-skoteino-diadiktyo-kai-kyvernoegklima/.

Κωνσταντίνου, Κ. (2018). *Οι σημαντικότερες σύγχρονες τάσεις της Αντεγκληματικής Πολιτικής.* SocialPolicy.gr. https://socialpolicy.gr/2018/06/%CE%BF%CE%B9-%CF%83%CE%B7%CE%BC%CE%B1%CE%BD%CF%84%CE%B9%CE%

BA%CF%8C%CF%84%CE%B5%CF%81%CE%B5%CF%82%CF%83%CF%8D%CE%B3%CF%87%CF%81%CE%BF%CE%BD%CE%B5%CF%82%CF%84%CE%AC%CF%83%CE%B5%CE%B9%C F%82-%CF%84.html#_ftn13

Μπόση, Μ., & Βασιλειάδης, Η. (2016). *Οργανωμένο έγκλημα και αδύναμες κρατικές δομές σε περίοδο κρίσης: Μια αμφίδρομη σχέση.* Crime in Crisis. http://crime-in-crisis.com/%CE%BF%CF%81%CE%B3%CE%B1%CE%BD%CF%89%CE%BC%CE%AD%CE%BD%CE%BF-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%B1%CE%B [Accessed 22 January 2021]

NATO. (2021). *Νέες απειλές: η κυβερνο-διάσταση. Nato.int. Retrieved 24 March 2021,* from https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/GR/index.htm.

Ντόκος Γ. (2019). *Ψευδείς Ειδήσεις στο Διαδίκτυο – Φύση, Κίνδυνοι και Αντιμετώπιση.* Homo Digitalis.com

Παπανικολάου, Α. Γ. (2009). *Η προστασία της πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων σύμφωνα με τη σύμβαση για το κυβερνοέγκλημα του Συμβουλίου της Ευρώπης*. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΑΠΘ). 10.12681/eadd/26020

Παρθενοπούλου, Ν. (2018). *Ο ιός Stuxnet και το πυρηνικό πρόγραμμα του Ιράν*. ΚΕΔΙΣΑ - KEDISA. Retrieved 24 March 2021, from https://kedisa.gr/%CE%BF-%CE%B9%CF%8C%CF%82-stuxnet-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF-%CF%80%CF%85%CF%81%CE%B7%CE%BD%CE%B9%CE%BA%CF%8C-%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1-%CF%84%CE%BF%CF%85-%CE%B9/

Σταμούλη, Ε. (2016). *Οργανωμένο έγκλημα και οικονομική κρίση: τάσεις και μεταβολές.* Crime in Crisis. http://crime-in-crisis.com/%CE%BF%CF%81%CE%B3%CE%B1%CE%BD%CF%89%CE%BC%CE%AD%CE%BD%CE%BF-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%AE-%CE%BA%CF%81/

Στεργιούλης, Ε. (2020). *Παιδική Πορνογραφία*. Retrieved 17 April 2021, from https://www.capital.gr/me-apopsi/3493520/paidiki-pornografia

Συκιώτου, Α. (2018). *Η νέα τάση στην Αντεγκληματική πολιτική εστιάζει περισσότερο στην «τεχνολογική εξουδετέρωση» του εγκληματικού κινδύνου.* Crime Times. Retrieved 2021, from https://www.crimetimes.gr/%CE%B7-%CE%BD%CE%AD%CE%B1-%CF%84%CE%AC%CF%83%CE%B7-%CF%83%CF%84%CE%B7%CE%BD-%CE%B1%CE%BD%CF%84%CE%B5%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9/

Τσιγκανου, Ι. (2016). *Αντεγκληματική πολιτική και τυπικός κοινωνικός έλεγχος στην Ελλάδα της κρίσης.* Crime in Crisis. http://crime-in-crisis.com/%ce%b1%ce%bd%cf%84%ce%b5%ce%b3%ce%ba%ce%bb%ce%b7%ce%bc%ce%b1%cf%84%ce%b9%ce%ba%ce%ae-%cf%80%ce%bf%ce%bb%ce%b9%cf%84%ce%b9%ce%ba%ce%ae-%ce%ba%ce%b1%ce%b9-%cf%84%cf%85%cf%80%ce%b9%ce%ba%cf%8c%cf%82/#more-85

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

Χατζηβασιλείου, Χ. (2020). *Η εμπορία ανθρώπων με σκοπό τη σεξουαλική εκμετάλλευση μέσω διαδικτύου.* Retrieved 24 April 2021, from https://www.offlinepost.gr/2020/01/27/%CE%B7-%CE%B5%CE%BC%CF%80%CE%BF%CF%81%CE%AF%CE%B1-%CE%B1%CE%BD%CE%B8%CF%81%CF%8E%CF%80%CF%89%CE%BD-%CE%BC%CE%B5-%CF%83%CE%BA%CE%BF%CF%80%CF%8C-%CF%84%CE%B7-%CF%83%CE%B5%CE%BE%CE%BF%CF%85%CE%B1%CE%BB/

ACCOUNTANCY GREECE. (2021). *Το οικονομικό έγκλημα αυξάνεται και εξαπλώνεται σαν ιός.* ΠΕΡΙΟΔΙΚΟ ACCOUNTANCY GREECE. ΠΕΡΙΟΔΙΚΟ ACCOUNTANCY GREECE | ΠΕΡΙΟΔΙΚΟ ΟΙΚΟΝΟΜΙΚΟΥ ΛΟΓΙΣΜΟΥ. Retrieved 12 July 2021, from https://www.accountancygreece.gr/%CF%84%CE%BF-%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%B1%CF%85%CE%BE%CE%AC%CE%BD%CE%B5%CF%84%CE%B1%CE%B9-%CE%BA%CE%B1%CE%B9-%CE%B5/

Alkaabi, Ali and Mohay, George M. and McCullagh, Adrian J. and Chantler, Alan N.(2010). *Dealing with the problem of cybercrime.* In: Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, 4-6 October 2010, Abu Dhabi.

BBC News. (2021, April 12). *Iran says key Natanz nuclear facility hit by 'sabotage'*. BBC News. Retrieved June 7, 2021, from https://www.bbc.com/news/world-middle-east-56708778

Berasategui, G. (2021). *Cybercrime: Which ones are the most common threats today? - Red Points*. Red Points. Retrieved 28 February 2021, from https://www.redpoints.com/blog/cybercrime/.

Bitdefender. (2021). *4 τύποι κακόβουλου λογισμικού που πρέπει να γνωρίζετε.* Retrieved 29 April 2021, from https://bitdefender.gr/blog/4-typoi-kakoboulou-logismikou

BOSTON FBI. (2020). *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*. FBI. Fbi.gov. Retrieved 7 September 2021, from https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Brooks C. (2020). *The truth behind fake news and politics on social media.* MSUToday Michigan State University.

Carson A. & Farhall K. (2019). *The real news on 'fake news': politicians use it to discredit media, and journalists need to fight back.* The Conversation

Chadd, K. (2020). *The History Of Cybercrime And Cybersecurity, 1940-2020.* Retrieved 5 February 2021, from https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/

Chadwick, A. (2006). *Internet Politics.* Oxford: Oxford University Press.

CNN Greece. (2020). *Αυξήθηκε η διαδικτυακή σεξουαλική κακοποίηση παιδιών στην καραντίνα λόγω κορωνοϊού.* Retrieved 17 April 2021, from https://www.cnn.gr/kosmos/story/219925/ayxithike-i-diadiktyaki-sexoyaliki-kakopoiisi-paidion-stin-karantina-logo-koronoioy

Computer History Museum. (2021). *Computers | Timeline of Computer History | Computer History Museum.* Retrieved 5 February 2021, from https://www.computerhistory.org/timeline/computers/#:~:text=Started%20in%201943%2C%20the%20ENIAC,faster%20than%20any%20previous%20computer.

Corera, G. (2021). *Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz.* Retrieved 7 June 2021, from https://www.bbc.com/news/world-middle-east-56722181

Deutsch L., A. (2021). *Watch Out for These Top Internet Scams.* Retrieved 16 March 2021, from https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

Ehc, T. (2020). FBI: *Οι σωματέμποροι εντοπίζουν τα θύματα μέσω των social media και των dating sites.* Retrieved 24 April 2021, from https://www.secnews.gr/215267/fbi-somatemporoi-thymata-social-media-dating-sites/

Europa EU. (2021). *Συχνές ερωτήσεις για τα δικαιώματα πνευματικής ιδιοκτησίας.* Retrieved 20 April 2021, from https://euipo.europa.eu/ohimportal/el/web/observatory/faqs-on-copyright-cy#1

European Commision. (2021). *Cybersecurity Policies.* Retrieved 10 May 2021, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commision. (2021). *Cybersecurity Policy Brief Document*. Retrieved 10 May 2021, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commision. (2021). *Cybersecurity Strategy*. Retrieved 10 May 2021, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commision. (2015). *Cyber security*. European Commision. Retrieved from doi: 10.2837/411118

European Commission. (2015). *Special Eurobarometer 423 "Cyber Security"*. European Union.

Europol. (2021). *European Cybercrime Centre - EC3.* Retrieved 13 May 2021, from

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec

Europol. (2021). *Wannacry Ransomware*. Retrieved 29 April 2021, from https://www.europol.europa.eu/wannacry-ransomware

FACT. (2021). *Types of online digital piracy & solutions.* Retrieved 23 April 2021, from https://www.fact-uk.org.uk/consumer-advice/online-piracy/

FBI. (2021). *Nigerian Letter or "419" Fraud*. Federal Bureau of Investigation. Retrieved 15 March 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud

Florida Tech. (2021). *A Brief History of Cyber Crime.* Retrieved 5 February 2021, from https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

Forcepoint. (2021). *What is Malware?.* Retrieved 29 April 2021, from https://www.forcepoint.com/cyber-edu/malware

Grassi V. (2019). *Advertising.* Monmouth University Polling Institute.

Gr Times (2018). *Η Μαρία Σπυράκη για τα fake news.* Gr Times.net.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity.* Retrieved 15 March 2021, from https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#

Internetsafety101.org. (2021). *Sex Trafficking.* Retrieved 24 April 2021, from https://internetsafety101.org/trafficking

Jjay.cuny.edu. (2021). *The Cybercrime Problem. John Jay College of Criminal Justice.* Retrieved 16 February 2021, from https://www.jjay.cuny.edu/cybercrime- problem.

Kenton, W. (2020). *Copyright Infringement.* Retrieved 21 April 2021, from https://www.investopedia.com/terms/c/copyright-infringement.as

Koukouli, E. (2019). *Τι είναι το Διαδίκτυο των Πραγμάτων (IoT).* Study Care. Retrieved 22 January 2021, from https://studycare.gr/ti-einai-to-diadiktyo-ton-pragmaton-iot/

Lawspot. (2017). *Έγκλημα.* LAWSPOT. https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/egklima

Lawspot.gr. (2021). *Ηλεκτρονικό έγκλημα*. Lawspot. Retrieved 28 February 2021, from https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/ilektroniko-egklima

Lawspot.gr. (2017). *Μέτρα για την πρόληψη των επιθέσεων στον κυβερνοχώρο ζητά το Ευρωπαϊκό Κοινοβούλιο.* Retrieved 29 April 2021, from https://www.lawspot.gr/nomika-nea/metra-gia-tin-prolipsi-ton-epitheseon-ston-kyvernohoro-zita-eyropaiko-koinovoylio

Lawspot.gr. (2020). *Online πειρατεία στην Ελλάδα: Για πρώτη φορά δυνατότητα δυναμικού αποκλεισμού ιστοσελίδων (dynamic blocking injunction).* Retrieved 23 April 2021, from https://www.lawspot.gr/nomika-nea/online-peirateia-stin-ellada-gia-proti-fora-dynatotita-dynamikoy-apokleismoy-istoselidon

Lawspot.gr. (2018). *Προσβολή Πνευματικής Ιδιοκτησίας στο διαδίκτυο: Όσα χρειάζεται να γνωρίζετε για τη νέα διαδικασία notice and takedown*. Retrieved 21 April 2021, from https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/prosvoli-pneymatikis-idioktisias-sto-diadiktyo-osa-hreiazetai

Layton, J. (2021). *How to Avoid Copyright Infringement.* Retrieved 21 April 2021, from https://www.legalzoom.com/articles/how-to-avoid-copyright-infringement

MUJOVIĆ, V. (2018). *WHERE DOES CYBERCRIME COME FROM? THE ORIGIN & EVOLUTION OF CYBERCRIME.* Retrieved 5 February 2021, from https://www.le-vpn.com/history-cyber-crime-origin-evolution/

Napley K. (2017). *The Impact of Fake News: Politics.* Lexology

Plutis, D. (2020). *How to spot a bot on social media.* Avira Blog. Retrieved 31 January 2021, from https://www.avira.com/en/blog/how-to-spot-a-bot-on-social-media

Radware. (2021). *History of Network Security Methods.* Retrieved 15 February 2021, from https://www.radware.com/resources/network_security_history.asp

Repath, J. (2018). *The destructive effects of echo chambers on society.* The Pacer. Retrieved 5 September 2021, from https://www.thepacer.net/the-destructive-nature-of-echo-chambers/.

Rijnetu, I. (2019). *Top Online Scams Used by Cyber Criminals to Trick You.* Retrieved 15 March 2021, from https://heimdalsecurity.com/blog/top-online-scams/

Slaughter, A. (2021). *cyberspace*. The Chicago School of Media Theory. Retrieved 31 January 2021, from https://lucian.uchicago.edu/blogs/mediatheory/keywords/cyberspace/

Sznitka, E. (2020). *Human Trafficking and the Internet – Human sex trafficking in the United States and around the world is a serious, and growing problem that everyone should be educated about. To begin, what is the definition of sex trafficking?*. Retrieved 24 April 2021, from https://caclapeer.org/human-trafficking-the-internet/

Thorn. (2021). *Child Pornography and Sexual Abuse Statistics.* Retrieved 17 April 2021, from https://www.thorn.org/child-pornography-and-abuse-statistics

Trend Micro (2017). *Fake News and Cyber Propaganda: The Use and Abuse of Social Media.* Trend Micro PL.

UNODC. (2021). *Obstacles to cybercrime investigations.* Unodc.org. Retrieved 16 February 2021, from https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html

Webroot. (2021). *The Societal Costs of Digital Piracy.* Retrieved 23 April 2021, from https://www.webroot.com/us/en/resources/tips-articles/the-societal-costs-of-digital-piracy