ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΦΟΙΤΗΤΡΙΑ:

ΜΠΕΝΕΤΟΥ ΑΘΑΝΑΣΙΑ

ΕΠΙΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:

Κος ΝΤΕΜΙΡΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΑΤΡΑ 2021

ΠΡΟΛΟΓΟΣ

Η εποχή που ζούμε χαρακτηρίζεται ως η 4η βιομηχανική επανάσταση ή αλλιώς η επανάσταση της πληροφορίας. Ωστόσο, δεν υπάρχει κάποιος σαφής ορισμός του εγκλήματος στον κυβερνοχώρο στο ακαδημαϊκό περιβάλλον. Ορισμένες ποσοστώσεις το έχουν αναφέρει ως "ηλεκτρονικό έγκλημα", "έγκλημα στον υπολογιστή" και "έγκλημα που σχετίζεται με τον υπολογιστή." Έχουν υπάρξει διαφορετικές ταξινομήσεις του εγκλήματος στον κυβερνοχώρο. Ωστόσο υποστηρίζεται ότι το έγκλημα στον κυβερνοχώρο είναι ένα αδίκημα που διαπράττεται όταν ο υπολογιστής είναι το κύριο όργανο του εγκλήματος ή όταν ο υπολογιστής στοχεύει για το έγκλημα. Παρόλο που μια τέτοια ταξινόμηση δεν μπορεί να πωληθεί για αυτήν τη μελέτη, είναι απαραίτητη για την κατανόηση του όρου.

Τα εγκλήματα στον κυβερνοχώρο μπορούν να κατηγοριοποιηθούν σε Τύπο Ι και Τύπο ΙΙ ανάλογα με την ένταση των εγκλημάτων (Moore, 2016). Ο τύπος Ι αναφέρεται σε δραστηριότητες ηλεκτρονικού εγκλήματος που είναι τεχνικές, για παράδειγμα, το hacking. Από την άλλη πλευρά, ο τύπος ΙΙ στηρίζεται στην ανθρώπινη αλληλεπίδραση και όχι στην τεχνολογία. Οι εγκληματικές δραστηριότητες όπως η κλοπή ταυτότητας, η απάτη με πιστωτικές κάρτες, η παρενόχληση, η καταδίωξη και οι απειλητικές συμπεριφορές είναι γνωστό ότι είναι παραδοσιακά εγκλήματα που είναι πλέον εύκολο να ασκηθούν σε υπολογιστές. Τέτοια εγκλήματα μπορούν να υπάρχουν ανεξάρτητα χωρίς τεχνολογία υπολογιστών.

Ωστόσο, υπάρχει ένα άλλο φάσμα αδικημάτων που εξαρτώνται απόλυτα από τον κυβερνοχώρο. Αυτό σημαίνει ότι δεν μπορούν να υπάρξουν χωρίς τεχνολογία υπολογιστών. Οι εγκληματίες διαπίστωσαν ότι ήταν ευκολότερο να καταστρέψουν επιχειρήσεις μέσω της βλάβης στις βάσεις δεδομένων τους. Αξιοσημείωτο είναι ότι το 2015, υπήρξε μια μαζική κυβερνοεπίθεση που στόχευσε άτομα και επιχειρήσεις μέσω ransomware που ονομάζεται Cryptowall έκδοση 3.0 (Alazab & Broadhurst, 2015). Οι εγκληματίες έψαξαν, κρυπτογραφήσαν έγγραφα στους υπολογιστές των θυμάτων πριν τους ζητήσουν να πληρώσουν χιλιάδες δολάρια αν χρειαστεί ποτέ πίσω τα πρωτότυπά τους. Εκτιμήθηκε ότι αυτή η επίθεση προκάλεσε περίπου 325 εκατομμύρια δολάρια σε ζημιά. Τις τελευταίες δύο δεκαετίες, οι αδίστακτοι χρήστες της τεχνολογίας στον

κυβερνοχώρο συνέχισαν να διαπράττουν κυβερνοεξαρτώμενα και ανεξάρτητα εγκλήματα με εξελιγμένους και άνευ προηγουμένου τρόπους. Η κυβερνο -τεχνολογία έχει χρησιμοποιηθεί για να διαπράξει τις μεγαλύτερες θηριωδίες στα παγκόσμια συστήματα, όπως η εκλογική απάτη και τα προδοτικά αδικήματα. Είναι τόσο υψηλό το επίπεδο πολυπλοκότητας που δολοφονίες έχουν εκτελεστεί μέσω του κυβερνοχώρου. Για παράδειγμα, τον Ιανουάριο του 2002, οι Ηνωμένες Πολιτείες κατέγραψαν την πρώτη δολοφονία εγκλήματος στον κυβερνοχώρο, με την οποία ο δράστης προσέλαβε έναν γκουρού υπολογιστών για να αλλάξει τις συνταγές των αντιπάλων ασθενών του μέσω παραβίασης του συστήματος υπολογιστών του νοσοκομείου (Krausz & Walker, 2013). Κατά συνέπεια, αυτό κατέληξε σε λανθασμένη συνταγή που οδήγησε στο θάνατο ενός ασθενούς στα χέρια μιας αθώας νοσοκόμας.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή μου και επόπτη της εργασίας αυτής, κο Ντεμίρη Κωνσταντίνο.

Επιπλέον θα ήθελα να εκφράσω την ευγνωμοσύνη μου και την αγάπη προς την οικογένειά μου για την συμπαράστασή και την βοήθεια που μου παρείχαν καθόλη την διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Η εξέλιξη της Τεχνολογίας Πληροφοριών (ΤΠ) επέφερε επιτυχημένη επικοινωνία μέσω του Διαδικτύου, ακμάζουσες επιχειρήσεις και παγκόσμια αλληλεπίδραση μέσω πλατφορμών κοινωνικής δικτύωσης. Ωστόσο, αυτές οι εξελίξεις απειλούνται από εγκληματικές δραστηριότητες στον παγκόσμιο κυβερνοχώρο. Το ηλεκτρονικό έγκλημα έχει οδηγήσει σε σημαντική ζημιά όχι μόνο για τα άτομα αλλά και για τις επιχειρήσεις, προκαλώντας διαταραχές στην απασχόληση και μειωμένη εμπιστοσύνη για τις διαδικτυακές δραστηριότητες μιας εταιρείας. Οι ευθύνες αντιμετώπισης των δραστηριοτήτων στον κυβερνοέγκλημα βρίσκονται σε μεμονωμένες χώρες, οι οποίες θα πρέπει να διασφαλίζουν ότι προστατεύουν και ενδυναμώνουν τα ιδρύματα να δημιουργήσουν μια οργανωμένη εκστρατεία μετριασμού που παρακολουθεί τι συμβαίνει στον κυβερνοχώρο. Οι εγκληματίες στον κυβερνοχώρο σε όλο τον κόσμο μπορούν να οδηγηθούν στη δικαιοσύνη μόνο εάν υπάρχουν διαθέσιμοι και επαρκείς νόμοι για την καταπολέμηση του κακού. Επιπλέον, υπάρχει ανάγκη συμμετοχής σε προληπτικές στρατηγικές για την παρακολούθηση και την αποτροπή επιθέσεων στον κυβερνοχώρο

ABSTRACT

The evolution of Information Technology (IT) has brought about successful communication through the Internet, thriving businesses and global interaction through social networking platforms. However, these developments are threatened by criminal activity in cyberspace. Cybercrime has led to significant damage not only to individuals but also to businesses, causing disruptions in employment and diminished confidence in a company's online activities. Responsibilities for tackling cybercrime activities lie with individual countries, which should ensure that they protect and empower institutions to create an organized mitigation campaign that monitors what is happening in cyberspace. Cybercriminals around the world can only be brought to justice if there are sufficient and available laws to combat evil. In addition, there is a need to engage in preventive strategies to monitor and prevent cyber attacks.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της τεχνολογίας των πληροφοριών και η ευρεία χρήση του Διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές σε όλες τις καθημερινές δραστηριότητες, την παραγωγική διαδικασία, το εμπόριο, την εκπαίδευση, την ψυχαγωγία, ακόμα και στον τρόπο που σκέφτονται και ενεργούν οι σύγχρονοι άνθρωποι. Μαζί με αυτές τις αλλαγές, οι οποίες αποσκοπούν στη βελτίωση της ποιότητας της ζωής μας, αναπτύσσονται και εισάγονται νέες μορφές εγκληματικότητας. Αυτές οι νέες μορφές εγκλήματος διαπράττονται στο περιβάλλον της τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) και καλύπτονται από τον όρο ηλεκτρονικό έγκλημα, ο οποίος περιλαμβάνει επίσης το έγκλημα στον κυβερνοχώρο. Η τελευταία, σε αντίθεση με τις «παραδοσιακές» μορφές εγκλήματος, δεν έχει γεωγραφικούς περιορισμούς. Δηλαδή, ένα έγκλημα που διαπράττεται από έναν δράστη μπορεί να επηρεάσει πολλά άτομα που μπορεί να βρίσκονται σε διαφορετικές τοποθεσίες, είτε μέσα στην ίδια χώρα είτε όχι. Επιπλέον, υπό ορισμένες συνθήκες, αυτό μπορεί να συμβεί και ταυτόχρονα.

Προκειμένου οι αρμόδιες αρχές επιβολής του νόμου να διερευνήσουν και να διώξουν με επιτυχία ένα έγκλημα στον κυβερνοχώρο που έχει αναφερθεί από έναν πολίτη μιας συγκεκριμένης χώρας, συχνά πρέπει να υποκλέψουν, να παρακολουθούν και να επεξεργάζονται ψηφιακά ίχνη πληροφοριών σε περισσότερες από μία δικαιοδοσίες, δεδομένου ότι το αδίκημα μπορεί να προέρχεται από άλλες χώρες ή απλώς να διέρχεται από τα δίκτυα επικοινωνίας τους. Η μεγάλη ποικιλία της νομοθεσίας και των νομικών πλαισίων μεταξύ των διαφόρων χωρών παγκοσμίως μπορεί να προκαλέσει σημαντικές καθυστερήσεις στην απόκτηση των απαιτούμενων αδειών και την παροχή των ζητούμενων πληροφοριών ή μπορεί ακόμη και να εμποδίσει εντελώς την ποινική διαδικασία, λόγω της αδυναμίας απόδειξης της άμεσης εγκληματικής πρόθεσης. Ως εκ τούτου, προκειμένου να καταπολεμηθεί αποτελεσματικά το έγκλημα στον κυβερνοχώρο, απαιτείται διεθνής συνεργασία, ούτως ώστε να υιοθετηθεί ένα εναρμονισμένο νομοθετικό πλαίσιο και κατάλληλες διαδικασίες που θα επιταχύνουν τις διακρατικές έρευνες και διώξεις για το έγκλημα στον κυβερνοχώρο.

Δεδομένης της αύξησης των περιστατικών ηλεκτρονικού εγκλήματος στην Ελλάδα, μια κατάλληλη ομάδα της Ελληνικής Αστυνομίας ιδρύθηκε πρόσφατα για την αποτελεσματική αντιμετώπιση τέτοιων περιστατικών. Επιπλέον, με τις ενέργειες της εν λόγω αστυνομικής μονάδας, κατέστη πολύ εμφανής η ανάγκη αναθεώρησης ή/και

παράτασης της εθνικής νομοθεσίας ώστε να συμπεριληφθούν οι διάφορες και σύνθετες πτυχές του εγκλήματος στον κυβερνοχώρο.

ΚΕΦΑΛΑΙΟ 1ο Η ΈΝΝΟΙΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

1.1 ΙΣΤΟΡΙΑ ΚΑΙ ΕΞΕΛΙΞΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το έγκλημα στον κυβερνοχώρο είναι ένα παράπλευρο προϊόν ανάπτυξης του Διαδικτύου. Σε σύγκριση με το συμβατικό έγκλημα, το έγκλημα στον κυβερνοχώρο είναι νέο. Ωστόσο, το κόστος της καταστροφής του εγκλήματος στον κυβερνοχώρο δεν είναι μικρότερο από το συμβατικό έγκλημα.

Ωστόσο, εκπληκτικά, το πρώτο έγκλημα στον κυβερνοχώρο έχει καταγραφεί στις αρχές του 1820. Μια ομάδα υπαλλήλων του Joseph-Marie Jacquard προσπάθησε να σαμποτάρει τον αργαλειό που εφευρέθηκε από τον Jacquard φοβούμενοι ότι θα χάσουν τη δουλειά τους από τη συσκευή. Ωστόσο, αυτό είναι ένα παράδειγμα που διαφέρει αρκετά από το έγκλημα στον κυβερνοχώρο (Introduction to Cyber Crime).

Το έγκλημα στον κυβερνοχώρο που όλοι γνωρίζουν ότι εξαρτάται από το δίκτυο και τον σύγχρονο υπολογιστή βρέθηκε μετά την ανάπτυξη του σύγχρονου υπολογιστή και του Arpanet. Το πρώτο πρόγραμμα καταπολέμησης του ιού που ονομάζεται Creeper έγινε το 1971 από τον Bob Thomas, ο οποίος δεν είχε καμία πρόθεση να διεξάγει εγκληματικές δραστηριότητες (Thomas & Marc,2004) . Από τότε, κατασκευάστηκε αμέτρητο κακόβουλο λογισμικό. Παρά το γεγονός ότι το κακόβουλο λογισμικό γίνεται πιο περίπλοκο και λεπτό, οι κύριες λειτουργίες και σκοποί έχουν μόλις αλλάξει.

Καθώς η ανθρωπότητα βρίσκεται στην Εποχή της Πληροφορίας, η κοινωνία εξαρτάται όλο και περισσότερο από τον υπολογιστή και το Διαδίκτυο. Παρόλο που το κακόβουλο λογισμικό δεν έχει αλλάξει πολύ, ο τομέας άσκησης έχει διευρυνθεί ευρέως. Είναι η εξέλιξη της κοινωνίας που κάνει το έγκλημα στον κυβερνοχώρο να ευδοκιμεί. Εκτός από αυτό, το συμβατικό έγκλημα που οδηγεί την παλίρροια της Εποχής της Πληροφορίας προσαρμόζεται στον κόσμο με την ψηφιοποίηση. Το εμπόριο ναρκωτικών, το παράνομο εμπόριο όπλων και άλλες συμβατικές εγκληματικές δραστηριότητες άρχισαν να προσφέρουν ηλεκτρονική υπηρεσία που μειώνει την πιθανότητα σύλληψης.

1.2 ΟΡΙΣΜΟΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η κοινή παρεξήγηση του εγκλήματος στον κυβερνοχώρο είναι ότι το έγκλημα στον κυβερνοχώρο πρέπει να περιλαμβάνει υπολογιστή ή διαδίκτυο σε κάθε βήμα. Ωστόσο, δεν πραγματοποιούνται όλα τα βήματα σε υπολογιστή ή Διαδίκτυο.

Μια άλλη κοινή παρεξήγηση είναι ότι ο υπολογιστής είναι πάντα η διάπραξη ενός εγκλήματος. Ωστόσο, η αλήθεια είναι ότι, όταν ο υπολογιστής έχει υποστεί βλάβη από άλλους με κακόβουλη πρόθεση, μπορεί να ονομαστεί και έγκλημα στον κυβερνοχώρο. Για παράδειγμα, η δολιοφθορά το 1820 κατηγοριοποιείται ως έγκλημα στον κυβερνοχώρο. Οι άνθρωποι μπερδεύονται εύκολα, επειδή αυτό το είδος εγκλήματος επικαλύπτεται καταστρέφοντας την περιουσία άλλων.

Εν κατακλείδι, μπορεί κανείς να ορίσει το έγκλημα στον κυβερνοχώρο ως «Το έγκλημα που σχετίζεται με υπολογιστή, δίκτυο ή τεχνολογία πληροφοριών».

Υπήρξε πολυάριθμη επιστημονική εργασία στο παρελθόν που στόχευε στον καθορισμό του εγκλήματος στον κυβερνοχώρο σε διάφορες φάσεις της ιστορίας και υπό διάφορες συνθήκες. Το διεθνές περιοδικό Science and Information Security ορίζει το έγκλημα στον κυβερνοχώρο ως επιβλαβείς πράξεις που διαπράττονται από ή έναν υπολογιστή ή ένα δίκτυο. Ένας άλλος ορισμός αναδεικνύει το έγκλημα στον κυβερνοχώρο ως παράνομη συμπεριφορά που πραγματοποιείται από ηλεκτρονικές λειτουργίες και επιδιώκει να στοχεύσει συστήματα υπολογιστών και δεδομένα που επεξεργάζονται οι συσκευές. Από αυτούς τους ορισμούς, είναι σαφές ότι το έγκλημα στον κυβερνοχώρο συμβαίνει μέσα σε έναν εικονικό χώρο, κάτω από τον οποίο πληροφορίες που αφορούν ανθρώπους αντικείμενα, γεγονότα ή γεγονότα διαμορφώνονται σε μαθηματικά σύμβολα και μεταφέρονται μέσω τοπικών και παγκόσμιων δικτύων. Μεταξύ των πρώτων που έγραψαν για το έγκλημα στον υπολογιστή ήταν ο Donn Parker, ο οποίος θεωρήθηκε ο πρώτος εθνικός εμπειρογνώμονας για την ασφάλεια των υπολογιστών στις Ηνωμένες Πολιτείες. Ο Parker το όρισε ως κατάχρηση υπολογιστών λέγοντας ότι περιλαμβάνει σκόπιμες πράξεις στις οποίες το θύμα (τα) υφίσταται απώλεια ενώ άλλα κερδίζουν. Ωστόσο, παρελθόντα γεγονότα έχουν αποδείξει ότι οι δράστες μπορεί να μην έχουν πάντα κέρδος. Αξίζει να σημειωθεί ότι υπάρχει μια ομάδα εγκληματιών στον κυβερνοχώρο γνωστή ως «hacktivists». Πρόκειται για άτομα που διαμαρτύρονται για τις πολιτικές και τις πρακτικές των οργανώσεων. Για παράδειγμα, το 2010, η ομάδα Anonymous hacktivist επιτέθηκε σε Mastercard, Visa και Paypal ως αντίποινα για τη διακοπή δωρεών στο WikiLeaks (Grispos, 2019).

Το Foreign Affairs and International Trade του Καναδά σημειώνει ότι το έγκλημα στον κυβερνοχώρο είναι εγκληματική δραστηριότητα που διαπράττεται χρησιμοποιώντας υπολογιστές και δίκτυα υπολογιστών. Αυτό συνεπάγεται ότι η διευκόλυνση των παραδοσιακών εγκλημάτων χρησιμοποιώντας υπολογιστές εμπίπτει επίσης στο

έγκλημα στον κυβερνοχώρο. Παραδείγματα τέτοιου παραδοσιακού εγκλήματος περιλαμβάνουν παιδική πορνογραφία και διαδικτυακή απάτη. Ορισμένα εγκλήματα που μπορεί να καλύπτουν την έμμεση χρήση υπολογιστών για την εκτέλεση εγκλημάτων περιλαμβάνουν την επικοινωνία και την αποθήκευση δεδομένων και μπορεί να θεωρηθούν ως έγκλημα με τη βοήθεια υπολογιστή. Οι αυστραλιανοί νόμοι αναγνωρίζουν το ηλεκτρονικό έγκλημα ως αυτό που διεξάγεται μέσω υπολογιστή, στοχεύει στην τεχνολογία στον κυβερνοχώρο ή το χρησιμοποιεί για την αποθήκευση παράνομου υλικού. Αυτός ο ορισμός συμφωνεί με αυτόν του Wall, (2007) που διαιρεί το έγκλημα στον κυβερνοχώρο σε αδικήματα που στοχεύουν υπολογιστές και εγκλήματα που ενεργοποιούνται από υπολογιστές. Ο Cybercrime Act 2001 της Αυστραλίας χαρακτηρίζει το έγκλημα στον κυβερνοχώρο ως έγκλημα που προκαλεί βλάβη σε δεδομένα και συστήματα υπολογιστών. Ωστόσο, στα Ηνωμένα Αραβικά Εμιράτα, η νομοθεσία τους προσαρμόζεται ώστε να περιλαμβάνει αδικήματα κατά συστημάτων δεδομένων υπολογιστών και εγκλήματα που σχετίζονται με υπολογιστή, όπως πλαστογραφία, απάτη, απειλές και ξέπλυμα χρήματος.

Οι νόμοι των Ηνωμένων Πολιτειών ορίζουν το έγκλημα υπολογιστών ως έγκλημα που χρησιμοποιεί ή στοχεύει σε δίκτυα υπολογιστών που γενικά αναφέρονται σε ιούς, worms και επιθέσεις DoS. Το Ηνωμένο Βασίλειο έχει επίσης παρόμοια αντίληψη για εγκληματικές δραστηριότητες. Ωστόσο, ο νόμος για την κατάχρηση υπολογιστών στο Ηνωμένο Βασίλειο ορίζει ότι η χρήση δικτυωμένων υπολογιστών, τηλεφώνων ή τεχνολογίας Διαδικτύου για τη διεξαγωγή ή τη διευκόλυνση εγκλημάτων ισοδυναμεί με έγκλημα στον κυβερνοχώρο. Η ανάπτυξη της τεχνολογίας οδήγησε στη συνέχεια στην ανάπτυξη του όρου έγκλημα στον υπολογιστή. Ο Οργανισμός για την Οικονομία και την Ανάπτυξη (ΟΟΣΑ) σε συνοχή με τα κράτη μέλη των Ηνωμένων Εθνών κήρυξε εγκλήματα που σχετίζονται με τη χρήση υπολογιστή ως παράνομα και ανήθικα. Ομοίως, δήλωσαν επίσης τη συνήθη επεξεργασία και διάδοση δεδομένων χωρίς την άδεια του ιδιοκτήτη ως παράνομη συμπεριφορά. Οι συστάσεις του Συμβουλίου της Ευρώπης για το ποινικό δικονομικό δίκαιο υποδεικνύουν ότι τα αδικήματα στον τομέα της πληροφορικής συνιστούν παράνομο έγκλημα και δήλωσαν ότι οι εξουσίες διερεύνησης πρέπει να έχουν δικαίωμα σε πληροφορίες που υποβάλλονται σε επεξεργασία ή μεταφέρονται μέσω συστημάτων υπολογιστών.

Υπάρχουν ανισότητες στην περιγραφή του εγκλήματος στον κυβερνοχώρο σε διεθνές επίπεδο. Οργανισμοί όπως η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα

στον κυβερνοχώρο, η Σύμβαση της Ένωσης των Αραβικών Κρατών και το Σχέδιο συμβάσεων της Αφρικανικής Ένωσης έχουν επιχειρήσει να ορίσουν το έγκλημα στον κυβερνοχώρο, παρόλο που οι ορισμοί τους δεν γίνονται αποδεκτοί παγκοσμίως (Alazab & Broadhurst, 2015). Η Συμφωνία της Κοινοπολιτείας Ανεξάρτητων Κρατών χρησιμοποιεί τον όρο "πληροφορίες υπολογιστή" για να περιγράψει αδικήματα που σχετίζονται με εγκλήματα υπολογιστών. Από την άλλη πλευρά, η Συμφωνία Οργανισμού Συνεργασίας της Σαγκάης προτείνει τον όρο αδικήματα πληροφοριών ως εκμετάλλευση της ιδιοκτησίας πληροφοριών που την επηρεάζει για παράνομους σκοπούς. Ο όρος κυβερνοέγκλημα ή έγκλημα στον υπολογιστή ερμηνεύεται διαφορετικά από διάφορες παρατάξεις και δικαιοδοσίες σε όλο τον κόσμο. Κατά συνέπεια, όλα τα εγκλήματα στον κυβερνοχώρο δεν αντιμετωπίζονται ή ποινικοποιούνται με τον ίδιο τρόπο σε διαφορετικά κράτη. Αυτό σημαίνει ότι ένα συγκεκριμένο έγκλημα στον κυβερνοχώρο θα μπορούσε να είναι έγκλημα σε μια χώρα, αλλά να μην πληροί το κατώτατο όριο σε μια άλλη. Αυτή η ερευνητική εργασία θα χρησιμοποιήσει τον όρο έγκλημα στον υπολογιστή και έγκλημα στον κυβερνοχώρο εναλλακτικά για να δηλώσει το έγκλημα που χρησιμοποιεί ή στοχεύει δεδομένα και συστήματα υπολογιστών για τη διάπραξη παράνομης δραστηριότητας.

Υπήρξε πολυάριθμη επιστημονική εργασία στο παρελθόν που στόχευε στον καθορισμό του εγκλήματος στον κυβερνοχώρο σε διάφορες φάσεις της ιστορίας και υπό διάφορες συνθήκες. Το διεθνές περιοδικό Science and Information Security ορίζει το έγκλημα στον κυβερνοχώρο ως επιβλαβείς πράξεις που διαπράττονται από ή έναν υπολογιστή ή ένα δίκτυο. Ένας άλλος ορισμός αναδεικνύει το έγκλημα στον κυβερνοχώρο ως παράνομη συμπεριφορά που πραγματοποιείται από ηλεκτρονικές λειτουργίες και επιδιώκει να στοχεύσει συστήματα υπολογιστών και δεδομένα που επεξεργάζονται οι συσκευές. Από αυτούς τους ορισμούς, είναι σαφές ότι το έγκλημα στον κυβερνοχώρο συμβαίνει μέσα σε έναν εικονικό χώρο, κάτω από τον οποίο πληροφορίες που αφορούν ανθρώπους αντικείμενα, γεγονότα ή γεγονότα διαμορφώνονται σε μαθηματικά σύμβολα και μεταφέρονται μέσω τοπικών και παγκόσμιων δικτύων. Μεταξύ των πρώτων που έγραψαν για το έγκλημα στον υπολογιστή ήταν ο Donn Parker, ο οποίος θεωρήθηκε ο πρώτος εθνικός εμπειρογνώμονας για την ασφάλεια των υπολογιστών στις Ηνωμένες Πολιτείες. Ο Parker το όρισε ως κατάχρηση υπολογιστών λέγοντας ότι περιλαμβάνει σκόπιμες πράξεις στις οποίες το θύμα (τα) υφίσταται απώλεια ενώ άλλα κερδίζουν. Ωστόσο, παρελθόντα γεγονότα έχουν αποδείξει ότι οι δράστες μπορεί να

μην έχουν πάντα κέρδος. Αξίζει να σημειωθεί ότι υπάρχει μια ομάδα εγκληματιών στον κυβερνοχώρο γνωστή ως «hacktivists». Πρόκειται για άτομα που διαμαρτύρονται για τις πολιτικές και τις πρακτικές των οργανώσεων. Για παράδειγμα, το 2010, η ομάδα Anonymous hacktivist επιτέθηκε σε Mastercard, Visa και Paypal ως αντίποινα για τη διακοπή δωρεών στο WikiLeaks (Grispos, 2019).

Το Foreign Affairs and International Trade του Καναδά σημειώνει ότι το έγκλημα στον κυβερνοχώρο είναι εγκληματική δραστηριότητα που διαπράττεται χρησιμοποιώντας υπολογιστές και δίκτυα υπολογιστών. Αυτό συνεπάγεται ότι η διευκόλυνση των παραδοσιακών εγκλημάτων χρησιμοποιώντας υπολογιστές εμπίπτει επίσης στο έγκλημα στον κυβερνοχώρο. Παραδείγματα τέτοιου παραδοσιακού εγκλήματος περιλαμβάνουν παιδική πορνογραφία και διαδικτυακή απάτη. Ορισμένα εγκλήματα που μπορεί να καλύπτουν την έμμεση χρήση υπολογιστών για την εκτέλεση εγκλημάτων περιλαμβάνουν την επικοινωνία και την αποθήκευση δεδομένων και μπορεί να θεωρηθούν ως έγκλημα με τη βοήθεια υπολογιστή. Οι αυστραλιανοί νόμοι αναγνωρίζουν το ηλεκτρονικό έγκλημα ως αυτό που διεξάγεται μέσω υπολογιστή, στοχεύει στην τεχνολογία στον κυβερνοχώρο ή το χρησιμοποιεί για την αποθήκευση παράνομου υλικού. Αυτός ο ορισμός συμφωνεί με αυτόν του Wall, (2007) που διαιρεί το έγκλημα στον κυβερνοχώρο σε αδικήματα που στοχεύουν υπολογιστές και εγκλήματα που ενεργοποιούνται από υπολογιστές. Ο Cybercrime Act 2001 της Αυστραλίας χαρακτηρίζει το έγκλημα στον κυβερνοχώρο ως έγκλημα που προκαλεί βλάβη σε δεδομένα και συστήματα υπολογιστών. Ωστόσο, στα Ηνωμένα Αραβικά Εμιράτα, η νομοθεσία τους προσαρμόζεται ώστε να περιλαμβάνει αδικήματα κατά συστημάτων δεδομένων υπολογιστών και εγκλήματα που σχετίζονται με υπολογιστή, όπως πλαστογραφία, απάτη, απειλές και ξέπλυμα χρήματος.

Οι νόμοι των Ηνωμένων Πολιτειών ορίζουν το έγκλημα υπολογιστών ως έγκλημα που χρησιμοποιεί ή στοχεύει σε δίκτυα υπολογιστών που γενικά αναφέρονται σε ιούς, worms και επιθέσεις DoS. Το Ηνωμένο Βασίλειο έχει επίσης παρόμοια αντίληψη για εγκληματικές δραστηριότητες. Ωστόσο, ο νόμος για την κατάχρηση υπολογιστών στο Ηνωμένο Βασίλειο ορίζει ότι η χρήση δικτυωμένων υπολογιστών, τηλεφώνων ή τεχνολογίας Διαδικτύου για τη διεξαγωγή ή τη διευκόλυνση εγκλημάτων ισοδυναμεί με έγκλημα στον κυβερνοχώρο. Η ανάπτυξη της τεχνολογίας οδήγησε στη συνέχεια στην ανάπτυξη του όρου έγκλημα στον υπολογιστή. Ο Οργανισμός για την Οικονομία και την Ανάπτυξη (ΟΟΣΑ) σε συνοχή με τα κράτη μέλη των Ηνωμένων Εθνών κήρυξε

εγκλήματα που σχετίζονται με τη χρήση υπολογιστή ως παράνομα και ανήθικα. Ομοίως, δήλωσαν επίσης τη συνήθη επεξεργασία και διάδοση δεδομένων χωρίς την άδεια του ιδιοκτήτη ως παράνομη συμπεριφορά. Οι συστάσεις του Συμβουλίου της Ευρώπης για το ποινικό δικονομικό δίκαιο υποδεικνύουν ότι τα αδικήματα στον τομέα της πληροφορικής συνιστούν παράνομο έγκλημα και δήλωσαν ότι οι εξουσίες διερεύνησης πρέπει να έχουν δικαίωμα σε πληροφορίες που υποβάλλονται σε επεξεργασία ή μεταφέρονται μέσω συστημάτων υπολογιστών.

Υπάρχουν ανισότητες στην περιγραφή του εγκλήματος στον κυβερνοχώρο σε διεθνές επίπεδο. Οργανισμοί όπως η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, η Σύμβαση της Ένωσης των Αραβικών Κρατών και το Σχέδιο συμβάσεων της Αφρικανικής Ένωσης έχουν επιχειρήσει να ορίσουν το έγκλημα στον κυβερνοχώρο, παρόλο που οι ορισμοί τους δεν γίνονται αποδεκτοί παγκοσμίως (Alazab & Broadhurst, 2015). Η Συμφωνία της Κοινοπολιτείας Ανεξάρτητων Κρατών χρησιμοποιεί τον όρο "πληροφορίες υπολογιστή" για να περιγράψει αδικήματα που σχετίζονται με εγκλήματα υπολογιστών. Από την άλλη πλευρά, η Συμφωνία Οργανισμού Συνεργασίας της Σαγκάης προτείνει τον όρο αδικήματα πληροφοριών ως εκμετάλλευση της ιδιοκτησίας πληροφοριών που την επηρεάζει για παράνομους σκοπούς. Ο όρος κυβερνοέγκλημα ή έγκλημα στον υπολογιστή ερμηνεύεται διαφορετικά από διάφορες παρατάξεις και δικαιοδοσίες σε όλο τον κόσμο. Κατά συνέπεια, όλα τα εγκλήματα στον κυβερνοχώρο δεν αντιμετωπίζονται ή ποινικοποιούνται με τον ίδιο τρόπο σε διαφορετικά κράτη. Αυτό σημαίνει ότι ένα συγκεκριμένο έγκλημα στον κυβερνοχώρο θα μπορούσε να είναι έγκλημα σε μια χώρα, αλλά να μην πληροί το κατώτατο όριο σε μια άλλη. Αυτή η ερευνητική εργασία θα χρησιμοποιήσει τον όρο έγκλημα στον υπολογιστή και έγκλημα στον κυβερνοχώρο εναλλακτικά για να δηλώσει το έγκλημα που χρησιμοποιεί ή στοχεύει δεδομένα και συστήματα υπολογιστών για τη διάπραξη παράνομης δραστηριότητας.

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), η εγκληματικότητα μέσω υπολογιστών «αφορά κάθε παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που σχετίζεται με την αυτόματη επεξεργασία και διαβίβαση δεδομένων» (Karyda & Mitrou, 2007). Ανάλογα με τον τρόπο διάπραξης εγκλημάτων στον υπολογιστή, χωρίζονται σε:

- Εγκλήματα που διαπράττονται τόσο στον «πραγματικό» όσο και στον ψηφιακό κόσμο, π.χ. η συκοφαντία διαπράττεται επίσης με τη χρήση ηλεκτρονικού ταχυδρομείου (αποστολή ηλεκτρονικού ταχυδρομείου).
- Εγκλήματα που διαπράττονται μόνο σε περιβάλλον πληροφορικής (δηλαδή χωρίς τη χρήση του Διαδικτύου) και
- «Γνήσια» εγκλήματα στον κυβερνοχώρο, όπου η εγκληματική συμπεριφορά σχετίζεται αποκλειστικά με τον κυβερνοχώρο.

Επιπλέον, ανάλογα με το περιεχόμενο, τα εγκλήματα χωρίζονται σε:

- Εγκλήματα κατά της προσωπικότητας και της ιδιωτικής ζωής.
- Εγκλήματα κατά περιουσίας.
- Παράνομο και αθέμιτο/επιβλαβές περιεχόμενο.

Το έγκλημα στον κυβερνοχώρο διαθέτει ορισμένα ειδικά χαρακτηριστικά, εκ των οποίων τα πιο εμφανή είναι:

- **Ένας διασυνοριακός χαρακτήρας:** Τα αποτελέσματα μπορεί να συμβούν ταυτόχρονα σε πολλά μέρη, μερικές φορές επηρεάζοντας διαφορετικές χώρες ταυτόχρονα.
- **Τη «διακριτική ευχέρεια» της δέσμευσης:** Μπορεί να διαπραχθεί από οποιονδήποτε και να επηρεάσει οποιονδήποτε, χωρίς να απαιτείται η μετάβαση του δράστη σε άλλο τόπο. Επιπλέον, είναι αρκετά εύκολο να γίνει το οργανωμένο έγκλημα.
- **Δυσκολία έρευνας:** Η έρευνά του είναι αρκετά δύσκολη, λόγω των απαιτητικών απαιτήσεων για εξειδικευμένη κατάρτιση και εμπειρογνωμοσύνη.

1.3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Εάν ένας μηχανικός προσπαθήσει να αντιμετωπίσει μια δυσλειτουργική συσκευή, πρώτα θα εντοπίσει το πρόβλημα, στη συνέχεια θα προσπαθήσει να λύσει το πρόβλημα. Αν αντιμετωπίζει πάρα πολλά εμπόδια, θα τα σπάσει σε μικρά προβλήματα και θα τα κατακτήσει ένα ένα. Για να ελέγξει κανείς ή να λύσει ένα έγκλημα, πρέπει πρώτα να καταλάβει τι χαρακτηριστικό έχει, τι κίνητρο έχει ένας επιτιθέμενος και ποιες δυσκολίες αντιμετωπίζει.

Το έγκλημα στον κυβερνοχώρο, ως ένα νέο είδος εγκλήματος, έχει πολλά χαρακτηριστικά που είναι πιο ισχυρά από τα συμβατικά εγκλήματα. Αυτά τα χαρακτηριστικά τα καθιστούν πιο περίπλοκα για την επιβολή του νόμου από τα συμβατικά εγκλήματα.

1.3.1. ΔΙΕΘΝΙΚΟΤΗΤΑ

Σε σύγκριση με τα συμβατικά εγκλήματα, το έγκλημα στον κυβερνοχώρο είναι πολύ πιο γρήγορο και ισχυρότερο από τα προηγούμενα. Για παράδειγμα, η διακίνηση ναρκωτικών θα έπαιρνε μέρες μεταξύ των χωρών και ο λαθρέμπορος θα είχε τεράστιο κίνδυνο να συλληφθεί κατά τη μεταφορά. Αντίθετα, ένας χάκερ θα μπορούσε να χακάρει τον τραπεζικό λογαριασμό του οποίου η χώρα μπορεί να βρίσκεται στην άλλη άκρη της γης μέσα σε λίγα λεπτά και ο κίνδυνος να παγιδευτεί στη δράση είναι σχεδόν μηδενικός. Άλλωστε, χωρίς το κατάλληλο διεθνές δίκαιο, οι χάκερ θα μπορούσαν να περπατήσουν ελεύθεροι μετά τη διάπραξη εγκλήματος. Σε ορισμένες περιπτώσεις, ένας χάκερ με συγκεκριμένη γνώση του διεθνούς περιβάλλοντος θα μπορούσε να χρησιμοποιήσει τη σχέση μεταξύ των χωρών ως ασπίδα.

1.3.2. ΥΨΗΛΗ ΕΥΦΥΪΑ

Το έγκλημα στον κυβερνοχώρο χρειάζεται ορισμένες δεξιότητες όπως κάθε άλλο έγκλημα. Ωστόσο, σε αντίθεση με ορισμένα εγκλήματα μέρος του εγκλήματος απαιτεί εκτεταμένη γνώση στην επιστήμη των υπολογιστών. Εκτός από αυτό, ορισμένοι εγκληματίες πρέπει να είναι σε θέση να αναγνωρίσουν το αδύναμο σημείο σε μεγάλο αριθμό κωδικών. Πρέπει να καλύψουν το ψηφιακό τους αποτύπωμα σχολαστικά, ώστε να μην πιαστούν. Πρέπει να κάνουν σχέδια για τις επιθέσεις τους. Όλα αυτά τα χαρακτηριστικά τους καθιστούν ακόμη πιο δύσκολο να συλληφθούν από τις αρχές επιβολής του νόμου σε όλο τον κόσμο.

1.3.3. ΑΝΩΝΥΜΙΑ

Καθισμένοι πίσω από τον υπολογιστή, οι ταυτότητες των χρηστών του Διαδικτύου δεν είναι παρά αριθμός και γράμματα. Αυτές οι ταυτότητες μπορούν εύκολα να καλυφθούν και να τροποποιηθούν. Αυτό το χαρακτηριστικό δίνει στους ανθρώπους κουράγιο να κάνουν ό, τι φοβούνται να κάνουν στην πραγματική ζωή. Όσοι εκφοβίζονται στην πραγματική ζωή είναι πολύ πιθανό να συμπεριφέρονται εξαιρετικά στον κυβερνοχώρο για να απελευθερώσουν το θυμό και την ανικανοποίησή τους.

Οι ταυτότητες δίνουν στους ανθρώπους μια ευθύνη για τη συμπεριφορά τους (Shoemaker,2005). Ωστόσο, μόλις κρυφτεί η ταυτότητα, το αίσθημα ευθύνης πέφτει και οι άνθρωποι είναι σε θέση να παρουσιάσουν συμπεριφορές που τους καθιστούν υπεύθυνους στην πραγματική ζωή. Χαρακτηριστικό παράδειγμα είναι ο διαδικτυακός ρατσισμός. Μπορεί κανείς να βρεί πολλά σχόλια ρατσιστών σε διαδικτυακά μέσα όπως το YouTube, αλλά σπάνια στην πραγματική ζωή. Από τη στιγμή που η συμπεριφορά δεν συνδέεται πλέον με την ταυτότητα του καθένα ή το ποιος είναι, γίνεται πολύ πιο τολμηρός.

1.3.4. ΕΞΑΙΡΕΤΙΚΗ Οργάνωση

Με την ανάπτυξη της ασφάλειας του δικτύου, οι δυσκολίες διεξαγωγής εγκλήματος στον κυβερνοχώρο αυξάνονται με αυτό. Έτσι, αντί να δουλεύουν μόνοι και να αναλαμβάνουν όλο τον φόρτο εργασίας, οι εγκληματίες στον κυβερνοχώρο αποφασίζουν να συνεργαστούν και να μοιράσουν την εργασία. Ο καταμερισμός εργασίας καθιστά το έγκλημα στον κυβερνοχώρο πιο αποτελεσματικό και κερδοφόρο. Γενικά, αυτές οι ομάδες συναντιούνται σε διαδικτυακό φόρουμ. Επικοινωνούν μέσω των μέσων κοινωνικής δικτύωσης ή του chatnet darknet. Χωρίς να ξέρουν την

πραγματική ταυτότητα των άλλων. Αυτή η δομή καθιστά ακόμη πιο δύσκολη την επιβολή του νόμου για την σύλληψη ολόκληρου του οργανισμού.

1.4. ΚΙΝΗΤΡΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Υπάρχουν διάφοροι λόγοι για τους οποίους οι εγκληματίες στον κυβερνοχώρο εμπλέκονται στο έγκλημα. Ο κύριος λόγος είναι να κερδίσετε γρήγορα χρήματα. Αυτές οι ομάδες έχουν κίνητρο την απληστία και συχνά ασχολούνται με το ηλεκτρονικό εμπόριο, την ηλεκτρονική τραπεζική και την απάτη. Δεύτερον, τα εγκλήματα στον κυβερνοχώρο μπορούν να διαπραχθούν για κύρος και αναγνώριση. Οι περισσότεροι δράστες εδώ είναι νέοι που θέλουν να τραβήξουν την προσοχή και να νιώσουν σκληροί. Μπορεί να είναι ιδεαλιστές που θέλουν να βρίσκονται στο επίκεντρο αλλά να μην βλάπτουν κανέναν. Τρίτον, το έγκλημα στον κυβερνοχώρο μπορεί να δεσμευτεί για την καταπολέμηση μιας αιτίας που είναι βασική για τις πεποιθήσεις των δραστών. Σε αυτή την κατάσταση, οι δράστες δεν ενοχλούνται να προκαλέσουν βλάβη και καταστροφή, εφόσον επιτευχθούν οι στόχοι τους.

1.4.1. ΥΨΗΛΟ ΚΕΡΔΟΣ

Το ηλεκτρονικό έγκλημα είναι προσοδοφόρο. Οι άνθρωποι μπορούν να απεικονίσουν τους εγκληματίες στον κυβερνοχώρο ως πλοιάρχους της επιστήμης των υπολογιστών, προγραμματιστές με γνώση. Αντίθετα, οι περισσότεροι εγκληματίες στον κυβερνοχώρο δεν είναι. Χρησιμοποιούν απλώς το λογισμικό που αποκτούν. Σύμφωνα με μια συνέντευξη με ανώνυμους εγκληματίες στον κυβερνοχώρο, ένα ανεπιθύμητο ηλεκτρονικό ταχυδρομείο με ιστότοπο «ψαρέματος» κοστίζει περίπου 52 € και μπορεί να εκτιμήσει τα κέρδη έως και 520-650 € πριν κλείσει ο ιστότοπος αυτός οριστικά (Ιδιωτική συζήτηση με κυβερνοεγκληματία-Private communication with a cybercriminal). Η παράπλευρη ζημιά όπως ο λογαριασμός στα μέσα κοινωνικής δικτύωσης αποκλείεται. Το κέρδος είναι δέκα φορές μεγαλύτερο από την κύρια επένδυση. Σε άλλες χώρες, το κόστος για τη διεξαγωγή εγκλήματος στον κυβερνοχώρο είναι διαφορετικό, αλλά το κέρδος είναι παρόμοιο ακόμη και μεγαλύτερο (ILyin,2014).

Υπό το ζοφερό οικονομικό περιβάλλον σε όλο τον κόσμο, αυτή η βιομηχανία υψηλού κέρδους, αμελητέου κινδύνου προσελκύει εκατοντάδες και χιλιάδες ανθρώπους στην επιχείρηση. Πιστεύεται ότι αυτός είναι ο λόγος αύξησης του εγκλήματος στον κυβερνοχώρο σε όλο τον κόσμο.

Εκτός από αυτό, πολλές κυβερνοεγκληματικές ομάδες χρηματοδοτούνται καλά. Προσλαμβάνονται για να επιτεθούν σε αντιπάλους του εργοδότη τους, να αντλήσουν πολύτιμες πληροφορίες και να παρουσιάσουν άλλες παράνομες συμπεριφορές. Παρόλο που δεν ήταν δυνατή η εύρεση ακριβούς τιμής για διαφορετικές υπηρεσίες, οι ακριβείς υπηρεσίες βρέθηκαν κατά τη διάρκεια της έρευνας. Ορισμένοι χάκερ προς ενοικίαση προσφέρουν μόνο νομική υπηρεσία, πράγμα που σημαίνει ότι διεξάγουν ηθικές παραβιάσεις για άτομα ή εταιρείες για να εντοπίσουν την πιθανή παραβίαση της ασφάλειας ή να βρουν τον χαμένο κωδικό πρόσβασής τους. Αυτό το είδος χάκερ ονομάζεται "λευκό καπέλο". Ωστόσο, υπάρχουν επίσης πολλοί χάκερ που προσφέρουν παράνομες υπηρεσίες.

1.4.2. ΠΟΛΙΤΙΚΑ ΚΙΝΗΤΡΑ

Όπως αναφέρθηκε προηγουμένως, οι κυβερνοεγκληματικές ομάδες χρηματοδοτούνται καλά. Σε ορισμένες περιπτώσεις, οι χρηματοδότες είναι κυβερνήσεις. Καθώς η τεχνολογία μας φέρνει έναν βολικό και αποτελεσματικό τρόπο ζωής, μας φέρνει επίσης πιθανή απειλή. Οι κυβερνήσεις σε όλο τον κόσμο επίσης εκσυγχρονίζουν το σύστημά τους με τεχνολογία. Ωστόσο, καθιστά επίσης το κυβερνητικό σύστημα πιο ευάλωτο από πριν. Αμέτρητες ευαίσθητες κυβερνητικές πληροφορίες ψηφιοποιούνται και γίνονται στόχοι για χάκερ που εργάζονται για άλλες κυβερνήσεις.

Το πιο διαβόητο περιστατικό είναι γνωστό ως έργο PRISM. Η αμερικανική κυβερνητική υπηρεσία NSA διεξήγαγε (μπορεί ακόμη να διεξάγει) παράνομη παρακολούθηση σε παγκόσμια κλίμακα στο όνομα της αντιτρομοκρατίας. Φαίνεται ότι πολλές αμερικανικές επιχειρήσεις συμμετέχουν σε αυτό το έργο σε συνεργασία με την NSA. Αν και αρνήθηκαν τη συμμετοχή σε αυτό το έργο PRISM, ο πρώην εργολάβος της NSA Έντουαρντ Σνόουντεν παρουσίασε αρκετά πειστικά στοιχεία. Η αμερικανική κυβέρνηση συλλέγει μεγάλο αριθμό προσωπικών δεδομένων από όλους στον κόσμο, συμπεριλαμβανομένων υψηλόβαθμων κυβερνητικών αξιωματούχω. Οι ΗΠΑ έχουν ήδη δημιουργήσει τον δικό τους στρατό για κυβερνοπόλεμο που ονομάζεται United State Cyber Command (Wikipedia,2017). Ωστόσο, το ερώτημα είναι "Για άλλες χώρες, αν αυτό το είδος στρατιωτικών δραστηριοτήτων εντοπίστηκε σε άλλες χώρες, πρέπει να θεωρηθεί ως πράξη πολέμου;" (military.com,2016), αφού ο παραδοσιακός πόλεμος πρέπει να ακολουθεί αυστηρό διεθνές δίκαιο και συνθήκη. Αυτή η συμπεριφορά θα υπακούει επίσης στο νόμο και τη συνθήκη; Θα υπάρχουν στόχοι που προστατεύονται

από το νόμο και τη συνθήκη; Αυτό το είδος ερώτησης πρέπει να εξεταστεί, αλλά δεν συζητήθηκε περαιτέρω σε αυτή την εργασία.

Σε ορισμένες περιπτώσεις, η κυβέρνηση απολαμβάνει τους εγκληματίες στον κυβερνοχώρο ακόμη και τους τρομοκράτες, καθώς η συμπεριφορά τους είναι εναντίον κάποιου αντιπάλου της κυβέρνησης. Προσφέρουν πολιτικό άσυλο για τέτοιου είδους οργανώσεις. Με αυτόν τον τρόπο, θα μπορούσαν να επιτύχουν πολιτικό κέρδος μέσω αυτών.

Επίσης, υπάρχουν πολλές χώρες που ασχολούνται με τον κυβερνοχώρο. Φαίνεται ότι η πρόσφατη έξαρση ransomware είναι αρχικά κυβερνοόπλο από την NSA ή τη Βόρεια Κορέα. Αν και διαφορετικές ειδήσεις αναφέρονται από διαφορετικό πρακτορείο ειδήσεων, η ίδια θεωρία είναι ότι πρόκειται για κυβερνοόπλο που αναπτύχθηκε από την κυβέρνηση.

Ένα άλλο πρόσφατο περιστατικό είναι φήμες σχετικά με τη συμμετοχή της Ρωσίας στην προεκλογική εκστρατεία των προέδρων των ΗΠΑ. Η κατηγορία είναι ότι Ρώσοι χάκερ έθεσαν προσωρινά υπόψη τα εκλογικά δεδομένα για να βεβαιωθούν ότι ο Ντόναλντ Τραμπ θα κερδίσει τις εκλογές. Χωρίς καμία ισχυρή απόδειξη, αυτή η κατηγορία δεν μπορεί να σταθεί. Ωστόσο, αυτή η φήμη εφιστά την προσοχή στην κυβερνοασφάλεια της ηλεκτρονικής καμπάνιας (BBC,2017).

1.4.3. ΣΥΝΑΙΣΘΗΜΑΤΙΚΗ ΣΥΜΠΕΡΙΦΟΡΑ

Η συναισθηματική συμπεριφορά είναι ένας από τους κύριους λόγους για τους οποίους οι χάκερ κάνουν εγκλήματα στον κυβερνοχώρο. Μερικούς χάκερ τους χακάρουν για άλλους λόγους εκτός από το κέρδος. Η συμπεριφορά τους μπορεί να ξεκινήσει με μια μη κακόβουλη πρόθεση, αλλά και να κοστίσει ζημιά σε ανθρώπους σε όλο τον κόσμο.

Οι χάκερ είναι αρχικά ομάδες ανθρώπων που ενδιαφέρονται για την τεχνολογία, αλλά η συμπεριφορά τους μπορεί να είναι σε γκρίζο χώρο δικαίου. Έχουν την τάση να δείχνουν στους ανθρώπους τι είναι ικανοί να κάνουν. Έτσι, για αυτούς, το hacking είναι ένας τρόπος να επιδειχθούν στο κοινό. Ωστόσο, στην πορεία, θέτουν σε κίνδυνο την περιουσία άλλων με αυτόν τον τρόπο.

Υπάρχουν ακτιβιστές χάκερ που κάνουν hacking από πατριωτισμό. Το 1995, όταν οι ΗΠΑ έκαναν λάθος στην κινεζική πρεσβεία στο Βελιγράδι, Γιουγκοσλαβία, πολλοί κινέζοι ακτιβιστές χάκερ άρχισαν να ανταποδίδουν επιθέσεις σε κυβερνητικές ιστοσελίδες των ΗΠΑ και άλλες εγκαταστάσεις δικτύου.

Υπάρχουν πολλά άλλα συναισθήματα που μπορεί να οδηγήσουν ένα άτομο με γνώσεις υπολογιστών να κάνει εγκλήματα στον κυβερνοχώρο. Είναι απαραίτητο να κατανοήσει κανείς τα συναισθήματα των εγκληματιών στον κυβερνοχώρο για να βοηθήσει στον έλεγχο του κυβερνοεγκλήματος.

ΚΕΦΑΛΑΙΟ 2ο ΤΡΟΠΟΣ ΔΡΑΣΗΣ ΚΑΙ ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1. ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1.1. HACKING

Ο Gupta (2019) έχει ορίσει το hacking ως απόκτηση μη εξουσιοδοτημένης πρόσβασης ή συμβιβασμό συστημάτων για πρόσβαση. Ενώ το hacking μπορεί να χαρακτηριστεί ως εγκληματικό σε ορισμένες χώρες, υπάρχει ανάγκη για εμπειρογνώμονες για την ασφάλεια των πληροφοριών με τη γνώση του hacking για την αντιμετώπιση απειλών στον κυβερνοχώρο στους τομείς των επιχειρήσεων, της πολιτικής, των κοινωνικών μέσων και της εθνικής ασφάλειας. Υπάρχουν τρεις κύριοι τύποι χάκερ, σύμφωνα με τον Gupta, (2019). Ο πρώτος τύπος χάκερ είναι ο χάκερ του λευκού καπέλου που υπερασπίζεται τα συστήματα από άλλους επιτιθέμενους. Είναι εξουσιοδοτημένα και είναι κυρίως γνωστά για την παροχή ασφάλειας. Ο δεύτερος τύπος είναι ο χάκερ μαύρου καπέλου που λειτουργεί χωρίς εξουσιοδότηση. Αυτό το διαμέτρημα των χάκερ είναι επίσης γνωστό ως κακόβουλοι χάκερ και ενεργούν χωρίς την άδεια οποιουδήποτε είδους. Ο τρίτος τύπος είναι ο χάκερ Gray hat, του οποίου το ξίφος είναι δίκοπο. Μπορούν να είναι επιθετικά και αμυντικά, ανάλογα με τα οφέλη. Ο όρος γκρι χάκερ μπορεί επίσης να σημαίνει χάκερ των οποίων η πρόθεση είναι να προειδοποιήσουν τους άλλους για την ευπάθειά τους, ακόμη και αν μερικές φορές το κάνουν παράνομα.

Το hacking έχει τέσσερα βασικά στάδια, δηλαδή την αναγνώριση, τη σάρωση, την απόκτηση πρόσβασης και τη διατήρηση της πρόσβασης (Grispos, 2019). Σε πρώτο στάδιο, ο χάκερ προσπαθεί να βρει πληροφορίες σχετικά με τον στόχο του είτε ενεργά είτε παθητικά. Στη συνέχεια, ο επιτιθέμενος προχωρά στην αναζήτηση πολύ περισσότερων πληροφοριών σχετικά με τον στόχο, σαρώνοντας ή πραγματοποιώντας διάφορες αξιολογήσεις για να λάβει ευαίσθητες πληροφορίες σχετικά με τον στόχο. Η τρίτη φάση αποκτά πρόσβαση, κατά την οποία ο εισβολέας εκτελεί το hack. Ο εισβολέας εκμεταλλεύεται και εκτελεί μια ευπάθεια εκμετάλλευσης για να αποκτήσει πρόσβαση. Στην επόμενη φάση, ο εισβολέας εγκαθιστά backdoors ή Trojans για να διατηρήσει την πρόσβαση. Τέλος, διαγράφουν αρχεία καταγραφής και άλλες λεπτομέρειες για να μην πιαστούν. Το Lizard Squad είναι ένας τύπος μαύρου καπέλου μιας ομάδας χάκερ που έχει προσδιοριστεί ως παράδειγμα για αυτήν τη μελέτη. Η ιστορία και η δραστηριότητα της ομάδας μπορούν να εντοπιστούν στο 2014 όταν

επιτέθηκε στην πλατφόρμα παιχνιδιών του Xbox και του PlayStation, μοιράζοντας τη φιλοξενία μαζί τους. Η ομάδα πραγματοποίησε επίσης διάφορες επιζήμιες παραβιάσεις, όπως η κατάργηση του διαδικτύου στη Βόρεια Κορέα, η επίθεση στο δίκτυο PlayStation και η επίθεση στο Destiny, στην οποία άλλαξαν το λογότυπο της εταιρείας στην ιστοσελίδα τους (Grimes, 2017).

2.1.2. ΥΠΟΛΟΓΙΣΤΙΚΗ ΑΠΑΤΗ

Αυτή η μορφή ηλεκτρονικού εγκλήματος είναι επίσης γνωστή ως «ηλεκτρονικό ψάρεμα». Περιλαμβάνει καταστάσεις στις οποίες οι δράστες εμφανίζονται ως εκπρόσωποι ενός οργανισμού, με στόχο απευθείας τους πελάτες της τράπεζας (Doyle, 2011). Παλαιότερα εργαλεία επικοινωνίας όπως τηλέφωνα και ταχυδρομείο ήταν τα όργανα που χρησιμοποιούνταν για την απάτη και την εξαπάτηση ανθρώπων. Σήμερα, τα σύγχρονα εργαλεία όπως το ηλεκτρονικό ταχυδρομείο, τα μηνύματα κειμένου και οι συνομιλίες στα μέσα κοινωνικής δικτύωσης έχουν αντικαταστήσει τις παραδοσιακές μεθόδους και πλέον χρησιμοποιούνται για τη διάπραξη εγκλήματος στον κυβερνοχώρο. Οι απατεώνες υποδύονται νόμιμους αποστολείς, όπως τραπεζίτες και μπορούν να ξεφύγουν με βασικά διαπιστευτήρια, όπως ονόματα χρήστη, κωδικούς πρόσβασης και αριθμούς λογαριασμού. Σε αυτή τη μορφή εγκλήματος στον κυβερνοχώρο, οι απατεώνες στοχεύουν χειροκίνητα τους παραλήπτες μέσω κειμένων που αποστέλλονται μαζικά με τον αποστολέα να ελπίζει να επιπλέξει ανυποψίαστα θύματα να μοιραστούν τα προσωπικά τους δεδομένα. Οι εγκληματίες στον κυβερνοχώρο μπορεί επίσης να ενεργούν για να προωθούν συμφωνίες που φαίνονται πολύ καλές για να είναι αληθινές. Μπορεί να προσποιούνται ότι προσφέρουν στα θύματα «επενδυτικές» ευκαιρίες, μετά τις οποίες μετά από κάποιο χρονικό διάστημα εκθαμβώνονται με τα κεφάλαια των θυμάτων.

Σύμφωνα με την Έκθεση Ερευνών Παραβίασης Δεδομένων Verizon 2019, σχεδόν το ένα τρίτο όλων των παραβιάσεων αφορούσε αυτή τη μορφή απάτης στον υπολογιστή. Ο Casey (2011) αποδίδει την εκτόξευση των περιπτώσεων ηλεκτρονικού ψαρέματος σε καλά διαμορφωμένα ιδανικά εργαλεία που οι απατεώνες και οι δράστες χρησιμοποιούν ακόμη και με λίγες γνώσεις λογισμικού υπολογιστών. Το 2016, οι επιθέσεις ηλεκτρονικού "ψαρέματος" κατάφεραν να λάβουν κρίσιμους κωδικούς πρόσβασης από την ομάδα εκστρατείας της Χίλαρι Κλίντον κατά τη διάρκεια των γενικών εκλογών. Την ίδια χρονιά, μερικοί υπάλληλοι από το Πανεπιστήμιο του Κάνσας φέρεται να έχασαν την αμοιβή τους αφού έδωσαν πληροφορίες κατάθεσης

μισθού σε ψαράδες. Ο Grispos, (2019) σημειώνει ότι η διαθεσιμότητα των κιτ ηλεκτρονικού "ψαρέματος" έχει επιτρέψει στους κυβερνοεγκληματίες να πραγματοποιήσουν επιθέσεις ηλεκτρονικού "ψαρέματος", παρόλο που ορισμένοι από αυτούς έχουν πολύ μικρή γνώση του θέματος. Αυτά τα κιτ διατίθενται στο σκοτεινό ιστό, μια σκιερή και επικίνδυνη πλατφόρμα που χρησιμοποιείται συχνά για τη διεξαγωγή παράνομων επιχειρήσεων.

2.1.3. ΕΠΙΘΕΣΕΙΣ ΆΡΝΗΣΗΣ ΥΠΗΡΕΣΙΑΣ

Αυτές οι επιθέσεις περιλαμβάνουν μεγάλη ποσότητα κίνησης που αποστέλλεται σε ένα δίκτυο κεντρικού υπολογιστή καθιστώντας την απρόσιτη για τους κανονικούς χρήστες. Αυτές οι επιθέσεις δρουν για να αποτρέψουν τη σύνδεση ατόμων σε δίκτυο ή υπολογιστή. Στη συνέχεια, αυτές οι επιθέσεις αξιοποιούν πολυάριθμους υπολογιστές στον ιστό για να στέλνουν δεδομένα στον υπολογιστή ενός θύματος, αφήνοντάς τον ανίκανο να στείλει και να λάβει συνηθισμένη κίνηση στο Διαδίκτυο. Τέτοιες επιθέσεις αποδείχθηκαν επιζήμιες για τις επιχειρήσεις που απαιτούν τη λειτουργία του διαδικτύου. Κατά τη διάρκεια των επιθέσεων Dos, ο εισβολέας πλημμυρίζει έναν διακομιστή δικτύου με αιτήματα κάνοντας πολλά αιτήματα στον διακομιστή (Doyle, 2011). Αυτά τα αιτήματα είναι παράνομα και περιέχουν κατασκευασμένες διευθύνσεις επιστροφής που παραπλανούν τους διακομιστές υπολογιστών των θυμάτων καθώς πιστοποιούν τους αιτούντες. Κατά τη διάρκεια αυτής της διαδικασίας, το σύστημα κατακλύζεται και αποτυγχάνει να εκτελέσει κανονικές εργασίες. Οι πιο συνηθισμένες επιθέσεις Dos είναι οι Smurf Attacks και SYN Flood.

2.1.4. ΙΟΙ, TROJANS ΚΑΙ WORMS

Το όνομα Trojan προέρχεται από την αρχαία ελληνική μυθολογία. Οι Έλληνες ήθελαν να κατακτήσουν την πόλη της Τροίας αλλά τα τείχη της ήταν αδιαπέραστα. Έβαλαν τους καλύτερους στρατιώτες τους σε μια μεγάλη καμπυλότητα ενός Δούρειου ίππου που εξαπάτησε τους αντιπάλους τους να φέρουν τους στρατιώτες στα τείχη τους. Ομοίως, στη γλώσσα του υπολογιστή, το Trojan είναι ένα πρόγραμμα που χρησιμοποιείται στη συσκευή ενός θύματος εν αγνοία του. Παρέχει στον δράστη απομακρυσμένη πρόσβαση στον υπολογιστή του θύματος. Ένας ιός συνδέεται με προγράμματα ή αρχεία και μπορεί να εξαπλωθεί από υπολογιστή σε υπολογιστή αφήνοντας λοιμώξεις. Οι ιοί υπολογιστών, όπως και οι ανθρώπινοι ιοί, διαφέρουν ως προς τη σοβαρότητά τους και μπορούν να προκαλέσουν βλάβες στο λογισμικό, το

υλικό και τα έγγραφα. Οι υπολογιστές των θυμάτων είναι ευαίσθητοι στον ιό μόλις τρέξουν ή ανοίξουν μολυσμένα προγράμματα. Εξίσου ή πιο επικίνδυνο είναι το ζεστό που αναφέρεται σε μια υποομάδα του ιού που μπορεί να ταξιδέψει από τον έναν υπολογιστή στον άλλο χωρίς βοήθεια από κάποιο άτομο. Τα worms είναι εξαιρετικά επικίνδυνα καθώς μπορούν να αναπαραχθούν και να δημιουργήσουν καταστροφικά αποτελέσματα.

2.1.5. ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ

Η κυβερνο -τρομοκρατία είναι ένα ιδιαίτερο είδος εγκλήματος στον κυβερνοχώρο. Η κυβερνοτρομοκρατία, με τον ορισμό του CSIS, είναι «η χρήση εργαλείων δικτύου υπολογιστών για τον τερματισμό κρίσιμων εθνικών υποδομών (π.χ. ενέργεια, μεταφορές, κυβερνητικές επιχειρήσεις) ή τον εξαναγκασμό ή τον εκφοβισμό μιας κυβέρνησης ή άμαχου πληθυσμού» (Lewis,2002).

Με την ανάπτυξη τρομοκρατικών οργανώσεων, πολλά άτομα με υψηλή μόρφωση προσχώρησαν σε τρομοκρατικές ομάδες. Η προπαγάνδα τους άρχισε να εξελίσσεται από παραδοσιακά μέσα, όπως τηλεόραση, φυλλάδια, βίντεο στο Διαδίκτυο, διαδικτυακή ροή και ιστότοπους. Μετά από αυστηρούς διαδικτυακούς κανονισμούς μεταξύ των χωρών, οι τρομοκράτες άρχισαν να χρησιμοποιούν το deep web, γνωστό και ως dark web, για να στρατολογήσουν νέους και να διδάξουν στους ανθρώπους πώς να φτιάχνουν IED . Λόγω της διεθνούς χρήσης του Διαδικτύου, είναι σε θέση να ενθαρρύνουν τους ανθρώπους να πραγματοποιούν τρομοκρατικές επιθέσεις σε όλο τον κόσμο .Αποδεικνύεται ότι είναι πολύ πιο αποτελεσματική από την παραδοσιακή τους μέθοδο. Λόγω της μυστικότητας και της τεχνικής πρόκλησης του σκοτεινού ιστού, αυτό το είδος ιστότοπου είναι δύσκολο να κλείσει.

Το ISIS είναι απλώς η κορυφή του παγόβουνου. Υπάρχουν πολλές άλλες τρομοκρατικές ομάδες που χρησιμοποιούν την ίδια μέθοδο διάπραξης εγκλήματος. Σε ορισμένες περιπτώσεις, οι τρομοκρατικές ομάδες έχουν το δικό τους κυβερνοχώρο, όπως το «Κέντρο Πληροφόρησης του Ανατολικού Τουρκεστάν».

Εκτός από τα παραπάνω, εάν μια πολύ εκπαιδευμένη και οργανωμένη ομάδα σπάσει δημόσιες εγκαταστάσεις, όπως το σύστημα μεταφοράς, θα προκαλέσει δημόσιο πανικό που θα οδηγήσει σε όλεθρο. Η πιθανή ζημιά στη ζωή και την ευημερία, η χρηματοδότηση θα είναι ανεξέλεγκτη.

2.2. ΕΜΦΑΝΙΣΗ ΚΑΙ ΔΟΜΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Οι τεχνολογίες και οι επικοινωνίες αλλάζουν ραγδαία στη σύγχρονη εποχή, με αποτέλεσμα να αλλάζουν συνεχώς οι έννοιες του εγκλήματος και της εγκληματικότητας σε έναν διαδικτυακό κόσμο. Η επικράτηση των τεχνολογιών και του διαδικτύου έχει αλλάξει ριζικά τον τρόπο που οι άνθρωποι ζούν, επικοινωνούν, ταξιδεύουν, μοιράζονται πληροφορίες, μεταφέρουν κεφάλαια, εργάζονται και δημιουργούν επιχειρήσεις (Viano, 2017). Για να ξεκινήσει κανείς συζήτηση για το έγκλημα στον κυβερνοχώρο, τη θυματοποίηση στο διαδίκτυο και τη χρήση μεθόδων πρόληψης του εγκλήματος στον κυβερνοχώρο, είναι ζωτικής σημασίας να κατανοηθεί πώς προέκυψε ο κυβερνοχώρος, την έκταση του και το πώς ρυθμίζεται.

Σύμφωνα με το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα (2013), το ένα τρίτο του παγκόσμιου πληθυσμού (2,3 δισεκατομμύρια άνθρωποι) έχουν πρόσβαση στο Διαδίκτυο. Περίπου το 45% όλων των χρηστών του διαδικτύου είναι κάτω των 25 ετών. Ως εκ τούτου, ιδιαίτερα για τη νεότερη ομάδα, γίνεται πιο σπάνιο να συναντήσει κανείς ένα έγκλημα που δεν περιλαμβάνει ορισμένα στοιχεία σύνδεσης στο Διαδίκτυο. Το εξελισσόμενο περιβάλλον του διαδικτύου και των τεχνολογιών καθιστά τον προγραμματισμό και τις προβλέψεις γύρω από το έγκλημα στον κυβερνοχώρο αβέβαιο, ειδικά για τους φορείς επιβολής του νόμου. Ως αποτέλεσμα, το πεδίο του εγκλήματος στον κυβερνοχώρο συχνά δεν ρυθμίζεται ή ρυθμίζεται από ξεπερασμένα καταστατικά που δεν περιλαμβάνουν τις νεότερες εξελίξεις.

Τα εγκλήματα στον κυβερνοχώρο με σημαντικό αντίκτυπο έχουν συμβεί από τα πρώτα χρόνια του Διαδικτύου. Τον Μάιο του 2000, ένας ιός υπολογιστών που ονομάζεται "Love Bug" μολύνει υπολογιστές σε όλο τον κόσμο, συμπεριλαμβανομένων των κυβερνητικών υπηρεσιών στο Ηνωμένο Βασίλειο και τις ΗΠΑ, με αποτέλεσμα εκτιμώμενη ζημία μεταξύ 7-10 δισεκατομμυρίων δολαρίων. Ο πρωταρχικός ύποπτος ήταν φοιτητής κολλεγίου από τις Φιλιππίνες, ωστόσο όλες οι κατηγορίες αποσύρθηκαν και ο Onel de Guzman, ύποπτος τότε, δεν διώχθηκε, καθώς οι Φιλιππίνες δεν είχαν νόμους που κάλυπταν την παραβίαση υπολογιστών βάσει του οποίου θα μπορούσε να διωχθεί (Philippsohn , 2001).

Η έκθεση της Deloitte (2015) για τις τάσεις στην κυβερνοασφάλεια αναφέρει ότι το έγκλημα στον κυβερνοχώρο εξελίσσεται παράλληλα με τις τεχνολογίες και γίνεται όλο και πιο εξελιγμένο. Οι χάκερ δεν εκμεταλλεύονται πλέον στόχους ευκαιρίας, αλλά

έχουν την ελευθερία να επιλέξουν συγκεκριμένα άτομα, εταιρείες ή υπηρεσίες που γίνονται διαθέσιμα καθώς τα θύματα εμπιστεύονται όλο και περισσότερες πληροφορίες για να είναι ασφαλείς στο Διαδίκτυο, γεγονός που ανοίγει νέες ευκαιρίες για τους εγκληματίες. Μια άλλη πλευρά του κυβερνοχώρου που μπορεί να προκαλέσει πιθανά προβλήματα είναι η τεχνητή νοημοσύνη και τα drones, τα οποία μπορούν να χρησιμοποιηθούν ως παρακολούθηση, παραβίαση της ιδιωτικής ζωής των ανθρώπων ή ακόμη και ως θανατηφόρο όπλο. Ο Graham (2016) παρέχει ένα παράδειγμα χρήσης ρομπότ με θανατηφόρο αποτέλεσμα. Τον Ιούλιο του 2016, στο Ντάλας του Τέξας, η αστυνομία χρησιμοποίησε ένα ρομπότ για να βρει και να εξαλείψει έναν ελεύθερο σκοπευτή που σκότωσε πέντε αστυνομικούς. Η χρήση ρομπότ για τη δολοφονία υπόπτων είναι πραγματικά ασυνήθιστη, ωστόσο πολλές αστυνομικές δυνάμεις χρησιμοποιούν συχνά τηλεκατευθυνόμενα μη επανδρωμένα αεροσκάφη για να απενεργοποιήσουν ή να πυροδοτήσουν βόμβες.

Ο Yar (2006) υποστηρίζει ότι το ζήτημα του εγκλήματος στον κυβερνοχώρο έπρεπε να είχε αντιμετωπιστεί πολύ νωρίτερα στο πλαίσιο της κοινωνιολογίας, της ψυχολογίας και της εγκληματολογίας. Ο συγγραφέας δηλώνει ότι το μείζον ζήτημα για τη μελέτη του εγκλήματος στον κυβερνοχώρο είναι η απουσία οποιωνδήποτε τρέχοντων και συνεπών ορισμών του εγκλήματος. Ο Wall (2001) σημειώνει ότι ο όρος «έγκλημα στον κυβερνοχώρο» δεν έχει συγκεκριμένο ορισμό στο δίκαιο, ωστόσο ο όρος χρησιμοποιείται συχνά στην πολιτική, στα μέσα ενημέρωσης και στο σύστημα ποινικής δικαιοσύνης. Ο Yar προτείνει ότι αντί να προσπαθήσει κανείς να εννοήσει τον όρο «έγκλημα στον κυβερνοχώρο» ως ένα μοναδικό φαινόμενο, θα πρέπει να θεωρηθεί ως μια σειρά δραστηριοτήτων όπου τα δίκτυα τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) ή το διαδίκτυο είναι βασικές μεταβλητές. Από την άλλη πλευρά, οι Thomas & Loader (2000) όρισαν το έγκλημα στον κυβερνοχώρο ως έναν εννοούμενο όρο- «δραστηριότητες που μεσολαβούν από υπολογιστή, είτε είναι παράνομες είτε θεωρούνται παράνομες από ορισμένα μέρη και οι οποίες μπορούν να διεξαχθούν μέσω παγκόσμιων ηλεκτρονικών δικτύων» (Thomas & Loader, 2000, σελ. 3). Ο ορισμός που παρέχουν οι ακαδημαϊκοί αγγίζει μια κρίσιμη διάκριση μεταξύ εγκλήματος (πράξη που απαγορεύεται από το νόμο) και παρέκκλισης (πράξη που παραβιάζει άτυπα κοινωνικά πρότυπα), η οποία είναι σημαντική για περαιτέρω προβληματισμό σχετικά με τον ορισμό.

Παρά τις προσπάθειες πολλών ακαδημαϊκών να καταλήξουν σε έναν οριστικό ορισμό του φαινομένου, ο Wall (2008a) πιστεύει ότι υπάρχει ακόμη ένα κενό στην κατανόηση του τρόπου με τον οποίο κατασκευάζεται ο όρος «έγκλημα στον κυβερνοχώρο». Ο συγγραφέας ισχυρίζεται ότι ο νόμος στερείται σαφούς ορισμούς για το έγκλημα στον κυβερνοχώρο, ο οποίος οδηγεί στο κοινό να δημιουργήσει τη δική του αντίληψη για το τι είναι το έγκλημα, δημιουργώντας στη συνέχεια πολλούς μύθους γύρω από αυτό. Ο Wall πιστεύει ότι η προέλευση των εννοιών του εγκλήματος στον κυβερνοχώρο έγκειται σε μυθιστορήματα και ταινίες επιστημονικής φαντασίας, που ήταν οι πρώτες πηγές οπτικοποίησης του κυβερνοχώρου. Ένας άλλος σημαντικός παράγοντας, σύμφωνα με τον Wall, είναι η επιθυμία του κοινού για αξιόλογες πληροφορίες, συνέπεια και κίνητρο για τη συνεχή παραγωγή «σοκαριστικού» περιεχομένου από τα μέσα μαζικής ενημέρωσης, γεγονός που εξηγεί τα μέσα ενημέρωσης που προκαλούν συγκλονιστικό έγκλημα στον κυβερνοχώρο. Ως αποτέλεσμα, πολλοί μύθοι κατασκευάζονται γύρω από το έγκλημα στον κυβερνοχώρο, γεγονός που δημιουργεί λανθασμένες αντιλήψεις για αυτό στο κοινό (Wall, 2008β). Ως πηγή αυτής της μυθολογίας, ο συγγραφέας αναθεωρεί την περίληψη του House of Lords Science και Έκθεση επιτροπής επιλογής τεχνολογίας (House of Lords, 2007, σελ. 6). Για παράδειγμα, ο μύθος ενός «παντοδύναμου υπερ-χάκερ» που γνωρίζει νομικά κενά και είναι αδύνατο να εντοπιστεί. Ο Κέβιν Μίτνικ, ο οποίος ήταν το πρόσωπο του «παντοδύναμου υπερ-χάκερ» στη δεκαετία του 1990, αποδόμησε τον δικό του μύθο εξηγώντας ότι τότε τα επίπεδα ασφάλειας ήταν πολύ χαμηλότερα από τα σημερινά. Οι απλές λεπτομέρειες σύνδεσης, όπως το όνομα χρήστη «Διαχειριστής» και ο κωδικός πρόσβασης , ήταν κοινές και οι βασικές κινήσεις κοινωνικής μηχανικής, όπως το να πείσουν τους υπαλλήλους χαμηλού επιπέδου και να αποκτήσουν πρόσβαση στους κωδικούς πρόσβασής τους, που δεν ήταν δύσκολο να επιτευχθούν (Mitnick & Simon, 2002). Αυτοί οι μύθοι κατασκευάστηκαν στις πρώτες χρονιές εμφάνισης του διαδικτύου και δημιούργησαν κάποιες πεποιθήσεις γύρω από τον κυβερνοχώρο, οι οποίες εξακολουθούν να επηρεάζουν τις τρέχουσες αντιλήψεις του κοινού για το έγκλημα στον κυβερνοχώρο, καθώς και την αναγνώριση του εγκλήματος \ ως πραγματική απειλή. Από την άλλη πλευρά, ο Singleton (2013) υποστηρίζει ότι η απειλή του εγκλήματος εξαπλώνεται και κλιμακώνεται γρήγορα. Ο συγγραφέας δηλώνει επίσης ότι η αυξημένη χρήση του Διαδικτύου κατά τη διάρκεια της ιστορίας δημιούργησε το έγκλημα στον κυβερνοχώρο και τα πραγματικά ποσοστά θυματοποίησης στον γενικό πληθυσμό.

Οι Owen et al.,(2017), μέλη της UCLan Cybercrime Research Unit (UCRU) στο Πανεπιστήμιο του Central Lancashire, παρείχαν μερικές από τις πιο σύγχρονες εργασίες που αντιμετωπίζουν πιο σύγχρονα κενά στην εγκληματολογική θεωρία σχετικά με το έγκλημα στον κυβερνοχώρο. Οι συγγραφείς εξετάζουν το ζήτημα αυτό από διάφορες οπτικές γωνίες, προσπαθώντας να αποδείξουν ότι το έγκλημα στον κυβερνοχώρο πρέπει να θεωρηθεί ως ένα διεπιστημονικό ζήτημα. Στοιχεία όπως οι νόμοι που το διέπουν, οι τρόποι ρύθμισης του κυβερνοχώρου, η απόκλιση και η ταυτότητά του αναθεωρούνται στην εργασία από τις προοπτικές της εγκληματολογίας, της κοινωνιολογίας, της φιλοσοφίας, της επιστήμης των υπολογιστών και άλλων τομέων των κοινωνικών και εφαρμοσμένων επιστημών. Αυτό το έργο δείχνει πραγματικά πόσο περίπλοκο μπορεί να είναι το έγκλημα στον κυβερνοχώρο και γιατί πρέπει να αντιμετωπιστεί από διαφορετικές απόψεις και διαφορετικές φιλοσοφικές γωνίες λόγω της συνεχώς μεταβαλλόμενης φύσης του.

Ένας τρόπος εξέτασης του εγκλήματος στον κυβερνοχώρο στον τομέα της εγκληματολογίας είναι μέσω της εφαρμογής παραδοσιακών θεωριών, τις οποίες έχουν συντάξει πολλοί συγγραφείς. Ο Choi (2011) εφάρμοσε τη Θεωρία ρουτίνας δραστηριότητας (Routine Activity Theory - RAT) των Cohen & Felson (1979) για τα εγκλήματα στον κυβερνοχώρο, προσπαθώντας να εξετάσει ποιοι παράγοντες ευθύνονται για τη θυματοποίησή τους. Για να λειτουργήσει ο RAT υπάρχουν τρεις κύριοι παράγοντες που πρέπει να υπάρχουν ταυτόχρονα για να συμβεί η θυματοποίηση: ένας ενδιαφερόμενος δράστης, ένας κατάλληλος στόχος και η απουσία ενός ικανού κηδεμόνα. Ο Choi διαπίστωσε ότι τα διαφορετικά πρότυπα τρόπου ζωής συνδέονται άμεσα με τη θυματοποίηση στον κυβερνοχώρο. Ο συγγραφέας αναφέρει επίσης ότι ο McQuade (2006) πρότεινε αυτά τα ευρήματα νωρίτερα και τα προγράμματα πρόληψης του εγκλήματος της ποινικής δικαιοσύνης τα αγνόησαν. Επιπλέον, οι Holt & Bossler (2009) εφάρμοσαν τον RAT σε μια συγκεκριμένη μορφή εγκλήματος στον κυβερνοχώρο - την ηλεκτρονική παρενόχληση. Σύμφωνα με τα αποτελέσματα της έρευνας, οι ακαδημαϊκοί έβγαλαν διάφορα συμπεράσματα. Πρώτον, η συνηθισμένη χρήση υπολογιστή και η φυσική κηδεμονία είχαν μικρή επίδραση στα διαδικτυακά θύματα παρενόχλησης. Δεύτερον, η εμπλοκή σε αποκλίνουσες δραστηριότητες στον κυβερνοχώρο αυξάνει τον κίνδυνο θυματοποίησης. Ο Kigerl (2012) υιοθετεί μια άλλη προοπτική και εφαρμόζει τον RAT στο έγκλημα στον κυβερνοχώρο σε εθνικό και όχι σε ατομικό επίπεδο. Στόχος της έρευνάς του ήταν να ανακαλύψει τους πιο ακριβείς

προγνωστικούς παράγοντες υψηλής δραστηριότητας στον κυβερνοχώρο σε οποιαδήποτε συγκεκριμένη χώρα. Χρησιμοποιώντας ένα δείγμα 132 χωρών, ο ερευνητής μπόρεσε να συμπεράνει ότι τα πλουσιότερα έθνη είχαν υψηλότερα ποσοστά δραστηριότητας στον κυβερνοέγκλημα, σε μεγάλο βαθμό ως συνέπεια της πρόσβασης περισσότερων ατόμων στο διαδίκτυο. Ωστόσο, ο συγγραφέας υποστήριξε επίσης ότι η ανεργία αύξησε τα ποσοστά εμπλοκής στο κυβερνοέγκλημα (Kigerl, 2012).

Ένας άλλος τρόπος κατανόησης του φαινομένου του εγκλήματος στον κυβερνοχώρο είναι η εξέταση των βασικών κανονισμών και νόμων γύρω από το έγκλημα στον κυβερνοχώρο και των αλλαγών τους με την πάροδο του χρόνου. Ο Griffin (2012) υποστηρίζει ότι το κυβερνοέγκλημα είναι ένα πραγματικά ανεξερεύνητο πεδίο, με πολλές προκλήσεις και ζητήματα που πρέπει να αντιμετωπιστούν. Ο συγγραφέας μιλά για πτυχές στον κυβερνοχώρο όπως η ιδιωτικότητα, η ανωνυμία και τα δικαιώματα και προτείνει τρόπους με τους οποίους οι νόμοι μπορούν να δομηθούν γύρω από αυτές τις αρχές για την καλύτερη εφαρμογή σε υποθέσεις ηλεκτρονικού εγκλήματος και συζητά τους τρόπους χειρισμού τους από νομική σκοπιά. Για παράδειγμα, οι Gray et al., (2013) εξέτασαν την υπόθεση United States v. Jones από την άποψη της ιδιωτικής ζωής στον κυβερνοχώρο. Η τέταρτη τροπολογία στο σύνταγμα των ΗΠΑ υπονοεί ότι ένα άτομο έχει δικαίωμα στην ιδιωτική ζωή και επομένως ο δράστης δεν μπορεί να διωχθεί διότι, κατά τη διάρκεια της έρευνας, η κυβέρνηση θα εισβάλει στην ιδιωτική ζωή του δράστη προκειμένου να συγκεντρώσει στοιχεία εναντίον του. Οι ακαδημαϊκοί συζητούν αυτό το ζήτημα και πώς μπορεί να αντιμετωπιστεί η ιδιωτικότητα στον κυβερνοχώρο από τη σκοπιά του δικαίου. Επιπλέον, ο Dobrinoiu (2014) συζήτησε πώς αντιμετωπίζονται οι νόμοι όσον αφορά τις κλοπές ταυτότητας στη Ρουμανία. Τα εγκλήματα κλοπής ταυτότητας έγιναν πιο διαδεδομένα με τον κυβερνοχώρο να ανοίγει νέες ευκαιρίες για εγκληματικότητα , παράλληλα με τους οποίους οι νόμοι προσαρμόζονταν, αν και όχι αρκετά γρήγορα. Ο συγγραφέας συζητά τα ελαττώματα στη νομοθεσία με αναφορά σε διαφορετικά άρθρα του νόμου και δηλώνει ότι υπάρχει πολύς χώρος για παρεξήγηση και παρερμηνεία των νόμων που σχετίζονται με εγκλήματα κλοπής ταυτότητας.

Σύμφωνα με τον Wall (2015), οι άνθρωποι έχουν αρχίσει να αναγνωρίζουν ότι το έγκλημα στον κυβερνοχώρο υπάρχει και ότι αποτελεί πραγματική απειλή, ωστόσο, όταν υποβάλλονται δικαστικά περιστατικά εγκλήματος στον κυβερνοχώρο, είναι πολύ πιθανό να αναθεωρηθούν ως «παραδοσιακά» και όχι ως κυβερνοεγκλήματα. Ο συγγραφέας ισχυρίζεται ότι η κατάσταση των πραγμάτων που σχετίζονται με το

έγκλημα στον κυβερνοχώρο σίγουρα βελτιώνεται, αλλά υπάρχουν ακόμα πολλές προκλήσεις που πρέπει να αντιμετωπιστούν. Ο Baines (2013) παρέχει ένα παράδειγμα εγκλήματος στον κυβερνοχώρο που αντιμετωπίζεται ως πραγματική απειλή και έχει αρχίσει να αντιμετωπίζεται σωστά. Τον Ιανουάριο του 2013, το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος (European Cybercrime Centre - EC3) ιδρύθηκε ως μέρος της Europol στη Χάγη για να αντιμετωπίσει το ζήτημα του εγκλήματος στον κυβερνοχώρο στα κράτη μέλη της Ευρωπαϊκής Ένωσης. Το 2014, το νέο τμήμα της Ιντερπόλ, το Κέντρο Ψηφιακού Εγκλήματος, άρχισε να λειτουργεί, με στόχο να εντοπίσει τα εγκλήματα στον κυβερνοχώρο σε διάφορους κλάδους, όπως ακαδημαϊκούς, οργανώσεις της κοινωνίας των πολιτών και κυβερνητικές αρχές. Παρ 'όλα αυτά, το ζήτημα του εγκλήματος στον κυβερνοχώρο πρέπει ακόμη να αντιμετωπιστεί από την οπτική γωνία του γενικού πληθυσμού, καθώς όχι μόνο οι οργανώσεις και οι αρχές επηρεάζονται από κυβερνοεπιθέσεις. Το επίκεντρο αυτής της μελέτης που συνέταξαν οι Habirovs & Arturs (2018) στόχευσε στον γενικό πληθυσμό επειδή οι άνθρωποι εξακολουθούν να αντιμετωπίζουν κυβερνοεπιθέσεις, αν και αυτό το μέρος του θέματος του εγκλήματος στον κυβερνοχώρο δεν λαμβάνει επαρκή προσοχή.

2.3. ΗΛΕΚΤΡΟΝΙΚΟ ΈΓΚΛΗΜΑ ΚΑΙ ΠΡΟΣΩΠΙΚΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΣΚΕΥΕΣ

Τις τελευταίες δύο δεκαετίες, η χρήση τεχνολογιών υπολογιστών για κινητά έχει αυξηθεί σημαντικά (Ladd et al.,2010). Οι Προσωπικές Ηλεκτρονικές Συσκευές (Personal Electronic Devices - PED) πρόκειται να αναθεωρηθούν στο βαθμό που συνδέονται και χρησιμοποιούν το Διαδίκτυο. Για παράδειγμα, οι μαθητές που χρησιμοποιούν PED για σπουδές χρησιμοποιούν πιθανότατα συσκευές όπως smartphone ή φορητούς υπολογιστές για πρόσβαση στο διαδίκτυο για πληροφορίες. Το ιατρικό προσωπικό είναι πιθανό να χρησιμοποιήσει PED σε συνθήκες εργασίας για να επικοινωνήσει ή να αποκτήσει πρόσβαση σε πληροφορίες σχετικά με τους ασθενείς. Η χρήση των PED στον σύγχρονο κόσμο συνεπάγεται τη χρήση του διαδικτύου στις περισσότερες περιπτώσεις.

Τα smartphone διαθέτουν ιδιαίτερα τον μοναδικό συνδυασμό τεχνολογιών όπως ψηφιακές φωτογραφικές μηχανές, μουσική και περιεχόμενο πολυμέσων και είναι γνωστό ότι η παρουσία και η χρήση τους έχει μετατοπίσει τις ανθρώπινες αλληλεπιδράσεις στην κοινωνία (Koo et al.,2015), επιτρέποντας στη συνέχεια να

γίνουν πιο σύνθετα εγκλήματα στον κυβερνοχώρο. Για παράδειγμα, το 2013 στις ΗΠΑ, το 70% όλων των κινητών συσκευών ήταν smartphone (Hardawar, 2012). Ακόμη και στον τομέα της ακαδημαϊκής κοινότητας, οι Hossain & Ahmed (2016) μελέτησαν τη χρήση smartphone από φοιτητές στο Μπαγκλαντές και διαπίστωσαν ότι η συντριπτική πλειοψηφία των φοιτητών χρησιμοποιούσε smartphone για ακαδημαϊκούς σκοπούς. Επιπλέον, οι μελετητές διαπίστωσαν ότι η χρήση ακαδημαϊκών εφαρμογών smartphone από τους μαθητές για την υποστήριξη των μαθησιακών αναγκών τους αυξάνεται επίσης (Woodcock et al.,2012). Ο Bomhold (2013) διαπίστωσε ότι το 76% των προπτυχιακών φοιτητών των ΗΠΑ χρησιμοποιούν smartphone για να βρουν ακαδημαϊκές πληροφορίες. Μια παρόμοια μελέτη σε φοιτητές ιατρικής σε παρισινό πανεπιστήμιο έδειξε ότι μόνο το 3,3% των ερωτηθέντων δεν χρησιμοποίησαν κινητές συσκευές σε κλινικούς χώρους εργασίας για πρόσβαση σε ιατρικές ή άλλες πληροφορίες (Scott et al., 2017). Μια άλλη μελέτη δείχνει επίσης ότι σήμερα πάνω από το 95% των νέων ενηλίκων στις ΗΠΑ έχουν smartphone και, επιπλέον, το 30% εξ αυτών δηλώνουν ότι «δεν μπορούν να ζήσουν» χωρίς smartphone (Gibson, 2014).

Οι προαναφερθείσες μελέτες έχουν δείξει ότι η χρήση προσωπικών ηλεκτρονικών συσκευών (PED) με την πάροδο του χρόνου αυξάνεται. Παρ 'όλα αυτά, μπορεί να συζητηθεί ο τρόπος με τον οποίο τα PED ενσωματώνονται στην καθημερινή μας και αν τα smartphone είναι ωφέλιμα ή όχι. Οι Chen & Ji (2015) υποστήριξαν ότι πολλές έρευνες έχουν μελετήσει την ευρεία χρήση των smartphone και των προσωπικών ηλεκτρονικών συσκευών μεταξύ των μαθητών, ωστόσο, οι τρόποι με τους οποίους τα smartphone επηρεάζουν το στυλ σκέψης των μαθητών δεν έχουν ακόμη ληφθεί υπόψη. Οι ακαδημαϊκοί διαπίστωσαν ότι η χρήση των smartphone για ακαδημαϊκούς σκοπούς επηρέασε θετικά την απόδοσή τους, ωστόσο, οι μαθητές που χρησιμοποίησαν smartphones για μη ακαδημαϊκούς σκοπούς είχαν χειρότερες επιδόσεις. Οι Wang et al., (2014) έχουν συζητήσει πώς τα smartphones αλλάζουν πτυχές της καθημερινής ζωής σε ένα παράδειγμα ταξιδιωτών από τις ΗΠΑ. Χάρη στις εφαρμογές smartphone, όπου οι επιλογές ταξιδιού, όπως τρένα, αεροπλάνα και ξενοδοχεία βρίσκονται σε ένα μέρος, ο τουρισμός γίνεται πιο προσιτός και οι διαδικασίες λήψης αποφάσεων γίνονται ευκολότερες, αλλάζοντας το σχήμα του καταναλωτισμού. Ομοίως, οι Fuentes & Svingstedt (2017) διερεύνησαν πώς η εισαγωγή των smartphones είχε αλλάξει τις αγοραστικές συνήθειες του γενικού πληθυσμού. Τα smartphone επηρεάζουν θετικά την εμπειρία αγορών για τους καταναλωτές, παρέχοντάς τους νέες ευκαιρίες και

περισσότερες επιλογές, επιτρέποντας στη συνέχεια στους καταναλωτές να συγκρίνουν τιμές, κάτι που δημιουργεί μια νέα προοπτική για την οικονομία (Kourouthanasis & Giaglis, 2012). Ως μειονέκτημα, οι Kourouthanassis & Giaglis (2012) αναφέρουν ότι η εισαγωγή των smartphones στην εμπειρία αγορών μπορεί να προκαλέσει στους καταναλωτές άγχος ως συνέπεια μιας τόσο μεγάλης επιλογής προϊόντων καθώς και ν ανοίξει νέες ευκαιρίες για εγκλήματα στον κυβερνοχώρο.

Ένας άλλος σημαντικός τομέας στον οποίο στηρίζεται πολύ το διαδίκτυο και τα PED στη σύγχρονη εποχή είναι η ιατρική. Οι άνθρωποι έχουν αρχίσει να εμπιστεύονται τις πιο ιδιωτικές πληροφορίες τους, όπως τα αρχεία υγειονομικής περίθαλψης στο Διαδίκτυο, γεγονός που καθιστά το ζήτημα του εγκλήματος στον κυβερνοχώρο ακόμη πιο λεπτό. Οι Koivunen et al., (2015) μελέτησαν πώς οι ηλεκτρονικές συσκευές εφαρμόζονται στη διαδικασία επικοινωνίας των επαγγελματιών υγείας. Τα PED και το διαδίκτυο άνοιξαν νέες ευκαιρίες για επικοινωνία, κάτι που είναι ιδιαίτερα σημαντικό για το προσωπικό της υγειονομικής περίθαλψης. Οι ερευνητές διαπίστωσαν ότι οι νέες διαδικτυακές μέθοδοι επικοινωνίας, όπως το email και οι εφαρμογές σε smartphone, αποδείχθηκαν χρήσιμες, βελτιώνοντας τις ικανότητες του προσωπικού, καθώς και την οργάνωση των καθημερινών λειτουργιών και των διοικητικών εργασιών. Παρ 'όλα αυτά, θέτει επίσης ερωτήματα σχετικά με την ασφάλεια των πληροφοριών και παρέχει νέες ευκαιρίες για εγκλήματα στον κυβερνοχώρο. Προχωρώντας ακόμη περισσότερο στον τομέα της υγειονομικής περίθαλψης και της χρήσης των PEDs, οι Mobasheri et al., (2015) έχουν διερευνήσει πώς χρησιμοποιούνται τα smartphone και οι συσκευές tablet κατά τη διάρκεια χειρουργικών επεμβάσεων. Οι συγγραφείς δηλώνουν ότι υπάρχουν διάφοροι τρόποι εφαρμογής των PEDs στη χειρουργική, από τον προγραμματισμό και την πλοήγηση της λειτουργίας έως τη διαγνωστική και χειρουργική εκπαίδευση.

Τα smartphone και άλλα PED έχουν αποδειχθεί χρήσιμα για τη βελτίωση της ποιότητας ζωής για πολλούς ανθρώπους, ωστόσο, το θέμα έχει επίσης αντιμετωπίσει αντιρρήσεις. Οι Škařupová et al., (2015) μελέτησαν το φαινόμενο της υπερβολικής χρήσης διαδικτύου (excessive internet use - EIU) στην Ευρώπη. Με την εισαγωγή των smartphones, δραστηριότητες στο Διαδίκτυο, όπως τα τυχερά παιχνίδια στο διαδίκτυο και τα κοινωνικά δίκτυα έχουν μπει στη ζωή των νέων. Τώρα, οι νέοι δεν χρειάζεται να πάνε κάπου για διασκέδαση ή να κοινωνικοποιηθούν επειδή έχουν πρόσβαση σε διαδικτυακή ψυχαγωγία με τη μορφή διαδικτυακών παιχνιδιών και επικοινωνία με

άλλους ανθρώπους με μια μορφή κοινωνικών δικτύων. Με τέτοιες δραστηριότητες που έφεραν στη ζωή των εφήβων, περνούν όλο και περισσότερο χρόνο στο διαδίκτυο παρά εκτός σύνδεσης (Livingstone et al., 2011). Ο Spada (2014) αναφέρει ότι η προβληματική χρήση του διαδικτύου (Problematic Internet Use- PIU) έγινε παγκόσμιο και διαδεδομένο ζήτημα που μπορεί να οδηγήσει σε αρνητικές συνέπειες στην καθημερινή ζωή, όπως παραμέληση των κοινωνικών δραστηριοτήτων και σχέσεων της πραγματικής ζωής, αρνητικό αντίκτυπο στην υγεία και τα εργασιακά καθήκοντα και την αλλαγή του προγράμματος ύπνου καθώς και διατροφικών συνηθειών. Ο συγγραφέας αναφέρει επίσης ότι το PIU μπορεί ακόμη και να θεωρηθεί ψυχιατρική διαταραχή, ωστόσο απαιτείται περαιτέρω έρευνα. Το να ξοδεύει κανείς περισσότερο χρόνο στο διαδίκτυο προκαλεί εθισμό σε διαδικτυακές δραστηριότητες, οδηγώντας σε σοβαρά ζητήματα όπως, για παράδειγμα, τροχαία ατυχήματα που επηρεάζονται από την προσοχή. Σύμφωνα με την Εθνική Υπηρεσία Ασφάλειας της Κυκλοφοριακής Ασφάλειας (2016), η περισπασμένη οδήγηση σκότωσε 3.179 άτομα στις ΗΠΑ και τραυμάτισε περίπου 431.000 άλλους το 2014. Επιπλέον, τα μηνύματα κειμένου κατά την οδήγηση αυξάνουν την πιθανότητα εμπλοκής σε ένα κρίσιμο για την ασφάλεια γεγονός 23,2 φορές (Olson et al., 2009). Η απόσπαση της προσοχής μεταξύ των πεζών είναι επίσης ένας κρίσιμος κίνδυνος για την ασφάλεια, ωστόσο είναι δύσκολο να εκτιμηθεί ο αριθμός των ατυχημάτων ως συνέπεια ενός περισπασμένου πεζού. Μια άλλη μελέτη που σχετίζεται με τις συγκρούσεις που επηρεάζονται από την απόσπαση της προσοχής πραγματοποιήθηκε στις Κάτω Χώρες σε δείγμα ποδηλάτων (Goldenbeld et al., 2012). Οι ακαδημαϊκοί μελέτησαν διαφορετικές ηλικιακές ομάδες ποδηλατών από 12 έως 50+ ετών και διαπίστωσαν ότι οι νεαροί ενήλικες ποδηλάτες (18-34 ετών) ήταν συχνότεροι χρήστες PED. Επιπλέον, οι συγγραφείς διαπίστωσαν ότι οι έφηβοι ποδηλάτες και οι νέοι ενήλικες ποδηλάτες που χρησιμοποιούσαν ηλεκτρονικές συσκευές σε κάθε ταξίδι είχαν μεγαλύτερο κίνδυνο να εμπλακούν σε τροχαίο.

Συνοψίζοντας, η χρήση των PED και του διαδικτύου έχει αυξηθεί με την πάροδο του χρόνου και αυτοί οι παράγοντες έχουν επηρεάσει θετικά την ποιότητα ζωής του ανθρώπου, αλλά έχουν επίσης προκαλέσει αντιπαραθέσεις και διάφορα πιθανά θέματα υγείας και ασφάλειας. Το σημείο αναφοράς είναι ότι νέες ευκαιρίες για εγκλήματα στον κυβερνοχώρο έγιναν προσβάσιμες και οι άνθρωποι έγιναν πιο εκτεθειμένοι σε εγκλήματα στον κυβερνοχώρο. Ωστόσο, τα δεδομένα προέρχονται κυρίως από τις ευρωπαϊκές χώρες ή τις ΗΠΑ και το θέμα σπάνια διερευνάται στο Ηνωμένο Βασίλειο.

2.4. Έκθεση στο Ηλεκτρονικό Έγκλημα

Η χρήση του Διαδικτύου και των smartphone γίνεται όλο και πιο διαδεδομένη και οι άνθρωποι θέλουν να εμπιστεύονται τις ηλεκτρονικές συσκευές με όλο και περισσότερες προσωπικές πληροφορίες λόγω της απασχόλησης και των κοινωνικών δεσμεύσεων, στη συνέχεια ανησυχώντας όλο και περισσότερο για την ασφάλεια αυτών των πληροφοριών στον κυβερνοχώρο. Σύμφωνα με μια έρευνα που μελέτησε τους χρήστες του διαδικτύου εντός της Ευρωπαϊκής Ένωσης, το 76% των ερωτηθέντων πίστευαν ότι ο κίνδυνος θυματοποίησης εγκλημάτων στον κυβερνοχώρο έχει αυξηθεί (Baker, 2013). Παρά το γεγονός αυτό, μόνο το 46% των ερωτηθέντων είχε αλλάξει οποιονδήποτε κωδικό πρόσβασης κατά τη διάρκεια του περασμένου έτους και μόνο το 12% ήταν θύματα μιας διαδικασίας τραπεζικής απάτης στο διαδίκτυο ή είχαν παραβιάσει τους λογαριασμούς ηλεκτρονικού ταχυδρομείου ή κοινωνικών μέσων. Η GFI Software Corporation (2015) πραγματοποίησε μια ανεξάρτητη μελέτη που εξέτασε τις ανησυχίες των πολιτών του Ηνωμένου Βασιλείου και των ΗΠΑ για το έγκλημα στον κυβερνοχώρο. Τα αποτελέσματα της έρευνας έδειξαν ότι το 46% των ερωτηθέντων ήταν θύματα τουλάχιστον μία φορά το προηγούμενο έτος. Ένα άλλο ενδιαφέρον εύρημα είναι ότι το 71,5% των Αμερικανών πολιτών πιστεύει ότι οι εγκληματίες στον κυβερνοχώρο αποτελούν σοβαρή απειλή για την εθνική ασφάλεια και οι μισοί από τους ερωτηθέντες δήλωσαν ότι το έγκλημα στον κυβερνοχώρο κάνει τη ζωή τους πιο δύσκολη. Οι ερευνητές αναφέρουν επίσης ότι τα ευρήματα στις ΗΠΑ μπορούν να προβληθούν στη δημογραφία του Ηνωμένου Βασιλείου, με μια μικρή διαφορά. Οι Mesko & Bernik (2011) έχουν επίσης μελετήσει τον φόβο και την επίγνωση του εγκλήματος στον κυβερνοχώρο, αλλά στη Σλοβενία. Οι συγγραφείς δηλώνουν ότι η συντριπτική πλειοψηφία του «φόβου του εγκλήματος στον κυβερνοχώρο» προκαλείται από διαφορετικούς μύθους που περιβάλλουν το θέμα, καθώς και από ανακριβείς αναπαραστάσεις των μέσων ενημέρωσης (Wall D. S., 2008b). Κατά τη διάρκεια μιας μελέτης στη Σλοβενία, διαπιστώθηκε συσχέτιση μεταξύ του φόβου για το έγκλημα στον κυβερνοχώρο και της ευαισθητοποίησης για πιθανές συνέπειες του εγκλήματος και υποστηρίχθηκε ότι ο φόβος για το κυβερνοέγκλημα δεν εξαρτάται από την πραγματική κατάσταση ενός εγκλήματος (Mesko & Bernik, 2011). Οι συγγραφείς δηλώνουν επίσης ότι οι άνθρωποι στη Σλοβενία είναι καλά ενημερωμένοι για τους διαφορετικούς τύπους εγκλημάτων στον κυβερνοχώρο, ωστόσο

γνωρίζουν κυρίως αυτά που απεικονίζονται στα μέσα μαζικής ενημέρωσης και όχι εκείνα από τα οποία είναι πιο πιθανό να επηρεαστούν.

Ο Goucher (2010) ανέλυσε τα αποτελέσματα της έρευνας όπου το 65% από περίπου 77.000 ερωτηθέντες από διαφορετικές χώρες ήταν θύματα κυβερνοεγκλήματος. Το βασικό αποτέλεσμα είναι ότι το 26% των ερωτηθέντων ένιωσαν «αβοήθητοι» ως συνέπεια του εγκλήματος στον κυβερνοχώρο και επιπλέον, μόνο το 44% από αυτούς ανέφεραν το έγκλημα στην αστυνομία. Αυτό οδηγεί στο συμπέρασμα ότι είτε το έγκλημα στον κυβερνοχώρο αντιμετωπίζεται κακώς, είτε οι άνθρωποι απλά δεν γνωρίζουν την πραγματικότητα της πρόληψης, καθώς το 80% των ερωτηθέντων δήλωσαν ότι δεν περίμεναν τη σύλληψη των δραστών. Οι Hernandez-Castro & Boiten (2014) μελέτησαν την επικράτηση του εγκλήματος στον κυβερνοχώρο στο Ηνωμένο Βασίλειο, όπου περίπου το 80% των νοικοκυριών είχαν σύνδεση στο Διαδίκτυο το 2012 (UK: Office for National Statistics, 2013). Οι ερευνητές ανέλυσαν την έρευνα εγκλήματος της Αγγλίας και της Ουαλίας (Crime Survey of England and Wales - CSEW) 2011/2012 και διαπίστωσαν ότι το 37% των χρηστών του διαδικτύου ανέφεραν ότι ήταν θύματα με τη μορφή ιού υπολογιστή και μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα, μεταξύ άλλων.

Οι De Voe & Murphy (2011) έδωσαν ένα παράδειγμα της κλίμακας κυβερνο-εκφοβισμού-ενός νέου τύπου εγκλήματος που προκύπτει από τη διαδεδομένη χρήση του διαδικτύου και των smartphone. Οι ακαδημαϊκοί ανέλυσαν στατιστικά δεδομένα που συλλέχθηκαν από την Εθνική Έκθεση Θυματοποίησης του Εγκλήματος (National Crime Victimization Survey - NCVS) στις ΗΠΑ και τα στοιχεία έδειξαν ότι περίπου 1.521.000 μαθητές δέχθηκαν κυβερνοεκφοβισμό εντός ή εκτός σχολικής ιδιοκτησίας. Μια άλλη έρευνα, η οποία διερεύνησε το έγκλημα στον κυβερνοχώρο και την επικράτηση του διαδικτύου και των κινητών συσκευών, πραγματοποιήθηκε στην Ελλάδα (Papanikolaou, et al., 2013). Οι ακαδημαϊκοί συζήτησαν στατιστικά στοιχεία που παρέχονται από το Υπουργείο Προστασίας του Πολίτη της Ελληνικής Κυβέρνησης και διαπίστωσαν ότι οι περισσότερες δραστηριότητες εγκλημάτων στον κυβερνοχώρο διαπράχθηκαν μέσω του κοινωνικού δικτύου Facebook. Η πλειοψηφία (203 από το σύνολο των 327) εγκλημάτων στον κυβερνοχώρο που διαπράχθηκαν μέσω χρήσης του Facebook είναι περιπτώσεις πιθανής αυτοκτονίας. Οι συγγραφείς ολοκληρώνουν την εργασία λέγοντας ότι το έγκλημα στον κυβερνοχώρο πιθανότατα θα γίνει ένα από τα κυρίαρχα εγκλήματα ως αποτέλεσμα της τεχνολογικής επανάστασης.

Προχωρώντας, ο Leukfeldt (2014) παρείχε μια μελέτη περίπτωσης για ένα συγκεκριμένο έγκλημα στον κυβερνοχώρο που ονομάζεται «phishing» στο Άμστερνταμ. Το ηλεκτρονικό "ψάρεμα" ορίζεται ως η πράξη της κλοπής των ψηφιακών διαπιστευτηρίων κάποιου, για παράδειγμα των διαπιστευτηρίων τραπεζικών λογαριασμών στο διαδίκτυο. Ο ερευνητής παρείχε δεδομένα σχετικά με το κόστος ηλεκτρονικού ψαρέματος στις τράπεζες στις Κάτω Χώρες και το Ηνωμένο Βασίλειο για να δείξει ότι η απειλή είναι πραγματική και ότι το phishing εμφανίζεται ως μια συγκεκριμένη μορφή εγκλήματος στον κυβερνοχώρο. Στο Ηνωμένο Βασίλειο, οι τράπεζες έχασαν ένα ισοδύναμο 41,2 εκατ. Ευρώ το 2011, φθάνοντας περαιτέρω τα 46,2 εκατ. Ευρώ το 2012 (Financial Fraud Action UK, 2013). Στις Κάτω Χώρες το 2011 και το 2012 ο αριθμός ζημιών είχε φτάσει τα 35 εκατομμύρια ευρώ (Nederlandese Vereniging van Banken, 2012). Περαιτέρω στην εργασία, ο συγγραφέας παρέχει μια εκτεταμένη μελέτη περίπτωσης για διάφορες μορφές και τεχνικές ηλεκτρονικού ψαρέματος και παρέχει συμβουλές για το πώς μπορεί να αντιμετωπιστεί το ζήτημα. Οι Dimc & Dobovsek (2013) μελέτησαν τις αντιλήψεις για εγκλήματα στον κυβερνοχώρο ανθρώπων στη Σλοβενία και τις ΗΠΑ, εστιάζοντας στην επίγνωση και πραγματική συμπεριφορά. Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι υπάρχει διαφορά μεταξύ του επιπέδου ευαισθητοποίησης και του επιπέδου της πραγματικής επίπτωσης των μεθόδων ασφάλειας. Ένα άλλο ενδιαφέρον εύρημα από ακαδημαϊκούς κατά τη διάρκεια της έρευνας ήταν ότι οι αντιλήψεις για την ασφάλεια στον κυβερνοχώρο εξαρτώνται από τη φυσική τοποθεσία. Οι ερωτηθέντες από μια μικρή χώρα όπως η Σλοβενία αισθάνθηκαν ασφαλέστεροι από τους συμμετέχοντες από τις σημαντικά μεγαλύτερες ΗΠΑ

Μια άλλη μελέτη για τη θυματοποίηση των μαθητών στις ΗΠΑ διεξήχθη από τον Choi (2008) ο οποίος διερεύνησε πώς οι διαδικτυακές συμπεριφορές επηρέασαν την έκθεση σε εγκλήματα στον κυβερνοχώρο. Ανέλυσε έρευνες αυτοαναφοράς, οι οποίες περιελάμβαναν διαφορετικές ερωτήσεις που σχετίζονται με θέματα όπως μέτρα ασφάλειας υπολογιστών, διαδικτυακός τρόπος ζωής και τρόπος ζωής στον κυβερνοχώρο. Ο συγγραφέας ήταν σε θέση να παράσχει εμπειρικά στοιχεία ότι τόσο η συμπεριφορά στον κυβερνοχώρο όσο και η ψηφιακή κηδεμονία είναι σημαντικές πτυχές κατά την αναθεώρηση της θυματοποίησης του εγκλήματος στον κυβερνοχώρο, η οποία κατά συνέπεια επέτρεψε την εφαρμογή του RAT σε εγκλήματα. Από την άλλη πλευρά, ο Jardine (2015) υποστηρίζει ότι το έγκλημα στον κυβερνοχώρο δεν είναι τόσο

συνηθισμένο όσο αντιπροσωπεύεται σε διαφορετικές στατιστικές εκθέσεις και ο συγγραφέας αναφέρει ότι η διαδικτυακή θυματοποίηση είναι σχετικά ασυνήθιστη. Δηλώνει επίσης ότι τα δεδομένα σχετικά με την εμφάνιση εγκλήματος στον κυβερνοχώρο δεν αντιπροσωπεύονται με ακρίβεια με τη μορφή αριθμού επιθέσεων ετησίως και προτείνει ότι η έκταση των δεδομένων για το κυβερνοέγκλημα απαιτεί στροφή της εστίασης προς τους χρήστες, οι οποίοι στη συνέχεια θα πρέπει να αναπαρασταθούν ως περιστατικά ανά χίλια άτομα ετησίως. Αναλύοντας τις εκθέσεις ασφάλειας των εταιρειών πληροφορικής από αυτήν την οπτική γωνία, υποστήριξε ότι η πραγματική κατάσταση του κυβερνοχώρου είναι πολύ πιο ασφαλής από ό, τι εμφανίζεται σε άλλες πηγές και κοινώς πιστεύεται.

Οι Nasi et al., (2015) πραγματοποίησαν μια πολυεθνική μελέτη (Φινλανδία, ΗΠΑ, Γερμανία και Ηνωμένο Βασίλειο) χρησιμοποιώντας ένα μέγεθος δείγματος 3506 ατόμων ηλικίας 15 έως 30 ετών και βασίστηκαν στη δήλωσή τους ότι το έγκλημα στον κυβερνοχώρο είναι ασυνήθιστο. Καθόρισαν επίσης τους σημαντικότερους προγνωστικούς παράγοντες της διαδικτυακής θυματοποίησης ως εξής: άνδρες, νεαρή ηλικία, μετανάστες, μη ενεργή κοινωνική ζωή εκτός σύνδεσης, αστική κατοικία και μη διαβίωση με γονείς. Οι συγγραφείς υπονοούν περαιτέρω ότι ο RAT μπορεί να εφαρμοστεί στον κυβερνοχώρο για να εξηγήσει τη θυματοποίηση. Μια άλλη άποψη σχετικά με τα ποσοστά εγκλημάτων στον κυβερνοχώρο που παρουσιάζονται εσφαλμένα και ότι η πραγματική κατάστασή του είναι καλύτερη από ό, τι γενικά γίνεται αντιληπτή παρέχεται από τους Bidgoli & Grossklags (2016), οι οποίοι πιστεύουν ότι αυτές οι δηλώσεις είναι συνέπεια της υποαναφοράς του εγκλήματος. Οι ακαδημαϊκοί δηλώνουν ότι παράγοντες όπως μικρές οικονομικές ζημιές, ψυχολογικά ή συναισθηματικά τραύματα ως συνέπεια του εγκλήματος που έχουν διαπράξει είναι ιδιαίτερα ευαίσθητου χαρακτήρα, καθιστούν ορισμένους τύπους εγκλημάτων στον κυβερνοχώρο να μην αναφέρονται. Ένας άλλος σημαντικός παράγοντας μπορεί να είναι ότι τα θύματα δεν γνωρίζουν πού και πώς να αναφέρουν σωστά και αποτελεσματικά κυβερνοεγκλήματα.

Ένας διαφορετικός τρόπος μέτρησης του εγκλήματος στον κυβερνοχώρο είναι η οικονομική προοπτική σχετικά με τις ζημίες στον κυβερνοχώρο. Τα στοιχεία και οι αριθμοί διαφορετικών κυβερνητικών, διεθνών ή τραπεζικών πηγών μπορούν να παρέχουν μια άλλη προοπτική σχετικά με την έκθεση στον κυβερνοέγκλημα. Οι Armin et al. (2015) εξέτασαν την έκθεση στο έγκλημα στον κυβερνοχώρο από οικονομική

άποψη μεταξύ 2010 και 2015 για να προβλέψουν το συνολικό κόστος του εγκλήματος στον κυβερνοχώρο στην οικονομία το 2020. Ο κύριος στόχος της μελέτης ήταν να αναδείξει τα ζητήματα που προκαλούν ζημιά στην οικονομία και να παράσχει συμβουλές σχετικά πώς να αρνηθεί αυτή τη ζημιά τα επόμενα 5 χρόνια. Οι ακαδημαϊκοί εξέτασαν στατιστικά στοιχεία σχετικά με το έγκλημα στον κυβερνοχώρο από διάφορες πηγές και εκτίμησαν ότι η ζημιά στην παγκόσμια οικονομία από το έγκλημα στον κυβερνοχώρο ανέρχεται σε 300 δισεκατομμύρια ευρώ ετησίως (McAfee & CSIS, 2014a). Αυτό μπορεί να φαίνεται αρκετά μεγάλο, αλλά σε αναλογία ανέρχεται μόνο στο 0,4% της αξίας του ακαθάριστου εγχώριου προϊόντος (ΑΕΠ) της ΕΕ, που ισοδυναμεί με 13 δισεκατομμύρια ευρώ (McAfee και CSIS, 2014β). Η εταιρεία λογισμικού προστασίας από ιούς Norton πραγματοποίησε τη δική της έρευνα με μέγεθος δείγματος 24 διαφορετικών χωρών που μετρούσε τη ζημιά του εγκλήματος στον κυβερνοχώρο ως 110 δισεκατομμύρια δολάρια ετησίως. Οι ερευνητές υποστηρίζουν, ωστόσο, ότι τα περισσότερα εγκλήματα στον κυβερνοχώρο παραμένουν αναφερόμενα και, επιπλέον, πολλά θύματα κυβερνοεγκλήματος δεν γνωρίζουν καν ότι έχουν θυματοποιηθεί (Norton Antivirus Software, 2012). Ένα τραπεζικό κακόβουλο λογισμικό που ονομάζεται «Dridex botnet» είναι ένα πρακτικό παράδειγμα της ζημιάς που μπορεί να προκληθεί στην οικονομία. Η Εθνική Υπηρεσία Εγκλήματος (National Crime Agency - NCA) στο Ηνωμένο Βασίλειο δήλωσε ότι αυτός ο τύπος botnet έκλεψε περίπου 20 εκατομμύρια λίρες από τραπεζικούς λογαριασμούς στο διαδίκτυο για αρκετούς μήνες (National Crime Agency, 2015).

Όπως φαίνεται, τα «botnets» είναι μια δαπανηρή και αποτελεσματική μέθοδος διάπραξης εγκλήματος στον κυβερνοχώρο που ορίζεται ως ένα δίκτυο μολυσμένων υπολογιστών που ελέγχεται από έναν διοικητή botnet για την εκτέλεση ποικίλων κυβερνοεγκλημάτων (de Graaf et al.,2012) όπως η διανεμημένη άρνηση -επιθέσεις υπηρεσιών (distributed denial-of-service attacks - DDoS), εξόρυξη bitcoin, ανεπιθύμητη αλληλογραφία, κλοπή πληροφοριών ή απάτη με κλικ (Wagenaar, 2012). Ο Wagen (2015) αναφέρει επίσης ότι η τεχνική botnet του εγκλήματος στον κυβερνοχώρο μπορεί να εννοηθεί από εγκληματολογική άποψη, εφαρμόζοντας τον RAT . Ένας άλλος τρόπος εκτίμησης του ζητήματος είναι από την οπτική της Θεωρίας της Ορθολογικής Επιλογής (Rational Choice Theory - RCT) που δίνει έμφαση στη διαδικασία λήψης αποφάσεων του δράστη (Clarke & Cornish, 1986), όπου ένας ορθολογικός δράστης δημιουργεί το botnet εργαλείο για τον εαυτό του ή τους άλλους.

Από την άλλη πλευρά, οι Ngo & Paternoster (2011) εφάρμοσαν επίσης το RAT σε ένα θέμα θυματοποίησης του εγκλήματος στον κυβερνοχώρο μελετώντας φοιτητές των ΗΠΑ και κατέληξαν στο συμπέρασμα ότι ούτε οι ατομικοί ούτε οι καταστατικοί παράγοντες επηρέασαν σταθερά την πιθανότητα θυματοποίησης του εγκλήματος στον κυβερνοχώρο. Οι συγγραφείς δηλώνουν ότι ένα θεωρητικό πλαίσιο διαφορετικό από το RAT πρέπει να εφαρμοστεί στην εξήγηση της θυματοποίησης. Επιπλέον, ο Dupont (2017) επικεντρώθηκε σε ζητήματα και περιορισμούς επιβολής στον έλεγχο και τη ρύθμιση μεγάλων διεθνών εγκλημάτων στον κυβερνοχώρο, χρησιμοποιώντας το παράδειγμα των botnets. Ο Dupont, ωστόσο, συζητά μόνο τρεις κύριες προσεγγίσεις που χρησιμοποιήθηκαν για την καταπολέμηση των botnets: πρώτον, η σύλληψη χάκερ για να προκαλέσει αποτρεπτικό αποτέλεσμα. Δεύτερον, ανάπτυξη λογισμικού που αποτρέπει την επίθεση, και τρίτον, κυβερνητικές ενέργειες με τη μορφή μείωσης βλαβών και ευαισθητοποίησης. Αναλύοντας αυτές τις προσεγγίσεις, οι μελετητές κατέληξαν στο συμπέρασμα ότι δεν υπάρχουν αρκετά διαθέσιμα δεδομένα για την αξιολόγηση της αποτελεσματικότητας τέτοιων προσεγγίσεων, καθώς η συντριπτική πλειοψηφία αυτών των δεδομένων βρίσκονται σε ιδιωτικούς οργανισμούς όπως οι πάροχοι υπηρεσιών Διαδικτύου, οι εταιρείες λογισμικού και οι εταιρείες μηχανών αναζήτησης. Λέγοντας αυτό, το «botnet» είναι μόνο ένα από τα πολλά ζητήματα που εξετάζονται κατά τη μέτρηση ζημιών από οικονομικό έγκλημα στον κυβερνοχώρο.

Παρά το ζήτημα της έλλειψης δεδομένων, το Υπουργείο Άμυνας (ΥΠ) στο Ηνωμένο Βασίλειο πιστεύει ότι προηγούμενες μελέτες που στοχεύουν στο κόστος του εγκλήματος στον κυβερνοχώρο υπερεκτίμησαν το ζήτημα και δεν διαφοροποίησαν το άμεσο από το έμμεσο κόστος του αδικήματος (Anderson, et al., 2013). Ως παράδειγμα, οι συγγραφείς εξέτασαν μια επίθεση botnet μεγάλης κλίμακας από το 2010, όπου οι ιδιοκτήτες του κακόβουλου λογισμικού κέρδισαν μόλις περίπου 2,7 εκατομμύρια δολάρια, ενώ οι παγκόσμιες δαπάνες πρόληψης ήταν πάνω από 1 δισεκατομμύριο δολάρια. Επομένως, ενώ ο αντίκτυπος του εγκλήματος στον κυβερνοχώρο μπορεί να μετρηθεί από την άποψη της οικονομικής ζημίας σε μια χώρα ή ολόκληρο τον κόσμο, θα πρέπει να γίνει σωστά με σαφή διάκριση μεταξύ των κερδών των εγκληματιών και του κόστους πρόληψης αυτών των εγκλημάτων στον κυβερνοχώρο. Συνοψίζοντας, οι άνθρωποι σε όλο τον κόσμο ανησυχούν για τα θύματα του εγκλήματος στον κυβερνοχώρο και, με τη διερεύνηση μιας ευρείας ποικιλίας εγκλημάτων στον κυβερνοχώρο, γίνεται προφανές ότι η πιθανότητα θύματος στον κυβερνοχώρο είναι

αρκετά υψηλή. Συζητώντας στατιστικά στοιχεία σχετικά με την έκθεση στο έγκλημα στον κυβερνοχώρο, είναι σημαντικό να έχει κατά νου ότι η έκθεση μπορεί να μετρηθεί με διαφορετικούς τρόπους, όπως οικονομικό αντίκτυπο, περιστατικά που αναφέρθηκαν από την αστυνομία, περιστατικά θυματοποίησης αυτοαναφερόμενων και απαρατήρητα περιστατικά. Στο πλαίσιο αυτής της μελέτης που συντάχθηκε απο τους Habirovs & Arturs (2018), η έκθεση στο έγκλημα στον κυβερνοχώρο πρόκειται να μετρηθεί σε μια μορφή αυτοαναφερόμενης θυματοποίησης..

ΚΕΦΑΛΑΙΟ 3ο ΕΠΙΠΤΩΣΕΙΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΚΑΤΑΠΟΛΕΜΗΣΗ

3.1. ΕΠΙΠΤΩΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στη σύγκριση του εγκλήματος στον κυβερνοχώρο με το συμβατικό έγκλημα, δεν υπάρχει μεγάλη διαφορά επειδή και τα δύο προκαλούν παραβίαση των νομικών κανόνων. Έχει υποστηριχθεί ότι οι εγκληματίες κυβερνοχώρου έχουν χρησιμοποιηθεί διάφορα κανάλια για τη διανομή παράνομων μηνυμάτων ηλεκτρονικού ταχυδρομείου, ιστότοπων, καθώς και απλά εγκλήματα, όπως η λήψη παράνομων μουσικών αρχείων. Ο Wall (2007) υποστηρίζει ότι οι διεθνείς εγκληματίες κλέβουν πνευματική ιδιοκτησία για τη δική τους ή κατόπιν αιτήματος των κυβερνήσεων τους. Οι απώλειες υπολογίζονται σε 10 δισεκατομμύρια δολάρια ετησίως. Η Γερμανία, για παράδειγμα, εκτίμησε τις δικές της απώλειες IP από τη βιομηχανική κατασκοπεία σε 25-50 δισεκατομμύρια δολάρια, μεγάλο μέρος των οποίων οφείλεται στην αδύναμη ασφάλεια στο Διαδίκτυο. Αξιοσημείωτο είναι ότι οι περισσότερες επιχειρήσεις δεν αναφέρουν ζημίες από εγκλήματα στον κυβερνοχώρο, υποδεικνύοντας ότι ο αριθμός μπορεί να είναι υψηλότερος. Άλλες εταιρείες που έχουν χακαριστεί επιλέγουν να αποκρύψουν τις πληροφορίες για να αποτρέψουν τους πελάτες και τους επενδυτές που φοβίζουν. Το χρηματοπιστωτικό σύστημα γίνεται όλο και περισσότερο στόχος των εγκληματιών στον κυβερνοχώρο. Τείνουν να πηγαίνουν μετά από αυτόματες πωλητές, πιστωτικές κάρτες και ηλεκτρονικούς τραπεζικούς λογαριασμούς. Σε ένα μόνο παράδειγμα, μια ρωσική συμμορία πήρε 9,8 εκατομμύρια δολάρια από ATM κατά τη διάρκεια του Σαββατοκύριακου της Εργατικής Πρωτομαγιάς. Η απειλή για το έγκλημα στον κυβερνοχώρο έχει γίνει ευρέως αγγίζοντας όλες τις γωνιές του πλανήτη και επηρεάζοντας τις αναπτυξιακές προσπάθειες κοινωνικά και οικονομικά. Καθώς οι ευκαιρίες ξεδιπλώνονται, έφεραν μαζί τους νέες ευκαιρίες για διάπραξη εγκλημάτων .Υποστηρίζεται ότι το έγκλημα στον κυβερνοχώρο δεν έχει δημιουργήσει νέα εγκλήματα, αλλά έχει παράσχει μια πρόσθετη μέθοδο μέσω της οποίας ευδοκιμούν αδικήματα όπως κλοπή, εκβιασμός, παράνομες διαδηλώσεις και τρομοκρατία. Σύμφωνα με τον Moore (2016) η τρομοκρατία στον κυβερνοχώρο λαμβάνει πολλές μορφές όπως φυσική καταστροφή μηχανημάτων, απομακρυσμένη παρέμβαση δικτύων υπολογιστών, διακοπή κυβερνητικών δικτύων και μέσα μαζικής ενημέρωσης. Ένα καλό παράδειγμα τέτοιας καταστροφής είναι το 2015 όταν ένας φερόμενος ως Ρώσος κυβερνοεπιθέτης κατέλαβε τον έλεγχο του "Κέντρου Ελέγχου Prykarpatnergo

(Prykarpatnergo Control Center -PCC)" στη Δυτική Ουκρανία. Αυτό το περιστατικό άφησε περίπου 230000 άτομα χωρίς ρεύμα για έως και 6 ώρες.

Πίνακας 1.1 δείχνει την κατανομή των χρηστών του διαδικτύου σε όλο τον κόσμο

World Regions	Population (2020 Est)	Population % of the world	Internet Users 31st May 2020	Growth 2000-2020
Africa	1,340,598,447	17.2%	526,710,313	11,567%
Asia	4,294,516,659	55.1%	2,366,213,308	1,970%
Latin America	834,995,1997	10.7%	727,848,547	592%
Middle East	260,991,960	3.3%	453,702,292	2,411%
North America	368,869,647	4.7%	183,212,099	5,477%
Australia	42,690,838	0.5%	38,917,600	279%

3.2. ΚΟΙΝΩΝΙΚΕΣ ΠΤΥΧΕΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η εκτεταμένη χρήση των Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) στην καθημερινή μας ζωή έχει δημιουργήσει έναν ισχυρό δεσμό μεταξύ των δύο. Ως εκ τούτου, κάθε είδους έγκλημα στον κυβερνοχώρο θα μπορούσε δυνητικά να σχετίζεται με την κοινωνική μας ζωή, είτε άμεσα είτε έμμεσα, γεννώντας έτσι νέες μεθόδους διάπραξης εγκλημάτων στον κυβερνοχώρο με τη χρήση ΤΠΕ.

Η έλλειψη της κατάλληλης ενημέρωσης και κατάρτισης των χρηστών είναι ίσως ένας από τους πιο σημαντικούς λόγους που επιτρέπουν τέτοια περιστατικά ηλεκτρονικού εγκλήματος να λάβουν χώρα ή να γίνουν το «καύσιμο» που τους κρατά σε λειτουργία (π.χ. για μηνύματα απάτης και αλυσιδωτές επιστολές). Οι χρήστες που δεν γνωρίζουν τους πιθανούς κινδύνους του κυβερνοχώρου τείνουν να γίνονται τα συχνότερα θύματα. Επιπλέον, δεδομένου ότι κατά πάσα πιθανότητα δεν θα διαφυλάξουν την ιδιωτικότητά τους με τον κατάλληλο τρόπο, σε συνδυασμό με την έλλειψη γνώσεων και εμπειρίας τους όσον αφορά ζητήματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, οι επιπτώσεις μιας τέτοιας επίθεσης εναντίον τους ενδέχεται να ενισχυθούν σημαντικά. Η κατάσταση μπορεί να επιδεινωθεί ακόμη περισσότερο σε περιπτώσεις όπου το άτομο είναι αναλφάβητο στον υπολογιστή. Αρκετά τέτοια περιστατικά έχουν καταγραφεί, τα

οποία προκάλεσαν υπερβολικές αντιδράσεις από την πλευρά του θύματος, οι οποίες σε ορισμένες περιπτώσεις οδήγησαν σε ακραίες καταστάσεις, όπως η αυτοκτονία.

Επιπλέον, η εκτεταμένη χρήση προσωπικών ηλεκτρονικών συσκευών μπορεί να βοηθήσει τους εγκληματίες του κυβερνοχώρου στην εκτέλεση των παράνομων πράξεών τους. Από τη στιγμή που τέτοιες συσκευές συνήθως έχουν τη δυνατότητα σύνδεσης στο Διαδίκτυο, η επιφάνεια της επίθεσης αυξάνεται δραματικά, κάτι που παρέχει και τη δυνατότητα απομακρυσμένων επιθέσεων. Για παράδειγμα, η κλοπή ενός κινητού τηλεφώνου ή ενός tablet μπορεί να προσφέρει στον δράστη μια μεγάλη συλλογή προσωπικών και ιδιωτικών φωτογραφιών, μια μεγάλη λίστα διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεφώνου, ή ακόμα και ένα σύνολο διαπιστευτηρίων (ονόματα χρήστη και κωδικούς πρόσβασης) για σύνδεση σε διάφορες διαδικτυακές υπηρεσίες. Κατά συνέπεια, ο δράστης μπορεί να εκμεταλλευτεί τις προαναφερθείσες πληροφορίες για την πραγματοποίηση κλοπής ταυτότητας, απειλώντας και εκβιάζοντας το θύμα με πολλούς τρόπους.

Ίσως ένα από τα πιο δημοφιλή μέσα αλληλεπίδρασης των χρηστών στον κυβερνοχώρο είναι η χρήση ηλεκτρονικών πλατφορμών κοινωνικής δικτύωσης (π.χ. Facebook, Flickr, Twitter, Google+, hi5, Bebo, Foursquare), κυρίως στον ελεύθερο χρόνο τους. Για να χρησιμοποιήσουν αυτές τις πλατφόρμες, οι χρήστες πρέπει να δημιουργήσουν ένα προφίλ με ορισμένες προσωπικές πληροφορίες και μπορούν στη συνέχεια να ανεβάσουν πληροφορίες πλούσιες σε περιεχόμενο που αποτελούνται από κείμενο, εικόνες και βίντεο, καθώς και να αλληλεπιδρούν μεταξύ τους με διάφορους τρόπους, όπως να συζητήσουν ιδιωτικά ή σε ομάδες μέσω υπηρεσιών συνομιλίας, να βάλουν ετικέτες στους φίλους τους σε φωτογραφίες, να εκφράσουν την προτίμησή τους μέσω π.χ. λειτουργίες "like" και "+1", κοινή χρήση της τρέχουσας θέσης ή δραστηριότητας και ούτω καθεξής. Στις περισσότερες περιπτώσεις, ωστόσο, οι χρήστες ανεβάζουν υπερβολικές ποσότητες προσωπικών πληροφοριών και λόγω της απουσίας κατάλληλων πολιτικών ελέγχου πρόσβασης ή/και διαμόρφωσης, δημιουργούν σοβαρά ζητήματα ασφάλειας που θα μπορούσαν να οδηγήσουν σε παραβιάσεις του προσωπικού απορρήτου (δικές τους ή/και των επαφών τους).

Τέλος, το έγκλημα στον κυβερνοχώρο σχετίζεται επίσης με τις τρέχουσες κοινωνικοπολιτικές συνθήκες. Για παράδειγμα, τα τελευταία χρόνια, η Ελλάδα υποφέρει από οικονομική κρίση, η οποία συνδέεται σε κάποιο βαθμό με την αύξηση των περιστατικών οικονομικού εγκλήματος στον κυβερνοχώρο. Τέτοια παραδείγματα

είναι οι ψεύτικες εταιρείες εύρεσης εργασίας που ζητούν προκαταβολικά αμοιβή και υπόσχονται να προσφέρουν θέσεις εργασίας, αν και ποτέ δεν το κάνουν, ταξιδιωτικοί πράκτορες που προσφέρουν εξαιρετικά φθηνά πακέτα διακοπών που δεν φτάνουν ποτέ στους πελάτες που τα έχουν πληρώσει, παράνομες υπηρεσίες τυχερών παιχνιδιών σε απευθείας σύνδεση που διαφημίζουν ιδιαίτερα δελεαστικές πληρωμές.

3.3. ΜΕΘΟΔΟΙ ΠΡΟΛΗΨΗΣ

Όπως έχει διαπιστωθεί προηγουμένως, οι άνθρωποι στη σύγχρονη κοινωνία εκμεταλλεύονται την τεχνολογική πρόοδο και τις προσωπικές ηλεκτρονικές συσκευές, με το Διαδίκτυο να γίνεται συγκεκριμένα ένα σημαντικό χαρακτηριστικό της καθημερινής ζωής της πλειοψηφίας των ανθρώπων. Ο Eddolls (2016) αναφέρει ότι η απειλή για το έγκλημα στον κυβερνοχώρο αυξάνεται συνεχώς ως συνέπεια της προσαρμογής των εγκληματιών στον κυβερνοχώρο στα σύγχρονα μέτρα ασφαλείας και της διαδικτυακής συμπεριφοράς των χρηστών. Ο συγγραφέας υποστηρίζει ότι, ανεξάρτητα από τα μέτρα ασφαλείας που εφαρμόζονται, οι εγκληματίες είναι πάντα ένα βήμα μπροστά. Ο λόγος πίσω από αυτό είναι ότι το έγκλημα στον κυβερνοχώρο δεν αντιμετωπίζεται όπως θα έπρεπε. Ο Eddolls πιστεύει ότι το έγκλημα στον κυβερνοχώρο πρέπει να αντιμετωπίζεται ως αδίκημα ύψιστης προτεραιότητας λόγω της ζημιάς που μπορεί να προκαλέσει. Για να ξεπεράσει κανείς τους εγκληματίες στον κυβερνοχώρο, πρέπει να κάνει την πρόληψη του εγκλήματος στον κυβερνοχώρο ύψιστη προτεραιότητα, να κρίνει ρεαλιστικά την πραγματική κατάσταση του εγκλήματος στον κυβερνοχώρο και να χρησιμοποιήσει κατάλληλες μεθόδους πρόληψης του εγκλήματος στον κυβερνοχώρο. Οι Akhgar & Brewster (2016) παρείχαν μια συλλογή συζητήσεων για διαφορετικά θέματα γύρω από το έγκλημα στον κυβερνοχώρο. Το βιβλίο είναι χτισμένο ως χάρτης πορείας για την πρόληψη του εγκλήματος στον κυβερνοχώρο, ξεκινώντας από διαφορετικές τάσεις και προκλήσεις του εγκλήματος στον κυβερνοχώρο και της κυβερνοτρομοκρατίας, πώς μπορεί να αντιμετωπιστεί από νομική, ηθική και ιδιωτική άποψη, πώς μπορεί να αντιμετωπιστεί από τεχνολογική άποψη και τέλος μια συζήτηση για τις εξελίξεις στην έρευνα. Ο Koops (2016) ορίζει επτά «μεγάλες τάσεις» της σημερινής κοινωνίας και τεχνολογιών που μπορούν να συνοψιστούν ως το διαδίκτυο που γίνεται η υποδομή των πάντων, το μεταβαλλόμενο πρότυπο του εγκλήματος στον κυβερνοχώρο και η διάλυση της ιδιωτικής ζωής. Με βάση αυτές τις τάσεις, ο συγγραφέας προτείνει επτά προκλήσεις

για την ασφάλεια της κοινωνίας, όπως υπόγειες αγορές, διατήρηση των ανθρωπίνων δικαιωμάτων και ρύθμιση και οργάνωση του κυβερνοχώρου. Οι Roosendaal et al., (2016) συζήτησαν την εφαρμογή των νόμων και του νομικού πλαισίου για την προστασία δεδομένων στον κυβερνοχώρο, λαμβάνοντας υπόψη τον τρόπο με τον οποίο θα αλληλεπιδρούσε με άλλες αρχές, όπως η ελευθερία του λόγου και η ακαδημαϊκή ελευθερία.

Πριν αναλυθούν οι τεχνικές πρόληψης του εγκλήματος, θα ήταν επωφελές να αντιμετωπιστεί ο φόβος του εγκλήματος (fear of crime - FOC) ως εγκληματολογική έννοια. Το συναίσθημα «φόβος» μπορεί να θεωρηθεί ως ένα μείγμα διαφορετικών συναισθημάτων, εκτιμήσεων κινδύνου και αντιλήψεων, πράγμα που σημαίνει ότι ο φόβος είναι ένα πολύ υποκειμενικό συναίσθημα (Ditton et al, 1999). Επιπλέον, ο Wynne (2008) υποστηρίζει ότι ο φόβος είναι μια φυσική απάντηση στο έγκλημα. Οι Gooch & Williams (2015) δηλώνουν ότι παρόλο που το FOC μπορεί να είναι γνήσιο, είναι συχνά παράλογο επειδή δεν βασίζεται σε πραγματική ανάλυση μιας κατάστασης. Για παράδειγμα, οι Gooch & Williams συζήτησαν καταστάσεις με ηλικιωμένους που φοβόντουσαν να βγουν έξω επειδή φοβόντουσαν ότι θα τους ληστέψουν. Ωστόσο, στατιστικά, οι ηλικιωμένοι είναι λιγότερο πιθανό να πέσουν θύματα με τέτοιο τρόπο. Αυτό το είδος παραδείγματος θα μπορούσε να εφαρμοστεί θεωρητικά στο κυβερνοχώρο. Οι ακαδημαϊκοί Roberts et al., (2013) ανέλυσαν την Αυστραλιανή Έρευνα Κοινωνικών Στάσεων του 2007 με θέμα πώς ο φόβος του κυβερνοεγκλήματος διαφέρει από τον φόβο του παραδοσιακού εγκλήματος και είχαν καταλήξει ότι η ανησυχία για εγκλήματα στον κυβερνοχώρο που σχετίζονται με την ταυτότητα (όπως κλεμμένες πιστωτικές κάρτες ή άλλες μορφές κλοπής ταυτότητας) ταιριάζει ή υπερβαίνει την ανησυχία των παραδοσιακών εγκλημάτων που βασίζονται στον τόπο.

Ένα άλλο σημαντικό στοιχείο στη συζήτηση σχετικά με τους νόμους περί προστασίας δεδομένων είναι η διαφορά μεταξύ των χωρών. Οι Choras et al., (2016) συζητούν τρόπους με τους οποίους η κυβερνοασφάλεια αναδύεται από τεχνολογικές προοπτικές και τρόπους για να προωθήσουν ακόμη περισσότερο την πρόοδο της τεχνολογικής πρόληψης του εγκλήματος στον κυβερνοχώρο. Οι συγγραφείς συζητούν παραδείγματα των πιο σύγχρονων μέτρων βιολογικής ασφάλειας, πώς αυτά τα μέτρα δείχνουν θετικό αντίκτυπο στα ποσοστά έκθεσης στον κυβερνοέγκλημα και πώς μπορούν να εφαρμοστούν ακόμη περισσότερο για να είναι ακόμη πιο επιτυχημένα. Και τέλος, οι Choras et al., (2016) παρουσίασαν μια συζήτηση για περαιτέρω πιθανές εξελίξεις στον

φορέα των ερευνών για την πρόληψη του εγκλήματος στον κυβερνοχώρο. Οι μελετητές αναθεωρούν διάφορα έργα που στοχεύουν στην πρόληψη του κυβερνοεγκλήματος, χρησιμοποιώντας διαφορετικούς τεχνολογικούς χειρισμούς σύγχρονων ηλεκτρονικών συσκευών και διαδικτυακού περιβάλλοντος,μέσω πρακτικών παραδειγμάτων που παρέχουν επιχειρήματα για περαιτέρω εξελίξεις. Ο Bernik (2014) παρείχε ένα βιβλίο όπου συζήτησε μεθόδους εκμετάλλευσης του κυβερνοχώρου. Υποστήριξε επίσης ότι το κυβερνοέγκλημα θα μπορούσε να προληφθεί μέσω παρέμβασης στις τεχνολογίες ή με την προσαρμογή των νόμων σχετικά με αυτό.

Όσον αφορά την πρόληψη της θυματοποίησης του εγκλήματος στον κυβερνοχώρο σε τεχνολογικό επίπεδο, οι Reyns et al., (2016) διερεύνησαν αυτό το θέμα και διεξήγαγαν έρευνα που στόχευε στον εντοπισμό παραγόντων που μπορεί να επηρεάσουν την προληπτική συμπεριφορά στον κυβερνοχώρο και το πέτυχαν εξετάζοντας τις σχέσεις μεταξύ της έκθεσης στον κυβερνοχώρο, της θυματοποίησης του κυβερνοεγκλήματος και της διαδικτυακής επικοινωνίας μέσα σε ένα πλαίσιο ευκαιριών. Οι ακαδημαϊκοί κατέληξαν στο συμπέρασμα ότι η έκθεση στον κυβερνοχώρο και οι συνήθεις δραστηριότητες στην διαδικτυακή επικοινωνία ήταν προγνωστικά για τα θύματα του εγκλήματος στον κυβερνοχώρο .Επιπλέον, συνήχθη το συμπέρασμα ότι η λήψη προληπτικών μέτρων στο Διαδίκτυο αναιρεί την πιθανότητα θεμελιώδους διατριβής θύματος ηλεκτρονικού εγκλήματος, η οποία είναι ότι η αλληλεπίδραση στις τεχνολογίες μπορεί να είναι αποτελεσματική στις στρατηγικές πρόληψης του κυβερνοεγκλήματος. Ο Mahoney (2016) παρείχε πρακτικές συμβουλές για το πώς να συνεργαστεί κανείς με σύγχρονες τεχνολογίες για να αποφύγει τη θυματοποίηση. Για παράδειγμα, τα σύγχρονα μέτρα ασφαλείας όπως ο έλεγχος ταυτότητας δύο παραγόντων, που προσθέτει ένα ακόμη επίπεδο ασφάλειας πάνω από το βασικό όνομα χρήστη και κωδικό πρόσβασης με τη μορφή επιβεβαίωσης της σύνδεσης από κινητή συσκευή, έχουν αποδειχθεί αποτελεσματικά. Ο συγγραφέας αναφέρει επίσης ότι μια άλλη σημαντική συμπεριφορά που πρέπει να χρησιμοποιηηθεί είναι να λαμβάνει κανείς ενημερώσεις λογισμικού μόνο από αξιόπιστες πηγές. Οι Rughinis & Rughinis (2014) ανέλυσαν τα αποτελέσματα μιας έρευνας χρηστών του Διαδικτύου από διαφορετικές χώρες της Ευρωπαϊκής Ένωσης με θέμα τη συμπεριφορά στον κυβερνοχώρο και την έκθεση στο κυβερνοέγκλημα στο πλαίσιο συνήθων δραστηριοτήτων. Οι ακαδημαϊκοί ομαδοποίησαν τους ερωτηθέντες σύμφωνα με τις διαδικτυακές τους δραστηριότητες, τα μέτρα έκθεσης και κυβερνοεγκλήματος που

εφαρμόστηκαν και κατέληξαν σε πέντε τύπους: εξερευνητής, αντιδραστικός, συνετός, τυχερός και περιστασιακός. Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι ο διαχωρισμός των χρηστών σε απευθείας σύνδεση σε πέντε ομάδες μπορεί να είναι χρήσιμος για την ανάλυση του είδους των τεχνικών πρόληψης που λειτουργούν και ποιου είδους στρατηγικές έχουν σχεδιαστεί λανθασμένα. Παρέχουν ως παράδειγμα: λόγω του γεγονότος ότι οι τρέχουσες εκστρατείες πρόληψης του εγκλήματος στον κυβερνοχώρο απευθύνονται σε γονείς και νέους χρήστες που είναι «εξερευνητές» και «τυχεροί» τύποι, οι «συνετοί» χρήστες, που αποτελούν την πλειοψηφία, δεν έχουν συνήθως τις ανησυχίες τους στο πλαίσιο αυτών των εκστρατειών πρόληψης.

Από την άλλη πλευρά, το έγκλημα στον κυβερνοχώρο θα μπορούσε να αντιμετωπιστεί από νομοθετική άποψη. Ωστόσο, πρέπει να ληφθεί υπόψη ότι διαφορετικές χώρες προσαρμόζουν διαφορετικά τους νόμους. Στην Αγγλία και την Ουαλία, οι κύριοι νόμοι που καλύπτουν το έγκλημα στον κυβερνοχώρο είναι ο «Νόμος για την κατάχρηση υπολογιστών» του 1990 και ο «Νόμος για σοβαρό έγκλημα» του 2015 που προσαρμόζονται και αναπτύσσονται προκειμένου να αντιμετωπίσουν τα πιο σύγχρονα ζητήματα του κυβερνοχώρου. Ωστόσο, στις Φιλιππίνες για παράδειγμα, ο νόμος για την πρόληψη του εγκλήματος στον κυβερνοχώρο θεσπίστηκε μόνο το 2012, όταν το κράτος αναγνώρισε τελικά τη σημασία της ασφάλειας των πληροφοριών στον κυβερνοχώρο (Celine, 2013). Πρώτα απ 'όλα, η πράξη αφορά παράνομη πρόσβαση σε ένα σύστημα υπολογιστή, λαμβάνοντας υπόψη το απόρρητο και τις υποκλοπές τυχόν μη δημόσιων μεταδόσεων. Δεύτερον, απαγορεύει κατηγοριοποιημένες απάτες που σχετίζονται με υπολογιστή, όπως πλαστογραφία δεδομένων, τροποποίηση ή διαγραφή δεδομένων, κλοπή ταυτότητας και άλλα. Και τέλος, αντιμετωπίζονται επίσης αδικήματα που σχετίζονται με το περιεχόμενο με τη μορφή ανεπιθύμητων διαφημίσεων καθώς και τον καθορισμό όλων των εγκλημάτων στον κυβερνοχώρο σύμφωνα με τους ισχύοντες νόμους. Ο Mayer (2016) υποστήριξε την τρέχουσα κατάσταση των νόμων σχετικά με το έγκλημα στον κυβερνοχώρο στις ΗΠΑ, δηλώνοντας ότι το ομοσπονδιακό καταστατικό και ο νόμος περί απάτης και κατάχρησης υπολογιστών θα μπορούσαν να προσαρμοστούν. Ο συγγραφέας ισχυρίζεται ότι οι νόμοι στοχεύουν πολύ συχνά σε εγκλήματα χαμηλού επιπέδου, όπως οι λανθασμένοι χειρισμοί των κυβερνητικών υπαλλήλων, γεγονός που αφήνει σοβαρά κενά στη νομοθεσία, επιτρέποντας στους εγκληματίες να διαπράξουν εγκλήματα στον κυβερνοχώρο μεγάλης κλίμακας που προκαλούν δισεκατομμύρια ζημίες και ακόμη δεν αντιμετωπίζονται. Ο Mayer συζητά

διαφορετικούς νόμους για το έγκλημα στον κυβερνοχώρο και προτείνει προσαρμογές που θα μπορούσαν να γίνουν για να καλύψουν αυτό το κενό.

Επίσης, όσον αφορά τις προσαρμογές του νόμου, ο Fick (2009) αναφέρει ότι για να αντιμετωπιστεί σωστά και αποτελεσματικά το έγκλημα στον κυβερνοχώρο, η νομοθετική εστίαση πρέπει να εστιάζεται στην πρόληψη και όχι στη δίωξη. Ο Fick στηρίζει τη διατριβή του στη δήλωση ότι η πρόληψη είναι πολύ πιο αποτελεσματική από τη δίωξη λόγω διαφόρων παραγόντων που συζητήθηκαν νωρίτερα, όπως το έγκλημα «χωρίς θύματα», τα θύματα που δεν γνωρίζουν το έγκλημα, το έγκλημα στον κυβερνοχώρο που δεν αναφέρεται, οι δυσκολίες στον εντοπισμό των παραβατών κ.λπ.

Παρόλο που ορισμένοι συγγραφείς πιστεύουν ότι οι τεχνολογικές αλληλεπιδράσεις και οι νομοθετικές προσαρμογές είναι οι κύριες προσεγγίσεις για την πρόληψη του εγκλήματος στον κυβερνοχώρο, διαφορετικές χώρες και διαφορετικοί οργανισμοί έχουν πειραματιστεί με άλλες προσεγγίσεις. Ο Buono (2014) συζητά πώς θα μπορούσε να αντιμετωπιστεί το έγκλημα στον κυβερνοχώρο μέσω της ευαισθητοποίησης. Το άρθρο των Dimc & Dobosek (2013) που υποστηρίζει τη θέση της ευαισθητοποίησης ως αποτελεσματικής στρατηγικής συζητήθηκε νωρίτερα. Συνοψίζοντας, το κύριο σημείο της μελέτης τους είναι να υποστηριχθεί ότι η πρόληψη του εγκλήματος στον κυβερνοχώρο μέσω δημόσιων εκστρατειών για τρόπους προστασίας στο διαδίκτυο και γενικές στρατηγικές ευαισθητοποίησης για το έγκλημα στον κυβερνοχώρο είναι αποτελεσματικές. Επισημαίνεται επίσης ότι η νομοθεσία για το έγκλημα στον κυβερνοχώρο δεν είναι ακόμη αρκετά σαφής και περιεκτική και ότι το έγκλημα στον κυβερνοχώρο πρέπει να θεωρείται διεθνές. Οι Kratchman et al.,(2008) έχουν επίσης συζητήσει την προοπτική της πρόληψης μέσω της ευαισθητοποίησης, αλλά μόνο σε επίπεδο εταιρειών και οργανισμών. Λαμβάνοντας υπόψη τα πιο διαδεδομένα εγκλήματα στον κυβερνοχώρο (ιοί και DDoS), προτάθηκε ότι η ζημιά σε διαφορετικές εταιρείες και οργανισμούς στις ΗΠΑ θα μπορούσε να ελαχιστοποιηθεί σημαντικά μέσω στρατηγικών ευαισθητοποίησης. Οι συγγραφείς πρότειναν ότι οι εταιρείες θα πρέπει να έχουν εσωτερικούς ελεγκτές των οποίων τα καθήκοντα θα είναι να αξιολογούν την κατάσταση προστασίας από εγκλήματα στον κυβερνοχώρο σε μια εταιρεία και να παρέχουν συμβούλιο για τον τρόπο βελτίωσης της άμυνας στον κυβερνοέγκλημα.

Οι Almadhoob & Valverde (2014) διερεύνησαν επίσης πώς μπορεί να αντιμετωπιστεί το ζήτημα του εγκλήματος στον κυβερνοχώρο σε οργανισμούς μέσω της προσθήκης

κυβερνοασφάλειας εντός εταιρειών. Οι συγγραφείς δηλώνουν ότι μετά τα γεγονότα της Αραβικής Άνοιξης το 2011, το Βασίλειο του Μπαχρέιν υπέστη αυξανόμενα ποσοστά εγκλημάτων στον κυβερνοχώρο που πρέπει να αντιμετωπιστούν. Οι συγγραφείς σημείωσαν εκ νέου ότι τα πιο δημοφιλή εγκλήματα στον κυβερνοχώρο ήταν οι ιοί που αποστέλλονταν μέσω ηλεκτρονικού ταχυδρομείου για να αποκτήσουν πρόσβαση σε υπολογιστή μέσα σε έναν οργανισμό ή μια επίθεση DDoS και μελέτησαν πόσο προετοιμασμένα και ενημερωμένα ήταν τα τμήματα πληροφορικής των μεγάλων οργανισμών στο Βασίλειο του Μπαχρέιν. Οι συγγραφείς ολοκλήρωσαν τη μελέτη τους προτείνοντας ότι οι επίσημες συζητήσεις σχετικά με το θέμα της κυβερνοασφάλειας εντός οργανισμών με σκοπό την ενημέρωση των αρμοδίων, καθώς και των εργαζομένων, για τις πιο σύγχρονες απειλές και μέτρα ασφαλείας θα συμβάλουν στη μείωση των ποσοστών εγκληματικότητας στον κυβερνοχώρο. Ωστόσο, πρέπει να σημειωθεί ότι οι συγγραφείς δεν μπόρεσαν να συλλέξουν μεγάλο δείγμα δεδομένων, καθώς το Βασίλειο του Μπαχρέιν διαθέτει περιορισμένους πόρους και πραγματοποιήθηκε με ένα δείγμα 34 οργανισμών.

Συνεχίζοντας, οι Leppanen & Kankaanranta (2017) μελέτησαν τη διερεύνηση του εγκλήματος στον κυβερνοχώρο στο πλαίσιο της αστυνομικής δύναμης στη Φινλανδία. Οι συγγραφείς δηλώνουν ότι τα τελευταία χρόνια, η επιβολή του νόμου στη Φινλανδία επικεντρώθηκε σε μεγάλο βαθμό στη βελτίωση της πρόληψης του εγκλήματος στον κυβερνοχώρο, συμμετέχοντας σε διαφορετικά προγράμματα κατάρτισης στον κυβερνοχώρο μέσω συνεργασίας με τους Nordic Computer Forensics Investigators. Η μελέτη τους παρέχει μια εμπεριστατωμένη συζήτηση για το πώς λειτουργούν οι διαδικασίες διερεύνησης εγκλημάτων στον κυβερνοχώρο εντός της αστυνομίας, πώς διεξάγεται η εκπαίδευση διερεύνησης του εγκλήματος στον κυβερνοχώρο και πώς θα μπορούσε να βελτιωθεί. Ο κύριος στόχος ήταν να δείξει μια άλλη μορφή πρόληψης του εγκλήματος στον κυβερνοχώρο - δηλαδή την ιατροδικαστική έρευνα μέσω υπολογιστή. Οι Habirovs & Arturs (2018) συζήτησαν τις πρακτικές συνέπειες της ιατροδικαστικής έρευνας σε υπολογιστή σε μια μελέτη περίπτωσης μιας διαδικτυακής έρευνας για παιδο-πορνογραφία. Πρώτον, οι συγγραφείς αναθεώρησαν το ζήτημα της διαδικτυακής παιδικής πορνογραφίας από την προοπτική της πρόληψης της εγκληματικότητας κατάστασης, και στη συνέχεια συζήτησαν πώς θα μπορούσαν να βελτιωθούν οι διαδικασίες έρευνας από τεχνολογική άποψη. Ο Murashbekov (2015) αναθεώρησε το θέμα της πρόληψης του εγκλήματος στον κυβερνοχώρο στις αναπτυσσόμενες χώρες

και τρόπους με τους οποίους θα μπορούσε να βελτιωθεί. Συγκρίνει τον τρόπο αντιμετώπισης του εγκλήματος στον κυβερνοχώρο στη Δημοκρατία του Καζακστάν με αυτόν των δυτικών χωρών. Ο συγγραφέας δηλώνει ότι τα ποσοστά εγκλημάτων στον κυβερνοχώρο στη Δημοκρατία του Καζακστάν είναι χαμηλότερα σε σύγκριση με την ΕΕ ή τις ΗΠΑ, επειδή οι δυτικές χώρες δίνουν έμφαση σε διαφορετικές τακτικές, μεθόδους και στρατηγικές πρόληψης, ενώ η Ρωσία επικεντρώνεται στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο από νομοθετική σκοπιά. Ο Murashbekov υποστηρίζει ότι το έγκλημα στον κυβερνοχώρο πρέπει να αντιμετωπιστεί από ειδικούς της επιβολής του νόμου και της ασφάλειας στον κυβερνοχώρο, ωστόσο, η έρευνα δείχνει ότι διαφορετικές τεχνικές μέθοδοι προστασίας αποδείχθηκαν επίσης επιτυχημένες. Οι Rashkovski et al., (2015) συνέταξαν επίσης μια μελέτη όπου διερεύνησαν την αποτελεσματικότητα της διαφορετικής πρόληψης του εγκλήματος στον κυβερνοχώρο από νομοθετικές καθώς και γενικές προσεγγίσεις στην πρώην Γιουγκοσλαβική Δημοκρατία της Μακεδονίας. Οι συγγραφείς συζητούν διάφορα άρθρα του Ποινικού Κώδικα της Μακεδονίας που αφορούν συγκεκριμένα το έγκλημα στον κυβερνοχώρο και υποστηρίζουν ότι μερικά από τα πιο αποτελεσματικά θα μπορούσαν να εφαρμοστούν σε διεθνές επίπεδο. Οι ακαδημαϊκοί πιστεύουν ότι η κατάσταση στη Μακεδονία είναι απόδειξη ότι το έγκλημα στον κυβερνοχώρο θα μπορούσε να αντιμετωπιστεί από νομοθετική άποψη και να δώσει συστάσεις σε διεθνείς οργανισμούς για να διερευνήσουν τη νομοθεσία της Μακεδονίας σχετικά με την πρόληψη του εγκλήματος στον κυβερνοχώρο.

Οι Harris & Singla (2014) μελέτησαν τον αντίκτυπο του εγκλήματος στον κυβερνοχώρο στην οικονομία της Ιρλανδίας και εκτίμησαν τον αντίκτυπο σε 630 εκατομμύρια ευρώ. Οι συγγραφείς διερεύνησαν τους κινδύνους και τις απειλές του εγκλήματος στον κυβερνοχώρο από την άποψη της οικονομίας, πώς το έγκλημα στον κυβερνοχώρο επηρεάζει την κατάσταση της οικονομίας και πώς να αναιρέσει τους κινδύνους από την άποψη της οικονομίας. Οι Harris & Singla διερεύνησαν τις κυβερνητικές επενδύσεις στην κυβερνοασφάλεια και τη συσχέτιση της αποτελεσματικότητας και κατέληξαν στο συμπέρασμα ότι εάν η κυβέρνηση επενδύσει περισσότερα χρήματα στην ασφάλεια στον κυβερνοχώρο, θα μπορούσε να μειώσει τις ζημιές στον κυβερνοέγκλημα, εξοικονομώντας στη συνέχεια χρήματα. Επιπλέον, η μελέτη θέτει το σημείο ευαισθητοποίησης και πόσο κρίσιμης σημασίας είναι για το επιχειρηματικό και κυβερνητικό περιβάλλον. Μια άλλη σύγχρονη τεχνική

πρωτογενούς πρόληψης χρησιμοποιήθηκε από το Πανεπιστήμιο του Κεντρικού Αρκάνσας στα τέλη του 2017 (Anonymous, 2017). Το πανεπιστήμιο έχει δημιουργήσει ένα λεγόμενο «cyber-range» όπου οι φοιτητές μπορούν να βιώσουν κυβερνοεπιθέσεις που προσομοιώνονται από υπολογιστή σε πραγματικό χρόνο για να μάθουν και να εξερευνήσουν διαφορετικές μεθόδους πρόληψης του κυβερνοεγκλήματος. Επιπλέον, ένα νέο μάθημα πτυχίου στην κυβερνοασφάλεια ξεκινά το φθινόπωρο του 2018. Ο κυβερνήτης του Αρκάνσας πιστεύει ότι η απειλή για κυβερνοέγκλημα είναι πραγματική και τόνισε τη σημασία της εκπαίδευσης που σχετίζεται με τις επιστήμες των υπολογιστών.

Όπως αναφέρθηκε προηγουμένως, διαφορετικές χώρες αντιμετωπίζουν το έγκλημα στον κυβερνοχώρο από διαφορετικές προοπτικές, ωστόσο ορισμένες χώρες αναγνωρίζουν το κυβερνοέγκλημα ως διεθνές ζήτημα και προσπαθούν να συμβάλουν στην πρόληψή του σε διεθνές επίπεδο. Ο Li (2007) συζήτησε το έγκλημα στον κυβερνοχώρο ως διεθνές ζήτημα και πώς το πρόβλημα του κυβερνοεγκλήματος θα μπορούσε να εξισορροπηθεί στον κόσμο. Δήλωσε ότι ορισμένοι διεθνείς οργανισμοί έχουν ήδη κάνει βήματα για τη συζήτηση του θέματος του εγκλήματος στον κυβερνοχώρο - για παράδειγμα, το δίκτυο πληροφοριών των Ηνωμένων Εθνών για το έγκλημα και τη δικαιοσύνη (Δίκτυο πληροφοριών των Ηνωμένων Εθνών για το έγκλημα και τη δικαιοσύνη, 1999) και την Ομάδα Εργασίας για το Ηλεκτρονικό Έγκλημα των Αστυνομικών Επιτρόπων (2000). Ο συγγραφέας συζητά περαιτέρω συγκεκριμένες τροποποιήσεις στις νομοθεσίες που πραγματοποιούνται από επαγγελματίες διεθνείς οργανισμούς αστυνόμευσης του εγκλήματος, όπως η Ιντερπόλ, το Συμβούλιο της Ευρώπης (The Council of Europe - COE), η Ομάδα των Οκτώ (G8), τα Ηνωμένα Έθνη (ΟΗΕ) και άλλοι. Καταλήγει στο συμπέρασμα ότι έχουν ήδη γίνει πολλές διαφορετικές νομοθετικές προσαρμογές σε σχέση με το έγκλημα στον κυβερνοχώρο, ωστόσο εξακολουθούν να υπάρχουν πολλά κενά στους νόμους σε διεθνές επίπεδο. Ο Li συζητά επίσης ότι ορισμένοι σημαντικοί οργανισμοί, όπως ο ΟΗΕ, θα πρέπει να έχουν μεγαλύτερο αντίκτυπο, καθώς έχουν μεγαλύτερη επιρροή.

Άλλοι ακαδημαϊκοί διερεύνησαν τις πιο πρόσφατες τεχνολογικές εφευρέσεις και πώς θα μπορούσαν να χρησιμοποιηθούν στον τομέα της πρόληψης του εγκλήματος στον κυβερνοχώρο. Οι Mills & Byun (2006) συζήτησαν τη βιομετρία όταν μόλις παρουσιάστηκε και πρότειναν τρόπους με τους οποίους θα μπορούσαν να χρησιμοποιηθούν για την προστασία των καταναλωτών. Οι συγγραφείς εξηγούν ότι η

βιομετρική προστασία σε μορφή σάρωσης δακτυλικών αποτυπωμάτων, σάρωσης ίριδας, αναγνώρισης φωνής ή προσώπου θα μπορούσε να προσθέσει ένα ακόμη επίπεδο προστασίας στις προσωπικές ηλεκτρονικές συσκευές. Υποστηρίζουν ότι με τη χρήση τέτοιων τεχνολογιών στην ασφάλεια στον κυβερνοχώρο, τα ποσοστά εγκλημάτων στον κυβερνοχώρο θα μπορούσαν να μειωθούν εκθετικά. Χρόνια αργότερα, οι Frost & Sullivan (2014) ανέλυσαν επίσης βιομετρικές τεχνολογίες στην καταναλωτική αγορά και κατέληξαν στο συμπέρασμα ότι η βιομετρία των δακτυλικών αποτυπωμάτων θα είναι κυρίαρχη στο μέλλον. Σήμερα, τα περισσότερα σύγχρονα smartphones διαθέτουν τουλάχιστον μία τεχνολογία βιομετρικής αναγνώρισης, όπως δακτυλικό αποτύπωμα, σάρωση ίριδας ή αναγνώριση προσώπου και φωνής. Ο Maher (2017) προχώρησε ακόμη περισσότερο και διερεύνησε πώς η τεχνητή νοημοσύνη (artificial intelligence - AI) θα μπορούσε να βοηθήσει στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Οι ακαδημαϊκοί συζήτησαν τεχνολογίες όπως η μηχανική μάθηση, η βαθιά μάθηση και η ανάλυση χρηστών και οντοτήτων (User and Entity Behavior Analytics -UEBA). Η τεχνολογία UEBA θα μπορούσε να χρησιμοποιηθεί για τον εντοπισμό απειλών αναλύοντας τις δραστηριότητες του δικτύου και εντοπίζοντας κακόβουλη συμπεριφορά, στη συνέχεια αναφέροντάς την σε έναν χειριστή. Η UEBA μπορεί να διδαχθεί τα πρότυπα της κανονικής συμπεριφοράς του δικτύου και, μέσω ενός αλγορίθμου, να μάθει να ανιχνεύει τυχόν αποκλίσεις. Ο συγγραφέας αναφέρει ότι η UEBA παρέχει σχεδόν 100% αναφορά ακρίβειας.

Εν κατακλείδι, η απειλή για το έγκλημα στον κυβερνοχώρο είναι πολύ πραγματική και πολλοί άνθρωποι σε όλο τον κόσμο ανησυχούν για την έκθεση σε διαφορετικά εγκλήματα στον κυβερνοχώρο. Ως εκ τούτου, αναγνωρίζεται και αντιμετωπίζεται από εγκληματολόγους και διάφορους ιδιωτικούς και κυβερνητικούς καθώς και διεθνείς οργανισμούς. Η πρόληψη του εγκλήματος στον κυβερνοχώρο προχωράει, αναπτύσσεται παράλληλα με την τεχνολογική πρόοδο.Κατά συνέπεια, το συμπέρασμα αν τα ποσοστά χρήσης προσωπικών ηλεκτρονικών συσκευών και η έκθεση σε εγκλήματα στον κυβερνοχώρο έχουν θετικές συσχετίσεις με τη χρήση μηχανισμών πρόληψης ή εάν το θέμα του εγκλήματος στον κυβερνοχώρο εξελίσσεται και η πρόληψη του κυβερνοεγκλήματος πρέπει να αντιμετωπιστεί πιο σοβαρά.

3.4. Ο ΡΟΛΟΣ ΤΗΣ ΠΑΓΚΟΣΜΙΟΠΟΙΗΣΗΣ ΣΤΗΝ ΠΡΟΛΗΨΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στην εποχή της παγκοσμιοποίησης, η τεχνολογία των πληροφοριών διαδραματίζει πολύ σημαντικό ρόλο. Με την απόκτηση τεχνολογίας και πληροφοριών, μια χώρα έχει επαρκές κεφάλαιο για να γίνει νικήτρια στον παγκόσμιο ανταγωνισμό. Η ζωή της σημερινής κοινωνίας, σιγά-σιγά άρχισε να βιώνει μια πολύ μεγάλη αλλαγή. Η αλλαγή είναι η αλλαγή της βιομηχανικής εποχής στην εποχή της τεχνολογίας και της πληροφορίας που βρίσκεται πίσω από την επίδραση της προχωρημένης εποχής της παγκοσμιοποίησης, η οποία καθιστά τους υπολογιστές, το διαδίκτυο και την ταχεία ανάπτυξη της τεχνολογίας των πληροφοριών το κύριο μέρος που πρέπει να υπάρχει ή δεν πρέπει να λείπει στις ζωές των ανθρώπων σήμερα, διότι στην εποχή της παγκοσμιοποίησης, αν όχι η τελειοποίηση της τεχνολογίας των πληροφοριών είναι συνώνυμη με τον αναλφαβητισμό.

Από την αρχή, οι άνθρωποι αναζητούσαν πάντα την ευκολία να διεκπεραιώνουν δραστηριότητες για την ικανοποίηση των αναγκών τους. Αυτό έχει εκπληρωθεί με την πρόοδο της τεχνολογίας. Ωστόσο, οι άνθρωποι εξακολουθούν να μην είναι ικανοποιημένοι, έτσι ψάχνουν πάντα για τη δυνατότητα της ευκολίας στην ικανοποίηση των αναγκών τους. Από την άλλη πλευρά, για την επίτευξη των αναγκών τους, συμβαίνει συχνά ότι κάποιος κάνει πραγματικά κάτι απαίσιο (Loqman, 2006). Οι πρόοδοι στην τεχνολογία και την πληροφορία που σηματοδοτούνται από την εμφάνιση του Διαδικτύου, και είναι το αποτέλεσμα μιας τεχνολογικής επανάστασης που συνεργάζεται συνεργατικά με την τεχνολογία των πληροφοριών και τους υπολογιστές, στην ανάπτυξή τους έχουν προκαλέσει ταχείες αλλαγές στη δομή της κοινωνίας από τον αγροτικό στο βιομηχανικό κόσμο, από τον βιομηχανικό στον κόσμο της πληροφορική, που τελικά έφεραν και δημιούργησαν νέα πρότυπα, μοντέλα και τρόπους ζωής σε ένα νέο κόσμο, δηλαδή τον εικονικό κόσμο (κυβερνοχώρο).

Το διαδίκτυο έχει ενσωματωθεί με ανθρώπινες δραστηριότητες που κυμαίνονται από μικρές και απλές δραστηριότητες σε σημαντικές και πολύπλοκες δραστηριότητες. Αυτή η πραγματικότητα είναι ένα πλεονέκτημα της τεχνολογίας. Με τις υπηρεσίες τεχνολογίας του Διαδικτύου, πολλές εταιρείες ασκούν διάφορες επιχειρηματικές δραστηριότητες, όπως διαδικτυακό μάρκετινγκ, πωλήσεις εξ αποστάσεως και ηλεκτρονικό εμπόριο. Ένα άλλο παράδειγμα είναι η χρήση των μέσων ενημέρωσης του διαδικτύου ως μέσο υποστήριξης στην κράτηση/κράτηση εισιτηρίων (αεροπλάνα,

τρένα), ξενοδοχεία, πληρωμή τηλεφωνικών λογαριασμών, ηλεκτρικό ρεύμα, έχει κάνει τους καταναλωτές πιο άνετους και ασφαλείς στην εκτέλεση των δραστηριοτήτων τους. Οι καταναλωτές δεν χρειάζεται να εγκαταλείψουν το σπίτι και την ουρά για να πάρουν την υπηρεσία που θέλουν, επειδή η διαδικασία παραγγελίας / κράτησης μπορεί να γίνει στο σπίτι, το γραφείο, ακόμη και σε ένα όχημα, καθώς και το επίπεδο ασφαλείας στις συναλλαγές είναι σχετικά εγγυημένη, επειδή οι συναλλαγές πραγματοποιούνται online (Mansur, 2005).

Οι δραστηριότητες του δικτύου οικονομικής παγκοσμιοποίησης που προκαλούνται από την πρόοδο της τεχνολογίας των πληροφοριών όχι μόνο μεταβάλλουν τα πρότυπα της οικονομικής παραγωγικότητας αλλά αυξάνουν και τα επίπεδα παραγωγικότητας και ταυτόχρονα προκαλούν διαρθρωτικές αλλαγές στην πολιτική ζωή, τον πολιτισμό, την κοινωνική ζωή και επίσης την έννοια του χρόνου σε διάφορα στρώματα της κοινωνίας. Η τεχνολογία πληροφοριών εκτός από το θετικό της αντίκτυπο, έχει και αρνητικό αντίκτυπο στην κοινωνική ζωή των χρηστών της. Αυτή η αρνητική επίπτωση ονομάζεται σκοτεινή πλευρά της προηγμένης τεχνολογίας. Αυτός ο αρνητικός αντίκτυπος είναι η εμφάνιση διαφόρων αντικοινωνικών συμπεριφορών, αποκλίνουσας συμπεριφοράς και εγκλημάτων που βασίζονται στο διαδίκτυο και τον κυβερνοχώρο.

Η εμφάνιση του εγκλήματος στον κυβερνοχώρο θα λέγαμε προς προσιδιάζει με την «εποχή των κακοηθών ναρκών». Ένας φανταστικός και εικονικός χώρος, ένας χώρος ή μια ζώνη όπου ο καθένας μπορεί να διεξάγει δραστηριότητες που μπορούν να γίνουν στην καθημερινή κοινωνική ζωή με τεχνητό τρόπο. Ο καθένας μπορεί να επικοινωνεί μεταξύ τους, να απολαμβάνει την ψυχαγωγία και να έχει πρόσβαση σε ό,τι νομίζει ότι μπορεί να φέρει ευχαρίστηση ή ίσως ικανοποίηση. Υπάρχουν διάφορες προσφορές στον κυβερνοχώρο σύμφωνα με τις παγκόσμιες πληροφορίες που πωλούνται από τους καπιταλιστές που είναι πρόθυμοι να δικαιολογήσουν κάθε μέσο για να κάνουν κέρδος. Ακόμη και ειρωνικά, σκοπεύουν επίσης να υπονομεύσουν την ηθική, ιδεολογική και θρησκευτική αντοχή άλλων εθνών στη γη που είναι διαφορετικά από τον εαυτό τους. Ο χαρακτηρισμός του εγκλήματος στον κυβερνοχώρο, όπως αναφέρεται από τον Barda Nawawi Arief (2018) είναι σύμφωνος με τη Σύμβαση του 2001 για το έγκλημα στον κυβερνοχώρο στη Βουδαπέστη της Ουγγαρίας, δηλαδή:

- Μη έγκυρη πρόσβαση: σκόπιμη εισαγωγή ή πρόσβαση σε σύστημα υπολογιστή χωρίς δικαιώματα

- Παράνομη υποκλοπή: εσκεμμένα και χωρίς δικαιώματα που επισφραγίζουν ή κρατούν κρυφά τη διαβίβαση και διαβίβαση δεδομένων μη δημόσιου υπολογιστή προς, από ή εντός συστήματος πληροφορικής που χρησιμοποιεί τεχνικά βοηθήματα
- Παρεμβολή δεδομένων: σκοπίμως και χωρίς δικαιώματα καταστροφής, αλλαγής ή διαγραφής δεδομένων υπολογιστή
- Παρεμβολή συστήματος: εκ προθέσεως μη εξουσιοδοτημένη παρέμβαση ή σοβαρή παρέμβαση στη λειτουργία συστήματος πληροφορικής·
- Κατάχρηση συσκευών: την κατάχρηση του εξοπλισμού πληροφορικής, συμπεριλαμβανομένων των προγραμμάτων ηλεκτρονικών υπολογιστών, των κωδικών πρόσβασης των υπολογιστών
- Πλαστογραφία σχετική με ηλεκτρονικούς υπολογιστές, ήτοι παραποίηση (εκ προθέσεως και χωρίς δικαιώματα εισαγωγής, τροποποίησης, διαγραφής αυθεντικών δεδομένων, τα οποία δεν είναι αυθεντικά με πρόθεση να χρησιμοποιηθούν ως αυθεντικά δεδομένα)
- Απάτη σχετική με ηλεκτρονικούς υπολογιστές, δηλαδή απάτη (εκ προθέσεως και χωρίς δικαιώματα που προκαλούν απώλεια αγαθών/πλούτου τρίτων με την εισαγωγή, αλλαγή, διαγραφή δεδομένων ηλεκτρονικών υπολογιστών ή με παρέμβαση στη λειτουργία υπολογιστών/συστημάτων ηλεκτρονικών υπολογιστών, με στόχο την απόκτηση οικονομικών οφελών για τους ίδιους ή άλλους)
- Αδικήματα που σχετίζονται με το περιεχόμενο και συγκεκριμένα αδικήματα που σχετίζονται με την παιδική πορνογραφία
- Αδικήματα που σχετίζονται με παραβιάσεις δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων και συγκεκριμένα αδικήματα που σχετίζονται με την παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας.

Η τεχνολογία των πληροφοριών και οι τηλεπικοινωνίες κατάφεραν να αλλάξουν τη σειρά και το πρότυπο παραγωγής, εμπορίου και επενδύσεων των πολυεθνικών εταιρειών και των παγκόσμιων εταιρειών. Ο κυβερνοχώρος έχει αλλάξει ριζικά τη σχέση μεταξύ νομικά σημαντικών (online) φαινομένων και φυσικής θέσης. Η αύξηση των παγκόσμιων δικτύων υπολογιστών έχει καταστρέψει τη σχέση μεταξύ γεωγραφικής θέσης και:

- Κυβερνητικής εξουσίας για την επιβολή ελέγχου στην επιγραμμική συμπεριφορά
- Επιρροής της διαδικτυακής συμπεριφοράς σε άτομα ή αγαθά
- Κυβερνητικής νομιμότητα για τη ρύθμιση παγκόσμιων φαινομένων, και
- Της ικανότητας της επικράτειας να ενημερώνει τα άτομα που διασχίζουν τα σύνορα σχετικά με το εφαρμοστέο δίκαιο.

Αυτή η ριζική αλλαγή είναι μια συντριβή των ορίων, που κατεδαφίζει την ιεραρχία και διαλύει τη γραφειοκρατία. Φυσικά, αυτή η αλλαγή προκαλεί οτιδήποτε έρχεται σε επαφή με την τεχνολογία των πληροφοριών να υποστεί προσαρμογές, έτσι ώστε η παγκοσμιοποίηση να απαιτεί επίσης αλλαγές στο εμπόριο, τις επενδύσεις, την τεχνολογία των πληροφοριών και ούτω καθεξής πολιτικές που παρέχουν περισσότερη ελευθερία κίνησης, έτσι ώστε το κεφάλαιο, η τεχνολογία και η εργασία να μπορούν να μετακινούνται εύκολα μεταξύ των χωρών εδαφική κυριαρχία του κράτους. Δεν είναι λάθος αν το απαιτεί η παγκοσμιοποίηση, διότι συνδέεται με την πρόοδο της τεχνολογίας των πληροφοριών που δημιουργεί το έγκλημα στον κυβερνοχώρο, το δυναμικό πρόκλησης βλάβης σε διάφορους τομείς όπως η πολιτική, η οικονομία, η κοινωνική και η κουλτούρα, που είναι πολύ πιο ανησυχητική από άλλα εγκλήματα υψηλής έντασης και ακόμη και στο μέλλον μπορεί να διαταράξει την εθνική οικονομία μέσω δικτύων υποδομών που βασίζονται στην ηλεκτρονική τεχνολογία (τράπεζες, τηλεπικοινωνίες, δορυφόροι, δίκτυα ηλεκτρικής ενέργειας και δίκτυα εναέριας κυκλοφορίας).

Δεδομένης της φύσης του διαδικτύου που υπερβαίνει τα εθνικά σύνορα, επιλύει προβλήματα χρόνου και τόπου και λειτουργεί στον κυβερνοχώρο, το διαδίκτυο γεννά διάφορες μορφές δραστηριοτήτων που δεν ρυθμίζονται πλήρως από την ισχύουσα νομοθεσία. Το γεγονός αυτό έχει κάνει τον κόσμο να συνειδητοποιήσει την ανάγκη για κανονισμούς που διέπουν τις δραστηριότητες στο διαδίκτυο. Σε ένα κράτος δικαίου η εξουσία που είναι μια αντανάκλαση της πολιτικής που εκδηλώνεται σε κάθε πολιτική απαιτεί μια ρυθμιστική / νομική βάση, έτσι ώστε η νομιμότητα της πολιτικής να μπορεί να εξηγηθεί. Σε ένα παγκόσμιο πλαίσιο, η νομική πολιτική δεν μπορεί μόνο να προστατεύει τα εθνικά συμφέροντα, αλλά πρέπει επίσης να προστατεύει τα διασυνοριακά συμφέροντα, όπως συμβαίνει με τα εγκλήματα στον κυβερνοχώρο που είναι διεθνικού χαρακτήρα. Η παγκοσμιοποίηση των νόμων και η πολιτική οδηγούν τους κανονισμούς των αναπτυσσόμενων χωρών σχετικά με τις επενδύσεις, το εμπόριο,

τις υπηρεσίες, την τεχνολογία των πληροφοριών και άλλους οικονομικούς τομείς να προσεγγίσουν τις ανεπτυγμένες χώρες (σύγκλιση), καθώς και τους κανονισμούς σχετικά με τις δραστηριότητες του κυβερνοχώρου που δεν μπορούν να διαχωριστούν από τις σχέσεις με άλλες χώρες. Ο επείγων χαρακτήρας της εθνικής ρύθμισης των δραστηριοτήτων στον κυβερνοχώρο βασίζεται σε τρεις κύριες σκέψεις (Siregar & Sinaga, 2021):

- την ανάγκη για ασφάλεια δικαίου για τους δράστες των δραστηριοτήτων στον κυβερνοχώρο, διότι δεν έχει προσαρμοστεί επαρκώς στις υφιστάμενες ρυθμίσεις·
- τις προσπάθειες για την πρόβλεψη των επιπτώσεων που προκύπτουν από τη χρήση της τεχνολογίας πληροφοριών· και
- την ύπαρξη παγκόσμιων μεταβλητών, δηλαδή ο ελεύθερος ανταγωνισμός και η ανοικτή αγορά.

Σύμφωνα με τον Soekanto (2020), η πρόοδος της τεχνολογίας θα συμβαδίζει με την εμφάνιση αλλαγών στον κοινωνικό τομέα. Οι αλλαγές στην κοινωνία μπορεί να αφορούν κοινωνικές αξίες, κοινωνικούς κανόνες, πρότυπα συμπεριφοράς, οργάνωση, και δομή κοινωνικών θεσμών. Γενικά, μια κοινωνία που βιώνει αλλαγές λόγω της τεχνολογικής προόδου γεννά πολλά κοινωνικά προβλήματα. Αυτό συμβαίνει επειδή η κατάσταση της ίδιας της κοινότητας δεν είναι έτοιμη να δεχτεί την αλλαγή ή μπορεί επίσης να συμβαίνει επειδή οι αξίες της κοινότητας έχουν αλλάξει κατά την αξιολόγηση των παλαιών συνθηκών ως συνθήκες που δεν είναι πλέον αποδεκτές. Αυτά τα νομικά ζητήματα συνδέονται στενά με την ανάπτυξη της ρύθμισης της τεχνολογίας των πληροφοριών (κυβερνοχώρος) σήμερα.

Η ανάπτυξη του νομικού τομέα αναμένεται να συμβάλει στην ανάπτυξη της εποχής της πληροφορικής και στην επιτάχυνση της οικονομικής ανάπτυξης. Όλες οι οικονομικές δραστηριότητες που ασκούνται χωρίς ισχυρή νομική βάση θα οδηγήσουν εύκολα σε διάφορα προβλήματα, στα οποία αυτά τα προβλήματα όταν υπολογίζονται οικονομικά (κέρδη και ζημίες) θα οδηγήσουν σε υψηλό κόστος. Η βούληση για ένα ασφαλές και σαφές διεθνές εμπορικό κλίμα για τη διεθνή κοινότητα και για τη δημιουργία βιώσιμης εμπορικής απελευθέρωσης στους τομείς των επενδύσεων, της εργασίας, των υπηρεσιών για την ενθάρρυνση αυξημένων ρυθμών οικονομικής ανάπτυξης και ανάπτυξης σε όλο τον κόσμο, ξεκίνησε από την ίδρυση της Γενικής Συμφωνίας

Δασμών και Εμπορίου (ΓΣΔΕ) μέσω μιας σειράς διαπραγματεύσεων που οδήγησαν στη δημιουργία του Παγκόσμιου Οργανισμού Εμπορίου (ΠΟΕ).

Η ασφάλεια και η σαφήνεια (βεβαιότητα) των συναλλαγών δεν μπορεί να αγνοηθεί κατά τη διασφάλιση της συνέχειας των συναλλαγών, ιδίως στην τρέχουσα εποχή της παγκοσμιοποίησης, όπου οι εμπορικές συναλλαγές δεν περιορίζονται πλέον από διαφορές στην απόσταση, το εθνικό υπόβαθρο, το νομικό σύστημα, τη θέση, το κεφάλαιο, το επίπεδο εκπαίδευσης. , κατοικία, και ούτω καθεξής. Τα προβλήματα που προκύπτουν αν δεν αντιμετωπιστούν άμεσα θα προκαλέσουν διάφορες συγκρούσεις που καθιστούν αδύνατο τον σκοπό της συναλλαγής, τόσο από οικονομική άποψη όσο και από μια καλή σχέση. Οι νομοθετικές ρυθμίσεις ως μέρος των υποστηρικτικών στοιχείων των δραστηριοτήτων οικονομικής ανάπτυξης μπορούν να συμβάλουν σημαντικά στην επιτάχυνση της οικονομικής ανάπτυξης. Η οικονομική ανάπτυξη απαιτεί μια σταθερή νομική βάση, έτσι ώστε η ύπαρξη νόμων και κανονισμών να έχει μια θετική επιρροή.

Οι κανονισμοί στον τομέα της τεχνολογίας των πληροφοριών πρέπει να περιέχουν όλα τα προβλήματα που σχετίζονται με τη χρήση τους, όπως νομικά, οικονομικά, θεσμικά ζητήματα, επίλυση διαφορών και ούτω καθεξής. Η ρύθμιση της τεχνολογίας των πληροφοριών θα διευκολύνει την εφαρμογή της ανάπτυξης καθώς και την αξιολόγηση της χρήσης της τεχνολογίας. Σχετικά με τη ρύθμιση της τεχνολογίας των πληροφοριών (κυβερνοχώρος), υπάρχουν παράγοντες που οδηγούν στην ανάγκη για άμεση θέσπιση νόμου που ρυθμίζει τις δραστηριότητες στον κυβερνοχώρο, μεταξύ άλλων:

- Οι πραγματικές συνθήκες που δείχνουν ότι σχεδόν κάθε ανθρώπινη ζωή έχει επηρεαστεί από τη χρήση των δραστηριοτήτων της τεχνολογίας των πληροφοριών. Ξεκινώντας από τις ανάγκες των παιδιών έως τις ανάγκες των ενηλίκων, που κυμαίνονται από τον οικιακό εξοπλισμό έως τις ανάγκες της εξελιγμένης κρατικής άμυνας και ασφάλειας, είναι λοιπόν ειρωνικό ότι για τόσο περίπλοκες δραστηριότητες δεν υπάρχει νομοθεσία που να τις ρυθμίζει.
- Οι υφιστάμενοι κανονισμοί (ο ισχύων νόμος) δεν μπόρεσαν να απαντήσουν στα προβλήματα που προκύπτουν στον τομέα της τεχνολογίας των πληροφοριών. Η λογική συνέπεια αυτής της κατάστασης είναι ότι παρεμποδίζεται η χρήση της τεχνολογίας·
- Υπάρχουν ανησυχίες από ορισμένους ομίλους (ιδίως από εκείνους που βρίσκονται στον επιχειρηματικό κόσμο) σχετικά με την απουσία νομικών

εγγυήσεων κατά την άσκηση δραστηριοτήτων μέσω εγκαταστάσεων τεχνολογίας πληροφοριών, αν δεν έχουν θεσπιστεί οι εν λόγω κανονισμοί. Πρέπει να σημειωθεί ότι η ασφάλεια των δραστηριοτήτων είναι ένας από τους καθοριστικούς παράγοντες για τη δημιουργία ενός καλού επιχειρηματικού κλίματος.

- Όλα τα κράτη, ως μέρη της παγκόσμιας κοινότητας, δεν μπορούν να αποφύγουν τη βελτίωση των νομικών τους μέσων, ιδίως εκείνων που σχετίζονται με την τεχνολογία των πληροφοριών, ώστε να μην αποκλειστούν από τη διεθνή σκηνή.
- Ο ανταγωνισμός στον αγώνα για ξένες επενδύσεις γίνεται όλο και πιο έντονος, ενώ πολλές χώρες του κόσμου σε προσπάθεια προσέλκυσης ξένων επενδυτών για να εισέλθουν στη χώρα τους παρέχουν διάφορα είδη εγκαταστάσεων. Η έλλειψη ετοιμότητας μιας χώρας να συντάξει ένα νόμο για την τεχνολογία πληροφοριών είναι ένας από τους παράγοντες που εμποδίζει την είσοδο ξένων επενδύσεων.

Η επιρροή της διαμόρφωσης του νόμου για την τεχνολογία πληροφοριών έχει ως εξής:

- Εγγύηση της βεβαιότητας και της ασφάλειας στην επιχειρηματική δραστηριότητα. Σε αναπτυσσόμενες χώρες το ζήτημα της ασφάλειας και της ασφάλειας των επιχειρήσεων αποτελεί ύψιστη προτεραιότητα που πρέπει να υλοποιηθεί. Ο φόβος της εθνικοποίησης, όπως συνέβη αρκετές δεκαετίες πριν, είναι μια κακή εμπειρία που κάθε εταιρεία που σκοπεύει να επενδύσει σε τέτοια κράτη μπορεί να αποφύγει όσο το δυνατόν περισσότερο. Ως εκ τούτου, ευελπιστούμε ότι μέσω της θέσπισης ενός νόμου για την τεχνολογία των πληροφοριών, οι εγγυήσεις ασφάλειας και βεβαιότητας στην επιχειρηματική δραστηριότητα, ιδίως όσον αφορά τις δραστηριότητες που βασίζονται στην τεχνολογία των πληροφοριών, θα υλοποιηθούν περισσότερο.
- Μπαίνοντας στην εποχή της τεχνολογίας της πληροφορίας, φυσικά, οι συμβατικές οικονομικές δραστηριότητες μπορούν σταδιακά να αποφευχθούν. Το γεγονός αυτό έχει αρχίσει να εφαρμόζεται στην εμπορία μετοχών στο χρηματιστήριο όροφο, όπου η διαπραγμάτευση έχει πραγματοποιηθεί χωρίς χαρτί. Επίσης στο τελωνείο, η επεξεργασία των εγγράφων είναι πλήρως μηχανογραφημένη. Το ίδιο ισχύει και όταν τα μέσα του Διαδικτύου χρησιμοποιούνται σε δραστηριότητες ηλεκτρονικού εμπορίου. Δεν θα υπάρχουν φυσικές συναντήσεις μεταξύ των μερών, συμφωνίες δεν θα γίνονται

πλέον σε ένα κομμάτι χαρτί, υπογραφές δεν θα γίνονται πλέον σε ένα κομμάτι χαρτί και δεν θα είναι χειρόγραφα. Λόγω της τάσης προς τα εικονικά φαινόμενα, η θέσπιση ενός νόμου για την τεχνολογία των πληροφοριών/νόμου για τον κυβερνοχώρο που παρέχει τη βάση για την εγκυρότητα των συμβάσεων ηλεκτρονικά θα έχει αντίκτυπο στην αύξηση του αριθμού των συναλλαγών, επειδή οι επιχειρηματικοί εταίροι μπορούν να διαπραγματεύονται μόνο μέσω ηλεκτρονικών συσκευών.

- Η προστασία των ατομικών δικαιωμάτων, τόσο των ατόμων όσο και των εταιρειών που δεν έχουν ρυθμιστεί από την υφιστάμενη νομοθεσία (υφιστάμενη νομοθεσία) μπορεί να αποτελέσει παράγοντα ώθησης της εισόδου ξένων επενδύσεων. Η εμπειρία στην Ελβετία ή τη Σιγκαπούρη έχει αποδείξει ότι με τη διατήρηση των προσωπικών δικαιωμάτων (ακόμη και αν χρησιμοποιούνται μερικές φορές από άτομα που τα παραβιάζουν), η οικονομική δραστηριότητα σε αυτές τις χώρες δείχνει σχετικά ενθαρρυντικούς αριθμούς. Ως εκ τούτου, ευελπιστούμε ότι κατά τη διαμόρφωση του νόμου για την τεχνολογία των πληροφοριών, η ρύθμιση των ατομικών δικαιωμάτων περιλαμβάνεται σε μία από τις διατάξεις.
- Οι οικονομικές δραστηριότητες, τόσο εγχώριου όσο και διεθνούς χαρακτήρα, είναι πάντα στοιχειωμένο από τη δυνατότητα των διαφορών που προκύπτουν. Οι μηχανισμοί επίλυσης διαφορών που έχουν υιοθετηθεί από τα μέρη συχνά δεν είναι ικανοποιητικοί, παρόλο που υπάρχουν αποδεικτικά στοιχεία. Το πρόβλημα που προκύπτει είναι πώς η θέση των αποδεικτικών στοιχείων σε συναλλαγές με το διαδίκτυο, το οποίο είναι ως επί το πλείστον με τη μορφή κωδίκων και όλα τα ψηφιακά στοιχεία μπορούν να εξισωθούν με αποδεικτικά στοιχεία που είναι γνωστά μέχρι στιγμής, όπως τα γραπτά αποδεικτικά στοιχεία. Σε αυτό το σημείο ο ρόλος του νόμου για την τεχνολογία πληροφοριών/του νόμου για τον κυβερνοχώρο θα παράσχει ασφάλεια στα αποδεικτικά στοιχεία, έτσι ώστε τα μέρη να μπορούν να τα προλάβουν όταν προκύψει διαφορά στο μέλλον.
- Ο προσδιορισμός της δικαιοδοσίας είναι επίσης επιρρεπής σε προβλήματα. Κάθε συμβαλλόμενο μέρος επιθυμεί πάντα την επίλυση των διαφορών που προκύπτουν στη χώρα του, με την ελπίδα ότι θα είναι πιο επικερδής γι' αυτούς. Το πρόβλημα που προκύπτει σχετικά με τον προσδιορισμό της δικαιοδοσίας

είναι να καθορίσει ποιο δικαστήριο είναι εξουσιοδοτημένο να επιλύσει τη διαφορά, αν η διαφορά προκύπτει ως αποτέλεσμα μιας συναλλαγής που διεξάγεται μέσω του διαδικτύου, αν το δικαστήριο όπου ο παραλήπτης είναι ή ο αποστολέας είναι εγκατεστημένος ή τι αν η συναλλαγή πραγματοποιείται σε διεθνή περιοχή. Για παράδειγμα, μια συμφωνία για την πραγματοποίηση μιας συναλλαγής συνάπτεται κατά την επιβίβαση σε ένα αεροπλάνο ή πλοίο επειδή χρησιμοποιεί υπολογιστή. Ο νόμος για την τεχνολογία των πληροφοριών/ο νόμος για τον κυβερνοχώρο θα μπορούσε να παράσχει σαφήνεια σχετικά με το ζήτημα του καθορισμού της δικαιοδοσίας·

- Ο τομέας της φορολογίας είναι ένα πολύ σημαντικό στοιχείο που πρέπει να λαμβάνεται υπόψη κατά την άσκηση μιας επιχειρηματικής δραστηριότητας, διότι αυτό το πρόβλημα θα επηρεάσει σε μεγάλο βαθμό τη λειτουργία μιας επιχειρηματικής δραστηριότητας. Ο φόρος είναι μια υποχρέωση για τους επιχειρηματικούς φορείς. Ως εκ τούτου, στην πράξη, τα μέρη τείνουν να μειώσουν τις φορολογικές δαπάνες όσο το δυνατόν περισσότερο. Στις συναλλαγές με το διαδίκτυο, είναι δυνατόν να επιβληθεί διπλή φορολογία, επειδή το φορολογικό υποκείμενο στη χώρα του έχει εισπραχθεί φόρος, ενώ σε άλλες χώρες υπόκειται επίσης σε φόρο επί των συναλλαγών που κάνει. Η φορολογική πτυχή απαιτεί επίσης σαφήνεια στη ρύθμιση του νόμου για την τεχνολογία των πληροφοριών, έτσι ώστε οι επιχειρηματικοί φορείς στον τομέα της τεχνολογίας των πληροφοριών να μην αποθαρρύνονται από το να επενδύσουν λόγω ασαφών φορολογικών ρυθμίσεων.

Πολιτική Πρόληψης του Ηλεκτρονικού Εγκλήματος

Η σημασία του νόμου για την τεχνολογία των πληροφοριών που καλύπτει όλα τα εγκλήματα στον κυβερνοχώρο (νόμος για τον κυβερνοχώρο), ο οποίος αναμένεται να ρυθμίζει τη χρήση της τεχνολογίας των πληροφοριών συνολικά είναι κάτι που δεν μπορεί να καθυστερήσει άλλο. Οι πραγματικές συνθήκες έχουν αποδείξει ότι η απουσία του νόμου για τον κυβερνοχώρο έχει ως αποτέλεσμα την εμφάνιση διαφόρων μορφών ανησυχίας κατά την εκτέλεση εικονικών δραστηριοτήτων. Το να επιτρέψουμε να συνεχιστεί αυτή η ανησυχία είναι πολύ σημαντικό για την οικονομική ανάπτυξη, τόσο μικροοικονομική όσο και μακροοικονομική. Η εμπειρία των ανεπτυγμένων χωρών δείχνει ότι υπάρχει σημαντική σχέση μεταξύ της βέλτιστης χρήσης της τεχνολογίας της πληροφορίας και της επιταχυνόμενης οικονομικής ανάπτυξης. Στο

τέλος, η οικονομική ανάπτυξη θα οδηγήσει σε αυξημένη οικονομική ανάπτυξη. Η εμπειρία στις ανεπτυγμένες χώρες μπορεί να χρησιμοποιηθεί ως αντανάκλαση για να διαμορφώσει αμέσως ένα νόμο για την τεχνολογία πληροφοριών / νόμο για τον κυβερνοχώρο που καλύπτει όλες τις δραστηριότητες στον κυβερνοχώρο, δεδομένης της μεγάλης επιρροής που έχει η διαμόρφωση του νόμου για τον κυβερνοχώρο στην επιτάχυνση της οικονομικής ανάπτυξης.

Όσον αφορά τη ρύθμιση του εγκλήματος στον κυβερνοχώρο, ο Muladi είδε τρεις προσεγγίσεις (Raharjo, 2002):

- Μια σφαιρική προσέγγιση που απαιτεί μια νέα γενική ρύθμιση της ηλεκτρονικής εγκληματικότητας, η οποία περιλαμβάνει διάφορες μορφές πράξεων όπως χειραγώγηση, καταστροφή, κλοπή και χρήση υπολογιστών ενάντια στο νόμο και χωρίς εξουσία (πρόσβαση σε σύστημα επεξεργασίας δεδομένων). Αυτό φαίνεται, για παράδειγμα, στο σουηδικό νόμο περί δεδομένων του 1973.
- Μια εξελικτική προσέγγιση (evolutionary approach) που επιδιώκει να μεταρρυθμίσει ή να τροποποιήσει τη διατύπωση των παραδοσιακών εγκλημάτων προσθέτοντας αντικείμενα και τρόπους για τη διάπραξη εγκλημάτων υπολογιστών στη διατύπωσή της. Η πρόσθεση σε αυτήν την περίπτωση μπορεί να σημαίνει τροποποίηση ή με τη μορφή συμπλήρωσης. Παραδείγματα είναι ο νόμος του 1985 περί τροποποίησης του ποινικού κώδικα στον Καναδά.
- Συμβιβασμός μεταξύ της παγκόσμιας προσέγγισης και της εξελικτικής προσέγγισης, η οποία επιτυγχάνεται με τη συμπερίληψη των υπολογιστών στην κωδικοποίηση του ποινικού δικαίου.

3.5. ΔΙΕΘΝΕΙΣ ΠΡΟΣΠΑΘΕΙΕΣ ΚΑΤΑΠΟΛΕΜΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Έχουν γίνει προσπάθειες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο από διάφορες οργανώσεις όπως τα Ηνωμένα Έθνη, η Ευρωπαϊκή Ένωση, το Συμβούλιο της Ευρώπης και η Ιντερπόλ. Μεταξύ των στόχων των Ηνωμένων Εθνών είναι η υποστήριξη της οικονομικής ανάπτυξης και της τήρησης του διεθνούς δικαίου και ασφάλειας. Ο ΟΗΕ υιοθέτησε τη Σύμβαση των Ηνωμένων Εθνών κατά του Διακρατικού Οργανωμένου Εγκλήματος με σκοπό την καταπολέμηση του

οργανωμένου εγκλήματος. Ο ΟΗΕ έχει στο παρελθόν εκδώσει εκθέσεις σχετικά με μέτρα για τον περιορισμό της εγκληματικότητας υψηλής τεχνολογίας και των υπολογιστών. Κατά τη διάρκεια του 11ου συνεδρίου του ΟΗΕ για την πρόληψη του εγκλήματος, πραγματοποιήθηκε εργαστήριο συζήτησης για να συζητηθεί η πιθανή συνεργασία μεταξύ εθνών και ιδιωτικού τομέα για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. η επιτροπή συνέστησε στα Ηνωμένα Έθνη να βοηθήσουν τις χώρες μέλη στη διαχείριση του εγκλήματος στον κυβερνοχώρο · ότι θα πρέπει να παρέχει εκπαίδευση σε άλλα κράτη μέλη και επίσης να ενισχύει τη διεθνή επιβολή του νόμου.

Ο ΟΗΕ συνέβαλε επίσης στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο ιδρύοντας τη "Διεθνή Ένωση Τηλεπικοινωνιών(International Telecommunication Union- ITU)" που συντονίζει τη διεθνή χρήση των τηλεπικοινωνιών βελτιώνοντας παράλληλα τις υποδομές της .Μέρος των στόχων της ITU είναι η επίλυση παγκόσμιων ζητημάτων, όπως η ενίσχυση της κυβερνοασφάλειας. Το 2002, η ITU ανέπτυξε δείγματα κατευθυντήριων γραμμών νομοθεσίας για να επιτρέψει στα κράτη μέλη να αναπτύξουν εναρμονισμένους νόμους για το έγκλημα στον κυβερνοχώρο. Οι χώρες μέλη της Ευρωπαϊκής Ένωσης συνεργάζονται με συνέπεια για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η συνεργασία ενισχύεται μεταξύ των χωρών μελών μέσω της Επιτροπής της Ευρωπαϊκής Ένωσης και του συμβουλίου της. Η ΕΕ υιοθέτησε μια πολιτική που επιτρέπει την υιοθέτηση ουσιαστικών νομοθετικών λόγων για την αντιμετώπιση δραστηριοτήτων στον κυβερνοχώρο και την πρόσληψη άρτια εκπαιδευμένου προσωπικού επιβολής του νόμου .Οι ερευνητές του συνέχισαν να συνεργάζονται με μελετητές και ειδικούς πληροφορικής για την προώθηση προτύπων για έρευνες στον κυβερνοχώρο. Ομοίως, το " Συμβούλιο της Ευρώπης(Council of Europe-COE)" ασχολείται με δραστηριότητες που προσπαθούν να περιορίσουν την εγκληματικότητα στον υπολογιστή. Από το 2001, το COE απαιτεί από τα μέλη του να έχουν νόμους για το έγκλημα στον κυβερνοχώρο και κατάλληλες αρχές επιβολής του νόμου. Η G8 έχει επίσης επικεντρωθεί στην καταπολέμηση του διακρατικού οργανωμένου εγκλήματος. Μέσω της υποομάδας του σχετικά με το έγκλημα υψηλής τεχνολογίας, συμβουλεύει και βοηθά τα κράτη μέλη σχετικά με το έγκλημα στον υπολογιστή. Επιπλέον, η υποομάδα προσφέρει συστάσεις για τα κράτη μέλη της να θεσπίσουν νομοθεσία που να τους ενισχύει ενάντια στις εγκληματικές δραστηριότητες υψηλής τεχνολογίας. Από την άλλη πλευρά, η Ιντερπόλ, μια οργάνωση που διευκολύνει

τους αστυνομικούς σε όλο τον κόσμο, συμβάλλει σημαντικά στη μάχη κατά του εγκλήματος στον κυβερνοχώρο. Αστυνομικοί από χώρες μέλη της Ιντερπόλ μπορούν να έχουν πρόσβαση ο ένας στις βάσεις δεδομένων του άλλου. Μια τέτοια συνεργασία διευκολύνει την οργάνωση να καταπολεμήσει σημαντικές εγκληματικές δραστηριότητες, συμπεριλαμβανομένου του εγκλήματος στον κυβερνοχώρο (Alsmadi, 2019). Η συνεργασία μεταξύ της Ιντερπόλ και ιδιωτικών οντοτήτων όπως η Microsoft της επιτρέπει να αντιμετωπίζει και να εξουδετερώνει τις επικείμενες απειλές

3.6. Η ΣΥΜΒΑΣΗ ΤΗΣ ΒΟΥΔΑΠΕΣΤΗΣ ΓΙΑ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Οι μορφές της ηλεκτρονικής εγκληματικότητας ποικίλλουν και εξελίσσονται μαζί με τη συνεχή τεχνολογική ανάπτυξη. Για να αντιμετωπιστεί αυτή η ιδιαιτερότητα, ήταν απαραίτητη μια διακυβερνητική συνεργασία, προκειμένου να οδηγηθούμε στη σύνθεση μιας ολοκληρωμένης και αποτελεσματικής στρατηγικής για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Ο στόχος αυτός επετεύχθη στη Διάσκεψη για την Ηλεκτρονική Εγκληματικότητα (Σύμβαση για την Εγκληματικότητα στον Κυβερνοχώρο), που πραγματοποιήθηκε στη Βουδαπέστη, τα συμπεράσματα της οποίας οριστικοποιήθηκαν στη Σύμβαση που υπογράφηκε στο τέλος της διάσκεψης στις 23 Νοεμβρίου 2001.

Στη Σύμβαση της Βουδαπέστης, η οποία ουσιαστικά είναι η πρώτη διεθνής συμφωνία για την καταπολέμηση του ηλεκτρονικού εγκλήματος, που υπογράφηκε από 26 υπουργούς των ευρωπαϊκών χωρών (συμπεριλαμβανομένης της Ελλάδας), υπάρχουν επεξηγήσεις και κανονισμοί για όλα τα είδη εγκλημάτων στον υπολογιστή. Αν και η σύμβαση αυτή έχει υπογραφεί από την Ελλάδα, δεν έχει ακόμη εγκριθεί, μέσω της διαμόρφωσης σχετικής εθνικής νομοθεσίας. Η προσπάθεια αυτή ξεκίνησε πολύ πρόσφατα από τον Υπουργό Δικαιοσύνης της Ελλάδας, ο οποίος διέταξε τη σύσταση νομοθετικής επιτροπής, στόχος της οποίας θα ήταν, μεταξύ άλλων, η ενσωμάτωση των διατάξεων της Σύμβασης στο ελληνικό εθνικό δίκαιο.

Στην εν λόγω σύμβαση τονίζεται η ανάγκη για διεθνή και αμοιβαία συνδρομή για την επιβολή του νόμου μεταξύ των χωρών για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και επίσης εγείρεται το κρίσιμο ερώτημα σχετικά με την αρμοδιότητα και τη δικαιοδοσία των δικαστηρίων για τέτοια εγκλήματα. Οι στόχοι της Σύμβασης ήταν:

- Εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών μελών στον τομέα του εγκλήματος στον κυβερνοχώρο.
- Η θέσπιση του εσωτερικού δικονομικού ποινικού δικαίου που είναι απαραίτητη όχι μόνο για τη διερεύνηση, δίωξη και επιδικαστική απόφαση του εγκλήματος στον κυβερνοχώρο (καθώς και για άλλα εγκλήματα που διαπράττονται με τη χρήση συστημάτων πληροφορικής), αλλά και για τη συλλογή αποδεικτικών στοιχείων που βρίσκονται σε ηλεκτρονική μορφή.
- Η θέσπιση ταχέων και αποτελεσματικών κανόνων στη διεθνή συνεργασία και επικοινωνία.

Η σύμβαση περιλαμβάνει:

- Ουσιαστικές διατάξεις του ποινικού δικαίου.
- Διατάξεις ποινικού δικονομικού δικαίου.
- Διατάξεις για τη διεθνή δικαστική συνεργασία.

Η ανάγκη για διεθνή νομική εναρμόνιση επισημάνθηκε επίσης από τον Clough (2013), ο οποίος ισχυρίστηκε ότι είναι επιτακτική ανάγκη να διευκολυνθεί η διεθνής συνεργασία προκειμένου να εξαλειφθούν οι «ασφαλείς παράδεισοι» για τους εγκληματίες του κυβερνοχώρου. Στο έργο του, θεωρώντας τη Σύμβαση της Βουδαπέστης ως σημείο εκκίνησης, εξετάζει τον βαθμό στον οποίο η εναρμόνιση είναι εφικτή και παρουσιάζει τις διάφορες διεθνείς και περιφερειακές νομοθετικές τροποποιήσεις που έχουν προστεθεί παγκοσμίως για την αντιμετώπιση πιθανών ζητημάτων του εγκλήματος στον κυβερνοχώρο. Ωστόσο, καταλήγει στο συμπέρασμα ότι λόγω των ασύμβατων και ασυνεπών εθνικών νομοθεσιών, η διαδικασία εναρμόνισης παρεμποδίστηκε σημαντικά.

Όσον αφορά την κύρωση της Σύμβασης από τις Ηνωμένες Πολιτείες, ο Marler (2002) καταλήγει στο συμπέρασμα ότι τα οφέλη για τη θέσπιση της Σύμβασης υπερτερούν των πιθανών απειλών για το δικαίωμα της ιδιωτικής ζωής που θα προκύψουν μέσω της απαίτησης για παρακολούθηση και παρακολούθηση των επικοινωνιών. Μόλις επικυρωθεί η Σύμβαση της Βουδαπέστης από την Ελλάδα, θα καλυφθούν διάφορα κενά που υπάρχουν σήμερα στο νομικό πλαίσιο, δεδομένου ότι η Σύμβαση στοχεύει σε τρεις βασικούς στόχους:

- Εναρμόνιση του ουσιαστικού ποινικού δικαίου.
- Εναρμόνιση του Δικονομικού Ποινικού Δικαίου.

- Καθιέρωση κανόνων για διεθνή δικαστική συνεργασία.

Οι διάφορες ουσιαστικές διατάξεις του ποινικού δικαίου υπάρχουν στο πρώτο τμήμα του δεύτερου κεφαλαίου της σύμβασης και καλύπτουν τις ακόλουθες κατηγορίες εγκληματικότητας:

- Εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας δεδομένων και συστημάτων (άρθρα 2-6).
- Εγκλήματα σχετικά με υπολογιστές (άρθρα 7-8).
- Εγκλήματα σχετικά με το περιεχόμενο των δεδομένων (άρθρο 9).
- Εγκλήματα κατά της διανοητικής ιδιοκτησίας και συγγενικά δικαιώματα (άρθρο 10).

ΚΕΦΑΛΑΙΟ 4ο ΦΟΡΕΙΣ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΗΝ ΕΛΛΑΔΑ

4.1. Η ΕΛΛΗΝΙΚΗ ΕΙΣΑΓΓΕΛΙΑ ΚΥΒΕΡΝΟ-ΕΓΚΛΗΜΑΤΟΣ

Σύμφωνα με το Προεδρικό Διάταγμα 100/2004, εντός του Αστυνομικού Τμήματος Αττικής, Υποδιαίρεση Οικονομικών Εγκλημάτων Αρχαιοτήτων και Ηθικής, ιδρύθηκε και τέθηκε σε λειτουργία το 5ο Τμήμα Κυβερνοεγκλήματος, το οποίο ήταν υπεύθυνο για τη δίωξη εγκλημάτων που διαπράχθηκαν μέσω του Διαδικτύου. Στις 3 Ιανουαρίου 2005 ιδρύθηκε και λειτούργησε το αντίστοιχο τμήμα της Αστυνομικής Διεύθυνσης Θεσσαλονίκης. Στη συνέχεια, η δομή αυτών των τμημάτων ηλεκτρονικού εγκλήματος αναδιοργανώθηκε, βελτιώθηκε και εξειδικευόταν. Ως εκ τούτου, με το Προεδρικό Διάταγμα 9/2011 [8] ιδρύθηκε και τέθηκε σε λειτουργία τον Ιούλιο του 2011 η Αστυνομική Μονάδα Δίωξης Οικονομικού και Ηλεκτρονικού Εγκλήματος (Financial Police and Cyber Crime Unit - FCCPU), ως ανεξάρτητη Κεντρική Υπηρεσία υπαγόμενη στην Ελληνική Αστυνομία και εποπτευόμενη/ελεγχόμενη από τον Αρχηγό της Ελληνικής Αστυνομίας.

Σχεδόν έναν χρόνο μετά την ίδρυσή της, η Ελληνική Υποδιαίρεση Δίωξης Ηλεκτρονικού Εγκλήματος (Greek Cyber Crime Prosecution Subdivision - GCCPS) έχει να επιδείξει σημαντικά αποτελέσματα για το 2012. Συγκεκριμένα, συνολικά 458 άτομα κατηγορήθηκαν για διάπραξη διαφόρων εγκλημάτων στον κυβερνοχώρο και συνελήφθησαν συνολικά 104 άτομα. Σε ό,τι αφορά τα κατάφωρα εγκλήματα, η συντριπτική πλειοψηφία τους αφορούσε την παιδική πορνογραφία (55,77 %), ακολουθούμενη από την παραβίαση πνευματικών δικαιωμάτων (11,54 %), τη δορυφορική πειρατεία (5,77 %), διάφορες απάτες στο Διαδίκτυο (5,77 %), τις παραβιάσεις της ιδιωτικής ζωής στις τηλεπικοινωνίες (3,85 %), τις παραβιάσεις της ιδιωτικής ζωής (2,8 %) η παραβίαση των συστημάτων πληροφορικής (0,96%) και τα υπόλοιπα κατάφωρα εγκλήματα χωρίς κατηγορία προστέθηκαν στο 13,46%. Ένα άλλο πολύ σημαντικό επίτευγμα ήταν η πρόληψη των προσπαθειών αυτοκτονίας που εντοπίστηκαν, είτε επειδή τα άτομα ήθελαν να αυτοκτονήσουν για προσωπικούς λόγους και δημοσιοποίησαν τις προθέσεις τους μέσω ιστότοπων κοινωνικής δικτύωσης (κυρίως του Facebook), είτε επειδή είχαν πέσει θύματα άλλων ειδών εγκλημάτων στον κυβερνοχώρο, όπου ο δράστης είχε ασκήσει αφόρητη ψυχολογική πίεση σε αυτά.

Συγκεκριμένα, το GCCPS κατάφερε να αποτρέψει συνολικά 265 απόπειρες αυτοκτονίας, που κυμαίνονται από 11 έως 32 υποθέσεις τον μήνα. Αξίζει να σημειωθεί ότι ο αριθμός των υποθέσεων που σχετίζονται με το χρηματοπιστωτικό έγκλημα στον κυβερνοχώρο αντιπροσώπευε το 87% των συνολικών καταγεγραμμένων υποθέσεων. Χρησιμοποιώντας τα δεδομένα μιας υπηρεσίας ηλεκτρονικής βοήθειας, οι Vlachos et al. (2011) εκτίμησαν ότι μεταξύ των ετών 2007 και 2009 ο αριθμός των υποθέσεων ηλεκτρονικού εγκλήματος που σχετίζονται με οικονομική απάτη ανερχόταν στο 49,4 % των 491 συνολικών υποθέσεων. Η παρατηρούμενη αύξηση του χρηματοπιστωτικού εγκλήματος στον κυβερνοχώρο αποτελεί επομένως ισχυρό δείκτη πιθανής συσχέτισης με την ελληνική οικονομική κρίση που ξεκίνησε γύρω στα μέσα του 2010.

4.2. Η ΜΟΝΑΔΑ ΔΙΩΞΗΣ ΟΙΚΟΝΟΜΙΚΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η Οικονομική Αστυνομία και η Μονάδα Κυβερνοεγκλήματος ιδρύθηκαν ως ανεξάρτητη κεντρική Υπηρεσία, σε επίπεδο Αστυνομικής Διεύθυνσης, η οποία τελεί υπό την εποπτεία του Αρχηγείου της Ελληνικής Αστυνομίας και τελεί υπό την εποπτεία και τον έλεγχο του Αρχηγού της Ελληνικής Αστυνομίας. Η προαναφερθείσα Μονάδα έχει την έδρα της στην Αττική, ασκεί τις αρμοδιότητές της σε όλη την ελληνική επικράτεια (εκτός από τις περιοχές όπου είναι υπεύθυνη η Ακτοφυλακή), όπως ορίζεται από ειδικές διατάξεις και η αποστολή της είναι η πρόληψη και καταστολή οικονομικών εγκλημάτων, καθώς και εγκλημάτων που διαπράττονται μέσω του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η FPCCU, εκτός από το προσωπικό της, περιλαμβάνει επίσης την υποδιαίρεση της Οικονομικής Αστυνομίας και την υποδιαίρεση της Εισαγγελίας για την Δίωξη του Ηλεκτρονικού Εγκλήματος (Vlachos et al., 2011).

4.3. Η ΥΠΟΔΙΑΙΡΕΣΗ ΓΙΑ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ανεξάρτητο τμήμα της FPCCU είναι επίσης η Υποδιαίρεση Δίωξης Ηλεκτρονικού Εγκλήματος (Subdivision of Cyber Crime Prosecution - SCCP), με έδρα την Αθήνα, με πανεθνική εμβέλεια. Η υποδιαίρεση για την εγκληματικότητα στον κυβερνοχώρο υποδιαιρείται περαιτέρω σε:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στο οποίο έχει ανατεθεί η συνεχής αναζήτηση μέσω του

Διαδικτύου και άλλων μέσων ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης, με στόχο την ανίχνευση, τη διερεύνηση και τη δίωξη ποινικών πράξεων που διαπράττονται μέσω αυτών σε ολόκληρη τη χώρα, εκτός από εκείνες που ορίζονται στην κατωτέρω περίπτωση.

- Το Τμήμα Προστασίας Ανηλίκων, στο οποίο έχει ανατεθεί η διερεύνηση και η δίωξη εγκλημάτων που διαπράττονται κατά ανηλίκων, μέσω της χρήσης του διαδικτύου και άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Δικαιωμάτων Διανοητικής Ιδιοκτησίας, στο οποίο έχει ανατεθεί η διαχείριση υποθέσεων που αφορούν παράνομη διείσδυση σε συστήματα πληροφορικής, κλοπή, καταστροφή ή παράνομη διανομή λογισμικού, ψηφιακών δεδομένων και οπτικοακουστικού υλικού, που έχουν διαπραχθεί σε ολόκληρη τη χώρα, καθώς και η παροχή βοήθειας σε άλλες αρμόδιες υπηρεσίες που ερευνούν τέτοιες περιπτώσεις, όπως ορίζεται στην ισχύουσα νομοθεσία.
- Το Τμήμα Ασφάλειας Τηλεπικοινωνιών, το οποίο λειτουργεί όπως ορίζεται στις διατάξεις της απόφασης 7001/2/1261 και της κοινής υπουργικής απόφασης (Β’ 1879) των Υπουργών Εσωτερικών, Οικονομίας και Οικονομικών, Δικαιοσύνης στις 28 Αυγούστου 2009.

Προκειμένου να εκπληρώσει την αποστολή της, η Υποδιαίρεση Κυβερνο-Εγκλήματος συνεργάζεται με τις τοπικές Ελληνικές Αστυνομικές Υπηρεσίες, καθώς και με άλλες αρμόδιες Υπηρεσίες, αρχές και φορείς και διαθέτει τους απαραίτητους πόρους. Επιπλέον, στο πλαίσιο της αποστολής της, συνεργάζεται με τις αρμόδιες υπηρεσίες, οργανισμούς και φορείς της Ευρωπαϊκής Ένωσης, σύμφωνα με τις ισχύουσες διατάξεις και τις διεθνείς συμφωνίες και συμβάσεις. Οι διατάξεις του νόμου 2472/1997 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, εφαρμόζονται κατά την επεξεργασία και ανταλλαγή πληροφοριών και δεδομένων που πραγματοποιούνται στο πλαίσιο της αποστολής της Μονάδας. Το προσωπικό της υποδιαίρεσης λαμβάνει εκτεταμένη εκπαίδευση, τόσο σε τοπικό όσο και σε εξωτερικό επίπεδο, για την αποτελεσματική εκπλήρωση της αποστολής της (Vlachos et al., 2011).

Για την αντιμετώπιση των ολοένα αυξανόμενων και μεταβαλλόμενων μορφών ηλεκτρονικής εγκληματικότητας και για την εκπλήρωση του σκοπού και της

αποστολής της, η Υποδιαίρεση Δίωξης Ηλεκτρονικού Εγκλήματος διαθέτει μια ιδιαίτερα τεχνολογική υποδομή και στελεχώνεται από νέους επιστήμονες υψηλής ειδίκευσης, οι οποίοι κατέχουν μεταπτυχιακά και διδακτορικά πτυχία στον ευρύτερο τομέα της Πληροφορικής. Επιπλέον, διαθέτουν υψηλό επίπεδο θεωρητικής και εμπειρικής εμπειρογνωμοσύνης στον τομέα των τηλεπικοινωνιών, των δικτύων και της εξέτασης ψηφιακών στοιχείων.

Το Ελληνικό Κέντρο Κυβερνοεγκλήματος (ΕΚΚ) Το Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ) σε συνεργασία με τον Ελληνικό Αυτορυθμιστικό Φορέα Διαδικτυακού Περιεχομένου (Safenet), τη Νομική Σχολή, τις Οικονομικές και Πολιτικές Επιστήμες του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης (ΑΠΘ) και το Κέντρο Μελετών Ασφάλειας (ΚΕΜΕΑ) ένωσαν τις δυνάμεις τους για να ιδρύσουν το Ελληνικό Κέντρο Κυβερνοεγκλήματος (Greek Cybercrime Center - GCC), συντονισμένη ευρωπαϊκή προσπάθεια με σκοπό τη βελτίωση της εκπαίδευσης και της έρευνας στον τομέα κυβερνοεγκλήματος. Οι στόχοι του είναι:

- Προώθηση της εκπαίδευσης για το κυβερνοέγκλημα και της πανεπιστημιακής εκπαίδευσης στην Ελλάδα.
- Βελτίωση της έρευνας σε εστιασμένους τομείς του εγκλήματος στον κυβερνοχώρο, όπως δικτυορομπότ και κυβερνοεπιθέσεις.
- Κινητοποίηση της ελληνικής εκλογικής περιφέρειας στον τομέα του ηλεκτρονικού εγκλήματος.
- Συνεργασία με παρόμοια κέντρα ώστε να μεγιστοποιηθεί η απορρόφηση των αποτελεσμάτων.

Το ΕΚΚ σχεδιάζει να βελτιώσει την κατανόηση του ηλεκτρονικού εγκλήματος για τις νέες γενιές επιστημόνων και φοιτητών νομικής μέσω μιας σειράς πανεπιστημιακών μαθημάτων. Επιπλέον, μέσω μιας σειράς βραχυπρόθεσμων ιδιαίτερα εστιασμένων μαθημάτων κατάρτισης, το ΕΚΚ σχεδιάζει να βελτιώσει την κατανόηση της έννοιας του εγκλήματος στον κυβερνοχώρο για το υπάρχον προσωπικό των Τοπικών Εκπαιδευτικών Αρχών (Local Education Authorities - LEA), τις δικαστικές αρχές και τους βιομηχανικούς υπαλλήλους.

Στο πλαίσιο του προγράμματος της ΕΕ «ΕΚΚ: Ένα Κέντρο Αριστείας για την Εκπαίδευση, την Έρευνα και την Εκπαίδευση στην Ελλάδα», η 1η συνεδρίαση του Συμβουλευτικού Συμβουλίου πραγματοποιήθηκε στις 12 Σεπτεμβρίου 2013 στις

εγκαταστάσεις του Συνεδριακού Χώρου ΚΕΜΕΑ, με τη συμμετοχή των Εταίρων του Έργου Κοινοπραξίας. Στη συνεδρίαση αυτή, αναλύθηκε η έννοια του εγκλήματος στον κυβερνοχώρο και εξετάστηκε ο ακριβής ρόλος της συμβουλευτικής επιτροπής. Στη συνέχεια, σκιαγραφήθηκε η δομή του έργου, παρουσιάστηκαν λεπτομερώς οι ερευνητικές δραστηριότητες, καθώς και οι μελλοντικές δράσεις του ΕΚΚ. Αξίζει να σημειωθεί ότι έγινε σημαντική αναφορά στο ισχύον νομικό πλαίσιο και τις δομές σχετικά με το έγκλημα στον κυβερνοχώρο, καθώς και στις μεμονωμένες δράσεις του σχεδίου. Δόθηκε μεγάλη έμφαση στην ανάγκη δημιουργίας εθνικής στρατηγικής για την ασφάλεια ενάντια στο κυβερνοέγκλημα, σύμφωνα με τα τελευταία πρότυπα της ΕΕ.

4.4. ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΚΥΒΕΡΝΟ-ΈΓΚΛΗΜΑ

4.4.1. Η ΑΝΑΓΚΗ ΓΙΑ ΝΟΜΟΥΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Αναμφίβολα, η ηλεκτρονική εγκληματικότητα είναι μια συνεχώς αυξανόμενη μορφή εγκληματικότητας, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, η οποία μεταλλάσσεται καθώς εμφανίζονται καινοτόμες και εξελιγμένες μέθοδοι διάπραξης αδικημάτων. Αυτό οφείλεται κυρίως στην ταχεία ανάπτυξη των τεχνολογικών συστημάτων, τη χρήση του Διαδικτύου από έναν διαρκώς αυξανόμενο αριθμό χρηστών, τη δυσκολία ανίχνευσης/απόδειξης (ιατροδικαστική υπολογιστών και δικτύων) και φυσικά την ανωνυμία που μπορεί δυνητικά να προσφέρει στους χρήστες του. Η Μονάδα έχει κληθεί συχνά για τη διερεύνηση παραβάσεων, όπου ο παραβάτης μπορεί να βρίσκεται οπουδήποτε στον κόσμο και η παρακολούθηση της θέσης του απαιτεί χρονοβόρες και εξειδικευμένες τεχνικές έρευνες. Από την ίδρυση της υποδιεύθυνσης της Δίωξης Εγκλημάτων στον Κυβερνοχώρο, ο αριθμός των εγκλημάτων και των ποινικών υποθέσεων που κλήθηκε να διερευνήσει, είτε αυτεπαγγέλτως μέσω προκαταρκτικής έρευνας δυνάμει του άρθρου 243 του Κώδικα Ποινικής Δικονομίας, είτε μέσω του αιτήματος του εισαγγελέα για τη διεξαγωγή προκαταρκτικής έρευνας, γνώρισε ταχεία ανάπτυξη, κυρίως λόγω των λόγων που αναφέρονται στην ανωτέρω παράγραφο. Επιπλέον παράγοντες που συνέβαλαν σε αυτήν την ανάπτυξη είναι οι ακόλουθοι:

- Ο συνεχώς αυξανόμενος αριθμός ευρυζωνικών συνδέσεων στην Ελλάδα. Σύμφωνα με τις εκθέσεις της Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων που είναι διαθέσιμες στο κοινό, οι ευρυζωνικές συνδέσεις στα τέλη Δεκεμβρίου

του 2012 ανήλθαν σε 2.689.428, ενώ στα τέλη του 2010 ήταν 2.250.000 ενεργές ευρυζωνικές συνδέσεις στην Ελλάδα. Από μόλις 488.000 ενεργές συνδέσεις στα τέλη του 2006, ο αριθμός σχεδόν τριπλασιάστηκε δύο χρόνια αργότερα, φτάνοντας τις 1.400.000 στα τέλη του 2008. Το γεγονός αυτό και μόνο έδωσε στους εγκληματίες ένα αναπτυσσόμενο «ψηφιακό» πεδίο για τις παράνομες πράξεις τους.

- Η φύση των αρμοδιοτήτων της μονάδας ηλεκτρονικού εγκλήματος. Το γεγονός ότι οι ευθύνες της δεν περιορίζονται στην τοπική αρμοδιότητα της Αττικής, αλλά απλώνονται σε όλη τη χώρα.

Επιπλέον, αξίζει να σημειωθεί ότι σε τέτοιες περιπτώσεις εκτελούνται όλες οι απαραίτητες πράξεις έρευνας που είναι αναγκαίες για την εξακρίβωση του αδικήματος και την αποκάλυψη του ή των δραστών. ταυτόχρονα, διεξάγεται μια σωστή ψηφιακή έρευνα, η οποία περιλαμβάνει ένα σύνολο ενεργειών για τον εντοπισμό ψηφιακών δεδομένων σε συστήματα και συσκευές υπολογιστών, προκειμένου να επιλυθεί μια υπόθεση. Περιλαμβάνει επίσης μεθόδους και τεχνικές ηλεκτρονικής εγκληματολογίας για τη διατήρηση της ακεραιότητας και της αυθεντικότητας των δεδομένων. Επιπλέον, λόγω της αρμοδιότητας και του αντικειμένου των υπό έρευνα υποθέσεων, κατασχέθηκε μεγάλος όγκος ψηφιακών ή ηλεκτρονικών μέσων/εκθεμάτων και τα (ψηφιακά) αποδεικτικά στοιχεία των υπό έρευνα εγκλημάτων βρίσκονται κυρίως στην αποθήκευση μνήμης των προαναφερθέντων μέσων/εκθεμάτων.

Το εύρος των κυβερνο-εγκλημάτων και των υποθέσεων όπου το διαδίκτυο χρησιμοποιήθηκε ως μια απλή πλατφόρμα για τη διάπραξη εγκλημάτων και λύθηκε στην Ελλάδα από τη Μονάδα Κυβερνοεγκλήματος είναι αρκετά μεγάλο. Για να αναφέρουμε μερικά: απάτη που σχετίζεται με υπολογιστές, πλαστογραφία που σχετίζεται με υπολογιστές, κλοπή ταυτότητας, κατάχρηση συσκευών, παράνομη πρόσβαση (hacking, cracking), κατασκοπεία δεδομένων, παράνομη υποκλοπή και παρεμβολή δεδομένων και συστημάτων, διακεκριμένη διάρρηξη και κλοπή, συκοφαντική δυσφήμηση και ψευδείς πληροφορίες, συκοφαντία, δυσφήμηση ανώνυμης εταιρείας, εγκληματική οργάνωση, κυβερνο-εκβιασμό, ρατσισμό και εξύμνηση της βίας, spamming, phishing, κυκλοφορία παραποιημένων προϊόντων, αδικήματα που σχετίζονται με τα δικαιώματα πνευματικής ιδιοκτησίας και τα εμπορικά σήματα, των παραβιάσεων της ιδιωτικής ζωής και των ιδιωτικών δεδομένων, της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, του κυβερνοπολέμου, της

κυβερνοτρομοκρατίας, της τρομοκρατίας, των εγκλημάτων πνευματικής ιδιοκτησίας, της παιδικής πορνογραφίας, της διάδοσης ερωτικού ή πορνογραφικού υλικού, της αναζήτησης και κακοποίησης παιδιών, της διαδικτυακής παρακολούθησης, της παραβίασης της μνήμης των νεκρών, της διακίνησης ναρκωτικών, του λαθρεμπορίου.

4.4.2. ΔΥΣΚΟΛΙΕΣ ΠΟΥ ΣΥΝΑΝΤΩΝΤΑΙ ΚΑΤΑ ΤΗ ΔΙΕΡΕΥΝΗΣΗ ΕΓΚΛΗΜΑΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Λαμβάνοντας υπόψη ότι η προστασία της ιδιωτικής ζωής των επικοινωνιών μέσω Διαδικτύου προστατεύεται με το προεδρικό διάταγμα 47/2005, ενώ η διαδικασία για την παρακολούθηση τους περιγράφεται στο άρθρο 4 του νόμου 2225/94. Το γεγονός αυτό και μόνο καθιστά σχεδόν αδύνατο τον εντοπισμό των παραπτωμάτων που διαπράττονται μέσω του Διαδικτύου, όπου το μόνο χρήσιμο στοιχείο είναι το ηλεκτρονικό ίχνος του δράστη της πράξης. Όταν τα εγκλήματα διαπράττονται μέσω δημόσια διαθέσιμων δικτύων, όπου ο καθένας μπορεί να αποκτήσει πρόσβαση σε (όπως WiFi hotspots σε αεροδρόμια και κέντρα πόλεων), η ταυτοποίηση του δράστη είναι εξαιρετικά δύσκολη. Υπάρχουν επίσης πολλές περιπτώσεις όπου ο δράστης ζει στο εξωτερικό, οι οποίες απαιτούν αστυνομική και δικαστική συνεργασία προκειμένου να προχωρήσει η έρευνα. Ωστόσο, μια τέτοια διαδικασία είναι πολύ χρονοβόρα και δεν εγγυάται την επιτυχία της, λόγω των διαφορών στη νομοθεσία για την εγκληματικότητα στον κυβερνοχώρο μεταξύ των διαφόρων χωρών.

ΚΕΦΑΛΑΙΟ 5ο ΣΥΜΠΕΡΑΣΜΑ

Αναμφίβολα, η τεχνολογία των υπολογιστών έχει διευρύνει το φάσμα των εγκλημάτων, τα οποία απαιτούν εμπειρογνωμοσύνη και προηγμένη εκπαίδευση στην τεχνολογία πληροφορικής. Υπάρχει αρκετή διαμάχη σχετικά με τη σημασία των όρων. Ενώ κάθε έγκλημα μπορεί να διευκολυνθεί με τη χρήση ηλεκτρονικών υπολογιστών ή ΤΠΕ, σε πολλές περιπτώσεις η χρήση ηλεκτρονικών υπολογιστών δεν αλλάζει τον θεμελιώδη χαρακτήρα ενός εγκλήματος· οι χρηματισμοί παραμένουν χρηματισμοί, ανεξάρτητα από το αν τα χρήματα στάλθηκαν ηλεκτρονικά ή όχι. Ωστόσο, η χρήση υπολογιστή μπορεί να επηρεάσει το επίπεδο και την τιμωρία του εγκλήματος. Σε κάθε περίπτωση, η εισαγωγή των συστημάτων πληροφοριών και επικοινωνιών αποτελεί ποιοτική αλλαγή, σύμφωνα με τους προαναφερθέντες λόγους. Αξίζει να σημειωθεί ότι η ηλεκτρονική εγκληματικότητα προηγείται χρονολογικά και λογικά της κατηγορίας των εγκλημάτων στον κυβερνοχώρο (Parker, 2003).

Σύμφωνα με τον ορισμό του Parker (1989), κάθε παραβίαση του ποινικού δικαίου που περιλαμβάνει γνώση της τεχνολογίας των υπολογιστών για τη διάπραξη, τη διερεύνηση ή τη δίωξή τους μπορεί να θεωρηθεί έγκλημα που σχετίζεται με υπολογιστές. Ο ορισμός αυτός περιλαμβάνει και τις τρεις κύριες κατηγορίες: ηλεκτρονική εγκληματικότητα με την αυστηρή έννοια του όρου, οποιοδήποτε ηλεκτρονικό έγκλημα και κακοποίηση (σκόπιμες πράξεις όπου οι δράστες θα μπορούσαν να έχουν κέρδος και τα θύματά τους θα μπορούσαν να έχουν υποστεί απώλεια).

Η ανάπτυξη της επιστήμης και της τεχνολογίας ενθαρρύνει όλο και περισσότερο τις προσπάθειες ανανέωσης στην αξιοποίηση των τεχνολογικών αποτελεσμάτων. Η ανάπτυξη της τεχνολογίας πληροφοριών και επικοινωνιών εξελίσσεται με ταχείς ρυθμούς τόσο σε παγκόσμιο όσο και σε περιφερειακό επίπεδο. Αυτές οι εξελίξεις διευκόλυναν τελικά την παγκόσμια κοινότητα να έχει πρόσβαση σε όλες τις πληροφορίες και την επικοινωνία χωρίς να γνωρίζει τα όρια του χώρου και του χρόνου, έτσι ώστε να χαθούν τα όρια της πρόσβασης σε πληροφορίες. Ωστόσο, η ανάπτυξη της τεχνολογίας των πληροφοριών και των επικοινωνιών δεν έχει μόνο θετικές επιπτώσεις, όπως η εύκολη πρόσβαση στις πληροφορίες ή την ελεύθερη επικοινωνία, αλλά έχει και αρνητικές επιπτώσεις που μπορούν να απειλήσουν την κυριαρχία της χώρας. Αυτό μπορεί να φανεί από τα πολλά εγκλήματα που συμβαίνουν στον κυβερνοχώρο (κυβερνοέγκλημα) (Saputri et al., 2020).

Από την αρχή της ιστορίας τους, οι άνθρωποι αναζητούν πάντα ευκολία στην εκτέλεση των δραστηριοτήτων για την επίτευξη της ζωής. Έχει εκπληρωθεί με την πρόοδο της τεχνολογίας. Παρ 'όλα αυτά, οι άνθρωποι εξακολουθούν να μην είναι ικανοποιημένοι, έτσι ώστε πάντα να αναζητούν τη δυνατότητα να καλύψουν εύκολα τις ανάγκες τους. Η ταχεία ανάπτυξη της τεχνολογίας επιφέρει πρόοδο σε όλες σχεδόν τις πτυχές της ανθρώπινης ζωής. Όλες οι πτυχές της ανθρώπινης ζωής είναι άρρηκτα συνδεδεμένες και δεν μπορούν καν να διαχωριστούν από τις τεχνολογικές εξελίξεις. Ειδικά μπαίνοντας στην εποχή της παγκοσμιοποίησης, όπου διάφορα είδη αλλαγών προσφέρονται ή πωλούνται από την παγκόσμια αγορά και οποιοδήποτε έθνος, έτσι ώστε οι άνθρωποι σε διάφορα μέρη του κόσμου εξακολουθούν να απολαμβάνουν τον αντίκτυπο σύμφωνα με τις πληροφορίες και τις αλλαγές που διεισδύουν. Μέσω της παγκοσμιοποίησης των πληροφοριών που έχουν πραγματικά εισέλθει σε σπίτια, σχολεία και θρησκευτικούς θεσμούς, οι άνθρωποι συρρέουν στην πρόσβαση και να απολαμβάνουν διάφορες μορφές πληροφοριών σχετικά με την πολιτιστική επανάσταση σε άλλες χώρες ή έθνη στη γη (Ilmich et al., 2019).

Στους ανθρώπους δίνεται συνεχώς ένα πιάτο που ονομάζεται "μενού της αλλαγής", το οποίο τους κατευθύνει τους ανθρώπους να γίνουν ένα άλλο ανθρώπινο ον, ένα ανθρώπινο στιλ που είναι σύμφωνο με τους στόχους του καθεστώτος παγκοσμιοποίησης. Μπορούμε να πούμε ότι η παγκοσμιοποίηση σε αυτήν την περίπτωση είναι μια μεγάλη στροφή οικονομικής και πολιτικής δύναμης που προκαλείται κυρίως από τεχνολογικές εφευρέσεις. Η Barbara Parker (1996) δίνει τον ακόλουθο ορισμό της παγκοσμιοποίησης: Υπάρχει μια αυξανόμενη αίσθηση ότι τα γεγονότα που συμβαίνουν σε όλο τον κόσμο συγκλίνουν γρήγορα για να διαμορφώσουν έναν ενιαίο, ολοκληρωμένο κόσμο όπου οι οικονομικές, κοινωνικές, πολιτιστικές, τεχνολογικές, επιχειρηματικές, άλλες επιρροές διασχίζουν παραδοσιακά σύνορα και σύνορα όπως έθνη, εθνικές κουλτούρες, χρόνος, διάστημα, και επιχειρηματικές βιομηχανίες με αυξανόμενη ευκολία. Υπάρχει μια αυξανόμενη έννοια ότι τα γεγονότα σε όλο τον κόσμο ενώνονται γρήγορα για να σχηματίσουν έναν ενιαίο και ολοκληρωμένο κόσμο όπου οι οικονομικές, κοινωνικο-πολιτιστικές, τεχνολογικές, επιχειρηματικές και άλλες επιρροές στα παραδοσιακά σύνορα, όπως οι χώρες, εθνικές κουλτούρες, ο χρόνος και ο χώρος και οι επιχειρηματικοί κλάδοι αυξάνονται εύκολα. Η παγκοσμιοποίηση είναι μια συνέπεια που δεν μπορεί να αποφευχθεί από καμία χώρα. Η παγκοσμιοποίηση κάνει τον κόσμο χωρίς σύνορα, οι χώρες ανταγωνίζονται

ελεύθερα σε διάφορους τομείς και μερικές φορές διασχίζουν τη δικαιοδοσία μιας χώρας. Η παγκοσμιοποίηση του κόσμου θεωρείται αποτέλεσμα της ανάπτυξης της τεχνολογίας των πληροφοριών, ειδικά στη χρήση του κυβερνοχώρου ως μέσο ηλεκτρονικής επικοινωνίας για τη διάδοση των πληροφοριών σε όλο τον κόσμο.

Η ανακάλυψη της τεχνολογίας των πληροφοριών έχει αντίκτυπο σε διάφορες πτυχές μιας χώρας, όπως η εθνική κυριαρχία, για παράδειγμα σε σχέση με την εξάλειψη των εμπορικών φραγμών με ποινικές υποθέσεις στον κυβερνοχώρο. Ένα από τα προϊόντα της επιστήμης και της τεχνολογίας είναι η τεχνολογία πληροφοριών ή κοινώς γνωστή ως τεχνολογία τηλεπικοινωνιών. Στην ανάπτυξή της, με την ανακάλυψη του υπολογιστή ως προϊόν της επιστήμης και της τεχνολογίας. Μετά υπήρξε σύγκλιση μεταξύ της τεχνολογίας τηλεπικοινωνιών, των μέσων ενημέρωσης και των υπολογιστών. Η σύγκλιση της τεχνολογίας επικοινωνιών, των μέσων και των υπολογιστών είχε ως αποτέλεσμα ένα νέο εργαλείο που ονομάζεται Διαδίκτυο (Internet). Η τεχνολογική πρόοδος που είναι αποτέλεσμα του ανθρώπινου πολιτισμού, εκτός από το θετικό αντίκτυπο, με την έννοια ότι μπορεί να χρησιμοποιηθεί προς όφελος της ανθρωπότητας, έχει επίσης αρνητικό αντίκτυπο στην ανθρώπινη ανάπτυξη και τον πολιτισμό, δηλαδή την εξοικονόμηση τρωτών σημείων που είναι σίγουρα πολύ επικίνδυνα, δηλαδή την εμφάνιση του εγκλήματος στον κυβερνοχώρο που έχει γίνει μια παγκόσμια κοινότητα γνωστή ως έγκλημα στον κυβερνοχώρο.

Τα εγκλήματα που χρησιμοποιούν την τεχνολογία, δηλαδή την τεχνολογία πληροφοριών, ιδίως τους υπολογιστές και το διαδίκτυο (ηλεκτρονικό έγκλημα) έχουν φθάσει σε ανησυχητικό στάδιο. Οι πρόοδοι στην τεχνολογία των πληροφοριών, εκτός από το να φέρει στον κόσμο των επιχειρήσεων μια επαναστατική (ψηφιακή εποχή επανάστασης) που είναι όλο πρακτικό, αποδεικνύεται ότι έχει μια τρομερή σκοτεινή πλευρά, όπως η πορνογραφία, το ηλεκτρονικό έγκλημα, ακόμη και η ψηφιακή τρομοκρατία, οι πόλεμοι για τα απόβλητα των πληροφοριών, και οι χάκερ.

Παρά τη σχετικά νεαρή ηλικία του ηλεκτρονικού εγκλήματος, πρόκειται για ένα ταχέως αναπτυσσόμενο είδος εγκλήματος με πολύ διακριτά χαρακτηριστικά. Η έντασή της, σε συνδυασμό με τον διεθνικό χαρακτήρα της και την ποικιλομορφία της νομοθεσίας μεταξύ των χωρών, έχει προκαλέσει την ανάγκη διεθνούς συνεργασίας στο θέμα αυτό, με στόχο την ανάπτυξη ενός εναρμονισμένου διεθνούς πλαισίου για την αποτελεσματική αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Ένα από τα

ορόσημα προς αυτήν την κατεύθυνση ήταν η λεγόμενη Σύμβαση της Βουδαπέστης, η οποία υπεγράφη από αρκετές χώρες, συμπεριλαμβανομένης της Ελλάδας.

Παρά το γεγονός ότι η Ελληνική Αστυνομία έχει πολύ πρόσφατα συστήσει ειδική Μονάδα για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο, το νομικό πλαίσιο πρέπει να αναθεωρηθεί και να επεκταθεί, ώστε να συμπεριλάβει τις διάφορες πτυχές του εγκλήματος στον κυβερνοχώρο και να ενσωματώσει τις διατάξεις της Σύμβασης της Βουδαπέστης, κάνοντας έτσι ένα βήμα μπροστά στην Ελλάδα για να γίνει ενεργό μέλος του συμμαχικού παγκόσμιου αγώνα κατά του εγκλήματος στον κυβερνοχώρο.

ΠΗΓΕΣ - ΒΙΒΛΙΟΓΡΑΦΙΑ

Akhgar, B., & Brewster, B. (2016). Combatting Cybercrime and Cyberterrorism : Challenges, Trends and Priorities. Springer.

Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: data from the Australian cybercrime pilot observatory. In *Cybercrime Risks and Responses* (pp. 103-120). Palgrave Macmillan, London.

Almadhoob, A., & Valverde, R. (2014). Cybercrime Prevention in the Kingdom of Bahrain via IT Security Audit Plans. Journal of Theoretical and Applied Information Technology, 274-292.

Alsmadi, I. (2019). *The NICE cyber security framework: Cyber security intelligence and analytics*. Springer.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. The Economics of Information Security and Privacy, 265- 300.

Anonymous. (2017). Fighting Cybercrime. Arkansas Business, 30.

Arief, B. N. (2003). *Kapita selekta hukum pidana*. Citra Aditya Bakti.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 Cybercrime Economic Costs: No Measure No Solution. Toulouse: 2015 10th International Conference on Availability, Reliability and Security.

Baines, V. (2013). Fighting the Industrialization of Cybercrime. UN chronicle, 10-12. B

Baker, J. (2013, November 22). Survey: Most Europeans fear cybercrime but fewer take security measures. Retrieved from PCWorld: https://www.pcworld.com/article/2066460/surveymost-europeans-fear-cybercrime-but-fewer-take-security-measures.html

Barda Nawawi Arief, S. H. (2018). *Masalah penegakan hukum dan kebijakan hukum pidana dalam penanggulangan kejahatan*. Prenada Media.

BBC. 2017. Russia: The scandal Trump can`t shake. [ONLINE] Available at: http://www.bbc.com/news/world-us-canada-38966846. [Accessed 19 June 2017].

Bernik, I. (2014). Focus Series: Cybercrime and Cyber Warfare. John Willey & Sons.

Bidgoli, M., & Grossklags, J. (2016). End user cybercrime reporting: what we know and what we can do to improve it. Cybercrime and Computer Forensic (ICCCF), 1-6.

Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. ERA Forum, 1-8.

Celine, J. (2013). The Philippines Cybercrime Prevention Act. International Financial Law Review.

Chen Thomas, Robert Jean-Marc (2004). "The Evolution of Viruses and Worms" (PDF). Retrieved 2016-03-02.

Chen, R.-S., & Ji, C.-H. (2015). Investigating the relationship between thinking style and personal electronic device use and its implications for academic performance. Computers in Human Behavior, 177-183.

Choi, K.-S. (2011). Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimisation. In K. Jaishankar, Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour (pp. 229-252). Boca Raton: Taylor & Francis Group.

Choraś, M., Kozik, R., & Maciejewska, I. (2016). Emerging Cyber Security: Bio-inspired Techniques and MITM Detection in IoT. Combatting Cybercrime and Cyberterrorism, 193-207.

Clarke, R. V., & Cornish, D. B. (1986). The Reasoning Criminal: Rational Choice Perspectives on Offending. Springer

Clough, J. (2013, July). The Budapest Convention on cybercrime: Is harmonisation achievable in a digital world. In *2nd International Serious and Organised Crime Conference (ISOC 2013). South Bank, Australia*.

David Shoemaker. Dec 20 2005. Personal Identity and Ethics. [ONLINE] Available at: https://plato.stanford.edu/entries/identity-ethics/ [Accessed 19 June 2017].

de Graaf, D., Shosha, A. F., & Gladyshev, P. (2012). BREDOLAB: shopping in the cybercrime underworld. 4th International Conference on Digital Forensics & Cyber Crime. Retrieved from https://ulir.ul.ie/handle/10344/2896

Deloitte. (2015). Cybersecurity Survey 2015. Retrieved from Deloitte: https://www2.deloitte.com/ca/en/pages/risk/articles/cybersecurity-survey-2015.html

DeVoe, J., & Murphy, C. (2011). Student Reports of Bullying and Cyber-Bullying: Results from the 2009 School Crime Supplement to the National Crime Victimization Survey. National Center for Education Statistics.

Dimc, M., & Dobovsek, B. (2013). Perception of Cybercrime by Selected Internet Users in Slovenia and USA. Journal of Criminal Justice & Security, 338-356.

Ditton, J., Bannister, J., Gilchrist, E., & Farrall, S. (1999). Afraid or Angry? Recalibrating the 'Fear' of Crime. International Review of Victimology, 83-99.

Dobrinoiu, M. (2014). ID Theft in Cyberspace. Lex et Scientia, 117-120. Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. Crime, Law and Social Change, 97-116.

Doyle, C. (2011). Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. Network Security, 5-8

Fick, J. (2009). Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime. Journal of Digital Forensics, Security and law.

Financial Fraud Action UK. (2013, March 12). Decline in fraud losses stalled by rise in deception crime aimed at consumers. Retrieved from Financial Fraud Action UK.

Friend, C., Grieve, L. B., Kavanagh, J., & Palace, M. (2020). Fighting Cybercrime: A Review of the Irish Experience. *International Journal of Cyber Criminology*, *14*(2), 383-399.

Frost, & Sulivan. (2014). Smartphone fingerprint biometrics to drive consumer uptake. Biometric Technology Today, 1-2.

Fuady, M. (2007). Dinamika teori hukum.

Fuentes, C., & Svingstedt, A. (2017). Mobile phones and the practice of shopping: A study of how young adults use smartphones to shop. Journal of Retailing and Consumer Services, 137-146.

GFI Software. (2015, February 26). US Cyber Security Survey: Fear of Cyber Crime Up 66 Percent. Retrieved from CISION: PR Newswire: https://www.prnewswire.com/news-releases/uscyber-security-survey-fear-of-cyber-crime-up-66-percent-300042043.html

Gibson, M. (2014, January 23). Cell Phone Statistics: Updated 2013. Retrieved from Arkadin Collaboration Services: https://www.accuconference.com/blog/cell-phone-statisticsupdated-2013/

Goldenbeld, C., Houtenbos, M., Ehlers, E., & De Waard, D. (2012). The use and risk of portable electronic devices while cycling among different age groups. Journal of Safety Research, 1-8.

Gooch, G., & Williams, M. (2015). A Dictionary of Law Enforcement. Oxford University Press.

Goucher, W. (2010). Being a cybercrime victim. Computer Fraud & Security, 16-18.

Graham, D. (2016). The era of lethal police robots has arrived. Defense One.

Gray, D., Citron, D. K., & Rinehart, L. C. (2013). Fighting Cybercrime After "United States v. Jones". The Journal of Criminal Law and Criminology, 745-801.

Griffin, R. C. (2012). Cybercrime. J. Int'l Com. L. & Tech., 136.

Grispos, G. (2019). Criminals: Cybercriminals. *Encyclopedia of Security and Emergency Management*, 1-7.

Habirovs, Arturs (2018) Factors that shape cybercrime victimisation and use of prevention measures in England and Wales. Masters thesis, University of Huddersfield

Hardawar, D. (2012, March 29). The magic moment: Smartphones now half of all U.S. mobiles. Retrieved from Venturebeat: https://venturebeat.com/2012/03/29/the-magic-momentsmartphones-now-half-of-all-u-s-mobiles/

Harris, M., & Singla, R. (2014). Cybercrime Costs. Accountancy Ireland, 34-36.

Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. Computer Fraud & Security, 5-8.

Hossain, E., & Ahmed, Z. (2016). Academic use of smartphones by university students: a developing country perspective. The Electronic Library, 651-665.

House of Lords. (2007). Personal Internet security, Volume I: report. Science and Technology Committee. London: The Stationery Office Limited

Howard, P. N., & Gulyas, O. (2014). Data breaches in Europe: Reported breaches of compromised personal records in europe, 2005-2014. *Available at SSRN 2554352*.

Ilmih, A. A., Hartono, K., & Musofiana, I. (2019). LEGAL ASPECTS OF THE USE OF DIGITAL TECHNOLOGY THROUGH SHARIA ONLINE TRANSACTIONS IN TRADITIONAL MARKETS IN INCREASING COMMUNITY ECONOMY. *International Journal of Law Reconstruction*, *3*(2), 114-122.

Ilmih, A. A., Hartono, K., & Musofiana, I. (2019). LEGAL ASPECTS OF THE USE OF DIGITAL TECHNOLOGY THROUGH SHARIA ONLINE TRANSACTIONS IN TRADITIONAL MARKETS IN INCREASING COMMUNITY ECONOMY. *International Journal of Law Reconstruction*, *3*(2), 114-122.

Introduction to Cyber Crime http://www.inf.tsu.ru/WebDesign/libra3.nsf/161d3ebc95608f55c62571f5003467e9/3b47f7a6821 452fdc62572040016d843/$FILE/cybercrime.pdf

James A. Lewis December 2002 Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Online] Center for Strategic and International Studies Page 1

Jardine, E. (2015, July 24). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. Global Commission on Internet Governance Paper Series.

Karyda, M., & Mitrou, L. (2007, August). Internet forensics: Legal and technical issues. In *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)* (pp. 3-12). IEEE.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 470-486.

Koivunen, M., Niemi, A., & Hupli, M. (2015). The use of electronic devices for communication with colleagues and other healthcare professionals – nursing professionals' perspectives. Journal of Advanced Nursing, 620-631.

Koo, C., Chung, N., & Kim, H.-W. (2015). Examining explorative and exploitative uses of smartphones: a user competence perspective. Information Technology & People, 133-162

Kourouthanassis, P. E., & Giaglis, G. M. (2012). Introduction to the special issue mobile commerce: the past, present, and future of mobile commerce research. International Journal of Electronic Commerce, 5-18.

Kratchman, S., Jacob, L. S., & Smith, L. M. (2008). The Perpetration and Prevention of Cybercrimes. Internal Auditing, 3-8,10,12.

Krausz, M., & Walker, J. (2013). *The true cost of information security breaches and cyber crime*. IT Governance Publishing.

Kusumah, M. W. (1986). Perspektif, teori dan kebijakan hukum.

Ladd, D. A., Datta, A., Sarker, S., & Yu, Y. (2010). Trend in mobile computing withing the IS discipline. Communication of the Association for Information Systems, 285-306.

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime prevention, 157-175.

Leukfeldt, E. R. (2014). Cybercrime and Social Ties. Trends in Organized Crime, 231-249.

Li, X. (2007, September). International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology.

Livingstone, S., Haddon, L., Gorzig, A., & Ólafsson, K. (2011). Risk and Safety on the Internet. The perspective of European Children. London: EU Kids Online.

Loqman, L. (2006). *Kapita Selekta Tindak Pidana Di Bidang Perekonomian*. Datacom.

Maher, D. (2017). Can artificial intelligence help in the war on cybercrime? Computer Fraud & Security, 7-9.

Mahoney, R. (2016). Preventing Cybercrime. Business NH Magazine, 20-22.

Mansur, D. M. A. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Tiga Serangkai.

Marler, S. L. (2002). The Convention on cyber-crime: Should the United States ratify. *New Eng. L. Rev.*, *37*, 183.

Mayer, J. (2016). Cybercrime litigation. University of Pennsylvania law review, 1480.

McAfee & CSIS. (2014a, June 6). Stopping Cybercrime can positively. Retrieved from http://www.mcafee.com/uk/about/news/2014/q2/2014060

McAfee and CSIS. (2014b). Economic Impact Cybercrime 2. McQuade, S. C. (2006). Understanding and managing cyber crime. Boston: Pearson/Allyn and Bacon.

Md, M. (1998). Mahfud. Politik Hukum di Indonesia.

Mesko, G., & Bernik, I. (2011). Cybercrime: Awareness and Fear. 2011 European Intelligence and Security Informatics Conference (pp. 28-33). Ljubljana: University of Maribor.

MILITARY.COM. 2016. When Does A Cyber Attack Constitute An Act Of War? We Still Don`t Know. [ONLINE] Available at: http://taskandpurpose.com/cyber-attack-constitute-act-war-stilldont-know/. [Accessed 19 June 2017].

Mills, J. E., & Byun, S. (2006). Cybercrimes against Consumers: Could Biometric Technology Be the Solution? IEEE Internet Computing, 64-71.

Mitnick, K., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. New York: John Wiley and Sons.

Mobasheri, M., Johnston, M., Syed, U. M., King, D., & Darzi, A. (2015). The uses of smartphones and tablet devices in surgery: A systematic review of the literature. Surgery, 1352-1371.

Moore, M. (Ed.). (2016). *Cybersecurity breaches and issues surrounding online threat protection*. IGI Global.

Murashbekov, O. B. (2015). Methods for Cybercrime Fighting Improvement in Developed Countries. The Journal of Internet Banking and Commerce.

Nasi, M., Oksanen, A., Keipi, T., & Rasanen, P. (2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 203-210.

National Crime Agency. (2015). Network Security. Network Security, 3.

National Highway Traffic Safety Administration. (2016). Effect of Electronic Device Use on Pedestrian Safety: A Literature Review. Annals of Emergency Medicine, 233-234.

Nederlandese Vereniging van Banken. (2012). Dutch Banking Association. Annual Report 2012. Amsterdam: Nederlandse Vereniging van Banken

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 773-793.

Norton Antivirus Software. (2012). Cybercrime costs 110bn a year – maybe more. Computer Fraud & Security, 3, 20

Olson, R. L., Hanowski, R. J., Hickman, J. S., & Bocanegra, J. (2009). Driver distraction in commercial vehicle operations. U.S. Department of Transportation DOT, Federal Motor Carrier Safety Administration FMCSA.

Owen, T., Noble, W., & Speed, F. C. (2017). New Perspectives on Cybercrime. Springer.

Papanikolau, A., Vlachos, V., Papathanasiou, A., Chaiklais, K., Dimou, M., & Karadimou, M. (2013). Cyber crime in Greece: How bad is it? Belgrade: 2013 21st Telecommunications Forum Telfor (TELFOR).

Parker, B., Clegg, S. R., Hardy, C., & Nord, W. R. (1996). Evolution and revolution: from international business to globalization. *Managing Organizations. Current Issues*.

Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual .

Parker, D. B. (2003). Computer crime. In *Encyclopedia of Computer Science* (pp. 349-353).

Philippsohn, S. (2001). Trends in Cybercrime - An Overview of Current Financial Crimes on the Internet. Computers and Security, 53-69.

Private communication with a cybercriminal

Rahardjo, S., & Hukum, S. (2004). Perkembangan. *Metode, dan Pilihan Masalah, Surakarta: Muhammadiyah University Press*.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti.

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. European Journal on Criminal Policy and Research, 127-151.

Reyns, B., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. Crime Prevention and Community Safety, 38-59.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2012). Fear of Cyber-Identity Theft and Related Fraudulent Activity. Psychiatry, Psychology and Law, 315-328.

Roosendaal, A., Kert, M., Lyle, A., & Gasper, U. (2016). Data Protection Law Compliance for Cybercrime and Cyberterrorism Research. Combatting Cybercrime and Cyberterrorism, 81- 96.

Rughiniş, C., & Rughiniş, R. (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. Computers & Security, 111-125.

Saputri, D. P., Surryanto, D. W., & Risman, H. (2020). Indonesian Cyber Diplomacy: Asean-Japan Online Cyber Exercise. *Technium Soc. Sci. J.*, *9*, 453.

Scott, K. M., Nerminathan, A., Alexander, S., Phelps, M., & Harrison, A. (2017). Using mobile devices for learning in clinical settings: A mixed-methods study of medical student, physician and patient perspectives. British Journal of Educational Technology, 176-190.

Singleton, T. (2013). Fighting the Cybercrime Plague. Journal of Corporate Accounting & Finance, 3-7.

Siregar, G. T., & Sinaga, S. (2021). The Law Globalization in Cybercrime Prevention. *International Journal of Law Reconstruction*, *5*(2), 211-227.

Škařupová, K., Ólafsson, K., & Blinka, L. (2015). The effect of smartphone use on trends in European adolescents' excessive Internet use. Behaviour & Information Technology, 68-74.

Soekanto, S. (2020). *Pokok-pokok sosiologi hukum*. Rajawali pers.

Soekanto, S. (2020). *Pokok-pokok sosiologi hukum*. Rajawali pers.

Spada, M. M. (2014). An overview of problematic Internet use. Addictive Behaviors, 3-6.

Thomas, D., & Loader, B. (2000). Cybercrime: Law neforcement, Security and Surveillance in the Information Age. London: Routledge.

United Nations Crime and Justice Information Network. (1999). International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime. International Review of Criminal Policy, 43-44.

Viano, E. C. (2017). Cybercrime, Organized Crime, and Societal Responses. Springer, Cham.

Vlachos, V., Minou, M., Assimakopouos, V., & Toska, A. (2011). The landscape of cybercrime in Greece. *Information Management & Computer Security*.

Wagenaar, P. (2012). Detecting Botnets Using File System Indicators. University of Twente.

Wall, D. (2001). Cybercrimes and the Internet. In D. Wall, Crime and the Internet. London: Routledge.

Wall, D. (2005/15). The Internet as a Conduit for Criminal Activity. In A. Pattavina, Information Technology and the Criminal Justice System (pp. 77-98). Thousand Oaks: Sage.

Wall, D. S. (2008a). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. International Review of Law, Computers & Technology, 45-63.

Wall, D. S. (2008b). Cybercrime and the Culture of Fear. Information, Communication & Society, 861- 884.

Wang, D., Xiang, Z., & Fesenmaier, D. R. (2014). Smartphone use in Everyday Life and Travel. Journal of Travel Research, 52-63

Wignjosoebroto, S. (2008). Hukum dalam masyarakat: perkembangan dan masalah.

Woodcock, B., Middletion, A., & Nortcliffe, A. (2012). Considering the smart phone learner: an investigation into student interest in the use of personal technology to enhance their learning. Student Engagement and Experience Journal, 1-15.

Wynne, T. (2008). An Investigation into the Fear of Crime: Is there a Link between the Fear of Crime and the Likelihood of Victimisation? Internet Journal of Criminology, 1-29.

Yar, M. (2006). Cybercrime and Society. SAGE Publications

Yuri Ilyin. 2014. Cybercrime, Inc.: how profitable is the business?. [BLOG] Kaspersky Available at: https://blog.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/15034/ [Accessed 19 June 2017].