ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ : ΚΟΙΝΩΝΙΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΣΤΡΑΤΗΓΙΚΕΣ ΑΝΑΠΤΥΞΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ :

ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ: ΑΠΕΙΛΕΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΓΙΑ ΤΟ ΜΕΛΛΟΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΦΟΙΤΗΤΡΙΑ: ΙΩΑΝΝΑ – ΜΑΡΙΑ ΚΩΝ. ΣΤΑΘΟΠΟΥΛΟΥ
(Α.Μ. 3032202004019)

ΕΠΙΒΛΕΠΩΝ : ΚΑΘΗΓΗΤΗΣ ΘΕΟΔΩΡΟΣ ΠΑΠΑΘΕΟΔΩΡΟΥ

ΙΟΥΛΙΟΣ 2022

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή του Πανεπιστημίου Πελοποννήσου και επιβλέποντά μου κ. Θεόδωρο Παπαθεοδώρου για την ανάθεση της συγκεκριμένης εργασίας, καθώς και για τις πολύτιμες συμβουλές του καθ' όλη την διάρκεια εκπόνησής της. Η συνδρομή του ήταν ιδιαιτέρως σημαντική, καθότι, το κυβερνοέγκλημα είναι ένα φαινόμενο σύγχρονο και διαρκώς εξελισσόμενο.

Τέλος ευχαριστώ όλους τους διδάσκοντες του συγκεκριμένου μεταπτυχιακού για τις γνώσεις, που μας μετέφεραν και την άριστη συνεργασία.

ΠΕΡΙΛΗΨΗ

Είναι γεγονός ότι, η τεχνολογία εξελίσσεται με αλματώδεις ρυθμούς. Ένα από τα σημαντικότερα επιτεύγματά της είναι το διαδίκτυο, το οποίο έχει εισβάλλει σε όλους τους τομείς της ανθρώπινης δραστηριότητας και προσφέρει εύκολη πρόσβαση σε πάσης φύσεως πληροφορίες και εργασίες. Με τα νέα δεδομένα, που έχουν δημιουργηθεί, ο άνθρωπος έχει αποκτήσει πολλές δυνατότητες και πλέον ο ηλεκτρονικός υπολογιστής δεν λείπει από κανένα εργασιακό ή ιδιωτικό χώρο, τουλάχιστον στις αναπτυγμένες χώρες. Όμως το διαδίκτυο εκτός από την αλματώδη εξέλιξη, που έχει επιφέρει, εγκυμονεί και πολλούς κινδύνους διότι, η ανωνυμία, που πρωτίστως εξασφαλίζει, επιτρέπει την τέλεση παράνομων πράξεων. Αυτό έχει ως αποτέλεσμα μία νέας μορφής εγκληματικότητα, το κυβερνοέγκλημα να έχει κάνει την εμφάνισή του και να ενισχύεται διαρκώς ένεκα και της παρατεταμένης παγκόσμιας οικονομικής ύφεσης. Η αντιμετώπισή του από τις αρμόδιες αρχές συναντά πολλές και σημαντικές δυσκολίες με κύριες την ασάφεια του νομοθετικού πλαισίου και την έλλειψη εκπαίδευσης και εμπειρίας των εμπλεκομένων. Είναι προφανές ότι, έχουν συντελεστεί βήματα για τον περιορισμού αυτού του εγκληματικού φαινομένου, το οποίο διαρκώς εξελίσσεται και λαμβάνει νέες μορφές, όμως αυτός ακριβώς είναι ο κύριος λόγος, για τον οποίο επιβάλλεται η ενίσχυση των διακρατικών συνεργασιών και η συνεργασία των αρμοδίων φορέων.

Λέξεις κλειδιά : διαδίκτυο, κυβερνοέγκλημα, ποινική αντιμετώπιση, αντεγκληματική Πολιτική, διακρατική συνεργασία, πρόληψη, ασφάλεια.

SUMMARY

It is a fact that technology is evolving at a rapid pace. One of its most important achievements is the internet, which has invaded all areas of human activity and offers easy access to all kinds of information and tasks. With the new data that have been created, everyone has acquired many capabilities and now the computer is not missing from any workplace or private space, at least in developed countries. But the internet, in addition to the big development that it has brought, carries many risks because of the anonymity, which primarily ensures, allows the performance of illegal acts. This results in a new form of crime, cybercrime which has emerged and it is steadily intensified due to the prolonged global economic recession. Dealing with it by the competent authorities encounters many and important difficulties, mainly the ambiguity of the legal framework and the lack of education and experience of those involved. It is obvious that steps have been taken to reduce this criminal phenomenon, which is constantly evolving and taking new forms, but this is precisely the main reason why it is necessary to strengthen transnational cooperation and the cooperation of the competent bodies.

Keywords: internet, cybercrime, criminal prosecution, anti-crime policy, transnational cooperation, prevention, security.

Περιεχόμενα

Εισαγωγή

Είναι προφανές ότι, το διαδίκτυο έχει μεταβάλλει άρδην τον τρόπο λειτουργίας των σύγχρονων κοινωνιών. Η επιτάχυνση του ρυθμού διεκπεραίωσης πολλών καθημερινών εργασιών, η ελεύθερη πρόσβαση σε κάθε είδους πληροφορία και η διαχείριση μεγάλου όγκου δεδομένων αναμφίβολα συμβάλλουν στην βελτίωση της ποιότητα ζωής μας. Συνακόλουθα, όλες οι ανθρώπινες δραστηριότητες έχουν επηρεαστεί από τα σύγχρονα τεχνολογικά μέσα και βέβαια έχουν αναδειχθεί νέες μορφές επικοινωνίας, αλλά και νέες μορφές εγκληματικότητας. Παραδοσιακά εγκλήματα μεταλλάσσονται με την χρήση της τεχνολογίας, ενώ αναδεικνύονται και νέα είδη εγκληματικότητας, με αποτέλεσμα να αποτελεί επιτακτική ανάγκη η λήψη νομοθετικών πρωτοβουλιών, προσαρμοσμένων στις νέες προκλήσεις.

Υπό τα δεδομένα αυτά αντικείμενο της παρούσας εργασίας αποτελεί η μελέτη του κυβερνοεγκλήματος, των απειλών, αλλά και των προκλήσεων, που δημιουργεί για τις σύγχρονες κοινωνίες. Με την παραδοχή ότι, παρά την ραγδαία ανάπτυξη της τεχνολογίας και την εξέλιξη των εγκληματικών συμπεριφορών, εντούτοις το προστατευτικό πλαίσιο, σε παγκόσμιο επίπεδο, εξακολουθεί να μην είναι επαρκές, είναι χρήσιμη η μελέτη και η εξαγωγή συμπερασμάτων για τους τρόπους, με τους οποίους οι χρήστες του διαδικτύου θα παραμένουν προστατευμένοι κατά την περιήγησή τους, αλλά και η αποτελεσματική αντιμετώπιση εκ μέρους των διωκτικών αρχών τέτοιου είδους εγκληματικών συμπεριφορών.

Η παρούσα εργασία αποτελεί προϊόν βιβλιογραφικής ανασκόπησης και καταβλήθηκε προσπάθεια αναζήτησης πηγών μέσω του διαδικτύου και συγκεκριμένα με την χρήση λέξεων κλειδιά, όπως κυβερνοέγκλημα, κυβερνοασφάλεια, διαδίκτυο (σε ελληνική και αγγλική απόδοση).

Κατόπιν της έρευνας, που προηγήθηκε, καταρτίστηκε η δομή της εν λόγω εργασίας, η οποία χωρίζεται σε δύο μέρη. Το πρώτο μέρος και συγκεκριμένα το πρώτο κεφάλαιο αναφέρεται στην τυπολογία του κυβερνοεγκλήματος και συγκεκριμένα εκκινά με μία ιστορική αναδρομή στην εξέλιξη του διαδικτύου, ενώ αποσαφηνίζονται έννοιες, όπως ο ορισμός και η τεχνολογία του διαδικτύου. Στο δεύτερο κεφάλαιο γίνεται εκτενής αναφορά στο κυβερνοέγκλημα ως νέα μορφή εγκληματικότητας και σοβαρή απειλή, ενώ για την καλύτερη κατανόηση του ζητήματος κρίθηκε αναγκαία η ανάλυση και η απαρίθμηση των κατηγοριών των κυβερνοεγκλημάτων. Κατόπιν αυτών ακολουθεί η καταγραφή των ειδικών χαρακτηριστικών, των εργαλείων και των τεχνικών, αλλά και η αναφορά στο προφίλ των κυβερνοεγκληματιών, καθότι, από την μελέτη της σχετικής βιβλιογραφίας προέκυψε ότι, συγκεντρώνουν κάποια ιδιαίτερα χαρακτηριστικά.

Το δεύτερο μέρος της παρούσας εργασίας είναι εξίσου σημαντικό διότι, αναφέρεται στην αντεγκληματική πολιτική ενάντια στο κυβερνοέγκλημα και απαρτίζεται από δύο κεφάλαια. Στο πρώτο εξ αυτών αναλύονται ζητήματα ουσιαστικού ποινικού δικαίου, ενώ ακολουθούν δύο πολύ σοβαρά θέματα, τα οποία προέκυψαν, από την βιβλιογραφική επισκόπηση και πρόκειται αφενός μεν

για τη καταγραφή των νομικών δυσχερειών στην αντιμετώπιση αυτού του είδους των εγκλημάτων, αλλά και στα ζητήματα δικαιοδοσίας (εξεύρεσης δηλαδή των αρμοδίων αρχών αστυνομικών, εισαγγελικών, δικαστικών κ.α., που καλούνται να επιληφθούν), τα οποία ανακύπτουν, κατά την τέλεσή τους. Στο κλείσιμο του κεφαλαίου αυτού γίνεται καταγραφή της Ευρωπαϊκής και Ελληνικής νομοθεσίας, προκειμένου να καταστεί σαφές συνολικά το νομοθετικό πλαίσιο. Ακολουθεί το δεύτερο κεφάλαιο στο οποίο απαριθμούνται οι φορείς και οι μέθοδοι αντιμετώπισης σε εθνικό και διεθνές επίπεδο, καθότι, είναι προφανές ότι, η εξάπλωση του κυβερνοεγκλήματος καθιστά αναγκαία την διακρατική συνεργασία, προκειμένου να διασφαλιστεί η περιήγηση στο διαδίκτυο, αλλά και η εξάρθρωση των κυβερνοεγκληματιών, οι οποίοι είναι είτε μεμονωμένα άτομα, είτε συνηθέστερα εγκληματικές οργανώσεις με σαφή ιεραρχία και υποδομή.

Στο τέλος αυτής της εργασίας αποτυπώνονται κάποια συμπεράσματα και προτάσεις ως αποτέλεσμα της προηγηθείσας έρευνας, οι οποίες θα αποτελέσουν το εφαλτήριο μιας επόμενης έρευνας, καθότι, το κυβερνοέγκλημα είναι ένα φαινόμενο διαρκώς εξελισσόμενο, ενώ απεναντίας ως προς την δίωξή του από τις αρμόδιες αρχές, παρατηρούνται σοβαρές αρρυθμίες, οι οποίες επικεντρώνονται στην έλλειψη εκπαίδευσης και εμπειρίας, αλλά και στο νομοθετικό πλαίσιο, το οποίο είναι ασαφές και μη κωδικοποιημένο. Τα ανωτέρω καθιστούν επιτακτική την ανάγκη για στενή συνεργασία των αρμοδίων αρχών (αστυνομικές και δικαστικές) σε διεθνές και εσωτερικό επίπεδο, αλλά και την συμπόρευση των νομοθετικών παρεμβάσεων με τις συνεχείς εξελίξεις στον χώρο του κυβερνοεγκλήματος.

Μέρος Ι. Η Τυπολογία του Κυβερνοεγκλήματος

Κεφάλαιο 1 : Η τεχνολογία της πληροφορίας ως μέσο

1.1 Ιστορική αναδρομή και εξέλιξη του διαδικτύου

Το internet, όπως το γνωρίζουμε και το χρησιμοποιούμε σήμερα, αποτελεί την συνέχεια του ARPANET (Advanced Research Projects Agency Network), ενός δικτύου, το οποίο γεννήθηκε το 1969 με δαπάνες του αμερικάνικου Υπουργείου Εθνικής Άμυνας. Ο σκοπός του εγχειρήματος αυτού ήταν αφενός μεν να υπάρξει διασύνδεση με στρατιωτικούς ερευνητικούς οργανισμούς, αφετέρου δε να μελετηθεί πειραματικά η τεχνολογία της μεταγωγής πακέτων (packet switching). Κατ' αυτό τον τρόπο επιχειρήθηκε τα δεδομένα, μέσω της ίδιας γραμμής, να μεταδίδονται σε περισσότερους του ενός χρήστες και έτσι να διασφαλίζεται η επικοινωνία, ακόμα και στην περίπτωση, που κάποια συστήματα, ετίθεντο εκτός λειτουργίας (Γασπαρινάτου, Μ., 1305 επ.).

Με αυτή την επιδίωξη το εν λόγω πρώτο δίκτυο ξεκίνησε να λειτουργεί από το University of California στο Λος Άντζελες το 1969 και τους επόμενους μήνες προστέθηκαν και το University of Utath, το University of California στην Santa Barbara και το ίδρυμα Research Institute International. Μέσω της διασύνδεσης αυτής τα προαναφερόμενα πανεπιστήμια – ερευνητικά κέντρα απέκτησαν την δυνατότητα να ανταλλάσσουν τα δεδομένα τους μέσω ειδικών δικτύων και να αναπτύξουν μία αλληλεπίδραση μέσω αυτής της πρωτόγνωρης για την εποχή άμεσης επικοινωνίας.

Εν συνεχεία και συγκεκριμένα εν μέσω της δεκαετίας του 1970 το ARPANET επεκτάθηκε, απέκτησε περισσότερους χρήστες, όχι πλέον μόνο πανεπιστημιακά ιδρύματα και ερευνητικά κέντρα, με αποτέλεσμα όποιος διέθετε έναν υπολογιστή, αλλά και άδεια σύνδεσης σε πανεπιστημιακό υπολογιστή να δύναται να συνδεθεί. Ιδιαίτερα δημοφιλής, αποδείχθηκε, μέσω του συστήματος αυτού, η χρήση του ηλεκτρονικού ταχυδρομείου, μέσω του οποίου επιτεύχθηκε η αποστολή μηνυμάτων και οι χρήστες είχαν την δυνατότητα να επικοινωνούν και ανταλλάσσουν απόψεις για διάφορα θέματα.

Εν συνεχεία οι ερευνητές της ARPA και συγκεκριμένα το 1973 πειραματίστηκαν για την δημιουργία ενός νέου προγράμματος, το οποίο αποσκοπούσε στην διασύνδεση και ανόμοιων δικτύων και στην μεταφορά δεδομένων από το ένα δίκτυο στο άλλο. Στα πλαίσια αυτής της ερευνητικής προσπάθειας γεννήθηκε το Internet Protocol, γνωστό IP, από το οποίο προέκυψε το Internet.

Ακολούθησε μία περίοδος, κατά την οποία η τεχνολογική πρόοδος ήταν ταχύτατη και ραγδαία, οπότε και γενικεύτηκε η χρήση του ηλεκτρονικού ταχυδρομείου, ενώ ήδη είχε δημιουργηθεί το Πρωτόκολλο Ελέγχου Μετάδοσης, γνωστό ως TCP (Transmission Control Protocol). Το TCP/IP συνέβαλε στην επέκταση της δικτύωσης των υπολογιστών, με αποτέλεσμα όλο και περισσότεροι υπολογιστές πανεπιστημίων να συνδέονται στο ARPANET, το οποίο καταργήθηκε το 1990, δίνοντας την θέση του στο INTERNET.

1.2 Ορισμός διαδικτύου

Το διαδίκτυο (INTERNET) είναι ένα σύστημα παγκόσμιας εμβέλειας, το οποίο απαρτίζεται από διασυνδεδεμένα δίκτυα υπολογιστών, με συνηθέστερη ομάδα πρωτοκόλλων το TCP/IP, αν και δεν είναι η μοναδική. Οι ηλεκτρονικοί υπολογιστές εντάσσονται λοιπόν σε ένα κοινό δίκτυο επικοινωνίας και ανταλλάσσουν μηνύματα, με την χρήση διαφόρων πρωτοκόλλων. Αυτό το κοινό δίκτυο είναι το διαδίκτυο.

Η λειτουργία του διαδικτύου διέπεται από την αρχή της ουδετερότητας, σύμφωνα με την οποία το διαδίκτυο αυτοδιαχειρίζεται, δηλ. δεν διευθύνεται από κάποιο κεντρικό οργανισμό, το οποίο σημαίνει ότι, οι πληροφορίες διακινούνται ελεύθερα και η πρόσβαση στις ιστοσελίδες και τις υπηρεσίες του διαδικτύου είναι ίση και δεν υφίστανται διακρίσεις ως προς τον χρήστη, τον ιστότοπο κ.α.(Κοτσακά, Δ., 2015).

Αξίζει να σημειωθεί ότι, το έτος 2016 ο ΟΗΕ υιοθέτησε ψήφισμα για την ελευθερία πρόσβασης στο διαδίκτυο, με σαφή καταδίκη των χωρών, που εμποδίζουν ή δυσχεραίνουν την πρόσβαση των κατοίκων τους. Παρά την ομόφωνη αποδοχή του υπήρξαν χώρες, οι οποίες εξέφρασαν επιφυλάξεις, όπως η Ρωσία (σημ. κατά τον μήνα Μάρτιο του 2022 και λίγο αφότου είχε ξεκινήσει η ρωσική εισβολή στην Ουκρανία ο Πρόεδρος Πούτιν απαγόρευσε την χρήση των μέσων κοινωνικής δικτύωσης στο εσωτερικό της χώρας), η Κίνα κ.α., γεγονός, το οποίο βέβαια δεν μας προκαλεί έκπληξη διότι, σε αυτές συχνά εκδηλώνονται ποικίλες παραβιάσεις στην προστασία των ατομικών ελευθεριών. Σύμφωνα με το προαναφερθέν ψήφισμα αναγνωρίζεται η συμβολή του Διαδικτύου στην προαγωγή της βιώσιμης ανάπτυξης παγκοσμίως. Επίσης ζητείται από τις χώρες να αναλάβουν δράση για την γεφύρωση του ψηφιακού χάσματος, ενώ τέλος τονίζεται ότι, ο σεβασμός της ιδιωτικότητας στο Διαδίκτυο είναι κομβικής σημασίας για την διασφάλιση του δικαιώματος της ελεύθερης έκφρασης, καταδικάζοντας παράλληλα τις παραβιάσεις των ατομικών δικαιωμάτων, κατά την ενάσκηση του δικαιώματος ελεύθερης έκφρασης στο Ίντερνετ (Σπανδόνη, Ε., 2016).

1.3 Τεχνολογία διαδικτύου

Το διαδίκτυο είναι λοιπόν ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, που, όπως προαναφέρθηκε χρησιμοποιούν τα πρωτόκολλα TCP / IP. Ο παγκόσμιος ιστός (www) είναι η πιο σημαντική υπηρεσία του Διαδικτύου, με συνέπεια συχνά να δημιουργείται σύγχυση των όρων διαδίκτυο και παγκόσμιος ιστός. Η τυποποίηση των βασικών πρωτοκόλλων συντονίζεται από την Internet EngineeringTask Force (IETF). Από τα μέσα της δεκαετίας του 1990 η χρήση του σημείωσε ραγδαία αύξηση, με αποτέλεσμα πλέον το διαδίκτυο να έχει ουσιαστικά εισβάλλει σε όλες τις εκφάνσεις της ανθρώπινης δραστηριότητας (Αβούρης, Ν., 2017).

Κεφάλαιο 2 : Το Κυβερνοέγκλημα ως νέα μορφή εγκληματικότητας και σοβαρή απειλή

2.1 Ορισμός κυβερνοεγκλήματος

Προκειμένου να προχωρήσουμε στην εμβάθυνση του κυβερνοεγκλήματος κρίνεται απαραίτητο να διατυπώσουμε έναν ορισμό του. Ως εγκλήματα στον κυβερνοχώρο νοούνται οι αξιόποινες πράξεις, που τελούνται με την χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων και τιμωρούνται με συγκεκριμένες ποινές, οι οποίες προβλέπονται από την ελληνική νομοθεσία (Καργόπουλος, Α., 2018 με παραπομπή σε Επιτροπή COM (2007) 267 τελικό).

Ως εκ τούτου κυβερνοέγκλημα εν γένει (cyber – enabled crimes) είναι το έγκλημα, το οποίο τελείται με την χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών (Καργόπουλος, Α., 2018). Βέβαια εκτός από τον όρο κυβερνοέγκλημα, όπως προκύπτει από την επισκόπηση της οικείας βιβλιογραφίας, πολύ συχνά συναντούμε και άλλες ορολογίες, όπως ηλεκτρονικό έγκλημα (electronic crime), ψηφιακό έγκλημα (digital crime), διαδικτυακό έγκλημα (internet crime), έγκλημα υψηλής τεχνολογίας, έγκλημα με χρήση ηλεκτρονικών υπολογιστών (computer crime) και επιγραμμικό έγκλημα (online crime). Αξίζει να σημειωθεί ότι, στην Ευρωπαϊκή Σύμβαση του Συμβουλίου της Ευρώπης δεν διατυπώνεται συγκεκριμένος ορισμός (Φαρσεδάκης, Ι., 2009).

Θα πρέπει να επισημανθεί ότι, το κυβερνοέγκλημα αποτελεί πλέον την πιο προσοδοφόρα εγκληματική δραστηριότητα. Όπως έχει τονιστεί στην ειδική επιτροπή του αμερικανικού Κογκρέσου από ειδικούς, τα προερχόμενα από το κυβερνέγκλημα κέρδη υπερέβησαν τα αντίστοιχα από το εμπόριο ναρκωτικών. Εκτίμηση, η οποία επιβεβαιώνεται και από το FBI, το οποίο υπολόγισε ότι, τα κέρδη παγκοσμίως υπερβαίνουν το ένα τρισεκατομμύριο δολάρια, επισημαίνοντας ότι τα πραγματικά κέρδη είναι σαφώς πολλαπλάσια καθότι, μόνο το 15% των διαπραχθέντων εγκλημάτων αναφέρονται στις αρχές (Φαρσεδάκης, Ι., 2009).

2.2 Κατηγορίες κυβερνοεγκλημάτων : γνήσια και μη γνήσια, hacking – craching – malware – spamming – phishing – pharming – διαδικτυακή τρομοκρατία – διαδικτυακός εκφοβισμός – παιδική πορνογραφία – οικονομικό έγκλημα.

Μία πρώτη και βασική διάκριση των κυβερνοεγκλημάτων είναι σε γνήσια και μη γνήσια. Με τον όρο γνήσια κυβερνοεγκλήματα νοούνται οι αξιόποινες πράξεις, οι οποίες τελούνται μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών, το οποίο σημαίνει ότι, το

διαδίκτυο αποτελεί το μέσο και ταυτόχρονα συνιστά στοιχείο της αντικειμενικής τους υπόστασης, όπως η προβολή σε ζωντανή μετάδοση (live streaming) βίντεο σεξουαλικής κακοποίησης ανηλίκων. Επίσης ως γνήσια κυβερνοεγκλήματα – stricto sensu (cyber offences) νοούνται και αυτά, τα οποία στρέφονται εναντίον ηλεκτρονικών δικτύων επικοινωνίας και συστημάτων πληροφοριών δηλ. στην περίπτωση αυτή τα δίκτυα και τα συστήματα αποτελούν τα προσβαλλόμενα αγαθά, όπως επιθέσεις σε βάρος πληροφοριακών συστημάτων. Με τον όρο μη γνήσια κυβερνοεγκλήματα αναφερόμαστε σε παραδοσιακές μορφές εγκλημάτων, όπως η εξύβριση, η δυσφήμιση, η απειλή κ.α οι οποίες δύναται να τελεστούν και μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών δηλ. στην περίπτωση αυτή το διαδίκτυο συνιστά το μέσο τέλεσης (Γερμανός, Γ. και Γεωργίου, Ν., σελ. 71 επ.).

Κατόπιν της προαναφερόμενης βασικής διάκρισης των κυβερνοεγκλημάτων, εν συνεχεία θα αναφερθούμε στα βασικά είδη ηλεκτρονικών εγκλημάτων, τα οποία είτε προέκυψαν από την εξέλιξη του διαδικτύου, είτε προϋπήρχαν, αλλά η εμφάνιση των ηλεκτρονικών υπολογιστών συνέβαλαν στην περαιτέρω ανάπτυξή τους.

Όπως αναφέρεται στην Εθνική Στρατηγική Κυβερνοσφάλειας 2020 - 2025 της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης οι αλματώδεις τεχνολογικές εξελίξεις σε συνδυασμό με την άνοδο του βιοτικού επιπέδου των λαών της Ευρωπαϊκής Ένωσης έχουν ευνοήσει την αύξησης των πάσης φύσεως κυβερνοεπιθέσεων. Από μεμονωμένες απειλές κυβερνοεγκληματιών έως επιθέσεις, οι οποίες φέρεται να προέρχονται από τρίτες χώρες, το συγκεκριμένο περιβάλλον είναι ρευστό και μεταβαλλόμενο, καθιστώντας την αποτελεσματική αντιμετώπιση μία δύσκολη εξίσωση. Για τον λόγο καθίσταται επιτακτική ανάγκη η περιοδική αναθεώρηση της εθνικής και ευρωπαϊκής στρατηγικής (Εθνική Στρατηγική Κυβερνοσφάλειας 2020 -2025, σελ. 10 επ.). Ενόψει και των προαναφερομένων, οι βασικές επιθέσεις, που παρατηρούνται και καταγράφονται, είναι οι ακόλουθες :

i) Hacking – craching

Με τον όρο hacker αναφερόμαστε σε χρήστες υπολογιστών, οι οποίοι είναι γνώστες και έχουν την δυνατότητα να παραβιάζουν συστήματα (δηλ. να σπάνε την ασφάλειά τους, γι’ αυτό και ο όρος craker). Αν θελήσουμε να σκιαγραφήσουμε το προφίλ των hacker θα καταλήξουμε ότι, πρόκειται για άτομα, τα οποία, τις περισσότερες φορές είναι επαγγελματίες, ωστόσο υπάρχουν και αυτοί, οι οποίοι δεν ασχολούνται επαγγελματικά, αλλά έχουν εντρυφήσει και έχουν αποκτήσει εξειδικευμένες γνώσεις. Οι hacker διακρίνονται σε τρεις κατηγορίες : τους black hat, τους white hat και τους grey hat.

Οι black hat hackers είναι χρήστες υπολογιστών, με αυξημένες τεχνικές γνώσεις, οι οποίοι, μεταξύ άλλων, ενεργούν κακόβουλα και συγκεκριμένα οργανώνουν επιθέσεις DOS/DDOS, παρεμβαίνουν σε ιστοσελίδες αναλαμβάνοντας τον έλεγχο και ανεβάζοντας αγενή συνθήματα και υποκλέπτουν προσωπικά δεδομένα χρηστών και στοιχεία ταυτοτήτων.

Οι white hat – ethical hackers εκκινούν με ηθικά κίνητρα, αντίθετα από τους black hat hackers. Διαθέτουν εξειδικευμένες γνώσεις, εργάζονται κυρίως σε εταιρείες και σκοπό έχουν να συμβάλουν στην προστασία των δικτύων υπολογιστών. Δεν είναι παράδοξο και έχει συμβεί ένας black hat hacker να μετεξελιχθεί σε white hat hacker ή και το αντίστροφο. Στην συγκεκριμένη κατηγορία εντάσσονται και οι academic hacker, οι οποίοι στρέφουν το ενδιαφέρον τους στον σχεδιασμό νέων έξυπνων προγραμμάτων.

Τέλος οι grey hat hackers είναι χρήστες μη επαγγελματίες, οι οποίοι κατέχουν βασικές δεξιότητες χρήσης ηλεκτρονικών υπολογιστών. Η συμπεριφορά τους κάποιες φορές αγγίζει τα όρια της παραβατικότητας, όπως χρήση ‘’σπασμένου’’ λογισμικού, κοινή χρήση ταινιών κ.α.

Παρότι, στην κυβερνοτρομοκρατία θα αναφερθούμε αναλυτικά παρακάτω, στο σημείο αυτό θα πρέπει να τονιστεί ότι, οι επιθέσεις χάκερ και οι κινήσεις των χακτιβιστών δεν συνιστούν κυβερνοτρομοκρατία. Ενδεχομένως οι σκοπιμότητές τους να είναι πολιτικές, αλλά δεν προκαλούν σημαντικές βλάβες στο κοινωνικό σύνολο. Οι αλλοιώσεις και οι αποκλεισμοί ιστοσελίδων, που αποτελούν τα μέσα για να περάσουν πολιτικά μηνύματα και θέσεις, συνήθως δεν επιφέρουν ιδιαίτερη ζημία. Είναι προφανές ότι, προκαλείται αναστάτωση, αλλά δεν διασπείρεται φόβος ή κίνδυνος στους πολίτες. Ειδική μνεία στο σημείο αυτό θα πρέπει να κάνουμε στους επιθετικούς κωδικούς, όπως το Code Red worm και ο ιός I LOVE YOU, οι οποίοι ναι μεν είχαν ως αποτέλεσμα ζημιές δισεκατομμυρίων δολαρίων, δεν απείλησαν όμως ανθρώπινες ζωές (Καρυστινού, Β., 2016).

ii) Malware

Με τον όρο malware (σύντμηση των λέξεων malicius και software) αναφερόμαστε σε προγράμματα, τα οποία είναι ικανά να παραβιάσουν την ασφάλεια των ηλεκτρονικών υπολογιστών με σκοπό κυρίως να υποκλέψουν προσωπικά δεδομένα. Οι ηλεκτρονικοί ιοί (viruses), τα ηλεκτρονικά σκουλήκια (worms), καθώς και οι δούρειοι ίπποι (trojan horses) είναι τα συνηθέστερα μέσα παραβίασης ηλεκτρονικών υπολογιστών, μέσω της διασποράς κακόβουλου λογισμικού. Άλλα είδη, λιγότερα συνηθισμένα στην χρήση, είναι τα εξής : λογική βόμβα, βακτήρια, scareware, bots – zombies, rootkits κ.α..

Εν συνεχεία θα παρατεθούν κάποιες ειδικότερες πληροφορίες για τους ιούς, τους δούρειους ίππους και τα ηλεκτρονικά σκουλήκια. Οι ιοί είναι προγράμματα ειδικά σχεδιασμένα, προκειμένου να μολύνουν άλλα προγράμματα. Η δυνατότητα εύκολης και γρήγορης αναπαραγωγής οδηγεί στην τάχιστη μετάδοση, με αποτέλεσμα να προκαλείται δυσλειτουργία ή καθολική καταστροφή συστημάτων. Οι συγκεκριμένοι ιοί δύνανται να μολύνουν τον σκληρό δίσκο του υπολογιστή, να καταστρέψουν διάφορα τμήματα του λογισμικού ή ακόμα και προγράμματα.

Όσον αφορά στους δούρειους ίππους πρόκειται για κακόβουλο λογισμικό, που συνήθως έχει την μορφή παιχνιδιού και στοχεύει στην πραγματικότητα στην υποκλοπή προσωπικών στοιχείων χρηστών του διαδικτύου. Μέσω ενός μυστικού σημείου ο επιτιθέμενος βρίσκει την δυνατότητα εισόδου σε ένα σύστημα, με τα αποτελέσματα, που αναφέρθηκαν ανωτέρω.

Το σκουλήκι είναι και αυτό κακόβουλο λογισμικό, το οποίο αφενός μεν επιβαρύνει το δίκτυο με άχρηστη δραστηριότητα, αφετέρου δε πολλαπλασιάζεται αυτόματα με αποτέλεσμα να αποκτάται πρόσβαση σε προσωπικά στοιχεία.

iii) Spamming

Πρόκειται για μηνύματα ανεπιθύμητης αλληλογραφίας και συγκεκριμένα για μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία απευθύνονται σε πολλαπλούς αποδέκτες και προέρχονται από ανώνυμο αποστολέα. Το οικονομικό κέρδος από αυτήν την δραστηριότητα είναι πολύ μεγάλο για τους spammers και εντοπίζεται στον μικρό αριθμό ανταπόκρισης από τους παραλήπτες. Βέβαια συμβαίνει σε κάποιες περιπτώσεις και υπάρχει η πιθανότητα να πρόκειται για νόμιμη αλληλογραφία, ήτοι όταν πρόκειται για μήνυμα, που ο αποδέκτης έχει επιλέξει να λαμβάνει από τον αποστολέα. Όμως τα μηνύματα spam εκτός από διαφήμιση μπορεί να είναι οικονομικές απάτες, μηνύματα για την διάδοση κακόβουλου λογισμικού κ.α..

Συνεπώς το Spam αποτελεί συνιστά μορφή ανεπιθύμητης επικοινωνίας, που αποστέλλεται μαζικά. Συνήθως είναι ένα email, που απευθύνεται σε πάρα πολλούς παραλήπτες, αλλά δύναται να παραδοθεί και μέσω μηνυμάτων, SMS και κοινωνικών μέσων. Το Spam δεν αποτελεί το ίδιο ένα εργαλείο, αλλά ορισμένες από τις καμπάνιες χρησιμοποιούν τεχνικές, όπως phishing, spearphishing, vishing, smishing ή διάδοση κακόβουλων επισυναπτόμενων αρχείων ή συνδέσμων.

iv) Phishing – pharming

Το phising στα ελληνικά μπορούμε να το αποδώσουμε με τον όρο ηλεκτρονικό ψάρεμα, καθώς πρόκειται για μία διαδικασία, κατά την οποία ο θύτης εμφανίζεται ως αξιόπιστος, προκειμένου να προσελκύσει χρήστες και τελικά να υποκλέψει προσωπικά τους στοιχεία, όπως στοιχεία τραπεζικών λογαριασμών, καρτών κ.α.. Συνήθης περίπτωση και ιδιαίτερα συχνή στην εποχή μας είναι όταν ο χρήστης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου δήθεν από την τράπεζά του, με το οποίο του ζητείται να επιβεβαιώσει τα στοιχεία της ηλεκτρονικής πρόσβασης στον λογαριασμό του, με την αιτιολογία ότι, δήθεν ο λογαριασμός έχει παραβιαστεί ή έχει κλειδωθεί. Στο μήνυμα περιλαμβάνεται και σύνδεσμος, ο οποίος δήθεν οδηγεί στο ασφαλές ηλεκτρονικό περιβάλλον της τράπεζας, πλην όμως το αληθές είναι ότι, τα στοιχεία φθάνουν στον τρίτο, ο οποίος αποκτά έτσι πρόσβαση στον λογαριασμό και αποσπά παρανόμως τα χρήματα του θύματος, δίχως το τελευταίο να αντιλαμβάνεται τι έχει συμβεί.

Το ηλεκτρονικό ψάρεμα αποτελεί λοιπόν μορφή διαδικτυακής επίθεσης, με την οποία ο εγκληματίας επιχειρεί να αποσπάσει ευαίσθητες πληροφορίες από το θύμα. Με το πρόσχημα της αίσθησης επείγοντος ή φόβου το θύμα εξαναγκάζεται να συμμορφωθεί. Σε αυτές τις περιπτώσεις οι αποδέκτες είτε είναι άδηλος αριθμός ανώνυμων χρηστών, είτε εξατομικευμένα θύματα.

Με τον όρο pharming αναφερόμαστε σε προγράμματα, τα οποία έχουν την δυνατότητα να επαναδρομολογούν την κυκλοφορία των δεδομένων και αυτό σημαίνει ότι, ο χρήστης, ο οποίος θέλει να επισκεφθεί μία ιστοσελίδα και να πραγματοποιήσει συναλλαγή οικονομικού περιεχομένου με την

χρήση των προσωπικών του κωδικών, ανακατευθύνεται σε αντίγραφο αυτής. Θεωρώντας ότι, είναι η γνήσια και ασφαλής καταχωρεί τα στοιχεία του με αποτέλεσμα να αποκτάται πρόσβαση σε αυτά από τον θύτη. Επίσης μία άλλη περίπτωση είναι η αποστολή προγραμμάτων μέσω ηλεκτρονικού ταχυδρομείου, τα οποία, εφόσον εγκατασταθούν στον υπολογιστή του θύματος, υποκλέπτουν στοιχεία, με συνέπεια την οικονομική ζημία.

v) Διαδικτυακή τρομοκρατία

Στην εποχή μας η χρήση υπολογιστών έχει επεκταθεί τόσο πολύ, ώστε πλέον να είναι δυνατή και η τέλεση τρομοκρατικών επιθέσεων μέσω αυτών. Εύλογα γεννάται το ερώτημα για ποιο λόγο επιλέγεται το συγκεκριμένο μέσο. Η απάντηση είναι απλή, είναι πιο φθηνό σε σχέση με μία ‘’πραγματική’’ επίθεση, είναι ιδιαίτερα δυσχερές να εντοπιστούν οι δράστες, είναι δυνατή η ταυτόχρονη επίθεση εναντίον πολλών στόχων σε διάφορα μέρη της γης, αποτελεί πρόσφορο μέσο για την διάδοση ιδεών, δεδομένου ότι, εξασφαλίζεται η ανωνυμία και η πραγματική ταυτότητα αυτού που διατυπώνει μία άποψη τρομοκρατικού περιεχομένου.

Η καθηγήτρια ηλεκτρονικών επιστημών και ερευνήτρια της κυβερνοτρομοκρατίας Ντόροθι Ντένινγκ απέδωσε τον εξής ορισμό: «Κυβερνοτρομοκρατία είναι η σύγκλιση του κυβερνοχώρου με την τρομοκρατία. Αφορά παράνομες επιθέσεις εναντίον υπολογιστών, δικτύων και πληροφοριών με σκοπό τον εκφοβισμό μιας κυβέρνηση ή των πολιτών, ώστε να επιτευχθούν πολιτικοί ή κοινωνικοί στόχοι. Επιπλέον, για να μπορεί να χαρακτηριστεί κυβερνοτρομοκρατική μια τέτοια επίθεση πρέπει να οδηγεί σε βία κατά ατόμων ή περιουσιών και να προκαλεί τέτοια ζημιά ώστε να προκαλεί φόβο (δηλ. επιθέσεις που να οδηγούν σε θάνατο ή σωματικές βλάβες, εκρήξεις, ή σημαντικές οικονομικές απώλειες). Σοβαρές επιθέσεις κατά ηλεκτρονικών υποδομών θα μπορούσαν να χαρακτηριστούν κυβερνοτρομοκρατικές ανάλογα με τα κίνητρα και την επίδρασή τους» (Καρυστινού, Β., 2016).

Προκειμένου να διαφανεί το μέγεθος του κινδύνου της κυβερνοτρομοκρατίας, θα πρέπει να παραθέσουμε στο σημείο αυτά τα όσα είχε πει ο τότε υποψήφιος Τζορτζ Μπους πριν την 11η Σεπτεμβρίου και ενόσω ήταν σε εξέλιξη η προεκλογική του εκστρατεία: «Οι Αμερικανικές δυνάμεις είναι ασθενείς και οικονομικά παραμελημένες, την στιγμή που καλούνται να αντιμετωπίσουν μια στρατιά καινούριων απειλών και προκλήσεων: την διάδοση όπλων μαζικής καταστροφής, την ανατολή της κυβερνοτρομοκρατίας, τον πολλαπλασιασμό πυρηνικών εξοπλισμών». Με αφορμή τα ανωτέρω είναι προφανές ότι, τα γεγονότα της 11ης Σεπτεμβρίου προκάλεσαν σοκ σε ολόκληρο τον πλανήτη, πλην όμως μία ξαφνική και σοβαρή κυβερνο-επίθεση δεν αποτελεί πλέον κάτι μακρινό, για τον λόγο αυτό η ανθρωπότητα πρέπει να παραμείνει σε εγρήγορση και να είναι προετοιμασμένη, προκειμένου να δύναται να αντιμετωπίσει τις καταστροφικές της συνέπειες.

vi) Διαδικτυακός εκφοβισμός

Διαδικτυακός εκφοβισμός υφίσταται στην περίπτωση όταν κάποιος παρενοχλεί ένα άτομο χρησιμοποιώντας την τεχνολογία. Η παρενόχληση αυτή μπορεί να επαναλαμβάνεται τακτικά ή όχι και να έχει την μορφή εκφοβισμού, επιθετικότητας, τρομοκρατικής ή αυταρχικής συμπεριφοράς. Οι

μορφές, που μπορεί να λάβει ο διαδικτυακός εκφοβισμός είναι η αποστολή ανήθικων μηνυμάτων, ο αποκλεισμός ατόμων από εφαρμογές συνομιλιών, το hacking ενός ξένου λογαριασμού, η δημοσίευση ενοχλητικών φωτογραφιών, διάδοση προσβλητικών φημών, ειδήσεων, κατηγοριών κ.α.

Το θύμα διαδικτυακού εκφοβισμού βιώνει έντονο άγχος και φόβο, καθότι, τις περισσότερες φορές ο αποστολέας των μηνυμάτων είναι ανώνυμος, ως εκ τούτου δεν γνωρίζει ποιος είναι ο θύτης - ενορχηστρωτής των επιθέσεων. Ένα άλλο χαρακτηριστικό του διαδικτυακού εκφοβισμού είναι ότι, λόγω της χρήσης της τεχνολογίας, μπορεί να τελεστεί οποτεδήποτε και οπουδήποτε, το οποίο σημαίνει ότι, όταν τα μηνύματα ή οι φωτογραφίες δημοσιευθούν στο διαδίκτυο έχουν άμεση πρόσβαση σε αυτά πάρα πολλοί χρήστες, με ό,τι αυτό συνεπάγεται για τα θύματα της επίθεσης. Είναι σημαντικό να ειπωθεί ότι, στον διαδικτυακό εκφοβισμό συνήθως εμπλέκονται πολλά και διαφορετικά άτομα, τα οποία δεν γνωρίζουν πάντα προσωπικά το θύμα.

Προκειμένου να προβούμε σε μία συστηματική αποτύπωση του φαινομένου του διαδικυακού εκφοβισμού, είναι σημαντικό στο σημείο αυτό να αναφερθούμε σε κάποια χαρακτηριστικά, που παρατηρούνται στα προφίλ θυτών και θυμάτων. Οι θύτες περιγράφονται ως άτομα επιθετικά, παρορμητικά, εχθρικά, χωρίς ενσυναίσθηση, τα οποία τείνουν να έχουν τάσεις κυριαρχίας και επιβολής. Επίσης αισθάνονται ανασφάλεια, ανεπάρκεια και κατωτερότητα. Όσον αφορά το οικογενειακό τους περιβάλλον, είναι περιθωριοποιημένοι, με υπερπροστατευτικούς γονείς, οι οποίοι τους έχουν ευνουχίσει και αρκετοί έχουν εγκαταλείψει νωρίς το σχολείο. Τα θύματα είναι κυρίως άτομα απομονωμένα, υπερκινητικά, παχύσαρκα, με διαφορετικό σεξουαλικό προσανατολισμό και κατεξοχήν ανώριμα. Δεν έχουν πολλούς φίλους, δεν είναι δηλαδή δημοφιλείς, ενώ συχνά εμφανίζουν αισθήματα άγχους, απομόνωσης και διακατέχονται από πάρα πολλές φοβίες. Οι επιθέσεις, που δέχονται, τους τραυματίζουν ψυχικά και μάλιστα συχνά κατηγορούν τους εαυτούς τους για όσα τους συμβαίνουν, γι' αυτό και αρκετά θύματα έχουν προσπαθήσει να θέσουν τέλος στην ζωή τους μέσω αυτοχειρίας (Κωνσταντοπούλου, Β., 2018).

vii) Παιδική πορνογραφία

Πρόκειται για μια ιδιαιτέρως ειδεχθή και αποτρόπαια μορφή εγκληματικότητας. Η παιδική πορνογραφία παρότι, λαμβάνει την μορφή, που της προσδίδει η νομοθεσία κάθε χώρας, έχει μία κοινή αφετηρία, ήτοι ότι, καταλαμβάνει τις περιπτώσεις συμμετοχής ανηλίκων παιδιών, τα οποία συμμετέχουν σε διαφόρων ειδών σεξουαλικές αναπαραστάσεις. Στην κατηγορία αυτή εντάσσονται και οι περιπτώσεις, που οι εικόνες αποτελούν προϊόν επεξεργασίας κυρίως από ηλεκτρονικό υπολογιστή.

Από τη δεκαετία του '90, οπότε και άρχισε να σημειώνεται η ραγδαία αύξηση της χρήσης των νέων τεχνολογιών, η παιδική πορνογραφία αποτέλεσε μία ιδιαιτέρως προσοδοφόρα δραστηριότητα, της τάξεως δισεκατομμυρίων δολαρίων. Ιστοσελίδες με κρυπτογραφημένα χαρακτηριστικά, προκειμένου να εξασφαλίζεται η ανωνυμία των πελατών ξεκίνησαν να κάνουν την εμφάνισή τους,

με αποτέλεσμα αυτή την στιγμή να είναι εξαιρετικά δύσκολο να υπολογισθεί (έστω και κατά προσέγγιση) ο συνολικός αριθμός των παράνομων ιστότοπων παιδικής πορνογραφίας, αλλά και τα κέρδη, που απορρεούν από την επισκεψιμότητα σε τέτοιους είδους σελίδες. Σίγουρα βέβαια ομιλούμε για δισεκατομμύρια δολάρια ετησίως με την τάση να είναι δυστυχώς αυξητική.

Η εύκολη και φθηνή προσβασιμότητα στο διαδίκτυο ακόμα για τα παιδιά, τα καθιστούν εύκολο στόχο των παιδόφιλων, οι οποίοι με την χρήση προφανώς ψεύτικων προφίλ τα προσεγγίζουν για να ικανοποιήσουν τα αρρωστημένα πάθη τους. Η πανδημία του κορωνοϊού μεγέθυνε το ήδη οξυμένο πρόβλημα, καθότι, τα παιδιά παρέμεναν κλεισμένα στο σπίτι, συχνά χωρίς την επίβλεψη των γονέων τους, με πρόσβαση όμως στο διαδίκτυο, με αποτέλεσμα τα καταγγελλόμενα περιστατικά να έχουν σημειώσει αύξηση και εξ αυτού του λόγου.

Η Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης προβλέπει τις ακόλουθες μορφές παιδικής πορνογραφίας, ήτοι την συμμετοχή ανηλίκου σε σεξουαλικές δραστηριότητες, την συμμετοχή ατόμου, το οποίο προσποιείται ότι, είναι ανήλικο σε σεξουαλικές δραστηριότητες και τις ρεαλιστικές εικόνες, με ανηλίκους να συμμετέχουν σε σεξουαλικές δραστηριότητες.

Τα κυκλώματα παιδοφιλίας, τα οποία ασχολούνται με την συλλογή και διάδοση πορνογραφικού υλικού, με απώτερο σκοπό την ικανοποίηση των ιδίων, αλλά και τρίτων προσώπων δρουν τις περισσότερες φορές σε περισσότερες από μία χώρες. Η συνεχής διόγκωση του φαινομένου είναι προφανές ότι, έχει θορυβήσει την διεθνή κοινότητα. Μάλιστα και εντός των ευρωπαϊκών τειχών και συγκεκριμένα σε χώρες, όπως η Δανία, η Ισπανία, η Γερμανία, η Ιταλία, η Ολλανδία, η Σουηδία και το Ηνωμένο Βασίλειο δρουν τέτοιου είδους κυκλώματα, τα οποία με την χρήση προηγμένων τεχνολογικών μεθόδων δυσχεραίνουν ιδιαιτέρως τις αρχές να τα εξιχνιάσουν.

Ειδική αναφορά θα πρέπει στο σημείο αυτό να γίνει στα grooming, τα οποία είναι chat rooms, που συμμετέχουν παιδόφιλοι, προσποιούμενοι ότι, είναι παιδιά, προκειμένου να προσελκύσουν ανηλίκους και εν συνεχεία να τους κακοποιήσουν. Ο σχεδιασμός είναι να αναπτύξουν κατ' αρχήν φιλική σχέση με τα πιθανά θύματα, να κερδίσουν την εμπιστοσύνη τους και να αποσπάσουν, όσο γίνεται περισσότερες πληροφορίες σχετικά με τον τόπο κατοικίας τους, το οικογενειακό περιβάλλον τους, τις παρέες τους, τις εξωσχολικές δραστηριότητές τους και τις σεξουαλικές εμπειρίες τους. Μετά το πρώτο αυτό στάδιο αρχίζουν να αποστέλλουν φωτογραφίες σεξουαλικού περιεχομένου, με σκοπό να πείσουν τα υποψήφια θύματα ότι, είναι κάτι αποδεκτό και φυσιολογικό, ενώ χτίζοντας σταδιακά μία στενή επαφή τα αποτρέπουν να μιλήσουν στους γονείς, στους φίλους ή στο σχολείο, η κατάληξη είναι ότι, τελικά αναπτύσσουν αισθήματα ενοχής τα ίδια τα παιδιά.

Προκειμένου να αντιληφθεί κανείς το μέγεθος του προβλήματος της παιδικής πορνογραφίας, θα πρέπει να αναφερθούμε στην επιχείρηση «Ore» στη Βρετανία. Κατόπιν αποστολής από το FBI στοιχείων για 7300 θεωρούμενους ως Βρετανούς κατόχους πιστωτικών καρτών, οι οποίοι ήταν εγγεγραμμένοι σε πορνογραφική ιστοσελίδα, οργανώθηκε επιχείρηση και συνελήφθησαν 1300

άτομα, μεταξύ των οποίων δάσκαλοι, κοινωνικοί λειτουργοί, λειτουργοί παροχής φροντίδων υγείας, γιατροί, στρατιώτες και 50 αστυνομικοί (Φαρσεδάκης, Ι., 2009). Εν συνεχεία και συγκεκριμένα τον Μάιο του 2017, το FBI σε συνεργασία με πολλές ευρωπαϊκές αστυνομίες, κατόρθωσε να επιτύχει εξάρθρωση ενός τεράστιου κυκλώματος στο διαδίκτυο κατόπιν κοπιαστικής έρευνας, η οποία διήρκεσε μεγάλο χρονικό διάστημα. Στο επίκεντρο των ερευνών βρέθηκαν οι διαχειριστές του ιστότοπου Playpen με 150.000 χρήστες παγκοσμίως. Ο συγκεκριμένος ιστότοπος παρείχε στους χρήστες του την δυνατότητα να έχουν πρόσβαση σε υλικό παιδικής πορνογραφίας και σεξουαλικής κακοποίησης παιδιών διαφόρων ηλικιών, δηλαδή νήπια, αιμομιξία κ.α.. (Στεργιούλης, Ε., 2020).

Με αφορμή τα προαναφερόμενα και δεδομένου ότι, στην χώρα μας η κοινωνία έχει ένα σταθερά παραδοσιακό συντηρητικό χαρακτήρα, είναι κρίσιμο η παιδική πορνογραφία να αποτελέσει θέμα συζήτησης στη σχολική κοινότητα καθότι, ειδικά τα τελευταία χρόνια παρατηρείται έξαρση του φαινομένου. Βεβαίως για να συμβεί αυτό και να είναι αποτελεσματικό, είναι επιβεβλημένη η εξειδικευμένη επιμόρφωση των εκπαιδευτικών. Είναι, τέλος, σημαντικό, εκτός από την θέσπιση και την τήρηση ενός αυστηρού νομοθετικού πλαισίου, η πολιτεία σε κεντρικό, περιφερειακό και τοπικό επίπεδο να αναλάβει ενεργό δράση για την καταπολέμηση του φαινομένου, ενώ και ο ρόλος των των ΜΜΕ είναι κρίσιμος και αποφασιστικός κυρίως σε επίπεδο πρόληψης. Κλείνοντας θα πρέπει να τονιστεί ότι, ο εντοπισμός των παιδόφιλων είναι εξαιρετικά δυσχερής διότι, πρόκειται για εγκλήματα με αυξημένο σκοτεινό αριθμό εγκληματικότητας. Σε διεθνές επίπεδο είναι γεγονός ότι, λαμβάνονται πρωτοβουλίες για την καταπολέμηση αυτού του ιδιαιτέρως σοβαρού εγκληματικού φαινομένου, το οποίο έχει παγκόσμιες διαστάσεις, πλην όμως δεν παρατηρείται περιορισμός του.

viii) Οικονομικό έγκλημα

Όταν μιλάμε για διαδικτυακά οικονομικά εγκλήματα αναφερόμαστε κατ' αρχήν σε απάτες με την χρήση υπολογιστών, μέσω των οποίων υποκλέπτονται ή παραποιούνται προσωπικά δεδομένα, με σκοπό το παράνομο οικονομικό κέρδος. Η παραποίηση συνίσταται στην διαγραφή ή στην αλλοίωση δεδομένων προσωπικού χαρακτήρα.

Τα τελευταία χρόνια έχει κάνει την εμφάνισή της μια ιδιαίτερη μορφή οικονομικού εγκλήματος που προσδιορίζεται από τα μέσα τέλεσης ή και από το αντικείμενο της αξιόποινης πράξης, το λεγόμενο ηλεκτρονικο-οικονομικό έγκλημα, το οποίο συνίσταται στην επέμβαση τρίτου σε ηλεκτρονικό υπολογιστή, που έχει ως αποτέλεσμα την προσβολή οικονομικών έννομων αγαθών. Ενδεικτικά στην κατηγορία αυτή εντάσσονται οι εμπορικές απάτες μέσω του ηλεκτρονικού υπολογιστή και του ίντερνετ, η μη εξουσιοδοτημένη πρόσβαση, η βιομηχανική κατασκοπεία, οι πυραμίδες, οι επενδυτικές απάτες, η χειραγώγηση των τιμών μετοχών του χρηματιστηρίου, οι απάτες με πιστωτικές κάρτες, η παράνομη μεταφορά κεφαλαίων από ηλεκτρονικούς τραπεζικούς λογαριασμούς, οι παραβιάσεις πνευματικής ιδιοκτησίας, το ξέπλυμα μαύρου χρήματος στο διαδίκτυο κλπ. (Περπέρης, Α., 2019).

Μία άλλη πτυχή αυτού του φαινομένου είναι ότι, οι σύγχρονες συνθήκες ζωής και η ανάπτυξη της τεχνολογίας συνέβαλαν στην προώθηση των ηλεκτρονικών συναλλαγών και στην άνθηση του ηλεκτρονικού εμπορίου. Πρόκειται για μία μορφή εμπορικών συναλλαγών, η οποία επεκτείνεται όλο και περισσότερο γιατί συνδυάζει την ευκολία και την ταχύτητα (ο καθένας μας με το πάτημα ενός κουμπιού έχει την δυνατότητα να προμηθευτεί διάφορα είδη από όλο τον κόσμο), πλην όμως έχει συνδεθεί, κατά μία έννοια και με το ηλεκτρονικό έγκλημα. Χωρίς βεβαία να υπάρχει διάθεση δαιμονοποίησης του ηλεκτρονικού εμπορίου, αναμφισβήτητα για τον περιορισμό της παράνομης εκμετάλλευσης των ηλεκτρονικών αγορών είναι δεδομένο ότι, απαιτείται συνεργασία της ευρωπαϊκής και της διεθνούς κοινότητας διότι, όπως προειπώθηκε η εγκληματικότητα εντός του κυβερνοχώρου λαμβάνει πολλές και διαφορετικές μορφές.

Εν προκειμένω, όσον αφορά στα οικονομικά εγκλήματα, τα οποία τελούνται μέσω διαδικτύου δεν έχουν μόνο μία μορφή, αλλά διακρίνονται σε περισσότερες κατηγορίες ανάλογα με τον θύτη, το θύμα, το είδος της δραστηριότητας κ.α.. Σημαντική πτυχή αυτού του είδους των παραβατικών συμπεριφορών είναι τα εγκλήματα ‘’λευκού κολάρου’’, ορολογία, της οποίας την πατρότητα έχει ο Αμερικανός εγκληματολόγος E.H. Sutherland (1883-1950), ο εν λόγω μόλις το 1940 αναφέρθηκε στην εγκληματική συμπεριφορά ατόμων με «υψηλή κοινωνική θέση», τα οποία εκδηλώνουν παραβατική συμπεριφορά στα πλαίσια των επαγγελματικών τους δραστηριοτήτων. Αυτό το στοιχείο, δηλ. το υψηλό κοινωνικό status διακρίνει τους συγκεκριμένους παραβάτες από τους προερχόμενους από την κατώτερη κοινωνικοοικονομική τάξη, του «μπλε κολάρου», δηλαδή, αυτούς, που φορούν την φόρμα του εργάτη. Όσον αφορά στο ηλεκτρονικό οικονομικό έγκλημα έχει διαπιστωθεί ότι, άτομα με υψηλή κοινωνική θέση υιοθετούν συχνά τέτοιου είδους εγκληματικές συμπεριφορές καθότι, έχουν την δυνατότητα να διαθέτουν σύγχρονα τεχνολογικά μέσα, ωστόσο αποτελούν εξίσου συχνά και θύματα, διότι, η οικονομική τους επιφάνεια αποτελεί πόλο έλξης επίδοξων εκμεταλλευτών. Εκτός από φυσικά πρόσωπα ακόμα και το ίδιο το κράτος ενδέχεται να αποτελέσει κυρίως το θύμα τέτοιου είδους αξιόποινων πράξεων, που σχετίζονται με το ηλεκτρονικό οικονομικό έγκλημα (Μπρίνιας, 2020).

Το κοινό σημείο αυτού του είδους των εγκλημάτων είναι η παράνομη πρόσβαση και η εν συνεχεία επεξεργασία των στοιχείων τρίτων προσώπων, εν αγνοία τους, με σκοπό την οικονομική εκμετάλλευσή τους. Μία ειδική μορφή, ιδιαίτερα αναπτυγμένη στις σύγχρονες αναπτυγμένες κοινωνίες είναι η οικονομική κατασκοπεία, η οποία συνίσταται στην παράνομη πρόσβαση στα οικονομικά στοιχεία μιας επιχείρησης από συνήθως, δωροδοκούμενο ή εκβιαζόμενο υπάλληλο, για λογαριασμό κάποιας άλλης ανταγωνίστριας επιχείρησης, η οποία αποσκοπεί στην χρησιμοποίησή τους και στην απόκτηση συγκριτικών εταιρικών πλεονεκτημάτων εκ μέρους της.

Άλλη πτυχή του ηλεκτρονικού οικονομικού εγκλήματος είναι και το λεγόμενο «ξέπλυμα βρώμικου χρήματος», δηλαδή η παράνομη διαδικασία νομιμοποίησης εσόδων από προγενέστερη οργανωμένη εγκληματική δραστηριότητα, με προφανή σκοπό το οικονομικό όφελος. Πρόκειται για

μία νέα μορφή νομιμοποίησης εσόδων εντός κυβερνοχώρου, σε σχέση με το πρόσφατο παρελθόν όταν τα παράνομα έσοδα επιχειρείτο να νομιμοποιηθούν κυρίως μέσω της αγοράς ακριβών έργων τέχνης αυτοκινήτων, ακινήτων, κοσμημάτων, επιχειρήσεων κ.α..

Στο σημείο αυτό θα πρέπει να γίνει ειδική αναφορά στην περίπτωση τριών νεαρών Ελλήνων, οι οποίοι το 2014 παρέλυσαν ουσιαστικά το Facebook, με σκοπό να παράγουν bitcoin. Όπως ανέφερε χαρακτηριστικά ο κ. Μανώλης Σφακιανάκης : «Δημιούργησαν έναν ιό, με τον οποίο μόλυναν τόσο τα προφίλ των χρηστών, όσο και των φίλων τους. Μπλοκάροντας το λογισμικό του Facebook, έπιασαν σαν χταπόδι όλο τον κόσμο, με μοναδικό στόχο να κατασκευάσουν το ψηφιακό νόμισμα». Οι συγκεκριμένοι ιδιοφυείς νεαροί, όπως χαρακτηρίστηκαν, διέδωσαν το κακόβουλο λογισμικό lecpetex αποκτώντας έτσι πρόσβαση σε ξένους υπολογιστές και υποκλέπτοντας κωδικούς ηλεκτρονικών ταχυδρομείων, προκειμένου εν συνεχεία να παράγουν bitcoin. Μετά την εξάρθρωση του κυκλώματος το Facebook ευχαρίστησε δημόσια την Ελληνική Αστυνομία και τον έμπειρο υψηλόβαθμο αξιωματικό κ. Μανώλη Σφακιανάκη για τη διαλεύκανση της υπόθεσης και τη σύλληψη των δραστών (Μιχαλοπούλου, Ν., 2017).

Η Ευρωπαϊκή Ένωση έχοντας έλθει αντιμέτωπη με αυτή την νέα μορφή εγκληματικότητας, η οποία θέτει σε κίνδυνο τα οικονομικά συμφέροντα προσώπων και κρατών, επιχείρησε να λάβει πρωτοβουλίες για την αποτελεσματική αντιμετώπιση. Μία στοχευμένη κίνηση προς την κατεύθυνση αυτή αποτελεί η ίδρυση του κέντρου της Europol για το έγκλημα στον κυβερνοχώρο, μέσω της οποίας επιχειρείται να επιτευχθεί η διακρατική αντιμετώπιση του ηλεκτρονικού εγκλήματος (και όχι μόνο του οικονομικού, όπως η απάτη με την χρήση καρτών πληρωμών κ.α.). Με προτεραιότητα την σφυρηλάτηση της συνεργασίας με τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και την χάραξη ενός μακροπρόθεσμου στρατηγικού σχεδιασμού έχουν δημιουργηθεί δύο βασικές ομάδες, ήτοι η ομάδα Ψηφιακής Ανάλυσης, καθώς και η ομάδα Ανάλυσης Εγγράφων. Προκειμένου να διαφανεί η ανάγκη περιορισμού του κυβερνοεγκλήματος θα πρέπει να επισημανθεί ότι, όπως προκύπτει από σχετικές αναλύσεις, κοστίζει στα κράτη-μέλη της Ε.Ε. 265 δισεκατομμύρια ευρώ ανά έτος. Για την παγκόσμια οικονομία το αντίστοιχο ποσό ανέρχεται στα 900 δισεκατομμύρια και αυτό αφορά μόνον το οικονομικό κόστος (Μπρίνιας, 2020).

2.3 Ειδικά χαρακτηριστικά.

Η ραγδαία αύξηση της εγκληματικότητας στον κυβερνοχώρο επιβάλλει και τον εκσυγχρονισμό του ποινικού δικαίου, το οποίο καλείται να ανταποκριθεί σε νέα δεδομένα και προκλήσεις. Είναι προφανές ότι, έγκλημα στον Κυβερνοχώρο έχει κάποια συγκεκριμένα και ιδιαίτερα χαρακτηριστικά, τα οποία και καταδεικνύουν την ανάγκη θέσπισης νέων κανόνων, ανανέωσης των παλαιών και προσαρμογής στις νέες ιδιάζουσες συνθήκες, που έχουν δημιουργηθεί.

Ειδικότερα το κυβερνοέγκλημα τελείται σε μόλις ελάχιστα δευτερόλεπτα, με αποτέλεσμα, τις περισσότερες φορές το θύμα να το αντιλαμβάνεται εκ των υστέρων. Εξ αντιδιαστολής οι θύτες έχουν

βαθειά και άριστη γνώση του διαδικτύου και δρουν ανώνυμα με αποτέλεσμα να τελούν ηλεκτρονικά εγκλήματα, χωρίς να είναι ευχερής η εξιχνίαση και η άσκηση των προβλεπόμενων ποινικών διαδικασιών εναντίον τους. Συγκεκριμένα υπάρχουν κυβερνοεγκληματίες, οι οποίοι έχουν υψηλές τεχνικές γνώσεις και προηγμένες πρακτικές, υπάρχουν όμως και άλλοι αρχάριοι, οι οποίοι επιζητούν εύκολους στόχους, που δεν διαθέτουν μέτρα κυβερνοασφάλειας.

Η κατοχή ενός ηλεκτρονικού υπολογιστή είναι αρκετή, προκειμένου ο θύτης να διαπράξει ένα ηλεκτρονικό έγκλημα, εύκολα και ανέξοδα και εντός του οικείου χώρου του. Όπως έχει ήδη ειπωθεί είναι δυνατόν να τελεστεί εντός ενός ή περισσοτέρων κρατών, γι' αυτό και η διακρατική συνεργασία είναι όχι μόνο σημαντική, αλλά ουσιαστικά επιβεβλημένη, διότι σε αντίθετη περίπτωση η εξιχνίαση είναι ιδιαιτέρως δυσχερής. Τούτο δε διότι, οι προπαρασκευαστικές ενέργειες, οι πράξεις αλλά και τα αποτελέσματα του κυβερνοεγκλήματος συνήθως συντελούνται ταυτοχρόνως σε διαφορετικές χώρες με διακριτές δικαιοδοσίες. Η ανωνυμία του διαδικτύου ένεκα συγκεκριμένων τεχνολογικών υποδομών συνιστά σημαντικό επιβοηθητικό παράγοντα στην δυσχέρεια εντοπισμού του δράστη και στην συγκέντρωση του αποδεικτικού υλικού, γι' αυτό και μεγάλος αριθμός τέτοιου είδους αδικημάτων παραμένει ανεξιχνίαστος. Τέλος το είδος των εγκλημάτων π.χ. παιδική πορνογραφία κ.α. πολλές φορές αποτρέπουν τα θύματα, τα οποία βιώνουν αισθήματα ντροπής από την αναφορά τους ενώπιον των αρμοδίων αρχών, με αποτέλεσμα να μην καταγγέλλονται και συνακόλουθα να μην διώκονται.

Κλείνοντας θα πρέπει να τονιστεί ότι, τα κυβερνοεγκλήματα (αναλόγως της μορφής τους) δύνανται να έχουν σοβαρές και συχνά μη επανορθώσιμες συνέπειες, αφού στρέφονται κατά των περιουσιακών αγαθών, της γενετήσιας αξιοπρέπειας, της ιδιωτικότητας, της ασφάλειας, της υγείας, ακόμα και της ίδιας της ζωής του ατόμου. Εξάλλου, είναι προφανές ότι, αυτού του είδους η εγκληματικότητα συνεχώς εμπλουτίζεται και λαμβάνει διαφορετικές μορφές, το οποίο σημαίνει ότι, αυξάνονται οι πιθανότητες ο καθένας μας να αποτελέσει θύμα.

2.4 Εργαλεία και τεχνικές.

Όπως έχει ήδη αναφερθεί ως άνω και συγκεκριμένα στο κεφάλαιο, εντός του οποίου αναλύθηκαν τα είδη των κυβερνοεγκλημάτων, οι κυβερνοεγκληματίες μετέρχονται συγκεκριμένων τεχνικών και χρησιμοποιούν ειδικά εργαλεία για την τέλεση τέτοιου είδους εγκλημάτων.

Τα κυριότερα εξ αυτών είναι τα παρακάτω :

- το κακόβουλο λογισμικό – επιβλαβές λογισμικό (malicius software / malware ή badware) : πρόκειται για λογισμικό ικανό να βλάψει ένα υπολογιστή με ή χωρίς ξενιστή.

- ο ιός (virus) : έχει την δυνατότητα αντιγραφής με καταστρεπτικά αποτελέσματα και προϋποθέτει την ύπαρξη ξενιστή.

- ο δούρειος ίππος (trojan horse) : πρόκειται για κακόβουλο λογισμικό, που πείθει τον χρήστη ότι, επιτελεί κάποια απαραίτητη λειτουργία, στην πραγματικότητα όμως έχει την δυνατότητα να εγκαταστήσει στον υπολογιστή κακόβουλα προγράμματα, χωρίς να απαιτείται η ύπαρξη ξενιστή.

- το σκουλήκι υπολογιστή (computer worm) : πρόκειται για ένα επίσης κακόβουλο πρόγραμμα υπολογιστή, το οποίο έχει την δυνατότητα να αναπαράγεται και με την χρήση δικτύου υπολογιστών στέλνονται αντίγραφα σε άλλους υπολογιστές, χωρίς να απαιτείται ξενιστής.

- το botnet : πρόκειται για λογισμικό, που μολύνει ξένους υπολογιστές, τους καθιστά υποχείρια (υπολογιστές ‘’ζόμπι’’) και μέσω αυτού πραγματοποιεί επιθέσεις.

- το phishing : πρόκειται για την προσπάθεια απόσπασης ευαίσθητων προσωπικών πληροφοριών του χρήστη (π.χ. ονόματα, κωδικούς πρόσβασης σε προσωπικές υπηρεσίες), από αποστολέα, ο οποίος προσποιείται ότι, είναι αξιόπιστος.

- το e mail spoofing : πρόκειται για αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, τα οποία προέρχονται από πλαστή διεύθυνση.

- το smishing : πρόκειται για την αποστολή μηνυμάτων κινητού τηλεφώνου, τα οποία ομοίως προέρχονται επίσης από πλαστή διεύθυνση.

- το pharming : πρόκειται για την ανακατεύθυνση της επισκεψιμότητας από ένα ιστότοπο σε άλλο πλαστό, ως αποτέλεσμα μιας κυβερνοεπίθεσης.

- dos – ddos attacks : με την χρήση ενός υπολογιστή στόχου επιχειρείται να τεθεί σε λειτουργική αδράνεια ένας άλλος υπολογιστή με την αποστολή μη αποδεκτού όγκου δεδομένων (Καργόπουλος, Α, 2018).

2.5 Είδη κυβερνοεγκληματιών : προφίλ - κίνητρα και βασικά χαρακτηριστικά.

Το διαδίκτυο στις μέρες μας έχει διαδοθεί τόσο πολύ, ώστε πλέον έχουν την δυνατότητα πρόσβασης όλα τα κοινωνικά στρώματα. Προς επίρρωσιν αυτών θα πρέπει να αναφέρουμε ότι, πλέον υπάρχουν 4,66 δισεκατομμύρια ενεργοί χρήστες του διαδικτύου παγκοσμίως, αριθμός που αντιστοιχεί σχεδόν στο 60% του παγκόσμιου πληθυσμού. Προκειμένου να σκιαγραφήσουμε το προφίλ των κυβερνοεγκληματιών θα ξεκινήσουμε από τον ρόλο των κινήτρων ως προς την τέλεση τέτοιου είδους εγκλημάτων. Τα συνηθέστερα κίνητρα των δραστών ηλεκτρονικών εγκλημάτων, τα οποία αποτυπώνουν και τα βασικά χαρακτηριστικά της προσωπικότητάς τους, είναι τα εξής :

i) Απλή διασκέδαση. Στην περίπτωση αυτή ο σκοπός του δράστη δεν είναι να αποκομίσει οικονομικό όφελος, αλλά κυρίως να ‘’διασκεδάσει’’ εις βάρος των άλλων χρηστών. Συνηθέστερη περίπτωση οι νεαρής ηλικίας χάκερ, οι οποίοι αισθάνονται ότι, το διαδίκτυο αποτελεί ένα ‘’παιχνίδι’’ και στην πλειοψηφία τους διαθέτουν προηγμένο τεχνολογικό εξοπλισμό.

ii) Οικονομικό όφελος. Ίσως πλέον να πρόκειται για το συνηθέστερο κίνητρο των κυβερνοεγκληματιών, οι οποίοι επιδιώκουν να αποκτήσουν παράνομη πρόσβαση σε υπολογιστικά συστήματα με σκοπό το αθέμιτο οικονομικό κέρδος. Στο οικείο κεφάλαιο έλαβε χώρα αναφορά σε μορφές ηλεκτρονικών – οικονομικών εγκλημάτων. Οι συγκεκριμένοι κυβερνοεγκληματίες φέρουν τα χαρακτηριστικά του λευκού περιλαιμίου και είναι στην πλειοψηφία τους μορφωμένοι, πλην όμως στην παρούσα φάση αντιμετωπίζουν επαγγελματικά προβλήματα, με πολλούς από αυτούς να έχουν βιώσει μία έντονη επαγγελματική καταστροφή ή απόρριψη.

iii) Ανάγκη κάλυψης συναισθηματικών αναγκών – κενών, όπως είναι τα αισθήματα μειονεξίας, ο θυμός, η εκδίκηση, η ανάγκη διάκρισης και απόκτησης κύρους και προσοχής. Αυτού του είδους οι κυβερνοεγκληματίες εκδηλώνουν παραβατικές συμπεριφορές, όπως είναι η διασπορά ιών, οι επιθέσεις και οι δυσφημίσεις μέσω ψεύτικων κυρίως προφίλ, η εκδικητική πορνογραφία (revenge porn), η τρομοκράτηση ωθούμενοι από αισθήματα εκδίκησης, θυμού, νοσηρής απογοήτευσης και στην πλειοψηφία τους είναι σύζυγοι, σύντροφοι, φίλοι οι οποίοι έχουν εισπράξει την απόρριψη, υπάλληλοι, που απολύθηκαν, πρώην συνεργάτες, έφηβοι, οι οποίοι έχουν βιώσει και οι ίδιοι εκφοβισμό.

iv) Πολιτικά κίνητρα. Η περίπτωση αυτή αναφέρεται σε κυβερνοεπιθέσεις σε ιστοσελίδες και δίκτυα από εξτρεμιστές, οι οποίοι ωθούνται από αισθήματα μίσους και επιχειρούν να διαδώσουν τα προπαγανδιστικά μηνύματά τους, ενώ στην κατηγορία αυτή εντάσσονται και οι επιθέσεις σε κυβερνητικές υπηρεσίες.

v) Σεξουαλικά κίνητρα. Πρόκειται αφενός μεν για τους παιδόφιλους, οι οποίοι διαχειρίζονται υλικό παιδικής πορνογραφίας, που εξασφαλίζουν προσεγγίζοντας ανήλικα και κερδίζοντας αρχικά την εμπιστοσύνη τους, αφετέρου δε για βιαστές – δολοφόνους, οι οποίοι γνωρίζουν τα θύματά τους μέσω του διαδικτύου και κυρίως των μέσων κοινωνικής δικτύωσης, έχουν αρχικά διαδικτυακή επικοινωνία, δημιουργείται εξ αυτού μία σχέση και εν συνεχεία συναντιούνται με την τραγική κατάληξη του βιασμού ή της δολοφονίας.

vi) Ψυχικά ασθενείς, όπως σχιζοφρενείς, παρανοϊκοί, νοσούντες με διπολικοί διαταραχή και άλλες σοβαρές ψυχικές ασθένειες, οι οποίοι προτιμούν τον απρόσωπο χώρο του διαδικτύου για να εκδηλώσουν παραβατικές συμπεριφορές, δεδομένου ότι, στον πραγματικό κόσμο είναι εύκολο να διαπιστωθεί η νοσηρότητά τους (Περπέρης, Α., 2019).

Όπως λέει ο καθηγητής Nedelec η έρευνα του προφίλ των κυβερνοεγκληματιών είναι δυσχερής. Αυτό συμβαίνει διότι, στο διαδίκτυο υπάρχει ανωνυμία. Μάλιστα η μελέτη είναι συνεχής διότι, η τεχνολογική εξέλιξη είναι αλματώδης και σύμφωνα και με άλλους ερευνητές πολλοί κυβερνοεγκληματίες έχουν ως αφετηρία, ιδιαίτερα οι χάκερ, την επιθυμία να βρεθούν σε ένα ηλεκτρονικό σύστημα. Υπάρχουν και αρκετοί άλλοι κυβερνοεγκληματίες, οι οποίοι έχουν επιλέξει να χρησιμοποιούν τις γνώσεις και τις δεξιότητές τους για να αποκομίσουν παράνομο περιουσιακό όφελος. Είναι προφανές λοιπόν ότι, απαιτείται υπόβαθρο για την επιτυχή συμμετοχή στους

περισσότερους τύπους κυβερνοεγκλημάτων, εν αντιθέσει με άλλες μορφές εγκληματικότητας, που η τεχνική εμπειρογνωμοσύνη δεν συνιστά προϋπόθεση (Nedelec, J.).

Ειδική μνεία στο σημείο αυτό θα πρέπει να γίνει στην δράση των κυβερνοεγκληματιών κατά την διάρκεια της πανδημίας του κορωνοϊού. Σε αυτές τις πρωτόγνωρες συνθήκες οι συγκεκριμένοι παραβάτες έχουν καταφέρει να προκαλέσουν μαζικές παραβιάσεις, εκβιάζοντας και αποκτώντας πρόσβαση στα πληροφοριακά συστήματα επιχειρήσεων, ιδιωτών κ.α.. Αυτό συμβαίνει διότι, η χρήση του cloud και των προσωπικών συσκευών για τους σκοπούς της εργασίας εξ αποστάσεως καθιστούν εύκολους στόχους όσους εργάζονται κατ' αυτό τον τρόπο.

Όπως αναφέρεται από την Interpol, το 2020 σημειώθηκε αύξηση στην παραβατικότητα μέσω κακόβουλου λογισμικού τουλάχιστον κατά ένα τρίτο συγκριτικά με το προηγούμενο έτος, ενώ το ηλεκτρονικό ψάρεμα αυξήθηκε τουλάχιστον κατά 50%. Επίσης σε διάστημα τεσσάρων μηνών το 2020 καταγράφηκαν περίπου 907.000 ανεπιθύμητα μηνύματα και 48.000 κακόβουλα URL2. Οι κυβερνοεπιθέσεις κατά την περίοδο της πανδημίας αυξήθηκαν κατά 35%, ενώ αξίζει να σημειωθεί ότι, την ίδια περίοδο οι απόπειρες κυβερνοεπιθέσεων στην ναυτιλία και στην υπεράκτια ενέργεια αυξήθηκαν σε ποσοστό 400% και όσο συνεχίζεται η εξ αποστάσεως εργασία είναι δεδομένο ότι, τα αυξημένα ποσοστά θα διατηρούνται. Τα ανωτέρω επισημαίνονται στο σημείο αυτό διότι, άπτονται της ανάλυσης του προφίλ των κυβερνοεγκληματιών, οι οποίοι είναι προφανές ότι, εκμεταλλεύονται τις εκάστοτε επικρατούσες και ιδίως ιδιάζουσες συνθήκες για την επίτευξη των παράνομων στόχων τους (Cyber Security, 2021).

Μέρος ΙΙ. Η αντεγκληματική Πολιτική ενάντια στο Κυβερνοέγκλημα.

Κεφάλαιο 3 : Η Ποινική Αντιμετώπιση

3.1 Νομικές δυσχέρειες στην αντιμετώπιση του κυβερνοεγκλήματος

Η αντιμετώπιση των εγκλημάτων του κυβερνοχώρου συγκεντρώνει εκ προοιμίου κάποιες σημαντικές δυσχέρειες. Η κυριότερη εξ αυτών είναι ότι, απαιτείται εκ μέρους όλων των εμπλεκομένων, ήτοι από το στάδιο της προδικασίας έως τουλάχιστον την εκδίκαση της κάθε τέτοιου είδους υπόθεση όχι μόνο νομική κατάρτιση, αλλά και τεχνικό υπόβαθρο, μέσω της κατάλληλης εκπαίδευσης, προκειμένου να δύναται να προσεγγιστεί αυτή η νέας μορφής εγκληματικότητα. Εξίσου σημαντικό, το οποίο αντιμετωπίστηκε ως δυσκολία και κατά την εκπόνηση της συγκεκριμένης εργασίας είναι η έλλειψη επαρκούς επιστημονικής βιβλιογραφίας και αρθρογραφίας, η οποία δικαιολογείται καθότι, το κυβερνοέγκλημα, όπως έχει ήδη επισημανθεί, είναι σχετικά πρόσφατο και συνεχώς εναλλάσσεται και εξελίσσεται.

Τα ανωτέρω ζητήματα σε συνδυασμό με την επικράτηση της αγγλικής ορολογίας κυρίως ως προς την απόδοση τεχνικών όρων και ζητημάτων, αλλά και την απουσία εκπαίδευσης των εμπλεκομένων, έχουν δημιουργήσει ένα σημαντικό ζήτημα στην ελληνική έννομη τάξη. Οι ανακριτικές, εισαγγελικές και κυρίως αστυνομικές αρχές των επαρχιακών Εισαγγελιών, όταν έρχονται αντιμέτωπες, με ένα αδίκημα, το οποίο εμφανίζει στοιχεία ηλεκτρονικού εγκλήματος σπεύδουν να διαβιβάσουν την δικογραφία στην Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, η οποία εδρεύει στην Αθήνα (Υποδιεύθυνση εδρεύει και στην Θεσσαλονίκη). Αυτή η τακτική έχει ως αποτέλεσμα την υπερφόρτωση της συγκεκριμένης εξειδικευμένης υπηρεσίας με πληθώρα υποθέσεων, ο χειρισμός των οποίων δεν προϋποθέτει πάντα την ύπαρξη ειδικής τεχνογνωσίας, πέραν των παραδοσιακών δικονομικών τακτικών, που ακολουθούνται σε άλλα εγκλήματα.

Μάλιστα, προκειμένου να περιοριστεί το φαινόμενο αυτό, το οποίο υποδηλώνει και μία γενική απροθυμία ή έστω αδυναμία προσέγγισης τέτοιου είδους ζητημάτων, η Εισαγγελία του Αρείου Πάγου παρενέβη και εξέδωσε την υπ' αριθμ. 2/2019 εγκύκλιό της, με την οποία επισημαίνεται, μεταξύ άλλων ότι, έχει παρατηρηθεί να αποστέλλονται στην Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος το σύνολο σχεδόν των υποθέσεων, που σχετίζονται με τεχνολογίες πληροφορικής και επικοινωνιών, χωρίς κανένα κριτήριο, δηλαδή χωρίς να εξετάζεται η πολυπλοκότητα ή αν απαιτούνται ειδικές γνώσεις για την διενέργεια προκαταρκτικής εξέτασης ή προανάκρισης. Σημειώνεται δε ότι, η τακτική αυτή έχει δυσχεράνει το έργο της συγκεκριμένης υπηρεσίας, με συνέπεια σοβαρές υποθέσεις κυβερνοεγκλημάτων να κωλυσιεργούν ως προς την διερεύνησή τους, ένεκα της αποστολής ποινικών δικογραφιών ήσσονος σημασίας.

Με σκοπό λοιπόν τον περιορισμό αυτού του φαινομένου ζητήθηκε από τον κ. Εισαγγελέα του Αρείου Πάγου η συνδρομή των Εισαγγελικών Αρχών της χώρας, στους οποίους επισημαίνεται ότι, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.), με έδρα την Αθήνα είναι επιφορτισμένη να διερευνά ποινικές υποθέσεις γνήσιων κυβερνοεγκλημάτων (ήτοι αυτών που στρέφονται εναντίον

ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή και με χρήση αυτών (π.χ. άρθρο 370Γ ΠΚ «Παράνομη πρόσβαση σε πληροφοριακό σύστημα», άρθρο 386Α Π.Κ. «Απάτη με Υπολογιστή», άρθρο 292ΑΠ.Κ.«Παρακώλυση λειτουργίας πληροφοριακών συστημάτων», όπως ισχύουν κ.λπ.), καθώς και να ασχολείται με την ανακάλυψη, εξιχνίαση και δίωξη των εγκλημάτων, που διαπράττονται αποκλειστικά και μόνο μέσω του Διαδικτύου.

Απαραίτητη δε προϋπόθεση για την ενασχόληση της συγκεκριμένης υπηρεσίας είναι για την διερεύνηση του εκάστοτε συμβάντος να απαιτούνται ειδικές γνώσεις τεχνικής ή ψηφιακής έρευνας για την άντληση στοιχείων από τον Κυβερνοχώρο, προκειμένου να ταυτοποιηθούν οι αρχικά άγνωστοι δράστες. Μάλιστα στην ως άνω αναφερόμενη εγκύκλιο διαλαμβάνεται μνεία ότι, μετά την ολοκλήρωση των ενεργειών, που απαιτούν ειδικές γνώσεις, όλες οι υπόλοιπες ανακριτικές πράξεις θα πρέπει να συντελούνται από τις αρμόδιες Αστυνομικές Υπηρεσίες, στις οποίες και θα διαβιβάζονται αμελλητί οι δικογραφίες με σκοπό την περαίωσή τους. Ενδεικτικά αναφέρονται οι εξής : λήψη καταθέσεων μαρτύρων, απολογιών κατηγορουμένων, ανωμοτί υπόπτων, ταυτοποίηση στοιχείων, φυσική εξακρίβωση, εγχείρηση εγγράφων, απλή περιήγηση στο διαδίκτυο, εκτύπωση στοιχείων και αρχείων από διαδίκτυο, ψηφιακό δίσκο ή USB, διενέργεια απομαγνητοφωνήσεων τηλεφωνικών συνδιαλέξεων, οι οποίες έχουν καταγραφεί στα πλαίσια ποινικής έρευνας κ.α. (Εγκύκλιος ΕισΑΠ, 2019).

3.2. Ζητήματα δικαιοδοσίας

Το κυβερνοέγκλημα, όπως έχει ήδη αναλυθεί, έχει την δυνατότητα να υπερβαίνει σύνορα και να εξελίσσεται διαρκώς. Αυτός είναι ο λόγος, που δεν είναι δυνατόν, να μιλάμε για αποτελεσματική αντιμετώπιση αποκλειστικά και μόνο σε εθνικό επίπεδο.

Όσον αφορά ειδικότερα στην συλλογή των ηλεκτρονικών αποδείξεων είναι ιδιαιτέρως δυσχερής, διότι, τα δεδομένα μεταβάλλονται και οι ειδικές γνώσεις αποτελούν αναγκαία προϋπόθεση. Για την υπερπήδηση αυτών των δυσχερειών επιβάλλεται διεθνής δικαστική συνεργασία, η οποία όμως συχνά παρεμποδίζεται από τις αποκλίσεις στις εθνικές έννομες τάξεις και τις συγκρούσεις δικαιοδοσίας. Το κυβερνοέγκλημα ωστόσο, ένεκα των ειδικών χαρακτηριστικών του, ανατρέπει στην πράξη τις κλασσικές θεωρίες περί εδαφικότητας και εθνικής δικαιοδοσίας, λόγω του υπερεθνικού χαρακτήρα του κυβερνοχώρου.

Προς την κατεύθυνση αυτή, η «Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο» έχει ως σκοπό, μεταξύ άλλων, την προώθηση της διακρατικής συνεργασίας μεταξύ των κρατών – μελών για την καταπολέμηση του κυβερνοεγκλήματος, με την βασική επισήμανση ότι, αυτά θα πρέπει να διαθέτουν τα κατάλληλα εργαλεία για τον εντοπισμό, τη διερεύνηση και τη δίωξη του κυβερνοεγκλήματος.

Ενόψει των προαναφερομένων, κομβικής σημασίας καθίσταται ο ρόλος της Eurojust, η οποία με σκοπό την αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος, προωθεί την διακρατική συνεργασία. Με γνώμονα την γρήγορη ολοκλήρωση των δικαστικών αιτημάτων, δεδομένου ότι, ομιλούμε για διαφορετικές εσωτερικές έννομες τάξεις και την άμεση συμμετοχή της δικαστικής εξουσίας σε επιχειρήσεις κυβερνοεγκλήματος, επιχειρείται να διασφαλιστεί η συλλογή δεδομένων, τα οποία δύνανται να αποτελέσουν παραδεκτά ηλεκτρονικά αποδεικτικά στοιχεία σε μεταγενέστερες δικαστικές διαδικασίες (Eurojust, Συνοπτική Παρουσίαση, 2020).

Κλείνοντας ειδική μνεία θα πρέπει να γίνει στο άρθρο 1 του Ν. 4285/2014, το οποίο προστέθηκε μετά το άρθρο 2 του Ν. 927/1979 και προβλέπει ότι, όταν οι πράξεις των προηγουμένων άρθρων (σημ. Καταπολέμηση ρατσισμού) τελούνται μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, τόπος τέλεσης θεωρείται και η Ελληνική Επικράτεια, εφόσον στο έδαφος της παρέχεται πρόσβαση στα συγκεκριμένα μέσα, ανεξάρτητα από τον τόπο εγκατάστασής τους. Με την προσθήκη αυτή επιχειρείται να αρθούν τυχόν αμφισβητήσεις δικαιοδοσίας και εγκαθιδρύεται η ελληνική ανεξάρτητα από το εάν ο δράστης χρησιμοποιεί για την πράξη του υλικό, που φιλοξενείται σε σύστημα πληροφορικής εγκατεστημένο στη χώρα, καθώς και όταν το υλικό που χρησιμοποιεί φιλοξενείται σε σύστημα πληροφορικής που βρίσκεται στην Ελλάδα, ανεξάρτητα από το αν αυτός βρίσκεται στο έδαφος της Επικράτειας (βλ. Αιτιολογική Έκθεση Ν. 4285/2014, άρθρα 2 και 3).

3.3 Ηλεκτρονική απόδειξη

Για την αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος είναι ιδιαίτερης σημασίας η ηλεκτρονική απόδειξη. Τα τρία συνηθέστερα είδη ηλεκτρονικών αποδείξεων, των οποίων δύναται να γίνει χρήση στα πλαίσια νομίμων διαδικασιών, είναι τα εξής : α) υλικό από δημόσιες ιστοσελίδες και μέσα κοινωνικής δικτύωσης, με δυνατότητα πρόσβασης στον οποιονδήποτε, β) ηλεκτρονικά μηνύματα και έγγραφα σε ψηφιακή μορφή, χωρίς γενική δυνατότητα πρόσβασης και γ) δεδομένα, η προσεκτική χρήση των οποίων είναι δυνατόν να οδηγήσει στην πηγή, αλλά όχι στο περιεχόμενο επικοινωνίας ενός ατόμου. Επίσης αντικείμενο ηλεκτρονικής απόδειξης μπορεί να αποτελέσει ένα κείμενο, μία εικόνα, μία φωτογραφία κ.α.. Πηγές προέλευσης δεδομένων δύνανται να αποτελέσουν κινητά τηλέφωνα, ηλεκτρονικοί υπολογιστές, ιστοσελίδες κ.α.. Όσον αφορά στο μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) αποτελεί ηλεκτρονική απόδειξη, καθότι προέρχεται από ένα ηλεκτρονικό σύστημα και περιλαμβάνει μεταδεδομένα, δηλ. δεδομένα, τα οποία προέρχονται από άλλα δεδομένα (Μιχαηλίδου, Χ., 2018).

Η ψηφιακή απόδειξη είναι ιδιαιτέρως κρίσιμη για την εξιχνίαση του κυβερνοεγκλήματος, αλλά και για την καταδίκη του κυβερνοεγκληματία. Στην πρώτη φάση της διερεύνησης πιθανές ενέργειες είναι η ανάλυση ύποπτου λογισμικού, η ανάκτηση σβησμένων ή κατεστραμμένων αρχείων, η αποκωδικοποίηση, η αναγνώριση χρηστών μέσω δεδομένων κίνησης κ.α.. Στην δεύτερη φάση

αναφερόμαστε στην παρουσίαση (είτε μέσω εκτύπωσης, είτε μέσω ηλεκτρονικών μέσων) της ψηφιακής απόδειξης μέσα στις δικαστικές αίθουσες, προκειμένου να συνεκτιμηθεί με τα υπόλοιπα συνήθη αποδεικτικά στοιχεία.

Προκειμένου να διαφανεί η χρησιμότητα των ψηφιακών αποτυπωμάτων, θα παρατεθούν κάποια συνήθη παραδείγματα : ύποπτος, για την τέλεση του αδικήματος της παιδικής πορνογραφίας δύναται να εντοπισθεί μέσω των μηχανών αναζήτησης τέτοιου είδους διαδικτυακών σελίδων. Μάλιστα ψηφιακές κάμερες, που υπάρχουν για την παραγωγή συναφούς οπτικού υλικού περιλαμβάνουν ειδικές πληροφορίες, τις οποίες, εάν εντοπίσουν, οι αρμόδιες αρχές, δύνανται να οδηγηθούν στην τοποθεσία λήψης τους. Επίσης οι κυβερνοεγκληματίες, οι οποίοι αναζητούν και κατεβάζουν πορνογραφικό υλικό, δύνανται να εντοπιστούν από την μοναδική ταυτότητα που παράγεται κατά την εγκατάσταση του λογισμικού διαμοιρασμού των αρχείων (Μιχαηλίδου, Χ., 2018).

3.4 Ευρωπαϊκή και Ελληνική Νομοθεσία

i) Η διάταξη του άρθρου 19 του Συντάγματος

Στο άρθρο 19 Συντάγματος ορίζεται ότι, το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Τα ζητήματα της άρσης του απορρήτου κατόπιν διατάξεων των Εισαγγελικών και Δικαστικών Αρχών τα ρύθμισε κατ' αρχήν ο εκτελεστικός του άρθρου 19 παρ.1 του Συντάγματος νόμος. Πρόκειται για τον Ν. 2225/1994 (ΦΕΚ 121Α). Στο άρθρο 3 αυτού ορίζονται τα της άρσεως του απορρήτου των επικοινωνιών για λόγους εθνικής ασφάλειας, ενώ στο άρθρο 4 τα της άρσεως του απορρήτου για την διακρίβωση σοβαρών εγκλημάτων.

Η ιδιωτική σφαίρα του ατόμου περιλαμβάνει πρωτίστως τις ιδιωτικές του σχέσεις, ακριβώς επειδή οι σχέσεις αυτές συνεπάγονται την επικοινωνία με την μορφή αποστολής κάθε είδους μηνυμάτων. Ο γνώμονας είναι η ανάγκη προστασίας της ιδιωτικής σφαίρας και κατ' επέκταση της μεταβίβασης μηνυμάτων από τις παρεμβάσεις της δημόσιας αρχής ιδίως ως προς την παραβίαση της μυστικότητας και της εμπιστευτικότητας του απορρήτου των μηνυμάτων. Θα πρέπει να τονιστεί ότι, αντικείμενο προστασίας δεν είναι το μήνυμα καθ' εαυτό, το οποίο ούτως ή άλλως προστατεύεται από το άρθρο 14 του Συντάγματος, που προστατεύει την ελευθερία έκφρασης και διάδοσης της γνώμης, αλλά το απόρρητο του μηνύματος (Δαγτόγλου, Π., σελ. 350 επ.).

Η συγκεκριμένη προστασία του απορρήτου περιλαμβάνει όχι μόνο τα γραπτά μηνύματα, αλλά και κάθε μορφής ιδιωτικής μη δημόσιας επικοινωνίας (τηλεφωνήματα κ.α.). Βέβαια εν προκειμένω γεννώνται διάφορα ζητήματα π.χ. όταν ο ίδιος ο αποστολέας επιθυμεί την δημοσιότητα αυτής, όπως συμβαίνει στην περίπτωση μιας ανοικτής δημόσιας επιστολής στα μέσα κοινωνικής

δικτύωσης, μίας δημοσιευμένης διαφήμισης, μίας αγγελίας κ.α.. Στην περίπτωση αυτή δεν τυγχάνει εφαρμογής το άρθρο 19 του Συντάγματος, το οποίο προϋποθέτει εμπιστευτική μορφή επικοινωνίας. Είναι εξάλλου προφανές ότι, προστατεύεται κάθε ιδιωτική επικοινωνία ανεξαρτήτως του προσωπικού ή επαγγελματικού χαρακτήρα της (Δαγτόγλου, Π., σελ. 350 επ.).

Βεβαίως, όπως έχει ήδη ειπωθεί, υφίστανται απαγορεύσεις για την εμπιστευτικότητα του απορρήτου της επικοινωνία, στις περιπτώσεις, που υφίσταται αντίθεση στους νόμους, την δημόσια τάξη, την ασφάλεια του κράτους και τα χρηστά ήθη. Το ίδιο το Σύνταγμα θέτει τα όρια για την αποδέσμευση των δικαστικών και εισαγγελικών αρχών από το απόρρητο της επικοινωνίας. Είναι αυτονόητο όμως ότι, προς αποφυγή περιπτώσεων καταστρατήγησης του Συντάγματος απαιτείται να τηρούνται οι ανάλογες εγγυήσεις (Δαγτόγλου, Π., σελ. 355 επ.).

Όσον αφορά στις ηλεκτρονικές επικοινωνίες, σύμφωνα με την νομοθεσία, απόρρητα θεωρούνται: 1) Το περιεχόμενο της επικοινωνίας (περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων), 2) η ταυτότητα του καλούντος και του καλουμένου, παραλήπτη και αποστολέα και 3) τα δεδομένα θέσης της τερματικής συσκευής (γεωγραφικός εντοπισμός). Η διαδικασία για τη νόμιμη άρση του απορρήτου καθορίζεται λεπτομερώς στην ισχύουσα νομοθεσία και συγκεκριμένα στον Ν. 2225/1994, Ν. 3115/2003, Ν.3674/2008, Ν.3917/2011, ΠΔ47/2005. Να σημειωθεί τέλος ότι, η παραβίαση της νομοθεσίας περί απορρήτου των επικοινωνιών συνεπάγεται την επιβολή διοικητικών κυρώσεων εις βάρος παρόχων ηλεκτρονικών επικοινωνιών, οι οποίες αναλόγως της βαρύτητας δύνανται να λάβουν την μορφή σύστασης, χρηματικού προστίμου, ανάκλησης του δικαιώματος παροχής υπηρεσιών από την ΑΔΑΕ και άλλες Δημόσιες Αρχές. Επομένως, κάθε χρήστης υπηρεσιών ηλεκτρονικών επικοινωνιών έχει την δυνατότητα, εάν παραβιάζεται το απόρρητο της επικοινωνίας του, να αιτηθεί έννομη προστασία (Lawspot, 2018).

ii) Το Ευρωπαϊκό και Διεθνές πλαίσιο και η Ελληνική νομοθεσία ενσωμάτωσης

Στο σημείο αυτό της εργασίας κρίνεται σκόπιμο να λάβει χώρα μία αναλυτική απαρίθμηση των νομοθετημάτων (εθνικών, υπερεθνικών, νόμων οδηγιών κ.α.), τα οποία σχετίζονται με την καταπολέμηση του κυβερνοεγκλήματος. Χρήσιμος οδηγός σε αυτήν την προσπάθεια αποτελεί η καταγραφή του Αλεξάνδρου – Ιωάννη Καργόπουλου, Πρωτοδίκη, Εθνικού Εμπειρογνώμονα στον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ε.Ε., στα πλαίσια της εκπαίδευσης των Δικαστικών και Εισαγγελικών Λειτουργών στην Εθνική Σχολή Δικαστών (Καργόπουλος, Α., 2018).

Σημαντικό επίτευγμα για την καταπολέμηση του κυβερνοεγκλήματος συνιστά η Σύμβαση της Βουδαπέστης (23-11-2001) και το Πρόσθετο Πρωτόκολλο αυτής (28-01-2003). Επίσης σε ευρωπαϊκό επίπεδο συναντούμε αρκετές οδηγίες, οι οποίες στοχεύουν στην αντιμετώπιση ειδικών μορφών κυβερνοεγκλήματος, όπως η Οδηγία 2011/93/ΕΕ για την παιδική πορνογραφία, η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά πληροφοριακών συστημάτων και η Οδηγία 2017/541 για την καταπολέμηση της τρομοκρατίας.

Ειδικότερα στην πρώτη κατά σειρά Οδηγία, η οποία αναφέρεται στην παιδική πορνογραφία ορίζεται στο άρθρο 5 παρ. 3 ότι, η εν γνώσει απόκτηση πρόσβασης σε παιδική πορνογραφία μέσω της τεχνολογίας των επικοινωνιών και πληροφοριών τιμωρείται με στερητική της ελευθερίας ποινή το ανώτατο όριο της οποίας ανέρχεται σε τουλάχιστον ένα έτος. Στο άρθρο 348Α Π.Κ. ορίζεται ότι, όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή, ενώ στις επόμενες παραγράφους προβλέπονται και οι επιβαρυντικές περιστάσεις. Σημειωτέον ότι, το ανωτέρω άρθρο εμπεριέχεται στον Ν. 4267/2014, ο οποίος ψηφίστηκε, με σκοπό την ενσωμάτωση της Οδηγίας 2011/93/ΕΕ.

Η Οδηγία 2017/541 για την καταπολέμηση της τρομοκρατίας αναφέρεται σε συμπεριφορές συνδεόμενες ιδίως με αλλοδαπούς τρομοκράτες μαχητές και την χρηματοδότηση της τρομοκρατίας, οι οποίες μορφές θα πρέπει να τιμωρούνται και όταν τελούνται και μέσω του διαδικτύου, ενώ διαλαμβάνονται αναφορές και για την στρατολόγηση, αλλά και για την διάδοση μηνυμάτων μέσω του διαδικτύου. Είναι προφανές ότι, η συγκεκριμένη Οδηγία αποτελεί προϊόν της ανάγκης για προστασία ενάντια σε τρομοκρατικές επιθέσεις, οι οποίες τα τελευταία χρόνια έχουν σημειωθεί σε πολλές ευρωπαϊκές χώρες (βλ. Γαλλία, Γερμανία κ.α.).

Επίσης ειδικής μνείας θα πρέπει να τύχει η Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά πληροφοριακών συστημάτων, στο προοίμιο της οποίας αναφέρεται ότι, η σύμβαση αποτελεί το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών. Η συγκεκριμένη Οδηγία στηρίζεται σε ένα βαθμό στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο του 2001, η οποία χρησιμεύει ως πρότυπο για την εθνική και την περιφερειακή νομοθεσία και δημιουργεί κοινή βάση συνεργασίας εντός της ΕΕ, αλλά και πέραν αυτής. Αναφέρεται στην παράνομη πρόσβαση (α. 3), στην παράνομη υποκλοπή (α. 6), στην παράνομη παρεμβολή σε δεδομένα (α. 5), στην παράνομη παρεμβολή σε σύστημα (α. 4) και σε εργαλεία, που χρησιμοποιούνται για την διάπραξη τέτοιου είδους αδικημάτων. Μάλιστα για την καλύτερη καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η Οδηγία απευθύνει έκκληση για περισσότερη διεθνή συνεργασία μεταξύ των δικαστικών αρχών και των αρχών επιβολής του νόμου (LAWSPOT, 2017).

Όσον αφορά στην Σύμβαση της Βουδαπέστης για το κυβερνοέγκλημα θα πρέπει να γίνουν κάποιες επισημάνσεις. Στα άρθρα 2-6 λαμβάνει χώρα αναφορά σε αδικήματα κατά της ασφάλειας, της ακεραιότητας και της λειτουργίας των ψηφιακών δεδομένων και των πληροφοριακών συστημάτων, όπως η παράνομη πρόσβαση (α. 2), η υποκλοπή (α. 3), οι παρεμβολές σε δεδομένα (α. 4), οι παρεμβολές σε συστήματα (α. 5) και η αθέμιτη χρήση συσκευών (α. 6). Στα άρθρα 7-10

απαριθμούνται αδικήματα, τα οποία τελούνται με την χρήση υπολογιστών, όπως η πλαστογραφία σχετικά με υπολογιστές (α. 7), η απάτη σχετικά με υπολογιστές (α. 8), η παιδική πορνογραφία με χρήση υπολογιστή (α. 9), οι παραβιάσεις της πνευματικής ιδιοκτησίας με χρήση υπολογιστή (α. 10). Η Σύμβαση της Βουδαπέστης χαρακτηρίζεται από ουδέτερη γλώσσα και ορολογία και γίνεται προσπάθεια να συμπεριλάβει και τις μελλοντικές τεχνολογίες, δεδομένης και της συνεχούς εξέλιξης του κυβερνοεγκλήματος. Αποσκοπεί επίσης στην εναρμόνιση των νομοθεσιών των κρατών – μελών, στον εμπλουτισμό των δικονομικών διατάξεων με νέες μεθόδους και στην ισχυροποίηση των διακρατικών συνεργασιών, στην προώθηση της δικαστικής συνδρομής και στην εγκαθίδρυση ενός δικτύου, το οποίο θα λειτουργεί σε εικοσιτετράωρη βάση (Καργόπουλος, Α., 2018).

iii) Το ισχύον Ελληνικό Νομοθετικό Πλαίσιο

Ο Ν. 4411/2016 αναφέρεται στην «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών – Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».

Όπως αναφέρεται στην αιτιολογική του έκθεση η ραγδαία ανάπτυξη της χρήσης του Διαδικτύου (Internet), η ψηφιοποίηση, η σύγκλιση και η εκτεταμένη διασύνδεση των συστημάτων πληροφοριών, παρέχουν σημαντική διευκόλυνση στη διάπραξη ποινικών αδικημάτων διασυνοριακού χαρακτήρα, για τους λόγους αυτούς κρίνεται επιβεβλημένη η προσαρμογή των εθνικών νομοθεσιών των κρατών – μελών στα νέα δεδομένα και η προώθηση των διακρατικών συνεργασιών (βλ. Αιτιολογική Έκθεση και συγκεκριμένα Προοίμιο Ν. 4411/2016). Ειδικότερα μετά την ψήφιση του ανωτέρω νομοθετήματος στον Ελληνικό Ποινικό Κώδικα συμπεριλήφθησαν διατάξεις, οι οποίες σχετίζονται με τον περιορισμό του κυβερνοεγκλήματος και συγκεκριμένα μεταξύ άλλων το άρθρο 370Γ παρ. 2 Π.Κ. για την παράνομη πρόσβαση σε πληροφοριακά συστήματα σε συνδυασμό με το άρθρο 370Δ για την παράνομη αντιγραφή προγραμμάτων υπολογιστών, το άρθρο 292 Β Π.Κ. για την παρακώλυση λειτουργίας των πληροφοριακών συστημάτων, το άρθρο 370Ε Π.Κ. για την παρακολούθηση, αποτύπωση μη δημοσίων διαβιβάσεων δεδομένων, το άρθρο 386Α Π.Κ. για την απάτη με υπολογιστή, το άρθρο 348 Α Π.Κ. για την πορνογραφία ανηλίκων (Καργόπουλος, Α., 2018).

Είναι προφανές ότι, η Ελληνική Νομοθεσία έχει εκσυγχρονιστεί και έχει εναρμονιστεί στα νέα δεδομένα, όσον αφορά στο κυβερνοέγκλημα. Ωστόσο οι προαναφερόμενες ποινικές προβλέψεις δεν αρκούν για την αποτελεσματική αντιμετώπιση αυτής της πολυεπίπεδης εγκληματικότητας, η οποία, όπως έχει ήδη επισημανθεί, συνεχώς εξελίσσεται και εφευρίσκει νέες μεθόδους. Υπάρχουν και ειδικές μορφές, όπως η διασπορά κακόβουλου λογισμικού, για την οποία δεν εμπεριέχεται ειδική

πρόβλεψη στην ελληνική νομοθεσία και αντιμετωπίζεται με την εφαρμογή του ισχύοντος νομοθετικού πλαισίου. Με αυτές τις σκέψεις είναι προφανές ότι, απαιτούνται και άλλες νομοθετικές παρεμβάσεις και περαιτέρω εναρμόνιση της εθνικής νομοθεσίας με τα ευρωπαϊκά δεδομένα, ιδίως για την προστασία των περισσότερο ευάλωτων πολιτών (όπως παιδιά, οικονομικά αδύναμους κ.α.). Προς επίρρωσιν αυτών έχει ιδιαίτερη σημασία να παρατεθεί η άποψη της Ίλβα Γιόχανσον, Επιτρόπου Εσωτερικών Υποθέσεων της ΕΕ, η οποία σε δελτίο τύπου, μεταξύ άλλων, αναφέρει τα εξής, με αφορμή της πανδημία του κορωνοϊού και το κυβερνοέγκλημα : "Η πανδημία του νέου κορονοϊού επιβράδυνε πολλές πλευρές της φυσιολογικής ζωής μας. Όμως, δυστυχώς, επιτάχυνε την εγκληματική δραστηριότητα στο διαδίκτυο. Το οργανωμένο έγκλημα εκμεταλλεύεται τους ευάλωτους ανθρώπους, δηλαδή ανθρώπους που μόλις βγήκανε στην ανεργία, εκτεθειμένες επιχειρήσεις ή το χειρότερο όλων παιδιά" (CAPITAL.gr, 2020).

Κεφάλαιο 4 : Φορείς Αντιμετώπισης

4.1 Ελληνικοί φορείς

i) Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Με το Π.Δ. 178/2014 ιδρύθηκε η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Αθήνα και η Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με έδρα την Θεσσαλονίκη. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει ως σκοπό την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που τελούνται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής κεντρική Υπηρεσία και υπάγεται απευθείας στον κ. Αρχηγό της Ελληνικής Αστυνομίας. Στην νέα αναβαθμισμένη δομή της αποτελείται από τα εξής τμήματα : α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και ε. Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων (astynomia.gr).

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, στην οποία έχει γίνει αναφορά και σε άλλα κεφάλαια της παρούσης, έχει καταφέρει να εξιχνιάσει πάρα πολλές υποθέσεις κυβερνοεγκλημάτων στην χώρα μας, οι οποίες σχετίζονται κυρίως με διαδικτυακές απάτες, παιδική πορνογραφία, υποθέσεις παράνομου στοιχηματισμού και τυχερών παιχνιδιών μέσω διαδικτύου, οικονομικής εξαπάτησης των πολιτών, μέσω αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου εκβιαστικού περιεχομένου, απάτες σεξουαλικής εκβίασης κ.α.. Τέλος πολύ συχνά με ανακοινώσεις της στα Μέσα μαζικής ενημέρωσης και στα μέσα κοινωνικής δικτύωσης επιδιώκει να ευαισθητοποιήσει και εφιστά την προσοχή των πολιτών σε τέτοιου είδους φαινόμενα, τα οποία πλέον σημειώνονται σε σχεδόν καθημερινή βάση.

ii) Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Σύμφωνα με την διάταξη του άρθρου 1 του Ν. 3115/2003, η οποία τελεί σε εναρμόνιση με την παράγραφο 2 του άρθρου 19 του Συντάγματος, συστάθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών. Η αποστολή της εν λόγω Αρχής, η οποία είναι συνταγματικά κατοχυρωμένη, είναι η προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και η ασφάλεια των δικτύων και πληροφοριών. Στα πλαίσια των αρμοδιοτήτων της εντάσσεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, σύμφωνα με τα οριζόμενα στις οικείες νομοθετικές διατάξεις.

Η ΑΔΑΕ ως ανεξάρτητη αρχή διατηρεί την διοικητική της αυτοτέλειας και εδρεύει στην Αθήνα. Οι αποφάσεις της κοινοποιούνται στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους

υποβάλλεται Έκθεση των ετήσιων πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης, στους αρχηγούς των κοινοβουλευτικών κομμάτων και στο Ευρωπαϊκό Κοινοβούλιο. Επίσης η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο, σύμφωνα τα όσα προβλέπονται στον Κανονισμό της Βουλής.

Πρόσφατα και αυτό έχει ξεχωριστό ενδιαφέρον ο Χρήστος Ράμμος, Πρόεδρος της Αρχής Διασφαλίσεως του Απορρήτου των Επικοινωνιών, Αντιπρόεδρος του Συμβουλίου της Επικρατείας ε.τ. και άλλα δύο μέλη ήγειραν επιφυλάξεις σχετικά με τα προβλήματα συμβατότητας με υπέρτερης τυπικής ισχύος κανόνες δικαίου της προσφάτως ψηφισθείσης από την Βουλή διατάξεως του άρθρου 87 του Ν. 4790/2021. Με την συγκεκριμένη διάταξη διατηρείται, κατ' αρχήν η αρμοδιότητα της ΑΔΑΕ, να γνωστοποιεί σε εκείνους, το απόρρητο των οποίων ήρθη για την διακρίβωση κακουργημάτων (άρθρο 4 του Ν. 2225/1994), την επιβολή του μέτρου, μετά την λήξη του και υπό την προϋπόθεση ότι, δεν διακυβεύεται ο σκοπός, για τον οποίο είχε διαταχθεί, υπό την επιπρόσθετη, όμως, προϋπόθεση ότι πρέπει, εφεξής, να προηγείται της σχετικής απόφασης της ΑΔΑΕ η σύμφωνη γνώμη του Εισαγγελέα του Αρείου Πάγου. Με την ίδια, όμως, διάταξη ρητώς καταργείται, πλέον και σε κάθε περίπτωση η αρμοδιότητα της ΑΔΑΕ να γνωστοποιεί την λήψη του μέτρου της άρσης, μετά την λήξη αυτής, ακόμη και αν δεν διακυβεύεται πλέον ο σκοπός για τον οποίο διατάχθηκε, στις περιπτώσεις, που η λήψη του μέτρου είχε γίνει για λόγους εθνικής ασφάλειας (άρθρο 3 του Ν. 2225/1994).

Όπως όμως ρητώς επισημαίνεται από τον Πρόεδρο και τα δύο άλλα μέλη της Αρχής, η εν λόγω νομοθετική πρόβλεψη είναι πολύ πιθανόν να δημιουργήσει σοβαρά ζητήματα συμβατότητας με την συνταγματική διάταξη του άρθρου 19 παρ. 1 (προστασία του απορρήτου των επικοινωνιών στην οποία έγινε αναφορά ανωτέρω) και με την διάταξη του άρθρου 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) και τέλος με το άρθρο 7 (Σεβασμός της Ιδιωτικής και Οικογενειακής Ζωής) του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Ειδικότερα σε αρκετές περιπτώσεις έχει κριθεί από το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) ότι, εάν ο θιγόμενος δεν πληροφορηθεί ότι, στο παρελθόν ήρθη το απόρρητο το επικοινωνιών του, αποστερείται παντελώς της δυνατότητας να αιτηθεί δικαστική προστασία και να ασκήσει τα προβλεπόμενα ένδικα μέσα για την παράνομη ή καταχρηστική και υπέρμετρη εις βάρος του χρήση του μέτρου, απαγόρευση, η οποία οδηγεί σε αποκλεισμό του δικαιώματος του για την προστασία του ιδιωτικού του βίου (constitutionalism.gr, 2021).

Όλα τα παραπάνω αναφέρονται, καθότι, οι νομικές προκλήσεις, που τίθενται ένεκα της εξέλιξης του κυβερνοεγκλήματος, είναι πολλές και σημαντικές και είναι προφανές ότι, οι εθνικές έννομες τάξεις, οι οποίες στην πλειοψηφία τους έχουν αναπτύξει σημαντικά εργαλεία, δεν δύνανται να το πατάξουν μεμονωμένα, αντιθέτως η διακρατικές συνεργασίες είναι επιβεβλημένες. Στον αντίποδα η αντιμετώπιση των κυβερνοεγκλημάτων σε καμία περίπτωση δεν θα πρέπει να οδηγήσει

σε μία εκ προοιμίου καταστρατήγηση συνταγματικών και υπερεθνικών εγγυήσεων του απορρήτου των επικοινωνιών και της ιδιωτικότητας του ατόμου.

iii) Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες

Το αδίκημα της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες προβλέπεται στον Ν. 4557/2018, ο οποίος πρόσφατα τροποποιήθηκε από τον Ν. 4816/2021, κατόπιν εναρμόνισης της χώρας μας με την υπ' αριθμ. 1673/2018 (ΕΕ) οδηγία του Ευρωπαϊκού Κοινοβουλίου. Οι ποινικές διατάξεις του Ν. 4557/2018 περιγράφουν ένα από τα δυσχερέστερα στην τυποποίηση του αδικήματα λόγω της πολυπλοκότητας και της πολυμορφίας εμφάνισής του στην πράξη.

Ειδικής μνείας θα πρέπει να τύχει η διάταξη του άρθρου 42 παρ. 7 του Ν. 4557/2018, στην οποία προβλέπεται η δυνατότητα δέσμευσης τραπεζικών λογαριασμών, τίτλων, θυρίδων και χρηματοπιστωτικών μέσων, εν γένει, καθώς και η απαγόρευση μεταβίβασης οποιουδήποτε περιουσιακού στοιχείου, κατόπιν έκδοσης διάταξης του Προέδρου της Αρχής Καταπολέμησης της Νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (Γερμανός Γ., Γεωργίου Ν., σελ 275 επ.). Προϋποθέσεις εφαρμογής της διάταξης είναι : α) η διεξαγωγή έρευνας από την αρχή προς εντοπισμό πράξεων νομιμοποίησης ή βασικών αδικημάτων, β) η συνδρομή βάσιμων υπονοιών ότι, έχει τελεστεί βασικό αδίκημα ή πράξη νομιμοποίησης και γ) η συνδρομή επείγουσας περίπτωσης (λ.χ. κίνδυνος άμεσης εξαφάνισης περιουσιακών στοιχείων μέσω αλλεπάλληλων μεταβιβάσεων και συγκάλυψης ιχνών αδικημάτων των δραστών). Πρόκειται για μέτρο, που λαμβάνει η αρχή σε βάρος υπόπτου προκειμένου, στο πλαίσιο της έρευνας της, α) να συλλέξει πληροφορίες και αποδείξεις για την τέλεση βασικών αδικημάτων και πράξεων νομιμοποίησης και β) να αδρανοποιήσει τα περιουσιακά στοιχεία του υπόπτου, διατηρώντας αυτά ακέραια, εμποδίζοντας τον, παράλληλα, ιδίως από τη χρήση του οικονομικού (τραπεζικού) συστήματος.

Μάλιστα σε εξαιρετικά επείγουσες περιπτώσεις όταν προκύπτουν υπόνοιες ότι, μία συναλλαγή σχετίζεται με εγκληματικές δραστηριότητες ή με την χρηματοδότηση τρομοκρατίας δύναται να διαταχθεί από τον Πρόεδρο της Αρχής η προσωρινή δέσμευση της περιουσίας ή η αναστολή της συγκεκριμένης συναλλαγής. Είναι λοιπόν προφανές ενόψει όλων των προαναφερομένων ότι, οι αρμόδιες αρχές (δικαστικές, εισαγγελικές, εποπτικές κ.α.) οφείλουν να συνεργάζονται για την επίτευξη του σκοπού της καταπολέμησης εγκληματικών συμπεριφορών και στο πεδίο του κυβερνοεγκλήματος (Γερμανός Γ., Γεωργίου Ν., σελ 275 επ.).

4.2 Συνεργασίες σε διεθνές και ευρωπαϊκό επίπεδο

i) ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) δημιουργήθηκε, προκειμένου τα κράτη – μέλη της Ευρωπαϊκής Ένωσης να αντιμετωπίσουν από κοινού και αποτελεσματικά το κυβερνοέγκλημα, το οποίο πλήττει την ασφάλεια των δικτύων και των συναλλαγών. Ο κανονισμός λειτουργίας του ENISA είναι ο κανονισμός (ΕΕ) 2019/881 του Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον «Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια» και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών, ο οποίος και κατήργησε τον κανονισμό (ΕΕ) αριθμ. 526/2013 (βλ. https://www.enisa.europa.eu).

Ο συγκεκριμένος Οργανισμός εδρεύει στην χώρα μας και συγκεκριμένα στην Αθήνα και διατηρεί και ένα δεύτερο γραφείο στο Ηράκλειο Κρήτης. Μάλιστα πρόσφατα η έδρα του Enisa στην Αθήνα μεταφέρθηκε σε νέες κτιριακές εγκαταστάσεις συνολικού εμβαδού 7.000 τ.μ. στην οδό Εθνικής Αντιστάσεως 72 και Αγαμέμνονος στο Χαλάνδρι, τα εγκαίνια των οποίων τελέστηκαν στις 17 Μαρτίου 2022, παρουσία του αρμόδιου υπουργού Κυριάκου Πιερρακάκη, του ευρωπαίου επιτρόπου Μαργαρίτη Σχοινά και πλήθους αξιωματούχων από την ΕΕ. Κατά την τελετή των εγκαινίων ο εκτελεστικός διευθυντής του ENISA, Juhan Lepassaar ανέφερε τα εξής ενδιαφέροντα, ενδεικτικά της προτεραιότητας, που θέτει η Ευρωπαϊκή Ένωση για την αντιμετώπιση του κυβερνοεγκλήματος : ‘Η νέα έδρα παρέχει στον ENISA μια σταθερή βάση για την υλοποίηση της εντολής του για την επίτευξη ενός κοινού υψηλού επιπέδου κυβερνοασφάλειας στην Ευρώπη, με ένα “νέο σπίτι” για το προσωπικό και τους συνεργάτες μας εντός της κοινότητας της κυβερνοασφάλειας’’. Με αφορμή την ίδια εκδήλωση ο κ. Σχοινάς ανέφερε τα εξής : “Ο ENISA γεννήθηκε από την επιθυμία να κάνει τις ευρωπαϊκές κοινωνίες και τους πολίτες μας στον κυβερνοχώρο ασφαλείς. Είναι ολόκληρος ο ευρωπαϊκός τρόπος ζωής, που καλείται να προστατεύσει ο ENISA. Χαιρετίζω θερμά τα εγκαίνια των νέων γραφείων της ENISA εδώ στην Αθήνα. Αυτό είναι ένα νέο βήμα για τον Οργανισμό. Και ένα ακόμη σημάδι της μέγιστης σημασίας του για την ασφάλεια ολόκληρης της Ε.Ε. στον σημερινό κόσμο” (digitallife.gr).

Στην τελευταία ετήσια έκθεση του ENISA διαλαμβάνεται ειδική αναφορά για την πανδημία του κορωνοϊού, η οποία κατέστησε περισσότερο ευάλωτους δημόσιους και ιδιωτικούς οργανισμούς, αλλά και τα άτομα στις κυβερνοεπιθέσεις. Μάλιστα, όπως επισημαίνεται σε μεγάλο κίνδυνο έχουν εξελιχθεί και οι χάκερ, οι οποίοι προσφέρουν υπηρεσίες επ’ αμοιβή. Όπως προκύπτει από τα στοιχεία του Οργανισμού στο ‘’μάτι του κυκλώνα’’ των χάκερ βρέθηκαν οι υπηρεσίες υγείας, αναζητώντας πληροφορίες για τα εμβόλια. Όμως και στον δημόσιο τομέα, αλλά και στον κλάδο των παρόχων ψηφιακών υπηρεσιών αναφέρθηκε μεγάλος αριθμός επιθέσεων τύπου ransomware, στις οποίες οι χάκερ κρυπτογραφούν τα δεδομένα και ζητούν λύτρα για να τα ξεκλειδώσουν. Τέλος μία ιδιαιτέρως

σοβαρή απειλή κυβερνοασφάλειας, η οποία επισημαίνεται στην έκθεση, είναι τα fake news και γενικά η παραπληροφόρηση, που ιδιαίτερα κατά την διάρκεια της πανδημίας εκτοξεύτηκαν στα μέσα κοινωνικής δικτύωσης. Στην εν λόγω έκθεση οι υπεύθυνοι του ευρωπαϊκού οργανισμού σημειώνουν χαρακτηριστικά ότι, οι επενδύσεις στον τομέα της κυβερνοασφάλειας δεν βρίσκονται ακόμη σε υψηλά επίπεδα (βλ. https://www.enisa.europa.eu).

Αξίζει να σημειωθεί ότι, στην προηγούμενη ετήσια έκθεση του 2020 ως κορυφαίες απειλές στον χώρο της κυβεροασφάλειας εμφανίζονται οι εξής : malware (κακόβουλο λογισμικό), web-based attacks (επιθέσεις βασισμένες στον ιστό), phishing (ηλεκτρονικό ψάρεμα), web application attacks (επιθέσεις σε εφαρμογές web), spam (ανεπιθύμητη αλληλογραφία), distributed denial of service (κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών), identity theft (κλοπή ταυτότητας), data breach (διαρροή δεδομένων), insider threat (εσωτερική απειλή), botnets, physical manipulation damage, theft and loss (φυσικά συμβάντα), information leakage (διαρροή πληροφοριών), ransomware (λυτρισμικό), cyber espionage (κυβερνοκατασκοπεία) και cryptojacking (κακόβουλη εξόρυξη κρυπτονομισμάτων). Θα πρέπει να σημειωθεί ότι, ο ENISA κάθε χρόνο δημοσιεύει μία έκθεση (ENISA THREAT LANDSCAPE) με αναφορές στις σημαντικότερες επιθέσεις κατά πληροφοριακών συστημάτων σύμφωνα με τα διαθέσιμα στοιχεία, ενώ διαλαμβάνει αναφορές για τις αναδυόμενες τάσεις και τους διαφαινόμενους κινδύνους ((Γερμανός Γ., Γεωργίου Ν., σελ 160 επ.).

ii) INTERPOL

Η Interpol (International Criminal Police Organization, δηλ. Διεθνής Οργάνωση Εγκληματολογικής Αστυνομίας) εδρεύει στην Λυών της Γαλλίας και αποτελεί διακρατικό οργανισμό. Αποστολή της είναι η αμοιβαία συνεργασία μεταξύ των κρατών, προκειμένου να αντιμετωπίζεται αποτελεσματικά το έγκλημα σε παγκόσμιο επίπεδο. Οι μορφές εγκληματικότητας, με τις οποίες ασχολείται η Interpol είναι, μεταξύ άλλων, η τρομοκρατία, τα εγκλήματα κατά του περιβάλλοντος, η διακίνηση ναρκωτικών, η εμπορία ανθρώπων, τα εγκλήματα λευκού κολάρου, τα εγκλήματα πολέμου, τα εγκλήματα κατά της ανθρωπότητας και βεβαίως το κυβερνοέγκλημα (Γερμανός Γ., Γεωργίου Ν., σελ 302 επ.).

Όσον αφορά στο κυβερνοέγκλημα η Interpol έχει ξεκινήσει τα τελευταία χρόνια εκστρατεία ευαισθητοποίησης του κοινού με το βασικό μήνυμα #OnlineCrimeIsRealCrime, προκειμένου να γίνει αντιληπτή η σοβαρότητα και ο υψηλός κίνδυνος, που αυτό δημιουργεί. Σκοπός της καμπάνιας είναι αφενός μεν να ενημερωθεί το κοινό σχετικά με τις κορυφαίες απειλές στον κυβερνοχώρο, αφετέρου δε να περιοριστεί ο κίνδυνος, μέσω της παροχής απλών και κατανοητών συμβουλών. Ιδιαίτερα ενδιαφέρον είναι ότι, με σκοπό να υπάρξει αποτελεσματική αντιμετώπιση του κυβερνοεγκλήματος η Interpol ανακοίνωσε το 2017 την συνεργασία της με την εταιρεία Cisco, ιδιαίτερα στο σκέλος της ασφάλειας των πληροφοριών, με βασική στόχευση το οργανωμένο έγκλημα στον κυβερνοχώρο. Η ανταλλαγή τεχνογνωσίας με την μορφή κατάρτισης για τους εργαζόμενους και της Interpol και της Cisco αποτελεί τον πυρήνα αυτής της συνεργασίας (Θεοδωρίδης, Στ., 2017).

iii) Europol – Cepol

Ήδη με την Συνθήκη του Μαάστριχτ η δημιουργία υπερεθνικών οργανισμών για την αποτελεσματική αντιμετώπιση της οργανωμένης εγκληματικότητας αποτέλεσε προτεραιότητα. Μεταξύ των μορφών εγκληματικότητας, που καλούνται να προσεγγίσουν, περίοπτη θέση κατέχει το έγκλημα στον κυβερνοχώρο, το οποίο πολλές φορές έχει ειπωθεί στην παρούσα ότι, δεν γνωρίζει εδαφικά σύνορα και διαρκώς διαλαμβάνει εξελιγμένες μεθόδους.

Η Ευρωπαϊκή Αστυνομία (Europol) σκοπό έχει την προώθηση της συνεργασίας μεταξύ των κρατών – μελών της Ευρωπαϊκής Ένωσης για την αποτελεσματική αντιμετώπιση της εγκληματικότητας μέσω της ανταλλαγής πληροφοριών, αποδεικτικών στοιχείων και την παροχή τεχνικής υποστήριξης (βλ. https://www.europol.europa.eu/). Όσον αφορά στην πάταξη του κυβερνοεγκλήματος η Europol έχει επιδείξει σημαντικές δράσεις με πρόσφατη το κλείσιμο της παράνομης πλατφόρμας RaidForums και την κατάσχεση της υποδομή της, στα πλαίσια της επιχείρησης Tourniquet, μιας σύνθετης επιχείρησης της Europol για την υποστήριξη ανεξάρτητων ερευνών στις ΗΠΑ, τη Βρετανία, τη Σουηδία, την Πορτογαλία και τη Ρουμανία. Η "RaidForums", που ξεκίνησε το 2015, είχε τουλάχιστον μισό εκατομμύριο χρήστες και ήταν ένα από τα πιο σημαντικά φόρουμ χάκερ στον κόσμο (naftemporiki.gr).

Η Cepol ιδρύθηκε την 1η Ιουλίου 2016 και έχει έδρα την Βουδαπέστη της Ουγγαρίας. Αποστολή της είναι η κατάρτιση και εκπαίδευση των εμπλεκόμενων παραγόντων επιβολής του νόμου στα κράτη – μέλη της Ευρωπαϊκής Ένωσης. Η CEPOL επιδιώκει την συνεργασία και την διασύνδεση όχι μόνο στο εσωτερικό της Ένωσης, αλλά και με τρίτες χώρες, προκειμένου να επιτευχθεί η συλλογική αντιμετώπιση των νέων μορφών εγκληματικότητας, μεταξύ αυτών και του κυβερνοεγκλήματος. Μάλιστα μέσω της διοργάνωσης εκπαιδευτικών δραστηριοτήτων, που σκοπό έχουν την παροχή ποιοτικής εκπαίδευσης σε πιστοποιημένους διαπραγματευτές και σε άμεσα εμπλεκομένους λειτουργούς, εναρμονισμένης στα σύγχρονα δεδομένα και με βασικούς άξονες την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος, επιδιώκεται η θωράκιση του ενιαίου χώρου ασφάλειας της Ευρωπαϊκής Ένωσης (βλ. https://www.cepol.europa.eu/).

iv) EUROJUST

Η Eurojust (European Union Agency for Criminal Justice Cooperation) έχει την έδρα της στην Χάγη και αποστολή της είναι η συνεργασία των κρατών – μελών της Ένωσης στο πεδίο της ποινικής δικαιοσύνης. Αποσκοπεί στον συντονισμό μεταξύ των κρατών – μελών και την εμπέδωση της συνεργασίας μεταξύ τους στις περιπτώσεις σοβαρών εγκλημάτων και ιδίως όταν αυτά αφορούν περισσότερες της μιας χώρες. Επίσης έχει την δυνατότητα να παράσχει επιχειρησιακή, τεχνική και οικονομική υποστήριξη όταν απαιτούνται διασυνοριακές δράσεις και έρευνες. Μάλιστα προς τον σκοπό αυτό η Eurojust διοργανώνει σε τακτά χρονικά διαστήματα συνεδριάσεις με την συμμετοχή εισαγγελικών και δικαστικών λειτουργών από τα κράτη – μέλη για την ανταλλαγή πληροφοριών και

τον συντονισμό δράσεων προς την πάταξη του οργανωμένου εγκλήματος (βλ. https://www.eurojust.europa.eu/).

Η Eurojust έχει εντάξει στους κόλπους της το Ευρωπαϊκό Δικαστικό Δίκτυο για το Έγκλημα στον Κυβερνοχώρο (European Judicial Cybercrime Network), το οποίο διοργανώνει συναντήσεις εργασίας μεταξύ εθνικών αρχών, που εμπλέκονται με την πάταξη του κυβερνοεγκλήματος, προκειμένου να υπάρξει αποτελεσματική αντιμετώπιση σε υπερεθνικό επίπεδο. Βασικά θέματα, με τα οποία έχει ενασχόληση το Δίκτυο είναι τα θύματα των κυβερνοεγκλημάτων, η πρόσβαση στα δεδομένα, τα ηλεκτρονικά αποδεικτικά στοιχεία, η εκπαίδευση των εμπλεκομένων και η διατήρηση των δεδομένων. Στο σημείο αυτό ειδική μνεία θα πρέπει να γίνει στο Sirius (Sirius Cross – Border Acces to Electronic Evidence), αποτέλεσμα της συνεργασίας μεταξύ Eurojust και Europol, το οποίο αποτελεί μία πλατφόρμα ανταλλαγής πληροφοριών, με σκοπό την αποτελεσματική αντιμετώπιση στο ιδιαιτέρως σημαντικό ζήτημα των ηλεκτρονικών αποδεικτικών στοιχείων (Γερμανός Γ., Γεωργίου Ν., σελ 294 επ.).

v) Σύμβαση κατά του Διεθνικού Οργανωμένου Εγκλήματος

Η Διεθνής Σύμβαση για το Οργανωμένο Έγκλημα εγκρίθηκε στις 12-15 Δεκεμβρίου 2000 από τα 121 μέλη του ΟΗΕ και η ισχύς της εκκίνησε το 2003, αποτελώντας προφανώς ένα πολύ σοβαρό διακρατικό εργαλείο στην μάχη για την αποτελεσματική πάταξη αυτής της μορφής εγκληματικότητας. Στην σύμβαση περιλαμβάνεται ο ορισμός και η περιγραφή της εγκληματικής ομάδας, η οποία ορίζεται ως εξής (UNTOC) «Οργανωμένη εγκληματική ομάδα» σημαίνει: «Μία δομημένη ομάδα τριών ή περισσότερων προσώπων που υφίσταται για κάποια χρονική περίοδο και ενεργεί από κοινού με σκοπό την τέλεση ενός ή περισσότερων σοβαρών εγκλημάτων ή αδικημάτων που θεσπίζονται σύμφωνα με την παρούσα Σύμβαση, με απώτερο σκοπό την απόκτηση, άμεσα ή έμμεσα, οικονομικού ή άλλου υλικού οφέλους» (astynomia.gr).

Η εν λόγω Σύμβαση, η οποία συνιστά σημαντικό όπλο και για την αντιμετώπιση του κυβερνοεγκλήματος σε υπερεθνικό επίπεδο και τα τρία συνοδευτικά πρωτόκολλα, ήτοι το Πρωτόκολλο για την Πρόληψη, Καταστολή και Τιμωρία της Διακίνησης Προσώπων, ιδιαίτερα Γυναικών και Παιδιών και το Πρωτόκολλο κατά της Λαθραίας Διακίνησης Μεταναστών από την Γη, την Θάλασσα και τον Αέρα, καθώς και το Πρωτόκολλο κατά της παράνομης κατασκευής και διακίνησης πυροβόλων όπλων, τμημάτων και συστατικών τους και πυρομαχικών, κυρώθηκαν στην χώρα μας με τον Ν. 3875/2010. Στον συγκεκριμένο Νόμο προβλέπεται, μεταξύ άλλων, η ποινικοποίηση της συμμετοχής σε οργανωμένη εγκληματική ομάδα, η ποινικοποίηση της νομιμοποίησης προϊόντων εγκλήματος, η ποινικοποίηση της διαφθοράς, ενώ όσον αφορά στην εγκαθίδρυση της δικαιοδοσίας, στο άρθρο 15 προβλέπεται η δυνατότητα συνεργασίας καθότι, ορίζεται ότι, εάν ένα Κράτος Μέρος, που ασκεί την Δικαιοδοσία του, έχει ενημερωθεί ή πληροφορήθηκε με άλλο τρόπο, ότι ένα ή περισσότερα Κράτη Μέρη διεξάγουν έρευνα, δίωξη ή δικαστική διαδικασία για την ίδια πράξη, οι αρμόδιες αρχές των εν λόγω Κρατών Μερών θα

διαβουλεύονται καταλλήλως μεταξύ τους για να συντονίσουν τις ενέργειές τους (βλ. Ν. 3875/2010, δημ. NOMOS).

Όπως πρόσφατα έγινε γνωστό και δεδομένης της διεθνούς έξαρσης στο πεδίο του κυβενροεγκλήματος έχει ξεκινήσει η συζήτηση για μια νέα διεθνή σύμβαση, η οποία θα στοχεύει στην καταπολέμηση της χρήσης των τεχνολογιών πληροφοριών και των επικοινωνιών για εγκληματικούς σκοπούς. Η Ευρωπαϊκή Ένωση, η οποία και συμμετέχει στις διαπραγματεύσεις, θα λάβει υπόψη την Σύμβαση της Βουδαπέστης του 2001 για το κυβερνοέγκλημα, ενώ θα δώσει ιδιαίτερη έμφαση στην εξασφάλιση της προστασίας για τα ανθρώπινα δικαιώματα, όπως αναφέρουν χαρακτηριστικά Ευρωπαίοι αξιωματούχοι (Lawspot.gr, 2022).

Κεφάλαιο 5 : Μέθοδοι αντιμετώπισης

5.1 Προστασία υπολογιστών και θυμάτων για ασφαλή περιήγηση στο διαδίκτυο

Όπως έχει προκύψει από τα όσα έχουν ήδη αναφερθεί, πρωταρχικής σημασίας είναι να αντιληφθούμε όλοι όσοι χρησιμοποιούμε τα διαδίκτυο ότι, οφείλουμε να λαμβάνουμε πρωτίστως εμείς οι ίδιοι μέτρα αυτοπροστασίας. Προς την κατεύθυνση αυτή και με σκοπό τον περιορισμό της έξαρσης των κυβερνοεγκλημάτων κρίνεται απαραίτητη η παράθεση κάποιων πρακτικών συμβουλών για την ασφαλή πλοήγηση στο διαδίκτυο, το οποίο σε καμία περίπτωση δεν θα πρέπει να το δαιμονοποιούμε, αλλά απεναντίας να το αντιμετωπίζουμε ως ένα χρήσιμο εργαλείο εργασίας, μελέτης και ψυχαγωγίας.

Συγκεκριμένα όσον αφορά στα παιδιά, τα οποία και λόγω του νεαρού της ηλικίας τους, αλλά και της αλματώδους εξέλιξης της τεχνολογίας, αποτελούν τα περισσότερα ευάλωτα και συνήθη υποψήφια θύματα, είναι ιδιαιτέρως κρίσιμο να μην κοινοποιούν τα προσωπικά τους στοιχεία σε άλλους χρήστες του διαδικτύου, να μην δίδουν πληροφορίες για την οικογενειακή τους κατάσταση, να μην αποστέλλουν προσωπικές τους φωτογραφίες σε άγνωστους παραλήπτες, να μην ανοίγουν ηλεκτρονικές σελίδες με την σήμανση ‘’άνω των 18’’, να μην ανοίγουν ηλεκτρονικά μηνύματα και συνημμένα αρχεία από αγνώστους, να κρατούν μυστικούς του κωδικούς πρόσβασης από το ηλεκτρονικό ταχυδρομείο και να αποφεύγουν τις κατ’ ιδίαν συναντήσεις και επαφές με άτομα, που γνώρισαν στο διαδίκτυο (βλ. safeinternet4kids.gr).

Όμως για την αποτελεσματική προστασία των παιδιών από τις απειλές του διαδικτύου είναι προφανές ότι, εξέχουσας σημασίας είναι ο ρόλος των γονέων, οι οποίοι οφείλουν, αποδεχόμενοι την προσφορά της τεχνολογίας, να λάβουν τα αναγκαία μέτρα. Ειδικότερα, είναι πολύ σημαντικό οι γονείς, ακόμα και εάν δεν είναι οι ίδιοι εξοικειωμένοι, με την πλοήγηση στο internet να προσπαθούν να ενημερώνονται μέσω της συμμετοχής σε συμβουλευτικές ομάδες, της μελέτης επίκαιρων άρθρων ή ακόμα και των επισκέψεων σε ειδικούς επιστήμονες, επίσης όπως σε όλα τα ζητήματα έτσι και στο συγκεκριμένο, είναι πρωταρχικής σημασίας η διαρκής και ειλικρινής επικοινωνία γονέων και παιδιών και η ανταλλαγή απόψεων και πληροφοριών για αγαπημένα διαδικτυακά παιχνίδια, ιστοσελίδες και βεβαίως η γνώση της ταυτότητας των διαδικτυακών φίλων, χωρίς διάθεση επικριτική και αυστηρά ελεγκτική, η δημιουργία και η τήρηση κανόνων για την ασφαλή πλοήγηση είναι ένα ακόμα χρήσιμο εργαλείο, όπως και η διαρκής υπενθύμιση στα παιδιά περί αναφοράς στους γονείς τους για κάθε τι, που ενδεχομένως τα προβλημάτισε ή τα έφερε σε άβολη θέση κατά την πλοήγησή τους, η προμήθεια ενός λογισμικού γονικού ελέγχου προφανώς και μπορεί να συμβάλλει στην προστασία των παιδιών από ακατάλληλες ιστοσελίδες ή ακόμα και στην τήρηση συγκεκριμένου χρονικού πλαισίου περιήγησης, τέλος η κοινή οικογενειακή πλοήγηση ενδεχομένως δύναται να αποτελέσει μία ευχάριστη δραστηριότητα για όλα τα μέλη ανεξαρτήτως ηλικίας (βλ. safeinternet4kids.gr).

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο (Safer Internet Day), η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης δημοσιοποίησε κάποιες πρακτικές οδηγίες με σκοπό την ενδυνάμωση της ασφάλειας και της ιδιωτικότητας κατά την περιήγησή μας στο Διαδίκτυο, όπως : εγκατάσταση στον υπολογιστή μας λογισμικού antivirus και προστασίας firewall, αποφυγή της χρήσης αμφιλεγόμενων εφαρμογών, χρήση σύνθετων κωδικών πρόσβασης, οι οποίοι σε καμία περίπτωση δεν θα πρέπει να είναι προφανείς και να παραπέμπουν στα προσωπικά στοιχεία του χρήστη (π.χ. αρχικά επωνύμου, ημερομηνία γέννησης κ.α.), τακτική λήψη αντιγράφων ασφαλείας των δεδομένων μας σε εξωτερικούς σκληρούς δίσκους ή στο Cloud, προκειμένου να είναι αποθηκευμένα με ασφάλεια, ιδιαίτερη προσοχή για την ιστοσελίδα μέσω της οποίας αποστέλλουμε προσωπικά στοιχεία (κωδικοί πρόσβασης, αριθμό τραπεζικής κάρτας κ.α.) εάν λειτουργεί με το πρωτόκολλο https, προσοχή στα παραπλανητικά emails και συνημμένα έγγραφα (phishing emails), τα οποία προέρχονται από άγνωστους αποστολείς, αποφυγή κοινοποίησης προσωπικών και ευαίσθητων πληροφοριών στα μέσα κοινωνικής δικτύωσης και τέλος χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication), όπου υποστηρίζεται, ώστε να υφίσταται ένα πρόσθετο μέτρο ασφαλείας για την θωράκιση του λογαριασμού μας (βλ. https://mindigital.gr/kyvernoasfaleia).

Ένα πεδίο, στο οποίο συχνά εκδηλώνονται εγκληματικές συμπεριφορές είναι οι οικονομικές συναλλαγές στο διαδίκτυο. Κάποιες χρήσιμες πρακτικές συμβουλές, δεδομένου ότι, οι περισσότεροι από εμάς πραγματοποιούμε αφενός μεν τραπεζικές και συναφείς συναλλαγές, αφετέρου και ηλεκτρονικές αγορές είναι οι εξής : είναι προτιμότερο να πραγματοποιούμε τέτοιου είδους εργασίες από τον προσωπικό μας υπολογιστή και να αποφεύγουμε τα internet cafe και άλλους δημόσιους χώρους, να αλλάζουμε συχνά τους κωδικούς πρόσβασης, που χρησιμοποιούμε, τους οποίους δεν φυλάσσουμε σε πορτοφόλια, τσάντες, ατζέντες κ.α.., καθότι, είναι εύκολο να αποκτήσουν πρόσβαση τρίτα άτομα και βεβαίως να μην συμπεριλαμβάνουμε προσωπικά μας στοιχεία σε αυτούς (π.χ. ημερομηνία γέννησης), να ενημερώνουμε άμεσα για την ενδεχόμενη απώλειά τους τον φορέα, που αφορούν (π.χ. internet banking), να πραγματοποιούμε τις αγορές μας από αξιόπιστα ηλεκτρονικά καταστήματα, να απενεργοποιούμε την ένδειξη της αυτόματης καταχώρησης – αποθήκευσης των προσωπικών μας στοιχείων ή των στοιχείων της κάρτας μας, να φροντίζουμε για την ασφάλεια του υπολογιστή μας μέσω της λήψης νέων ενημερωμένων προγραμμάτων και τέλος να αποφεύγουμε το άνοιγμα μηνυμάτων από άγνωστους αποστολής και την λήψη συνημμένων – μη αξιόπιστων εγγράφων (βλ. astynomia.gr).

Κλείνοντας ειδικής αναφοράς θα πρέπει να τύχουν τα μέσα κοινωνικής δικτύωσης (facebook, instagram κ.α.), των οποίων οι περισσότεροι τυγχάνουμε χρήστες και για τον λόγο αυτό απαιτείται ιδιαίτερη προσοχή. Είναι ιδιαιτέρως σημαντικό να διαφυλάσσουμε και να μην κοινοποιούμε τους κωδικούς για την πρόσβασή μας σε αυτά, να κάνουμε χρήση των ρυθμίσεων ασφαλείας, προκειμένου το προφίλ μας και τα στοιχεία μας να είναι προσβάσιμα μόνο στους φίλους μας και βέβαια να είμαστε

επιφυλακτικοί στο υλικό, που κοινοποιούμε σε αυτά διότι, ακόμα και στην περίπτωση, που απενεργοποιήσουμε το προφίλ μας, πολλές πληροφορίες θα διατηρηθούν στο διαδίκτυο (βλ. kethi.gr).

Συμπεράσματα – Προτάσεις

Είναι προφανές ότι, το κυβερνοέγκλημα αποτελεί μία νέας μορφής εξελισσόμενης εγκληματικότητας τόσο στην Ελλάδα, όσο και διεθνώς. Αυτό συμβαίνει διότι, δεν γνωρίζει σύνορα και εγγυάται σε μεγάλο βαθμό την ανωνυμία των εγκληματιών. Η ολοένα και αυξανόμενη χρήση του διαδικτύου και η πρόοδος, η οποία έχει επέλθει από τις καινοτόμες τεχνολογίες, έχουν προσδώσει νέες μορφές στις παραδοσιακές εγκληματικές συμπεριφορές και έχουν καταστήσει ευάλωτους ακόμα και τους ενημερωμένους χρήστες.

Αξίζει να σημειωθεί και προς επίρρωσιν των προαναφερομένων ότι, στην χώρα μας, σύμφωνα με έρευνα του ΕΚΚΕ στο πλαίσιο του διεθνούς έργου "World Internet Project", την οποία δημοσίευσε η διαΝΕΟσις 7 στους 10 Έλληνες έχουν πρόσβαση στο διαδίκτυο και το ποσοστό αυτό εκτινάσσεται στο 100% για τους νέους κάτω των 35 ετών. Επίσης σύμφωνα με την ίδια έρευνα το 11,5% των ερωτώμενων δηλώνει ότι τους έχουν ζητήσει online τραπεζικές ή άλλες προσωπικές πληροφορίες ενώ το 7,2% δηλώνουν ότι, τους έχουν εκφοβίσει ή παρενοχλήσει μέσω διαδικτύου. Τέλος όσον αφορά στην ιδιωτικότητα στο διαδίκτυο το 59,3% των ερωτώμενων απάντησε ότι, "αισθάνεται ότι ελέγχει την ιδιωτικότητά τους στο διαδίκτυο", ενώ ιδιαίτερο ενδιαφέρον έχει ότι, το 48,1% θεωρεί ότι "κυβέρνηση δεν πρέπει να ελέγχει το διαδίκτυο περισσότερο από όσο το κάνει τώρα" (Νικολαίδης, Η., 2020).

Οι δυσχέρειες, που ήδη έχουν αναλυθεί στην παρούσα εργασία, όσον αφορά στην συγκέντρωση των αποδείξεων, στον εντοπισμό των δραστών, αλλά και σε επίπεδο διακρατικών συνεργασιών αποτελούν ανασταλτικό παράγοντα αφενός μεν στον περιορισμό αυτού του πολυποίκιλου εγκληματικού φαινομένου, αφετέρου δε στην καταγραφή του συνόλου των εγκλημάτων, τα οποία τελούνται στο διαδίκτυο, πολλά εκ των οποίων παραμένουν μη καταγγελόμενα και συνακόλουθα ανεξιχνίαστα. Μάλιστα η χρήση εξελιγμένων τεχνολογικών συστημάτων, σε συνδυασμό με την υψηλή τεχνογνωσία των δραστών, καθιστούν την πάταξη του κυβερνοεγκλήματος μία δύσκολη εξίσωση.

Προς την κατεύθυνση αυτή καταβάλλεται προσπάθεια και αυτό είναι εμφανές και στην χώρα μας για τον εκσυγχρονισμό της εθνικής μας νομοθεσίας και την συμπόρευσή της με τα ευρωπαϊκά δεδομένα, προκειμένου να επιτευχθεί μία αποτελεσματική αντεγκληματική πολιτική στον τομέα αυτό. Βέβαια παρά τα βήματα, τα οποία έχουν ήδη συντελεστεί στο εσωτερικό, το μοντέλο, το οποίο ακολουθείται με την υπερσυγκέντρωση αυτού του είδους των υποθέσεων στις Υπηρεσίες Δίωξης Ηλεκτρονικού Εγκλήματος κυρίως της Αθήνας και της Θεσσαλονίκης αποδεικνύεται σε μεγάλο βαθμό αναποτελεσματικό, διότι, παρά την άριστη δουλειά των εκεί εργαζομένων, παρατηρούνται καθυστερήσεις στην εξιχνίαση και συσσώρευση υποθέσεων, πολλές εκ των οποίων δεν απαιτούν ειδικές τεχνολογικές γνώσεις για την διαλεύκανσή τους.

Είναι λοιπόν ιδιαιτέρως σημαντικό να επέλθουν καίριες τομές ως προς την αποτελεσματική δίωξη του κυβερνοεγκλήματος, οι οποίες εντοπίζονται στην ταχεία ενσωμάτωση των ευρωπαϊκών δεδομένων, αλλά και στον εκσυγχρονισμό του ανακριτικού συστήματος με βασικούς άξονες την ταχύτητα στην συγκέντρωση των αποδεικτικών στοιχείων και την ταυτόχρονη τήρηση των εγγυήσεων του σεβασμού των ατομικών ελευθεριών. Προς την κατεύθυνση αυτή είναι κομβικής σημασίας η συνεχής εκπαίδευση πρωτίστως των φορέων, που εμπλέκονται στην εξιχνίαση τέτοιου είδους αδικημάτων, αλλά και των χρηστών του διαδικτύου, οι οποίοι χρησιμοποιούν τις υπηρεσίες του διαδικτύου είτε για προσωπικούς, είτε για επαγγελματικούς λόγους.

Εν κατακλείδι και δεδομένου ότι, το κυβερνοέγκλημα έχει παγκόσμια εμβέλεια, αποτελεί μία ισχυρή απειλή για τα κράτη και τα άτομα ξεχωριστά πλήττοντας μία σειρά εννόμων αγαθών περιουσιακών και προσωπικών πρωτίστως. Ως εκ τούτου η σφυρηλάτηση των διακρατικών συνεργασιών και του εναρμονισμού των εσωτερικών νομοθεσιών είναι κομβικής σημασίας για την αποτελεσματική αντιμετώπιση.

Κλείνοντας και όσον αφορά στην παρούσα εργασία θα πρέπει να σημειωθεί ότι, καταβλήθηκε προσπάθεια να καταγραφούν οι βασικές πτυχές του κυβερνοεγκλήματος σε εθνικό και ευρωπαϊκό – διεθνές επίπεδο. Οι κυριότερες δυσκολίες, που παρατηρήθηκαν, ήταν οι περιορισμένες βιβλιογραφικές αναφορές, όχι μόνο σε ελληνικές αλλά και σε ξενόγλωσσες, γεγονός, το οποίο επιρρωνύει την άποψη περί διαρκούς μετεξέλιξης αυτού του ιδιάζοντος εγκληματικού φαινομένου. Θα είχε ιδιαίτερο ενδιαφέρον, στα πλαίσια συνέχισης αυτής της προσπάθειας, η περαιτέρω διερεύνηση, με ποσοτική μέθοδο και βασικότερα σημεία αναφοράς την προσέγγιση χρηστών του διαδικτύου (μέσω του σχεδιασμού και διαμοιρασμού ειδικών ερωτηματολογίων), αλλά και φορέων, που εμπλέκονται στην εξιχνίαση τέτοιου είδους εγκλημάτων, προκειμένου να αντληθούν χρήσιμα στοιχεία και να χρησιμοποιηθούν για την εκ νέου χάραξη και επικαιροποίηση σημείων της εθνικής αντεγκληματικής πολιτικής στον συγκεκριμένο τομέα.

ΒΙΒΛΙΟΓΡΑΦΙΑ - ΜΕΛΕΤΕΣ:

Αβούρης, Ν. (2017). *Τεχνολογίες του διαδικτύου.* Διαθέσιμο στο https://docplayer.gr/46693574-Tehnologies-diadiktyoy.html

Γασπαρινάτου, Μ. (2016). *Έγκλημα και ποινική καταστολή σε εποχή κρίσης. Τιμητικός τόμος για τον καθηγητή Νέστορα Κουράκη.* Α.Ν. ΣΑΚΚΟΥΛΑΣ.

Γερμανός, Γ., Γεωργίου, Ν. (2021). *ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ, ΠΡΟΛΗΨΗ / ΔΙΕΡΕΥΝΗΣΗ/ ΑΝΤΙΜΕΤΩΠΙΣΗ.* Αθήνα.

Δαγτόγλου, Πρ. (2005). *ΣΥΝΤΑΓΜΑΤΙΚΟ ΔΙΚΑΙΟ – ΑΤΟΜΙΚΑ ΔΙΚΑΙΩΜΑΤΑ Α'.* Εκδόσεις Αντ. Ν. Σάκκουλα (Αθήνα).

Θεοδωρίδης, Στ. (2017). Η Cisco συνεργάζεται με την Interpol για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.
Διαθέσιμο στο https://texnologia.net/h-cisco-sunergazetai-me-thn-interpol-gia-thn-katapolemhsh-tou-egklhmatos-sto-kuvernoxoro/2017/11
Δημοσιεύτηκε στις 21-11-2017

Καργόπουλος, Α. (2018). Κυβερνο-έγκλημα : *Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου.*
Διαθέσιμο στο https://www.esdi.gr › epimorfosi › kargopoulos

Καρυστινού, Β. (2016). *Κυβερνοτρομοκρατία: Πραγματική Απειλή ή Σύγχρονη Νεύρωση;*
Διαθέσιμο στο http://www.menoeuropi.gr/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%84%CF%81%CE%BF%CE%BC%CE%BF%CE%BA%CF%81%CE%B1%CF%84%CE%AF%CE%B1-%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE-%CE%B1%CF%80%CE%B5%CE%B9/
Δημοσιεύτηκε την 01-06-2016

Κολλιδάς Γ. (2020). Άποψη: «Σκοτεινό Διαδίκτυο» και κυβερνοέγκλημα.
Διαθέσιμο στο https://www.kathimerini.gr/economy/561084904/apopsi-skoteino-diadiktyo-kai-kyvernoegklima/
Δημοσιεύτηκε στις 22-09-2020

Κοτσακά, Δ. (2015). *Η αρχή της ουδετερότητας του διαδικτύου*.
Διαθέσιμο στο *https://opengov.ellak.gr/2015/07/06/i-archi-tis-oudeterotitas-tou-diadiktiou/*

Κωνσταντοπούλου, Β. (2018). *Διαδικτυακός Εκφοβισμός.*
Διαθέσιμο στο https://www.frodida.org/Article/322/el/Diadiktuakos-Ekfovismos/
Δημοσιεύτηκε στις 05-03-2018

Μαυρίδης, Ι. (2015). *Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα.*
Διαθέσιμο στο https://repository.kallipos.gr › 05_chapter_13

Μιχαηλίδου, Χ. (2018). *Κυβερνοέγκλημα και ηλεκτρονική απόδειξη – ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά.*
Διαθέσιμο στο https://theartofcrime.gr/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%AE-%CE%B1%CF%80%CF%8C%CE%B4/
Δημοσιεύτηκε τον 11/2018

Μιχαλοπούλου, Ν. (2017). *Μανώλης Σφακιανάκης: Ψηφιακό έγκλημα, η επόμενη γενιά.*
Διαθέσιμο στο *https://longform.protothema.gr/bitdefender/manolis-sfakianakis-psifiako-egklima/*
Δημοσιεύτηκε τον 04/2017.

Μπρίνιας, Μ. (2020). *Ηλεκτρονικό Οικονομικό Έγκλημα και ο ρόλος της Europol.*
Διαθέσιμο στο https://odeth.eu/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%BF%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CE%BF/
Δημοσιεύτηκε στις 04-06-2020

Nedelec, J.. *Πώς οι εγκληματίες του κυβερνοχώρου διαφέρουν από τους τακτικούς εγκληματίες.*
Δημοσιεύτηκε https://eyewated.com/%CF%80%CF%8E%CF%82-%CE%BF%CE%B9-%CE%B5%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1%CF%84%CE%AF%CE%B5%CF%82-%CF%84%CE%BF%CF%85-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF%CF%85/

Νικολαίδης, Η. (2019). *Τα Βήματα Της Ελλάδας Προς Μια Εθνική Στρατηγική Κυβερνοασφάλειας.*
Δημοσιεύτηκε στο *https://www.dianeosis.org/2019/04/ethniki-stratigiki-kivernoasfalias/*

Νικολαίδης, Η. (2020). *Οι Έλληνες και το ίντερνετ.*
Διαθέσιμο στο https://www.dianeosis.org/2020/06/oi-ellines-kai-to-internet/
Δημοσιεύτηκε τον Ιούνιο 2020

Παπαπροδρόμου, Γ. (2021). *Τεχνολογία και Κυβερνοέγκλημα: Σύνθετες προσεγγίσεις για σύνθετα ζητήματα.*
Διαθέσιμο στο *https://www.naftemporiki.gr/story/1778438/texnologia-kai-kubernoegklima-sunthetes-proseggiseis-gia-suntheta-zitimata*
Δημοσιεύτηκε στις 19-09-2021

Περπέρης, Α. (2019). *Ο ρόλος των κινήτρων και των ευκαιριών στην δόμηση του προτύπου του ηλεκτρονικού – οικονομικού εγκλήματος.*

Διαθέσιμο στο *https://lawtakpap.blogspot.com/2019/06/blog-post.html*

Δημοσιεύτηκε στις 27-06-2019

Σπανδόνη, Ε. (2016). *Η ελεύθερη πρόσβαση στο διαδίκτυο ως βασικό ανθρώπινο δικαίωμα.*

Διαθέσιμο στο *https://gr.pcmag.com/migrated-64254-mobile-apps/21729/e-eleuthere-prosbase-sto-diadiktuo-os-basiko-anthropino-dikaioma*

Στεργιούλης, Ε. (2020). *Παιδική πορνογραφία.*

Διαθέσιμο στο *https://www.capital.gr/me-apopsi/3493520/paidiki-pornografia*

Δημοσιεύτηκε στις 07-11-2020

Φαρσεδάκης, Ι. (2009). *Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του.*

Διαθέσιμο στο *https://criminology.panteion.gr/index.php?option=com_content&view=article&id=386:%CF%84%CE%BF-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BF-%CE%BA%CE%B1%CE%B9-%CE%B7-%CE%B1%CE%BD%CF%84%CE%B9%CE%BC%CE%B5%CF%84%CF%8E%CF%80%CE%B9%CF%83%CE%AE-%CF%84%CE%BF%CF%85&catid=128&lang=el&Itemid=717*

ΔΙΑΔΙΚΤΥΑΚΟΙ ΙΣΤΟΤΟΠΟΙ :

Διαδίκτυο, κίνδυνοι και προστασία: Τι πρέπει να γνωρίζουμε.

Διαθέσιμο στο https://www.xronos.gr/reportaz/diadiktyo-kindynoi-kai-prostasia-ti-prepei-na-gnorizoyme

Δημοσιεύτηκε στις 04-11-2017

Πόσο καλά ενημερωμένοι είναι οι Ευρωπαίοι για το κυβερνοέγκλημα;

Διαθέσιμο στο ***https://www.moneyreview.gr/business-and-finance/18856/poso-kala-enimeromenoi-einai-oi-eyropaioi-gia-to-kyvernoegklima/***

Capital. Gr (2020). *Europol: Πώς ο κορονοϊός ευνόησε το κυβερνοέγκλημα.*

Διαθέσιμο στο https://www.capital.gr/diethni/3485715/europol-pos-o-koronoios-eunoise-to-kubernoegklima

Δημοσιεύτηκε στις 05-10-2020

Constitutionalism.gr (2021). *Αντίθεση του άρθρου 87 Ν. 4790/2021 προς τις εγγυήσεις της ΕΣΔΑ για διαφύλαξη του απορρήτου των επικοινωνιών*.

Διαθέσιμο στο https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/

Δημοσιεύτηκε στις 04-07-2021

Cyber Security (2021). *Μοντέλα franchise από κυβερνοεγκληματίες και συνταγές για cyber χτυπήματα.*

Διαθέσιμο στο *https://unicertcollege.edu.gr/en/2021/04/06/%CE%BC%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%B1-franchise-%CE%B1%CF%80%CF%8C-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B5%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1%CF%84%CE%AF%CE%B5%CF%82-%CE%BA%CE%B1%CE%B9/*

Δημοσιεύτηκε στις 06-04-2021

digitallife.gr (2022). *ENISA: Στην Αθήνα χτύπα πλέον η καρδιά της κυβερνοασφάλειας της Ευρώπης.*

Διαθέσιμο στο https://www.digitallife.gr/enisa-stin-athina-chtypa-pleon-i-kardia-tis-kyvernoasfaleias-tis-evropis-93075

Δημοσιεύτηκε στις 21-03-2022

kethi.gr (2021). *Πώς να είμαι ασφαλής χρησιμοποιώντας το internet και τα social media.*

Διαθέσιμο στο https://www.kethi.gr/blog/pos-na-eimai-asfalis-hrisimopoiontas-internet-kai-ta-social-media

Δημοσιεύτηκε στις 28-01-2021

Lawspot.gr (2018). *Η προστασία του απορρήτου των επικοινωνιών: Ενημερωτικό υλικό από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών Με αφορμή τον Ευρωπαϊκό Μήνα για την Ασφάλεια στον Κυβερνοχώρο.*

Διαθέσιμο στο *https://www.lawspot.gr/nomika-nea/i-prostasia-toy-aporritoy-ton-epikoinonion-enimerotiko-yliko-apo-tin-arhi-diasfalisis-toy*

Δημοσιεύτηκε στις 09-10-2018

Lawspot.gr (2022). *Ξεκινούν οι διαπραγματεύσεις η νέα σύμβαση των Ηνωμένων Εθνών κατά του κυβερνοεγκλήματος.*

Διαθέσιμο στο https://www.lawspot.gr/nomika-nea/xekinoyn-oi-diapragmateyseis-i-nea-symvasi-ton-inomenon-ethnon-kata-toy-kyvernoegklimatos

Δημοσιεύτηκε στις 30-03-2022

naftemporiki.gr (2022). *Europol: Έκλεισε μία από τις μεγαλύτερες πλατφόρμες χάκερ στον κόσμο - Πώς είχε αποκτήσει «όνομα».*

Διαθέσιμο στο https://www.naftemporiki.gr/story/1853105/europol-ekleise-mia-apo-tis-megaluteres-platformes-xaker-ston-kosmo-pos-eixe-apoktisei-onoma

Δημοσιεύτηκε στις 12-04-2022

ΕΓΚΥΚΛΙΟΙ :

Εισαγγελία Αρείου Πάγου (2019). *ΘΕΜΑ: «Παροχή οδηγιών σχετικά με την λειτουργία και αρμοδιότητες της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος και της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας - Αποστολή ποινικών δικογραφιών και εισαγγελικών παραγγελιών που αφορούν μόνο σοβαρές υποθέσεις γνήσιων κυβερνοεγκλημάτων και εφ' όσον αυτές απαιτούν εξειδικευμένη τεχνική ή ψηφιακή έρευνα και υπάγονται στην αρμοδιότητα της υπηρεσίας»*. Διαθέσιμο στο https://eisap.gr/sites/default/files/circulars/%CE%95%CE%93%CE%9A%CE%A5%CE%9A%CE%9B%CE%99%CE%9F%CE%A3%202-2019.pdf

ΝΟΜΟΘΕΣΙΑ :

Αιτιολογική Έκθεση Ν. 4285/2014. *«Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση - πλαίσιο 2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328)»*. Διαθέσιμο στο https://lawdb.intrasoftnet.com/nomos/2_nomothesia_graph.php

Αιτιολογική Έκθεση Ν. 4411/2016. *«Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών – Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης – πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις»*. Διαθέσιμο στο https://lawdb.intrasoftnet.com/nomos/2_nomothesia_graph.php

Ν. 3875/2010. *Κύρωση και Εφαρμογή της Σύμβασης των Ηνωμένων Εθνών κατά του Διεθνικού Οργανωμένου Εγκλήματος και των τριών Πρωτοκόλλων αυτής και συναφείς διατάξεις. Διαθέσιμο στο https://lawdb.intrasoftnet.com/nomos/2_nomothesia_artl_current.php*

ΠΑΡΟΥΣΙΑΣΕΙΣ ΕΠΙΣΗΜΩΝ ΦΟΡΕΩΝ :

ΕΘΝΙΚΗ ΑΡΧΗ ΚΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (2020). ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 -2025 - ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ. Δημοσιεύτηκε στο *https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7*

%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ (2020). *Η κυβερνοασφάλεια στην νέα ψηφιακή εποχή.*

Διαθέσιμο:

https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/risk/gr_SEV_Deloitte_Cybersecurity_noexp.pdf

Eurojust (2020). Συνοπτική Παρουσίαση.

Διαθέσιμο στο *https://www.eurojust.europa.eu/sites/default/files/2020-11/Cybercrime-Report_Summary_EL.pdf*

ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΕΛΙΔΕΣ :

- http://www.astynomia.gr
- https://www.cepol.europa.eu/
- https://www.consilium.europa.eu
- *https://cyberalert.gr*
- https://www.enisa.europa.eu
- https://www.eurojust.europa.eu
- https://www.europol.europa.eu/
- https://www.interpol.int
- http://www.kemea.gr

-https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/eyropaiko-plaisio-gia-tis-epitheseis-kata-ton-systimaton

- https://mindigital.gr/kyvernoasfaleia
- https://www.saferinternet.gr
- https://saferinternet4kids.gr › cyberb