ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος Εργασίας : Κρυπτογράφηση και εσωτερική ασφάλεια στην Ε.Ε

Ονοματεπώνυμο:Ελευθέριος ΤΑΜΒΑΚΟΣ

Αθήνα 2017

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τριμελής Εξεταστική Επιτροπή

Λίλιαν Μήτρου: Επιβλέπουσα καθηγήτρια

ΡΙΖΟΜΥΛΙΩΤΗΣ Παναγιώτης: καθηγητής

ΝΙΚΟΛΑΙΔΗ Μαρία : καθηγήτρια

Ο ΤΑΜΒΑΚΟΣ Ελευθέριος

δηλώνω υπεύθυνα ότι:

1)Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2)Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ

Η ανάπτυξη των τηλεπικοινωνιών και του ηλεκτρονικού εμπορίου, έχουν οδηγήσει σε μια συνεχώς διευρυμένη αγορά τεχνολογιών, αλλά και στην εξερεύνηση και διαρκή γνωριμία ενός νέου κόσμου, του ψηφιακού, για τον οποίο οι περισσότεροι από εμάς δεν έχουν αντιληφθεί τις πραγματικές του διαστάσεις και δυνατότητες.

Μέσα σε αυτό τον ψηφιακό κόσμο, η εγκαθίδρυση της Κοινωνίας της Πληροφορίας (ΚτΠ) και η ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ) είχε ως αποτέλεσμα την ταυτόχρονη διείσδυση του εγκλήματος στον ψηφιακό χώρο/κυβερνοχώρο και την εκμετάλλευσή του για την προαγωγή – διευκόλυνση εγκληματικών σκοπών.

Ένα από τα κυριότερα εμπόδια των Αρχών Επιβολής του Νόμου στον ψηφιακό κόσμο είναι η χρήση της κρυπτογράφησης, η οποία σε συνδυασμό με την ταχύτητα, ασφάλεια, τον συντονισμό και την γεωγραφική διαπερατότητα, σε εγκλήματα διεθνικού και διασυνοριακού χαρακτήρα, εξασφαλίζουν, την ανωνυμία των χρηστών και αδυναμία ταυτοποίησης και από τις Αρχές Επιβολής του Νόμου.

Υπάρχει όμως και η άλλη διάσταση , μιας και η κρυπτογράφηση χρησιμοποείται, από τις επιχειρήσεις/βιομηχανια για να προστατεύσουν την πνευματική τους ιδιοκτησία και να διατηρήσουν ασφαλείς δεσμούς με τους συνεταίρους, προμηθευτές΄ ή/και πελάτες τους.

Οι τράπεζες επίσης για να διασφαλίσουν την εμπιστευτικότητα και αυθεντικότητα των οικονομικών συναλλαγών και τέλος οι Αρχές Επιβολής του Νόμου για να αποτρέψουν τη διείσδυση στις επικοινωνίες των Αρχών ασφάλειας από «εισβολείς». Επίσης στην ιδιωτική σφαίρα, οι πολίτες με την χρήση της κρυπτογράφησης δύνανται να προστατεύσουν τα προσωπικά τους δεδομένα και την επικοινωνία.

Μπορούμε λοιπόν, να θεωρήσουμε ότι η κρυπτογράφηση είναι σημαντική για τη δόμηση μιας ασφαλούς παγκόσμιας πληροφοριακής υποδομής ,για τις επικοινωνίες και το ηλεκτρονικό εμπόριο, αλλά δεν είναι πανάκεια και δυσχεραίνει την ανακάλυψη ευρημάτων/στοιχείων και την συλλογή κρίσιμων πληροφοριών, κατά τη διάρκεια των ποινικών ερευνών, θέτοντας έτσι σοβαρά ζητήματα ασφάλειας.

Η παρούσα διπλωματική, αναφέρεται στην ανάλυση των σύγχρονων απειλών ασφάλειας στον ψηφιακό κόσμο, καθώς και την αναγκαιότητα/ εφικτότητα δημιουργίας ενός κοινού κώδικα/νόρμας των Εθνικών/Ευρωπαικών Αρχών Επιβολής του Νόμου για την καταπολέμηση των απειλών που απορρέουν, από την χρήση της κρυπτογράφησης σε συνάρτηση με την Εθνική, Ευρωπαϊκή, περιφερειακή και παγκόσμια ασφάλεια.

Αρχικά, στο πρώτο κεφάλαιο αναλύεται η έννοια του φυσικού και ψηφιακού κόσμου,ώστε να γίνουν κατανοητά στην συνέχεια, τα όρια και οι βασικές διαφορές των δύο αυτών κόσμων. Αμέσως μετά, στο δεύτερο κεφάλαιο περιγράφεται η ευρεία έννοια της ασφαλείας (εσωτερική και εξωτερική ασφάλεια) και το θεματολόγιο της Ε.Ε για την ασφάλεια, τα έτη 2015-2020.Στο τρίτο κεφαλαίο γίνεται προσπάθεια ανάλυσης του Ευρωπαϊκού και Διεθνούς περιβάλλοντος ασφάλειας μέσα από την καταγραφή γεγονότων με την μέθοδο P.E.S.T.E.L.Στο τέταρτο κεφάλαιο γίνεται μια παράθεση των κυριότερων απειλών στον κυβερνοχώρο με έμφαση στη σχέση της καθεμίας με την κρυπτογράφηση. Περαιτέρω, στο πέμπτο κεφάλαιο αναλύεται συνοπτικά η έννοια της κρυπτογράφησης και πιο εκτενώς η χρήση της σήμερα , σε σχέση με το έγκλημα και τις απειλές για την ασφάλεια στην Ευρώπη. Στο έκτο κεφάλαιο αναλύεται η νομοθεσία σε εθνικό και ευρωπαϊκό επίπεδο ενώ στο αμέσως επόμενο κεφάλαιο τίθενται κάποιοι προβληματισμοί ως προς την ιδιωτικότητα και την χρήση της κρυπτογράφησης Στο όγδοο κεφάλαιο περιγράφονται οι προτάσεις, και τα συμπεράσματα.

Abstract

The development of telecommunications and e-commerce has led to an ever-expanding technology market, but also to the exploration and constant acquaintance of a new world, the digital one, for which most of us have not idea on its real dimensions and capabilities.

In this digital world, the establishment of the Information Society (IS) and the development of Information and Communication Technologies (ICT) have resulted in the simultaneous penetration of crime in the digital space / cyber space and its exploitation in the promotion for criminal purposes.

One of the main obstacles of the Law Enforcement Agencies (LEAS) in the digital world is the use of encryption, which in combination with speed, security, coordination and geographic permeability, especially in transnational and cross-border crimes, ensures the anonymity of the users. But encryption is needed by businesses to protect their intellectual property and establish secure ties with their partners, suppliers and customers, like the banks to ensure the confidentiality and authenticity of financial transactions as well as Law Enforcement Agencies to prevent penetration of police communications. Also in the private sphere, EU citizens using encryption protects their personal data and their means of communications.

We can therefore assume that encryption is important for building a secure global information infrastructure for communications and e-commerce while also creating barriers to discovering findings and obtaining information during criminal investigations, thus seriuosly posing Security issues.

This diploma deals with the analysis of modern security threats in the digital environment and the necessity / feasibility of creating a common code for addressing the national / European law enforcement authorities against the threats that arise from the use of encryption for criminal purposes in nexus with national, European, regional and global security .Initially, the first chapter analyzes the concept of the physical and digital world in order to understand later the boundaries and the basic differences of these two worlds. The second chapter then describes the broad concept of security (internal and external security) and an EU security agenda for the years 2015-2020. In the third chapter an effort is made to analyze the European and international security environment by recording events using the method PESTEL. In the fourth chapter there is a citation of the main cyber threats with emphasis on everyone's relationship to encryption. Furthermore, the fifth chapter briefly analyzes the concept of encryption and more extensively uses it today, with regard to crime and security threats in Europe. The sixth chapter discusses legislation at National and European level, and

in the next chapter some privacy and encryption concerns are raised. The eighth chapter analyzes some suggestions, initiatives and concludes about the whole study of the use of the encryption and the EU internal security.

ΕΙΣΑΓΩΓΗ

Ζούμε σε μια εποχή, που από πολλές απόψεις, μπορεί να χαρακτηριστεί μεταβατική.Ένας παράγοντας που ενισχύει αυτόν τον χαρακτηρισμό, είναι οι μεταβολές που συντελούνται σε πολλούς τομείς της ανθρώπινης δραστηριότητας και οι οποίες κατά κύριο λόγο οφείλονται στις τεχνολογίες που έχει εξελίξει ο άνθρωπος κατά τον τελευταίο αιώνα.

Αναφερόμαστε στην τεχνολογία του διαδικτύου, η οποία έχει προέλθει από τη σύγκλιση σε ένα ενιαίο πλαίσιο των Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (ΤΠΕ), οι οποίες ενσωματώνουν τη συσσωρευτική γνώση του ανθρώπου σε πολλά πεδία.

Το Διαδίκτυο, αποτελεί μία νέα παγκόσμια πλατφόρμα δραστηριότητας στην οποία έχουν εύκολη πρόσβαση οι άνθρωποι προκειμένου να επικοινωνήσουν, να συνεργαστούν, να λάβουν ή να παρέχουν υπηρεσίες, να ψυχαγωγηθούν και γενικά για να δραστηριοποιηθούν με σχεδόν όσους τρόπους δραστηριοποιούνται και στην πραγματική ζωή.

Κάποτε και για μισό αιώνα η τηλεόραση ήταν η νέα απειλή και το μήνυμα ανέφερε: «Η τηλεόραση θα άλλαζε τον κόσμο όπως τον γνώριζαν έως τότε οι άνθρωποι» [1].Το ίδιο ακριβώς θα μπορούσε να ειπωθεί σήμερα για το διαδίκτυο.

Το διαδίκτυο έχει ή/και πρόκειται να προκαλέσει ακόμα μεγαλύτερη επανάσταση σε σχέση με την τηλεόραση, ενώ οι επιδράσεις του είναι ήδη βαθύτερες από αυτές της «μικρής οθόνης». Τα τελευταία χρόνια έχει γνωρίσει ραγδαία εξάπλωση, καθώς κατάφερε να αποκτήσει σχεδόν 2 δισεκατομμύρια χρήστες και ένα (1) δισεκατομμύριο ιστοσελίδες παγκοσμίως, προσφέροντας έναν αστείρευτο όγκο πληροφοριών, μια ακατάπαυστη ροή ενημέρωσης, ανταλλαγής μηνυμάτων, ψυχαγωγίας και γενικότερα υλικού που παράγεται και διοχετεύεται από τους ίδιους τους χρήστες.

Ασφαλώς αυτές οι αλλαγές δεν είναι μόνο θετικές, αλλά έχουν και αρνητικές προεκτάσεις. Άρχισαν δηλαδή να προκύπτουν ζητήματα, τεχνολογικής, οικονομικής, πολιτικής αλλά και κοινωνικής φύσης.

Μια παράμετρος μπορεί να θεωρηθεί το γεγονός ότι αυτά τα τεχνολογικά συστήματα και οι νέες τεχνολογίες έδωσαν την δυνατότητα στους εγκληματίες ,και το οργανωμένο έγκλημα (πολλαπλά τεχνικά συστήματα λογισμικού και «hardware», κρυπτογράφηση, διεθνής

[1]Οι **New York Times**,το 1948 ,έγραφαν ότι το « [….Το Αμερικανικό νοικοκυριό βρίσκεται στο κατώφλι μιας επανάστασης...η νοικοκυρά σπανίως γνωρίζει που ειναι η κουζίνα,τα παιδια αφήνουν το απογευματινό τους ,ενώ ο πατερας αφήνει ανοιχτή στο χολ την τσάντα του και όλα αυτά γίνονται λόγω της ύπαρξης της τηλεόρασης…]»

κινητικότητα) την δυνατότητα να δρα με ανωνυμία μην αφήνοντας ίχνη όπως παραδοσιακά τα γνωρίζουμε (ψηφιακά) δυσχεραίνοντας το έργο των Αρχών επιβολής του Νόμου.

Παράλληλα μέσα από την διαμόρφωση μιας κοινωνιας της πληροφορίας (ΚτΠ[2].) έγινε δυνατή η ελευθερία της έκφρασης και άσκησης των θεμελιωδών δικαιωμάτων ,προωθήθηκε η πολιτική και κοινωνική ένταξη παγκοσμίως, καταργήθηκαν τα σύνορα μεταξύ χωρών κοινοτήτων και πολιτών και έγινε απλούστερη η κοινή χρήση πληροφοριών και ιδεών ανά την υφήλιο.

Αναφερόμενοι στην ταχύτητα και την δύναμη των νέων τεχνολογιών μας έρχεται στο νου το κύμα διαδηλώσεων στις χώρες της υποσαχάριας Βόρειας Αφρικής και την Μέσή Ανατολή ,η αποκαλούμενη Αραβική Άνοιξη[3].ως χαρακτηριστικό παράδειγμα διάδοσης ειδήσεων(και με την μορφή viral) σε ταχύτατο χρόνο στο κινητό κάθε χρήστη/πολίτη αυτών των χωρών.

Αναφερόμενοι στην κρυπτογράφηση και την πρόσβαση στα δεδομένα που διακινούνται στο διαδίκτυο μας έρχεται στο νού η αλλαγή της νομοθεσίας από τις Αμερικανικές Αρχές για προληπτικούς λόγους μετα την 11ης Σεπτεμβρίου[4]για την παρακολούθηση του «internet» και των «e-mail»

---

[2]Ως κοινωνία της πληροφορίας αναφέρεται αυτή όπου η παραγωγή, διανομή, χρήση, ενσωμάτωση και διαχείριση πληροφοριών αποτελεί σημαντική οικονομική, πολιτική και πολιτιστική δραστηριότητα. Σκοπός μιας κοινωνίας της πληροφορίας είναι να κερδίσει ανταγωνιστικό πλεονέκτημα διεθνώς, δια μέσου της χρήσης της πληροφορικής (IT) με δημιουργικό και παραγωγικό τρόπο.Οι άνθρωποι που έχουν τα μέσα να συμμετέχουν σε αυτή τη μορφή κοινωνίας ορισμένες φορές ονομάζονται «ψηφιακοί πολίτες». Αυτή αποτελεί και μια από τις δωδεκάδες ετικέτες που υποδηλώνουν ότι οι σύγχρονοι άνθρωποι μπαίνουν σε μία νέα μορφή κοινωνίας.Η σύλληψη της έννοιας ανήκει στον Daniel Bell ο οποίος διαμόρφωσε το περιεχόμενο της στις Αρχές της δεκαετίας του 1960[2].Ο Bell υποστήριζε ότι ο η μεταβιομηχανική κοινωνία είναι η «κοινωνία της πληροφορίας».

[3]Αραβική Άνοιξη (αραβικά: الربيع العربي) ονομάστηκε ένα κύμα διαδηλώσεων και διαμαρτυριών στη Μέση Ανατολή και τη Βόρεια Αφρική που εκδηλώθηκε από τις 18 Δεκεμβρίου του 2010.Πριν τη συγκεκριμένη χρονική περίοδο, το Σουδάν ήταν η μόνη Αραβική χώρα που ανέτρεψε επιτυχώς δικτατορικά καθεστώτα το 1964 και το 1985. Εκδηλώθηκαν εξεγέρσεις στην Τυνησία και την Αίγυπτο, εμφύλια σύρραξη στη Λιβύη, εξεγέρσεις στο Μπαχρέιν, τη Συρία και την Υεμένη. Μεγάλες διαδηλώσεις έγιναν επίσης στην Αλγερία, το Ιράν, το Ιράκ, την Ιορδανία, το Μαρόκο και το Ομάν. Μικρότερες οργανωμένες διαμαρτυρίες έγιναν στο Τζιμπουτί, το Κουβέιτ, τον Λίβανο, τη Μαυριτανία, τη Σαουδική Αραβία, και το Σουδάν. Κοινό γνώρισμα των διαδηλώσεων ήταν οι μαζικές διαμαρτυρίες με καμπάνιες, απεργίες, πορείες, καθώς και η χρήση κοινωνικών δικτύων όπως το Facebook, το Twitter και το YouTube, για την οργάνωση, την επικοινωνία, και την ενημέρωση περί των προσπαθειών των κρατών για καταπίεση και λογοκρισία.Το σύνθημα των διαδηλωτών στον Αραβικό κόσμο ήταν *Ash-sha'ab yurid isqat an-nizam* που σημαίνει ο λαός θέλει να πέσει το καθεστώς (شعبيريدإسقاطالنظامال)

[4]Στις 11 Σεπτεμβρίου 2001, εκδηλώθηκαν τρομοκρατικές επιθέσεις εναντίον στόχων στις Ηνωμένες Πολιτείες. Σε τέσσερα πολιτικά αεροσκάφη εκδηλώθηκε αεροπειρατεία, και τα τρία από αυτά οδηγήθηκαν από τους αεροπειρατές και προσέκρουσαν στους Δίδυμους Πύργους του Παγκόσμιου Κέντρου Εμπορίου και το Πεντάγωνο, ενώ το τέταρτο συνετρίβη σε ανοικτό χώρο. Οι Δίδυμοι Πύργοι κατέρρευσαν λίγη ώρα μετά τις συγκρούσεις των αεροσκαφών επάνω τους, προκαλώντας χιλιάδες

Η Ευρώπη άργησε να συνειδητοποιήσει την απειλή και τους κινδύνους αυτής της ραγδαίας αύξησης της τεχνολογίας και της κρυπτογράφησης καθώς τα μηνύματα για την κατάσταση στο διεθνές περιβάλλον ασφαλειας έδειχναν το αντίθετο.

Έτσι, μια σειρά τρομοκρατικών επιθέσεων[5] μετά το 2012 σε διάφορες Ευρωπαικές πρωτεύουσες κατέδειξαν τα νέα όπλα του παγκόσμιου τζιχάντ και αλλά και την χρήση του διαδικτύου και της κρυπτογράφησης από τους εξτρεμιστές .

Το «ρευστό» περιβάλλον ασφαλείας, οι νέες τεχνολογίες ,το μεταναστευτικό ζήτημα που διογκώθηκε από την κατάσταση στη Συρία και το Ιράκ ενέτειναν το κλίμα ανασφάλειας εντός της Ε.Ε δημιουργώντας όσο ποτέ άλλοτε την ανάγκη για καθαρές λύσεις σε επίπεδο Ε.Ε.

Όλα τα ανωτέρω εύλογο ήταν να προκάλεσουν συζητήσεις για ταχείες νομοθετικές αλλαγές στην χρήση των νέων τεχνολογιών στους κύκλους της Ε.Ε. Έτσι ξεκίνησε η αναπροσαρμογή για στις αντιτρομοκρατικές και αντεγκληματικές πολιτικές και δράσεις της Ε.Ε για την εσωτερική ασφάλεια στην Ε.Ε.

απώλειες: εκτός των 19 αεροπειρατών, συνολικά από τις επιθέσεις, 2973 άνθρωποι έχασαν την ζωή τους και 24 μένουν αγνοούμενοι.

[5]Τρομοκρατικές Επιθέσεις που πραγματοποίησαν ριζοσπαστικοποιημένοι ευρωπαίοι πολίτες «μοναχικοί λύκοι, ξένοι μαχητές) κατά την επιστροφή τους από το πεδίο των εμφύλιων συγκρούσεων στην Μ. Ανατολή.

ΚΕΦΑΛΑΙΟ 1^{ο} : ΦΥΣΙΚΟΣ-ΨΗΦΙΑΚΟΣ ΚΟΣΜΟΣ

Οι ενέργειες/δράσεις μας ως άνθρωποι λαμβάνουν χώρα σε δύο ειδών χώρους τον υλικό/ φυσικό χώρο και τον άυλο ψηφιακό κόσμο (ή Κυβερνοχώρο).

Απαραίτητη προϋπόθεση, για την κατανόηση των δύο κόσμων αλλά, και της κατανόησης των εγκλημάτων που υφίστανται μέσα σε αυτούς και κυρίως στον ψηφιακό κόσμο είναι η προσπάθεια προσέγγισης της έννοιας του κυβερνοχώρου και των χωρικών τους εννοιών.

1.1 ΦΥΣΙΚΟΣ ΚΟΣΜΟΣ

Η έννοια του «χώρου» απαιτεί σταθερά σημεία αναφοράς (και ο κυβερνοχώρος στερείται διαστάσεων, σαφώς καθορισμένων ορίων και αμετακίνητων σημείων προσανατολισμού). Με τον όρο «κυβερνοχώρος[6] [7]» νοείται το περιβάλλον που έχει δημιουργηθεί από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές[8].

Ωστόσο, το μόνο βέβαιο σημείο αναφοράς μέσα σε αυτόν είναι ο άνθρωπος και οι πράξεις του. Θα μπορούσαμε λοιπόν επιπλέον, να ορίσουμε τον κυβερνοχώρο ως, το σύνολο των αποτυπωμένων σε μαγνητικό υλικό, ανθρώπινων πράξεων[9].

Από την άλλη, τα φυσικά ,υλικά όρια δεν είναι απλές αυταρχικές δημιουργίες. Αν και στηρίζονται ενίοτε σε ιστορικά ατυχήματα, τα φυσικά όρια, σε σχέση με το νόμο, έχουν λογική εφαρμογή και ύπαρξη στον πραγματικό κόσμο.

Η σύνδεσή τους με την ανάπτυξη και εφαρμογή νομικών κανόνων στηρίζεται λογικά σε έναν αριθμό σχετικών θεωρήσεων:

Ισχύς (power)

Ο έλεγχος επί του φυσικού διαστήματος των ανθρώπων και των αγαθών στηρίζεται στο γεγονός ότι το φυσικό διάστημα (χώρος) είναι προσδιοριστικό χαρακτηριστικό της εθνικής κυριαρχίας (sovereignty) και της κρατικής υπόστασης (statehood).

Αντίκτυπος (effect)

---

[6]Σύμφωνα με τη Λενιώ Μυριβήλη (PhD) «ο κυβερνοχώρος αναφέρεται ως ψηφιακός τόπος της τεχνοεπιστήμης, για άλλους είναι ένας ιδιαίτερος χώρος διεπαφής υποκειμένων, πρακτικών και τεχνολογιών. Μερικές φορές ο κυβερνοχώρος παρουσιάζεται ως χώρος διαφυγής απ΄ την «πραγματικότητα», αφού σε αυτόν μπορούμε να μεταμορφωνόμαστε κατά βούληση. Άλλες φορές πάλι φαντάζει ως υβριδικός χώρος μέσα στον οποίο συμφιλιώνονται και μετουσιώνονται πολιτισμικοί πόλοι» Περιγραφή Περιγραφή μαθήματος Κουλτούρα και κυβερνοχώρος στο Πανεπιστήμιο Αιγαίου, Τμ. Πολ. Τεχν. και Επικοινωνίας, Τμ. Πολ. Τεχν. και Επικοινωνίας[3

[7]Αγγλική λέξη (cyberspace),πρωτοχρησιμοποιήθηκε από τον William Gibson στο "Burning Chrome"http://www.eeei.gr/interbiz/articles/cybspace.htm

[8]http://hyperion.math.upatras.gr/courses/newcommmedia99-00/papers99-00/coyne-kybe.html

[9]http://www.eeei.gr/interbiz/articles/cybspace.htm

Η αλληλεπίδραση μεταξύ φυσικών ορίων και των ορίων της νομικής ύλης αντανακλά τη βαθιά ριζωμένη σχέση μεταξύ φυσικής εγγύτητας και συνεπειών κάθε ειδικότερης συμπεριφοράς.

Νομιμότητα (legitimacy).

Τα πρόσωπα – εντός γεωγραφικά προσδιορισμένων ορίων – είναι η υπέρτατη πηγή της νομοπαραγωγικής αρχής σχετικά με δραστηριότητες εντός αυτών των ορίων.

Ειδοποίηση (notice)

Τα φυσικά όρια είναι επίσης κατάλληλα για την περιγραφή και σχεδίαση του νομικού διαστήματος, στο φυσικό κόσμο, επειδή παράγουν σημάνσεις αλλαγής κανόνων, όταν τα όρια παραβιάζονται.

1.2 Ψηφιακος κοσμος & Κυβερνοχωρος

Ο «κυβερνοχώρος» αναφέρεται ως ψηφιακός τόπος της τεχνοεπιστήμης, ενώ για άλλους είναι ένας ιδιαίτερος χώρος διεπαφής υποκειμένων, πρακτικών και τεχνολογιών.

Μερικές φορές ο «κυβερνοχώρος» παρουσιάζεται ως χώρος διαφυγής από την «πραγματικότητα», αφού σε αυτόν μπορούμε να μεταμορφωνόμαστε κατά βούληση. Άλλες φορές πάλι φαντάζει ως υβριδικός χώρος μέσα στον οποίο συμφιλιώνονται και μετουσιώνονται πολιτισμικοί πόλοι»[10].

Είναι επίσης αυτός που υπονομεύει δραστικά τη νομική διασύνδεση μεταξύ φυσικής περιοχής (τόπος τέλεσης) και πράξης, εφόσον η τελευταία λαμβάνει χώρα στον ιστό.

Το διαδίκτυο είναι εκείνο που καταστρέφει το δεσμό μεταξύ γεωγραφικού προσδιορισμού και:

- Της αρμοδιότητας/παρέμβασης των τοπικών κυβερνήσεων επί της διαδικτυακής συμπεριφοράς.
- Των αποτελεσμάτων της διαδικτυακής συμπεριφοράς επί ατόμων και αγαθών.
- Της νομιμότητας των προσπαθειών του κράτους να επιβάλλει εφαρμόσιμους κανόνες σε παγκόσμια φαινόμενα.
- Της ικανότητας της φυσικής περιοχής να παραγάγει ειδοποιήσεις αναφορικά με το ποια κανονιστικά σύνολα εφαρμόζονται.

Ο κυβερνοχώρος υπερβαίνει τα εδαφικά όρια και η ταχύτητα διαβίβασης μηνυμάτων στο δίκτυο είναι σχεδόν ανεξάρτητη από τη φυσική θέση.

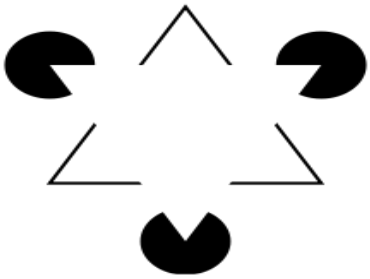
[10]Σύμφωνα με τη Λενιώ Μυριβήλη (PhD) Περιγραφή μαθήματος Κουλτούρα και κυβερνοχώρος στο Πανεπιστήμιο Αιγαίου, Τμ. Πολ. Τεχν. και Επικοινωνίας

Τα μηνύματα διαβιβάζονται από τη μία φυσική θέση στην άλλη, χωρίς εξασθένηση, παρακμή, ουσιώδη καθυστέρηση και χωρίς φυσικά εμπόδια, που διαφορετικά θα κρατούσαν γεωγραφικά απομονωμένα μέρη και ανθρώπους ,διαχωρισμένα μεταξύ τους.

Όταν επικοινωνεί κανείς με κάποιον άλλο σε απευθείας σύνδεση δεν υπάρχει καμία αίσθηση του φυσικού χώρου, καθώς τα κυβερνοταξίδια δεν μπορούν να μετρηθούν με την κυριολεκτική έννοια του όρου μέτρηση.{ …«Διασκορπισμένος στο Διαδίκτυο», «ο χώρος μου δεν μπορεί πλέον να καθοριστεί με καθαρά φυσικά κριτήρια…[11]}

Ο «κυβερνοχώρος»[12] έχει καταστεί σαφέστατα μέσο και πεδίο εγκλήματος (όπως και το 5ο πεδίο πολέμου[13],) και παράλληλα με τη διάδοση της τεχνολογίας των υπολογιστών σε όλες τις πλευρές της ζωής, και την διασύνδεση των υπολογιστών σε διεθνή δίκτυα το έγκλημα έγινε πιο επικίνδυνο και διεθνοποιημένο[14].

Τα νέα συστήματα έχουν ειδικά χαρακτηριστικά που διευκολύνουν τους δράστες αλλά δυσχεραίνουν το έργο των διωκτικών αρχών (πολλαπλά συστήματα λογισμικού και «hardware», έλλειψη εμπειρίας πολλών χρηστών, ανωνυμία, κρυπτογράφηση, διεθνής κινητικότητα).



Ο «κυβερνοχώροσ» μοιάζει με το λευκό τρίγωνο της εικόνας 1, εμφανίζεται εικονικά, και ενώ δεν « υπάρχει» είναι εικονικό καταφέρνει και ενώνει υπολογιστές σε όλον τον κόσμο.

1.3 Ψηφιακος Κοσμος

1.3.1 Βαθυς Ιστος (DeepWeb)

[11]Στο βιβλίο της, The Pearly Gates of Cyberspace, (Οι μαργαριταρένιες πύλες του κυβερνοχώρου) η επιστημονική συγγραφέας Margaret Wertheim υποστηρίζει ότι το Διαδίκτυο μας παρέχει μια νέα έννοια του χώρου –τον αλληλοσυνδεόμενο «χώρο» του παγκόσμιου δικτύου υπολογιστών

[12] Άλλες ονομασίες για τη λέξη «κυβερνοχώρος», εκτός από cyberspace είναι οι εξής: net (δίκτυο), information superhighway (λεωφόρος των πληροφοριών,ή διαδίκτυο).

[13]Κυβερνοπόλεμος (Cyberwar): Σύνολο ενεργειών που λαμβάνουν χώρα από ένα κράτος προκειμένου αυτό να διεισδύσει στα δίκτυα Η/Υ άλλης Χώρας , με σκοπό να προκαλέσει ζημία ή αναταραχή σε αυτά.

[14]Βλ. ΛΙΛΙΑΝ ΜΗΤΡΟΥ Δίκαιο και κοινωνία στον 21ο αιώνα εκδόσεις Σακκουλά.

Ο όρος αναφέρεται σε κάθε διαδικτυακό περιεχόμενο, το οποίο για ποικίλους λόγους, δεν μπορεί να καταλογογραφεί (indexed) από μηχανή αναζήτησης, π.χ. Google. Αυτός ο ορισμός περιλαμβάνει δυναμικές ιστοσελίδες, «μπλοκαρισμένες» σελίδες, ιδιωτικές σελίδες, κ.λπ[15].

Ο Βαθύς Ιστός (επίσης γνωστός[16] και ως **Deepnet**, **Undernet**, το **αόρατο Web** ή το **κρυμμένο Web**) είναι το περιεχόμενο του παγκόσμιου ιστού (WorldWideWeb), που δεν ανήκει στον Επιφανειακό Ιστό (SurfaceWeb.) [17,18]

1.3.2 Σκοτεινος Ιστος (Dark Web)

Ο «Σκοτεινός Ιστός» ορίζεται ως το τμήμα του διαδικτύου, το οποίο σκόπιμα αποκρύπτεται από τις μηχανές αναζητήσεις μέσω «μεταμφιεσμένων» διευθύνσεων IP και είναι προσβάσιμος μόνο σε σκιώδεις χρήστες.

Ένα χαρακτηριστικό γνώρισμα του σκοτεινού διαδικτύου είναι και τα δίκτυα ανωνυμίας, όπως το «Tor», που λειτουργεί μέσω μιας σειράς ανώνυμων συνδέσεων.

Το «Tor» είναι ουσιαστικά μηχανισμός δρομολόγησης, που σχεδιάστηκε για τη διατήρηση της ανωνυμίας του χρήστη του διαδικτύου, δημιουργώντας εναλλακτικά μονοπάτια για τη δρομολόγηση της κυκλοφορίας.

Ο μηχανισμός που χρησιμοποιεί το «Tor» ονομάζεται «onion routing» (δρομολόγηση κρεμμύδι) δημιουργήθηκε για πρώτη φορά από το Εργαστήριο Ναυτικών Ερευνών των ΗΠΑ.[19]

1.3.3 Βαθυς Ιστος vs Σκοτεινος Ιστος

α. Το κοινό σημείο των δύο «ιστών» αφορά στο γεγονός ότι αμφότεροι είναι κρυμμένοι από τις εμπορικές μηχανές αναζήτησης.

[15]Below the Surface: Exploring the Deep Web, 2015, https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

[16]Ο Mike Bergman, ιδρυτής του BrightPlanet, που επινόησε τη φράση, είχε πει πως το να ψάχνει κανείς στο Internet σήμερα είναι σαν να σέρνει ένα δίχτυ στην επιφάνεια του ωκεανού: πολλά μπορεί να πιαστούν στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκονται βαθιά και επομένως δεν μπορούν να πιαστούν. Οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες, και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Το deep Web είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό Web.

[17]Είναι ο καταλογοποιημένος ιστός, που αντιπροσωπεύει το διαθέσιμο στο κοινό, αναζητήσιμο με κοινές μηχανές αναζήτησης, τμήμα του παγκόσμιου ιστού.

[19]Πηγή: ιστοσελίδα https://www.onion-router.net/

Ο μεν «Βαθύς Ιστός» είναι αχανής και υπερβαίνει το 90% του μεγέθους του διαδικτύου, ο δε «Σκοτεινός Ιστός», πιθανότατα, δεν υπερβαίνει το 0,1%. Ο «Βαθύς Ιστός» περιλαμβάνει εκτός του «Βαθύ Ιστού» καθεαυτού, περιλαμβάνει και «καθημερινό» περιεχόμενο, όπως διαδικτυακά fora που απαιτούν εγγραφή ή δυναμικά δημιουργούμενες σελίδες, όπως ένας λογαριασμός Gmail κ.λπ.

Για τον «Σκοτεινό Ιστό» θεωρούμε αυτόν που εννοούν οι άνθρωποι, συνήθως, όταν αναφέρονται στα «άθλια», «κρυφά» σημεία του διαδικτύου (όπου μπορεί κανείς να αγοράσει ναρκωτικά, όπλα, υλικό παιδικής πορνογραφίας κ.λπ.).

β. Ο χρήστης του διαδικτύου δεν αφήνει κατά την πλοήγησή του, «ηλεκτρονικά ίχνη» που χαρακτηρίζονται από μοναδικότητα (ουσιαστικά πρόκειται για την **«**ηλεκτρονική του ταυτότητα»). Το «ηλεκτρονικό ίχνος» προσδιορίζεται από τρεις (3) υπό-ιδιότητες, στις οποίες οφείλεται η προαναφερόμενη μοναδικότητα: τη διεύθυνση πρωτοκόλλου (IP Address), την ημεροχρονολογία και τη ζώνη ώρας.

ΚΕΦΑΛΑΙΟ 2^{ο} : ΈΝΝΟΙΑΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ (SECURITY) /ΘΕΩΡΗΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

2.1 ΑΣΦΑΛΕΙΑ /ΠΡΟΣΕΓΓΙΣΗ ΤΗΣ ΕΝΝΟΙΑΣ

Η έννοια της Ασφάλειας, είναι ένα πλέγμα πολλών παραγόντων .Ο όρος Ασφάλεια, εννοιολογικά, είναι ιδιαίτερα ευρύς, ωστόσο προσδιορίζεται ως η επιδίωξη της ελευθερίας από απειλές, καθώς και η ικανότητα των κρατών και των κοινωνιών να διατηρούν την ανεξάρτητη ταυτότητά τους ενάντια σε δυνάμεις μεταβολής, τις οποίες θεωρούν εχθρικές.

Δεν είναι δυνατόν, να προβαίνει κάποιος σε εκτιμήσεις ή σε λήψη αποφάσεων, αγνοώντας την επίδραση της φτώχειας στην κοινωνική συνοχή, την έλλειψη ασφάλειας τροφίμων ή την ανεπάρκεια ύδατος σε σχέση με τη βία και την κοινωνική αποσταθεροποίηση, την επίδραση της διαφθοράς και του οργανωμένου εγκλήματος, την τρομοκρατία και τις υβριδικές απειλές στην οικονομική πρόοδο και κοινωνική ευημερία.

Ακόμη ως ασφάλεια μπορούμε να θεωρήσουμε την επιβίωση, και μια σειρά από ενδιαφέροντα που σχετίζονται με την επιβίωση/ύπαρξη.

Σε κάθε περίπτωση η έννοια της ασφάλειας περιλαμβάνει τους ακόλουθους πέντε τομείς:

α. Στρατιωτική (military): Αφορά στην δύο επιπέδων (two level interplay) διατήρηση των επιθετικών/αμυντικών ικανοτήτων του κράτους και τις αντιλήψεις των κρατών για τις προθέσεις αλλήλων.

β. Πολιτική (political): Αφορά στην οργανωτική σταθερότητα των κρατών, κυβερνητικών συστημάτων και ιδεολογιών που τους παρέχουν νομιμότητα.

γ. Οικονομική (economic): Αφορά στην προσβασιμότητα του κράτους σε πόρους και αγορές, απαραίτητα στοιχεία για την ευμάρεια και την πολιτική ισχύ.

δ. Κοινωνική (Social): Αφορά στην ικανότητα των κοινωνιών να αναπαράγουν τα παραδοσιακά πολιτικά, γλωσσικά και σχεσιακά τους μοτίβα, την εθνική και θρησκευτική τους ταυτότητα, καθώς και τα έθιμά τους εντός αποδεκτών συνθηκών εξέλιξης.

ε. Περιβαλλοντική (environmental): Αφορά στη διατήρηση της τοπικής και πλανητικής βιόσφαιρας, ως του ζωτικού υποστηρικτικού συστήματος των ανθρώπινων δραστηριοτήτων.

Οι πέντε αυτοι τομείς λειτουργούν ως συγκοινωνούντα δοχεία και πρέπει να λαμβανονται υπόψιν κάθε φορά που αναφερόμαστε στην ασφάλεια.

2.2 Η Εσωτερικη ασφαλεια -Θεωρητικη Προσεγγιση της εννοιας.

Εσωτερική Ασφάλεια ***(Homeland Security***): Είναι ένας όρος που περιλαμβάνει τα πεδία της δημόσιας και κρατικής ασφάλειας (Public and State Security), τη δημόσια τάξη (Public Order), την προστασία των συνόρων (Border Control and Protection) και την πολιτική προστασία (Civil Protection). Τα πεδία αυτά αποτελούν πεδία ενδιαφέροντος των Σωμάτων Ασφαλείας / Αρχών Επιβολής του Νόμου.

Ένας άλλος ορισμός της εσωτερικής ασφάλειας μπορεί να θεωρηθεί ως: Το σκέλος του τομέα ασφαλείας που αφορά στην πρόληψη και καταστολή της εγκληματικότητας και έχει άμεση σχέση με την καθημερινή ασφάλεια του πολίτη. Η αποστολή αυτή έχει ανατεθεί θεσμικά στην Ελληνική Αστυνομία κατά κύριο λόγο και στις λοιπές Αρχές Επιβολής του Νόμου[20] (Πυροσβεστική, Ελληνική Ακτοφυλακή, Τελωνεία, ΣΔΟΕ).

2.3 Η Εξωτερικη ασφαλεια -Θεωρητικη Προσεγγιση της εννοιας.[21]

Η εξωτερική ασφάλεια, συνδέεται κυρίως με την εδαφική ακεραιότητα και την προάσπιση των θεμελιωδών συμφερόντων ενός κράτους.

Αποτελεί θεσμό του δημοσίου δικαίου διότι αντιπροσωπεύει ένα πεδίο που διέπεται από κανόνες δικαίου και χαρακτηρίζεται από τη συντεταγμένη λειτουργία θεσμών της κρατικής εξουσίας. Επιβάλλει την οργανωμένη αντίδραση απέναντι στην απειλή, την ενοποίηση και τον συντονισμό επιμέρους αρμοδιοτήτων και χειρισμών καθώς και την ενεργοποίηση του δυναμικού της Χώρας συνολικά.

Η εξωτερική ασφάλεια είναι έτσι συνδυασμένη με καταστάσεις που λαμβάνουν χώρα στο διεθνές σύστημα και οι οποίες θεμελιώνουν ένα σύστημα αμοιβαίας συλλογικής ασφάλειας.

[20] Βλ. ΠΔ 135/2013 ,Ποιες είναι οι Αρχές Επιβολής του Νόμου.
[21] AnagnostopoulosKonstantinosMsc2016

Συνεπώς, οι απειλές σε βάρος της εθνικής ασφάλειας δεν περιορίζονται μόνο στις απειλές κατά της ανεξαρτησίας και της ακεραιότητας της Χώρας, αλλά και σε απειλές κατά του διεθνούς συστήματος γενικότερα. Είναι έννοιας ευρύτερη από αυτή της άμυνας.

Στην έννοια της εξωτερικής ασφάλειας εμπίπτει ο σχεδιασμός και έλεγχος της καθημερινής δραστηριότητας των διεθνών σχέσεων, η συλλογή και επεξεργασία των πληροφοριών, η χάραξη και ο χειρισμός της πολιτικής.

Απαραίτητο στοιχείο είναι ο ελεγκτικός ρόλος της πολιτικής εξουσίας επί του συνόλου του δυναμικού της πολιτείας, του στρατού, της εθνικής άμυνας , των κατασταλτικών δηλαδή δυνάμεων, καθώς και η στενή συνεργασία μεταξύ της πολιτικής ηγεσίας και αυτής των εμπλεκόμενων φορέων της άμυνας και κυρίως του στρατού.

Οι Ένοπλες Δυνάμεις συγκροτούν μία υπηρεσία του κράτους, η οποία διέπεται από τους κανόνες οργάνωσης και λειτουργίας των κρατικών υπηρεσιών, που ισχύουν στο πλαίσιο της δημοκρατικής νομιμότητας.

2.4 Συναφεια Εσωτερικης και Εξωτερικης Ασφαλειας

Σε επίπεδο στρατηγικής έχει επανειλημμένα διατυπωθεί η ανάγκη για τη διασύνδεση της εξωτερικής και της εσωτερικής ασφάλειας.

Η πρώτη επίσημη αναφορά για τη διασύνδεση εσωτερικής και εξωτερικής ασφάλειας γίνεται στο Ευρωπαϊκό Συμβούλιο του Τάμπερε το 1999, στο κείμενο συμπερασμάτων του οποίου αναφέρεται ότι οι ανησυχίες που έχουν καταγραφεί για ζητήματα Εσωτερικών Υποθέσεων και Δικαιοσύνης της Ε.Ε θα πρέπει να ενταχθούν και σε άλλες πολιτικές και αντιλήψεις.

Δόθηκε έτσι το έναυσμα για την συμπερίληψη ζητημάτων εσωτερικής ασφάλειας στον καθορισμό άλλων πολιτικών συμπεριλαμβανομένης της εξωτερικής δράσης της Ευρωπαϊκής Ένωσης.

Σε αυτήν τη λογική, το Ευρωπαϊκό Συμβούλιο της Φέιρα το 2000 διαμόρφωσε έναν κατάλογο προτεραιοτήτων εξωτερικής πολιτικής ο οποίος σημείωνε ότι μεγάλο μέρος των προκλήσεων που αφορούν τον τομέα των Εσωτερικών Υποθέσεων και Δικαιοσύνης, προέρχονται από το εξωτερικό (εξωτερικές απειλές ,τρίτα κράτη) και άρα χρήζουν αντίστοιχης αντιμετώπισης.

Τα τελευταία χρόνια γεγονότα που καθιστούν την σχέση εξωτερικής και της εσωτερικής ασφάλειας σύμμετρη αλλά επιβεβαιώνουν τη εξάπλωση του διασυνοριακού εγκλήματος και της τρομοκρατίας είναι αρκετά όπως οι τρομοκρατικές βομβιστικές επιθέσεις στη Μαδρίτη και στο Λονδίνο αλλά και οι πρόσφατες τρομοκρατικές επιθέσεις στο Παρίσι, στην Γερμανία

και σε άλλες πόλεις στην καρδιά της Ευρώπης ,το φαινόμενο των ξένων επιστρεψάντων μαχητών/υποστηριχτών του Ισλαμικού κράτους (DAESH/ISIS/IS) από τα πεδία των συγκρούσεων στην Συρία και στο Ιράκ και τα χτυπήματα των μοναχικών λύκων “lone wolf”.

Έτσι ,το ρευστό αυτό περιβάλλον ασφάλειας στην Μέση Ανατολή, συνδέονται άμεσα τόσο με την εσωτερική ασφάλεια και το σοβαρό και οργανωμένο έγκλημα, τους διακινητές, τους ξένους μαχητές όσο και με την εξωτερική ασφάλεια των Κ-Μ (εξωτερικά σύνορα, διασυνοριακό διεθνικό έγκλημα).

Η εσωτερική ασφάλεια της Ε.Ε και η παγκόσμια ασφάλεια είναι αλληλοεξαρτημένες και αλληλένδετες. Η απάντηση της Ε.Ε πρέπει να είναι ολοκληρωμένη και να βασίζεται σε δέσμη δράσεων οι οποίες συνδυάζουν τις εσωτερικές και τις εξωτερικές διαστάσεις, με σκοπό να ενισχυθούν οι δεσμοί μεταξύ δικαιοσύνης και εσωτερικών υποθέσεων καθώς και κοινής ασφάλειας και αμυντικής πολιτικής

2.5 Πρωτοβουλιες της Ε.Ε για την διατηρηση της εσωτερικης της ασφαλειας

2.5.1 Το Ευρωπαϊκο θεματολογιο για την ασφαλεια

Στόχος της Ευρωπαϊκής Ένωσης είναι να διασφαλίσει στα Κ-Μ ότι θα διαβιούν σε έναν χώρο ελευθερίας, ασφάλειας και δικαιοσύνης χωρίς εσωτερικά σύνορα.

Πολλές από τις σημερινές ανησυχίες για την ασφάλεια οφείλονται στην αστάθεια που παρατηρείται στην άμεση γειτονία της Ε.Ε και στις μεταβαλλόμενες μορφές ριζοσπαστικοποίησης, βίας και τρομοκρατίας οι οποίες αποτυπώνονται στην ανάλυση του περιβάλλον ασφάλειας που θα παραθέσουμε αμέσως μετά.

Μολονότι την ευθύνη για την ασφάλεια φέρουν κυρίως τα κράτη μέλη, οι διακρατικές απειλές όπως η τρομοκρατία δεν μπορούν να αντιμετωπιστούν αποτελεσματικά χωρίς κοινή Ευρωπαϊκή προσέγγιση.

Αναπτύσσονται λοιπόν εργαλεία, υποδομές και το περιβάλλον που απαιτούνται σε Ευρωπαϊκό επίπεδο ώστε οι Εθνικές Αρχές να συνεργάζονται αποτελεσματικά για την αντιμετώπιση της κοινής πρόκλησης επίπεδο των κρατών μελών και των οικείων αρχών Επιβολής του Νόμου και σε στενή συνεργασία με τους οργανισμούς της Ε.Ε.

Σε αυτό το πλαίσιο τα θεσμικά όργανα της Ε.Ε ψήφισαν το ευρωπαϊκό θεματολόγιο για την ασφάλεια μια ανανεωμένη στρατηγική για την Εσωτερική ασφάλεια για την πενταετία 2015-2020 έχοντας ως προσδοκία η Ε.Ε να είναι ένας χώρος ασφάλειας όπου τα άτομα προστατεύονται με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων.

Παρότι η Ε.Ε ,πρέπει να παραμένει σε εγρήγορση απέναντι σε άλλες αναδυόμενες απειλές για τις οποίες είναι πιθανό να απαιτηθεί επίσης συντονισμένη απόκριση εκ μέρους της, το θεματολόγιο δίνει προτεραιότητα στην τρομοκρατία, το οργανωμένο έγκλημα και το έγκλημα στον κυβερνοχώρο ως αλληλοσυνδεόμενους τομείς με έντονη διασυνοριακή διάσταση.

Προκειμένου να μεγιστοποιηθούν τα οφέλη των υφιστάμενων μέτρων της Ε.Ε και, όπου αυτό είναι αναγκαίο, να υπάρξουν νέες και συμπληρωματικές δράσεις, απαιτείται ενίσχυση των πυλώνων δράσης της Ε.Ε.

Πέντε είναι οι βασικές Αρχές συνεργασίας στις οποίες δίνεται βάση από τα όργανα της Ε.Ε.

<u>α. Βασικές Αρχές συνεργασίας</u>

- Πρώτον, να διασφαλιστεί ομοιομορφία με τα θεμελιώδη δικαιώματα. Η ασφάλεια και ο σεβασμός των θεμελιωδών δικαιωμάτων δεν αποτελούν αντικρουόμενους στόχους, αλλά συμβατές και συμπληρωματικές επιδιώξεις της πολιτικής.
- Δεύτερον, απαιτείται μεγαλύτερη διαφάνεια, λογοδοσία και δημοκρατικός έλεγχος για την εμπέδωση της εμπιστοσύνης των πολιτών**.**
- Τρίτον , Να εφαρμοστεί και να τρέξει ο υφιστάμενος νομικός μηχανισμός της Ε.Ε**.**
- Τέταρτον, Συγκερασμός των ενεργειών μεταξύ των Κ-Μ στο πλαίσιο της διυπηρεσιακής και διατομεακής συνεργασίας.
- Πέμπτον, Να επιτευχθεί η συνένωση όλων των εσωτερικών και εξωτερικών διαστάσεων της ασφάλειας και να επανεκτιμηθεί ο ρόλος αυτών.

Ενίσχυση των πυλώνων δράσης της Ε.Ε

Σε επιχειρησιακό επίπεδο, η καλύτερη και στενότερη συνεργασία συνεπάγεται πρώτα από όλα εφαρμογή των υφιστάμενων μέσων από όλους τους εμπλεκόμενους φορείς - τα θεσμικά όργανα και τους οργανισμούς της Ε.Ε, τα κράτη μέλη και τις εθνικές Αρχές Επιβολής του Νόμου.

Και στο θεματολόγιο για το 2015-2020 η τρομοκρατία, το οργανωμένο έγκλημα και το έγκλημα στον κυβερνοχώρο υπογραμμίζονται ως οι τρεις βασικές προτεραιότητες για άμεση ανάληψη δράσης.- .

Ειδικότερα:

1^{ος} Βελτιωμένη ανταλλαγή πληροφοριών.

{…..Η Ε.Ε θα πρέπει να εστιασθεί κατά πρώτο λόγο στην πλήρη εφαρμογή των κανόνων που ήδη υπάρχουν, όπως το πλαίσιο Prum, και στην έγκριση των προτάσεων που έχουν ήδη

κατατεθεί, όπως η ευρωπαϊκή οδηγία για τα στοιχεία καταστάσεων ονομάτων επιβατών[22], ο κανονισμός για την Europol και η μεταρρύθμιση της προστασίας δεδομένων .Αυτό θα αποτελέσει ήδη σημαντικό βήμα προόδου με τη δημιουργία μιας σαφούς, ασφαλούς και κατάλληλα ρυθμιζόμενης δέσμης εργαλείων για την παροχή στις Αρχές πληροφοριών που χρειάζονται, υπό την προϋπόθεση ότι αξιοποιούνται στο έπακρο οι δυνατότητες που προσφέρουν αυτά τα εργαλεία. Βασικά μέσα, όπως το Σύστημα Πληροφοριών Σένγκεν, ο κώδικας συνόρων του Σένγκεν και το ECRIS, θα πρέπει επίσης να τελούν υπό επανεξέταση και να συμπληρώνουν τυχόν ασυνέχειες }

2ος Αυξημένη επιχειρησιακή συνεργασία

Η αύξηση των συνεργειών μεταξύ των οργανισμών της Ε.Ε, ο συστηματικότερος συντονισμός και η ολόπλευρη χρήση εργαλείων όπως οι Κοινές Ομάδες Έρευνας ,η καθιέρωση της ευρωπαϊκής εισαγγελίας θα αποτελέσουν πραγματική διαφορά για την πρόληψη, τον εντοπισμό και την αντιμετώπιση των απειλών για την ασφάλεια.

3ος Κατάρτιση, χρηματοδότηση, έρευνα και καινοτομία.

Η ασφάλεια πρέπει να αποτελεί βασική προτεραιότητα σε ευρύ φάσμα χρηματοδοτικών μηχανισμών, προγραμμάτων έρευνας και καινοτομίας καθώς και πρωτοβουλιών κατάρτισης. Οι υφιστάμενες προτεραιότητες θα πρέπει να προσαρμόζονται όταν απαιτείται.

β. <u>Ο κυβερνοχώρος & οι προτεραιότητες της Ε.Ε για την ασφάλεια</u>

Μέχρι το 2010 οι φορείς της Ε.Ε είχαν θέσει τρείς βασικές προτεραιότητες για την Ευρωπαϊκή ασφάλεια.

Οι πρόσφατες τρομοκρατικές επιθέσεις στο Παρίσι, στην Κοπεγχάγη, τις Βρυξέλλες,την Γερμανία το Λονδίνο και την Ισπανία (Βαρκελώνη), καταδεικνύουν την ανάγκη για σθεναρή κοινή απάντηση της Ε.Ε απέναντι στην τρομοκρατία και τους αλλοδαπούς τρομοκράτες μαχητές θέτοντας την τρομοκρατία ως πρώτη προτεραιότητα για την ασφάλεια στην Ε.Ε.

Τα τελευταία χρόνια το σοβαρό και οργανωμένο διασυνοριακό έγκλημα βρίσκει νέες διεξόδους για εγκληματικές ενέργειες καθώς και νέους τρόπους δράσης με τεράστιο ανθρώπινο, κοινωνικό και οικονομικό κόστος και βρίσκεται για ευνόητους λόγους σαν δεύτερη προτεραιότητα στην Ε.Ε.

Το έγκλημα στον κυβερνοχώρο από την άλλη έχει τεθεί σαν η Τρίτη προτεραιότητα για την

[22] Οριστικοποίηση του έργου των συνομοθετών για τη δημιουργία ενός Ευρωπαϊκού συστήματος καταστάσεων ονομάτων επιβατών (PNR).

ασφαλεια καθώς αποτελεί ολοένα αυξανόμενη απειλή για τα θεμελιώδη δικαιώματα των πολιτών και την οικονομία, καθώς και για την ανάπτυξη μιας επιτυχημένης ψηφιακής ενιαίας αγοράς.

Οι εγκληματίες του κυβερνοχώρου μπορούν να δρουν εκτός της Ένωσης καταβάλλοντας ελάχιστη προσπάθεια και αντιμετωπίζοντας ελάχιστο κίνδυνο, να βλάπτουν υποδομές ζωτικής σημασίας και μεγάλο αριθμό θυμάτων σε όλα τα κράτη μέλη ταυτόχρονα.

Τα παραπάνω επιτυγχάνονται μέσα από την κατάχρηση των τεχνικών ανωνυμοποίησης των ανώνυμων μηχανισμών πληρωμών και μηχανισμών & εργαλείων κρυπτογράφησης διενεργώντας εξ αποστάσεως παράνομο εμπόριο ναρκωτικών ή όπλων ή νομιμοποίηση εσόδων από παράνομες δραστηριότητες.

ΚΕΦΑΛΑΙΟ 3^{Ο} : ΑΝΑΛΥΣΗ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΑΣΦΑΛΕΙΑΣ/P.E.S.T.E.L.

Πριν εξετάσουμε το σύνολο των απειλών που υφίστανται επί του παρόντος στον κυβερνοχώρο εστιάζοντας γεωγραφικά στην Ευρωπαϊκή ασφάλεια και την συνάφεια τους με την κρυπτογράφηση θα ήταν δόκιμο να έχουμε μια συνολική εικόνα του σύγχρονου Περιβάλλοντος ασφάλειας. Για τον λόγο αυτό επιλέχτηκε η μέθοδος PESTEL προκειμένου να αποτυπωθεί η τρέχουσα κατάσταση τόσο στο εσωτερικό όσο και σε περιφερειακό και εθνικό επίπεδο ασφαλείας.

Πιο αναλυτικά έχουμε:

3.1 ΕΘΝΙΚΌ ΠΕΡΙΒΆΛΛΟΝ ΑΣΦΆΛΕΙΑΣ

- Πολιτικοί παράγοντες προς θεώρηση (political factors)

Επικράτηση του Ρεπουμπλικάνου υποψηφίου στις Αμερικανικές εκλογές του 2016,

Το πολιτικό περιβάλλον επηρεάζεται και από το μεταναστευτικό ζήτημα

Η παράμετρος του Ελληνικού χρέους

Το Κυπριακό ζήτημα, το οποίο εισέρχεται εκ νέου σε καμπή

Η πολιτική αστάθεια της Τουρκίας η οποία επηρεάζει σαφώς τις διμερείς σχέσεις

Το ειδικό βάρος της επίσκεψης του Προέδρου των ΗΠΑ εντός του 2016 ως θεσμού αλλά και ως προσωπικότητας, με διατηρούμενη ισχύ λόγου και επιρροής, καίτοι απερχομένου.

- Οικονομικοί παράγοντες προς θεώρηση (economic factors)

Η συνεχιζόμενη από το 2009 οικονομική κρίση της Ελλάδας

Η υψηλή ανεργία

Το υψηλό εξωτερικό χρέος της Χώρας

Η συνέχιση των διαρθρωτικών αλλαγών και των μεταρρυθμίσεων, απαραίτητη προϋπόθεση και κατά τον αμερικανό Πρόεδρο.

Η οικονομική επιβάρυνση που τίθεται στην ελληνική οικονομία από τη διαχείριση του μεταναστευτικού.

Ο Αγωγός ΤΑΡ, ως μείζων ξένη επένδυση στην Ελλάδα, και αναμένεται να εμπλέξει 150 ελληνικές εταιρείες, δημιουργώντας τουλάχιστον 8.000 θέσεις εργασίας.

- Κοινωνικοί παράγοντες προς θεώρηση (social factors)

Η μεταβληθείσα δημογραφία και ανθρωπογεωγραφία της Χώρας

Η εκδηλούμενη «κοινωνική αντιπαράθεση» τμημάτων της ελληνικής κοινωνίας (ακροαριστερά, ακροδεξιά), που επηρεάζεται από την οικονομική κρίση, την ανεργία, το μεταναστευτικό κ.ά.

Η επιβάρυνση που τίθεται στην ελληνική οικονομία από τη διαχείριση του μεταναστευτικού.

- Τεχνολογικοί παράγοντες προς θεώρηση (technological factors)

Η χρήση των μέσων κοινωνικής δικτύωσης, και ιδιαίτερα του Twitter, ως εργαλείων άμεσης κινητοποίησης μελών, ομάδων , ενόψει πράξεων ακτιβισμού, εξτρεμισμού και τρομοκρατίας.

Η δύναμη του διαδικτύου, ως μέσου προπαγάνδας, μέσω άμεσης διάδοσης (viral) γεγονότων.

Η συμπόρευση του διαδικτύου με τις νέες μορφές τρομοκρατίας τα τελευταία χρόνια.

Η χρησιμοποίηση της τεχνολογίας (διαδίκτυο)και της κρυπτογράφησης τόσο από άτομα του Οργανωμένου εγκλήματος όσο και από εξτρεμιστικά στοιχεία για τις παράνομες δραστηριότητές τους και ο διαρκής αγώνας των Αρχών Επιβολής του Νόμου .

- Περιβαλλοντικοί παράγοντες προς θεώρηση (environmental factors)

  Το συνολικό περιβάλλον ασφαλείας επηρεάζεται από υπό-περιβάλλοντα όπως: Καταστήματα κράτησης, Hot-Spots κ.λπ.
- Νομοθετικοί παράγοντες προς θεώρηση (legal factors)

Έλλειψη ολιστικής προσέγγισης, κωδικοποιημένης και εναρμονισμένης νομοθεσίας για το αντικείμενο της κρυπτογράφησης σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, η οποία θα επιτρέπει την αποτελεσματική έρευνα και δίωξη των διεθνών εγκληματικών – τρομοκρατικών δραστηριοτήτων με τη χρήση τεχνολογιών κρυπτογράφησης.

3.2 Ευρωπαϊκο Περιβαλλον ασφαλειας/παραγοντες προς θεωρηση

Η επιθετική ρητορική της Τουρκίας απέναντι στην Ε.Ε σε ό,τι αφορά στη διαχείριση των προσφυγικών/μεταναστευτικών ροών, καθώς και στις δηλώσεις του Τούρκου Προέδρου περί αναθεώρησης διεθνών συνθηκών.

Η πολιτική κατάσταση και το διαμορφούμενο περιβάλλον ασφαλείας στην Τουρκία, σε σχέση με τις πρόσφατες εξελίξεις (τρομοκρατικές ενέργειες, συνταγματική μεταρρύθμιση κ.λπ.), καθώς και οι εν γένει αλληλεπιδράσεις που αναπτύσσονται, ιδίως αναφορικά με την προσφυγική – μεταναστευτική κρίση.

Η μεταβολή στην πολιτική ηγεσία της Βουλγαρίας.

Οι δηλώσεις του Διευθυντή της Europol Ρομπ Γουεϊνράιτ (28-11-2016)[23], αλλά και αξιωματούχων, σχετικά με τον αυξημένο κίνδυνο εκδήλωσης τρομοκρατικών επιθέσεων στην Ευρώπη, το προσεχές διάστημα.

Η εμφαίνουσα ισχυροποίηση της απήχησης ακροδεξιών πολιτικών δυνάμεων στην Ευρώπη, εκμεταλλευόμενα την άνοδο της ξενοφοβίας λόγω και των προσφυγικών ροών.

Οι συνέπειες της διαφαινόμενης «ήττας» του DAESH στα εμπόλεμα πεδία της Μέσης Ανατολής επιφέρει μία σειρά από επιπτώσεις για το περιβάλλον εσωτερικής ασφάλειας της Ένωσης, όπως:

Η «νομιμοποίηση» των συμμετεχόντων στις επιθέσεις Κ-Μ, ως στόχων.

Η αύξηση των αριθμών επιστροφής ξένων μαχητών σε χώρες της Ε.Ε.

Η «μόλυνση» των μεταναστευτικών/προσφυγικών ροών.

3.3 Διεθνες περιβαλλον ασφαλειας/παραγοντες προς θεωρηση

Η εκλογή στη θέση του Προέδρου των ΗΠΑ Τράμπ, σε συνδυασμό με συγκεκριμένες προεκλογικές δηλώσεις/θέσεις του, μέρος των οποίων φαίνεται να έχει εκκινήσει προς υλοποίηση, όπως:

Η επιδιωκόμενη προσέγγιση με τη Ρωσία, η άσκηση κριτικής σε χώρες της Ε.Ε, αναφορικά με τη μεταναστευτική τους πολιτική.

Η λήψη αυστηρότερων μέτρων για τις αμερικανικές πόλεις που προστατεύουν παράτυπους μετανάστες.

Η απόσυρση των ΗΠΑ από τη συμφωνία ελεύθερου εμπορίου μεταξύ των χωρών του ειρηνικού (TPP), στην οποία συμμετέχουν 12 χώρες που αντιπροσωπεύουν το 40% της παγκόσμιας οικονομίας.

Η άνοδος της Κίνας στην παγκόσμια πολιτική και οικονομική σκηνή συνέπεια της παγκοσμιοποίηση της διεθνούς οικονομία και της απεμπλοκής της από μια μακρόχρονη περίοδο εσωστρέφειας. Οικονομικοί Αναλυτές εκτιμούν ότι αν δεν παρουσιαστούν απρόβλεπτα προσκόμματα, θα καταστεί η μεγαλύτερη οικονομία διεθνώς ως το 2025[24],[25].

[23]http://www.naftemporiki.gr/story/1176544/europol-pithani-mia-tromokratiki-energeia-stin-europi-prosexos.

[24] Οικονομικοί Αναλυτές εκτιμούν ότι αν δεν παρουσιαστούν απρόβλεπτα προσκόμματα, θα καταστεί η μεγαλύτερη οικονομία διεθνώς ως το 2025

[25] http://www.eliamep.gr/old/eliamep/files/OP06.012846.pdf / Η ραγδαία πολιτική και οικονομική άνοδος της Κίνας και οι επιπτώσεις για την παγκόσμια οικονομική και πολιτική σκηνή

Παρατηρήσεις

Τα ανωτέρω αναλυθέντα συνθέτουν την εικόνα της Ασφάλειας σε Διεθνές και Ευρωπαϊκό επίπεδο και μας βοηθούν να κατανοήσουμε το σύγχρονο διεθνές περιβάλλον οριοθετώντας την δική μας θέση μας τόσο σαν χώρα όσο και σαν Ευρωπαϊκή Ένωση στην παγκόσμια σκακιέρα.

Η φύση των απειλών στο σύγχρονο περιβάλλον ασφαλείας, επιτάσσει τη συνεργασία όλων των θεσμικών παικτών της διεθνούς σκηνής. Η ΚτΠ με τις ασύλληπτες ταχύτητες, μας έχει «κληρονομήσει» με νέες, πρωτόγνωρες και απρόβλεπτες απειλές, που επιβάλλουν σε κράτη και διεθνείς οργανισμούς να απαντήσουν με αξιοπιστία και αποτελεσματικότητα. [26]

[26]Η Ε.Ε δεν σχεδιάσθηκε ώστε να αποτελέσει κάποιο είδος στρατιωτικής συμμαχίας. Σύμφωνα με τη Συνθήκη του Άμστερνταμ (1997), η εδαφική υπεράσπιση της Ε.Ε είχε ανατεθεί στο ΝΑΤΟ. Ωστόσο, μετά τον πόλεμο στο Κόσοβο το 1999, το Ευρωπαϊκό Συμβούλιο αποφάσισε ότι η η Ένωση θα πρέπει να έχει την ικανότητα αυτόνομης δράσης έτσι ώστε να ανταποκρίνεται κατάλληλα σε διεθνείς κρίσεις, χωρίς να προκαταλαμβάνεται από τις αποφάσεις του ΝΑΤΟ. Έτσι, ξεκίνησαν να λαμβάνονται πρωτοβουλίες με σκοπό την αύξηση της στρατιωτικής ικανότητας της Ε.Ε, με απώτερο σκοπό την σύσταση ολοκληρωμένης στρατιωτικής δύναμης έτσι ώστε να διασφαλίζεται η εδαφική της ακεραιότητα ενάντια σε εξωτερικούς κινδύνους περνώντας παράλληλα και ένα μήνυμα ότι δε πρόκειται να ξεσπάσει ποτέ ξανά πόλεμος μεταξύ των χωρών της Ένωσης.

ΚΕΦΑΛΑΙΟ 4^{Ο} : ΨΗΦΙΑΚΕΣ ΑΠΕΙΛΕΣ

4.1Σύγχρονες ψηφιακές απειλές στην Ε.Ε

Η ανάλυση των απειλών για το οργανωμένο έγκλημα στον κυβερνοχώρο (IOCTA 2016) επιβεβαιώνει ότι το έγκλημα στον ψηφιακό κόσμο εξακολουθεί να αποτελεί σημαντική απειλή για την εσωτερική ασφάλεια σε ολόκληρη την Ευρώπη, με τον αριθμό των καταγεγραμμένων στον κυβερνοχώρο υποθέσεων να ξεπερνούν αυτές που συνδέονται με τα παραδοσιακά εγκλήματα σε ορισμένα κράτη μέλη της Ε.Ε[27].

Στον κυβερνοχώρο συνεχίζεται η ανταλλαγή γνώσεων, εργαλείων και ‘’υπηρεσιών’’ σε ολόκληρο το φάσμα των εγκληματιών από αρχάριους μέχρι και στους επαγγελματίες συμπεριλαμβανομένων φυσικά του ευρύτερου χώρου της τρομοκρατίας και του εξτρεμισμού.

Η έκταση στην οποία εξτρεμιστικές ομάδες χρησιμοποιούν τον κυβερνοχώρο ως εργαλείο (σε σχέση με το 2015) για τη διεξαγωγή επιθέσεων φαίνεται να περιορίζεται, η διακίνηση εργαλείων και παράνομων εμπορευμάτων όμως αυξάνεται, όπως πυροβόλα όπλα και αλλά παράνομα εργαλεία μέσω του σκοτεινού διαδικτύου (dark net,) ώστε η όποια μείωση περιγράφηκε για την εγκληματική δραστηριότητα στον κυβερνοχώρο να τείνει να αναστραφεί εις βάρος της εσωτερικής ασφαλείας στην Ε.Ε.

Η ισχυρή κρυπτογράφηση είναι άκρως σημαντική για το ηλεκτρονικό εμπόριο και για άλλες επιχειρηματικές δραστηριότητες στον κυβερνοχώρο, ενώ η διασφάλιση επαρκούς ασφάλειας εξαρτάται από τις Αρχές Επιβολής του Νόμου που έχουν την ικανότητα να ερευνούν επιτυχώς την εγκληματική δραστηριότητα.

Πριν αναλύσουμε τις σύγχρονες ψηφιακές απειλές σύμφωνα με σχετική έκθεση του Ευρωπαϊκού Οργανισμού της Europol δόκιμο είναι να προσεγγίσουμε εν τάχει την έννοια του εγκλήματος στον Κυβερνοχώρο(Cybercrime) και του Ηλεκτρονικού Εγκλήματος (Computer crime) .

4.2 Κυβερνοέγκλημα (Cyber Crime)

[27]Europol Director Rob Wainwright says: “The relentless growth of cybercrime remains a real and significant threat to our collective security in Europe. Europol is concerned about how an expanding cybercriminal community has been able to further exploit our increasing dependence on technology and the Internet.

«Κυβερνοέγκλημα» είναι αυτό που διαπράττεται ή διευκολύνεται μέσω διαδικτύου δηλαδή κάθε εγκληματική δραστηριότητα που εμπλέκει υπολογιστές και δίκτυα. Η μορφή του ποικίλλει από την απάτη έως τα «ανεπιθύμητα» e-mails (spam)[28].

Το «κυβερνοέγκλημα» περαιτέρω περιλαμβάνει (με κριτήριο το χώρο τέλεσης):

- Τα εγκλήματα που είναι δυνατόν να τελεστούν τόσο στο «φυσικό» κόσμο, όσο και στο διαδίκτυο, όπως π.χ. η συκοφαντική δυσφήμηση (η οποία τελείται και με αποστολή e-mail).
- Τα εγκλήματα που είναι δυνατόν να τελεστούν μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς τη χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370Γ παρ. 1 του Π.Κ., π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή cd-Rom σε ηλεκτρονικό υπολογιστή.
- Τα«γνήσια εγκλήματα κυβερνοχώρου», με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο.

Το «κυβερνοέγκλημα» κυμαίνεται κατά μήκος ενός φάσματος δραστηριοτήτων:

Στο ένα άκρο εντοπίζονται εγκλήματα που εμπλέκουν θεμελιώδεις παραβιάσεις προσωπικής ή επιχειρηματικής ιδιωτικότητας, όπως οι επιθέσεις στην ακεραιότητα των πληροφοριών που διατηρούνται σε ψηφιακές αποθήκες και η χρήση παρανόμως κτηθεισών ψηφιακών πληροφοριών, για τον εκβιασμό φυσικών προσώπων.

Στο μέσον του φάσματος τοποθετούνται τα εγκλήματα περί τις «ψηφιακές» συναλλαγές και κινήσεις, όπως η απάτη, η διακίνηση υλικού παιδικής πορνογραφίας, η ψηφιακή πειρατεία και η παραχάραξη. Πρόκειται για συγκεκριμένα εγκλήματα, με συγκεκριμένα θύματα, ενώ ο εγκληματίας κρύβεται στην ανωνυμία του διαδικτύου.

Στο άλλο άκρο του φάσματος παρατηρούνται τα αδικήματα που αποδιαρθρώνουν τις πραγματικές εργασίες του διαδικτύου, όπως «spam», «hacking» και επιθέσεις «αρνήσεως υπηρεσιών» ενάντια σε συγκεκριμένους ιστοτόπους, καθώς και ενέργειες «κυβερνοτρομοκρατίας»[29].

4.3 Ηλεκτρονικό έγκλημα (computer crime)

Το «ηλεκτρονικό έγκλημα» προηγείται χρονικά και λογικά της κατηγορίας των κυβερνοεγκλημάτων. Κατά τον V. Zur Muhlen *εγκληματικότητα δια μέσου των υπολογιστών*

[28]US Department of Justice, Bureau of Justice Assistance, National Crime Prevention Council (2012).
[29]Η χρήση του διαδικτύου για την πρόκληση δημοσίων αναταραχών, ακόμη και θανάτων.

αποτελεί κάθε εγκληματική συμπεριφορά στην οποία ο υπολογιστής είναι εργαλείο ή σκοπός της πράξης.[30]

Ως ηλεκτρονικό έγκλημα θεωρείται η εγκληματική πράξη, η οποία για να τελεστεί απαιτείται η γνώση υπολογιστών[31].Κατ' άλλη προσέγγιση, θεωρείται η εγκληματική συμπεριφορά, κατά την οποία ο ηλεκτρονικός υπολογιστής καθίσταται εργαλείο ή αντικείμενο της εγκληματικής επίθεσης[32].

Ήταν λογικό επακόλουθο με την εμφάνιση της συνεχούς δικτύωσης των ηλεκτρονικών υπολογιστών, τα νομικά ζητήματα να αλλάξουν και να γίνουν πιο πολύπλοκα.

Έτσι και η ανάγκη νομικής αντιμετώπισης αυτών των νεοεμφανιζόμενων εγκληματικών συμπεριφορών έγινε πιο επιτακτική.

Ειδικότερα κάποια χαρακτηριστικά που εντοπίζουμε στο Ηλεκτρονικό έγκλημα είναι τα εξής:

- Η έλλειψη βίας, {χωρίς αυτό να σημαίνει ότι οι συνέπειες της δεν σχετίζονται σε ορισμένες περιπτώσεις με βίαιες συμπεριφορές}.
- Το διαδικτυακό έγκλημα διαπράττεται σε χρόνο ελάχιστων δευτερολέπτων. Η αμεσότητα αυτή έχει αποτέλεσμα τέτοια ταχύτητα τέλεσης που πολλές φορές δεν γίνεται αντιληπτό ούτε το ίδιο το θύμα.

Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά δεδομένα και λόγω της φύσης του, έχει δημιουργήσει μια σειρά ζητημάτων και προβληματικών, κατά τη διερεύνησή του από τις διωκτικές Αρχές, στο πεδίο του ποινικού δικαίου και της ποινικής δικονομίας, καθώς πολλές φορές είναι δύσκολο να προσδιοριστεί:

α) ο τόπος τέλεσης του εγκλήματος και

β) ο ακριβής χρόνος τέλεσης.

Η διευρυνόμενη διασύνδεση των Η/Υ καταλύει τα εθνικά σύνορα και οι δράστες διαπράττουν τα εγκλήματά τους χωρίς αυτά να συνδέονται με ένα συγκεκριμένο τόπο.

Αναμφίβολα, το «διαδικτυακό/ηλεκτρονικό» έγκλημα ανήκει στην κατηγορία των διεθνών εγκλημάτων, και τούτο αποδεικνύεται περίτρανα από το γεγονός ότι τα αποτελέσματα-συνέπειες του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους, ενώ λόγω της

[30]Όπως παρατηρείται (Ι. Αγγελής) δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στη διεθνή νομοθεσία, ούτε στη διεθνή νομολογία. Την Ελληνική δικαστική πρακτική δεν έχει απασχολήσει ακόμα περίπτωση σχετική με το έγκλημα στο διαδίκτυο. Οι υπάρχουσες μέχρι τώρα (ελάχιστες) ποινικές αποφάσεις αφορούν εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) και όχι εγκλήματα του κυβερνοχώρου (cybercrimes).

[31]Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual. Technical Report OJP-86-C-002, U.S. Department of Justice, National Institute of Justice, Office of Justice Program. 2nd edition

[32]Samodulska, M. CRIMES COMMITTED VIA THE INTERNET–SELECTED ASPECTS.

εκτεταμένης διαδικτύωσης καθίσταται εξαιρετικά δύσκολος ο προσδιορισμός του πραγματικού τόπου τέλεσής του, πόσο μάλλον του ιδίου του δράστη.

Τα ανωτέρω έχουν σαν αποτέλεσμα:

- Η «παραβατικότητα» να καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο.
- Τα εγκλήματα αυτά να μπορούν να πραγματοποιηθούν από τον καθένα, αλλά και να πλήξουν τον καθένα. Δεν χρειάζεται καν να εγκαταλείψει κανείς τον χώρο του σπιτιού του.
- Το «computer crime» έχει αποκτήσει κινητικότητα και διεθνή χαρακτήρα.
- Το Διαδίκτυο έχει αποκτήσει μεγάλη ελκυστικότητα για το οργανωμένο έγκλημα αλλά και την τρομοκρατία.

Οι εξελίξεις αυτά θέτουν σοβαρότατα ζητήματα για το ποινικό δίκαιο και την ικανότητα των Διωκτικών αρχών να ανταπεξέλθουν τόσο σε επίπεδο καταστολής όσο και προβλεπτικά υπονομεύοντας τα θεμέλια της εσωτερικής ασφάλειας στην Ευρωπαϊκή Ένωση.

4.4 Οι απειλες στον κυβερνοχωρο για το 2016

Σύμφωνα με την σειρά ιεράρχησης της Europol οι απειλές στον κυβερνοχώρο συνίστανται στις ακόλουθες:

1.Malware (κακόβουλο λογισμικό).

2.On line child exploitation (διακίνηση υλικού παιδικής εκμετάλλευσης).

3.Payment fraud (απατές πληρωμής)

4.Social Engineering (κοινωνική μηχανική).

5.Data breach & Network attacks (παραβίαση δεδομένων και επίθεση σε δίκτυα).

6.Attacks on critical insfracture (επίθεση σε κρίσιμες υποδομές).

7.Criminal Financial crimes (οικονομικές συναλλαγές μέσω διαδικτύου).

8.Criminal Communications online (διαδικτυακή επικοινωνία των εγκληματιών).

9. Dark net & hidden services (σκοτεινό διαδίκτυο και υπηρεσίες ανωνυμίας).

10.The convergence of cybercrime & terrorism (Η σύγκλιση του διαδικτύου με την τρομοκρατία

11.Social Media (Μέσα κοινωνικής δικτύωσης)

12. Big data33,iot and the cloud (Ιντερνέτ των πραγμάτων ,Υπηρεσίες που ανήκουν στο σύννεφο).
13. internet Governance (Διαδίκτυο και Διακυβέρνηση).

4.4.1 MALWARE (ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ)

Ως «κακόβουλο λογισμικό»,«επιβλαβές λογισμικό[34]» (malicious software/malware[35]) χαρακτηρίζεται αυτό που έχει κατασκευάσει και προγραμματιστεί με «εντολές» προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα *«ξενιστή»* και σε αυτό που δεν χρειάζεται *«ξενιστή»* και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα. Τα κύρια ειδη κακόβουλου Λογισμικού είναι τα ακόλουθα:

Ιός (Virus): είναι κακόβουλο λογισμικό το οποίο εξαπλώνεται σε χρήσιμα προγράμματα ενός ξένου υπολογιστή με αποτέλεσμα να βλάπτει χρήσιμα αρχεία ενός χρήστη.

Δούρειος Ίππος (Trojan): είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης. Το λογισμικό αυτό παραπλανούν τον χρήστη και χρησιμοποιείται από το οργανωμένο έγκλημα για να υποκλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο συστήματος.

Σκουλήκι (Worm*):* είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά του να πολλαπλασιάζεται αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου.

Rootkit: έχει την ιδιαιτερότητα να κρύβει κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας. Αυτά τα προγράμματα κάποιες φορές λειτουργούν προστατευτικά για τους χάκερ διαγράφοντας τις πληροφορίες του εισβολέα.

Η διάδοση κακόβουλου λογισμικού εξακολουθεί να είναι ο ακρογωνιαίος λίθος για την πλειοψηφία των εγκλημάτων στον κυβερνοχώρο.

---

[33] Boyd, Dana? Crawford, Κέιτ (21του Σεπτεμβρίου, 2011). "Έξι Προκλήσεις για Big Data". *Social Science Research Network: Μια δεκαετία στην Ώρα Διαδικτύου: Συμπόσιο για τη δυναμική του Διαδικτύου και της Κοινωνίας.*

[34] Peter Mell Karen, Kent Joseph, Nusbaum (2005). *Guide to Malware Incident Prevention and Handling*. NIST σελ. 101.

[35] ΚΑΤΣΙΚΑΣ, ΣΩΚΡΑΤΗΣ. Ασφάλεια Υπολογιστών. Ελληνικό Ανοικτό Πανεπιστήμιο, σελ. 248. ISBN 960–538–226–1.

Τα κακόβουλα λογισμικά διαφέρουν στην λειτουργία και τις δυνατότητες τους ενώ τα σημαντικότερα που αντιμετώπισαν για το 2016 οι Αρχές Επιβολής του Νόμου στην Ε.Ε είναι οι τύποι *ransomware*[36] και *stealers.*

Η ESET[37] ζήτησε από ειδικούς να υλοποιηθεί μια έκθεση για τάσεις σε θέματα ασφάλειας ώστε να βοηθηθούν οι επιχειρήσεις και οι χρήστες να μπορέσουν να κατανοήσουν τις προηγμένες τακτικές και τεχνικές που χρησιμοποιούνται από τους χάκερ (κρυπτογραφία, ανωνυμία, κ.α).

Από τα κυριότερα ramsonware[38] που κυκλοφόρησαν το 2014 και χρησιμοποίησε τεχνικές και στοιχειά κρυπτογράφησης ώστε να πετύχει τους στόχους του ήταν το CTB LOCKER και το CRYPTOWALL τα οποία χρησιμοποίησαν τα κανάλια ανωνυμίας των ανώνυμων ψηφιακών νομισμάτων, των γνωστών Bitcoins τα οποία θα αναλυθούν παρακάτω καθώς για μερικούς ερευνητές αποτελούν το νόμισμα του μέλλοντος.

Την 12-05-2017 συνέβη η μεγαλύτερη επίθεση ransomware χρησιμοποιώντας ένα από τα exploit της NSA που διέρρευσαν πρόσφατα από την ομάδα Shadow Brokers .Οι επιτιθέμενοι μπόρεσαν να προσβάλλουν υπολογιστές σε παγκόσμιο επίπεδο με το WannaCry (ένα exploit των Windows το οποίο ασπάστηκε από το εργαλείο EternalBlue της NSA). Η Microsoft έχει κυκλοφορήσει ήδη μια ενημέρωση για αυτήν την ευπάθεια, αλλά πολλοί χρήστες και οργανισμοί δεν έκαναν τον κόπο να ενημερώσουν τα συστήματά τους.[39]

4.4.2 ONLINE CHILD SEXUAL EXPLOITATION (ΣΕΞΟΥΑΛΙΚΗ ΕΚΜΕΤΑΛΛΕΥΣΗ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ)

[36] http://www.ant1news.gr/news/tech/article/464854/to-2017-einai-i-xronia-ransomware

[37]Η ESET[37] ζήτησε από τους ειδικούς της να ετοιμάσουν μία έκθεση με τις κυριότερες τάσεις σε ζητήματα ασφάλειας για το 2017 [37] στην οποία περιλαμβάνονται πληροφορίες σχετικά με τις πιο πρόσφατες επιθέσεις, καθώς και προβλέψεις για τα θέματα που θα απειλήσουν την ασφάλεια στον κυβερνοχώρο

Σύμφωνα με αυτή την έκθεση καταγράφεται μία νέα τάση στον ορίζοντα του ransomware. Πρόκειται για το "Ransomware of Things" ή RoT, δηλαδή τη δυνατότητα των εγκληματιών του κυβερνοχώρου να επιτίθενται σε συσκευές, κρατώντας τις "ομήρους" και στη συνέχεια, να απαιτούν την καταβολή λύτρων με αντάλλαγμα την αποκατάσταση του ελέγχου από το χρήστη.

Επίσης, το 2017 θα είναι η χρονιά κατά την οποία η αδίστακτη απειλή του ransomware θα αρχίσει να μεταναστεύει πιο συστηματικά σε άλλες πλατφόρμες, πέρα από τους υπολογιστές και τα smartphones, πρωταρχικός σκοπός των οποίων, μάλιστα, δεν είναι η επεξεργασία δεδομένων ή ψηφιακών επικοινωνιών. Η έκθεση "The Trends 2017: Security held ransom report", χωρίζεται σε εννέα κεφάλαια, το καθένα με επίκεντρο μια σημαντική πτυχή της ασφάλειας των πληροφοριών. Τα περισσότερα από τα κεφάλαια ασχολούνται με τις απειλές, είτε βάσει τύπου (Ransomware, Ευπάθειες, και Mobile), είτε βάσει κλάδου (Υγεία, Υποδομές Ζωτικής Σημασίας, και Gaming).

[38]http://www.thereport.gr/200000-pc-%CE%B1%CF%80%CF%8C-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B5%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7-%CE%BC%CE%B5-%CE%B9%CF%8C-ransomware-%CF%83%CE%B5-150-%CF%87%CF%8E%CF%81%CE%B5%CF%82/

[39] https://secnews.gr/157129/kill-switch-domain-for-wannacry-ransomware/

Η χρήση του διαδικτύου ως μια πλατφόρμα/εργαλείου μέσα από το οποίο διαμοιράζονται αποθηκεύονται, αλλά και επικοινωνούν οι εγκληματίες με τα νεαρά θύματα τους, είναι μία από τις πιο καταστροφικές και αποτρόπαιες πτυχές του Διαδικτύου.

Η *υιοθέτηση του Λουξεμβούργου,* όπου ορίζονται οι κατευθυντήριες γραμμές και η ορολογία για την προστασία των παιδιών από τη Σεξουαλική Εκμετάλλευση και Σεξουαλική Κακοποίηση)[40] αποτελεί σημαντικό έγγραφο για την επίτευξη συναίνεσης σχετικά με τις βασικές έννοιες που δύνανται να ενισχύσουν την συνεργασία μεταξύ των ενδιαφερόμενων φορέων, συμπεριλαμβανομένων των ερευνητών, των δικαστικών αρχών και κοινωνικών κρατικών υπηρεσιών προστασίας του παιδιού.

Αυτή η διαδικασία του διαδικτυακού καταναγκασμού υποστηρίζεται από ένα φάσμα στρατηγικών χειραγώγησης από τους δράστες, οι οποίες συνήθως περιλαμβάνουν τη χρήση εξαναγκασμού, με απειλές και εκφοβισμό, αλλά και στρατηγικές, παραπλάνησης όπως η πλαστοπροσωπία, το hacking, ή μεσω της παραποίησης της φωτογραφίας ενός υποψήφιου θύματος.

Κοινά εργαλεία που χρησιμοποιούνται από τους παραβάτες περιλαμβάνουν φυσικά εργαλεία ανωνυμίας IP, **κρυπτογράφηση** για δύο συσκευές και επικοινωνίες, εικονικές (virtual) διαμορφώσεις και τεχνικές αποθήκευσης στο σύννεφο, σε απροσδιόριστους λογαριασμούς, ή χαρτοφυλάκια τα οποία δεν είναι καθόλου εύκολο να ταυτίσουν ένα υποκείμενο, ενώ περιέχουν στοιχειά η πορνογραφικό υλικό το οποίο βρίσκεται σε «cloud» περιβάλλον.

4.4.3PAYMENT FRAUD (ΑΠΑΤΕΣ ΠΛΗΡΩΜΗΣ)

Οι επιθέσεις με κακόβουλο λογισμικό ‘’malware΄΄ που στοχεύουν ATM, καθώς και η μέθοδος απάτης (CNP[41]) (card not present transaction) όσο και οι απάτες σε ηλεκτρονικές συναλλαγές με κάρτες χωρίς την φυσική παρουσία του κατόχου της κάρτας πληρωμής, κλιμακώνονται, και αντιπροσωπεύουν επί του παρόντος το 66% της συνολικής απάτης με κάρτες αξίας στην Ευρωπαϊκή Ένωση. Οι νέες μορφές απάτης πληρωμής με κάρτες κοντινού πεδίου (N[i]FC)[42],[43]

[40]Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, http://www.ilo.org/wcmsp5/groups/public/ed_norm/ipec/documents/instructionalmaterial/wcms_490167.pdf, 2016

[41] https://en.wikipedia.org/wiki/Card_not_present_transaction

[42]Η **επικοινωνία κοντινού πεδίου** (**near field communication**, **NFC**) αποτελεί μια πρότυπη τεχνολογία συνδεσιμότητας, η οποία διαδίδεται και εξελίσσεται ραγδαία με κύριο σκοπό τη λύση αρκετών προβλημάτων, σύγχρονων αλλά και μελλοντικών. Είναι μια μικρής εμβέλειας ασύρματη τεχνολογία, η οποία λειτουργεί στη συχνότητα των 13,56 MHz και μεταφέρει δεδομένα με ρυθμό έως και 424 kbps και έχει γίνει γνωστή κυρίως μέσω της χρήσης της από τα κινητά τελευταίας γενιάς (smartphones). Η

για ηλεκτρονικές συναλλαγές όλο και περισσότερο απασχολούν τις Αρχές Επιβολής του Νόμου.

Η συναλλακτική δραστηριότητα μεταξύ κυβερνοεγκληματίων παραμένει εξ ολοκλήρου εντός ψηφιακού κόσμου.

Εδώ το συνηθέστερα χρησιμοποιούμενο νόμισμα C2C (Criminal 2 criminal trensaction) συναλλαγών είναι το Bitcoin.

Το, **κρυπτονόμισμα** Bitcoin έχει γίνει νόμισμα της επιλογής για ένα μεγάλο μέρος της εγκληματικότητας στον κυβερνοχώρο και λόγω της αυξημένης εμπιστοσύνης από την κοινότητα των ψηφιακών χρηστών άλλα και τις δικλείδες ασφαλείας που προτείνει στους χρήστες.

Παράλληλα η γρήγορη διάδοση και καθιέρωσή του δημιούργησε την ανάγκη για την περαιτέρω εξέλιξη ανάλογων νομισμάτων ανωνυμίας που μέχρι σήμερα δεν έχουν φθάσει το επίπεδο δημοτικότητας του Bitcoin.

4.4.4 SOCIAL ENGINEERING (ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ)

Κοινωνική μηχανική (Social engineering) είναι η πράξη που είναι κυρίως συνδεδεμένη με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα.

Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά. Παρόλο που ο όρος ίσως να μην είναι ακριβής ή επιτυχημένος έχει πλέον καθιερωθεί[44].Ο πρώην εγκληματίας υπολογιστών και αργότερα σύμβουλος ασφαλείας πληροφορικών συστημάτων *Κέβιν Μίτνικ* διέδωσε τον όρο «κοινωνική μηχανική»,

---

λειτουργία της βασίζεται στην επαφή ή στην προσέγγιση, σε απόσταση περίπου τεσσάρων με πέντε εκατοστών, της συσκευής που περιέχει το τσιπ NFC, σε κάποια άλλη συσκευή που περιλαμβάνει τον κατάλληλο αισθητήρα.

[43]**NFC και Bluetooth** :Πρόκειται για τεχνολογίες υψηλής συχνότητας ασύρματης επικοινωνίας μικρής εμβέλειας που περιλαμβάνονται σε ηλεκτρονικές συσκευές για εύκολη και ασφαλή αλληλεπίδραση ανάμεσα σε δύο ηλεκτρονικές συσκευές. Το NFC είναι μία τεχνολογία ασύρματης σύνδεσης η οποία μπορεί να χρησιμοποιηθεί για μια αμφίδρομη αλληλεπίδραση ανάμεσα σε ηλεκτρονικές συσκευές εντός κάποιων εκατοστών. Το Bluetooth είναι επίσης μία ασύρματη τεχνολογία η οποία σχεδιάστηκε για την αλληλεπίδραση μεταξύ των συσκευών επικοινωνίας εντός 10 μέτρων εμβέλειας χωρίς φυσική σύνδεση.

Το NFC έχει πολύ μεγάλη χρησιμότητα στην καθημερινότητα και εφαρμόζεται σε πάρα πολλούς τομείς. Ο διαμοιρασμός αρχείων γίνεται με πάρα πολύ εύκολο τρόπο απλά ακουμπώντας την μια συσκευή με την άλλη. Η πληρωμή ενός λογαριασμού γίνεται εξίσου εύκολα ακουμπώντας τις συσκευές και πληκτρολογώντας το ποσό.

[44] *ΧΑΚΕΡ ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ*, Γκιούρδας, 2η Έκδοση (2001),ISBN 960-512-259-6, στη σελ. 555

επισημαίνοντας ότι είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης από ένα σύστημα από το να προσπαθήσεις να τον σπάσεις.[45]

Στηρίζεται κυρίως στην ανθρώπινη περιέργεια ή την απληστία και στην άγνοια ενώ η κλασική τεχνική είναι το '' δόλωμα'' ένας ρεαλιστικός Δούρειος Ίππος[46].

4.4.5 DATA BREACHES AND NETWORK ATTACKS (ΠΑΡΑΒΙΑΣΗ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΕΠΙΘΕΣΗ ΣΕ ΔΙΚΤΥΑ).[47]

Όταν αναφερόμαστε σε Data Breaches μιλάμε για παραβίαση προσωπικών, ευαίσθητων πληροφοριών που μπορούν να αφορούν την υγεία ,προσωπικά δεδομένα , εμπορικά μυστικά ή πνευματική ιδιοκτησία .Επίσης νοείται η εισβολή ενός hacker σε ένα εταιρικό δίκτυο για να κλέψει ευαίσθητα δεδομένα.

Παράδειγμα:

Σε ένα περιβάλλον υγειονομικής περίθαλψης, ο νόμος για την φορητότητα/προσβασιμότητα πληροφοριών Ασφαλίσεων Υγείας και Πράξη Ευθύνης (HIPAA Health Insurance Portability and Accountability Act) υπαγορεύει ποιος έχει δικαίωμα γνώσης ατομικών φακέλων ασθενών (το όνομα, την ημερομηνία γέννησης, τον αριθμό κοινωνικής ασφάλισης και το ιστορικό της υγείας).Οι περισσότερες παραβιάσεις δεδομένων περιλαμβάνουν υπερέκθεση ,ευάλωτων αδόμητων δεδομένων - αρχεία, έγγραφων και ευαίσθητες πληροφορίες.[48]

Ως **ασφάλεια Δικτύου Υπολογιστών (network sec)** νοείται η ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του.

Εκτός αυτού, θεωρείται η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες

Οι κυριότερες μέθοδοι επίθεσης σε ένα δίκτυο **(network attacks)** έως σήμερα είναι οι εξής:

- Denial-of-Service (DoS): Αποστολή περισσοτέρων αιτήσεων σύνδεσης από όσες μπορεί να επεξεργαστεί ένας server.

[45] Mitnick, K: "CSEPS Course Workbook" (2004), p. 4, Mitnick Security Publishing.

[46] Ο επιτιθέμενος αφήνει ένα CD ή ένα φλασάκι ή κάποιο χαρτάκι με διευθύνσεις στο Διαδίκτυο και κωδικούς εισόδου σε κάποιο σημείο που "δήθεν" κάποιος ξέχασε. Το υποψήφιο θύμα πιθανά θα χρησιμοποιήσει αυτό το μέσο στον υπολογιστή του ή θα μπει στη διεύθυνση που βρήκε.

[47] http://searchsecurity.techtarget.com/definition/data-breach.

[48] *"Παναμάς έγγραφα Διαρροή: Η νέα κανονική;" Xconomy. 04.26.2016 / 08/20/2016.*

- (Unauthorized access attacks): (Μη εξουσιοδοτημένη πρόσβαση) διάφοροι τρόποι επίθεσης που εμπεριέχουν την ανάκτηση του δικαιώματος εισόδου, εκτέλεσης εντολών, ή ανάκτησης πληροφορίας σε ένα μηχάνημα που δεν παρέχει τέτοιες υπηρεσίες στον επιτιθέμενο.
- Password attacks: Αποτελεί την μέθοδο εύρεσης ενός password, είτε με επαναληπτικό τρόπο δοκιμάζοντας όλους τους δυνατούς συνδυασμούς, είτε με αποκρυπτογράφηση του password δοκιμάζοντας όλους τους δυνατούς συνδυασμούς των πιθανών κλειδιών κρυπτογράφησης.
- Trojan Horses: Είναι ένα πρόγραμμα που περιέχει η εγκαθιστά μία «κακόβουλη» (malicious) εφαρμογή.
- Network packet sniffers: Είναι ένα πρόγραμμα ή μηχάνημα το οποίο μπορεί να υποκλέψει κίνηση που μεταφέρεται από ένα δίκτυο.

4.4.6 Attacks on Critical Infrastructure (Διαδικτυακές Επιθέσεις σε κρίσιμες υποδομές)

Ως κρίσιμες υποδομές θεωρούνται τα περιουσιακά στοιχεία και οι δομές εκείνες που είναι ζωτικής σημασίας απαραίτητα για τη λειτουργία της κοινωνίας και της οικονομίας σε σημείο που, η καταστροφή τους ,θα έχει διαδοχικά και καίρια αποτελέσματα στην λειτουργία της κρατικής υπόστασης.

Λόγω των ανωτέρω και ο όρος συνήθως συνδέεται με τις ακόλουθες εγκαταστάσεις:

Παραγωγή ηλεκτρικής ενέργειας, μεταφοράς και διανομής, παραγωγή φυσικού αερίου, τη μεταφορά και τη διανομή ,πετρέλαιο και προϊόντα πετρελαίου στην παραγωγή, μεταφορά και διανομή, τηλεπικοινωνιών ,παροχή νερού (πόσιμο νερό, τα απόβλητα ύδρευσης /αποχέτευσης, οι οποίες προκύπτουν από τα επιφανειακά ύδατα (π.χ. φράγματα και οι υδατοφράκτες), γεωργία, την παραγωγή τροφίμων και τη διανομή, θέρμανσης (π.χ. φυσικό αέριο , πετρέλαιο, τηλεθέρμανση),της δημόσιας υγείας (νοσοκομεία, ασθενοφόρα) συστήματα μεταφοράς (προμήθεια καυσίμων, σιδηροδρομικό δίκτυο, αεροδρόμια, λιμάνια, εσωτερική ναυσιπλοΐα),χρηματοοικονομικές υπηρεσίες (τράπεζες, εκκαθάριση),υπηρεσίες ασφαλείας (αστυνομία, το στρατό).

4.4.7 Criminal finance Crime (Οικονομικη απατη στο διαδικτυο)

Νοείται η διαδικασία πραγματοποίησης διαδικτυακών πληρωμών μεταξύ μελών του οργανωμένου εγκλήματος και κοινών εγκληματιών για προσφερόμενες εγκληματικές υπηρεσίες η για αγορά διαφόρων υλικών .Είναι λογικό οι εγκληματίες να προσπαθούν να συναλλάσονται με ασφάλεια δηλαδή ανωνυμία για αυτό ο μηχανισμός πληρωμών

υπαγορεύεται σε μεγάλο βαθμό από τις αγορές μέσω του σκοτεινού διαδικτύου του λεγόμενου και Dark net ενώ χρησιμοποιούνται σχεδόν αποκλειστικά ψηφιακά νομίσματα Bitcoin.[49] [50]

Η μεταφορά χρημάτων από χρηματοπιστωτικά όπως η Western Union[51] ή MoneyGram ,οι προπληρωμές κάρτες και οι πιστωτικές κάρτες επίσης συνεχίζουν να αποτελούν ένα δημοφιλές τρόπο δράσης σε τέτοιου είδους πληρωμές C2C(Criminal 2 Criminal).

4.4.8 Criminal communications online (Διαδικτυακη επικοινωνια εγκληματιων)

Ως προς τα εργαλεία και τις εφαρμογές που χρησιμοποιούνται από τους εγκληματίες αυτά ελάχιστα έχουν μεταβληθεί σε σχέση με το παρελθόν καθώς οι εγκληματίες προσανατολίζονται σε οικείες σε αυτούς εφαρμογές.

Τα τελευταία χρονιά διακρίνεται μια τάση και κάποιες κινήσεις/ πρωτοβουλίες του δημόσιου αλλά και του ιδιωτικού φορέα ως προς το θέμα της προστασίας της ιδιωτικής ζωής και την ασφάλεια πάντα σε συνάφεια με την κρυπτογράφηση και τα νομικά κενά που εντοπίζονται

Υπάρχουν επί του παρόντος εν εξελίξει συζητήσεις σχετικά με το εάν ή όχι τα δικαστήρια μπορούν ή πρέπει να αναγκάσουν ύποπτους δράστες να αποκαλύψουν τον κώδικα/κλειδι της κρυπτογράφησης τους. Ορισμένες χώρες έχουν ήδη ενσωματώσει αυτήν την πολιτική στην Εθνική τους Νομοθεσία (π.χ. Ηνωμένο Βασίλειο).

Σε αυτήν την κατηγορία διάφορες web-based πλατφόρμες επικοινωνίας, όπως chatrooms ή ανοικτά φόρουμ εξακολουθούν να χρησιμοποιούνται συνήθως για C2C επικοινωνίες, όπως πχ ασφαλή, **κρυπτογραφημένα** email τα οποία είναι εύκολα διαθέσιμα.

Ένα ευρέως χρησιμοποιούμενο εργαλείο είναι το Jabber[52] και πιστεύεται ότι είναι από τα προτιμώμενα μέσο επικοινωνίας για πιο καταρτισμένους εγκληματίες του κυβερνοχώρου.

---

[49]Το Bitcoin είναι ένα ψηφιακό νόμισμα.Δεν υπάρχει επισήμως σε καμία φυσική μορφή, κερμάτων ή χαρτονομισμάτων.Δεν παράγεται από καμία συγκεκριμένη χώρα. Δεν ελέγχεται από καμία συγκεκριμένη τράπεζα ή κυβέρνηση. Ως Bitcoin νοείται ένα peer-to-peer σύστημα πληρωμών και ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα.Ανήκει στην κατηγορία cryptocurrency, καθώς χρησιμοποιεί μεθόδους κρυπτογραφίας για τη δημιουργία και διαχείριση των χρημάτων, και για την επιβεβαίωση της εγκυρότητας των συναλλαγών.

[50]https://www.pcsteps.gr/13691-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-bitcoin.

[51]**Western Union:** Διεθνές σύστημα ηλεκτρονικών πληρωμών εκτέλεσης εντολής αυθημερόν. Η καταβολή στο δικαιούχο διενεργείται με μετρητά. Εξυπηρετεί πληρωμές από και προς το εξωτερικό. Απευθύνεται σε όλους εσάς που επιθυμείτε να στείλετε ή να λάβετε χρήματα μέσα σε λίγα λεπτά.Πλεονεκτήματα:Αμεση μεταβίβαση των χρημάτων μέσα σε λίγα λεπτά από την στιγμή της αποστολής τους, Αξιοπιστία και απόλυτη ασφάλεια στις συναλλαγές -Μοναδικός κωδικός. Παγκόσμιο Δίκτυο σημείων παροχής της υπηρεσίας.Οι πληρωμές πραγματοποιούνται στο νόμισμα της Χώρας προορισμού, ή σε δολάρια

4.4.9 DARK NETS AND HIDDEN SERVICES (ΣΚΟΤΕΙΝΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΑΝΩΝΥΜΙΑΣ)[53]

Το «dark net» ή «σκοτεινό δίκτυο» είναι ένα δίκτυο μέσα στο διαδίκτυο , που προσεγγίζεται μόνο με συγκεκριμένο λογισμικό, διαμορφώσεις, ή άδειες, χρησιμοποιώντας συχνά πρωτόκολλα και θύρες μη τυποποιημένων επικοινωνιών.

Υπάρχουν δύο είδη dark net:

Τα δίκτυα F2F (φίλος προς φίλο), (συνήθως χρησιμοποιούνται για την ανταλλαγή αρχείων με σύνδεση peer-to-peer[54] και δίκτυα ανωνυμίας όπως το Tor [55]μέσω μιας σειράς ανώνυμων συνδέσεων. Ο όρος για το κρυπτογραφημένο dark net είναι Clearne[56] ή δίκτυο επιφανείας. Αυτό εμπεριέχεται στην έννοια του dark web ενός ανώνυμου διαδικτυακού ιστού στον οποίο σκιώδεις χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες[57].

Το 2015 ήταν μια ταραχώδης χρονιά για τις αγορές dark net, με την παραοικονομία να μαστίζεται από μεγάλες απάτες και το κλείσιμο της αγοράς που δραστηριοποιούνταν στο dark net με την επωνυμία evolution[58].

Το Μάρτιο του 2015, η αγορά Evolution έκλεισε με τους διαχειριστές του να φέρονται να έχουν αποκομίσει με παράνομο τρόπο 11 εκατομμύρια ευρώ από τους πελάτες τους.

Τρεις μεγάλες αγορές dark net τερμάτισαν την δραστηριότητα τους μέσα σε διάστημα 12 μηνών χωρίς καμία εμφανή η αφανής δράση των αρχών Επιβολής του Νόμου, τονίζοντας την εγγενή μεταβλητότητα της αγοράς dark net στην παγκόσμια οικονομία και τα ρίσκα που μπορεί να έχει ο οποιοσδήποτε χρήστης ενώ για άλλη μια φορά αποτυπώνεται το κενό των αρχών ασφάλειας πάνω σε αυτές τις πρακτικές.

---

[52] Το Extensible Messaging and Presence Protocol (XMPP) (παλαιότερη ονομασία Jabber) είναι ένα σύνολο ανοιχτών πρωτοκόλλων άμεσης επικοινωνίας (instant messaging), βασισμένα στην XML. Λογισμικό Jabber είναι εγκατεστημένο σε χιλιάδες διακομιστές (server) ανά το Διαδίκτυο (Internet) και χρησιμοποιείται από τουλάχιστον 10 εκατομμύρια χρήστες παγκοσμίως, σύμφωνα με τα στοιχεία της Jabber Software Foundation.Σε αντίθεση με τα περισσότερα πρωτόκολλα άμεσης επικοινωνίας, το Jabber είναι ένα ανοιχτό πρότυπο.Επίσης, όπως και με την ηλεκτρονική αλληλογραφία, μπορείτε να επικοινωνήσετε με οποιονδήποτε χρήστη, όποιοι και αν είναι οι εμπλεκόμενοι διακομιστές (ο δικός σας και ο δικός του).

[53]https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[55] https://el.wikipedia.org/wiki/Tor

[56] Miller, Tessa (10 January 2014). «How Can I Stay Anonymous with Tor?». Life Hacker. Ανακτήθηκε στις 7 June 201

[57] Wood, Jessica (2010). «The Darknet: A Digital Copyright Revolution». *Richmond Journal of Law and Technology* **16**

[58] DeepDot Web, Evolution Marketplace Exit Scam: Biggest Exit Scam Ever?,

Έρευνες κατέδειξαν ότι, σχεδόν το 30% των κρυφών υπηρεσιών σχετίζονται με κάποια μορφή παράνομης δραστηριότητας. Η πλειοψηφία των ερευνών Επιβολής του Νόμου σχετικά με την dark net έχει επικεντρωθεί σε αγορές/διαδικτυακές πλατφόρμες που πωλούν παράνομα ναρκωτικά ή τουλάχιστον, τους πωλητές και τους αγοραστές αυτών. Οι εν λόγω πώληση όπλων, σε κίνδυνο τα δεδομένα ή άλλες παράνομες προϊόντα όπως τα φαρμακευτικά και χημικά προϊόντα αποτελεί βασικός στόχος για τις Αρχές Επιβολής του Νόμου. [59]

Μία από τις κύριες προκλήσεις για την επιβολή του Νόμου είναι η ικανότητα να λειτουργούν νόμιμα σε αυτά τα περιβάλλοντα, με το ένα τέταρτο των ερωτηθέντων στελεχών να δηλώνουν την σαφώς περιορισμένη δράση τους σε αυτό το περιβάλλον από την εθνική τους νομοθεσία.

4.4.10 THE CONVERGENCE OF CYBER AND TERRORISM (Η ΣΥΓΚΛΙΣΗ ΤΗΣ ΤΡΟΜΟΚΡΑΤΙΑΣ ΚΑΙ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ).

Η «κατάχρηση» της τεχνολογίας και των νόμιμων online εργαλείων και υπηρεσίες δεν αποτελεί εξαίρεση στο πεδίο της τρομοκρατίας.

Οι τρομοκράτες γίνονται ολοένα και πιο ικανοί στο να κρύβουν τα ίχνη τους και τις δραστηριότητες τους με τη χρήση εργαλείων και υπηρεσιών ανωνυμοποίησης και την χρήση κρυπτογράφησης.

Επιπλέον, η ανωνυμία που παρέχουν τα κρυπτονομίσματα και κυριότερα η χρήση τους στις συναλλαγές που λαμβάνουν χώρα στις αγορές (dark markets,) φαίνεται να οδηγεί τους τρομοκράτες να χρησιμοποιούν ευρέως αυτό το νόμισμα.

Αγαθά και υπηρεσίες που προσφέρονται στο dark net όπως το δίκτυο ανωνυμίας Tor είναι εύκαιρα σε διάφορά δρώντα γκρουπ του Οργανωμένου εγκλήματος συμπεριλαμβανομένων των τρομοκρατικών ομάδων. Τέτοια αγαθά εναλλάσσονται μεταξύ κακόβουλου λογισμικού όπως κλεμμένα όπλα, μέχρι σε **crowdfunding sites**[60] μέσω των οποίων συνειδητά ή μη χρηματοδοτούνται παράνομες ομάδες και μεταξύ αυτών και τρομοκρατικές.

[59] Daniel Moore, Thomas Rid, Cryptopolitik and the Darknet, 2016

[60]Crowdfunding πολύ απλά είναι η χρηματοδότηση από το πλήθος. Συνήθως αναφερόμαστε στη χρηματοδότηση κάποιου έργου /project ή κάποιας ιδέας από πολλούς ανθρώπους, οι οποίοι προσφέρουν μικρά ποσά ο καθένας, αλλά από τη συμβολή όλων καλύπτεται ο οικονομικός στόχος για κάθε έργο.Συνήθως , το crowdfunding αφορά περιπτώσεις μικρο-χρηματοδότησης από 5.000-50.000 ευρώ και δεν περιορίζεται σε επιχειρηματικές ιδέες, αλλά και στη χρηματοδότηση Life Projects για σπορ, τέχνες, ιατρικές ανάγκες, εκπαίδευση, ταξίδια, εθελοντισμό κλπ.Επίσης, το

Η «κατάχρηση» της τεχνολογίας γέννησε τους «κυβερνοτρομοκράτες» άτομα που συνήθως διαθέτουν σημαντικά οικονομικά κεφάλαια για τη διενέργεια των χτυπημάτων τους, ενώ χρησιμοποιούν την τεχνολογία Η/Υ και το διαδίκτυο για σχεδιασμό επιχειρήσεων, συλλογή κεφαλαίων, διάδοση προπαγάνδας, ανταλλαγή απόψεων και στρατολόγηση.

Η «κυβερνοτρομοκρατία» περιλαμβάνει προμελετημένες και πολιτικά υποκινούμενες κυβερνοεπιθέσεις, ενώ πιθανοί στόχοι της είναι τα κυβερνητικά δίκτυα Η/Υ, τα οικονομικά δίκτυα, τα εργοστάσια παραγωγής ενέργειας, τα πληροφοριακά δίκτυα ελέγχου εναέριας κυκλοφορίας.κ.α.

Η «κυβερνοτρομοκρατία» εστιάζει στη χρήση του διαδικτύου από μη κυβερνητικούς δρώντες, ώστε να επηρεάσει την οικονομική και τεχνολογική υποδομή ενός κράτους.

Παρόλα αυτά, σήμερα οι περισσότεροι χρήση του διαδικτύου από τους τρομοκράτες, σχετίζεται με τη χρήση των απλοϊκών εργαλείων και μια διαδεδομένη χρήση των social media για την προπαγάνδα, την επικοινωνία, τις προσλήψεις και τις διάδοση γνώσης αλλά και ειδήσεων χωρίς να αποκαλύπτεται η γεωγραφική τους θέση ή η ταυτότητά τους.

4.4.11.Social media (Μεσα κοινωνικησ δικτυωσησ)

Το διαδίκτυο διαδραματίζει θεμελιώδη ρόλο στην ριζοσπαστικοποίηση του φαινομένου των ξένων μαχητών γεγονός το οποίο είναι στις προτεραιότητες δράσης της Ε.Ε μέχρι το 2020.

Τα μέσα κοινωνικής δικτύωσης παρέχουν ευκαιρίες σε άτομα που δρουν συνήθως μόνα τους ευκαιρίες για να εκδηλώσουν την υποστήριξη και την πίστη τους σε τρομοκρατικές ομάδες, χωρίς να χρειάζεται να εγκαταλείψουν το σπίτι τους.

Ο ρόλος του διαδικτύου (και των κοινωνικών μέσων μαζικής ενημέρωσης), έχει γίνει ένα από τα σημαντικότερα θέματα στη συζήτηση στους κύκλους της Ε.Ε για την καταπολέμηση της ριζοσπαστικοποίησης.

Οι Ευρωπαίοι «αλλοδαποί μαχητές» που αναχώρησαν για τις ζώνες του πολέμου της Μέσης Ανατολής και της Βόρειας Αφρικής ,αλλά και τα τρομοκρατικά χτυπήματα που πραγματοποίησαν στην Ευρώπη ριζοσπαστικοποιημενοι Ευρωπαίοι πολίτες κατά την επιστροφή τους και οι πυρήνες που δημιούργησαν, καταδεικνύουν τον καταλυτικό ρόλο της διαδικασίας της ριζοσπαστικοποίησης στην ενδυνάμωση του βίαιου εξτρεμισμού και της τρομοκρατίας.-

---

crowdfunding μπορεί να αποτελέσει πολύτιμο εργαλείο για τη χρηματοδότηση Μη Κερδοσκοπικών Οργανώσεων (ΜΚΟ).

Έως τώρα δεν υπάρχουν στοιχεία που να υποδηλώνουν ότι το διαδίκτυο οδηγεί ή διεγείρει τα άτομα στον εξτρεμισμό.

Παρ 'όλα αυτά, μπορεί να πει κανείς ότι το διαδίκτυο μπορεί να εκπληρώσει ορισμένες λειτουργίες που επιτρέπουν σε ένα άτομο να εδραιώσει τη διαδικασία ριζοσπαστικοποίησης. Πρώτον, καθιστά ένας μεγάλος όγκος των εξτρεμιστικών και τρομοκρατικών υλικό εύκολα στη διάθεση του χρήστη. Αυτό μπορεί να ενισχύσει το χρήστη ιδεολογική προδιάθεση και ζωοτροφών σε επιχειρήματά του.

Επιπλέον, ο χρήστης έχει δικαίωμα επιλογής μεταξύ των πληροφοριών που βρίσκονται διαθέσιμες στο διαδίκτυο (ανοιχτές πηγές πληροφόρησης).

Τέλος, ο χρήστης μπορεί αναζητήσει ευκολότερα και να προσεγγίσει άτομα ομοϊδεάτες άμεσα με ένα κλικ και με την ασφάλεια που του προσφέρει το διαδίκτυο.

Έτσι για παράδειγμα, κάποιος ενώ δυσκολεύεται να μοιραστεί τις ριζοσπαστικές απόψεις του με άτομα που δρουν στο φυσικό περιβάλλον που ζει και εργάζεται, ίσως να είναι σε θέση ή να μην τον ενοχλεί μια διαδικτυακή απρόσωπη συζήτηση επικοινωνία με άγνωστα άτομα με κοινές ιδέες ή πεποιθήσεις.

4.4.12 Big data[61], IOT and the Cloud (Ιντερνετ των πραγματων ,Υπηρεσιες που ανηκουν στο συννεφο)

Τα «Big Data»[62] δημιουργούνται ουσιαστικά από τα πάντα γύρω μας ανά πάσα στιγμή. Κάθε ψηφιακή αλληλεπίδραση με μέσα μαζικής δικτύωσης παράγει δεδομένα, από το browsing στον υπολογιστή και το online λιανεμπόριο μέχρι τις αγορές στο iTunes και τα likes στο Facebook. Τα δεδομένα αυτά αλιεύονται από πολλαπλές πηγές, με τρομακτική ταχύτητα, όγκο και ποικιλία. Για να εξαγάγει όμως κάνεις ουσιαστική αξία από αυτά, θα πρέπει να έχει στην κατοχή του τη βέλτιστη επεξεργαστική ισχύ, τα κατάλληλα εργαλεία ανάλυσης και φυσικά, τις ανάλογες δεξιότητες.

Όροι όπως» Big Data»[63] και Data Analytics βρίσκονται πλέον στο επίκεντρο των συζητήσεων των IT τμημάτων ανά τον κόσμο, για αυτό και η εξοικείωση με αυτούς αποτελεί μονόδρομος. Αν υπάρχει βέβαια συναίνεση για ένα πράγμα όσων αφορά τα Big Data σήμερα, είναι ότι στην πραγματικότητα δεν έχουν έναν συγκεκριμένο ορισμό.

[61]Boyd, Dana? Crawford, Κέιτ (21 του Σεπτεμβρίου, 2011). "Έξι Προκλήσεις για Big Data". *Social Science Research Network: Μια δεκαετία στην Ώρα Διαδικτύου: Συμπόσιο για τη δυναμική του Διαδικτύου και της Κοινωνίας.*

[62] http://www.fortunegreece.com/article/big-data-i-nea-emmoni-ton-megalon-epichiriseon/

[63]Ο Josh Dreller, ιδιοφυΐα και Διευθυντής της Έρευνας Αγοράς στην Kenshoo, τα περιγράφει απλά ως «κάτι υπερβολικά μεγάλο για να χωρέσει σε ένα υπολογιστικό φύλλο του Excel».

Το «*internet of things»* πρακτικά περιγράφει τη διασύνδεση συσκευών και επαγγελματικού εξοπλισμού που χρησιμοποιούμε καθημερινά σε ένα ευρύτερο δίκτυο, με στόχο την αύξηση της αποτελεσματικότητάς τους και κατά συνέπεια της ποιότητας ζωής αλλά πρωτίστως την παραγωγικότητα των χρηστών.

Το «smartphone» μας πλέον, δύναται να τηρεί το ημερολόγιο και τα εισιτήρια για τις πτήσεις μας, ενημερώνοντάς μας για το πότε πρέπει να ξεκινήσουμε. Το cloud ημερολόγιο μας πληροφορεί για τον καιρό ώστε να ντυθούμε κατάλληλα και να μην ξεχάσουμε τυχόν αξεσουάρ.Το αυτοκίνητό μας συνδέεται σε ένα κεντρικό σύστημα και ελέγχει την κίνηση στους δρόμους προτείνοντάς μας τη βέλτιστη διαδρομή. Τώρα, συνδυάζοντας κάποιος όλα τα παραπάνω, έχει μια πρώιμη ιδέα του τι σημαίνει «internet of things»[64].

Στην ουσία λοιπόν, το διαδίκτυο δεν χρησιμεύει μόνο στους ανθρώπους αλλά και στις μηχανές, τα προϊόντα, τα πράγματα. Όχι βέβαια για να περιηγούνται ελεύθερα αλλά για να επικοινωνήσουν μεταξύ τους, να «συνεννοηθούν» και να συντονιστούν προκειμένου να υπηρετήσουν όσο το δυνατόν αποδοτικότερα τον τελικό αποδέκτη όλων των ενεργειών τους, τον άνθρωπο. Πέραν της ανθρώπινης πραγματικότητας, υπάρχει ήδη μία ακόμα, εκείνη των μηχανών.

4.4.13 INTERNET GOVERNANCE (ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ Η ΔΙΑΚΥΒΕΡΝΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ)

Η Διακυβέρνηση του Διαδικτύου είναι η ανάπτυξη και η εφαρμογή των κοινών αρχών, κανόνων, τους κανόνες, τις διαδικασίες λήψης αποφάσεων, καθώς και τα προγράμματα που διαμορφώνουν την εξέλιξη και τη χρήση του Διαδικτύου.

Ο ορισμός της διακυβέρνησης του Διαδικτύου έχει αμφισβητηθεί από διαφορετικές ομάδες σε όλη την πολιτική και ιδεολογική γραμμές.[65] Ένας από τους κύριους συζητήσεων αφορά το κύρος και την συμμετοχή ορισμένων παραγόντων, όπως οι εθνικές κυβερνήσεις, εταιρικών οντοτήτων και της κοινωνίας των πολιτών, για να παίξει ένα ρόλο στη διακυβέρνηση του Διαδικτύου.

Μια ομάδα εργασίας που συγκροτήθηκε μετά ΟΗΕ ξεκίνησε Παγκόσμια Διάσκεψη Κορυφής για την Κοινωνία της Πληροφορίας (WSIS) πρότεινε τον εξής ορισμό της διακυβέρνησης του Διαδικτύου, στο πλαίσιο της έκθεσης του Ιουνίου του 2005:

[64] http://popaganda.gr/internet-things-aftos-o-megalos-agnostos/

[65]Malte Ziewitz / Christian Pentzold, «Σε αναζήτηση της διακυβέρνησης του Διαδικτύου: Εκτέλεση σειρά με ψηφιακά δικτυωμένο περιβάλλον"

Διακυβέρνηση του Διαδικτύου είναι η ανάπτυξη και η εφαρμογή από τις κυβερνήσεις, τον ιδιωτικό τομέα και την κοινωνία των πολιτών, στους αντίστοιχους ρόλους τους, κοινές Αρχές, κανόνες, κανόνες, διαδικασίες λήψης αποφάσεων, καθώς και τα προγράμματα που διαμορφώνουν την εξέλιξη και τη χρήση του Διαδικτύου. [66]

Η Διακυβέρνηση του Διαδικτύου δεν πρέπει να συγχέεται με την Ηλεκτρονική Διακυβέρνηση. Το 2016 οι κυριότερες συζητήσεις συνδέονταν σχετικά με τη διαπίστευση των Προσωπικών Δεδομένων και τη μεσολάβηση σε υπηρεσίες όπως η μεταρρύθμιση του ‘’WHO IS DNS ‘’και στη γενίκευση της χρήσης της μετάφρασης διευθύνσεων Carrier-Grade Δίκτυο ([67]CGN) με τεχνολογίες από τους παρόχους υπηρεσιών διαδικτύου (ISP[68]).

[66] "Έκθεση της Ομάδας Εργασίας για τη Διακυβέρνηση του Διαδικτύου (WGIG)"

[67]**Carrier-grade NAT (CGN),** επίσης γνωστή ως **μεγάλης κλίμακας NAT (LSN),** είναι μια προσέγγιση για IPv4 σχεδιασμό του δικτύου στο οποίο , έχουν ρυθμιστεί με το ιδιωτικό δίκτυο διευθύνσεις που έχουν μεταφραστεί σε δημόσιες διευθύνσεις IPv4 από middlebox δικτύου διεύθυνση μεταφραστής συσκευές ενσωματωμένες στο δίκτυο του διαχειριστή δικτύου, που επιτρέπει την ανταλλαγή μικρές πισίνες των δημοσίων διευθύνσεων μεταξύ πολλών sites.

[68]Ο **πάροχος υπηρεσιών Διαδικτύου(iso)** είναι ένας οργανισμός, κερδοσκοπικός ή μη, που παρέχει στους συνδρομητές και χρήστες του, συχνά μέσω χρηματικού ή άλλου αντιτίμου, διάφορες υπηρεσίες, οι οποίες σχετίζονται με το Διαδίκτυο (ίντερνετ), όπως πρόσβαση σε ιστοσελίδες, ανταλλαγή ηλεκτρονικών μηνυμάτων (e-mail) αλλά και ανταλλαγή αρχείων (file sharing), επικοινωνία χρηστών σε πραγματικό χρόνο (chat) κ.λ.π.

ΚΕΦΑΛΑΙΟ 5^{ο} : ΚΡΥΠΤΟΓΡΑΦΗΣΗ

5.1Η ΕΝΝΟΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Ένας από τους αρχαιότερους μηχανισμούς ασφαλείας που μπορούν να χρησιμοποιηθούν στην παροχή του απορρήτου των δεδομένων είναι η κρυπτογράφηση. Σκοπός της είναι η εξασφάλιση προστασίας της ιδιωτικότητας, κρατώντας την πληροφορία κρυφή.

Η αντίστροφη διαδικασία της κρυπτογράφησης είναι η **αποκρυπτογράφηση** δηλαδή η μετατροπή των κρυπτογραφημένων πληροφοριών σε κάποια κατανοητή μορφή. Αυτό μπορεί να γίνει με τη στενογραφία, την τέχνη της απόκρυψης δεδομένων μέσα σε άλλα δεδομένα.

Η πληροφορία είναι κρυμμένη μέσα στο μέσο, έτσι ώστε να μην γίνει αντιληπτή από ανεπιθύμητα άτομα, άλλα μόνο από τον παραλήπτη που για τον οποίο προορίζεται. Αυτό ουσιαστικά καταλήγει στη χρήση απαραίτητων δυαδικών ψηφίων σε ένα αθώο αρχείο για την αποθήκευση των ευαίσθητων δεδομένων.

Η κρυπτογραφία είναι και μια τεχνική κρυπτογράφησης και αποκρυπτογράφησης. Εν τάχει ο σκοπός της κρυπτογραφίας ,συνίσταται στη δημιουργία των κατάλληλων συνθηκών έτσι ώστε δύο ή περισσότερα μέρη να μπορούν να επικοινωνήσουν και να ανταλλάξουν μηνύματα με ασφάλεια χωρίς να απειλούνται από κάποιον εξωτερικό παράγοντα.[69]

Στην κρυπτογραφία χρησιμοποιούνται κάποιοι βασικοί όροι, οι οποίοι είναι οι εξής:

- Κρυπτογράφηση (encryption):Η διαδικασία κατά την οποία, με τη χρήση ενός κρυπτογραφικού αλγόριθμου, το αρχικό μήνυμα μετασχηματίζεται σε μία κωδικοποιημένη μορφή.
- Αποκρυπτογράφηση (decryption): Η αντίστροφη διαδικασία της κρυπτογράφησης.
- Κρυπτογραφικός αλγόριθμος (cipher): Η μέθοδος που χρησιμοποιείται για την μετατροπή του αρχικού μηνύματος.
- Κρυπτογραφικό κλειδί (key): Χρησιμοποιείται κατά την διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης
- Αρχικό κείμενο (plaintext): Το μήνυμα το οποίο υπόκειται στην διαδικασία της κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (ciphertext): Το αποτέλεσμα που προκύπτει μέσω της διαδικασίας της κρυπτογράφησης.

[69] https://en.wikipedia.org/wiki/Cryptography

5.1.1 Βασικες Μορφες Κρυπτογραφησης

- Κρυπτογράφηση End-to-end.

Σύστημα επικοινωνίας, κατά το οποίο, μόνο τα άτομα που επικοινωνούν μπορούν να διαβάσουν τα μηνύματα. Δεν υπάρχει δυνατότητα πρόσβασης στα κρυπτογραφικά κλειδιά, που είναι απαραίτητα για την αποκρυπτογράφηση των συνομιλιών.

- *Κρυπτογράφηση πλήρους συσκευής & πλήρους δίσκου* (full device & full disk).

Στην κρυπτογράφηση πλήρους συσκευής δεν κρυπτογραφούνται μόνο όλα τα δεδομένα, αλλά αυτό γίνεται με τέτοιο τρόπο, ώστε να συνδυάζονται ή αναμιγνύονται με το υλισμικό [70](hardware). Έτσι, καθίσταται εξαιρετικά δυσχερής η αποκωδικοποίηση των δεδομένων.

Η κρυπτογράφηση πλήρους δίσκου είναι επίσης χαρακτηριστικό των προσωπικών υπολογιστών. Η κρυπτογράφηση δίσκου είναι η τεχνολογία που προστατεύει την πληροφορία, μετατρέποντάς την σε μη αναγνώσιμο κώδικα, άρα και μη αποκωδικοποιήσιμο από μη εξουσιοδοτημένα πρόσωπα.

Η συγκεκριμένη μορφή κρυπτογράφησης χρησιμοποιεί κρυπτογραφημένο λογισμικό ή υλισμικό κάθε δυαδικού ψηφίου δεδομένων, το οποίο περιέχεται σε δίσκο. Η έκφραση «κρυπτογράφηση πλήρους δίσκου» συχνά σημαίνει ότι οτιδήποτε σε ένα δίσκο κρυπτογραφείται.

5.1.2 Αφανης Ψηφιακη Επικοινωνια & Κρυπτογραφηση

Η ανάπτυξη των τηλεπικοινωνιών και του ηλεκτρονικού εμπορίου έχουν οδηγήσει σε μια συνεχώς διευρυνόμενη αγορά τεχνολογιών ψηφιακής κρυπτογράφησης.

Οι επιχειρήσεις χρειάζονται την κρυπτογράφηση για να προστατεύσουν την πνευματική τους ιδιοκτησία και να εγκαταστήσουν ασφαλείς δεσμούς με τους συνεταίρους, προμηθευτές και πελάτες τους. Οι τράπεζες χρειάζονται τη συγκεκριμένη τεχνολογία για να διασφαλίσουν την εμπιστευτικότητα και αυθεντικότητα των οικονομικών συναλλαγών.

Οι Αρχές Επιβολής του Νόμου χρησιμοποιούν την συγκεκριμένη τεχνολογία για να αποτρέψουν τη διείσδυση στις αστυνομικές επικοινωνίες αλλά και για να γνωρίσουν και να διεισδύσουν σε αυτό τον κόσμο. Στην εξατομικευμένη ιδιωτική σφαίρα, τα άτομα, με το συγκριμένο εργαλείο, προστατεύουν την προσωπική τους επικοινωνία. Η κρυπτογράφηση

[70] https://el.wiktionary.org/wiki/%CF%85%CE%BB%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C

είναι σημαντική για τη δόμηση μιας ασφαλούς παγκόσμιας πληροφοριακής υποδομής για τις επικοινωνίες και το ηλεκτρονικό εμπόριο.

Ωστόσο, όπως και κάθε άλλη τεχνολογική καινοτομία, έχει διττή χρήση (dual use), καθώς στα χέρια εγκληματιών και τρομοκρατών μετατρέπεται σε πανίσχυρο εργαλείο απόκρυψης δραστηριότητας/κινήσεών τους

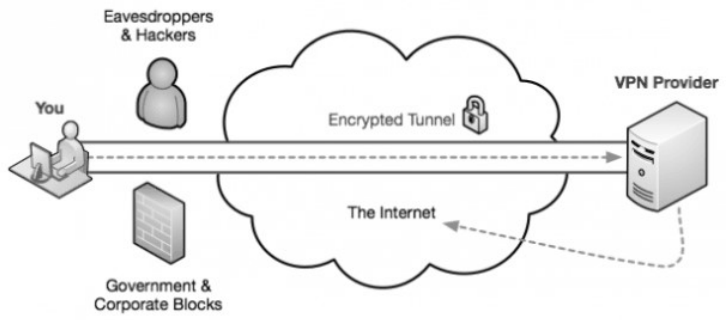
Η κρυπτογράφηση μπορεί να καταστήσει ανέφικτη την ανακάλυψη ευρημάτων και την απόκτηση πληροφοριών, κατά τη διάρκεια των ποινικών ερευνών.

Επίσης, εξουδετερώνει την ανακριτική διείσδυση στις επικοινωνίες, που διαδραματίζει εξαιρετικά σημαντικό ρόλο στην αποτροπή τρομοκρατικών επιθέσεων και τη συγκέντρωση πληροφοριών αναφορικά με τις διεθνείς απειλές.

Η εισαγωγή του ψηφιακού περιβάλλοντος και των Η/Υ μετέβαλε το τοπίο δραστικά. Πλέον, η κρυπτογράφηση της διαδικτυακής επικοινωνίας χρησιμοποιείται ευρέως και ασκεί άμεσο αντίκτυπο στο περιβάλλον της Επιβολής του Νόμου. Οι τεχνολόγοι περιγράφουν τη συγκεκριμένη διαδικασία με τη χρήση της λέξης “OPSEC” (Operational Security[71]).

[71] Τα τηλέφωνα μιας χρήσης εξασφαλίζουν ανωνυμία (τηλέφωνα burner).

5.2 ΚΡΥΠΤΟΓΡΆΦΗΣΗ & VPN (VIRTUAL PRIVATE NETWORK) [72]



α. Τι είναι το VPN

Το Virtual Private Network είναι ένα εικονικό, ιδιωτικό δίκτυο. Επί της ουσίας είναι ένα δίκτυο με τα χαρακτηριστικά του LAN ("τοπικές" διευθύνσεις IP, δυνατότητα File Sharing, δημιουργία τοπικών servers, Internet Connection Sharing) στο οποίο μπορούν να συνδεθούν, με κρυπτογραφημένη σύνδεση υψηλής ασφάλειας, υπολογιστές από ολόκληρο τον κόσμο.

Από όπου και αν συνδέεται ο υπολογιστής, η σύνδεσή του αποκτάει τα χαρακτηριστικά της βάσης του VPN, όπως, π.χ., η εξωτερική IP.

Έτσι, αν συνδεθούμε σε ένα VPN στις Η.Π.Α, και από εκεί στο YouTube, στο youtube θα φαινόμαστε ότι βρισκόμαστε στις ΗΠΑ και εισερχόμαστε με αμερικανική IP, ενώ από την άλλη πλευρά θα έχουμε πρόσβαση και σε βίντεο που απευθύνονται μόνο σε πολίτες των ΗΠΑ.

β. Ποιες είναι οι χρήσεις του

Αν και απλό στην περιγραφή του, ένα VPN έχει πολλές διαφορετικές χρήσεις:

Πρόσβαση σε περιορισμένα site Εκτός από συγκεκριμένα βίντεο του youtube, υπάρχουν υπηρεσίες όπως το Pandora, το Netflix και το Hulu που δεν αφήνουν πρόσβαση σε χώρες εκτός των ΗΠΑ. Η πρόσβαση μέσω VPN λύνει αυτό το πρόβλημα

Παραδείγματα χρήσης:

- Εάν πχ στην εργασία, μας έχουν μπλοκάρει την πρόσβαση στο Facebook ή το

[72] Ένα εικονικό ιδιωτικό δίκτυο (συνήθως αναφέρεται σαν VPN, Virtual Private Network) είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες που ταξιδεύουν να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο.Ένα VPN συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους.

YouTube εάν συνδεθείτε με ένα VPN μπορείτε να πλοηγηθείτε ελεύθερα όπου θέλετε.

- Επαγγελματίες που ταξιδεύουν συχνά, δύνανται να κάνουν χρήση ενός VPN στημένου στην επιχείρηση προκειμένου να έχουν πρόσβαση σε όλους τους τοπικούς πόρους (π.χ. shares στον εταιρικό server).
- Ενα VPN στο σπίτι μπορεί να μας επιτρέψει από οπουδήποτε να έχουμε πρόσβαση σε υπηρεσίες όπως το Remote Desktop, τα τοπικά shares, ή ακόμα και να παίξουμε παιχνίδια μέσω Internet σαν να ήμασταν στο ίδιο τοπικό δίκτυο LAN.
- Ας υποθέσουμε ότι θέλουμε να χρησιμοποιούμε μια ελεύθερη σύνδεση WiFi (δημόσια ή την ξεκλείδωτη του γείτονα), σε όποια σελίδα μπαίνουμε που δεν είναι HTTPS, όλη μας η δραστηριότητα είναι εμφανής σε όποιον ενδιαφέρεται να κοιτάξει. Ενώ, αν συνδεθούμε σε ένα VPN, το μόνο που θα φαίνεται είναι η ασφαλής σύνδεση με το VPN, και όλα τα άλλα δεδομένα θα παραμείνουν κρυμμένα στο VPN.
- Η χρήση του VPN συνίσταται από τους περισσότερους στο να κατεβάσουν αρχεία μέσω BitTorrent – κάτι χρήσιμο ακόμα και για νόμιμα αρχεία, αν κάποιος συγκεκριμένος ISP μειώνει εσκεμμένα την κίνηση μέσω BitTorrent.

Η Σύνδεση σε ένα VPN δεν απαιτεί εξειδικευμένες τεχνικές γνώσεις για να συνδεθεί ένας υπολογιστής με Windows 7 σε VPN. Ουσιαστικά, αρκεί να πάμε στο Start Menu, να γράψουμε VPN στην αναζήτηση και να κάνουμε κλικ στην επιλογή "Set up a virtual private network (VPN) connection".

Συνήθως, η χρήση τέτοιων VPN γίνεται σε χώρες όπου υπάρχει πολλή λογοκρισία όπως την Τουρκία ή Β.Κορέα και έτσι με αυτό τον τρόπο παρακάμπτονται οι οποιοιδήποτε περιορισμοί που έχει επιβάλει η χώρα.

Αν οι Αρχές της Χώρας είναι ενήμερες για την χρήση και την δράση των VPN μπορεί να γίνει χρήση των stealth VPNs οι οποίες αποτρέπουν εντελώς την οποιαδήποτε παρέμβαση και ανίχνευση. Αυτές προσφέρουν κατάργηση αποκλεισμού κάθε ιστοσελίδας, ανεξάρτητα από τη γεωγραφική θέση ή το τείχος προστασίας που έχουν, παρέχουν κρυπτογράφηση και μπορούν να παρακάμψουν ακόμα και τα πιο αυστηρά firewall μεγάλων χωρών.

Τα συστήματα VPN χωρίζονται σε διάφορες κατηγορίες ανάλογα με το τι προσφέρουν και τι είδους τεχνολογία χρησιμοποιούν. Κατηγοριοποιούνται σύμφωνα με τα επίπεδα ασφαλείας που παρέχουν, τα πρωτόκολλα που χρησιμοποιούν, τα στρώματα που χρησιμοποιούν για την σύνδεση.

Η χρήση των VPN συμπερασματικά είναι μια επιλογή για παράκαμψη της λογοκρισίας και της κατασκοπείας.

5.3 Κρυπτογραφηση & Πρωτοκολλο HTTPS

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο αλλά συνδυάζει το απλό HTTP [73]πρωτόκολλο και τις δυνατότητες κρυπτογράφησης που μπορεί να προσφέρει το πρωτόκολλο SSL.

Σκοπός της δημιουργίας του είναι να δηλώνει ποιά διεύθυνση http είναι ασφαλή και ποια όχι. Πολλές φορές βρεθήκαμε αντιμέτωποι στο περιηγητή μας με μια σελίδα που μας έλεγε προχωρήστε με δική σας ασφάλεια. Ο λόγος ήταν γιατί το πιστοποιητικό SSL[74] δεν μας επέτρεπε να προχωρήσουμε γιατί θα ήμασταν εκτεθειμένοι σε κακόβουλους χρήστες.

Η κρυπτογράφηση που χρησιμοποιείται μας εξασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν μπορούν να κλαπούν από άλλους κακόβουλους χρήστες/τρίτους. Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του δικτύου να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού.

Στην συνέχεια ,το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης, η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νόμιμος και ότι το πιστοποιητικό είναι έγκυρο.

Έτσι, οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει. Σήμερα οι πλείστες ιστοσελίδες του διαδικτύου το χρησιμοποιούνε για την ασφάλεια των πελατών τους λόγω των ευαίσθητων πληροφοριών που διακινούνται (π.χ Facebook, Bet365,τράπεζες, ταξιδιωτικές σελίδες, YouTube κ.α.

5.4 Κρυπτογραφηση & Εικονικες Κοινοτητες (Virtual Communities)

Οι εικονικές κοινότητες είναι δίκτυα ατόμων ή ομάδων, τα οποία δεν διασυνδέονται απαραίτητα γεωγραφικά. Ο όρος εικονικός τίθεται για να υπονοήσει μεν μία μη φυσική

[73]Στο http συνδεόμαστε με κάποιον φυλλομετρητή (browser) για να δούμε μία ιστοσελίδα ή γενικά κάποιο έγγραφο σε κάποιον server.Έτσι αφού πληκτρολογήσουμε στον browser την ιστοσελίδα που θέλουμε μέσω του http, ο server το καταλαβαίνει ότι επικοινωνούμε με αυτό το πρωτόκολλο και κάνει τις απαραίτητες ενέργειες για να μας εμφανίζει το αντίστοιχο έγγραφο - ιστοσελίδα.
Πρόκειται για τα αρχικά των λέξεων HyperText Transfer Protocol.

[74] ***Το πρωτόκολλο SSL (Secure Sockets Layer)*** *Χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.*

σύνδεση, χωρίς όμως αυτό να σημαίνει ότι η σύνδεση αυτή είναι ασθενέστερη της συμβατικής φυσικής σύνδεσης μεταξύ κοινοτήτων.

Η κρυπτογράφηση διατηρεί υψωμένους τους «τοίχους» των πραγματικοτήτων (οντοτήτων) του κυβερνοχώρου. Αυτό πρακτικά σημαίνει ότι η πρόσβαση ελέγχου (access control), τα δικαιώματα πρόσβασης (access rights) και τα προνόμια τροποποίησης (modification privileges) παραμένουν απρόσβατα χάρη στην κρυπτογράφηση.

Το φάσμα είναι αρκετά ευρύ ώστε να περιλαμβάνει από εκκλησίες (π.χ. Καθολική Εκκλησία) έως διεθνείς εγκληματικές και τρομοκρατικές ομάδες. Οι εικονικές κοινότητες εκτείνονται στην υφήλιο, υπερβαίνουν τα εθνικά σύνορα και δημιουργούν μία αίσθηση συμμαχίας, «ανήκειν» και κοινότητας.

Αναμφισβήτητα, υπάρχουν περισσότερες εικονικές κοινότητες απ’ ό,τι έθνη-κράτη και οι δεσμοί που ενώνουν τα μέλη τους είναι πιο ισχυροί ακόμη και από τα σοβινιστικά εθνικιστικά συναισθήματα .Κάθε ομάδα, η οποία διαμορφώνεται επί τη βάσει μίας κοινής ιδεολογίας ή ενός ειδικού συμφέροντος, είναι ικανή να μεταμορφωθεί σε συνεκτική κοινότητα.

Η χρήση εργαλείων κρυπτογράφησης διαδικτυακής επικοινωνίας (crypto tools) από εγκληματίες ή εγκληματικές ομάδες (τρομοκρατία, παιδική πορνογραφία κ.λπ.) αποτελεί σημείο αναφοράς από εκείνους που αντιτίθενται στην απεριόριστη πρόσβαση ιδιωτών στη συγκεκριμένη τεχνολογία.

5.5 Κρυπτογραφηση & Dark web.

5.5.1 Ο ιστος του Dark Net

Το dark net είναι ένας παγκόσμιος ιστός πλήρως αυτόνομος. Λειτουργεί παράλληλα με το γνωστό διαδίκτυο και προσφέρει μυστικότητα και ανωνυμία. Η ανίχνευση της ηλεκτρονικής ταυτότητας των χρηστών είναι σχεδόν αδύνατη, γεγονός που είναι ήδη γνωστό στις κοινότητες

Η άκρα μυστικότητα του dark net προσφέρει το ιδανικό καταφύγιο για εμπόρους ναρκωτικών, δίκτυα τρομοκρατίας και ένα ευρύ φάσμα εγκληματικότητας και παράνομου περιεχομένου. Οι μέθοδοι εντοπισμού που χρησιμοποιούν οι διωκτικές υπηρεσίες δεν είναι αποτελεσματικές στο dark net, καθιστώντας το έτσι ουσιαστικά ανεξέλεγκτο.

5.5.2 Το Dark web

Υπάρχει μια σύγχυση ανάμεσα στο λεγόμενο Deep Web και το Dark Web.

Το Deep Web είναι μια τεράστια συλλογή όλων των sites του διαδικτύου, που δεν είναι προσβάσιμα από τις μηχανές αναζήτησης. Αυτές οι unindexed ιστοσελίδες περιλαμβάνουν τεράστιους όγκους περιεχομένου, όπως forums που απαιτείται εγγραφή, δυναμικές ιστοσελίδες, υπηρεσίες σαν το Gmail και πολλά άλλα.

Το «Σκοτεινό Δίκτυο» (Dark Web[75]), ειναι μια μικρή περιοχή του «Βαθύ Ιστού» (Deep Web), που είναι προσβάσιμο μονό μέσω του Tor Onion και οι σελίδες εκεί δεν είναι ανιχνεύσιμες από τις μηχανές αναζήτησης. Σε αυτό υπάρχουν επίσης πάρα πολλά sites αγορών απ' όπου διακινούνται επίσης, προσωπικά δεδομένα που έχουν κλαπεί.

Το πραγματικό Dark Web, πιθανόν αντιπροσωπεύει λιγότερο από το 0,01% του web ενώ συχνά συνδέεται με διακίνηση ναρκωτικών, όπλων, πλαστών εγγράφων παιδικής πορνογραφίας, μηνυμάτων μεταξύ τρομοκρατών ομάδων. Πάραυτα δεν περιέχει μόνο σκοτεινές σελίδες όσο το θέλει η ονομασία.

Ένα εργαλείο που έχει προσαρμόσει αντιγράψει την λειτουργία του Tor WikiLeaks ονομάζεται SecureDrop, και είναι ένα λογισμικό που ενσωματώνει τις κρυφές υπηρεσίες του Tor με οποιοδήποτε ειδησεογραφικό οργανισμό λαμβάνοντας ανώνυμες υποβολές.

5.5.3 Χρησεις του Dark Web & Κρυπτογραφηση

Όπως ειπώθηκε ,το κλειδί για να μπει κανείς στο Darkweb είναι το Tor[76].Το Tor χρησιμοποιείται από τα torrents όπου μπορεί κάποιος να κατεβάσει προγράμματα και ταινίες δωρεάν.

Το Tor είναι η πύλη και για το Deep Web καθώς το δίκτυο λειτουργεί σε όλες τις πλατφόρμες.

Επίσης το Tor WikiLeaks, μια κρυφή υπηρεσία που δημιουργήθηκε για να δεχτεί διαρροές από ανώνυμες πηγές καθώς και ένα παρόμοιο εργαλείο που ονομάζεται I2P κρυπτογραφούν την κυκλοφορία του Ιστού σε στρώματα και την “πετάνε” σε τυχαία επιλεγμένους υπολογιστές σε όλο τον κόσμο. Ο καθένας από αυτούς τους servers αφαιρεί ένα από τα στρώματα της ενιαίας κρυπτογράφησης πριν περάσει τα δεδομένα στον επόμενο server.

[75]Σύμφωνα με τον συγγραφέα του άρθρου Andy Greenberg το Dark Web αντιπροσωπεύει το 0.01% του Web και όχι το 90% όπως συχνά αναφέρουν blogs και Media.

[76] https://en.wikipedia.org/wiki/Tor_(anonymity_network)

Επίσης υπάρχει και μία άλλη εναλλακτική, το Tails OS, ένα λειτουργικό που μπορεί κανείς να χρησιμοποιήσει ανά πάσα στιγμή και σε οποιονδήποτε υπολογιστή, εφόσον είναι bootable από DVD (ιδανική περίπτωση).

Το Facebook, ξεκίνησε πρόσφατα μια ιστοσελίδα στο Dark Web με στόχο την καλύτερη προστασία σε χρήστες που επισκέπτονται την ιστοσελίδα με Tor για να αποφύγουν την επιτήρηση και τη λογοκρισία.

Με τους πιο βασικούς τεχνικούς όρους, το Dark Web αποτελείται από έναν σχετικά μικρό αριθμό websites, σε σχέση με το κανονικό Web, τα οποία:

α) δεν είναι ορατά στις μηχανές αναζήτησης (κρυπτογραφημένα),

β) για να τα προσπελάσει κάποιος χρειάζεται να διαθέτει έναν ειδικό browser όπως τον Tor, ο οποίος αποκρύπτει την IP διεύθυνσή του.

Από τη στιγμή που θα βρεθεί κάποιος, μέσω του Tor, στο επονομαζόμενο Dark Web, γίνεται ιδιαίτερα δύσκολο να προσδιορίσει ποιος ή τι άλλο βρίσκεται στο δίκτυο - κάτι που αποτελεί και τον ίδιο το σκοπό της ύπαρξής του. Κι αυτό ακριβώς το χαρακτηριστικό είναι που κάνει το Dark Web ιδιαίτερα δημοφιλές σε όσους επιθυμούν να διατηρήσουν κρυφή την ταυτότητά τους, όπως οι διακινητές υλικού παιδικής πορνογραφίας ή ναρκωτικών.

Έτσι οι διευθύνσεις IP των εν λόγω ιστοσελίδων διατηρούνται κρυφές, κάτι όμως που δεν σημαίνει ότι είναι κατ 'ανάγκη μυστικές.

Κρυμμένες υπηρεσίες στο Tor[77], όπως τα sites που πωλούν ναρκωτικά Silk Road, Silk Road 2, Agora και Evolution είχαν εκατοντάδες χιλιάδες τακτικούς χρήστες. Έτσι πχ η διεύθυνση Silk

[77] Το Tor (συντομογραφία του The onion router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο. Το λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης. Η χρήση Tor κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη, συμπεριλαμβανομένου επισκέψεων σε κάποια ιστοσελίδα, διαδικτυακές αναρτήσεις, προγράμματα άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας, κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του.

Το Tor μπορεί επίσης να προσφέρει ανωνυμοποίηση στους διακομιστές στη μορφή της υπηρεσίας απόκρυψης τοποθεσίας, η οποία αποτελείται από πελάτες του Tor ή κόμβους που τρέχουν ειδικά διαμορφωμένο λογισμικό διακομιστών. Αντί να αποκαλύπτουν τη διεύθυνση IP των διακομιστών (και άρα τη διαδικτυακή τοποθεσία τους) οι κρυμμένες υπηρεσίες είναι προσβάσιμες μέσω Tor-specific .onion pseudo top-level domain (TLD), ή αλλιώς pseudomain.

Το Tor είναι αποκεντρωμένο με βάση τον σχεδιασμό του. Δεν υπάρχει δηλαδή άμεσα αναγνώσιμη λίστα των κρυμμένων υπηρεσιών. Υπάρχει ένας αριθμός ανεξάρτητων κρυμμένων υπηρεσιών που εξυπηρετούν αυτό το σκοπό.

Road κάθε άλλο από μυστική ήταν. Όποιος τρέχει Tor και ξέρει το url ενός site, (τελειώνει σε «.onion») μπορεί εύκολα να επισκεφθεί τις παράνομες online αγορές.

Οι συναλλαγές γίνονται σχεδόν αποκλειστικά με το ψηφιακό κρυπτονόμισμα Bitcoin, ώστε να μην μπορεί να εντοπιστούν εύκολα πωλητές και αγοραστές.

Συμπερασματικά πρόκειται για ένα μέρος όπου συγκεντρώνει χιλιάδες ανθρώπους από όλο τον κόσμο, οι οποίοι κάνοντας χρήση της κρυπτογραφημένης, ψηφιακά οχυρωμένης ανωνυμίας μπορούν να μοιραστούν μεταξύ τους ότι επιθυμούν.

5.6 Κρυπτοαναρχια[78] (Crypto Anarchy)

Η κρυπτοαναρχία (crypto anarchy) είναι μια φράση που διατυπώθηκε αρχικώς από τον Timothy C.May για να περιγράψει ένα πιθανό (ενδεχομένως αναπότρεπτο) πολιτικό αποτέλεσμα από την ευρεία χρήση τεχνολογιών κρυπτογράφησης.

Συνιστά διεθνή απειλή, η οποία μεγεθύνεται από το μείζον διεθνές επικοινωνιακό σύστημα, το διαδίκτυο. Η κρυπτοαναρχία μπορεί να θεωρηθεί και ως ο πολλαπλασιασμός της κρυπτογραφίας που παρέχει το πλεονέκτημα της προσβασιμότητας, αλλά όχι και της προστασίας από δυνητικούς κινδύνους και βλάβες.

Δεν διασφαλίζει την προστασία των χρηστών και των οργανισμών από ηλεκτρονικά ατυχήματα και καταχρήσεις. Είναι σαν «*ένα αυτοκίνητο χωρίς φρένα, χωρίς ζώνες ασφαλείας, χωρίς πινακίδες, εχθρικό προς το περιβάλλον και στο οποίο δεν μπορείς να μπεις εάν ξεχάσεις τα κλειδιά σου μέσα σε αυτό».*

Οι δυνητικοί κίνδυνοι της κρυπτογραφίας έχουν εντοπιστεί εδώ και δύο δεκαετίες[79].

Η λύση δεν είναι η παγκόσμια καταστολή των επικοινωνιών και των εργαλείων κρυπτογράφησης, αλλά μάλλον η υπεύθυνη χρήση αυτών των τεχνολογιών, ώστε να μην οδηγούν σε κοινωνική αταξία.

---

[78] Κρυπτοαναρχία & Παράνομη Συναλλακτική Δραστηριότητα. Η αντιμετώπιση αυτής της απειλής απαιτεί διεθνή προσέγγιση, τόσο για τη διασφάλιση της διεθνούς επικοινωνίας μέσω εθνικών συνόρων όσο και για την ηλεκτρονική παρακολούθηση από τις κυβερνήσεις της εγκληματικής και τρομοκρατικής δραστηριότητας, που λαμβάνει χώρα εντός των αρμοδιοτήτων τους. Η βασική ιδέα είναι ότι όσο περισσότερο οι συναλλαγές λαμβάνουν χώρα πίσω από το πέπλο της κρυπτογράφησης καθίσταται ολοένα και ευκολότερο για τα πρόσωπα να συνάπτουν επιχειρηματικές σχέσεις οι οποίες εκπίπτουν του πεδίου των παραδοσιακών εθνών κρατών. Για παράδειγμα, ταυτόχρονα με το γεγονός ότι συγκεκριμένες παράνομες συναλλαγές εξαπλώνονται περισσότερο καθίσταται και δυσκολότερο για τα σύγχρονα έθνη κράτη να επιβάλλουν στο εσωτερικό την πολιτική τους (φορολογικοί νόμοι, έλεγχος μαύρης αγοράς).

[79]Οι αμερικανικές υπηρεσίες έρευνας και δίωξης, ήδη από το 1995, αντιμετώπισαν την κρυπτογραφημένη διαδικτυακή επικοινωνία σε υποθέσεις τρομοκρατίας, παιδικής πορνογραφίας, ναρκωτικών, κατασκοπείας, δολοφονιών κ.λπ.

5.7 Κρυπτογραφηση & Τρομοκρατια

Καθώς η κρυπτογράφηση γίνεται ολοένα και περισσότερο μέρος των ηλεκτρονικών συσκευών και των διαδικτυακών εφαρμογών διαμοιρασμού μηνυμάτων, ένα εύρος εγκληματικών δρώντων, περιλαμβανομένων των ισλαμιστών τρομοκρατών εκμεταλλεύονται την τεχνολογία για να επικοινωνούν και να αποθηκεύουν πληροφορίες, αποφεύγοντας έτσι την ανίχνευση και την ενοχοποίηση (φαινόμενο "going dark"[80]).

Έτσι οι υπηρεσίες πληροφοριών και εσωτερικής Ασφάλειας στρέφουν όλο και περισσότερο το ενδιαφέρον τους στην τεχνολογία και την πιθανή η πραγματική χρήση της κρυπτογράφησης από τρομοκρατικές ομάδες.

Παρά τη δημόσια αντιπαράθεση και στις δύο πλευρές του Ατλαντικού μεταξύ κυβερνητικών υπηρεσιών και τεχνολογικών υπηρεσιών, τόσο οι υποστηρικτές των ατομικών ελευθεριών όσο και υψηλοί αξιωματούχοι της εθνικής ασφάλειας, επιχειρηματολογούν ότι με το να δημιουργηθούν «παραθυράκια» και δυνατότητες ανάκτησης επικοινωνιών από τις Αρχές Επιβολής του Νόμου θα προκαλέσει μεγαλύτερο κακό.

Η διαδεδομένη σύγχυση για την πραγματική λειτουργία της κρυπτογράφησης θα παρέμενε.

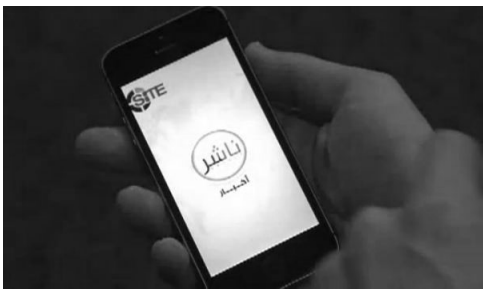
Οι τεχνολόγοι έχουν προ πολλού συνειδητοποιήσει ότι τα κανονιστικά μέτρα έχουν πολύ μικρές πιθανότητες να αναστρέψουν τη διαδικασία. Εκτός από το γεγονός ότι λογισμικό εγγράφεται σε άλλες χώρες, αυτό που δεν έχει γίνει πλήρως κατανοητό στη δημόσια αντιπαράθεση είναι ότι ο πηγαίος κώδικας (source code), αφ' εαυτού, πίσω από την κρυπτογράφηση "end-to-end", είναι ευρέως διαθέσιμος στο διαδίκτυο.

Αυτό σημαίνει ότι, πέρα από την απίθανη εκδοχή κλεισίματος του διαδικτύου ελάχιστα μπορούν να γίνουν για να ανασχεθούν τα άτομα, περιλαμβανομένων των τρομοκρατών, από την δημιουργία και προσωπική εκμετάλλευση του δικού τους λογισμικού κρυπτογράφησης.

5.7.1 Τρομοκρατια & Κοινωνικα Δικτυα (Online Social Networks)

Τα online κοινωνικά δίκτυα (OSNs), όπως τα Twitter, Facebook και YouTube, έχουν αναδειχθεί ως μείζονα μέσα επικοινωνίας μεταξύ ατόμων για το διαμοιρασμό και την ανταλλαγή πληροφοριών αναφορικά με μια μεγάλη ποικιλία γεγονότων του πραγματικού κόσμου.

[80] http://www.urbandictionary.com/define.php?term=Going%20Dark



Φυσικά, τα κοινωνικά δίκτυα έχουν διττή χρήση, καθώς, ενώ χρησιμοποιούνται θετικά για επικοινωνία και ανταλλαγή πληροφοριών, ταυτόχρονα αποτελούν – αρνητικά – εργαλείο υποστήριξης της τρομοκρατίας.

Οι τρομοκράτες, μέσω του Ιστού και των κοινωνικών δικτύων, διαμοιράζουν πληροφορίες, διαχέουν προπαγάνδα, στρατολογούν νέα μέλη και σχεδιάζουν επιθέσεις. Για παράδειγμα, η τρομοκρατική οργάνωση al-Shabaab χρησιμοποίησε το Twitter, κατά τη διάρκεια της επίθεσης στο Westgate, στην πρωτεύουσα Ναϊρόμπι της Κένυας (διάχυση πληροφορίας και ανάληψη ευθύνης)

Το Ισλαμικό Κράτος (ΙΚ), περισσότερο από οποιαδήποτε άλλη τρομοκρατική οργάνωση, έχει στηρίξει την επικοινωνιακή στρατηγική του και την προώθηση των ακραίων ιδεολογικών θέσεών του στις προαναφερόμενες διαδικτυακές πλατφόρμες.

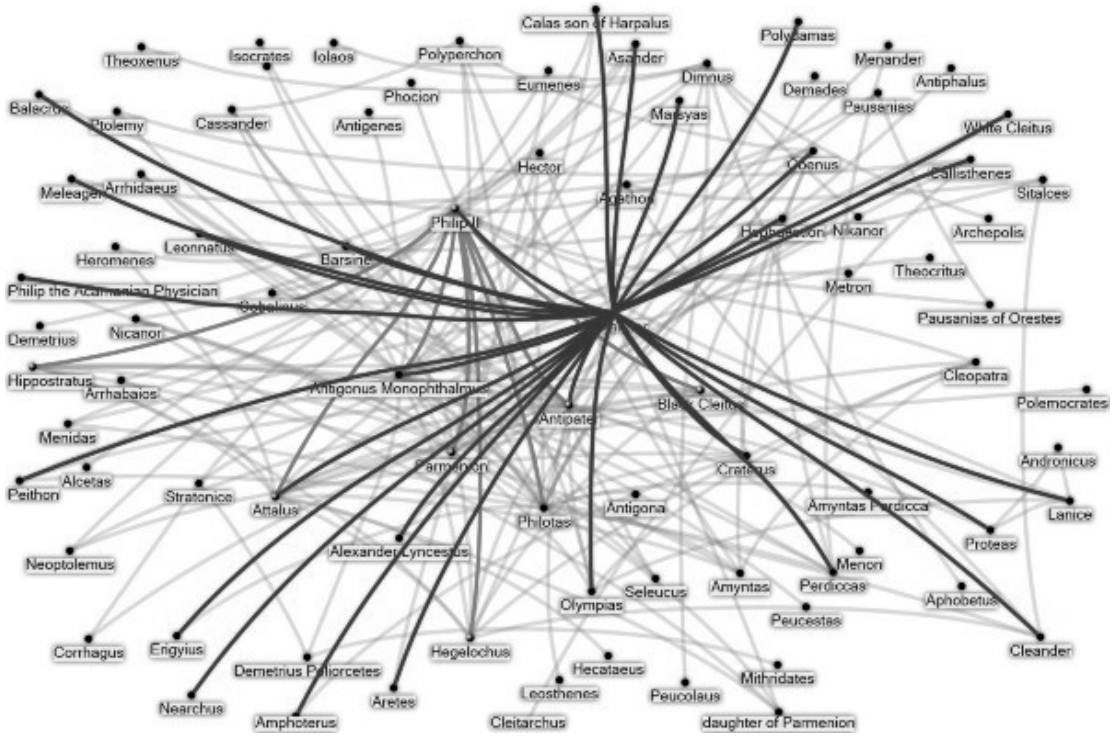
Παρά το γεγονός ότι το ΙΚ έχει στη διάθεσή του μία ποικιλία από ψηφιακά εργαλεία διάχυσης της προπαγάνδας του, ιδιαίτερο ενδιαφέρον παρουσιάζει η ευρεία χρήση της υπηρεσίας Twitter[81]. Χαρακτηριστικά, μετά από έρευνα του Ινστιτούτου Brookings σε ένα δείγμα 20.000 λογαριασμών χρηστών – υποστηρικτών του IS, προέκυψαν τα ακόλουθα ευρήματα:

Μολονότι το δείγμα περιορίστηκε σε 20.000 λογαριασμούς, από Σεπτέμβριο έως και Δεκέμβριο του 2014, οι σχετικοί λογαριασμοί εκτιμήθηκαν σε τουλάχιστον 46.000 και, ενδεχομένως, έως και 70.000 όχι όμως ταυτόχρονα ενεργοί.

Το μεγαλύτερο μέρος των χρηστών τοποθετήθηκε γεωγραφικά σε κατεχόμενα εδάφη της τρομοκρατικής οργάνωσης στη Συρία και στο Ιράκ, αλλά και στη Σαουδική Αραβία (με σημαντικό μέρος αυτών να προέρχεται από τις ΗΠΑ και το Ηνωμένο Βασίλειο).

Σχεδόν ένας στους πέντε χρήστες είχε προεπιλεγμένη γλώσσα χρήσης την αγγλική, ενώ τα τρία τέταρτα την αραβική.

[81]Αν και η δραστηριοποίηση της οργάνωσης στο Twitter θεωρείται ως νευραλγική για τη διάδοση του εν γένει αφηγήματος του IS, δεν πρέπει να παραβλέπεται ο ρόλος οπτικοακουστικών πλατφορμών, όπως το YouTube. Η συντονισμένη ανάρτηση βίντεο με σχετικό προπαγανδιστικό περιεχόμενο συνεισφέρει αποτελεσματικά στους στόχους αυτοπροβολής του ΙΚ, εξασφαλίζοντας μία εντυπωσιακά υψηλή θέαση (views).



Οι εν λόγω λογαριασμοί είχαν κατά μέσο όρο περίπου 1.000 ακόλουθους (followers) ο καθένας – αριθμός πολύ υψηλός σε σχέση με ένα συνηθισμένο λογαριασμό – και ήταν, παράλληλα, ομοίως περισσότερο ενεργοί (αποστολή μηνυμάτων κ.λπ.).

Μεγάλο μέρος της επιτυχίας χρήσης της πλατφόρμας αποδόθηκε στην ύπαρξη ενός ισχυρού πυρήνα «υπερδραστήριων χρηστών», στην οποία αποδόθηκε η χρήση 500 έως 2.000 λογαριασμών.

Το 69% των χρηστών έκανε χρήση της πλατφόρμας μέσω λογισμικού Android, ενώ το 30% και το 1% αντίστοιχα χρησιμοποίησαν συσκευές iPhone και Blackberry.

5.7.2 Εργαλεια Χρησης των OSNs απο τις Τρομοκρατικες Οργανωσεις

Τα μέσα κοινωνικής δικτύωσης παρέχουν εύκολη πρόσβαση, δεν ελέγχονται εύκολα από τις κυβερνήσεις, εξασφαλίζουν παγκόσμιο κοινό και ανωνυμία και μέσω της κρυπτογράφησης πετυχαινουν ταχεία ροή πληροφοριών.

Στο σημερινό περιβάλλον ταχείας ανάπτυξης της Πληροφορίας και Τεχνολογιών Επικοινωνιών, τα online κοινωνικά δίκτυα δύναται να χρησιμοποιηθούν για τους ακόλουθους σκοπούς:

Ανταλλαγή Πληροφοριών. Μέσω λογισμικών κρυπτογράφησης, οι τρομοκράτες μπορούν να

απευθύνονται σε ένα ευρύ κοινό, να επικοινωνούν μεταξύ τους και να διασφαλίζουν την επικοινωνία τους[82].

Στρατολόγηση & Εκπαίδευση. Το διαδίκτυο έχει καταστεί κρίσιμο εργαλείο στα χέρια των τρομοκρατών για τη διάδοση των μηνυμάτων και τη στρατολόγηση νέων υποστηρικτών[83].

Σχεδιασμός Επιθέσεων. Τα online κοινωνικά δίκτυα χρησιμοποιούνται από τους τρομοκράτες για το σχεδιασμό επιθέσεων λόγω της ασφαλούς επικοινωνίας και του ταχύτατου διαμοιρασμού μηνυμάτων

Χρηματοδότηση. Μέσω διαδικτυακών συναλλαγών και ηλεκτρονικού ταχυδρομείου, οι ομάδες διεξάγουν χρηματοδότηση στα κοινωνικά δίκτυα.

Κυβερνοεπιθέσεις.[84] Οι κυβερνοεπιθέσεις αναφέρονται στη χρήση εργαλείων ηλεκτρονικής δικτύωσης για την επίθεση σε άλλα ηλεκτρονικά δίκτυα ή εθνικά συστήματα επικοινωνιών (κυβερνητικές επιχειρήσεις μεταφορών και ενέργειας).

Προπαγάνδα. Μολονότι τα κοινωνικά δίκτυα ασκούν σημαντικό αντίκτυπο στην κοινωνική δομή, ταυτόχρονα οι τρομοκράτες τα χρησιμοποιούν για τη διάχυση της προπαγάνδας τους. Η προπαγάνδα σχετίζεται με ιδεολογικές διευκρινίσεις της τρομοκρατικής εκστρατείας. Μπορεί να συμπεριλάβει μηνύματα, επιδείξεις, περιοδικά, ήχο και αποσπάσματα από video βίαιων πράξεων[85].

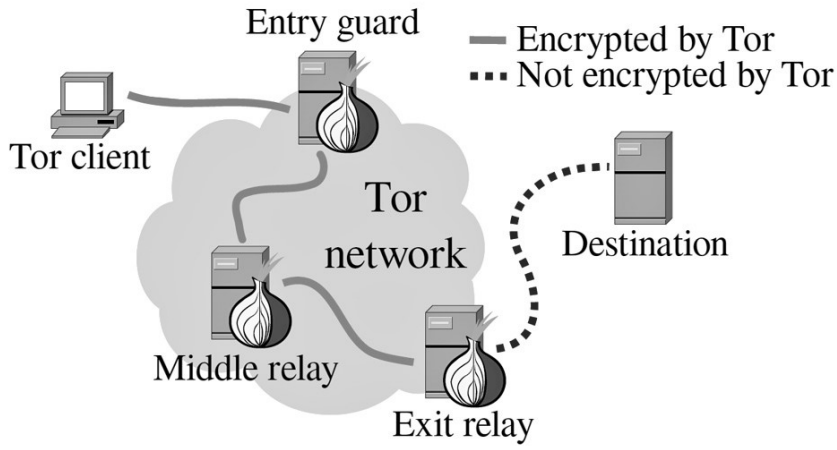
5.8Τρομοκρατία & Δίκτυο Tor

[82]Χαρακτηριστικό παράδειγμα, η χρήση λογισμικών κρυπτογράφησης από την al-Qaeda (mujahedeen secrets 1 & 2

[83] Έρευνα του πανεπιστημίου G. Washington (Homeland Security Institute, 2009).

[84] **Cracking ε**ίναι η παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, η αλλαγή των κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους.Στόχος του cracker είναι μέσω της μη εξουσιοδοτημένης πρόσβασης στο σύστημα υπολογιστών και των δεδομένων του η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους βλάβης.**Hacking** είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση της ικανότητας να εισβάλουν σε ένα υπολογιστικό σύστημα. Ένας hacker, μπορεί να εισέλθει σε ένα σύστημα και να προκαλέσει ζημία, παραβιάζοντας το απόρρητο της ηλεκτρονικής αλληλογραφίας, μπλοκάροντας τις υπηρεσίες του συστήματος ή «κλέβοντας» πολύτιμα αρχεία και δεδομένα οργανισμών.

[85]Συναφώς, η έννοια της κυβερνοπροπαγάνδας αφορά στην εμφύτευση, μέσω διαδικτύου, στο ασυνείδητο του δέκτη του μηνύματος μιας ιδέας, της εκκόλαψής και αποκρυστάλλωσής της, καθώς επίσης της ανάδυσής της στο συνειδητό, ως νομιζόμενης επιλογής του δέκτη.



Μία υποκουλτούρα που συχνάζει στο Dark Web είναι και οι τρομοκράτες που χρειάζονται ένα ανώνυμο δίκτυο άμεσα διαθέσιμα και γενικά απρόσιτο. Θα ήταν αρκετά δύσκολο για τους τρομοκράτες να διατηρήσουν μια ιστοσελίδα στο κανονικό διαδίκτυο λόγω της ευκολίας πρόσβασης στο site.

Οι τρομοκρατικές οργανώσεις, επίσης, ψάχνουν στο Σκοτεινό Web σαν μια εναλλακτική λύση επικοινωνίας μέσω του Διαδικτύου.Το 2007, ο Mark Burgess, διευθυντής του Παγκόσμιου Ινστιτούτου Ασφάλειας στις Βρυξέλλες, προειδοποίησε ότι «η υπερβολική εστίαση σχετικά στο κλείσιμο των ιστοσελίδων θα μπορούσε να είναι αντιπαραγωγική, δεδομένου ότι κατά πάσα πιθανότητα οι τρομοκρατικές δυνάμεις μεταφέρουν τις ιστοσελίδες τους στο λεγόμενο Dark Web»

Η τρομοκρατία εκμεταλλεύεται συχνά καταστάσεις όπως τη φτώχεια, για να σχηματίσει online αποκλίνουσες ομάδες: «ομάδες ατόμων ευπαθών κοινωνικά, οικονομικά και ψυχολογικά θα μπορούσε να αποτελέσουν ένα γόνιμο έδαφος για την πρόσληψη ατόμων σε δυνητικά βίαιες καταστάσεις, ιδιαίτερα για τους νέους».

Στην κατανόηση του πώς λειτουργούν οι εξτρεμιστικές ομάδες στο σκοτεινό Web, θα πρέπει να μελετήσουμε το έργο του καθηγητή Chen του Πανεπιστημίου της Αριζόνα, ο οποίος έχει δημοσιεύσει πολυάριθμα άρθρα σχετικά με τα εργαλεία των Jihadist στο σκοτεινό διαδίκτυο Dark Web.

Ο Chen και η ομάδα του έχουν αναπτύξει μεθόδους για την παρακολούθηση της εξάπλωσης των επικίνδυνων ιδεών μέσω ορισμένων Jihad forums του Παγκόσμιου Ιστού.

«Χρησιμοποιώντας ένα μαθηματικό μοντέλο γνωστό σαν SIR, που χρησιμοποιείται από επιδημιολόγους για να καταγράψουν τη μετάδοση μιας νόσου, οι ερευνητές κατέληξαν στο

συμπέρασμα ότι ο ρυθμός «μόλυνσης» μπορεί να «φτιάξει» 2 βομβιστές αυτοκτονίας κάθε 10.000 άτομα. Οι αναλύσεις των forums του Dark Web δείχνουν επίσης ότι όσο περισσότεροι είναι οι συμμετέχοντες σε ένα forum, τόσο πιο βίαια γίνονται τα μηνύματά τους».

Ένα από τα χαρακτηριστικά των τρομοκρατικών δικτυακών ιστοσελίδων είναι η ικανότητά τους να διαχειρίζονται τις ραγδαίες αλλαγές των διευθύνσεων στο Διαδίκτυο.

Όταν οι Αρχές αναγκάσουν ένα site για να μετακινηθεί, τα ανεπίσημα δίκτυα (chatrooms ή e-mail) αναλαμβάνουν δράση. Ενημερώνουν όλους τους υποστηρικτές της ομάδας για τη νέα διεύθυνση του δικτύου. Αυτό το σύστημα διανομής νέων διευθύνσεων » από στόμα σε στόμα» φαίνεται να είναι πολύ αποτελεσματικό.

5.9 Η περιπτωση του Ισλαμικου Κρατους (ΙΚ)[86] .

5.9.1 Γενικα περι Χαλιφατου

Όνειρο του τζιχαντιστικού κινήματος ,ήταν η αναδημιουργία του Χαλιφάτου, παραμένοντας πρακτικά ως μια ρομαντική ιδέα, εφόσον η δημιουργία ενός σύγχρονου κράτους υπό αυτές τις προϋποθέσεις παραβιάζει καθέτως και οριζοντίως τους κανόνες του διεθνούς δικαίου.

Ιστορικά, η δημιουργία της έννοιας του Ισλαμικού Κράτους αντλεί την κοσμοθεωρία της ήδη από το θάνατο του Προφήτη Μωάμεθ, όπου και συναντάται η διεθνής κοινότητα των ουλεμάδων (μουσουλμάνοι θρησκευτικοί λόγιοι), η οποία αναπτύσσει την έννοια της τζιχάντ, προεκτείνοντας τα διδάγματα του Προφήτη.

Το Ισλαμικό Κράτος του Ιράκ και της Συρίας (ΙΚΙΣ) ή για χάριν συντομίας Ισλαμικό Κράτος (ΙΚ), αναδύθηκε στη διεθνή σκηνή, σε μια εποχή απόλυτης αποσταθεροποίησης και αναταραχής στη Μέση Ανατολή. Η Συρία και το Ιράκ βρίσκονταν σε πόλεμο έχοντας υποστεί συνεχείς βομβαρδισμούς απο διάφορες δυνάμεις, η Λιβύη ήταν στα πρόθυρα νέας εμφύλιας σύρραξης, η Αίγυπτος σε αναταραχή με τον στρατό να κυριαρχεί απόλυτα και το Ισραήλ να βρίσκεται εκ νέου σε πόλεμο με τη Γάζα.

Η μεγάλη τζιχάντ, σύμφωνα με τη θεωρία, συνδέεται με πνευματικές διδαχές και αποτελεί τον αγώνα του ατόμου ενάντια στους καθημερινούς πειρασμούς. Η μικρή τζιχάντ αποτελεί την φυσική πάλη ενάντια στον εχθρό, έχοντας τόσο αμυντική όσο και επιθετική σημασία. Η

[86]Το Ισλαμικό Κράτος (αραβικά:الدولـــة الإســـلامية, αντ-νταουλάτ αλ-ισλαμίγια), αρχικά γνωστό ως (ISIS) Ισλαμικό Κράτος του Ιράκ και του Λεβάντε (ο όρος «Λεβάντε» αναφέρεται επίσης ως «Ανατολής», «Συρίας» ή «Αλ-Σαμ») είναι μία ενεργή τζιχαντιστική τρομοκρατική οργάνωση του Ιράκ και της Συρίας. Στις 29 Ιουνίου 2014, το ISIS αλλάζει το όνομα του σε Ισλαμικό κράτος και κηρύτει μονομερώς την ίδρυση χαλιφάτου, σε μια έκταση που περιέχει περιοχές της Συρίας και του Ιράκ, ορίζοντας στην θέση του «χαλίφη» και «ηγέτη των απανταχού μουσουλμάνων» τον επικεφαλής της, Αμπού Μπακρ αλ-Μπαγκντάντι (γνωστό έκτοτε ως «Χαλίφης Ιμπραήμ»).

επιθετική τζιχάντ μπορεί να κηρυχθεί μόνο απο τον χαλίφη και αποστολή της είναι η επεκτατική πολιτική, η εξάπλωση του Ισλάμ και όχι η προστασία του.

Το ΙΚ οφείλει τον διεθνή χαρακτήρα του κυρίως στην πάγια και γνωστή πια τακτική του: αυτήν της "προπαγάνδας του φόβου", μέσω του διαδικτύου και των social media. Το ΙΚ, με τον νεωτεριστικό του χαρακτήρα και προσηλυτίζοντας εθελοντές εξειδικευμένους στους υπολογιστές και την χρήση των social media, κατόρθωσε σε πολύ σύντομο χρονικό διάστημα να σπείρει τον φόβο σε όλο τον κόσμο, μεταδίδοντας σκηνές ακραίας βίας μέσα από καλογυρισμένα βίντεο και πλήθος φωτογραφιών με βασανιστήρια, σε τέτοια ανάλυση ώστε να μπορούν εύκολα να προβληθούν ακόμα και μέσω ενός smartphone.

Ο προπαγανδιστικός μηχανισμός του ΙΚ, ανέλαβε την διεξαγωγή μιας ηλεκτρονικής τζιχάντ (cyber jihad). Στο νέο αυτό είδος πολέμου, πρωτοστατούν το υλικό πολυμέσων (βίντεο, φωτογραφίες, ηχητικά ντοκουμέντα και μουσική) και οι σύγχρονες πλατφόρμες επικοινωνίας όπως το Twitter, το Facebook, το Instagram, το YouTube, το Diaspora, το Ask.fm και το Tumblr, μέσω των οποίων σκιαγραφείται το όραμα της ανασύστασης του Χαλιφάτου που θα συσπειρώσει τους απανταχού μουσουλμάνους.

Την υπεροχή και την αποτελεσματικότητα της προπαγάνδας του ΙΚ μέσω των ΜΚΔ(Μέσων κοινωνικής δικτύωσης) αναγνωρίζουν και οι αντιτρομοκρατικές υπηρεσίες και κυβερνοπολέμου των ΗΠΑ, όπως για παράδειγμα το Κέντρο Στρατηγικών Αντιτρομοκρατικών Επικοινωνιών (Center for Strategic Counterterrorism Communications- CSCC).

5.9.2 Κρυπτογραφηση & ΙΚ

Προπαγάνδα & κυβερνοεπιθέσεις

Οι τζιχαντιστές-χάκερ του (/DAESH) έχουν δημιουργήσει μια οργάνωση η οποία αποκαλείται «Ισλαμικό Κράτος – Τμήμα Hacking» (Islamic State Hacking Division)ή ΚυβερνοΧαλιφάτο (Cyber Caliphate) η οποία είναι υπεύθυνη για πολλές κυβερνοεπιθέσεις σε κυβερνητικές ιστοσελίδες των ΗΠΑ, της Γαλλίας και άλλων χωρών.

Η δράση του Cyber Caliphate εστιάζεται στη παραβίαση ιστοτόπων και ιστοσελίδων με σκοπό την εκτέλεση ψυχολογικών επιχειρήσεων και προπαγάνδας, την κλοπή ευαίσθητων δεδομένων και την πρόκληση ψηφιακών δολιοφθορών.

Η ομάδα ξεκίνησε τη δράση της στις Αρχές του 2015, με επίθεση στο λογαριασμό Twitter και YouTube της Κεντρικής Στρατιωτικής Διοίκησης των ΗΠΑ (United States Central Military Command).

Παράλληλα έχει παραβιάσει και άλλες ιστοσελίδες και ηλεκτρονικές εφημερίδες όπως την International Business Times, ενώ είναι υπεύθυνη για επιθέσεις σε 19.000 γαλλικές ιστοσελίδες, μόνο τον Ιανουάριο του 2015, μετά την τρομοκρατική επίθεση στο γαλλικό περιοδικό CharlieHebdo .

Οι χάκερς της οργάνωσης είναι εξαιρετικά δύσκολο να εντοπιστούν και να ταυτοποιηθούν. Κυρίως δρουν μέσω του Dark Web προκειμένου να ασκήσουν προπαγάνδα, να συνδιαλλάζουν και να αναζητήσουν οικονομικούς πόρους για τη χρηματοδότηση των επιχειρήσεων τους.

Σημαίνον πρόσωπο του Cyber Caliphate, θεωρείτο ο Γιουνάι Χουσεΐν[87] (JunaiHussein) ο οποίος ανήκε στην ηγετική ομάδα της οργάνωσης.

Ο Γιουνάι απασχόλησε για πρώτη φορά τις Αρχές όταν συνελήφθη το 2012 στο Ηνωμένο Βασίλειο (ΗΒ), με την κατηγορία της παραβίασης του λογαριασμού της ηλεκτρονικής αλληλογραφίας του Τόνυ Μπλερ. Αξιοποιώντας τις γνώσεις του εκτέλεσε αναρίθμητες κυβερνοεπιθέσεις, αποσπώντας απόρρητα στοιχεία που αφορούσαν τις Αμερικανικές δυνάμεις και το προσωπικό τους στο Ιράκ, ενώ παράλληλα στρατολογούσε άτομα από τη Δύση για λογαριασμό του ΙΚ μέσω των κοινωνικών δικτύων. [88]

<u>Hacking</u>

Μεγάλο ενδιαφέρον δείχνουν οι τζιχαντιστές για την κλοπή ευαίσθητων προσωπικών δεδομένων αξιωματούχων και κυβερνητικών υπαλλήλων και στελεχών που υπηρετούν στις Ένοπλες Δυνάμεις των ΗΠΑ και άλλων δυτικών κρατών που έχουν χαρακτηρίσει ως εχθρικά.

Ο Κοσσοβάρος χάκερ, ΆρντιτΦερίζι (Ardit Ferizi) διείσδυσε στο δίκτυο των ηλεκτρονικών υπολογιστών μιας αμερικανικής εταιρίας και απέσπασε τα ονόματα, τις ηλεκτρονικές διευθύνσεις, τους κωδικούς και άλλα ευαίσθητα προσωπικά δεδομένα, 1351 στρατιωτικών και άλλων κυβερνητικών υπαλλήλων τα οποία δημοσίευσε στην λίστα θανάτου αφού τα παρέδωσε στο ΙΚ. Σύμφωνα με δηλώσεις κυβερνητικού αξιωματούχου είναι η πρώτη φορά που συνδυάζεται η παραβίαση υπολογιστικών συστημάτων (hacking) με την τρομοκρατία, ένδειξη της εφαρμογής των μεθόδων κυβερνοπολέμου από μέλη τρομοκρατικών οργανώσεων [89]

Ακόμη οι επιθέσεις του Παρισιού σύμφωνα με ερευνητές στοιχεία οδηγούν στην εκτίμηση ότι κάποιοι από τους τρομοκράτες χρησιμοποιούσαν κρυπτογραφημένες εφαρμογές για να

[87] http://wwlp.com/2015/12/11/is-isis-beating-fbi-cia-with-their-encryption/
[88] http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/
[89] (Γρίβα, Cyber Caliphate - Η ηλεκτρονική μορφή τουΧαλιφάτου 2016).

καταφέρουν να συντονίσουν υπό κάλυψη τις επιθέσεις στο Παρίσι ,χωρίς αυτό να έχει επιβεβαιωθεί από τις Αρχές Ασφάλειας της Γαλλίας.[90]

Η πιθανή χρήσης της κρυπτογράφησης στις επιθέσεις του Παρισιού είναι ένας ακόμη λόγος για τον οποίο στις ΗΠΑ αλλά και στην Ευρωπαϊκή Ένωση έχουν αυξηθεί οι δημόσιες συζητήσεις για το κατά εύκολο είναι για τους ανακριτές και στις Αρχές Επιβολής του Νόμου το ζήτημα της κρυπτογράφησης των αρχείων ,δεδομένων και των επικοινωνιών.

Ο Διευθυντής του FBI James Comey δήλωσε λίγο μετά τις επιθέσεις έδρα σε Αστυνομικό Τμήμα της Νέας Υόρκης ότι *«η χρήση της κρυπτογράφησης είναι στο επίκεντρο των τρομοκρατικών οργανώσεων που δρουν στις μέρες μας."*

Πολλές εταιρείες τεχνολογίας αύξησαν τη χρήση της κρυπτογράφησης μετά τις πληροφορίες που δημοσιοποιήθηκαν από τον Edward Snowden ότι τα προγράμματα επιτήρησης των ΗΠΑ είχαν ευρεία πρόσβαση σε ιδιωτικές επικοινωνίες των Αμερικανών και ιδιωτών σε όλο τον κόσμο.

5.10 ΚΡΥΠΤΟΓΡΆΦΗΣΗ & BITCOIN

α.Γενικά περί του Bitcoin

Το Bitcoin είναι ένα ψηφιακό νόμισμα. Περιλαμβάνει χαρακτηριστικά τα οποία βασίζονται στην κρυπτογραφία και τις ψηφιακές υπογραφές, με στόχο την ασφάλεια του δικτύου του.

Οι μονάδες του νομίσματος ονομάζονται Bitcoins και χρησιμοποιούνται για την αποθήκευση και τον διαμοιρασμό αξίας μεταξύ των χρηστών. Όσοι είναι κάτοχοι μονάδων Bitcoin μπορούν να πραγματοποιούν αγοραπωλησίες αγαθών ή υπηρεσιών καθώς και μεταφορές χρημάτων, όπως ακριβώς θα τις έκαναν και με πραγματικά χρήματα. Για την εξυπηρέτηση του κοινού, υπάρχουν ανταλλακτήρια Bitcoin όπου κάποιος μπορεί να αγοράσει ή να πουλήσει Bitcoins ή ακόμα και να τα αλλάξει σε κάποια άλλη μορφή χρήματος.

Το Bitcoin αποτελεί ένα αποκεντρωμένο δίκτυο πληρωμών, ενώ το λογισμικό του είναι ανοικτού κώδικα (open source protocol), γεγονός που επιτρέπει στον καθένα να έχει πρόσβαση σε αυτό.

Αυτό συνεπάγεται την ελεύθερη αντιγραφή και ανάπτυξη λογισμικού βασισμένη στο υπάρχον πρότυπο. Βασικός στόχος του λογισμικού του Bitcoin είναι η θέσπιση και τήρηση

[90] http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/

κανόνων, όσον αφορά την παραγωγή και την διακίνηση των Bitcoins αλλά και την συγκέντρωση πληροφοριών για τις ήδη υπάρχουσες μονάδες με απώτερο σκοπό την παροχή εγγύησης καλής λειτουργίας, χωρίς την ύπαρξη κάποιου ενδιάμεσου φορέα.

Όπως αναφέρθηκε προηγουμένως το Bitcoin είναι ένα ψηφιακό νόμισμα και δεν υπάρχει κάποια αντιστοιχία σε φυσική μορφή. Οι χρήστες είναι εφοδιασμένοι με "κλειδιά", με τη βοήθεια των οποίων επικυρώνουν την αυθεντικότητα της συναλλαγής και επιτρέπουν την ολοκλήρωση της.

Τα "κλειδιά" είναι αποθηκευμένα στο ψηφιακό πορτοφόλι (digital wallet) του χρήστη και αποτελούν το μοναδικό μέσο για την επιτυχημένη εκτέλεση μιας συναλλαγής.

Ωστόσο, η ανταλλαγή μονάδων Bitcoin μεταξύ των χρηστών δεν αποτελεί τον μοναδικό τρόπο ώστε να αποκτήσει κάποιος Bitcoins. Για την παραγωγή νέων μονάδων Bitcoin, υπάρχει μια διαδικασία η οποία ονομάζεται εξόρυξη (mining) και η οποία προϋποθέτει την επίλυση ενός μαθηματικού προβλήματος.

Στη διαδικασία αυτή μπορεί να λάβει μέρος κάθε χρήστης, εφόσον έχει εγκατεστημένο στη συσκευή του το λογισμικό του Bitcoin. Σε ένα γενικό πλαίσιο, κάθε δέκα λεπτά κάποιος χρήστης λύνει ένα πρόβλημα και μπορεί στη συνέχεια να επικυρώσει συναλλαγές.

Η όλη διαδικασία έχει ως αποτέλεσμα, ο χρήστης να λαμβάνει ως ανταμοιβή νέες μονάδες Bitcoin.Επίσης, ιδιαίτερη εντύπωση προκαλεί η αυξανόμενη δυσκολία για την παραγωγή νέων μονάδων Bitcoins, ώστε να αποφευχθεί η υπερπροσφορά και να μπορεί το Bitcoin να διατηρεί την αξία του.

β. Πως λειτουργεί το Bitcoin

Για να εκκινήσει κανείς την ενασχόληση του με το Bitcoin[91], θα ήταν φρόνιμο να γνωρίζει την ερμηνεία και τον ρόλο κάποιων κομβικών εννοιών. Σε αυτό το σημείο, να αναφέρουμε ότι η ομαλή και εύρυθμη λειτουργία του δικτύου του Bitcoin βασίζεται στην κρυπτογραφία, καθώς είναι αυτή η οποία προσφέρει την ασφάλεια που απαιτούν οι χρήστες.

Ωστόσο, δεν είναι απαραίτητο να είναι κανείς γνώστης κρυπτογραφίας για να ασχοληθεί με το Bitcoin.

Αρχικά, ο χρήστης θα πρέπει να δημιουργήσει το ηλεκτρονικό του πορτοφόλι (Bitcoin wallet), όπου θα είναι αποθηκευμένα τα κεφάλαια του. Για να γίνει αντιληπτή η σημασία του ηλεκτρονικού πορτοφολιού, μπορούμε να το παρομοιάσουμε με ένα συμβατικό πορτοφόλι ή έναν αριθμό λογαριασμού.Για την ευκολία των χρηστών, υπάρχουν διάφοροι τύποι

[91] https://dspace.lib.uom.gr/bitstream/2159/19590/6/GlavinasDimitriosMsc2016.pdf

πορτοφολιών, όπως για παράδειγμα το πορτοφόλι για φορητές συσκευές (mobile wallet) ή το διαδικτυακό πορτοφόλι (online wallet).

Μέσω του πορτοφολιού του, ο χρήστης μπορεί να πραγματοποιεί πληρωμές ή αγορές αγαθών καθώς και να λαμβάνει μονάδες Bitcoin. Πέρα από τα κεφάλαια του χρήστη, το ηλεκτρονικό πορτοφόλι περιλαμβάνει και άλλες σημαντικές για τον χρήστη πληροφορίες όπως τα ψηφιακά κλειδιά (digitalkeys), τα οποία είναι απαραίτητα για την εκτέλεση των εκάστοτε συναλλαγών, καθώς και την διεύθυνση Bitcoin (Bitcoin address) του χρήστη.

Η μεταφορά μονάδων Bitcoin μεταξύ των χρηστών γίνεται μέσω συναλλαγών Ακολούθως, οι συναλλαγές γνωστοποιούνται και διαδίδονται στο δίκτυο του Bitcoin. Στη συνέχεια, εκτελείται η διαδικασία της επαλήθευσης των συναλλαγών, η οποία ονομάζεται εξόρυξη (mining) και οι επιτυχής συναλλαγές καταλήγουν σε ένα δημόσιο αρχείο συναλλαγών τύπου (blockchain).

γ. Φύλαξη Bitcoins εκτός-δικτύου

Ένα σοβαρό θέμα που καλούνται να αντιμετωπίσουν οι χρήστες Bitcoin είναι οι ασφαλής φύλαξη των κρυπτονομισμάτων τους. Είναι περισσότερο επιθυμητό τα Bitcoins να αποθηκεύονται εκτός υπολογιστή ώστε να μειωθεί ο κίνδυνος απώλειας από ιούς ή σφάλματα που μπορεί να προκύψουν τόσο στο υλικό όσο και στο λογισμικό του υπολογιστή. Προφανώς, οι χρήστες αναζητούν λύσεις ώστε να αποφύγουν την απώλεια των χρημάτων τους.

δ. Εταιρείες Φύλαξης Bitcoins

Μια εταιρεία η οποία ασχολείται με τη φύλαξη πολύτιμων λίθων είναι η GoldMoney Group, η οποία εδρεύει στη Βρετανία, αποφάσισε και προχώρησε στην ίδρυση του Natagio.

Το Natagio είναι μια θυγατρική της εταιρεία η οποία η οποία προσφέρει στους πελάτες της αποθήκευση των Bicoins τους εκτός δικτύου, με προσωπικό κλειδί διεύθυνσης.

Το κλειδί του κάθε χρήστη κρυπτογραφείται και αποθηκεύεται σε συσκευές αποθήκευσης οι οποίες τοποθετούνται σε ασφαλή χρηματοκιβώτια.

Η εταιρεία GoldMoney Group η οποία οφείλεται στην εμπιστοσύνη των πελατών της περνά σήμερα πλέον σε άλλα επίπεδα. Το μεγαλύτερο κέρδος σε κύρος της εταιρείας είναι η δυνατότητα αποθήκευσης των Bitcoins εκτός δικτύου, και φυσικά η πολυετείς φήμη της σε θέματα φύλαξης.

Η εταιρεία επιπλέον δίνει στους πελάτες της τη δυνατότητα να έχουν απομακρυσμένη πρόσβαση στα Bitcoins, με χρήση, φυσικά, two-factor authentication. Η χρήση της υπηρεσίας αυτής δεν έχει επιπλέον χρέωση.

Μια ακόμη εταιρεία η οποία δίνει τη δυνατότητα φύλαξης Bitcoin εκτός δικτύου είναι η Elliptic Vault.Τα Bitcoins αποθηκεύονται σε κρυπτογραφημένα αρχεία, τα οποία αποθηκεύονται σε διασφαλισμένες τοποθεσίες.

Το ιδιαίτερο και ταυτόχρονα αποκλειστικό της συγκεκριμένης υπηρεσίας είναι ότι η Lloyd's[92] του Λονδίνου εγγυάται την αξία των αποθηκευμένων Bitcoins. Προφανώς η παραπάνω υπηρεσία απαιτεί κάποια επιπλέον χρέωση, ανάλογα με το ποσό των Bitcoins τα οποία θέλει να διασφαλίσει.

ε. Bitcoin και παράνομες δραστηριότητες

Το Bitcoin αποτελεί ένα εικονικό νόμισμα, το οποίο σε μεγάλο βαθμό προσφέρει ανωνυμία στους χρήστες του χωρία να είναι «πανάκεια» μιας και έχουν καταγραφεί περιστατικά όπου κλονίστηκε η φήμη του[93].Το γεγονός αυτό αποτέλεσε σημαντικό παράγοντα ώστε να χρησιμοποιηθεί ως μέσο ανταλλαγής σε παράνομες δραστηριότητες, με απώτερο στόχο την ενίσχυση της διατήρησης της ανωνυμίας των δραστών αλλά και την δυνατότητα να μεταφερθούν χρηματικά ποσά που πολλές φορές είναι άγνωστος ο τρόπος απόκτησης τους.(νομιμοποίηση εσόδων από παράνομες δραστηριότητες)

στ. Bitcoin & σκοτεινό διαδίκτυο (Dark web)

Η εμπλοκή του Bitcoin στις αγοραπωλησίες της ιστοσελίδας "Silk Road", αποτελεί ίσως την πιο σημαντική από τις παράνομες δραστηριότητες στις οποίες έχει εμπλακεί .

Το "Silk Road"[94],αποτέλεσε μέρος του λεγομένου σκοτεινού διαδικτύου (dark web) και ενεπλάκη στην παράνομη διακίνηση ναρκωτικών ουσιών. Μέσω της τεχνολογίας που χρησιμοποιούνταν στην ιστοσελίδα, παρέχονταν ανωνυμία στους χρήστες της, γεγονός πολύ σημαντικό δεδομένου των δραστηριοτήτων που λάμβαναν χώρα σε αυτή.[95]

---

[92]Η Lloyds TSB Group plc είναι οικονομικό ίδρυμα με γραφείο που έχει έδρα το Λονδίνο, που όμως δραστηριοποιείται και στις ΗΠΑ, στην Ευρώπη, τη Μέση Ανατολή και την Ασία. Ιδρύθηκε το 1995 έπειτα από τη συγχώνευση των τραπεζών Lloyds Bank και Trustee Savings Bank (TSB). Η έδρα του τραπεζικού οργανισμού είναι στην οδό Γκρέσαμ, στον αριθμό 25 , στο Λονδίνο.Σήμερα είναι ο πέμπτος μεγαλύτερος τραπεζικός οργανισμός στο Ηνωμένο Βασίλειο. Δραστηριοποιείται στην Αγγλία και στην Ουαλία με το όνομα Lloyds TSB και στη Σκωτία ως Lloyds TSB Scotland. Οι δραστηριότητες του Lloyds TSB Group οργανώνονται σε τρία πεδία: τις συναλλαγές λιανικών πωλήσεων και υποθηκών, στις ασφάλειες και στις επενδύσεις και στις συναλλαγές χονδρικής πώλησης και σε εκείνες του εξωτερικού.

[93] http://startupper.gr/%CF%84%CE%BF-bitcoin

[94] Το "Silk Road", ξεκίνησε τη δράση του τον Φεβρουάριο του 2011, ενώ τον Οκτώβριο του 2013 πραγματοποιήθηκε για πρώτη φορά η παύση της λειτουργίας μετά από επιχείρηση της αμερικανικής υπηρεσίας F.B.I.. Ένα μήνα αργότερα η ιστοσελίδα επανήλθε σε λειτουργία αλλά ένα χρόνο αργότερα, το Νοέμβριο του 2014 έγινε και πάλι παύση των εργασιών της.

[95] {Wikipedia, Silk Road (marketplace) 2016}

Ωστόσο, παρά τα επίπεδα ασφαλείας που προσέφερε η εν λόγω ιστοσελίδα, για την ενίσχυση της διατήρησης της ανωνυμίας των χρηστών, μεγάλο μέρος των συναλλαγών γινόταν με την χρήση του εικονικού νομίσματος Bitcoin.

Κατά τις επιχειρήσεις που πραγματοποιήθηκαν για την παύση των λειτουργιών του "Silk Road" κατασχέθηκαν πάνω από 144 χιλιάδες Bitcoin, τα οποία κατά την περίοδο της κατάσχεσης αντιστοιχούσαν σε περισσότερα από 122 εκατομμύρια δολάρια. Το μεγαλύτερο μέρος των κατασχεθέντων Bitcoin ρευστοποιήθηκε μέσω δημοπρασιών που διενεργήθηκαν από της αμερικανικές υπηρεσίες. [96]

Σήμερα η εξάπλωση τις χρήσης του αλλά και της αξίας του συνεχίζεται .Η αξία του μάλιστα ανέβηκε κατά 33% το 2016 με αποκορύφωμα τη πρώτη Πέμπτη του Μαρτίου, 2017[97] όταν για πρώτη φορά από τη δημιουργία του, το Bitcoin ξεπέρασε την τιμή του χρυσού.Ένα Bitcoin έφτασε δηλαδή να ισοδυναμεί με 1.268 δολάρια, την ώρα που μια ουγκιά χρυσού αντιστοιχούσε σε 1.233 δολάρια.

Βέβαια οι αναλυτές επισημαίνουν πως είναι ίσως άστοχο να συγκρίνει κανείς τον χρυσό με το Bitcoin, μιας και η αξία του χρυσού προσδιορίζεται και με βάση πραγματικά δεδομένα(πχ το βάρος του), ενώ το ηλεκτρονικό νόμισμα είναι εντελώς θεωρητικό .

5.11 Κρυπτογραφηση & Block chain

Εάν προσπαθούσαμε να περιγράψουμε όσο πιο απλά την διαδικασία του Blockchain θα λέγαμε ότι πρόκειται για μια βάση δεδομένων όπου καταχωρούνται διάφορες συναλλαγές με μεγάλη ασφάλεια και απόλυτη πιστοποίηση, και αντίγραφά της μπορεί να βρίσκονται σε πολλά δικτυακά σημεία, τα οποία ενημερώνονται ταυτόχρονα και είναι προσβάσιμα απ' όλα τα μέρη.

Αν και χρησιμοποιείται παρόμοια τεχνολογία με αυτή του ψηφιακού νομίσματος bitcoin,είναι και πολλά περισσότερα από αυτό. Η διαδικασία του Block chain εφαρμόζει τις πρακτικές χρηματοδότησης στον χρηματοπιστωτικό τομέα, μειώνοντας κατά κύριο λόγο δραστικά τους φραγμούς στην είσοδο νεοφυών (startup) εταιρειών στην βιομηχανία.[98]

•Πώς λειτουργεί η τεχνολογία blockchain

Επί της ουσίας αναφέρεται σε μια σειρά καταχωρίσεων που αφορούν συναλλαγές, σε ένα δημόσιο κατάστιχο (ledger). Κάθε καινούρια ομάδα καταχωρήσεων -ένα «block»- συνδέεται

[96] (Coindesk, US Government to Sell 44,000 BTC in Final Silk Road Auction 2015)

[97]http://www.kathimerini.gr/898784/article/texnologia/diadiktyo/to-bitcoin-3eperase-se-a3ia-ton-xryso

[98] Η λεγόμενη FinTech (χρηματοοικονομική τεχνολογία).

με τα προηγούμενα, δημιουργώντας μία «αλυσίδα» καταχωρίσεων, δηλαδή ένα «blockchain».

Τα blocks αυτά συνδέονται μεταξύ τους. Προκύπτουν δε μέσα από μια διαδικασία που ονομάζουμε «proof of work», κατά την οποία επιτυγχάνεται η αλγοριθμική επίλυση ενός «δύσκολου» υπολογιστικού προβλήματος.

Κατ' αυτό τον τρόπο, το blockchain λειτουργεί ως ένα αποκεντρωμένο (decentralized) λογιστικό καθολικό, το οποίο είναι κοινό για όλους τους συμμετέχοντες , μιας και όλοι οι εμπλεκόμενοι αποθηκεύουν ένα αντίγραφό του κάτι που εξασφαλίζει την ασφάλεια και η διαφάνεια των συναλλαγών.

Η ειδοποιός διαφορά -αναφορικά με την προστασία- προκύπτει από το γεγονός ότι δεν είναι πλέον απαραίτητη η ύπαρξη μιας ενδιάμεσης «έμπιστης» αρχής **(πχ. μιας τράπεζας),** ενώ η εμπιστοσύνη των συναλλασσομένων μερών βασίζεται σε αλγοριθμική επιβεβαίωση.

- Τα οφέλη από τη χρήση της τεχνολογίας blockchain

Η δημόσια πρόσβαση στο blockchain διευκολύνει τη διαφάνεια στις συναλλαγές και τη διάχυση της πληροφορίας. Στο ίδιο πλαίσιο, διευκολύνεται η ελεγκτική διαδικασία με την εξάλειψη κάθε ενδεχομένου παραβάσεων, ακριβώς εξαιτίας της δημόσιας φύσης των δεδομένων.

Ταυτόχρονα, εκλείπει και η ανάγκη για ενδιάμεσα μέρη που αυξάνουν τα κόστη, αφού όλες οι πληροφορίες που αφορούν στη συναλλαγή βρίσκονται κρυπτογραφημένες μέσα στο blockchain.

Παράδειγμα:

Οι τράπεζες μπορούν να εξοικονομήσουν αρκετά δισεκατομμύρια κάθε χρόνο με την ελαχιστοποίηση του χρόνου διακανονισμού, των settlement fees και των cross-border πληρωμών.

Έκθεση της InnoVentures (ισπανικής τράπεζας Santander) αναφέρει ότι οι τεχνολογίες που βασίζονται στο blockchain, μπορούν να προσφέρουν μείωση στα κόστη τραπεζικών κοντά στα 15-20 δισ. δολάρια ετησίως μέχρι το 2020», χρήματα τα οποία θα συνεισφέρουν άμεσα στην κερδοφορία των χρηματοπιστωτικών ιδρυμάτων.

Ως μέτρο σύγκρισης, το προαναφερθέν ποσό -που αφορά μόνο στις υποδομές συναλλαγών θα αποτελεί μόνο το 30% του συνολικού παγκόσμιου τζίρου από τις απάτες που σχετίζονται με πιστωτικές κάρτες (credit card fraud) έως το 2020.

Ήδη, τράπεζες με διεθνή δραστηριότητα (Deutsche Bank, Santander, BNP Paribas) και πολλοί οργανισμοί από το χώρο των χρηματοπιστωτικών υπηρεσιών, όπως η Visa, η Citi και ο

NASDAQ, επιδιώκουν να υπερισχύσουν του ανταγωνισμού, συνεργώντας με πάροχους blockchain τεχνολογίας, ώστε να διασφαλίσουν τις υφιστάμενες υποδομές και να επωφεληθούν από τη μη-γραμμική καινοτομία που εισάγει η συγκεκριμένη τεχνολογία.

Στα παραπάνω υπάρχει και *ελληνική πρόταση από το blockpoint.io*

Το blockpoint.io με τη χρήση του blockpoint API, δίνει τη δυνατότητα σε χρηματοπιστωτικά ιδρύματα ή/και σε λιανεμπόρους να δημιουργήσουν τα δικά τους institutional blockchains, να στήσουν ψηφιακά νομίσματα για σχήματα πιστότητας καταναλωτή και να υλοποιήσουν blockchain mobile πορτοφόλια.

Από τα ανωτέρω συνάγεται ότι το Blockchain θα πρέπει να θεωρηθεί σαν μια από τις νέες τεχνολογίες (τα βιομετρικά συστήματα, το cloud computing, οι γνωσιακοί υπολογιστές, η μηχανική μάθηση, οι κβαντικοί υπολογιστές και η ρομποτική) οι οποίες θα αποτελέσουν τη βάση για την επόμενη γενιά χρηματοοικονομικών συναλλαγών.

5.12 Κρυπτογραφηση & Κυβερνοεπιθεσεις

Ως κυβερνοεπίθεση μπορούμε να θεωρήσουμε ένα περιστατικό μία δράση από άτομο η άτομα που δύναται να προκαλέσει ζημιά να επηρεάσει την εμπιστευτικότητα ,την ακεραιότητα ή την διαθεσιμότητα ενός αυτοματοποιημένου πληροφοριακού συστήματος.

Η ενέργεια αυτή κάτω υπό προϋποθέσεις μπορεί σύμφωνα με το διεθνές & εθνικό δίκαιο να συνιστά άδικη πράξη ή παράνομη ενώ υπό συγκεκριμένες συνθήκες μπορεί να εξισωθεί με ένοπλη επίθεση. Ο σκοπός αυτός διαφέρει κατά περίπτωση, γενικώς όμως ανήκει σε μια από τις παρακάτω κατηγορίες.[99]

- Εκμετάλλευση (exploitation)

Στην περίπτωση της εκμετάλλευσης βασικός στόχος του δράστη είναι η υποκλοπή πληροφοριών από το στόχο ή τις πηγές πληροφοριών που είναι συνδεδεμένες με αυτόν.

- Παραπλάνηση (deception)

Στην περίπτωση αυτή ο δράστης επιτρέπει στο στόχο του να εξακολουθεί να λειτουργεί, αλλά παραποιεί τις πληροφορίες τις οποίες αυτός συλλέγει ,αναλύει η παράγει, στοχεύοντας ουσιαστικά στο σύστημα λήψης αποφάσεων του αντιπάλου.

- Καταστροφή (destruction)

Στην περίπτωση της καταστροφής ο επιτιθέμενος, μέσω της χρήσης πληροφοριακών συστημάτων ,καθίστα αδύνατη τη λειτουργία του στόχου καταστρέφοντας τον ίδιο η τα

[99]Μαυρόπουλος ΠαναγίωτηςΥπγος ε.α «Η κυβερνοάμυνα στην Υπηρεσία της Εθνικής Στρατηγικής» Εθνικές Επάλξεις ,Νοέμβριος –Δεκέμβριος 2010

συστήματα υποστήριξης που είναι απαραίτητα για την λειτουργία του .Στην περίπτωση αυτήν πρωταρχικός στόχος δεν είναι τα πληροφοριακά συστήματα του αντιπάλου αλλά η κρίσιμη υποδομή του.

- Διακοπή λειτουργίας η εξουδετέρωση (Denial of service ή disruption)

Στην περίπτωση επιθέσεων διακοπής λειτουργίας (dos) η εξουδετέρωσης ο επιτιθέμενος δεν καταστρέφει το στόχο αλλά τον θέτει εκτός λειτουργίας η τον καθιστά αναξιόπιστο για κάποια χρονικά διαστήματα απαγορεύοντας στους νόμιμους χρήστες την εξυπηρέτηση τους.

Το 2016[100] πολλαπλασιάστηκαν οι κυβερνοεπιθέσεις σε σχέση με προηγούμενες χρονιές.

Οι επιθέσεις το 2016 πραγματοποιήθηκαν με τη χρήση «ζόμπι έξυπνων συσκευών» (συσκευές που εκμεταλλεύονται οι χάκερς για τις επιθέσεις τους), οι οποίες σε συνδυασμό δημιουργούν έναν «στρατό IoT συσκευών» ή αλλιώς ένα botnet (ένα δίκτυο υπολογιστών που ελέγχεται εξ αποστάσεως χωρίς τη γνώση ή την έγκριση του νόμιμου χρήστη ή την δυνατότητα πρόσβασης λόγω ισχυρής κρυπτογράφησης).

Όσες περισσότερες συσκευές «καταταγούν» σε αυτά τα botnets[101] τόσο μεγαλύτερος ο όγκος άχρηστων δεδομένων που μπορεί να διανεμηθεί.

Η μεγαλύτερη επίθεση που έλαβε χώρα το 2016 περιλάμβανε εκατοντάδες χιλιάδες συσκευές να χρησιμοποιούνται ταυτόχρονα στην επίθεση όπου «πρωταγωνίστησε» το Mirai botnet. [102]Το τρομακτικό γεγονός με τη συγκεκριμένη υπόθεση, ήταν ότι η επίθεση ήταν σχετικά απλή.

Όπως προκύπτει από τα ευρήματα έκθεσης[103], «το 2016, διαπιστώθηκαν επίσης ευρείας κλίμακας επιθέσεις από ένα ιό με την ονομασία ransomware[104] Όπως αποδεικνύεται από δύο μελέτες περιπτώσεων που έγιναν στο πλαίσιο της έκθεσης της Symantec, οι επιθέσεις αυτές χαρακτηρίζονται από υψηλό επίπεδο τεχνογνωσίας, ενώ χρησιμοποιούνται τεχνικές που βλέπουμε συχνότερα σε εκστρατείες κυβερνοκατασκοπείας.

Μία επιτυχημένη επίθεση σε έναν οργανισμό μπορεί ενδεχομένως να μολύνει χιλιάδες υπολογιστές, προκαλώντας μαζική λειτουργική ζημιά και σοβαρή βλάβη στα έσοδα, ή στη φήμη.

[100]http://www.tanea.gr/news/world/article/5392716/ayksanontai-oi-kybernoepitheseis-stis-epixeirhseis-symfwna-me-ekthesh-ths-symantec/
[101] https://en.wikipedia.org/wiki/Botnet
[102] https://en.wikipedia.org/wiki/Mirai_(malware)
[103] STR2016 Ransomware and Businesses της Symantec Corp. (NASDAQ: SYMC)
[104]http://www.huffingtonpost.gr/2016/10/12/eidiseis-koinonia-ransomware-upologistes-ellada-pws-na-antimetwpiseis_n_12453334.html

Οι επιθέσεις ransomware ενώ δρούσαν, μέχρι σήμερα, σε μεγάλο βαθμό, αδιακρίτως, πλέον δείχνουν ένα αυξανόμενο ενδιαφέρον για στοχευμένες επιθέσεις σε επιχειρήσεις κυβερνοκατασκοπείας. Επίσης παρατηρείται στροφή προς το crypto-ransomware συνεχίζεται. Οι νέες παραλλαγές που έχουν ανακαλυφθεί, μέχρι τώρα, μέσα στο 2016, φτάνει στο 80%.

5.13 Κρυπτογραφηση & VoIP

Τηλεφωνία VOIP[105]

Το Voice over IP ή VoIP106 ή τηλεφωνία μέσω διαδικτύου ή ΦεΔΠ δηλαδή "Φωνή επί διαδικτυακού πρωτοκόλλου", χαρακτηρίζει μια ομάδα πρωτοκόλλων/τεχνολογιών η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον και στην ουσία χωρίς κόστος.

Οι συνομιλίες αυτές παραδοσιακά γίνονταν αποκλειστικά μέσω PC που ήταν συνδεδεμένο με το Διαδίκτυο (Internet) και διέθετε μικρόφωνο, ακουστικά και το κατάλληλο λογισμικό. Η κλήση κατέληγε σε ένα άλλο, ανάλογα εξοπλισμένο,PC χωρίς να υπάρχει κάποια επιπλέον χρέωση, εκτός από αυτή της πρόσβασης στο Διαδίκτυο, αφού στη συγκεκριμένη επικοινωνία δεν μεσολαβεί κάποιος παραδοσιακός φορέας τηλεπικοινωνιών (π.χ. ΟΤΕ) παρά μόνο το Διαδίκτυο.

Η ορολογία "τηλέφωνο VoIP", κυριολεκτικά σημαίνει μια συσκευή που δεν συνδέεται στην πρίζα του ΟΤΕ, ή άλλου παρόχου, αλλά στο δίκτυο, σαν ηλεκτρονικός υπολογιστής. Μέσω δικτύου μπορεί να συνδεθεί τελικά σε ένα τηλεφωνικό κέντρο που υπάρχει στο χώρο που θα εγκατασταθεί, ή σε έναν πάροχο VoIP.

Το VoIP -σαν τεχνολογία- υπάρχει από τις Αρχές τις δεκαετίας του '90, αλλά άρχισε να γίνεται ιδιαίτερα διαδεδομένο στις Αρχές του 2000.

Με το ανάλογο λογισμικό (για παράδειγμα εφαρμογή (app), μια οποιουδήποτε Android, iOS ή άλλου λειτουργικού συστήματος συσκευή, μπορεί να χρησιμοποιηθεί σαν VOIP τηλέφωνο.

Mia Voip Τηλεφωνική συσκευή συνδέεται με μία Ethernet θύρα ή ασύρματα στο Gateway/router του ιντερνετ.

Μέσω μίας φιλικής προς τον χρήστη διεπαφής ρυθμίζονται οι παράμετροι που χρειάζονται για να λειτουργήσει ο SIP[107] λογαριασμός σας.

[105] https://el.wikipedia.org/wiki/VoIP

[107]Το SIP (Session Initiation Protocol = Πρωτόκολλο εκκίνησης συνόδου) είναι πρωτόκολλο επικοινωνίας μέσω δικτύων υπολογιστών, που χρησιμοποιείται κυρίως για την πραγματοποίηση, την

α. Τηλέφωνα usb VoIP

Πρόκειται για μια συσκευή USB που συνδέεται σε μία θύρα USB ενός υπολογιστή και χρησιμοποιώντας μια τηλεφωνική εφαρμογή SIP/ VoIP- συμπεριφέρεται όπως ακριβώς ένα τηλέφωνο. Ουσιαστικά δεν είναι τίποτα περισσότερο από ένα μικρόφωνο μαζί με ηχεία, αλλά αφού θυμίζει σε εμφάνιση περισσότερο ένα κανονικό τηλέφωνο, εμπνέει περισσότερο τον χρήστη να το χρησιμοποιήσει.

β. Τηλεφωνικά κέντρα VoIP

Το πρότυπο VoIP για τα τηλεφωνικά κέντρα είναι το SIP (Session Initiate Protocol) που έχει πολλές υλοποιήσεις από διάφορους κατασκευαστές τηλεφώνων και άλλων συσκευών. Χρησιμοποιείται και στα τηλεφωνικά κέντρα τύπου Asterisk μαζί με το IAX2 (Inter Asterisk Exchange).

Με τηλεφωνικά κέντρα (PBX - Private Box eXchange) που χρησιμοποιούν VoIP μπορούμε να διαχειριζόμαστε σε τοπικά δίκτυα τις κλήσεις μας και έτσι να έχουμε μικρότερο κόστος τηλεφωνημάτων ή και δωρεάν εφόσον τα κέντρα αυτά επικοινωνούν μεταξύ τους.

γ. Τηλέφωνα SIP λογισμικού

Ένα τηλέφωνο SIP θυμίζει και συμπεριφέρεται ακριβώς όπως ένα κανονικό ‘τηλέφωνο’. Ωστόσο, είναι συνδεδεμένο απευθείας με το δίκτυο δεδομένων. Τα τηλέφωνα αυτά έχουν ενσωματωμένη μια μίνι συσκευή hub[108], ώστε να μπορούν να μοιράζονται τη σύνδεση δικτύου με τον υπολογιστή. Έτσι, δεν χρειάζεστε ένα πρόσθετο σημείο δικτύου για το τηλέφωνο.

δ. Οι Συσκευές SIP

Είναι τηλέφωνο SIP είναι κατά βάση ένα πρόγραμμα το οποίο χρησιμοποιεί το μικρόφωνο και τα ηχεία του υπολογιστή σας, ή τα συνδεδεμένα ακουστικά, για να σας επιτρέψει να πραγματοποιείτε ή να λαμβάνετε κλήσεις. Παραδείγματα τηλεφώνων SIP είναι το JPhone της εταιρείας SJlabs, το Xten και άλλα.

Επιπλέον υπάρχει η δυνατότητα να χρησιμοποιηθεί ως VOIP και η υπάρχουσα αναλογική (σταθερή) συσκευή σας, προσθέτοντας έναν προσαρμογέα ATA. Ένας προσαρμογέας ATA[109]

τροποποίηση και τον τερματισμό τηλεφωνικών κλήσεων VoIP και επιτρέπει την μεταφορά πολυμεσικών πληροφοριών είτε μέσω του διαδικτύου, είτε μέσω ενός τοπικού δικτύου.

[108] https://el.wikipedia.org/wiki/Hub

[109]Προσαρμογείς Τηλεφώνου (ATA).Ένας προσαρμογέας αναλογικού τηλεφώνου (analog telephone adapter - ATA) είναι μια συσκευή που ενσωματώνει λειτουργίες VoIP, συνδέεται σε ένα τοπικό δίκτυο, μέσω μιας θύρας Ethernet, και επιτρέπει σε αναλογικά τηλέφωνα ή συσκευές fax, που συνδέονται σε αναλογικές θύρες (fxs), να πραγματοποιούν κλήσεις μέσω του IP δικτύου. Τα ATA είναι

σας επιτρέπει να συνδέσετε το βύσμα του δικτύου Ethernet στον προσαρμογέα και μετά να συνδέσετε σε αυτόν το τηλέφωνο.

Τα τηλέφωνα SIP είναι ίδια με τα τηλέφωνα VoIP ή τα λογισμικά τηλεφώνου. Είναι τηλέφωνα που σας επιτρέπουν να κάνετε τηλεφωνικές κλήσεις χρησιμοποιώντας την τεχνολογία VoIP.

Υπάρχουν δύο τύποι τηλεφώνων SIP.

- Ο πρώτος τύπος είναι το τηλέφωνο SIP με υλισμικό. Μοιάζει με την κοινή τηλεφωνική συσκευή, αλλά μπορεί να δεχτεί και να πραγματοποιήσει κλήσεις χρησιμοποιώντας το διαδίκτυο αντί για το παραδοσιακό σύστημα PSTN
- Τα τηλέφωνα SIP μπορεί επίσης να βασίζονται σε λογισμικό. Στην περίπτωση αυτή, επιτρέπουν να χρησιμοποιήσετε οποιονδήποτε υπολογιστή ως τηλέφωνο μέσω ακουστικών με μικρόφωνο ή/και κάρτας ήχου.
- Επίσης απαιτούν ευρυζωνική σύνδεση και σύνδεση με πάροχο υπηρεσιών VOIP ή διακομιστή SIP[110]

ε. Η λειτουργία του VoIP

Με τη VoIP τηλεφωνία, η φωνή μας μετατρέπεται σε πακέτα δεδομένων και μεταδίδεται μέσω του δημόσιου δικτύου Internet ή μέσα σε ένα εσωτερικό δίκτυο υπολογιστών. Τα πακέτα αυτά δεδομένων μετατρέπονται σε κανονικό τηλεφωνικό σήμα προτού τερματίσουν στο άλλο τηλεφωνικό άκρο (σταθερό, κινητό ή VoIP τηλεφωνική συσκευή).

Τα βασικά στοιχεία που αποτελούν την διαδικασία είναι η μετατροπή του αναλογικού σήματος φωνής σε ψηφιακή μορφή και η αποκωδικοποίηση/μετατροπή του σε πακέτα IP για μετάδοση μέσω Internet, η διαδικασία αυτή αναστρέφεται στο άκρο που λαμβάνει την κλήση.

Μπορεί να γίνει μετάδοση πάνω από μίας τηλεφωνικής κλήσης στην ίδια ευρυζωνική τηλεφωνική γραμμή. Με τον τρόπο αυτό, η φωνή μέσω IP μπορεί να διευκολύνει την προσθήκη τηλεφωνικών γραμμών στις επιχειρήσεις.

Οι ενοποιημένες επικοινωνίες είναι ασφαλείς με την τεχνολογία φωνής μέσω IP, αφού επιτρέπει την ενσωμάτωση άλλων υπηρεσιών που είναι διαθέσιμες στο διαδίκτυο, όπως η συνομιλία μέσω βίντεο, η ανταλλαγή μηνυμάτων κ.λπ.

Για τηλεφωνικά κέντρα, το Asterisk αποτελεί κάτι σαν μονόδρομο, καθώς και το SIPX.

μια οικονομική λύση που επιτρέπει σε υφιστάμενες τηλεφωνικές συσκευές να ενσωματωθούν σε ένα δίκτυο υπηρεσιών VoIP και να πραγματοποιούν τηλεφωνικές κλήσεις.

[110] https://www.3cx.com/global/gr/ip-pbx/android-iphone-voip/

στ. Πλεονεκτήματα των συνδέσεων VoIP

Το κύριο πλεονέκτημα είναι το κόστος: οι κλήσεις μέσω VoIP κοστίζουν φθηνότερα από τις κλήσεις μέσω παραδοσιακής τηλεφωνίας. Με κανονική χρήση του τηλεφώνου (δηλαδή αν δεν μιλάτε 15 ώρες ημερησίως), ακόμα και αν πληρώνετε κάθε κλήση VoIP που κάνετε, τελικά πληρώνετε λιγότερο από τα πακέτα των παρόχων παραδοσιακής τηλεφωνίας που σας δίνουν δωρεάν κλήσεις.

Συγκεντρωτικά, τα πλεονεκτήματα θα λέγαμε πως είναι τα εξής:

Μειωμένες χρεώσεις για κλήσεις εσωτερικού δεδομένου ότι δεν υφίσταται ο διαχωρισμός μεταξύ

Διαχείριση ενός μόνο δικτύου και για τη φωνητική επικοινωνία και για τη μεταφορά δεδομένων, αντί δύο δικτύων.

Μπορείτε πολύ εύκολα να προσθέσεις κι άλλους αριθμούς χωρίς καθυστερήσεις κι αλλαγές στο υλικό της υπάρχουσας υποδομής σας.

Έχει τη δυνατότητα να μεταφέρει το ήδη υπάρχον τηλεφωνικό μας νούμερο σε έναν VoIP πάροχο.

Πλήθος υπηρεσιών στον ίδιο VoIP αριθμό χωρίς παραπάνω χρεώσεις με εύκολη διαχείριση από το λογαριασμό σας

Διαχείριση του τηλεφωνικού σου νούμερου από όπου και αν βρίσκεστε αρκεί να έχετε πρόσβαση στο Internet.

η. Τρωτότητα/θέματα ασφάλειας VoIP

Το VoIP είναι ένα σύστημα που βασίζεται στο Διαδίκτυο, πράγμα που το καθιστά εκτεθειμένο σε μια σειρά τρωτών σημείων τα οποία δεν υπάρχουν κατά τη χρήση των παραδοσιακών τηλεφωνικών γραμμών.

Οι γραμμές VoIP είναι ευαίσθητες στους ίδιους τύπους επιθέσεων στους οποίους εκτείθενται η σύνδεση διαδικτύου και το e-mail σας και επομένως, πριν εγγραφείτε για υπηρεσία VoIP , πρέπει να γνωρίζετε αυτά τα πιθανά τρωτά σημεία.

Η VoIP τηλεφωνία είναι άμεσα εξαρτημένη από την σύνδεσή μας και από το modem router, αν υπάρξει απώλεια ηλεκτροδότησης τότε παύει και η λειτουργία της. Εκτός φυσικά κι αν υπάρχει κάποιο UPS ή γεννήτρια.Γι αυτό το λόγο πάντα προτείνεται να υπάρχει και μία γραμμή τηλεφώνου (PSTN) για πιθανές κλήσεις σε αριθμούς εκτάκτων αναγκών (199, 166 κλπ).

Ένα άλλο μειονέκτημα των VoIP συνδέσεων είναι η όχι και τόσο καλή ποιότητα της φωνής, η οποία εξαρτάται από την ποιότητα του δικτύου (και όχι από την ταχύτητα, όπως εσφαλμένα πιστεύουν πολλοί).

Επειδή δεν μπορείτε να ελέγξετε πόσα και ποια μηχανήματα μεσολαβούν μεταξύ του τηλεφώνου σας και των διακομιστών του παρόχου VoIP που συνδέεστε, είναι πιθανό δυσλειτουργίες ή καθυστερήσεις αυτών των μηχανημάτων να επηρεάσουν τη συνομιλία σας. Παρόμοιες καθυστερήσεις συμβαίνουν όταν συνδέεστε σε μια ιστοσελίδα και υπάρχει καθυστέρηση μέχρι να φορτωθεί.

Σύμφωνα με την εταιρεία ασφάλειας Norton, συνοψίζονται στα εξής:

- Αλληλογραφία spam/Η υπηρεσία VoIP υπόκειται στον δικό της τύπο ανεπιθύμητου μάρκετνιγκ, γνωστού ως «Spam over Internet Telephony» (Spam μέσω τηλεφωνίας Internet) ή SPIT.
- Διακοπές/ Επιθέσεις διαδικτύου, όπως οι ιοί και ιοί τύπου worm, μπορεί να διαταράξουν την υπηρεσία ή ακόμη και να θέσουν την υπηρεσία VoIP εκτός λειτουργίας.
- Ηλεκτρονικό «ψάρεμα» (phishing)[111] μέσω φωνής γνωστό και ως «vishing»[112], αυτό συμβαίνει όταν ένας επιτιθέμενος έλθει σε επαφή χρησιμοποιώντας τη γραμμή VoIP και επιχειρεί να σας ξεγελάσει ώστε να αποκαλύψετε πολύτιμα προσωπικά δεδομένα, όπως στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού.
- Απώλεια ιδιωτικού απορρήτου/Ενώ παρα πολλές εφαρμογές VoIP εξασφαλίζουν πλεόν μια ανώνυμη επικοινωνία λογω της κρυπτογράφησης που χρησιμοποιούν το μεγαλύτερο μέρος της κυκλοφορίας VoIP δεν είναι κρυπτογραφημένο, καθιστώντας εύκολο για τους εισβολείς να παρακολουθούν τελικά τις συνομιλίες VoIP .
- Παράνομη πρόσβαση./ Hacker μπορούν να αποκτήσουν πρόσβαση στη σύνδεση VoIP και να χρησιμοποιήσουν τη γραμμή σας για να πραγματοποιούν κλήσεις.

[111] Το **Phishing** είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο 'θύτης' υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία, και την άγνοια του χρήστη-'θύματος', με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί.Στην ελληνική αποκαλείται 'Ηλεκτρονικό Ψάρεμα', κι αυτό γιατί αγγλικός όρος δεν απέχει πολύ από αυτό. Ο όρος Phishing, που πρώτο χρησιμοποιήθηκε από τον χάκερ Khan C Smith και υιοθετήθηκε στη συνέχεια από όλη την κοινότητα των χάκερς, προέρχεται από το αγγλικό 'fishing' (ψάρεμα), καθώς η διαδικασία με την οποία ο θύτης παρουσιάζεται ως η αξιόπιστη οντότητα ώστε να προσελκύσει τους χρήστες, θυμίζει την διαδικασία του δολώματος στο ψάρεμα.

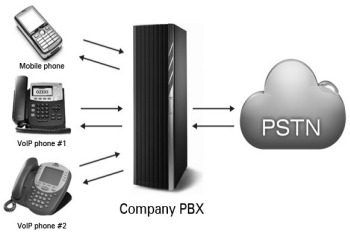
[112] https://www.techopedia.com/definition/4159/vishing

Σε ορισμένες περιπτώσεις, μπορεί ακόμη και να πουλήσουν τα στοιχεία της σύνδεσής σας στη μαύρη αγορά (dark net) η να υπάρχουν ήδη εκεί χωρίς να το γνωρίζει ο χρήστης

Μόλις βρεθούν εντός του οικιακού δικτύου σας, οι hacker μπορούν να ψάξουν για ευαίσθητα στοιχεία που ενδέχεται να έχουν αποθηκευθεί στον υπολογιστή.

Ο αναλυτής/ερευνητης τεχνολογίας των ip δικτύων Aditya Mishra, σε ένα συνέδριο αναφερόμενος στην τρομοκρατική επίθεση στο ξενοδοχείο στο Μουμπαι Ινδίας τον Νοέμβριο του 2008[113] δήλωσε ότι οι τρομοκράτες συνομιλούσαν με VoIP τεχνολογία .Συγκεκριμένα συνομίλησαν κάνοντας χρήση μιας εικονικής τηλεφωνικής σύνδεση μιας ιδιωτικής εταιρείας PBX [114](Private Branch eXchange) η οποία ονομαζόταν Callphonex, με έδρα το New Jersey των ΗΠΑ και η οποία σύνδεση παραχωρήθηκε από αυτήν την εταιρεία (με θυγατρική μια εταιρεία στο Βέλγιο) ενώ συνδέονταν με 5 τηλεφωνικούς αριθμούς DID (Direct Inward Dialers).

Οι κλήσεις υποτίθεται ότι έπρεπε να προέρχονται από την εικονική σύνδεση των ΗΠΑ, αλλά συνδέονταν μέσω της callphonex σε πέντε *εικονικές* / εσωτερικές DID τηλεφωνικές συνδέσεις Αυστρίας οι οποίες



[113]Ο αριθμός των νεκρών από τις συντονισμένες τρομοκρατικές επιθέσεις στη Βομβάη (Μουμπάι) έφτασε τους 160 και των τραυματιών στους 327. Στις επιχειρήσεις των ινδικών δυνάμεων ασφαλείας για την απελευθέρωση των ξένων υπηκόων στα δύο ξενοδοχεία, σκοτώθηκαν 9 ένοπλοι ισλαμιστές, 8 ξένοι υπήκοοι και 15 μέλη των δυνάμεων ασφαλείας. Ομάδα Ινδών κομάντος πραγματοποιεί επιχείρηση στο εβραϊκό κέντρο Νάριμαν Χάους της Βομβάης.

[114] **Ιδιωτικά τηλεφωνικά κέντρα PBX (Private Branch eXchange).**Τα ιδιωτικά PBX τηλεφωνικά κέντρα είναι συσκευές οι οποίες παρέχουν υπηρεσίες τηλεφωνίας σε μια εταιρεία. Με το PBX πραγματοποιούνται συνδέσεις μεταξύ των εσωτερικών τηλεφώνων μιας επιχείρησης, ενώ παράλληλα μπορούν να γίνουν συνδέσεις με το δημόσιο τηλεφωνικό δίκτυο(PSTN) μέσω εξωτερικών γραμμών. Επίσης μπορούμε να δημιουργήσουμε ένα εικονικό τηλεφωνικό κέντρο PBX μέσω ενος υπολογιστή, το οποίο έχει μηδαμινό κόστος και μας παρέχει όλες τις βασικές λειτουργίες ενος κανονικού PBX συστήματος. Το βασικότερο πλεονέκτημα που παρέχουν τα PBX τηλεφωνικά κέντρα, είναι η μείωση των τηλεπικοινωνιακών δαπανών διότι παρακάμπτουν την μεσολάβηση κάποιου πάροχου τηλεφωνικών υπηρεσιών, συνεπώς και την χρέωση προς αυτόν. Μερικά από τα βασικά χαρακτηριστικά που περιλαμβάνουν τα σύγχρονα PBX είναι: Αυτόματος διανομέας κλήσης (ACD),Προώθηση κλήσεων (call forwarding),Αναμονή κλήσεων (call waiting) ,Συνδιάσκεψη (conference),Auto attendant (σύνδεση εισερχόμενων κλήσεων απευθείας με κάποιο εσωτερικό χωρίς την μεσολάβηση χειριστή),Μουσική αναμονής κλήσεων (music on hold),Αυτόματος τηλεφωνητής (voice mail),IVR (interactive voice response).

αντιστοιχούσαν σε φυσιολογικούς αριθμούς κινητών τηλεφώνων.

Όπως ειπώθηκε η εικόνα που είχαν οι Αρχές ασφαλείας για τις συγκεκριμένες τηλ συνδέσεις ήταν παραπλανητική καθόσον οι τρομοκράτες (πακιστανικής καταγωγής) εμφανίζονταν ως άτομα με τηλ σύνδεση ΗΠΑ διενεργώντας κλήσεις σε αυστριακές τηλεφωνικές συνδέσεις.

θ.Μειονεκτήματα

Πρακτικά όμως θα λέγαμε πως η VOIP είναι τόσο ασφαλής, όσο και η παραδοσιακή τηλεφωνία,. απλά δίνει την δυνατότητα κρυπτογράφησης της συνομιλίας (αφού η συνομιλία μεταδίδεται ψηφιακά), κάτι που την κάνει υπό ορισμένες προϋποθέσεις ασφαλέστερη από την παραδοσιακή.

Έχουν παρουσιαστεί καθυστερήσεις στον ήχο ή ακόμα και παντελής αδυναμία σύνδεσης. Αυτό μπορεί να οφείλεται είτε στο πρόγραμμα (VoIP Client) το οποίο χρησιμοποιείτε στον τύπο του κινητού ή ακόμα και το δίκτυο 3G.

Τρόποι χρήσης του VoIP

Με software-softphone.:Με ένα σετ ακουστικών-μικροφώνου και μία τηλεφωνική γραμμή με σύνδεση στο διαδίκτυο κάθε υπολογιστής μπορεί να χρησιμοποιηθεί ως μία μονάδα VoIP . Στην πράξη όμως συστήματα softphone δεν θα πρέπει να χρησιμοποιούνται όταν υπάρχουν ανησυχίες για την ασφάλεια ή την ιδιωτικότητα. Ιοί, worms και άλλα κακόβουλα προγράμματα είναι μία πολύ συνηθισμένη απειλή σε υπολογιστές που συνδέονται στο διαδίκτυο, και πολλά απ’ αυτά είναι πολύ δύσκολο να εντοπιστούν και να αντιμετωπιστούν με επιτυχία.

Είναι γνωστό ότι μέσω των web browsers και των κενών ασφαλείας που έχουν, ένας χρήστης μπορεί να μολυνθεί ακόμα και όταν απλώς σερφάρει σε σελίδες του διαδικτύου χωρίς ο ίδιος να το αντιληφθεί.

Επίσης χρησιμοποιείται για την παραμετροποίηση του τηλεφώνου, ώστε να ρυθμιστούν δυνατότητες όπως η συνδιάσκεψη τριών ή περισσότερων ατόμων, η προώθηση κλήσεων κλπ. Ορισμένες από αυτές τις συσκευές είναι σχεδιασμένες με “βάση”, παρέχοντας την ίδια ευκολία με το συμβατικό ασύρματο τηλέφωνο.

Με συσκευή ATA (Analog telephone adapter)/ όπου μπορούν να συνδεθούν τα αναλογικά τηλέφωνα και να λειτουργήσουν σε δίκτυα VoIP.

Με φορητές μονάδες./ Οι ασύρματες μονάδες VoIP έχουν αρχίσει να γίνονται ιδιαίτερα δημοφιλείς, ειδικά από την στιγμή που πολλές εταιρίες έχουν ήδη εγκαταστήσει βάσεις δικτυακού εξοπλισμού 802.11.

Τα προϊόντα ασύρματου VoIP παρουσιάζουν όμως πρόσθετες προκλήσεις σε ότι αφορά την ασφάλεια.

Το WEP, χαρακτηριστικό ασφαλείας του 802.11b προσφέρει πολύ μικρή ή καθόλου προστασία.

Σήμερα περισσότεροι από 600 εκατομμύρια άνθρωποι σε όλο τον κόσμο χρησιμοποιούν τεχνολογίες VoIP για την επικοινωνία τους, είτε το ξέρουν (Skype) είτε δεν το ξέρουν (εναλλακτικοί πάροχοι) και λειτουργεί είτε μόνο για εξερχόμενες κλήσεις, είτε και για εισερχόμενες με χρήση κανονικού τηλεφωνικού αριθμού (DID).

5.14 Κρυπτογραφηση & Smartphone's

Τα έξυπνα κινητά, χρησιμοποιούνται σε κάθε είδους μορφής επικοινωνία όπως τηλεφωνικές κλήσεις, αποστολή μηνυμάτων, αποστολή e-mail, επικοινωνία με την οικογένεια και τους φίλους μέσα από διάφορα μέσα κοινωνικής δικτύωσης (Facebook, twitter) ή εφαρμογών άμεσων μηνυμάτων (viber, WhatsApp).

Η χρήση τους ,δεν περιορίζεται μόνο στην βασική επικοινωνία όπου ήδη κυκλοφορούν εκατοντάδες εφαρμογές επικοινωνίας με δυνατότητα κρυπτογράφησης[115] αλλά και στην εξυπηρέτηση άλλων αναγκών όπως το e-banking, αεροπορικές κρατήσεις εισιτηρίων, αγοραπωλησίες προϊόντων, γεωγραφική πλοήγηση περιοχών, παρακολούθηση ταινιών και πολλών άλλων δραστηριοτήτων.

Στις έξυπνες συσκευές ανήκουν εκτός από τα κινητά τηλέφωνα, τα tablet, PDAs, αναγνώστες eBook κ.α.[116]Τα κινητά που βασίζονται στο λειτουργικό σύστημα Android είναι υβριδικές συσκευές, ικανές να κάνουν τη δουλειά ενός τηλεφώνου και ενός υπολογιστή. Οι συσκευές αυτές καταχωρούν μεγάλο αριθμό δεδομένων (data) δηλαδή προσωπικά δεδομένα, από εικόνες, βίντεο, λογαριασμούς mail και σε social η ακόμα και λογαριασμούς πιστωτικών η άλλων καρτών.

Έτσι, στην περίπτωση των έξυπνων κινητών αναφερόμαστε σε τουλάχιστον δύο περιπτώσεις κρυπτογράφησης .

α. Δεδομένα συσκευής

Η διαδικασία είναι εύκολη και εφικτή από τον καθέναν.Η κρυπτογράφηση είναι ένας τρόπος ενίσχυσης της ασφάλειας ενός μηνύματος ή ενός αρχείου κατά τον οποίο τα περιεχόμενα

[115] https://www.whatsapp.com/security/?l=el

[116] Βλ Mislan, 2008

ανακατεύονται ώστε να μπορεί να τα διαβάσει μόνο κάποιος που έχει το κατάλληλο κλειδί κρυπτογράφησης για να τα βάλει στη σωστή σειρά.

Για παράδειγμα, εάν αγοράσατε κάτι μέσω Internet, τότε οι πληροφορίες για την συναλλαγή (όπως η διεύθυνση, ο αριθμός τηλεφώνου και ο αριθμός της πιστωτικής σας κάρτας) συνήθως κρυπτογραφούνται για την εξασφάλισή τους. την απόκρυψη εγκληματικής δραστηριότητας δεν είναι καινούρια.

Ήδη, από το 1970 οι αμερικανικές Αρχές (FBI) είχαν εκδώσει εγκυκλίους αναφορικά με το «σπάσιμο» κωδίκων για την απόκτηση ευρημάτων και την ανάσχεση εγκλημάτων τα οποία διέθεταν κρυπτογράφηση.Παρακάτω θα μελετήσουμε συνοπτικά την υπόθεση που το 2016 απασχόλησε τα ΜΜΕ για αρκετό χρονικό διάστημα και το αποτέλεσμα δεν είχε νικητή και ηττημένο.

Πριν ένα χρόνο γίναμε μάρτυρες της διένεξης και απροθυμίας μιας εκ των μεγαλύτερων επιχειρήσεων της Apple να συνεργαστεί με το FBI στο αίτημα του να «σπάσει» την κρυπτογράφηση της συσκευής,

Ο CEO της apple *Τιμ Κουκ, χαρακτήρισε,* «*Επικίνδυνη» και «άνευ προηγουμένου» την απόφαση δικαστηρίου κατόπιν αιτήματος του FBI για πρόσβαση στο κινητό τηλέφωνο του Σαγέντ Φαρούκ, του ζεύγους των δύο δραστών του μακελειού στο Σαν Μπερναρντίνο στις ΗΠΑ.*

Ειδικότερα, το FBI ήθελε η Apple[117] να προβεί σε αλλαγές στο SIF (System Information File), το λογισμικό που «τρέχει» στη συσκευή και να δημιουργήσει ένα νέο SIF για το iPhone του Φαρούκ[118] και να το περάσει σε αυτό, ανοίγοντας λειτουργίες τις οποίες κανονικά δεν έχουν τα iPhone.

Το Ομοσπονδιακό γραφείο ερευνών επιθυμούσε σύμφωνα με εκπροσώπους του να μην προβεί η συσκευή μόνη της σε αυτόματη διαγραφή, που υπαγορεύεται από κάποιες ρυθμίσεις ασφαλείας (μετά από 10 αποτυχημένες προσπάθειες εισαγωγής κωδικού).Ωστόσο, ο [119]Τιμ Κουκ, σε επιστολή του στους πελάτες της εταιρείας, δήλωσε πως

[117] Ο Syed Rizwan Farook και Tashfeen Malik) ήταν οι δύο δράστες της τρομοκρατικής επίθεσης στο Περιφερειακό Κέντρο στο San Bernardino ,της Καλιφόρνια, στις 2 Δεκεμβρίου, 2015. Σε αυτή την επίθεση, σκότωσαν 14 αμάχους και τραυμάτισαν 22 άτομα.

[118] https://en.wikipedia.org/wiki/Rizwan_Farook_and_Tashfeen_Malik

[119] Ο Timothy Donald 'Tim' Cook (γεννημένος 1 του Νοεμβρίου 1960) είναι ο τρέχων και ο έβδομος Διευθύνων Σύμβουλος της Apple (CEO), Ο Cook εντάχθηκε στην Apple τον Μάρτιο του 1998 ως αντιπρόεδρος στον τομέα των πωλήσεων ενώ στις 24 Αυγούστου, 2011 έγινε Διευθύνων Σύμβουλος για όλη την εταιρεία. Κατά τη διάρκεια της θητείας του έχει υποστηρίξει για την πολιτική αναμόρφωση των διεθνών και εγχώριων επιτήρηση, την ασφάλεια στον κυβερνοχώρο, την εταιρική

δεν θέλει να δημιουργήσει μία «back door», που θα επέτρεπε πρόσβαση στο τηλέφωνο με άλλον τρόπο πέραν αυτού του κωδικού ασφαλείας.

Κατά την Apple, μια «πίσω πόρτα» στο iPhone δεν θα έκανε απλά το τηλέφωνο του Φαρούκ προσβάσιμο στην αμερικανική κυβέρνηση, αλλά θα αποδυνάμωνε το iPhone γενικότερα, καθώς θα υπήρχε πάντα μια «κερκόπορτα» την οποία κακόβουλοι χρήστες θα μπορούσαν να βρουν και να χρησιμοποιήσουν.

Η όλη υπόθεση είχε προκαλέσει αίσθηση στον χώρο της τεχνολογίας, με φίρμες και φορείς του χώρου (μεταξύ των οποίων η Google, αλλά και το Information Security Council, που αντιπροσωπεύει την Google, το Facebook, τη Microsoft, τη Samsung, τη Blackberry και άλλες) να εκφράζουν τη στήριξή τους στην Apple, κάνοντας λόγο για επικίνδυνο προηγούμενο.

Παράλληλα, τη στήριξή του προς την εταιρεία εξέφρασε και ο Έντουαρντ Σνόουντεν, κάνοντας λόγο για έναν κόσμο όπου οι πολίτες βασίζονται στην Apple για να υπερασπιστεί τα δικαιώματά τους αντί για το FBI.

Στην άλλη πλευρά, υπέρ του FBI στην υπόθεση αυτή τάχθηκε ο Λευκός Οίκος, αλλά και ο υποψήφιος για το χρίσμα των Ρεπουμπλικάνων στις προεδρικές εκλογές του 2016,και νυν πρόεδρος των ΗΠΑ Ντόναλντ Τραμπ .

Σε δημοσίευμα των *New York Times* αναφέρεται ότι οι δικηγόροι της αμερικανικής κυβέρνησης και της Apple διαπραγματεύονταν επί δύο μήνες για τη συγκεκριμένη υπόθεση, μέχρι την κατάρρευση των συνομιλιών και την προσφυγή στο δικαστήριο.

Η εγκληματολογική ανάλυση των έξυπνων κινητών (forensic) είναι ένας νέος είδος συλλογής ψηφιακών πειστηρίων όπου οι πληροφορίες ανακτώνται από ένα κινητό τηλέφωνο. Στηρίζεται στην εξόρυξη δεδομένων[120]/στοιχείων από την εσωτερική μνήμη του τηλεφώνου όταν υπάρχει η δυνατότητα πρόσβασης στα δεδομένα με διαφορά εργαλεία.

Διατίθενται διάφορα εργαλεία λογισμικού για την ανάκτηση και ανάλυση δεδομένων από smartphone.

φορολόγηση τόσο σε εθνικό όσο και στο εξωτερικό, αμερικανικής κατασκευής, καθώς και τη διαφύλαξη του περιβάλλοντος.

[120]Εξόρυξη δεδομένων (ή ανακάλυψη γνώσης από βάσεις δεδομένων) είναι η εξεύρεση μιας (ενδιαφέρουσας, αυτονόητης, μη προφανούς και πιθανόν χρήσιμης) πληροφορίας ή προτύπων από μεγάλες βάσεις δεδομένων με χρήση αλγορίθμων ομαδοποίησης ή κατηγοριοποίησης και των αρχών της στατιστικής, της τεχνητής νοημοσύνης, της μηχανικής μάθησης και των συστημάτων βάσεων δεδομένων. Στόχος της εξόρυξης δεδομένων είναι η πληροφορία που θα εξαχθεί και τα πρότυπα που θα προκύψουν να έχουν δομή κατανοητή προς τον άνθρωπο έτσι ώστε να τον βοηθήσουν να πάρει τις κατάλληλες αποφάσεις.

Τα εργαλεία αυτά είναι ουσιαστικής σημασίας για να εξαχθούν ψηφιακές ενδείξεις οι οποίες μπορούν να χρησιμοποιηθούν αργότερα από τις Αρχές Επιβολής του Νόμου ως αποδείξεις σε νομικές υποθέσεις.

β. Εφαρμογές άμεσων μηνυμάτων (instant messages)

β1.Η εφαρμογή άμεσων μηνυμάτων WhatsApp.

Το WhatsApp Messenger είναι μία ιδιόκτητη εφαρμογή άμεσης ανταλλαγής μηνυμάτων για smartphones. Εκτός από την ανταλλαγή μηνυμάτων κειμένου, οι χρήστες μπορούν να στείλουν ο ένας στον άλλο εικόνες, βίντεο, ήχους και μηνύματα πολυμέσων.

Από τις 15 Αυγούστου του 2012, το προσωπικό της WhatsApp υποστηρίζει ότι τα μηνύματα είναι κρυπτογραφημένα στην "τελευταία έκδοση" του λογισμικού WhatsAppγια iOS και Android (μη συμπεριλαμβανομένων των BlackBerry, Windows Phone και Symbian), χωρίς να προσδιορίζει την εφαρμογή μεθόδου κρυπτογράφησης.

Το WhatsApp είναι μια από τις πιο δημοφιλής εφαρμογές για ανταλλαγή μηνυμάτων, κλήσεων μέσω internet και αρχείων όπως φωτογραφίες και video. [121]Ανάλογες εφαρμογές είναι το viber, αλλά και το skype και πολλές άλλες που υπόσχονται κρυπτογράφηση και διαφύλαξη προσωπικών δεδομένων.

Η κρυπτογράφηση των συνομιλιών στο WhatsApp έκανε αρχικά την εμφάνιση της το 2014 αλλά είχε κενά και δεν υποστήριζε όλες τις πλατφόρμες.

Πλέον όμως η εφαρμογή υποστηρίζει ολοκληρωμένη κρυπτογράφηση για όλα τα mobile λειτουργικά συστήματα, όπως Android, Windows, iOS και BlackBerry. Πιο ειδικά αυτό σημαίνει πως αν κάποιος χρήστης για παράδειγμα με iOS στείλε κάποιο μήνυμα σε κάποιον άλλο χρήστη με Android π.χ το μήνυμα θα είναι κρυπτογραφημένο και θα μπορεί να διαβαστεί μόνο από αυτούς τους 2 και κανέναν άλλο, σύμφωνα με την εταιρεία

Η κρυπτογράφηση ισχύει για όλες τις ενέργειες που είναι διαθέσιμες από την εφαρμογή του WhatsApp, όπως ανταλλαγή μηνυμάτων, αρχείων και κλήσεων.

Μία«αδυναμία» στο σύστημα ασφάλειας του WhatsApp μπορεί χρησιμοποιηθεί κατά τέτοιον τρόπο ώστε να επιτρέψει στο Facebook και σε άλλα μέσα κοινωνικής δικτύωσης να

[121] Η εταιρεία και κατά συνέπεια η εφαρμογή WhatsApp έχει εξαγοραστεί από το Facebook από το 2014 και αυτή τη στιγμή είναι η δεύτερη πιο δημοφιλής «social» εφαρμογή στο κόσμο.

παρακολουθούν τα κρυπτογραφημένα μηνύματα που έχουν αποσταλεί μέσω της συγκεκριμένης υπηρεσίας, σύμφωνα με Βρετανική εφημερίδα.[122]

Από την άλλη πλευρά το Facebook ισχυρίζεται ότι κανείς δεν μπορεί να υποκλέψει τα μηνύματα του WhatsApp, ούτε καν το προσωπικό της εταιρείας και ότι με αυτόν τον τρόπο διασφαλίζεται η ιδιωτική ζωή των χρηστών της εφαρμογής.

Όμως μία νέα έρευνα δείχνει ότι η εταιρεία θα μπορούσε στην πραγματικότητα να διαβάσει τα μηνύματα που αποστέλλονται μέσω του WhatsApp και ότι αυτό οφείλεται στον τρόπο με τον οποίο η εφαρμογή έχει θέσει σε λειτουργία το σύστημα κρυπτογράφησης end-to-end.

Η εφαρμογή WhatsApp χρησιμοποιεί κρυπτογράφηση end-to-end που υποτίθεται ότι παράγει μοναδικά κλειδιά ασφαλείας χρησιμοποιώντας το Signal protocol, που δημιουργήθηκε από την εταιρεία Open Whisper Systems.

Ωστόσο, η εφαρμογή παρέχει ακόμη και στους offline χρήστες κλειδιά κρυπτογράφησης. Ο αποστολέας από την άλλη μπορεί να στείλει εκ νέου κρυπτογραφημένα μηνύματα με νέα κλειδιά. Έτσι μπορεί να στείλει μηνύματα που δεν έχουν παραδοθεί και πάλι.

Ο παραλήπτης δεν έχει ενημερωθεί για την αλλαγή στην κρυπτογράφηση, ενώ ο αποστολέας ενημερώνεται μόνο εφόσον έχει επιλέξει να λαμβάνει προειδοποιήσεις για την κρυπτογράφηση και μόνο εφόσον τα μηνύματα έχουν σταλεί εκ νέου. Συγκεκριμένα αυτή η μέθοδος της «εκ νέου κρυπτογράφησης» δίνει πρόσβαση στο WhatsApp να διαβάζει τα μηνύματα του κάθε χρήστη.

Το κενό ασφαλείας ανακαλύφθηκε από τον Tobias Boelter, έναν κρυπτογράφο και ερευνητή ασφαλείας στο Πανεπιστήμιο της Καλιφόρνιας. Ο κ. Boelter ανέφερε στον Guardian: «Αν ζητηθεί από την WhatsApp από κάποια κυβερνητική υπηρεσία να αποκαλύψει τα μηνύματά της, μπορεί να παραχωρήσει πρόσβαση με την αλλαγή κλειδιών».

Ο Boelter φέρεται να ενημέρωσε το Facebook για το θέμα από τον Απρίλιο του 2016. Η εταιρεία είχε πει τότε στον κρυπτογράφο ότι το ζήτημα ήταν ήδη γνωστό και το χαρακτήρισε ως μία «αναμενόμενη συμπεριφορά»

Στην ίδια λογική και η πολιτική της εταιρείας Facebook, όταν εξαγόρασε το WhatsApp η οποία είχε υποσχεθεί ότι δεν πρόκειται να ξεκινήσει την συλλογή προσωπικών δεδομένων των χρηστών, ενώ τον Αύγουστο του 2016 έγινε γνωστό ότι άλλαξε η πολιτική στο WhatsApp το οποίο ξεκίνησε να μοιράζεται αριθμούς τηλεφώνου, ονόματα προφίλ, φωτογραφίες και άλλα δεδομένα με το Facebook.

[122]https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages

Τον Οκτώβριο του 2016 οι δικαστικές Αρχές της Βιρτζίνια κάλεσαν την εταιρεία Open Whispers Systems, που αναπτύσσει και την εφαρμογή App Signal, μια κρυπτογράφηση ανοιχτής πηγής (σ.σ.: δηλαδή όχι εμπορικά προστατευμένου λογισμικού) να παραδώσει στοιχεία (metadata) δύο χρηστών του συγκεκριμένου λογισμικού για μια έρευνα σε ομοσπονδιακό επίπεδο. Η εταιρεία, χρησιμοποιώντας την Αμερικανική Ένωση Υπεράσπισης Πολιτικών Ελευθεριών (ACLU), προσέφυγε στα δικαστήρια για να αντιμετωπίσει το αίτημα.

Σε αντίθεση με άλλα συστήματα, όπως το WhatsApp της Facebook, δεν κρατάει και δεν αποθηκεύει στοιχεία χρηστών του συστήματός της ούτε και λίστες εκείνων με τους οποίους ο χρήστης επικοινωνεί. Ετσι, τα στοιχεία που παρέδωσε στις Αρχές αφορούν το πότε επικοινώνησαν οι δύο συγκεκριμένοι χρήστες για τελευταία φορά.

Για τη συγκέντρωση τέτοιων στοιχείων στις ΗΠΑ[123] συνήθως χρειάζονται εντάλματα έρευνας υπογεγραμμένα από δικαστή (εισαγγελέα).Αλλά τα λεγόμενα δεδομένα επικοινωνίας (ποιος μιλάει με ποιον, πόσο συχνά, metadata) μπορούν να αποκτηθούν και με μια απλή κλήτευση για παροχή στοιχείων.

[123]Με τον σχετικό νόμο, που είχε ψηφισθεί το 1986, το Κογκρέσο έδινε τη δυνατότητα να κατάσχονται από τις Αρχές «ιστορικά αρχεία επικοινωνιών», αλλά εξαιρούσε τα στοιχεία επικοινωνίας των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Πάντως, ο Αλ Γκιντάρι επικεφαλής του πανεπιστημίου Στάφορντ «για την ιδιωτικότητα στο Διαδίκτυο και στην κοινωνία» υποστηρίζει ότι η νομοθεσία αυτή αναφέρεται σε έναν τεχνολογικό κόσμο πριν από τη συγχώνευση φωνής και δεδομένων.

ΚΕΦΑΛΑΙΟ 6^{Ο} : ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ

6.1 ΕΘΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Το ελληνικό δίκαιο περιέχει διάσπαρτα διαφορά νομοθετήματα που αφορούν το έγκλημα στον κυβερνοχώρο σε διαφορετικές χρονικές στιγμές για την κρυπτογράφηση δεδομένων και επικοινωνιών και την αξιοποίηση αυτών σε ποινικές υποθέσεις ,χωρίς όμως να προβλέπεται κάτι ειδικό στην κείμενη Νομοθεσία.

Τα νομοθετήματα είναι αποτέλεσμα μιας αντίδρασης του νομοθέτη σε συγκεκριμένα ζητήματα που προέκυψαν κατά καιρούς ή πρόκειται για ρυθμίσεις που συνοδεύουν/ολοκληρώνουν ένα συνολικό νομοθέτημα (π.χ. νομοθεσία για προστασία προσωπικών δεδομένων).

Ειδικότερα :

Στο Ελληνικό δίκαιο υπάρχουν διάφορα νομοθετήματα που αναφέρονται αναλογα με την ερμηνεία τους στο εγκλημα στο διαδίκτυο όπως λχ η ποινική προστασία του απορρήτου (άρθρο 370 ΠΚ) ,η ποινική προστασία των προσωπικών δεδομένων (Ν.2472/97) ,το Οικονομικό Ηλεκτρονικό Έγκλημα (άρθρο 386 ΠΚ),ή ανακριτική διείσδυση ΚΠΔ ,253^{Α} στο άρθρο 1 παρ α,δ, και έ τα οποία συνδέονται με την συλλογή πληροφοριών στο διαδίκτυο ,(παρ δ καταγραφή δραστηριότητας υποκειμένου με ειδικά τεχνικά μέσα πέρα της εικόνας και ήχου & τα οποία φυσικά προυποθέτουν την ύπαρξη σοβαρών ενδείξεων ότι έχει τελεσθεί αξιόποινη πράξη των παραγράφων 1 και 2 του άρθρου 187 ή αξιόποινη πράξη του άρθρου 187Α του Ποινικού Κώδικα), η απάτη με υπολογιστή, η Παράνομη πρόσβαση σε απόρρητα, η κατοχή και διακίνηση παιδικής πορνογραφίας σε ηλεκτρονικό υπολογιστή/στο Διαδίκτυο κ.α

Στο άρθρο 3 του ΠΔ. 47/2005 ΦΕΚ επίσης πιο συγκεκριμένα προβλέπονται τα είδη και οι μορφές επικοινωνίας, που υπόκεινται στην άρση του απορρήτου ανάμεσα σε αυτά και οι επικοινωνίες μέσω του διαδικτύου (Internet).

Ενώ στο άρθρο 4 παρ.1 εδάφιο ε περιγράφεται από τον Έλληνα Νομοθέτη μεταξύ άλλων και η τηλεφωνική επικοινωνία μέσω διαδικτύου (VoIP)[124].

[124]«Στο σύστημα τηλεφωνικής επικοινωνίας, μέσω διαδικτύου (VoIP) έχουν αναπτυχθεί εφαρμογές και λογισμικά επικοινωνίας κατά τα οποία, μόνο τα άτομα που επικοινωνούν μπορούν να διαβάσουν τα μηνύματα που ανταλλάσσονται έχοντας δυνατότητα διαγραφής και μη τήρησης της ιστορικότητας τους».

Ακόμη θα μπορούσαμε να αναφερθούμε στην παρ.5 εδαφ.7 του ΠΔ 47/2005 για ειδικές περιπτώσεις στις υπηρεσίες διαδικτύου προβλέπεται: «Κρυπτογράφηση με δημόσιο/ιδιωτικό κλειδί. Σε περίπτωση κρυπτογραφημένου περιεχομένου, που βασίζεται στις Αρχές του δημόσιου κλειδιού, η αρμόδια αρχή επιτρέπεται να έχει πρόσβαση στο ιδιωτικό (ή δημόσιο κατά περίπτωση) κλειδί του παραλήπτη (ή αποστολέα) ώστε να μπορεί να αποκτά πρόσβαση στο περιεχόμενο».

Αξιον λόγου είναι όμως ο πρόσφατος νόμος 4411/2016 όπου μεταξύ άλλων νομοθετημάτων περιλαμβάνει την ενσωμάτωση της οδηγίας 2013/40/Ε.Ε για τις επιθέσεις κατά συστημάτων πληροφοριών, ρυθμίζοντας έτσι ζητήματα για το έγκλημα στον κυβερνοχώρο και περιλαμβάνοντας ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής μεταξύ άλλων διατάξεων».

Πέραν της κύρωσης μίας ιδιαίτερα σημαντικής Σύμβασης (Βουδαπέστη 2001), έστω και με καθυστέρηση ετών, ο Νόμος 4411/2016 περιλαμβάνει, μεταξύ άλλων, μία σειρά τροποποιήσεων στον Ποινικό Κώδικα και τον Κώδικα Ποινικής Δικονομίας.

Οι κυριότερες αλλαγές εν τάχει είναι οι εξής;

- Στον Ποινικό κώδικα:

Μεταξύ των λοιπών άρθρων που τροποποιούνται ήταν και το άρθρο 370Γ του Ποινικού Κώδικα όπου αντικαθίσταται και προστίθεται από το άρθρο 370 δ ,περιλαμβάνοντας αλλαγές στις προϋποθέσεις για την άρση απορρήτου οι οποίες δεν θα αναλυθούν στην παρούσα εργασία. Επίσης προέβλεπε τα ακόλουθα:

- Στην Ποινική Δικονομία

Στο άρθρο 282 του Κώδικα Ποινικής Δικονομίας αναφορικά με την προσωρινή κράτηση και τους περιοριστικούς όρους.

- Στην Πολιτική Δικονομία

Με το άρθρο εικοστό τέταρτο του ν.4411/2016 τροποποιείται η παράγραφος 2 του άρθρου 147 του Κώδικα Πολιτικής Δικονομίας

- Άλλες διατάξεις:

Ο Νόμος 4411/2016 περιλαμβάνει μία σειρά διατάξεων αναφορικά με ζητήματα που αφορούν σε ποινικές διώξεις και εκτέλεση ποινών όπως:

Το άρθρο όγδοο προβλέπει την παραγραφή και μη άσκηση δίωξης.

Το άρθρο ένατο προβλέπει την παραγραφή και μη εκτέλεση ποινών υπό όρο

Το άρθρο δέκατο πέμπτο τροποποιεί τις διατάξεις του Νόμου 4322/2015.

6.2 Ευρωπαϊκη Νομοθεσια

6.2αΤο Συμβούλιο της Ευρώπης έχει ασχοληθεί με το έγκλημα στον Κυβερνοχώρο .Συγκεκριμένα στις 23 Νοεμβρίου 2001 στη Βουδαπέστη υπογράφηκε η πρώτη διεθνής σύμβαση «για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο» και «άνοιξε» προς υπογραφή και υπογράφτηκε από τριάντα χώρες τότε (από 26 μέλη του Ευρωπαϊκού Συμβουλίου και 4 χώρες μη μέλη Καναδάς, Ιαπωνία, Ν. Αφρική και ΗΠΑ που συμμετείχαν, όμως, στο σχεδιασμό της συνθήκης).Οπως αναφέραμε παραπάνω η σύμβαση κυρώθηκε με τον ν 4411/2016.

Το δεσμευτικό αυτό κείμενο μπορούν να υπογράψουν και άλλες χώρες που δεν είναι μέλη του Συμβουλίου της Ευρώπης, μετά από πρόσκληση της Επιτροπής Υπουργών. Μεταξύ των χωρών που υπόγραψαν την συνθήκη ήταν και η Ελλάδα.

Η συνθήκη τέθηκε σε ισχύ από τη στιγμή που επικυρώθηκε από πέντε κράτη, τουλάχιστον τρία από τα οποία είναι μέλη του Συμβουλίου της Ευρώπης.

Σκοποί της Σύμβασης που ενσωματώθηκε στην κείμενη νομοθεσία με νόμο είναι οι ακολουθοι:

- Η εναρμόνιση των εσωτερικών ποινικών νομοθεσιών των κρατών μελών στον τομέα της εγκληματικότητας στον Κυβερνοχώρο.
- Η θέσπιση εσωτερικών δικονομικών ποινικών διατάξεων, που είναι απαραίτητες για την έρευνα, δίωξη και εκδίκαση των εγκλημάτων του Κυβερνοχώρου, καθώς και των άλλων εγκλημάτων που διαπράττονται με τη χρήση συστημάτων ηλεκτρονικών υπολογιστών, αλλά και για τη συλλογή αποδεικτικών στοιχείων, που βρίσκονται σε ηλεκτρονική μορφή.
- Η θέσπιση γρήγορων και αποτελεσματικών κανόνων στον τομέα της διεθνούς συνεργασίας και επικοινωνίας.

Η Σύμβαση επίσης περιέχει:

α) Διατάξεις ουσιαστικού ποινικού δικαίου όπως :Αδικήματα που αφορούν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων που έχουν αποθηκευτεί σε υπολογιστικά συστήματα και των συστημάτων Η/Υ. (παράνομή πρόσβαση, η αθέμιτη παγίδευση υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.)

β) Διατάξεις ποινικού δικονομικού δικαίου.Οι διατάξεις ποινικού δικονομικού δικαίου αναφέρονται σε θέματα:Ταχείας διαφύλαξης δεδομένων αποθηκευμένων σε σύστημα

υπολογιστή), Ταχείας διαφύλαξης και γνωστοποίησης διακινουμένων δεδομένων ,Εντολής παροχής πληροφοριών (production order).Έρευνας και κατάσχεσης αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή (Search and Seizure of stored Computer data) κ.α

γ) Διατάξεις διεθνούς Δικαστικής συνεργασίας.

Οι διατάξεις διεθνούς δικαστικής συνεργασίας αναφέρονται:

Στην έκδοση, σε γενικές Αρχές σχετικές με την αμοιβαία συνδρομή παροχή αυθόρμητων πληροφοριών, κ.α στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών (Expedited preservation of stored computer data).

Ακόμη περιέχει ρυθμίσεις για την συνέργεια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων ενώ υπογραμμίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και τίθεται το ιδιαίτερα σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά.

6.2β. Επίσης η οδηγία 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για « την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου» ρυθμίζει θέματα που αφορούν την επεξεργασία των προσωπικών δεδομένων ενός υποκειμένου ,του εκτελών την επεξεργασία οσον αφορά την ασφαλεια των δεδομένων (προσπέλαση, κρυπτογράφηση κ.α).

6.3 Ηλεκτρονικα αποδεικτικα στοιχεια και κρυπτογραφηση[125],[126]

Όταν αναφερόμαστε σε ηλεκτρονικά αποδεικτικά στοιχεία νοούνται όλα τα ηλεκτρονικά δεδομένα που συνδέονται με άδικη πράξη και μπορεί να αποτελέσουν σημαντικά ευρήματα στο πλαίσιο της ποινικής διαδικασίας.

Από την άλλη και πέρα αυτών των δεδομένων που χρησιμοποιούνται για δικαστική χρήση στο πλαίσιο της απονομής δικαιοσύνης συλλέγονται, ανταλλάσσονται και επεξεργάζονται δεδομένα/πληροφορίες αποκλειστικά για τον σκοπό της καταπολέμησης ή πρόληψης τα οποία δεν αποτελούν ηλεκτρονικά αποδεικτικά στοιχεία.

[125] Βρυξέλλες, 23 Νοεμβρίου 2015 (OR. en) 14369/15 JAI 895 COPEN 319 DROIPEN 150 CYBER 110

[126] Βρυξέλλες, 23 Νοεμβρίου 2015 (OR. en) 14369/15 JAI 895 COPEN 319 DROIPEN 150 CYBER 110

Οι προληπτικές αυτές ενέργειες θεωρούνται ιδιαίτερα σημαντικές για τις έρευνες προς διακρίβωση εγκλημάτων, στις οποίες δύναται να προβούν οι Αρχές της Επιβολής του Νόμου στο πλαίσιο της διατήρησης της εσωτερικής ασφάλειας και την επιβολή της έννομης τάξης προλαμβάνοντας δράσεις του σοβαρού οργανωμένου εγκλήματος και της τρομοκρατίας.

Στην δεδομένη χρονική περίοδο βρίσκονται εν εξελίξει διεργασίες ,από το συμβούλιο της Ε.Ε σε συναφή ζητήματα, όπως στα ηλεκτρονικά αποδεικτικά στοιχεία, στη θέσπιση δηλαδή πλαισίου συνεργασίας με τους παρόχους υπηρεσιών δεδομένου του κρίσιμου ρόλου τους, καθώς και την εξασφάλιση της μέγιστης επιχειρησιακής ετοιμότητας του Δικαστικού σώματος που χειρίζεται υποθέσεις /έρευνες στον κυβερνοχώρο.

Στην περίπτωση αυτή και δεδομένου ότι ένας σημαντικός όγκος των ηλεκτρονικών δεδομένων/στοιχείων είναι κρυπτογραφημένος και η κρυπτογράφηση εμφανίζεται συχνά ή σχεδόν πάντοτε στο πλαίσιο των ποινικών ερευνών τα τελευταία χρόνια, θα πρέπει να υπάρξει διαχωρισμός ή έστω να ληφθούν υπόψη σε μια μελλοντική συνθήκη/απόφαση-πλαίσιο ,οι εν εξελίξει διεργασίες.

Εν τάχει είναι προτιμότερο ο διαχωρισμός στο παρόν στάδιο της διαδικασίας κρυπτογράφησης από τις εξειδικευμένες διεργασίες για τα ηλεκτρονικά αποδεικτικά στοιχεία, χωρίς να αποκλείεται η ανάγκη συντονισμού και η δυνατότητα μελλοντικής συγχώνευσης των δύο ενεργειών, γεγονός που έχει εκφραστεί και από τα Κ-Μ.

6.4 Χαρτογραφηση της καταστασης στο συνολο των χωρων της Ε.Ε

Το διεθνές και Ευρωπαϊκό περιβάλλον ασφάλειας, ,οι δίαυλοι επικοινωνίας στο διαδίκτυο ,τα διάφορα μέσα κοινωνικής δικτύωσης, η αυξανόμενη χρήση της κρυπτογράφησης από τους τρομοκράτες οι πρόσφατες επιθέσεις στην καρδιά της Ευρώπης δημιούργησαν την ανάγκη για εξεύρεση μίας λύσης στο ζήτημα της κρυπτογράφησης τόσο των δεδομένων όσο και των επικοινωνιών.

Κάτω από αυτές τις συνθήκες συνήλθε τον περασμένο Ιούλιο άτυπη σύνοδος των υπουργών Δικαιοσύνης αφιερωμένη στην κρυπτογράφηση.

Η συζήτηση αυτή είχε ως αποτέλεσμα να αναγνωριστούν τα προβλήματα που προκύπτουν σε αυτό το πλαίσιο και να εκχωρηθεί εντολή με σκοπό να δοθεί συνέχεια στη διερεύνηση του ζητήματος.

Η Προεδρία πριν από το άτυπό συμβούλιο υπουργών διακίνησε ερωτηματολόγιο έχοντας ως σκοπό την αξιολόγηση της τρέχουσας κατάστασης για την κρυπτογράφηση (υπό το πρίσμα

των αρχών Επιβολής του Νόμου των Κ-Μ) και πάνω στη βάση αυτή, να εξεταστούν πιθανές κατευθύνσεις.

Από τις συνεισφορές των Κ-Μ εξήχθησαν σημαντικά συμπεράσματα τα οποία συνίστανται εν τάχει στα ακόλουθα:

- Η κρυπτογράφηση εμφανίζεται συχνά ή σχεδόν πάντοτε στο πλαίσιο των ποινικών ερευνών.
- Υπάρχει σχετική εμπειρία τόσο σε κρυπτογραφημένα ηλεκτρονικά μηνύματα ή σε άλλες μορφές ηλεκτρονικής επικοινωνίας ή/και εμπορικών εφαρμογών όπως το Facebook, το Skype, το Whatsapp ή το Telegram) όσο και για την εκτός γραμμής κρυπτογράφηση.
- Ύποπτος ή κατηγορούμενος που έχει στην κατοχή του μια ψηφιακή συσκευή/ηλεκτρονικά δεδομένα έχει τη νομική υποχρέωση να παράσχει στις Αρχές Επιβολής του Νόμου τα κλειδιά/τους κωδικούς κρυπτογράφησης, στην πλειοψηφία των περιπτώσεων των χωρών της Ε.Ε βάσει του δικαιώματος της μη αυτοενοχοποίησης.
- Σε ορισμένα κράτη μέλη έχουν υιοθετηθεί διαφορετικές νομοθετικές προσεγγίσεις που παρέχουν τέτοιες δυνατότητες είτε σε σχέση με το ύποπτο ή/και τρίτους.
- Οι πάροχοι υπηρεσιών υποχρεούνται, σύμφωνα με το εθνικό δίκαιο, να παρέχουν στις Αρχές Επιβολής του Νόμου τα κλειδιά/τους κωδικούς κρυπτογράφησης και δεν απαιτείται σε κάθε περίπτωση Δικαστική εντολή.
- Η παρακολούθηση /ο έλεγχος των ροών κρυπτογραφημένων δεδομένων για την παροχή αποκρυπτογραφημένων δεδομένων είναι δυνατή/δυνατός υπό ορισμένες προϋποθέσεις που καθορίζονται από το εθνικό δίκαιο των χωρών αρκεί να υπάρχει προηγούμενη δικαστική εντολή·
- Η έλλειψη επαρκούς τεχνικής ικανότητας σε σχέση με αποτελεσματικές τεχνικές λύσεις για την αποκρυπτογράφηση και αντίστοιχο εξοπλισμό περιλαμβάνεται μεταξύ των πρώτων τριών προκλήσεων, ενώ ακολουθεί η έλλειψη επαρκών χρηματοδοτικών πόρων και η ανικανότητα προσωπικού.

Αυτό που συνάγεται και από τις απαντήσεις των ΚΜ είναι η ανάγκη λήψης ***μέτρων με πρακτικό προσανατολισμό*** δηλαδή στην πολιτικές και πρακτικές λύσεις παρά στη θέσπιση νομοθεσίας.

ΚΕΦΑΛΑΙΟ 7^{ο} : ΗΘΙΚΑ ΖΗΤΗΜΑΤΑ

7.1 Ιδιωτικότητα και Κρυπτογράφηση

Η χρήση των τεχνολογιών κρυπτογράφησης καθίσταται απαραίτητη, ιδιαίτερα ενόψει της ανάπτυξης της ασύρματης πρόσβασης. Χρειαζόμαστε μηχανισμούς απόδειξης της γνησιότητας ολοένα και πιο ποικίλους για να καλυφθούν οι διάφορες ανάγκες μας στο σύγχρονο περιβάλλον Σε ορισμένα περιβάλλοντα, μπορεί να χρειάζεται ή να επιθυμούμε να παραμείνουμε ανώνυμοι. Σε άλλα, μπορεί να χρειάζεται να μπορεί να αποδειχθεί κάποιο χαρακτηριστικό χωρίς να αποκαλυφθεί η ταυτότητά μας, όπως το γεγονός ότι κάποιος είναι ενήλικος, υπάλληλος ή πελάτης μιας συγκεκριμένης επιχείρησης. Σε άλλες καταστάσεις, τέλος, μπορεί να είναι απαραίτητο να αποδειχθεί η ταυτότητά μας.

Επίσης τα φίλτρα λογισμικού καθίστανται ολοένα και πιο πολύπλοκα, γεγονός που μας επιτρέπει να προστατευθούμε, εμείς οι ίδιοι ή τα πρόσωπα που τελούν υπό την επιμέλειά μας, από δεδομένα που δεν επιθυμούμε, όπως το ανεπιθύμητο περιεχόμενο, το ανεπιθύμητο ηλεκτρονικό ταχυδρομείο, κακόβουλα λογισμικά και άλλες μορφές επίθεσης.

Η εφαρμογή και διαχείριση τέτοιων αξιώσεων ασφαλείας στο Διαδίκτυο και τα νέα δίκτυα συνεπάγεται σημαντικά έξοδα για τη βιομηχανία και τους χρήστες είναι ως εκ τούτου σημαντικό να ενθαρρυνθεί η καινοτομία και η εμπορική χρήση της τεχνολογίας και των υπηρεσιών ασφαλείας.

Έτσι οι επιχειρήσεις, οι δημόσιοι φορείς ενθαρρύνονται να χρησιμοποιούν την κρυπτογράφηση για να προστατεύσουν τα οικεία δεδομένα και τις ηλεκτρονικές τους επικοινωνίες.

Χαρακτηριστικές είναι οι πολλές εμπορικά διαθέσιμες πλατφόρμες επικοινωνίας που πλέον κρυπτογραφούνται από προεπιλογή (όλο και περισσότερο συναντάται η *κρυπτογράφηση από άκρη σε άκρη*,{end to end}.

Δεν θα πρέπει παρόλα τα ανωτέρω να λησμονηθεί το γεγονός, ότι η χρήση κρυπτογράφησης στερεί τη δυνατότητα συγκέντρωσης αποδεικτικών στοιχείων ζωτικής σημασίας για τις Αρχές Επιβολής του Νόμου προς διακρίβωση εγκλημάτων.

7.2Δίκαιο Vs Τεχνολογία/ασφάλεια-Νέα ρυθμιστικά μοντέλα[127]

Τα τελευταία χρόνια οι ραγδαίοι ρυθμοί της τεχνολογικής καινοτομίας επιβάλλουν την αναθεώρηση ορισμένων παραδοχών ως προς τον τρόπο «παραγωγής» και επιβολής του δικαίου.

Οι αλλαγές θα μπορούσαν να κατηγοριοποιηθούν σε τρεις μεγάλες κατηγορίες/θεματικές

Σε αυτές που προβάλλουν την έννοια της αυτορρύθμισης, σε αυτές που επικεντρώνονται στην αντιμετώπιση των δικαιικών προβλημάτων μέσω των τεχνολογικών λύσεων και σε αυτές που εμμένουν στην αυτοδυναμία των πολιτειακών θεσμών ως προς την ικανότητα ρύθμισης στον Κυβερνοχώρο .

Ας δούμε εν συντομία αυτές τις παραδοχές:

α. Υποκατάσταση του δικαίου από την τεχνολογία

Καθόσον το δίκαιο είναι στατικό και η παραγωγή του αργή, ενώ από την άλλη η τεχνολογία και οι απειλές που σχετίζονται με αυτή (ψηφιακές απειλές) εξελίσσονται ραγδαία και δυναμικά, τίθεται όλο και πιο συχνά το απλοϊκό ερώτημα « .. είναι σε θέση το δίκαιο να παρακολουθεί έστω την εξέλιξη των νέων τεχνολογιών ..?».

Επιπλέον πρέπει να αναρωτηθούμε αν η αδυναμία αυτή οδηγεί σε μια αντιστροφή της σχέσης και η επίλυση των προβλημάτων μπορεί πλέον να επιτευχθεί μόνο μέσω της ενσωμάτωσης του δικαίου στην τεχνολογία ή –υπό άλλη προσέγγιση μέσω της εγκατάλειψης του δικαίου στην τεχνολογία.

Αυτό το μοντέλο πάσχει όμως από την απουσία αντιπροσωπευτικής συζήτησης σε σχέση με το περιεχόμενο και τη δημόσιας πολιτική και ίσως να στερείται δημοκρατικής νομιμοποίησης.

β. Τεχνολογική ουδετερότητα του δικαίου

Η ταχύτητα της τεχνολογίας σήμερα είναι τέτοια ώστε όταν υιοθετείται η νομοθεσία, έχει ήδη απολέσει την πραγματική ρυθμιστική της ικανότητα καθώς η υποκείμενη τεχνολογία έχει ήδη αλλάξει. Είναι αναπόφευκτο για τον νομοθέτη όταν νομοθετεί να έχει υπόψη του μια συγκεκριμένη τεχνολογία η ακριβέστερα ένα συγκεκριμένο επίπεδο ανάπτυξής της

[127] Βλ .Λιλιαν Μήτρου, το δίκαιο στην κοινωνία της πληροφορίας ,εκδόσεις Σάκκουλα,σελ. από 51 έως 62,/Νέα ρυθμιστικά μοντέλα για την ΚτΠ.

,καθώς και μια συγκεκριμένη και χρονικά προσδιορισμένη ,πολιτιστική κατανόηση της τεχνολογίας.128

Επομένως η τεχνολογική ουδετερότητα σε ένα περιβάλλον τεχνολογικής πολλαπλότητας μπορεί να επιτευχτεί μόνο με τη χρήση γενικών και αόριστων εννοιών.

Παραμένει αμφίβολο κατά πόσο μπορεί να υπάρξει κανονιστική συμμόρφωση δηλαδή οι γενικές και αόριστες έννοιες να ανταποκριθούν στις τεχνολογικές εξελίξεις.(Οι ρυθμίσεις της προστασίας προσωπικών δεδομένων είναι ένα χαρακτηριστικό παράδειγμα του φαινομένου ότι το παραδοσιακό πλέον νομικό οπλοστάσιο έχει φτάσει στα όριά του).

Αναλύοντας τα ανωτέρω διαφαίνεται ότι διαθέτουν το απαραίτητο θεσμικό οπλοστάσιο και την αντίστοιχη τεχνολογική εργαλειοθήκη για να εξασφαλίζουν –τουλάχιστον– το minimum των προστατευόμενων ατομικών δικαιωμάτων, σε ένα παγκοσμιοποιημένο περιβάλλον διαρκούς κινητικότητας πολιτών.

Τα ανωτέρω δύο μοντέλα που αναπτύχθηκαν έρχονται πιο κοντά σε αυτό που θα πρέπει να έχει κατά νου οποιαδήποτε συνθήκη απόφαση, υιοθετήσουν τα ΚΜ υπό το πρίσμα των αρχών Επιβολής του Νόμου.

[128] Βλ. H.Burkert,όπ.π.(σημ 30),σύμφωνα με τον οποίο το διαδίκτυο οδήγησε οριστικά στην εγκατάλειψη του μύθου του τεχνολογικά ουδέτερου δικαίου.

ΚΕΦΑΛΑΙΟ 8ο: ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΔΙΑΤΗΡΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΈΝΩΣΗ

Η διατήρηση της ασφάλειας στον κυβερνοχώρο αποτελεί μια από τις πρώτες γραμμές άμυνας κατά του εγκλήματος.

Προς χάριν της ανάγκης για διατήρηση της εσωτερικής ασφάλειας στον ευρύτερο γεωγραφικό χώρο της Ευρώπης, είναι αναγκαίο να διασφαλίζεται η ασφάλεια των ατόμων και της κοινωνίας με μια ισόρροπη λύση που θα διασφαλίζει και την προστασία των ανθρωπίνων δικαιωμάτων.

8.1 ΠΡΩΤΟΒΟΥΛΙΕΣ

Προς αυτή την κατεύθυνση υπήρξαν πρωτοβουλίες και εκτιμάται ότι θα αποτελέσουν τους πυλώνες για όποια μελλοντική ευρωπαϊκή νομοθετική πρωτοβουλία όπως:

- Η δράση της Europol και του ENISA[129] για τη συγκρότηση κοινής ομάδας για την ασφάλεια και την προστασία στο διαδίκτυο με σκοπό να συζητηθούν, να αξιολογηθούν και να αναζητηθούν λύσεις για την αντιμετώπιση της κατάχρησης της κρυπτογράφησης και της ανωνυμίας στο διαδίκτυο.
- Η εναρκτήρια συνεδρίασή του Ευρωπαϊκού δικαστικού δικτύου για το έγκλημα στον κυβερνοχώρο (EJCN) στις 24 Νοεμβρίου 2016.

8.2 ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

[129] Ο **ENISA** αποτελεί ένα Ευρωπαικό κέντρο εμπειρογνωμοσύνης σε θέματα Ασφάλειας των Δικτύων και Πληροφοριών και προωθεί τη συνεργασία ανάμεσα στο δημόσιο και ιδιωτικό τομέα.Ο ENISA δημιουργήθηκε για να ενδυναμώσει τη δυνατότητα της Ευρωπαϊκής Ένωσης, των Κρατών μελών της Ε.Ε. και της επαγγελματικής κοινότητας να αποφεύγει, να διευθύνει και να ανταποκρίνεται σε προβλήματα που αφορούν την ασφάλεια των δικτύων και πληροφοριών.Προκειμένου να διασφαλίσει την εκπλήρωση των στόχων του όπως περιγράφονται στον κανονισμό του, οι δράσεις του Οργανισμού επικεντρώνονται στα εξής:Την παροχή συμβουλών και βοήθειας στην Επιτροπή και τα Κράτη μέλη όσο αφορά την ασφάλεια των πληροφοριών και την ανάπτυξη του μεταξύ τους διαλόγου με τη βιομηχανία προκειμένου να διευθύνουν προβλήματα σχετικά με την ασφάλεια σε προϊόντα υλικού και λογισμικούΤη συλλογή και ανάλυση δεδομένων για τα περιστατικά ασφαλείας στην Ευρώπη και τους πιθανούς κινδύνουςΤην προώθηση μεθόδων διαχείρισης κρίσεων προκειμένου να ενδυναμώσει τη δυνατότητα να ελέγχουμε απειλές σε θέματα ασφαλείας των πληροφοριώνΤην αύξηση της γνώσης και της συνεργασίας ανάμεσα στους διαφορετικούς παράγοντες στο πεδίο της ασφάλειας των πληροφοριών, κυρίως με το αναπτύσσει δημόσιες και ιδιωτικές συνεργασίες με τη βιομηχανία σε αυτό τον τομέα.

α. Ορόσημο στην εφαρμογή της στρατηγικής της Ε.Ε για την ασφάλεια στον κυβερνοχώρο πρόκειται να αποτελέσει η έγκριση του σχεδίου οδηγίας για την ασφάλεια δικτύων και πληροφοριών.[130]

Η εν λόγω οδηγία θα βελτιώσει την συνεργασία μεταξύ των αρχών Επιβολής του Νόμου και θα διασφαλίσει την οικοδόμηση ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο από τις αρμόδιες Αρχές των κρατών μελών .Η διασφάλιση της πλήρους εφαρμογής της υφιστάμενης νομοθεσίας της Ε.Ε συνιστά το πρώτο βήμα για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.

β.Η αξιολόγηση και άλλων σχετικών οδηγιών από τα αρμόδια όργανα και φορείς της Ε.Ε Επιτροπή για τη λήψη περαιτέρω μέτρων πχ η απόφαση-πλαίσιο του 2001[131] για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών δεν αποτυπώνει πλέον τη σημερινή πραγματικότητα και τις νέες προκλήσεις, όπως είναι τα εικονικά νομίσματα (bitcoin) και οι πληρωμές κινητήςτηλεφωνίας.

γ.Η συνεργασία των Δικαστικών αρχών στο πλαίσιο της ισχύουσας νομοθεσίας ώστε να διασφαλίζεται ταχύτερη διασυνοριακή πρόσβαση σε στοιχεία και πληροφορίες, λαμβάνοντας υπόψη τις τρέχουσες και μελλοντικές τεχνολογικές εξελίξεις όπως είναι πχ το υπολογιστικό νέφος και το διαδίκτυο των πραγμάτων.

δ.Η κοινή διαπίστωση ότι η συλλογή ηλεκτρονικών αποδεικτικών στοιχείων σε πραγματικό χρόνο για ζητήματα όπως ιδιοκτήτες διευθύνσεων IP ή άλλα ηλεκτρονικά αποδεικτικά στοιχεία και η διασφάλιση της αποδοχής αυτών των στοιχείων ενώπιον των δικαστηρίων αποτελούν ουσιώδη ζητήματα .

ε.Η συναντίληψη ότι στο πλαίσιο της διατήρησης της ασφάλειας στο ευρωπαϊκό περιβάλλον πρέπει να δημιουργηθούν το ταχύτερο κανόνες οι οποίο θα επιτρέπουν στις Αρχές Επιβολής του Νόμου τη δυνατότητα να αποκτούν πρόσβαση στα στοιχεία που χρειάζονται για την προστασία της ιδιωτικής ζωής των πολιτών κατά της σοβαρής πολυεγκληματικότητας και της τρομοκρατίας στον ψηφιακό κόσμο.

στ. Η εξ ορισμού συνεργασία με τον ιδιωτικό τομέα για την κοινή προσπάθεια καταπολέμησης του ηλεκτρονικού εγκλήματος από συμπράξεις μεταξύ δημόσιου και ιδιωτικού τομέα.

Στο έγκλημα στον κυβερνοχώρο θα πρέπει να συνεργεί ολόκληρη η αλυσίδα: από το Ευρωπαϊκό κέντρο για εγκλήματα στον κυβερνοχώρο της Europol, τις ομάδες αντιμετώπισης

[130] COM(2013) 48 final της 7.2.2013.
[131] Απόφαση-πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου της 28.5.2001.

καταστάσεων αναγκών τεχνικών πληροφορικής των Κ-Μ που πλήγονται από την επίθεση έως τους παρόχους υπηρεσιών διαδικτύου οι οποίοι δύναται να προειδοποιούν τους τελικούς χρήστες των υπηρεσιών τους προσφέροντας παράλληλα την θεσμική τεχνική προστασία.

8.3 ΠΡΟΤΑΣΕΙΣ -ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΔΡΑΣΕΙΣ

Η σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, (2001) που έχουν επικυρώσει τα περισσότερα κράτη μέλη και προσφάτως και η χώρα μας παραμένει το διεθνές πρότυπο συνεργασίας.

Όλα τα κράτη μέλη θα πρέπει να κυρώσουν τη σύμβαση.

Ενδεικτικά αναφέρονται προτάσεις μερικές εκ των οποίων ανήκουν ήδη στο θεματολόγιο για την ασφάλεια της Ε.Ε στον κυβερνοχώρο:

- Συνέχιση κινήσεων όπως αυτής της ομάδας εργασίας Ε.Ε-ΗΠΑ για την ασφάλεια στον κυβερνοχώρο και της παγκόσμιας συμμαχίας κατά της σεξουαλικής εκμετάλλευσης παιδιών στο διαδίκτυο που αποδεικνύουν και την αξία της διεθνούς συνεργασίας.
- Επίτευξη των καταλλήλων εγγυήσεων από την Eurojust ώστε να διευκολύνεται η ανταλλαγή βέλτιστων πρακτικών και να εντοπίζονται οι προκλήσεις όσον αφορά τη συλλογή και τη χρήση ηλεκτρονικών αποδεικτικών στοιχείων σε έρευνες και διώξεις ηλεκτρονικών εγκλημάτων.
- Η διασφάλιση της δυνατότητας κάλυψης από τη δικαστική έρευνα, της δίωξης και της αμοιβαίας δικαστικής συνδρομής των σχετικών σύγχρονων μέσων επικοινωνίας όπως για παράδειγμα το πρωτόκολλο μεταφοράς φωνής μέσω του διαδικτύου (VoIP).
- Παγίωση εκπαιδεύσεων από την Europol, αναφορικά με τη μεθοδολογία και τους κινδύνους της χρήσης τεχνολογίας κρυπτογράφησης για εγκληματικούς σκοπούς.
- Περαιτέρω ανάπτυξη και εξέλιξη της Europol (ενίσχυση των τεχνικών δυνατοτήτων που ήδη διατίθενται στο πλαίσιο της Europol). Μεταξύ άλλων και ως Ευρωπαϊκού κέντρου εμπειρογνωμοσύνης για την κρυπτογράφηση σε αγαστή συνεργασία με τον ENISA.
- Πρωτοβουλίες από όλα τα κράτη μέλη του Ευρωπαϊκού Δικαστικού δικτύου (EJCN) για τα εγκλήματα στον κυβερνοχώρο και ατζέντα που θα περιλαμβάνει ανταλλαγή πληροφοριών, ορθών πρακτικών και εμπειρογνωμοσύνης, για τις πρακτικές και λειτουργικές πτυχές που σχετίζονται με την κρυπτογράφηση.

- Στενή συνεργασία και διαβουλεύσεις μεταξύ της Europol, της Eurojust και του δικτύου για την αντιμετώπιση των προκλήσεων που απορρέουν από την κρυπτογράφηση.
- Εμβάθυνση των πρακτικών/λειτουργικών πτυχών των σχετικών με την κρυπτογράφηση προγραμμάτων κατάρτισης για τις Αρχές Επιβολής του Νόμου που παρέχονται από οργανισμούς της Ε.Ε και αύξηση των προσπαθειών δημιουργίας ικανοτήτων με σκοπό να εξασφαλιστεί ότι οι αρμόδιοι χειριστές διαθέτουν κατάλληλες και επικαιροποιημένες γνώσεις και ικανότητες ώστε να λαμβάνουν και να επεξεργάζονται ηλεκτρονικά αποδεικτικά στοιχεία.

8.4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι ουσιαστικές δικονομικές διασφαλίσεις, οι εγγυήσεις της προστασίας δεδομένων και ο απόλυτος σεβασμός του κράτους δικαίου είναι η κοινή πλατφόρμα η οποία πρέπει να αποτελεί το θεμέλιο οποιασδήποτε πολιτικής πρωτοβουλίας και πρακτικής λύσης για την αποτελεσματικότερη διεξαγωγή της ποινικής διαδικασίας και την χρήση της κρυπτογράφησης εντός της Ε.Ε.

Σε αυτό το πλαίσιο απαιτείται συνεχής προσεκτική εξισορρόπηση των αναγκών των συστημάτων ποινικής δικαιοσύνης σε διαδικασίες που αφορούν το έγκλημα στο διαδίκτυο/κυβερνοχώρο υπό το πρίσμα των καθιερωμένων αρχών στον τομέα των θεμελιωδών δικαιωμάτων.

Η Ε.Ε μέσα από τα όργανα και τους φορείς άσκησης πολιτικής πρέπει να είναι σε θέση να αντιδρά σε απροσδόκητα γεγονότα, να εκμεταλλεύεται νέες ευκαιρίες, να προδιαγράφει τις μελλοντικές τάσεις ως προς τους κινδύνους για την ασφάλεια και να προσαρμόζεται σε αυτές.

Κρίνεται λοιπόν επιτακτική μια διεθνή προσέγγιση τόσο για τη διασφάλιση της διεθνούς επικοινωνίας μέσω εθνικών συνόρων όσο και για την ηλεκτρονική παρακολούθηση από τις Αρχές ασφάλειας τόσο των ΚΜ ξεχωριστά όσο και της εγκληματικής και τρομοκρατικής δραστηριότητας, που λαμβάνει χώρα εντός των Ευρωπαϊκών συνόρων.

Εν κατακλείδι τα κράτη μέλη της Ε.Ε καλούνται να συνεργαστούν και να δράσουν από κοινού ώστε τα αμέσως επόμενα χρόνια , να έχει δημιουργηθεί ένας αυθεντικός χώρος ενωσιακής ασφάλειας που θα αφορά τον φυσικό κόσμο(διασυνοριακή ασφάλεια, τρομοκρατία, μετανάστευση) και τον ψηφιακό (ψηφιακές απειλές/κυβερνοασφάλεια).

ΒΙΒΛΙΟΓΡΑΦΙΑ

1.Barney, C. (2004) Information Technology for Energy Managers.

2.Bethencourt J., L. W. (2007, July). Establishing dark net connections: an evaluation of usability and security. In Proceedings of the 3rd symposium on Usable privacy and security.

3.Biddle P., E. P. (2002). The darknet and the future of content protection In Digital Rights Management. Springer Berlin Heidelberg.

4.Brenner, B. (2015, February 12) Attackers using new ms sql reflection techniques. Retrieved from [132].

5.Couts, A. (2012, November 27). The next generation of hacker hunting will happen in real time. Retrieved from Digital trends.[133]

6.Generation-hacker-hunting- ip- viking- norse- corp/#:eMtKrGC36PnozA.

7.Cyberwars: Watching the US and China in Real-Time. (2014, July 2). Retrieved from stories by Williams:[134]

8.RAND _TR406 /Security Challenges to the Use and Deployment of Disruptive Technologies by https://www.rand.org/pubs/monographs/MG475.html The Global Technology Revolution 2020.

9.Executive Summary Bio /Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications.

10.[135]Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing.

11.Https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA 2016)Strategic, policy and tactical updates on the fight against cybercrime.

12.Dark Market “Η αόρατη απειλή πίσω από τη οθόνη του υπολογιστή’’ Misha Glenny 2011 εκδόσεις Πάπυρος, Eng “Dark market , Cyber thieves ,Cyber cops and You”

[132] https://blogs.akamai.com/2015/02/plxsert-warns-of-ms-sql-reflection- attacks.html
[133] http://www.digitaltrends.com/web/next-
[134] https://storiesbywilliams.com/tag/microsoft-ds/
[135] Neil Robinson, Maarten Botterman, Lorenzo Valeri, David S. Ortiz, Andreas Ligtvoet, Rebecca Shoob, Edward Nason

13. ΕΙΚΟΝΕΣ ΚΡΑΤΩΝ ΣΤΡΑΤΗΓΙΚΗ ΕΠΙΚΟΙΝΩΝΙΑ ΗΠΙΑ ΙΣΧΥΣ ΚΑΙ ΜΜΕ «Αθανάσιος Ν, ΣΑΜΑΡΑΣ 2012.
14. Τα Μέσα Επικοινωνίας στον 21ο αιώνα ,Στέλιος Παπαθανασίου 2010.
15. Δίκαιο της Πληροφορίας, Χαροκόπειο Πανεπιστήμιο, Προσωπικές σημειώσεις καθηγήτριας κ.Λίλιαν Μήτρου.
16. Το Δίκαιο στην Κοινωνία της πληροφορίας Λίλιαν Μήτρου 2002.
17. Το διαδίκτυο ως χώρος δημιουργίας, ελευθερίας και ασυδοσίας προστασία και προσβολή του ιδιωτικού βίου ,ιδιωτικότητα στο web 2.0 Λιλιαν Μήτρου
18. Συμβούλιο της Ευρωπαϊκής Ένωσης ST 7779/1/15 REV 1 /Εγχειρίδιο για την ανταλλαγή πληροφοριών στον τομέα της επιβολής του νόμου
19. Συμβούλιο της Ευρωπαϊκής Ένωσης 14260/16 EXT 1/ Εφαρμογή του προγράμματος για την καταπολέμηση της τρομοκρατίας που καθόρισε το Ευρωπαϊκό Συμβούλιο
20. Council of the European Union 6183/4/15 REV 4 Subject: EU Cybersecurity Strategy: Road map development
21. Συμβούλιο της Ευρωπαϊκής Ένωσης/ 13771/1/16 REV 1 Φόρουμ της ΕΕ για το Διαδίκτυο
22. Συμβούλιο της Ευρωπαϊκής Ένωσης 15119/16 8765/1/16 ASILE 13 EURODAC 3 ENFOPOL 132 CODEC 630
23. Συμβούλιο της Ευρωπαϊκής Ένωσης 14369/15 /Αποτελεσματικό σύστημα ποινικής δικαιοσύνης στην ψηφιακή εποχή
24. Συμβούλιο της Ευρωπαϊκής Ένωσης 7033/16/ Έκθεση προς το Ευρωπαϊκό Κοινοβούλιο και τα εθνικά κοινοβούλια σχετικά με τις εργασίες της μόνιμης επιτροπής επιχειρησιακής συνεργασίας σε θέματα εσωτερικής ασφάλειας
25. Θέματα ανακριτικής διείσδυσης στην επισύνδεση συνομιλιών που διεξάγονται μέσω ip/Πανεπιστήμιο Αιγαίου, Σάμος 2016
26. Τα μέσα επικοινωνίας στον 21ο αιώνα ,Στέλιος Παπαθανασόπουλος εκδόσεις καστανίωτη
27. Συμβούλιο της Ευρωπαϊκής Ένωσης 11660/13 Πολιτική ασφαλείας για τη διασφάλιση των πληροφοριών όσον αφορά την υποδομή δημόσιας κλείδας.

ΙΣΤΟΣΕΛΙΔΕΣ

1.https://www.enisa.europa.eu/news

2.https://www.fbi.gov/

3.https://www.europol.europa.eu/

4.https://www.interpol.int/

5.http://www.eulisa.europa.eu/Pages/default.aspx

6.https://www.easo.europa.eu/

7.https://edps.europa.eu/edps-homepage_en?lang=en

8.http://ec.europa.eu/eurostat/en/web/crime/overview

9.http://europa.eu/european-union/contact/social-networks_

10.http://wwlp.com/2015/12/11/is-isis-beating-fbi-cia-with-their-encryption/

11.http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/

12.http://edition.cnn.com/politics

13.http://www.eurojust.europa.eu/about/Pages/annual-reports.aspx

14.https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016