ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΨΥΧΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Το Ηλεκτρονικο–οικονομικό έγκλημα: Ερευνητική προσέγγιση

Περπέρης Απόστολος

Τριμελής Συμβουλευτική Επιτροπή

Μαγγανάς Αντώνης - Ομ. Καθηγητής, επιβλέπων
Λάζος Γρηγόρης - Καθηγητής, μέλος
Λαμπροπούλου Έφη - Καθηγήτρια, μέλος

ΑΘΗΝΑ, ΙΟΥΝΙΟΣ 2015

ΠΕΡΙΕΧΟΜΕΝΑ

Σύνοψη

Η παρούσα διατριβή έχει ως αντικείμενο τη διερεύνηση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος. Ειδικότερα μελετά ποιες είναι οι συγκεκριμένες περιστασιακές συνθήκες που συνθέτουν την καταλληλότητα της εγκληματικής ευκαιρίας, το *πού* και *πώς* του ηλεκτρονικο-οικονομικού εγκλήματος. Ποιός είναι ο τρόπος ζωής των ατόμων, ποιες συνηθισμένες δραστηριότητες τα εκθέτουν σε πιθανούς κινδύνους, τα καθιστούν κατάλληλους στόχους και μπορούν να δημιουργήσουν την κατάλληλη εγκληματική ευκαιρία για πιθανούς δράστες με κίνητρο να τα θυματοποιήσουν στον ψηφιακό χώρο.

Το απαραίτητο θεωρητικό υπόβαθρο παρέχεται από την ενοποιημένη προσέγγιση των θεωριών που εστιάζουν στο εγκληματικό γεγονός και τη διαμόρφωση των «εγκληματικών ευκαιριών», όπως οι θεωρίες της ορθολογικής επιλογής, των καθημερινών δραστηριοτήτων, των εγκληματικών προτύπων και της στρατηγικής περιστασιακής πρόληψης του εγκλήματος.

Βασικός στόχος της παρούσας διατριβής είναι η κατασκευή του προτύπου των εγκληματικών ευκαιριών του ηλεκτρονικο-οικονομικού εγκλήματος.

Η βασική μέθοδος που ακολουθεί είναι η συστηματική βιβλιογραφική ανασκόπηση.

Λέξεις –Κλειδιά:

Ηλεκτρονικό έγκλημα, Οικονομικό έγκλημα, εγκληματικό πρότυπο, εγκληματική ευκαιρία, ορθολογική επιλογή, καθημερινές δραστηριότητες, περιστασιακή πρόληψη εγκλήματος.

Abstract

The subject of this study is the pattern of the digital-economic crime. Particularly it examines the situational factors, the *where* and *how*, that form the suitability of the criminal opportunity for the digital-economic crime to occur. The person's routine activities on line, their digital life style, where they go and what they do on line could expose them as suitable targets to potential criminals with motive.

The proposed theoretical background is provided by an integrated approach of theories, such as Rational choice theory (RCT), Routine activities theory (RAT), Crime pattern theory and the "Situational crime prevention" strategy, that focus on the structure of the opportunities for crime.

The main *purpose* of this study is to define structure of the crime pattern of the electronic-economic crime.

The systematic literature review is chosen as the method to approach the subject of the study.

Key-words:

Electronic crime, economic crime, crime pattern, criminal opportunity, rational choice, routine activities, situational crime prevention.

Πρόλογος

Η παρούσα διατριβή έχει ως αντικείμενο τη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος από την οπτική των «εγκληματικών ευκαιριών» που ανήκουν στην προσέγγιση της περιβαλλοντικής εγκληματολογίας. Συγκεκριμένα, εφαρμόζοντας προσεγγίσεις, που μέχρι τώρα είχαν πεδίο εφαρμογής κυρίως στις παραδοσιακές μορφές εγκλήματος, εξετάζει τη σχέση ηλεκτρονικού - οικονομικού εγκλήματος, τη διαμόρφωση της εγκληματικής ευκαιρίας και του εγκληματικού προτύπου ενώ προτείνει και τρόπους πρόληψης και αντιμετώπισής του.

Οι λόγοι που οδήγησαν στην επιλογή του συγκεκριμένου θέματος είναι η επικαιρότητα των ζητημάτων της ηλεκτρονικής και οικονομικής εγκληματικότητας. Ερέθισμα αποτέλεσε και η κατά σειρά ετών ενασχόληση του γράφοντος με οικονομολογικού ενδιαφέροντος θέματα, κατά την επαγγελματική του απασχόληση στη δευτεροβάθμια εκπαίδευση. Το αρχικό ενδιαφέρον του, για τις απόψεις του Edwin Sutherland και την οικονομική εγκληματικότητα, προκάλεσε η ανάθεση από τον καθηγητή Ιάκωβο Φαρσεδάκη της πρώτης του εργασίας, σε προπτυχιακό ακόμα επίπεδο, με θέμα τον «Επαγγελματία κλέφτη».

Θα ήθελα να ευχαριστήσω, για την επιστημονική καθοδήγηση και συμβουλές που μου παρείχαν, τον επιβλέποντα καθηγητή κο Μαγγανά και τους καθηγητές-μέλη της τριμελούς επιτροπής, κα Λαμπροπούλου και κο Λάζο.

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

Οι κοινωνίες του 21ου αιώνα έχουν χαρακτηριστεί μεταβιομηχανικές ή «κοινωνίες της γνώσης και της πληροφορίας». Η γνώση και η πληροφορία καθίστανται βασικές παραγωγικές δυνάμεις προσδίδοντας νέο περιεχόμενο στις παραγωγικές και στις κοινωνικές σχέσεις. Συνιστούν μια νέα μορφή κεφαλαίου, το κοινωνικό, που τείνει να αντικαταστήσει την κυριαρχία του βιομηχανικού κεφαλαίου με τη δημιουργία νέων κοινωνικών ελίτ, των πανεπιστημίων, των κυβερνητικών θεσμών, αυτών που βασίζονται στην ανάπτυξη της γνώσης και της πληροφορίας. Οι βασικές κοινωνικές διακρίσεις και η δημιουργία πλούτου δεν θα βασίζονται πλέον στην ιδιοκτησία βιομηχανικού κεφαλαίου αλλά στην δυνατότητα πρόσβασης και αξιοποίησης της γνώσης και της πληροφορίας. Οι εξελίξεις αυτές οφείλονται στην πρόοδο της πληροφορικής και των επικοινωνιών που οδήγησαν στην εκμηχάνιση των υπηρεσιών και την σχετική αυτονόμησή τους από την βιομηχανική παραγωγή.[1] Η χρηματιστική αγορά, με τη δημιουργία των νέων και ανώνυμων ηλεκτρονικών μέσων πληρωμής, επιταχύνει την δυνατότητα μεταφοράς χρήματος παγκοσμίως. Οι παραδοσιακοί τρόποι πληρωμών σταδιακά περιορίζονται και αντικαθίστανται από τη νέα μορφή ηλεκτρονικών πληρωμών μέσω του διαδικτύου. Στην ίδια κατεύθυνση, κινούνται οι προσπάθειες προκειμένου να καταστούν οι συναλλαγές ασφαλέστερες. Η σύγκλιση των υπηρεσιών έχει τεράστιο αντίκτυπο σε πολλές γεωγραφικές περιοχές ταυτόχρονα.

Οι εφαρμογές της τεχνολογίας στην κοινωνία και στην οικονομία δεν ασκούν μόνο θετικές επιδράσεις διευκολύνοντας την παραγωγή προϊόντων και υπηρεσιών από επιχειρήσεις και οργανισμούς, τις τηλεπικοινωνίες με την ταχύτατη μετάδοση δεδομένων και υπηρεσιών, αλλά ταυτόχρονα έχουν διευρύνει τις δυνατότητες για τη διάπραξη εγκλημάτων. Οι εγκληματίες εκμεταλλεύονται ολοένα και περισσότερες ευκαιρίες με τη χρησιμοποίηση των νέων ψηφιακών εργαλείων και προϊόντων που είναι διαθέσιμα μέσω του διαδικτύου και της ψηφιακής τεχνολογίας. Το διαδίκτυο διευρύνει τις ευκαιρίες για κάθε είδος εγκληματία να διαπράξει εγκληματικές πράξεις, με μικρό σχετικά κίνδυνο, επειδή του δίνεται η δυνατότητα να καλύψει τα αποδεικτικά στοιχεία των πράξεων αυτών. Όσο εξελίσσεται η τεχνολογία, ο υπολογιστής χρησιμοποιείται περισσότερο, τόσο για διάπραξη καινοφανών μορφών εγκλήματος, που διαπράττονται μόνο μέσω του υπολογιστή και του διαδικτύου, όσο και παραδοσιακών που διαπράττονται όμως πλέον με σύγχρονο τρόπο. Ο διαδικτυακός κόσμος έχει πλέον καταστεί, με αυξανόμενο ρυθμό, ευάλωτος σε εγκληματικές δραστηριότητες και το 43% του κοινού χαρακτηρίζει το κυβερνο-έγκλημα ως πρόβλημα[2].

Η αξιολόγηση του κινδύνου από την Europol (Ευρωπαϊκή Αστυνομική Υπηρεσία) για το πληροφορικό και το οργανωμένο έγκλημα περιγράφει το σκηνικό σε αυτόν τον χώρο, δίνει μια επισκόπηση των πιο κοινών εγκλημάτων που διαπράττονται μέσω της χρήσης της τεχνολογίας και αποτιμά το κόστος τους. Το διαδίκτυο λοιπόν, μπορεί να χρησιμοποιηθεί για την οργάνωση και εκτέλεση εγκληματικών δραστηριοτήτων ως μέσο επικοινωνίας, ως μηχανισμός στρατολόγησης, ως χώρος αγοραπωλησίας ή παροχής χρηματοπιστωτικών υπηρεσιών. Στις παράνομες αυτές δραστηριότητες περιλαμβάνονται μεταξύ άλλων η μη εξουσιοδοτημένη πρόσβαση (hacking), η ηλεκτρονική απάτη, η απάτη με αντικείμενο κάρτες πληρωμής, η διανομή άσεμνου υλικού που αφορά παιδιά, η διακίνηση ναρκωτικών, η

[1] Βλ. σχετικά: McGrew Tony, Hall Stuart Held & David (Eds) (1992), σσ. 255- 256, Drucker Peter (1969), σ. 328 και Etzioni - Halevy (1999), σ. 49

[2] Burden Kit, & Creole Palmer (2003), σσ. 222-227

νομιμοποίηση εσόδων από παράνομες δραστηριότητες, η κυβερνο-τρομοκρατία, επιθέσεις σε κρίσιμα δίκτυα υποδομής πληροφοριών κλπ.

Οι ζημιές και οι βλάβες που προκαλούν στα θύματα είναι πολύ σοβαρές. Εκτός από την οικονομική ζημία που επιφέρουν στα άτομα και στις νόμιμες επιχειρήσεις, υπονομεύουν όχι μόνο την ασφάλεια καθαυτή, αλλά ακόμα και την αίσθηση ατομικής και οικονομικής ασφάλειας των Ευρωπαίων πολιτών, στερούν έσοδα από τις δημόσιες αρχές, αποφέρουν τεράστια κέρδη και αυξάνουν την ισχύ των εγκληματικών δικτύων.[3]

Ουσιαστικά ο κύριος στόχος για τους εγκληματίες είναι να κερδίσουν χρήματα. Το οικονομικό κέρδος είναι ο σημαντικότερος κινητήριος παράγοντας για τους εγκληματίες, ανεξάρτητα από τη δραστηριότητά τους. Το οικονομικό κέρδος είναι το πιο συνηθισμένο κίνητρο, ανεξάρτητα από τον πολιτισμό ή τα χαρακτηριστικά του παραβάτη. Για το λόγο αυτό, είναι σημαντικό να γίνει κατανοητό το πώς οι νέες τεχνολογίες μπορούν να χρησιμοποιηθούν παρανόμως για την απόκτηση οικονομικού κέρδους. Ακόμη και στην περίπτωση παραγωγής και διάδοσης εικόνων κακοποίησης παιδιών στο Διαδίκτυο, το οικονομικό κέρδος είναι συχνά ο τελικός στόχος του εγκληματία. Το ηλεκτρονικό έγκλημα είναι πιο κερδοφόρο από πολλά άλλα εγκλήματα, εκμεταλλευόμενο τις ευκαιρίες σε παγκόσμια κλίμακα και με χαμηλό κόστος τέλεσης.

Οι νέες μορφές οργανωμένου εγκλήματος αυξάνονται ειδικά με τη διεύρυνση της Ευρωπαϊκής Ένωσης (ΕΕ). Τα νέα ζητήματα γίνονται επείγοντα επειδή η ανάπτυξη τεχνολογίας είναι γρηγορότερη από τους νόμους και τους κανονισμούς. Τα ζητήματα όπως η προστασία των δεδομένων, η φύλαξη των δεδομένων και η προστασία της ιδιωτικότητας συζητούνται ιδιαίτερα σε κάθε χώρα. Οι διεθνείς οργανισμοί προσπαθούν να τα αντιμετωπίσουν σε πολιτικό επίπεδο προκειμένου να βρεθεί μια λύση.

Η ψηφιακή τεχνολογία τις τελευταίες δεκαετίες έχει επιδράσει στην αλλαγή του τρόπου ζωής εκατομμυρίων ανθρώπων ανά τον κόσμο, μεταφέροντας πολλές από τις καθημερινές συνήθειές τους, από το φυσικό στο ψηφιακό περιβάλλον. Ο κυβερνοχώρος ή ψηφιακό περιβάλλον συνιστά το κοινό δίκτυο, τον κοινό τόπο στον οποίο οι δράστες με κίνητρο μπορούν να αναζητούν και να συναντούν κατάλληλους (ευάλωτους) στόχους-θύματα. Ο εκμηδενισμός των αποστάσεων άλλωστε που προσφέρει το διαδίκτυο αυξάνει την εγγύτητα και προσβασιμότητα των δραστών σε πιθανούς στόχους και καθιστά τους τελευταίους απεριόριστους σε αριθμό.

Οι διαδικτυακές επικοινωνίες και δραστηριότητες αφορούν όλες τις εκφάνσεις της προσωπικής και της κοινωνικής ζωής των ατόμων και εντάσσονται στον κυρίαρχο τρόπο ζωής. Οι παραπάνω επιδράσεις δεν αφορούν μόνο τις νόμιμες δραστηριότητες στον ψηφιακό χώρο αλλά και τις παράνομες.

Συνακόλουθα οι σύγχρονες εγκληματολογικές προσεγγίσεις θα πρέπει να προσαρμόζουν και να αναπροσαρμόζουν τα θεωρητικά πλαίσια των μελετών τους ανάλογα με τις αλλαγές που σημειώνονται στις ευκαιριακές δομές των ψηφιακών εγκλημάτων. Για το λόγο αυτό διατυπώνονται νέες θεωρητικές προσεγγίσεις ή επεκτείνονται οι ήδη υπάρχουσες.

Μέχρι τώρα οι σχετικές μελέτες, έχουν ως αντικείμενο, άλλες το έγκλημα πληροφορικής - ή κάποια από τις μορφές του, και άλλες το οικονομικό ή το έγκλημα του λευκού περιλαιμίου. Ελάχιστες από αυτές ασχολήθηκαν με την σχέση ηλεκτρονικού και οικονομικού εγκλήματος ή

3 Βλ. Ευρωπαϊκή Επιτροπή, Βρυξέλλες (2013)

όσες ασχολήθηκαν εφήρμοσαν αποσπασματικά κάποια από τις υπάρχουσες εγκληματολογικές θεωρίες. Όπως αναφέρει ο Moitra το πλήθος των μέχρι τώρα ερευνών στερούνται θεωρητικού πλαισίου ή εστιάζουν μονόπλευρα στο ηλεκτρονικό έγκλημα εναντίον των επιχειρήσεων, ενώ οι σχετικές έρευνες για την ατομική θυματοποίηση είναι περιορισμένες.[4] Η γνώση που μας παρέχει η υπάρχουσα βιβλιογραφία είναι σχετικά περιορισμένη και όσον αφορά τους παράγοντες που επιδρούν στη θυματοποίηση, όπως στις περιπτώσεις που ο υπολογιστής είναι ο στόχος, όπως ο hacking και η προσβολή από κακόβουλα προγράμματα.[5]

Στο επίπεδο ερευνών η υπάρχουσα βιβλιογραφία και οι σχετικές (θυματολογικές) έρευνες είναι ακόμα ολιγάριθμες, βασίζονται περισσότερο σε μικρά και πιθανόν μη αντιπροσωπευτικά δείγματα φοιτητών[6] και λιγότερο σε ευρύτερα δείγματα του γενικού πληθυσμού, έχουν χαμηλούς δείκτες ανταπόκρισης και συμμετοχής.[7] Άλλωστε, οι θυματολογικές έρευνες αντιμετωπίζουν τον περιορισμό ότι τα θύματα δεν αποτελούν αντιπροσωπευτικά δείγματα του γενικού πληθυσμού.[8] Παρά τους περιορισμούς τους όμως, κάποιες από αυτές τις μελέτες μας παρέχουν τα κατάλληλα θεωρητικά και μεθοδολογικά εργαλεία για την κατανόηση του τρόπου με τον οποίο, οι συνηθισμένες δραστηριότητες ρουτίνας, ο τρόπος ζωής μπορούν να δημιουργήσουν την κατάλληλη εγκληματική ευκαιρία για πιθανούς δράστες με κίνητρο και να επιδράσουν στη θυματοποίηση των ατόμων.[9]

Το ζήτημα, που θέτουν αρκετοί ερευνητές, είναι η αναγκαιότητα διατύπωσης γενικών θεωριών και εφαρμογής μιας διαφορετικής προσέγγισης κατά την έρευνα των οικονομικών εγκλημάτων όπου η ψηφιακή τεχνολογία αποτελεί το στόχο αλλά και το μέσο.[10]

Δράστης και θύμα, μέχρι τις αρχές της δεκαετίας του ’70, αποτελούσαν δυο ξεχωριστά αντικείμενα εγκληματολογικής ανάλυσης. Αντιμετωπίζονταν, κυρίως από τις -θετικιστικής προέλευσης- θεωρίες, ως δυο διαφορετικοί πληθυσμοί χωρίς τίποτα κοινό μεταξύ τους. Οι ανάλογες μελέτες θεωρούσαν τους δράστες ως «παθολογικούς», πνευματικά ασταθείς, με «διαφορετικό» τρόπο σκέψης. Όπως έδειξαν όμως νεότερες μελέτες, τα περισσότερα εγκλήματα διαπράττονται από άτομα απόλυτα «φυσιολογικά» που δρουν ευκαιριακά και (ορθο)λογικά με συνηθισμένα κίνητρα και ανάγκες όπως ο καθένας, καθιστώντας τη διάκριση της έννοιας του δράστη και του θύματος καθαρά τεχνητή. Η συμπεριφορά των δραστών κινητοποιείται από την επιδίωξη οφέλους, ικανοποίησης, κοινωνικής καταξίωσης, κύρους, δύναμης, περιπέτειας, συγκίνησης ή διασκέδασης, όπως και των μη-δραστών στη διάρκεια των καθημερινών τους ασχολιών στην εργασία ή στον ελεύθερο χρόνο τους. Όπως τόνισαν οι Sutherland & Cressey, η εγκληματική, όπως και η μη-εγκληματική συμπεριφορά αποτελούν έκφραση των ίδιων αναγκών και αξιών. Η διαφορά τους δεν είναι στην ύπαρξη των στόχων, αλλά στη χρήση των μέσων για την επιδίωξη των στόχων. Συχνά η θυματοποίηση κάποιου αποτελεί κίνητρο για εγκληματική συμπεριφορά και του ίδιου, δίνοντάς του το απαραίτητο

[4] Όπως αναφέρεται στον Choi Kyung-shick (2008), σσ. 308-333

[5] Wilsem van, Johan. (2013), σσ. 437 – 453

[6] Όπως αυτή του Choi, βλ. Choi, Kyung-shick (2008), σσ.308-333

[7] Wilsem van, Johan. (2013), σσ. 437 – 453

[8] Βλ. Budd 1999, Lauritsen 2001, όπως αναφέρονται στο Pratt Travis C., Holtfreter Kristy & Reisig Michael (2010), σσ. 267-296

[9] Reyns Brandford, Henson Billy & Fisher Bonnie (2011), σσ. 1149-1169.

[10] Βλ. Bossler Adam, Buruss George (2011), σσ.38-67 και Bossler Adam, & Holt, Thoma (2009), σσ. 400-420.

κίνητρο (π.χ. εκδίκηση) και εκλογίκευση (π.χ. ανάκτηση των «απολεσθέντων»). Αλλά μπορεί να συμβεί και το αντίθετο, δηλαδή η εμπλοκή του ατόμου σε παράνομες δραστηριότητες ή ο συγχρωτισμός του με πιθανούς δράστες, κατά τις συνηθισμένες του δραστηριότητες, μπορεί να οδηγήσει στη δική του θυματοποίηση. Οι ρόλοι «δράστης» και «θύμα» εύκολα μπορούν να αντιστραφούν. Δεν είναι σπάνιο το φαινόμενο, ένα άτομο που προσπαθεί να εξαπατήσει κάποιο άλλο στο τέλος να πέφτει το ίδιο θύμα απάτης. Όπως και εργαζόμενοι, που αισθάνονται ότι είναι θύματα των εργοδοτών τους, επιδιώκουν να εκδικηθούν κλέβοντας αντικείμενα ή καταχρώμενοι χρήματα ή ακόμα και σαμποτάροντας την επιχείρηση στην οποία εργάζονται. Από τα προηγούμενα συμπεραίνεται ότι οι δυο ιδιότητες, αυτή του δράστη και αυτή του θύματος, συνδέονται στενά, λειτουργούν συμπληρωματικά και μπορούν να εναλλάσσονται. Το ποιος θα είναι ο δράστης και ποιος το θύμα, συχνά εξαρτάται από τους περιστασιακούς παράγοντες.[11]

Από τα παραπάνω αναδεικνύεται η ανάγκη περαιτέρω διερεύνησης του φαινομένου του ηλεκτρονικο-οικονομικού εγκλήματος, στο πλαίσιο μιας ολιστικής και πολυπαραγοντικής προσέγγισης που θα εξετάζει όσο γίνεται περισσότερες από τις πολυποίκιλες πτυχές του.

Το εγκληματολογικό ενδιαφέρον της παρούσας μελέτης είναι στην κατεύθυνση, όχι μόνο της καταλληλότητας των στόχων-θυμάτων όπως κάνουν μέχρι τώρα οι ανάλογες θυματολογικές μελέτες, αλλά και στην κατεύθυνση των πιθανών δραστών. Η παρούσα μελέτη χρησιμοποιώντας τη μέθοδο της συστηματικής βιβλιογραφικής ανασκόπησης και της μετα-ανάλυσης, διασυνδέει προσεγγίσεις που εστιάζουν στο εγκληματικό γεγονός καθαυτό και στη διαμόρφωση της εγκληματικής ευκαιρίας για τη διερεύνηση του ηλεκτρονικο-οικονομικού εγκλήματος. Η συστηματική ανασκόπηση επιτρέπει στον ερευνητή την αντικειμενική προσέγγιση του πλούτου της εγκληματολογικής βιβλιογραφίας και την κριτική ανάλυση των σχετικών μελετών.

Οι διάφορες προσεγγίσεις που εστιάζουν στο εγκληματικό γεγονός, όπως αυτές της περιβαλλοντικής εγκληματολογίας, έχουν μέχρι τώρα εφαρμοστεί μεμονωμένα, κυρίως στις θυματολογικές μελέτες της αστεακής εγκληματολογίας και τη μελέτη για το φόβο του εγκλήματος.

Η παρούσα διατριβή αποτελεί μια πρωτότυπη μελέτη και συμβάλλει στην επιστήμη της εγκληματολογίας επειδή, αφενός εισάγει την έννοια του «ηλεκτρονικο-οικονομικού» εγκλήματος και αφετέρου συγκροτεί το θεωρητικό πλαίσιό της στη βάση της σύνθεσης των επιμέρους εγκληματολογικών προσεγγίσεων για τη διερεύνηση του ηλεκτρονικο-οικονομικού εγκλήματος, εστιάζοντας το ενδιαφέρον όχι μόνο στην πλευρά του θύματος αλλά και σε αυτή του δράστη.

Πιο συγκεκριμένα, στο θεωρητικό πλαίσιο της παρούσας μελέτης συνδυάζονται οι βασικές έννοιες από τις νεότερες (μετά τη δεκαετία ’70) θεωρίες, που προέρχονται κυρίως από το πεδίο της περιβαλλοντικής εγκληματολογίας, όπως αυτές της «ορθολογικής επιλογής», των «καθημερινών δραστηριοτήτων», των «εγκληματικών προτύπων» και η στρατηγική για την «περιστασιακή πρόληψη του εγκλήματος». Οι προσεγγίσεις αυτές αναφέρονται ως «εναλλακτικές» και ως θεωρίες των «εγκληματικών ευκαιριών»[12], επειδή εστιάζουν στη διαμόρφωση των περιστασιακών συνθηκών του εγκλήματος και θεωρούν την εγκληματική συμπεριφορά ως «φυσιολογική» στο πλαίσιο καθημερινών δραστηριοτήτων των ατόμων (είτε

[11] Βλ. Fattah Ezzat (2008)

[12] Clarke Ronald (1995)

δράστη, είτε θύματος), σε αντίθεση με τις θεωρίες που εξετάζουν την εγκληματική συμπεριφορά ως παθολογική και διαφορετική από την μη εγκληματική. Οι εναλλακτικές αυτές προσεγγίσεις είχαν μέχρι τώρα πεδίο εφαρμογής στην πρόληψη του εγκλήματος στις πόλεις, στην καταπολέμηση του φόβου του εγκλήματος, στη μελέτη της σχέσης εγκλήματος και οικιστικής/βιομηχανικής ανάπτυξης στις πόλεις, στη μελέτη του παραδοσιακού εγκλήματος δρόμου ή αποσπασματικά σε κάποια από τις μορφές του οικονομικού ή του ηλεκτρονικού εγκλήματος. Η παρούσα μελέτη έχει **στόχο** την εφαρμογή τους στη μελέτη των ηλεκτρονικο-οικονομικών εγκλημάτων, τόσο σε επίπεδο διαμόρφωσης του εγκληματικού τους προτύπου όσο και σε επίπεδο αντιμετώπισης.

Τον πυρήνα των βασικών θεωριών της περιβαλλοντικής εγκληματολογίας, που συνθέτουν την προτεινόμενη θεωρητική προσέγγιση για τη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος, αποτελούν οι εξής:

1. Η θεωρία της **ορθολογικής επιλογής** (Rational Choice Theory - RCT) των Cornish και Clarke.[13]

Επηρεασμένη από την οικονομική θεωρία και τη φιλοσοφία του ωφελιμισμού, η προσέγγιση αυτή θεωρεί ότι το έγκλημα αποτελεί αποτέλεσμα εσκεμμένων αποφάσεων που λαμβάνουν οι δράστες με βάση υπολογισμούς που κάνουν σταθμίζοντας τα αναμενόμενα οφέλη (σε χρήμα, κύρος, θέση, ικανοποίηση) με το κόστος δηλαδή τους πιθανούς κινδύνους σύλληψης ή καταδίκης. Η απόφαση και επιλογή δεν είναι απόλυτα ελεύθερη αλλά υπόκειται σε περιορισμούς που θέτουν ο χρόνος, οι ικανότητες και οι πληροφορίες που είναι διαθέσιμες στον δράστη.

Οι πιθανοί δράστες με κίνητρο δρουν σε μεγάλο βαθμό ορθολογικά, εσκεμμένα, με στόχο τη διαπίστωση των περιστασιακών συνθηκών που διαμορφώνουν την εγκληματική ευκαιρία, το πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος και το ρόλο της ατομικής – ορθολογικής επιλογής σε αυτό. Σύμφωνα με την οπτική που υιοθετούμε, η (σχετική) ορθολογικότητα των πιθανών δραστών γίνεται μέσω της διερεύνησης των κινήτρων των δραστών.

2. Η θεωρία των **καθημερινών δραστηριοτήτων** (Routine Activities Theory - RAT) των Cohen και Felson.

Η αλλαγή των κοινωνικο-οικονομικών δομών μεταπολεμικά, του τρόπου ζωής, οι τεχνολογικές εξελίξεις, η εργασία -και των γυναικών- έξω από το σπίτι, η διάνυση μεγάλων αποστάσεων, η δημιουργία νέων προϊόντων συντελούν, σύμφωνα με τους Cohen και Felson, στη δημιουργία εγκληματικών ευκαιριών. Οι Cohen και Felson θεωρούν ότι η δομή της εγκληματικής ευκαιρίας συντίθεται στην βάση της ταυτόχρονης συνύπαρξης τριών παραγόντων: α) ενός δράστη με κίνητρο, β) ενός κατάλληλου και διαθέσιμου στόχου – θύματος και γ) την απουσία ικανής φύλαξης του στόχου. Η τροποποίηση ενός ή περισσότερων από αυτά τα στοιχεία – παράγοντες οδηγούν στην αλλαγή της εγκληματικής ευκαιρίας και των πιθανοτήτων θυματοποίησης.[14]

Ουσιαστικά, η θεωρία των καθημερινών δραστηριοτήτων των Cohen & Felson, αποτελεί συνέχεια της θεωρίας της **έκθεσης** του **τρόπου ζωής** (Life style - exposure) των Hindelang, Gottfredson και Garofalo. Η τελευταία μελετά την θυματοποίηση των ατόμων με βάση τον καθημερινό τρόπο ζωής τους που μπορεί να τα εκθέτει σε κίνδυνο θυματοποίησης, όπως το

[13] Clarke Ronald & Cornish Derek (2002), σσ. 291-296

[14] Cohen, Lawrence. E. και Felson, Markus (1979), σσ. 588–608

να συχνάζουν σε συγκεκριμένα μέρη, να συγχρωτίζονται με δράστες παράνομων ενεργειών ή να εμπλέκονται τα ίδια σε κάποια παραβατική δραστηριότητα.[15]

3. Η θεωρία των **εγκληματικών προτύπων** (crime pattern) των Brantingham.[16] Το εγκληματικό πρότυπο διαμορφώνεται στη βάση των περιβαλλοντικών συνθηκών που οι δράστες συναντούν κατά τη διάρκεια των καθημερινών τους δραστηριοτήτων. Οι περιβαλλοντικές αυτές συνθήκες περιλαμβάνουν τους κόμβους, τα μονοπάτια και τα όρια των περιοχών μεταξύ των οποίων κινούνται οι δράστες στο πλαίσιο των δραστηριοτήτων της καθημερινής τους ρουτίνας και που είναι πιθανότερο να συναντήσουν κάποια εγκληματική ευκαιρία. Οι κόμβοι αφορούν σημαντικά μέρη όπου συχνάζουν οι δράστες στα πλαίσια της εργασίας ή της διασκέδασής τους. Τα μονοπάτια είναι διαδρομές που ακολουθούν οι δράστες κινούμενοι μεταξύ των κόμβων. Τα όρια είναι σύνορα μεταξύ διαφόρων χώρων ή χρήσης αυτών των χώρων. Το έγκλημα είναι πιθανότερο να συμβεί σε κόμβους, μονοπάτια και όρια όπου είναι γνώριμα στους δράστες. Η θεωρία αυτή εξετάζει το εγκληματικό γεγονός, τον πιθανό δράστη, το στόχο, το συγκεκριμένο χώρο, το χρόνο και την περίσταση στο ίδιο περιβαλλοντικό σκηνικό που συγκροτεί το εγκληματικό πρότυπο[17].

4. Η **περιστασιακή πρόληψη του εγκλήματος**. [18]

Από τη δεκαετία του ’60 αρκετές εγκληματολογικές μελέτες (Jacobs 1961, Jeffery 1971) επικεντρώθηκαν στη σχέση εγκλήματος και δομημένου περιβάλλοντος ανασύροντας τις μελέτες της σχολής του Σικάγου για τη σύνδεση της ανθρώπινης συμπεριφοράς με το φυσικό περιβάλλον. Ο Newman χρησιμοποίησε τον όρο *υπερασπίσιμος χώρος* (defensible space) για να περιγράψει τη σχέση αυτή και να προτείνει τρόπους πρόληψης του εγκλήματος μέσω του κατάλληλου περιβαλλοντικού σχεδιασμού. Ο υπερασπίσιμος χώρος αφορά τη δημιουργία ενός χώρου, όπου οι εγκληματικές δραστηριότητες θα αποθαρρύνονται με τον κατάλληλο σχεδιασμό είτε των κτιρίων είτε ολόκληρης της κοινότητας.

Ο Clarke συνδύασε τις θεωρίες των καθημερινών δραστηριοτήτων και της ορθολογικής επιλογής, τις οποίες ονομάζει των «εγκληματικών «ευκαιριών», για την «περιστασιακή πρόληψη του εγκλήματος».[19]

Όπως θα διαφανεί και από την βιβλιογραφική ανασκόπηση που ακολουθεί η παρούσα μελέτη δεν ταυτίζεται και δεν υιοθετεί ένα και μοναδικό θεωρητικό εργαλείο. Η προσέγγιση που γίνεται είναι πολύπλευρη, ακριβώς λόγω του πολύπλοκου και πολυδιάστατου χαρακτήρα του εγκληματικού φαινομένου. Το θεωρητικό μοντέλο που ακολουθεί αποτελεί συνδυασμό διαφορετικών επιμέρους προσεγγίσεων. Συνδετικό κρίκο μεταξύ των θεωριών αυτών αποτελεί η κοινή οπτική που υιοθετούν εστιάζοντας στους περιστασιακούς παράγοντες, στο εγκληματικό γεγονός και στην ύπαρξη της εγκληματικής ευκαιρίας. Αυτές οι προσεγγίσεις παρουσιάζονται παρακάτω στην ανασκόπηση της σχετικής βιβλιογραφίας για να αναδειχθεί εκείνη που κάθε φορά ταιριάζει και προσεγγίζει καλύτερα το αντικείμενο μελέτης μας σε κάθε διαφορετική πτυχή του. Η καθεμιά από αυτές φωτίζει τις πολυποίκιλες πλευρές των υπό διερεύνηση θεμάτων έτσι ώστε αλληλο-συμπληρώνονται χωρίς να συγκρούονται μεταξύ τους. Οι προσεγγίσεις αυτές έχουν κοινό ότι εστιάζουν στη δόμηση της «εγκληματικής ευκαιρίας»

[15] Cook PhilipT. (1986), σσ. 1-27, Gottfredson Michael R. & Hindelang Michael J. (1981)
[16] Brantigham Patricia L. & Brantigham Paul J., (2008), σσ. 259-294.
[17] Brantigham Patricia L. & Brantigham Paul J. (1993), σσ. 3-28
[18] Jeffery C. Ray & Zahm Diane (2008)
[19] Clarke Roland (1995)

και συγκροτούν το θεωρητικό πλαίσιο της μελέτης μας, που βοηθά τόσο στην διατύπωση των ερευνητικών προτάσεων αλλά και στον έλεγχό τους.

Κοινά στοιχεία των θεωριών αυτών, που αποτελούν την εναλλακτική προσέγγιση (ως προς τις θετικιστικές θεωρίες), συνιστούν τα παρακάτω:

- ✓ Η εστίαση στην εγκληματική **ευκαιρία**, στο εγκληματικό γεγονός, στην απόφαση του δράστη για εμπλοκή και στις περιστασιακές συνθήκες που συνθέτουν την ευκαιριακή δομή του εγκλήματος, παρά στα αίτια του εγκλήματος. Το έγκλημα θεωρείται ως μια φυσιολογική και αναμενόμενη απάντηση των ατόμων (δραστών) σε περιβαλλοντικά ερεθίσματα, ευκαιρίες, προκλήσεις, ανάγκες, έλλειψη εναλλακτικών λύσεων. Έτσι οι ευκαιρίες, οι περιστασιακοί παράγοντες διαδραματίζουν σημαντικότερο ρόλο από τα μόνιμα ψυχικά χαρακτηριστικά των δραστών.
- ✓ Αναζητούν τα **πρότυπα** (μοτίβα) του εγκλήματος, τον τρόπο δράσης των εγκληματιών, τον τόπο και το χρόνο που αυτοί αλληλεπιδρούν με τους στόχους τους, το ρόλο του περιβάλλοντος, το ποιες είναι οι συνηθισμένες δραστηριότητες των ατόμων που τους καθιστούν κατάλληλους στόχους.
- ✓ Η αναγνώριση ότι η εγκληματική συμπεριφορά δεν αποτελεί μια παθολογική, απρόβλεπτη, ασυνήθιστη συμπεριφορά, που χαρακτηρίζεται από παράλογα κίνητρα, αλλά μια **ορθολογική**, ηθελημένη **συμπεριφορά** που επιδιώκει στόχους, όπως και η μη εγκληματική με την οποία μοιράζεται πιο πολλές ομοιότητες παρά διαφορές.
- ✓ Τα **κίνητρα** παίζουν ρόλο στην ορθολογική απόφαση του πιθανού δράστη να πλήξει συγκεκριμένο στόχο-θύμα. Η ορθολογικότητα στις επιλογές και αποφάσεις του δράστη, που έγκειται στον υπολογισμό κόστους – οφέλους, δεν βασίζεται τόσο στην έννοια της ελεύθερης βούλησης αλλά περιορίζεται από προσωπικούς, περιστασιακούς και περιβαλλοντικούς παράγοντες, από την αντίληψή του για τον επιδιωκόμενο σκοπό και τα διαθέσιμα σε αυτόν μέσα.
- ✓ Συνακόλουθα οι πρακτικές αντιμετώπισης του εγκλήματος δεν βασίζονται τόσο στην ποινική καταστολή, στη μεταχείριση και στη «θεραπεία» του εγκληματία, όσο στο χειρισμό των περιβαλλοντικών συνθηκών, στην **πρόληψη των περιστασιακών παραγόντων**, στη μείωση της προσφοράς εγκληματικών ευκαιριών, στη θωράκιση του στόχου και γενικά στην αλλοίωση της δομής του εγκληματικού προτύπου.[20]

Ο βασικός στόχος της παρούσας διατριβής είναι η κατασκευή ενός γενικού προτύπου των εγκληματικών ευκαιριών του ηλεκτρονικο-οικονομικού εγκλήματος που θα βοηθήσει τόσο στην κατανόηση αυτού του είδους εγκληματικής δραστηριότητας όσο και στη διατύπωση προτάσεων για αποτελεσματικότερους και πιο ανέξοδους τρόπους αντιμετώπισής του.

Επιμέρους στόχους αποτελούν η εξέταση:

- των συμπεριφορών ρουτίνας των χρηστών των ψηφιακών τεχνολογιών που τους καθιστούν ευάλωτους στόχους σε δράστες με κίνητρο,
- της σχέσης μεταξύ εγκλήματος ψηφιακής τεχνολογίας και οικονομικού εγκλήματος η οποία συντελεί στη δόμηση της προτεινόμενης έννοιας του «ηλεκτρονικο-οικονομικού εγκλήματος,

[20] Βλ. Fattah Ezzat (2008) και Brantigham Patricia L. & Brantigham Paul J., όπ.

- της εφαρμοσιμότητας των θεωριών των «εγκληματικών ευκαιριών» που προέρχονται από το χώρο της περιβαλλοντικής εγκληματολογίας για τη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος,
- του ρόλου των κινήτρων και της ευκαιρίας για την διαμόρφωση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος.

Η παρούσα διατριβή είναι χωρισμένη σε δυο μέρη. Το πρώτο μέρος περιλαμβάνει το θεωρητικό πλαίσιο, την ανασκόπηση της προϋπάρχουσας βιβλιογραφίας, τις εννοιολογικές διασαφηνίσεις και κατηγοριοποιήσεις ενώ στο δεύτερο μέρος γίνεται η εφαρμογή των προσεγγίσεων του θεωρητικού πλαισίου στη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος και εξετάζονται οι τρόποι αντιμετώπισης. Ειδικότερα:

Η παραπάνω εισαγωγή αποτελεί το πρώτο κεφάλαιο του παρόντος πονήματος, όπου εξηγήθηκε η ερευνητική πρόταση, ο σκοπός, η μέθοδος και τα κίνητρα της μελέτης και παρουσιάστηκε σύντομα το θεωρητικό του πλαίσιο.

Ακολουθεί το δεύτερο κεφάλαιο με την βιβλιογραφική ανασκόπηση, την εκτενέστερη παρουσίαση του επιλεγέντος θεωρητικού πλαισίου, τις απαραίτητες εννοιολογικές οριοθετήσεις και τη διατύπωση των θεωρητικών προτάσεων της διατριβής.

Στο τρίτο κεφάλαιο παρουσιάζεται η εξέλιξη στη μελέτη της έννοιας του οικονομικού εγκλήματος, των ερμηνευτικών του προσεγγίσεων, τα χαρακτηριστικά του, τα κίνητρα του δράστη, το κόστος που επιφέρει στην κοινωνία και ο ρόλος της παγκοσμιοποίησης για τη διάδοση του οικονομικού εγκλήματος.

Στο τέταρτο κεφάλαιο εξηγούνται η έννοια και τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος, το κόστος του για την κοινωνία, τα οφέλη για τον δράστη, τα κίνητρα και το προφίλ του.

Η σχέση μεταξύ οικονομικού και ηλεκτρονικού εγκλήματος εξετάζεται στο πέμπτο κεφάλαιο και δομείται η έννοια του ηλεκτρονικο-οικονομικού εγκλήματος. Διακρίνονται οι μορφές των ηλεκτρονικο-οικονομικών εγκλημάτων και τα χαρακτηριστικά τους.

Στο έκτο κεφάλαιο γίνεται η κατηγοριοποίηση των ηλεκτρονικών και οικονομικών εγκλημάτων και διακρίνονται τα είδη των καθαρά ηλεκτρονικών εγκλημάτων που η ψηφιακή τεχνολογία αποτελεί τον στόχο, από τα ηλεκτρονικο-οικονομικά εγκλήματα που η τεχνολογία αποτελεί το μέσο δια του οποίου διευκολύνεται η τέλεση. Τα καθαρά ηλεκτρονικά εγκλήματα, όπως η διάδοση ιών, συχνά αποτελούν εργαλείο του πιθανού δράστη για να προσβάλλει στόχους που θα του αποδώσουν οικονομικό όφελος, για το λόγο αυτό εξετάζονται και περιλαμβάνονται στο αντικείμενό μας.

Στο έβδομο κεφάλαιο εξετάζονται συστηματικά οι έρευνες που επιχείρησαν την εφαρμογή των διαφόρων προσεγγίσεων των εγκληματικών «ευκαιριών» στη μελέτη κάποιας από τις μορφές του ηλεκτρονικού - οικονομικού εγκλήματος.

Στο όγδοο κεφάλαιο επιχειρείται η μετα-ανάλυση των προηγούμενων ερευνών και δομούνται τα στοιχεία που αποτελούν το εγκληματικό πρότυπο και διαμορφώνουν την «καταλληλότητα» της εγκληματικής ευκαιρίας του ηλεκτρονικο-οικονομικού εγκλήματος: ο κοινός τόπος, η εγγύτητα, τα κίνητρα του δράστη, η εκτίμηση του αναμενόμενου οφέλους από την πλευρά του, η ύπαρξη ή η απουσία των ικανών φυλάκων. Καταγράφονται ακόμα τα δημογραφικά χαρακτηριστικά των χρηστών ψηφιακών τεχνολογιών, γιατί σχετίζονται με την καταλληλότητά τους ως πιθανοί στόχοι.

Το ένατο κεφάλαιο διαπραγματεύεται τα νομοθετικά μέτρα που θεσπίστηκαν τόσο σε επίπεδο κρατών, όσο και υπερεθνικών οργανισμών, όπως η Ευρωπαϊκή Ένωση, ο Ο.Ο.Σ.Α κλπ. και εκθέτονται οι δυσκολίες καταπολέμησης του ηλεκτρονικο – οικονομικού εγκλήματος.

Τα πρακτικά μέτρα πρόληψης του ηλεκτρονικο-οικονομικού εγκλήματος που προτείνονται από την σκοπιά των θεωριών των «εγκληματικών ευκαιριών», παρουσιάζονται στο δέκατο κεφάλαιο. Ειδικότερα προτείνονται και παρουσιάζονται μέτρα που λαμβάνονται από τις διωκτικές αρχές, από άτομα (χρήστες/καταναλωτές ψηφιακών τεχνολογιών) και από επιχειρήσεις, που θα μειώνουν τις ευκαιρίες για τη διάπραξη του ηλεκτρονικο-οικονομικού εγκλήματος, θα καθιστούν το στόχο λιγότερο ελκυστικό και την ανακάλυψη του δράστη πιο πιθανή.

Στα συμπεράσματα γίνεται εκτίμηση των αποτελεσμάτων της διατριβής, για το αν επιβεβαιώθηκαν οι ερευνητικές υποθέσεις της και σε ποιο βαθμό, αναφορά στις δυσκολίες που παρουσιάστηκαν, στους περιορισμούς της μελέτης και γίνονται προτάσεις για περαιτέρω έρευνες.

Στο τέλος παρατίθεται η βιβλιογραφία, τα διαγράμματα, οι πίνακες και το παράρτημα στο οποίο συμπεριλήφθησαν στοιχεία που δεν θεωρήθηκε σκόπιμο να αναφερθούν στο κύριο μέρος, όπως χαρακτηριστικές υποθέσεις ηλεκτρονικο-οικονομικών εγκλημάτων από την ειδησεογραφία και οδηγίες που δίνουν επίσημοι φορείς στους χρήστες της ψηφιακής τεχνολογίας για την προστασία τους.

Τα στάδια τα οποία ακολουθήθηκαν στο πλαίσιο της παρούσας διατριβής ήταν:

- Η διατύπωση του ερευνητικού ερωτήματος και σκοπού της μελέτης.
- Η επιλογή του θεωρητικού πλαισίου.
- Η επιλογή των μεθόδων διερεύνησης.
- Οι εννοιολογικές διευκρινήσεις και διατύπωση των λειτουργικών ορισμών της μελέτης.
- Ο καθορισμός των κριτηρίων επιλογής ή αποκλεισμού προγενέστερων μελετών με βάση τους ορισμούς που δόθηκαν,
- Η αναζήτηση σχετικής βιβλιογραφίας,
- Η αξιολόγηση και επιλογή των μελετών.
- Η κριτική καταγραφή και σύνθεση των δεδομένων.
- Η παρουσίαση των αποτελεσμάτων.
- Η εξαγωγή συμπερασμάτων.

ΜΕΡΟΣ Α΄

ΚΕΦΑΛΑΙΟ 2. ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ

Οι προσεγγίσεις για τη σύγχρονη οικονομική και την ηλεκτρονική εγκληματικότητα, τόσο για την ερμηνεία όσο και για την αντιμετώπισή της, εφαρμόζουν όμοια θεωρητικά σχήματα που χρησιμοποιούνται στην μελέτη της παραδοσιακής εγκληματικότητας. Παρακάτω παρουσιάζονται αυτές τις προσεγγίσεις, με ιστορική – χρονολογική σειρά και στη συνέχεια γίνεται η διασύνδεσή τους και η εφαρμογή τους στη προσέγγιση και την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος.

Στο τέλος του κεφαλαίου διατυπώνονται οι θεωρητικές προτάσεις της παρούσας μελέτης.

2.1. Ιστορική εξέλιξη των θεωριών. Οι πρωτοπόροι

Από τις πρώτες προσπάθειες ερμηνείας, αν όχι η πρώτη, του εγκληματικού φαινομένου δίνεται από τον Αριστοτέλη που αναφέρει ότι οι άνθρωποι διαπράττουν τα εγκλήματα στο πλαίσιο της επιδίωξης υπερβολικών ανέσεων, να αποκομίσουν ικανοποίηση χωρίς κόπο και πόνο. Τα μεγαλύτερα εγκλήματα προκαλούνται μάλιστα ως ατομική επιλογή, από την υπερβολή και όχι από την ανάγκη.[21]

Τις θεωρητικές βάσεις των σύγχρονων εγκληματολογικών προσεγγίσεων παρέχουν δυο κεντρικές και αντίθετες, ως ένα βαθμό, μεταξύ τους παραδοσιακές προσεγγίσεις: η κλασική σχολή της εγκληματολογίας και ο θετικισμός. Η πρώτη θεωρεί ότι η ανθρώπινη φύση βασίζεται στην ελεύθερη βούληση, την ηθική ευθύνη και την ορθολογική συμπεριφορά, ενώ σύμφωνα με τον δεύτερο η ανθρώπινη φύση μελετάται θετικιστικά στα πλαίσια που έθεσαν η βιολογία, η ψυχολογία και η κοινωνιολογία από το 19^{ο} αιώνα.[22]

2.1.1. Η κλασική σχολή

Οι βασικές απόψεις των κυριότερων εκπροσώπων της κλασικής σχολής, Cesare Beccaria και Jeremy Bentham εστιάζουν στο νομικό ορισμό του εγκλήματος. Η συμπεριφορά του ατόμου είναι σκόπιμη και διέπεται από την ελευθερία βούλησης[23] και από την αρχή του *ηδονισμού*, επιδιώκοντας την ευχαρίστηση, την ηδονή και την αποφυγή της δυσαρέσκειας ή πόνου. Η προβλεπόμενη ευχαρίστηση που προκαλεί μια πράξη συνυπολογίζεται με την πιθανή δυσαρέσκεια (όπως την τιμωρία). Η ποινή πρέπει να προκαλεί στο δράστη μεγαλύτερη δυσαρέσκεια από την ευχαρίστηση που συνεπάγεται η παραβίαση του νόμου και να αποτελεί μέσο γενικής πρόληψης που να λειτουργεί με το μικρότερο δυνατό κόστος.[24]

---

[21] Βλ. Αριστοτέλη, *Ηθικά Νικομάχεια*, Ενότητα 10, για την *αρετή*: «Επιπλέον, το να κάνει κανείς λάθος γίνεται με πολλούς τρόπους, όμως το να πράττει κανείς το σωστό γίνεται με έναν μόνο τρόπο (γι' αυτό και το ένα είναι εύκολο, ενώ το άλλο δύσκολο, εύκολο το να αποτύχει κανείς στο σκοπό του, δύσκολο όμως το να τον επιτύχει)· γι' αυτούς λοιπόν τους λόγους γνώρισμα της κακίας είναι η υπερβολή και η έλλειψη, ενώ της αρετής (είναι) η μεσότητα· γιατί καλοί (γινόμαστε) με ένα μόνο τρόπο, ενώ κακοί με πολλούς. Είναι, λοιπόν, η αρετή μια έξη (συνήθεια) που ***επιλέγεται ελεύθερα από το άτομο***, η οποία βρίσκεται στη μεσότητα σε σχέση με εμάς, που καθορίζεται από τη λογική και συγκεκριμένα, κατά τη γνώμη μου (με τη λογική) που καθορίζει ο φρόνιμος άνθρωπος. Και (είναι) μεσότητα (που βρίσκεται) ανάμεσα σε δύο κακίες, που η μια βρίσκεται από την πλευρά της υπερβολής, ενώ η άλλη από την πλευρά της έλλειψης· και, ακόμα, είναι μεσότητα, διότι άλλες από αυτές (τις κακίες) υπολείπονται και άλλες ξεπερνούν το πρέπον και στα συναισθήματα και στις πράξεις, ενώ η αρετή και βρίσκει και επιλέγει το μέσον».

[22] Jeffery C. Ray & Zahm Diane L. (2008)

[23] Σπινέλλη, Καλλιόπη (2005), σσ. 183-186 και Adler Freda, Mueller Gerhard, Laufer William (1998) σσ. 48-49

[24] Σπινέλλη, Καλλιόπη (2005), σσ. 183-186

Η αρχική θεωρία του (οικονομολόγου) Beccaria, όπως και του Bentham, βρήκε πλήθος εφαρμογών και συνεχιστών, όχι μόνο στην εγκληματολογία αλλά και ευρύτερα στις κοινωνικές επιστήμες. Η υπόθεση ότι η ανθρώπινη συμπεριφορά κινητοποιείται από την επιδίωξη του μέγιστου δυνατού οφέλους όχι μόνο επέτρεψε τη δόμηση μοντέλων πρόβλεψής της, αλλά κατέστησε και την οικονομική επιστήμη την πιο «επιτυχημένη» μεταξύ των κοινωνικών επιστημών. Το σχήμα «μεγιστοποίηση οφέλους – ελαχιστοποίηση κόστους/πόνου» εφαρμόστηκε από την οικονομική επιστήμη για τη διατύπωση της «βασικής οικονομικής αρχής» ή «οικονομικού αξιώματος», που διέπει τη συμπεριφορά των οικονομούντων ατόμων (επιχειρήσεων και καταναλωτών). Δηλαδή τα άτομα, προκειμένου να καλύψουν καλύτερα τις παραγωγικές ή τις καταναλωτικές τους ανάγκες, επιδιώκουν τη μεγιστοποίηση του οφέλους τους: το μέγιστο δυνατό οικονομικό κέρδος με το λιγότερο δυνατό κόστος.[25]

Σύγχρονες εγκληματολογικές προσεγγίσεις όπως η οικονομική προσέγγιση του εγκλήματος, οι θεωρίες της ορθολογικής επιλογής, των καθημερινών δραστηριοτήτων, η προσέγγιση της πρόληψης του εγκλήματος, που συμπεριλαμβάνονται στο θεωρητικό μοντέλο που δομεί την παρούσα μελέτη, βασίζονται στο σχήμα «ικανοποίησης-πόνου» και μεγιστοποίησης οφέλους που προέρχεται από την κλασική σχολή και την οικονομική θεωρία.[26] Άλλωστε ο Beccaria θεωρήθηκε ο πρώτος οικονομολόγος που εφήρμοσε την ορθολογική επιλογή και την οικονομική ανάλυση στο πεδίο μελέτης του εγκληματικού φαινομένου και της αντιμετώπισής του.[27] Ο Schumpeter μάλιστα τοποθετεί τον Beccaria μαζί με τον Adam Smith στους ιδρυτές της κλασικής οικονομικής θεωρίας.[28]

2.1.2. Η θετική σχολή

Η ανάπτυξη των θετικών (φυσικών) επιστημών και της ιατρικής στις αρχές του 19ου αι. συνετέλεσε στην ανάπτυξη μιας ακόμη τάσης στην εγκληματολογία, της θετικιστικής, που θεωρεί την ανθρώπινη συμπεριφορά όχι ως αποτέλεσμα της ελεύθερης βούλησης του ατόμου αλλά της επίδρασης (πίεσης) βιολογικών, ψυχολογικών και κοινωνικών παραγόντων.[29] Η θετική προσέγγιση πρόταξε την επιστημονική μελέτη της ανθρώπινης συμπεριφοράς αντικαθιστώντας τη θεώρηση της κλασικής σχολής για έμφαση στην ποινική μεταχείριση με ένα βιολογικό και μπηχεϋβιοριστικό μοντέλο που περιλαμβάνει, αφενός την ιατρική, ψυχολογική μεταχείριση, με στόχο την επανένταξη του εγκληματία[30] και αφετέρου τη βελτίωση των παθογόνων κοινωνικο-οικονομικών δομών της κοινωνίας.

Ειδικότερα, η Ιταλική θετική σχολή, με σημαντικότερους εκπροσώπους τους Cesare Lombroso, τον Enrico Ferri και τον Raffaele Garofalo, επηρεασμένη από τις ιδέες του Διαφωτισμού και αυτές των Auguste Comte και Charles Darwin, στηρίχτηκε σε διαφορετικές παραδοχές από αυτές της κλασικής. Εστίασε στον εγκληματία και όχι στο έγκλημα. Ο εγκληματίας δεν έχει ελεύθερη βούληση αλλά γεννιέται με προδιάθεση να εγκληματήσει. Ως

[25] Scott John (2000)

[26] Jeffery C. Ray & Zahm Diane L. (2008), σ.324

[27] Harcourt Bernard (2013)

[28] Ο Schumpeter αποκάλεσε τον Beccaria ως τον «Ιταλό» Adam Smith και τον Adam Smith ως το «Σκωτσέζο» Beccaria, βλ. Harcourt Bernard (2013)

[29] Adler Freda, Mueller Gerhard, Laufer William (1998), σ. 48

[30] Βλ. Γιωτοπούλου-Μαραγκοπούλου Αλίκη (1984), σ.σ.83-96 αναφορά στους Pinel, Prichard, Morel, Lombroso, Garofalo που προέρχονται από τους κλάδους της ψυχιατρικής, της βιολογίας και της ψυχολογίας.

εκ τούτου το άτομο δεν έχει ευθύνη, η ποινή πρέπει να είναι αόριστη με στόχο την αναμόρφωση του εγκληματία.[31]

2.1.3. Η οικολογική σχολή

Η κοινωνιολογική προσέγγιση ανάγεται στο έργο του Emile Durkheim ο οποίος, απορρίπτοντας τους βιολογικούς και ψυχολογικούς παράγοντες, πρότεινε τους κοινωνικούς για την εξήγηση της ανθρώπινης συμπεριφοράς, ακόμα και της εγκληματικής.

Την κοινωνιολογική προσέγγιση του Emile Durkheim ακολούθησαν, σε ένα βαθμό και οι θεωρητικοί της Σχολής του Σικάγου στις αρχές του 20ου αιώνα. [32]

Οι θεωρητικοί της οικολογικής Σχολής του Σικάγου, όπως οι Robert Park και Ernest Burgess, Clifford Shaw και Henry McKay, μελέτησαν την ανθρώπινη συμπεριφορά ως αποτέλεσμα της επίδρασης του περιβάλλοντος και των κοινωνικών συνθηκών και όχι ατομικών βιολογικών ή ψυχολογικών παραγόντων. Οι Robert Park και Ernest Burgess, μελέτησαν τον αστικό χώρο χρησιμοποιώντας μεθόδους όπως παρατήρηση, ερωτηματολόγια, συνεντεύξεις, κοινωνική χαρτογράφηση[33].

Όπως ο Durkheim έδωσε έμφαση στο ρόλο της ραγδαίας κοινωνικής αλλαγής και της χαλάρωσης του κοινωνικού ελέγχου στο μακρο-επίπεδο της ευρύτερης κοινωνίας, έτσι και οι θεωρητικοί του Σικάγου στο πλαίσιο της «ανθρώπινης οικολογίας» διερεύνησαν την επίδραση της ραγδαίας αλλαγής και της κοινωνικής αποδιοργάνωσης όμως στο μικρο-επίπεδο της συνοικίας.[34] Ακολούθησαν αφενός τις απόψεις του Emile Durkheim για το ρόλο που διαδραματίζουν οι κοινωνικές σχέσεις και οι ταχύρυθμες κοινωνικές μεταβολές για την τήρηση των κανόνων, την ικανότητα προσαρμογής του ατόμου, την ανομία, την αποτελεσματικότητα του κοινωνικού ελέγχου και τη σύγκρουση των αξιών, αφετέρου διαφοροποιήθηκαν από αυτόν ως προς το ρόλο των διαπροσωπικών σχέσεων για την κοινωνική συνοχή. [35]

Ο Robert Merton ακολούθησε επίσης τη θεωρία του Emile Durkheim. Επέκτεινε μάλιστα τη θεωρία της ανομίας στο σχήμα «πολιτισμικοί στόχοι» - «θεσμοθετημένα μέσα», θέτοντας ως στόχο την εξακρίβωση του ρόλου των κοινωνικών δομών στην άσκηση πίεσης σε ορισμένα άτομα να επιδεικνύουν αντισυμβατική συμπεριφορά.[36]

Οι παραπάνω απόψεις επηρέασαν σημαντικό μέρος σύγχρονων ερευνών, που εκτός από την αντικειμενική διάσταση του περιβάλλοντος χώρου μελετούν και την υποκειμενική, το πώς αντιλαμβάνονται τα ίδια τα άτομα τον χώρο. Οι μελέτες αυτές, συνδυάζοντας την χωροταξία του εγκλήματος με την υποκειμενική πρόσληψή του από τα άτομα και τον φόβο του εγκλήματος, κατασκευάζουν γνωστικούς χάρτες.[37]

2.2. Οι νεότερες θεωρίες της ατομικής επιλογής

Οι περιπτώσεις όχι μόνο των παραδοσιακών αλλά και των οικονομικών εγκλημάτων εξετάζονται πλέον σήμερα από μελετητές κάτω από το πρίσμα της «ορθολογικής επιλογής» (Rational choice) και - όπως αυτή εφαρμόστηκε στη μελέτη πολλών κατηγοριών εγκλημάτων -

[31] Σπινέλλη, Καλλιόπη (2005), σσ. 190-193
[32] Jeffery C. Ray & Zahm Diane L. (2008)
[33] Κυριαζή Νότα (2002), σ. 248
[34] Σπινέλλη, Καλλιόπη (2005), σσ. 241-243
[35] Βλ. Λαμπροπούλου Έφη (2009)
[36] Burke Roger Hopkins (2009), σ.106
[37] Ζαραφωνίτου Χριστίνα (2001), σσ. 186-196

την θεωρία των «κοινωνικών ανταλλαγών» του George Homans, από την «οικονομική προσέγγιση» του Gary Becker, τη «θεωρία της ορθολογικής επιλογής» των Cornish και Clarke, τη θεωρία των «καθημερινών δραστηριοτήτων» (Routine activities theory) των Marcus Felson και Lawrence Cohen, τις προσεγγίσεις για την «πρόληψη του εγκλήματος» τις οποίες και θα παρουσιάσουμε παρακάτω. Οι θεωρίες αυτές έχουν βάση ότι η ανθρώπινη συμπεριφορά είναι ορθολογική και επιδιώκει τη μεγιστοποίηση του οφέλους (κέρδους) και την ελαχιστοποίηση του πόνου (κόστους), σύμφωνα με το μοντέλο ωφέλεια – ζημία, όπως αυτό διατυπώθηκε από την κλασική θεωρία.[38]

Η Θεωρία της Ορθολογικής Επιλογής, έχει τις βάσεις στις ιδέες της κλασικής σχολής της εγκληματολογίας στο έργο του Cesare Beccaria «Περί Εγκλημάτων και Ποινών» στα τέλη του 18ου αιώνα (1764) και του Jeremy Bentham, ιδρυτή του σύγχρονου Ωφελιμισμού (Utilitarianism)[39].

Η οικονομική επιστήμη εφαρμόζει τη θεωρία της Ορθολογικής Επιλογής στη μελέτη των προβλημάτων της παραγωγής, κατανομής και κατανάλωσης υλικών αγαθών και υπηρεσιών μέσω των μηχανισμών της αγοράς.

Οι προσπάθειες των οικονομικών θεωριών, όπως αυτή του Gary Becker[40], συνέτειναν στην έκφραση των ωφελιμιστικών θεωριών σε μαθηματικούς όρους όπου τα άτομα επιδιώκουν την μεγιστοποίηση της ωφέλειας ή ικανοποίησης επιλέγοντας ανάμεσα σε εναλλακτικές και υπολογίζοντας σε κάθε μια τα κέρδη και τα κόστη. Το έγκλημα αντιμετωπίστηκε ως «επαγγελματική» επιλογή, όπως κανείς θα επέλεγε μια νόμιμη απασχόληση, στο πλαίσιο των καθαρά οικονομικών όρων της «προσφοράς» και «ζήτησης». Η εγκληματική επιλογή μοιάζει πιο πρόσφορη από την νόμιμη δραστηριότητα, αν είναι πιο επωφελής ή λιγότερο επιζήμια.[41]

Ένας ορθολογικός δράστης λειτουργεί με παρόμοιο τρόπο όπως τα οικονομούντα άτομα, ο ορθολογικός καταναλωτής και ο ορθολογικός επιχειρηματίας, με βάση το λεγόμενο στην Οικονομική επιστήμη «Οικονομικό Αξίωμα»: Η επίτευξη του μέγιστου οφέλους – με τη μικρότερη δυνατή θυσία (κόστος). Είναι προφανής η εφαρμογή της ορθολογικής συμπεριφοράς σε κάθε τομέα ανθρώπινων δραστηριοτήτων, τόσο νόμιμων όσο και παράνομων.

Σε αυτή την οπτική στράφηκε το ενδιαφέρον και άλλων κοινωνικών επιστημόνων που διατύπωσαν με τη σειρά τους θεωρίες με βάση την κεντρική ιδέα ότι κάθε δραστηριότητα είναι ορθολογική και ότι τα άτομα πριν δράσουν υπολογίζουν τα αναμενόμενα οφέλη και τα αντίστοιχα κόστη.[42]

Σύμφωνα με πολλούς θεωρητικούς[43] της «Ορθολογικής Επιλογής» η ενίσχυση των συμπεριφορών μέσω των κατάλληλων κινήτρων είναι μέγεθος μετρήσιμο σύμφωνα με την ποσότητα και την αξία του. Παρά τη δυσκολία μέτρησης της ανταμοιβής, όπως η κοινωνική αποδοχή, θεωρούν ότι ακόμα και αυτή μπορεί να εκφραστεί με όρους μετρήσιμους όπως το χρήμα, ο χρόνος ή η χρησιμότητα. Η έννοια της χρησιμότητας στα οικονομικά εκφράζει την ικανοποίηση που νοιώθει ο καταναλωτής από την κατανάλωση ενός προϊόντος. Οι

[38] Jeffery C. Ray & Zahm Diane (2008) , σσ.336-.339

[39] Βλ. Felson Marcus & Cohen Lawrence E. (1980), σ.396, αναφορά στον Gibbons, D.C. (1977), *Society, Crime and Criminal Careers*. Prentice-Hall, Englewood Cliffs, N.J.

[40] Adler Freda, Mueller Gerhard, Laufer William (1998), σ.171

[41] Clarke Roland. V. & Felson Marcus (2008), σ.5

[42] Jeffery C. Ray & Zahm Diane L. (2008), σ.321

[43] Scott John (2000)

θεωρητικοί αυτοί κατασκευάζουν μάλιστα γραφικές παραστάσεις ή μαθηματικούς τύπους, κατά τα πρότυπα της οικονομικής επιστήμης,[44] για να απεικονίσουν την άριστη επιλογή δραστηριοτήτων που μεγιστοποιεί τη χρησιμότητα[45] ή τη σχετική χρησιμότητα ενός αγαθού ή αξίας σε όρους κάποιου άλλου.[46] Υπάρχει δηλαδή για το άτομο - κοινωνικό δρώντα (νομοταγή ή εγκληματία) ένας δείκτης σχετικής χρησιμότητας του ενός αντικειμένου σε όρους κάποιου άλλου: αν η χρησιμότητα, δηλαδή ο βαθμός ικανοποίησης που προκύπτει από την Α΄ επιλογή είναι μεγαλύτερη από αυτή της Β΄, τότε θα προτιμηθεί η Α΄.

Από την πλευρά της κοινωνιολογίας οι αντίστοιχες αρχές της Ορθολογικής δράσης χρησιμοποιούνται για την διερεύνηση παραγόντων όπως χρόνος, πληροφορία, αποδοχή, γόητρο που λαμβάνουν μέρος σε κοινωνικές αλληλεπιδράσεις ως κίνητρα για δράση. Τα άτομα εξετάζονται υπό το πρίσμα ότι δρουν με κίνητρα τις επιθυμίες, τις ανάγκες τους ή τους στόχους που εκφράζουν τις προτιμήσεις τους. Λειτουργούν με βάση τις προτιμήσεις τους και τους περιορισμούς που τους τίθενται ή αλλιώς με βάση τα μέσα που διαθέτουν για την επίτευξη των στόχων τους, υπολογίζοντας τις διάφορες εναλλακτικές δράσεις και επιλέγουν εκείνη που αναμένεται να τους αποδώσει τα καλύτερα οφέλη.[47]

Οι κοινωνιολόγοι έτσι αναγνώρισαν, με τη σειρά τους, το γεγονός ότι τα άτομα δρουν ορθολογικά, χωρίς παράλληλα να παραγνωρίζουν ότι υπάρχουν και ανθρώπινες συμπεριφορές που περιλαμβάνουν τόσο ορθολογικά όσο και μη ορθολογικά στοιχεία, όπως οι μορφές συμπεριφοράς που στηρίζονται στην παράδοση, τη συνήθεια, το συναίσθημα και το αξιακό σύστημα των ατόμων (κατά τον γνωστό Βεμπεριανό ιδεότυπο της δράσης). Οι θεωρητικοί της κλασικής «Ορθολογικής Δράσης», παρόλα αυτά επιμένουν ότι κάθε κοινωνική δράση είναι αμιγώς ορθολογιστική και «υπολογιστική» και ότι προκαλείται από ορθολογικά κίνητρα.

2.2.1. Η « Θεωρία της Κοινωνικής Ανταλλαγής»

Οι βασικές αρχές λοιπόν της ανθρώπινης δράσης έχουν κοινές βάσεις τόσο στη φιλοσοφία, όσο και στις κοινωνικές επιστήμες. Ο «ηδονισμός» και ο «ωφελιμισμός» των φιλοσόφων, αποκαλείται «ενίσχυση» ή «ανταμοιβές» από τους ψυχολόγους και «χρησιμότητα» από τους οικονομολόγους.[48] Αυτή η παραδοχή, που ενέπνευσε τα οικονομολογικά μοντέλα ερμηνείας της δράσης, όπως αυτή του Gary S. Becker, αποτελεί τη βάση στην οποία δομήθηκε η «Θεωρία Ορθολογικής Δραστηριότητας» ή της «Ορθο-λογικής επιλογής» (Rational Choice Theory) και η εφαρμογή της στην κοινωνική αλληλεπίδραση η οποία λαμβάνει τη μορφή της «Θεωρίας της Κοινωνικής Ανταλλαγής» (exchange theory).

Από τους πρωτοπόρους που εφάρμοσαν την ορθολογική επιλογή της κλασικής σχολής, στην κοινωνική θεωρία ήταν ο George Homans ο οποίος έβαλε τα θεμέλια της «θεωρίας της Κοινωνικής Ανταλλαγής» (social exchange theory), στο έργο του "Social behavior as exchange" το 1958[49]. Ο Homans, και οι συνεργάτες του Thibaut, Kelley και Blau συνδύασαν τις βασικές αρχές της συμπεριφοριστικής ψυχολογίας με τη μικρο-οικονομική θεωρία εφαρμόζοντάς τις

[44] Βλ. Μαυράκης Εμμανουήλ (2004)
[45] Winston Gordon.C. (1989), σσ., 67-86
[46] Piliavin Irving, Gartner Rosemary, Thornton Craig & Matsueda Ross L. (1986), σσ. 101-119
[47] Scott John (2000)
[48] Wilson & Hernstein, όπως αναφέρονται στο Cornish Derek (1993), σσ. 351-382
[49] Emerson Richard M. (1976)

στη μελέτη της αλληλεπίδρασης σε μικρές ομάδες και της πίεσης για συμμόρφωση που αυτές ασκούν στα μέλη τους. [50]

Ο Homans όρισε την κοινωνική ανταλλαγή ως την ανταλλαγή δραστηριοτήτων, περισσότερο ή λιγότερο επωφελών, μεταξύ τουλάχιστον δυο προσώπων.[51] Επηρεασμένος από τον συμπεριφορισμό του Skinner θεωρεί ότι η ανθρώπινη συμπεριφορά υπόκειται στα εξαρτημένα αντανακλαστικά, όπως και αυτή των ζώων, δηλαδή διαμορφώνεται με βάση την ανταμοιβή (θετικός ενισχυτής) ή την τιμωρία (αρνητικός ενισχυτής). Οι άνθρωποι τείνουν να επαναλαμβάνουν συμπεριφορές που έχουν θετικά για αυτούς αποτελέσματα ή όφελος (επιτυχία, αποδοχή, φιλία, υποστήριξη κλπ.) και να αποφεύγουν εκείνες που αποφέρουν δυσαρέσκεια, τιμωρία ή κόστος σε κόπο, χρόνο, χρήμα. Έτσι μαθαίνουν από τις προγενέστερες εμπειρίες τους, και αν το λάβουμε αυτό υπόψη μπορούμε να ερμηνεύσουμε τη συμπεριφορά τους.

Αργότερα ο Homans αναγνώρισε και το γεγονός ότι, όχι μόνο οι ανταμοιβές και οι ποινές αποτελούν ορθολογικά κίνητρα της ατομικής συμπεριφοράς αλλά και η υπόσχεση (πιθανότητα) ανταμοιβής ή η απειλή τιμωρίας λειτουργούν ως κίνητρα εξίσου ενισχυτικά ή αποτρεπτικά.

Βασική παραδοχή στη θεωρία της ορθολογικής δραστηριότητας είναι ότι τα σύνθετα κοινωνικά φαινόμενα ερμηνεύονται από τις επιμέρους ατομικές δράσεις από τις οποίες αποτελούνται. Έτσι η πιο στοιχειώδης μονάδα κοινωνικής ζωής είναι η ατομική συμπεριφορά και δράση. Οι κοινωνικοί θεσμοί και η κοινωνική αλλαγή εξηγούνται ως αποτέλεσμα της δράσης και της αλληλεπίδρασης μεταξύ των ατόμων. Δεν υπάρχει, για τον Homans ανεξαρτησία των κοινωνικών δομών, «η κοινωνία απλά έχει δημιουργηθεί από τον άνθρωπο και στην κοινωνία δεν υπάρχει κάτι άλλο εκτός από αυτά που βάζουν οι άνθρωποι σε αυτή»[52].

Ακόμα και σε πολύπλοκους θεσμούς και οργανισμούς η πολυπλοκότητα αυτή προκύπτει ως μια αλυσίδα διασυνδεδεμένων ατομικών δράσεων, ένα σύνολο άμεσων και έμμεσων ανταλλαγών που πραγματοποιούνται μεταξύ των ατόμων με κίνητρο το χρήμα και την κοινωνική αναγνώριση.

Κατά την αλληλεπίδραση μεταξύ των ατόμων παρατηρείται αμοιβαία ενίσχυση των συμπεριφορών. Κάθε μέρος "ανταμείβει ή τιμωρεί" τη συμπεριφορά του άλλου και έτσι μέσω της ανταλλαγής αμοιβών και ποινών οικοδομείται η κοινή τους συμπεριφορά και σχέση. Το όφελος που προκύπτει για το κάθε άτομο κατά την αλληλεπίδρασή του με ένα άλλο υπολογίζεται από τη διαφορά «ανταμοιβές (οφέλη) μείον κόστος (συνέπειες)». Η αμοιβαία ανταλλαγή θα συνεχίζεται για όσο διάστημα και τα δυο μέρη πραγματοποιούν «κέρδη». Όταν το ένα μέρος βρίσκει την αλληλεπίδραση αυτή περισσότερο επιζήμια παρά συμφέρουσα, τότε η αλληλεπίδραση δεν μπορεί να συνεχιστεί και θα αναζητηθούν εναλλακτικές αλληλεπιδράσεις που θα είναι πιθανότερα πιο επικερδείς.

Οι σχέσεις κοινωνικής ανταλλαγής μπορούν κάλλιστα να αποτελούν σχέσεις δύναμης και εξουσίας επειδή σπάνια τα δυο μέρη συμμετέχουν ισότιμα και συνεισφέρουν το ίδιο, με χρόνο, κόπο ή χρήμα, στην μεταξύ τους ανταλλαγή. Έτσι το αποτέλεσμα της συγκεκριμένης ανταλλαγής εξαρτάται από το συσχετισμό δυνάμεων μεταξύ των συμμετεχόντων μερών. Η διαπραγματευτική δύναμη του κάθε μέρους διαφέρει ανάλογα με το βαθμό εξάρτησής του από την ανταλλαγή αυτή και με το πλήθος των εναλλακτικών επιλογών που διαθέτει. Αν τα

[50] Emerson Richard M. (1976)

[51] Homans George (1961), σ. 13

[52] Homans George (1961), σ. 385

άτομα δεν διαθέτουν άλλες εναλλακτικές επιλογές ως μέσα για την επίτευξη των στόχων τους πλην της δεδομένης, τότε είναι άμεσα εξαρτώμενα από αυτή και δεν διαθέτουν ικανή δύναμη για να επηρεάσουν το «τίμημα» που θα κληθούν να πληρώσουν για τη συμμετοχή τους στη συγκεκριμένη σχέση. Έχουμε δηλαδή τη δημιουργία ενός μονοπωλίου, αν το δούμε με οικονομικούς όρους, όπου αυτό έχει την δύναμη να καθορίζει, όχι μόνο την «προσφερόμενη ποσότητα» του αγαθού, αλλά και την «τιμή» του. Όπως μάλιστα στις οικονομικές συναλλαγές παρατηρούνται συγκεκριμένες μορφές αγοράς, που εκτός από το μονοπώλιο περιλαμβάνουν το ολιγοπώλιο, τον πλήρη και τον ατελή ανταγωνισμό[53], έτσι και οι κοινωνικές ανταλλαγές, με βάση τη δύναμη των συμμετεχόντων ποικίλλουν στις παραπάνω μορφές.[54]

Ο Homans θεωρεί ότι ο πιο σημαντικός και γενικευμένος «ενισχυτής», που εφαρμόζεται σε πλήθος εξειδικευμένων περιπτώσεων είναι η επιδίωξη της «αποδοχής», της «επιδοκιμασίας» (approval). Μάλιστα συσχετίζει άμεσα την αποδοχή με το χρήμα επειδή και τα δυο αποτελούν γενικά μέσα «κοινωνικών ανταλλαγών» και το ένα, το χρήμα, μπορεί να οδηγεί στο άλλο την αποδοχή. Οι οικονομικές συναλλαγές για παράδειγμα που πραγματοποιούνται με την ανταλλαγή του χρήματος και αφορούν στην απόκτηση οικονομικών αγαθών, όπως ένα αυτοκίνητο, μπορεί να περιλαμβάνουν και κοινωνικές ανταλλαγές όπως η αναγνώριση και το γόητρο που μπορεί να απολαμβάνει ο αγοραστής από το κοινωνικό του περιβάλλον. Με παρόμοιο τρόπο ο εγκληματίας, π.χ. ο κλέφτης ενός αυτοκινήτου, εκτός από την ικανοποίηση που του δίνει η χρησιμοποίηση του αυτοκινήτου, μπορεί να απολαμβάνει και την αναγνώριση των άλλων κλεφτών ως ικανός και επιδέξιος κλέφτης. Εκτός όμως από το όφελος υπάρχει κάποιο κόστος και στις δυο περιπτώσεις δράσης. Για τον αγοραστή του αυτοκινήτου κόστος σημαίνει δαπάνη χρήματος, ενώ για τον κλέφτη μπορεί να συνεπάγεται ποινές και κοινωνική απαξίωση αν συλληφθεί και καταδικαστεί. Για το λόγο αυτό και οι δυο σταθμίζουν προηγουμένως λογικά τα υπέρ και τα κατά, τα οφέλη και τα κόστη από τη συγκεκριμένη δράση τους. Αν τα οφέλη (ικανοποίηση, χρησιμότητα αγαθού, αναγνώριση, δύναμη κλπ.) θα είναι μεγαλύτερα από τα κόστη (χρήμα, προσπάθεια, πιθανότητα τιμωρίας κλπ.), τότε η δράση είναι πιο πιθανή ενώ αν τα κόστη είναι μεγαλύτερα από τα αναμενόμενα οφέλη, τότε η δράση μπορεί να μεταφέρεται προς την κατεύθυνση εναλλακτικών επιλογών. [55]

2.2.2. Η οικονομική προσέγγιση του εγκλήματος από τον G.S. Becker

Ο οικονομολόγος Gary S. Becker ήταν από τους πρωτοπόρους που εφήρμοσε την μικρο-οικονομική ανάλυση στην ερμηνεία ευρύτερων ανθρώπινων δραστηριοτήτων, εκτός των οικονομικών, με το έργο του «Έγκλημα και Τιμωρία: Μια Οικονομική Προσέγγιση» που δημοσίευσε στο Journal of Political Economy το 1968 για το οποίο και βραβεύτηκε με νόμπελ οικονομίας.

---

[53] Οι *Μορφές αγοράς* είναι γνωστές από την Πολιτική Οικονομία:

1) Ο *Πλήρης ανταγωνισμός* που διαθέτει μεγάλο αριθμό επιχειρήσεων και αγοραστών ενώ το προϊόν θεωρείται ομοιογενές. Ομοιογενές είναι το προϊόν το οποίο ουσιαστικά δεν διαφέρει σε τίποτα, στα μάτια των αγοραστών, από κάποιο αντίστοιχο προϊόν που παράγουν άλλες επιχειρήσεις . Οι επιχειρήσεις από μόνες τους δεν μπορούν να επηρεάσουν την τιμή του προϊόντος.

2) το *Μονοπώλιο*, όπου υπάρχει μόνο μία επιχείρηση και μεγάλος αριθμός αγοραστών. Η επιχείρηση καθορίζει και την τιμή του προϊόντος.

3) ο *Μονοπωλιακός Ανταγωνισμός*: Υπάρχουν πολλές επιχειρήσεις και πολλοί αγοραστές ενώ το προϊόν θεωρείται διαφοροποιημένο.

4) το *Ολιγοπώλιο* όπου υπάρχουν λίγες επιχειρήσεις ενώ το προϊόν μπορεί να είναι είτε ομοιογενές είτε διαφοροποιημένο. Συνήθως υπάρχει μία μεγάλη, ηγετική επιχείρηση η οποία καθορίζει την τιμή.

[54] Scott John (2000)

[55] Scott John (2000)

Η έμπνευση του Becker προήλθε από μια προσωπική του εμπειρία, όταν ένα πρωί είχε καθυστερήσει για την εξέταση ενός φοιτητή, στο πανεπιστήμιο που εργαζόταν ως καθηγητής οικονομικών και δεν έβρισκε θέση να παρκάρει το αυτοκίνητο του. Τότε αναρωτήθηκε μήπως άξιζε τον κόπο να παρκάρει παράνομα και να πληρώσει την κλήση προκειμένου να μην καθυστερήσει. Έτσι συνέκρινε το αναμενόμενο όφελος που θα είχε μια τέτοια πράξη, την αποφυγή καθυστέρησης και συνακόλουθης δυσαρέσκειας από πλευράς των συναδέλφων του και του φοιτητή, την αποφυγή πληρωμής παρκινγκ κλπ., με το πιθανό κόστος της παρανομίας που θα διέπραττε παρκάροντας κοντά στο πανεπιστήμιο, σε σημείο όμως που δεν επιτρεπόταν. Το πιθανό αυτό κόστος υπολόγισε ως το γινόμενο κόστος κλήσης επί την πιθανότητα εντοπισμού. Τελικά αποφάσισε να το κάνει γιατί έκρινε ότι αυτό τον συνέφερε. Όταν εξέταζε τον φοιτητή του έθεσε μάλιστα το ίδιο πρόβλημα που είχε απασχολήσει κι εκείνον νωρίτερα, ο φοιτητές δεν απάντησε.[56] Πρόστιμο δεν πλήρωσε επειδή δεν υπήρχε κλήση στο αυτοκίνητό του, όμως το όφελος του Becker ήταν μεγαλύτερο. Η ιδέα του αυτή τον βοήθησε να δημοσιεύσει το παραπάνω έργο του (Έγκλημα και Τιμωρία: Μια Οικονομική Προσέγγιση).[57]

Ο Becker, όπως και οι υποστηρικτές της «Ορθολογικής Δραστηριότητας», εμπνευσμένος από την κλασική θεωρία και τα έργα του Beccaria [58] και του Bentham[59], δεν θεωρεί ότι οι εγκληματίες διαφέρουν σημαντικά ως προς τα κίνητρα της συμπεριφοράς τους από τα υπόλοιπα άτομα. Το έγκλημα μπορεί να μελετηθεί με όρους «ικανοποίησης – δυσαρέσκειας» ή όπως το εκφράζουν οι οικονομολόγοι με όρους «χρησιμότητας –κόστους».[60] Θεωρεί ότι και οι εγκληματίες λειτουργούν ορθολογικά όπως κάθε άλλο άτομο, όχι όμως με την καθαρά υλιστική έννοια αλλά ως ορθολογικά άτομα που, πριν προβούν στο συγκεκριμένο έγκλημα, εκτός από τα πιθανά κέρδη προϋπολογίζουν και τις πιθανότητες να συλληφθούν και να καταδικαστούν, όπως και τη βαρύτητα της ποινής ως πιθανό κόστος. Αν ο πιθανός δράστης θεωρήσει τις συνέπειες (κόστη) του εγκλήματος μεγαλύτερες από τα αναμενόμενα κέρδη, την πράξη υπερβολικά ριψοκίνδυνη, τα κέρδη υπερβολικά μικρά και τα αναμενόμενα οφέλη από μια νόμιμη δραστηριότητα - ως εναλλακτική της παράνομης - μεγαλύτερα, το πιθανότερο είναι να μην διαπράξει το έγκλημα. Αντίθετα, αν το προσδοκώμενο κέρδος από το έγκλημα είναι υψηλότερο από αυτό της νόμιμης εργασίας, τότε αυτό αποτελεί την προσφορότερη εναλλακτική που διαθέτει και θα προβεί στην τέλεση της πράξης.[61]

Το μέγεθος της εγκληματικής δραστηριότητας δεν εξαρτάται μόνο από την ορθολογικότητα και τις επιθυμίες του πιθανού δράστη αλλά και από τις κοινωνικο-οικονομικές συνθήκες που δημιουργούνται από την αντεγκληματική πολιτική (όπως οι δαπάνες για αστυνόμευση, οι επιβαλλόμενες ποινές) και από τις ευκαιρίες για απασχόληση και εκπαίδευση, στοιχεία που ο G.Becker θεωρεί ουσιώδη στην οικονομική προσέγγιση του εγκλήματος.

Ο G.Becker εστιάζει την ανάλυσή του όχι μόνο στον ορθολογικό δράστη αλλά και στην «ορθολογική κοινωνία», η οποία επίσης (πρέπει να) υπολογίζει τα κόστη και τα οφέλη από την καταπολέμηση του εγκλήματος. Ξεκινά τη δημοσίευσή του με τη διαπίστωση ότι, εφόσον

[56] Becker Gary S. (1993), σσ. 385-409
[57] Χατζής Αριστείδης (2010), σσ. 455-467
[58] Βλ. Beccaria, Cesare (1986)
[59] Βλ. Bentham, Jeremy (1931)
[60] Jeffery C. Ray & Zahm Diane L. (2008), σ.335
[61] Becker Gary S. (1993), ό.π.

η υπακοή στους κανόνες δικαίου δεν είναι αυτονόητη, είναι απαραίτητη η διάθεση κεφαλαίων – ιδιωτικών και δημόσιων – για την πρόληψη του εγκλήματος αλλά και τη σύλληψη των εγκληματιών.[62]

Η κοινωνία πρέπει να καταπολεμά το έγκλημα μέχρι το σημείο όπου το κοινωνικό κόστος της καταπολέμησης δεν υπερβαίνει το κοινωνικό όφελος από την καταπολέμηση αυτή. Χρησιμοποιεί σαν παράδειγμα την ποινικοποίηση των ναρκωτικών, ότι αυτή δεν συμφέρει την κοινωνία επειδή οι φυλακές έχουν υπερπληθυσμό κρατουμένων για ναρκωτικά. Η κοινωνία πληρώνει υπερβολικό κόστος για τη σύλληψη, την καταδίκη και τη φυλάκιση ατόμων για παράβαση των νόμων περί ναρκωτικών, σε σχέση με το όφελος που αποκομίζει και αφού δεν αξίζει τον κόπο προτείνει την αποποινικοποίηση.[63]

Τα συνολικά δημόσια έξοδα για την καταπολέμηση του εγκλήματος μπορούν να μειωθούν, ενώ οι αναμενόμενες ποινές μένουν σταθερές, με τη μείωση των εξόδων σύλληψης των δραστών και την παράλληλη αύξηση του μεγέθους των ποινών για όσους τελικά καταδικάζονται. Οι πιο ριψοκίνδυνοι παραβάτες όμως αποθαρρύνονται περισσότερο από την μεγαλύτερη πιθανότητα σύλληψης και καταδίκης παρά από την μεγαλύτερη αυστηρότητα των ποινών. Αυτό η πολιτεία θα πρέπει να το λάβει υπόψη προκειμένου να πετύχει τα καλύτερα δυνατά αποτελέσματα. [64]

Ο Becker προτείνει την εφαρμογή της ίδιας οικονομικής προσέγγισης για τη μελέτη της επιβολής του οποιουδήποτε νόμου όπως την εφαρμογή της εργατικής νομοθεσίας, τους νόμους για τη μόλυνση της ατμόσφαιρας, την παραβίαση ασφάλειας, το εμπορικό δίκαιο, το φορολογικό κλπ. Πράγματι η οικονομική προσέγγιση του εγκλήματος έχει χρησιμοποιηθεί από την αμερικάνικη Επιτροπή για τις ποινές[65] για τη θέσπιση κανονισμών που ακολουθούν οι δικαστές κατά την καταδίκη κατηγορουμένων για διάφορα ομοσπονδιακά αδικήματα.

Όσον αφορά το είδος των ποινών, τα χρηματικά πρόστιμα είναι προτιμότερα από τις ποινές φυλάκισης ή άλλες μορφές ποινών, αποτρέπουν περισσότερο τους εγκληματίες επειδή τους δημιουργούν κόστος, το οποίο μάλιστα αποτελεί έσοδο για την πολιτεία. Έτσι προτείνει την, κατά το δυνατόν μεγαλύτερη, αντικατάσταση των ποινών φυλάκισης με χρηματικά πρόστιμα ανάλογα με το μέγεθος της ζημίας που ο δράστης προκαλεί στην κοινωνία. Αρκεί βέβαια αυτός να έχει την οικονομική δυνατότητα να πληρώσει και το μέγεθος της ζημιάς να είναι μετρήσιμο με χρηματικούς όρους και όχι ανυπολόγιστο, όπως θα ήταν στις περιπτώσεις των ανθρωποκτονιών.

Το πρόστιμο, σύμφωνα με τον G.Becker, έχει πολλά πλεονεκτήματα αν ο εγκληματίας αποζημιώσει χρηματικά την κοινωνία γιατί τότε εκείνη ικανοποιείται έχοντας αντισταθμιστικά οφέλη. Αντίθετα, αν ο εγκληματίας καταδικαστεί σε ποινή φυλάκισης και οι δυο πλευρές έχουν απώλεια: ο εγκληματίας χάνει την ελευθερία του και η κοινωνία δαπανά χρήματα για φυλακές και για την μεταχείριση του εγκληματία. Η φυλάκιση θα πρέπει να είναι το έσχατο σωφρονιστικό μέτρο, όταν δεν υπάρχει άλλη δυνατότητα ποινής, γιατί πολύ απλά αυτή κοστίζει στην κοινωνία πολύ παραπάνω.[66] Ακόμα η καταδίκη σε ποινή φυλάκισης συχνά δεν είναι από μόνη της αρκετή και επιβάλλονται συμπληρωματικές ποινές.

[62] Becker, Gary S. (1968), σσ. 169-217
[63] Bahrani Mahmoud (2012)
[64] Becker Gary.S. (1993), ό.π.
[65] The U.S. Sentencing Commission
[66] Bahrani Mahmoud., ό.π.

Έτσι το ερώτημα που τίθεται από τον Becker – και που αποτελεί τον κεντρικό σκοπό του άρθρου του- είναι «πόσα (χρηματικά) κεφάλαια να χρησιμοποιηθούν και πόσες ποινές να καταλογιστούν προκειμένου να επιβληθούν οι κανόνες δικαίου της κοινωνίας» ή διαφορετικά «πόσο έγκλημα μπορεί να επιτραπεί και πόσοι δράστες μπορούν να αφεθούν ατιμώρητοι»;[67] Ριζοσπαστική, στο ζήτημα αυτό είναι η άποψη του G.Becker για το αν η κοινωνία μπορεί να εξαλείψει εντελώς το έγκλημα, επειδή η κοινωνία δεν αντέχει οικονομικά (και όχι μόνο) και δεν μπορεί να εξαλείψει πλήρως την εγκληματικότητα. Θεωρεί ότι κάτι τέτοιο μπορεί να είναι πιθανό, δεν είμαστε όμως καθόλου σίγουροι ότι αυτό είναι και επιθυμητό, γιατί υπάρχει ένα άριστο επίπεδο εγκλήματος, το μέγεθος του οποίου η κοινωνία θέλει, μπορεί και συμφέρει να καταπολεμήσει. Η περαιτέρω καταπολέμηση, μετά από αυτό το επίπεδο, αποβαίνει πολύ ασύμφορη για την κοινωνία, γιατί θα πρέπει να επιβάλλει πολύ αυστηρότερες ποινές, όχι μόνο χρηματικές αλλά και ποινές φυλάκισης. Αυτό θα καθιστούσε την εξάλειψη της εγκληματικότητας υπερβολικά δαπανηρή, όχι μόνο χρηματικά αλλά και σε όρους κοινωνικού κόστους. Για παράδειγμα, ο G.Becker χρησιμοποιεί την κομμουνιστική Κίνα, όπου το έγκλημα είναι σε πολύ περιορισμένη κλίμακα, όμως εκεί η κυβέρνηση έχει θεσπίσει αυστηρότατες ποινές και αυστηρούς περιορισμούς στην ιδιωτική ζωή με αποτέλεσμα να μην είναι ανεκτή μια τέτοια μορφή κοινωνίας. Έτσι θα πρέπει να σταθμιστούν τα υπέρ και τα κατά, οι ωφέλειες και οι ζημίες και από πλευράς κοινωνίας.

Τα οικονομικά μαθηματικά του G.S.Becker

Ο Becker πρότεινε ένα μοντέλο με μαθηματικούς τύπους, με βάση τους οποίους μπορεί να υπολογιστεί το Αναμενόμενο Κόστος του εγκλήματος δηλαδή η κοινωνική βλάβη από το έγκλημα, οι δαπάνες σε οικονομικά κεφάλαια και οι ποινές για την ελαχιστοποίηση των κοινωνικών ζημιών.

Το έγκλημα, σύμφωνα με τον G. Becker, παρά το ότι αποτελεί μια σημαντικότατη οικονομική δραστηριότητα ή «βιομηχανία» είχε, μέχρι τότε, διαλάθει της προσοχής των οικονομολόγων. Ο Becker χρησιμοποίησε μια έκθεση της αμερικάνικης «Επιτροπής για το Έγκλημα», σύμφωνα με την οποία το οικονομικό κόστος του εγκλήματος, στις ΗΠΑ κατά το 1965, υπολογίστηκε στα περίπου 21 δις δολάρια ή πάνω από 4% του αμερικανικού ΑΕΠ (βλ. Πίνακα 1), για να ποσοτικοποιήσει τη σχέση μεταξύ αριθμού τελεσθέντων εγκλημάτων και του οικονομικού κόστους του εγκλήματος και να παραστήσει τη σχέση αυτή με μαθηματικούς τύπους. [68]

ΠΙΝΑΚΑΣ 1
ΟΙΚΟΝΟΜΙΚΟ ΚΟΣΤΟΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ [69]

ΕΙΔΟΣ ΕΓΚΛΗΜΑΤΟΣ	ΚΟΣΤΟΣ (εκατ. Δολ.)
Εγκλήματα κατά προσώπων	**815**
Εγκλήματα κατά περιουσίας	**3,932**
Παράνομα αγαθά και υπηρεσίες	**8,075**

[67] Becker Gary (1968), σ.σ.169-217
[68] Becker Gary (1968), ό.π.
[69] Είναι ο πίνακας που χρησιμοποίησε ο Becker για να στηρίξει τις απόψεις του, από την President's Commission (1967d, σ. 44) βλ. Becker Gary (1968), σ.171

Άλλα εγκλήματα	**2,036**
Σύνολο	**14,858**
Δημόσιες δαπάνες για αστυνομία, ποινικές διώξεις και δικαστήρια.	**3,178**
Δημόσιες δαπάνες για Φυλακές	**1,034**
Ιδιωτικές δαπάνες για την αντιμετώπιση του εγκλήματος	**1,910**
Γενικό Σύνολο	**20,980**

Το μοντέλο του Becker περιλαμβάνει μεταβλητές και δείκτες όπως η σχέση ανάμεσα στον αριθμό:

Α. των τελεσθέντων εγκλημάτων και το κόστος από αυτά.

Β. των τελεσθέντων εγκλημάτων και των ποινών που επιβάλλονται σε αυτά.

Γ. των τελεσθέντων εγκλημάτων, των συλλήψεων, των καταδικών και των δημόσιων δαπανών για αστυνομία και δικαστήρια.

Δ. των καταδικών και του κόστους για φυλακές ή για εναλλακτικές μορφές ποινής.

Ε. των τελεσθέντων εγκλημάτων και την ιδιωτική δαπάνη για μέτρα προστασίας.[70]

Το κίνητρο της πολιτείας, για την ποινικοποίηση κάποιων συμπεριφορών και την καταπολέμηση του εγκλήματος, είναι η αποτροπή της Ζημίας/Βλάβης στα μέλη της κοινωνίας από τέτοιες συμπεριφορές. Η Ζημία (Ζ) αυτή είναι συνάρτηση του επιπέδου της παράνομης Δραστηριότητας (Δ):

$$Z = f(\Delta)$$

Δηλαδή όσο αυξάνει το επίπεδο της παράνομης Δραστηριότητας (Δ), τόσο αυξάνει το μέγεθος της βλάβης που προκαλείται στο κοινωνικό σύνολο (Ζ).

Η Οριακή Ζημία (Ο.Ζ.) είναι η επιπλέον ζημία (dZ) που προκύπτει για το κοινωνικό σύνολο από την επιπλέον αύξηση της παράνομης Δραστηριότητας κατά μια μονάδα (dΔ):

$$\mathbf{O.Z} = \frac{\mathbf{DZ}}{\mathbf{D\Delta}} \mathbf{> 0}$$

Το Όφελος (Ο) είναι επίσης συνάρτηση του επιπέδου της παράνομης Δραστηριότητας (Δ) που σημαίνει ότι το όφελος αυξάνεται ανάλογα:

$$\mathbf{O = f(\Delta)}$$

Αντίστοιχα το Οριακό όφελος (Ο.Ο) θα είναι το επιπλέον όφελος από την επιπλέον αύξηση της παράνομης Δράσης κατά μια μονάδα:

$$\mathbf{O.O} = \frac{\mathbf{dO}}{\mathbf{d\Delta}} \mathbf{> 0}$$

Η διαφορά μεταξύ Οφέλους και Κόστους μας δίνει το καθαρό κέρδος ή τη καθαρή ζημία (Κ):

$$\mathbf{K = O - Z}$$

Από ένα επίπεδο και έπειτα η επιπλέον αύξηση της παράνομης Δραστηριότητας επιφέρει ολοένα μειούμενα οριακά οφέλη για τον εγκληματία και αυξανόμενη οριακή ζημία για την κοινωνία.

[70] Becker Gary (1968), ό.π.

Με καθαρά οικονομολογικούς όρους, η κοινωνία θα πρέπει να καταπολεμά το έγκλημα για όσο διάστημα το οριακό όφελος από τη μείωση της εγκληματικότητας κατά μια μονάδα υπερβαίνει το αντίστοιχο κόστος.[71]

Το άριστο (αποτελεσματικό) μέγεθος αντεγκληματικής πολιτικής, που θα πρέπει να εφαρμοστεί για την αντιμετώπιση των συνεπειών τους εγκλήματος εξαρτάται, μεταξύ άλλων και από το κόστος σύλληψης και καταδίκης των δραστών, το είδος των ποινών που επιβάλλονται (φυλάκιση ή πρόστιμα).[72]

Η άποψη του G.Becker, για την εγκληματική συμπεριφορά από τη σκοπιά της κλασικής οικονομικής θεωρίας, ακολουθήθηκε και από άλλες μελέτες που είχαν ως συνισταμένη ότι η συμπεριφορά του ατόμου είναι ορθολογική και ως εκ τούτου η κοινωνία πρέπει να απαντήσει με μέτρα καταστολής όπως περισσότερες ποινές και φυλακές. [73]

Η Εθνική Ακαδημία Επιστημονικών Επιτροπών για την Επανένταξη, εξετάζοντας αυτές τις οπτικές, για περισσότερη καταστολή, κατέληξε στο συμπέρασμα ότι είναι προτιμότερο να εφαρμόζονται θεραπευτικά και βελτιωτικά προγράμματα για επαγγελματική κατάρτιση και καλύτερες επαγγελματικές ευκαιρίες.[74]

Ο James Coleman βρίσκει σημαντική ανεπάρκεια στην άμεση εφαρμογή της – οικονομικού τύπου – ορθολογικής επιλογής, για τους κοινωνικούς δρώντες.

Η ***κριτική*** που ασκήθηκε στην οικονομίστικη αντίληψη της θεωρίας της Ορθολογικής δράσης συνοψίζεται στο ότι δεν εξηγεί:

- τη συλλογική συμπεριφορά, αλλά μόνο την ατομική.
- την επίδραση των κοινωνικών αξιών όπως η εμπιστοσύνη, η φιλαλληλία και η αμοιβαιότητα στη δράση των ατόμων.
- το πώς θα γνωρίζουμε αν ο πιθανός δράστης είχε, κατά τη στιγμή της απόφασης, επαρκείς και ακριβείς πληροφορίες για την εκτίμηση του αποτελέσματος της πράξης του, ώστε να τις λάβουμε υπόψη στο αν αυτός έκανε την επεξεργασία των πληροφοριών του με τον πιο αποτελεσματικό – ορθολογικό τρόπο. Έρευνες, όπως των Carroll και Weaver 1986, δείχνουν ότι πολλοί δράστες δεν είναι καθόλου σίγουροι για τις πιθανότητες σύλληψης ή και καταδίκης αν συλληφθούν.
- αν οι έννοιες της ορθολογικής και της συνειδητής επιλογής μας δίνουν ξεκάθαρα τα χαρακτηριστικά του γεγονότος, του τι συμβαίνει κατά τη στιγμή της διάπραξης του εγκλήματος.
- το πώς θα μπορούσαμε να κάνουμε πιο σαφείς προβλέψεις για το εγκληματικό συμβάν και το πώς θα μπορούσαμε να το αποτρέψουμε αυτό.[75]

Η απάντηση που δίνουν οι θεωρητικοί της Ορθολογικής δράσης στις κριτικές αυτές είναι ότι η δράση των ατόμων γίνεται με σκοπό την επιδίωξη του ατομικού τους συμφέροντος, ακόμα και όταν επιλέγουν να βοηθήσουν κάποιον ή στην περίπτωση άλλων αξιών, ότι απλά είναι υποχρεωμένα να δράσουν με βάση αυτές.[76]

[71] Bahrani Mahmoud., ό.π.

[72] Becker, Gary S. (1968), ό.π.

[73] Βλ. Jeffery C. Ray & Zahm Diane L. (2008), σ.335 αναφορά στους Philips and Votey 1981, Adreano and Siegfried 1980, Witte 1980, Rottenberg 1973

[74] Jeffery C. Ray & Zahm Diane L. (2008), σ.335

[75] Trasler Gordon (2008), σ.305

[76] Scott John (2000)

Το οικονομίστικο σχήμα του G.Becker γνώρισε κριτική και από τους Clarke και Felson, οι οποίοι επιχείρησαν το συνδυασμό της ορθολογικής επιλογής με τις καθημερινές δραστηριότητες, όπως και με άλλες θεωρίες.

Τα βασικά σημεία της κριτικής των Clarke και Felson είναι τα εξής:

- Δόθηκε έμφαση στα υλικά και χρηματικά στοιχεία των ωφελειών σε βάρος των μη υλικών, όπως η αναγνώριση, η εξουσία κλπ.
- Τα διαφορετικά είδη εγκλημάτων λαμβάνονται υπόψη ως μια και μόνη μεταβλητή στις μαθηματικού τύπου εξισώσεις.
- Δεν λαμβάνεται υπόψη η ευκολία με την οποία οι εγκληματίες αποφεύγουν τη σύλληψη και η δυσκολία της κοινωνίας να επιβάλλει ποινές.
- Η μαθηματικοποίηση της εγκληματικής συμπεριφοράς από τους οικονομολόγους απαιτεί δεδομένα που δεν είναι διαθέσιμα ή είναι αποτέλεσμα, συχνά αυθαίρετων, υποθέσεων.
- Με το να θεωρείται το έγκλημα ως αποκλειστικά υπολογιστική πράξη παραγνωρίζεται η ευκαιριακή δομή και ο αυθορμητισμός που παρατηρούνται σε πολλά είδη εγκλήματος, δηλ. το γεγονός ότι πολλά εγκλήματα γίνονται στο πλαίσιο της νόμιμης εργασίας κάποιου ο οποίος εκμεταλλεύεται την εργασία αυτή για να ανακαλύψει κατάλληλες ευκαιρίες για διάπραξη παράνομων δραστηριοτήτων.[77]
- Το οικονομικό μοντέλο προσφοράς – ζήτησης δεν έχει απόλυτη εφαρμογή, γιατί ενώ υπάρχει προσφορά θυμάτων, δεν υπάρχει ζήτηση από τα θύματα για να θυματοποιηθούν.
- Το απόλυτα ορθολογικό, οικονομικό μοντέλο μεγιστοποίησης του οφέλους δεν μπορεί να εφαρμοστεί στις περιπτώσεις των παρορμητικών και παθολογικών εγκλημάτων.[78]

Προτάθηκαν έτσι διάφορες επεκτάσεις και τροποποιήσεις των ορθολογικών επιλογών, ειδικά για να μπορέσει να γίνει εφαρμογή στην πρόληψη του εγκλήματος από τους Clarke και Felson που θα εξετάσουμε παρακάτω.

2.3. Οι θεωρίες που εξετάζουν το ρόλο των «εγκληματικών ευκαιριών» από την οπτική της περιβαλλοντικής εγκληματολογίας

Η περιβαλλοντική εγκληματολογία εστιάζει στον τόπο και στον τρόπο που τα άτομα και οι οργανώσεις οργανώνουν τις δραστηριότητές τους και πώς αυτές οι ενέργειες επηρεάζονται από τους χωροταξικούς παράγοντες. Η περιβαλλοντική εγκληματολογία αποτελεί κλάδο της εγκληματολογίας που αντλεί τις βασικές της θεωρητικές παραδοχές, για τη μελέτη του εγκλήματος, της εγκληματικότητας και της θυματοποίησης, από την ανθρωπο-οικολογία.[79]

Η ανθρώπινη οικολογία αφορά τη μελέτη των αλληλεπιδράσεων ανάμεσα στον ανθρώπινο πληθυσμό και τα φυσικά, τα πολιτισμικά και τα κοινωνικά χαρακτηριστικά του περιβάλλοντός του. Ο όρος «ανθρώπινη οικολογία» πρωτο-χρησιμοποιήθηκε από τους Robert Park & Ernest Burgess το 1921 στο έργο τους «An Introduction to the Science of Sociology». Εκεί όρισαν την ανθρώπινη οικολογία (human ecology) ως «τη μελέτη της οργάνωσης του χώρου και του χρόνου των ανθρώπων σε σχέση με τις επιλεκτικές και οικιστικές δυνάμεις του

[77] Clarke Ronald V. (1995), σσ. 91-150

[78] Clarke Ronald V. & Felson Marcus (2008), σ.5

[79] Bottoms Antony & Wiles Paul (2002), σ. *620*

περιβάλλοντος». Σε αντιστοιχία με την «φυσική» οικολογία, η ανθρωπο-οικολογία χρησιμοποιείται για να εξηγήσει το ρόλο των βιοτικών παραγόντων για την κοινωνική οργάνωση και τη χωροταξική κατανομή των ανθρώπινων ομάδων. Στη θέση του όρου περιβάλλον προτιμάται η έννοια «χώρος».[80]

Η περιβαλλοντική εγκληματολογία τονίζει ότι η γεωγραφική κατανομή των παραβάσεων, της θυματοποίησης και της κατοικίας των δραστών δεν είναι τυχαία. Η συγκέντρωση του εγκλήματος και της εγκληματικότητας στο χώρο σχετίζεται με εγκληματολογικά δεδομένα, όπως το γεγονός ότι ένας σχετικά μικρός αριθμός παραβατών ευθύνεται για τη διάπραξη ενός δυσανάλογα μεγάλου αριθμού εγκλημάτων[81.]

Το γεγονός ότι η περιβαλλοντική εγκληματολογία δημιουργήθηκε το δέκατο ένατο αιώνα, των μεγάλων τεχνολογικών και κοινωνικο-οικονομικών αλλαγών, της εκβιομηχάνισης και της αστικοποίησης δεν αποτελεί σύμπτωση. Το εγκληματικό φαινόμενο συνδέθηκε, από πολλούς ερευνητές, με αυτές τις αλλαγές.[82]

Η διάπραξη των εγκλημάτων, συχνά διευκολύνεται από τις **ευκαιρίες** που μπορεί να παρέχει ένα περιβάλλον. Πολλά από τα εγκλήματα, μεταξύ αυτών και τα μη βίαια οικονομικά και ηλεκτρονικά εγκλήματα, τελούνται λόγω της ύπαρξης των κατάλληλων ευκαιριών που παρουσιάζονται όταν ένας πρόθυμος δράστης συναντήσει σε χώρο και χρόνο ένα κατάλληλο στόχο και αποφασίζει να τον «πλήξει» στο πλαίσιο των, κατά τα άλλα νόμιμων, συνηθισμένων δραστηριοτήτων της επαγγελματικής ή μη απασχόλησης του.

Κατά τη δεκαετία του ’60 αναπτύχθηκαν θεωρίες όπως αυτή «των ευκαιριών» (opportunity theory) από τους Richard Cloward και Lloyd Ohlin η οποία έχει ως βάση τις θεωρίες πίεσης (strain theory) που εμπνεύστηκε ο Robert Merton από το έργο του Emile Durkheim.[83]

Τη δεκαετία του ‘70 αναπτύχθηκαν νεοπαγείς θεωρίες, στο πλαίσιο της ευρύτερης περιβαλλοντικής εγκληματολογικής προσέγγισης, βασισμένες σε απλές παραδοχές, αρχές που πηγάζουν από το παλιό σχήμα: «η ευκαιρία κάνει την κλέφτη»[84]. Οι θεωρίες αυτές αντλούν βάσεις τόσο από το νεοκλασικισμό (την κοινωνική ανταλλαγή, την ορθολογική επιλογή), όσο και από το θετικισμό της (πρώτης) οικολογικής σχολής του Σικάγου, από το διαφορικό συγχρωτισμό και το έγκλημα του λευκού περιλαιμίου που ανέπτυξε ο Sutherland, από την αρχική θεωρία των εγκληματικών ευκαιριών των Cloward και Ohlin και την «ανθρώπινη οικολογία» του Amos Hawley.[85] Ανασύρθηκαν θεωρίες, όπως του Beccaria για την «ελεύθερη βούληση και επιλογή» ή ο *ωφελιμισμός* του Bentham, οι οποίες συνδυάστηκαν με τις νέες προσεγγίσεις, από το χώρο της περιβαλλοντικής εγκληματολογίας και δομήθηκαν οι πιο σύγχρονες θεωρητικές προσεγγίσεις που χρησιμεύουν και για την προσέγγιση των οικονομικών και ηλεκτρονικών εγκλημάτων.

Στη σύγχρονη οικολογική θεωρία αναπτύχθηκε η τάση της *Περιεκτικής ή Ολοκληρωμένης* Οικολογίας (integrative ecology) που αποτελεί μια προσπάθεια να ενσωματωθούν σε ένα ενιαίο θεωρητικό πλαίσιο στοιχεία από τις θεωρίες της κοινωνικής μάθησης, της

[80] Roderick J. Lawrence (2001)
[81] Bottoms Antony & Wiles Paul (2002), σ. 620
[82] Bottoms A. and Wiles P. (2002), σ. 621
[83] Parsi Boetig, Brian R. (2004)
[84] Felson, Marus. & Clarke, Roland.V. (1998)
[85] Goldstein Arnold P. (1994), σσ.52-53

ορθολογικής επιλογής και από τις πολιτισμικές θεωρίες[86]. Οι απαρχές αυτής της θεωρητικής τάσης στην οικολογία βρίσκονται στην εξελικτική οικολογική θεωρία των Lawrence Cohen και Richard Machalek, την οποία επέκτεινε έπειτα ο Bryan Vila (1994). Η εστίαση εδώ είναι στην ανθρώπινη προσαρμογή στο περιβάλλον με την ιδιαίτερη μελέτη των πολιτιστικών γνωρισμάτων που βασίζονται στις κοινωνικά αποκτημένες γνώσεις και συμπεριφορές. Αυτή η προσέγγιση επιτρέπει στους εγκληματολόγους να «ενσωματώσουν στη μελέτη τους οικολογικούς παράγοντες που καθορίζουν το ποιες ακριβώς ευκαιρίες υπάρχουν για το έγκλημα, τους παράγοντες εκείνους που, σε μικρο-επίπεδο, επηρεάζουν τη διάπραξη μιας εγκληματικής πράξης σε μια συγκεκριμένη χρονική στιγμή και εκείνους τους παράγοντες που, σε μακρο-επίπεδο, επηρεάζουν την ανάπτυξη των ατόμων στην κοινωνία κατά τη διάρκεια του χρόνου»[87].

Οι πιο σύγχρονες θεωρίες της περιβαλλοντικής εγκληματολογίας (environmental criminology), που εξετάζονται παρακάτω, απέσυραν το ενδιαφέρον των κοινωνικών επιστημόνων από τους εγκληματογόνους παράγοντες που δημιουργούν οι κοινωνικές συνθήκες, όπως η φτώχεια, η ανεργία, το εκπαιδευτικό επίπεδο κλπ. και εστίασαν περισσότερο στις ευκαιρίες που δίνονται στον παραβάτη για να βελτιώσει την προσωπική του κατάσταση δραστηριοποιούμενος με βάση τις (ορθο)λογικές εναλλακτικές επιλογές που του παρουσιάζονται. Έτσι, από τη δεκαετία του ’70 η περιβαλλοντική εγκληματολογία περιλαμβάνει ένα σύνολο από θεωρίες που έχουν ως κοινό στοιχείο ότι εστιάζουν στο εγκληματικό γεγονός, στις εγκληματικές **ευκαιρίες**, στις περιστασιακές συνθήκες που αξιολογούνται από τους πιθανούς δράστες και στα ιδιαίτερα χαρακτηριστικά του περιβάλλοντος στο οποίο αυτό διαδραματίζεται. Για το λόγο αυτό οι θεωρίες αυτές ονομάζονται, από θεωρητικούς όπως ο Clarke[88], οι Brantigham[89], οι Benson, Madensen & Eck[90] και άλλοι, θεωρίες των **«εγκληματικών ευκαιριών».**

Το εγκληματικό γεγονός πρέπει να εξετάζεται ως το αποτέλεσμα της αλληλεπίδρασης των δραστών, των θυμάτων ή στόχων και του νόμου στο πλαίσιο συγκεκριμένου σκηνικού σε συγκεκριμένο τόπο και χρόνο. Έτσι κάποιοι «περιβαλλοντικοί εγκληματολόγοι»[91] στράφηκαν στην εξέταση του φυσικού και του δομημένου περιβάλλοντος - εκτός από του κοινωνικού- και της επίδρασής του στους χώρους του εγκλήματος όπως και την κατανομή του σε αυτούς. Απέσυραν την προσοχή από τους εγκληματογόνους παράγοντες, θεώρησαν τα εγκληματικά κίνητρα ως δεδομένα και εστίασαν στο εγκληματικό γεγονός καθεαυτό[92], στις συνθήκες, τα πρότυπα (patterns) τέλεσης του εγκλήματος[93], στο πώς και όχι το γιατί[94].

Η παραδοσιακή εγκληματολογία εστιάζει στην εγκληματικότητα και τους βιολογικούς, ψυχολογικούς ή και κοινωνικούς παράγοντες που επηρεάζουν τη δημιουργία του εγκληματία. Τα μέτρα αντιμετώπισης στοχεύουν στην μεταχείριση και «θεραπεία» του εγκληματία με την απομάκρυνση των εγκληματογόνων παραγόντων και την εφαρμογή

[86] Lanier M.M. & Henry S. (1994), σ. 199

[87] Vila Bryan (1994), σσ. 311-351

[88] Clarke Roland (1995)

[89] Brantigham Patricia L. & Brantigham Paul J. (2008), σ.260

[90] Benson, Michael,. Madensen Tamara D, &. Eck John E (2009)

[91] Βλ. Felson, Cohen, Cornish, Clarke, Brantingham P. L. & Brantingham P., Benson, et.al, όπου εξετάζονται αναλυτικότερα παρακάτω.

[92] Brantigham Patricia L. & Brantigham Paul J. (2008), σ.260

[93] Brantigham Patricia L. & Brantigham Paul J. (2008), ό.π.

[94] Benson, Michael,. Madensen Tamara D, &. Eck John E (2009)

προγραμμάτων επανένταξης. Η περιβαλλοντική εγκληματολογία έχει αντικείμενο το «έγκλημα» ως γεγονός, ενώ ο «εγκληματίας» αποτελεί απλά ένα από τα στοιχεία που συμμετέχουν στο εγκληματικό γεγονός.

Οι εγκληματολόγοι που υιοθετούν την νεότερη οπτική της περιβαλλοντικής εγκληματολογίας προσπαθούν να ανακαλύψουν εγκληματικά πρότυπα (επαναλαμβανόμενα μοτίβα) τα οποία ερμηνεύονται με αναφορά τις περιβαλλοντικές και περιστασιακές συνθήκες. Μέσα από τη σκιαγράφηση των προτύπων του εγκλήματος προκύπτουν και οι στρατηγικές αντιμετώπισης οι οποίες εστιάζουν στην πρόληψη του εγκλήματος παρά στην μεταχείριση του εγκληματία.

Οι βασικές παραδοχές της περιβαλλοντικής εγκληματολογίας είναι:

- Η εγκληματική συμπεριφορά επηρεάζεται από το πώς το άτομο αλληλεπιδρά με το άμεσο περιβάλλον του.
- Η κατανομή του εγκλήματος στο χώρο και το χρόνο δεν είναι τυχαία αλλά το έγκλημα τείνει να συγκεντρώνεται σε περιβάλλοντα - σε χώρους και χρόνο - που παρουσιάζουν εγκληματικές ευκαιρίες και διευκολύνουν την διάπραξη του εγκλήματος.
- Η γνώση των εγκληματογόνων παραγόντων, των εγκληματικών προτύπων επιτρέπει την ανάπτυξη αποτελεσματικών μεθόδων αποτροπής του εγκλήματος μέσω της αλλοίωσης της εγκληματικής ευκαιρίας εστιάζοντας σε συγκεκριμένα μέρη και σε συγκεκριμένο χρόνο.[95]

Οι σύγχρονες θεωρήσεις στο πλαίσιο της περιβαλλοντικής εγκληματολογίας επιχειρούν συνθετικές προσεγγίσεις των κεντρικών θεωριών, όπως της ορθολογικής επιλογής (των Clarke και Cornish)[96], των «καθημερινών δραστηριοτήτων» (των Cohen και Felson), των εγκληματικών προτύπων» (των Brantingham και Brantingham[97]) συνδυάζοντάς τις υπό το πρίσμα των «εγκληματικών ευκαιριών»[98] και της στρατηγικής «περιστασιακής πρόληψης του εγκλήματος» (του Jeffery στις ΗΠΑ[99] και του Clarke[100] στο Η.Β.) μέσω του κατάλληλου περιβαλλοντικού σχεδιασμού.

Ειδικότερα, η νέα αντίληψη στην περιβαλλοντική εγκληματολογία εξετάζει τα χωροταξικά πρότυπα του εγκλήματος, τις διαδικασίες με τις οποίες οι πιθανοί δράστες αναγνωρίζουν τους πιθανούς στόχους-χώρους και τις ευκαιρίες για δράση ως αποτέλεσμα μιας πολυεπίπεδης διαδικασίας λήψης της (ορθολογικής) απόφασης.[101] Στο πλαίσιο αυτό εντάσσεται και η αντιμετώπιση των εγκλημάτων επειδή το δομημένο περιβάλλον μπορεί να επηρεάσει το επίπεδο εγκληματικής δράσης των πιθανών δραστών, άρα ελέγχοντας το περιβάλλον αυτό μπορούμε να ελέγξουμε και την εγκληματική δραστηριότητα.[102]

Οι ευκαιρίες για τη διάπραξη εγκλήματος, οι περιστασιακές και περιβαλλοντικές συνθήκες λαμβάνουν κεντρική θέση στις εγκληματολογικού ενδιαφέροντος μελέτες και εξετάζονται πλέον ως αιτιώδεις παράγοντες για κάθε μορφή εγκλήματος, ακόμα και για τα οικονομικά και ψηφιακά. Η μετακίνηση αυτή του ενδιαφέροντος από τις κοινωνικο-οικονομικές δομές προς

[95] Wortley Richard & Mazerolle Lorrain, eds (2011), σ.σ. 2-3
[96] Cornish Derek B., Clarke Ronald V. (1986)
[97] Brantigham Patricia L & Brantigham Paul.J. (2008), σσ. 259-294
[98] Felson,Marcus. & Clarke,Roland (1997) και Felson,Marcus. & Clarke,Roland (1998)
[99] Jeffery C. Ray & Zahm Diane L (2008), σσ.329-330
[100] Clarke Ronald V. (1995) και Clarke Ronald V. (1997)
[101] Burke Roger Hopkins (2009), σ.195
[102] Burke Roger Hopkins (2009), σ.196

τις περιβαλλοντικές και ευκαιριακές, από την προσωπικότητα του δράστη προς το γεγονός και όχι τα βαθύτερα αίτιά του, επέτρεψε την κατανόηση του πώς και του γιατί τα εγκλήματα διαφοροποιούνται στο χώρο και το χρόνο, γιατί τα εγκλήματα δεν κατανέμονται ομοιόμορφα μεταξύ όλων των γεωγραφικών περιοχών αλλά συγκεκριμένα εγκλήματα δείχνουν προτίμηση σε συγκεκριμένους χώρους και χρόνους. Η διαφοροποίηση αυτή των εγκλημάτων στο χώρο και το χρόνο δεν οφείλεται τόσο στην διαφορετική διαθεσιμότητα πιθανών δραστών αλλά κυρίως στην ύπαρξη διαφορετικών κατάλληλων ευκαιριών στους δράστες που διαμορφώνουν την «ευκαιριακή δομή» της κάθε - εγκληματικής - δραστηριότητας. Η προσέγγιση αυτή μας επιτρέπει και τον αποτελεσματικότερο σχεδιασμό της αποτροπής, μέσω της αλλαγής των ευκαιριακών δομών του εγκλήματος, όχι μόνο των παραδοσιακών εγκλημάτων «δρόμου» αλλά και αυτών του λευκού περιλαιμίου, των οικονομικών ή των άλλων μη βίαιων εγκλημάτων.[103]

Μεταξύ αυτών που συγκαταλέγονται στις θεωρίες των «εγκληματικών ευκαιριών», εκτός από τη θεωρία της ορθολογικής επιλογής των Clarke και Cornish, είναι και οι θεωρίες των «καθημερινών δραστηριοτήτων», των «εγκληματικών προτύπων» και όπως αυτές εφαρμόζονται από την θεωρία για την «περιστασιακή πρόληψη του εγκλήματος».

Τα κοινά χαρακτηριστικά των θεωριών αυτών εστιάζουν, όχι τόσο στον δράστη και τα κίνητρά του μεμονωμένα, αλλά στον δράστη, το θύμα/στόχο, το χώρο και το χρόνο ως παράγοντες που συνδυαστικά δημιουργούν τις εγκληματικές ευκαιρίες.[104]

Η βασική διαφορά, επισημαίνει ο Cook, των νέων θεωριών «εγκληματικών ευκαιριών» από την αρχική των Cloward and Ohlin, είναι ότι οι νέες εμπλέκουν την οικονομική θεωρία και την ορθολογική επιλογή στη διαδικασία λήψης της απόφασης και τον τρόπο αλληλεπίδρασης πιθανών δραστών και θυμάτων, ενώ η αρχική θεωρία δίνει έμφαση στη διαδικασία της κοινωνικής μάθησης. Για τους Cloward and Ohlin η επίδραση των εγκληματικών ευκαιριών στην συμπεριφορά είναι έμμεση μέσω του συγχρωτισμού με την παραβατική υποκουλτούρα.[105]

Οι βασικές αρχές των νεότερων θεωριών, που παρουσιάζονται παρακάτω και που εστιάζουν στο ρόλο των «εγκληματικών ευκαιριών», συνοψίζονται από τους Felson και Clarke ως εξής:

1. Οι εγκληματικές ευκαιρίες παίζουν ρόλο στη δημιουργία κάθε είδους εγκλήματος.
2. Οι εγκληματικές ευκαιρίες είναι εξαιρετικά εξειδικευμένες.
3. Οι εγκληματικές ευκαιρίες είναι συγκεντρωμένες και όχι τυχαία διασκορπισμένες στο χώρο και το χρόνο.
4. Οι εγκληματικές ευκαιρίες εξαρτώνται από τις καθημερινές δραστηριότητες ρουτίνας
5. Το ένα έγκλημα μπορεί να δημιουργεί τις ευκαιρίες για ένα άλλο.
6. Μερικά αντικείμενα είναι πιο ελκυστικά κατά τη δημιουργία ευκαιριών.
7. Οι εγκληματικές ευκαιρίες δημιουργούνται και από τις κοινωνικές και τεχνολογικές αλλαγές.
8. Το έγκλημα μπορεί να περιοριστεί αν περιορίσουμε τις παρεχόμενες ευκαιρίες.
9. Με τον περιορισμό των ευκαιριών μέσω άσκησης προληπτικής πολιτικής συνήθως δεν μετατοπίζεται η εγκληματική δραστηριότητα σε άλλο μέρος.

[103] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626
[104] Goldstein Arnold P. (1994), σσ.52-53
[105] Cook Philip T., (1986), ό.π.

10. Ο περιορισμός των ευκαιριών σε ένα μέρος επιτυγχάνει και τη μείωση των δεικτών εγκληματικότητας στην ευρύτερη κοινότητα ή κοινωνία. [106]

2.3.1. Η προσέγγιση της ορθολογικής επιλογής των Ronald V. Clarke και Derek Cornish από την προοπτική των «εγκληματικών ευκαιριών»

Διάφορες προσπάθειες εφαρμογής της «Ορθολογικής Επιλογής» έχουν γίνει σε πλήθος εγκληματολογικών θεωριών και περιπτώσεων παρέκκλισης όπως στη «θεωρία των Καθημερινών δραστηριοτήτων», τη μελέτη εγκλημάτων όπως ληστείας, χρήσης ναρκωτικών, βανδαλισμών, του εγκλήματος του Λευκού Περιλαιμίου και στην πρόληψη της «περιστασιακής» εγκληματικότητας.

Την αναζωπύρωση του κλασικισμού και της ατομικής - Ορθολογικής Επιλογής για την εφαρμογή της στην μελέτη του εγκλήματος, έφεραν οι Ronald V. Clarke και Derek Cornish με το έργο τους "The Reasoning Criminal: Rational Choice Perspectives on Offending" το 1986. Με αυτό επιχειρούν μια σύνθεση εγκληματολογικών προσεγγίσεων, κυρίως τον ωφελιμισμό της κλασικής σχολής (Beccaria, Bentham), της οικονομικής θεωρίας (G.Becker) και των ψυχολογικών μελετών για τη διαδικασία λήψης αποφάσεων[107]. Το θεωρητικό υπόβαθρο της προσέγγισης της ορθολογικής επιλογής των Clarke και Cornish αντλείται εκτός από την κλασική άποψη της ορθολογικής επιλογής και από τις οικονομικές θεωρίες. Επιδιώκοντας όμως να αποφύγουν τα μειονεκτήματα και την κριτική που είχε ασκηθεί στις τελευταίες[108], περί υπερβολικού οικονομικισμού και μαθηματικοποίησης της εγκληματικής συμπεριφοράς, οι Clarke και Cornish πρότειναν τα διαγράμματα «λήψης της απόφασης». Έτσι έδωσαν έμφαση στην λήψη της απόφασης η οποία στηρίζεται και σε μη καθαρά οικονομικά κίνητρα, όπως την ανάγκη για απόκτηση status, ικανοποίηση εγωισμού, επιδίωξη συγκινήσεων και «περιπέτειας», σε συνδυασμό με την παραδοχή της περιορισμένης ορθολογικότητας της απόφασης η οποία περιορίζεται από τον διαθέσιμο χρόνο, τις ικανότητες και τις απαραίτητες πληροφορίες.[109]

Η ορθολογική επιλογή των Clarke και Cornish εστιάζει στο εγκληματικό γεγονός καθεαυτό, στο σκηνικό του εγκλήματος και στους περιστασιακούς του παράγοντες παρά στους δράστες[110]. Η απαρχή της θεωρίας των Clarke και Cornish βρίσκεται στο πλαίσιο της εργασίας του Clarke, σε συνεργασία με τον Pat Mayhew και άλλους για το Home Office το 1983, για την «περιστασιακή» πρόληψη του εγκλήματος μέσω των αλλαγών του περιβάλλοντος και της εμπόδισης των «εγκληματικών ευκαιριών».[111] Στην εργασία αυτή τέθηκε από τον Clarke το θεωρητικό πλαίσιο που ήταν ένας συνδυασμός θεωριών «ευκαιριών», όπως των καθημερινών δραστηριοτήτων και της ορθολογικής επιλογής.[112] Αφού παρατήρησε ότι η περιστασιακή πρόληψη του εγκλήματος, όπως εφαρμόστηκε από διάφορες βρετανικές μελέτες, εστίαζε στην επιτήρηση, στην προστασία των στόχων και στην περιβαλλοντική διαχείριση, πρότεινε ότι και το άτομο-δράστης θα πρέπει να αποτελέσει μέρος αυτού του σκηνικού.[113]

[106] Felson,Marcus. & Clarke,Roland (1998), σσ. 1-34
[107] Cornish Derek (1993), σσ. 351-382
[108] Βλ. παραπ.
[109] Clarke Ronald V. (1995), σσ. 91-150
[110] Clarke Ronald V. (1997)
[111] Βλ. Clarke Ronald V. & Cornish Derek (2002), σσ. 291-296 και Clarke Ronald V. (1995), σσ. 91-150
[112] Clarke Ronald V. (1997)
[113] Jeffery C. Ray & Zahm Diane L. (2008), σ.336

Σύμφωνα με την άποψη της Ορθολογικής Επιλογής, όπως αυτή εκφράστηκε από τους Clarke και Cornish, το έγκλημα είναι μια ορθολογική δράση που πραγματοποιείται από συνηθισμένους ανθρώπους οι οποίοι αντιδρούν σε συγκεκριμένη πίεση, ευκαιρίες και περιστασιακές προκλήσεις.[114]

Βασική θέση τους αποτελεί ότι ο εγκληματίας δεν διαφέρει από τον μη εγκληματία, είναι ορθολογικός και όχι παθολογικός, αναζητά οφέλη από το έγκλημα και ότι στη διαδικασία λήψης αποφάσεων υπολογίζει, ορθολογικά, τα αναμενόμενα οφέλη και κόστη. Απομακρύνουν το ενδιαφέρον μελέτης από τα αίτια του εγκλήματος και εστιάζουν την έμφαση στα γεγονότα, τις περιστάσεις, τις ευκαιρίες και στις αποφάσεις του δράστη κατά την διάρκεια της «καριέρας» του. Ο ρόλος και η σημασία των κινήτρων, όπως και για τις οικονομικές και συμπεριφορικές θεωρίες τοποθετούνται στη βάση «ανταμοιβή – τιμωρία», γι αυτό σημαντικός είναι και ο ρόλος της κοινωνικής μάθησης στην εγκληματική καριέρα. [115]

Ο πιθανός εγκληματίας αποφασίζει (επιλέγει) να διαπράξει ένα συγκεκριμένο έγκλημα προκειμένου να ικανοποιήσει τις ανάγκες του. Αυτή η στοχοθετημένη και εθελούσια συμπεριφορά συνοδεύεται από δύσκολους υπολογισμούς των προσπαθειών που θα καταβληθούν, των κινδύνων που θα αναληφθούν και των πιθανών ανταμοιβών από τη διάπραξη ενός συγκεκριμένου εγκλήματος.[116]

Οι βασικές απόψεις των Cornish και Clarke για την ορθολογική επιλογή στην ανθρώπινη συμπεριφορά συνοψίζονται στις εξής προτάσεις:

1. Η ανθρώπινη συμπεριφορά είναι ορθολογική (αν και σε περιορισμένα πλαίσια).
2. Η ανθρώπινη συμπεριφορά είναι αποτέλεσμα αλληλεπίδρασης και προσαρμογής.
3. Οι αντιλήψεις, οι αποφάσεις και οι επιλογές του δράστη αποτελούν δείκτες των παραπάνω διαδικασιών αλληλεπίδρασης.
4. Επειδή η σχέση αλληλεπίδρασης ατόμου – κατάστασης είναι διαφορετική σε κάθε δράστη απαιτείται προσέγγιση που θα εστιάζει στο συγκεκριμένο εγκληματικό γεγονός.
5. Επειδή επιδρούν διαφορετικές μεταβλητές, διαφορετικά στάδια και χρόνοι λήψης της απόφασης, απαιτείται διάκριση του γεγονότος καθαυτού από τη διαδικασία εμπλοκής σε αυτό.

Η πρώτη αποτελεί και την πιο σημαντική από όλες τις προτάσεις, ενώ οι υπόλοιπες προτάσεις αποτελούν την πρακτική εφαρμογή της πρώτης στην μελέτη της εγκληματικής συμπεριφοράς.[117]

Η διαδικασία λήψης της απόφασης του εγκληματία στηρίζεται στην ορθολογικότητα, την εκτίμηση των κινδύνων και της ωφέλειας. Οι Clarke και Cornish δέχονται την «περιορισμένη ορθολογικότητα» του πιθανού εγκληματία, δηλαδή η ορθολογικότητά του περιορίζεται από το χρόνο, τις ικανότητές του, τους ηθικούς ενδοιασμούς και τις διαθέσιμες πληροφορίες.

Η απόφαση του πιθανού δράστη διέρχεται από δυο φάσεις. Πρώτα η φάση της «αρχικής εμπλοκής», της διερεύνησης του κατά πόσο η εμπλοκή του με το συγκεκριμένο έγκλημα τον ικανοποιεί, δηλαδή καλύπτει τις ανάγκες του. Αυτή επηρεάζεται από την παρούσα κατάστασή του, όπως την επιτακτική του ανάγκη για χρήματα, από τις προηγούμενες εμπειρίες του και μαθησιακούς παράγοντες. Τέτοιοι παράγοντες είναι η προηγούμενη

[114] Burke Roger Hopkins (2009), σ.44
[115] Clarke Ronald V. & Cornish Derek (2002), σσ. 291-296
[116] Adler Freda, et.al. (1998), σ.171
[117] Cornish Derek (1993), σσ. 351-382

εμπειρία του με το έγκλημα και τις διωκτικές αρχές, οι ηθικές αξίες, η αυτοεκτίμηση και η ικανότητα μακροχρόνιου σχεδιασμού. Έπειτα ακολουθεί η φάση της επιλογής του είδους του εγκλήματος που θα τελέσει, το οποίο θα εξαρτηθεί από διάφορους παράγοντες, από την κάθε συγκεκριμένη περίσταση και κυρίως από την προσωπική του κατάσταση.

Οι Clarke και Cornish θεωρούν ότι οι περισσότερες θεωρίες της περιβαλλοντικής κοινωνιολογίας (όπως της Σχολής του Σικάγου) μέχρι τώρα αγνοούν, παραβλέπουν τους παράγοντες που επηρεάζουν την απόφαση του ατόμου να προβεί στο συγκεκριμένο έγκλημα κάτω από τις συγκεκριμένες περιστάσεις, δηλαδή ότι εστιάζουν στην εγκληματική εμπλοκή και όχι στο εγκληματικό γεγονός και τις συνθήκες τέλεσής του, συνθήκες οι οποίες επηρεάζουν και την απόφαση για την τέλεση. Η εστίαση στο γεγονός και στις συνθήκες, γίνεται όχι μόνο γιατί το κάθε είδος εγκλήματος ανταποκρίνεται σε ιδιαίτερες ανάγκες, αλλά και γιατί οι περιστάσεις κάτω από τις οποίες λαμβάνονται οι αποφάσεις διαφέρουν ανάμεσα στους διάφορους παραβάτες[118]. Η μελέτη της διαδικασίας λήψης της απόφασης και των περιστάσεων μας επιτρέπει να κατανοήσουμε όχι μόνο το γιατί συγκεκριμένα άτομα κάνουν εγκλήματα κάτω από συγκεκριμένες συνθήκες, αλλά και τους τρόπους αντιμετώπισης τέτοιων εγκλημάτων.[119]

Κεντρική θέση στην ορθολογική θεώρηση του Clarke κατέχει ο τρόπος που τα άτομα επεξεργάζονται γνωστικά τα δεδομένα του περιβάλλοντος για τη λήψη της απόφασης. Η θεώρηση εστιάζει έτσι στην οπτική του ατόμου και το πώς αυτό το άτομο προσλαμβάνει και αξιολογεί τις πληροφορίες για τις ευκαιρίες που δίνει το περιβάλλον για τη μεγιστοποίηση του οφέλους και την ελαχιστοποίηση του κόστους. Τα άτομο δεν αντιδρά μηχανιστικά στα ερεθίσματα του περιβάλλοντος, αλλά, πριν αποφασίσει να εμφανίσει κάποια συμπεριφορά, παρεμβάλλονται και γνωστικές διαδικασίες επεξεργασίας των δεδομένων του περιβάλλοντος. Έτσι διασυνδέονται οι δυο θεωρίες που υποστήριξε ο Clarke, και που φαινομενικά έχουν αντίθετες βάσεις: ο θετικισμός για την πρόληψη της περιστασιακής εγκληματικότητας με τον κλασικισμό στον οποίο βασίζεται η ορθολογική επιλογή.[120]

Η απόφαση του πιθανού εγκληματία για τη διάπραξη του εγκλήματος (ή ενός συγκεκριμένου εγκλήματος που θα προτιμηθεί έναντι κάποιοι άλλου) δομείται από μια ποικιλία χαρακτηριστικών που αποκαλούνται ιδιότητες δόμησης επιλογής (choice structure properties). Κάθε τύπος διαφορετικού εγκλήματος περιλαμβάνει το δικό του μίγμα ιδιοτήτων δόμησης της επιλογής. Αυτές οι ιδιότητες κατηγοριοποιούνται ως εξής:[121]

α) ο αριθμός των πιθανών στόχων και η προσβασιμότητά τους.

β) η εξοικείωση με την επιλεγμένη μέθοδο.

γ) το οικονομικό όφελος.

δ) η εξειδίκευση που απαιτείται.

ε) ο χρόνος που απαιτείται για να ολοκληρωθεί η δράση.

στ) οι φυσικοί κίνδυνοι που ενέχονται.

ζ) ο κίνδυνος σύλληψης και η βαρύτητα της ποινής

η) οικονομικό κόστος και διάθεση πόρων ή μέσων (εργαλεία, αυτοκίνητο κλπ.)

θ) άλλοι παράγοντες που πρέπει να συνεκτιμηθούν.

[118] Clarke Ronald V. & Cornish Derek (2002), σσ. 291-296

[119] Clarke Ronald V. & Cornish Derek (2002), *ό.π.*

[120] Jeffery C. Ray & Zahm Diane L. (2008), σ.337

[121] Clarke Roland. και Cornish Derek (1987), σσ. 933–948

Οι παραπάνω παράγοντες - ιδιότητες σχετίζονται με τις ευκαιρίες, τα κόστη, τα οφέλη και τις διάφορες εναλλακτικές επιλογές για το κάθε συγκεκριμένο έγκλημα.

Οι συγγραφείς μάλιστα, στη θέση των μαθηματικών τύπων του G.Becker, κατασκεύασαν «διαγράμματα ροής»[122] για να απεικονίσουν τα διάφορα μοντέλα εγκληματικών αποφάσεων και την ποικιλία των παραγόντων που επηρεάζουν τη διαδικασία απόφασης για εμπλοκή σε συγκεκριμένο είδος εγκληματικής δραστηριότητας.[123]

Επεκτάσεις – εφαρμογές της θεωρίας της ορθολογικής επιλογής

Στην πορεία και άλλοι υποστηρικτές της θεωρίας της Ορθολογικής Δραστηριότητας χρησιμοποίησαν μαθηματικά μοντέλα και μεθόδους της μικρο-οικονομικής ανάλυσης για να προσεγγίσουν τομείς εγκληματολογικού ή κοινωνιολογικού ενδιαφέροντος, όπως ο Hechter (1987) για τις σχέσεις των εθνικών μειονοτήτων και οι Goldthorpe (1996), Breen and Rottman (1995) για την κοινωνική κινητικότητα και την αναπαραγωγή των ανισοτήτων, ο Gary Becker[124] για το έγκλημα και το γάμο κ.ά.[125]

Κάποιοι, όπως ο Gordon Winston, πρότειναν τη θεώρηση της «ατελούς ορθολογικής επιλογής» σύμφωνα με την οποία δεν μπορούν όλοι και πάντα να κάνουν πλήρως ορθολογικές επιλογές. Ο βαθμός της ορθολογικότητας ποικίλλει σε κάθε άτομο ανάλογα με το είδος της απόφασης και τη δεδομένη χρονική στιγμή.[126]

Ο Heath θεωρεί ότι η καθαρά ορθολογική επιλογή, που περιλαμβάνει πλήρη γνώση των δεδομένων, χωρίς λάθη και ανάληψη ρίσκου, δεν μπορεί να εφαρμοστεί.[127]

Ο Gordon Trasler πρότεινε τη διεύρυνση της ορθολογικής επιλογής, που βασίζεται σε καθαρά οικονομικό - ωφελιμιστικό μοντέλο, με τη προσθήκη της θεωρίας της «προδιάθεσης» (dispositional theory). Σύμφωνα με τη θεώρηση αυτή η διάπραξη ή όχι του εγκλήματος εξαρτάται από τα χαρακτηριστικά ή τις στάσεις του ατόμου και ασχολείται με τους μηχανισμούς κατά τους οποίους πολλοί άνθρωποι δεν εμπλέκονται σε εγκληματικές δραστηριότητες, παρά το γεγονός ότι οι στόχοι είναι ελκυστικοί και ο κίνδυνος της τιμωρίας μοιάζει απόμακρος. Έτσι η ωφελιμιστική προσέγγιση της ορθολογικότητας της δράσης προτάθηκε να τροποποιηθεί με τη διάκριση μεταξύ των συμπεριφορών που είναι πλήρως ορθολογικές και των πιο μακροπρόθεσμων και πιο σταθερών αποφάσεων ή στάσεων που περιλαμβάνουν και μη ορθολογικά στοιχεία όπως ηθικές ή αξιακές επιλογές και αποφάσεις που δεν έχουν άμεση σχέση με τη πιθανή σύλληψη και διαφυγή.[128]

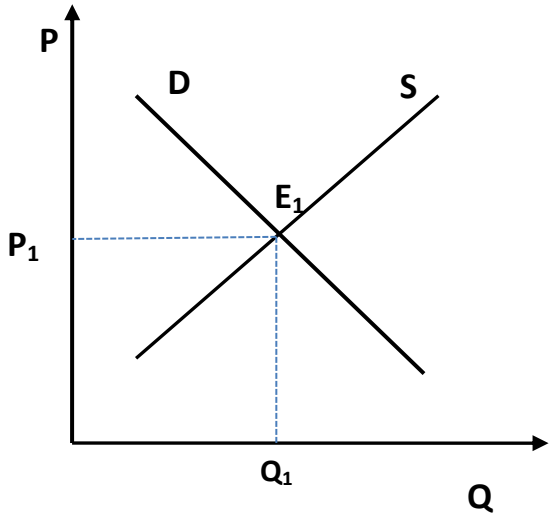
Ο ίδιος ο Clarke δέχεται επίσης την ιδέα της περιορισμένης ορθολογικότητας ως στοιχείο της διαδικασίας λήψης των αποφάσεων.[129] Σε συνεργασία με τον Cornish στο «The Reasoning Criminal», αναφέρει ότι ο όρος «ορθολογική» χρησιμοποιείται με την έννοια της περιορισμένης ορθολογικότητας (limited or bounded rationality), του στρατηγικού σχεδιασμού, της επεξεργασίας των πληροφοριακών δεδομένων, της συνεκτίμησης των

[122] Βλ. Παράρτημα Διαγράμματα Clarke R. V και Cornish D.
[123] Βλ. Clarke Ronald V. και Cornish Derek (2002), ό.π.
[124] Βλ. Becker, Gary S. (1976) και Becker Gary. S. (1981)
[125] Scott John (2000)
[126] Winston Gordon.C. (1989), σσ.67-86
[127] Akers Ronald L. (1990-1991), σσ. 653-676
[128] Trasler Gordon (2008), σσ.305-322
[129] Jeffery C. Ray & Zahm Diane L. (2008), σ.337

εναλλακτικών επιλογών και ευκαιριών, ενώ ο όρος «επιλογή» σημαίνει ότι οι εγκληματίες παίρνουν αποφάσεις.[130]

Ο Philip Cook, επηρεασμένος και από το έργο του Clarke, επιχείρησε να συνδέσει την οικονομολογική οπτική της «ελεύθερης αγοράς» με τις διάφορες πτυχές των εγκληματικών ευκαιριών δίνοντας ιδιαίτερη σημασία στον τρόπο που αλληλεπιδρούν οι πιθανοί δράστες με τους πιθανούς στόχους. Οι εγκληματίες, αναφέρει ο Cook στη δική του διατύπωση για τις εγκληματικές ευκαιρίες, θεωρούν ελκυστικούς τους στόχους με βάση το αν αυτοί προσφέρουν υψηλή ανταμοιβή με μικρή προσπάθεια και χαμηλό κίνδυνο αντιμετώπισης νομικών συνεπειών. «Από την πλευρά τους τα πιθανά θύματα τείνουν να λαμβάνουν αυστηρότερα μέτρα προστασίας ανάλογα με το πόσο πιθανή θεωρούν τη θυματοποίηση τους διαφοροποιώντας έτσι και το εγκληματικό πρότυπο μέχρι σε ένα βαθμό. Η αλληλεπίδραση ή ισορροπία αυτή μεταξύ πιθανών δραστών και θυμάτων παρομοιάζεται από τον οικονομολόγο Cook με την αλληλεπίδραση/ισορροπία καταναλωτών και πωλητών σε πλαίσια μιας ελεύθερης αγοράς. Η ισορροπία στην αγορά του εγκλήματος μπορεί να διαταράσσεται από την κρατική παρέμβαση του συστήματος απονομής δικαιοσύνης». [131]

Σύμφωνα με την οικονομική θεωρία, σε καθεστώς ελεύθερης αγοράς (δηλ. χωρίς κρατική παρέμβαση), οι δυνάμεις της προσφοράς (S) και της ζήτησης (D), για την αγορά ενός προϊόντος (ορισμένο είδος εγκλήματος στην προκειμένη περίπτωση), ισορροπούν στο σημείο E_1 διαμορφώνοντας την τιμή (αξία) του προϊόντος του εγκλήματος σε P_1 και την ποσότητα σε Q_1 (βλ. σχήμα 1).

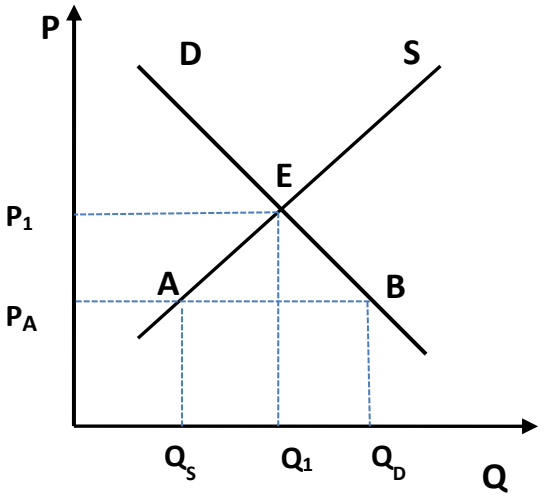


Σχήμα 1

Η κρατική παρέμβαση (με την μορφή αντεγκληματικής πολιτικής), στην αγορά του εγκλήματος, που καταλύει το καθεστώς ελεύθερης αγοράς - μιλώντας με οικονομολογικούς όρους, επιδιώκει τη δημιουργία «ανισορροπίας» και συγκεκριμένα «ελλείμματος προσφοράς» (QS – QD < 0) που θα σημαίνει μείωση της εγκληματικότητας. Στο σχήμα 2 η απόσταση ΑΒ απεικονίζει την ανισορροπία αυτή.

[130] Cornish Derek B. & Clarke Ronald V. (1986), σ. xviii

[131] Βλ. Cook Philip (1986), σσ. 1-27



Σχήμα 2

2.3.2. Η θεωρία των «Καθημερινών Δραστηριοτήτων»

Η θεωρία των «καθημερινών δραστηριοτήτων», με κύριους εμπνευστές τους Lawrence Cohen και Marcus Felson, αποτελεί μια από τις κύριες θεωρίες της Περιβαλλοντικής Εγκληματολογίας και της ομάδας των θεωριών των «εγκληματικών ευκαιριών» (Opportunity theories), εφαρμόζοντας την «ορθολογική επιλογή» σε διάφορες μορφές εγκληματικότητας, εστιάζει στα χαρακτηριστικά της δράσης, και όχι του δράστη.[132] Η θεωρία πιστεύει ότι για την ύπαρξη της εγκληματικής ευκαιρίας απαιτείται να συνυπάρχουν στο χώρο και το χρόνο τρεις παράγοντες: ένας ικανός δράστης, ένας κατάλληλος στόχος – θύμα και απουσία «ικανών φυλάκων».

Οι εγκληματικές πράξεις τελούνται όπως οι απλές καθημερινές δραστηριότητες, με τις οποίες παρατηρούνται όχι μόνο πολλά κοινά χαρακτηριστικά αλλά και αλληλεξαρτήσεις. Η θεωρία, εστιάζοντας στις αλλαγές των κοινωνικών συνθηκών μεταπολεμικά (ιδιαίτερα μεταξύ ’60 και ’80), στην αλλαγή και στη διασπορά των καθημερινών δραστηριοτήτων έξω από το σπίτι, πιστεύει ότι αυτό οδήγησε σε κοινωνική αποδιοργάνωση και διεύρυνε τις ευκαιρίες διάπραξης εγκλημάτων. Από τη μια πλευρά η τεχνολογία δημιούργησε ελκυστικά προϊόντα, τηλεοράσεις, αυτοκίνητα, υπολογιστές κλπ. που αποτελούν κατάλληλους στόχους. Από την άλλη, οι τεχνολογικές εξελίξεις προκάλεσαν αλλαγές στις καθημερινές συνήθειες των ανθρώπων. Για παράδειγμα η έξοδος της γυναίκας από το σπίτι και η είσοδός της στην αγορά εργασίας, η χρήση του αυτοκινήτου για μετάβαση στην εργασία σε μεγαλύτερες αποστάσεις αφήνει το σπίτι ανεπίβλεπτο, κατά τη διάρκεια των εργάσιμων ημερών, χωρίς την παρουσία ικανών φυλάκων.[133]

Τα κύρια σημεία της θεωρίας των καθημερινών δραστηριοτήτων δημοσιεύτηκαν από τους Cohen και Felson στο American Sociological Review το 1979 με τίτλο "Social change and crime rate trends: a routine activity approach"[134]

[132] Sutton David, (2014)
[133] Cohen Lawrence. E. και Felson Marcus (1979), σσ. 588–608
[134] Cohen Lawrence. E. και Felson Marcus (1979), σσ. 588–608

Η προσπάθεια των δυο εμπνευστών της θεωρίας, Cohen & Felson ήταν να ερμηνεύσει την άνοδο της εγκληματικότητας μετά το Β' Παγκόσμιο Πόλεμο, η οποία δεν μπορούσε να ερμηνευθεί επαρκώς από τις θεωρίες που εστίαζαν στις μακρο – κοινωνικο/οικονομικές συνθήκες, όπως η οικονομική ύφεση και οι δείκτες ανεργίας, επειδή είχε παρατηρηθεί (από την Εθνική Επιτροπή για τα Αίτια και την Πρόληψη της Βίας) το παρακάτω «παράδοξο» (αντιφατικό) κοινωνιολογικό φαινόμενο. Ενώ οι κοινωνικο-οικονομικές συνθήκες, που θεωρούνταν μέχρι τώρα υπεύθυνες για την πρόκληση των εγκλημάτων βίας είχαν βελτιωθεί σημαντικά, οι δείκτες των αντίστοιχων εγκλημάτων αυξήθηκαν αντί να μειωθούν. Για παράδειγμα, όπως αναφέρουν οι συγγραφείς, στις ΗΠΑ ο αριθμός των έγχρωμων που τελείωσε το Γυμνάσιο αυξήθηκε από το 43% στο 61% μεταξύ 1961 και 1968, οι δείκτες ανεργίας μειώθηκαν σημαντικά από το 1959 έως το 1967, το ποσοστό των κατοίκων των πόλεων που ζουν κάτω από το όριο της φτώχειας μειώθηκε από 11,3 σε 8,3 εκατομμύρια την ίδια περίοδο.

Από την άλλη πλευρά οι δείκτες εγκλημάτων βίας όπως ληστείες, επιθέσεις, βιασμοί και δολοφονίες, στο διάστημα 1960-1975 αυξήθηκαν κατά 263%, 164%, 174% και 188% αντίστοιχα, σύμφωνα με εκθέσεις του FBI. Όμοια αυξήθηκαν και οι δείκτες μη βίαιων εγκλημάτων όπως αυτά κατά της περιουσίας, π.χ. οι διαρρήξεις κατά 200%.

Οι Cohen και Felson απέδωσαν αυτή την αύξηση των δεικτών της εγκληματικότητας στην ευμάρεια των σύγχρονων κοινωνιών που προσφέρουν πολλές ευκαιρίες διάπραξης εγκλημάτων και πρότειναν το πρότυπο της αλλαγής των «καθημερινών δραστηριοτήτων» ή «δραστηριοτήτων ρουτίνας».

Οι συγγραφείς, στη δημοσίευσή τους, όρισαν ως καθημερινές δραστηριότητες:

> «κάθε επαναλαμβανόμενη και κυρίαρχη δραστηριότητα που ικανοποιεί βασικές ανάγκες του πληθυσμού και των ατόμων. Έτσι οι καθημερινές δραστηριότητες περιλαμβάνουν εκτός από την επαγγελματική ενασχόληση και την προμήθεια τροφής, στέγης, διασκέδασης, κοινωνικές συναναστροφές, εκπαίδευση και φροντίδα των παιδιών. Οι καθημερινές δραστηριότητες λαμβάνουν χώρα (1) στο σπίτι (2) στην εργασία εκτός σπιτιού και (3) σε άλλες δραστηριότητες εκτός σπιτιού, π.χ. διασκέδαση. Μετά το Β' Παγκόσμιο Πόλεμο υπάρχει μια μετατόπιση των δραστηριοτήτων που γίνονται εντός σπιτιού προς τις άλλες δυο»[135] (δηλαδή σε δραστηριότητες εκτός σπιτιού, π.χ. δουλειά, διασκέδαση).

Σύμφωνα με τη θεωρία των L. Cohen και M. Felson οι δομικές αλλαγές των προτύπων των δραστηριοτήτων ρουτίνας μπορεί να επηρεάσουν την συνύπαρξη, στο χώρο και το χρόνο, των τριών βασικών στοιχείων –παραγόντων που απαιτούνται για να τελεστεί ένα έγκλημα, δηλαδή:

α) ένα άτομο με δυνατότητα, θέληση και κίνητρο (motivated offender), να διαπράξει το έγκλημα,[136] που θα μπορούσε να είναι ο οποιοσδήποτε έχει την κατάλληλη ευκαιρία να τελέσει το αδίκημα είτε είναι περιστασιακός, είτε «χρόνιος» παραβάτης.[137]

β) έναν κατάλληλο στόχο/ θύμα (suitable victim), που μπορεί να είναι ένα πορτοφόλι ή ένα αυτοκίνητο, ένα αντικείμενο με αξία, ορατό, προσβάσιμο κοντά στο τόπο διαμονής ή εργασίας του δράστη. Η ελκυστικότητα του αντικειμένου - στόχου αυξάνει ανάλογα με τη

[135] Cohen Lawrence & Felson Marcus (1979), σ.593

[136] αργότερα ο Felson το μετέτρεψε σε "likely offender".

[137] Cusson Maurice (2002), σ.72

φορητότητά του, το πόσο ελαφρύ είναι. Η τεχνολογία έχει συμβάλλει σε αυτή την κατεύθυνση με τη δημιουργία φορητών και ακριβών συσκευών.[138]

γ) η απουσία ικανών φυλάκων (επαρκούς φύλαξης) που θα αποτρέψει το έγκλημα (absence of capable guardian). «Ικανοί φύλακες» δεν είναι κατ' ανάγκη η αστυνομία, αλλά κυρίως ο ιδιοκτήτης του αντικειμένου-στόχου, οι γονείς, οι γείτονες, οι φίλοι ή άλλοι άτυποι φορείς που ασκούν φυσική φύλαξη.[139] Σε μια μικρή κοινότητα με άτομα που γνωρίζονται και συνδέονται μεταξύ τους υπάρχουν λίγες ευκαιρίες για έγκλημα.

Ο Felson, για να τονίσει το προηγούμενο επιχείρημά του, χρησιμοποιεί το παράδειγμα των ισραηλινών κιμπούτς όπου η εγκληματικότητα είναι χαμηλή επειδή ακριβώς δεν υπάρχει κάτι που να αξίζει κανείς να κλέψει και δεν μπορεί να πάει πουθενά με αυτό. Αντίθετα οι χαλαρότεροι κοινωνικοί δεσμοί που παρατηρούνται σε μια μεγαλούπολη και η χρήση του αυτοκινήτου καθιστούν τον άτυπο κοινωνικό έλεγχο πιο αναποτελεσματικό.[140]

Αν υπάρχει κίνητρο, όπως το κέρδος, που να είναι άξιο λόγου και ο στόχος του εγκλήματος δεν προστατεύεται αρκετά (έλλειψη ελέγχου), υπάρχει ευκαιρία ώστε το έγκλημα θα τελεστεί.

Η απουσία οποιουδήποτε από τα παραπάνω στοιχεία είναι ικανή για να αποτρέψει την επιτυχημένη ολοκλήρωση της εγκληματικής ενέργειας. Αντίθετα η συνύπαρξη, στον κατάλληλο χώρο και χρόνο, δράστη και θύματος (αν πρόκειται για πρόσωπο) ή στόχου (αν πρόκειται για αντικείμενο) χωρίς την παρουσία ικανής φύλαξης, είναι αρκετά για να προκαλέσουν μεγάλης κλίμακας αύξηση της εγκληματικότητας. Δεν είναι οι αλλαγές των κοινωνικών ή άλλων δομικών συνθηκών, αλλά οι αλλαγές στις καθημερινές συνήθειες που μεταβάλλουν τη συνύπαρξη των πιθανών δραστών με τα κατάλληλα θύματα, κατά την απουσία ικανών φυλάκων, στο χώρο και το χρόνο αυξάνοντας τις ευκαιρίες για τη διάπραξη εγκλημάτων και τους δείκτες εγκληματικότητας. Κατά συνέπεια σημαντικός παράγοντας αναδεικνύεται η ύπαρξη ή η απουσία επαρκούς ελέγχου. Αν ο έλεγχος (η φύλαξη, η αστυνόμευση κλπ.) μειωθεί τότε η εγκληματικότητα θα αυξηθεί. Οι δείκτες αύξησης της εγκληματικότητας είναι ανάλογοι με τον αριθμό των «κατάλληλων» στόχων και την απουσία ατόμων που θα προστάτευαν αυτούς τους στόχους. Η ευθύνη της διάπραξης του εγκλήματος μοιράζεται από το δράστη στο θύμα –στόχο[141].

Η θεωρία των «Καθημερινών Δραστηριοτήτων» αρχικά ασχολήθηκε με την ερμηνεία των «εγκλημάτων βίας και κατά της ιδιοκτησίας» (predatory violations) με χρήση άμεσης φυσικής επαφής. Ως «εγκλήματα βίας και κατά της ιδιοκτησίας» οι συγγραφείς ορίζουν «τις παράνομες πράξεις κατά τις οποίες κάποιος σκόπιμα παίρνει (κλέβει) ή προκαλεί βλάβες σε άλλο άτομο ή στην περιουσία του». Αυτά απαιτούν τη φυσική επαφή ενός τουλάχιστον δράστη με κάποιον άλλον, τον οποίο ο δράστης επιχειρεί να προσβάλλει είτε τον ίδιο ως πρόσωπο ή την περιουσία του. Οι συνθήκες κάτω από τις οποίες συμβαίνουν αυτές οι παραβιάσεις δεν είναι τυχαίες ούτε ασήμαντες, αντίθετα είναι σημαντικά δομικά φαινόμενα». Στόχος τους, αρχικά, δεν ήταν να μελετήσουν τα κίνητρα των δραστών, τα οποία παίρνουν ως δεδομένα, αλλά το πώς οι κοινωνικές δομές συμβάλλουν στη μετατροπή των εγκληματικών κινήτρων σε δράση. Κατά τη γνωστή θεώρηση του Durkheim για το «έγκλημα ως φυσιολογικό φαινόμενο», τα διάφορα αδικήματα αντιμετωπίζονται από την θεωρία των

[138] Cusson, ό.π.
[139] Cusson, ό.π.
[140] Felson Marcus (1986), σσ. 119-128
[141] Cohen, Lawrence & Felson Marcus (1979), ό.π.

«Καθημερινών Δραστηριοτήτων» ως κανονικές δραστηριότητες ρουτίνας. Η εγκληματική συμπεριφορά αλληλεπιδρά με άλλες καθημερινές (κανονικές) δραστηριότητες και μοιράζεται με αυτές κοινές συμπεριφορές. Γι αυτό η εστίαση γίνεται στο πώς η οργάνωση των καθημερινών δραστηριοτήτων, για την εξασφάλιση των προς το ζην, συνδέεται με τα αδικήματα που απαιτούν φυσική επαφή για την τέλεσή τους (direct-contact predatory violations).[142]

Όπως αναφέρουν οι ίδιοι οι συγγραφείς της θεωρίας, η χρήση του όρου παραβίαση (violation) προτιμήθηκε επειδή αναφέρεται άμεσα στο γεγονός, ενώ ο όρος έγκλημα δεν αναφέρθηκε σκόπιμα, γιατί αφορά γενικότερη κατηγορία. Με την ίδια λογική, για την άμεση φυσική επαφή του δράστη, αποφεύχθηκε η χρήση του όρου θύμα και προτιμήθηκε ο όρος στόχος επειδή το θύμα μιας κλοπής ή διάρρηξης δεν χρειάζεται απαραίτητα να είναι παρόν κατά τη διάρκεια του εγκληματικού γεγονότος. Ακόμα στη θέση του κινήτρου (motivation) οι συγγραφείς χρησιμοποίησαν την έννοια τάση ή ροπή (inclination), στην προσπάθειά τους να επιτύχουν τη σαφή διάκριση και αποστασιοποίησή τους από τη μελέτη των κινήτρων του δράστη και να εστιάσουν στο γεγονός της δράσης καθαυτής.[143] Στην κατεύθυνση αυτή, το τρίτο στοιχείο της θεωρίας, η «απουσία ικανών φυλάκων», είναι πολύ σημαντικό επειδή η εστίαση στην απουσία παρά στην παρουσία αποσείει το ενδιαφέρον από την προσωπικότητα, τα κίνητρα και τη μελέτη των ψυχολογικών αιτίων του εγκλήματος.[144]

Η θεωρία των «Καθημερινών Δραστηριοτήτων» συσχετίζει την εγκληματικότητα με την καθημερινή κοινωνική αλληλεπίδραση των ατόμων (δραστών), τα οποία δρώντας ορθολογικά κάνουν τις επιλογές τους βασισμένα στις ευκαιρίες για δράση που τους παρουσιάζονται με την συνύπαρξη, στο χώρο και το χρόνο, κατάλληλων στόχων με ανεπαρκή φύλαξη. Οι εγκληματίες δεν περιφέρονται άσκοπα στο χώρο, αλλά όπως ο καθένας έχουν τυποποιημένες συμπεριφορές ρουτίνας οι οποίες συνίστανται στην αποφυγή στόχων με φύλαξη και την προτίμηση θυμάτων που η καθημερινή ρουτίνα τους είναι μακριά από ικανούς φύλακες.

Το έγκλημα, από τη σκοπιά αυτή είναι μια φυσιολογική συμπεριφορά και μπορεί να διαπραχθεί όχι μόνο από «σκληρούς»[145] ή επαγγελματίες εγκληματίες αλλά από τον οποιοδήποτε έχει την κατάλληλη ευκαιρία[146]. Η ευκαιρία συμπεριλαμβάνει τη συνύπαρξη των τριών παραπάνω παραγόντων οι οποίοι μεταφράζονται για το δράστη σε ωφέλεια, κέρδη, κοινωνική αναγνώριση από τη μια πλευρά και κόστος, κίνδυνο σύλληψης και επιβολής ποινής από την άλλη.

Οι ρίζες της θεωρίας βρίσκονται στην κοινωνική και φυσική οικολογία και στις ιδέες του Amos Hawley[147] για το χώρο και το χρόνο:

1) το «ρυθμό» (rhythm), την περιοδικότητα με την οποία συμβαίνουν τα εγκληματικά γεγονότα.

2) Το «τέμπο» ή μέτρο (tempo), δηλαδή τον αριθμό των εγκληματικών γεγονότων που σημειώνονται σε ένα μέρος, π.χ. ένα δρόμο, για κάθε μονάδα χρόνου, π.χ. σε μια μέρα.

3) Τον «συγχρονισμό» (timing) των διαφορετικών αλληλεξαρτώμενων δραστηριοτήτων. Όπως ο συγχρονισμός των ρυθμών του δράστη με αυτούς του θύματος.[148]

[142] Felson Marcus & Cohen Lawrence (1980), σ.390

[143] Clarke Roland & Felson Marcus (2008), σ.σ.2-3

[144] Clarke Roland & Felson Marcus (2008), ό.π.

[145] Michael Brent, "The Routine Activities Theory in Delinquency", x.x.

[146] Review of the Roots of Youth Violence: Literature Reviews, Volume 5, Chapter 3

[147] Βλ. Hawley Amos (1950)

Συσχέτιση του χώρου και του χρόνου των καθημερινών δραστηριοτήτων με τις πιθανότητες θυματοποίησης είχαν επιχειρήσει και οι Hindelang, Gottfredson και Garofalo το 1978 με το μοντέλο «***έκθεσης του τρόπου ζωής***» (Lifestyle exposure model), το οποίο εξελίχθηκε και αναλύθηκε εκτενέστερα από τους Cohen και Felson.[149]

Ως τρόπο ζωής (lifestyle) ο Hindelang και οι συνεργάτες του ορίζουν τις «καθημερινές δραστηριότητες ρουτίνας τόσο στον επαγγελματικό χώρο όσο και στους χώρους διασκέδασης». Τα περιβάλλοντα στα οποία κινούνται και δρουν, ο χρόνος, ο χώρος, οι συναντήσεις με άλλους ανθρώπους, εκθέτουν τα άτομα σε διαφορετικές πιθανότητες θυματοποίησης. Άλλοτε οι κίνδυνοι αυτοί είναι μεγαλύτεροι κι άλλοτε μικρότεροι ανάλογα με τον τρόπο ζωής των ατόμων. Η ενασχόληση με ριψοκίνδυνες δραστηριότητες (όπως το να συχνάζουν σε κακόφημους δρόμους) μπορεί να γίνεται μέσω ορθολογικών επιλογών του ατόμου.[150] Σε κάθε συγκεκριμένη έκθεση των ατόμων σε τέτοιους κινδύνους η πιθανότητα θυματοποίησης εξαρτάται και από το κατά πόσο αποτελούν «επιθυμητό» και «ευπρόσβλητο» στόχο.[151]

Ο Choi θεωρεί την προοπτική των καθημερινών δραστηριοτήτων των Cohen και Felson απλώς μια επέκταση της αρχικής θεωρίας της «έκθεσης του τρόπου ζωής» (lifestyle-exposure theory) του Hindelang και της ομάδας του. Οι «ατομικές επαγγελματικές δραστηριότητες και οι δραστηριότητες κατά τον ελεύθερο χρόνο» μετατράπηκαν από τους Cohen και Felson σε «κατάλληλο στόχο» και έπειτα οι ίδιοι προσέθεσαν τα στοιχεία του «δράστη με κίνητρο» και τους «ικανούς φύλακες» [152].

Για το λόγο αυτό και άλλοι μελετητές, όπως ο Fawn T. Ngo εξετάζουν τις δυο αυτές θεωρίες (των καθημερινών δραστηριοτήτων και έκθεσης του τρόπου ζωής) ως ενσωματωμένες σε μια που ονομάζουν θεωρία του τρόπου ζωής - των καθημερινών δραστηριοτήτων (LRAT- Life style Routine Activity Theory) η οποία εφαρμόζεται τόσο στη μελέτη του εγκλήματος όσο και της θυματοποίησης.[153]

Σύμφωνα με τους Lawrence Sherman, Patrick Gartin & Michael Buerger, η θεωρία των καθημερινών δραστηριοτήτων ενσωματώνει έννοιες από ένα ευρύτερο φάσμα θεωριών όπως για το «δράστη με κίνητρο» (των Wilson και Herrnstein), την προσέγγιση των ευκαιριών για την προσφορά κατάλληλης ιδιοκτησίας για να αποτελέσει στόχο κλοπής (του Gould), της θεωρίας του τρόπου ζωής για την προσφορά κατάλληλων θυμάτων (του Hindelang και συνεργατών και του Miethe και συνεργατών), τις εργασίες για τη «θωράκιση του στόχου» (του Jeffrey) και για την αποτρεπτική ικανότητα του επίσημου και ανεπίσημου κοινωνικού ελέγχου (του Sherman) που υπονοεί η ύπαρξη «ικανών φυλάκων».[154]

Μετά τη δημοσίευση της εργασίας των Cohen και Felson το 1979, η αντεγκληματική πολιτική στις ΗΠΑ στράφηκε στην υπεράσπιση των δικαιωμάτων του θύματος και την προστασία του από την εγκληματικότητα. Η πολιτική αυτή υποστηρίχθηκε από τον πρόεδρο Ρ. Ρήγκαν που εκλέχθηκε ακριβώς εκείνη την περίοδο και χαρακτηρίστηκε από την αυξημένη

[148] Όπως αναφέρουν οι Cohen Lawrence. E. και Felson Marcus (1979), 588–608 (σ. 590)
[149] βλ. Goldstein Arnold P. (1994), σ.53
[150] Choi Kyung-shick (2008), σσ. 308–333
[151] Cook Philip (1986), σ. 6
[152] Choi Kyung-shick (2008)
[153] Ngo Fawn T. (2011), σσ. 773–793
[154] Σύμφωνα με Sherman Lawrence, Gartin Patrick & Buerger Michael (1989)

εγρήγορση και αγωνία για το έγκλημα με μηδενική ανοχή για τον δράστη και τα κίνητρά του.[155]

Η κεντρική ιδέα της θεωρίας έχει απεικονιστεί από τον John Eck ως ένα τρίγωνο, το λεγόμενο «τρίγωνο του εγκλήματος» ή «τρίγωνο ανάλυσης προβλήματος»[156]. Στην πραγματικότητα πρόκειται για δυο τρίγωνα όπου το ένα περικλείει το άλλο.

Στις τρεις πλευρές του εσωτερικού τριγώνου τοποθετούνται οι τρεις παράγοντες: δράστης, θύμα και τόπος με απουσία φύλαξης.

Στην μια πλευρά του τριγώνου τοποθετείται ο πιθανός δράστης ο οποίος είναι ικανός, πρόθυμος και με κίνητρο κάποιο όφελος, αλλά, πάνω από όλα, του παρουσιάζεται η ευκαιρία στο πλαίσιο των καθημερινών δραστηριοτήτων του, να συναντήσει τον κατάλληλο στόχο, στον κατάλληλο τόπο και χρόνο. [157]

Στην δεύτερη πλευρά τοποθετείται ο στόχος ή το θύμα που ο πιθανός δράστης θεωρεί επιθυμητό, ευάλωτο και πιο προσοδοφόρο. Αυτό μπορεί να είναι ένα πρόσωπο, ένα αντικείμενο ή ένα μέρος όπου οι «φύλακες» είναι απόντες, αδύναμοι ή διεφθαρμένοι.

Στην τρίτη πλευρά του τριγώνου βρίσκονται οι «φύλακες» οι οποίοι προσπαθούν να προστατεύσουν τα πιθανά θύματα ή τους στόχους από ενδεχόμενες εγκληματικές επιθέσεις και μπορεί να είναι η αστυνομία ή μια μητέρα που προσέχει το παιδί της στην παιδική χαρά.

Η παρουσία ελκυστικών τόπων - στόχων με αδύναμους διαχειριστές, αναποτελεσματικούς φύλακες και αδιάφορους διευθυντές θα προκαλέσει το ενδιαφέρον πιθανών δραστών για καθημερινή δραστηριότητα. [158]

Ένας στόχος με ικανό φύλακα είναι λιγότερο πιθανό να πέσει θύμα κάποιας επίθεσης. Οι φύλακες μπορεί να είναι:

α) επίσημοι φορείς που έχουν ως κύριο και συνειδητό έργο τη φύλαξη, όπως αστυνομία, ιδιωτικοί φύλακες (security), «πορτιέρηδες» ή άλλο προσωπικό ασφαλείας στις επιχειρήσεις.

β) ανεπίσημοι ή ακούσιοι φορείς, όπως γείτονες, φίλοι, γονείς, δάσκαλοι, συνάδελφοι κλπ.

Για το ζήτημα της εννοιολόγησης της καταλληλότητας των στόχων η θεωρία των καθημερινών δραστηριοτήτων των Cohen και Felson παρέχει συγκεκριμένη περιγραφή των χαρακτηριστικών τους. Οι Cohen και Felson χρησιμοποίησαν τα αρχικά VIVA (value, inertia, visibility, accessibility)[159] για να περιγράψουν ως κατάλληλο το στόχο που διαθέτει «αξία», «φορητότητα» (ευκολία μεταφοράς), «θεατότητα» και «προσβασιμότητα» χωρίς να γίνεται διαφοροποίηση μεταξύ έμψυχων ή άψυχων στόχων.

Ακόμα πιο λεπτομερή περιγραφή της καταλληλότητας των στόχων επιχείρησε, από την πλευρά της ορθολογικής επιλογής, ο Clarke ο οποίος πρόσθεσε ότι για μια τέτοια περιγραφή, δεν επαρκούν απλά τα χαρακτηριστικά του στόχου αλλά απαιτείται να λαμβάνονται υπόψη και άλλοι παράγοντες όπως το είδος του εγκλήματος, τα κίνητρα του δράστη και τα διαθέσιμα σε αυτόν μέσα. Έτσι ο Clarke πρότεινε το δικά του μοντέλο καταλληλότητας του στόχου που ονόμασε CRAVED από τα αρχικά των λέξεων concealable, removable, available, valuable, enjoyable and disposable δηλ. ο κατάλληλος στόχος διακρίνεται από δυνατότητα απόκρυψης, απόσπασης, διαθεσιμότητα ή προσβασιμότητα, αξία, προκαλεί ευχαρίστηση και

[155] Parsi Brian R Boetig (2004)

[156] Wortley Richard & Mazerolle Lorraine (2011), σ.74

[157] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), σσ. 341-374

[158] Center for problem oriented policing: "A Theory of Crime Problems" (2014)

[159] Cohen Lawrence και Felson Marcus (1979), 588–608, σ. 590

αναλωσιμότητα[160]. Το σχήμα αυτό χρησιμοποιήθηκε για να μελετηθεί η καταλληλότητα των στόχων κλοπής σε καταστήματα, αυτοκίνητα, διαρρήξεις κατοικιών, κινητών τηλεφώνων, τσαντών κλπ.[161]

Ο R. Clarke πρότεινε τη διεύρυνση της θεωρίας προσθέτοντας ένα ακόμα στοιχείο, τους «διευκολυντές του εγκλήματος» (crime facilitators), τα σημαντικά εργαλεία για κάθε είδος εγκλήματος. [162] Έτσι, η πιθανότητα να επιτύχει ο καθένας από τους εμπλεκόμενους το στόχο του εξαρτάται και από τα μέσα ή εργαλεία που διαθέτει:

Οι εγκληματίες χρησιμοποιούν όπλα, αυτοκίνητα, ή διαρρηκτικά εργαλεία, ιούς (προκειμένου για υπολογιστές) κλπ. για να αποκτήσουν πρόσβαση σε μέρη που δεν επιτρέπεται, να καταβάλλουν το θύμα τους ή για να αποφύγουν τους φύλακες και τη σύλληψη.

Οι φύλακες, για να ασκήσουν αποτελεσματική φύλαξη μεταχειρίζονται εργαλεία ως συστήματα ασφαλείας όπως κλειδαριές, φράχτες, φωτισμός, κάμερες παρακολούθησης χώρων, συναγερμοί, προγράμματα προστασίας υπολογιστών κλπ.

Η προσθήκη ή η αφαίρεση κάποιων από τα παραπάνω στοιχεία – εργαλεία μας δίνει διαφορετικές πιθανότητες επιτυχούς έκβασης των προσπαθειών καθενός.[163]

Με την ίδια λογική απεικονίζεται αντίστοιχα και η αντιμετώπιση του εγκλήματος από τον κοινωνικό έλεγχο ως ένα εξωτερικό τρίγωνο που στις πλευρές του απεικονίζονται τρία είδη «επιβλεπόντων»:

1) Οι «διαχειριστές» (handlers), μια έννοια που πρόσθεσε αργότερα ο M.Felson[164], οι οποίοι είναι πρόσωπα που επιβλέπουν και μπορούν να επηρεάσουν τη δραστηριότητα των πιθανών δραστών. Τέτοιοι μπορεί να είναι οι γονείς, οι κοντινοί συγγενείς, οι φίλοι, οι δάσκαλοι, οι προπονητές κλπ. για την περίπτωση των ανηλίκων και οι κοντινοί συνεργάτες, οι φίλοι, οι συγγενείς, ακόμα και τα παιδιά των ενηλίκων πιθανών δραστών.
2) Οι «φύλακες» (guardians), με τη στενή έννοια, οι οποίοι επιβλέπουν το στόχο του εγκλήματος και αποτελούν τους εκπροσώπους του επίσημου κοινωνικού ελέγχου, όπως η αστυνομία.
3) Οι «ιδιοκτήτες» ή οι «διευθυντές» (managers) του χώρου, μια έννοια που οφείλεται στον Eck[165], είναι εκείνοι που επιβλέπουν τις συνθήκες του εγκλήματος, έχουν το δικαίωμα να ορίζουν ή περιορίζουν την πρόσβαση και τις συμπεριφορές στο χώρο αυτό, να τον προστατεύουν όπως και τα πρόσωπα που βρίσκονται μέσα.

Μετά την κριτική που ασκήθηκε ο Felson άλλαξε τον όρο «εγκληματίας με κίνητρο» σε «πιθανός εγκληματίας» και πρόσθεσε ένα τέταρτο στοιχείο την «απουσία Διαχειριστή». Όπως είδαμε και παραπάνω, ο διαχειριστής μπορεί να είναι κάποιος που σχετίζεται με τον πιθανό εγκληματία, π.χ. γονέας ή παιδί και ασκεί σε αυτόν κάποια μορφή ελέγχου.

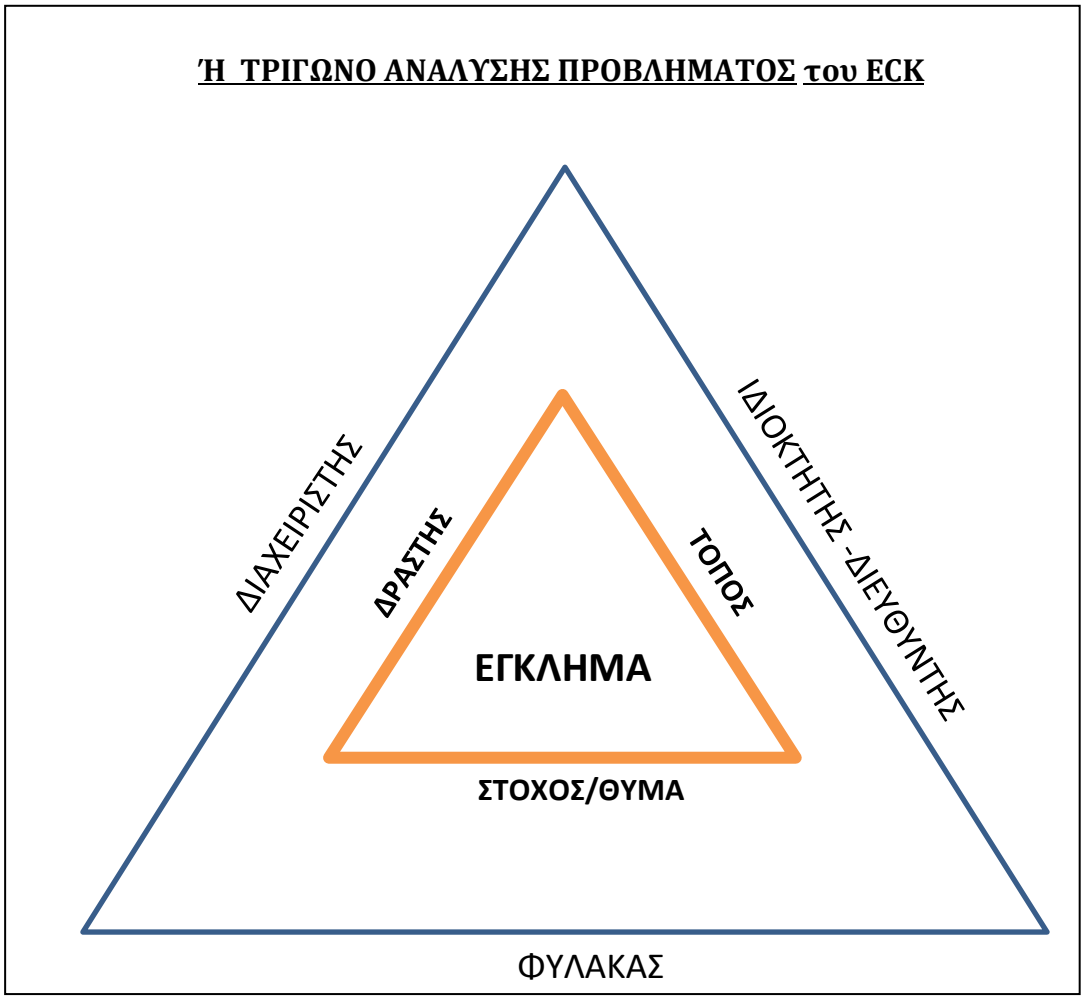
Η απουσία των παραπάνω επιβλεπόντων κάνει το έγκλημα εφικτό. Όταν ο πιθανός δράστης ξεφεύγει από την επίβλεψη των «διαχειριστών», ανακαλύψει στόχους χωρίς

[160] Βλ. Clarke Ronald V. (1999)
[161] Pires Stephen & Clarke Ronald V. (2011)
[162] Clarke Ronald V. (1997), σ.12
[163] Center for problem oriented policing, ό.π.
[164] Felson, Marcus (1986), σσ. 119–128
[165] Eck, John E. (1994)

«φύλακες», σε συνθήκες που δεν παρακολουθούνται από τους «διευθυντές», το έγκλημα θα τελεστεί.[166]

[166] Center for problem oriented policing: A Theory of Crime Problems, ό.π.

Σχήμα 3. ΤΡΙΓΩΝΟ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ [167]



[167] Center for problem oriented policing: A Theory of Crime Problems, ό.π.

Κριτική, επεκτάσεις, διασυνδέσεις της θεωρίας Καθημερινών Δραστηριοτήτων

Η κριτική που ασκήθηκε στην θεωρία των Cohen και Felson επικεντρώθηκε στην απλουστευτική μορφή που παρουσιάζει, εστιάζει περισσότερο στην περιγραφή του εγκλήματος παρά την ερμηνεία του (Jeffery, 1993),[168] παραγνωρίζοντας τους εγκληματογόνους παράγοντες της συμπεριφοράς των ατόμων και τα κίνητρα που την προκαλούν. [169] Ακόμα ένα σημαντικό σημείο κριτικής εστιάζει στην αδυναμία της θεωρίας να παρέχει συγκεκριμένες ελέγξιμες ερευνητικές υποθέσεις σχετικά με δεδομένες καταστάσεις δραστών και θυμάτων. [170]

Οι Cohen και Felson στις δικές τους έρευνες βρήκαν ότι οι δραστηριότητες έξω από το σπίτι αυξάνουν τον κίνδυνο θυματοποίησης[171]. Αντίθετα μελετητές όπως οι Miethe, Stafford & Long τονίζουν ότι συγκεκριμένες δραστηριότητες αυξάνουν την επίβλεψη των στόχων και μειώνουν αντίστοιχα τις πιθανότητες θυματοποίησης. Για παράδειγμα οι δραστηριότητες στο σχολικό και το εργασιακό περιβάλλον αυξάνουν τον αριθμό των ικανών φυλάκων. Επίσης οι Miethe, Stafford & Long επισήμαναν ότι η θεωρία των Καθημερινών Δραστηριοτήτων επικεντρώνεται σε παροδικές αλληλεπιδράσεις των τριών στοιχείων, παραγνωρίζοντας κοινωνικά χαρακτηριστικά όπως το εισόδημα, το φύλο, η ηλικία, η φυλή, η οικογενειακή κατάσταση και ότι η θεωρία έχει περισσότερο εφαρμογή στα εγκλήματα κατά της περιουσίας παρά στα βίαια εγκλήματα.[172]

Από την άλλη πλευρά, υπάρχει πλήθος από μελέτες που επιβεβαιώνουν τη σχέση των καθημερινών δραστηριοτήτων με την εγκληματική δραστηριότητα. Ο τρόπος ζωής στον τόπο κατοικίας ή εργασίας, οι καθημερινές επαφές με άλλα άτομα, ο χρόνος στον οποίο πραγματοποιούνται αυτές οι δραστηριότητες δείχνουν να επηρεάζουν την παρουσία πιθανών δραστών, κατάλληλων στόχων, την απουσία επαρκούς φύλαξης και την συνακόλουθη πιθανότητα ύπαρξης της κατάλληλης ευκαιρίας για το εγκληματικό γεγονός.[173]

Πολλές από τις θυματολογικές έρευνες που ακολούθησαν (Garofalo 1987, Lynch, 1987, Maxfield 1984, Miethe, Stafford, and Long 1987, Miethe and Meier 1990, Sampson and Wooldredge 1987)[174] και (Kennedy & Forde 1990, Massey Krohn & Bonati 1989, Roneck & Maier 1991; [175] Sherman Gartin & Buerger 1989[176]) επιβεβαίωσαν τη σχέση μεταξύ του κινδύνου θυματοποίησης και του τρόπου ζωής, των καθημερινών δραστηριοτήτων, που αυξάνει τις πιθανότητες να συναντηθούν πιθανός δράστης και στόχος.[177]

[168] Jeffery, C.Ray (1993)

[169] Massey James, Krohn Marvin, & Bonati Lisa M. (1989)

[170] Meier & Miethe 1993, όπως αναφέρονται στο: Choi Kyung-shick (2008)

[171] Cohen Lawrence & Felson Marcus (1979), σ.605

[172] Miethe Terance D., Mark C. Stafford, & Scott Long (1987)

[173] Goldstein Arnold P. (1994), σ.56

[174] Βλ. ακόμα Cohen, Kluegel, & Land (1981), Cohen & Felson (1979), Hindelang, Gottfredson & Garofalo (1978), Miethe & McDowall (1993), Wilcox Rountree, Land, & Miethe (1994), Miethe & Meier (1990), όπως αναφέρονται στο Madriz Esther (1996)

[175] όπως αναφέρονται στο: Choi Kyung-shick (2008), ό.π.

[176] Sherman Lawrence, Gartin Patrick & Buerger Michael (1989)

[177] Madriz Esther (1996), ό.π.

Η Elizabeth Groff[178] χρησιμοποιώντας ένα μοντέλο προσομοίωσης σε υπολογιστή υπολόγισε ότι όταν αυξάνεται ο χρόνος που περνάει κάποιος έξω από το σπίτι (από 30% έως 70%) αυξάνονται και οι πιθανότητες να εμπλακεί με την αστυνομία.[179]

Οι Kennedy και Forde το 1990, βρήκαν συσχέτιση της θυματοποίησης από επιθέσεις με τις δραστηριότητες ρουτίνας, ιδιαίτερα των νέων και ανύπαντρων αντρών, έξω από το σπίτι, στη δουλειά ή τη διασκέδαση. Σε παρόμοια συμπεράσματα κατέληξε και η έρευνα των Messner και Tardiff το 1985 για τις ανθρωποκτονίες στη Ν. Υόρκη, όταν επιβεβαιώθηκε η υπόθεσή τους ότι η τοποθεσία και ο τύπος της ανθρωποκτονίας συσχετίζονταν με δημογραφικούς (φύλο, ηλικία, οικογενειακή κατάσταση) και χρονικούς (temporal) παράγοντες (ώρα της ημέρας, εβδομάδα και έτος) που επηρεάζουν το είδος των καθημερινών δραστηριοτήτων των ατόμων, δραστών και θυμάτων.[180]

Η Madriz ερευνώντας τη σχέση μεταξύ της θεωρίας των Cohen και Felson και την αντίληψη του κινδύνου στο χώρο εργασίας συμπέρανε ότι η θεωρία επιβεβαιώνεται από τα ευρήματα. Οι παράγοντες που επηρεάζουν την έκθεση σε κίνδυνο, όπως η «εγγύτητα στον πιθανό δράστη» και «η ελκυστικότητα του στόχου» παρουσιάζουν μεγαλύτερη συσχέτιση με την αντίληψη του κινδύνου στο χώρο εργασίας από ότι τα δημογραφικά και κοινωνικο-οικονομικά χαρακτηριστικά. Η αντίληψη του κινδύνου μετρήθηκε στα ίδια επίπεδα μεταξύ ανδρών και γυναικών και διαφορετικών ηλικιακών ομάδων.[181]

Ο Osgood, όπως και ο Miethe, επισήμανε την αγνόηση, αρχικά, της σημασίας στο κίνητρο του εγκληματία από τους Cohen και Felson. Έτσι πρότεινε την - κάποιου είδους - ανταμοιβή ή όφελος ως κίνητρο στην ευκαιρία διάπραξης κάποιας εγκληματικής δραστηριότητας. Τέτοιου είδους βραχυπρόθεσμα κίνητρα μπορούν να είναι η επιδεικτική κατανάλωση, η επίδειξη «σκληράδας» και το αίσθημα ικανοποίησης. [182]

Προσπάθεια εφαρμογής της μέσω μαθηματικών μοντέλων δεν έλειψαν και από τη θεωρία των «Καθημερινών Δραστηριοτήτων».

Οι Farrell, Clark κ.ά, χρησιμοποιώντας τις «καθημερινές δραστηριότητες» πρότειναν ένα μαθηματικό μοντέλο ερμηνείας της κατ' εξακολούθηση θυματοποίησης σε περιοχές με μεγάλη εγκληματικότητα[183]. Οι Farrell, Clark, Ellingworth και Pease, κατασκεύασαν ένα μαθηματικό μοντέλο για να συσχετίσουν την θεωρία των καθημερινών δραστηριοτήτων με την επαναλαμβανόμενη θυματοποίηση από εγκλήματα βίας και κατά της ιδιοκτησίας, σε περιοχές που συγκεντρώνουν υψηλή εγκληματικότητα. Διαπίστωσαν ότι το μέγεθος συμμετοχής των κατάλληλων στόχων δεν έπαιζε σημαντικό ρόλο στη συγκέντρωση της εγκληματικότητας. Αντίθετα η προσφορά δραστών με κίνητρο και η απουσία ικανών φυλάκων επηρέασαν τόσο το (στατιστικό) δείκτη συγκέντρωσης εγκληματικότητας (αριθμός περιστατικών) όσο και τη συχνότητα επαναλαμβανόμενης θυματοποίησης. Ακόμα διαπίστωσαν ότι η θυματοποίηση γεννά νέα θυματοποίηση, δηλαδή η πιθανότητα επαναλαμβανόμενης θυματοποίησης αυξάνεται από το γεγονός της προγενέστερης θυματοποίησης. Η προηγούμενη θυματοποίηση επηρεάζει την αντίληψη του δράστη για την καταλληλότητα του στόχου. Η καταλληλότητα του στόχου δεν μπορεί να διαπιστωθεί με

[178] Groff Elizabeth (2008)
[179] Morrow Jordan (2014)
[180] Goldstein Arnold P. (1994), σ.55
[181] Madriz Esther (1996), σσ. 407-418
[182] Osgood, D. Wayne, Wilson Janet , O'Malley Patrick, Bachman Jerald & Johnston Lloyd (1996)
[183] Farrell Graham, Clark Ken, Ellingworth Dan, Pease Ken (2005)

ασφάλεια από τον πιθανό δράστη πριν τη πρώτη θυματοποίηση, μόνο εικασίες μπορεί να κάνει σχετικά. Μετά τη διάπραξη του εγκλήματος όμως διαπιστώνεται αν η εικασία αυτή ήταν σωστή και άρα αν ο στόχος ήταν κατάλληλος ή όχι. Οι δράστες επαναλαμβανόμενων εγκλημάτων απέναντι στον ίδιο στόχο είναι συχνά τα ίδια άτομα, επειδή προτιμούν να πλήξουν στόχους που έχουν ήδη διαπιστώσει την καταλληλότητά τους, από προηγούμενη δράση, παρά να αναζητήσουν νέους, αμφίβολης καταλληλότητας στόχους. Έτσι, οι ερευνητές καταλήγουν στο συμπέρασμα ότι τα βασικά στοιχεία της θεωρίας των καθημερινών δραστηριοτήτων ερμηνεύουν ικανοποιητικά τη συγκέντρωση υψηλών δεικτών εγκληματικότητας σε ορισμένες περιοχές.[184]

Η προσθήκη του ωφελιμιστικού κινήτρου του εγκληματία επιτυγχάνει έτσι την διασύνδεση της θεωρίας «Καθημερινών Δραστηριοτήτων» με τη θεωρία της «Ορθολογικής επιλογής».[185] Ο ίδιος ο Felson έγραψε ότι η «ορθολογική επιλογή» εφαρμόζεται στις καθημερινές δραστηριότητες του πιθανού εγκληματία κατά την αλληλεπίδρασή του με τους πιθανούς στόχους και τους πιθανούς φύλακες, γιατί υπάρχουν διαφορετικές πιθανότητες για οφέλη ή κόστη σε διαφορετικές περιστάσεις.[186] Ακόμα ο Felson τόνισε ότι η αρχή της «ήσσονος προσπάθειας», από την ορθολογική επιλογή, εφαρμόζεται και στις εγκληματικές δραστηριότητες επειδή τα άτομα επιδιώκουν να ξοδεύουν το λιγότερο χρόνο ακολουθώντας τη συντομότερη διαδρομή και χρησιμοποιούν τα ευκολότερα μέσα στη δράση τους. Η αρχή αυτή επιβεβαιώνεται από τα ευρήματα ερευνητών για την «εγκληματική διαδρομή», όπως των Carter και Hill το 1980. Οι ερευνητές διαπίστωσαν ότι οι εγκληματικές ευκαιρίες αυξάνονται όσο μειώνεται η απόσταση μεταξύ τόπου κατοικίας του δράστη και τόπου τέλεσης, απόσταση η οποία διανύεται μέσα από γνώριμες για το δράστη διαδρομές.[187] Από την άλλη, έρευνες για το «εγκληματικό ταξίδι», όπως του Morris, διαπίστωσαν διαφοροποίηση εγκληματικότητας ανάμεσα στον τόπο κατοικίας των δραστών σε σχέση με τον τόπο δράσης τους.[188]

Σε συνεργασία με τον Ronald Clarke, ο M.Felson επιχείρησε να συνδυάσει τις δυο θεωρίες, των «Καθημερινών Δραστηριοτήτων» με τη θεωρία της «Ορθολογικής επιλογής», τόσο μεταξύ τους όσο και άλλες θεωρίες, όπως αυτήν της «περιστασιακής πρόληψης του εγκλήματος[189]», τονίζοντας την μεταξύ τους συμβατότητα και αμοιβαία υποστήριξη.[190]

Προσπάθεια διασύνδεσης των δυο θεωριών των «καθημερινών δραστηριοτήτων» και της «ορθολογικής επιλογής» (RAT – RCT), τόσο μεταξύ τους όσο και με την οικονομική θεωρία, παρατηρούμε και στο άρθρο "Human Ecology and Crime: A Routine Activity Approach"(1980)[191] των αρχικών εμπνευστών της RAT, Felson και L.Cohen, όπου αναφέρουν ότι η θεωρία τους είναι «συνεπής με τις οικονομικές αρχές της ατομικής επιλογής που βασίζεται στον υπολογισμό κόστους, οφέλους, κινδύνων κλπ.»[192]

Ακόμα ο Felson σε συνεργασία και με τον Hirschi επιχείρησε σύνθεση των προσεγγίσεων της «καθημερινής δραστηριότητας» με την «ορθολογική επιλογή» και με τη θεωρία του

[184] Farrell Graham, Clark Ken, Ellingworth Dan, Pease Ken (2005)
[185] Brunet, James R. (2002)
[186] Jeffery C. Ray & Zahm Diane L. (2008), σ.338
[187] Goldstein Arnold P. (1994), σσ. 56-57
[188] Ζαραφωνίτου Χριστίνα (1996), σσ. 97-98 και Ζαραφωνίτου Χριστίνα (2004), σ.143
[189] Situational crime prevention
[190] Clarke Ronald V. & Felson Marcus (2008), σ.1
[191] Felson Marcus & Cohen Lawrence E. (1980)
[192] Felson Marcus & Cohen Lawrence E. (1980), σ. 404

«κοινωνικού ελέγχου» του Hirschi, υποστηρίζοντας ότι οι θεωρίες αυτές μάλλον αλληλοσυμπληρώνονται παρά αντικρούουν η μια την άλλη. Η θεωρία του Hirschi χρησιμοποιεί την παραδοχή της ορθολογικής επιλογής, ότι το άτομο αποφασίζει με την ελεύθερη βούλησή του να κάνει τις επιλογές αυτές που του μεγιστοποιούν την ευχαρίστηση και του προκαλούν το μικρότερο πόνο. Ο Hirschi υποστηρίζει επίσης ότι όλα τα άτομα έχουν πιθανότητες να διαπράξουν εγκλήματα όταν δεν υπάρχουν μέτρα κοινωνικού ελέγχου, μέτρα περιορισμού της δράσης των ατόμων.[193] Η τελευταία άποψη δεν απέχει πολύ από αυτή του Felson και του Cohen για την απουσία «ικανών φυλάκων». Ο Felson θεωρεί ότι η «ορθολογική επιλογή» ασχολείται με το περιεχόμενο των αποφάσεων, ενώ η προσέγγιση της «καθημερινής δραστηριότητας», από την πλευρά της, διευκρινίζει το οικολογικό πλαίσιο που παρέχει ένα σύνολο επιλογών από το οποίο λαμβάνονται οι αποφάσεις. [194]

Οι Cornish και Clarke βρίσκουν επίσης ομοιότητες μεταξύ των θεωριών του Felson και Hirschi στο επίπεδο των θέσεών τους για τη ανθρώπινη φύση και στο ότι οι προσεγγίσεις της ορθολογικής επιλογής δεν ασχολούνται μόνο με το έγκλημα, αλλά και με την εγκληματικότητα, όχι μόνο με την έννοια και το περιεχόμενο της λήψης των αποφάσεων, αλλά και με το ιστορικό και το παρόν πλαίσιό τους.[195]

2.3.3. Η Θεωρία των «εγκληματικών προτύπων»

Μια άλλη προσπάθεια διασύνδεσης των «περιβαλλοντολογικών» θεωριών, ακόμα πιο πολυ-παραγοντική και πολυσυλλεκτική, έγινε από τους Brantigham Patricia L. & Brantigham Paul J. στο πλαίσιο της θεωρίας των «εγκληματικών προτύπων».

Όπως σημειώνουν οι συγγραφείς, από τη δεκαετία του ’70, στην ερμηνεία της εγκληματικότητας[196] προστέθηκε μια εναλλακτική προσέγγιση η οποία εστιάζει στα εγκληματικά γεγονότα και όχι στα αίτια της συμπεριφοράς. Αυτή η νέα προσέγγιση προτείνει την εξήγηση των εγκλημάτων ως σύμπλεγμα προτύπων συμπεριφοράς και γεγονότων που προκαλούνται από ποικιλία παραγόντων. Ενώ καμία μονο-παραγοντική προσέγγιση δεν θα μπορούσε να ερμηνεύσει το σύνολο των κατηγοριών του εγκλήματος, τα πρότυπα των εγκληματικών γεγονότων θα μπορούσαν να προσεγγίσουν πολυπαραγοντικά τις διάφορες συνθήκες τέλεσής τους.[197]

Οι βασικές απόψεις της εναλλακτικής προσέγγισης έχουν αναπτυχθεί και εκφραστεί από διάφορες επιμέρους θεωρίες όπως: της «ορθολογικής επιλογής» των Cornish και Clarke, των «καθημερινών δραστηριοτήτων» των Felson και Cohen, της «περιβαλλοντικής εγκληματολογίας» (ή εγκληματικών προτύπων) των Brantingham, του «τρόπου ζωής» των Hildelang κ.ά, την «στρατηγική ανάλυση» του Cusson, των «εγκληματικών ευκαιριών» των Barlow ή των Carroll και Weaver και τις επεκτάσεις των θεωριών αυτών όπως την «περιστασιακή πρόληψη του εγκλήματος» του Clarke, την «πρόληψη του εγκλήματος μέσω περιβαλλοντικού σχεδιασμού» του Jeffery, την ανάλυση των «θερμών σημείων» (Hot Spots) του Block κλπ. [198]

[193] Jeffery C. Ray & Zahm Diane L. (2008), σ.338

[194] Cornish Derek & Clarke Ronald, (1986), σ.10

[195] Cornish Derek & Clarke Ronald, (1986), ό.π.

[196] Την κοινωνιολογική οπτική εξέφρασαν οι Sutherland (1937), Taylor, Walton & Young (1973), Gottfredson & Hirschi, βλ. Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 260

[197] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 260

[198] Brantigham Patricia L. & Brantigham Paul J. (2008), ό.π.

Αυτές οι θεωρίες, σύμφωνα με τους Brantingham[199], παρά τις επιμέρους διαφορές τους παρουσιάζουν πολλά κοινά όπως:

1. Τα εγκληματικά γεγονότα αποτελούν την κατάληξη μιας διαδικασίας σταδιακής απόφασης η οποία, στις περισσότερες των περιπτώσεων οδηγεί σε ορθολογικές, μη τυχαίες και προβλέψιμες δράσεις.[200]
2. Η απόφαση για τη διάπραξη κάθε συγκεκριμένου εγκλήματος λαμβάνεται από κάποιον που διαθέτει την ετοιμότητα, το κίνητρο, τη γνώση και την κατάλληλη ευκαιρία που του παρουσιάζεται στο πλαίσιο των κανονικών (μη-εγκληματικών) καθημερινών του δραστηριοτήτων σε γνώριμα μέρη, όπως γειτονιά, εργασία, χώροι διασκέδασης κ.ά. όπου περνά σημαντικό μέρος του χρόνου του.[201]
3. Τα κίνητρα ή η ετοιμότητα συνδέονται με την επίτευξη στόχων, απόκτηση οικονομικού οφέλους, επιθυμία για συναρπαστική δράση, διασκέδαση, εξουσία ή από τη ροπή στη βία, τη συναισθηματική συμπεριφορά, την εκδικητικότητα.[202]
4. Η μετουσίωση της απόφασης σε δράση επηρεάζεται από την ψυχολογική, την κοινωνική κατάσταση του δράστη, το οικονομικό περιβάλλον, τις προηγούμενες εμπειρίες του και τις διαθέσιμες ευκαιρίες.[203]
5. Ο αριθμός και η χρονολογική σειρά των αποφάσεων διαφέρουν ανάλογα με τον τύπο του κάθε εγκλήματος. Κάποια εγκλήματα απαιτούν μεγαλύτερο χρόνο κατά τη λήψη της απόφασης, ενώ κάποια άλλα λιγότερο.[204]
6. Το επίπεδο εγκληματικής ετοιμότητας κάθε ατόμου διαφέρει ανάλογα με το χρόνο, τον τόπο, την ατομική κατάσταση και τις συνθήκες της συγκεκριμένης τοποθεσίας.[205]
7. Οι πιθανοί δράστες, οι ευκαιρίες για δράση, άρα και τα εγκλήματα, δεν κατανέμονται ομοιόμορφα στον χώρο και τον χρόνο. Συγκεκριμένες μορφές εγκλήματος τείνουν να συγκεντρώνονται στις τοποθεσίες των στόχων και στα πρότυπα των καθημερινών διαδρομών των πιθανών δραστών. Οι τοποθεσίες αυτές διαφοροποιούνται ανάλογα με την ώρα της ημέρας, τα χαρακτηριστικά των στόχων, τον περιβάλλοντα χώρο και την κατάσταση γύρω από τον πιθανό στόχο. Έτσι οι καθημερινές δραστηριότητες ρουτίνας τόσο των δραστών όσο και των στόχων διαμορφώνουν το πρότυπο των ευκαιριών για δράση.[206]

Η καταλληλότητα του στόχου συνδέεται όχι μόνο με τις ιδιότητες του στόχου αλλά και με αυτές του περιβάλλοντός του. Η επιλογή του κατάλληλου στόχου είναι από μόνη της μια πολυσύνθετη διαδικασία απόφασης, ανάλογα με την αντίληψη και γνώση του περιβάλλοντος. Τα άτομα διαμορφώνουν «εικόνες» για το περιβάλλον τους ανάλογα με τα χαρακτηριστικά

[199] Brantigham Patricia L. & Brantigham Paul J. (2008), σσ. 261-262

[200] Βλ. Clarke & Cornish Derek (1985), Cusson (1983), Brantigham Patricia L. & Brantigham Paul J., 1978, et.al. στο Brantigham Patricia L. & Brantigham Paul J (2008), σ. 261

[201] Βλ. Clarke Roland & Cornish Derek (1985), Brantigham Patricia L. & Brantigham Paul J. (1981) και (1984)

[202] Βλ. Cusson 1(983), West (1982), όπως αναφέρονται στο Brantigham Patricia L. & Brantigham Paul J., ό.π., σ. 262

[203] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 262

[204] Βλ. Maguiren(1982), Gabor et.al.(1987), όπως αναφέρονται στο Brantigham Patricia L. & Brantigham Paul J., ό.π.

[205] Βλ. Cromwell et.al.(1991), Brantingham (1991), Gottfredson & Hirschi (1990), όπως αναφέρονται στο Brantigham Patricia L. & Brantigham Paul J., ό.π.

[206] Βλ, Felson (1987), Cohen & Felson 1979, όπως αναφέρονται στο Brantigham Patricia L. & Brantigham Paul J., ό.π.

του περιβάλλοντος, τις λεπτομέρειες, τις συνθήκες που συνδέονται με την κάθε δεδομένη δράση.

Σύμφωνα με τους Brantingham, αυτές οι «εικόνες», που αντανακλούν την διαδικασία σχηματισμού της αντίληψης των αντικειμένων της πραγματικότητας στο πλαίσιο του πολύπλοκου περιβάλλοντος, αποτελούν μοντέλα, πρότυπα (templates, prototypes, place schemata) [207]. Τα πρότυπα αυτά διαφέρουν ανάλογα με το είδος εγκλήματος, τον εγκληματία και τις συνθήκες. Από την άλλη παρατηρούνται ομοιότητες στον τρόπο με τον οποίο τα άτομα εμπλέκονται με το έγκλημα και τον τρόπο που αντιλαμβάνονται τις εικόνες του περιβάλλοντος, έτσι ώστε μπορούμε να δημιουργήσουμε γενικευμένα μοντέλα (templates) που θα μας επιτρέψουν να ερμηνεύουμε τα συγκεκριμένα εγκληματικά πρότυπα (crime patterns).

Συνδυάζοντας τα κοινά σημεία των διαφορετικών θεωριών, που συγκροτούν τη νέα προσέγγιση της περιβαλλοντικής εγκληματολογίας, οι Brantingham πρότειναν τη θεωρία των «εγκληματικών προτύπων». Η θεωρία διερευνά τα πρότυπα του εγκλήματος και της εγκληματικής συμπεριφοράς. Τα πρότυπα είναι κατανοητά επειδή διαθέτουν ομοιότητες αν τα δούμε υπό την οπτική της διαδικασίας λήψης της απόφασης, σε συνδυασμό με τα κίνητρα, τις ευκαιρίες, το σκηνικό που διαδραματίζεται η δράση των εγκληματιών και των θυμάτων. Το πρότυπο αφορά «την περιγραφή αναγνωρίσιμων διασυνδέσεων αντικειμένων, διαδικασιών ή ιδεών». Έτσι μπορούμε να κατασκευάσουμε διακριτά πρότυπα για τους εγκληματίες και τα εγκλήματα. Όλα τα εγκλήματα, οι αποφάσεις και οι διαδικασίες διάπραξης των εγκλημάτων μπορούν να μελετηθούν με τη χρήση προτύπων. Άλλα πρότυπα σχηματίζονται στη βάση του συγκεκριμένου γεγονότος που ενεργοποιεί τη δράση, ενώ άλλα επηρεάζονται από τις προηγούμενες εμπειρίες, την διαθεσιμότητα κατάλληλων στόχων, το σκηνικό της δράσης, το χώρο, την περίσταση και τους ευρύτερους κοινωνικο-οικονομικούς παράγοντες και τα περιβάλλοντα που σχετίζονται με την ετοιμότητα του δράστη.[208]

Τα πρότυπα αυτά γίνονται πιο εμφανή όταν τα εγκλήματα εξετάζονται στο πλαίσιο και ως αποτέλεσμα ενός πολυσύνθετου περιβάλλοντος. Το περιβάλλον αποτελεί για το έγκλημα ένα σκηνικό που διαρκώς μεταβάλλεται και παραλλάσσεται. Τα εγκλήματα δεν έχουν τυχαία ή ομοιόμορφη διασπορά στο χώρο, το χρόνο και στην κοινωνία, μεταξύ των διαφορετικών γειτονιών, κοινωνικών ομάδων ή των διαφορετικών δραστηριοτήτων ενός ατόμου κατά την διάρκεια των καθημερινών του ενασχολήσεων ή την διάρκεια της ζωής του. Για να κατανοήσουμε την εγκληματική συμπεριφορά και να κατασκευάσουμε ξεκάθαρα πρότυπα πρέπει να ερμηνεύσουμε τα εγκληματικά γεγονότα σε σχέση με τις παραλλαγές του περιβάλλοντος, σαν μια δράση σε μια κατάσταση που η διαδικασία της απόφασης διαδραματίζεται σε ένα διαρκώς εναλλασσόμενο σκηνικό. Η διαδικασία της απόφασης μελετάται ως αποτέλεσμα διασύνδεσης των δραστηριοτήτων του δράστη με αυτό του θύματος, των κινήτρων του δράστη σε συνδυασμό με το σκηνικό των ευκαιριών.[209]

Έτσι το έγκλημα λαμβάνει χώρα όταν α) ένας δράστης με ετοιμότητα, β) συναντά ένα κατάλληλο στόχο, γ) σε μια κατάσταση που ενεργοποιεί την ετοιμότητα του δράστη. Στο πλαίσιο αυτό το έγκλημα αντιμετωπίζεται ως ένα γεγονός του οποίου τα στοιχεία αποτελούν μεταβλητές. Πρώτα η ετοιμότητα διαφέρει από άτομο σε άτομο, ανάλογα με την μεταβολή του σκηνικού του περιβάλλοντος στο χώρο και το χρόνο και την αντίληψη του ατόμου για τις

[207] Βλ. Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 287

[208] Brantigham Patricia L. & Brantigham Paul J. (2008), σσ. 288-290

[209] Brantigham Patricia L. & Brantigham Paul J. (1993)

ευκαιρίες που του παρουσιάζονται. Δεύτερον η καταλληλότητα των στόχων διαφοροποιείται ανάλογα με το πώς αυτοί κατανέμονται διαφορετικά στο χώρο και το χρόνο και όταν το περιβάλλον αλλάζει. Τρίτον, η κατάσταση που ενεργοποιεί την συμπεριφορά διαφοροποιείται ανάλογα με την κατανομή των στόχων και την ετοιμότητα του δράστη. Τα κίνητρα επηρεάζουν την εγκληματική δράση, ενώ και τα χαρακτηριστικά του στόχου και οι αποφάσεις σχετικά με την καταλληλότητα των ευκαιριών επηρεάζουν, με τη σειρά τους, τα κίνητρα.[210]

Οι πιθανοί δράστες, σύμφωνα με τη θεωρία των Brantingham, ανακαλύπτουν στόχους στο πλαίσιο των καθημερινών δραστηριοτήτων τους κινούμενοι ανάμεσα σε γνώριμα «κομβικά» σημεία δράσης (κόμβοι, nodes), όπως είναι το σπίτι, η εργασία, μέρη που συχνάζουν για διασκέδαση κλπ. Τους κόμβους διασυνδέουν «μονοπάτια», δίοδοι (paths), όπως δρόμοι, δίκτυα επικοινωνίας ή άλλοι οδοί που χρησιμοποιούν τα άτομα καθημερινά.[211] Ακόμα, το αστικό περιβάλλον περιλαμβάνει «όρια» (edges) που διαχωρίζουν με σαφήνεια τον έναν χώρο από τον άλλον. Τα όρια μπορεί να είναι φυσικά, όπως ένα ποτάμι που προσδιορίζει τα σύνορα μεταξύ δυο ιδιοκτησιών ή νοητά, όπως τα ισχυρά νοητικά σχήματα που συνιστά η διαφορετική χρήση γης μεταξύ δυο πλευρών ενός δρόμου ή τα τοπικά όρια που προσδιορίζονται από την ύπαρξη διαφορετικών ομάδων ανθρώπων.[212]

Το έγκλημα συγκεντρώνεται σε κόμβους (nodes) με υψηλά επίπεδα δραστηριότητας, κατά μήκος κεντρικών οδών (paths) και στα όρια (edges). Έτσι η οικιστική πύκνωση τείνει να συγκεντρώνει εγκλήματα κατά της ιδιοκτησίας, τα βίαια εγκλήματα συγκεντρώνονται σε χώρους διασκέδασης (μπαρ κλπ.) και σε οικοδομικά τετράγωνα. Οι περιοχές που εμφανίζουν περισσότερα εγκλήματα κατά της περιουσίας είναι αυτές που βρίσκονται κοντά σε κόμβους, όπως σχολεία, κέντρα διασκέδασης, κεντρικούς δρόμους, σε πυκνοκατοικημένες γειτονιές με ανομοιογενή πληθυσμό (από πλευράς φυλετικών και πολιτισμικών χαρακτηριστικών) και κατοίκους που περνούν τον περισσότερο χρόνο τους εκτός κατοικίας.[213]

Αν δούμε το αστικό περιβάλλον, στην διάσταση της περιβαλλοντικής ποικιλομορφίας, σε συνδυασμό με το ότι συγκεκριμένα εγκλήματα συνδέονται με ορισμένα κοινωνικο-οικονομικά χαρακτηριστικά τότε τα οικιστικά πρότυπα γίνονται ευδιάκριτα. Παράλληλα χαρτογραφώντας αυτές τις περιοχές που κινούνται, κατοικούν, εργάζονται, διασκεδάζουν οι πιθανοί δράστες εγκλημάτων, ως καθημερινή τους δραστηριότητα, μπορούμε να εντοπίσουμε τα πραγματικά σημεία που συγκεντρώνουν την εγκληματική δραστηριότητα.

Η διάκριση μεταξύ των πιθανών δραστών, σε «εσωτερικούς», γνωστούς ή «δικτυωμένους» (insiders) και «εξωτερικούς», αγνώστους ή «παρείσακτους» (outsiders), είναι σημαντική για την κατανόηση του σχηματισμού του «μοντέλου» (template) του εγκλήματος από τον δράστη και κατά συνέπεια του γενικότερου εγκληματικού προτύπου (pattern). Όπως αναφέρουν οι συγγραφείς, η παρουσία ξένων σε κοινότητες, όπως οι γειτονιές (ή σε οργανισμούς όπως οι επιχειρήσεις) ενεργοποιεί ταχύτερα το αίσθημα εδαφικότητας ή κτητικότητας που αναπτύσσουν κάποιοι άνθρωποι για μέρη ή αντικείμενα και κατά συνέπεια την αύξηση της επαγρύπνησης και της φύλαξης.[214]

Τα όρια συγκεντρώνουν μεγάλο αριθμό εγκλημάτων, επειδή εκεί οι άγνωστοι και οι ξένοι (outsiders) είναι πιο αποδεκτοί ή περνούν πιο απαρατήρητοι. Τα όρια είναι χώροι, με

[210] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 266
[211] Benson Michael, Madensen Tamara D, & Eck John E. (2009), σσ. 175-193
[212] Brantigham Patricia L. & Brantigham Paul J. (1993) , σσ. 17-18
[213] Brantigham Patricia L. & Brantigham Paul J. (1993), σ. 21
[214] Brantigham Patricia L. & Brantigham Paul J. (1993), σ. 20

πρόσβαση στον καθένα, που διαθέτουν χρήσεις και φυσικά χαρακτηριστικά, ιδιαίτερα οι κεντρικοί δρόμοι, που προσφέρουν κατάλληλες ευκαιρίες για εγκληματική δράση. [215]

Αντίθετα, οι «εσωτερικοί» πιθανοί εγκληματίες μπορούν να δραστηριοποιούνται εντός των ορίων του γνώριμου περιβάλλοντός τους, της κοινότητας, της γειτονιάς (ή της επιχείρησης) στο πλαίσιο των καθημερινών, νόμιμων απασχολήσεων τους, όπου περνούν απαρατήρητοι. Ανήκοντας εκεί, κοινωνικά και πολιτισμικά, έχουν αναπτύξει γνώση για την περιοχή, τις συνήθειες των άλλων ατόμων, τις συνθήκες φύλαξης των χώρων, συνήθως δεν θεωρούνται ύποπτοι πιθανών εγκλημάτων. Η γνώση, της γεωγραφικής περιοχής και των καθημερινών δραστηριοτήτων των ατόμων μέσα σε αυτή, δίνει τη δυνατότητα σχηματισμού ενός εγκληματικού προτύπου για ένα συγκεκριμένο εγκληματικό γεγονός.

Συνοψίζοντας τα σημαντικά στοιχεία που πρέπει να λαμβάνονται υπόψη, σύμφωνα με την άποψη των Brantingham, για το σχηματισμό του προτύπου είναι:

1) Η διαδικασία διάπραξης του εγκλήματος και το γεγονός που ενεργοποιεί την ετοιμότητα ή την επιθυμία του δράστη. Στο πλαίσιο κάποιας (καθημερινής) δραστηριότητας, συμβαίνει κάποιο γεγονός που «ενεργοποιεί» την επιθυμία ή την προθυμία του ατόμου το οποίο κρίνει ότι η περίσταση και ο χώρος είναι κατάλληλος για τη διάπραξη του εγκλήματος άμεσα ή ότι πρέπει να περιμένει και να επανέλθει όταν οι συνθήκες και ο χώρος θα είναι κατάλληλα.

2) Τα εγκληματικά πρότυπα και οι δραστηριότητες του δράστη. Οι πιθανοί δράστες των εγκλημάτων, όπως και οι μη δράστες, περνούν τον περισσότερο χρόνο τους σε νόμιμες καθημερινές δραστηριότητες που συνιστούν ένα πρότυπο σκηνικό στο οποίο διαδραματίζονται και οι εγκληματικές δραστηριότητες και που το πρότυπο αυτό μπορεί να μελετηθεί. Οι συγκεκριμένες δράσεις έχουν άμεση σχέση με τα προηγούμενα, πρόσφατα δημιουργημένα, πρότυπα καθημερινών δραστηριοτήτων. Αυτές διαμορφώνουν έναν χώρο δραστηριοτήτων από τον οποίο οι δράστες διαμορφώνουν έναν αναγνωρίσιμο χώρο (awareness space). Ο αναγνωρίσιμος χώρος δεν είναι απεριόριστος χρονικά και εδαφικά. Αρχικά οι δράστες ξεκινούν με κάποιο χώρο που γνωρίζουν από καθημερινές και νόμιμες δραστηριότητες. Ο κάθε δράστης, όπως και ο μη δράστης, γνωρίζει τους χώρους στους οποίους κινείται καθημερινά, το χώρο εργασίας, κατοικίας, διασκέδασης κλπ, οι χώροι αυτοί συμπίπτουν στον χρόνο με τις καθημερινές δραστηριότητες των θυμάτων/στόχων, έτσι διαμορφώνεται ένα πρότυπο εγκληματικής δράσης (activity space)[216]. Οι καθημερινές δραστηριότητες μπορούν να αλλάζουν σύμφωνα με τις προηγούμενες εμπειρίες και καθώς αλλάζουν οι τρόποι μετακίνησης. Η επέκταση των μεγαλουπόλεων, των σύγχρονων μέσων μεταφοράς και των αυτοκινητοδρόμων διαφοροποιούν τόσο τα πρότυπα των μετακινήσεων, όσο και των δραστηριοτήτων ρουτίνας και του αναγνωρίσιμου χώρου. [217]

Οι καθημερινές δραστηριότητες, ο χώρος δράσης, τα γνώριμα μέρη και τα πρότυπα του εγκλήματος διαφέρουν από άτομο σε άτομο, όμως διαμορφώνουν γενικευμένα πρότυπα για κάθε κατηγορία ατόμων και τύπου εγκλήματος. Τα πρότυπα αυτά διαμορφώνονται στη κοινή βάση παραγόντων όπως το φύλο, η ηλικία, το εισόδημα, ο τόπος κατοικίας, τα κοινωνικά δίκτυα, οι χώροι διασκέδασης και ο γεωγραφικός χώρος διαδρομών ή δρόμων ταχείας κυκλοφορίας.

[215] Brantigham Patricia L. & Brantigham Paul J. (1993), σσ. 17-19

[216] Brantigham Patricia L. & Brantigham Paul J. (1993), σσ. 9-11

[217] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 269

Οι διαδικασίες των αποφάσεων, ο γνώριμος χώρος, η περίσταση, οι καθημερινές συνήθεις δραστηριότητες, δραστών και στόχων, η ύπαρξη στόχων, διαμορφώνουν το πρότυπο του εγκληματικού γεγονότος.

3) Η ετοιμότητα ή η επιθυμία του δράστη συνδέεται με κάποιο κίνητρο, με την επιδίωξη κάποιου σκοπού, που με τη σειρά τους συνδέονται με τις καθημερινές δραστηριότητες στο πλαίσιο των γνώριμων τόπων, τα γεγονότα που ενεργοποιούν τη δράση (triggering events) και το πρότυπο (template) για το τι αποτελεί κατάλληλο στόχο. Η ένταση της επιθυμίας ή ο βαθμός ετοιμότητας διαφέρει ανάλογα με τον τύπο του εγκλήματος, το χώρο, την περίσταση, τις προηγούμενες εγκληματικές εμπειρίες, την ηλικία και την κοινωνικο-οικονομική κατάσταση του ατόμου.

4) Η αλληλεπίδραση της διαδικασίας, του προτύπου, της δραστηριότητας και της ετοιμότητας σε συνδυασμό με το περιβαλλοντικό σκηνικό.[218]

Η άποψη των Brantigham για το σχηματισμό του εγκληματικού προτύπου αποτελεί μια σημαντικότατη συνεισφορά στην περιβαλλοντική αντίληψη του εγκλήματος. Θέτει ταυτόχρονα το εγκληματικό γεγονός, τον πιθανό δράστη, το στόχο, το συγκεκριμένο χώρο, χρόνο και περίσταση στο ίδιο περιβαλλοντικό σκηνικό (environmental backcloth) που μπορεί και αυτό με τη σειρά του να σχηματοποιηθεί, σε προβλέψιμο και σταθερό ή μη, πρότυπο[219].

2.3.4. Η στρατηγική της «περιστασιακής πρόληψης του εγκλήματος»

Η «περιστασιακή πρόληψη του εγκλήματος» εμφανίστηκε σχεδόν ταυτόχρονα σε Ηνωμένο Βασίλειο και ΗΠΑ κατά τη δεκαετία του ’70, εφαρμόστηκε στο σχεδιασμό για την πρόληψη κυρίως των εγκλημάτων κατά της ιδιοκτησίας παρά κατά των προσώπων.

Στις ΗΠΑ οι προσεγγίσεις αυτές, που πήραν την ονομασία «πρόληψη του εγκλήματος μέσω περιβαλλοντικού σχεδιασμού» ή όπως εκφράστηκε από τον Jeffery CPTED (crime prevention through environmental design), εστίασαν στη σημασία του φυσικού περιβάλλοντος για την ενθάρρυνση της διάπραξης ή την αποτροπή των ευκαιριών του εγκλήματος.

Ο Jeffery σημειώνει για το CPTED ότι όσον αφορά το έγκλημα εστιάζει στο περιβάλλον παρά στον εγκληματία. Προτιμότερο είναι να αντιμετωπίζουμε το έγκλημα πριν αυτό γίνει, διαμορφώνοντας το περιβάλλον, παρά να «μεταχειριστούμε» (αντιμετωπίσουμε) τον εγκληματία αφού εγκληματήσει. Με τον άμεσο έλεγχο του περιβάλλοντος, όπως με κάποιο μέτρο ασφαλείας π.χ. μια ατσάλινη μπάρα στη βιτρίνα, μειώνουμε τις εγκληματικές ευκαιρίες, ενώ με τα έμμεσα προληπτικά μέτρα κοινωνικής πολιτικής, όπως βελτίωση της εκπαίδευσης ή της επαγγελματικής κατάρτισης του εγκληματία, δεν θα τον αποτρέψουμε, συγκεκριμένα, να σπάσει τη βιτρίνα καταστήματος για να κλέψει.[220]

Ο Jeffery δεν αποδέχθηκε το κοινωνιολογικό-οικολογικό μοντέλο, που εστιάζει στη σχέση ατόμου με άτομο, την κοινωνική αποδιοργάνωση και την κοινωνική μάθηση, στην εξήγηση της συμπεριφοράς χωρίς αναφορά στον παράγοντα χρόνο και τόπο. Απέρριψε ακόμα το μοντέλο της ποινικής μεταχείρισης, της καταστολής και των ποινών, που ακολουθεί η κλασική σχολή και η ορθολογική επιλογή. Πρότεινε το βιολογικο-οικολογικό μοντέλο που εστιάζει στη σχέση ατόμου – φυσικού περιβάλλοντος και βασίζεται στο θετικισμό, στην ψυχολογική θεωρία μάθησης, στη βιολογία, στην ψυχολογία και στην περιβαλλοντική κοινωνιολογία που βλέπει το περιβάλλον περισσότερο στην φυσική παρά την κοινωνική του διάσταση.

[218] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 266
[219] Brantigham Patricia L. & Brantigham Paul J. (1993), σ.6
[220] Goldstein Arnold P. (1994), σσ.121-122

Μαθητής του Sutherland και του Burgess, ο Jeffery επιχείρησε να συνδέσει το διαφορικό συγχρωτισμό και τη διαδικασία μάθησης της εγκληματικής συμπεριφοράς με τους μηχανισμούς μάθησης της συμπεριφοριστικής προσέγγισης.[221]

Η κεντρική θέση του Jeffery[222] όπως αυτή σημειώνεται στο CPTED, είναι ότι η απάντηση κάθε οργανισμού στα ερεθίσματα του φυσικού του περιβάλλοντος είναι αποτέλεσμα εγκεφαλικής λειτουργίας. Έτσι το περιβάλλον επηρεάζει την συμπεριφορά αλλά μόνο μέσω του εγκεφάλου, κατά συνέπεια όλα τα μέτρα για την πρόληψη του εγκλήματος πρέπει να επικεντρωθούν όχι μόνο στο φυσικό περιβάλλον αλλά και στο άτομο και τις εγκεφαλικές του λειτουργίες.[223] Τα μέτρα αυτά δεν πρέπει να στηρίζονται στην ποινική καταστολή (σύλληψη - καταδίκη- φυλάκιση), αλλά στη θεραπευτική επιστημονική αντιμετώπιση και τον έλεγχο της συμπεριφοράς πριν αυτή εκδηλωθεί.[224]

Την ίδια εποχή, στο Ηνωμένο Βασίλειο η *πρόληψη* έχει τις απαρχές της στο έργο του Home Office Research Unit όταν οι ερευνητές του, Clarke, Mayhew και συνεργάτες, διαπίστωσαν ότι τα περιστασιακά και περιβαλλοντικά χαρακτηριστικά των σωφρονιστικών καταστημάτων ανηλίκων είχαν πιο αιτιώδη σχέση με την παραβατική συμπεριφορά από ότι τα προσωπικά χαρακτηριστικά των ανηλίκων δραστών. Η κατάλληλη αντιμετώπιση, με την αλλαγή ή μετατροπή των περιστασιακών και περιβαλλοντικών συνθηκών, θα μπορούσε να βοηθήσει όχι μόνο στη μείωση των αποδράσεων και της υποτροπής των καταδικασθέντων, αλλά και στην πρόληψη των εγκληματικών ευκαιριών του καθημερινού εγκλήματος. Η αρχική εργασία του Clarke είχε πολλά κοινά σημεία με αυτή του Jeffery, ενώ ο αργότερα ο Clarke, προσχώρησε στο οικονομικό μοντέλο της ορθολογικής επιλογής.[225]

Η προσέγγιση της ορθολογικής επιλογής των Clarke και Cornish εφαρμόστηκε στην περιστασιακή πρόληψη του εγκλήματος, μεταφέροντας το πεδίο μελέτης στο γεγονός καθαυτό ως μονάδα ανάλυσης, σε δυο κατευθύνσεις, αρχικά της διερεύνησης συγκεκριμένων εγκλημάτων και έπειτα στην αναζήτηση πολιτικών ελέγχου του εγκλήματος. Το πρώτο καθίσταται εφικτό μέσω της μελέτης της διαδικασίας λήψης της απόφασης για τη κατανόηση της επιλογής του στόχου και της μεθόδου διάπραξης του εγκλήματος. Το δεύτερο, η ανάπτυξη πολιτικών περιπτωσιολογικών μέτρων αντιμετώπισης συνίσταται στην ανάπτυξη μεθόδων που θα αυξάνουν το ρίσκο και το μέγεθος της καταβαλλόμενης προσπάθειας, θα μειώνουν το αναμενόμενο όφελος από το συγκεκριμένο έγκλημα, μειώνοντας παράλληλα τις πιθανότητες να μετατοπιστεί το έγκλημα κάπου αλλού.[226]

Ο Ronald V.Clarke, λαμβάνοντας υπόψη του τις δυο προσεγγίσεις, του Home Office και CPTED στην εργασία του, για την περιστασιακή πρόληψη του εγκλήματος, πρότεινε ότι η πρόληψη θα πρέπει να περιλαμβάνει μέτρα, σύμφωνα με πέντε διαστάσεις.

Πρώτη, η διάσταση της απαιτούμενης προσπάθειας, σε κόπο, χρόνο, δυσκολία, για την τέλεση του εγκλήματος.

Δεύτερη, η πιθανότητα ανακάλυψης της δράσης.

Τρίτη, τα αναμενόμενα οφέλη από δράση.

[221] Cornish Derek (1993), σσ. 351-382

[222] Όπως διαμορφώθηκε στην έκδοση του 1977 για το Crime Prevention through Environmental Design του Jeffery.

[223] Jeffery C. Ray & Zahm Diane L. (2008), σ.340

[224] Jeffery C. Ray & Zahm Diane L. (2008), σ. 346

[225] Jeffery C. Ray & Zahm Diane L (2008), σ.323

[226] Cornish Derek (1993), σσ. 351-382

Τέταρτη, οι περιβαλλοντικές συνθήκες που δημιουργούν ευκαιρίες για την δράση.

Πέμπτη διάσταση, η δυνατότητα του δράστη να σχηματίσει ικανές δικαιολογίες για την δράση του.

Τα μέτρα αυτά:

α) απευθύνονται σε ιδιαίτερα εξειδικευμένες μορφές εγκλημάτων,

β) περιλαμβάνουν την συστηματική διαχείριση του άμεσου περιβάλλοντος,

γ) συντείνουν στην δυσχέρεια διάπραξης, την αύξηση της πιθανότητας ανακάλυψης του δράστη και του συνακόλουθου ρίσκου από πλευράς του, την μείωση του αναμενόμενου για το δράστη οφέλους και της πιθανής εκλογίκευσης της δράσης του.[227]

Έτσι, σε αντίθεση με τις επικρατούσες μέχρι τότε αντιλήψεις, για προληπτική πολιτική ή για πολιτική επανένταξης που απευθύνονται στα χαρακτηριστικά του ατόμου – εγκληματία, η περιστασιακή πρόληψη του εγκλήματος εστιάζει στην αλλαγή των περιβαλλοντικών συνθηκών και τη μείωση των εγκληματικών ευκαιριών. Αυτό γίνεται με την αύξηση της πιθανότητας να προσλάβουν οι πιθανοί εγκληματίες τη διάπραξη του εγκλήματος ως υπερβολικά κοπιαστική, ριψοκίνδυνη και κοστοβόρο διαδικασία.[228]

Ο Rick Linden, σύμφωνα με την περιστασιακή πρόληψης του εγκλήματος, πρότεινε ότι οι στρατηγικές πρόληψης πρέπει να κατευθύνονται σε πέντε τομείς σύμφωνα με την παρακάτω τυπολογία:

1. Προγράμματα κοινωνικής ανάπτυξης, όπου μέσω εκπαιδευτικών προγραμμάτων για γονείς, παιδιά και ενηλίκους αποσκοπείται η αλλαγή των κοινωνικών συνθηκών και η συνακόλουθη μείωση του αριθμού των δραστών με κίνητρο.
2. Περιστασιακή πρόληψη που εστιάζει στο εγκληματικό γεγονός καθαυτό, με την αύξηση της φύλαξης και τη μείωση της ελκυστικότητας πιθανών στόχων.
3. Κοινωνικά προγράμματα πρόληψης του εγκλήματος με την εμπλοκή των μελών της κοινότητας στην φύλαξη των στόχων.
4. Διοικητικά και νομοθετικά μέτρα για την ρύθμιση των επιχειρηματικών δραστηριοτήτων.
5. Αστυνομικά προληπτικά μέτρα, όπως η αύξηση των περιπολιών και προληπτικών ελέγχων σε περιοχές που συγκεντρώνουν υψηλούς δείκτες εγκληματικότητας.[229]

Ένα από τα κεντρικά σημεία κριτικής που δέχθηκαν όλες οι προσεγγίσεις των «εγκληματικών ευκαιριών» ήταν το θέμα της μετατόπισης (displacement). Αυτό αφορά την άποψη ότι αν εμποδίσουμε τις ευκαιρίες ώστε το συγκεκριμένο έγκλημα να μην συμβεί σε ορισμένο χώρο και χρόνο, τότε αυτό θα λάβει άλλη μορφή και θα μεταφερθεί σε κάποιο άλλο στόχο, χρόνο, χώρο ή θα τελεστεί με άλλη μέθοδο[230]. Πράγματι κάποιες μελέτες φάνηκε να υποστηρίζουν με τα ευρήματα τους αυτήν την άποψη.[231]

Όμως άλλες έρευνες[232] όχι μόνο δεν επιβεβαίωσαν μετατόπιση της εγκληματικότητας,[233] αλλά διαπίστωσαν αντίθετα «διασπορά της ωφέλειας», δηλαδή ότι τα προληπτικά μέτρα

[227] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626

[228] Goldstein Arnold P. (1994), σσ.121-122

[229] Linden Rick (2007), σσ. 139 - 159

[230] Cornish Derek (1993)

[231] Βλ. αναφορά σε Press 1971, Chaiken , Lawless, & Stevenson 1974, στο Goldstein Arnold P. (1994), σσ. 129-130

[232] Βλ. Barr and Pease 1990, Ekblom 1988, Gabor 1990, στο Goldstein Arnold P., ό.π. και στο Clarke Ronald V. (1997), σ.28

είχαν το επιθυμητό αποτέλεσμα στη μείωση των εγκλημάτων γενικότερα και όχι μόνο αυτών στα οποία τα μέτρα αρχικά απευθυνόταν.[234]

Άλλωστε η εφαρμογή προσεγγίσεων που εστιάζουν στην λήψη απόφασης, όπως αυτή της ορθολογικής επιλογής, μπορούν να εξηγήσουν και να αντιμετωπίσουν καλύτερα το θέμα της μετατόπισης του εγκλήματος μέσω της μελέτης των κινήτρων και των άλλων παραγόντων που επηρεάζουν τις αποφάσεις των δραστών. Η προσέγγιση της ορθολογικής επιλογής, μέσω της λειτουργίας της ως θεωρία ανάλυσης εστιασμένη στην προληπτική πολιτική της δράσης σε μικρο – επίπεδο, προσφέρει το μοντέλο κατανόησης του μηχανισμού λήψης της εγκληματικής απόφασης σε συνδυασμό με τη διάπραξη του εγκλήματος (βλ. και «στρατηγική ανάλυση» του Cusson) αλλά και με την αρχική εμπλοκή.[235]

Σύμφωνα με τον Cornish, η χρησιμοποίηση μιας ανάλυσης που εστιάζει στη διαδικασία λήψης της απόφασης για τη διάπραξη του συγκεκριμένου εγκλήματος επιτρέπει την εξήγηση των διαδικασιών της αρχικής εμπλοκής, της διάπραξης, της συνέχισης της δράσης ή της διακοπής της, αλλά και την αντιμετώπιση των εγκληματικών γεγονότων. Με τον τρόπο αυτό αποφεύγονται οι αδυναμίες των παραδοσιακών εγκληματολογικών προσεγγίσεων που παραγνωρίζουν την επίδραση των ευκαιριακών παραγόντων που είναι πάντα παρόντες, των κινήτρων, των συνηθειών και των περιστάσεων και επηρεάζουν τις στιγμιαίες δράσεις των ατόμων.[236]

2.3.5. Η σημασία του διαφορικού συγχρωτισμού και της έννοιας του λευκού περιλαιμίου στην προσπάθεια διασύνδεσης των επιμέρους εννοιών και θεωριών

Ο διαφορικός συγχρωτισμός και η προσέγγιση της κοινωνικής αλληλεπίδρασης αποτελούν κομβικές έννοιες που τονίζουν τη σημασία της μάθησης, της αλληλεπίδρασης και της επικοινωνίας για την εμπλοκή των ατόμων σε εγκληματικές δραστηριότητες και που επιτρέπουν τη σύνδεση θεωριών που αρχικά φαίνονται ως ασύνδετες μεταξύ τους:

Α. Των κινήτρων με τις ευκαιρίες: η συμβολική αλληλεπίδραση βλέπει το **κίνητρο** ως μια «συμβολική κοινωνική κατασκευή» της πραγματικότητας που περιλαμβάνει ορισμούς ατομικών καταστάσεων ως επιθυμητών, επωφελών ή αδιάφορων. Η νοηματοδότηση που κάνουν τα άτομα σε κάθε κοινωνική κατάσταση και στην κοινωνική πραγματικότητα δομεί τις εμπειρίες τους και τους κάνει, πριν κινητοποιηθούν σε δράση, να θεωρούν κάποιες συγκεκριμένες συμπεριφορές ή **ευκαιρίες** πιο κατάλληλες ή ενδιαφέρουσες έναντι κάποιων άλλων. Η συμβολική κοινωνική κατασκευή της πραγματικότητας, εκτός από τον ορισμό της πραγματικότητας, δίνει τη δυνατότητα στα άτομα να προβλέπουν και τις πιθανές αντιδράσεις των άλλων κι έτσι να προσαρμόζουν ανάλογα και τη συμπεριφορά τους.[237]

Β. Των θεωριών *ελέγχου,* που θεωρούν τον ανεπίσημο έλεγχο ως στοιχείο που πιέζει τα άτομα να συμμορφώνονται με το νόμο, με τις θεωρίες υποκουλτούρας που πιστεύουν αντίθετα ότι ο ανεπίσημος κοινωνικός έλεγχος πιέζει για τη μη συμμόρφωση, όπως συμβαίνει με την ένταξη του ατόμου σε παραβατική ομάδα.[238] Ο διαφορικός συγχρωτισμός μας δίνει την

[233] Jeffery C. Ray & Zahm Diane L (2008), σ.337
[234] Goldstein Arnold (1994),σσ.129-130 και στο Clarke Ronald V. (1997), σ.28
[235] Cornish Derek (1993)
[236] Cornish Derek (1993), βλ. σ. 367
[237] Coleman James W. (1987), σσ.406-439
[238] Braithwaite John. (1989), σ.193

απαραίτητη θεωρία «σημείου καμπής» (tipping points theory)[239] όπου η ισορροπία μεταξύ συμμόρφωσης (θεωρίες ελέγχου) και μη συμμόρφωσης (θεωρίες για τις υποκουλτούρες) διαμορφώνεται στη βάση της υπερίσχυσης του ευνοϊκού χαρακτηρισμού υπέρ της μιας ή της άλλης επιλογής. Το έγκλημα τελείται όταν οι χαρακτηρισμοί είναι πιο θετικοί για την παραβίαση του νόμου παρά για τη συμμόρφωση.[240]

Γ. Μεταξύ των θεωριών μάθησης και των προσεγγίσεων για το ρόλο των «εγκληματικών ευκαιριών» που αρχικά φαίνονται ασύμβατες.[241] Ο Ronald Akers, υιοθετώντας τη βασική πρόταση του Sutherland ότι το έγκλημα μαθαίνεται μέσω της κοινωνικής αλληλεπίδρασης, εξετάζει τις θεωρίες κοινωνικής μάθησης ως άμεση επέκταση του διαφορικού συγχρωτισμού. Τα άτομα διαφέρουν ως προς την έκθεσή τους σε κοινωνικά πρότυπα και κανόνες συμπεριφοράς επειδή αλληλεπιδρούν με άλλους, δηλαδή λόγω του διαφορικού συγχρωτισμού. Ο Akers πρότεινε την προσθήκη, μιας καινούριας έννοιας, δίπλα στο διαφορικό συγχρωτισμό, αυτή της «διαφορικής ενίσχυσης» που την όρισε ως «εξισορρόπηση μεταξύ των αναμενόμενων ανταμοιβών με τις αναμενόμενες ποινές» διασυνδέοντας τη κοινωνική μάθηση και το διαφορικό συγχρωτισμό με τον ωφελιμισμό, το συμπεριφορισμό και την οικονομική θεωρία.[242]

Όπως αναφέρθηκε παραπάνω, οι εγκληματίες, είτε προέρχονται από τα κατώτερα στρώματα και είναι περιτριγυρισμένοι από παράνομους, είτε από τα μεσαία και ανώτερα (με το λευκό κολάρο) που βρίσκονται σε ιδιαίτερες επιχειρηματικές καταστάσεις στις οποίες η παρανομία αποτελεί παράδοση, μαθαίνουν και εμπλέκονται στις παραβατικές συμπεριφορές και τις τεχνικές του εγκλήματος, με παράλληλη απομάκρυνσή τους από τους νομοταγείς πολίτες.

Οι απόψεις αυτές, από το διαφορικό συγχρωτισμό, είναι εμφανείς και στις πιο σύγχρονες προσεγγίσεις της περιβαλλοντικής εγκληματολογίας για το ρόλο της αλληλεπίδρασης και της εγγύτητας των ατόμων, στο πλαίσιο των καθημερινών τους δραστηριοτήτων, με πιθανούς δράστες, της εμπλοκής των ατόμων με παράνομες δραστηριότητες που καθιστά τους ίδιους ως κατάλληλους στόχους και το πώς οι δράστες ανακαλύπτουν εγκληματικές ευκαιρίες κινούμενοι σε γνώριμα μέρη.

Ο διαφορικός συγχρωτισμός αποτελεί θεωρητικό εργαλείο που χρησιμοποιούν θυματολογικές έρευνες για την ερμηνεία των διαφορικών κινδύνων θυματοποίησης των ατόμων και για τη σύνδεση δραστών με τα θύματα. Έτσι το ρίσκο, ο κίνδυνος θυματοποίησης εξαρτάται σε μεγάλο βαθμό από την άμεση επαφή (αλληλεπίδραση και επικοινωνία) που έχουν οι πιθανοί δράστες με κατάλληλα θύματα/στόχους στο πλαίσιο των συνηθισμένων τους δραστηριοτήτων. Ο διαφορικός κίνδυνος θυματοποίησης αποτελεί, σε μεγάλο βαθμό, τμήμα του διαφορικού συγχρωτισμού των θυμάτων με πιθανούς δράστες και της διαφορικής έκθεσης σε αυτούς. Η συχνή και έντονη αλληλεπίδραση των ατόμων με δράστες που έχουν κίνητρο αυξάνει την έκθεση σε κινδύνους.[243] Ο τρόπος ζωής των ατόμων και οι κοινωνικές τους ασχολίες, οι τεχνολογικές εξελίξεις, που συντελούν σε κοινωνική αποδιοργάνωση, αυξάνουν ή μειώνουν το βαθμό συγχρωτισμού και έκθεσής τους σε πιθανούς δράστες και συνακόλουθα τις ευκαιρίες για εγκληματική δράση. Οι προτάσεις αυτές αποτελούν και

[239] Σύμφωνα με τον Glaser Daniel όπως αναφέρει ο Braithwaite, βλ. Braithwaite John, ό.π. σ. 193
[240] Braithwaite John. (1989), ό.π.
[241] Braithwaite John (1989),. σσ. 189-190
[242] Βλ. Akers (2001), όπως αναφέρουν οι Pratt Travis C., Cullen, Francis T. Sellers, et.al. (2010)
[243] Βλ. Fattah Ezzat (2008)

βασικές αρχές της θεωρίας του «τρόπου ζωής» των Hidelang, Gottfredson και Garofalo και των «καθημερινών δραστηριοτήτων» των Felson & Cohen.[244]

Όσον αφορά την θεωρία για το έγκλημα του λευκού περιλαιμίου, ειδικά μετά την κριτική που δέχτηκε ο Sutherland την συμπλήρωσε, με μια απολογητική μελέτη (που δημοσιεύθηκε μετά θάνατον)[245], επισημαίνοντας τρεις παράγοντες (στοιχεία) για τη δημιουργία των οικονομικών εγκλημάτων:

Πρώτος παράγοντας είναι η ύπαρξη «ευκαιρίας για τη διάπραξη τέτοιου εγκλήματος, όπως οι απαραίτητες συνθήκες και τα κατάλληλα μέσα. Αν οι κατάλληλες περιστάσεις, η ευκαιρία δεν είναι παρούσα το έγκλημα είναι δύσκολο να τελεστεί.

Δεύτερο, η «πίεση» που μπορεί να ασκείται στα υποκείμενα από την ένταση της ανάγκης που πιέζει για ικανοποίηση, π.χ. η ανάγκη εκπλήρωσης οικονομικών υποχρεώσεων πιθανόν να οδηγήσει κάποιο άτομο σε κατάχρηση που διαφορετικά δεν θα διέπραττε.

Τρίτο, οι «δυνατότητες εναλλακτικής συμπεριφοράς» δηλαδή η παρουσία ή η απουσία ασφαλιστικών δικλείδων για την παρεμπόδιση διάπραξης του εγκλήματος.[246]

Τα στοιχεία αυτά που πρόσθεσε ο Sutherland προσφέρουν την απαραίτητη διασύνδεση των θεωριών που εστιάζουν στο ρόλο των εγκληματικών ευκαιριών, τόσο μεταξύ τους, όσο και με τις θεωρίες του Sutherland για το διαφορικό συγχρωτισμό και το έγκλημα του λευκού περιλαιμίου:

- Ο πρώτος από τους παραπάνω παράγοντες, τονίζει την ανάγκη ύπαρξης κατάλληλης «ευκαιρίας» για την τέλεση των οικονομικών εγκλημάτων και μας δείχνει τη σχέση της θεωρίας του Sutherland με τις σύγχρονες θεωρίες της περιβαλλοντικής εγκληματολογίας που εστιάζουν στην ύπαρξη των «εγκληματικών ευκαιριών».
- Η «πίεση», ο δεύτερος παράγοντας που πρόσθεσε ο Sutherland, αποτελεί στοιχείο το οποίο επηρεάζει το άτομο κατά τη διαδικασία λήψης της απόφασης και συνδέεται με την θεωρία των Clarke και Cornish για την προσέγγιση της **ορθολογικής επιλογής**[247].
- Ο τρίτος παράγοντας, οι «δυνατότητες εναλλακτικής συμπεριφοράς» αποτελούν βασικό στοιχείο στις οικονομολογικής προέλευσης θεωρίες και την θεωρία ορθολογικής επιλογής, ενώ η «παρουσία ασφαλιστικών δικλείδων» για την παρεμπόδιση διάπραξης του εγκλήματος προσιδιάζει στην παρουσία ή την απουσία **ικανών φυλάκων** που αποτελεί το τρίτο –και κυριότερο – στοιχείο της θεωρίας των Cohen και Felson για τις **καθημερινές δραστηριότητες ρουτίνας**.[248]

2.4. Συγκρότηση θεωρητικού πλαισίου μελέτης

Τα κοινά στοιχεία των παραπάνω θεωριών είναι ότι εξετάζουν το έγκλημα από την άποψη των «εγκληματικών ευκαιριών», εστιάζοντας όχι μόνο στα χαρακτηριστικά του δράστη, όπως κάνουν μέχρι τώρα οι παραδοσιακές εγκληματολογικές θεωρίες, αλλά και σε αυτά των στόχων και γενικότερα στις περιστασιακές συνθήκες που συνδέονται με ένα συγκεκριμένο έγκλημα.

[244] Βλ. Clarke Roland (1995)

[245] Βλ. Κουράκης Νέστορας (1998), σσ.206-207, αναφορά στον Sutherland (1944)

[246] Κουράκης Νέστορας (1998), σσ.206-207

[247] Βλ. παρακάτω για τη θεωρία της *ορθολογικής επιλογής* των Clarke και Cornish για την διαδικασία λήψης της –ορθολογικής – απόφασης.

[248] Βλ. παρακάτω για τη θεωρία των καθημερινών δραστηριοτήτων

Από την άλλη, τα σημεία στα οποία διαφέρουν μεταξύ τους οι παραπάνω θεωρίες (των καθημερινών δραστηριοτήτων, της ορθολογικής επιλογής, των εγκληματικών προτύπων και η στρατηγική της περιστασιακής πρόληψης του εγκλήματος) είναι κυρίως στον τρόπο με τον οποίο εξετάζουν το θέμα της επιλογής του κατάλληλου στόχου. Η θεωρία της ορθολογικής επιλογής δίνει προτεραιότητα στη μελέτη των ιδιοτήτων δόμησης των «επιλογών» για κάθε διαφορετικό τύπο εγκλήματος, οι οποίες περιλαμβάνουν τις δυσκολίες, το ρίσκο και τα αναμενόμενα οφέλη. Τα «εγκληματικά πρότυπα» από τη μεριά τους εκτιμούν τη σημασία των «κόμβων δραστηριοτήτων» (activity nodes) και της μετακίνησης ανάμεσα σε τέτοια σημεία. Οι δυο αυτές προσεγγίσεις εξηγούν ικανοποιητικά τον τρόπο που γίνεται η επιλογή του στόχου, ως προς το ποια αντικείμενα και υπό ποιες συνθήκες αποτελούν κατάλληλους (ελκυστικούς) στόχους.[249]

Η κοινωνική δράση των ατόμων είναι κατά αρχήν κατανοήσιμη αν διαθέτουμε αρκετά πληροφοριακά δεδομένα για τις συνθήκες κάτω από τις οποίες διαδραματίζεται. Η εγκληματική συμπεριφορά θα πρέπει αντίστοιχα να εξετάζεται υπό το πρίσμα ότι κατ' αρχήν δεν διαφοροποιείται από τη μη-εγκληματική. Αυτή η οπτική διαφέρει σημαντικά από εκείνη που εξετάζει το έγκλημα με όρους ψυχοπαθολογίας ή παθολογίας κοινωνικών συνθηκών.

Θα μπορούσαμε να σημειώσουμε ότι παρά την φαινομενική πληθώρα θεωριών και ερμηνευτικών σχημάτων για τα οικονομικά εγκλήματα αλλά και το απλό έγκλημα, κανένα από αυτά δεν γίνεται γενικά αποδεκτό ως ικανό να παράσχει μια ολοκληρωμένη προσέγγιση και ερμηνεία του πολυσύνθετου εγκληματικού φαινομένου φωτίζοντας κάθε σκοτεινή πλευρά του. Κάθε ένα από αυτά ρίχνει φως σε μια ή σε ορισμένες μόνο πλευρές του φαινομένου με αποτέλεσμα να είναι απαραίτητη μια πολυπαραγοντική και συνθετική προσπάθεια ερμηνείας του.

Η ανεπάρκεια των απλουστευτικών, μονοπαραγοντικών ερμηνευτικών προσεγγίσεων που εστιάζουν στην παθολογικότητα της συμπεριφοράς του εγκληματία έχει ως τώρα επισημανθεί από διάφορους μελετητές και έχει τονιστεί η ανάγκη μιας πολυπαραγοντικής προσέγγισης που, στο πλαίσιο της περιβαλλοντικής οπτικής, θα δίνει την απαραίτητη σημασία στις συνθήκες τέλεσης του εγκληματικού γεγονότος, το περιβάλλον (χώρο και χρόνο), την ύπαρξη των κατάλληλων ευκαιριών και τα κίνητρα του πιθανού δράστη ο οποίος δεν διαφέρει σε ατομικά ή κοινωνικά χαρακτηριστικά από τον μη δράστη. [250]

Όπως πρότεινε ο Cornish,[251] για την δόμηση μιας συνεκτικής μεταθεωρίας για την ανθρώπινη συμπεριφορά και δράση θα πρέπει να συμπεριλαμβάνονται κάποιες κοινές προϋποθέσεις όπως:

- ✓ Διερευνητική προσέγγιση του θέματος της ελεύθερης βούλησης.
- ✓ Οι υποθέσεις σχετικά με την ανθρώπινη συμπεριφορά θα πρέπει να διατυπώνονται σε σχέση με τις επικρατούσες συνθήκες στο χώρο και το χρόνο. Άρα η δράση των ατόμων θα πρέπει να θεωρηθεί υπό το πρίσμα της αλληλεπίδρασης μεταξύ ατόμων και καταστάσεων.
- ✓ Οι διάφορες καταστάσεις περιλαμβάνουν σκηνικά, όχι μόνο με φυσικά αντικείμενα αλλά και με άλλους ανθρώπους, τα οποία διευκολύνουν ή περιορίζουν τη δράση.

[249] Pires Stephen & Clarke Ronald V. (2011)
[250] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 260
[251] Cornish Derek. (1993)

- ✓ Σημαντικά ακόμα χαρακτηριστικά των καταστάσεων είναι οι ανταμοιβές ή οι συνέπειες (τιμωρίες, ποινές κλπ), και έννοιες όπως η μεγιστοποίηση, η βελτιστοποίηση, η ικανοποίηση ή άλλες εκδοχές της έννοιας του υπολογισμού για τα οφέλη ή τα κόστη που περιέχονται σε αυτές τις καταστάσεις ως κριτήρια επιλογής ανταπόκρισης των ατόμων στις απαιτήσεις του περιβάλλοντος. [252]

Η παρούσα διατριβή είναι πρωτότυπη μελέτη και συνιστά συμβολή στην επιστήμη της Εγκληματολογίας. Η συμβολή της διακριβώνεται στο επίπεδο της ολιστικής και πολυπαραγοντικής θεωρητικής προσέγγισης από την οπτική της περιβαλλοντικής εγκληματολογίας που εφαρμόζει για να εξετάσει τις πολυποίκιλες πτυχές του φαινομένου της ηλεκτρονικο-οικονομικής εγκληματικότητας, έννοια που εισάγει επίσης η παρούσα μελέτη. Το εγκληματολογικό ενδιαφέρον της διατριβής είναι στην κατεύθυνση, όχι μόνο της καταλληλότητας των στόχων - θυμάτων, όπως κάνουν μέχρι τώρα οι θυματολογικές μελέτες, αλλά και στην κατεύθυνση των πιθανών δραστών. Μέχρι τώρα τα στοιχεία αυτά δεν έχουν εξεταστεί συνδυαστικά, στη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος, από την υπάρχουσα βιβλιογραφία.

Στο πλαίσιο της παρούσας διατριβής επιχειρείται η σύνθεση υφιστάμενων προσεγγίσεων σε ευρύτερο θεωρητικό σχήμα που θα επιτρέψει τη δόμηση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος, των στοιχείων που συνθέτουν την εγκληματική του ευκαιρία, για την προσέγγιση του εγκληματικού γεγονότος τόσο ερμηνευτικά όσο και από την άποψη της αντιμετώπισης και πρόληψής του. Η σύνθεση αυτή θα μας επιτρέψει να μελετήσουμε όλα τα στοιχεία που συμμετέχουν στη διαμόρφωση του εγκληματικού γεγονότος και να κατανοήσουμε το πώς αυτό συμβαίνει. Πιο συγκεκριμένα, χρησιμοποιούμε τις προσεγγίσεις για τη διαμόρφωση των «εγκληματικών ευκαιριών» όπως της ορθολογικής επιλογής, των καθημερινών δραστηριοτήτων, των εγκληματικών προτύπων και της περιστασιακής πρόληψης του εγκλήματος, που προέρχονται από την οπτική της περιβαλλοντικής εγκληματολογίας. Οι θεωρίες αυτές μας παρέχουν το κατάλληλο θεωρητικό υπόβαθρο με τις κοινές τους βάσεις να μας επιτρέπουν να επιχειρήσουμε τόσο την μεταξύ τους διασύνδεση, όσο και την σύνθεσή τους σε ένα ισχυρό θεωρητικό «μίγμα» που θα εφαρμόζεται στην ερμηνεία αλλά και την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος. Το αποτέλεσμα της σύνθεσης αυτής θα αποτελέσει το απαραίτητο θεωρητικό πλαίσιο της παρούσας μελέτης.

2.5. Ερευνητικές υποθέσεις μελέτης

Οι σχετικές με το θέμα προϋπάρχουσες μελέτες, εστιάζουν η καθεμιά σε ένα ή περισσότερα από τα παραπάνω στοιχεία της εγκληματικής ευκαιρίας, αφήνοντας κενά στην συνολική απεικόνιση του φαινομένου. Η παρούσα μελέτη δίνει έμφαση σε όλα αυτά τα στοιχεία ταυτόχρονα, χωρίς να τονίζεται η ιδιαίτερη σημασία του ενός έναντι κάποιου άλλου, εφαρμόζοντάς τα στη μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος.

Με βάση τις παραπάνω θεωρητικές προσεγγίσεις το κεντρικό ερευνητικό ερώτημα της παρούσας διατριβής αφορά το ποιος είναι ο τρόπος που δομείται το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος, ποια είναι τα ιδιαίτερα στοιχεία που σχηματίζουν την εγκληματική του ευκαιρία. Έτσι η ερευνητική μας υπόθεση (πρόταση) διατυπώνεται ως εξής:

[252] Brantigham Patricia L. & Brantigham Paul J. (2008), σ. 260

«Το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος διαμορφώνεται στη βάση της αλληλεπίδρασης των δραστών με κατάλληλους στόχους στο πλαίσιο καθημερινών δραστηριοτήτων στον ψηφιακό χώρο που δημιουργούν κατάλληλες ευκαιρίες διάπραξης ηλεκτρονικο-οικονομικών εγκλημάτων».

Για τη διερεύνηση της παραπάνω κεντρικής θεωρητικής πρότασης διατυπώνονται τα επιμέρους ερευνητικά ερωτήματα της παρούσας μελέτης ως ακόλουθα:

1. Ποια κοινά στοιχεία παρουσιάζει το ηλεκτρονικό έγκλημα με το οικονομικό έγκλημα, ποια η μεταξύ τους σχέση; Λόγω της παγκοσμιοποίησης της οικονομίας και της πληροφορικής τεχνολογίας η οποία, εκτός από σύγχρονα μέσα, παρέχει τη δυνατότητα στις εγκληματικές δραστηριότητες να είναι διεθνείς, το πληροφορικό έγκλημα βρίσκει νέες οδούς διάπραξης μέσω του κυβερνοχώρου. Έτσι υποθέτουμε ότι η φύση των περισσότερων ηλεκτρονικών εγκλημάτων έχει οικονομικό χαρακτήρα από την άποψη των κινήτρων και του προσδοκώμενου οφέλους για το δράστη.
2. Πώς συνδέεται η συχνότητα και η ένταση της αλληλεπίδρασης των ικανών δραστών με τα κατάλληλα θύματα/στόχους στο ψηφιακό περιβάλλον με αντίστοιχο κίνδυνο θυματοποίησης; Συγκεκριμένα:

α) το κατά πόσο η συχνότερη και με μεγαλύτερη διάρκεια δραστηριότητα των ατόμων σε ψηφιακά δίκτυα (διαδίκτυο, χρήση υπολογιστών, τηλεφώνων, κλπ.) τα καθιστά πιο ευάλωτο στόχο και τα υποβάλλει σε μεγαλύτερο κίνδυνο θυματοποίησης.

β) Ποιες συγκεκριμένες «ριψοκίνδυνες» δραστηριότητες καθημερινής ρουτίνας καθιστούν τους χρήστες ευάλωτους στόχους και τους συνδέουν με πιθανούς δράστες δημιουργώντας εγκληματικές ευκαιρίες;

γ) Ποιες είναι οι περιστασιακές συνθήκες που διαμορφώνουν το εγκληματικό πρότυπο; Ποιος ο ρόλος του διαδικτύου στη δημιουργία κοινού τόπου συνάντησης δραστών – στόχων. Πώς το διαδίκτυο συμβάλλει στην εγγύτητα του δράστη με τους στόχους – θύματα, εκμηδενίζει τις αποστάσεις και αυξάνει τις διαθέσιμες εγκληματικές ευκαιρίες.

3. Ποιο είναι το κίνητρο που ενεργοποιεί τη δράση των ηλεκτρονικο –οικονομικών εγκληματιών; Οι δράστες των ηλεκτρονικο-οικονομικών εγκλημάτων υποθέτουμε ότι λειτουργούν ορθολογικά ως ένα βαθμό, με βάση κάποιο κίνητρο για την επιλογή του στόχου τους στη βάση της υποκειμενικής εκτίμησης του αναμενόμενου οφέλους (ικανοποίηση αναγκών π.χ. χρήμα, φήμη) σε σχέση με το κόστος σε χρόνο, κόπο, χρήμα, απώλεια κύρους, κίνδυνο επισήμανσης και καταδίκης.
4. Το τέταρτο ερευνητικό ερώτημα αφορά το κατά πόσο η έλλειψη ικανών φυλάκων, όπως μέτρων προστασίας των ψηφιακών συστημάτων από πλευράς χρηστών δημιουργεί κατάλληλες εγκληματικές ευκαιρίες και πώς συνδέεται με τον κίνδυνο θυματοποίησης. Ποιά συστήματα ή τρόποι προστασίας, αποτελούν αποτελεσματικά μέσα πρόληψης και αντιμετώπισης της ηλεκτρονικο-οικονομικής εγκληματικότητας;

Για την διακρίβωση της εφαρμοσιμότητας των παραπάνω προτάσεων στο ηλεκτρονικο – οικονομικό έγκλημα είναι απαραίτητες, αφενός κάποιες εννοιολογικές αποσαφηνίσεις και οριοθετήσεις και αφετέρου η βήμα –προς –βήμα αντιπαραβολή τους με τα δεδομένα των υφιστάμενων θεωρητικών και εμπειρικών προσεγγίσεων.

Η αναλυτική κριτική παρουσίαση των σχετικών θεωρητικών προσεγγίσεων αλλά και των αντίστοιχων ερευνητικών δεδομένων επιτρέπει τη συστηματική διερεύνηση και τη μεταξύ τους σύγκριση με σκοπό τη σύνθεση των επιμέρους στοιχείων κάθε προσέγγισης σε ενιαίο

θεωρητικό σχήμα και την υποστήριξη των θεωρητικών προτάσεων της παρούσας διατριβής. Οι προϋπάρχουσες θεωρίες της περιβαλλοντικής εγκληματολογίας, με παράλληλη ενσωμάτωση αναλυτικών εννοιών, βοηθούν στη σύνθεση της θεωρητικής μας προσέγγισης.

Η βιβλιογραφική έρευνα, η συστηματική βιβλιογραφική ανασκόπηση, η ανάλυση περιεχομένου και οι μέθοδοι της επαγωγής και της αναγωγής επιλέχθηκαν ως βασικές μέθοδοι της παρούσας διατριβής.

Η επιλογή της μεθόδου της συστηματικής βιβλιογραφικής έρευνας δημοσιευμένων ερευνών και άρθρων, αλλά και η ανάλυση περιεχομένου της σχετικής ειδησεογραφίας, επιτρέπει τον εντοπισμό, την επιλογή και την κριτική αποτίμηση των σχετικών ερευνών. Έτσι επιτυγχάνεται η αξιοποίηση του πλούτου της εγκληματολογικής σκέψης, καταγράφοντας, συγκρίνοντας και επιλέγοντας τις καταλληλότερες μελέτες για την αποσαφήνιση των βασικών εννοιών, τον προσδιορισμό του κεντρικού περιεχομένου τους, τη διασύνδεσή τους με συγκεκριμένες περιπτώσεις εγκληματικότητας, αλλά και την οριοθέτηση και διερεύνηση του αντικειμένου της παρούσας μελέτης. Πιο συγκεκριμένα, απαιτείται η αποσαφήνιση των ερευνητικών ερωτημάτων, ο σχεδιασμός της πορείας της μελέτης, ο καθορισμός των κριτηρίων επιλογής ή απόρριψης του πρωτογενούς υλικού που θα μελετηθεί (δημοσιευμένων άρθρων, μελετών, ερευνών κλπ.). Τέλος γίνεται η σύνθεση των αποτελεσμάτων και η εξαγωγή συμπερασμάτων.

Η επαγωγή, δηλαδή η πορεία της μελέτης από το ατομικό και το ειδικό προς το γενικό μέρος, χρησιμεύει για την εξαγωγή και τη σύνθεση γενικότερων συμπερασμάτων από τη μελέτη περιπτώσεων εγκληματικών δράσεων, που θα εφαρμόζονται σε γενικότερες περιπτώσεις, ιδιαίτερα για την πρόληψη των μορφών εγκληματικότητας που αποτελούν το αντικείμενο μελέτης μας. Από την άλλη, η αναγωγή είναι απαραίτητη για την βήμα προς βήμα ερευνητική διακρίβωση της εφαρμοσιμότητας των γενικότερων θεωρητικών προσεγγίσεων στις ειδικότερες θεωρητικές προτάσεις που διατυπώθηκαν παραπάνω και αποτελούν τις βασικές θέσεις της παρούσας διατριβής.

2.6. Θεωρητικοί και λειτουργικοί ορισμοί

Για την διακρίβωση των θεωρητικών προτάσεων της παρούσας μελέτης είναι απαραίτητες κάποιες εννοιολογικές διασαφηνίσεις, να δοθούν δηλαδή οι αναγκαίοι ορισμοί. Οι ορισμοί αυτοί χρησιμοποιούνται παρακάτω για την εφαρμοσιμότητα των προσεγγίσεων των «εγκληματικών ευκαιριών» στην μελέτη του ηλεκτρονικο-οικονομικού εγκλήματος, την αντιμετώπισή του και για τον έλεγχο των θεωρητικών προτάσεων της παρούσας διατριβής. Συγκεκριμένα, στο πλαίσιο της μετα-ανάλυσης, απαιτείται η επαναδιατύπωση κάποιων από τις βασικές έννοιες που χρησιμοποιούν οι θεωρίες αυτές, όπως της έννοιας του «χώρου», της «εγγύτητας», της «έκθεσης», της «ελκυστικότητας» του στόχου και των «ικανών φυλάκων».

Ο πρώτος ορισμός αφορά το στοιχείο της συνύπαρξης δράστη και στόχου σε ένα **κοινό «τόπο».** Ο πιθανός δράστης μπορεί να συναντά και να αλληλεπιδρά με τα υποψήφια θύματα από απόσταση μέσω κάποιου **δικτύου**. Η έννοια του τόπου θα πρέπει λοιπόν να επεκταθεί ώστε να περιλαμβάνει όλους τους τρόπους, τα δίκτυα επικοινωνίας που επιτρέπουν την αλληλεπίδραση μεταξύ δράστη με κίνητρο και στόχου-θύματος και «προσφέρουν στο δράστη έναν «κοινό χώρο» συνάντησης με το στόχο του. Η **συνάντηση /αλληλεπίδραση** πιθανών δραστών με τους κατάλληλους στόχους γίνεται σε ψηφιακό περιβάλλον, χώρο και χρόνο. Φυσική επαφή υπάρχει μόνο μεταξύ δράστη - μέσου και μεταξύ στόχου – μέσου. Δηλαδή ο δράστης, όπως και το θύμα έρχεται σε φυσική επαφή μόνο με το εργαλείο που είναι π.χ. το

τηλέφωνο ή ο υπολογιστής, ενώ δράστης και θύμα δεν έρχονται σε φυσική αλλά μόνο σε ψηφιακή επαφή μεταξύ τους.

Πιθανός δράστης ηλεκτρονικο-οικονομικού εγκλήματος θεωρείται κάποιος, που συναντά την κατάλληλη *ευκαιρία*, διαθέτει το κατάλληλο *κίνητρο*: χρήμα, ευχαρίστηση, φήμη, εξουσία, διατήρηση status και που λαμβάνει μια ορθολογική απόφαση για την τέλεση κάποιου οικονομικού εγκλήματος με χρήση ηλεκτρονικού υπολογιστή ή άλλων ψηφιακών και δικτυακών μέσων.

Η **ορθολογικότητα** στην **απόφαση** του δράστη δεν θεωρείται πλήρης, γιατί αυτός δεν μπορεί να διαθέτει όλες τις απαραίτητες πληροφορίες και δεδομένα, αλλά περιορισμένη και περιλαμβάνει την (υποκειμενική) στάθμιση από πλευράς πιθανού δράστη της αναμενόμενης ωφέλειας έναντι του κόστους.

Εγκληματικό κίνητρο, θεωρείται, από τους περισσότερους ερευνητές της οικονομικής εγκληματικότητας, μια σειρά συμβολικών κατασκευών και νοηματοδοτήσεων του δρώντος υποκειμένου για το ποιες συμπεριφορές και ποιοι στόχοι κρίνονται ως κατάλληλοι ή επιθυμητοί και ποιοι όχι.[253] Το κίνητρο έχει υποκειμενική διάσταση γιατί αφορά τις προσωπικές του επιθυμίες και ανάγκες.[254]

Για το **οικονομικό έγκλημα** υιοθετείται ο θεωρητικός ορισμός για το έγκλημα του λευκού περιλαιμίου του Edelhertz, ο οποίος αφαίρεσε το κριτήριο του status και το όρισε ως:

«μια παράνομη πράξη ή σειρά παράνομων πράξεων που διαπράττεται με μη-φυσικά μέσα με μυστικότητα δόλο (ή πονηριά), με σκοπό την απόκτηση χρημάτων ή περιουσίας, την αποφυγή πληρωμής ή απώλειας χρημάτων ή περιουσίας, ή για την απόκτηση επιχειρηματικών ή προσωπικού πλεονεκτήματος»[255].

Ηλεκτρονικο-οικονομικό έγκλημα θεωρείται η προσβολή οικονομικών έννομων αγαθών που γίνεται με εμπλοκή οποιουδήποτε δικτύου, συστήματος υπολογιστών ή άλλων ηλεκτρονικών συσκευών επικοινωνίας όπου χρησιμοποιούνται ως στόχος ή μέσα του εγκλήματος. Ως εκ τούτου το έγκλημα αυτό δεν περιλαμβάνει χρήση φυσικής βίας.

Ως **«καθημερινή» δραστηριότητα ρουτίνας** θεωρείται η συνηθισμένη ενασχόληση των ατόμων, τόσο των πιθανών δραστών, όσο των πιθανών θυμάτων/στόχων, στο πλαίσιο της εργασίας ή του ελεύθερου χρόνου τους.

Κατάλληλος στόχος/θύμα θεωρείται κάποιος ευάλωτος στόχος, που δεν διαθέτει επαρκή μέσα προστασίας, δηλαδή ικανή φύλαξη. Λόγω της μη φυσικής επαφής με το θύμα, η επιλογή του στόχου από το δράστη δεν γίνεται με βάση τα προσωπικά χαρακτηριστικά του θύματος.

Ικανή φύλαξη θεωρείται η ύπαρξη απαραίτητων μέσων προστασίας, φυσικών ή ηλεκτρονικών όπως αντιϊκά προγράμματα, τείχη προστασίας κλπ., αλλά και η εκπαίδευση χρηστών και ειδικών σχετικά με τη χρήση της τεχνολογίας και τους κινδύνους.

Το εγκληματικό πρότυπο του γεγονότος και της εγκληματικής συμπεριφοράς, αφορά «την περιγραφή αναγνωρίσιμων διασυνδέσεων αντικειμένων, διαδικασιών ή ιδεών». Τα πρότυπα έχουν ομοιότητες ως προς τη δόμηση της ευκαιρίας: την διαδικασία λήψης της απόφασης, τα κίνητρα, τις οδούς που ακολουθούνται, το σκηνικό που διαδραματίζεται η δράση των εγκληματιών και των θυμάτων.[256]

[253] Coleman James.W. (1987) , σ.156
[254] Coleman James.W. (1987), σ.171
[255] Braithwaite John (1985), σσ. 1-21
[256] Brantigham Patricia L. & Brantigham Paul J. (2008), σσ. 288-290

Εγκληματική ευκαιρία, αποτελεί «την πιθανή πορεία μιας δράσης που διευκολύνεται από ένα ιδιαίτερο σύνολο κοινωνικών συνθηκών το οποίο ο δράστης ενσωματώνει στο ατομικό του σύστημα διαθέσιμων συμπεριφορών».[257]

Η πιθανή συμπεριφορά μετατρέπεται σε ευκαιρία όταν το άτομο αποκτά επίγνωση για αυτή και εμπίπτει στην κατηγορία των δράσεων που πραγματικά επιθυμεί να πράξει. Μια ευκαιρία θεωρείται κατάλληλη ή όχι αν τη δούμε από την πλευρά του δράστη. Αν πολλοί τη βλέπουν ως τέτοια, τότε μπορούμε να πούμε ότι είναι ελκυστική ευκαιρία με καθολική έννοια.[258]

Η **καταλληλότητα ή η ελκυστικότητα** μιας **ευκαιρίας** έχει πιο αντικειμενική διάσταση από το κίνητρο και δομείται, σύμφωνα με τον Coleman από τέσσερεις παράγοντες: α) την αντίληψη του δράστη για το προσδοκώμενο όφελος, β) την αντίληψη του δράστη για τους πιθανούς κινδύνους ανακάλυψης, σύλληψης και τιμωρίας, γ) τη συνάφεια της ευκαιρίας ως προς τις ιδέες, τις εκλογικεύσεις και τα πιστεύω του πιθανού δράστη, δ) την συνεκτίμηση της συγκεκριμένης εγκληματικής ευκαιρίας με άλλες πιθανές ευκαιρίες (για νόμιμη συμπεριφορά) που παρουσιάζονται στην αντίληψη του δράστη. Έτσι η καταλληλότητα της ευκαιρίας ουσιαστικά δομείται από την αλληλεπίδραση του κινήτρου του δράστη με τις δομικές συνθήκες της ευκαιρίας.[259]

Ο όρος **έκθεση** αφορά τη συχνότητα με την οποία ένα άτομο αλληλεπιδρά με πιθανούς δράστες/κινδύνους. Στο πραγματικό περιβάλλον υπάρχουν συγκεκριμένες καθημερινές δραστηριότητες που συνδέονται με κίνδυνο έκθεσης και θυματοποίησης των ατόμων[260]. Έτσι και στο ψηφιακό περιβάλλον η **«έκθεση»** των θυμάτων στους πιθανούς δράστες εκφράζεται με την επίδειξη συγκεκριμένης διαδικτυακής συμπεριφοράς και σχετίζεται με την χρονική διάρκεια αυτών των δραστηριοτήτων. [261]

Ο όρος **εγγύτητα** αναφέρεται στην απόσταση, γεωγραφική ή ψηφιακή, μεταξύ δράστη και κατάλληλου στόχου.[262] Η «εγγύτητα», στην περίπτωση των παραδοσιακών εγκλημάτων αφορά την φυσική πρόσβαση του πιθανού δράστη με το στόχο του στο γεωγραφικό χώρο. Η διαφορά στην περίπτωση του ψηφιακού εγκλήματος είναι το γεγονός ότι το υποψήφιο θύμα δεν βρίσκεται σε φυσική εγγύτητα με τον δράστη, αλλά με τα εργαλεία και τα μέσα που αυτός χρησιμοποιεί μέσω της σύγχρονης τεχνολογίας των ψηφιακών δικτύων. Τέτοια ψηφιακά εργαλεία μπορεί να είναι κακόβουλα προγράμματα, όπως ιοί, με οποία ο δράστης μπορεί να αποκτήσει πρόσβαση στο στόχο του, για να τον βλάψει ή να κλέψει δεδομένα εξ αποστάσεως[263].

[257] σύμφωνα με τον Coleman , βλ.Coleman James.W. (1987), σ.156
[258] Coleman James.W., ό.π
[259] Coleman James.W. (1987), σσ.171-172
[260] Mustaine Elizabeth E. & Tewksbury Richard (1998)
[261] Holt Thomas J. & Bossler Adam (2013)
[262] Βλ. Cohen (1981), Hindelang (1978), Miethe & Meier (1990, 1994), όπως αναφέρει η Popp, Ann Marie (2012)
[263] Holt Thomas J. & Bossler Adam (2013)

ΚΕΦΑΛΑΙΟ 3. Η ΜΕΛΕΤΗ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1. Η έννοια του οικονομικού εγκλήματος

Όπως είδαμε παραπάνω σύμφωνα με τον ορισμό του Sutherland το οικονομικό έγκλημα ή έγκλημα του «Λευκού Περιλαιμίου», διαπράττεται από άτομα με υψηλό οικονομικο-κοινωνικό status, κατά τη διάρκεια της επαγγελματικής τους ενασχόλησης εκμεταλλευόμενα την εμπιστοσύνη του κοινωνικού τους περίγυρου προβάλλοντας την εικόνα του «τίμιου».

Έκτοτε έχει δοθεί πλήθος ορισμών, εννοιολογικών διακρίσεων και κατηγοριοποιήσεων του οικονομικού εγκλήματος. Πολλοί μελετητές έχουν αναρωτηθεί αν ο ορισμός του Sutherland λόγω της ευρύτητάς του, αναφέρεται περισσότερο στο κοινωνικό status του δράστη, τον επαγγελματικό του ρόλο, τα χαρακτηριστικά του εγκλήματος ή σε κάποιο συνδυασμό ανάμεσα στα παραπάνω χαρακτηριστικά. Όμως ακριβώς αυτή η ευρύτητα είναι που αφήνει το περιθώριο να περιλάβουμε σε αυτή τη μορφή εγκλήματος όχι μόνο τις περιπτώσεις απάτης, κατάχρησης, ξεπλύματος χρήματος, φοροδιαφυγής κλπ, αλλά ακόμα και τους θανάτους υπαλλήλων από δηλητηριάσεις που προκαλούνται από αμελείς επιχειρήσεις σε χώρους εργασίας.

Προτάθηκε λοιπόν μια τεράστια συλλογή όρων και ορισμών, που αποτυπώνουν τις εννοιολογικές, θεωρητικές και ιδεολογικές διαφορές των εμπνευστών τους, όπως εγκληματικότητα των ανώτερων στρωμάτων, των ελίτ, των ισχυρών, των εταιριών, των οργανώσεων, των επαγγελματιών, των υπαλλήλων, της επαγγελματικής δραστηριότητας, κατά της εμπιστοσύνης, οικονομική εγκληματικότητα, επίσημα, κυβερνητικά ή πολιτικά εγκλήματα, παρανομίες, παραβάσεις, παραβιάσεις, παρέκκλιση, κακή διαχείριση και άλλοι. Μετά από τις δεκαετίες άκαρπων εννοιολογικών συζητήσεων, οι περισσότεροι μελετητές έχουν συμφωνήσει ότι διαφωνούν.[264] Αν και οι περισσότεροι τον απέφυγαν παρά τον ασπάστηκαν, ο αρχικός ορισμός του Sutherland παραμένει.

Μια επέκταση της έννοιας του εγκλήματος του λευκού περιλαιμίου θα επέτρεπε να περιλάβουμε τα εγκλήματα που διαπράττονται από την επιχείρηση ή για όφελος της επιχείρησης, όπως περιβαλλοντικά εγκλήματα, παραβάσεις των κανόνων υγιεινής ή ασφάλειας στους χώρους εργασίας, της εργατικής νομοθεσίας κλπ.[265]

Παρά την ευρύτητα του, όπως είδαμε, ο ορισμός του Sutherland για τα «εγκλήματα του λευκού περιλαιμίου» πιθανόν παραβλέπει κάποιες συμπεριφορές που δεν εντάσσονται σε αυτόν. Παραγνωρίζει δηλαδή το γεγονός ότι υπάλληλοι μιας επιχείρησης σε χαμηλότερη ιεραρχία και με χαμηλότερο κοινωνικο-οικονομικό status μπορούν να έχουν πρόσβαση στους πόρους και τα δεδομένα της ώστε να μπορούν να διαπράξουν εγκλήματα για όφελος ή σε βάρος της.

Έτσι οι Clinard και Quinney διέκριναν δυο κατηγορίες εγκλημάτων λευκού περιλαιμίου:

1. Εγκλήματα εργασίας από εργαζόμενους στην επιχείρηση, ανεξαρτήτως θέσης στην ιεραρχία της.

2. Εγκλήματα της επιχείρησης εναντίον άλλης επιχείρησης, των καταναλωτών, του περιβάλλοντος ή γενικότερα της κοινωνίας. [266]

Οι Hagan και Simon διέκριναν τις «παραβάσεις λευκού περιλαιμίου» σε δυο μεγάλες υποκατηγορίες: «παραβάσεις λευκού περιλαιμίου» και «παραβάσεις της άρχουσας τάξης».

[264] Shapiro Susan P (2002)
[265] Grabosky Peter N. & Walkley Sascha (2007), σσ. 358-375
[266] Λάζος Γρηγόρης (2001), σσ. 59-60

Οι μορφές των «εγκλημάτων λευκού περιλαιμίου» που γίνονται ως μέρος της νόμιμης εργασίας είναι τα «εγκλήματα των επιχειρήσεων» ή «οργανωσιακά εγκλήματα» (organizational crime) τα οποία γίνονται με σκοπό το όφελος για την επιχείρηση και τα «εγκλήματα στο χώρο εργασίας» ή «εργασιακά, υπαλληλικά» (occupational crime) με σκοπό το όφελος του ίδιου του ατόμου.[267]

Ο Sutherland δεν διακρίνει τα εγκλήματα που διαπράττονται από τα μέλη μιας επιχείρησης για όφελος της επιχείρησης αυτής από εκείνα που διαπράττονται σε βάρος της.

Έτσι οι κλοπές που διαπράττουν οι υπάλληλοι σε βάρος της επιχείρησης όπου εργάζονται είναι το ίδιο εγκλήματα λευκού περιλαιμίου (αρκεί αυτοί να είναι ευυπόληπτοι) όπως και η εξαπάτηση των καταναλωτών από πλευράς των επιχειρήσεων. Αυτή η διαφοροποίηση σχετίζεται με το κοινωνικό και οικονομικό επίπεδο του δράστη. Για παράδειγμα τα πιο σύνθετα, ευρείας κλίμακας επιχειρηματικά εγκλήματα, όπως παραβάσεις αντιμονοπωλιακών νόμων, τείνουν να διαπράττονται από λευκούς μεσήλικες με υψηλότερο κοινωνικό, οικονομικό επίπεδο από τον μέσο δράστη. Πιο εξατομικευμένα, λιγότερο οργανωμένα οικονομικά εγκλήματα όπως απάτη και κατάχρηση, συνήθως διαπράττονται από άτομα με χαμηλότερη οικονομική σταθερότητα και κοινωνικό status[268].

Η διαφοροποίηση αυτή προκάλεσε συζητήσεις μεταξύ των εγκληματολόγων για το βαθμό διάκρισης μεταξύ των οικονομικών εγκλημάτων και των κοινών εγκλημάτων που διαπράττονται στο δρόμο.

Έτσι σε δεύτερο επίπεδο οι συζητήσεις εστιάστηκαν στο κοινωνικο-οικονομικό επίπεδο του δράστη και εάν αυτό αφορά αποκλειστικά άτομα των ανώτερων κοινωνικών στρωμάτων ή μπορεί να εφαρμοστεί αναλογικά σε οποιαδήποτε κοινωνική κατηγορία ή ομάδα όπου ο δράστης ασκεί κάποια μορφή δύναμης πάνω στα μέλη της ομάδας. Πάνω στο ζήτημα ο Gilbert Geis υποστηρίζει ότι το έγκλημα του λευκού περιλαιμίου δεν θα πρέπει να συγχέεται με το οικονομικό έγκλημα γενικότερα (όπου θεωρείται κάθε παραβίαση ποινικών ή άλλων αυστηρών κανόνων επαγγελματικής δεοντολογίας), επειδή ως έγκλημα του λευκού περιλαιμίου θεωρείται αυτό που τελείται αποκλειστικά από άτομα της ανώτερης τάξης ενώ για τα οικονομικής φύσης εγκλήματα που διαπράττονται από μέλη των κατωτέρων τάξεων υπάρχει διαφορετική ερμηνευτική προσέγγιση άρα και εννοιολόγηση. Έτσι η έμφαση δίνεται στο κοινωνικο-οικονομικό επίπεδο των δραστών οι οποίοι θα πρέπει να διαθέτουν υψηλό κοινωνικό και οικονομικό στάτους για να θεωρούνται εγκληματίες με το λευκό περιλαίμιο.[269]

Από την άλλη αρκετές έρευνες[270] διαπιστώνουν ότι πολλά από τα οικονομικά εγκλήματα, όπως απάτες με πιστωτικές κάρτες, ηλεκτρονικά εγκλήματα, εξαπάτηση καταναλωτών κ.λπ. δεν είναι απαραίτητο να διαπράττονται από άτομα με υψηλό στάτους αλλά οι δράστες τους μπορεί να είναι απλοί καθημερινοί άνθρωποι, τα χαρακτηριστικά των οποίων δεν διαφέρουν σημαντικά από αυτά των δραστών του κοινού εγκλήματος. Το κριτήριο λοιπόν της ευυποληψίας δεν είναι και το ασφαλέστερο δυνατό και στη θέση του έχουν προταθεί άλλα κριτήρια όπως η κοινωνική τάξη, η πρόσβαση στη διαχείριση κεφαλαίων και η εστίαση στα χαρακτηριστικά του εγκλήματος και όχι του δράστη[271]. Το τελευταίο έχει ιδιαίτερη σημασία επειδή, από τη μια η εστίαση του Sutherland είναι στον παραβάτη και χρησιμοποιεί ερμηνείες

[267] Λάζος Γρηγόρης (2013), σσ. 34-36
[268] Coleman James W. (1987), σσ. 406-439
[269] Δημόπουλος Χαράλαμπος (1988), σ. 39
[270] Coleman James.W., ό.π.
[271] Shapiro Susan (1990)

που αναφέρονται σε συμπεριφορά μεμονωμένων ατόμων, ενώ από την άλλη καταγράφει παρανομίες επιχειρήσεων χαρακτηρίζοντας τις ως «υπότροπες και καθ' έξην».

Έτσι οι διάφοροι ορισμοί που κατά καιρούς διατυπώθηκαν για το έγκλημα του λευκού περιλαιμίου μπορούν να ενταχθούν σε μια από τις δυο κύριες κατηγορίες:

Α. Η πρώτη κατηγορία ορισμών αφορά αυτούς που εστιάζουν στον εγκληματία, τα χαρακτηριστικά και το κριτήριο της ευυποληψίας του δράστη.

Β. Η δεύτερη κατηγορία που εστιάζει στο έγκλημα και τα χαρακτηριστικά της δράσης έτσι όπως τα ορίζει ο νόμος.

Ο Edelhertz διατύπωσε με τη σειρά του ένα ορισμό βασισμένο όχι στα χαρακτηριστικά του δράστη αλλά του εγκλήματος, στον τρόπο δράσης και το αντικείμενο του εγκλήματος καθιστώντας ασήμαντο το κριτήριο του «ευυπόληπτου» status.[272] Έτσι όρισε το έγκλημα του λευκού περιλαιμίου ως:

«μια παράνομη πράξη ή σειρά παράνομων πράξεων που διαπράττεται με μη-φυσικά μέσα με μυστικότητα δόλο (ή πονηριά), με σκοπό την απόκτηση χρημάτων ή περιουσίας, την αποφυγή πληρωμής ή απώλειας χρημάτων ή περιουσίας, ή για την απόκτηση επιχειρηματικών ή προσωπικού πλεονεκτήματος»[273].

Όπως αναφέρει ο Freiberg, με την πάροδο του χρόνου, οι διάφοροι μελετητές του, τείνουν να περιλαμβάνουν στο έγκλημα του λευκού περιλαιμίου οποιαδήποτε πράξη επαγγελματικής παραβατικότητας, ανεξάρτητα από το status των ατόμων, που περιλαμβάνει παραβίαση νόμου ή επαγγελματικών αρχών δεοντολογίας (professional ethics). Υπό αυτήν τη μορφή, έχει προταθεί ότι το έγκλημα του λευκού περιλαιμίου περιλαμβάνει τώρα σχεδόν οποιαδήποτε μορφή παρανομίας εκτός από τα συμβατικά εγκλήματα δρόμου. [274]

Πιο πρόσφατα, εγκληματολόγοι που ασχολούνται με το έγκλημα του λευκού περιλαιμίου άρχισαν να διατυπώνουν ορισμούς που λαμβάνουν υπόψη τις τεχνολογικές και οικονομικές αλλαγές και το στάτους μεσαίας κοινωνικής θέσης αρκετών δραστών κλασικού εγκλήματος του λευκού περιλαιμίου.

Οι Wheeler, Weisburd και Bode όρισαν το έγκλημα του λευκού περιλαιμίου ως «οικονομικές παραβάσεις που διαπράττονται με τη χρήση συνδυασμού απάτης, εξαπάτησης ή απιστίας» και υποστήριξαν πως αυτός ο ορισμός είναι αρκετά ευρύς ώστε να περιλάβει ολόκληρο το εύρος των παράνομων δραστηριοτήτων που απασχολούν τα ομοσπονδιακά δικαστήρια.[275] Πράγματι, όπως παρατηρούμε δεν περιλαμβάνεται ούτε στον ορισμό αυτό το κριτήριο του υψηλού status ή της ευυποληψίας.

Από την πλευρά του ο Quinney θεωρεί ότι το οικονομικό έγκλημα είναι αυτό που διαπράττεται κατά τη διάρκεια της επαγγελματικής ενασχόλησης[276]. Ένας τέτοιος ορισμός είναι, κατά τη γνώμη μας τόσο ευρύς που θα μπορούσε να περιλαμβάνει πλειάδα παραβατικών συμπεριφορών, μεταξύ των οποίων υπεξαιρέσεις αξίας εκατομμυρίων από μεγαλο-στελέχη εταιρειών μέχρι μικροκλοπές εμπορευμάτων από υπαλλήλους εμπορικών καταστημάτων, μη κάνοντας έτσι καμία διάκριση ούτε προς την αξία της οικονομικής ζημίας ούτε και ως προς το κοινωνικό στάτους των δραστών.

Τέτοιοι ορισμοί, που ανάγουν το οικονομικό έγκλημα ως δραστηριότητα αποκλειστικά κατά την επαγγελματική ενασχόληση, γενικότερα παραγνωρίζουν ένα φάσμα οικονομικών

[272] Shover Neil (2007), σσ. 81-97
[273] Braithwaite John. (1985), σσ. 1-21
[274] Freiberg Arie (1992), σσ. 1-19
[275] Wheeler Stanton, Weisburd David, & Bode Nancy (1982), σσ. 641–659
[276] Quinney Earl (1963), σσ. 179–185.

παραβάσεων που δεν έχουν να κάνουν με την επαγγελματική ενασχόληση κάποιου, όπως για παράδειγμα οι φορολογικές ή τελωνειακές απάτες και απάτες επιδοτήσεων από πολίτες σε βάρος του δημοσίου ή της Ε.Ε.

Κατά τον Donn Parker:

> «Κάθε απόπειρα ή πρακτική που αφορά στην παρεμπόδιση της ελεύθερης επιχείρησης ή στην προώθηση του αθέμιτου ανταγωνισμού, στη διατάραξη της εμπιστοσύνης έναντι ενός ατόμου ή μιας επιχείρησης, στην παραβίαση της εργασιακής διαδικασίας ή στη διακινδύνευση των καταναλωτών ή της πελατείας, συνιστά έγκλημα λευκού περιλαιμίου»[277].

Για τον Curt Bartol:

> «τα οικονομικά εγκλήματα γενικά χαρακτηρίζονται από την παράνομη απόκτηση χρημάτων ή αγαθών ή καταστροφή περιουσίας για κέρδος»[278].

Σύμφωνα με το FBI Εγκλήματα Λευκού Περιλαιμίου θεωρούνται «οι παράνομες ενέργειες με δόλο, απόκρυψη, κατάχρηση εμπιστοσύνης, που δεν βασίζονται στη χρήση ή απειλή φυσικής βίας. Συνήθως διαπράττονται από άτομα ή οργανισμούς για απόκτηση χρημάτων, υπηρεσιών ή να διασφαλίσουν προσωπικό, πολιτικό ή επαγγελματικό πλεονέκτημα»[279].

Οι Hagan και Simon όπως και το Εθνικό Κέντρο Εγκλημάτων Λευκού Περιλαιμίου των ΗΠΑ χρησιμοποιούν τον ορισμό «παραβάσεις λευκού περιλαιμίου» που είναι:

> «Ο σχεδιασμός παρανόμων ή ανήθικων πράξεων απάτης που διαπράττεται από ένα άτομο ή ένα οργανισμό κατά την διάρκεια νόμιμης απασχόλησης από άτομο το οποίο έχει υψηλή ή ευυπόληπτη κοινωνική θέση για προσωπικό κέρδος ή κέρδος του οργανισμού το οποίο παραβιάζει την εμπιστοσύνη του κοινού».[280]

Οι διαφωνίες σχετικά με τους ορισμούς πολλές, διαφωνίες οι οποίες σύμφωνα με τον Λάζο «εμπεριέχουν αποκλίσεις σε ότι αφορά τις αξίες, την πολιτική, τη θεωρία, την επιστημολογία και τη μεθοδολογία όχι μόνο της εγκληματολογίας, αλλά όλων των κοινωνικών επιστημών».[281]

Κοινό στοιχείο στους παραπάνω ορισμούς αποτελεί η απουσία του κριτηρίου του (υψηλού) κοινωνικού στάτους, που είχε αρχικά τεθεί από τον εμπνευστή της θεωρίας (τον Sutherland) για το έγκλημα του λευκού περιλαιμίου, και η εστίαση στο οικονομικό κίνητρο από πλευράς δράστη. Τα στοιχεία αυτά μας αναγκάζουν πλέον, όταν μιλάμε για τέτοιου είδους συμπεριφορές, να αναφερόμαστε καλύτερα σε αυτά ως «οικονομικά εγκλήματα» παρά ως «εγκλήματα του λευκού περιλαιμίου».

3.2. Οι ερμηνευτικές προσεγγίσεις της οικονομικής εγκληματικότητας

Οι διάφορες ερμηνευτικές προσεγγίσεις για την κατανόηση του ηλεκτρονικού εγκλήματος από τη μια αλλά και του οικονομικού (με τις όποιες επιμέρους ορολογίες και εννοιοδοτήσεις έχουν προταθεί) από την άλλη, έχουν κοινή βάση τόσο μεταξύ τους όσο και με αυτές που έχουν προταθεί για την ερμηνεία του εγκληματικού φαινομένου γενικότερα.

[277] Λάζος Γρηγόρης (2001), σ. 57
[278] Bartol Curt (1999)
[279] Καπαρδή Μαρία, Καπαρδής Ανδρέας, Κουράκης Νέστορας (2001), σσ. 61-62
[280] Βλ. Helmkamp, Ball και Townsend, 1996 όπως αναφέρονται στο Λάζος Γρηγόρης (2013), σ.32
[281] Λάζος Γρηγόρης (2013), σ. 39

Οι διάφορες ερμηνευτικές προσεγγίσεις, μπορούν να ενταχθούν σε κάποια από τις παρακάτω τρεις κατηγορίες:

Πρώτον, οι θεωρίες που αποδίδουν το έγκλημα σε ατομικούς παράγοντες.

Δεύτερον, οι προσεγγίσεις που βλέπουν τις εργασιακές συνθήκες ως εγκληματογόνο παράγοντα.

Τρίτον, οι θεωρίες που εστιάζουν στις ευκαιρίες που προσφέρει το επιχειρησιακό περιβάλλον για τη διάπραξη παράνομων πράξεων.

Από τη σκοπιά της πρώτης κατηγορίας παραγόντων, οι ερευνητές που ασχολούνται με το επαγγελματικό έγκλημα (Coleman, Croall, Wheeler, Hirschi & Gottfredson) αναζητούν τις ερμηνείες του εγκλήματος του λευκού περιλαιμίου από κοινού με το παραδοσιακό έγκλημα, στις ατομικές συνθήκες όπως η οικονομική πίεση, η άδικη μεταχείριση και τα ατομικά χαρακτηριστικά[282]. Από την άλλη, οι θεωρητικοί που ασχολούνται με το επιχειρηματικό έγκλημα εστιάζουν στις οργανωσιακές θεωρίες που επικεντρώνονται στις συνθήκες που επικρατούν στη γενική ατμόσφαιρα μιας επιχείρησης και που διευκολύνουν το έγκλημα, πιστεύουν ότι χρειάζονται διαφορετικές οπτικές γωνίες εξήγησης του οικονομικού και του κοινού εγκλήματος[283].

Σύμφωνα με τον Coleman:

> «ο στόχος της πλειονότητας των εγκληματιών λευκού περιλαιμίου είναι το οικονομικό κέρδος ή η επιτυχία στον εργασιακό τομέα. Μολονότι τα εγκλήματα λευκού περιλαιμίου προκαλούν πολύ περισσότερους θανάτους και ζημιές από ότι άλλοι τύποι εγκλημάτων, αυτή η βία είναι υποπροϊόν του παραπτώματος, όχι του άμεσου στόχου όπως είναι στη βιαιοπραγία ή το φόνο. Είναι έλλογα, υπολογιστικά εγκλήματα και όχι εγκλήματα πάθους».[284]

Η Croall θεωρεί ως βασικό παράγοντα τέλεσης εγκλήματος την απληστία και θεωρεί τον εγωισμό και τον ατομικισμό ως εγγενείς αξίες στον καπιταλισμό.

Ο Cressey, από την πλευρά του υιοθετεί ένα πιο ατομικιστικό μοντέλο ερμηνείας και αποδίδει την κατάχρηση σε εσωτερικευμένα προσωπικά οικονομικά προβλήματα. Από μελέτη που διεξήγαγε σε διοικητικά στελέχη διαπίστωσε άμεση σχέση μεταξύ ατομικών παραγόντων των ανώτερων στελεχών και της διάπραξης εγκλήματος.

Ο Clinard με τη μελέτη του τόνισε τη σημασία της προσωπικότητας των ανώτερων στελεχών για τη διαμόρφωση της εσωτερικής δομής και κλίματος αποξένωσης στην επιχείρηση. Το σύστημα αξιών και ιδεών με το οποίο λειτουργούν τα ανώτερα στελέχη δημιουργούν ένα σύστημα άτυπων κανόνων στην επιχείρηση που οδηγεί στην αποξένωση μεταξύ των ατόμων. Οι επιχειρήσεις μάλιστα που εξαρτώνται άμεσα σημαντικά από την τεχνολογία της πληροφορίας είναι πιο ευάλωτες σε τέτοιες επιδράσεις.[285]

Οι Hirschi & Gottfredson διατύπωσαν, μια θεωρία εξήγησης της εγκληματικής συμπεριφοράς η οποία αποδίδει, τόσο το συνηθισμένο όσο και το έγκλημα του λευκού περιλαιμίου, στην απουσία αυτοελέγχου από πλευράς του δράστη. Υποστηρίζουν ότι ο

[282] Langton Lynn & Piquero Nicole (2007), σσ. 1-15.
[283] Reed Gary E & Yeager Peter Cleary (1996)
[284] Coleman James.W. (1987b), σσ. 406-439
[285] Backhouse James & Gurpreet Dhillon (1995)

εγκληματίας με το λευκό περιλαίμιο εμφανίζει παρόμοια χαρακτηριστικά με αυτά των κοινών εγκληματιών και κυρίως έλλειψη αυτοελέγχου.[286]

Οι «θεωρίες της ετικέτας» ή του «στιγματισμού» στο πλαίσιο της εγκληματολογίας της κοινωνικής αντίδρασης, με κυριότερους εκπροσώπους τους Edwin Lemert, Howard Becker, Stanley Cohen και άλλους, υποστηρίζουν ότι ένα άτομο δεν γίνεται εγκληματίας παρά μόνο εφόσον έχει χαρακτηριστεί ως τέτοιο από τους φορείς της κοινωνικής αντίδρασης μέσα από μια κοινωνική διαδικασία φιλτραρίσματος. Αυτό που διαφοροποιεί τον εγκληματία από τον μη-εγκληματία είναι ότι στον πρώτο έχει επιτυχημένα αποδοθεί η ετικέτα του εγκληματία.[287] Το έγκλημα δεν είναι αυθύπαρκτο αλλά αποτελεί μια κοινωνική κατασκευή, δημιουργείται από την κοινωνία που καθορίζει τους κανόνες, το τι συνιστά παραβίαση αυτών των κανόνων όπως και τις ποινές που επιβάλλονται στους παραβάτες. Σύμφωνα λοιπόν με τη θεωρία της ετικέτας οι εγκληματίες με το λευκό περιλαίμιο, αποφεύγοντας τη σύλληψη και τον στιγματισμό, διατηρούν σχέσεις εμπιστοσύνης με την ευρύτερη κοινωνία και παράλληλα μια θετική κοινωνική ταυτότητα και εικόνα του εαυτού τους μη θεωρώντας τις πράξεις τους ως εγκληματικές.

Οι ατομοκεντρικές προσεγγίσεις δεν επαρκούν από μόνες τους να δώσουν ικανοποιητικές απαντήσεις στην ερμηνεία του φαινομένου.

Πολλοί θεωρητικοί ασκώντας κριτική στην αιτιολογική προσέγγιση του Sutherland έχουν προτείνει τα δικά τους ερμηνευτικά σχήματα, μακρο-κοινωνιολογικής προσέγγισης, για το έγκλημα του λευκού περιλαιμίου τα οποία θα μπορούσαμε να εντάξουμε σε δύο γενικές κατηγορίες. Αυτά που προέρχονται από τη θεωρία της ανομίας και τα μαρξιστικής προέλευσης σχήματα που ενέπνευσαν την εγκληματολογία της κοινωνικής αντίδρασης και που βλέπουν το έγκλημα ως μια κοινωνική κατασκευή αποτέλεσμα της προσπάθειας των ανώτερων τάξεων να υπερασπιστούν και να επιβάλλουν τα συμφέροντά τους πάνω στα λιγότερο ευνοημένα κοινωνικά στρώματα.

Αμερικανοί θεωρητικοί χρησιμοποίησαν τη θεωρία της ανομίας του Durkheim και τη μετεξέλιξη της σε θεωρία πίεσης από τον Merton στην προσπάθειά τους να εξηγήσουν τα υψηλά επίπεδα εγκληματικότητας στις Ηνωμένες πολιτείες. Ο Durkheim απέδωσε την ανομία στις αιφνίδιες κοινωνικές αλλαγές, ενώ ο Merton αντίθετα εστίασε στη σταθερότητα των κοινωνικών δομών επιχειρηματολογώντας ότι η αμερικανική κοινωνία δίνει μεγαλύτερη έμφαση στην επίτευξη των στόχων, όπως πλούτος και γόητρο, από ό,τι στα θεσμικά αναγνωρισμένα μέσα (σκληρή δουλειά, επιμονή κ.λπ.).

Οι Messner Steven & Rosenfeld Richard διατύπωσαν και παρουσίασαν τη θεωρία της «θεσμικής ανομίας» (Institutional Anomie Theory)[288]. Υποστήριξαν ότι η αμερικανική κουλτούρα είναι παγιδευμένη στην αξία της ατομικής οικονομικής επιτυχίας μέσω ανταγωνισμού με περιορισμένα μέσα. Αυτό οδηγεί σε μια υπερβολική έμφαση στην οικονομία σε βάρος της σημασίας των μη οικονομικών θεσμών όπως η οικογένεια, η εκπαίδευση, η πρόνοια κ.λπ. Η έμφαση στον στόχο της ατομικής οικονομικής επιτυχίας σε συνδυασμό με τα περιορισμένα μέσα για την επιδίωξή της οδηγεί τα άτομα στο να καινοτομούν και να επινοούν εναλλακτικά μέσα, ακόμα και αθέμιτα, για να επιτύχουν τους θεμιτούς στόχους. Η προσπάθεια για οικονομική επιτυχία είναι ατέρμονη επειδή πάντα

[286] Hirschi Travis, & Gottfredson Michael R. (1987)

[287] Δασκαλάκης Ηλίας (1985), σσ. 133-134 και 145-155

[288] Messner Steven & Rosenfeld Richard (1994)

υπάρχει το περιθώριο για περισσότερο πλούτο και αποτελεί κίνητρο εξίσου για τους πλούσιους όσο και για τους φτωχούς. Για τον λόγο αυτό, σύμφωνα με τους Messner & Rosenfeld, οι δείκτες εγκληματικότητας είναι πιο αυξημένοι στις Ηνωμένες Πολιτείες σε σχέση με τις άλλες αναπτυγμένες χώρες οι οποίες δεν δίνουν τόσο μεγάλη έμφαση στην οικονομία αλλά στους μη οικονομικούς θεσμούς δημιουργώντας μηχανισμούς κοινωνικού ελέγχου που οδηγούν σε χαμηλότερη εγκληματικότητα.[289]

Άλλοι μελετητές του εγκλήματος του λευκού περιλαιμίου, όπως ο Passas, επηρεασμένοι και αυτοί από τη θεωρία της ανομίας του Merton, προτείνουν τις θεωρίες «ελέγχου» (Control theories) και «έντασης» (Strain theories) για την εξήγηση του φαινομένου. Έτσι τα οικονομικά εγκλήματα μπορεί να θεωρηθεί ότι αποτελούν μια «καινοτόμο αντίδραση των στελεχών των επιχειρήσεων στην ένταση που προκαλείται από τη δυσκολία προσαρμογής στις ανταγωνιστικές συνθήκες για τη διατήρηση και επαύξηση των κερδών» [290]. Συχνά τα μεσαία στελέχη πιέζονται να επιλέξουν ανάμεσα στην αποτυχία επίτευξης των στόχων που θέτει η ανώτερη διοίκηση και στο να επιδιώξουν τους στόχους με άνομα μέσα στη λογική του «κάν' το, αλλά μη μου πεις πώς το έκανες»[291].

Ο Braithwaite προσπαθεί να συνδυάσει στοιχεία, από τις περισσότερες παραδοσιακές εγκληματολογικές θεωρίες όπως τη θεωρία για τις υποκουλτούρες, τη θεωρία της «ετικέτας», τις θεωρίες «ελέγχου» και «έντασης», για να διατυπώσει μια ολοκληρωμένη θεωρία για το επιχειρηματικό έγκλημα.

Η κεντρική ιδέα της θεωρίας του για την εξήγηση του εγκλήματος των επιχειρήσεων, που ο Braithwaite την ονομάζει θεωρία των «ακραίων σημείων» (theory of tipping points), στηρίζεται στην θεωρία της ανομίας του Merton ότι το έγκλημα εξαρτάται από τη διαθεσιμότητα των νόμιμων και μη νόμιμων ευκαιριών για να επιτευχθούν οι στόχοι της επιχείρησης, το βαθμό στον οποίο αντίπαλες επιχειρήσεις και οργανισμοί την αναγκάζουν να υιοθετεί αθέμιτα μέσα, το κατά πόσο τα στελέχη ενός οργανισμού ή μιας επιχείρησης υπόκεινται σε σοβαρό αποκλεισμό των νόμιμων ευκαιριών επίτευξης των στόχων και κατά πόσο έχουν την ευκαιρία διάπραξης εγκλήματος. Όταν οι νόμιμες ευκαιρίες είναι μπλοκαρισμένες τότε ευνοείται η υιοθέτηση μιας υποκουλτούρας παρανομίας. Ιδιαίτερη σημασία έχει πάντα, όπως και για τη θεωρία του Sutherland, η αρνητική ερμηνεία για τη συμμόρφωση σε σχέση με την ερμηνεία για τη μη συμμόρφωση με τους κανόνες, εφόσον από τη μια επιδρούν οι δυνάμεις ελέγχου που πιέζουν για συμμόρφωση και από την άλλη της εγκληματικής υποκουλτούρας που πιέζουν για μη συμμόρφωση. Το έγκλημα διαπράττεται όταν οι ορισμοί της συμπεριφοράς που είναι ευνοϊκοί για την παραβίαση του νόμου υπερισχύουν των ορισμών που είναι κατά της παραβίασης του.[292]

Ο Steven Box διατείνεται ότι οι επιχειρήσεις εγκληματούν όταν μεγαλώνει η αβεβαιότητα και η αστάθεια στο εσωτερικό (υπάλληλοι, καταναλωτές, ανταγωνιστές) ή στο εξωτερικό (κράτος, νομοθεσία, κοινωνικό σύνολο) περιβάλλον τους[293] χρησιμοποιώντας παράνομα

[289] Schoepfer Andrea & Piquero Nicole (2006), σσ. 227-235
[290] Slapper Gary, & Steve Tombs (1999), σσ. 131-136.
[291] Braithwaite John (1985)
[292] Braithwaite John (1994), σσ.187-213
[293] Box Steven (1983), σ.35-37

μέσα, με θύματα τους ανταγωνιστές τους, τους καταναλωτές, το κράτος, είτε το κοινωνικό σύνολο γενικότερα με σκοπό τη διατήρηση της κερδοφορίας τους[294].

Μια άλλη, ριζοσπαστική τάση ερμηνείας του εγκλήματος του λευκού περιλαιμίου, μαρξιστικής προέλευσης, βλέπει το έγκλημα στο χώρο της οικονομίας ως αναπόφευκτο αποτέλεσμα του καπιταλισμού. Οι μεγάλες επιχειρήσεις και οργανισμοί αποτελούν χώρο εγκληματογένεσης στο βαθμό που ανταμείβουν τα επιτεύγματα ακόμα και σε βάρος του εξωτερικού τους περιβάλλοντος. Ένας από τους κυριότερους εκπροσώπους των μαρξιστών ο Ολλανδός W. Bonger αποδίδει, τόσο το παραδοσιακό έγκλημα όσο και το έγκλημα «με τα κουστούμια» σε απληστία και εκμετάλλευση των διαπροσωπικών σχέσεων που δημιουργούνται στον καπιταλιστικό καταμερισμό της εργασίας. Σύμφωνα με τον καταμερισμό αυτό, η αξία χρήσης της εργασίας έχει αντικατασταθεί από την ανταλλακτική αξία επειδή ο παραγωγός ανταλλάσσει το υπερπροϊόν της δικής του εργασίας με το υπερπροϊόν της εργασίας των άλλων. Το έγκλημα, δημιουργείται έτσι, αφενός από τις άθλιες συνθήκες που επιβάλλονται στην εργατική τάξη από τον καπιταλισμό και αφετέρου η εγκληματική συμπεριφορά των μελών της αστικής τάξης προέρχεται από απληστία όταν αναπτύσσεται ο καπιταλισμός.[295]

3.2.1. Η Συμβολική αλληλεπίδραση και η κοινωνιολογική προσέγγιση του E. Sutherland στη μελέτη του οικονομικού εγκλήματος

Στο Πανεπιστήμιο του Σικάγου αναπτύχθηκε επίσης η κοινωνική ψυχολογία και η θεωρία της «Συμβολικής Αλληλεπίδρασης» από τον George Herbert Mead και τον Herbert Blumer.[296] Αυτοί ακολουθήθηκαν μεταπολεμικά από τους Erving Goffman και Howard Becker και μπορούμε πλέον να μιλάμε για τη (δεύτερη) Σχολή του Σικάγου, αυτή της Συμβολικής αλληλεπίδρασης.[297]

Ο Sutherland από τη συμβολική αλληλεπίδραση είχε εμπνευστεί το «Διαφορικό Συγχρωτισμό» και έπειτα τη θεωρία του για την εγκληματικότητα του «Λευκού Περιλαιμίου» με έμφαση στην κοινωνική μάθηση και τις πολιτισμικές αξίες. Τα άτομα εγκληματούν επειδή συγχρωτίζονται, αλληλεπιδρούν με εγκληματικά πρότυπα και αξίες.[298]

Ακολουθώντας την κοινωνιολογική οπτική του Durkheim, ο Sutherland προσέγγισε το έγκλημα από κοινωνιολογική σκοπιά. Πρότεινε ότι ο ρόλος του κοινωνιολόγου θα πρέπει να είναι, η μετά από προσεκτική διερεύνηση, διατύπωση καθολικών θεωριών για την κοινωνία. Ως «κοινωνία» εννοεί περισσότερο ένα γενικό και αφηρημένο σύνολο παρά την συγκεκριμένη κοινότητα ή έθνος ή το γεωγραφικά τοποθετημένο σύνολο. Ως ιδιαίτερο πεδίο ενδιαφέροντος επέλεξε τη μελέτη της εγκληματικής συμπεριφοράς, όχι τόσο από την πλευρά του ελέγχου του εγκλήματος, αλλά περισσότερο για την ερμηνεία που μπορεί η μελέτη αυτής της συμπεριφοράς να δώσει για τα κοινωνικά πράγματα. Για τον λόγο αυτό πρότεινε μια γενική, καθολική θεωρία η οποία να παρέχει ερμηνεία όχι μόνο της εγκληματικής συμπεριφοράς αλλά και άλλων μορφών κοινωνικής συμπεριφοράς. Με τον τρόπο αυτό, θεωρούσε ο Sutherland ότι παραμένει συνεπής με το στόχο του κοινωνιολόγου να κατανοεί την κοινωνία κατασκευάζοντας μια γενική θεωρία για την κοινωνία η οποία θα εστιάζει στην εγκληματική

[294] Slapper Gary & Tombs Steve (1999), σσ. 134.
[295] Braithwaite John (1989), ό.π.
[296] Blumer Herbert (1966), σσ. 535- 544
[297] Βλ. Λαμπροπούλου Έφη (2009)
[298] Cote Suzette (2002), σσ. 76-77

συμπεριφορά. Παρόλα αυτά, ήταν απαισιόδοξος για τη δυνατότητα της κοινωνιολογίας να διατυπώνει ερευνητικά ερωτήματα που θα είναι άμεσα συνδεδεμένα με τους παραπάνω γενικούς στόχους. Πίστευε ότι είναι μεν εύκολο να διατυπωθούν ερευνητικές υποθέσεις που θα οδηγούν σε συγκεκριμένα ευρήματα και συμπεράσματα, αυτά όμως θα είναι δύσκολο να έχουν γενική εφαρμογή και δεν θα προάγουν την κοινωνιολογία ως επιστήμη.[299]

Ο Edwin Sutherland επικέντρωσε το ενδιαφέρον των ερευνών στην παραβατική συμπεριφορά των ανώτερων στρωμάτων της κοινωνίας. Χαρακτηριστική ήταν η «προεδρική ομιλία» του ως ο 29ος πρόεδρος στην Αμερικανική Εταιρεία Κοινωνιολογίας στη Φιλαδέλφεια το Δεκέμβριο του 1939, με θέμα την «Εγκληματικότητα Λευκού Περιλαιμίου»[300] που αποτέλεσε μια από τις ελάχιστες τέτοιες ομιλίες που έτυχαν πρωτοσέλιδης δημοσιότητας στον ημερήσιο τύπο της εποχής. Μια από τις εφημερίδες της Φιλαδέλφειας περιγράφει μάλιστα ότι το κοινό έμεινε έκπληκτο όταν ο καθηγητής Sutherland πέταξε επιδεικτικά ένα πακέτο από κοινωνιολογικά βιβλία στον κάδο των αχρήστων. Η εργασία του Sutherland, θεωρείται έκτοτε έργο ισάξιο σε σημασία με τη διατριβή του Lombroso για τον «Εγκληματία Άνθρωπο»[301] και υποστηρίχθηκε από τον Hermann Mannheim ότι αν υπήρχε Νόμπελ εγκληματολογίας θα έπρεπε να είχε αποδοθεί στον Sutherland για την εργασία του στο έγκλημα λευκού περιλαιμίου.[302]

Η προσπάθεια του Sutherland ήταν αφενός να εστιάσει στο υποκείμενο της δράσης και αφετέρου να διακρίνει τον ευυπόληπτο εγκληματία με το λευκό περιλαίμιο από τον εγκληματία που προέρχεται από τα χαμηλά στρώματα, που συνήθως φέρει φόρμα μπλε χρώματος αλλά και να διευρύνει το αντικείμενο έρευνας προς κάθε κατεύθυνση του δημόσιου (οικονομικού, επιστημονικού, πολιτικού) βίου, αρκεί να πρόκειται για δραστηριότητες που αφορούν την επαγγελματική και όχι την ιδιωτική ζωή του δράστη.

Τα εγκλήματα λευκού περιλαιμίου, σύμφωνα με τον αρχικό ορισμό του Sutherland, διαπράττονται από «άτομα ευυπόληπτα με ψηλό κοινωνικό status, κατά την πορεία των επαγγελματικών τους ενασχολήσεων εκμεταλλευόμενα την εμπιστοσύνη του κοινωνικού τους περίγυρου προβάλλοντας την εικόνα του τίμιου».

Το έγκλημα του λευκού περιλαιμίου είναι πραγματικό έγκλημα ενώ συνήθως δεν αντιμετωπίζεται ως τέτοιο. Ο Sutherland το καθιστά αντικείμενο μελέτης της εγκληματολογίας επειδή αποτελεί παραβίαση του ποινικού νόμου, όπως και τα εγκλήματα του κοινού ποινικού δικαίου.

Ο Sutherland για τον ορισμό των Εγκλημάτων Λευκού Περιλαιμίου, έδωσε έμφαση:

- Στο κοινωνικό status των εγκληματιών. Το έγκλημα του Λευκού Περιλαιμίου διαπράττεται από άτομα ευυπόληπτα με υψηλό κοινωνικο-οικονομικό επίπεδο.
- Στην εργασιακή σχέση. Γίνεται κατά τη διάρκεια μιας αξιοσέβαστης επαγγελματικής, επιστημονικής ή πολιτικής ενασχόλησης και όχι στον ιδιωτικό βίο.
- Στο ότι διαπράττεται από άτομα που γνωρίζουν, εκ των έσω, τις λειτουργίες μιας επιχείρησης.[303]

[299] *American Sociological Association*, www.asanet.org Απρίλιος (2007)
[300] Sutherland Edwin (1940), σσ. 1–12
[301] ανακοίνωση του Porterfield κατά το 6ο Διεθνές Συνέδριο Εγκληματολογίας στη Μαδρίτη.
[302] βλ. Box Steven (1983), σ.18
[303] Λάζος Γρηγόρης (2001), σσ. 55-56

Το εισόδημα και η περιουσία των ατόμων δεν μπορούν να αποτελούν τα μοναδικά κριτήρια. Όπως αναφέρει ο Sutherland:

«Πολλά άτομα χαμηλού κοινωνικο-οικονομικού επιπέδου μπορούν να είναι εγκληματίες του λευκού περιλαιμίου, με την έννοια ότι είναι καλοντυμένα, μορφωμένα και έχουν υψηλά εισοδήματα, όμως η έννοια του λευκού περιλαιμίου αφορά «αξιοσέβαστα», «κοινωνικά αποδεκτά» και «άξια θαυμασμού» άτομα. Μερικά απ' αυτά τα άτομα μπορεί να μην είναι καλοντυμένα ή μορφωμένα ή πλούσια, παρόλο που τα μέλη των ανώτερων τάξεων συνήθως ξεπερνούν αυτά των κατώτερων όσον αφορά τα παραπάνω χαρακτηριστικά».[304]

Ο Sutherland με τη μελέτη του βρήκε ότι η ποινική δίωξη των εγκλημάτων με το λευκό περιλαίμιο μπορεί συχνά να αποφευχθεί εξαιτίας της πολιτικής ή οικονομικής σπουδαιότητας των ατόμων που εμπλέκονται σε αυτά, εξαιτίας της δυσκολίας συγκέντρωσης στοιχείων εναντίον τους, ή εξαιτίας της φανερής ασημαντότητας των εγκλημάτων. Ακόμα οι πράξεις μπορεί να είναι ποινικά κολάσιμες, αλλά οι δράστες τους αποφεύγουν το στίγμα μιας ποινικής καταδίκης αφού συχνά δικάζονται σε αστικά δικαστήρια, με βάση νόμους των Ομοσπονδιακών Επιτροπών, όπως της Ομοσπονδιακής Επιτροπής Εμπορίου των ΗΠΑ (Federal Trade Commission Law), που επιβάλλουν πρόστιμα και σπάνια στα ποινικά δικαστήρια που επιβάλλουν ποινές στερητικές της ελευθερίας. Κάτω από αυτές τις προϋποθέσεις είναι πιο πιθανό ότι οι δράστες των εγκλημάτων λευκού περιλαιμίου θα αποφύγουν, παρά ότι θα υποστούν την καταδίκη.[305]

Ερώτημα, σύμφωνα με τον Sutherland, είναι το κριτήριο της παραβίασης του ποινικού νόμου. Αυτό που συχνά αναφέρεται ως τέτοιο κριτήριο είναι η ύπαρξη καταδίκης από ποινικό δικαστήριο, το οποίο όμως ο Sutherland δεν θεωρεί ως επαρκές κριτήριο, επειδή πολλοί από αυτούς που διαπράττουν εγκλήματα δεν καταδικάζονται στα ποινικά δικαστήρια. Το κριτήριο της παραβίασης του ποινικού νόμου θα πρέπει να ισχύει το ίδιο για όλους τους δράστες εγκλημάτων, ανεξάρτητα από την κοινωνική τους τάξη. Δεν θα πρέπει να ισχύει το «πνεύμα» του νόμου μόνο για τους εγκληματίες με το λευκό κολάρο, ενώ το «γράμμα» του νόμου για τους άλλους εγκληματίες.[306]

Ο κοινωνιολόγος Sutherland, λαμβάνοντας υπόψη του τόσο τους ατομικούς όσο και τους κοινωνικούς παράγοντες, χρησιμοποιεί τις θεωρίες της «κοινωνικής αποδιοργάνωσης» και του «διαφορικού συγχρωτισμού» όχι μόνο για την ερμηνεία του εγκλήματος του λευκού περιλαιμίου αλλά και του εγκληματικού φαινομένου γενικότερα. Έτσι, ο Sutherland εξετάζει το φαινόμενο της εγκληματικότητας σε δύο βάσεις: μία που αφορά το άμεσο περιβάλλον του δράστη και που ερμηνεύεται με τη θεωρία του «διαφορικού συγχρωτισμού» (Differential association) και μια που αφορά την ευρύτερη κοινωνία και που ερμηνεύεται από τη θεωρία της «κοινωνικής αποδιοργάνωσης» (Social disorganization).

Η πρώτη από αυτές τις θεωρητικές βάσεις, η θεωρία του «Διαφορικού συγχρωτισμού», που είναι εμπνευσμένη από τους «νόμους της μίμησης» του Tarde, προσπαθεί να δώσει μια εξήγηση όχι μόνο στο γενικό εγκληματικό φαινόμενο αλλά και ειδικότερα στα «Εγκλήματα Λευκού Περιλαιμίου» και στην επαγγελματική εγκληματικότητα.

Σύμφωνα με τη θεωρία του «διαφορικού συγχρωτισμού» κάθε συμπεριφορά διδάσκεται, έτσι και η εγκληματική συμπεριφορά διδάσκεται μέσα από το συγχρωτισμό, την επικοινωνία

[304] Sutherland Edwin, ό.π.

[305] Sutherland Edwin (1945), σσ. 132-139.

[306] Sutherland Edwin (1940), ό.π.

με ομάδες που ακολουθούν εγκληματικά πρότυπα και συμπεριφορές. Οι πιθανότητες να προσαρμοσθεί κάποιος στις αρχές και τα πρότυπα μιας τέτοιας εγκληματικής ομάδας είναι μεγαλύτερες όταν οι επαφές που έχει με τα εγκληματικά πρότυπα αυτής της οικείας ομάδας, είναι κατά συχνότητα, διάρκεια, χρονική προτεραιότητα και ένταση, ισχυρότερα των επαφών του με πρότυπα άλλων μη εγκληματικών ομάδων. Η εγκληματική εκπαίδευση χρησιμοποιεί τους ίδιους μηχανισμούς με οποιοδήποτε άλλο είδος εκπαίδευσης. Η διαδικασία αυτής της εγκληματικής εκπαίδευσης περιλαμβάνει τη διδασκαλία ενός συμπλέγματος συχνά δύσκολων και πολύπλοκων τεχνικών που απαιτούνται για την επιτυχή εκτέλεση της παράβασης, την αποφυγή της σύλληψης, την οριοθέτηση των κινήτρων και την εκλογίκευση των συμπεριφορών. Αυτή η οριοθέτηση και η εκλογίκευση αφορά την ευνοϊκή ή μη ευνοϊκή ερμηνεία των νόμων. Κάποιος παραβαίνει το νόμο όταν οι αρνητικές ερμηνείες για αυτόν επικρατήσουν σε σχέση με τις ευνοϊκές. Το κριτήριο αυτό αποτελεί και το σημαντικότερο για τη μετάβαση κάποιου ατόμου στην εγκληματική πράξη. Η εγκληματική συμπεριφορά αποτελεί έκφραση των ίδιων γενικών αναγκών και αξιών με την μη εγκληματική συμπεριφορά, οπότε μπορεί να εξηγηθεί σύμφωνα με αυτές τις ανάγκες και αξίες.

Στη βάση μιας διαδικασίας επικοινωνίας και μάθησης το άτομο δημιουργεί σχέσεις με κοινωνικές ομάδες με διάφορη εκάστοτε τοποθέτηση (θετική ή αρνητική) απέναντι στο νόμο και ακολουθεί σε μεγαλύτερο ή μικρότερο βαθμό τα πρότυπα των ομάδων αυτών. Απλά και μόνο επαφή με μέλη των ομάδων και τα πρότυπα τους δε συνεπάγεται και υιοθέτηση εγκληματικής συμπεριφορά. Απαιτείται αποδοχή και υιοθέτηση των εγκληματικών προτύπων και μάλιστα σε βαθμό που να υπερισχύουν αυτά τα πρότυπα έναντι άλλων μη εγκληματικών επιδράσεων από το περιβάλλον. Αν τελικά συμβεί κάτι τέτοιο τότε θα πρέπει, σύμφωνα με τη θεωρία, να αναμένεται η «μετάβαση στη πράξη».

Για την ερμηνεία των εγκλημάτων του λευκού περιλαιμίου πιο συγκεκριμένα, η θεωρία του «Διαφορικού συγχρωτισμού» συνδέεται με την παρατήρηση ότι, στο πλαίσιο των εμπορικών και οικονομικών σχέσεων, τα άτομα τείνουν να κινούνται σε μια ζώνη που τοποθετείται στα όρια μεταξύ θεμιτής και αθέμιτης συμπεριφοράς. Στο χώρο αυτό θεωρείται σχετικά ανεκτή η συνήθεια των συναλλασσόμενων να αντιγράφουν ο ένας τον άλλο (μιμητισμός). Έτσι για λόγους μιμητισμού, ή για λόγους αυτοσυντήρησης και επιβίωσης των υπαλλήλων εντός της επιχείρησης και του επιχειρησιακού ανταγωνιστικού χώρου όπου δρουν, εκμανθάνονται αθέμιτοι, παράνομοι μέθοδοι μέσω των οποίων επιδιώκονται αντίστοιχα αθέμιτοι σκοποί. Το πώς και πότε, τα άτομα ξεπερνούν τους ηθικούς δισταγμούς και εμπόδια και περνούν στη πράξη εξηγείται από τη γενικότερη θεωρία του διαφορικού συγχρωτισμού και της κοινωνικής αποδιοργάνωσης, σύμφωνα με τον Sutherland που ήταν επηρεασμένος από την προηγούμενη εργασία του σχετικά με τον επαγγελματία κλέφτη.

Ο Sutherland θεωρούσε τους εγκληματίες με το λευκό περιλαίμιο, στις υψηλές κοινωνικές θέσεις, το αντίθετο των επαγγελματιών κλεφτών. Το κοινό στοιχείο στις δύο ομάδες εγκληματιών είναι η εγκληματική δραστηριότητα ως μέρος των επαγγελματικών δραστηριοτήτων, της εκπαίδευσης, της καθοδήγησης και των εξειδικευμένων δεξιοτήτων που απαιτούνται για την εκτέλεσή τους. Οι εγκληματίες από τα κατώτερα στρώματα αρχίζουν τη σταδιοδρομία τους σε συνοικίες και οικογένειες με άσχημες συνθήκες, περιτριγυρισμένοι από παράνομους από τους οποίους μαθαίνουν τις παραβατικές συμπεριφορές και τις τεχνικές του εγκλήματος, με παράλληλη απομάκρυνσή τους από τους νομοταγείς πολίτες. Αυτοί που γίνονται εγκληματίες με το λευκό κολάρο συνήθως ξεκινούν την καριέρα τους σε καλές συνοικίες και σπίτια, αποφοιτούν από «καλά» κολέγια που προβάλλουν υψηλές ιδέες και

ιδανικά. Εισέρχονται στις ιδιαίτερες επιχειρηματικές καταστάσεις κατά τις οποίες η παρανομία αποτελεί ουσιαστικά παράδοση, μαθαίνουν αυτό τον τρόπο συμπεριφοράς όπως κάθε άλλη αξία. Η διαδικασία είναι κατ' ουσίαν η ίδια και στις δύο τάξεις εγκληματιών.

Η σημαντική διαφορά μεταξύ του επαγγελματία κλέφτη και του εγκληματία με το λευκό περιλαίμιο, πιστεύει ο Sutherland, ότι βρίσκεται στον αυτοπροσδιορισμό των δραστών. Οι επαγγελματίες κλέφτες όταν μιλούν για τον εαυτό τους είναι ειλικρινείς και παραδέχονται ότι είναι κλέφτες, ενώ αυτοί με το λευκό περιλαίμιο πιστεύουν ότι είναι τίμιοι άνθρωποι. Και ίσως γι' αυτό και ο Sutherland περιγράφει το έγκλημα του λευκού περιλαιμίου ως «έγκλημα των ανώτερων τάξεων, τα μέλη της οποίας φορούν λευκό κολάρο και είναι αξιοσέβαστοι ή τουλάχιστον ευυπόληπτοι άνθρωποι».[307]

Ο **διαφορικός συγχρωτισμός** οδηγεί στο έγκλημα γιατί η κοινότητα δεν είναι καλά οργανωμένη εναντίον αυτής της συμπεριφοράς. Υπάρχουν οι αντικρουόμενες δυνάμεις, του νόμου που πιέζουν για συμμόρφωση και των δυνάμεων που πιέζουν από την αντίθετη για παραβίασή του. Αυτό που μια κοινωνική ομάδα θεωρεί θεμιτό ή αναγκαίο μπορεί να θεωρείται εγκληματικό από κάποια άλλη κοινωνική ομάδα. Στις επιχειρήσεις οι «κανόνες του παιχνιδιού» συγκρούονται με τους κανόνες δικαίου. Ο επιχειρηματίας, ακόμα και αν επιθυμεί να τηρήσει τους κανόνες, οδηγείται από τους ανταγωνιστές του στο να υιοθετήσει τους δικούς τους κανόνες και μεθόδους. Στις επιχειρήσεις άτομα και ομάδες ενδιαφέρονται περισσότερο για το κέρδος και για τα ατομικά τους συμφέροντα παρά για το γενικό κοινωνικό συμφέρον. Κατά συνέπεια δεν είναι εύκολο για την κοινότητα να ακολουθήσει ένα σταθερό μέτωπο ενάντια στο έγκλημα. Οι καλύτερες επιχειρηματικές οργανώσεις και επιτροπές εναντίον του εγκλήματος, που τις αποτελούν επιχειρηματίες και επαγγελματίες, επιτίθενται εναντίον των διαρρηκτών, των ληστών και των κοινών απατεώνων αλλά παραβλέπουν τα εγκλήματα των δικών τους μελών. Η ίδια αντίφαση συμβαίνει και με τις δυνάμεις που επιδρούν στις κατώτερες τάξεις. Η κοινωνική αποδιοργάνωση επιδρά και στις δύο τάξεις με τον ίδιο τρόπο.[308]

Η δεύτερη βάση για την εξήγηση της εγκληματικότητας, σύμφωνα με τον Sutherland, προσφέρεται από τη θεωρία της **«κοινωνικής αποδιοργάνωσης».** Με τον όρο «κοινωνική αποδιοργάνωση» εννοείται μια γενικότερη παρέκκλιση της κοινωνίας από παραδεκτά πρότυπα ή στόχους, με συνέπεια, αφενός την έλλειψη «νομιμοποιήσεως» και κοινωνικής αποδοχής των επίσημων νομικών ρυθμίσεων και αφ' ετέρου την ανάπτυξη, στη θέση αυτών των ρυθμίσεων, άλλων, ειδικότερων «ορισμών» που αφορούν τη δραστηριότητα επί μέρους κοινωνικών ομάδων. Κατά την κοινωνική αποδιοργάνωση λείπουν οι πρωταρχικοί εκείνοι κανόνες του κοινωνικού οικοδομήματος, που αποτελούν τους συνδετικούς κρίκους που θα συνδέουν τους γραπτούς και καθιερωμένους νόμους με αυτούς που πρόκειται να τεθούν. Αντί αυτών υιοθετούνται άλλοι κανόνες που ρυθμίζουν απλώς τις σχέσεις προς τις μικρότερες κοινωνικές ομάδες. Σε μια σύγχρονη πλουραλιστική κοινωνία υπάρχουν κοινωνικές ομάδες με διαφορετικά πρότυπα, κανόνες και αξίες που ερμηνεύουν διαφορετικά τους σκοπούς και τα μέσα που παρέχει η κοινωνία για την επιδίωξή τους. Κάθε άτομο ανήκει σε περισσότερες από μία κοινωνικές ομάδες, κάθε μια απ' αυτές έχει διαφορετικές αξίες και αντιλήψεις για το σωστό ή το λάθος, το αποδεκτό ή το μη αποδεκτό. Όπως είναι φυσικό, όταν αυτές οι ομάδες ακολουθούν και προτρέπουν σε εγκληματικά πρότυπα, η επίδραση των υπόλοιπων νόμιμων

[307] Geis Gilbert, Meier Robert, Salinger Lawrence (editors) (1995), σσ. 24-25
[308] Sutherland Edwin (1940), ό.π.

ομάδων ή θεσμών αρχίζει να εξασθενεί, με τελική κατάληξη την διάπραξη εγκλημάτων από τα μέλη της που βρίσκονται σε μια «κατάσταση ανομίας» μη γνωρίζοντας τον κοινωνικά αποδεκτό τρόπο συμπεριφοράς. [309]

Η εξήγηση λοιπόν, που δίνει ο Sutherland, για τα δύο είδη εγκλημάτων, αυτά των ανώτερων και εκείνα των κατωτέρων τάξεων είναι κοινή και προσφέρεται από τη θεωρία του «διαφορικού συγχρωτισμού» και της «κοινωνικής αποδιοργάνωσης». Αυτές οι δύο θεωρίες αποτελούν τις βάσεις για την ερμηνεία των εγκλημάτων του λευκού περιλαιμίου όσο και της κοινής εγκληματικότητας. Η αναζήτηση των αιτίων του εγκλήματος λευκού περιλαιμίου προσδιορίζεται από τον Sutherland στη βάση κοινωνικών φαινομένων και προσωποπαγών χαρακτηριστικών του δράστη όπως το κοινωνικο – οικονομικό του επίπεδο, παρά σε βιολογικά και ψυχικά του χαρακτηριστικά. Επ' αυτού, οι μελετητές διαφωνούν μεταξύ τους για την εστίαση της έννοιας, όχι στις πράξεις, αλλά στα συγκεκριμένα χαρακτηριστικά του παρανομούντος ατόμου και στο χαρακτηρισμό των παραπτωμάτων του σαν εγκλήματα. [310]

Με τις θεωρίες του αυτές, ο Sutherland προσπαθεί να καταρρίψει τις ερμηνείες του εγκλήματος με όρους ατομικής ή κοινωνικής παθολογίας τονίζοντας ότι είναι δύσκολο να δεχτούμε τις αντιλήψεις ότι επιχειρήσεις ή επιχειρηματίες μπορεί να παραβαίνουν τον νόμο εξαιτίας «δύσκολων παιδικών χρόνων ή ψυχολογικών προβλημάτων». Απ' αυτή την άποψη ο σκοπός του Sutherland, να αναμορφώσει την εγκληματολογική θεωρία και να στρέψει την έρευνα για τις αιτιολογικές προσεγγίσεις σε άλλες πτυχές, πέτυχε. Από την άλλη όμως είναι υπό αμφισβήτηση το κατά πόσο η δική του θεωρία μπορεί να εφαρμοστεί - όπως ο ίδιος υποστηρίζει - για την ερμηνεία του εγκλήματος γενικότερα επειδή επιμένει ότι η κατασκευή της ατομικής πραγματικότητας αποτελεί αποκλειστικό προϊόν της συναναστροφής με άλλους και τα άτομα αυτομάτως υιοθετούν τα πρότυπα και τους ορισμούς αυτών με τους οποίους συναναστρέφεται. Παρότι μεγάλο μέρος της συμπεριφοράς είναι πράγματι αποτέλεσμα εκμάθησης στάσεων, αξιών και ορισμών από άλλους, ακόμα και αν τα άτομα μαθαίνουν την εγκληματική συμπεριφορά μέσα από τη συναναστροφή και την προσαρμογή τους με τις αξίες εγκληματικών ομάδων, η θεωρία του Sutherland δεν καταφέρνει να εξηγήσει το πώς δημιουργήθηκαν αρχικά οι συμπεριφορές, τα πρότυπα και οι ορισμοί και το αν αυτοί υπόκεινται σε αλλαγή, το πώς και γιατί οι ομάδες που τα υιοθετούν έγιναν εξαρχής εγκληματικές. Γιατί ένα άτομο υιοθετεί τους κώδικες της ομάδας ενώ κάποιο άλλο όχι; πώς εξηγεί τη διάπραξη εγκλημάτων από άτομα που δεν έχουν επηρεαστεί από άλλους εγκληματίες ή ομάδες, όπως τα εγκλήματα πάθους; Σε ποιο βαθμό οι συναναστροφές με εγκληματίες είναι αίτιο και σε ποιο αποτέλεσμα της εγκληματικής συμπεριφοράς;[311] Ο Braithwaite μάλιστα περιγράφει τη θεωρία του «διαφορικού συγχρωτισμού» ως «κοινότυπη αναδιατύπωση της θεωρίας της κοινωνικής μάθησης»[312].

Η κριτική, που έχει κατά καιρούς, ασκηθεί στην άποψη του Sutherland για το έγκλημα του λευκού περιλαιμίου, εστιάζεται αφενός στον ορισμό του εγκλήματος του λευκού περιλαιμίου και αφετέρου στην αιτιολογική προσέγγιση για την ερμηνεία του και την αντιμετώπιση του.

Οι συζητήσεις σχετικά με την έννοια που εισήγαγε ο Sutherland αφορούσαν σε ένα πρώτο επίπεδο στο κατά πόσο αυτή αναφέρεται σε κάποιο συγκεκριμένο τύπο εγκλήματος ή σε μια

[309] Sutherland Edwin (1940), ό.π.
[310] Βλ. κριτική από τον Tappan
[311] Williams Katherine (1991), σσ. 197-198.
[312] Slapper Gary & Tombs Steve (1999), σ. 114

συγκεκριμένη κατηγορία εγκληματιών ή συνιστά κάποια συγκεκριμένη μέθοδο διάπραξης οικονομικού εγκλήματος με την οποία ο δράστης ευελπιστεί να εξασφαλίσει τη μη σύλληψη και τιμωρία του. Μετά τον πρώτο ορισμό που έδωσε ο Sutherland για το έγκλημα του λευκού περιλαιμίου, ακολούθησε πλήθος συζητήσεων και διαφωνιών σχετικά με το ποια εγκλήματα και ποιοι εγκληματίες θα πρέπει να θεωρηθούν με το λευκό περιλαίμιο.

Όσον αφορά τον **ορισμό** του εγκλήματος του λευκού περιλαιμίου είναι τόσο ευρύς που εγείρει ένα σύνολο απροσδιοριστίας και ασαφειών. Αυτό, επειδή συμπεριλαμβάνει ένα μεγάλο εύρος παραβατικών συμπεριφορών, που έχουν ελάχιστα κοινά στοιχεία μεταξύ τους και μεγάλη διαβάθμιση ως προς το είδος τους, τον αριθμό και την ιδιότητα των εμπλεκομένων και το βαθμό θυματοποίησης. Τέτοια εγκλήματα είναι για παράδειγμα το οργανωσιακό, το κρατικό, το επαγγελματικό έγκλημα, η παραπλανητική διαφήμιση, οι απάτες στις επιχειρήσεις, οι παραπλανητικές πληροφορίες για την πορεία μετοχών στα χρηματιστήρια, η βιομηχανική κατασκοπεία, η κατασκευή και πώληση ελαττωματικών αυτοκινήτων, η μόλυνση και καταστροφή του περιβάλλοντος από βιομηχανίες, η πώληση επικίνδυνων φαρμάκων κ.λπ. που απειλούν την υγεία και τις ζωές εκατομμυρίων ανθρώπων.

Έντονη κριτική, για τον ορισμό του εγκλήματος του λευκού περιλαιμίου δέχθηκε ο Sutherland και από τον νομικό-κοινωνιολόγο Paul Tappan[313] που θεωρεί ότι αυτή η νέα κατηγορία εγκλήματος δημιουργεί προβλήματα, όχι μόνο εννοιολόγησης και αιτιολόγησης του, αλλά και προβλήματα άσκησης δημόσιας πολιτικής όσον αφορά στην αντιμετώπισή του, επειδή τα δικαστήρια και το σωφρονιστικό σύστημα δεν μπορούν να προσφέρουν αποτελεσματική πρόληψη, μεταχείριση και επανεκπαίδευση των δραστών τέτοιων εγκλημάτων.[314]

Ένα άλλο σημείο που προκάλεσε αντιδράσεις η άποψη του Sutherland για το έγκλημα του λευκού περιλαιμίου, μετά απ' αυτά του ορισμού και της αναζήτησης των αιτίων, είναι το ζήτημα της αντιμετώπισης του δράστη από το σύστημα απονομής δικαιοσύνης. Όπως είδαμε ο Sutherland υποστήριξε μεταξύ άλλων ότι τα μέλη των ανώτερων οικονομικά τάξεων αντιμετωπίζουν ευνοϊκότερες ποινές από τα δικαστήρια όταν και εφόσον επισημαίνονται από τις αρχές. Τα αποτελέσματα των ερευνών πάνω στο ζήτημα είναι μάλλον αντιφατικά. Κάποιες από τις έρευνες, όπως αυτή του Levi[315] και αυτή της Shapiro[316], υποστηρίζουν την άποψη του Sutherland. Κάποιες άλλες, όπως των Weisburd και συνεργατών, την αμφισβητούν με τα ευρήματά τους να δείχνουν ότι επιβάλλονται αυστηρότερες ποινές από τα δικαστήρια στους δράστες οικονομικών εγκλημάτων που ανήκουν στα ανώτερα κοινωνικά στρώματα[317].

Εδώ θα μπορούσαμε να σημειώσουμε πως η αυστηρότητα αυτή των δικαστηρίων προς τους εγκληματίες με το λευκό περιλαίμιο, στο βαθμό που ισχύει κάτι τέτοιο, θα μπορούσε να είναι και αποτέλεσμα των σημαντικών επισημάνσεων του Sutherland - και των εγκληματολόγων που τον ακολούθησαν - για τη βαρύτητα, την έκταση τέτοιων αδικημάτων και τις συνέπειες (οικονομικές, κοινωνικές και περιβαλλοντικές) που συνεπάγεται η διάπραξή τους.

[313] όταν μάλιστα ο Sutherland ήδη θεωρείτο πολύ εξέχουσα προσωπικότητα για να του ασκήσει κανείς άμεση κριτική.
[314] Tappan Paul (1947), σσ. 96 - 102
[315] Levi Michael (1989), σσ.86-109
[316] Shapiro Susan (1990)
[317] Nelken David (1994), σσ.355-392.

Ο Sutherland, καταλήγοντας, πρότεινε οι εγκληματολόγοι να διατυπώσουν θεωρίες που να μην εξετάζουν μόνο την εγκληματικότητα των κατωτέρων τάξεων -και τους παράγοντες που την προκαλούν με όρους ψυχολογικής ή κοινωνικής παθογένειας - αλλά και αυτή των ανώτερων τάξεων. Ακόμα πρότεινε να μην υπάρχει διαφορετική εφαρμογή του νόμου λόγω της διαφορετικής κοινωνικής θέσης μεταξύ των δύο κατηγοριών δραστών. [318] Στο συμπέρασμα του βιβλίου του, αναφέρει ότι οι ανώτερες τάξεις διαπράττουν πολλά εγκλήματα, αλλά δεν μπορούμε να πούμε αν τα μέλη τους εγκληματούν περισσότερο ή λιγότερο από αυτά της εργατικής τάξης, γιατί τα στοιχεία δεν είναι αρκετά ακριβή για να δικαιολογήσουν τις συγκρίσεις και δεν έχουμε διαθέσιμα κοινά πρότυπα και ορισμούς. [319]

3.3. Τα χαρακτηριστικά του οικονομικού εγκλήματος

Παρακάτω εξετάζουμε τα κυριότερα χαρακτηριστικά των οικονομικών εγκλημάτων προκειμένου να τα αντιπαραβάλλουμε με αυτά του ηλεκτρονικού-πληροφορικού εγκλήματος για να μελετήσουμε τη μεταξύ τους σχέση η οποία είναι σχέση γένους – είδους. Το ηλεκτρονικό δηλαδή έγκλημα αποτελεί σήμερα ένα πολύ σημαντικό κομμάτι του ευρύτερου οικονομικού εγκλήματος και εμφανίζει πολλά κοινά κύρια χαρακτηριστικά με αυτό.

Όπως είδαμε παραπάνω το έγκλημα του λευκού περιλαιμίου, σύμφωνα με τον Sutherland, διαπράττεται από άτομα με υψηλό κύρος που κατέχουν σημαντική κοινωνική θέση κατά τη νόμιμη απασχόλησή του. Τα εγκλήματα και οι εγκληματίες του λευκού περιλαιμίου διαφέρουν πολύ σημαντικά σε σχέση με τα παραδοσιακά εγκλήματα και τους κοινούς εγκληματίες. Τα εγκλήματα του λευκού περιλαιμίου είναι πιο πολύπλοκα, οργανωμένα, με μεγαλύτερη διάρκεια και επικερδέστερα σε σχέση με τα κοινά εγκλήματα. Όσον αφορά τους δράστες τους αυτοί γενικά είναι μεγαλύτερης ηλικίας, πιο μορφωμένοι, πιο ευκατάστατοι και κοινωνικά περισσότερο προσαρμοσμένοι.

Τέτοια εγκλήματα μπορεί να αφορούν εγκλήματα που διαπράττονται από τις επιχειρήσεις για αποκόμιση οφέλους για τις ίδιες ή σε βάρος των επιχειρήσεων από εργαζόμενους ή τρίτους. Παραδείγματα αποτελούν οι παραβιάσεις των κανονισμών ασφάλειας των εργοστασίων, λογιστικές απάτες, κλοπή σε βάρος της επιχείρησης από τους εργαζόμενους ή τα στελέχη, υπερβολικές χρεώσεις σε βάρος πελατών, υπερβολικές χρεώσεις από πλευράς στελεχών ή υπαλλήλων σε βάρος της επιχείρησης, κέρδη στο χρηματιστήριο με χρήση παράνομων πληροφοριών, δωροδοκίες, παράνομος έλεγχος τιμών από καρτέλ εταιρειών, μισθολογικές ή ασφαλιστικές απάτες κλπ.[320]

Όσον αφορά το **θύμα** του οικονομικού εγκλήματος, αυτό δεν είναι κατ' ανάγκη μόνο κάποιο φυσικό πρόσωπο αλλά μπορεί να είναι κάποιο κοινωνικό αγαθό, κοινωνικές αξίες, το φυσικό περιβάλλον, συλλογικές οργανώσεις, επιχειρήσεις, το κράτος. Έτσι μια αντιπροσωπευτική κατηγοριοποίηση των οικονομικών θυμάτων σύμφωνα με τους Kiefl & Lamnek, είναι:

α. Ατομικό ή προσωπικό οικονομικό θύμα, π.χ. θύμα απάτης.

β. Επιχειρήσεις ή οργανισμοί

γ. Συλλογικά θύματα, π.χ. η οικονομία της Ε.Ε ή του κράτους.

Στις δυο τελευταίες, ιδιαίτερα περιπτώσεις η διάπραξη του αδικήματος διευκολύνεται από τον απρόσωπο, ανώνυμο και πολύπλοκο χαρακτήρα του θύματος, την πιθανόν μικρότερη

[318] Sutherland Edwin (1940), ό.π.

[319] Sutherland (1983), σ. 264

[320] Κραμβία –Καπαρδή Μαρία, Τσολάκης Χρίστος (2011), σ. 25

αποδοκιμασία που εγείρει από το κοινό και το συνακόλουθα μικρότερο ενδιαφέρον για επίσημη κοινωνική αντίδραση απέναντι σε αυτό το είδος εγκλήματος. [321]

3.3.1. Τα χαρακτηριστικά του δράστη οικονομικού εγκλήματος

Τα εγκλήματα λευκού περιλαιμίου σύμφωνα με την Croall έχουν τα ακόλουθα χαρακτηριστικά:

1. Περιορισμένη Θέαση. Τα ίχνη τους καλύπτονται εύκολα, τα θύματα συχνά δεν γνωρίζουν καν ότι έπεσαν θύματα.
2. Πολυπλοκότητα, από πλευράς νόμων, χωρών που εμπλέκονται στη δικαιοδοσία και τεχνικών εξαπάτησης που χρησιμοποιούνται.
3. Διάχυση ευθύνης. Στα εγκλήματα αυτά εμπλέκονται πολλά άτομα μέσω Η/Υ από διαφορετικές εταιρείες και χώρες με αποτέλεσμα να είναι δύσκολο για τις αρχές να αποδείξουν και να αποδώσουν την ευθύνη.
4. Διάχυση της θυματοποίησης. Θύματα μπορεί να είναι το κράτος, μια εταιρεία ή πολλά άτομα ώστε συχνά δεν υπάρχει συγκεκριμένο και προσδιορίσιμο θύμα.
5. Δυσκολία ανίχνευσης, προσαγωγής στη δικαιοσύνη και απόδειξης της ευθύνης στο δικαστήριο λόγω μη επαρκούς συνεργασίας των θυμάτων με τις αρχές επειδή αυτά δεν επιθυμούν να λάβουν αρνητική φήμη αν γίνει γνωστή η υπόθεση.
6. Επιεικείς ποινές. Λόγω διασυνδέσεων, οικονομικής ευχέρειας για καλό συνήγορο πολλοί εγκληματίες του λευκού κολάρου επιτυγχάνουν είτε απαλλαγή είτε βραχύχρονη φυλάκιση.
7. Διέπονται από ασαφή νομοθεσία η οποία δεν περιγράφει με ακρίβεια τα στοιχεία του εγκλήματος. Οι δράστες εφευρίσκουν νέες μεθόδους διάπραξης πχ. μέσω του ίντερνετ.[322]

Ο Manheim έχει προτείνει τα εξής **χαρακτηριστικά** για το έγκλημα του λευκού περιλαιμίου:

Πρώτο, το υψηλό οικονομικο-κοινωνικό επίπεδο του δράστη.

Δεύτερο, η παραβίαση κανόνων δικαίου οι οποίοι δεν είναι κατ' ανάγκη ποινικοί.

Τρίτο, οι κανόνες αυτοί θα πρέπει να ορίζουν ανοικτά και περιγραφικά το σύνολο των επιτρεπόμενων επαγγελματικών δραστηριοτήτων των ατόμων.

Ακόμα συνάπτονται οι εξής **ιδιότητες** του εγκλήματος του λευκού περιλαιμίου:

Η πρώτη ιδιότητα αφορά την εκμετάλλευση της εμπιστοσύνης των θυμάτων.

Η δεύτερη, ότι το έγκλημα διαπράττεται με εξειδικευμένο, επιμήχανο τρόπο, πράγμα που καθιστά την ανακάλυψη του δράστη δύσκολη αν όχι αδύνατη. Συχνή είναι η χρησιμοποίηση νομικών κενών και διαφόρων μεσαζόντων ή υπαλλήλων με αποτέλεσμα την αφάνεια του πραγματικού δράστη.

Η τρίτη, ότι οι δράστες γνωρίζουν ότι διαπράττουν κάποιο αδίκημα, διαφωνούν όμως με τον παράνομο χαρακτήρα που αποδίδεται στην πράξη αυτή. Έχουν δηλαδή μια θετική εικόνα για τον εαυτό τους και θετική στάση για την πράξη τους.[323]

Σύμφωνα με επισκόπηση της αγγλόφωνης βιβλιογραφίας από την Κραμβιά-Καπαρδή οι δράστες των οικονομικών εγκλημάτων με δόλο παρουσιάζουν τα εξής χαρακτηριστικά:

1. Έχουν ώριμη ηλικία, 36-50 ετών.

[321] Βλ. Δημόπουλος Χαράλαμπος (1988), σσ. 138-143
[322] Καπαρδής Ανδρέας (2001), σ.24
[323] Βλ. Δημόπουλος Χαράλαμπος (1988), σσ. 70-71 και σελ 134

2. Έχουν ειδίκευση σε ορισμένης μορφής οικονομικό έγκλημα.
3. Είναι άνδρες.
4. Έχουν μόρφωση πάνω από το μέσο όρο εκπαίδευσης.
5. Παρουσιάζουν χαμηλό αυτοέλεγχο και μειωμένη συνείδηση.
6. Εμφανίζουν έλλειψη ηθικών αρχών.
7. Είναι εγωκεντρικοί.
8. Δεν αισθάνονται τύψεις για τις πράξεις τους και δεν αναλογίζονται τις συνέπειες τους.
9. Εκλογικεύουν τη συμπεριφορά τους ώστε να μην νοιώθουν ενοχές.
10. Είναι εθισμένοι στα οικονομικά οφέλη. [324]

Όπως αναφέρουν οι Κραμβιά -Καπαρδή και Τσολάκης, σύμφωνα με την έρευνα της ACFE[325] στο 57% των υποθέσεων απάτης οι δράστες κατείχαν διευθυντική θέση ή ήταν ιδιοκτήτες, οι περισσότεροι από τους μισούς είχαν ηλικία 36 έως 50 έτη, κατείχαν πτυχίο ή μεταπτυχιακό με γνώση των λογιστικών συστημάτων, ήταν άνδρες, παντρεμένοι με παιδιά, κατείχαν θέση εμπιστοσύνης (διευθυντές ή λογιστές), καλή κοινωνική θέση και καλή ψυχική υγεία. Ακόμα το 81% από αυτούς δεν είχαν κάποια καταδίκη, το 7% είχε καταδίκη και το 14% είχε απολυθεί λόγω απάτης.[326]

Τα κοινωνικά και επαγγελματικά χαρακτηριστικά του δράστη, όπως τα όρισε ο Sutherland, είναι το υψηλό κοινωνικό status, η ευυποληψία και η απασχόληση σε επαγγελματική θέση με κύρος και δύναμη και διαδραματίζουν σημαντικό ρόλο στη διαμόρφωση των εγκληματικών ευκαιριών που του παρουσιάζονται.[327] Όμως, από την άποψη της αντιμετώπισης αυτού του είδους εγκληματικότητας, τα στοιχεία αυτά έχουν λιγότερη σημασία σε σχέση τα χαρακτηριστικά των εγκλημάτων του λευκού περιλαιμίου. Έτσι προτείνεται η εστίαση περισσότερο στα χαρακτηριστικά της δράσης και λιγότερο του δράστη.

Σχετικά με την παραδοσιακή προσέγγιση του Sutherland και των συνεχιστών του για το υψηλό κοινωνικο-οικονομικό επίπεδο του δράστη οι Piquero και Benson σημειώνουν δυο σημαντικότατες παρατηρήσεις. Πρώτον, ότι τα στελέχη επιχειρήσεων που καταδικάστηκαν από την αμερικανική δικαιοσύνη για έγκλημα λευκού περιλαιμίου δεν διέθεταν οικονομική ή κοινωνική ισχύ. Ανήκαν στη μεσαία τάξη, με μέτρια εισοδήματα και συνηθισμένη επαγγελματική θέση ως μικρο-επιχειρηματίες ή απασχολούμενοι ως απλοί υπάλληλοι σε δουλειές γραφείου. Δεύτερο, ότι ένα σημαντικό ποσοστό (40%) από αυτούς είχαν και προηγούμενη σύλληψη ή εμπλοκή με το ποινικό σύστημα. Το ένα τρίτο από τους καταδικασθέντες συνελήφθηκαν ξανά μετά την αρχική τους καταδίκη. Τα δυο αυτά στοιχεία δείχνουν ότι οι εγκληματίες του λευκού περιλαιμίου που τελικά καταδικάζονται δεν είναι ούτε μέλη της κοινωνικής ελίτ ούτε και τόσο ευυπόληπτοι πολίτες.[328]

Για τα περισσότερα από τα εγκλήματα του λευκού περιλαιμίου, όπως αναφέρουν οι Benson και Madensen, ισχύει ότι:

α) Ο δράστης διαθέτει πρόσβαση στο πιθανό θύμα ή στόχο του εκμεταλλευόμενο την επαγγελματική του θέση που του δίνει τη δυνατότητα να το αναγνωρίσει και να το προσεγγίσει.

[324] Κραμβιά-Καπαρδή Μαρία (2001), σσ. 140-141.
[325] Ένωση Πιστοποιημένων Ελεγκτών κατά της απάτης
[326] Κραμβία –Καπαρδή Μαρία, Τσολάκης Χρίστος (2011), σσ.39-41
[327] Benson Michael. & Madensen Tamara (2007), σ. 612
[328] Piquero Nicole & Benson Michael L. (2004)

β) Η δράση του εγκληματία γίνεται στο πλαίσιο των νόμιμων δραστηριοτήτων του, ως εκ τούτου είναι δύσκολο να αποδειχθεί η βλάβη που προκαλείται ή ο δόλος που απαιτείται. [329]

γ) Ο δράστης χρησιμοποιεί την εξαπάτηση ή την συγκάλυψη για να καλύψει τα ίχνη της δράσης του τόσο από το πιθανό θύμα όσο και από τις διωκτικές αρχές. Όταν το υποψήφιο θύμα προσελκύεται σε μια απατηλή συναλλαγή δεν μπορεί να γνωρίζει τον πραγματικό της σκοπό.

δ) Ο δράστης βρίσκεται σε γεωγραφική απόσταση από τον στόχο ή το θύμα χωρίς να απαιτείται η φυσική επαφή μαζί του κατά τη στιγμή της διάπραξης του εγκλήματος. Η επικοινωνία ή η συναλλαγή μπορεί να γίνει εξ αποστάσεως μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή άλλου ψηφιακού μέσου.

ε) Ο δράστης βρίσκεται σε απροσδιόριστη ψυχική κατάσταση κατά την τέλεση του εγκλήματος με την νομική έννοια της σκοπούμενης βλάβης, ότι κανείς δεν μπορεί να διακρίνει τις εγκληματικές προθέσεις και σκοπούς του δράστη όπως για παράδειγμα συμβαίνει στα κοινά εγκλήματα όπου η σκόπιμη δράση είναι διακριτή κατά τη διάπραξη του εγκλήματος. Για το έγκλημα του λευκού περιλαιμίου οι δραστηριότητες συμβαίνουν μέσα στα συνηθισμένα όρια των καθημερινών νόμιμων ενασχολήσεων, στο πλαίσιο των οποίων απάτες μπορεί να θεωρηθούν απλά λάθη και ως εκ τούτου δεν εκλαμβάνονται ότι εμπεριέχουν εγκληματικό δόλο.[330]

Τα χαρακτηριστικά της εγκληματικής ευκαιρίας για τον δράστη του πιο συνηθισμένου είδος εγκλήματος λευκού περιλαιμίου, όπως είναι η απάτη, συνίστανται σε τρία κοινά στοιχεία:

α) Ο δράστης έρχεται σε επικοινωνία (εγγύτητα) με το πιθανό στόχο ενημερώνοντας τον για κάποιο προϊόν ή υπηρεσία που του προσφέρεται.

β) Το υποψήφιο θύμα πείθεται μέσω ψεύτικων εγγράφων ή δηλώσεων ότι πρόκειται για μια καλή και νόμιμη ευκαιρία.

γ) Ο δράστης πείθει το θύμα να του μεταβιβάσει χρηματικά ποσά με τη συναίνεση του.[331]

Οι Piquero και Benson πρότειναν το «διακοπτόμενο και περιστασιακά επηρεαζόμενο» (punctuated situationally dependent offending) πρότυπο εγκληματικής καριέρας. Σύμφωνα με το πρότυπο αυτό ο εγκληματίας του λευκού περιλαιμίου, μετά από μια σύντομη εμπειρία εμπλοκής με παραβατική δραστηριότητα κατά την νεαρή ηλικία, ακολουθεί μια περίοδο συμμόρφωσης και νομοταγούς συμπεριφοράς κατά την ηλικία των 20 και 30 οπότε και αρχίζει πάλι να παρανομεί ως εγκληματίας του λευκού περιλαιμίου. Η δραστηριότητα αυτή ξεκινά περιστασιακά, ενεργοποιούμενη από συμπτωματικούς παράγοντες εξωτερικούς προς τον δράστη. Η εγκληματική ευκαιρία του παρουσιάζεται μόνο όταν, πρώτον, ο δράστης αποκτά συγκεκριμένη επαγγελματική θέση, δεύτερον, στο πλαίσιο της οποίας αντιμετωπίζει κάποια κρίσιμη κατάσταση ή σημαντική δυσκολία η οποία του παρέχει το απαιτούμενο κίνητρο για να εκμεταλλευτεί την επαγγελματική του θέση και την ευκαιρία. Η δεύτερη αυτή εμπλοκή του δράστη με την παραβατικότητα δεν αποτελεί κατ΄ανάγκη συνέχιση της αρχικής, στη νεαρή του ηλικία οπότε και διέθετε διαφορετική προσωπικότητα από την τωρινή, επειδή η εγκληματική του πορεία είχε διακοπεί για μεγάλο διάστημα από περίοδο συμμόρφωσης. [332]

3.3.2. Η έννοια των κινήτρων

[329] Benson Michael. & Madensen Tamara (2007), σσ. 618-619
[330] Benson Michael. & Madensen Tamara (2007), σ.613
[331] Benson Michael & Madensen Tamara (2007), σ. 617
[332] Piquero Nicole & Benson Michael L. (2004), ό.π.

Ο Abraham Maslow με τη θεωρία των αναγκών[333] τόνισε τη σημασία των κινήτρων για την παρακίνηση των ατόμων σε κάποια δράση. Η ικανοποίηση των αναγκών αποτελεί τη βασική παραδοχή πάνω στην οποία στηρίζεται η θεωρία του Α. Maslow. Οι άνθρωποι δρουν για να ικανοποιήσουν τις ανάγκες τους, αυτό αποτελεί και το **κίνητρο** της δράσης. Όσο περισσότερο όμως ικανοποιούνται οι ανάγκες τόσο μικρότερο είναι το κίνητρο για δράση. Όταν ικανοποιηθεί πλήρως μια ανάγκη παύει πλέον να αποτελεί κίνητρο και κάποια άλλη ανάγκη παίρνει τη θέση της.

Σύμφωνα με τον Α. Maslow οι ανάγκες που κινητοποιούν τον άνθρωπο σε δράση ιεραρχούνται και ταξινομούνται σε:

1. Φυσιολογικές - βιολογικές ανάγκες που συνδέονται με την ύπαρξη του ανθρώπου, όπως το νερό, την τροφή, την ένδυση, την κατοικία και είναι οι πρώτες ανάγκες που προσπαθεί να ικανοποιήσει ο άνθρωπος.

2. Ανάγκες για ασφάλεια. Ο κάθε άνθρωπος θέλει να αισθάνεται σιγουριά για την ύπαρξή του και την μελλοντική ικανοποίηση των αναγκών του, να αισθάνεται ασφαλής έναντι των κινδύνων του περιβάλλοντος επιδιώκοντας να εξασφαλίσει μόνιμη απασχόληση, σύνταξη, κατοικία κτλ.

3. Κοινωνικές ανάγκες, δηλ. το αίσθημα του να ανήκει κάποιος σε κοινωνικές ομάδες, να γίνεται αποδεκτός, να διατηρεί φιλικές σχέσεις, να προσφέρει και να δέχεται αγάπη.

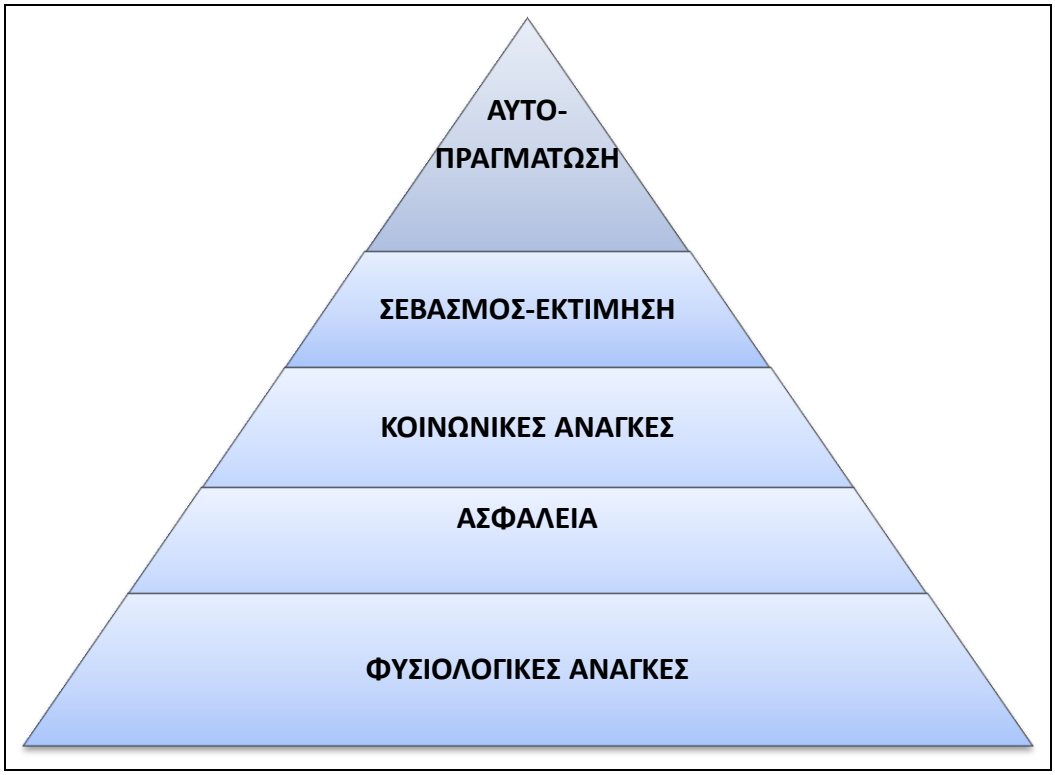
4. Εγωιστικές ανάγκες ή αναγνώρισης από τους άλλους, όπως η ανάγκη για φήμη, κύρος, εκτίμηση, σεβασμό, ανάγκη για επιτυχία, αυτοσεβασμό και αυτοεκτίμηση. Αυτή η κατηγορία των αναγκών είναι πιο δύσκολο να ικανοποιηθεί από ότι οι προηγούμενες και συνδέεται με τη διατήρηση ενός τρόπου ζωής με διασκέδαση, ταξίδια, περιουσία και ως εκ τούτου αποτελεί σημαντικό κίνητρο για τη διάπραξη εγκλήματος λευκού περιλαιμίου με τη μορφή απάτης.

5. Ανάγκες ολοκλήρωσης δηλαδή να γίνει κάποιος αυτό που ονειρεύεται, να ικανοποιήσει τους στόχους που έχει θέσει για τον εαυτό του, να αξιοποιήσει όλη του τη δυναμικότητα.

Οι παραπάνω ανάγκες είναι ιεραρχικά δομημένες με βάση την προτεραιότητα τους για ικανοποίηση, δηλαδή πρώτα ικανοποιούνται οι βιολογικές ανάγκες (βάση πυραμίδας) και έπειτα εμφανίζονται οι ανάγκες για ασφάλεια και αφού ικανοποιηθούν αυτές, έστω και σε κάποιο βαθμό παίρνουν τη θέση τους οι επόμενες κ.ο.κ.

[333] Maslow Abraham (1943)

Σχήμα 4. Η Πυραμίδα των Αναγκών του Maslow



Ο άνθρωπος, όσο ικανοποιεί κάποιες ανάγκες, επιθυμεί ολοένα και περισσότερα αγαθά και προσπαθεί συνεχώς να ικανοποιήσει καλύτερα τις ανάγκες του. Αυτά που επιθυμεί εξαρτώνται από αυτά που ήδη έχει. Έτσι η προσπάθειά του να ικανοποιήσει τις ανάγκες του συνεχίζεται σε όλη του τη ζωή.[334] Αυτό μπορεί να οδηγήσει κάποια άτομα στην απληστία και το οικονομικό έγκλημα για να πετύχουν την ικανοποίηση της ανώτερης κατηγορίας αναγκών ακόμα και με τη χρήση μη νόμιμων μέσων.[335]

Άλλωστε όπως τόνισαν οι Sutherland και Cressey, τόσο η σύννομη όσο και η εγκληματική συμπεριφορά αποτελούν εκφράσεις των ίδιων αναγκών και αξιών. Οι κλέφτες κλέβουν προκειμένου να βρουν χρήματα, ενώ οι νομοταγείς δουλεύουν για να καλύψουν την ίδια ανάγκη. Η διαφορά τους δεν έγκειται στο σκοπό που επιδιώκουν αλλά στα μέσα που χρησιμοποιούν.[336]

3.3.3. Τα κίνητρα του οικονομικού εγκλήματος

Ο Coleman εξέτασε την εγκληματική συμπεριφορά του λευκού περιλαιμίου ως συνδυασμό κινήτρων και ευκαιριών που είναι διαθέσιμες σε άτομα που κατέχουν θέσεις ισχύος. Τα κίνητρα των στελεχών επιχειρήσεων, συνδέονται σε πολλά σημεία με την ορθολογική επιλογή επειδή αυτά σχετίζονται κυρίως με επιδίωξη οικονομικού κέρδους, να φαίνονται επιτυχημένοι στους άλλους ή με το φόβο απώλειας των ήδη κεκτημένων.

Ο Coleman διέκρινε την μελέτη των κινήτρων σε τέσσερα μέρη:

α) το πρώτο αφορά το ρόλο της προσωπικότητας του κάθε ατόμου για τη διαμόρφωση του κινήτρου του εγκλήματος. Για μεγάλο διάστημα επικρατούσε η άποψη ότι ο εγκληματίας

[334] Maslow Abraham. (1943)
[335] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος (2011), σ.46
[336] Βλ. Fattah Ezzat (2008)

διέθετε μια ψυχοπαθολογική προσωπικότητα. Ο ίδιος ο Sutherland ήταν από τους πρώτους που υποστήριξε την φυσιολογικότητα των δραστών με το λευκό περιλαίμιο. Πράγματι οι εμπειρικές έρευνες συμφωνούν ότι, από ψυχιατρική άποψη, οι εγκληματίες του λευκού περιλαιμίου είναι φυσιολογικοί, χωρίς αυτό να σημαίνει ότι η προσωπικότητα τους δεν παίζει ρόλο στην εγκληματογένεση. Κάποιες μελέτες, όπως του Bromberg, βρήκαν ότι οι εγκληματίες αυτού του είδους είναι εγωκεντρικοί, πεισματάρηδες, με αίσθηση ανωτερότητας και υπεροχής. Ο John Spencer διαπίστωσε ότι είναι ριψοκίνδυνοι και τολμηροί σε μεγάλο βαθμό με τάση να επιδιώκουν να συγχρωτίζονται με άτομα υψηλότερης κοινωνικής θέσης, να παρέχουν στα παιδιά τους ακριβή ιδιωτική εκπαίδευση και να είναι διατεθειμένοι να αναλάβουν υψηλότερο οικονομικό ρίσκο προκειμένου να το πετύχουν.[337]

β) το δεύτερο μέρος της μελέτης των κινήτρων ασχολείται με την κουλτούρα, τόσο της γενικότερης κοινωνίας που εγείρει ηθικούς φραγμούς στην εγκληματική συμπεριφορά, όσο και της «κουλτούρας του ανταγωνισμού» των μεγάλων επιχειρήσεων που τονίζει τις ανταμοιβές από την παράνομη δραστηριότητα. Η αποκόμιση οικονομικού οφέλους αποτελεί ένα από τα θεμελιώδη κίνητρα του εγκλήματος λευκού περιλαιμίου και η επιθυμία γρήγορου και εύκολου κέρδους προβάλλεται ως ο συχνότερος λόγος διάπραξής του, σύμφωνα με έρευνα του Robert Lane. Άλλοι κινητοποιούνται σε εγκληματική δράση από το φόβο «να μην απολέσουν τα ήδη κεκτημένα» ή όπως διαπίστωσαν οι Weisburd, Wheeler, Wating και Bode από το φόβο «της πτώσης», που διακατέχει τα μέλη της μεσαίας τάξης, από τη κοινωνική θέση των ισχυρών που παίζουν κυρίαρχο ρόλο στο οικονομικό σύστημα και τον τρόπο ζωής που έχουν καταφέρει να πετύχουν με θυσίες.

Η κουλτούρα του ανταγωνισμού θέτει τον πλούτο και την επιτυχία ως βασικούς στόχους για τα άτομα στις δυτικές κοινωνίες. Ο ανταγωνισμός και η προσπάθεια για την ατομική επιτυχία σημασιοδοτείται ως θετικός, όχι μόνο για το χαρακτήρα των ατόμων, όπου ανταμείβονται οι πιο ικανοί και σκληρά εργαζόμενοι, αλλά και για την οικονομική ανάπτυξη των κοινωνίας γενικότερα. Αυτό δίνει την απαραίτητη νομιμοποίηση και κοινωνική αποδοχή της ανωτερότητας των πλουσίων ως ικανών και εργατικών και την κατωτερότητα των φτωχών ως φυσιολογικό αποτέλεσμα της ανικανότητας και της τεμπελιάς. Η εξιδανίκευση του επιτυχημένου και ο στιγματισμός του φτωχού λειτουργεί ενισχυτικά, αφενός για το κίνητρο της ατομικής επιτυχίας και αφετέρου για το φόβο και την ανασφάλεια της αποτυχίας.

Τα ευρήματα αυτά συνάδουν με τις βασικές αρχές της κλασικής σχολής των Beccaria και Bentham για επιδίωξη μέγιστης ικανοποίησης και ελάχιστου πόνου ως κίνητρο της συμπεριφοράς.

Οι οικονομίες της αγοράς είναι στενά συνδεδεμένες με τις έννοιες του κέρδους και της ζημίας και μάλιστα το κέρδος του ενός μέρους μπορεί να συνδέεται με τις απώλειες του άλλου. Η χρήση του χρήματος, ως γενικό μέσο συναλλαγών και ως μέτρο της αξίας των αγαθών, των κερδών και των ζημιών, ενισχύει τον ανταγωνιστικό χαρακτήρα για την επιδίωξη του προσωπικού οφέλους. Ο ατομοκεντρισμός των βιομηχανικών κοινωνιών συμβάλλει ώστε τα άτομα να θεωρούνται δράστες που δρουν αυτόνομα προβάλλοντας το προσωπικό έναντι του συλλογικού συμφέροντος και αναγκών[338].

γ) το τρίτο αφορά τους μηχανισμούς εξουδετέρωσης των παραπάνω ηθικών φραγμών από τους πιθανούς δράστες. Οι Matza και Sykes περιέγραψαν τις «τεχνικές εξουδετέρωσης» [339] ως

[337] Coleman James.W. (1995)

[338] Coleman James.W. (1995)

[339] «δικαιολόγησης» ή «ουδετεροποίησης» (neutralization), βλ. Sykes Gresham M., Matza David (1957)

μηχανισμούς που δίνουν τη δυνατότητα στα άτομα να υπερβαίνουν τις ηθικές αρχές, τον κοινωνικό έλεγχο και τους κανονιστικούς περιορισμούς που θέτουν οι κοινωνικοί θεσμοί με σκοπό την αποτροπή των εγκληματικών δράσεων. Τα άτομα αναπτύσσουν εκλογικεύσεις για να δικαιολογούν τις πράξεις τους, προτού αυτές λάβουν χώρα και να εξουδετερώνουν το χαρακτηρισμό τους ως παραβατικών.

Οι Sykes και Matza θεώρησαν τις τεχνικές ουδετεροποίησης ως σημαντικό κομμάτι της έννοιας του «ευνοϊκού ορισμού για την παραβίαση του νόμου» στο πλαίσιο του διαφορικού συγχρωτισμού του Sutherland και τις διέκριναν σε πέντε κατηγορίες:

1. Η άρνηση της ευθύνης, ότι η εγκληματική πράξη έγινε ακούσια, κατά λάθος ή ήταν αποτέλεσμα πίεσης έξω από τον έλεγχο του δράστη.
2. Η άρνηση της ζημίας που προκαλεί η εγκληματική δράση, ότι δεν παθαίνει κανείς τίποτα, ότι πρόκειται για δάνειο ή ότι το θύμα έχει πολλά χρήματα και δεν θα του λείψουν.
3. Η άρνηση του θύματος, ότι δεν ήταν άδικη η πράξη και ότι αποτελεί ένα είδος δίκαιης εκδίκησης, ανταπόδοσης, που το θύμα άξιζε να λάβει ενώ ο δράστης νοιώθει ως Ρομπέν των δασών.
4. Η καταδίκη των κατήγορων, όπου οι εκπρόσωποι του κοινωνικού ελέγχου θεωρούνται υποκριτές, παραβάτες οι ίδιοι ή έχουν ιδιοτελή κίνητρα. Η αστυνομία κατηγορείται ως βίαιη, διεφθαρμένη, οι δάσκαλοι κάνουν διακρίσεις και οι γονείς «ξεσπούν πάνω στα παιδιά τους».
5. Η αφοσίωση σε υψηλότερη αξία, όπως η παροχή βοήθειας σε φίλους που ανήκουν στην ίδια υποκουλτούρα, αφορά εκλογικεύσεις του τύπου «δεν το έκανα για μένα», «όλοι τα βάζουν μαζί μου» ή «το άξιζαν να το πάθουν». [340]

Ο Cressey αξιοποίησε τις τεχνικές ουδετεροποίησης των Sykes και Matza στη μελέτη του οικονομικού εγκλήματος. Σύμφωνα με τον Cressey, οι καταχραστές για παράδειγμα, δικαιολογούν την πράξη τους πιστεύοντας ότι «απλά δανείζονται τα χρήματα και ότι θα τα επιστρέψουν μόλις μπορέσουν. Αν μπορεί κάποιος να χρησιμοποιήσει κάτι και να το βάλει πίσω στη θέση του κανείς δεν παθαίνει τίποτα και είναι όλα εντάξει». Βέβαια οι δράστες εμπλεκόμενοι ολοένα και περισσότερο στην παράνομη δραστηριότητα είτε συλλαμβάνονται είτε συνειδητοποιούν ότι ποτέ δε θα μπορέσουν να επιστρέψουν όλα τα χρήματα. Σε άλλες μορφές εγκλήματος του λευκού περιλαιμίου οι εκλογικεύσεις που γίνονται είναι ότι η δράση τους «δεν βλάπτει κανέναν», ότι «παράνομη ναι αλλά όχι εγκληματική», ότι «το ίδιο κάνουν όλοι» ή ότι «ο ίδιος ο νόμος είναι άδικος». Για παράδειγμα οι επιχειρηματίες ισχυρίζονται ότι η (νομική) παρέμβαση και οι περιορισμοί του κράτους παραβιάζουν την βασική αρχή της ιδεολογίας του ελεύθερου ανταγωνισμού και της οικονομικής ελευθερίας και ως εκ τούτου ο νόμος είναι που προκαλεί βλάβη στο κοινωνικό σύνολο και όχι οι παρανομίες των επιχειρήσεων.

Μια εκλογίκευση που χρησιμοποιείται περισσότερο από υπαλλήλους που εγκληματούν ενάντια της επιχείρησης που εργάζονται είναι ότι κάνουν την παρανομία προκειμένου να επιβιώσουν ή να βοηθήσουν φίλους και συγγενείς.

Άλλη εκλογίκευση, για τα επαγγελματικά εγκλήματα, τις κλοπές από υπαλλήλους κυρίως, είναι ότι ο δράστης δικαιούται τα χρήματα λόγω εκμετάλλευσης του από την επιχείρηση ή ότι η επιχείρηση τους οφείλει κάτι παραπάνω. [341]

[340] Sykes Gresham M.,& Matza David (1957), ό.π.

[341] Βλ. Coleman James.W. (1995), σσ. 366-369 αναφορά στον Cressey.

Ο Mattera θεωρεί ότι τα μικρο-εγκλήματα των εργαζομένων αποτελούν μια μορφή μεταλλαγμένης πάλης με στόχο την αναδόμηση των κοινωνικών σχέσεων και την καθιέρωση ελέγχου από τους εργάτες.[342]

Ο Cressey θεωρεί ότι ο κάθε δράστης δεν εφαρμόζει πάντα αποκλειστικά δικές του εκλογικεύσεις αλλά στις περισσότερες των περιπτώσεων χρησιμοποιεί τις τεχνικές εξουδετέρωσης που μαθαίνει από άλλους στο πλαίσιο της επιχειρηματικής κουλτούρας η οποία παρέχει στα άτομα όχι μόνο τα απαραίτητα κίνητρα αλλά και τις κατάλληλες εκλογικεύσεις.[343]

δ) Τέλος σημαντικός είναι ο ρόλος των πολύπλοκων οργανισμών και επιχειρήσεων στη διαμόρφωση των κινήτρων των ατόμων. Οι μεγάλες επιχειρήσεις για να επιβιώσουν χρησιμοποιούν μηχανισμούς πίεσης και ελέγχου της συμπεριφοράς ώστε να πείσουν μεγάλο αριθμό υπαλλήλων να εμπλακούν σε παράνομες δραστηριότητες. [344]

Σύμφωνα με τον Coleman το κίνητρο αποτελεί ένα σύστημα συμβολικών κατασκευών που ορίζει κάποιους στόχους και δραστηριότητες ως κατάλληλους και επιθυμητούς και άλλους όχι. Έτσι το κίνητρο εξετάζεται από την πλευρά της συμβολικής αλληλεπίδρασης και το νόημα που τα ίδια τα άτομα δίνουν σε συγκεκριμένες καταστάσεις και την κοινωνική πραγματικότητα αλλά και τις αντιδράσεις που αναμένουν από τους άλλους. Η αντίφαση που προκαλείται κατά την εφαρμογή της συμβολικής αλληλεπίδρασης, στη μελέτη των κινήτρων του εγκλήματος του λευκού περιλαιμίου, έχει να κάνει με το γεγονός ότι οι κοινωνικές προσδοκίες του «γενικευμένου άλλου» για συμμόρφωση με τα καθιερωμένα πρότυπα και κανόνες έρχονται σε αντίθεση με τις προσδοκίες των «σημαντικών άλλων». Οι σημαντικοί άλλοι στην προκειμένη περίπτωση είναι τα ανώτερα στελέχη των επιχειρήσεων τα οποία αντιπροσωπεύουν την κουλτούρα του ανταγωνισμού των επιχειρήσεων και ασκούν πίεση στα άτομα ακόμα και να παραβαίνουν τους ηθικούς φραγμούς και κανόνες προκειμένου να ανταποκριθούν στην επίτευξη των στόχων που επιβάλλει ο ατομοκεντρικός και ανταγωνιστικός χαρακτήρας του οικονομικού ορθολογισμού που διέπει τις βιομηχανικές κοινωνίες. Η αντίφαση αυτή ξεπερνιέται με την ανάπτυξη των τεχνικών εξουδετέρωσης και τις εκλογικεύσεις που αποδυναμώνουν την επίδραση των κανονιστικών προτύπων της ευρύτερης κοινωνίας προς όφελος της (υπο)κουλτούρας του ανταγωνισμού που αναπτύσσεται σε συγκεκριμένες κοινωνικές ομάδες, όπως οι επιχειρήσεις που προσδιορίζουν και παρουσιάζουν στα μέλη τους μια ιδιαίτερη κοινωνική πραγματικότητα απομονωμένη από την ευρύτερη κοινωνία. [345]

Ένας από τους πιο αποτελεσματικούς μηχανισμούς συμμόρφωσης των υπαλλήλων για να ανταποκριθούν στις προσδοκίες και τους στόχους των επιχειρήσεων είναι ο φόβος της απόλυσης ή της μη αναμενόμενης προαγωγής. Έτσι η υπακοή, η αφοσίωση και η συμμόρφωση με τις προσδοκίες των προϊσταμένων παίζουν σημαντικό ρόλο για την επιτυχία του υπαλλήλου. Η χρήση αυτή της «αποφυγής του πόνου»[346] είναι αναγκαίος αλλά όχι ικανός παράγοντας για την εξασφάλιση της συμμόρφωσης του υπαλλήλου. Ο άλλος παράγοντας είναι η καλλιέργεια της επιχειρησιακής υποκουλτούρας που διαμορφώνει τη συμπεριφορά των υπαλλήλων υποσυνείδητα με διάφορους τρόπους, το ήθος, οι αξίες και οι στάσεις της

[342] Λάζος Γρηγόρης, (2001), σσ. 56 -60
[343] Coleman James.W. (1995), σσ. 366-369
[344] Coleman James.W. (1995), σσ. 369-372
[345] Coleman James.W. (1987), σ.156
[346] σύμφωνα με την κλασική ωφελιμιστική θεωρία

επιχείρησης, ιδιαίτερα των ανώτερων στελεχών, που συγκροτούν μια κοινωνική πραγματικότητα με δικό της ηθικό κώδικα απέναντι στην παράνομη συμπεριφορά. Οι ηθικές αξίες των χαμηλότερων στελεχών πρέπει να θυσιάζονται για χάρη της καριέρας και να αναπροσαρμόζονται, για να βρίσκονται σε συμφωνία με αυτές της διοίκησης, αν κάποιος θέλει να φτάσει προς την κορυφή της ιεραρχίας. Όπως σημειώνει ο Coleman «η αποτελεσματική διοικητική γραφειοκρατία απαιτεί ηθικό κομφορμισμό ή καλύτερα ανήθικο ρεαλισμό». Τα καλά προσαρμοσμένα διοικητικά στελέχη λειτουργούν με κυνικό τρόπο προς όφελος της επιχείρησης χωρίς έννοια για τις ηθικές επιπτώσεις των πράξεων τους. Οι στάσεις αυτές είναι σε συμφωνία με αυτό που ο C.W.Mills ονόμασε «δομική ανηθικότητα» της αμερικάνικης κοινωνίας. [347]

Έρευνα της Harvard Business Review διαπίστωσε ότι τα τέσσερα από τα πέντε στελέχη βιομηχανιών θεωρούν τις πρακτικές των εταιριών τους ως ανήθικες και τέσσερα από τα επτά ότι η συμπεριφορά άλλων στελεχών θα παραβίαζε τους ηθικούς κώδικες αν ήξεραν ότι δεν θα αποκαλυφτούν[348]. Μια ακόμα έρευνα σε ανώτερα στελέχη των 57 μεγαλύτερων αμερικάνικων επιχειρήσεων διαπίστωσε ότι αυτά πίστευαν πως η ανήθικη συμπεριφορά είναι ευρέως διαδεδομένη στις βιομηχανίες και ότι θα πρέπει πια να θεωρείται ως μέρος των καθημερινών επιχειρηματικών δραστηριοτήτων ρουτίνας. [349]

Η χαοτική δομή και το μέγεθος των κολοσσιαίων οργανισμών διευκολύνει τον έλεγχο της συμπεριφοράς των υπαλλήλων μέσω του ορισμού της πραγματικότητας στο εσωτερικό τους. Κάθε εργαζόμενος, στο πλαίσιο του εσωτερικού καταμερισμού της εργασίας, ασχολείται με μικρό μόνο μέρος της συνολικής παραγωγής μη έχοντας επίγνωση του συνολικού προϊόντος, έτσι αν αναρωτηθεί για τις νομικές συνέπειες της οικονομικής δραστηριότητας της επιχείρησης του υπενθυμίζεται ότι αυτό δεν δική του αρμοδιότητα αλλά της ανώτερης διοίκησης. Ταυτόχρονα τα ανώτερα στελέχη αποποιούνται των νομικών ευθυνών τους, διαχέοντας την ευθύνη της επίτευξης στόχων που απαιτούν χρήση ακόμα και παράνομων μέσων σε κατώτερα στελέχη, ξεκαθαρίζοντας ότι εκείνοι δεν θέλουν ούτε να ακούνε για παράνομες δραστηριότητες.

Η επιχείρηση ελέγχει τη συμπεριφορά των μελών της μέσω μιας σειράς νοηματοδοτήσεων των καταστάσεων που αυτά αντιμετωπίζουν κατά τη διάρκεια των καθημερινών επαγγελματικών δραστηριοτήτων τους. Η επιχείρηση ορίζει τους στόχους, τα μέσα, το που θα πρέπει να εστιαστεί η προσοχή των υπαλλήλων και που όχι. Το σύνολο αυτών των ορισμών εμφανίζει τις παράνομες δραστηριότητες να θεωρούνται κανονικές, ως μέρος της καθημερινής ρουτίνας.

Το εγχείρημα αυτό διευκολύνεται από το γεγονός της απομόνωσης των στελεχών από τον έξω κόσμο επειδή λόγω φόρτου εργασίας αφοσιώνονται, με στρατιωτική πειθαρχία, στα ανώτερα στελέχη και ο συγχρωτισμός τους με άλλα άτομα εξαντλείται σε αυτά του ίδιου κύκλου. Έτσι δεν υπάρχει η απαξίωση και η καταδίκη της παράνομης συμπεριφοράς από εξωτερικούς φορείς ελέγχου. Κάποιοι μάλιστα από τους υπαλλήλους που τελικά συνελήφθησαν εξέφρασαν την απορία και την έκπληξή τους γιατί οι πράξεις τους θεωρήθηκαν εγκληματικές από τον έξω κόσμο. [350]

[347] Coleman James.W. (1995), σσ. 369-372

[348] Βλ. Coleman James.W. (1987), σ.160 αναφορά σε Baumhart 1961.

[349] Βλ. Coleman James.W. (1987), σ.160 αναφορά σε Silk & Vogel 1976.

[350] Coleman James. W. (1995), σσ. 369-372

Ο Coleman ήδη είχε επισημάνει ότι δεν αρκούν τα κίνητρα αλλά θα πρέπει να υπάρχει και η κατάλληλη ευκαιρία. Η κατανομή των ευκαιριών διαφέρει σημαντικά ανάμεσα στα δύο φύλα, στα διάφορα επαγγέλματα, τους οργανισμούς και τις βιομηχανίες.[351]

Παρατηρούμε εδώ ότι οι απόψεις του Coleman για τα κίνητρα και τις ευκαιρίες υποστηρίζουν τη θεωρία των καθημερινών δραστηριοτήτων τόσο σε σχέση με την ύπαρξη του εγκληματία με κίνητρο, την παραβίαση των κανόνων στη διάρκεια των καθημερινών επαγγελματικών δραστηριοτήτων ρουτίνας, όσο και την απουσία ικανών φυλάκων που σε αυτή την περίπτωση είναι η – μη – ύπαρξη εξωτερικών προς την επιχείρηση άτυπων φορέων που θα ελέγχουν την παράνομη δράση των στελεχών της επιχείρησης η οποία διαδραματίζεται στο πλαίσιο των καθημερινών τους δραστηριοτήτων ρουτίνας.

3.3.4. Τα χαρακτηριστικά των θυμάτων του οικονομικού εγκλήματος

Από την άποψη των φορέων που θυματοποιούνται από περιπτώσεις απάτης οι σχετικές έρευνες της ACFE για το 2010 δείχνουν ότι συχνότερα θύματα είναι οι βιομηχανίες, οι τραπεζικές ή οικονομικές υπηρεσίες και οι κρατικές ή δημόσιες υπηρεσίες. Οι μεγαλύτερες επιχειρήσεις συγκεντρώνουν μεγαλύτερες πιθανότητες να πέσουν θύματα οικονομικού εγκλήματος ενώ οι μικρότερες να πέσουν θύματα επαγγελματικής απάτης με παραποίηση επιταγών και λογιστική απάτη και υφίστανται αναλογικά μεγαλύτερη οικονομική ζημία[352].

Τα διευθυντικά στελέχη θυματοποιούν συνηθέστερα εταιρείες που δραστηριοποιούνται στους τομείς των υπηρεσιών μεταφορών, επικοινωνιών και εκδόσεων, τις πωλήσεις, τα τυχερά παιχνίδια, τον τουρισμό και τη ψυχαγωγία.

Στο πλαίσιο έρευνάς τους οι Krambia-Kapardis & Zopiatis, προσδιορίζουν τους τύπους της απάτης από εργαζόμενους, από διευθυντικά στελέχη και από τρίτους. Από πλευράς υπαλλήλων των επιχειρήσεων προτιμάται η κλοπή μετρητών χρημάτων με κυριότερους στόχους να αποτελούν οι οικονομικές ή ασφαλιστικές υπηρεσίες, οι εταιρείες ηλεκτρισμού, μεταφορών, επικοινωνιών, εκδόσεων, κτηματομεσιτικών υπηρεσιών και οικοδομών. Ο τύπος της απάτης που διαπράττουν τα διευθυντικά στελέχη αφορά κυρίως τη «σύγκρουση συμφερόντων» και «περιττές αγορές» με προτιμώμενους τομείς κατά σειρά τις μεταφορές, τις επικοινωνίες, τις εκδόσεις, τις πωλήσεις, τα τυχερά παιχνίδια, τον τουρισμό και τη ψυχαγωγία.[353]

Θύματα απάτης από τρίτους είναι συχνότερα οι βιομηχανίες, οι μεταφορές, οι επικοινωνίες, οι εκδόσεις και οι πωλήσεις με κυριότερη μορφή απάτης την έκδοση ακάλυπτης ή πλαστής επιταγής.[354]

3.4. Το κόστος του οικονομικού εγκλήματος

Ένα από τα κύρια χαρακτηριστικά του οικονομικού εγκλήματος και ειδικά αυτό του λευκού περιλαιμίου είναι το κόστος που επιφέρει στο κοινωνικό σύνολο που μπορεί να έχει τη μορφή

[351] Coleman James.W (1995), σσ. 360-381

[352] Σύμφωνα με Thomas & Gibson (2003), όπως αναφέρουν οι Κραμβία –Καπαρδή Μαρία, Τσολάκης Χρίστος (2011), σ. 44

[353] Όπως αναφέρουν οι Κραμβία –Καπαρδή Μαρία &Τσολάκης Χρίστος (2011), σ. 44. Οι συγγραφείς όμως δεν διευκρινίζουν τι ορίζεται ως «σύγκρουση συμφερόντων» και «περιττές αγορές». ΣτΣ, μπορούμε μόνο να υποθέσουμε ότι η «σύγκρουση συμφερόντων» μπορεί να αφορά περιπτώσεις αθέμιτης συμπεριφοράς από τα στελέχη μιας εταιρείας όταν π.χ συνδιαλέγονται με άλλη εταιρεία, ενώ «περιττές» θεωρούνται οι αγορές αγαθών ή υπηρεσιών από τα διευθυντικά στελέχη για ιδία χρήση, τα έξοδα όμως χρεώνονται στην εταιρεία.

[354] Κραμβία –Καπαρδή Μαρία &Τσολάκης Χρίστος (2011), σσ. 42-44

της οικονομικής, της φυσικής ζημιάς ή ακόμα και κοινωνικής ζημιάς όπως στο «ηθικό κλίμα», στις αξίες και τα πρότυπα της κοινωνίας.[355]

Ο Sutherland είχε επισημάνει ότι οι οικονομικές απώλειες από το έγκλημα του λευκού περιλαιμίου, αν και πολύ μεγάλες, είναι λιγότερο σημαντικές από τη ζημιά που προκαλείται στις κοινωνικές σχέσεις. Τα εγκλήματα του λευκού περιλαιμίου παραβιάζουν την εμπιστοσύνη και δημιουργούν χαλάρωση των κοινωνικών ηθών και κοινωνική αποδιοργάνωση μεγάλης κλίμακας, ενώ τα άλλα είδη εγκλημάτων έχουν μικρότερη επίδραση στους κοινωνικούς θεσμούς και την κοινωνική οργάνωση. [356]

1. Για το οικονομικό κόστος έχουν γίνει αρκετές μελέτες αν και οι εκτιμήσεις δεν μπορεί να είναι απόλυτα ακριβείς, λόγω: α) των διαφορετικών ορισμών για το τι συνιστά έγκλημα του λευκού περιλαιμίου και τι οικονομικό έγκλημα, β) του μεγάλου σκοτεινού αριθμού εγκληματικότητας που παρουσιάζει, γ) δεν υπάρχει μια ενιαία αποδεκτή μέθοδος υπολογισμού του κόστους ακόμα και για τις περιπτώσεις που καταγγέλλονται, επισημαίνονται και καταγράφονται στις στατιστικές της δικαιοσύνης.[357]

Το **οικονομικό κόστος** του εγκλήματος του λευκού περιλαιμίου συχνά είναι πολλαπλά μεγαλύτερο από τα κοινά εγκλήματα. Ενδεικτικά αναφέρει ο Sutherland ότι ένα μόνο στέλεχος σε αλυσίδα καταστημάτων καταχράστηκε μέσα σε ένα χρόνο 600.000 $, ποσόν το οποίο ήταν έξι φορές περισσότερο από τις ετήσιες απώλειες 500 διαρρήξεων και ληστειών που συνέβησαν στην εν λόγω αλυσίδα.[358]

Οι πιο συντηρητικές εκτιμήσεις, όπως αναφέρουν οι Meier και Short, τοποθέτησαν το κόστος του οικονομικού εγκλήματος στις ΗΠΑ για το 1974 στα 40 δις δολάρια ετησίως (US Chamber of Commerce), ενώ για το 1976 το ανέβασαν στα 44 δις δολάρια (Οικονομική Επιτροπή του αμερικανικού κογκρέσου). Άλλες μελέτες που ακολούθησαν ανεβάζουν το κόστος του οικονομικού εγκλήματος από 100 έως 200 δις δολάρια ετησίως και οι περισσότερες αναφέρουν ότι οι εκτιμήσεις τους είναι συντηρητικές και πως πιθανότατα το οικονομικό κόστος είναι ακόμα πιο υψηλό.[359]

Μεταγενέστεροι υπολογισμοί και συγκρίσεις, του Barkan (1997), τοποθετούν το ετήσιο κόστος του εγκλήματος του λευκού περιλαιμίου στα 415 δις δολάρια, 32 φορές μεγαλύτερο από κόστος του κοινού εγκλήματος που εκτιμήθηκε στα 13 δις δολάρια.

Υπολογισμοί των Helmkamp, Townsend και Sundra, του «Εθνικού κέντρου εγκλήματος του λευκού περιλαιμίου» για λογαριασμό του Υπουργείου Δικαιοσύνης των ΗΠΑ, εκτίμησαν το κόστος διάφορων ειδών οικονομικού εγκλήματος ανάμεσα σε 426 δις και 1,7 τρις δολάρια ετησίως (1996). Τα είδη αυτά αφορούν κλοπές από υπαλλήλους (5 έως 435 δις δολ.), κλοπή εμπορευμάτων (3,5 έως 10 δις), απάτες στον τομέα της υγείας (10 έως 100 δις), καταναλωτικές και προσωπικές απάτες (40 έως 100 δις), ασφαλιστικές (17 έως 100 δις) και φορολογικές απάτες επιχειρήσεων (7 έως 50 δις), απάτες υπολογιστών και άλλων εγκλημάτων υψηλής τεχνολογίας (100 εκ. έως 40 δις), απάτες με επιταγές (815 εκ. έως 10 δις) και πιστωτικές κάρτες (730 εκ. έως 3 δις), επιχειρηματικό και οργανωσιακό έγκλημα (200 έως 565 δις), ξέπλυμα μαύρου χρήματος (100 έως 215 δις), πλαστογραφία, τραπεζική απάτη

[355] Meier Robert F. & Short James F. Jr (1995), σ.σ.80-81
[356] Sutherland Edwin (1940), ό.π.
[357] Friedrichs David (2010), σ.49
[358] Όπως αναφέρουν οι Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013)
[359] Meier Robert F. & Short James F. Jr (1995), σ.σ.81-82

(καταθέσεων και δανείων 8,1 έως 25 δις), τηλεπικοινωνιακές απάτες (2 έως 9 δις), απάτες υποθηκών (30 δις) κλπ.[360]

Όπως αναφέρουν η Κραμβιά –Καπαρδή και Τσολάκης, η Ένωση Πιστοποιημένων Ελεγκτών κατά της Απάτης (ACFE) υπολόγισε το κόστος της επαγγελματικής απάτης στις ΗΠΑ για το 2008 σε 994 δις δολάρια ετησίως, ενώ για το 2010 το εκτίμησε σε ποσοστό 5% του ΑΕΠ κάθε χώρας. Έτσι το κόστος της επαγγελματικής απάτης σε παγκόσμιο επίπεδο υπολογίστηκε από την ACFE σε 2,9 τρις δολάρια.[361] Αντίστοιχα το ΑΕΠ της Ελλάδας κατά το 2009 ήταν 260 δις ευρώ με βάση το 5% το αντίστοιχο κόστος της απάτης στη χώρα μας υπολογίζεται σε 13 δις ευρώ.[362]

Για το Ηνωμένο Βασίλειο κατά το 2005, οι ζημιές από απάτη στις οικονομικές υπηρεσίας ήταν περίπου 1,478 δις ευρώ, σε άλλους τομείς 1,382 δις, σε βάρος ιδιωτών 2,75 δις, στο δημόσιο τομέα 9.522 δις ευρώ.[363]

Χαρακτηριστικότερη περίπτωση εταιρικής απάτης αποτελεί η απάτη «πυραμίδα» της Enron με κόστος 65 δις δολαρίων, ενώ η Enron κήρυξε χρεωκοπία στο ύψος του 1 τρις δολαρίων. Εκτός από τις οικονομικές, τεράστιες ήταν και οι απώλειες σε χιλιάδες θέσεις εργασίας[364] και οι παράπλευρες ζημιές, όπως οι απώλειες στο κλίμα επιχειρηματικής εμπιστοσύνης, στην αρνητική ανάπτυξη θέσεων εργασίας για τα προσεχή χρόνια.[365]

Σημαντικό επίσης είναι και το κόστος για τη λήψη μέτρων πρόληψης και καταπολέμησης (ποινικής δίωξης και καταδίκης) της απάτης που υπολογίστηκε από τους Levi και Barrows σε περίπου 13,9 δις λίρες στερλίνες ή 20,6 δις ευρώ.[366]

Σύμφωνα με την 6η Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα της PwC (PriceWaterhouseCoopers) στην Ελλάδα, το 50% των οργανισμών που έχουν πληγεί από οικονομικό έγκλημα σημείωσαν απώλειες από 100.000 έως 100 εκατομμύρια δολάρια. [367]

Πιο πρόσφατες εκτιμήσεις τοποθετούν το συνολικό ιδιωτικό και δημόσιο οικονομικό κόστος από τις απάτες στον τομέα υγείας υπολογίζεται σε πάνω από 170 δις δολάρια ετησίως, ενώ οι απώλειες που οφείλονται στην κλοπή ταυτότητας στα 48 δις.[368]

Σύμφωνα και με την Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα της PwC στην Ελλάδα εκτός του οικονομικού κόστους, καταγράφεται ότι οι οργανισμοί υφίστανται και σημαντικές παράπλευρες απώλειες από το οικονομικό έγκλημα, που αφορούν την εταιρική φήμη (31%), τις επιχειρησιακές σχέσεις των εργαζομένων 23% και το ηθικό του προσωπικού (25%).[369]

Φυσικά οι παραπάνω υπολογισμοί δεν περιλαμβάνουν όλες τις επιπτώσεις που μπορεί να επιφέρει το έγκλημα του λευκού περιλαιμίου στα θύματα και που ανεβάζουν το συνολικό οικονομικό κόστος. Οι επιπτώσεις αυτές μπορεί να αφορούν ηθική βλάβη, πόνο και απώλειες από την θυματοποίηση, υποβάθμιση της ποιότητας ζωής, έμμεσο οικονομικό κόστος όπως

[360] Helmkamp James C., Townsend Kitty J., & Sundra Jenny A. (2014)
[361] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.29
[362] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.30
[363] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.29
[364] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.27
[365] Friedrichs David (2010), σ.51
[366] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.30
[367] Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014, βλ. και Πίνακα 10.
[368] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), ό.π.,
[369] Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014, βλ. και Πίνακα 11.

υψηλότερη φορολογία, μεγαλύτερο κόστος αγαθών και υπηρεσιών (όπως στον τομέα των ασφαλειών) και υψηλότερο κόστος απονομής δικαιοσύνης. [370]

2. Οι φυσικές ζημίες που δεν περιλαμβάνονται στα παραπάνω οικονομικά κόστη διακρίνονται σε ζημιές που αφορούν:

α) τους εργαζόμενους των ίδιων των επιχειρήσεων, όπως οι παραβιάσεις των κανόνων ασφαλείας κατά την εργασία που έχουν αποτέλεσμα την προσβολή των εργαζομένων από μολύνσεις, έκθεση σε χημικά και άλλους κινδύνους που αργά ή γρήγορα επιφέρουν την αρρώστια ή και τον θάνατο.

β) τους καταναλωτές, όπως αρρώστιες και θανάτους πολιτών που προέρχονται, από ακατάλληλα φάρμακα, ρουχισμό, οχήματα, παιδικά παιχνίδια ή τροφές. [371]

Ακόμα δεν είναι λίγες οι περιπτώσεις θανάτων από ατυχήματα σε βιομηχανίες όπως η έκρηξη που έγινε σε πλατφόρμα άντλησης πετρελαίου στη Βόρειο θάλασσα με αποτέλεσμα το θάνατο 168 ατόμων ή τα πυρηνικά δυστυχήματα του Τσερνομπίλ και της Φουκουσίμα με ανυπολόγιστες συνέπειες.[372] Οι περιπτώσεις αυτές συχνά αναφέρονται ως «ατυχήματα» ή «καταστροφές» όμως τα περισσότερα από αυτά θα μπορούσαν να είχαν αποφευχθεί αν είχαν ληφθεί τα αναγκαία μέτρα.[373]

γ) την ευρύτερη κοινότητα, όπως η μόλυνση του περιβάλλοντος που προκαλεί καρκίνο ή άλλες αρρώστιες και ο θόρυβος. Μια μελέτη στις ΗΠΑ βρήκε ότι αποφεύχθηκαν 14000 θάνατοι για το 1978 ως απόρροια της εφαρμογής του νόμου για την ατμοσφαιρική ρύπανση (Clean Air Act 1970).[374]

Στις περιπτώσεις μόλυνσης του περιβάλλοντος ή ατυχημάτων στους χώρους εργασίας που περιγράφονται παραπάνω είναι δύσκολο να βρεθούν οι υπαίτιοι και να αποδοθούν οι αντίστοιχες ευθύνες γιατί δεν μπορεί εύκολα να αποδειχθεί: α) ο δόλος ή η αμέλεια που προκάλεσαν τη ζημιά, β) η αιτιώδης σύνδεση της ζημιάς στους εργαζόμενους ή τους πολίτες με τις συγκεκριμένες επιβαρυντικές συνθήκες στους χώρους εργασίας ή το περιβάλλον, γ) το χρονικό πλαίσιο που συνέβη η επιζήμια δράση.[375]

3. Οι ζημιές στο «ηθικό κλίμα» την εμπιστοσύνη και τις κοινωνικές αξίες προέρχονται από το γεγονός ότι οι εγκληματίες του λευκού περιλαιμίου αποτελούν «εξέχοντα μέλη της κοινωνίας, με υψηλή, αξιοσέβαστη κοινωνική θέση και πλούτο που η συμπεριφορά τους απαιτεί μεγαλύτερη κοινωνική υπευθυνότητα». Η παραβίαση της εμπιστοσύνης των κοινωνικών μελών, που αποτελεί στοιχειώδη παράγοντα της ομαλής κοινωνικής συμβίωσης, συνιστά μεγάλο κίνδυνο για την αξιοπιστία των κοινωνικών κανόνων και κλονίζει την εμπιστοσύνη μεταξύ του κοινού και των θεσμών, των δημόσιων λειτουργών, μεταξύ των πελατών και των επιχειρήσεων ή των επαγγελματιών, των υπαλλήλων και των επιχειρήσεων. Το έγκλημα του λευκού περιλαιμίου και το οικονομικό έγκλημα, παραβιάζοντας την εμπιστοσύνη και την πεποίθηση ότι όλοι πραγματώνουν το ρόλο τους, επιφέρει καταστροφικές συνέπειες για την κοινωνική συνοχή.[376]

[370] Helmkamp James C., Townsend Kitty J., & Sundra Jenny A. (2014)
[371] Meier Robert F. & Short James F. Jr (1995), σσ.82-83
[372] Κραμβιά –Καπαρδή Μαρία & Τσολάκης Χρίστος (2011), σ.33
[373] Friedrichs David (2010), σ.54
[374] Meier Robert F. & Short James F. Jr (1995), σσ.82-83
[375] Friedrichs David (2010) σ.54
[376] Meier Robert F. & Short James F. Jr. (1995), σσ. 84-85

Το οικονομικό έγκλημα του λευκού περιλαιμίου λοιπόν συνοδεύεται από οικονομικές και ηθικές συνέπειες μεγάλων διαστάσεων που κλονίζουν το οικονομικο-πολιτικό σύστημα. [377]

3.5. Οικονομικό έγκλημα σε επίπεδο κρατών και παγκοσμιοποίηση

Ο όρος παγκοσμιοποίηση αναφέρεται στην διάδοση ή μετακίνηση οικονομικών στοιχείων, αγαθών, ιδεών, ατόμων, ακόμα και ιών ανά τον κόσμο. Αφορά λοιπόν την απελευθέρωση όλων εκείνων των στοιχείων του υλικού και του πνευματικού πολιτισμού που μέχρι τώρα περιορίζονταν σε εθνικά πλαίσια και σύνορα. Το αποτέλεσμα είναι ο αυξανόμενος όγκος και η ποικιλία διεθνών συναλλαγών, η ελεύθερη ροή ανθρώπων και κεφαλαίου, η ταχύτατη διάχυση της τεχνολογίας και η συνακόλουθα αυξανόμενη αλληλεξάρτηση των χωρών παγκοσμίως μέσω του διεθνούς καταμερισμού εργασίας.

Σε σχέση με το οικονομικό έγκλημα και ειδικότερα με το έγκλημα του λευκού περιλαιμίου, έχει σημειωθεί ότι η παγκοσμιοποίηση δεν αποτελεί καμία πρόσφατη καινοτομία. Από τα παλαιότερα χρόνια έχουν παρατηρηθεί περιπτώσεις κλοπής οικονομικών (εμπορικών ή βιομηχανικών) μυστικών, όπως για παράδειγμα η κλοπή του μυστικού των Κινέζων για την εκτροφή του μεταξιού από τους Βυζαντινούς ή τη «διαρροή» των μυστικών της υφαντουργίας των βρετανών προς την Αμερικανική βιομηχανία.

Σήμερα, η διαφορά είναι ότι με την παγκοσμιοποίηση το οικονομικό έγκλημα έχει κι αυτό λάβει ευρύτατη έκταση και πολύ μεγαλύτερη ταχύτητα τέλεσης και διάδοσης. Μελετητές, όπως ο Neal Shover, σημειώνουν μάλιστα ότι αυτά τα τεράστια μεγέθη ευκαιριών που προσφέρει η παγκοσμιοποίηση στα οικονομικά εγκλήματα έχουν καταστήσει την καταπολέμηση τους, από τις διωκτικές αρχές των λιγότερο ισχυρών οικονομικά χωρών, πολύ δύσκολη υπόθεση.[378] Η δυνατότητα διαρκούς κινητικότητας των κεφαλαίων δίνει την ευκαιρία στους πιθανούς δράστες, όπως επιχειρήσεις με παράνομες δραστηριότητες, να απευθύνουν τις δραστηριότητες αυτές και το στόχο τους σε χώρες όπου λείπει το κατάλληλο νομικό πλαίσιο ή που εξασφαλίζουν αποποινικοποίηση ή έστω ατιμωρησία υπό την απειλή απόσυρσης των επενδύσεων και των κεφαλαίων τους σε άλλη χώρα.

Η κατάρρευση οικονομικών κολοσσών ως αποτέλεσμα δράσης οικονομικών εγκληματιών, συχνά γνωστοί και ως «οικονομικοί δολοφόνοι» μπορεί να επιφέρει επιπτώσεις σε παγκόσμιο επίπεδο. Κλονίζουν την επιχειρηματική πίστη, την ψυχολογία των διεθνών επενδυτών, την εμπιστοσύνη στις αγορές παγκοσμίως και απαιτούν τις κυβερνήσεις τη διάθεση τεράστιων χρηματικών ποσών για την αναχρηματοδότηση τραπεζών και χρηματοπιστωτικών ιδρυμάτων προκειμένου να αποσοβηθούν οι κίνδυνοι της διάχυσης των επιπτώσεων της κρίσης σε όλους τους τομείς της οικονομίας και της κοινωνίας (παραγωγή, απασχόληση, εισόδημα, ζήτηση).

Οι παγκόσμιες επιπτώσεις τέτοιας κλίμακας εγκληματικών δραστηριοτήτων μπορεί να αποδειχθούν ανυπολόγιστες.

Οι πιο οικονομικά εύρωστες και πολιτικά ισχυρές χώρες μπορούν να αντιμετωπίζουν και να αντιπαρέρχονται αποτελεσματικότερα τις επιπτώσεις των οικονομικών εγκλημάτων ως θύματα και να συνεχίζουν να προσελκύουν διεθνείς επενδύσεις. Αντίθετα οι οικονομίες μικρότερων χωρών, όπως η Ελλάδα, είναι πολύ πιο ευάλωτες σε οικονομικές επιθέσεις και ανάλογους εκβιασμούς και υπόκεινται σε ανυπολόγιστες και μη αντιμετωπίσιμες συνέπειες.[379]

[377] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), ό.π.
[378] Grabosky Peter. (2009), σσ.129-171
[379] Grabosky Peter. (2009), σσ.129-171

Χαρακτηριστικό το παράδειγμα της Γκόλντμαν Σακς (Goldman Sachs), μιας από τις μεγαλύτερες τράπεζες και μεγαλύτερο οικονομικό παράγοντα των ΗΠΑ που δραστηριοποιούνται παγκοσμίως σε πλήθος χρηματοοικονομικών υπηρεσιών με πελάτες εταιρείες και κυβερνήσεις, θεωρείται από αναλυτές υπεύθυνη για την τρέχουσα οικονομική κατάσταση, όχι μόνο στις ΗΠΑ, αλλά και παγκοσμίως και σε άλλες χώρες, όπως είναι η Ελλάδα.[380]

[380] Dunbar Nicholas, Martinuzzi Elisa (2012)

ΚΕΦΑΛΑΙΟ 4. Η ΜΕΛΕΤΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

4.1. Η έννοια του ηλεκτρονικού εγκλήματος

Το «έγκλημα υπολογιστών» μπορεί ευρύτερα να οριστεί ως «η εγκληματική δραστηριότητα στην οποία εμπλέκεται μια υποδομή τεχνολογίας πληροφοριών».

Γενικά ως έγκλημα υπολογιστών ή πληροφορικό έγκλημα (Computer crime), κυβερνοέγκλημα (cybercrime), ηλεκτρονικό έγκλημα (e-crime), έγκλημα υψηλής τεχνολογίας (hi-tech crime), εννοούμε την εγκληματική δραστηριότητα κατά την οποία ένας υπολογιστής ή ένα δίκτυο είναι η πηγή, το εργαλείο, ο στόχος, ή το περιβάλλον ενός εγκλήματος.[381]

Εκτός από το πρόβλημα στον ορισμό του πληροφορικού εγκλήματος, του κυβερνο-εγκλήματος και του εγκλήματος υψηλής τεχνολογίας, ο κοινός παρονομαστής είναι η χρήση της τεχνολογίας για να πραγματοποιηθούν οι εγκληματικές δραστηριότητες. Η τεχνολογία περιλαμβάνει όχι μόνο τις συσκευές αλλά και τις υπηρεσίες που προσφέρονται από τους προμηθευτές της. Οι υπολογιστές μπορούν να είναι όχι μόνο ο στόχος αλλά και τα μέσα για να διαπραχτούν τα εγκλήματα. Σήμερα ο κύριος στόχος στα εγκλήματα υψηλής τεχνολογίας είναι η παραβίαση της ιδιωτικότητας και η κλοπή στοιχείων που μπορούν να γίνουν με διάφορους τρόπους. Η μη εξουσιοδοτημένη πρόσβαση (hacking), το σπάσιμο κωδικών πρόσβασης, η παραβίαση πνευματικών δικαιωμάτων, η κλοπή ταυτότητας, η διάδοση των κακόβουλων κωδίκων και οι εικόνες παιδικής πορνογραφίας είναι ακριβώς μερικά παραδείγματα των τρόπων με τους οποίους οι εγκληματίες μπορούν να εκμεταλλευτούν τη χρησιμοποίηση της τεχνολογίας. Η χρήση του διαδικτύου είναι το κύριο μέσο στη διευκόλυνση αυτής της εγκληματικής διαδικασίας.

Αν και οι όροι «έγκλημα υπολογιστών» ή «κυβερνο-έγκλημα» περιορίζονται στην περιγραφή της εγκληματικής δραστηριότητας στην οποία ο υπολογιστής ή το δίκτυο είναι ένα απαραίτητο μέρος του εγκλήματος, αυτοί οι όροι μερικές φορές χρησιμοποιούνται για να συμπεριλάβουν επίσης παραδοσιακά εγκλήματα, όπως η απάτη, η κλοπή, ο εκβιασμός, η παραποίηση και η κατάχρηση, όπου οι υπολογιστές ή τα δίκτυα χρησιμοποιούνται για να διευκολύνουν την παράνομη δραστηριότητα.

Παρά το γεγονός ότι πολλά από τα εγκλήματα που διαπράττονται με τη χρήση υπολογιστή δεν είναι καινοφανή, ως προς τη μορφή τους (απάτη, κατάχρηση κλπ.), είναι καινοφανή και μοναδικά όλα τα υπόλοιπα χαρακτηριστικά τους, όπως ο τόπος όπου βρίσκεται η βάση των δραστών (οι επιθέσεις μπορούν να εξαπολύονται από μακριά), το περιβάλλον της δράσης, το αντικείμενο των επιθέσεων (κλοπή δεδομένων ή προγραμμάτων), οι χρησιμοποιούμενοι μέθοδοι και το είδος των χρηματικών κεφαλαίων.

Ο ειδικός σε θέματα ασφάλειας υπολογιστών Parker από την αρχή διαπίστωσε τη δυσκολία ορισμού για το έγκλημα υπολογιστών. Στην πρώτη έκθεσή της, η ομάδα εργασίας που συνέστησε για τη «κατάχρηση υπολογιστών», όρισε ότι:

> «κατάχρηση ή κακή χρήση υπολογιστών συνιστούν όλοι οι τύποι πράξεων που συνδέονται άμεσα με υπολογιστές ή τη μεταφορά στοιχείων τους, κατά τις οποίες τα θύματα αθέλητα υφίστανται ή θα μπορούσαν να έχουν υποστεί απώλειες, τραυματισμούς, ζημία, ή οι δράστες ηθελημένα λαμβάνουν ή θα μπορούσαν να έχουν λάβει κέρδος».[382]

[381] http://en.wikipedia.org/wiki/Computer_crime

[382] Parker Donn, (2007), ό.π.

Όπως δέχεται και ο ίδιος ο Parker, ο ορισμός που έδωσε περιλαμβάνει ένα ευρύ φάσμα περιστατικών. Η κακή χρήση υπολογιστών περιλαμβάνει έγκλημα «λευκού περιλαιμίου», βανδαλισμό, κακόβουλες ενέργειες. Μια κατηγορία πράξεων που αφορούν κακή χρήση υπολογιστών, μπορεί να εμπίπτουν στο καθαρά ποινικό φάσμα, όπου ο θύτης συλλαμβάνεται, δικάζεται, καταδικάζεται για ένα συγκεκριμένο ποινικό αδίκημα. Μια άλλη κατηγορία που συνεπάγεται αστικές ποινές ή εξωδικαστικό συμβιβασμό και τέλος μια κατηγορία πράξεων των οποίων οι δράστες τιμωρούνται με διοικητικά από την επιχείρηση μέτρα, π.χ. με απόλυση.

Στη συνέχεια, σημειώνει όμως, ο στόχος της ομάδας του την εποχή εκείνη, ήταν να ορίσει την κατάχρηση και την κακή χρήση υπολογιστών (computer abuse) ώστε να περιλάβει ευρύτερα οποιοδήποτε είδος γεγονότος συνδέεται με την επικοινωνία δεδομένων και υπολογιστών και στοιχείων ή όπου ο δράστης είχε αποκτήσει και χρησιμοποιήσει κάποια ειδική γνώση σχετική με υπολογιστές. Περιλάμβανε οποιοδήποτε γεγονός που θα οδηγούσε σε κάποια χρήσιμη γνώση για τη βελτίωση της ασφάλειας πληροφοριών. Με τον ευρύ ορισμό απέφευγε την ανάλωση σε συζητήσεις για το εάν ένα γεγονός συνιστά ή όχι έγκλημα υπολογιστή[383]. Άλλωστε γενικότερα η έννοια του «εγκλήματος» είναι από τις πιο αμφιλεγόμενες ως προς τον ορισμό της από τους εγκληματολόγους και τους φορείς του κοινωνικού ελέγχου. Όπως και η έννοια του «εγκλήματος του λευκού περιλαιμίου» έχει γνωρίσει πολλούς διαφορετικούς ορισμούς και κριτική από τότε που πρωτο-χρησιμοποιήθηκε από τον Sutherland, όπως είδαμε σε άλλο σημείο.

Η κακή χρήση υπολογιστών (computer abuse) αποτελεί, κατά τον Parker, ένα πολυπρόσωπο πρόβλημα που φαίνεται διαφορετικό από διαφορετικές οπτικές γωνιές, όπως αυτές των δραστών, των θυμάτων, των διωκτικών αρχών, των ειδικών στους υπολογιστές, τους εγκληματολόγους και τους άλλους επιστήμονες που ασχολούνται με το θέμα.

Η έκθεση του Parker, προς το SRI, συνάντησε από την αρχή πολλές αντιδράσεις από κατασκευαστές και γραφεία υπηρεσιών υπολογιστών, από επιχειρήσεις και άλλους που δεν επιθυμούσαν τη γνωστοποίηση της «σκοτεινής» πλευράς των υπολογιστών αλλά να ελαχιστοποιήσουν τη σημασία και τον αντίκτυπο της κατάχρησης και της κακής χρήσης υπολογιστών. Αυτοί υποστήριξαν ότι η κατάχρηση υπολογιστών απαιτεί ότι η πράξη δεν θα μπορούσε να γίνει χωρίς τη χρήση υπολογιστή. Ένας τέτοιος ορισμός, όμως εκείνη την εποχή (αρχές ΄70) θα είχε περιορίσει την κατάχρηση και την κακή χρήση υπολογιστών τότε σε πολύ λίγες περιπτώσεις.

Παρά την εννοιολογική σύγχυση που συνεπάγεται η χρήση των όρων «έγκλημα» υπολογιστών και «κακή χρήση» υπολογιστών ως περίπου συνώνυμες, η αποφυγή ιδιαίτερων αναλύσεων και εξειδικεύσεων, που αποτελούν αδυναμίες του ορισμού του εγκλήματος υπολογιστών από τον Parker, η μελέτη του αυτή συνιστά την πρώτη συστηματικά οργανωμένη και συνειδητή προσπάθεια προσέγγισης του νέου φαινομένου. Αποτέλεσε σημείο σταθμό που σηματοδοτεί όχι μόνο την έναρξη του διαλόγου πάνω στο πρόβλημα αλλά και την δημιουργία των πρώτων νομοθετημάτων στην οποία και ο ίδιος ο Parker συμμετείχε ενεργά.

Ο August Bequai όρισε το σχετικό με υπολογιστές έγκλημα ως:

[383] Parker Donn (2007), ό.π.

> «τη χρήση υπολογιστή για τη διάπραξη ενεργειών απάτης, απόκρυψης και πανουργίας που έχουν ως αντικειμενικό τους σκοπό την απόκτηση ιδιοκτησίας, χρήματος, υπηρεσιών και πολιτικού και επιχειρηματικού πλεονεκτήματος».[384]

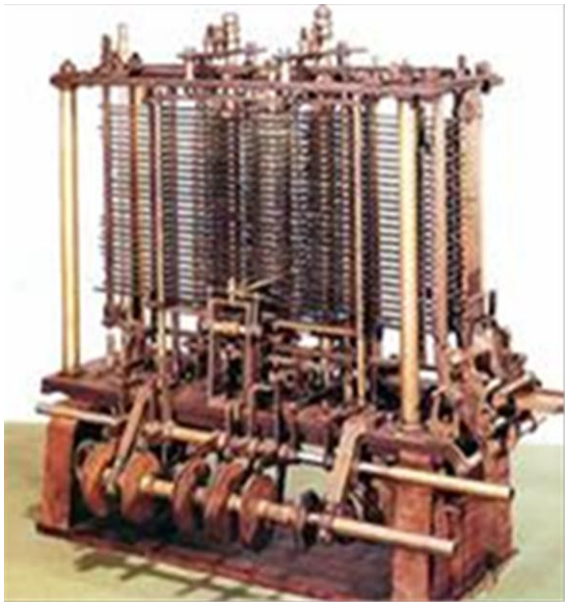
Παρατηρούμε ότι ο ορισμός του Bequai έχει σαφώς πιο περιορισμένο πεδίο εφαρμογής σε σχέση με αυτόν του Parker και είναι εμφανώς επηρεασμένος από την ενασχόληση του Bequai με το έγκλημα του Λευκού περιλαιμίου επειδή είναι σαφείς οι διαφαινόμενοι συσχετισμοί των χαρακτηριστικών του ηλεκτρονικού με αυτά του οικονομικού εγκλήματος, όπως η αναφορά στην απάτη και στο σκοπό του οικονομικού οφέλους ή πλεονεκτήματος.

Το 1801 το κίνητρο του κέρδους παρότρυνε τον Jacquard Joseph, έναν ιδιοκτήτη υφαντουργίας στη Γαλλία, να σχεδιάσει τον πρόδρομο της κάρτας υπολογιστών. Ήταν η πρώτη μηχανή που χρησιμοποιούσε διάτρητες κάρτες για τον έλεγχο μιας σειράς ακολουθιών που επέτρεπαν την επανάληψη μιας σειράς όμοιων βημάτων στην ύφανση ειδικών υφασμάτων. Αρκούσε η αλλαγή μιας διάτρητης κάρτας για να αλλάξει το μοτίβο που έπλεκε το μηχάνημα. Ήταν το πρώτο βήμα για την ανάπτυξη του προγραμματισμού ηλεκτρονικών υπολογιστών.

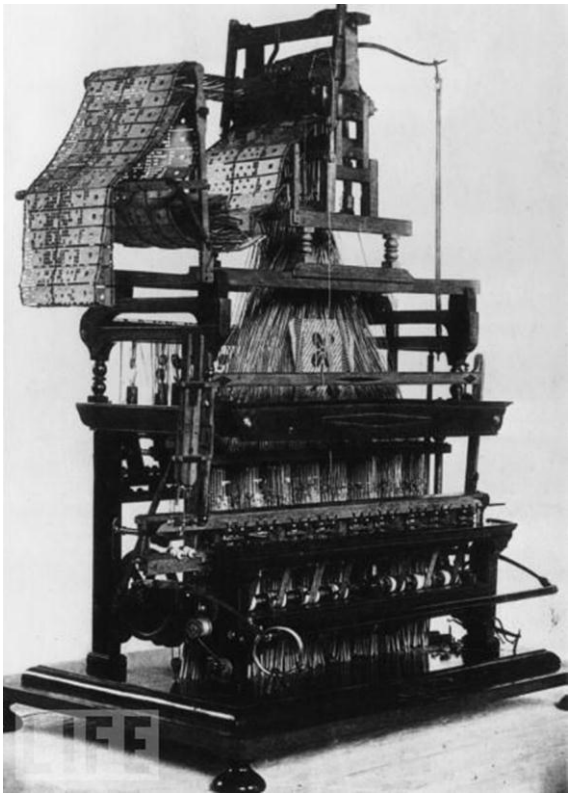
Οι υπάλληλοι του Jacquard, θορυβημένοι από την απειλή στην παραδοσιακή απασχόλησή τους και την ενδεχόμενη απώλεια του εισοδήματος τους, διενεργούσαν συχνά δολιοφθορές στο μηχάνημα και ήταν αποφασισμένοι να αποθαρρύνουν τον Jacquard από την περαιτέρω χρήση της νέας τεχνολογίας. Το πρώτο, ίσως, έγκλημα υπολογιστών είχε διαπραχθεί. [385]

[384] Βλ. Λάζος Γρηγόρης (2001), σ.42
[385] Mac Millan (2014)

Ο ΑΡΓΑΛΕΙΟΣ ΤΟΥ JOSEPH-MARIE JACQUARD [386]



ΕΙΚΟΝΑ 1



ΕΙΚΟΝΑ 2

[386] http://www.e-crime.gr/crime.htm και http://www.thanko.eu/?p=1735, Νοέμβριος 2014

Σήμερα, το ηλεκτρονικό έγκλημα περιλαμβάνει, από τη μια παραδοσιακές μορφές παραβατικής δραστηριότητας, όπως κλοπή, απάτη, πλαστογραφία, εκβιασμό κλπ., τα οποία υπόκεινται γενικά στις πράξεις που προβλέπει ο ποινικός κώδικας, αλλά και από την άλλη μια σειρά κακών χρήσεων και καταχρήσεων του υπολογιστή, οι οποίες θα μπορούσαν να χαρακτηριστούν εγκληματικές. Γι αυτό και ορισμένες από αυτές ποινικοποιήθηκαν.

Έχει γίνει πολλή συζήτηση μεταξύ των εμπειρογνωμόνων για το τι ακριβώς αποτελεί έγκλημα υπολογιστών ή σχετικό με υπολογιστή έγκλημα. Ακόμα και μετά από αρκετά έτη, δεν υπάρχει κανένας διεθνώς αναγνωρισμένος ορισμός αυτών των εννοιών.

Ο ορισμός που διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΟΣΑ, που συνεστήθη για να εξετάσει το θέμα της ηλεκτρονικής εγκληματικότητας θεωρεί ως:

> «ηλεκτρονικό έγκλημα μια πράξη που διαπράττεται με ηλεκτρονικό υπολογιστή και μπορεί να χαρακτηρισθεί παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων».[387]

Το 1989, η Ευρωπαϊκή Επιτροπή του Συμβουλίου της Ευρώπης για το πρόβλημα της εγκληματικότητας, ακολουθώντας μια προσπάθεια του ΟΟΣΑ[388] (OECD), εξέδωσε μια σειρά οδηγιών προς τους εθνικούς νομοθέτες, που απαρίθμησε τις δραστηριότητες οι οποίες θα έπρεπε να γίνουν αντικείμενο ποινικής αντιμετώπισης. Κατά την συζήτηση των λειτουργικών χαρακτηριστικών των επιδιωκόμενων στόχων, η Επιτροπή δεν επιχείρησε να δώσει έναν επίσημο ορισμό για το πληροφορικό έγκλημα (computer crime) και άφησε το εγχείρημα υιοθέτησης λειτουργικών ορισμών και κατηγοριοποιήσεων στην ευχέρεια των επιμέρους κρατών, ανάλογα με το εθνικό σύστημα δικαιοσύνης και τις παραδόσεις τους.

Γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο δεν υπάρχει ακόμα, όχι μόνο μεταξύ των επιστημόνων αλλά και στη διεθνή νομοθεσία και νομολογία. Ένας κοινός ορισμός των ηλεκτρονικών εγκλημάτων υπολογιστών που θα καθορίσει τι είναι κυβερνο-έγκλημα, τι έγκλημα υπολογιστών και τι έγκλημα υψηλής τεχνολογίας, παρά προσπάθεια που καταβάλλεται από νομοθέτες, ερευνητές, και το προσωπικό των φορέων του τυπικού ελέγχου, είναι ακόμα δύσκολο να διατυπωθεί. Αυτό οφείλεται σε διάφορους λόγους όπως η διαφορετική εσωτερική νομοθεσία που ισχύει στα κράτη μέλη της Ε.Ε. με αποτέλεσμα διαφορετικές προσεγγίσεις.

Αν και η Ευρωπαϊκή Σύμβαση για το κυβερνο-έγκλημα υπογράφηκε το 2001, έχει επικυρωθεί στην πράξη από μερικές μόνο χώρες και επομένως αυτή δεν μπορεί να θεωρηθεί ένα νομικό καθολικό σημείο αναφοράς ακόμα.

Σύμφωνα με την Europol «έγκλημα υψηλής τεχνολογίας» συνιστά η χρήση της τεχνολογίας πληροφοριών και τηλεπικοινωνιών για τη διάπραξη ή τη διεύρυνση μιας εγκληματικής πράξης, ενάντια σε ένα πρόσωπο, την ιδιοκτησία, την οργάνωση ή το συγκρότημα δικτύων ηλεκτρονικών υπολογιστών.

Για τον Fausto Pokar «το κυβερνο-έγκλημα (και οι υποκατηγορίες του) είναι η εγκληματική χρήση οποιουδήποτε δικτύου ή συστήματος υπολογιστών στο διαδίκτυο, επιθέσεις ή κατάχρηση ενάντια στα συστήματα και τα δίκτυα για εγκληματικούς λόγους, που

[387] Μυλωνόπουλος Χρήστος (2000), σ.14

[388] Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

χρησιμοποιούν τη νέα τεχνολογία ή νέα εγκλήματα που έχουν αναπτυχθεί με τη διάδοση του Διαδικτύου»[389].

Η Αυστραλιανή κυβέρνηση ορίζει ότι «ηλεκτρονικό έγκλημα (e-crime) είναι η διάπραξη αδικήματος με εμπλοκή ηλεκτρονικού υπολογιστή ή άλλων ηλεκτρονικών συσκευών επικοινωνίας που χρησιμοποιείται ως στόχος του αδικήματος ή λειτουργεί ως συσκευή αποθήκευσης σε ένα αδίκημα»[390].

Για τους παραπάνω ορισμούς θα μπορούσαμε να παρατηρήσουμε, ότι οι όροι «έγκλημα υπολογιστών», «πληροφορικό έγκλημα», «ηλεκτρονικό έγκλημα» και «σχετικό με υπολογιστή έγκλημα» συχνά χρησιμοποιούνται εναλλακτικά. Δεν υπάρχει πάντως, πλέον αμφισβήτηση, μεταξύ των μελετητών και των εμπειρογνωμόνων που έχουν προσπαθήσει να διατυπώσουν ορισμούς του εγκλήματος υπολογιστών, ότι το φαινόμενο υπάρχει. Εντούτοις, οι ορισμοί που έχουν παραχθεί τείνουν να αφορούν τη μελέτη για την οποία γράφτηκαν. Η πρόθεση των συντακτών να είναι ακριβείς με το πεδίο μελέτης τους και η χρήση ιδιαίτερων ορισμών, δημιουργεί συχνά ανακρίβειες όταν επιχειρηθεί η χρήση αυτών των ορισμών έξω από το προοριζόμενο πλαίσιό τους. Ένας καθολικός και παγκόσμια αποδεκτός ορισμός του εγκλήματος υπολογιστών δεν έχει επιτευχθεί, ενώ οι λειτουργικοί ορισμοί αποτελούν μάλλον τον κανόνα. Πολλοί από αυτούς λειτουργούν συμπληρωματικά, ενώ κάποιοι άλλοι διαζευκτικά, αναιρώντας ο ένας την επιστημονική σαφήνεια του άλλου.

Οι νομικοί ορισμοί, από πλευράς τους, απαιτούν μεγαλύτερη σαφήνεια και λεπτομέρεια, επειδή πρέπει να αποτελούν το ασφαλές πλαίσιο με το οποίο καθορίζονται οι συμπεριφορές που επιτρέπονται και αυτές που απαγορεύονται όπως και οι ποινές που επιβάλλονται στους παραβάτες. Για παράδειγμα όροι του τύπου «κακοχρησία υπολογιστών» και «κατάχρηση υπολογιστών» χρησιμοποιούνται συχνά, αλλά έχουν σημαντικά διαφορετικές επιπτώσεις. Το ποινικό δίκαιο αναγνωρίζει τις έννοιες της παράνομης πρόθεσης ή της πρόθεσης εξαπάτησης και της αξίωσης του δικαιώματος. Έτσι οποιοδήποτε ποινικό δίκαιο αφορά το έγκλημα υπολογιστών θα πρέπει να διακρίνει μεταξύ της τυχαίας κακής χρήσης ενός συστήματος ηλεκτρονικών υπολογιστών, της κακής χρήσης ηλεκτρονικών υπολογιστών από αμέλεια και της ηθελημένης, αναρμόδιας πρόσβασης ή της κακής χρήσης υπολογιστών, που ανέρχεται σε κατάχρηση υπολογιστών. Σύμφωνα με το νόμο η απλά ενοχλητική συμπεριφορά πρέπει να διακρίνεται με σαφήνεια από την εγκληματική συμπεριφορά.

Διάκριση ηλεκτρονικού – πληροφορικού εγκλήματος

Κατά τη γνώμη μας θα έπρεπε να γίνει ακόμα μια εννοιολογική διάκριση, αυτή μεταξύ ηλεκτρονικού και πληροφορικού εγκλήματος, παρά το γεγονός ότι κατά τη χρήση τους οι δυο έννοιες συνήθως ταυτίζονται. Αυτό θεωρείται απαραίτητο επειδή υπάρχει μια κατηγορία εγκλημάτων που τελούνται μεν με ηλεκτρονικά ή ψηφιακά μέσα αλλά τα μέσα αυτά δεν περιλαμβάνουν απαραίτητα τη χρήση του ηλεκτρονικό υπολογιστή. Μπορεί δηλαδή για την τέλεση μιας απάτης ή την πραγματοποίηση συναλλαγής με κλεμμένη πιστωτική κάρτα να χρησιμοποιείται το τηλέφωνο ή το φαξ, χωρίς ο ηλεκτρονικός υπολογιστής να αποτελεί το μέσο ή το στόχο του εγκλήματος.

Έτσι ως ηλεκτρονικό έγκλημα γενικότερα θα πρέπει να θεωρείται το έγκλημα που έχει ως στόχο ή που τελείται με τη χρήση σύγχρονης ηλεκτρονικής τεχνολογίας και ψηφιακών μέσων

[389] Pocar Fausto (2003)

[390] Australian Government (2004)

και τηλεπικοινωνιών. Από την άλλη πλευρά για πληροφορικό έγκλημα θα πρέπει να μιλάμε αποκλειστικά όταν ο ηλεκτρονικός υπολογιστής είναι το μέσο για την τέλεση ή ο στόχος του εγκλήματος. Υπό την έννοια αυτή το πληροφορικό είναι μέρος του ηλεκτρονικού εγκλήματος. Για χρηστικούς λόγους και λόγους αποφυγής συγχύσεως, στο πλαίσιο της παρούσας εργασίας θα χρησιμοποιήσουμε πάντως τις δυο έννοιες ως ταυτόσημες.

4.2. Η εξέλιξη της μελέτης του ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό έγκλημα ως έννοια και αντικείμενο άρχισε να απασχολεί τους μελετητές ουσιαστικά από τη δεκαετία του ’70.

Μέχρι τα μέσα του ’80 η έκταση των ηλεκτρονικών παραβάσεων ήταν τέτοια που δεν επέτρεπε την αυτοτελή αντιμετώπισή του ως ξεχωριστό αντικείμενο αλλά εξεταζόταν στο πλαίσιο του οικονομικού εγκλήματος. Από τότε και μετά η ευρύτερη διάδοση της πληροφορικής τεχνολογίας, με τη συνακόλουθη εξάπλωση των αδικημάτων που τελούνται με στόχο ή μέσω αυτής, συνετέλεσε στη σχετική αυτονόμηση του ηλεκτρονικού εγκλήματος ως ιδιαίτερο αντικείμενο μελέτης καινοφανών επιστημονικών κλάδων, όπως αυτών της πληροφορικής εγκληματολογίας ή της κυβερνο-εγκληματολογίας (cyber criminology): “Η μελέτη των παραγόντων της εγκληματικότητας του κυβερνοχώρου και των συνεπειών του στον φυσικό χώρο”[391]. Ως τέτοιο, αυτόνομο αντικείμενο, διαθέτει πλέον ορολογία και εννοιολογήσεις, δράστες με ιδιαίτερα, διακριτά χαρακτηριστικά, σε σχέση με το κοινό αλλά και το απλό οικονομικό έγκλημα, οι οποίοι αντιμετωπίζονται δικαιακά στο πλαίσιο ειδικότερων νομοθετημάτων. Σημείο αναφοράς τέτοιων νομοθετημάτων αποτελούν οι ομοσπονδιακοί νόμοι των ΗΠΑ, όπως αυτός του 1986 για την απάτη και προσβολή υπολογιστών που προέβλεπε τρία κακουργήματα και αντίστοιχα πλημμελήματα.

Οι ευρύτατες και ταχύτατες αλλαγές στην τεχνολογία δεν αφήνουν ανεπηρέαστες τις οικονομικές, ούτε τις κοινωνικές σχέσεις καθιστώντας και τη μελέτη του ηλεκτρονικού εγκλήματος ένα ασταθές και δυναμικό, διαρκώς μεταβαλλόμενο πεδίο με συνεχείς ανατροπές των δεδομένων, ανακατευθύνσεις και αναθεωρήσεις.[392]

4.2.1. Οι Πρωτοπόροι της μελέτης του ηλεκτρονικού εγκλήματος

Οι πρώτοι διανοητές του ηλεκτρονικού εγκλήματος έπρεπε να εστιάσουν σε τρεις κατευθύνσεις όσον αφορά την μελέτη του αντικειμένου. Αρχικά είχαν να πείσουν τους υπόλοιπους διανοητές για το αυτοτελές του αντικειμένου, προσπάθεια που είχε πεδίο δράσης έως τη δεκαετία του ’80. Ο επόμενος στόχος ήταν η δημιουργία ενός συνόλου εννοιών και κατηγοριοποιήσεων που να προσδιορίζει με σχετική ευστοχία τα όρια ενός διαρκώς μεταβαλλόμενου αντικειμένου. Η τρίτη κατεύθυνση προσπαθειών είχε να κάνει με την εξεύρεση ικανοποιητικών μέσων αντιμετώπισης, ποινικών και μη, του ηλεκτρονικού εγκλήματος.

Πρωτοπόρος στη μελέτη του «σχετικού με υπολογιστές» εγκλήματος είναι ο Donn Parker, μαθηματικός με ειδίκευση στον προγραμματισμό και τη μηχανική των υπολογιστικών εφαρμογών. Ο Parker άρχισε να ασχολείται με έγκλημα υπολογιστών από το 1964 όταν και εργαζόταν ως υπεύθυνος πληροφοριακών υπηρεσιών όπου και αναγκάστηκε να απολύσει έναν υπάλληλο – προγραμματιστή- για κλοπή πληροφοριακών υπηρεσιών.

[391] βλ. http://www.cybercrimejournal.com, Απρίλιος 2015

[392] Λάζος Γρηγόρης (2001), σσ. 25-28

Την ίδια εποχή τα μέσα ενημέρωσης είχαν αρχίσει να μεταδίδουν ειδήσεις για περιπτώσεις χειριστών ή προγραμματιστών ηλεκτρονικών υπολογιστών που συνελήφθησαν για απάτη, κλοπή, δολιοφθορά ή κατασκοπεία.

Η χρονική συγκυρία της αποκάλυψης των αδικημάτων αυτών δεν ήταν άσχετη με την ανακάλυψη και ευρύτατη διάδοση του mainframe υπολογιστή σε επιχειρήσεις και εκπαιδευτικούς οργανισμούς από τις αρχές του ’60. Από τότε ξεκίνησε μια νέα προσπάθεια για την ανάπτυξη καλύτερης ασφάλειας, για τη νομοθέτηση νέων νόμων, τη βοήθεια των πιθανών θυμάτων και την ενημέρωση της κοινωνίας για τη σκοτεινή πλευρά μιας ισχυρής νέας τεχνολογίας πληροφοριών.

Στη προσπάθεια του ο Parker βοηθήθηκε από τη Susan Nycum, δικηγόρο και διευθύντρια συστημάτων ηλεκτρονικών υπολογιστών στο πανεπιστήμιο του Στάνφορντ, με την οποία πρωτοστάτησε για την ανάπτυξη νομοθετικού πλαισίου για τους υπολογιστές κατά τις δεκαετίες του '70 και του '80.

Ο Parker ξεκίνησε επίσημα, με την μελέτη του εγκλήματος υπολογιστών, το 1970 όταν προσχώρησε στο ερευνητικό ίδρυμα του Στάνφορντ (SRI) ως προϊστάμενος του τμήματος πληροφοριών και ως σύμβουλος και ερευνητής. Από το 1970, έχει πάρει συνεντεύξεις από περισσότερους από 200 εγκληματίες υπολογιστών και έχει καταγραμμένες χιλιάδες υποθέσεις κακής χρήσης υπολογιστών, απάτης κλπ. Η εργασία αυτή χρησιμοποιήθηκε για την ανάπτυξη του πρώτου κώδικα επαγγελματικής συμπεριφοράς για την Ένωση υπολογιστικών μηχανημάτων (ACM). Συνέχισε την έρευνα και μετά από την συνταξιοδότηση του το 1997.[393]

Η έρευνα του Parker αρχικά οδήγησε στη σύνταξη της έκθεσης του 1971 η οποία προσδιόριζε τις απειλές που αφορούσαν την κακή χρήση υπολογιστών. Συνέστησε τη δημιουργία ειδικών μέτρων ασφάλειας, τη λήψη αντιγράφων από ευαίσθητα δεδομένα και πληροφορίες και τη δημιουργία φυσικών εμποδίων που να αποτρέπουν την αναρμόδια είσοδο σε κέντρα υπολογιστών. Η μελέτη έλαβε πολυεπιστημονική διάσταση με τη προσθήκη επιστημόνων από διάφορους κλάδους για να βοηθήσουν στην εξέταση του εγκλήματος υπολογιστών από διαφορετικές προοπτικές, τεχνικές, νομικές και κοινωνιολογικές. Αποτέλεσε την πρώτη προσπάθεια να τεκμηριωθεί και να καθοριστεί το πρόβλημα με βάση την πραγματική εμπειρία. Ο σκοπός της έκθεσης ήταν να προειδοποιηθούν, τόσο οι χρήστες υπολογιστών σε ιδιωτικές επιχειρήσεις και δημόσιους οργανισμούς, όσο και οι τεχνολογικές, οι νομικές και οι κοινωνιολογικές ερευνητικές κοινότητες για τη σοβαρότητα της φύσης, του βαθμού και των προοπτικών της κατάχρησης υπολογιστών ως αυξανόμενο κοινωνικό πρόβλημα.

Ένα από τα πρώτα και σημαντικότερα ζητήματα που ο Parker κλήθηκε να αντιμετωπίσει ήταν αυτό της διατύπωσης ορισμών για τα νέα είδη εγκλήματος. Στις δεκαετίες του ’50 και του ΄60 υπήρχαν μεγάλες διαφωνίες και αμφισβητήσεις μεταξύ των ειδικών ηλεκτρονικών υπολογιστών για τη φύση και τον ορισμό του προβλήματος. Το πρόβλημα ήταν καινοφανές για την πληροφορική τεχνολογία, όχι όμως και για την τεχνολογία τηλεπικοινωνιών όπου, ήδη από τα τέλη του ’50 ήταν γνωστές επιθέσεις από κλέφτες σε δίκτυα υπεραστικών τηλεπικοινωνιών.

[393] Parker Donn (2007)

4.2.2. Οι επίγονοι στη μελέτη του εγκλήματος υπολογιστών

Το έργο του Parker ακολουθήθηκε κι από άλλους σημαντικούς μελετητές του φαινομένου σε αυτά τα πρώτα του βήματα.

Ο νομικός και συγγραφέας August Bequai ήταν ένας από τους πρώτους που ασχολήθηκε με το ζήτημα της ασφάλειας της αναπτυσσόμενης βιομηχανίας επεξεργασίας δεδομένων και των τραπεζών. Ξεκίνησε με τη μελέτη του εγκλήματος του λευκού περιλαιμίου και σύντομα εξελίχθηκε σε ειδικό πάνω στο έγκλημα υπολογιστών. Ο Bequai έπαιξε σημαντικό ρόλο στη προσπάθεια θέσπισης νόμων σχετικών με το έγκλημα υπολογιστών, ήταν μάλιστα από τους συντάκτες του ομοσπονδιακού νομοσχεδίου για την προστασία των συστημάτων υπολογιστών (Federal Computer Systems Protection Act, 1978). Πρότεινε τη θέσπιση αυστηρών χρηματικών και ποινικών ποινών για την αντιμετώπιση του αυξανόμενου κύματος του εγκλήματος που σχετίζεται με υπολογιστές επειδή αυτό ξεπερνά τις αντίστοιχες προσπάθειες του συστήματος απονομής δικαιοσύνης να το ελέγξει. Μέσα από συγγράμματα και δημόσιες ομιλίες του, προσπαθούσε, μόνο με τη παρουσίαση αδημοσίευτων δεδομένων, να επηρεάσει τους νομοθέτες και την κοινή γνώμη για την ανάγκη σκληρότερης αντιμετώπισης των χιλιάδων κινδύνων που παρουσιάζει η εξάπλωση των υπολογιστών στη σύγχρονη κοινωνία.[394]

4.3. Τα Χαρακτηριστικά του ηλεκτρονικού εγκλήματος

Οι μέχρι σήμερα δικαστικές αποφάσεις αφορούν εγκλήματα που τελούνται με ηλεκτρονικούς υπολογιστές (computer crimes) και όχι αποκλειστικά εγκλήματα του κυβερνοχώρου (cyber crimes).

Το ηλεκτρονικό έγκλημα είναι γρήγορο από άποψη χρόνου τέλεσης και ολοκλήρωσης του και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Είναι εύκολο και ανέξοδο στη διάπραξή του, για όσους διαθέτουν τις απαραίτητες γνώσεις πληροφορικής και τον κατάλληλο εξοπλισμό.

Δεν απαιτεί τη φυσική μετακίνηση του δράστη, ο οποίος μπορεί να πλήττει, πολλαπλούς στόχους, από τον υπολογιστή του γραφείου ή του σπιτιού του.

Είναι διασυνοριακό έγκλημα, «χωρίς πατρίδα» και οι συνέπειες του μπορεί να πραγματοποιούνται ταυτόχρονα σε διαφορετικές χώρες, ενώ είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τελέσεώς του καθιστώντας αρκετά δύσκολη τη διερεύνηση του και τον εντοπισμό του δράστη.[395]

Οι εγκληματίες, στον κυβερνοχώρο ειδικότερα, πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα αλλά χρησιμοποιούν εικονική ταυτότητα και ψεύτικα στοιχεία.[396]

Για τη διερεύνησή του εγκλήματος στο διαδίκτυο απαιτείται συνεργασία των αρχών δυο ή περισσότερων κρατών, συνήθως του κράτους στο οποίο εκδηλώνεται αρχικά το έγκλημα και του κράτους όπου πιθανά βρίσκονται τα αποδεικτικά στοιχεία.

Ο «σκοτεινός αριθμός» της εγκληματικότητας στο χώρο του διαδικτύου μεγαλύτερος από ότι για το «κοινό» έγκλημα. Τα στατιστικά στοιχεία δεν είναι επαρκή τόσο για τον Ελληνικό, όσο και για τον διεθνή χώρο επειδή είναι ελάχιστες οι περιπτώσεις εγκλημάτων του κυβερνοχώρου που καταγγέλλονται. Όπως και για το έγκλημα του λευκού περιλαιμίου η

[394] Hollinger Richard R., Lanza-Kaduce L., (1997), σσ. 59-77

[395] http://www.sdtv.gr/news-126.html, Μάιος (2008)

[396] http://www.apodimos.com/arthra/05/Aug/, Απρίλιος (2008)

απροθυμία καταγγελίας, ειδικά από τα θύματα, οφείλεται στην προσπάθεια να μην αμφισβητείται η αξιοπιστία τους, οι οποίοι κατά κανόνα είναι εταιρείες.

Η αστυνομική διερεύνησή του είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις επίσης απαιτούνται και όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (εισαγγελείς, δικαστές, δικηγόρους).[397]

4.3.1. Τα κίνητρα του δράστη ηλεκτρονικού εγκλήματος

Τα συνήθη **κίνητρα** του κυβερνοεγκληματία είναι[398]:

α) Απλή **διασκέδαση**. Αυτό το κίνητρο, σύμφωνα με τον J.Maxwell, δεν αφορά την επιδίωξη κανενός είδους οικονομικού οφέλους αλλά αφορά κυρίως τους νεαρούς χάκερ, που αντιμετωπίζουν το διαδίκτυο με διάθεση για παιχνίδι και που αντίθετα μπορεί να αποτελεί ένα ακριβό χόμπι που απαιτεί τη χρήση εξελιγμένων υπολογιστικών συστημάτων.

β) Οικονομικό **κέρδος**. Αποτελεί το συνηθέστερο κίνητρο του τυπικού ηλεκτρονικο-οικονομικού εγκληματία που αποκτά παράνομη πρόσβαση σε υπολογιστικά συστήματα για να αποκομίσει κάποιο χρηματικό κέρδος. Περικλείει αρκετές επιμέρους μορφές οικονομικών εγκλημάτων όπως κατάχρηση, βιομηχανική κατασκοπεία, ακόμα και μίσθωση των υπηρεσιών του σε άλλους για παράνομη διαδικτυακή δράση. Οι εγκληματίες του λευκού περιλαιμίου αυτής της περίπτωσης είναι μορφωμένοι, επαγγελματίες σε επαγγελματική αδράνεια ή καταστροφή.

γ) **Κάλυψη συναισθηματικών αναγκών** όπως θυμό, εκδίκηση, απόκτηση αναγνώρισης, κύρους και προσοχής. Οι εγκληματίες στο διαδίκτυο που δρουν από θυμό ή εκδίκηση είναι κυρίως απογοητευμένοι εραστές ή σύζυγοι, απολυμένοι υπάλληλοι, συνεργάτες που αισθάνονται εξαπατημένοι ή άλλοι που πιστεύουν ότι έχουν υποστεί κάποια αδικία ή κακό. Τα εγκλήματα στο διαδίκτυο με τέτοια κίνητρα μπορεί να είναι κυβερνο-τρομοκράτηση, απειλές, δυσφήμιση, διασπορά ιών, επιθέσεις άρνησης υπηρεσιών κλπ.

δ) **Πολιτικά** κίνητρα. Οι επιθέσεις σε ιστοσελίδες και δίκτυα κάθε είδους εξτρεμιστών ή τρομοκρατών που προσπαθούν να διασπείρουν μίσος και προπαγάνδα, να επιτεθούν σε κυβερνητικές υπηρεσίες, να αποκομίσουν κέρδη για την χρηματοδότηση ή τον προγραμματισμό της δράσης τους.

ε) **Σεξουαλικά** κίνητρα. Τέτοια είναι αυτά των παιδόφιλων που διακινούν ή λαμβάνουν υλικό παιδικής πορνογραφίας, που προσεγγίσουν παιδιά με σκοπό την προσέλκυση τους σε φυσική συνάντηση, βιαστών και δολοφόνων που μέσω της γνωριμίας με τα υποψήφια θύματα στο διαδίκτυο αποκτούν την εμπιστοσύνη τους και αφού τα συναντήσουν στον φυσικό κόσμο τα βιάζουν ή/και τα δολοφονούν.

Στ) **Ψυχικές ασθένειες** όπως σχιζοφρένεια, παράνοια, παραισθήσεις και άλλες σοβαρές ψυχικές διαταραχές. Αυτά τα άτομα είναι ευκολότερο να καλύψουν την ασθένεια από τους άλλους στο ψηφιακό που δεν υπάρχει φυσική επαφή παρά στο φυσικό περιβάλλον όπου θα ήταν άμεσα αντιληπτοί. [399]

Ο Bloombecker, δικηγόρος και διευθυντής του Εθνικού Κέντρου Δεδομένων για το Πληροφορικό Έγκλημα (National Center for Computer Crime Data), από την πλευρά του ασχολήθηκε περισσότερο με τη **κατηγοριοποίηση** των μορφών του πληροφορικού

[397] Βλ. και παρακάτω για δυσκολίες αντιμετώπισης.
[398] Shinder Debra Littlejohn (2002), σ.113
[399] Shinder Debra Littlejohn (2002), σσ. 112-119

εγκλήματος σε **σχέση με τα κίνητρα** των δραστών του.[400] Θεωρούσε την ευαισθησία της ασφάλειας των υπολογιστικών δικτύων επικοινωνίας ως τη πιο σημαντική εξέλιξη στον τομέα της ασφάλειας υπολογιστών. Στην αναφορά του Computer Crime, Computer Security, Computer Ethics το 1986, τόνιζε ότι η εστίαση αποκλειστικά στους οικονομικούς κινδύνους που προέρχονται από τη δράση των hackers άφηνε κενά ασφαλείας και θα έπρεπε να δοθεί η απαραίτητη προσοχή σε όλες τις μορφές του πληροφορικού εγκλήματος επειδή οι εγκληματίες υπολογιστών δεν είναι απαραίτητα ιδιοφυίες στους υπολογιστές και διακρίνονται ολοένα και λιγότερο από τους κοινούς εγκληματίες, ενώ θύμα τους θα μπορούσε να αποτελέσει ο καθένας.[401]

Έτσι διέκρινε τους παρακάτω τύπους πληροφορικών εγκλημάτων με βάση το κίνητρο:

1. Κλοπή χρημάτων (45% για το ΄86 και 36% για το ΄88)
2. Κλοπή πληροφοριών (16% και 12% αντίστοιχα)
3. Ζημιά σε λογισμικό (16% και 2%)
4. Κακόβουλη αλλοίωση (6% και 6%)
5. Αλλοίωση για απάτη (6% και 2%)
6. Κλοπή υπηρεσιών (10% και 34%)
7. Παρενόχληση (0% και 2%)
8. Εκβιασμός (0% και 4%)

Εδώ θα παρατηρούσε κανείς ότι η συσχέτιση και ταύτιση των κατηγοριών του πληροφορικού εγκλήματος με αυτές των κινήτρων που οδηγούν τους κάθε είδους δράστες στη διάπραξη τους, χωρίς να δίδεται ο απαραίτητος ορισμός, μάλλον προκαλούν εννοιολογικές και ταξινομικές συγχύσεις, παρά συμβάλλουν στην ομαλή διεξαγωγή κάθε ασφαλούς διαλόγου και προβληματισμού. Ακόμα είναι μάλλον αμφισβητήσιμο το κατά πόσο ένα ποσοστό της τάξης του 0 έως 2% (βλ. παραπάνω για την παρενόχληση και τον εκβιασμό) μπορεί να οδηγήσει τον θεωρητικό στον σχηματισμό μιας διακριτής και στατιστικά σημαντικής κατηγορίας. Αμφισβητήσιμη είναι επίσης η παραπάνω κατηγοριοποίηση που πρότεινε ο Bloombecker «σε σχέση με τα κίνητρα» καθώς φαίνεται να συγχέονται τα κίνητρα με το στόχο του εγκλήματος.

Ο Bloombecker, στη συνέχεια, αναγνωρίζοντας ότι ο δραστικός περιορισμός του πληροφορικού εγκλήματος αποτελεί μάλλον μια ουτοπία, προσπαθεί να εστιάσει την προσοχή των ενδιαφερομένων μερών, όχι τόσο στην νομοθεσία, αλλά στην επαύξηση των μέτρων ασφάλειας με διαρκή ενημέρωση των υπεύθυνων συστημάτων ασφάλειας, ιδιαίτερα από τους πιο ειδικευμένους στο αντικείμενο που δεν είναι άλλοι από τους ίδιους τους παραβάτες.[402]

Ενδιαφέρουσες απόψεις για τα **κίνητρα** του ηλεκτρονικού εγκλήματος αποτελούν και αυτές του Hayes που πιστεύει ότι τα πληροφορικά εγκλήματα υποδηλώνουν τη δύναμη εκατομμυρίων εργαζομένων να προωθήσουν τα πολιτικά τους συμφέροντα απέναντι στους απανταχού εργοδότες.[403]

[400] Hollinger Richard C. (1997a) , σ. xx-xxi
[401] BloomBecker Buck (1997), σσ.35-42.
[402] Λάζος Γρηγόρης, (2001), σ.44
[403] Λάζος Γρηγόρης (2001), σσ. 56 -60

4.3.2. Το προφίλ του κυβερνο εγκληματία

Σύμφωνα με την Debra L. Shinder το προφίλ του κυβερνοεγκληματία περιλαμβάνει τα παρακάτω γενικά χαρακτηριστικά:

1. Στοιχειώδεις τουλάχιστον τεχνικές γνώσεις σχετικά με τη χρήση των κατάλληλων τεχνολογικών εργαλείων και μεθόδων. Ενώ ο απλός χρήστης των ηλεκτρονικών μέσων δεν χρειάζεται εξειδικευμένες γνώσεις για τις καθημερινές δραστηριότητες του στο διαδίκτυο, π.χ. να πλοηγηθεί στις ιστοσελίδες, να στείλει ηλεκτρονικά μηνύματα κλπ., πολλά από τα ηλεκτρονικά εγκλήματα απαιτούν από τον δράστη χρήση μεθόδων και εργαλείων με περισσότερη εξειδίκευση και εμπειρία από τα παραπάνω.[404]
2. Υποτίμηση του νόμου ή αίσθηση ότι βρίσκεται υπεράνω του νόμου. Σχεδόν κανείς δεν θεωρεί ότι οι πράξεις του είναι κακές αλλά τις δικαιολογεί. Έτσι και ο δράστης εγκλήματος στο διαδίκτυο θεωρεί ότι οι νόμοι που παραβαίνει είναι κακοί, παράλογοι και ως εκ τούτου είναι σωστό και δικαιολογημένο να τους παραβεί. Μερικές φορές μάλιστα, λόγω των ικανοτήτων, εμπειρίας, της θέσης ή των περιστάσεων πιστεύει ότι είναι υπεράνω του νόμου ή ότι ο νόμος δεν ισχύει στον κυβερνοχώρο.
3. Δημιουργία εικονικής προσωπικότητας και ζωής. Πολλοί δράστες στον κυβερνοχώρο δημιουργούν καινούριες, ψεύτικες ταυτότητες (προσωπικότητες) που, εκτός του ότι τους ευχαριστεί να υποδύονται κάποιον «άλλο», τις χρησιμοποιούν για να ξεγελάσουν θύματα, να κρύβονται και να αποφεύγουν τον εντοπισμό και τη σύλληψη.
4. Ριψοκίνδυνη προσωπικότητα που επιδιώκει να έχει τον έλεγχο των καταστάσεων. Για κάποιους εγκληματίες η αίσθηση του κινδύνου τους συναρπάζει, τους ελκύει και τους κάνει να αφιερώνουν μεγαλύτερες προσπάθειες σε ριψοκίνδυνες και παράνομες συμπεριφορές παρά σε νόμιμες. Άλλοι πάλι αρέσκονται στο να έχουν την αίσθηση του ελέγχου πάνω στη δράση των άλλων. Τα δυο αυτά χαρακτηριστικά μπορεί να συνυπάρχουν και στο ίδιο πρόσωπο.
5. Ο κάθε δράστης έχει ισχυρά και διαφορετικά κίνητρα από τους άλλους δράστες του κυβερνοεγκλήματος. Τα κίνητρα ποικίλλουν από το οικονομικό όφελος, τη σεξουαλική ικανοποίηση, την απληστία, το θυμό, την απόγνωση μέχρι και τα πολιτικά κίνητρα, ανάλογα με το δράστη και το είδος του εγκλήματος.

Οι νεαροί hacker σύμφωνα με τον J. Maxwell διακρίνονται στις εξής κατηγορίες:

- Οι **πρωτοπόροι**, που ενδιαφέρονται να μάθουν και να αποκτούν εμπειρία για το πώς λειτουργούν τα διάφορα τεχνολογικά συστήματα.
- Τα «**διαολάκια»,** που δεν έχουν την πρόθεση να προκαλέσουν ζημιά αλλά το κάνουν για παιχνίδι.
- Οι **εξερευνητές,** που θέλουν από περιέργεια να μπουν σε καινούρια δίκτυα και να δουν τι μπορούν να ανακαλύψουν εκεί.
- Οι **παίκτες,** που επιδιώκουν να αποδείξουν ότι μπορούν να νικήσουν τα συστήματα αποκτώντας τον έλεγχο τους.
- Οι **εθισμένοι,** που μπορεί να αποτελούν την μετεξέλιξη κάποιου από τους παραπάνω χαρακτήρες που αποκτούν ψυχική εξάρτηση από τη δραστηριότητα και την συνεχίζουν για να αισθάνονται καλά.[405]

[404] Shinder Debra Littlejohn, Ed. Tittel (2002), σσ. 113-118

[405] Shinder Debra Littlejohn (2002), σσ. 113-114

4.4. Τα δημογραφικά χαρακτηριστικά και οι διαδικτυακές ασχολίες των χρηστών ίντερνετ ως υποψήφια θύματα/στόχοι

Οι πιθανοί δράστες των ηλεκτρονικο-οικονομικών εγκλημάτων, όπως και τα κατάλληλα θύματα – πιθανοί στόχοι, συναντώνται σε ένα κοινό «χώρο», το διαδίκτυο, το δίκτυο υπολογιστών ή τηλεφωνίας. Οι δυο πλευρές αποτελούν χρήστες του ίδιου δικτύου το οποίο αποτελεί την «δεξαμενή» άντλησης τόσο πιθανών δραστών όσο και ελκυστικών στόχων.

Παρακάτω εξετάζονται τα δημογραφικά χαρακτηριστικά των χρηστών των σύγχρονων τεχνολογιών και του διαδικτύου και οι καθημερινές δραστηριότητες τους που μπορεί να τους καθιστούν πιθανούς στόχους ή στο πλαίσιο των οποίων, ως δράστες, ανακαλύπτουν πιθανούς στόχους για την τέλεση ηλεκτρονικο-οικονομικού εγκλήματος.

Στις διάφορες στατιστικές για τους χρήστες των τεχνολογιών και του διαδικτύου οι ομάδες που κυριαρχούν είναι οι νέοι άνδρες, με υψηλό μορφωτικό επίπεδο και εισόδημα, που προέρχονται από οικονομικά αναπτυγμένες χώρες.[406] Τα στοιχεία αυτά αποδεικνύουν την ύπαρξη ανισοτήτων, ως προς την πρόσβαση και την χρήση των ψηφιακών τεχνολογιών, που αντανακλούν –και σε ένα βαθμό αναπαράγουν- τις κοινωνικές ανισότητες. Οι ανισότητες αυτές συνιστούν το ψηφιακό χάσμα, μια διάκριση ανάμεσα σε προνομιούχους, που έχουν πρόσβαση στις τράπεζες πληροφοριών και άρα την δυνατότητα να διευρύνουν τις γνώσεις τους, το πολιτισμικό τους κεφάλαιο και τις δυνατότητες βελτίωσης της επαγγελματικής και κοινωνικής τους θέσης και σε μη προνομιούχους ή πληροφορικά αποκλεισμένους που δεν έχουν τις παραπάνω δυνατότητες.[407]

Παρά την ευρεία διάδοση της πληροφορικής και της χρήσης του διαδικτύου, τα δημογραφικά και κοινωνικά χαρακτηριστικά των χρηστών του διαδικτύου δείχνουν ότι:

Το 70% των χρηστών του διαδικτύου στις ΗΠΑ κατά το 2000, διέθεταν υψηλό εισόδημα – πάνω από 75000 δολάρια και το 75 % ήταν πανεπιστημιακής εκπαίδευσης έναντι μόλις 19% που διέθετε εισόδημα λιγότερο από 15000 δολάρια και 12,7% που είχαν ολοκληρώσει μόνο τη βασική εκπαίδευση[408].

Ανάμεσα στις διάφορες κατηγορίες δημογραφικών χαρακτηριστικών των χρηστών του ίντερνετ στις ΗΠΑ οι πιο ισχυροί δημογραφικοί παράγοντες, μεταξύ των ετών 2000 και 2011, παραμένουν η ηλικία, το φύλο, το μορφωτικό επίπεδο, το επίπεδο απασχόλησης και το ύψος του εισοδήματος.[409] Το ψηφιακό χάσμα στο ίδιο διάστημα μειώθηκε σημαντικά, χωρίς όμως να εξαλειφθεί, κυρίως όσον αφορά την φυλή και ειδικότερα τους έγχρωμους και τους λατινικής καταγωγής. Περίπου 4 στους δέκα έγχρωμους και ισπανόφωνους δεν χρησιμοποιούσαν το ίντερνετ το 2011 σε σχέση με 2 στους δέκα για το 2000 αντίστοιχα.[410]

Όσον αφορά τις διαδικτυακές δραστηριότητες των χρηστών με βάση τα δημογραφικά τους χαρακτηριστικά οι πιο δημοφιλείς είναι η χρήση του ηλεκτρονικού ταχυδρομείου (92%), η αναζήτηση στο διαδίκτυο (92%) η ανάγνωση ειδήσεων (76%), οι διαδικτυακές αγορές (71%), τα μέσα κοινωνική δικτύωσης (65%)[411], και το e-banking (61%). Η διαφοροποίηση (το ψηφιακό χάσμα) ως προς τα δημογραφικά χαρακτηριστικά αφορά την ηλικία, τη φυλή, το εισόδημα και το μορφωτικό επίπεδο. Πιο συγκεκριμένα οι λευκοί και οι μαύροι σε σχέση με τους λατίνους, οι νεότεροι σε σχέση με τους πιο μεγάλους (πάνω από 50 ετών), οι πιο

[406] Καϊτατζή - Γουίτλοκ, Σοφία (2003), σ. 217
[407] Λέανδρος Νίκος (2005), σ. 178
[408] Λέανδρος Νίκος (2005), σ. 102-3
[409] http://www.pewinternet.org/2012/04/13/digital-differences, Νοέμβριος 2014
[410] File Thom (2013, Βλ.και Πίνακες 2,3 και 4
[411] Purcell Kristen (2011)

μορφωμένοι (που έχουν τουλάχιστον φοιτήσει σε κολέγιο) σε σχέση με τους λιγότερο μορφωμένους και αυτοί με μεγαλύτερο εισόδημα (πάνω από 30000 $) είναι εκείνοι που επιδίδονται συχνότερα στις παραπάνω διαδικτυακές δραστηριότητες. [412]

Για την Ελλάδα τα αντίστοιχα ποσοστά των νοικοκυριών που έχουν πρόσβαση στο ίντερνετ από το σπίτι, σύμφωνα με την ΕΛ.ΣΤΑΤ. (Ελληνική Στατιστική Αρχή) για το 2013, αποκαλύπτουν ψηφιακό χάσμα μεταξύ λεκανοπεδίου Αττικής (69%) και υπόλοιπων περιοχών τη Ελλάδας (Βόρειου: 52%, Κεντρικής: 41% , Νησιών και Κρήτης: 48%, μεταξύ νεότερων και μεγαλύτερων σε ηλικία, μεταξύ μορφωμένων και λιγότερο ή καθόλου μορφωμένων ατόμων.[413]

Σχετικά με τι πιο δημοφιλείς δραστηριότητες στις ίδιες στατιστικές για το 2013, αναφέρεται[414] ότι στην Ελλάδα οι χρήστες του διαδικτύου το χρησιμοποιούν για:

- Αποστολή ή λήψη ηλεκτρονικών μηνυμάτων, 76%
- Ανεύρεση πληροφοριών για είδη και υπηρεσίες 83%
- Ανάγνωση ειδήσεων online 77%
- Συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης 60%
- Συναλλαγές με τις δημόσιες αρχές (Ηλεκτρονική Διακυβέρνηση: πληροφορίες, πρόσβαση σε έντυπα, επιστροφή συμπληρωμένων εντύπων) είναι 58%,
- Αναζήτηση πάσης φύσεως πληροφοριών με σκοπό τη γνώση και την ηλεκτρονική μάθηση 53%
- Ηλεκτρονική Υγεία (e-health) 56%
- Να παίξουν ή να κατεβάσουν παιχνίδια, εικόνες, ταινίες και μουσική 50%[415].
- Ταξιδιωτικές υπηρεσίες 38%
- Ηλεκτρονικές Αγορές 27%
- Τραπεζικές συναλλαγές 18%.

Οι περισσότερες από τις παραπάνω καθημερινές δραστηριότητες των απλών χρηστών μπορεί να τους καταστήσουν, υπό προϋποθέσεις, ευάλωτους στόχους δραστών με κίνητρο.

Στην Μ. Βρετανία, μια από τις χώρες με το μεγαλύτερο βαθμό διείσδυσης στις νέες τεχνολογίες, το 8% των χρηστών του διαδικτύου αναφέρει ότι έχει πέσει θύμα κυβερνοεγκλήματος, πάνω από 9 εκατομμύρια ότι έχουν παραβιαστεί οι διαδικτυακοί τους λογαριασμοί από χάκερ, καθιστώντας τη μορφή αυτή ως το πιο σημαντικό ηλεκτρονικό έγκλημα, ενώ το 2,3% του πληθυσμού έχει υποστεί απώλειες πάνω από 10000 λίρες ως θύμα ηλεκτρονικής απάτης. Οι περισσότεροι λογαριασμοί που παραβιάστηκαν αφορούσαν, e-banking, emails και λογαριασμούς σε μέσα κοινωνικής δικτύωσης. Το μέσο προσβολής είναι η δημιουργία κακόβουλου λογισμικού που προσβάλλει αρχικά τους λογαριασμούς κοινωνικής δικτύωσης των χρηστών, με απώτερο στόχο την πρόσβαση στους τραπεζικούς λογαριασμούς

[412] Βλ. Πίνακα 6, Πηγή:http://www.pewinternet.org/2012/04/13/digital-differences/#fn-188-40, Νοέμβριος 2014

[413] ΕΛ.ΣΤΑΤ. http://www.statistics.gr/portal/page/portal/ESYE/PAGE-themes?p_param=A1901&r_param=SFA20&y_param=2012_00&mytabs=0, Οκτώβριος 2014

[414] ΕΛ.ΣΤΑΤ. http://www.statistics.gr/portal/page/portal/ESYE/PAGE-themes?p_param=A1901&r_param=SFA20&y_param=2012_00&mytabs=0, Οκτώβριος 2014, Βλ. και Πίνακα 7.

[415] Το συγκεκριμένο στατιστικό στοιχείο αναφέρεται για το 2012, ενώ δεν είναι ακόμα διαθέσιμο για το 2013.

του e-banking μέσω phishing. Στο 33% των περιπτώσεων το έγκλημα ήταν επαναλαμβανόμενο.[416]

Στατιστικά στοιχεία σχετικά με τις καταγγελλόμενες παραβιάσεις στο διαδίκτυο

Σύμφωνα, με στοιχεία της ασφαλούς γραμμής στο διαδίκτυο Safeline[417] για την Ελλάδα το 2013, η παραβίαση προσωπικών δεδομένων είναι η κυρίαρχη κατηγορία παραβιάσεων με τον μεγαλύτερο αριθμό καταγγελιών 34%, οι οικονομικές απάτες (που σχετίζονται με τις προηγούμενες) ακολουθούν με ποσοστό 16% και η παιδική πορνογραφία με 12%.[418]

Σε ατομικό επίπεδο ενδιαφέρον παρουσιάζει η πρόσφατη[419] έρευνα του Παντείου Πανεπιστημίου, με επιστημονική υπεύθυνη την καθηγήτρια Χριστίνα Ζαραφωνίτου, σε δείγμα φοιτητών για την θυματοποίηση και τον φόβο του εγκλήματος στο διαδίκτυο.[420] Σύμφωνα με την έρευνα όσοι από τους φοιτητές έχουν πέσει θύματα παρουσιάζουν τα παρακάτω χαρακτηριστικά:

- Φύλο:

Γυναίκες: 21%, Άνδρες: 19.6%,

- Εμπειρία χρήσης διαδικτύου:

1 -5 χρόνια: 20.9%, 6 - 10 χρόνια: 21.2%, πάνω από 11 χρόνια: 17.5%.

- Επίπεδο εκπαίδευσης σχετική με υπολογιστές:

Καμία ιδιαίτερη εκπαίδευση: 16.6%, Ιδιαίτερη εκπαίδευση: 24.8%.

- Συχνότητα χρήσης διαδικτύου:

Σπάνια: 20%, Περισσότερο από μια φορά την εβδομάδα: 3.6%, Καθημερινά: 22.3%.

Σύμφωνα με την παραπάνω έρευνα του Παντείου Πανεπιστημίου για την θυματοποίηση και τον φόβο του εγκλήματος στο διαδίκτυο[421] βρέθηκε ότι η πλειονότητα των θυμάτων έχει θυματοποιηθεί επανειλημμένα (πάνω από 5 φορές).

Το στοιχείο αυτό επιβεβαιώνει την άποψη των εγκληματικών προτύπων ότι οι δράστες χρησιμοποιούν «οδούς» και βάλλουν στόχους που ήδη έχουν δοκιμάσει και γνωρίζουν.[422]

4.5. Το κόστος του ηλεκτρονικού εγκλήματος

Αντίστοιχες με αυτές του οικονομικού εγκλήματος είναι οι συνέπειες και το κόστος που επιφέρει το ηλεκτρονικό έγκλημα. Οι συνέπειες αυτές μάλιστα επιδεινώνονται λόγω της οικονομικής κρίσης και αφορούν τους εξής τομείς:

- ✓ Απώλειες πνευματικής ιδιοκτησίας και ευαίσθητων δεδομένων.
- ✓ Επαγγελματικές δυσλειτουργίες.
- ✓ Ζημιά στην εικόνα και τη φήμη των επιχειρήσεων.
- ✓ Πληρωμή αποζημιώσεων σε καταναλωτές ή συνεργαζόμενες επιχειρήσεις για αθέτηση συμβατικών υποχρεώσεων.
- ✓ Κόστη για λήψη μέτρων προστασίας και ασφάλειας.

[416] Paganini Pierluigi, ό.π.
[417] http://www.safeline.gr/kataggelies/statistika-stoiheia?set=1
[418] Βλ. ΠΙΝΑΚΑ 8
[419] Κατά την περίοδο συγγραφής του συγκεκριμένου κεφαλαίου της παρούσας διατριβής.
[420] Zarafonitou Christina & Koumentaki Evangelia (2014)
[421] Zarafonitou Christina & Koumentaki Evangelia (2014)
[422] Βλ. παραπ. Θεωρία εγκληματικών προτύπων και Farrell Graham, Clark Ken, Ellingworth Dan, Pease Ken (2005)

- ✓ Κόστη για πολιτικές επανόρθωσης και ανάκαμψης από κυβερνοεπιθέσεις.
- ✓ Εμπορικές και επαγγελματικές απώλειες και μείωση ανταγωνιστικότητας.[423]

Αποτελέσματα έρευνας του Ινστιτούτου Ponemon[424], έδειξαν ότι το κόστος του κυβερνοεγκλήματος για το 2013 έχει αυξηθεί κατά 78%, ενώ το κόστος επίλυσης μιας και μόνης επίθεσης υπολογίστηκε σε 1 εκατ. δολάρια. Πιο αναλυτικά τα ευρήματα της έρευνας έδειξαν:

- Το σύνολο της κυβερνο-δραστηριότητας υπολογίστηκε ανάμεσα σε 300 δις και 1 τρις δολάρια.
- Η πειρατεία υπολογίστηκε να συμμετέχει στο κόστος με 1 έως 16 δις δολάρια και η (παράνομη) διακίνηση φαρμάκων σε 600 δις δολάρια παγκοσμίως.[425]
- Το μέσο ετήσιο κόστος του κυβερνοεγκλήματος ανά οργανισμό ήταν 11,56 εκατ. δολάρια με έκταση από 1,3 έως 58 εκατ. αυξημένο κατά 26% σε σχέση με το 2012.
- Το υψηλότερο κόστος υπέστησαν οι οργανισμοί στους τομείς της άμυνας, των οικονομικών υπηρεσιών και της ενέργειας.
- Η κλοπή δεδομένων είχε μεγάλη συμμετοχή στις συνολικές απώλειες με 43%, οι επιχειρηματικές δυσλειτουργίες, οι απώλειες στην παραγωγικότητα με 36%.
- Οι επιτυχημένες επιθέσεις εναντίον οργανισμών ήταν 122 ανά εβδομάδα.
- Ο μέσος χρόνος επίλυσης μιας κυβερνοεπίθεσης ήταν 32 μέρες και το κόστος από αυτό περίπου 1 εκ. δολ.
- Οι μικρές επιχειρήσεις αντιμετωπίζουν αναλογικά μεγαλύτερες απώλειες σε σχέση με τις μεγαλύτερες.
- Οι πιο δαπανηρές εσωτερικές διαδικασίες ήταν η ανάκτηση και η ανακάλυψη.

Η McAfee υπολόγισε ότι το κυβερνοέγκλημα και η κυβερνο-κατασκοπεία κοστίζουν στην αμερικάνικη οικονομία περίπου 300 δις δολάρια το χρόνο που σημαίνει το 0,04% του παγκόσμιου ακαθάριστου προϊόντος.[426]

Για την Μ. Βρετανία τα επίσημα στοιχεία της κυβέρνησης για το 2011 υπολόγισαν ότι το συνολικό κόστος του κυβερνοεγκλήματος ήταν 27 δις λίρες ετησίως, με το πιο διαδεδομένο έγκλημα αυτού του είδους να είναι η κλοπή ταυτότητας (identity theft) με κόστος 1,7 δις και οι διαδικτυακές απάτες (scams) με συμμετοχή στα 1,4 δις λίρες Αγγλίας. Για τις δημόσιες και ιδιωτικές επιχειρήσεις και οργανισμούς της Μ. Βρετανίας το κυβερνοέγκλημα ήταν από τα πιο επιζήμια με σημαντικότερα αυτά της κυβερνο-κατασκοπείας και της κλοπής πνευματικής ιδιοκτησίας.[427]

Μια άλλη σημαντική παράπλευρη απώλεια της διαδικτυακής εγκληματικής δραστηριότητας είναι η απώλεια 508000 θέσεων εργασίας μόνο για τις ΗΠΑ.

Η μελέτη του Ponemon τόνισε ότι:

> «οι οργανισμοί που χρησιμοποιούν τεχνολογίες αντικατασκοπείας ήταν πιο αποτελεσματικές στην επισήμανση και αντιμετώπιση των κυβερνοεπιθέσεων

[423] Paganini Pierluigi (2014)
[424] Το Ινστιτούτο Ponemon υποστηρίζεται από την εταιρεία HP και τα αποτελέσματα των ερευνών του χρησιμοποιούνται από άλλες επιχειρήσεις για να κάνουν χρήσιμες εκτιμήσεις σχετικά με τις πιο αποτελεσματικές και οικονομικές λύσεις για τον περιορισμό των κινδύνων από τις κυβερνοεπιθέσεις. Βλ. σχετικά Paganin Pierluigi ό.π.
[425] Βλ. Παράρτημα Διάγραμμα 6
[426] η Παγκόσμια Τράπεζα υπολόγισε το παγκόσμιο Ακαθάριστο προϊόν σε 70 τρις δολάρια για το 2011.
[427] Paganini, Pierluigi ό.π.

εξοικονομώντας σχεδόν 4 εκατ. δολάρια το χρόνο και απόσβεση κεφαλαίου της επένδυσης κατά 21%».[428]

Η ετήσια μελέτη της Symantec, μια από τις θεωρούμενες μεγαλύτερες έρευνες διαδικτυακού εγκλήματος εναντίον καταναλωτών βασισμένη σε αναφορές πάνω από 13000 ατόμων σε 24 χώρες, εξετάζει τις επικίνδυνες διαδικτυακές συμπεριφορές των καταναλωτών και το οικονομικό κόστος του κυβερνοεγκλήματος. Η ετήσια έκθεσή της για το 2013 εκτίμησε το κόστος του κυβερνοεγκλήματος για τους καταναλωτές σε 113 δις δολάρια σε ετήσια βάση αυξημένο κατά 50% και τον αριθμό των θυμάτων να έχει μειωθεί σε 378 εκατομμύρια άτομα. Οι χώρες με το μεγαλύτερο ποσοστό θυμάτων βρέθηκαν η Ρωσία με 85%, η Κίνα με 77% και η Νότιος Αφρική με 73%. Το μεγαλύτερο κόστος για τους καταναλωτές αναφέρθηκε για τις ΗΠΑ 38 δις, την Ευρώπη 13 δις και την Κίνα 37 δις δολάρια. [429]

Τέλος όπως αναφέρουν οι Smith, Grabosky και Urbas, μια από πιο πρόσφατες εκτιμήσεις ανεβάζουν το κόστος του κυβερνοεγκλήματος για τις εταιρείες σε 1 τρις δολάρια ετησίως.[430]

Όπως μπορούμε να παρατηρήσουμε από τα παραπάνω στοιχεία για το κόστος του ηλεκτρονικού εγκλήματος, συχνά το κόστος αυτό είναι δύσκολο να διακριθεί και να απομονωθεί από το κόστος του οικονομικού εγκλήματος, λόγω της αλληλοεπικάλυψης και συσχέτισης που παρουσιάζουν οι δυο αυτές μορφές εγκληματικότητας.

[428] Paganini, Pierluigi ό.π.
[429] Paganini, Pierluigi ό.π.
[430] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σ. 37

ΚΕΦΑΛΑΙΟ 5. ΣΧΕΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

5.1. Η έννοια του ηλεκτρονικο-οικονομικού εγκλήματος

Μετά τη δεκαετία του ’80, έχουμε την διάδοση της πληροφορικής, την εμφάνιση του ηλεκτρονικού υπολογιστή, την εξέλιξη των τηλεπικοινωνιών και τη δημιουργία εθνικών και παγκοσμίων δικτύων. Η πληροφορική τεχνολογία έγινε προσιτή σε ευρύτερες πληθυσμιακές ομάδες και δίνει ευκαιρίες τέλεσης πληροφορικών εγκλημάτων όχι μόνο σε ειδικούς πληροφορικής, αλλά και σε εργαζόμενους στο πλαίσιο της νόμιμης απασχόλησης τους.

Εμφανίζεται έτσι, τα τελευταία χρόνια μια ιδιαίτερη μορφή οικονομικού εγκλήματος, που προσδιορίζεται από τα μέσα τέλεσης ή και από το αντικείμενο της αξιόποινης πράξης που αποτελεί το ηλεκτρονικό -οικονομικό έγκλημα.

Όταν μια επέμβαση τρίτου σε ηλεκτρονικό υπολογιστή έχει ως αποτέλεσμα, εκτός των άλλων και την προσβολή οικονομικών έννομων αγαθών τότε μιλάμε για **ηλεκτρονικό οικονομικό έγκλημα**.

Τέτοια εγκλήματα είναι οι διάφορες εμπορικές απάτες μέσω ηλεκτρονικού υπολογιστή και του ίντερνετ, η μη εξουσιοδοτημένη πρόσβαση, η βιομηχανική κατασκοπεία, οι πυραμίδες, οι επενδυτικές απάτες, η χειραγώγηση των τιμών μετοχών του χρηματιστηρίου (όπου επενδυτές που χρησιμοποιούν το ίντερνετ τροφοδοτούνται σκόπιμα με παραπλανητικές πληροφορίες για προβλεπόμενες τιμές μετοχών), οι απάτες με πιστωτικές κάρτες, η παράνομη μεταφορά κεφαλαίων από ηλεκτρονικούς τραπεζικούς λογαριασμούς, οι παραβιάσεις πνευματικής ιδιοκτησίας, το ξέπλυμα μαύρου χρήματος στο διαδίκτυο κλπ.

Ο Ν. Κουράκης περιλαμβάνει το ηλεκτρονικό έγκλημα και το έγκλημα στο διαδίκτυο στο φάσμα του οικονομικού εγκλήματος ανάμεσα σε εγκλήματα όπως οι τελωνειακές απάτες, η φοροδιαφυγή, οι απάτες, οι απάτες στο χρηματιστήριο, η μόλυνση του περιβάλλοντος, το εμπόριο προσωπικών δεδομένων κλπ. [431]

Πολλές ακόμα μελέτες για το ηλεκτρονικό έγκλημα κάνουν μνεία για τη σχέση του με το οικονομικό, το έγκλημα του Λευκού Περιλαιμίου. Για τη σχέση αυτή υπάρχουν βασικά δυο τάσεις μελετών, η πρώτη από αυτές θεωρεί το πληροφορικό ως μέρος του εγκλήματος λευκού περιλαιμίου (Levi, Comer) και η δεύτερη τάση που βρίσκει μικρή σχέση ηλεκτρονικού εγκλήματος και εγκλήματος λευκού περιλαιμίου (Parker). [432]

Τα είδη και τα χαρακτηριστικά του εγκληματία που ασχολείται με τέτοιες μορφές παράνομης δραστηριότητας προσιδιάζουν σε πολλά σημεία με αυτά του εγκληματία με το λευκό περιλαίμιο.

5.2. Οι κατηγορίες των ηλεκτρονικο-οικονομικών εγκλημάτων σε σχέση με τα κίνητρα του δράστη

Σύμφωνα με την Shinder, τα οικονομικά εγκλήματα του λευκού περιλαιμίου στον κυβερνοχώρο περιλαμβάνουν διάφορες κατηγορίες όπως:

1. Η μη εξουσιοδοτημένη πρόσβαση στα αρχεία μια επιχείρησης με σκοπό την αλλαγή τους προς όφελος του εγκληματία, π.χ. να του δοθεί αύξηση μισθού ή καλύτερη αξιολόγηση.

[431] Λάζος Γρηγόρης (2004), σσ. 67 - 69

[432] Λάζος Γρηγόρης (2001), σ. 55

2. Η μη εξουσιοδοτημένη απόκτηση εμπιστευτικών πληροφοριών για την αγορά μετοχών ή άλλων επενδυτικών προϊόντων.
3. Η πώληση πληροφοριών της επιχείρησης σε τρίτους, συνεργάτες ή ανταγωνιστές με σκοπό τον εκβιασμό ή τη δωροληψία.
4. Η αλλοίωση των ηλεκτρονικών λογαριασμών της επιχείρησης ή των πελατών της προς όφελος του εγκληματία.
5. Η αλλοίωση των λογιστικών βιβλίων ή των δηλώσεων της επιχείρησης για τη παροχή εσφαλμένων πληροφοριών σε τρίτους, όπως επενδυτές, εφορία κλπ με σκοπό τη κάλυψη άλλων εγκλημάτων.

Σε σχέση με τα κίνητρά τους οι εγκληματίες αυτού του είδους εμπίπτουν στις εξής **κατηγορίες**:

α) Ο «πικραμένος» εγκληματίας που αισθάνεται προδομένος από την επιχείρηση στην οποία εργάζεται επειδή δεν πήρε την αύξηση που προσδοκούσε ή έλαβε μια αδίκως αρνητική αξιολόγηση. Δικαιολογεί την εγκληματική δράση του υιοθετώντας μια νοοτροπία τύπου «Ρομπέν των δασών» που παίρνει από τους πλούσιους και δίνει στους φτωχούς, όπως ο εαυτός του.

β) Ο «υπολογιστικός» τύπος ευφυούς εγκληματία που μόλις βρίσκει την κατάλληλη ευκαιρία θα διαπράξει το έγκλημα βάσει προγραμματισμένου σχεδίου με χρονική ακρίβεια για οικονομικό όφελος και χωρίς ηθικούς ενδοιασμούς. Τα κέρδη του εξάγονται σταδιακά και προσεκτικά σε ασφαλείς τοποθεσίες, όπως εταιρείες offshore ή τράπεζες σε εξωτικά μέρη για να αποφύγουν την επισήμανση. Αποσύρεται από τη δράση μετά από κάποιο διάστημα ή αφότου έχει συγκεντρώσει το χρηματικό ποσό που είχε υπολογίσει.

γ) Ο «απελπισμένος», που εγκληματεί ως απάντηση σε σοβαρά οικονομικά προβλήματα που αντιμετωπίζει λόγω υγείας, οικογενειακής κρίσης, κακών επενδυτικών επιλογών ή λόγω εμπλοκής του σε προβλήματα με το νόμο, ναρκωτικών, αλκοόλ, τζόγο κλπ. Αυτός ο τύπος εγκληματία όσο χειροτερεύει η κατάστασή του παρουσιάζεται πολύ απρόσεκτος στην κάλυψη των ιχνών του και άρα πιο εύκολα εντοπίσιμος. [433]

5.3. Τα Χαρακτηριστικά των δραστών του ηλεκτρονικο-οικονομικού εγκλήματος

Τα χαρακτηριστικά των δραστών οικονομικών εγκλημάτων (ιδιαίτερα αυτά του τύπου λευκού περιλαιμίου) μπορούμε να τα αντιπαραβάλλουμε με αυτά των ηλεκτρονικών εγκλημάτων. Όπως θα διαπιστώσουμε διαθέτουν πολλά κοινά χαρακτηριστικά.

Το υψηλό status του δράστη δεν αποτελεί κριτήριο σύμφωνα με το νομικό ορισμό του οικονομικού εγκλήματος, παρά μόνο για τον εγκληματολογικό ορισμό.[434]

Ο εγκληματίας πληροφορικής είναι σχετικά νέος, μορφωμένος, τύπου «Λευκού Περιλαιμίου», ευφυής, καιροσκόπος και ενθουσιώδης χρήστης της τεχνολογίας.

Μια ιδιαίτερη κατηγορία ηλεκτρονικού εγκληματία, ο χάκερ επιδίδεται, ερασιτεχνικά ή επαγγελματικά, με επιδεξιότητα στην αθέμιτη χρήση των Η/Υ για πρόκληση ζημιάς ή

[433] Shinder Debra Littlejohn (2002), σ. 121
[434] Ιωαννίδης Χρήστος (2001), σ.159

κατάχρηση και σφετερισμό χρημάτων και πληροφοριών,[435] προσωπική ικανοποίηση[436], ακόμα και αντεκδίκηση ενάντια στην επιχείρηση που τον εκμεταλλεύεται[437].

Σύμφωνα με τον Hollinger, παρά το γεγονός ότι το 30% των αμερικανικών νοικοκυριών διαθέτει Η/Υ, οι περισσότεροι ενήλικοι δεν διαθέτουν ιδιαίτερες γνώσεις στους υπολογιστές και μάλλον φοβούνται την πληροφορική τεχνολογία. Από την πλευρά τους οι περισσότεροι ηλεκτρονικοί εγκληματίες διαθέτουν υψηλό επίπεδο τεχνικών γνώσεων στους υπολογιστές, ανήκουν στην μεσαία ή ανώτερη κοινωνική τάξη, είναι λευκοί, μη βίαιοι και διαπράττουν αδίκημα για πρώτη φορά.

Παρόλα αυτά δε θα πρέπει να παραγνωριστεί και ένα ποσοστό περιπτώσεων που οι δράστες του ηλεκτρονικού εγκλήματος δεν διαθέτουν υψηλό status. Αυτές οι περιπτώσεις αφορούν κυρίως σε hackers, νέους σε ηλικία (εγκληματίες των «κοντών παντελονιών») με κίνητρο όχι τόσο το οικονομικό όφελος αλλά την επιδίωξη συγκινήσεων, δράσης, την ικανοποίηση της περιέργειας, την αντεκδίκηση κλπ. Οι χάκερ, από την πλευρά τους αντιμετωπίζουν, σύμφωνα με τον Hollinger, εντονότερη κινητοποίηση των διωκτικών αρχών λόγω αποτυχιών σε άλλους τομείς (καταπολέμηση ναρκωτικών, οργανωμένου εγκλήματος, οικονομικές απάτες κλπ.) και του αυξημένου φόβου για τις πληροφορικές τεχνολογίες από πλευράς κοινού. Παρόλα αυτά το ποσοστό καταδικών σε ποινές φυλάκισης είναι μικρό και οι περισσότερες περιπτώσεις αντιμετωπίζονται με άλλα μέτρα διοικητικής φύσεως, όπως απαγόρευση χρήσης Η/Υ και υπόσχεση για «καλή συμπεριφορά».[438]

5.4. Τα Χαρακτηριστικά του ηλεκτρονικο-οικονομικού εγκλήματος

Οι Newman Graeme & Clarke Roland εισήγαγαν το ακρωνύμιο SCAREM (Stealth, Challenge, Anonymity, Reconnaissance, Escape, Multiplicity) για να περιγράψουν τα χαρακτηριστικά του ηλεκτρονικού εγκλήματος στον τομέα του ηλεκτρονικού εμπορίου:

- **Απόκρυψη** (Stealth), το διαδίκτυο προσφέρει μεγαλύτερη δυνατότητα απόκρυψης της τέλεσης του εγκλήματος. Για παράδειγμα ο δράστης (hacker) μπορεί να μπει κρυφά στα αρχεία μιας τράπεζας, να πάρει αυτό που θέλει και να βγει χωρίς να αφήσει ίχνη.
- **Πρόκληση** (Challenge) για τους hackers να παραβιάσουν το σύστημα, ώστε να καυχώνται ότι το κατάφεραν.
- **Ανωνυμία** (Anonymity). Το διαδίκτυο προσφέρει τη δυνατότητα στο δράστη να διαφεύγει, εκμεταλλευόμενος τη διακριτικότητα και ανωνυμία που προσφέρουν οι ηλεκτρονικές επιχειρήσεις για συναλλαγές των πελατών τους.
- **Αναγνώριση**, η γνώση του κατάλληλου στόχου (Reconnaissance) από την καθημερινή ρουτίνα του δράστη. Ο δράστης μπορεί να εγκαταστήσει προγράμματα (spyware) παρακολούθησης των δραστηριοτήτων του στόχου του.
- **Διαφυγή** (Escape), η ικανότητα του δράστη να καλύπτει τα ίχνη του για να αποφύγει την σύλληψη χρησιμοποιώντας τις IP ή τον υπολογιστή κάποιου άλλου χρήστη, επιχείρησης ή πανεπιστημίου .
- **Πολλαπλότητα** (Multiplicity), δυνατότητα στον δράστη να πλήξει πολλούς στόχους ταυτόχρονα. Επίσης, η επιτυχής έκβαση κάποιας εγκληματικής δραστηριότητας του

[435] Ελληνίδης Χρίστος (2001), σ. 125
[436] Dreyfus Suelette (1998)
[437] Sieber Ulrich (1986), σ.17
[438] Hollinger Richard (1997b), σσ.50-51

δημιουργεί περισσότερες εγκληματικές ευκαιρίες, π.χ. η παραβίαση της βάσης δεδομένων μιας τράπεζας του δίνει τη δυνατότητα να πουλήσει ή να εκμεταλλευτεί ο ίδιος τα κλεμμένα στοιχεία πιστωτικών καρτών .[439]

Συνοψίζοντας τα γενικά χαρακτηριστικά που εμφανίζει το ηλεκτρονικό έγκλημα και συγκρίνοντάς τα με αυτά του οικονομικού εγκλήματος (συμπεριλαμβανομένου και του εγκλήματος λευκού περιλαιμίου) θα μπορούσαμε να επισημάνουμε πολλά κοινά μεταξύ τους.

Έτσι το ηλεκτρονικό – οικονομικό έγκλημα:

- Συχνά διαπράττεται στο πλαίσιο της νόμιμης απασχόλησης του δράστη από:

α) επιχειρήσεις εναντίον άλλων επιχειρήσεων (όπως η βιομηχανική κατασκοπία) για απόκτηση συγκριτικού πλεονεκτήματος.

β) υπαλλήλους μιας επιχείρησης στο πλαίσιο της νόμιμης απασχόλησης τους, όπου ο απασχολούμενος, καταχράται την ιδιότητα του ή εξ αφορμής της, εκτελεί την παράνομη πράξη.[440]

γ) τρίτους οι οποίοι αποκτούν μη εξουσιοδοτημένη πρόσβαση και διαπράττουν διάφορες πράξεις κακοχρησίας υπολογιστών.

- Η πράξη δεν στοχεύει κυρίως στη κάλυψη βιοτικών αναγκών επιβίωσης του δράστη, αλλά στην επίτευξη ανώτερου επίπεδου ανέσεως και ευμάρειας εναντίον του οικονομικού συμφέροντος των θυμάτων.
- Είναι έγκλημα που συνήθως διαπράττεται χωρίς τη χρήση φυσικής βίας, αποτελεί δηλαδή μια μορφή «αναίμακτου» εγκλήματος (αν εξαιρέσουμε τις περιπτώσεις τρομοκρατικών επιθέσεων και σοβαρών περιβαλλοντικών παραβιάσεων).
- Παρουσιάζει περιορισμένη θέαση, διάχυση της ευθύνης, διάχυση της θυματοποίησης (τα θύματα μπορεί να είναι άτομα, επιχειρήσεις, το κράτος ή το κοινωνικό σύνολο), δυσκολία ανίχνευσης, επιεικείς ποινές, ασαφή νομοθεσία.[441]
- Εμφανίζει μεγάλο «σκοτεινό αριθμό», συνήθως μεγαλύτερο από αυτόν του κοινού εγκλήματος.
- Οι δράστες του διαθέτουν υψηλό επίπεδο εκπαίδευσης ή ειδίκευσης στην πληροφορική τεχνολογία, ανήκουν στα μεσαία ή ανώτερα στρώματα, διαπράττουν τα εγκλήματα τους κυρίως κατά τη διάρκεια της επαγγελματικής τους ενασχόλησης.[442]
- Η διερεύνηση και δίωξη του από τις αρχές είναι πολύ δύσκολη και απαιτεί υψηλό επίπεδο εκπαίδευσης και εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις επίσης απαιτούνται και από όσους άλλους (εισαγγελείς, δικαστές, δικηγόρους, επιστήμονες) ασχολούνται με αυτή την μορφή εγκλήματος.
- Οι δράστες σε πολλές περιπτώσεις τυγχάνουν εξωδικαστικής αντιμετώπισης, π.χ. με διοικητικά μέτρα στο πλαίσιο των επιχειρήσεων.
- Ακόμα και οι περιπτώσεις των ηλεκτρονικών εγκλημάτων που προβλέπονται στο ποινικό δίκαιο αντιμετωπίζονται είτε από ήδη υπάρχουσες ρυθμίσεις που ισχύουν και για τα οικονομικά εγκλήματα είτε από ειδικά για το ηλεκτρονικό έγκλημα νομοθετήματα.

[439] Newman Graeme R. & Clarke Roland.V. (2003), σ.17
[440] Ιωαννίδης Χρίστος (2001), σ. 159
[441] βλ. σχετικά με τις δυσκολίες αντιμετώπισης.
[442] Δεν περιλαμβάνονται οι χάκερ οι οποίοι δεν έχουν οικονομικά κίνητρα.

- Εμφανίζει πολυπλοκότητα κατά την τέλεση του, απαιτεί γνώσεις, εμπειρία, εξοικείωση και πληροφορικό εξοπλισμό, καθιστώντας δύσκολη την τέλεση του από κάποιον που δεν διαθέτει τα παραπάνω «προσόντα» όπως θα μπορούσε να γίνει με τα εγκλήματα «του δρόμου».
- Το κόστος από τις απώλειες αλλά και για την αντιμετώπισή του είναι σημαντικά υψηλότερο από αυτό του κοινού εγκλήματος.
- Πολλά από τα σύγχρονα οικονομικά εγκλήματα (διαφόρων ειδών απάτες, ξέπλυμα χρήματος κλπ.) πλέον τελούνται με ή και απαιτούν τη σύμπραξη της πληροφορικής και ψηφιακής τεχνολογίας εφόσον το περιβάλλον στο οποίο διαδραματίζονται είναι πλέον ψηφιακό και δικτυακό.

Οι διαδικτυακές δραστηριότητες, όσον αφορά το είδος και τη συχνότητα, σύμφωνα με τις σχετικές έρευνες, φαίνεται να σχετίζονται με τον κίνδυνο θυματοποίησης. Η καθημερινή ενασχόληση με ριψοκίνδυνες δραστηριότητες στο διαδίκτυο, όπως το παράνομο κατέβασμα αρχείων κλπ. με παράλληλη έλλειψη μέτρων προστασίας της ταυτότητας του χρήστη αυξάνουν τον κίνδυνο θυματοποίησης.

5.5. Σχέση κυβερνο-εγκλήματος και οικονομικού εγκλήματος

Το έγκλημα στον κυβερνοχώρο, σύμφωνα με πολλούς μελετητές του αντικειμένου, αποτελεί μία ειδικότερη μορφή του εγκλήματος του «λευκού περιλαίμιου» (white-collar crime), αφού προϋποθέτει ιδιαίτερες ικανότητες, γνώσεις και επιδεξιότητα, όπως και τα απαραίτητα τεχνικά και οικονομικά μέσα. [443]

Έχει παρατηρηθεί ότι το έγκλημα λευκού περιλαιμίου αποτελεί μάλλον μια κοινωνική παρά νομική έννοια, η οποία αρχικά χρησιμοποιήθηκε όχι από δικηγόρους αλλά από κοινωνικούς επιστήμονες. Δεν υπάρχει καμία συγκεκριμένη παράβαση ή ομάδα παραβάσεων που μπορούν να προσδιοριστούν ως έγκλημα λευκού περιλαιμίου. Υπό αυτήν τη μορφή, το έγκλημα λευκού περιλαιμίου είναι μια έννοια με παρόμοιες δυσκολίες ορισμού με αυτή του κυβερνο-εγκλήματος.

Οι τεχνολογικές εξελίξεις κατά τη διάρκεια της τελευταίας δεκαετίας έχουν δημιουργήσει περαιτέρω περιπλοκές που περιβάλλουν τους τύπους προσώπων που είναι σε θέση να διαπράξουν το έγκλημα του λευκού περιλαιμίου. Ο δράστης μιας διαδικτυακής απάτης, παραδείγματος χάριν, μπορεί το ίδιο εύκολα να είναι ένας αυτοδίδακτος έφηβος που χρησιμοποιεί έναν προσωπικό υπολογιστή στο σπίτι όπως και ένας μορφωμένος επαγγελματίας στον εργασιακό του χώρο.

Η ουσία της έννοιας του εγκλήματος του λευκού περιλαιμίου, παραμένει εντούτοις στην κατάχρηση της εξουσίας και τη ρήξη της εμπιστοσύνης, περιλαμβάνοντας συνήθως την αναζήτηση του οικονομικού κέρδους ως κίνητρο. Μια απλή κατηγοριοποίηση διακρίνει τα εγκλήματα που διαπράττονται από συγκεκριμένους τύπους παραβατών, κυρίως επαγγελματίες και εργαζόμενους σε εταιρίες, από τα εγκλήματα που διαπράττονται με εξειδικευμένες μεθόδους, κυρίως οικονομικά αδικήματα που περιλαμβάνουν την εκλέπτυνση, τον προγραμματισμό και τη χρήση της τεχνολογίας κατά τη διάπραξη τους. [444]

Μεταξύ του κυβερνο-εγκλήματος (ηλεκτρονικό έγκλημα με χρήση δικτύων) και του οικονομικού εγκλήματος υφίσταται μια αλληλεξάρτηση η οποία δημιουργεί δύσκολα εννοιολογικά ερωτήματα. Αυτό οφείλεται εν μέρει επειδή τα περισσότερα εγκλήματα

[443] Σοφός Θεμιστοκλής (2014)

[444] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σσ. 27-30

ιδιοκτησίας που περιλαμβάνουν την απάτη ή την απιστία που έχουν διαπραχτεί τα τελευταία χρόνια εμπλέκουν τη χρήση των υπολογιστών, απλά επειδή οι σύγχρονες επιχειρήσεις στηρίζονται σε τόσο μεγάλο βαθμό στις ψηφιακές τεχνολογίες για λογιστική χρήση και για τη μεταφορά κεφαλαίων. Επιπλέον, μέρος του οικονομικού εγκλήματος αλληλεπικαλύπτεται με το έγκλημα του «λευκού περιλαιμίου», που διακρίνεται από τη σχετική εκλέπτυνσή του και το υπόβαθρο των δραστών του.

Το παρακάτω σχήμα των Smith R. & Grabosky P. παρέχει μια απεικόνιση της αλληλεξάρτησης μεταξύ των εννοιών του εγκλήματος του λευκού περιλαιμίου, του οικονομικού εγκλήματος και του κυβερνο-εγκλήματος.[445]

Σχήμα 5. Σχέση Οικονομικού – Ηλεκτρονικού εγκλήματος

Όπως μπορούμε να δούμε το κυβερνο- έγκλημα έχει κοινά σημεία τόσο με το έγκλημα λευκού περιλαιμίου όσο και με το οικονομικό έγκλημα. Μόνο ένα υποσύνολο των κυβερνο-εγκλημάτων δεν έχει κανένα οικονομικό χαρακτηριστικό από την άποψη του οικονομικού οφέλους που επιδιώκεται να προκύψει από τη δραστηριότητα. Σε αυτές περιλαμβάνονται οι περιπτώσεις της κυβερνο-παρενόχλησης και του κυβερνο-βανδαλισμού κατά τις οποίες χρησιμοποιούνται οι υπολογιστές για να πραγματοποιηθούν οι απειλές. Η διάδοση επιβλαβούς περιεχομένου συχνά έχει οικονομικά κίνητρα, όπως οι διαδικτυακές επιχειρήσεις που διαδίδουν παιδική πορνογραφία έναντι αμοιβής, ενώ άλλο περιεχόμενο όπως το ρατσιστικό υλικό γενικά δεν παρακινείται από οικονομικά κίνητρα. [446]

Έτσι, σε σχέση με το έγκλημα του λευκού περιλαιμίου, μπορούμε να διακρίνουμε το ηλεκτρονικό έγκλημα σε:

[445] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σσ. 27-30
[446] Smith Russell, Grabosky Peter & Urbas Gregor (2004), ό.π.

5.5.1. Ηλεκτρονικό έγκλημα που δεν αποτελεί μορφή του εγκλήματος λευκού περιλαιμίου.

Μεγάλο κομμάτι του ηλεκτρονικού εγκλήματος δεν μπορεί να συμπεριληφθεί στην έννοια του εγκλήματος λευκού περιλαιμίου που διαπράττεται από άτομα με υψηλό κύρος ή που εκμεταλλεύονται την επαγγελματική τους θέση.[447]

Από την άλλη πλευρά, δεν περιλαμβάνουν όλα τα εγκλήματα λευκού περιλαιμίου τη χρήση των ψηφιακών τεχνολογιών, αν και τον τελευταίο καιρό η μεγάλη πλειοψηφία το κάνει.

Το έγκλημα κατά της ιδιοκτησίας συχνά χρησιμοποιείται ως συνώνυμο του οικονομικού εγκλήματος. Κάποια προβλήματα εγείρονται σε σχέση με τα είδη της ιδιοκτησίας που προστατεύονται από το ποινικό δίκαιο. Ειδικότερα οι πληροφορίες, μέχρι σήμερα τουλάχιστον, θεωρούνται συνήθως έξω από το πεδίο της ποινικής προστασίας, αντί να εξετάζονται από μια σειρά νομοθετημάτων πνευματικής ιδιοκτησίας όπως τα πνευματικά δικαιώματα, τα διπλώματα ευρεσιτεχνίας, τα σχέδια και η προστασία εμπιστευτικών πληροφοριών. [448]

Οι πρώτοι ηλεκτρονικοί εγκληματίες ήταν κυρίως άτομα με τουλάχιστον υψηλή ειδίκευση και γνώση της ψηφιακής τεχνολογίας, δεν διέθεταν όμως υψηλό κύρος. Τα κοινωνικο-οικονομικά χαρακτηριστικά του δράστη δεν παίζουν τόσο σημαντικό ρόλο στις περισσότερες μορφές ηλεκτρονικού εγκλήματος ιδιαίτερα σε αυτό του κυβερνο-εγκλήματος. Ακόμα και νεαροί, όπως στην περίπτωση των χάκερ που αποτελούν σημαντικότατο κομμάτι του κυβερνοεγκλήματος, έχουν αποκτήσει εξειδικευμένες γνώσεις και δεξιότητες που ξεπερνούν ακόμα και επαγγελματίες του χώρου.

Το hacking λοιπόν αποτελεί την κατεξοχήν μορφή ηλεκτρονικού εγκλήματος που δεν αποτελεί μορφή του εγκλήματος λευκού περιλαιμίου.[449] Αυτό όμως δεν αποκλείει το γεγονός ότι το hacking αποτελεί «εργαλείο» για την τέλεση οικονομικών εγκλημάτων.

5.5.2. Ηλεκτρονικό έγκλημα που αποτελεί μορφή του εγκλήματος λευκού περιλαιμίου

Οι διάφορες μορφές απάτης ή τα οικονομικά εγκλήματα της απιστίας, έχουν κοινό τόπο με το έγκλημα λευκού περιλαιμίου, το οικονομικό έγκλημα και το κυβερνο-έγκλημα.

Τα πληροφορικά συστήματα γίνονται το κύριο εργαλείο για τη διάπραξη απάτης, φοροδιαφυγής, ακόμα και για επιθέσεις σε άλλες επιχειρήσεις με παράνομη πρόσβαση σε αρχεία και δίκτυα ή υποκλοπή επικοινωνιών για διενέργεια βιομηχανικής κατασκοπείας και άλλων παραβιάσεων.

Οργανισμοί και επιχειρήσεις χρησιμοποιούν τη σύγχρονη ψηφιακή τεχνολογία σαν εργαλείο εγκληματικών δραστηριοτήτων. Η πληροφορική τεχνολογία χρησιμοποιείται για την τήρηση οικονομικών στοιχείων, τιμολογίων, μισθολογικών στοιχείων των εργαζομένων και άλλων πληρωμών, οι επιχειρήσεις καθίστανται έτσι άμεσα εξαρτώμενες από αυτή.

Πλέον όχι μόνο οι επιχειρήσεις, οι οργανισμοί, τα υψηλόβαθμα στελέχη με υψηλό status, αλλά και απλοί εργαζόμενοι σε σύγχρονες επιχειρήσεις και οργανισμούς μπορούν να εκμεταλλεύονται τις εγκληματικές ευκαιρίες που προσφέρουν οι νέες τεχνολογίες.

[447] Grabosky Peter & Walkley Sascha (2007), σσ. 358-375
[448] Smith Russell, Grabosky Peter & Urbas Gregor (2004), ό.π.
[449] Grabosky Peter & Walkley Sascha, (2007), σσ. 358-375

Στις περιπτώσεις, όπως αυτές που ο ρόλος της είναι συμπτωματικός ή περιστασιακός για την τέλεση του εγκλήματος[450], η ψηφιακή τεχνολογία δημιουργεί έναν σημαντικά κοινό τόπο μεταξύ του ηλεκτρονικού και του οικονομικού εγκλήματος (ειδικά για τις περιπτώσεις των στελεχών που ενεργούν για λογαριασμό της επιχείρησης). Όλα σχεδόν τα αρχεία των επιχειρήσεων και οργανισμών καταχωρίζονται σε ψηφιακή μορφή, οπότε είναι φυσικό επακόλουθο το σύγχρονο επιχειρηματικό έγκλημα να λαμβάνει ψηφιακή μορφή και περιεχόμενο και συνιστά μια μεγάλης κλίμακας αλληλοεπικάλυψη του επιχειρησιακού εγκλήματος (του λευκού περιλαιμίου) με το ηλεκτρονικό. [451]

Μεγάλο μέρος των σύγχρονων οικονομικών εγκλημάτων με στόχο ή μέσο τον ηλεκτρονικό υπολογιστή, σύμφωνα με τον D.Parker, τελούνται από τους λεγόμενους insiders (εσωτερικούς ως προς την επιχείρηση) οι οποίοι διαθέτουν ιδιαίτερα προσόντα, γνώση, πρόσβαση, ευκαιρίες και δυνατότητες, αναπτύσσοντας εκλεπτυσμένες μεθόδους για να προκαλέσουν απώλειες πληροφοριακών δεδομένων στην επιχείρηση όπου εργάζονται ως έμπιστοι υπάλληλοι ή ανώτερα στελέχη.[452]

Η 6η Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα της PwC (Price Waterhouse Coopers) ως προς τους υπαιτίους του οικονομικού εγκλήματος για την Ελλάδα το 2011, αναφέρει ότι το 63% των στελεχών επιχειρήσεων που ρωτήθηκαν δήλωσαν ότι οι υπαίτιοι προέρχονταν μέσα από τον οργανισμό και το 31% ότι ήταν εκτός. Για τις απειλές που προέρχονται μέσα από τον οργανισμό, δήλωσαν ότι προέρχεται κυρίως από τα τμήματα Operations (39%) και Πληροφορικής (35%).[453]

Στις περιπτώσεις υπαλλήλων της επιχείρησης που διαπράττουν εγκλήματα αυτά μπορούν να είναι ψηφιακά ή παραδοσιακά, να τελούνται κατά την επαγγελματική τους ενασχόλησης αλλά να μη σχετίζονται κατ' ανάγκη άμεσα με αυτή. Υπάρχουν περιπτώσεις που οι εργαζόμενοι της επιχείρησης χρησιμοποιούν τα υπολογιστικά της συστήματα:

α) για να εξαπολύσουν επιθέσεις με ιούς ή να εισβάλλουν με παράνομη πρόσβαση σε δίκτυα άλλων οργανισμών, να παρενοχλήσουν άλλους στο διαδίκτυο, να κατεβάσουν ή να αποθηκεύσουν παράνομο υλικό.

β) περιπτώσεις που απλά η χρήση του διαδικτύου και των υπολογιστών της επιχείρησης από τους υπαλλήλους για δικό τους όφελος, όπως το άνοιγμα προσωπικών emails, η πλοήγηση στο διαδίκτυο κλπ. αποτελεί για αυτήν απώλεια εργατοωρών και της κοστίζει χρήματα.

Εκτός από τους εργαζόμενους στην επιχείρηση και τους χάκερ, είναι και οι επαγγελματίες εγκληματίες που πλέον εισέρχονται το πεδίο του ηλεκτρονικού εγκλήματος. Εφόσον το παραδοσιακό περιβάλλον στο οποίο δραστηριοποιούνται μετατρέπεται σε ηλεκτρονικό και αυτοματοποιημένο, αναγνωρίζουν πλέον και την δική τους ανάγκη για γνώση της πληροφορικής τεχνολογίας. Η πληροφορική δίνει τη δυνατότητα σε επαγγελματίες εγκληματίες και τα δίκτυα οργανωμένου εγκλήματος να καταστρώνουν ευρείας κλίμακας εγκληματικές επιχειρήσεις σε τομείς όπως λαθρεμπόριο ναρκωτικών, πορνεία, τζόγο και εκβιασμό.

[450] και που εξετάζονται σε άλλο σημείο.
[451] Grabosky Peter & Walkley Sascha (2007), ό.π.
[452] Parker Donn, (1987)
[453] Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014, βλ. και Πίνακα 9.

Η ανάπτυξη της πληροφορικής και των ψηφιακών τηλεπικοινωνιών έχει αποσυνδέσει την εγκληματική δραστηριότητα από την ανάγκη της γεωγραφικής εγγύτητας ως προς το στόχο. Έχει μάλιστα εκτιμηθεί ότι, ακριβώς λόγω των αλλαγών στις μορφές της πληροφορίας, τις μεθόδους και τους πόρους των εγκληματιών, ο συνολικός αριθμός περιστατικών επιχειρηματικού εγκλήματος θα μειωθεί κατά τα επόμενα χρόνια, ενώ το μέγεθος των απωλειών θα αυξηθεί δραματικά. Η πολυπλοκότητα της τεχνολογίας, η αυξανόμενη διάδοση και αποτελεσματικότητα των μέτρων ασφαλείας από τη μια και η αυξανόμενη ποσότητα, αλλά και η οικονομική αξία, των αποθηκευμένων σε πληροφοριακά συστήματα ψηφιακών, παρά γραπτών (σε χαρτί), δεδομένων από την άλλη, οδηγούν στην επαύξηση των ζημιών. Ο D. Parker εκτιμά ότι παράλληλα θα είναι ολοένα και λιγότερα τα άτομα που θα έχουν τη δυνατότητα διάπραξης τέτοιων εγκλημάτων, επειδή θα απαιτούνται ιδιαίτερα προσόντα[454], γνώσεις, πληροφορίες, πρόσβαση και πόροι. [455]

5.5.3. Συμπεράσματα για τη σχέση ηλεκτρονικού και οικονομικού εγκλήματος

Βλέπουμε λοιπόν ότι το ηλεκτρονικό έγκλημα παρουσιάζει πολλά κοινά χαρακτηριστικά στοιχεία, με το οικονομικό έγκλημα και ειδικότερα το αποκαλούμενο έγκλημα του Λευκού περιλαιμίου. Τα σημαντικότερα από αυτά τα κοινά χαρακτηριστικά, που συγκροτούν και το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος, συνοψίζονται στο ότι και τα δυο είδη εγκλήματος διαπράττονται χωρίς τη χρήση βίας, με προσπάθεια εξαπάτησης ή απόκρυψης της νόμιμης φύσης της δράσης, στο πλαίσιο μιας κατά τα άλλα νόμιμης ενασχόλησης (στην εργασία ή τον ελεύθερο χρόνο), την οποία ο δράστης εκμεταλλεύεται δρώντας παρασιτικά.[456]

Η συνέργεια του οικονομικού με το ηλεκτρονικό στοιχείο του εγκλήματος είναι σε βαθμό τέτοιο που συχνά δεν μπορούμε να διακρίνουμε αν πρόκειται για απλό οικονομικό ή απλό ηλεκτρονικό έγκλημα οπότε και μιλάμε για «ηλεκτρονικο-οικονομικό» έγκλημα.

[454] Παράβλ. με απόψεις όπως του Grabosky για *εκδημοκρατισμό* του διαδικτύου.
[455] Parker Donn (1987)
[456] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), ό.π.

ΚΕΦΑΛΑΙΟ 6. ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

Τα εγκλήματα σε σχέση με την ψηφιακή τεχνολογία έχουν λάβει διάφορες ονομασίες και κατηγοριοποιηθεί σε διάφορες μορφές από τους μελετητές που έχουν ασχοληθεί τα τελευταία χρόνια με αυτό το είδος εγκληματικής συμπεριφοράς. Ανάμεσα στις ονομασίες βρίσκονται: «έγκλημα υπολογιστών» ή «πληροφορικής» (computer crime), «έγκλημα σχετικό με υπολογιστές» (computer-related crime), «κυβερνοέγκλημα» (cybercrime), «έγκλημα υψηλής τεχνολογίας» (high-tech crime), «διαδικτυακό έγκλημα» (internet crime), «ηλεκτρονικό έγκλημα» (electronic crime), «έγκλημα δικτύων» (netcrime) κλπ.

6.1. Είδη ηλεκτρονικο-οικονομικών εγκλημάτων

Ανεξάρτητα με το πώς προτιμά κανείς να το ονομάζει, οι κυριότερες μορφές που προτείνονται από τους περισσότερους μελετητές του εγκλήματος της ψηφιακής τεχνολογίας, ανάμεσα σε αυτούς και ο ειδικός σε τέτοια εγκλήματα P. Grabosky, εντάσσονται σε μια από τις παρακάτω κατηγορίες.

Εγκλήματα ή αδικήματα που η σύγχρονη τεχνολογία αποτελεί:

1. **Το εργαλείο** του εγκλήματος, όταν ο υπολογιστής ή το δίκτυο χρησιμοποιείται ως το **μέσο** για την τέλεσή του.

Εγκλήματα όπως τα παραδοσιακά μπορούν να τελεστούν με διάφορα μέσα. Μια κατάχρηση, για παράδειγμα μπορεί να γίνει και με παραδοσιακά μέσα, χωρίς τη χρήση σύγχρονης τεχνολογίας, αλλά θα πραγματοποιούνταν με διαφορετικό τρόπο.[457]

Τα πληροφορικά ή άλλα ψηφιακά συστήματα μπορούν να χρησιμοποιούνται ως εργαλεία που διευκολύνουν την τέλεση παραδοσιακών εγκλημάτων όπως η διάδοση πορνογραφικού υλικού, διάφορες απάτες (όπως οι «νιγηριανές» κλπ.), διαδικτυακές δημοπρασίες, πλαστογραφίες, παρενοχλήσεις κλπ. που θα μπορούσαν να τελεστούν και χωρίς τη χρήση της ψηφιακής τεχνολογίας, όμως με αυτήν μπορούν να τελούνται σε πολύ ευρύτερο χώρο, σε λιγότερο χρόνο, με μεγαλύτερη ευκολία και σχετική ανωνυμία. [458]

Διαδεδομένη πλέον είναι η χρήση των ψηφιακών δικτύων και τεχνολογίας από διάφορους εγκληματίες όπως εγκληματίες με λευκό περιλαίμιο, ψηφιακούς απατεώνες που καταχρώνται την εμπιστοσύνη (con artists), χάκερ (hackers), ή κράκερ (crackers). [459]

Οι εγκληματίες λευκού περιλαιμίου, ιδιαίτερα ως εσωτερικοί μιας επιχείρησης χρησιμοποιούν την ψηφιακή τεχνολογία ως μέσο για διάφορα εγκλήματα όπως:

α) Αλλαγή των ηλεκτρονικών αρχείων με σκοπό την αύξηση μισθού, την αλλοίωση αρνητικής αξιολόγησης του υπαλλήλου, αλλοίωση των λογιστικών βιβλίων ή των οικονομικών απολογισμών για την παραπλάνηση επενδυτών, πελατών, της εφορίας ή για την κάλυψη άλλων εγκλημάτων.

β) Πρόσβαση σε πληροφορίες εκ των έσω για αγορά μετοχών, πώληση των πληροφοριών σε τρίτους ή χρήση αυτών για εκβιασμό.

γ) Χειραγώγηση ηλεκτρονικών λογαριασμών της επιχείρησης ή πελατών της για όφελος τους.[460]

[457] Shinder Debra Littlejohn, Tittel (2002), σ. 120
[458] Βλ. Grabosky Peter & Walkley Sascha (2007), σσ. 364-375 και Shinder Debra Littlejohn (2002), σ. 120
[459] Shinder Debra Littlejohn (2002), σ. 120
[460] Shinder Debra Littlejohn (2002), σ. 120

2. Ο **στόχος** του εγκλήματος.

Τα πληροφορικά συστήματα, τα ηλεκτρονικά αρχεία και δεδομένα επιχειρήσεων και οργανισμών μπορούν να αποτελούν στόχο με καταστροφικές για αυτές συνέπειες επειδή γίνονται ολοένα και πιο εξαρτώμενες από την ψηφιακή τεχνολογία. Οι κάθε είδους επιθέσεις από hackers, crackers ή κυβερνο-τρομοκράτες που έχουν σκοπό την κλοπή, την αλλοίωση ή την καταστροφή των ιστοσελίδων, των δικτύων, των αρχείων και άλλων ευαίσθητων δεδομένων των επιχειρήσεων, κρατικών ή άλλων οργανισμών απαιτούν τη χρήση της ψηφιακής τεχνολογίας. [461]

Μορφές ηλεκτρονικο-οικονομικού εγκλήματος, δηλαδή οικονομικά εγκλήματα που σχετίζονται άμεσα με τον ηλεκτρονικό υπολογιστή ως στόχο, συνιστούν:

- Η παραποίηση, διαγραφή ή καταστροφή στοιχείων (προγραμμάτων ή αρχείων) που βρίσκονται αποθηκευμένα στον ηλεκτρονικό υπολογιστή.
- Μη εξουσιοδοτημένη χρήση του ηλεκτρονικού υπολογιστή τρίτου (κλοπή χρήσης ή χρόνου).
- Κατασκοπεία του ηλεκτρονικού υπολογιστή.
- Το σαμποτάζ του ηλεκτρονικού υπολογιστή όπως μερική ή ολική αχρήστευση του ηλεκτρονικού υπολογιστή τρίτου.[462]

3. «**Περιστασιακή»** και απλά διευκολύνει την τέλεση του παραδοσιακού εγκλήματος.

Η ψηφιακή τεχνολογία εκτός από άμεσο μπορεί να διαδραματίζει και έμμεσο ρόλο στη διευκόλυνση των εγκλημάτων. Όλα τα αρχεία όπως τα οικονομικά αρχεία, τα λογιστικά βιβλία κλπ. των σύγχρονων επιχειρήσεων τηρούνται σχεδόν αποκλειστικά σε ψηφιακή μορφή, οι επικοινωνίες για τις συνεννοήσεις μεταξύ των εγκληματικών οργανώσεων, τρομοκρατών, δουλεμπόρων, διακινητών παράνομων υλικών, προϊόντων, φαρμάκων, κλπ. γίνονται με τη χρήση της ψηφιακής τεχνολογίας εκμεταλλευόμενα τις δυνατότητες κρυπτογράφησης και ανωνυμίας που αυτή μπορεί να προσφέρει. Στις περιπτώσεις αυτές ο ρόλος της ψηφιακής τεχνολογίας είναι συμπτωματικός ή περιστασιακός για την τέλεση του εγκλήματος. [463]

Στην έκθεση του, που ονομάστηκε Computer abuse, ο Parker ανέφερε ότι οι υπολογιστές, κατά την κατάχρηση και την κακή χρήση τους, διαδραματίζουν έναν ή περισσότερους από τους παρακάτω τέσσερις **ρόλους**[464]. Ο υπολογιστής ως:

1. Το **αντικείμενο** (object) των επιθέσεων. Οι υπολογιστές μπορούν εύκολα να αποτελούν στόχο επιθέσεων, γιατί μπορούν να κλαπούν ή να καταστραφούν πολύτιμα προγράμματα που βρίσκονται μέσα σε αυτούς ή ακόμα και οι ίδιοι οι υπολογιστές με πράξεις βανδαλισμού ή δολιοφθοράς. Έχουν αναφερθεί ακόμα και περιπτώσεις που υπολογιστές έχουν βληθεί με όπλα.
2. Το **υποκείμενο** (subject). Όταν ο υπολογιστής αποτελεί το περιβάλλον στο οποίο διεξάγονται πράξεις χωρίς εξουσιοδότηση, όπως οι επιθέσεις από ιούς και «δούρειους ίππους»[465]. Ακόμα ο υπολογιστής παρέχει το περιβάλλον για τη διάπραξη παραδοσιακών εγκλημάτων, όπως απάτη, κλοπή, κατάχρηση, εκβιασμό, δολιοφθορά κλπ.

[461] Βλ. Grabosky Peter & Walkley Sascha (2007), σσ. 364-375 και Shinder Debra Littlejohn, Tittel Ed (2002), σ. 120
[462] Δημόπουλος Χαράλαμπος (1988), σσ. 100-102
[463] Βλ. Grabosky Peter & Walkley Sascha (2007), σσ. 364-375 και Shinder Debra Littlejohn, Tittel Ed, (2002), σ. 120
[464] Βλ. Parker Donn (1997), σσ.23-33 και Parker Donn (2000)
[465] Parker Donn. (2007), ό.π.

3. Το **Εργαλείο** δηλαδή το μέσο που χρησιμοποιείται για το σχεδιασμό, την ανάπτυξη, τον έλεγχο και την εκτέλεση των επιθέσεων. Για παράδειγμα αντί να χρησιμοποιηθεί ένα όπλο για μια ληστεία, χρησιμοποιείται ο υπολογιστής για τη παράνομη μεταφορά χρημάτων από το λογαριασμό ενός τρίτου.
4. **Σύμβολο** που χρησιμοποιείται για εκφοβισμό ή εξαπάτηση. Ο τέταρτος αυτός ρόλος τονίζει τη συμβολική σημασία του υπολογιστή για τη διάπραξη κάποιων μορφών επενδυτικής απάτης. Οι υπολογιστές παρέχουν στους απατεώνες έναν αέρα αξιοπιστίας και χρησιμοποιούνται συχνά για να εξαπατήσουν τα θύματα τους με επενδυτικά σχήματα και πυραμίδες. Πολλοί άνθρωποι τείνουν να πιστεύουν ως αληθή τα εξερχόμενα από υπολογιστή δεδομένα, στοιχείο που εκμεταλλεύονται οι απατεώνες. Για παράδειγμα ένας μεσίτης από τη Φλώριδα διέπραξε το 1981 μια απάτη 50 εκατομμυρίων δολαρίων πείθοντας τους πελάτες του ότι διέθετε έναν μεγάλο υπολογιστή και ένα μυστικό λογισμικό που του επέτρεπαν να συμμετέχει επιτυχώς σε ογκώδεις εμπορικές συναλλαγές. Στην πραγματικότητα, ο μόνος υπολογιστής που είχε ήταν ένα PC που χρησιμοποίησε για την αποστολή των παραπλανητικών επενδυτικών αναφορών στους πελάτες του. Άλλοτε πάλι ο υπολογιστής μπορεί να χρησιμοποιείται ως άλλοθι για τη διάπραξη του λάθους.[466]

Τα κοινά εγκλήματα υπολογιστών σύμφωνα με τον Donn Parker, περιλαμβάνουν:

Απάτη με κινητά τηλέφωνα (Cellular telephone fraud)
Αλλοίωση δεδομένων (Data alteration)
Καταστροφή και δολιοφθορά δεδομένων (Data destruction and sabotage)
Εκβιασμός για δεδομένα (Data extortion)
Κλοπή δεδομένων (Data theft)
Πλαστογραφία επιφάνειας εργασίας υπολογιστών (Desktop counterfeiting)
Κοινοποίηση των εμπιστευτικών στοιχείων (Disclosure of confidential data)
Βομβαρδισμός ηλεκτρονικών επιστολών (Electronic letter bombing)
Κλοπή ταυτότητας (Identity theft)
Καταναλωτική απάτη μέσω Διαδικτύου (Internet consumer fraud)
Απάτη μέσω PBX[467](PBX -Private Branch Exchange), είδος τηλεφωνικής απάτης όπου οι εισβολείς προσβάλλουν τηλεφωνικά κέντρα και αυτόματους τηλεφωνητές επιχειρήσεων για να πραγματοποιήσουν κλήσεις παράνομα[468].
Ανάγνωση ηλεκτρονικού ταχυδρομείου τρίτου χωρίς άδεια (Reading another person's e-mail without permission)
Πώληση ιδιόκτητων δεδομένων (Sale of proprietary data)
Πειρατεία λογισμικού (Software piracy)
Κλοπή υπεραστικών τηλεπικοινωνιακών καρτών (Stolen long-distance calling cards)
Αναρμόδια πρόσβαση και είσοδος σε συστήματα και πληροφορίες (Unauthorised access and entry to systems and information)
Απάτη υπηρεσίας προσωπικού τηλεφωνητή (Voice mail fraud).[469]

[466] Parker Donn, (2007), ό.π.
[467] Μόντεμ για εσωτερικά τηλεφωνικά δίκτυα.
[468] Βλ. http://www.rogers.com/business/mb/en/smallbusiness/shop/phone/fraudpbx
[469] Βλ. Watson Business Systems (2014) αναφορά σε Parker Donn (2000) και CSI/FBI (2006).

Η **Ευρωπαϊκή Σύμβαση** για το κυβερνο-έγκλημα στη Βουδαπέστη κάνει την διάκριση για τα εγκλήματα υπολογιστών. Οι παρακάτω μορφές εγκλημάτων κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών καθορίστηκαν και προσυπογράφηκαν από τα κράτη μέλη που έλαβαν μέρος στην σύνταξη της Σύμβασης για τον κυβερνοχώρο την 23-11-2001 στην Βουδαπέστη. Σύμφωνα με την Σύμβαση κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα για να καθιερώσει ως ποινικά αδικήματα τις συμπεριφορές που διέκρινε στις εξής κύριες κατηγορίες:

Α. Εγκλήματα ενάντια στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των **δεδομένων** υπολογιστών και των συστημάτων υπολογιστών. Η κατηγορία αυτή περιλαμβάνει τις υποκατηγορίες:

1) Παράνομη πρόσβαση (Illegal Access -hacking)
2) Αθέμιτη παγίδευση-Υποκλοπή (illegal interception)
3) Επέμβαση σε δεδομένα (Data interference)
4) Επέμβαση σε σύστημα (System Interference)
5) Κακή χρήση συσκευών (misuse of devises)

Β. Παραδοσιακά εγκλήματα που διαπράττονται με τη βοήθεια υπολογιστή (Computer-related offences), όπως πλαστογραφία και απάτη μέσω υπολογιστή.

Γ. Εγκλήματα σχετικά με το περιεχόμενο, όπως η παραγωγή, διακίνηση, απόκτηση και κατοχή περιεχομένου παιδικής πορνογραφίας.

Δ. Παραβάσεις σχετικές με πνευματικά δικαιώματα και πνευματική ιδιοκτησία που τελούνται μέσω υπολογιστή. [470]

Αυτή η διάκριση θα μπορούσε να είναι η πιο κατάλληλη ή τουλάχιστον η πιο αποδεκτή από όσους εμπλέκονται στη μελέτη του εγκλήματος υπολογιστών επειδή καλύπτει όλα τα σχετικά είδη εγκληματικών ενεργειών. Οι εσωτερικοί νόμοι, οι διαδικαστικοί κώδικες για τις επιχειρησιακές δραστηριότητες όμως διατηρούν την ισχύ τους και διαφέρουν ανάμεσα στις διάφορες ευρωπαϊκές χώρες. Στοιχεία που θα ήταν αποδεκτά ως αποδεικτικά του εγκλήματος σε μια χώρα μπορεί να μην γίνονται αποδεκτά σε μια άλλη, πράγμα που συνιστά ακόμα έναν ιδιαίτερο περιορισμό.

Ο ΟΟΣΑ διακρίνει πέντε κατηγορίες ηλεκτρονικού (σχετιζόμενου με υπολογιστές) εγκλήματος, με κριτήριο τη (σκόπιμη) συμπεριφορά από πλευράς παραβάτη:

1. Η χωρίς εξουσιοδότηση εισαγωγή ή αλλαγή ή καταστροφή δεδομένων σε έναν υπολογιστή.
2. Η αλλοίωση ή μείωση της αξιοπιστίας των δεδομένων του υπολογιστικού συστήματος.
3. Η χωρίς εξουσιοδότηση είσοδος σε συστήματα υπολογιστών και κλοπή ή αντιγραφή δεδομένων
4. Η παρεμπόδιση της ομαλής λειτουργίας συστημάτων υπολογιστών ή τηλεπικοινωνιών
5. Παραβίαση των δικαιωμάτων ιδιοκτησίας ηλεκτρονικού υλικού.[471]

Ο Wasik κάνει διπλή κατηγοριοποίηση του ηλεκτρονικού εγκλήματος.

Α. Με κριτήριο τη σκοπιμότητα της συμπεριφοράς τα εγκλήματα που σχετίζονται με υπολογιστές διακρίνονται:

1. Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή, π.χ. το hacking
2. Απάτη και κλοπή υπηρεσιών

[470] Convention on Cybercrime, Budapest, 23.XI.(2001)

[471] Λάζος Γρηγόρης (2001), σσ. 51-52

3. Συνδεδεμένες παραβάσεις, όπως φθορά ή καταστροφή, εκβιασμός κλπ.

Β. Με κριτήριο τον δράστη διακρίνει:

1. Το επιχειρηματικό πληροφορικό έγκλημα, όταν ο δράστης ανήκει στα διοικητικά στελέχη της επιχείρησης
2. Πληροφορικό έγκλημα που διαπράττεται από υπαλλήλους της επιχείρησης εναντίον των συμφερόντων της.
3. Κακοχρησία υπολογιστών από τρίτους.[472]

Σύμφωνα με τον Walden το Κυβερνο-έγκλημα (Cybercrime), διακρίνεται σε τρεις ευρύτερες κατηγορίες δραστηριότητας.

Πρώτον, τα σχετικά με υπολογιστή κυβερνο-εγκλήματα, όπως η απάτη και η κλοπή, όπου οι υπολογιστές είναι απλά τα εργαλεία για το έγκλημα, χειραγωγώντας τα δεδομένα για τη διάπραξη παραδοσιακών εγκληματικών δραστηριοτήτων.

Δεύτερον, κυβερνο-εγκλήματα σε σχέση με το περιεχόμενο, όπως η παραβίαση πνευματικών δικαιωμάτων και η παιδική πορνογραφία, όπου οι τεχνολογίες υπολογιστών και επικοινωνιών διευκολύνουν τη διανομή των παράνομων στοιχείων.

Η τρίτη κατηγορία περιλαμβάνει εκείνες τις δραστηριότητες όπου η πρόθεση είναι να προσβληθεί η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των υπολογιστών και των συστημάτων που συνδέονται με το Διαδίκτυο όπως και τα δεδομένα που υποβάλλονται για επεξεργασία σε αυτά, όπως το hacking και η διανομή ιών. [473]

Ο U. Sieber, με αφορμή τον ορισμό του ΟΟΣΑ[474], θέτει ως κριτήριο κατηγοριοποίησης το προστατευόμενο αγαθό που απειλείται και προτείνει την εξής διάκριση για το έγκλημα υπολογιστών:

α) Οικονομικά εγκλήματα σχετιζόμενα με υπολογιστές. Π.χ. απάτη, κατασκοπεία υπολογιστών, δολιοφθορά υπολογιστών.

β) **Προσβολές κατά των ατομικών δικαιωμάτων** μέσω υπολογιστών, όπως το δικαίωμα της ιδιωτικότητας του πολίτη.

γ) **Προσβολές κατά των υπερατομικών συμφερόντων** μέσω υπολογιστών, όπως προσβολές κατά την εθνικής ασφάλειας, τον έλεγχο της διασυνοριακής κίνησης δεδομένων, την ακεραιότητα των υπολογιστικών διαδικασιών και δεδομένων και δικτύων επικοινωνίας και τη νομιμοποίηση των αποφάσεων του κοινοβουλίου που σχετίζονται με υπολογιστές.

Τα οικονομικά εγκλήματα που τελούνται με υπολογιστές, παρουσιάζονται σύμφωνα με τον Sieber, ως το κύριο πεδίο των εγκλημάτων πληροφορικής και διακρίνονται έξι κύριες κατηγορίες τους:

- Απάτη εναντίον υπολογιστικών συστημάτων με χειραγώγηση υπολογιστή
- Κατασκοπεία υπολογιστών και κλοπή λογισμικού
- Δολιοφθορά υπολογιστών
- Κλοπή υπηρεσιών
- Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα
- Παραδοσιακά επιχειρησιακά εγκλήματα
- Εγκλήματα (business offences) που διευκολύνονται από υπολογιστικά συστήματα επεξεργασίας δεδομένων.[475]

[472] Λάζος Γρηγόρης (2001)., σ. 53
[473] Walden Ian (2003)
[474] Βλ. παραπάνω
[475] Sieber Ulrich (1986), σ.3

Αντίστοιχα με τις δυο κατηγορίες εγκλημάτων λευκού περιλαιμίου που διέκριναν οι Clinard και Quinney[476], έχουμε σύμφωνα με τον Wasik, τρεις τύπους πληροφορικού - οικονομικού εγκλήματος:

1. Εγκλήματα της επιχείρησης. Διαπράττονται από υπεύθυνους της επιχείρησης ή την ίδια εναντίον άλλης επιχείρησης για όφελος της. Μορφές τέτοιων εγκλημάτων αποτελούν η Βιομηχανική κατασκοπία, τα εγκλήματα κατά του κοινού ή του κράτους όπως οι εικονικές συναλλαγές από ασφαλιστικές εταιρείες μέσω προγράμματος.

2. Εγκλήματα εργασίας (insiders). Διαπράττονται από εργαζόμενους σε βάρος των εργοδοτών τους κατά την απασχόλησή τους και αφορά κλοπή hardware ή software, απάτη μέσω Η/Υ, κλοπή υπηρεσιών Η/Υ, hacking κ.ά.

3. Εξωτερικοί προς την επιχείρηση εγκληματίες (outsiders). Τέτοια περίπτωση αποτελεί η μη εξουσιοδοτημένη πρόσβαση (Hacking) με σκοπό την ανακάλυψη εμπιστευτικού υλικού, τη διάπραξη απάτης, τη πρόκληση ζημιάς σε προγράμματα ή δεδομένα.[477]

Όπως συμβαίνει και με το οικονομικό έγκλημα, ο «γνωστός αριθμός» του πληροφορικού εγκλήματος από επιχειρήσεις είναι πολύ μικρός, με ελάχιστες καταγγελίες και ακόμα πιο λίγες καταδικαστικές αποφάσεις για επιχειρήσεις. Περισσότερες είναι οι αντίστοιχες περιπτώσεις για εγκλήματα εργασίας από insiders και outsiders.

Μέχρι τις αρχές ΄90 τα 4 στα 5 τέτοια εγκλήματα ήταν από insiders και το ένα από outsiders ή σύμφωνα με το FBI το 71% διαπράττεται από insiders.[478] Η πρόβλεψη του Kovacich είναι ότι η αναλογία αυτή θα εξισορροπηθεί - υπέρ των outsiders – στις αρχές του 21ου αιώνα.[479]

Σύμφωνα και με μια άλλη μέτρηση, στο χώρο της τηλεπικοινωνιακής απάτης το 30% των απειλών προέρχεται από το εξωτερικό περιβάλλον της εταιρείας, ενώ για το 70% υπαίτιοι είναι οι ίδιοι οι εργαζόμενοι στην επιχείρηση.[480]

Εκτός των παραπάνω, έχουν κατά καιρούς προταθεί πολλά ακόμα ταξινομικά σχήματα, όπως αυτά των St.Shakelford, Sc.Charney, B.Hurewitz και Allen Lo[481] τα οποία παρουσιάζουν κοινά χαρακτηριστικά τόσο μεταξύ τους όσο και – κυρίως – με αυτό που αρχικά είχε προτείνει ο πρωτοπόρος σε αυτές τις μελέτες D.Parker, που εξετάσαμε παραπάνω.

Γενικά οι προσεγγίσεις που χρησιμοποιούνται για να ταξινομήσουν και να περιγράψουν τις απειλές από τις εγκληματικές ομάδες μέσω του Διαδικτύου ακολουθούν την ίδια μέθοδο κατηγοριοποίησης με αυτή του εγκλήματος υψηλής τεχνολογίας: «κάθετες και οριζόντιες χρήσεις της υψηλής τεχνολογίας».

Η κάθετη χρήση της υψηλής τεχνολογίας εμφανίζεται όταν ο υπολογιστής (ή δίκτυο υπολογιστών) είναι ο τελικός στόχος της εγκληματικής δραστηριότητας. Εγκλήματα όπως το hacking (άρνηση υπηρεσιών, Botnets, Zombies[482] κλπ), το επιβλαβές λογισμικό (ιοί, σκουλήκια, Δούρειοι Ίπποι), το Spamming, εκβιασμοί, κυβερνο-παρενόχληση κλπ. αποτελούν παραδείγματα στα οποία η παρουσία της μηχανής είναι θεμελιώδης για την ύπαρξη του εγκλήματος.

[476] Βλ. παραπάνω για τις δυο κατηγορίες εγκλημάτων λευκού περιλαιμίου.
[477] Λάζος Γρηγόρης (2001), σσ. 59-60
[478] Καϊτσάς Δημήτρης (2004), σ.77
[479] Λάζος Γρηγόρης (2001), ό,π., σσ. 56 -60
[480] Κωνσταντινόπουλος Γιώργος (2008) (αντιπρόεδρος του Ελληνικού Φορέα Πρόληψης Τηλεπικοινωνιακής Απάτης Ε.Φ.Τ.Α.)
[481] Λάζος Γρηγόρης (2001), σ. 51
[482] βλ. παρακάτω για Botnets και Zombies: *Μη εξουσιοδοτημένη πρόσβαση - Παραβίαση δεδομένων (Hacking)*

Η οριζόντια χρήση της υψηλής τεχνολογίας είναι όταν ο υπολογιστής χρησιμοποιείται ως εργαλείο προκειμένου να διευκολυνθούν στόχοι των εγκληματιών. Τέτοια εγκλήματα είναι: Ηλεκτρονικές απάτες, Ξέπλυμα μαύρου χρήματος, παιδική πορνογραφία, κυβερνο-τρομοκρατία, phishing, Κλοπή ταυτότητας- χρήση κλεμμένων πιστωτικών καρτών, πειρατεία λογισμικού, διακίνηση φαρμάκων, εκβιασμοί, κλπ.[483]

Τα κοινά στοιχεία στις διάφορες κατηγοριοποιήσεις για τα εγκλήματα υπολογιστών συνοψίζονται στο ότι ο υπολογιστής αποτελεί:

- το *στόχο* ή το αντικείμενο,
- το *μέσο* (εργαλείο),
- το *υποκείμενο* ή το περιβάλλον της προσβολής.

Παρακάτω διακρίνονται τα «καθαρά» ηλεκτρονικά εγκλήματα από τα εγκλήματα που απλά διευκολύνονται ως προς την τέλεση τους από την ψηφιακή τεχνολογία και είναι οικονομικής κυρίως φύσεως. Τα πρώτα αποτελούν παράνομες ή κακόβουλες πράξεις που δεν θα μπορούσαν να τελεστούν, με την ίδια μορφή ή έκταση συνεπειών στο πραγματικό - έξω από τον κυβερνοχώρο - περιβάλλον, σε πολλές περιπτώσεις όμως αποτελούν «προαπαιτούμενα» για την τέλεση ηλεκτρονικο-οικονομικού αδικήματος. Τα δεύτερα υπήρχαν ως μορφή παραβατικής δραστηριότητας και πριν την εμφάνιση του παγκόσμιου ιστού, αλλά πλέον διαπράττονται ως επί το πλείστον μέσω αυτού και τα περισσότερα από αυτά συνιστούν μορφή ηλεκτρονικο-οικονομικού εγκλήματος.

6.2. Τα είδη ηλεκτρονικού εγκλήματος όπου ο υπολογιστής αποτελεί στόχο

Συχνά τα καθαρά ηλεκτρονικά εγκλήματα αποτελούν «προαπαιτούμενα», εργαλεία για τα ηλεκτρονικά εγκλήματα οικονομικής φύσης, π.χ. το hacking σε προσωπικά δεδομένα που γίνεται για να χρησιμοποιηθούν σε απάτη με πιστωτικές κάρτες ή τραπεζικούς λογαριασμούς κλπ. Για το λόγο αυτό εξετάζονται παρακάτω οι μορφές του καθαρού κυβερνο-εγκλήματος σε σχέση με αυτές του οικονομικού.

6.2.1 Κυβερνο-βανδαλισμός ή ηλεκτρονικός βανδαλισμός

Ως «βανδαλισμός» σε ηλεκτρονικά συστήματα θεωρείται από τους Grabosky και Smith «η μη εξουσιοδοτημένη είσοδος (εισβολή) σε ένα υπολογιστή ή δίκτυο υπολογιστών με στόχο τη διατάραξη την ομαλής λειτουργίας του, την πρόκληση ζημιάς στον υπολογιστή ή τα δεδομένα του»[484].

Μορφές του κυβερνο-βανδαλισμού αποτελούν το hacking και η διάδοση ιών που εξετάζουμε αμέσως παρακάτω.

Αρχικά οι κυβερνο-βάνδαλοι κάνουν απλό hacking στους ιστοχώρους και έπειτα επεμβαίνουν αλλοιώνοντας στοιχεία τους με τρόπο που μπορεί μερικές φορές να είναι χιουμοριστικός, αλλά συχνά μπορεί να είναι και κακόβουλος ή ακόμα και πολιτικά παρακινούμενος.[485]

Οι Grabosky και Smith διακρίνουν τρεις βασικές μορφές ηλεκτρονικού βανδαλισμού. Η πρώτη περιλαμβάνει τη διαγραφή αρχείων και δεδομένων, η δεύτερη την κρυπτογράφηση των αρχείων με σκοπό την παρεμπόδιση της πρόσβασης τους και η τρίτη μορφή αφορά την

[483] http://www.europol.europa.eu/publications/Serious_Crime_Overviews /HTCThreatAssessment2007.pdf
[484] Grabosky Peter N & Russell Smith (1998), σ.47
[485] Burden Kit & Palmer Creole, ό.π.

υπερφόρτωση του συστήματος ώστε να καθυστερεί ή να καταρρέει η λειτουργία του μειώνοντας ή ακόμα και εξουδετερώνοντας έτσι τις δυνατότητες του.

Συχνά θύματα τέτοιων επιθέσεων είναι τα αμυντικά συστήματα χωρών, όπως των ΗΠΑ και τα υπολογιστικά συστήματα πανεπιστημίων από καταρτισμένους νεαρούς.[486]

6.2.2 Μη εξουσιοδοτημένη πρόσβαση - Παραβίαση δεδομένων (Hacking)

Το αρχέτυπο του ψηφιακού εγκληματία αποτελεί ο χάκερ που χρησιμοποιεί την τεχνολογία για να αποκτήσει -μη εξουσιοδοτημένη- πρόσβαση σε ιδιωτικά συστήματα υπολογιστών, συχνά με σκοπό να οικειοποιηθεί εμπιστευτικές πληροφορίες τις οποίες μπορεί να πουλήσει σε ανταγωνιστικές επιχειρήσεις, να αποκτήσει προσωπικό όφελος για να κλέψει, εκβιάσει ή να διαπράξει κάποιο άλλο είδος απάτης.[487]

Τέτοιο παράδειγμα χάκερ, Έλληνα μάλιστα, αποτελεί η περίπτωση ηλεκτρονικής βιομηχανικής κατασκοπείας, που διενεργήθηκε το 2002 από 58χρονο Έλληνα με συνεργάτη στην Αγγλία, όταν το λογισμικό που υποκλάπηκε από Γαλλική πολυεθνική εταιρεία πωλήθηκε μέσω διαδικτύου σε ανταγωνιστές της στον τομέα της αυτοκινητοβιομηχανίας και της αεροναυπηγικής.[488]

Ακόμα και στις περιπτώσεις που οι ενέργειες του χάκερ γίνονται απλά από περιέργεια ή για διασκέδαση, χωρίς δηλαδή πρόθεση να προκαλέσει ζημιά ή να υπεξαιρέσει χρήματα ή γνώσεις, αυτές συνιστούν παραβίαση νόμου, που ο δράστης γνωρίζει ότι παραβιάζει, καθώς εκκινεί λειτουργίες του υπολογιστή με σκοπό την – μη εξουσιοδοτημένη - πρόσβαση σε προγράμματα ή δεδομένα που βρίσκονται σε αυτόν.

Παράδειγμα χάκερ τέτοιας «αβλαβούς» μορφής είναι αυτή του διαβόητου Kevin Mitnik, όπου το 1995 κατάφερε να διεισδύσει στο σύστημα καυσίμων των πυραύλων της ΝΑΣΑ για να στείλει μια προειδοποίηση στο προσωπικό της ΝΑΣΑ, αναδεικνύοντας τα τρωτά σημεία του δικτύου. Όμως δεν προχώρησε τόσο ώστε να βάλει σε κίνδυνο την ασφάλεια του συστήματος, όπως το να βάλει σε λειτουργία έναν πύραυλο.[489]

Σύμφωνα με τους υπεύθυνους της Δίωξης Ηλεκτρονικού εγκλήματος της ΕΛ.ΑΣ, μπορούμε να διακρίνουμε τους "εγκληματίες του Κυβερνοχώρου" σε δύο κατηγορίες, σε hackers και σε crackers ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα:

α) Στους hackers που «επιτίθενται στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν κάποιο οικονομικό όφελος. Ως hacker μπορεί να ορισθεί το άτομο εκείνο το οποίο αποκτά χωρίς δικαίωμα πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών[490]. Στην κατηγορία αυτή ανήκουν, οι δράστες που "εισβάλουν" σε υπολογιστή δια της χρήσεως του Διαδικτύου για να μάθουν απλώς, κάποια προσωπικά στοιχεία, ή για να εντοπίσουν κάποιο πρόβλημα (τρύπα συστήματος) στην πληροφοριακή υποδομή εταιριών, τραπεζών κ.α. Οι hackers εμφανίστηκαν για πρώτη φορά κατά τη δεκαετία του 1970 στις ΗΠΑ, ως δράστες σε τηλεπικοινωνιακά συστήματα.

β) Στους crackers, που ενεργούν από οικονομικό όφελος και που δεν "εισβάλουν" απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της

[486] Grabosky Peter & Smith Russell, σσ. 48-49
[487] Burden Kit & Palmer Creole ό.π.
[488] http://www.cosmo.gr/pops/prart.aspx?ur=184968, Ιανουάριος (2008)
[489] Κουράκης Ν., στο Λάζος Γρηγόρης (2004), σ. 83
[490] Βλ. Κούρος Κωνσταντίνος (2014)

πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην τράπεζα για τη μεταφορά ενός ποσού στον λογαριασμό τους.»[491]

Όσον αφορά τον παραπάνω ορισμό, της Δίωξης ηλεκτρονικού εγκλήματος, θα μπορούσαμε να παρατηρήσουμε ότι είναι τόσο γενικός που θα ήταν δυνατό να περιλάβει ακόμα και τις περιπτώσεις όπου κάποιος αποκτά πρόσβαση στον ηλεκτρονικό υπολογιστή τρίτου με φυσικό τρόπο, όπως για παράδειγμα κάποιος υπάλληλος που βρίσκει ανοικτό τον υπολογιστή του προϊσταμένου του και διαγράφει ή αλλοιώνει αρχεία από αυτόν με σκοπό την εκδίκηση. Για αυτό θεωρούμε σκόπιμο ότι ο ορισμός αυτός θα έπρεπε να συμπληρωθεί από τη φράση «αποκτά απομακρυσμένη πρόσβαση παρακάμπτοντας τα όποια μέτρα ασφάλειας και προστασίας του υπολογιστή». Αυτό πρέπει να είναι σαφές σε ένα τέτοιο ορισμό γιατί κύριο στοιχείο της πρακτικής των χάκερ είναι ακριβώς αυτό της απομακρυσμένης πρόσβασης και της παραβίασης των κλειδωμάτων, των κωδικών και των συστημάτων προστασίας των δικτύων, όπου για παράδειγμα κάποιος χάκερ από τη Ρωσία μπαίνει στο Δίκτυο της ΝΑΣΑ στις ΗΠΑ.

Σύμφωνα με τους Grabosky και Walkley το hacking αρχικά αφορούσε την μη εξουσιοδοτημένη πρόσβαση σε πληροφορικά συστήματα από περιέργεια ή με άκακες προθέσεις ενώ το cracking τις κακόβουλες ενέργειες όπως την καταστροφή δεδομένων. Σταδιακά όμως ο όρος hacking χρησιμοποιείται συμπεριλαμβάνει και τις δυο έννοιες. Έτσι το hacking πλέον αφορά την μη εξουσιοδοτημένη πρόσβαση για επίθεση σε άλλο δίκτυο συστημάτων, την διάδοση κακόβουλου λογισμικού, ιών και «σκουληκιών», επιθέσεις άρνησης υπηρεσιών (DoS: Denial of Service) κλπ.[492]

Συνηθισμένη μεθοδολογία των χάκερ, για να ελέγχουν με απομακρυσμένη πρόσβαση υπολογιστές ή δίκτυα υπολογιστών, αποτελούν τα Botnets. Τα botnets ή BOTS, είναι κώδικες δικτύων μέσω των οποίων οι χάκερ μπορούν να αναλάβουν τον απομακρυσμένο έλεγχο υπολογιστή ή δικτύων «κατειλημμένων» και να επιτεθούν τελικά σε άλλες μηχανές μέσω του Διαδικτύου. Τα Botnets χρησιμοποιούν βλαβερό λογισμικό, όπως ιούς, δούρειους ίππους, «σκουλήκια» κλπ. για να ελέγχουν από μακριά υπολογιστές τους οποίους μετατρέπουν τελικά σε Zombies. Το Zombie είναι ένας υπολογιστής συνδεδεμένος με το Διαδίκτυο που έχει «καταληφθεί» από έναν χάκερ που έχει εγκαταστήσει έναν ιό υπολογιστών ή έναν Δούρειο ίππο. Γενικά, μια μηχανή zombie είναι μόνο μια από πολλές σε ένα botnet και χρησιμοποιείται για να εκτελέσει κάποιου είδους κακόβουλου κώδικα με μακρινή καθοδήγηση. Οι περισσότεροι ιδιοκτήτες των υπολογιστών zombie δεν γνωρίζουν ότι το σύστημά τους χρησιμοποιείται κατά αυτόν τον τρόπο. Οι υπολογιστές zombie χρησιμοποιούνται κυρίως για την αποστολή άχρηστων ή κακόβουλων ηλεκτρονικών μηνυμάτων (spam). Έχει υπολογιστεί ότι περίπου το 50% με 80% των συνολικών μηνυμάτων spam που διακινούνται στο Διαδίκτυο καθημερινά προέρχεται από υπολογιστές zombie. Με τρόπο αυτό οι spammers μπορούν να αποφύγουν τον εντοπισμό τους και χρησιμοποιούν το εύρος ζώνης (bandwidth) των ιδιοκτητών των υπολογιστών zombie για τους δικούς τους σκοπούς.[493]

[491] Βλ. Κούρος Κωνσταντίνος, ό.π.
[492] Grabosky Peter & Walkley Sascha (2007), σσ. 358-375
[493] Πηγή: http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm

6.2.3 Κακόβουλα προγράμματα και άλλο βλαβερό λογισμικό, Malware - Rootkit

Πρόκειται για λογισμικό που εισβάλλει στον υπολογιστή και μπορεί να δημιουργήσει ανεπιθύμητες παρενέργειες απειλώντας την ασφάλεια του χρήστη και του ηλεκτρονικού υπολογιστή.

Σύμφωνα με έρευνα της Google τουλάχιστον 450.000 από 4,5 εκατομμύρια ιστοσελίδες περιέχουν κακόβουλο κώδικα που μπορεί να μολύνει τον υπολογιστή του επισκέπτη με ιούς. Συγκεκριμένα, όταν ένας χρήστης μπαίνει σε ένα από αυτά τα sites, αυτόματα ενεργοποιεί άλλες ιστοσελίδες χωρίς να το καταλάβει. Αυτές ανοίγουν και εγκαθιστούν στον υπολογιστή του μικρά προγράμματα, τα οποία στην πιο αθώα εκδοχή τους κατασκοπεύουν τον κάτοχό του κι επιλέγουν τις διαφημίσεις που βλέπει μπαίνοντας σε ιστοσελίδες ή -στη χειρότερη περίπτωση- σκορπούν ιούς. Άλλες 700.000 ιστοσελίδες της έρευνας πιθανώς περιέχουν κώδικα που μπορεί να παραδώσει τον έλεγχο του υπολογιστή σε τρίτο, ο οποίος δρα αόρατα από απόσταση.[494]

Ως κακόβουλο λογισμικό (malware) χαρακτηρίζονται, εκτός των ιών, τα σκουλήκια (worms) που είναι ιοί που αναπαράγονται μέσω των δικτύων ηλεκτρονικών υπολογιστών, οι Δούρειοι Ίπποι (trojan horses) είναι προγράμματα που εισέρχονται στον υπολογιστή μέσω διαδικασιών που μοιάζουν ακίνδυνες και δρουν ως «κατάσκοποι» καταγράφοντας οτιδήποτε πληκτρολογείται στον Η/Υ και τα spyware που είναι προγράμματα που προσκολλώνται κρυφά σε άλλα προγράμματα που κατεβαίνουν από το Διαδίκτυο. Το κακόβουλο λογισμικό αφού εγκατασταθεί, παρακολουθεί τη δικτυακή δραστηριότητα του χρήστη ή βοηθά τον παράνομο να πάρει τον έλεγχο του υπολογιστή.

6.2.4 Διάδοση ιών ηλεκτρονικών υπολογιστών

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο Διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων ηλεκτρονικών υπολογιστών με ιούς.

Η διάδοση της χρήσης Η/Υ, αλλά και του διαδικτύου τα τελευταία 25 χρόνια, αποτέλεσε αφορμή για μια μικρή κατηγορία προγραμματιστών να πειραματιστούν πάνω στην ανάπτυξη μικρών προγραμμάτων που κάνουν δεδομένα να αλλοιώνονται ή να χάνονται, τον Η/Υ να δυσλειτουργεί ή ακόμα και να καταστρέφεται. Κάπως έτσι, σαν μια μάλλον κακόγουστη φάρσα, ξεκίνησε η ανάπτυξη και συγγραφή ιών για λειτουργικά συστήματα υπολογιστών. Στη διάρκεια του χρόνου όμως η «αστεία» πλευρά της υπόθεσης εξανεμίστηκε. Αν λοιπόν κάποιος σήμερα διαπιστώσει ότι ο Η/Υ του έχει κολλήσει ιό, μάλλον θα δυσανασχετήσει παρά θα γελάσει. Σήμερα υπάρχουν περίπου 80.000 ιοί, πολλοί από τους οποίους δημιουργούν ιδιαίτερα προβλήματα σε υπολογιστικά συστήματα χρηστών ή οργανισμών.

Όταν αναφερόμαστε σε ιούς των υπολογιστών εννοούμε (κακόβουλους) κώδικες δηλ. ειδικά προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή του χρήστη χωρίς την έγκρισή του και να μολύνουν άλλα αρχεία. Αποτελούν δηλαδή μια ακολουθία (ή σειρά ακολουθιών) συμβόλων που, όταν εκτελεστούν κάτω από ορισμένες συνθήκες ή σε ένα ορισμένο περιβάλλον, δημιουργούν ένα ακριβές ή παρόμοιο αντίγραφο της ακολουθίας το οποίο και τοποθετούν μέσα στον υπό-μόλυνση Η/Υ. Η τοποθέτηση γίνεται σε τέτοιο μέρος, όπου θα είναι δυνατή η μελλοντική εκτέλεση, το λεγόμενο «άνοιγμα» του αρχείου. Αυτή είναι και η επονομαζόμενη «αναπαραγωγή» (replication) του ιού μέσα στον

[494] http://www.simerini.com.cy/nqcontent.cfm?a_id=308817, Αύγουστος (2007)

υπολογιστή. Βέβαια, ένας ιός μπορεί να περιλαμβάνει και μια επιπλέον λειτουργία (payload), με την οποία θα κάνει ζημιά στο μολυσμένο σύστημα, χωρίς όμως αυτό να είναι αναγκαίο.

6.2.5 Τρόποι Μετάδοσης Ιών

Οι ιοί έχουν την ικανότητα να εξαπλώνονται από μόνοι τους και συνήθως διαδίδονται με:

- Εκκίνηση του Η/Υ από μολυσμένο αφαιρούμενο δίσκο.
- Εκτέλεση/άνοιγμα μολυσμένων αρχείων που επισυνάπτονται σε emails.
- Άνοιγμα/ανάγνωση ηλεκτρονικού ταχυδρομείου (email) που συνήθως στέλνουν άγνωστα άτομα, που περιέχουν καταστροφικό κώδικα που ενεργοποιείται αυτόματα με την ανάγνωση του email.
- Άνοιγμα/ανάγνωση μολυσμένων ιστοσελίδων.
- Μέσω πρόσβασης στο internet. Συγκεκριμένα, όλα σχεδόν τα λειτουργικά συστήματα, και κυρίως τα Windows, έχουν "τρύπες" ασφαλείας τις οποίες εκμεταλλεύονται κάποιοι ιοί για να μολύνουν τον Η/Υ, χωρίς να ζητήσουν την άδεια του χρήστη για εγκατάσταση κάποιου προγράμματος.

Ο ιός αφού εισαχθεί, προσπαθεί να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου στο πρόγραμμα επεξεργασίας κειμένου (word), παραπλανώντας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν ανοιχθούν τα εκτελέσιμα αρχεία (script) που τα μεταφέρουν.

Οι δράστες που διακινούν ιούς τιμωρούνται, από το ελληνικό δίκαιο, σύμφωνα με το άρθρο 381 του Π.Κ. αλλά έχουν και αστικές ευθύνες.[495]

6.2.6 Τα σκουλήκια (worms)

Τα «σκουλήκια» κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα e-mail σε όλη τη λίστα επαφών του Outlook. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Η μαζική αποστολή e-mail, εκτός από την κατασπατάληση του εύρους ζώνης της διαδικτυακής σύνδεσης σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.[496]

6.2.7 Οι Δούρειοι ίπποι (Trojans)

Πρόκειται για την ίσως πιο διαδεδομένη κατηγορία ιών, αν και οι Δούρειοι ίπποι από πολλούς δεν θεωρούνται ιοί επειδή δεν αναπαράγονται.

Ο Δούρειος ίππος (Trojan horse ή Trojans) είναι ένα πρόγραμμα που ενώ φαίνεται πως δουλεύει σωστά και με νόμιμο τρόπο, στην πραγματικότητα μπορεί να προκαλέσει αρκετές βλάβες. Ονομάζεται έτσι (όπως και ο Δούρειος Ίππος της Τροίας), γιατί μπορεί να μπει στον υπολογιστή μέσω διαδικασιών που θεωρούνται ακίνδυνες, όπως για παράδειγμα μέσω ενός

[495] Κούρος Κωνσταντίνος (2005)
[496] http://virus.gr/portal/node/32, Ιανουάριος (2008)

παιχνιδιού ή μέσω ενός προγράμματος ανίχνευσης ιών και έτσι να ξεγελάσει το χρήστη κρύβοντας την παρασκηνιακή του δραστηριότητα. Με την εκτέλεση του Trojan πιθανώς να υπάρξει σβήσιμο αρχείων από τον Η/Υ ή ακόμα και ολοκληρωτικό φορμάρισμα (format), δηλαδή διαγραφή και απώλεια δεδομένων του δίσκου.[497] Ένας δούρειος ίππος μπορεί να δράσει και ως κατάσκοπος, δηλαδή να παρακολουθεί όλη την κίνηση του υπολογιστή, να ξεκινήσει να καταγράφει οτιδήποτε πληκτρολογεί ο χρήστης στο πληκτρολόγιό του, να ξεκινά προγράμματα που τρέχουν στο παρασκήνιο, χωρίς να τα αντιλαμβάνεται καν ο χρήστης, να απενεργοποιεί τα προγράμματα προστασίας, να ελέγχει το πληκτρολόγιο, την οθόνη, τα αρχεία ή άλλα μέρη του υπολογιστή και να ειδοποιεί τον αποστολέα του ιού ότι ο υπολογιστής του χρήστη είναι ευάλωτος. Έτσι συλλέγει και αποστέλλει πληροφορίες κωδικών πρόσβασης, λογαριασμών, πιθανών τραπεζικών συναλλαγών και άλλα προσωπικά δεδομένα που συνιστούν κλοπή ταυτότητας.

Βλέπουμε λοιπόν ότι οι Δούρειοι ίπποι, όπως και οι άλλοι ιοί χρησιμοποιούνται ως εργαλεία από τους διάφορους διαδικτυακούς απατεώνες για την τέλεση άλλων, οικονομικής φύσεως κυρίως, εγκλημάτων που εξετάζουμε παρακάτω.

6.2.8 Τα προγράμματα «κατασκοπείας» (Spyware)

Το spyware είναι πρόγραμμα που μπορεί να προσκολληθεί κρυφά σε αρχεία που κατεβάζει ο χρήστης από το Διαδίκτυο. Το spyware μοιάζει με τους δούρειους ίππους στο ότι εισέρχεται στον υπολογιστή κατά τη διάρκεια εγκατάστασης ενός φαινομενικά ακίνδυνου λογισμικού, χωρίς να το αντιλαμβάνεται ο χρήστης. Μόλις κατέβει, αυτοεγκαθίσταται στον υπολογιστή και ξεκινά κρυφά την παρακολούθηση της διαδικτυακής του δραστηριότητας. Μπορεί επίσης να συγκεντρώνει πληροφορίες για τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, για τους κωδικούς πρόσβασης ακόμη και τους αριθμούς πιστωτικών καρτών.

Οι πληροφορίες που καταγράφει αποστέλλονται σε αυτόν που ελέγχει το spyware, που συνήθως είναι εταιρίες που ενδιαφέρονται να μάθουν το προφίλ του χρήστη για να του στέλνουν στη συνέχεια διαφημιστικό ή άλλο υλικό ανάλογα με τα ενδιαφέροντα του. Επιπλέον, στέλνει τις πληροφορίες που συλλέγει στην εγχώρια βάση των spyware μέσω της σύνδεσης του χρήστη.

Μια μορφή spyware είναι και τα adware που συλλέγουν πληροφορίες για το προφίλ του χρήστη, με στόχο αργότερα να προβάλλει διαφημίσεις στο πρόγραμμα που χρησιμοποιεί για περιήγηση στο διαδίκτυο, βάσει των πληροφοριών που έχει συλλέξει γύρω από τις συνήθειες του.[498]

6.2.9 Άρνηση υπηρεσιών (DoS)

Οι επιθέσεις άρνησης υπηρεσιών (DoS, Denial of Service Attacks) στοχεύουν στο να αποτρέψουν τους "νόμιμους" χρήστες από να αποκτήσουν πρόσβαση ή να χρησιμοποιήσουν μια υπηρεσία Διαδικτύου. Αυτές οι επιθέσεις μπορούν να λάβουν διάφορες μορφές, που περιλαμβάνουν συνηθέστερα την υπερχείλιση των κεντρικών υπολογιστών μιας επιχείρησης ή οργανισμού με εκατομμύρια ψεύτικων μηνυμάτων, καταναλώνοντας κατά συνέπεια όλο το διαθέσιμο εύρος ζώνης του συστήματος που γίνεται στόχος. Σε αυτές τις περιπτώσεις, ο δράστης σε καμία στιγμή δεν αποκτά πρόσβαση στο σύστημα του στόχου, δεν τροποποιεί οποιοδήποτε από το περιεχόμενό του, δεν προκαλεί καμία μόνιμη ζημία και επομένως καθίσταται πολύ δύσκολο να στοιχειοθετηθεί κάποιο αδίκημα για κακή χρήση υπολογιστών.

[497] http://www.saferinternet.gr, ό.π.
[498] http://www.saferinternet.gr, Ιανουάριος (2008)

Αυτή η ανεπάρκεια στο νόμο έχει αναγνωριστεί και σημαίνει ότι, προς το παρόν τουλάχιστον, πρέπει να στηριχθούμε στην ταξινόμηση των παραδοσιακότερων ποινικών αδικημάτων για να επιβάλουμε μια ποινικές κυρώσεις σε τέτοιες δραστηριότητες.[499]

6.3. Τα είδη του Κυβερνο-εγκλήματος (εγκλήματα μέσω του διαδικτύου) όπου ο υπολογιστής αποτελεί εργαλείο των επιθέσεων

Η Κυβερνο-τρομοκρατία, ο Κυβερνο-εκβιασμός, η πειρατεία ονόματος ιστοχώρων κλπ. που παρουσιάζονται παρακάτω αποτελούν, εκ πρώτης όψεως, καθαρά ηλεκτρονικά εγκλήματα, όμως μια ενδελεχέστερη διερεύνηση συχνά θα μας αποκαλύψει τον οικονομικό χαρακτήρα που μπορεί να υποκρύπτουν.

Σύμφωνα με έρευνα στη Μ. Βρετανία οι κυβερνο-τρομοκράτες που απειλούσαν ιδρύματα και οργανισμούς κέρδισαν πάνω από 400 εκατ. λίρες μόνο από το 1993 έως το 1995. Στο διάστημα αυτό καταγγέλθηκαν 40 περιπτώσεις απειλών σε τράπεζες στη Μ. Βρετανία και τις ΗΠΑ.[500]

Από την άποψη αυτή οι συγκεκριμένες μορφές κυβερνοεγκλημάτων εμπίπτουν στο πεδίο ανάλυσης της παρούσας μελέτης.

6.3.1. Κυβερνο-τρομοκρατία

Ως «τρομοκρατία» θεωρείται από το FBI «η παράνομη άσκηση δύναμης ή βίας εναντίον ατόμων ή περιουσίας με σκοπό τον εκφοβισμό ή τον εκβιασμό κυβερνήσεων ή κοινωνικών ομάδων για την επίτευξη πολιτικών ή κοινωνικών σκοπών», ενώ ως «κυβερνο-τρομοκρατία» (Cyber terrorism) ορίζεται «η χρήση των υπολογιστικών πόρων για τον εκφοβισμό ή τον εκβιασμό τρίτων».[501]

Στον παραπάνω ορισμό για την «κυβερνο-τρομοκρατία» σύμφωνα με το FBI περιλαμβάνονται ακόμα και οι περιπτώσεις hacking σε υπολογιστικά συστήματα νοσοκομείων για παραποίηση ιατρικών συνταγών που οδηγεί στη χορήγηση θανατηφόρας δόσης φαρμάκου με σκοπό την εκδίκηση. Οι περιπτώσεις κυβερνο-τρομοκρατίας περιλαμβάνουν τη χρήση υπολογιστικών συστημάτων για τον εκβιασμό ή τον εκφοβισμό ευρύτερων κοινωνικών σχηματισμών – και όχι μεμονωμένων ατόμων – απειλώντας κοινωνικά αγαθά, την υγεία και την ζωή μεγάλης μάζας του πληθυσμού.

6.3.2. Κυβερνο- εκβιασμός

Το ίντερνετ προσφέρει πολλαπλές ευκαιρίες, σε έναν αποφασισμένο εκβιαστή, να διαδώσει γρήγορα, χωρίς κόπο και αποτελεσματικά τις πληροφορίες που το θύμα (άτομο ή επιχείρηση) επιθυμεί να διατηρήσει μυστικές από το κοινό. Ακόμα και εάν το θύμα υποκύψει εκβιασμό, ο εκβιαστής μπορεί να συνεχίσει τη διάδοση των πληροφοριών χωρίς να μπορεί να εντοπιστεί εύκολα κρυμμένος πίσω από την ανωνυμία στο διαδίκτυο.[502]

6.3.3. Πειρατεία ονόματος ιστοχώρων

Η πειρατεία ονόματος ιστοχώρων (Domain name hijacking) έγινε ευρύτερα γνωστή ως δραστηριότητα κυβερνο-εγκλήματος τον Απρίλιο του 2000 όταν χάκερ μετέφεραν τα ονόματα των ιστοχώρων περισσότερων από 50 επιχειρήσεων σε εναλλακτικές ταχυδρομικές

[499] Πηγή Εφημερίδα «*Το Βήμα»* 16/02/2000, σσ. Δ.14-46.
[500] Computer & Information Science (2008)
[501] Computer & Information Science (2008)
[502] Burden Kit & Palmer Creole, ό.π.

διευθύνσεις. Αν και αυτός ο τύπος ηλεκτρονικής δραστηριότητας δεν ήταν νέος, έλαβε ευρύτατη δημοσιότητα επειδή "χτυπήθηκαν" διάφορες επιχειρήσεις μεγάλης εμβέλειας, συμπεριλαμβανομένων της Adidas και της Manchester United[503]. Το αποτέλεσμα αυτής της μαζικής πειρατείας ήταν να προκληθεί, από τη μια απώλεια υπηρεσιών Διαδικτύου και εισοδήματος για τις επιχειρήσεις που χτυπήθηκαν, και κλονισμός της εμπιστοσύνης του κοινού για την ασφάλεια του Διαδικτύου από την άλλη. Επίσης, ανέδειξε την αδυναμία ασφαλούς κατοχύρωσης των εμπορικών σημάτων και ονομάτων των προϊόντων (branding) στο ηλεκτρονικό περιβάλλον. Αρκεί μόνο η μεταφορά ενός ονόματος ιστοχώρου (Domain name) σε μια διεύθυνση που περιέχει πορνογραφικό ή άλλο εμπορικά ανεπιθύμητο υλικό για να επιτευχθεί σημαντική αλλοίωση των εμπορικών σημάτων ή δυσφήμιση για το νόμιμο ιδιοκτήτη του ονόματος περιοχών.

6.3.4. Ο Κυβερνοσφετερισμός (Cybersquatting)

Ο Κυβερνοσφετερισμός αφορούσε κυρίως παλαιότερες περιπτώσεις, όπου επιτήδειοι πρόλαβαν να κατοχυρώσουν εμπορικά σήματα εταιρειών στο διαδίκτυο, αποκτώντας τα δικαιώματα για το αντίστοιχο όνομα χώρου (domain name), με στόχο να τα πωλήσουν στους νόμιμους ιδιοκτήτες τους όταν αυτοί θελήσουν αργότερα να δραστηριοποιηθούν στο Internet. Με τον τρόπο αυτό αρκετές από τις μεγάλες και επώνυμες εταιρείες αναγκάσθηκαν να πληρώσουν μεγάλα ποσά για να αποκτήσουν μια ιστοσελίδα με το δικό τους όνομα, το οποίο όμως είχε φροντίσει να κατοχυρώσει νωρίτερα κάποιος άλλος.[504]

6.3.5. Συκοφάντηση - Προσβολή της υπόληψης

Η «προσβολή» της υπόληψης (Defamation) περιλαμβάνει τη διάδοση μέσω του διαδικτύου ψευδών πληροφοριών που μειώνουν την προσωπικότητα κάποιου ατόμου ή μιας επιχείρησης στα μάτια των υγιώς σκεπτόμενων ανθρώπων.[505]

6.3.6. Διάδοση πορνογραφικού υλικού

Μια από τις κυριότερες παραβατικές δραστηριότητες που έχουν βρει εκτενές πεδίο δράσης στο διαδίκτυο είναι η διάδοση πορνογραφικού υλικού. Η ανωνυμία, η ευκολία διάδοσης και η παράκαμψη των αρμοδίων ελεγκτικών αρχών αποτελούν κύριους παράγοντες που το ίντερνετ επιλέγεται για τέτοιου είδους δραστηριότητες.

Στο ίντερνετ υπάρχει πληθώρα ιστοσελίδων με ανάλογο περιεχόμενο και υλικό όπως φωτογραφίες, βίντεο, «θέαμα» σε απευθείας σύνδεση επί πληρωμή (live-cams) κλπ. Οι δημιουργοί αυτών των ιστοσελίδων είναι τις περισσότερες φορές οι ίδιοι που εκμεταλλεύονται τα παιδιά. Ένα πολύ μεγάλο μέρος του υλικού αυτού αφορά το λεγόμενο «μαλακό πορνό», όμως αρκετά συνηθισμένες είναι και οι περιπτώσεις του σκληρού και αυτές της παιδικής πορνογραφίας.[506]

Το κίνητρο των δραστών που διακινούν τέτοιο υλικό, εκτός από το σεξουαλικό πάθος είναι και η κερδοσκοπία, σύμφωνα με ομολογίες των ίδιων κατά τη σύλληψή τους από τη Δίωξη Ηλεκτρονικού εγκλήματος Αττικής. Ακόμα, το γεγονός ότι το πορνογραφικό υλικό που διακινείται μέσω διαδικτύου, σε 100.000 ιστοσελίδες, αποφέροντας ετήσιο τζίρο 1 δισ. € [507] δείχνει και τον οικονομικό χαρακτήρα αυτού του είδους ηλεκτρονικής εγκληματικότητας.

[503] Μάντσεστερ Γιουνάιτεντ, ποδοσφαιρική ομάδα
[504] Κέντρο ΠΛΗ.ΝΕ.Τ. Περ. Ενότητας Φλώρινας (2014)
[505] Burden Kit & Palmer Creole, ό.π.
[506] Burden Kit & Palmer Creole, ό.π.
[507] Κέντρο ΠΛΗ.ΝΕ.Τ. Περ. Ενότητας Φλώρινας (2014)

6.3.7. Ηλεκτρονική Παρακολούθηση - Παρενόχληση

Μια άλλη μορφή επιβλαβούς περιεχομένου έχει να κάνει με την παρενόχληση στον κυβερνοχώρο (Cyberstalking). Αν και δεν υπάρχει καθολικά αποδεκτός ορισμός, ο όρος χρησιμοποιείται για τις περιπτώσεις κατά τις οποίες κάποιο άτομο παρενοχλεί άλλα άτομα στο διαδίκτυο χρησιμοποιώντας διάφορους τρόπους επικοινωνίας όπως αποστολή κειμένων με ηλεκτρονικό ταχυδρομείο, σε «δωμάτια συζητήσεων» (chat rooms), σε «ομάδες αλληλογραφίας» (newsgroups) ή άμεσων μηνυμάτων με άσχημο περιεχόμενο, δημοσίευση δυσάρεστων φωτογραφιών ή μηνυμάτων για άλλους σε ιστολόγια (blogs) ή άλλες ιστοσελίδες, τη χρήση του ονόματος ξένου χρήστη (κλοπή ταυτότητας) με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο, αναπάντητες κλήσεις, προσβλητικά προφορικά μηνύματα. Οι θύτες μπορούν ακόμα, μέσω του ίντερνετ ή από τις συζητήσεις, να αποκτούν προσωπικά στοιχεία, όπως διευθύνσεις, τηλέφωνο κλπ. τα οποία χρησιμοποιούν για να επιτύχουν προσωπική συνάντηση με τα θύματά τους. Το αποτέλεσμα τέτοιων συναντήσεων είναι συχνά η πρόκληση φόβου, η διατάραξη της καθημερινής ζωής των θυμάτων ή ακόμα και η άσκηση φυσικής βίας πάνω τους.

Σύμφωνα με μελέτες η πλειοψηφία των δραστών ήταν άνδρες συνήθως με ιστορικό παραβάσεων ή ψυχικών διαταραχών, κατάθλιψη, σχιζοφρένεια, κατάχρηση αλκοόλ ή ουσιών. Ακόμα οι μελέτες για το προφίλ των δραστών δείχνουν ότι αυτοί είναι οικονομικά ανεξάρτητοι και μάλλον μεσαίας ή ανώτερης τάξης, με υψηλές γνώσεις στον τομέα των υπολογιστών, συναισθηματικά μόνοι που επιζητούν παρέα στον κυβερνοχώρο και που συχνά αποκτούν μανία με άτομα γνωρίζουν στο διαδίκτυο.[508]

6.4. Μορφές ηλεκτρονικο-οικονομικού εγκλήματος

Οι προηγούμενες μορφές, του γνήσιου κυβερνοεγκλήματος μπορούν να χρησιμοποιούνται ως εργαλεία των καθαρών μορφών του ηλεκτρονικού-οικονομικού εγκλήματος που απαιτούν τη χρήση ηλεκτρονικού υπολογιστή, tablet ή smartphone και διαδικτύου οι οποίες παρουσιάζονται παρακάτω.

6.4.1. Απάτες μέσω του διαδικτύου [509]

Το διαδίκτυο αποτελεί ένα ελκυστικό μέσο για κάθε είδους εγκληματία λόγω της αυξημένης ανωνυμίας (έλλειψη θεατότητας), της τεράστιας δεξαμενής αναζήτησης πιθανών θυμάτων και των αυξημένων προσδοκώμενων κερδών σε σχέση με το μικρό κόστος που απαιτείται από πλευράς παρανόμων. Η αναγνώριση και ανακάλυψη των διαδικτυακών απατεώνων είναι δύσκολη και πολύπλοκη διαδικασία λόγω της απαιτούμενης συνεργασίας πολλών εμπλεκόμενων υπηρεσιών και φορέων αλλά και της μη άμεσης επαφής που έχουν τα θύματα με τους θύτες μέσω του διαδικτύου. Οι τελευταίοι μπορεί να αποτελούνται από μεμονωμένα άτομα ή επιχειρήσεις μέχρι και συνδικάτα οργανωμένου εγκλήματος.

Απάτη στο διαδίκτυο (Internet Fraud) θεωρείται οποιοδήποτε είδος απάτης που χρησιμοποιεί ένα ή περισσότερα από τα περιεχόμενα του ίντερνετ, όπως δωμάτια συζητήσεων (chat rooms), διευθύνσεις ηλεκτρονικού ταχυδρομείου, πίνακες μηνυμάτων ή ιστοσελίδες για να πραγματοποιηθούν παράνομες συναλλαγές ή να μεταβιβαστούν τα κέρδη από αυτές σε οικονομικούς θεσμούς ή άλλους που έχουν σχέση με την απάτη.

[508] Stephens Gene (1995)
[509] *Internet Fraud,* Σεπτ. (2007)

Τα εγκλήματα απάτης στο διαδίκτυο περιλαμβάνουν διαδοχικά περισσότερες από μια διαφορετικές παράνομες ενέργειες, όπως τεχνικές phishing που χρησιμοποιούν κλοπή πνευματικής ιδιοκτησίας για να πραγματοποιήσουν κλοπή ταυτότητας κατά τη διάπραξη μιας απάτης. Οι αρμόδιες αρχές αποκαλύπτουν την απάτη από τον αρχικό μηχανισμό ή από τον κύριο σκοπό της απάτης όπως μπορεί να είναι μια απάτη σε διαδικτυακή δημοπρασία.

Οι περισσότερες από τις απάτες που διαπράττονται πλέον μέσω του διαδικτύου έχουν προϋπάρξει, με τη μια ή την άλλη μορφή, έξω από αυτό αλλά πάντα απαιτούσαν τη συνδρομή της τεχνολογίας για να τελεσφορήσουν. Οι πάνω από 1 δις πλέον χρήστες του διαδικτύου παγκοσμίως αποτελούν πιθανά θύματα απάτης όντας μόνο ένα κτύπημα πλήκτρου μακριά από τους απατεώνες.

Παρά τη δυσκολία υπολογισμού του κόστους των απωλειών που προέρχονται από απάτη στο ίντερνετ, σύμφωνα με την Επιτροπή Ομοσπονδιακού Εμπορίου των ΗΠΑ (Federal Trade Commission) κατά το 2006 η αξία της απώλειας λόγω απάτης μέσω του ίντερνετ ξεπέρασε το 1,1 δις δολάρια. Το 64% του συνόλου των καταγγελιών που συγκέντρωσε η επιτροπή αφορούσαν περιπτώσεις απάτης. Εξ αυτών περίπου οι μισές (48%) αφορούσαν απάτη στο διαδίκτυο. Από το σύνολο των περίπου 674.000 παραπόνων το 5% αφορούσε περιπτώσεις δημοπρασιών και το 36% κλοπής ταυτότητας.[510]

Το ηλεκτρονικό ταχυδρομείο και οι διάφορες ιστοσελίδες στο ίντερνετ αποτελούν τους δυο κυριότερους μηχανισμούς που χρησιμοποιούνται για να έλθουν σε επαφή οι απατεώνες με τα υποψήφια θύματα τους.

Οι απατεώνες στο διαδίκτυο στηρίζονται συχνά στην κοινωνική μηχανική (social engineering) ή την οπτική επικοινωνία με χρήση πειστικών «ηλεκτρονικών δολωμάτων», όπως μια παραπλανητική ιστοσελίδα ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου (phishing), για να αποσπάσουν εμπιστευτικές πληροφορίες και να παρασύρουν τα θύματα τους στην απάτη. Όσο πιο αληθοφανής και λεπτομερής εμφανίζεται η επικοινωνία τόσο πιθανότερο είναι ότι το θύμα θα δεχθεί την πληροφορία ως αληθινή και προερχόμενη από νόμιμη πηγή.[511]

Υπάρχουν διάφορες μορφές διαδικτυακής απάτης από εμπορικές απάτες μέχρι απάτες για συνεισφορά χρημάτων σε ανύπαρκτους φιλανθρωπικούς σκοπούς με πολλαπλά θύματα ταυτόχρονα.

Η διαδικτυακή απάτη διακρίνεται ανάλογα με το είδος της οικονομικής απάτης που διαπράττεται σε:

6.4.1.1. Απάτες διαδικτυακών δημοπρασιών

Οι απάτες σε δημοπρασίες (Auction Fraud) αποτελούν τη συχνότερα καταγγελλόμενη μορφή διαδικτυακής απάτης με 45% του συνόλου των 86.000 καταγγελιών που καταγράφηκαν από τις διωκτικές υπηρεσίες κατά το 2006 σύμφωνα με το Κέντρο Παραπόνων για Διαδικτυακά Εγκλήματα (Internet Crime Complaint Center) στις ΗΠΑ. Οι καταγγελίες αφορούσαν απώλειες 198 εκατ. δολαρίων λόγω της απάτης σε δημοπρασίες.[512]

Οι δημοπρασίες που διενεργούνται μέσω ιστοσελίδων στο ίντερνετ δε διαφέρουν ουσιαστικά από τις αγοραπωλησίες που γίνονται μέσω οίκων δημοπρασιών στο πραγματικό περιβάλλον. Οι πιθανοί αγοραστές και πωλητές ζητούν ή προσφέρουν μέσω των

[510] Federal Trade Commission (2006)
[511] *Internet Fraud*, Σεπτ. (2007)
[512] National White Collar Crime Center & Federal Bureau of Investigation, IC3 2006 Internet Crime Report, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf, ανακτήθηκε Σεπτ. 22 (2007)

διαδικτυακών δημοπρασιών κάθε είδος αντικειμένων, από αντίκες ή εικονική ιδιοκτησία μέχρι φαγητά. Μετά την κατοχύρωση του αντικειμένου σε αυτόν, ο αγοραστής καλείται να αποστείλει την αξία του. Απάτη συμβαίνει όταν το θύμα δεν λαμβάνει ποτέ το αντικείμενο που αγόρασε ή του παραδίδεται ένα διαφορετικό ή μικρότερης αξίας από αυτό αντικείμενο.

Χαρακτηριστική περίπτωση αποτελεί αυτή ενός 40άχρονου από το Σηάτλ των ΗΠΑ όπου καταδικάστηκε σε φυλάκιση 2 ετών για απάτη όταν χρησιμοποίησε διαφορετικά διαδικτυακά ονόματα για να πωλήσει μέσω διαδικτυακής δημοπρασίας στο eBay ηλεκτρονικό εξοπλισμό σε ανυποψίαστους πελάτες στους οποίους ποτέ δε παρέδωσε τα αντικείμενα που αγόρασαν. Ο 40χρονος για καλύψει την πραγματική του ταυτότητα άλλαζε συχνά παρόχους ίντερνετ (ISPs), δημιούργησε πολλαπλούς λογαριασμούς τραπεζών και πιστωτικών καρτών αλλά και ηλεκτρονικούς λογαριασμούς (user accounts) στο eBay και το PayPal. [513]

6.4.1.2. Απάτες ηλεκτρονικού εμπορίου

Με την ανάπτυξη του διαδικτύου και τη διάδοση των ηλεκτρονικών συναλλαγών δημιουργήθηκε ένας αυξανόμενος αριθμός χρηστών που χρησιμοποιούν το ίντερνετ για την παραγγελία και αγορά κάθε είδους αγαθών από διάφορα διαδικτυακά καταστήματα. Το ηλεκτρονικό εμπόριο διευκολύνει καθημερινά εκατομμύρια ανθρώπους και επιχειρήσεις.

Υπάρχει, όμως παράλληλα και μια ανησυχητική αύξηση ύποπτων εμπορικών ιστοχώρων που ζητούν την αποστολή προσωπικών δεδομένων και πληρωμή μέσω πιστωτικής κάρτας. Είναι βασικό η πρόσβαση σε εμπορικές ιστοσελίδες να γίνεται με ιδιαίτερη προσοχή και με εξακρίβωση αν αυτές λαμβάνουν υπόψη τους την κείμενη νομοθεσία και παρέχουν την υποχρεωτική ασφάλεια συναλλαγών και προσωπικών δεδομένων. Σε πολλές από τις περιπτώσεις αυτές τα αγαθά που έχουν αγοραστεί ουδέποτε φθάνουν στα χέρια του καταναλωτή, σε κάποιες άλλες ακόμα τα προσωπικά δεδομένα του και πολύ χειρότερα η πιστωτική του κάρτα χρησιμοποιείται από τρίτους χωρίς την δική του γνώση και συναίνεση. Τέτοιοι ιστοχώροι μπορούν να ασχολούνται με πώληση αγαθών, με ηλεκτρονικό τζόγο, ή ακόμα και με πορνογραφία.

Συνήθως αυτές οι ιστοσελίδες προέρχονται από τις λιγότερο ανεπτυγμένες χώρες, στις οποίες δεν υπάρχει η κατάλληλη νομοθεσία.[514]

Συνηθισμένη μορφή απάτης σε υπηρεσίες ηλεκτρονικού εμπορίου, παρόμοια με την παραπάνω περίπτωση απάτης σε δημοπρασίες, είναι η περίπτωση μη παράδοσης των υποσχόμενων αγαθών και υπηρεσιών ή μη πληρωμής τους (Non-Delivery of Merchandise, Payment, or Services).

Η ανωνυμία στο ίντερνετ προσφέρει την δυνατότητα σε διάφορες ψευτο-ιστοσελίδες να παραπλανούν καταναλωτές να αποστέλλουν πληρωμή για αγαθά (προϊόντα ή υπηρεσίες), συνήθως σε προσφορά, τα οποία όμως ποτέ δεν παραλαμβάνουν ή παραλαμβάνουν αγαθά πολύ μικρότερης αξίας από την διαφημιζόμενη. Δεν είναι σπάνιες και οι περιπτώσεις που συμβαίνει και το αντίθετο, καταναλωτές, στους οποίους έχουν αποσταλεί τα προϊόντα ή παρασχεθεί οι υπηρεσίες, να μην καταβάλλουν το συμφωνηθέν αντίτιμο.

Περίπτωση, παρόμοια με την παραπάνω, κάποιου ο οποίος αγόρασε από το Ebay ένα αεροπλάνο έναντι 16200 δολαρίων, έστειλε στον πωλητή, έναν άνδρα από τη Δυτ. Βιρτζίνια των ΗΠΑ, προκαταβολή 2000 δολαρίων αλλά ποτέ δεν έλαβε το αεροπλάνο. Όταν μάλιστα

[513] *Internet Fraud* (2007)
[514] http://www.saferinternet.gr/Default.aspx?tabid=38, Σεπτέμβριος 2006

κατάφερε να κάνει τον πωλητή να του απαντήσει με email ο τελευταίος τον κατηγόρησε για «παρενόχληση» και πούλησε το αεροπλάνο σε άλλον αγοραστή. Το θύμα κατήγγειλε το περιστατικό στο Κέντρο παραπόνων για το έγκλημα στο διαδίκτυο (Internet Crime Complaint Center- IC3).[515]

6.4.1.3. Απάτη με κόλπα Επαγγελματικών ευκαιριών

Κατά την απάτη με κόλπα επαγγελματικών ευκαιριών (Business Opportunity Schemes) το δέλεαρ που χρησιμοποιούν οι απατεώνες για να προσελκύσουν θύματα είναι η «ευκαιρία» γρήγορου πλουτισμού. Τα θύματα καλούνται να επενδύσουν από λίγα έως χιλιάδες δολάρια ή ευρώ στην ευκαιρία να κερδίσουν περισσότερα χρήματα χωρίς να μετακινηθούν από το σπίτι τους. Συχνά η απάτη βασίζεται στη χρήση του ίντερνετ και του υπολογιστή για την εκμετάλλευση των επιχειρηματικών ευκαιριών με εργασία από το σπίτι. Η αποστολή μαζικής ηλεκτρονικής αλληλογραφίας spam επιτρέπει στους απατεώνες να διαφημίσουν χιλιάδες επικερδείς ευκαιρίες. Βέβαια οι πληροφορίες και οι υποσχέσεις που παρέχονται για υποτιθέμενη οικονομική επιτυχία είναι συνήθως εντελώς ψεύτικες ή παρέχουν τελικά ασήμαντα κέρδη στα θύματα.[516]

6.4.1.4. Κλοπή ταυτότητας

Η κλοπή ταυτότητας (Identity Theft) είναι η παράνομη χρήση των στοιχείων ταυτότητας, όπως το όνομα, η ημερομηνία γέννησης, ο αριθμός μητρώου (φορολογικού, ασφαλιστικού κ.λπ.), κάποιου άλλου προσώπου. Η χρήση της ξένης ταυτότητας μπορεί να αφορά τη διάπραξη ή και τη διευκόλυνση δραστηριοτήτων που συνιστούν παραβίαση του νόμου.

Η κλοπή ταυτότητας διακρίνεται σε τέσσερις μορφές:

α) Η «οικονομική» κλοπή ταυτότητας (financial identity theft), όταν ο απατεώνας χρησιμοποιεί τα στοιχεία της ταυτότητας ενός άλλου ατόμου για οικονομικό όφελος. Αυτό μπορεί να περιλαμβάνει το άνοιγμα λογαριασμού στο όνομα του θύματος ή τη διαχείριση ενός ήδη υπάρχοντος λογαριασμού ή ακόμα για την αίτηση για λήψη δανείου.

β) Η «εγκληματική» κλοπή ταυτότητας (criminal identity theft), όταν ο εγκληματίας κατά τη σύλληψη του παρέχει στις διωκτικές αρχές τα στοιχεία της ταυτότητάς ενός άλλου προσώπου. Το αποτέλεσμα για το θύμα μπορεί να είναι η απόκτηση εγκληματικού φακέλου, χωρίς το ίδιο να το γνωρίζει, η άρνηση πρόσληψης σε εργασία, παροχής δανείων, δυσκολίες στις συναλλαγές, στιγματισμός κ.λπ.

γ) Η «αντιγραφή» ταυτότητας (Identity cloning), όταν ο απατεώνας οικειοποιείται την ταυτότητα του θύματος, ζώντας και δρώντας με τα δικά του στοιχεία.

δ) Η «επιχειρηματική ή εμπορική» κλοπή ταυτότητας (Business or commercial identity theft). Στην περίπτωση αυτή ο εγκληματίας χρησιμοποιεί το όνομα και τα στοιχεία, όχι ενός φυσικού προσώπου, αλλά μιας εταιρίας ή επιχείρησης για να προβεί σε παράνομες συναλλαγές.

Η κλοπή ταυτότητας μπορεί να διενεργείται όχι μόνο μέσω του ίντερνετ αλλά και με παραδοσιακές μεθόδους, όπως συμβαίνει και με τη κλοπή πιστωτικής κάρτας, με αγορά κλεμμένων αρχείων πελατών ξενοδοχείων, εστιατορίων κλπ. Ακόμα ψάξιμο σε κάδους

[515] Taylor Iris (2008)
[516] Βλ. Παράρτημα «Επενδυτικές/επαγγελματικές ευκαιρίες με εργασία από το σπίτι» και «Απάτη με email και με πρόσχημα την προσφορά εργασίας».

απορριμμάτων, κλοπή αλληλογραφίας, πορτοφολιού κλπ. για την απόκτηση οποιουδήποτε εγγράφου μπορεί να περιέχει τα στοιχεία της ταυτότητας κάποιου ατόμου.

Από την σκοπιά που μας ενδιαφέρει εδώ, το ίντερνετ αποτελεί, για τους εγκληματίες, ένα πρόσφορο τρόπο για την απόκτηση ευαίσθητων προσωπικών δεδομένων. Σύμφωνα με την έρευνα της Επιτροπής Ομοσπονδιακού Εμπορίου (FTC) των ΗΠΑ οι καταγγελίες για κλοπή ταυτότητας στο διαδίκτυο αφορούσαν το 36% του συνόλου των καταγγελιών για απάτη.

Χαρακτηριστική περίπτωση κλοπής ταυτότητας αυτή του M.R.B. 35 ετών από το Σαν Φρανσίσκο των ΗΠΑ με το ψευδώνυμο Iceman ο οποίος έκλεψε στοιχεία της ταυτότητας και των πιστωτικών καρτών 10.000 ατόμων εισβάλλοντας παράνομα (με hacking) στους υπολογιστές τραπεζών και υπηρεσιών επεξεργασίας πιστωτικών καρτών. Ο κατηγορούμενος πούλησε 100 αριθμούς πιστωτικών καρτών και στοιχεία ταυτότητας σε ένα άτομο από την Πεννσυλβάνια, λειτουργούσε επίσης ιστοσελίδα που παρείχε χώρο συζητήσεων ανάμεσα σε άτομα που έκλεβαν, πουλούσαν ή χρησιμοποιούσαν παράνομα πιστωτικές κάρτες τρίτων.

Η περίπτωση κλοπής ταυτότητας μέσω του διαμοιρασμού αρχείων ("peer-to-peer", p2p) στο διαδίκτυο συνιστά αυτή του G.T.K. που χρησιμοποιούσε τα δημοφιλή αυτά προγράμματα (p2p) για να εισβάλλει στα αρχεία των υπολογιστών άλλων χρηστών και να αποσπάσει πολύτιμες πληροφορίες για τα προσωπικά τους στοιχεία και τα οικονομικά τους δεδομένα. Έπειτα χρησιμοποιούσε αυτά τα στοιχεία για να εκδώσει πιστωτικές κάρτες με τις οποίες πραγματοποιούσε αγορές στο διαδίκτυο.[517]

6.4.1.5. Μέθοδοι απόσπασης προσωπικών δεδομένων

Κάποιες από τις κοινές πρακτικές ηλεκτρονικής συλλογής προσωπικών δεδομένων είναι το phishing, το spam και το pharming.

Ο όρος **phishing** (τεχνική ηλεκτρονικού ψαρέματος) έχει καθιερωθεί διεθνώς για να περιγράψει τη δημιουργία ιστοσελίδων επιχειρήσεων ή διευθύνσεων ηλεκτρονικού ταχυδρομείου (email) που μοιάζουν πραγματικές με σκοπό την παραπλάνηση ατόμων στο να καταχωρίσουν τα προσωπικά τους στοιχεία, όπως όνομα, αριθμούς λογαριασμού, πιστωτικών καρτών και κωδικούς πρόσβασης.

Οι επιθέσεις phishing χρησιμοποιούν την κοινωνική μηχανική και τεχνικά τρυκ για να υποκλέψουν τα προσωπικά δεδομένα των καταναλωτών. Από τη στιγμή που τα θύματα ανακαλύπτουν την κλοπή που υπέστησαν λίγα μπορούν να κάνουν για να αποκαταστήσουν την πιστοληπτική τους δυνατότητα, το καλό τους όνομα σε τραπεζικές «μαύρες λίστες» τύπου Τειρεσίας, ενώ θα πρέπει να παρακολουθούν τους λογαριασμούς τους για την πρόληψη νέων περιστατικών απάτης.

Σημειώνονται σημαντικά στοιχεία σχετικά με το phishing:

- Στον παγκόσμιο ιστό πραγματοποιούνται περισσότερες από 7 εκατομμύρια απόπειρες phishing κάθε μέρα.
- Οι Η.Π.Α. αποτελούν τη βάση από όπου εξαπολύονται οι περισσότερες επιθέσεις phishing στον κόσμο, φιλοξενώντας σχεδόν τους μισούς phishing servers (46%) από τους servers που υπάρχουν στον κόσμο
- Οι phishers εξελίσσονται και δημιουργούν νέες τεχνολογίες όπως Vishing και SMishing. Το Vishing είναι μία παραλλαγή του phishing όπου πιθανά θύματα παραπέμπονται στο να μην επιλέγουν ένα link, αλλά να καλούν σε ένα τηλέφωνο

[517] *Identity Theft (*2007)

δωρεάν το οποίο τους συνδέει αυτόματα με μία λίστα εγκληματιών όπου τους ζητούν να αποκαλύψουν προσωπικές πληροφορίες. Το SMishing είναι ένα μήνυμα phishing που στέλνεται μέσω μηνύματος SMS.[518]

Για την αποφυγή του phishing οι τράπεζες ενημερώνουν και συμβουλεύουν τους πελάτες τους – χρήστες των ηλεκτρονικών τραπεζικών υπηρεσιών (e-banking). Να μην απαντούν στα μηνύματα (e-mail) που τους στέλνουν επιτήδειοι με "φαινομενικό" αποστολέα την Τράπεζα και τους προτρέπουν να συνδεθούν με τον λογαριασμό τους. Θα πρέπει να τα αγνοήσουν και να μην προχωρήσουν σε καταχώρηση των στοιχείων τους.[519]

Το **spam** αποτελεί ανεπιθύμητη ηλεκτρονική αλληλογραφία (e-mail), που αποστέλλεται ταυτόχρονα σε πολλούς παραλήπτες. Υπάρχουν οι περιπτώσεις όπου αξιόπιστες εταιρίες ή απλοί χρήστες στέλνουν μαζικά e-mails σε λίστες αποδεκτών τους, εφόσον η μαζική αποστολή ηλεκτρονικού ταχυδρομείου αποτελεί έναν πολύ φθηνό και ταυτόχρονα μαζικό τρόπο διαφήμισης των προϊόντων και υπηρεσιών τους. Οι εταιρίες που αποστέλλουν μηνύματα spam χρησιμοποιούν ειδικό λογισμικό που ερευνά τις ιστοσελίδες και συλλέγει λογαριασμούς ηλεκτρονικού ταχυδρομείου που έχουν καταχωρηθεί σε αυτές. Για να καταφέρουν να παραπλανήσουν τον παραλήπτη και να τον κάνουν να ανοίξει το e-mail χρησιμοποιούν ψεύτικα στοιχεία αποστολέα και στο πεδίο «θέμα» τοποθετούν μια φράση που προσελκύει την προσοχή ή δημιουργεί την εντύπωση ότι το μήνυμα προέρχεται από φιλικό πρόσωπο. Για παράδειγμα: «Κερδίσατε στην κλήρωση!», «Χρόνια Πολλά» ή «Έχουμε καιρό να τα πούμε...»

Το spam ισοδυναμεί με τα άχρηστα μηνύματα ηλεκτρονικής αλληλογραφίας (junk mail) με διαφημιστικό κυρίως περιεχόμενο που αποστέλλονται στις διευθύνσεις χρηστών από διάφορους. Στις περισσότερες περιπτώσεις όμως τα spam αποστέλλονται με σκοπό την εξαπάτηση των παραληπτών. Συνήθη παραδείγματα είναι τα spam με περιεχόμενο που σχετίζεται με διαφημίσεις προϊόντων ή υπηρεσιών με πορνογραφία, φαρμακευτικά προϊόντα, φιλανθρωπία ή άλλες αμφίβολης αξιοπιστίας οικονομικές συναλλαγές. Κάποια άτομα παρασύρονται και απαντούν παρέχοντας τα στοιχεία που τους ζητούνται προκειμένου να αποκτήσουν τα προϊόντα της διαφήμισης. Οι απατεώνες έπειτα, χρησιμοποιούν τα στοιχεία αυτά για δικό τους όφελος, χωρίς φυσικά να αποστέλλουν τα προϊόντα.[520]

Σύμφωνα με μελέτη του πανεπιστημίου του Maryland, ο χρόνος που δαπανάται μόνο για τη διαγραφή του spam κοστίζει στις Αμερικανικές επιχειρήσεις 21,6 δις δολάρια ετησίως.

Τα μηνύματα spam αναγνωρίζονται από τα παρακάτω χαρακτηριστικά:

- Ο παραλήπτης δεν γνωρίζει τον αποστολέα.
- Οι εικόνες και τα κείμενα είναι σύνδεσμοι προς ιστοσελίδες. Επίσης τα κουμπιά «κλείσιμο», «ναι» και «όχι», δεν έχουν τη συνήθη λειτουργία τους, αλλά αντίθετα παραπέμπουν και αυτά σε ιστοσελίδες.
- Όταν το μήνυμα είναι σε ελληνική γλώσσα, συχνά έχει πολύ εμφανή συντακτικά και γραμματικά λάθη.
- Υπάρχει συχνά η ένδειξη «FW» (Forward, δηλαδή προώθηση) χωρίς αυτό βέβαια να σημαίνει απαραίτητα ότι πρόκειται για spam.

Το Pharming, είναι μια τεχνική όπου η προσπάθεια εξαπάτησης συνίσταται στην ανακατεύθυνση της διεύθυνσης της ιστοσελίδας που πληκτρολογεί ο χρήστης στο πρόγραμμα

[518] Πηγή: http://www.dart.gov.gr, Ιανουάριος (2008)
[519] Στο παράρτημα παρατίθεται ένα τέτοιο παραπλανητικό μήνυμα phishing
[520] *Internet Fraud (*2007)

περιήγησης. Η ανακατεύθυνση γίνεται, εν αγνοία του χρήστη, προς μια πλαστή ιστοσελίδα – παγίδα που έχει κατασκευάσει ο δράστης με σκοπό την απόσπαση εμπιστευτικών πληροφοριών και την κλοπή ταυτότητας του θύματος. Η τεχνική εκμεταλλεύεται τις αδυναμίες των διακομιστών DNS για να αποδώσουν ψεύτικες πληροφορίες διεύθυνσης ιστοχώρων.[521]

6.4.1.6. Ηλεκτρονική απάτη σε συναλλαγές του χρηματιστηρίου

Ηλεκτρονική απάτη σε συναλλαγές του χρηματιστηρίου συμβαίνει όταν επενδυτές μετοχών του χρηματιστηρίου που χρησιμοποιούν το διαδίκτυο ή το ηλεκτρονικό ταχυδρομείο τροφοδοτούνται σκόπιμα με παραπλανητική πληροφόρηση όσον αφορά την προβλεπόμενη συμπεριφορά των μετοχών. Οι επενδυτές, μέσω της εσφαλμένης φήμης που διαδίδεται στο διαδίκτυο, μπορεί να οδηγηθούν στην προσδοκία ότι η τιμή για μια μετοχή θα ανέβει λόγω μιας καινοτομίας που η εταιρεία δήθεν πρόκειται να εφαρμόσει και θα έχει ως αποτέλεσμα την αύξηση της παραγωγής, των εσόδων και συνακόλουθα της κερδοφορίας της εν λόγω εταιρείας.[522] Η απάτη προϋποθέτει ότι οι επενδυτές δεν διασταυρώνουν την πληροφορία που δέχονται από το ίντερνετ με άλλες πηγές. Οι απατεώνες περιμένουν μέχρι να αυξηθεί ικανοποιητικά η τιμή της μετοχής οπότε και πωλούν το δικό τους μερίδιο μετοχών αποκομίζοντας μεγάλα κέρδη ενώ οι εξαπατημένοι επενδυτές απομένουν με ένα στοκ υποτιμημένων πλέον μετοχών. Η τεχνική αυτή είναι διεθνώς γνωστή ως «φούσκωσε-και-παράτα/πούλα (pump-and-dump)».

Η εξαπάτηση μπορεί να γίνει και από την αντίθετη φορά. Οι «πληροφορίες» δηλαδή που διαχέονται στο ίντερνετ οδηγούν στην απαξίωση ορισμένων μετοχών τις οποίες αγοράζουν οι επιτήδειοι έναντι ευτελούς αξίας για να πωλήσουν αργότερα σε πολύ υψηλότερες τιμές. Εδώ τα θύματα δεν είναι μόνο οι εξαπατημένοι επενδυτές αλλά και η ίδια η εταιρία της οποίας η αξιοπιστία και το καλό εμπορικό όνομα στιγματίζεται.[523]

Χαρακτηριστική περίπτωση αυτή ενός 15χρονου ο οποίος κατά την περίοδο άνθησης των χρηματιστηρίων κατά το 2000, όταν η παρακολούθηση τιμών των μετοχών μέσω του διαδικτύου ήταν καθημερινή ενασχόληση πολλών ατόμων, έδειξε το πόσο εύκολο είναι να πραγματοποιήσει κάποιος το «pump-and-dump». Ο 15χρονος αγόρασε μετοχές με μηδενική αξία και έπειτα προώθησε την αύξηση της τιμής τους με δελτία τιμών ή πίνακες μηνυμάτων (message boards). Όταν κι άλλοι επενδυτές αγόρασαν πακέτα των μετοχών ο νεαρός πούλησε τις δικές του αποκομίζοντας κέρδη. Όταν η περίπτωση του υπέπεσε στην αντίληψη της Επιτροπής Ασφάλειας και Συναλλαγών των ΗΠΑ (U.S. Securities and Exchange Commission - SEC[524]), κατέθεσε αγωγή εναντίον του. Ο 15χρονος παρότι δεν παραδέχτηκε ότι έκανε κάτι κακό, τελικά συμβιβάστηκε επιστρέφοντας ένα μέρος από τα κέρδη του και συμφώνησε να μην το επαναλάβει.[525]

---

[521] Hallam-Baker Phillip, (2005)

[522] Κουράκης Νέστορας., *Ηλεκτρονικά Εγκλήματα και Εγκλήματα στο Διαδίκτυο* στο Λάζος Γρηγόρης (2004), σ.86

[523] *Internet Fraud (*2007)

[524] SEC, Κρατική υπηρεσία των ΗΠΑ, ιδρύθηκε το 1934, με καθήκον την προστασία των επενδυτών και των ασφαλιστικών αγορών. Πηγή http://financial-dictionary.thefreedictionary.com, ανακτήθηκε Απρίλιος (2008)

[525] http://www.abcsearch.com/jump2/?affiliate=tcz&subid=320&terms=stock%20fraud, ανακτήθηκε Απρίλιος (2008)

6.4.1.7. Επενδυτικές απάτες

Οι επενδυτικές απάτες (Investment Fraud) έχουν διάφορες μορφές. Συνήθως οι απατεώνες υπόσχονται στους επενδυτές υψηλά και γρήγορα κέρδη, ανεξαρτήτως ποσού αρχικής επένδυσης, σε μετοχές, αμοιβαία κεφάλαια, ξένα νομίσματα, χρυσό, πετρέλαιο, παλαιά νομίσματα και διάφορα άλλα εμπορεύματα.

Χρησιμοποιούνται διάφορα επενδυτικά σχήματα και τεχνικές προσέλκυσης των πιθανών θυμάτων. Οι πιο συνηθισμένες είναι οι επενδυτικές πυραμίδες, χρηματιστηριακές απάτες, επενδυτικές απάτες μέσω του διαδικτύου, οι απάτες προς μέλη συγκεκριμένων πληθυσμιακών ομάδων (affinity fraud). Στις περισσότερες περιπτώσεις τα επενδυτικά αυτά σχήματα πωλούνται από άτομα που είναι εκτός των αναγνωρισμένων χρηματιστηριακών και ασφαλιστικών γραφείων.

Οι επενδυτικές πυραμίδες αφορούν τη συλλογή χρηματικών κεφαλαίων από νέους επενδυτές για την αποπληρωμή των παλαιοτέρων. Παρά την νομιμοφανή όψη τους τέτοια πολυεπίπεδα επενδυτικά προϊόντα υπόσχονται γρήγορα κέρδη σε σύντομο διάστημα και τελικά καταρρέουν επειδή κάποια στιγμή δεν μπορούν να εντάξουν νέους επενδυτές για να συγκεντρώσουν χρήματα και να πληρώσουν τους παλαιότερους, έτσι πολλοί χάνουν τα χρήματα τους.

Στις επενδυτικές απάτες εντάσσονται και οι χρηματιστηριακές απάτες μέσω της χειραγώγησης της τιμής μετοχών. Όπως είδαμε και παραπάνω για την Ηλεκτρονική απάτη σε συναλλαγές του χρηματιστηρίου κάποιοι αγοράζουν ένα αριθμό μετοχών, διοχετεύουν παραπλανητικές πληροφορίες, που δήθεν διαθέτουν «εκ των έσω», για την εξέλιξη της τιμής τους και πείθουν άλλους επενδυτές να τις αγοράσουν σε μεγαλύτερη τιμή. Έπειτα όμως η τιμή της μετοχής «ξεφουσκώνει», οι απατεώνες κερδίζουν και οι επενδυτές χάνουν τα χρήματα τους.

Οι απάτες προς μέλη συγκεκριμένων ομάδων (affinity fraud) αποτελούν προσπάθεια εξαπάτησης των μελών ιδιαίτερων θρησκευτικών, εθνοτικών, επαγγελματικών ή κοινωνικών ομάδων με την πρόφαση παροχής βοήθειας προς αυτά. Το στοιχείο της εμπιστοσύνης και της αλληλεγγύης μεταξύ των μελών τέτοιων ομάδων εκμεταλλεύονται οι απατεώνες για να τα πείσουν να συμμετέχουν σε επενδύσεις άνευ αξίας. Η απάτη αυτού του είδους μπορεί να έχει διάφορες μορφές όπως προγράμματα δωρεών σε εκκλησίες ή συναλλάγματος για αλλοδαπούς μετανάστες.

Το ίντερνετ χρησιμοποιείται από τους απατεώνες για να προπαγανδίσουν αλλά να εκτελέσουν όλα τα είδη από τις επενδυτικές απάτες που περιγράφονται παραπάνω. Οι τρεις πιο συνηθισμένοι τρόποι για να διασπείρουν την «πληροφορία» για την επένδυση μέσω του διαδικτύου είναι τα μηνύματα επενδυτικών ειδήσεων στο ηλεκτρονικό ταχυδρομείο (investment newsletters), οι διαδικτυακοί πίνακες ανακοινώσεων (bulletin boards) και τα μαζικά μηνύματα ηλεκτρονικής αλληλογραφίας (spam).

Για τους υποψήφιους επενδυτές είναι πολύ δύσκολο να διακρίνουν τη διαφορά μεταξύ των πραγματικών και των πλασματικών επενδυτικών προϊόντων. Για αυτό η Επιτροπή Ασφαλειών και Συναλλαγών των ΗΠΑ (U.S. Securities and Exchange Commission) συμβουλεύει τους επενδυτές να μην βασίζονται αποκλειστικά σε πληροφορίες που βρίσκουν σε αυτά τα

μηνύματα που τους αποστέλλονται μέσω του διαδικτύου αλλά να τις διασταυρώνουν πριν προχωρήσουν στην επένδυση.[526]

Χαρακτηριστικές περιπτώσεις τέτοιας απάτης αποτελούν:

1. Επενδυτικές πυραμίδες (Ponzi schemes) στην Αλβανία. Δεν είναι υπερβολική η άποψη που υποστηρίζει ότι ένα μεγάλο μέρος του Αλβανικού πληθυσμού εγκατέλειψε τη χώρα μετά το 1997 όπου η μικρή αυτή χώρα γνώρισε την κατάρρευση των εκεί πυραμίδων (Ponzi schemes), οι οποίες υποστηρίζονταν από την κυβέρνηση.

Οι πυραμίδες στην Αλβανία άρχισαν να αναταράσσονται το φθινόπωρο του 1996, όταν μερικές άρχισαν να μειώνουν τα ποσοστά κερδών και έβαζαν περιορισμούς στους επενδυτές, πχ. επέτρεπαν ανάληψη κερδών αλλά όχι κεφαλαίου. Η διάρκεια τέτοιων πυραμίδων έχει σαν βασική προϋπόθεση τη φερεγγυότητα και εμπιστοσύνη του κοινού προς αυτές, οπότε μόλις αυτή η πίστη κλονίστηκε σταμάτησαν οι νέες καταθέσεις. Μέχρι τα μέσα Δεκεμβρίου 1996 δύο από τις μικρότερες πυραμίδες είχαν καταρρεύσει και αμφιβολίες άρχισαν να εκφράζονται για τη βιωσιμότητα των μεγαλύτερων πυραμίδων στις οποίες είχαν επενδυθεί πολλά εκατομμύρια. Το κοινό άρχισε να διαμαρτύρεται ενώ η κυβέρνηση και ο Πρόεδρος αρχικά τους είχαν βεβαιώσει για τη νομιμότητα των πυραμίδων. Με την κατάρρευση της κεντρικής πυραμίδας που δραστηριοποιούνταν στο νότο της Αλβανίας η εξέγερση ξέσπασε και ξεκίνησε η πολιτική και κοινωνική κρίση. [527]

2. Μια περίπτωση από τις ΗΠΑ συνιστά αυτή των αδερφών G. και R.A. οι οποίοι κατηγορήθηκαν για τη δημιουργία πυραμίδας τύπου Ponzi από το 1996 έως το 2003 όπου και συγκέντρωσαν εκατομμύρια δολαρίων από πολλούς επενδυτές με το πρόσχημα επένδυσης σε ακίνητα. Οι αδελφοί αντιμετώπισαν 12 κατηγορίες μεταξύ των οποίων ηλεκτρονική απάτη, συνομωσία και οι ποινές τους ήταν από 3 έως 8 χρόνια (37 έως 97 μήνες).[528]

6.4.1.8. Απάτες με πιστωτικές κάρτες και κάρτες ανάληψης μετρητών (ATM)

Λόγω της μεγάλης διάδοσης και έκτασης των συναλλαγών στο διαδίκτυο οι απάτες με πιστωτικές κάρτες λαμβάνουν μορφή χιονοστιβάδας. Αποτελούν την πιο κοινή μορφή απάτης και την πιο δύσκολα αντιμετωπίσιμη. Αρκετά μάλιστα, δίκτυα οργανωμένου εγκλήματος, ακόμα και διακίνησης ναρκωτικών, έχουν κάνει στροφή στη «καριέρα» τους προς αυτή τη πιο απλή, αποδοτική και σχετικά ασφαλέστερη εγκληματική δραστηριότητα.

Οι περιπτώσεις απάτης με πιστωτικές κάρτες που διαπράττονται στο διαδίκτυο εδώ εξετάζονται ταυτόχρονα με αυτές που διαπράττονται στο κανονικό περιβάλλον λόγω της άμεσης εμπλοκής των ηλεκτρονικών με τις φυσικές μεθόδους πραγματοποίησης τόσο των συναλλαγών όσο και των κλοπών.

Η απάτη με πιστωτική κάρτα αφορά την μη εξουσιοδοτημένη χρήση της και με πρόθεση εξαπάτηση για την απόκτηση αγαθού με κάποια αξία.[529]

Οι διαδικτυακοί πωλητές απαιτούν στοιχεία της πιστωτικής κάρτας του πελάτη, όπως ονοματεπώνυμο, αριθμό κάρτας, ημερομηνία λήξης κλπ., χωρίς τη φυσική παρουσία του πελάτη, έτσι δημιουργούνται ευκαιρίες που διάφοροι επιτήδειοι εκμεταλλεύονται για να εξαπατήσουν τους συναλλασσόμενους. Κλεμμένες ή πλαστογραφημένες πιστωτικές κάρτες

[526] *Securities/Investment Fraud* **(**2007)
[527] http://www.geocities.com/apatesgr/ponzi.htm#albania, ανακτήθηκε Απρίλιος (2008)
[528] *Securities/Investment Fraud* **(**2007)
[529] *Credit Card Fraud* (2007)

χρησιμοποιούνται για αγορές από το ίντερνετ. Με την ανακάλυψη ότι η χρήση της πιστωτικής κάρτας ήταν παράνομη, η τράπεζα που εξέδωσε την κάρτα αντιλογίζει το ποσό που χρεώθηκε στον πελάτη της απαιτώντας το πίσω από το κατάστημα που πραγματοποιήθηκε η αγορά. Από τη στιγμή που το εμπόρευμα έχει ήδη σταλεί, το κατάστημα χάνει τόσο το ίδιο το εμπόρευμα όσο και την είσπραξη της αξίας του. Ο αυθεντικός κάτοχος της κάρτας απευθυνόμενος στην τράπεζά του πρέπει να αμφισβητήσει τις ύποπτες χρεώσεις στο λογαριασμό του. Έτσι, στις περισσότερες των περιπτώσεων τέτοιου είδους απάτης, εκτός από το διαδικτυακό κατάστημα, θύμα μπορεί να είναι ακόμα ο κάτοχος της κάρτας και η εκδότρια αρχή της κάρτας (τράπεζα). Ακόμα τα ποινικά αδικήματα που διαπράττονται σε τέτοιες περιπτώσεις είναι επίσης περισσότερα από ένα, γιατί εκτός από την αρχική κλοπή της κάρτας προκύπτουν και εγκλήματα από την παράνομη χρήση της.[530]

Η κλοπή αλληλογραφίας από τις εισόδους πολυκατοικιών ή ακόμα και το ψάξιμο στα οικιακά απορρίμματα[531] χρησιμοποιείται για να αποκτηθούν αντίγραφα λογαριασμών με όλα τα ευαίσθητα προσωπικά στοιχεία που απαιτούνται για τη πραγματοποίηση συναλλαγών στο διαδίκτυο ή μέσω τηλεφώνου, χωρίς τη φυσική παρουσία του νόμιμου κατόχου ή της κάρτας καθαυτής.

Σήμερα πλέον είναι εφικτή η χρήση πιο «καθαρών» μεθόδων, με την υποκλοπή ευαίσθητων προσωπικών δεδομένων με ηλεκτρονικό τρόπο. Μέσω του διαδικτύου, οι κυβερνο-εγκληματίες μπορούν είτε να αγοράσουν, είτε να υποκλέψουν τα στοιχεία αυτά από ιστοσελίδες που διαθέτουν δεδομένα χρηστών και των πιστωτικών καρτών τους. Συχνή είναι ακόμα η πλαστογράφηση, με τη χρήση σύγχρονων ηλεκτρονικών υπολογιστών, της κάρτας (πιστωτικής ή ανάληψης μετρητών) ή μόνο της μαγνητικής ταινίας που φέρουν οι κάρτες και που περιέχουν όλα τα απαραίτητα στοιχεία του κατόχου. Οι απατεώνες δημιουργούν έτσι πλαστούς λογαριασμούς χρήστη και πραγματοποιούν πολλαπλές συναλλαγές αποκομίζοντας τεράστια παράνομα κέρδη.

Μια άλλη μέθοδος είναι η εγκατάσταση κακόβουλων προγραμμάτων, που είδαμε παραπάνω όπως spyware, Trojans ή “key loggers” που επιτρέπουν στον υποκλοπέα να παρακολουθεί τους χαρακτήρες που πληκτρολογεί ο χρήστης στον υπολογιστή του κατά την πραγματοποίηση συναλλαγών στο διαδίκτυο.

Αρκετές είναι και οι περιπτώσεις κλοπής των στοιχείων της πιστωτικής κάρτας πελατών από υπεύθυνους και υπαλλήλους επιχειρήσεων, ξενοδοχείων, εστιατορίων κ.λπ. οι οποίοι στη συνέχεια συνήθως πωλούν τα στοιχεία αυτά σε απατεώνες. Χαρακτηριστική είναι η περίπτωση σύλληψης κυκλώματος στο Σικάγο, όπου 12 άτομα μεταξύ των οποίων ιδιοκτήτες, διευθυντές και υπάλληλοι ξενοδοχείων έκλεβαν τους αριθμός των πιστωτικών καρτών από πελάτες τους που στη συνέχεια πωλούσαν σε κλεπταποδόχο. Μέσα σε έξι χρόνια δράσης ο αριθμός των κλεμμένων αριθμών καρτών έφτασε τις δέκα χιλιάδες.

Αντίστοιχη περίπτωση με την εμπλοκή υπαλλήλων από 40 εστιατόρια αποκαλύφθηκε πρόσφατα σε διάφορες πολιτείες των ΗΠΑ. Οι σερβιτόροι κατέγραφαν τα στοιχεία των πιστωτικών καρτών από πελάτες και στη συνέχεια τα πωλούσαν σε άτομα τα οποία αποκόμισαν πάνω από 3 εκατ. δολάρια από παράνομες συναλλαγές που πραγματοποίησαν

[530] *Credit Card Fraud* (2007)

[531] Σύμφωνα με έρευνα του Δήμου του Νόττινγχαμ ένας από τους πέντε οικιακούς κάδους απορριμμάτων περιέχει στοιχεία που θα μπορούσαν να χρησιμοποιηθούν από απατεώνες για τις παράνομες δραστηριότητες τους. Πηγή: Burden Kit & Palmer Creole (2003)

μέσω αυτών ενώ οι σερβιτόροι λάμβαναν 35 έως 50 δολάρια για κάθε κάρτα. Το κύκλωμα έδρασε από το Νοέμβριο του 2005 έως τον Απρίλιο του 2007.[532]

Στην Ελλάδα οι αρχές συνέλαβαν αλλοδαπό που κατείχε και χρησιμοποιούσε 120 κάρτες ανάληψης μετρητών.[533]

Έχει υπολογιστεί ότι το ποσοστό της απάτης με πιστωτικές κάρτες είναι 0,7% (ή 7 σεντς για κάθε 100 δολάρια) επί των παγκόσμιων συναλλαγών. Σε απόλυτα μεγέθη οι παράνομες συναλλαγές με πιστωτικές κάρτες στις Ηνωμένες Πολιτείες έφθαναν τα 788 εκατ. δολάρια για το 2004. Παρόμοιες εκτιμήσεις αναφέρουν ότι οι αντίστοιχες απώλειες στη μεγάλη Βρετανία για το 2006, ήταν 428 εκατομμύρια λίρες, ενώ για την Αυστραλία οι απώλειες ήταν 4 σεντς για κάθε 100 δολάρια συναλλαγών.

Σύμφωνα με την έρευνα του Cybersource το 2006 σε διαδικτυακές επιχειρήσεις, 3 δισεκατομμύρια δολάρια, ήτοι το 1,4% του συνόλου των εσόδων από συναλλαγές στο διαδίκτυο χανόταν λόγω πιστωτικής απάτης. Ακόμα η έρευνα βρήκε ότι το 1,3% του συνόλου των παραγγελιών προϊόντων οδήγησε σε περιπτώσεις απάτης. Το μέσο ποσό συναλλαγών, για τις περιπτώσεις απάτης ήταν 152 δολάρια ενώ για τις νόμιμες συναλλαγές 123 δολάρια.[534]

6.4.1.9. Απάτες με επιταγές

Απάτη με επιταγές αποτελεί η παραποίηση, αλλοίωση, πλαστογράφηση των στοιχείων μιας επιταγής ή η συνειδητή έκδοση μιας επιταγής που αντιστοιχεί σε έναν λογαριασμό που έχει κλείσει ή δεν έχει επαρκή κεφάλαια για να καλύψει το ποσό για το οποίο εκδόθηκε η επιταγή (ακάλυπτη).

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να διενεργείται η απάτη. Μεταξύ των τεχνικών αυτών είναι το άνοιγμα εικονικών λογαριασμών, η έκδοση επιταγών που αντιστοιχούν σε κλειστούς λογαριασμούς ή λογαριασμούς που δεν διαθέτουν επαρκή ποσά για την κάλυψη της επιταγής, η μεταφορά εικονικών χρηματικών ποσών μεταξύ πολλαπλών τραπεζικών λογαριασμών (check kiting), η αλλοίωση, παραχάραξη ή πλαστογράφηση των επιταγών.

Ιδιαίτερο ενδιαφέρον, από την άποψη της παρούσας εργασίας, παρουσιάζουν οι περιπτώσεις της αλλοίωσης ή παραχάραξης των επιταγών με σύγχρονα ηλεκτρονικά μέσα και του ανοίγματος λογαριασμών στο όνομα ατόμων που έχουν πέσει θύματα ηλεκτρονικής κλοπής της ταυτότητας.

Με το άνοιγμα εικονικών τραπεζικών λογαριασμών, βάσει στοιχείων ταυτότητας που είναι προϊόν (κυρίως ηλεκτρονικής) κλοπής, ο απατεώνας καταθέτει πλαστές ή αλλοιωμένες επιταγές και έπειτα αποσύρει το χρηματικό ποσό πριν η τράπεζα ή το θύμα αποκαλύψει την απάτη.

Σύγχρονες μονάδες ηλεκτρονικών υπολογιστών εξοπλισμένες με περιφερειακά όπως εκτυπωτές, σαρωτές τελευταίας τεχνολογίας, παρέχουν τη δυνατότητα στους απατεώνες να εμπλουτίσουν τις μεθόδους παραχάραξης ή πλαστογράφησης. Αφού αρχικά σβηστούν τα πραγματικά στοιχεία των επιταγών με τη χρήση χημικών μέσων, κυρίως οξέων, εκτυπώνονται έπειτα πάνω σε αυτή, μέσω υπολογιστή, τα πλαστά στοιχεία που επιθυμούν η παραχαράχτες. Η πλαστογράφηση μπορεί να γίνει επίσης με την οπτική ανάγνωση της αρχικής επιταγής μέσω

[532] Πηγή *CBS*, http://www.cbsnews.com/stories/2007/04/21/national/printable2713680.shtml., July (2007)
[533] http://www.ethnos.gr/article.asp?catid=11424&subid=2&tag=8400&pubid=820496 , Βλ. Παράρτημα για είδηση «Σύλληψης κυκλώματος παραχαρακτών».
[534] *Credit Card Fraud* (2007)

σαρωτή (σκάνερ), την αλλοίωση των στοιχείων της μέσω λογισμικού που διαθέτουν οι περισσότεροι υπολογιστές και την εκτύπωση της πλαστής επιταγής με ένα ποιοτικό λέιζερ εκτυπωτή. Με τον ίδιο τρόπο μπορούν να χρησιμοποιηθούν υπολογιστές για την πλαστογράφηση και άλλων μέσων πληρωμής όπως ταξιδιωτικών επιταγών, πιστωτικών καρτών, εμβασμάτων, εντολών πληρωμής, χαρτονομισμάτων αλλά και προσωπικών εγγράφων όπως ταυτοτήτων, διαβατηρίων, καρτών ασφάλισης, αδειών οδήγησης κλπ.[535]

6.4.1.10. Τυχερά παιγνίδια στο διαδίκτυο

Το ίντερνετ παρέχει σε «τζογαδόρους» εύκολη και παγκόσμιας εμβέλειας πρόσβαση σε χώρους τυχερών παιγνιδιών όπως τα κλασικά παιγνίδια του καζίνο, οι λοταρίες και τα κάθε είδους αθλητικά και αγωνιστικά στοιχήματα.

Τα τυχερά παιγνίδια (τζόγος) στο ίντερνετ αφορούν τη διαδικτυακή δραστηριότητα ατόμων που παίζουν κάποιο παιγνίδι με το στοιχείο της τύχης ή στοιχηματίζουν έναντι κάποιου τιμήματος για να αποκομίσουν κάποιο αβέβαιο οικονομικό όφελος.

Το κέντρο παραπόνων για το διαδικτυακό έγκλημα[536], το οποίο παρέχει στα θύματα απάτης μέσω του ίντερνετ ένα μηχανισμό διαδικτυακών καταγγελιών, ορίζει την απάτη μέσω τυχερών παιγνιδιών ως "τη διακινδύνευση χρημάτων έναντι της πιθανότητας να κερδηθεί ένα μεγαλύτερο χρηματικό ποσό ενώ υπάρχει παραπλάνηση ως προς την παρουσίαση των πιθανοτήτων ή των γεγονότων του παιγνιδιού". Συχνά οι παραπλανητικές ιστοσελίδες με τυχερά παιγνίδια εξαπατούν με "πειραγμένα" ή "στημένα" παιγνίδια, προσφέρουν κέρδη στα οποία ο παίκτης δεν μπορεί τελικά να έχει πρόσβαση ή απλά δεν του αποστέλλουν τα κέρδη ενώ ταυτόχρονα κακοδιαχειρίζονται (εκμεταλλεύονται) τις προσωπικές πληροφορίες και τα στοιχεία των παικτών. Ιδιαίτερα δράστες από ιστοσελίδες του εξωτερικού προσελκύουν άτομα δελεάζοντάς τα ότι θα κερδίσουν χρήματα από διεθνείς κληρώσεις και λοταρίες και έπειτα δεν αποστέλλουν τα υποτιθέμενα κέρδη ή απαιτούν πληρωμή για αμοιβές και φόρους.

Τα δημοφιλέστερα διαδικτυακά παιγνίδια είναι αυτά του καζίνο, στυλ Λας Βέγκας, και τα αθλητικά κυρίως, ποδοσφαιρικά στοιχήματα. Για τα τελευταία παρέχεται μάλιστα συνεχής ενημέρωση όσον αφορά στατιστικά και αγωνιστικές πληροφορίες με αποτέλεσμα αυτά τα στοιχήματα να είναι ευκολότερα και περισσότερο κατανοητά ακόμα και για τους αρχάριους παίκτες. Η διάδοσή τους διευκολύνεται και από το γεγονός ότι, αντίθετα με τον παραδοσιακό τζόγο, μέσω του ίντερνετ οι παίκτες διαθέτουν από το σπίτι και την εργασία τους εύκολη πρόσβαση, όχι μόνο σε τέτοιες ιστοσελίδες αλλά και στα χρήματά τους μέσω διαδικτυακών τραπεζικών συναλλαγών. Σύμφωνα με άρθρο της USA Today, κατά το 2005 υπήρχαν περισσότερα από 2000 ιστοσελίδες με τυχερά παιγνίδια που δημιουργούν 10 δις δολάρια τζίρο το χρόνο.

Παράνομα χαρακτηρίζονται τα τυχερά παιγνίδια όταν αυτά λαμβάνουν χώρα από ή προς τοποθεσίες όπου απαγορεύονται τέτοιου είδους δραστηριότητες ή ο τζόγος είναι απλά μια κάλυψη για εγκληματικές δραστηριότητες όπως ξέπλυμα βρώμικου χρήματος ή απάτες.

Όπως συμβαίνει με οποιαδήποτε κερδοφόρα επιχείρηση, έτσι και τα διαδικτυακά τυχερά παιγνίδια μπορούν να χρησιμοποιηθούν για παράνομες δραστηριότητες. Μια συνηθισμένη τέτοια δραστηριότητα είναι το ξέπλυμα "μαύρου" χρήματος, από συμμορίες, μαφιόζους και τρομοκράτες.[537]

[535] *Check Fraud (*2007)
[536] The Internet Crime Complaint Center (2007)
[537] *Internet Gambling (*2007)

Οι απατεώνες συνήθως έχουν τη βάση τους σε τρίτες χώρες, σε σχέση με τη χώρα όπου έχουν στήσει την ιστοσελίδα τους και τις χώρες των πιθανών θυμάτων, ενώ παράλληλα η σχετική ανωνυμία που προσφέρει το ίντερνετ κάνουν την ανακάλυψη και δίωξη τους πολύ δύσκολη υπόθεση.[538]

6.4.2. Ξέπλυμα Χρήματος

Το ξέπλυμα (μαύρου) χρήματος αφορά τα μέσα και τις πρακτικές που χρησιμοποιούν οι εγκληματίες για να καλύψουν την προέλευση των κερδών από τις παράνομες δραστηριότητες τους. Η διαδικασία αυτή του φιλτραρίσματος περιλαμβάνει σειρά διαδοχικών μεταβιβάσεων των χρημάτων έως ότου αυτό θεωρηθεί «καθαρό» ή ότι προέρχεται από νόμιμες δραστηριότητες.

Το κοινό στοιχείο όλων των προσπαθειών για να ξεπλυθεί το παράνομο χρήμα είναι η απόκρυψη της προέλευσης και της ιδιοκτησίας των χρημάτων, η διατήρηση του ελέγχου των κεφαλαίων και η αλλοίωση της μορφής του χρήματος ώστε να συρρικνωθούν τα τεράστια ποσά μετρητών που αποκτήθηκαν με τις παράνομες δραστηριότητες.

Η ανακάλυψη και εξακρίβωση των κεφαλαίων που είναι αποτέλεσμα ξεπλύματος, αποτελεί μια πολύ δύσκολη υπόθεση εξαιτίας της πολυπλοκότητας και του αριθμού των μεταβιβάσεων, της τεχνολογικής εξέλιξης αλλά και της διαφορετικής νομοθεσίας που ισχύει σε διαφορετικές χώρες με αποτέλεσμα να μην ευνοείται η μεταξύ τους συνεργασία στον τομέα της έρευνας και της δίωξης τέτοιων περιπτώσεων.[539] Σημαντικό ρόλο, στον τομέα της δυσκολίας εξακρίβωσης τέτοιων εγκλημάτων, παίζει και η πολυπλοκότητα των εγκληματικών δραστηριοτήτων, όπως λαθρεμπόριο όπλων ή ναρκωτικών, διαφθορά, παράνομη διακίνηση ανθρώπων (trafficking) κλπ., που ενέχονται στη δημιουργία του «βρώμικου» χρήματος. Αποτελεσματικό «ξέπλυμα χρήματος» σημαίνει για τους δράστες ότι η εξακρίβωση των εγκλημάτων και της ταυτότητας τους είναι πολύ δύσκολη για τις αρχές. Από την άλλη πλευρά η ανεύρεση και παρακολούθηση των ιχνών του χρήματος οδηγεί συχνά τις διωκτικές αρχές στην αποκάλυψη και καταπολέμηση τέτοιων μορφών εγκλήματος.

Η κάλυψη των παράνομων κεφαλαίων και η ανάμιξή τους με κεφάλαια νόμιμων επιχειρήσεων αποτελεί σε τέτοιες περιπτώσεις κοινή πρακτική των παράνομων αλλά και σημαντική απειλή για τις νόμιμες επιχειρήσεις. Το καλό όνομα της νόμιμης επιχείρησης αλλά και κατ' επέκταση η οικονομική της ευημερία και το συμφέρον των επενδυτών και των πιστωτών της διακυβεύονται από την εμπλοκή της, εκούσια ή ακούσια, σε τέτοιες δραστηριότητες. Σε ακραίες περιπτώσεις μπορεί να απειλείται και η οικονομική και πολιτική σταθερότητα μικρών κρατών όταν τα κεφάλαια που προέρχονται από παράνομες πηγές αποτελούν ένα όχι ευκαταφρόνητο κομμάτι του εθνικού πλούτου.[540]

Ένα σημαντικό κομμάτι του ξεπλύματος μαύρου χρήματος μπορεί κάλλιστα να χαρακτηριστεί ηλεκτρονικο-οικονομικό έγκλημα επειδή διενεργείται με σύγχρονα ηλεκτρονικά μέσα, δίκτυα τηλεπικοινωνιών και μέσω του διαδικτύου. Η επικάλυψη των παράνομων κεφαλαίων μπορεί πραγματοποιείται μέσω μιας αλυσίδας μεταφορών με ηλεκτρονικά μέσα όπως χρήση υπηρεσιών e-banking ή phone-banking δηλαδή ηλεκτρονικές συναλλαγές μέσω ίντερνετ ή τηλεφώνου. Με τον ίδιο τρόπο μπορεί να εξυπηρετείται και το στάδιο της ολοκλήρωσης όπου το βρώμικο χρήμα κατατίθεται άμεσα σε τραπεζικό οργανισμό

[538] *Internet Gambling* (2007)
[539] *Money laundering* (2006)
[540] Grabosky Peter & Smith Russell. (1998), σ.175

όπου χρησιμοποιείται έπειτα για δανειοδοτήσεις νόμιμων επιχειρήσεων με το οποίο κάνουν επενδύσεις. Τέτοια δάνεια δίνουν φοροαπαλλαγές πράγμα που επαυξάνει τις απώλειες από τις παράνομες δραστηριότητες για το κοινωνικό σύνολο.[541]

Στο απρόσωπο περιβάλλον του ίντερνετ, οι επιχειρήσεις είναι πιο ευάλωτες σε περιπτώσεις ξεπλύματος χρημάτων εφόσον δεν μπορούν να γνωρίζουν με ασφάλεια τα πραγματικά στοιχεία των πελατών τους, οι διαδικασίες είναι αυτοματοποιημένες και δεν μπορούν να εντοπίσουν ύποπτες μεταφορές χρημάτων. Για τους λόγους αυτούς απαιτείται από τις επιχειρήσεις, όπως τράπεζες, χρηματιστηριακά πρακτορεία κλπ. που δραστηριοποιούνται στους σχετικούς τομείς, να τηρούν με προσήλωση τη σχετική νομοθεσία και αυστηρές διοικητικές διαδικασίες ελέγχου της ταυτότητας των πελατών και διαδικασίες τήρησης αρχείων που θα αποτρέπουν και θα αποκαλύπτουν περιπτώσεις ξεπλύματος. Για παράδειγμα στις ΗΠΑ, ο νόμος περί παράνομων εσόδων του 2002 (Proceeds of Crime Act 2002) προβλέπει ότι κάθε νόμιμη επιχείρηση, που έχει βάσιμες υποψίες ότι κάποιος πελάτης της πιθανόν να εμπλέκεται σε περιπτώσεις ξεπλύματος, έχει την υποχρέωση να το καταγγείλει αντιμετωπίζοντας ποινική δίωξη αν δε το κάνει. Πάντως, παρά τα αυξημένα νομοθετικά μέτρα και τα μέτρα προστασίας που λαμβάνονται, οι εγκληματίες που εκμεταλλεύονται το διαδικτυακό περιβάλλον εκτιμάται ότι μάλλον αυξάνουν τη δραστηριότητα τους ελκυόμενοι από τα αυξημένα κέρδη.[542]

6.4.3. Κατάχρηση - Κλοπή από υπαλλήλους

Σύμφωνα με το FBI, κατάχρηση είναι «η κακή χρήση ή τοποθέτηση χρημάτων ή περιουσιακών στοιχείων που κάποιος έχει εμπιστευτεί τη διαχείριση ή τον έλεγχο σε κάποιον άλλο». Αυτό που διακρίνει την κατάχρηση από τις άλλες μορφές κλοπών είναι η παραβίαση της οικονομικής εμπιστοσύνης μεταξύ του νόμιμου κατόχου των κεφαλαίων και του παραβάτη-καταχραστή.

Η κλοπή από τους υπαλλήλους μιας επιχείρησης είναι ένα από τα πιο συνηθισμένα και δαπανηρά προβλήματα που αντιμετωπίζονται από τις σημερινές επιχειρησιακές οργανώσεις, είτε ιδιωτικές είτε δημόσιες. Περιλαμβάνονται, μεταξύ άλλων, η αφαίρεση προϊόντων, προμηθειών, υλικών, κεφαλαίων, αρχείων δεδομένων, πληροφοριών και πνευματικής ιδιοκτησίας.

Οι μέθοδοι, που ένας υπάλληλος μπορεί να χρησιμοποιεί για να κλέψει από την επιχείρηση ή οργανισμό όπου εργάζεται, εξαρτώνται από διάφορους παράγοντες, συμπεριλαμβανομένου του είδους των χρημάτων ή της περιουσίας που έχουν εμπιστευτεί στο άτομο και του βαθμού πρόσβασης στα κεφάλαια επιχείρησης που του έχει παραχωρηθεί ανάλογα με τη θέση του. Παραδείγματος χάριν, ένας ταμίας πολυκαταστημάτων να κλέψει από το ταμείο μετρητών, ενώ να μη μπορεί να κλέψει εμπορεύματα από τις αποθήκες. Άλλοι υπάλληλοι, με περισσότερη πρόσβαση μέσα στην επιχείρηση, μπορούν να κλέψουν παραποιώντας τους λογαριασμούς ή τις αποδείξεις δαπανών ή να ιδιοποιούνται τα κεφάλαια μέσω της τιμολόγησης ή των μισθοδοτικών καταστάσεων.[543]

Μια από τις δυσκολίες αντιμετώπισης της κατάχρησης από υπαλλήλους έγκειται τα διαφορετικά κίνητρα των δραστών. Μεγάλος αριθμός καταχρήσεων μπορεί να οφείλεται στην ευκαιρία ή την οικονομική ανάγκη που είχε ο δράστης για να τις διαπράξει, σε άσχημες

[541] Grabosky Peter & Smith Russell (1998), σ.177
[542] Burden Kit & Palmer Creole, ό.π.
[543] *Embezzlement/Employee Theft* (2007)

συνθήκες εργασίας, δυσαρέσκεια, έλλειψη ικανοποίησης και αναγνώρισης από τη διοίκηση, ενώ μια άλλη μερίδα καταχραστών-υπαλλήλων έχουν πιεστεί από τους συναδέλφους τους για να συμμετέχουν στην κατάχρηση. Αυτή η πίεση μπορεί να περιλαμβάνει μια σειρά άτυπων κυρώσεων, για αυτούς που δεν συμμορφώνονται με την παραβατική κουλτούρα, που μπορεί να φτάνουν την απομόνωση και την εξώθηση σε παραίτηση. Μάλιστα έρευνες, όπως του Mars, αναδεικνύουν το ρόλο της ανάπτυξης μιας ιδιαίτερης ηθικής, ευνοϊκής προς τη διάπραξη της κλοπής, ανάμεσα στην ομάδα των εργαζομένων και στην ανάπτυξη μιας πρακτικής που θα αποδώσει παράνομα οικονομικά οφέλη σε αυτούς αφενός, χωρίς να είναι ιδιαίτερα επιζήμια για την επιχείρηση αφετέρου[544].

Υπάρχουν πολλές περιπτώσεις όπου η κατάχρηση αφορά δημόσιο χρήμα όπως είναι αυτή μιας λογίστριας του Υπουργείου Οικιακής και Αστικής Ανάπτυξης των ΗΠΑ η οποία καταχράστηκε 1,7 εκατομ. δολάρια τα οποία και ξόδεψε σε τυχερά παιχνίδια στο καζίνο του Μισσισιπή. [545]

6.4.4. Παραβιάσεις πνευματικών δικαιωμάτων [546]

Η ευκολία με την οποία μπορούν να γίνονται οι ανταλλαγές αρχείων στο ίντερνετ μέσω ιστοσελίδων όπως ήταν το Napster[547], συντελεί στη διάδοση υλικού που εμπίπτει στη νομοθεσία περί προστασίας των πνευματικών δικαιωμάτων εταιριών και καλλιτεχνών. Η «πειρατεία» λογισμικού, μουσικής και βίντεο μέσω του ίντερνετ και της διακίνησης πλαστών ψηφιακών δίσκων (CD's, DVD's) λαμβάνει ολοένα πιο αυξημένες διαστάσεις. Για παράδειγμα στο Ηνωμένο Βασίλειο κατά το 2001 οι πωλήσεις πειρατικού υλικού ήταν αυξημένες κατά 30% αντιπροσωπεύοντας 27,6 εκατ. δολάρια τζίρο νόμιμων πωλήσεων. Παρά το γεγονός ότι πολλές ιστοσελίδες, μεταξύ των οποίων το piratebay και το Napster έκλεισαν, λόγω της καταδίκης τους από τα δικαστήρια για διευκόλυνση παραβίασης πνευματικών δικαιωμάτων από τρίτους, παραμένουν ακόμα σήμερα πολλές αντίστοιχες ιστοσελίδες και δίκτυα διαμοιρασμού – κυρίως μουσικών mp3 - αρχείων (peer to peer).

Στις περιπτώσεις κατά τις οποίες το υλικό που προέρχεται από πειρατεία χρησιμοποιείται για εμπορικούς σκοπούς, όπως πώληση, ενοικίαση ή δημόσια προβολή, μπορούν εκτός από αστικές να επιβάλλονται και ποινικές κυρώσεις με μέγιστη ποινή φυλάκισης ή κάθειρξης τα δέκα χρόνια.[548]

6.4.5. Οργανωμένο Έγκλημα

Η έννοια «οργανωμένο έγκλημα» μπορεί να περιλαμβάνει αρκετούς διαφορετικούς ορισμούς. Γενικά ως «οργανωμένο έγκλημα» εννοείται μια εγκληματική επιχείρηση με διάρκεια στο χρόνο, που δρα για να αποκτήσει κέρδη από πολυποίκιλες παράνομες δραστηριότητες οι οποίες έχουν ζήτηση από το κοινό. Η διάρκειά της στο χρόνο επιτυγχάνεται μέσω της συστηματικής χρήσης βίας, απειλών, ελέγχου μονοπωλίων και της διαφθοράς κρατικών λειτουργών. Όπως κάθε οργάνωση, οι εγκληματικές αυτές επιχειρήσεις διαθέτουν ιεραρχική δομή και καταμερισμό της εργασίας, ενώ τα κέρδη που αποκομίζουν είναι πολλαπλάσια σε σχέση με αυτά των νόμιμων επιχειρήσεων αλλά και των υπόλοιπων παράνομων δραστηριοτήτων. Συχνά οι δραστηριότητες τους επεκτείνονται σε νόμιμες

[544] Mars Gerald (1974), σσ.209-228.
[545] *Embezzlement/Employee Theft* (2006)
[546] Copyright infringements
[547] Το Napster ξεκίνησε το 1999 από δυο Αμερικανούς φοιτητές και κάποια στιγμή αριθμούσε 60 εκατ, χρήστες.
[548] Burden Kit & Palmer Creole, ό.π.

οικονομικές δραστηριότητες, κυρίως για να καλύψουν και να νομιμοποιήσουν τα παράνομα κέρδη τους.

Η Γραμματεία για το έγκλημα και τα ναρκωτικά του ΟΗΕ ορίζει το οργανωμένο έγκλημα ως «ένα δομημένο σύνολο ατόμων που συνυπάρχει για αρκετό διάστημα και διαπράττει από κοινού μια ή περισσότερες παράνομες δραστηριότητες με σκοπό την απόκτηση οικονομικού ή άλλου υλικού κέρδους».

Στις ΗΠΑ δεν υπάρχει ακριβής και καθολικά αποδεκτός νομικός ορισμός για το οργανωμένο έγκλημα. Ο νόμος του 1970 για το οργανωμένο έγκλημα (Organized Crime Control Act) που αποτελεί τον κυρίαρχο σχετικό νόμο για ολόκληρες τις ΗΠΑ ορίζει ως σχετική με οργανωμένο έγκλημα «κάθε πράξη ή απειλή στην οποία ενέχονται φόνος, απαγωγή, τζόγος, εμπρησμός, ληστεία, δωροδοκία, εκβιασμός, άσεμνα θέματα, έλεγχο παράνομων ουσιών, απάτη, διαφθορά, διακίνηση κλεμμένων ή παράνομων αγαθών, ξέπλυμα χρήματος».

Οι μορφές συμπεριφορών που εμπλέκονται με τις δραστηριότητες του οργανωμένου εγκλήματος μπορούν να κατηγοριοποιηθούν σε τρεις κατηγορίες. Σε κάθε μια από αυτές ενέχονται συγκεκριμένα εγκλήματα που τιμωρούνται από το νόμο. Αυτές είναι:

1. Η παροχή παράνομων υπηρεσιών.

Αφορά την απόπειρα ικανοποίησης της ζήτησης του κοινού για χρήμα, σεξ και τζόγο, τα οποία η νόμιμη κοινωνία δεν μπορεί να παράσχει μέσω των θεσμών της, δηλαδή των τραπεζών, του γάμου και των κρατικών τυχερών παιχνιδιών αντίστοιχα. Συγκεκριμένα τα εγκλήματα που διαπράττονται σε κάθε περίπτωση είναι η τοκογλυφία (δανεισμός με τόκο που υπερβαίνει τον νόμιμο), η εξώθηση σε πορνεία και ο παράνομος τζόγος.

2. Η παροχή παράνομων προϊόντων.

Αφορά συγκεκριμένα προϊόντα για οποία μερίδα της κοινωνίας εκφράζει ζήτηση αλλά δεν μπορούν να αποκτηθούν με νόμιμες διαδικασίες. Τέτοια είναι η αγορά και πώληση ναρκωτικών και η διανομή προϊόντων εγκλήματος όπως κλεμμένων αυτοκινήτων, όπλων, ηλεκτρονικού εξοπλισμού τα οποία κάποιοι καταναλωτές επιθυμούν να αγοράσουν σε χαμηλή τιμή αδιαφορώντας για την προέλευση τους.

3. Η εισβολή σε νόμιμες επιχειρήσεις – Παροχή «προστασίας».

Αυτό περιλαμβάνει τον εκφοβισμό και εκβιασμό εργαζομένων και επιχειρήσεων για την εξασφάλιση της εργασίας τους ή της εργασιακής ειρήνης. Οι εργαζόμενοι εκβιάζονται να δώσουν χρήματα με την απειλή της απώλειας της εργασίας τους και οι εργοδότες με την απειλή υποκινούμενων απεργιών ή την πρόκληση καταστροφών στην επιχείρηση. Συχνά ακόμη οι νόμιμοι ιδιοκτήτες εκβιάζονται μέσω απειλών να πωλήσουν ή να παραχωρήσουν τον έλεγχο της επιχείρησης σε τρίτους.

Στις δυο πρώτες μορφές συνήθως δεν εμπλέκεται κάποιο είδος άσκησης ή απειλής χρήσης βίας λόγω του συναινετικού χαρακτήρα των δραστηριοτήτων. Η προσφορά παράνομου στοιχήματος, δανείων ή ναρκωτικών στηρίζεται στην αντίστοιχη ζήτηση από πλευράς του κοινού για τέτοιου είδους προϊόντα και υπηρεσίες. Έτσι υπάρχει και από τα δυο μέρη, το οργανωμένο έγκλημα αφενός και το κοινό αφετέρου, αμοιβαία προσδοκία και συμφέρον για μελλοντικά κέρδη από στοιχήματα, δάνεια και άλλες παράνομες δραστηριότητες. Για τους λόγους αυτούς η άσκηση βίας εδώ δεν παίζει κάποιο άμεσο και ενεργό ρόλο, εκτός και αν κάποιο από τα δυο μέρη αισθάνεται «ριγμένο» από την συναλλαγή. Αντίθετα η βία ή η απειλή της χρησιμοποιείται κατά κόρον για τον έλεγχο ή την μονοπώληση κάποιας

παράνομης αγοράς όπως συμβαίνει στην τρίτη περίπτωση όπου το οργανωμένο έγκλημα περισσότερο προκαλεί τη δημιουργία ζήτησης κάποιας υπηρεσίας παρά εκμεταλλεύεται κάποια ήδη υπάρχουσα.

Περιπτώσεις δραστηριοτήτων που συνιστούν οργανωμένο έγκλημα, στον τομέα του ηλεκτρονικο-οικονομικού εγκλήματος, αποτελούν αυτές της καταδίκης ομάδας Κινέζων στη Ν. Υόρκη το 2006 για ξεκαθάρισμα λογαριασμών εναντίον αντίπαλης ομάδας οργανωμένου εγκλήματος. Πιο συγκεκριμένα η ομάδα κατηγορήθηκε για εκβιασμό, παρεμπόδιση μαρτύρων, λαθρεμπόριο και κυκλοφορία πλαστών DVD και CD που εισήγαγαν από την Κίνα, ξέπλυμα μαύρου χρήματος, διενέργεια παράνομου τζόγου και διακίνηση ναρκωτικών.

Ανάλογα κατηγορήθηκαν και τα μέλη δυο άλλων «οικογενειών» οργανωμένου εγκλήματος στις ΗΠΑ τον Απρίλιο του 2007 για απάτη ασφαλειών, εκβιασμό, απαγωγή, παρεμπόδιση μαρτύρων, ξέπλυμα μαύρου χρήματος, και χειραγώγηση μετοχών μέσω εκβιασμού χρηματιστών. [549]

Τα παραπάνω παραδείγματα καταδεικνύουν μάλιστα, τη σχέση αλληλεπίδρασης μεταξύ των διαφόρων μορφών οικονομικού εγκλήματος επειδή αυτά μπορεί να συνυπάρχουν στο κατηγορητήριο των ίδιων κατηγορουμένων και να αποτελούν παραδείγματα ταυτόχρονα για διαφορετικές μορφές εγκλημάτων.

6.4.6. Εμπορία/Διακίνηση Ναρκωτικών και φαρμάκων

Οι έμποροι φαρμάκων εκμεταλλεύονται όλο και περισσότερο το Διαδίκτυο για να πωλήσουν τις παράνομες ουσίες τους μέσω του κρυπτογραφημένου ηλεκτρονικού ταχυδρομείου και της τεχνολογίας του Διαδικτύου. Μερικοί έμποροι φαρμάκων κλείνουν τις συμφωνίες τους στα ίντερνετ - καφέ, χρησιμοποιούν ενδιάμεσους ιστοχώρους για να ανιχνεύσουν τις παράνομες συσκευασίες χαπιών και να ανταλλάξουν συνταγές για αμφεταμίνες σε δωμάτια συνομιλίας περιορισμένης πρόσβασης. Η άνοδος στο εμπόριο ναρκωτικών μέσω του Διαδικτύου θα μπορούσε να αποδοθεί ακριβώς στην έλλειψη της πρόσωπο με πρόσωπο επικοινωνίας. Αυτές οι ηλεκτρονικές συναλλαγές επιτρέπουν και σε πιο διστακτικά άτομα να αγοράσουν πιο άνετα τα παράνομα φάρμακα. Έτσι εξασθενίζει και η διαδικασία φιλτραρίσματος που θα γινόταν με την προσωπική επικοινωνία. Επιπλέον, οι παραδοσιακές συνταγές φαρμάκων, που ήταν προσεκτικά κρατημένες ως μυστικά, με τη σύγχρονη τεχνολογία υπολογιστών τίθενται τώρα στην διάθεση όποιου διαθέτει πρόσβαση στο διαδίκτυο. [550]

Τα τελευταία χρόνια έχουν αναπτυχθεί και τα ψηφιακά ναρκωτικά, τα «iDoser». Πλέον τα ναρκωτικά δεν παρέχονται και μεταφέρονται μόνο σε χημική μορφή (π.χ. χάπια, ενέσεις) αλλά κυκλοφορούν σε ψηφιακά αρχεία, που οι χρήστες μπορούν να κατεβάζουν από το διαδίκτυο. Το ναρκωτικό είναι κρυμμένο σε ηχητικά κύματα, που με ειδική επεξεργασία έχουν ενσωματωθεί σε απλά μουσικά αρχεία τύπου <.mp3> και πωλούνται ως αρχεία με την επέκταση <.drg>. Οι παράνομες ιστοσελίδες παρέχουν το κατάλληλο λογισμικό, οδηγίες χρήσης και την πρώτη «δόση» δωρεάν, ενώ τις υπόλοιπες δόσεις, με τη μορφή τραγουδιών σε μουσικά cd, πωλούν σχετικά φθηνά προσελκύοντας ακόμα και ανήλικους «αγοραστές».[551] Τα αρχεία αυτά περιέχουν υπόηχους, δηλαδή κύματα συχνότητας 3 έως 30 Hertz που προκαλούν διάφορες αντιδράσεις κατευθείαν στη λειτουργία του εγκεφάλου. Οι υπόηχοι έχουν

[549] Organized *Crime* (2007)
[550] http://en.wikipedia.org/wiki/Computer_crime#Harassment
[551] http://www.newsbomb.gr/ellada/news/story/240821/to-narkotiko-idoser-poy-trelainei-ton-egkefalo

χρησιμοποιηθεί ως κατασταλτικά μέσα σε χώρους όπως οι ντισκοτέκ και παλαιότερα σε στρατιωτικούς χώρους. Τα κύματα άλφα (από 7 έως 13 Hertz) παρουσιάζουν χαλαρωτική επίδραση, ενώ άλλα εύρη συχνοτήτων δημιουργούν υπερδιέγερση και ευφορία.[552]

6.4.7. Εμπορία Ανθρώπων, Ανθρωπίνων Οργάνων

Με τους ίδιους τρόπους, οι κάθε είδους «έμποροι» διαπραγματεύονται τα προϊόντα τους τα οποία μπορεί να είναι άνθρωποι ή διάφορα ανθρώπινα όργανα που διακινούνται μέσω του διαδικτύου.

Η εμπορία ανθρώπων (Human trafficking) περιλαμβάνει τη προσέλκυση, τη μεταφορά ή την παραλαβή των ανθρώπων με σκοπό την εκμετάλλευση. Τα παράνομα κέρδη από τη παγκόσμια βιομηχανία διακίνησης ανθρώπων υπολογίζονται σε 42,5 δισεκατομμύρια δολάρια ετησίως.[553]

6.4.8. Εμπορία Όπλων

Μέσω του διαδικτύου μπορεί να γίνεται και η διακίνηση όπλων, επίσης γνωστή ως Gunrunning, που αφορά το παράνομο εμπόριο (λαθρεμπόριο) όπλων και πυρομαχικών.[554]

6.5. Άλλα είδη ηλεκτρονικο-οικονομικού εγκλήματος

Εδώ κατατάσσουμε κάποιες μορφές παραδοσιακού οικονομικού εγκλήματος η τέλεση των οποίων διευκολύνεται απλά με τη χρησιμοποίηση ηλεκτρονικού υπολογιστή ή ψηφιακής τεχνολογίας.

6.5.1. Απάτες τηλεπωλήσεων

Για την απάτη στον τομέα των τηλεπωλήσεων ο απατεώνας, ως κύριο μέσο επικοινωνίας με τα πιθανά θύματα, χρησιμοποιεί απλά το τηλέφωνο ώστε να τα πείσει να του αποστείλουν χρήματα για υποτιθέμενες αγορές αγαθών, αγαθοεργίες κ.λ.π. Παρά το γεγονός ότι οι περισσότερες επιχειρήσεις τηλεπωλήσεων είναι νόμιμες, υπάρχει ένα κομμάτι τέτοιων επιχειρήσεων που πραγματοποιούν τεράστια κέρδη από απάτες (2,3 τρισεκατομμύρια δολάρια).[555]

Άλλες μορφές απάτης τηλεπωλήσεων είναι και οι διάφορες κληρώσεις ότι ο καταναλωτής δήθεν κέρδισε ταξίδια ή χρήματα σε λοταρίες για τα οποία θα πρέπει «μόνο» να προκαταβάλει τους φόρους οι οποίοι αντιπροσωπεύουν ποσά που τελικά καταλήγουν στους απατεώνες. [556]

6.5.2. Ασφαλιστικές απάτες

Ως ασφάλεια εννοείται ένα επενδυτικό εργαλείο από το οποίο ο επενδυτής προσδοκά να αποκομίσει οικονομικό όφελος μέσω ενεργειών τρίτων. Οι ασφαλιστικές απάτες αφορούν κακή διαχείριση ή παραπλάνηση σχετικά με τη σύναψη ασφαλειών. Η απάτη διαπράττεται όταν ζητείται η είσπραξη του ποσού μιας ασφάλειας ή αυξάνεται το απαιτούμενο ποσό της με την παροχή παραπλανητικών πληροφοριών σχετικά με τα δεδομένα της ζημίας που υπέστη ο ασφαλισμένος.

Οι ασφαλιστικές απάτες διακρίνονται σε «βαριές» (hard) και «ελαφριές» (soft). Οι βαριές περιπτώσεις αφορούν προσποίηση ατυχήματος, τραυματισμού, εμπρησμού, κλοπής ή άλλης

[552] http://www.freesymbolforum.com/index.php?topic=262.0
[553] http://en.wikipedia.org/wiki/Trafficking_in_Human_Beings
[554] http://en.wikipedia.org/wiki/Arms_trafficking
[555] Πηγή: Direct Marketing Association (2005)
[556] *Telemarketing Fraud (*2006)

απώλειας με σκοπό την παράνομη είσπραξη χρημάτων από ασφαλιστικές εταιρίες. Αυτοί οι κλέφτες συνήθως δρουν ατομικά, τα τελευταία χρόνια όμως εμφανίζονται και δίκτυα οργανωμένου εγκλήματος που εφαρμόζουν μεγάλα σχήματα απάτης για να κλέψουν εκατομμύρια.

Οι ελαφριές περιπτώσεις ασφαλιστικής απάτης αφορούν – κατά τα άλλα – τίμιους ανθρώπους οι οποίοι λένε «μικρά ψέματα» στις ασφαλιστικές τους εταιρίες για να καλύψουν το κόστος όταν η ζημία που υπέστησαν υπερβαίνει το ποσό της κάλυψης. Τέτοιες είναι κυρίως οι περιπτώσεις «στημένων» αυτοκινητιστικών ατυχημάτων όπου οι οδηγοί δυο οχημάτων συμφωνούν να προσποιηθούν ένα ατύχημα μεταξύ τους με σκοπό να λάβουν αποζημιώσεις για ζημιές που δεν έχουν σχέση με ατύχημα. Πολλοί το αντιμετωπίζουν ως μια αβλαβή παραποίηση των αριθμών, δεν παύει όμως να αποτελεί μια απάτη που τελικά οδηγεί στην αύξηση των ασφαλίστρων για όλους.

Περίπτωση παράνομης συνταγογράφησης για είσπραξη ποσού από ασφαλιστικές εταιρείες αποτελεί αυτή του γιατρού Dr.A.M. από τις ΗΠΑ που καταδικάστηκε σε 11 χρόνια κάθειρξη επειδή έγραφε παράνομες συνταγές για αυτοκινούμενα αναπηρικά καροτσάκια ακόμα και σε ασφαλισμένο ο οποίος μπορούσε να κάνει τζόκιν. Εκτός της ποινικής καταδίκης ο γιατρός έπρεπε και να αποζημιώσει δυο ασφαλιστικές εταιρείες. [557]

6.5.3. Απάτες στον τομέα υγείας

Ως απάτη στον τομέα υγείας (Health Care Fraud) θεωρείται είναι η σκόπιμη παραπλάνηση ή παρερμηνεία δεδομένων που οδηγούν σε παράνομες πληρωμές για την παροχή ιατρικών υπηρεσιών προς όφελος του ίδιου του ασφαλισμένου, του ιατρικού προσωπικού ή των ασφαλιστικών εταιριών και συνήθως εις βάρος των δημόσιων ασφαλιστικών ταμείων.

Συνηθισμένες μορφές τέτοιας απάτης είναι η χρέωση ιατρικών υπηρεσιών που δεν έχουν παρασχεθεί ή η υπερχρέωση υπηρεσιών που έχουν παρασχεθεί. Για παράδειγμα μπορεί κάποιος γιατρός να χρεώνει για εξετάσεις ή ιατρικές επισκέψεις που δεν έχουν πραγματοποιηθεί ή να υπερ-τιμολογεί για αυτές που έχουν πραγματοποιηθεί. Από την άλλη πλευρά μπορεί ο ίδιος ο ασφαλισμένος να ζητά από το γιατρό ή το θεραπευτήριο να υπερ-τιμολογεί τις αποδείξεις για τις παρασχεθείσες σε αυτόν ιατρικές υπηρεσίες προκειμένου να εισπράξει τη διαφορά από τον ασφαλιστικό φορέα του.

Μια από τις μεγαλύτερες εταιρίες προμήθειας φαρμάκων στις ΗΠΑ υποχρεώθηκε να καταβάλλει πρόστιμα 49,5 εκατομ. δολάρια επειδή εξαπάτησε την υπηρεσία ιατρικής βοήθειας σε 42 Πολιτείες με την αλλαγή της σύστασης των δόσεων φαρμάκων και τη μεταστροφή των ασθενών από επώνυμα φάρμακα σε φάρμακα ακριβότερης έκδοσης. [558]

6.5.4. Απάτες για αποζημιώσεις από καταστροφές

Αυτό το είδος απάτης αφορά τα αιτήματα προς τις δημόσιες υπηρεσίες για παροχή αποζημιώσεων μετά από διάφορες μαζικές καταστροφές, φυσικές ή μη, όπως πλημμύρες, σεισμοί, πυρκαγιές, τυφώνες, τρομοκρατικές ενέργειες κλπ. που πλήττουν ταυτόχρονα μεγάλο αριθμό ατόμων. Οι απώλειες μπορεί να τραυματισμοί ή θάνατοι προσώπων, ζημιές σε κατοικίες ή τον εξοπλισμό τους.

Η απάτη μπορεί να διενεργείται από τα ίδια τα θύματα των καταστροφών ή από άτομα που πείθουν τα θύματα να διεκδικήσουν μεγαλύτερα ποσά από αυτά που αναλογούν στην

[557] *Insurance Fraud (*2006)
[558] *Health Care Fraud (*2007)

ζημιά που υπέστησαν. Τα τρίτα αυτά άτομα μπορεί να είναι διεφθαρμένοι κρατικοί λειτουργοί, κατασκευαστές που δεν πραγματοποιούν την ολοσχερή αποκατάσταση των ζημιών που ανέλαβαν, ακόμα και άτομα που προφασίζονται τη διενέργεια δήθεν εράνων υπέρ των πληγέντων. Παραδείγματα από την πρόσφατη πραγματικότητα αποτελούν διάφορα μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου (spam) που απεστάλησαν δήθεν από τον Ερυθρό Σταυρό ζητώντας οικονομική βοήθεια υπέρ των θυμάτων της τρομοκρατικής ενέργειας της 11ης Σεπτεμβρίου ή αυτών από το «τσουνάμι» στον Ινδικό Ωκεανό. [559]

6.5.5. Απάτες Υποθηκευμένων ακινήτων

Η απάτη σε υποθήκες αφορά την από πλευράς καταναλωτών ή επαγγελματιών σκόπιμη παραποίηση των στοιχείων που οδηγούν κάποιο χρηματοπιστωτικό οργανισμό να χρηματοδοτήσει, αγοράσει ή ασφαλίσει ένα ενυπόθηκο δάνειο που διαφορετικά θα είχε αρνηθεί να πράξει. Χαρακτηριστικές είναι οι περιπτώσεις όπου αλλοιώνονται τα δεδομένα για την λήψη δανείων με ενέχυρο ιδιοκτησίες οι οποίες στην πραγματικότητα δεν υφίστανται.

Τρεις άνδρες από το Σαιντ Λούις των ΗΠΑ καταδικάστηκαν σε επιτήρηση και χρηματικές αποζημιώσεις επειδή φούσκωναν τεχνητά τις τιμές σπιτιών χρησιμοποιώντας εικονικούς αγοραστές για να εξαπατήσουν δανειστές. Η απάτη στηριζόταν στο γεγονός ότι είναι δύσκολος ο υπολογισμός της πραγματικής αξίας ανακαινισμένων κατοικιών. [560]

Στο κεφάλαιο αυτό εξετάστηκαν κατηγοριοποιημένες οι μορφές του ηλεκτρονικο-οικονομικού εγκλήματος και έγινε:

Α) Διάκριση των ηλεκτρονικών εγκλημάτων μεταξύ:

1. Εγκλημάτων μέσω του διαδικτύου όπου ο υπολογιστής αποτελεί στόχο και

2. Εγκλημάτων μέσω του διαδικτύου, όπου ο υπολογιστής αποτελεί εργαλείο των επιθέσεων.

Β) Διάκριση των οικονομικών εγκλημάτων που τελούνται με τη χρήση σύγχρονων τεχνολογιών, των υπολογιστών, του διαδικτύου ή άλλων ψηφιακών μέσων.

[559] *Disaster Fraud* (2007)
[560] *Mortgage Fraud* (2007)

ΜΕΡΟΣ Β΄

ΚΕΦΑΛΑΙΟ 7. ΕΦΑΡΜΟΓΗ ΤΩΝ ΘΕΩΡΗΤΙΚΩΝ ΠΡΟΣΕΓΓΙΣΕΩΝ ΓΙΑ ΤΗ ΔΟΜΗΣΗ ΤΩΝ «ΕΓΚΛΗΜΑΤΙΚΩΝ ΕΥΚΑΙΡΙΩΝ» ΣΤΗΝ ΚΑΤΑΝΟΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟ-ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στο κεφάλαιο αυτό, εξετάζεται η πιο πρόσφατη βιβλιογραφία και οι έρευνες σχετικά με την εφαρμογή των νεότερων προσεγγίσεων της περιβαλλοντικής εγκληματολογίας για τη διαμόρφωση των «εγκληματικών ευκαιριών» που συγκροτούν το θεωρητικό μας πλαίσιο. Ακόμα επιχειρείται η διασύνδεση των επιμέρους θεωρητικών προσεγγίσεων σε ενιαίο θεωρητικό σχήμα και διερευνάται η συμβολή καθεμιάς τους στη διαμόρφωση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος.

7.1. Η εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων

Η θεωρία των καθημερινών δραστηριοτήτων (RAT) μπορεί να αποτελέσει ένα κατάλληλο θεωρητικό πλαίσιο για την κατανόηση των «εγκληματικών ευκαιριών» με την διερεύνηση των μεθόδων με τις οποίες οι εγκληματίες προσεγγίζουν τα θύματα τους στον τόπο και τον χρόνο.

Οι διάφοροι ερευνητές καθιέρωσαν τις κομβικές έννοιες «ελκυστικότητα», «έκθεση», «εγγύτητα» σε πιθανούς κινδύνους και «φύλαξη» του στόχου ως μεταβλητές για τη διακρίβωση της εφαρμοσιμότητας της θεωρίας σε διάφορες μορφές θυματοποίησης. Η μεγαλύτερη *έκθεση*, *εγγύτητα* και *ελκυστικότητα* του στόχου σε δράστες με κίνητρο αυξάνουν τις πιθανότητες θυματοποίησης.[561]

Όπως κάθε άλλο (κοινό) έγκλημα, έτσι και τα ηλεκτρονικο-οικονομικά εγκλήματα διαθέτουν «ευκαιριακή δομή», δηλαδή τις συνθήκες που πρέπει να συντρέχουν στον τόπο και το χρόνο προκειμένου να τελεστούν. Όμως, αντί για την συνύπαρξη των τριών βασικών στοιχείων της θεωρίας «στον τόπο και το χρόνο», έχουμε τη δημιουργία κοινού τόπου στο πλαίσιο ενός εικονικού περιβάλλοντος ή αλληλεπιδράσεων που δημιουργούνται από την έλλειψη «ικανών φυλάκων».[562] Άλλωστε οι διαδικτυακές δραστηριότητες μπορούν να φέρουν το θύμα σε μεγάλη εγγύτητα με τον πιθανό δράστη, βέβαια με εικονικό, ψηφιακό τρόπο.[563]

Η θεωρία των «καθημερινών δραστηριοτήτων» χρησιμοποιήθηκε αρχικά για να ερμηνεύσει τα κοινά εγκλήματα (βίας και κατά της ιδιοκτησίας) και να συμβάλλει στην πρόληψη της περιστασιακής εγκληματικότητας. Στην πορεία επεκτάθηκε για να εφαρμόζεται και σε άλλες κατηγορίες εγκλημάτων όπως η οικονομική και ψηφιακή εγκληματικότητα, ιδιαίτερα κάποιες μορφές τους π.χ. η παράνομη μεταφορά (κατέβασμα) αρχείων, κατάχρηση, παράνομη πρόσβαση σε υπολογιστές, απάτες μέσω διαδικτύου[564].

Ακόμα επεκτάθηκε, από τον Felson μαζί με τον Clarke[565] και στην εγκληματικότητα του λευκού περιλαιμίου, τις παράνομες αγορές (π.χ. λαθρεμπόριο, ξέπλυμα χρήματος) στο έγκλημα εντός της τοπικής κοινότητας και στο επιχειρησιακό περιβάλλον.

[561] Reyns, Brandford, Henson Billy & Fisher Bonnie (2011)

[562] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.176

[563] Bossler Adam, & Holt Thomas (2009)

[564] Βλ. Felson και Boba 2010, Benson, Madensen, και Eck 2009, Bossler Adam και Holt 2009, Holtfreter, Reisig, and Pratt 2008, όπως αναφέρουν οι Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013) και Clarke Ronald V. (1997), σ.32

[565] Felson,M. & Clarke,R.V. (1997) και Felson, M. & Clarke, R.V. (1998)

Όσον αφορά τη θυματοποίηση στο διαδίκτυο, οι υπάρχουσες μελέτες είναι γενικά υποστηρικτικές της θεωρίας των καθημερινών δραστηριοτήτων με κάποιες εξαιρέσεις.

Ο Majid Yar θεωρεί περιορισμένη τη δυνατότητα εφαρμογής της θεωρίας των «καθημερινών δραστηριοτήτων» στη μελέτη των κυβερνο-εγκλημάτων γιατί, ενώ οι περισσότερες από τις βασικές έννοιες της θεωρίας συνάδουν με κάτι τέτοιο, δεν συμβαίνει το ίδιο και με το στοιχείο της «σύμπτωσης στο χώρο και το χρόνο». Ο Yar θεωρεί τον κυβερνοχώρο ως «ένα χωρο-χρονικά αποδιοργανωμένο και ασυνεχές περιβάλλον» (chronically spatio-temporally disorganized) και ως εκ τούτου δημιουργούνται προβλήματα κατά την εφαρμογή της θεωρίας για τα εγκλήματα στον κυβερνοχώρο.[566]

Μια από τις έρευνες, τα αποτελέσματα της οποίας δεν υποστήριξαν επαρκώς τα βασικά στοιχεία της θεωρίας των καθημερινών δραστηριοτήτων, είναι αυτή του F. Ngo που μελέτησε την επίδραση των περιστασιακών παραγόντων (από τις καθημερινές δραστηριότητες) και των ατομικών παραγόντων (από τη θεωρία του αυτοελέγχου των Gottfredson and Hirschi) σε σχέση με επτά τύπους θυματοποίησης από κυβερνοεγκλήματα (διάδοση ιών, ακούσια θέαση πορνογραφικού υλικού, σεξουαλική εκμετάλλευση, διαδικτυακή παρενόχληση από άγνωστο ή και από γνωστό, ηλεκτρονικό «ψάρεμα»/phishing και διαδικτυακή συκοφάντηση). Ο σκοπός της έρευνας του Ngo ήταν να προσδιορίσει το κατά πόσο το χαμηλό επίπεδο αυτοελέγχου και η έκθεση σε πιθανούς δράστες, μέσω της εμπλοκής σε επικίνδυνες διαδικτυακές δραστηριότητες και η απουσία ή η έλλειψη ικανών φυλάκων, επηρεάζουν τους επτά τύπους διαδικτυακής εγκληματικότητας.

Η έρευνα αυτή έγινε το 2010, διαδικτυακά, με ερωτώμενους τους φοιτητές αμερικανικού κολλεγίου. Στο ερωτηματολόγιο απάντησαν 295 φοιτητές δηλαδή το 19% του συνόλου των εγγεγραμμένων φοιτητών που ήταν 1533. Το ποσοστό αυτό κρίθηκε επαρκές από τον ερευνητή που αναφέρει ότι αποτελεί τυπικό ποσοστό ανταπόκρισης σε έρευνες μέσω διαδικτύου. Τα αποτελέσματα της έρευνας του Ngo έδειξαν ότι πράγματι η ύπαρξη χαμηλού αυτοελέγχου σχετίζεται με κίνδυνο οι χρήστες να πέσουν θύματα διαδικτυακής παρενόχλησης, τόσο από γνωστούς όσο και από αγνώστους. Το πιο εντυπωσιακό όμως από τα ευρήματα της έρευνας ήταν ότι η ύπαρξη ασφάλειας του υπολογιστή, με τη χρήση αντιϊκών προγραμμάτων, συσχετίζεται με την μόλυνση του υπολογιστή από ιό και με περιστατικά παρενόχλησης, ενώ θα αναμενόταν τα προγράμματα αυτά να λειτουργούν ως «ικανοί φύλακες». Βρέθηκε δηλαδή ότι όσοι χρησιμοποιούσαν antivirus και firewalls ήταν πιο επιρρεπείς σε ηλεκτρονικές επιθέσεις αυτού του είδους, από όσους δεν χρησιμοποιούσαν. Η εξήγηση, που έδωσε ο Ngo για το εύρημα αυτό, ήταν ότι πιθανόν οι χρήστες που χρησιμοποιούν προγράμματα ασφαλείας να αισθάνονται και πιο ασφαλείς, ακριβώς λόγω της ύπαρξης τέτοιων προγραμμάτων, και έτσι να παρασύρονται σε πιο «ριψοκίνδυνη» συμπεριφορά που τους καθιστά κατάλληλους στόχους. Ο ερευνητής, αναγνωρίζοντας τους περιορισμούς της μελέτης του, σημείωσε ότι το πανεπιστήμιο και το δείγμα που επέλεξε ίσως δεν είναι και τόσο αντιπροσωπευτικό για τις ΗΠΑ και πρότεινε την διενέργεια και άλλων ερευνών.[567]

Αντίθετα, υπάρχει πλήθος μελετών, οι οποίες παρουσιάζονται παρακάτω και που επιβεβαιώνουν την εφαρμοσιμότητα της θεωρίας των καθημερινών δραστηριοτήτων στη μελέτη των ηλεκτρονικο-οικονομικών εγκλημάτων.

[566] Yar Majid (2005)

[567] Ngo Fawn T. (2011)

Δυο από αυτές είναι οι έρευνες των Holtfreter Kristy, Reisig Michael και Pratt Travis το 2008[568] και Pratt Travis C., Holtfreter Kristy & Reisig Michael το 2010[569] που έγιναν σε δείγματα του γενικού πληθυσμού (και όχι σε φοιτητές κολεγίου).

Στη μελέτη ‘‘Low Self-control, Routine Activities and Fraud Victimization’’του 2008, οι ερευνητές εφήρμοσαν τη θεωρία του αυτοελέγχου (των Gottfredson & Hirschi) σε συνδυασμό με αυτή των καθημερινών δραστηριοτήτων για να εξετάσουν τη θυματοποίηση σε οικονομική απάτη. Τα ερευνητικά αποτελέσματα υποστήριξαν τόσο τη θεωρία του αυτοελέγχου όσο και των καθημερινών δραστηριοτήτων. Έτσι διαπιστώθηκαν τα παρακάτω:

Πρώτα, επιβεβαιώθηκε ότι, όπως για τον κίνδυνο θυματοποίησης από βίαια εγκλήματα, έτσι και για τις περιπτώσεις απάτης οι άνδρες διατρέχουν μεγαλύτερο κίνδυνο από τις γυναίκες.

Δεύτερο, ο τρόπος που τα άτομα περνούν το χρόνο τους ως διαδικτυακοί καταναλωτές και η έλλειψη αυτοελέγχου τα οδηγούν να παίρνουν παρορμητικές αποφάσεις που τα εκθέτουν σε κινδύνους. Όπως δεν υπάρχει τυχαία κατανομή των δραστών (απάτης), έτσι και η θυματοποίηση δεν αποτελεί κάποιο τυχαίο γεγονός αλλά συνδέεται με την παρορμητική, ριψοκίνδυνη οικονομική συμπεριφορά των καταναλωτών (θυμάτων απάτης).

Τρίτο, η αυξημένη οικονομική δραστηριότητα, με συναλλαγές εξ αποστάσεως (ίντερνετ, τηλέφωνο, e-mail, κλπ.) συνδέεται με αυξημένη έκθεση των καταναλωτών στο να αποτελέσουν αντικείμενο θυματοποίησης.

Το τέταρτο αφορά την αντιμετώπιση. Σύμφωνα με τους ερευνητές από τα ευρήματα της μελέτης τους προκύπτει ότι η μείωση των οικονομικά ριψοκίνδυνων συμπεριφορών, μέσω κατάλληλων προγραμμάτων ενημέρωσης του κοινού, οδηγεί στη μείωση και των πιθανοτήτων θυματοποίησης τόσο για τις περιπτώσεις οικονομικής απάτης, όσο και για άλλες περιπτώσεις όπως της κλοπής ταυτότητας.[570]

Στην δεύτερη μελέτη τους, “Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory” (2010), οι συγγραφείς ερεύνησαν την επίδραση των προσωπικών χαρακτηριστικών των χρηστών του διαδικτύου και των καθημερινών τους δραστηριοτήτων όπως οι αγορές στο διαδίκτυο, σε σχέση με την έκθεση των ατόμων σε πιθανούς δράστες. Αναφέρουν την τεράστια ανάπτυξη του ηλεκτρονικού εμπορίου, όπου οι αμερικανοί καταναλωτές το 2007 ξόδεψαν 157,3 δις δολ. σε διαδικτυακές αγορές, με πρόβλεψη για 316 δις δολ. για το 2010. Παρόλα αυτά, σημειώνουν οι συγγραφείς, οι περισσότερες έρευνες διαπίστωσαν ότι οι χρήστες (σε ποσοστό 70%) θεωρούν την πιθανότητα να πέσουν θύματα εγκλήματος στο διαδίκτυο πιο σοβαρή από το να πέσουν θύμα στον φυσικό κόσμο. Επίσης, ότι οι κίνδυνοι από την διαδικτυακή χρήση της πιστωτικής τους κάρτας υποσκελίζουν τα πλεονεκτήματα των ηλεκτρονικών αγορών. Όμως αυτοί οι χρήστες είναι και πιο επιφυλακτικοί στο να δίνουν τα στοιχεία της πιστωτικής τους κάρτας στο διαδίκτυο, κάνουν λιγότερες ηλεκτρονικές αγορές, περνούν λιγότερες ώρες στο διαδίκτυο και έτσι μειώνουν την έκθεσή τους σε πιθανούς κινδύνους. Πράγματι, από την έρευνα αυτή βρέθηκε ότι όσο περισσότερες ώρες περνάει κανείς στο διαδίκτυο και όσο περισσότερες διαδικτυακές συναλλαγές πραγματοποιεί, τόσο αυξημένη είναι η πιθανότητα να γίνει στόχος διαδικτυακής απάτης (ειδικά η δεύτερη μεταβλητή αυξάνει τις πιθανότητες κατά 290%).[571]

[568] βλ. Holtfreter Kristy, Michael D. Reisig, & Travis C. Pratt. (2008)
[569] Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010)
[570] Holtfreter Kristy, Michael D. Reisig, & Travis C. Pratt. (2008)
[571] Pratt Travis, Holtfreter Kristy & Reisig Michael (2010)

Επίσης, όσον αφορά τα προσωπικά χαρακτηριστικά, βρέθηκε ότι οι νέοι, οι άνδρες, οι έχοντες ιδιόκτητο σπίτι και οι πιο μορφωμένοι περνούν σημαντικά μεγαλύτερο χρόνο στο διαδίκτυο, ενώ το λιγότερο χρόνο αφιερώνουν οι μεγαλύτεροι και οι αφροαμερικανοί σε σχέση με τους λευκούς και τους ασιατικής καταγωγής. Για τη πραγματοποίηση συναλλαγών μέσω διαδικτύου βρέθηκε ότι περισσότερες αγορές πραγματοποιούν οι πιο εύρωστοι οικονομικά, οι παντρεμένοι, οι ιδιοκτήτες σπιτιών και οι πιο μορφωμένοι. Τα ευρήματα αυτά επιβεβαίωσαν προηγούμενες μελέτες[572] που συσχέτιζαν τα δημογραφικά χαρακτηριστικά με πρότυπα διαδικτυακής θυματοποίησης και με τη συχνότητα διαδικτυακής δραστηριότητας επιτρέποντας την γενίκευση και εφαρμογή του θεωρητικού πλαισίου των καθημερινών δραστηριοτήτων στη μελέτη της διαδικτυακής απάτης όπως πρότειναν και οι Newman & Clarke.[573]

Στη μελέτη της εγκληματικότητας του λευκού περιλαιμίου στον κυβερνοχώρο εφάρμοσαν τη θεωρία «καθημερινών δραστηριοτήτων» και οι Hutchings και Hayes για το «ηλεκτρονικό ψάρεμα» ή phishing.[574]

Ο Choi Kyung-shick εφήρμοσε το μοντέλο των «καθημερινών δραστηριοτήτων του τρόπου ζωής» (LRAT-Lifestyle/Routine Activity Theory) ερευνώντας τη διαδικτυακή συμπεριφορά των φοιτητών ενός αμερικανικού κολεγίου.[575] Χρησιμοποίησε ακόμα στο θεωρητικό του πλαίσιο τα συμπεράσματα έρευνας των Mustain και Tewksbury το 1998, οι οποίοι διερεύνησαν την εφαρμοσιμότητα της θεωρίας των καθημερινών δραστηριοτήτων στη θυματοποίηση φοιτητών από κλοπή. Οι Mustain και Tewksbury διαπίστωσαν ότι ο κίνδυνος θυματοποίησης δεν αυξάνεται απλά με το να περνάει κάποιος πολύ χρόνο σε δραστηριότητες εκτός σπιτιού (όπου υπάρχει απουσία ικανών φυλάκων), αλλά με το που πηγαίνει και το τι κάνει, με ποιες δραστηριότητες ασχολείται και πώς προστατεύει τον εαυτό του όταν βρίσκεται σε δημόσιο χώρο. Μια ακόμα σημαντική μεταβλητή είναι η εγγύτητα του στόχου (proximity) σε πιθανούς δράστες, με το να βρίσκεται κανείς σε επαφή με παραβάτες εμπλεκόμενος και ο ίδιος σε παραβατικές συμπεριφορές αυξάνεται ο κίνδυνος θυματοποίησής του. Οι Mustain και Tewksbury (1998) συμπέραναν ότι η εμπλοκή κάποιου σε παραβατικό τρόπο ζωής τον καθιστά «απρόθυμο» να καταγγείλει στις αρχές τη δική του θυματοποίηση. Το γενικό συμπέρασμα των Mustain και Tewksbury είναι ότι τα ευρήματα της έρευνάς τους παρέχουν ισχυρή υποστήριξη για την εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων και του τρόπου ζωής των ατόμων στην θυματοποίησή τους από κλοπή.[576]

Ακολουθώντας τις διαπιστώσεις των Mustain και Tewksbury, ότι ο τρόπος ζωής παίζει ρόλο στη θυματοποίηση του ατόμου στον φυσικό κόσμο, ο Choi υπέθεσε ότι το ίδιο συμβαίνει και στον ψηφιακό. Έτσι, διατύπωσε τη θεωρητική πρόταση ότι οι διαδικτυακές δραστηριότητες του ατόμου, επαγγελματικές και ψυχαγωγικές, δημιουργούν μεγαλύτερες ή μικρότερες πιθανότητες θυματοποίησης από ηλεκτρονικό έγκλημα. Έχει σημασία το που πηγαίνει, το τι κάνει το άτομο στο διαδίκτυο και πώς προστατεύει τον εαυτό του από την έκθεσή του σε πιθανούς δράστες και στην θυματοποίηση. Χρησιμοποιώντας το στοιχείο του

[572] Βλ. Chang & Samuel 2004, Farag et al. 2006, Korgaonkar & Wolin (2002), Ratchford et al. (2001), Soopramanien & Robertson 2007, όπως αναφέρονται στο Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010)

[573] Pratt Travis, Holtfreter Kristy & Reisig Michael (2010)

[574] Hutchings Alice & Hennessey Hayes (1992)

[575] Choi Kyung-shick, (2008a)

[576] Mustaine, Elizabeth E. & Richard Tewksbury (1998)

επιπέδου των δραστηριοτήτων του διαδικτυακού τρόπου ζωής και του επιπέδου των μέτρων προστασίας (ως ικανού «ψηφιακού» φύλακα) του υπολογιστή, ο ερευνητής διαπίστωσε ότι τα διαφορετικά πρότυπα του διαδικτυακού τρόπου ζωής διαμορφώνουν διαφορετικές πιθανότητες θυματοποίησης στο διαδίκτυο. Έτσι, μεγαλύτερο κίνδυνο θυματοποίησης διατρέχουν οι φοιτητές που επιδεικνύουν πλημμελή διαδικτυακή συμπεριφορά, περνώντας περισσότερες ώρες σε ριψοκίνδυνες συμπεριφορές, χωρίς τη λήψη απαραίτητων μέτρων προστασίας του υπολογιστή τους που λειτουργούν ως «ικανοί» φύλακες ("capable guardians", σύμφωνα με την RAT). Ως ριψοκίνδυνες συμπεριφορές ο συγγραφέας θεώρησε την επίσκεψη σε άγνωστες ιστοσελίδες, το κατέβασμα αρχείων μουσικής (mp3) ή δωρεάν προγραμμάτων, το κλικάρισμα σε εικόνες στο διαδίκτυο, χωρίς προφυλάξεις, ενώ ως μέτρα προστασίας του υπολογιστή θεωρούνται αντιικά προγράμματα (antivirus), τείχη προστασίας (firewall) και αντικατασκοπευτικά (antispyware), που λειτουργούν ως «ικανοί ψηφιακοί φύλακες».[577]

Οι Navarro Jordana & Jasinski Jana χρησιμοποίησαν την θεωρία «καθημερινών δραστηριοτήτων» (RAT) σε μορφές ψηφιακής εγκληματικότητας όπως τον κυβερνο-εκφοβισμό (cyber-bullying). Τονίστηκε στο θεωρητικό τους πλαίσιο, όσον αφορά τα τρία στοιχεία της θεωρίας (RAT), ότι για το πρώτο στοιχείο, τους «πιθανούς εγκληματίες» - υπάρχουν πολλοί, όπως και για το δεύτερο, οι «κατάλληλοι στόχοι» είναι ευάλωτοι άνθρωποι ή υπολογιστές. Ακόμα και το τρίτο στοιχείο, η «έλλειψη ικανής προστασίας», ισχύει στο διαδίκτυο, επειδή οι γονείς πιστεύουν ότι τα συστήματα/προγράμματα γονεϊκού ελέγχου που εγκαθιστούν στον υπολογιστή των παιδιών τους είναι αρκετά για να υποκαταστήσουν την επίβλεψη από τους ίδιους. Όμως τα προγράμματα αυτά δεν μπορούν να φιλτράρουν με ποιόν μιλάνε και τι λένε τα παιδιά στα διάφορα μέσα κοινωνικής δικτύωσης ή στα μηνύματα του ηλεκτρονικού ταχυδρομείου. Αυτό εξηγεί και σύμφωνα με τη θεωρία των «Καθημερινών Δραστηριοτήτων» γιατί το cyber-bullying είναι πολύ διαδεδομένο στο διαδίκτυο. Στα ευρήματα της έρευνας αναφέρεται ότι σημαντικό ρόλο παίζει το φύλο. Βρέθηκε ότι τα κορίτσια, εφηβικής ηλικίας, πέφτουν θύματα περισσότερο συχνά από τα αγόρια. Ακόμα βρέθηκε ότι πιο πιθανά θύματα είναι τα νεαρά άτομα που συμμετέχουν σε μέσα κοινωνικής δικτύωσης. [578]

Οι Reyns, Henson και Fisher, εφήρμοσαν και αυτοί τη θεωρία των καθημερινών δραστηριοτήτων για να μελετήσουν τη θυματοποίηση φοιτητών από την κυβερνο-παρενόχληση (cyberstalking). Ως μεταβλητές, για την μέτρηση των δεικτών του τρόπου ζωής που αυξάνει τον κίνδυνο θυματοποίησης από παρενόχληση στο διαδίκτυο, οι ερευνητές χρησιμοποίησαν και τα τρία βασικά στοιχεία της θεωρίας, δηλ. την ελκυστικότητα του στόχου, την έκθεση και την εγγύτητα στον πιθανό δράστη όπως και την ύπαρξη ικανών φυλάκων.

Οι μελετητές αναφέρουν ότι τα αποτελέσματα της έρευνάς τους ενίσχυσαν την εφαρμοσιμότητα της θεωρίας των καθημερινών δραστηριοτήτων στο περιβάλλον του κυβερνοχώρου και ειδικά για τη θυματοποίηση από παρενόχληση στο διαδίκτυο, αν και η κάθε ανεξάρτητη μεταβλητή παρουσίασε διαφορετικό βαθμό και πρόσημο συσχέτισης με την εξαρτημένη που ήταν η θυματοποίηση. Μικρότερη συσχέτιση έδειξαν η «ελκυστικότητα» του στόχου και η «έκθεση» στους πιθανούς δράστες, ενώ μεγαλύτερη συσχέτιση με τη

[577] Choi, Kyung-shick, (2008b)
[578] Navarro Jordana &. Jasinski Jana (2012)

θυματοποίηση είχαν η «επαρκής φύλαξη» (αρνητική), η «εγγύτητα» στους πιθανούς δράστες και ο «επικίνδυνος τρόπος ζωής» των πιθανών θυμάτων (θετική συσχέτιση).

Καταλήγοντας οι συγγραφείς πρότειναν την ταυτόχρονη συνεκτίμηση όλων των στοιχείων της θεωρίας LRAT επειδή από τα αποτελέσματα των συναφών ερευνών δεν προκύπτει η πρωτοκαθεδρία κάποιου συγκεκριμένου ή μεμονωμένου στοιχείου έναντι των υπολοίπων στην ερμηνεία των διαδικτυακών δραστηριοτήτων που αυξάνουν τον κίνδυνο θυματοποίησης. [579]

Ο Alex Kigerl στην δική του έρευνα προσπάθησε να εξακριβώσει την εφαρμοσιμότητα της θεωρίας RAT για το κυβερνοέγκλημα σε επίπεδο χωρών. Τα κεντρικά ευρήματα της έρευνας ανέδειξαν ότι το μέγεθος των χρηστών του ίντερνετ σε 132 χώρες σχετίζεται θετικά με την εμφάνιση κυβερνοεγκλήματος. Πιο συγκεκριμένα, όσο πιο πολλούς χρήστες διαδικτύου και μεγαλύτερο κατά κεφαλήν εισόδημα διαθέτει μια χώρα, τόσο πιο αυξημένους δείκτες κυβερνο-εγκληματικής δραστηριότητας με τη μορφή spam παρουσιάζει, επειδή η ύπαρξη πολλών χρηστών συνδέεται με την πληθώρα κατάλληλων στόχων όσο και πιθανών δραστών. Ακόμα ο Kigerl βρήκε ότι σε πλουσιότερες χώρες, που διαθέτουν καλύτερη τεχνολογία και περισσότερους ειδικούς σε θέματα πληροφορικής τεχνολογίας, η ανεργία στον τομέα της πληροφορικής παρουσίασε συσχέτιση με την αυξημένη δραστηριότητα στην αποστολή spam, ειδικά από πρώην εργαζόμενους εναντίον της επιχείρησης που τους απέλυσε. [580]

Την εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων στη μελέτη και την αντιμετώπιση των ψηφιακών εγκλημάτων πρότεινε και ο καθηγητής Χρήστος Τσουραμάνης ο οποίος θεωρεί ότι η ψηφιακή εγκληματικότητα είναι αποτέλεσμα της έλλειψης ασφάλειας των πληροφοριακών συστημάτων. Έτσι για τη διάπραξη τους απαιτείται: α) ένας δράστης που διαθέτει απαραίτητες γνώσεις και κίνητρα, β) ένας πιθανός στόχος – θύμα, όπως είναι το πληροφοριακό σύστημα μιας επιχείρησης, ενός οργανισμού ή ενός απλού ιδιώτη, χρήστη και γ) απουσία ή ανεπάρκεια μέσων προφύλαξης ή πρόληψης, όπως μέτρα ασφαλείας π.χ. τείχη προστασίας (firewalls) και αντιικά προγράμματα.

Επειδή ο πρώτος παράγοντας, ο δράστης, θεωρείται από τον Τσουραμάνη αστάθμητος και δεν μπορεί ως τέτοιος να αποτελέσει εύκολα αντικείμενο άμεσου προληπτικού ελέγχου, η σημασία του δεύτερου (πληροφοριακό σύστημα ως στόχος) είναι υπεράνω αμφισβήτησης, οπότε το βάρος της πρόληψης και της αντιμετώπισης για τα ψηφιακά εγκλήματα πρέπει να εστιάσει στον τρίτο, δηλ. τα μέτρα ασφαλείας των πληροφοριακών συστημάτων για τη μείωση των πιθανών επιθέσεων εναντίον τους.[581]

Η θεωρία των καθημερινών δραστηριοτήτων, παρά το ότι αρχικά διατυπώθηκε για την ερμηνεία της παραδοσιακής εγκληματικότητας (εγκλήματα βίας και εγκλήματα δρόμου), μπορεί να αποδεικνύεται πιο χρήσιμη για την ερμηνεία της ψηφιακής και οικονομικής εγκληματικότητας. Όταν παρουσιαστούν οι κατάλληλες συνθήκες όπου τα άτομα έχουν την δυνατότητα να διαπράξουν κάποιο έγκλημα στον ψηφιακό κόσμο, γενικά δεν θα αφήσουν την ευκαιρία να πάει χαμένη.[582]

Στην περίπτωση των παγκοσμιοποιημένων οικονομικών αλλά και των ψηφιακών εγκλημάτων οι προϋποθέσεις που θέτει η θεωρία των Καθημερινών Δραστηριοτήτων

[579] Reyns, Brandford, Henson Billy & Fisher Bonnie (2011)
[580] Kigerl Alex (2012)
[581] Τσουραμάνης Χρήστος, (2005), σσ. 163-164 και Τσουραμάνης Χρήστος (2006)
[582] Morrow Jordan (2014)

φαίνεται να ισχύουν: άτομα ή οργανώσεις (όχι κατ' ανάγκη εγκληματικές) με ικανό κίνητρο τα τεράστια οικονομικά κέρδη, απευθύνονται σε ευάλωτους οικονομικούς στόχους, εναντίον άλλων ατόμων ή οργανώσεων, ακόμα και κυβερνήσεων, που διαθέτουν περιορισμένα μέσα προστασίας.

Οι Grabosky & Walkley αναφέρουν ότι η θεωρία των καθημερινών δραστηριοτήτων αποτελεί μια από τις πιο «εκλεπτυσμένες και ισχυρές εγκληματολογικές θεωρίες που παρέχουν πολύ καλές ερμηνείες τόσο για την οικονομική όσο και για την ηλεκτρονική εγκληματικότητα». Οι ίδιοι συγγραφείς μάλιστα εξέτασαν το κίνητρο, την ευκαιρία και την ύπαρξη ή την απουσία ικανής φύλαξης στην μελέτη και των δυο αυτών μορφών εγκληματικότητας. [583]

7.2. Η εφαρμογή της θεωρίας των εγκληματικών προτύπων

Η θεωρία των εγκληματικών προτύπων όπως διατυπώθηκε από τους Brantingham, αντλώντας βασικές απόψεις και συνδυάζοντας κοινά στοιχεία από άλλες θεωρίες, κυρίως της περιβαλλοντικής εγκληματολογίας (όπως των καθημερινών δραστηριοτήτων), έχει ως βασικές θέσεις της ότι οι δράστες βρίσκουν τις ευκαιρίες διάπραξης των εγκλημάτων στη διάρκεια των κανονικών, νόμιμων ασχολιών τους και ότι αναζητούν το στόχο τους σε γνωστά μέρη όπου κινούνται καθημερινά.[584]

Η μελέτη των εγκληματικών προτύπων των ηλεκτρονικο-οικονομικών εγκλημάτων μας δίνει τη δυνατότητα να εξηγήσουμε την κατανομή τους στους στόχους, όχι του φυσικού αλλά του ψηφιακού περιβάλλοντος.

Όπως συμπέραναν ο Weisburd και οι συνεργάτες του, η επίγνωση των αντίστοιχων εγκληματικών ευκαιριών από πλευράς πιθανού δράστη σχετίζεται με τις εμπειρίες κατά την επαγγελματική του ενασχόληση. Η ευκαιρία για το οικονομικό έγκλημα διαμορφώνεται από τους «κόμβους» (nodes) και τα μονοπάτια (paths) που ακολουθούν οι δράστες. Οι χώροι εργασίας του δράστη σε μια νόμιμη ή παράνομη επιχείρηση, οι εξωτερικές επιχειρήσεις ή άλλοι οργανισμοί, οι πελάτες της επιχείρησης αποτελούν τέτοιους κόμβους. Οι πιθανοί δράστες κινούνται μεταξύ αυτών των κόμβων χρησιμοποιώντας τα δίκτυα επικοινωνίας των επιχειρήσεων ως δρόμους και μονοπάτια. [585]

Οι Piquero και Weisburd διέκριναν τρία βασικά εγκληματικά πρότυπα για την εγκληματική πορεία των δραστών του λευκού περιλαιμίου:[586]

1. το πρότυπο των «περιστασιακών» εγκληματιών, που το έγκλημα αποτελεί «εξαίρεση» (crime as an aberration) και οι οποίοι εμφανίζουν μόνο μια ή δυο συλλήψεις ενώ κατά τα άλλα διάγουν ένα συμβατικό βίο με κοινωνική αναγνώριση και συμμόρφωση.
2. Των εγκληματιών που «ανταποκρίνονται σε κάποια κρίσιμη κατάσταση ανάγκης» (crisis responders) και που «εκμεταλλεύονται την ευκαιρία» (opportunity takers) που τους παρουσιάζεται. Το πρότυπο αυτό αφορά εγκλήματα που τελούνται με την εμφάνιση ιδιαίτερων περιστάσεων (όπως αδυναμία αποπληρωμής χρεών) ή ευκαιριών που παρουσιάζονται σε πιθανούς δράστες κατά την τέλεση των κανονικών εργασιακών τους καθηκόντων και οι οποίοι δεν είχαν σχεδιάσει την εγκληματική δράση αλλά απλά

[583] Βλ. Grabosky Peter & Walkley Sascha (2007), σσ. 358-375
[584] Brantigham Patricia L. & Brantigham Paul J. (1993), σσ.5-9
[585] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.180
[586] Piquero Nicole & Weisburd David (2009)

άδραξαν την ευκαιρία που αντιλήφθηκαν ότι τους παρουσιάστηκε. Θα μπορούσαμε να τους χαρακτηρίσουμε ως περιστασιακούς εγκληματίες.

Μετά παρουσιάζεται ένα ενδιάμεσο πρότυπο, αυτών που «αναζητούν την ευκαιρία» (opportunity seekers), που σχεδιάζουν και δημιουργούν συνειδητά την κατάλληλη ευκαιρία για έγκλημα.

3. το πρότυπο του «στερεοτυπικού» εγκληματία που επανειλημμένα παραβιάζει το νόμο όχι μόνο για εγκλήματα του λευκού περιλαιμίου αλλά και για ένα ευρύτερο σύνολο κοινών παραβάσεων του νόμου. Οι εγκληματίες αυτού του προτύπου μοιάζουν περισσότερο με αυτούς του «κοινού» εγκλήματος, εμφανίζοντας χαμηλότερο αυτοέλεγχο, αστάθεια στην απασχόληση και σχολική αποτυχία. [587]

Όσον αφορά τα εγκλήματα του λευκού περιλαιμίου οι διάφορες μελέτες έχουν εστιάσει περισσότερο στα αίτια και λιγότερο στις ευκαιρίες που παρουσιάζονται για τη διάπραξή τους. Έτσι αντί να μελετούν τα κίνητρα, οι διάφορες θεωρίες της περιβαλλοντικής εγκληματολογίας που εστιάζουν στην ύπαρξη των (εγκληματικών) ευκαιριών, θέτουν στο επίκεντρο του ενδιαφέροντός τους το πώς διαπράττονται τα εγκλήματα. Τέτοιες ευκαιρίες βρίσκονται στο πλαίσιο της καθημερινότητας της νόμιμης απασχόλησης που δημιουργεί ή αποτρέπει τις συνθήκες διάπραξης εγκλημάτων. Η μετατόπιση του ενδιαφέροντος, σύμφωνα με τους Benson, Madensen και Eck, από το «γιατί» στο «πώς» επιτρέπει και τον καλύτερο σχεδιασμό της πρόληψης και της αντιμετώπισης των εγκλημάτων. [588]

Οι Benson, Madensen και Eck προσπάθησαν να διακριβώσουν εκείνα τα επαγγελματικά και επιχειρησιακά χαρακτηριστικά που μπορεί να διευκολύνουν τη διάπραξη εγκλημάτων με εξαπάτηση και κατάχρηση της θέσης κάποιου στην επιχείρηση και κατά τη διάρκεια της επαγγελματικής του ενασχόλησης.[589] Οι ερευνητές πιστεύουν ότι τα εγκλήματα Λευκού Περιλαιμίου γενικά είναι αποτέλεσμα της συνύπαρξης δυο παραγόντων: των νόμιμων δραστηριοτήτων στο πλαίσιο μιας επιχείρησης από τη μια και από την άλλη των παράνομων, «παρασιτικών» διαδικασιών που εμφανίζονται στο πλαίσιο των πρώτων. Κεντρική σημασία στη μελέτη των οικονομικών εγκλημάτων αποκτά λοιπόν το πώς οι δομές και τα συστήματα στο πλαίσιο νόμιμων επιχειρήσεων μπορεί να δημιουργούν ή να μειώνουν τις ευκαιρίες για εγκλήματα και το πώς οι εγκληματίες εκμεταλλεύονται τις νόμιμες διαδικασίες προκειμένου να τελέσουν παράνομες πράξεις. Οι εγκληματίες μπορούν να αποκτούν πρόσβαση στους στόχους- θύματά τους ιδιαίτερα μέσω των συστημάτων της επιχείρησης που διευκολύνουν την επαφή μαζί τους.[590]

Για τη μελέτη και τον έλεγχο του εγκλήματος λευκού περιλαιμίου οι Benson, Madensen και Eck πρότειναν την εφαρμογή των «εγκληματικών ευκαιριών» όπως αυτή συνίσταται από τις τρεις βασικές θεωρίες, των καθημερινών δραστηριοτήτων, των εγκληματικών προτύπων και της περιστασιακής πρόληψης του εγκλήματος, εφόσον αυτές μας παρέχουν το απαραίτητο θεωρητικό πλαίσιο για την κατανόηση του πώς οι εγκληματικές ευκαιρίες διαμορφώνονται από το άμεσο περιβάλλον του δράστη, πώς ανακαλύπτονται και αξιολογούνται από αυτόν. Για την εφαρμογή των θεωριών αυτών στο έγκλημα λευκού περιλαιμίου απαιτείται η κατά κάποιο τρόπο προσαρμογή τους.[591]

[587] Piquero Nicole &Weisburd David (2009)

[588] Benson Michael L., Madensen Tamara D., & Eck John E. (2009)

[589] Benson Michael L., Madensen Tamara D., & Eck John E. (2009)

[590] Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013)

[591] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.178

Η θεωρία των εγκληματικών προτύπων, όπως είδαμε παραπάνω, έχει ως βασική θέση ότι οι δράστες γνωρίζουν τις εγκληματικές ευκαιρίες στις καθημερινές τους δραστηριότητες κινούμενοι στα όρια οικείων τοποθεσιών και στο πλαίσιο νόμιμων ενασχολήσεων. Για την εφαρμογή των εγκληματικών προτύπων στην διερεύνηση του πώς κατανέμονται τα εγκλήματα του λευκού περιλαιμίου σε διάφορους κατάλληλους στόχους απαιτείται η προσαρμογή της θεωρίας, επειδή οι δράστες των οικονομικών εγκλημάτων αυτού του είδους δεν ανακαλύπτουν τις εγκληματικές ευκαιρίες μετακινούμενοι στο δρόμο, αλλά εκμεταλλεύονται τις ευκαιρίες που τους παρουσιάζονται στο πλαίσιο της επαγγελματικής τους ενασχόλησης. Έτσι οι «κόμβοι» και τα «μονοπάτια»[592] στα οποία οι εγκληματίες του λευκού περιλαιμίου ανακαλύπτουν τις ευκαιρίες διάπραξης βρίσκονται στις νόμιμες επιχειρήσεις όπου εργάζονται ή τις παράνομες τις οποίες έχουν συστήσει και περιλαμβάνουν διαδικασίες και δίκτυα με τα οποία αποκτούν επικοινωνία και συνεργάζονται με τους άλλους. Το έγκλημα είναι πιθανότερο να συμβεί στα μονοπάτια που χρησιμοποιούνται πιο συχνά και από περισσότερα άτομα, άρα στο πλαίσιο μεγαλύτερων δικτύων και περισσότερο συχνά εφαρμοζόμενων πρακτικών. Σύμφωνα ακόμα με τη θεωρία των εγκληματικών προτύπων των Brantigham το έγκλημα είναι πιθανότερο να συμβεί στα «όρια» που χωρίζουν περιοχές συγκεκριμένων δραστηριοτήτων γιατί εκεί συγκεντρώνονται περισσότεροι άγνωστοι οι οποίοι δεν μπορούν να αναγνωριστούν ότι ανήκουν ή όχι στο χώρο. Για τα εγκλήματα του λευκού περιλαιμίου τα όρια εμφανίζονται όταν δυο κόμβοι διασυνδέονται μέσω ενός μονοπατιού και όταν στο μονοπάτι αυτό δεν υπάρχει κάποιο κανονιστικό σύστημα ή ένα σύστημα αναγνώρισης και αποτροπής των εγκληματικών δραστηριοτήτων. Τα όρια βρίσκονται κοντά σε μονοπάτια που δεν ελέγχονται και κοντά στην κομβική βάση του δράστη.

Έτσι, εφαρμόζοντας τη θεωρία των εγκληματικών προτύπων και τη μελέτη των ηλεκτρονικο-οικονομικο-εγκλημάτων θα πρέπει να εξακριβωθούν οι «κόμβοι», να εντοπιστούν τα «μονοπάτια» και τέλος οι ευκαιρίες που αυτά περιλαμβάνουν.[593]

7.3. Η εφαρμογή της «περιστασιακής πρόληψης του εγκλήματος»

Η στρατηγική της περιστασιακής πρόληψης του εγκλήματος αποτελεί ουσιαστικά την εφαρμογή των θεωριών της περιβαλλοντικής εγκληματολογίας για τη δόμηση των «εγκληματικών ευκαιριών», όπως της ορθολογικής επιλογής, των καθημερινών δραστηριοτήτων και των εγκληματικών προτύπων στην πρόληψη του εγκλήματος. Η περιστασιακή πρόληψη του εγκλήματος εστιάζει και αυτή το ενδιαφέρον στο εγκληματικό γεγονός καθαυτό, στο πώς, στις συνθήκες του εγκλήματος παρά στον δράστη και τα κίνητρά του. Όμως, ενώ οι θεωρίες των καθημερινών δραστηριοτήτων και των εγκληματικών προτύπων ασχολούνται περισσότερο με το πώς, τον τρόπο που οι δράστες αποκτούν πρόσβαση στις εγκληματικές ευκαιρίες, η στρατηγική της «περιστασιακής πρόληψης του εγκλήματος» επικεντρώνεται στο γιατί κάποιες ευκαιρίες προσελκύουν περισσότερο τους εγκληματίες από κάποιες άλλες. [594] Ακόμα, αντλώντας βασικές απόψεις από την ορθολογική επιλογή θεωρεί ότι ο δράστης υπολογίζει τα οφέλη και τα κόστη[595] και επιχειρεί την διασύνδεση των εγκληματικών αποφάσεων σε σχέση με τα οφέλη και τα κόστη σε πέντε διαστάσεις:

[592] Για τους όρους *κόμβοι* και *μονοπάτια*, *δίκτυα* βλ. παράγραφο για τη «Θεωρία των «εγκληματικών προτύπων» των Brantingham.

[593] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.180

[594] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.183

[595] Cornish Derek & Clarke Roland (1986), σσ.1-6

1. την προσπάθεια που απαιτείται για την διάπραξη του εγκλήματος,
2. τους πιθανούς κινδύνους που συνεπάγεται η διάπραξη,
3. τις ανταμοιβές για τον δράστη,
4. τις περιστασιακές συνθήκες που ενθαρρύνουν το δράστη,
5. τις εκλογικεύσεις του δράστη για να προβεί στην τέλεση του εγκλήματος.

Έτσι, όπως πρότειναν οι Benson, Madensen και Eck, το έγκλημα είναι πιο πιθανό να τελεστεί όταν διαθέτει ευκολία διάπραξης, χαμηλό κίνδυνο επισήμανσης από τις διωκτικές αρχές, υψηλό αναμενόμενο όφελος, ενθάρρυνση από τις περιβάλλουσες συνθήκες και ικανή δικαιολογία. Τα παραπάνω ισχύουν για κάθε κατηγορία εγκλήματος, όπως και για τα οικονομικά εγκλήματα, όπου θα πρέπει να διακριβωθεί η παρουσία κάθε μιας από αυτές τις διαστάσεις των εγκληματικών ευκαιριών για την εφαρμογή της θεωρίας στη μελέτη τέτοιων μορφών εγκληματικής συμπεριφοράς.[596]

Για την εφαρμοσιμότητα των προτάσεων που προέρχονται από την περιστασιακή πρόληψη του εγκλήματος, οι Benson και Madensen πρότειναν: Πρώτον, να εστιάζουμε στις ειδικότερες μορφές εγκλήματος κατά τη διαμόρφωση των εγκληματικών ευκαιριών τους. Δεύτερο, να επαναπροσδιορίσουμε την έννοια του τόπου και να συμπεριλάβουμε σε αυτή τη δομή των δικτύων επικοινωνίας (που αποτελούν τα μονοπάτια, τις διόδους/paths)[597] που διευκολύνουν την επαφή δράστη και θύματος. Τρίτο, να λάβουμε υπόψη ότι οι δράστες των οικονομικών εγκλημάτων διαθέτουν υψηλότερο βαθμό ορθολογικότητας από ότι αυτοί των κοινών εγκλημάτων και συνακόλουθα είναι πιο προσαρμόσιμοι στις διάφορες αλλαγές των δομών που συνθέτουν την εγκληματική ευκαιρία.[598]

Οι Benson, Madensen και Eck συνεξέτασαν τις τρεις θεωρητικές απόψεις για τη δόμηση των «εγκληματικών ευκαιριών» εφαρμόζοντάς τις στο έγκλημα του λευκού περιλαιμίου στον τομέα της υγείας με σκοπό τη διακρίβωση των ιδιαίτερων εκείνων χαρακτηριστικών στοιχείων που δομούν την ύπαρξη κάθε συγκεκριμένης εγκληματικής ευκαιρίας και τις συνθήκες αποτροπής της. Παρά το γεγονός ότι οι μελετητές τις εξετάζουν συχνά κάτω από ίδιο θεωρητικό πρίσμα, το κάθε είδος εγκληματικής δραστηριότητας διαθέτει διαφορετικά χαρακτηριστικά ως προς την ευκαιρία διάπραξης της. Τα χαρακτηριστικά αυτά έχουν να κάνουν με το «πότε», το «που», το «ποιος» είναι ο δράστης και το «ποιος» είναι το θύμα. Για το λόγο αυτό οι Benson, Madensen και Eck πρότειναν την διάκριση μεταξύ των διαφορετικών ειδών εγκλημάτων, ακόμα και μεταξύ αυτών του λευκού περιλαιμίου, επειδή αυτή η κατηγορία από μόνη της περιλαμβάνει μεγάλος εύρος εγκληματικών δραστηριοτήτων.[599]

Σύμφωνα με τους Benson, Madensen και Eck, οι προτάσεις κατά την εφαρμογή των προσεγγίσεων των «εγκληματικών ευκαιριών» στην μελέτη του εγκλήματος του λευκού περιλαιμίου εστιάζονται στα εξής:

- Η ευκαιριακή δομή παρουσιάζεται σε όλα τα είδη εγκλήματος του λευκού περιλαιμίου και των μορφών του όπως το ηλεκτρονικο-οικονομικό έγκλημα.
- Η ευκαιριακή δομή διαφέρει ανάμεσα στα διαφορετικά είδη εγκλήματος του λευκού περιλαιμίου.

[596] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.183

[597] Για τους όρους *κόμβοι* και *μονοπάτια, δίκτυα* βλ. παράγραφο για τη «Θεωρία των «εγκληματικών προτύπων» των Brantingham.

[598] Benson Michael L., Madensen Tamara D. (2007), σ. 617

[599] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.184

- Οι θεωρίες των καθημερινών δραστηριοτήτων, των εγκληματικών προτύπων και η περιστασιακή πρόληψη του εγκλήματος μπορούν να εφαρμοστούν στη μελέτη του εγκλήματος του λευκού περιλαιμίου.
- Η γνώση του τρόπου διάπραξης των εγκλημάτων αυτών οδηγεί και στην αποτελεσματική πρόληψη και καταπολέμησή τους.
- Η κατάλληλη μέθοδος διερεύνησής τους είναι η μελέτης περίπτωσης (case studies). [600]

Στον τομέα της μελέτης του οικονομικού εγκλήματος και ειδικότερα της οικονομικής απάτης η Κραμβιά –Καπαρδή πρότεινε τη θεωρία ROP (Rationalization – Opportunity - Person) που αποτελεί μια προσπάθεια σύνθεσης: α) της στρατηγικής του Clarke για την περιστασιακή πρόληψη του εγκλήματος και των Cohen & Felson που τονίζουν τη σημασία των ευκαιριών (Opportunity) που δημιουργούνται για τη διάπραξη του οικονομικού εγκλήματος, [601] β) των κινήτρων του ατόμου (Person) με βάση τις ανάγκες που κινητοποιούν τα άτομα σε δράση όπως τις ιεράρχησε ο Maslow[602] και γ) των εκλογικεύσεων (Rationalization) που κάνουν τα άτομα για τις εγκληματικές πράξεις τους ώστε να μην νοιώθουν ενοχές σύμφωνα με τον Albrecht, τον Cressey και τον Matza.[603]

Η Κραμβιά - Καπαρδή στηρίχθηκε σε προγενέστερες σχετικές θεωρίες του Albrecht (1995), του Cressey (1986) και του Loebbecke (1989) και σε δικές της μελέτες υποθέσεων οικονομικής απάτης στην Μελβούρνη κατά το ’90[604] και στην Κύπρο[605] για να δομήσει το δικό της ερμηνευτικό μοντέλο προσέγγισης του οικονομικού εγκλήματος, που ονόμασε ROP και συνοψίζεται στα εξής. Η πιθανότητα διάπραξης απάτης (Pr -Probability) εξαρτάται από την συνύπαρξη των παρακάτω τριών μεταβλητών:

α) την ύπαρξη ενός ατόμου με ***κίνητρο*** και προδιάθεση (P). Τέτοια είναι τα άτομα που αντιμετωπίζουν οικονομικά ή άλλα προβλήματα, με εγωκεντρισμό, που επιδιώκουν τη διατήρηση της θέσης και του κύρους τους, με εθισμούς κλπ.

β) την ύπαρξη ***ευκαιρίας*** (O), όπως η πρόσβαση σε χρήματα, που ανακύπτει κυρίως από την *έλλειψη* τακτικού *ελέγχου* μιας εταιρείας ή άλλων επιτηρητών, η αντίληψη εξασφάλισης ατιμωρησίας, η ύπαρξη εύπιστων ατόμων ως θύματα.

γ) της ***εκλογίκευσης*** της συμπεριφοράς (R), σύμφωνα με τις τεχνικές εκλογίκευσης των Sykes και Matza. Οι δράστες θεωρούν ότι η συμπεριφορά τους δεν είναι έγκλημα, ότι δικαιούνται τα χρήματα που κλέβουν ή ότι η επιχείρηση αξίζει να χάσει τα χρήματα.[606]

Θα πρέπει να σημειώσουμε ότι και ο Kovavich, μελετώντας τα εγκλήματα εργασίας, θεωρεί ότι απαιτούνται οι τρεις –παραπάνω – προϋποθέσεις:

ι) Το κίνητρο, το τι ωθεί τα άτομα στη διάπραξη του εγκλήματος.

ιι) Η εκλογίκευση της πράξης. Η «λογική» αιτιολόγηση, ερμηνεία της πράξης του από το ίδιο το άτομο.

[600] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.189
[601] Κραμβιά- Καπαρδή Μαρία (2001), σσ. 139-141
[602] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ. 48
[603] Κραμβιά- Καπαρδή Μαρία (2001), σσ. 140-141
[604] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σσ. 46-48
[605] Κραμβιά- Καπαρδή Μαρία., (2001), σσ. 142-145
[606] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σσ. 50-51

ιιι) Η ευκαιρία διάπραξης του εγκλήματος. Τέτοια ευκαιρία έχουν περισσότερο οι Λογιστές, το προσωπικό ασφαλείας, οι υπεύθυνοι προώθησης του προϊόντος, το οικονομικό προσωπικό, οι αποθηκάριοι. [607]

Μετά την έρευνα που διεξήγαγε η Κραμβιά-Καπαρδή, στην Αυστραλία αλλά και στην Κύπρο, συμπέρανε ότι η θεωρία της ROP και το τρίπτυχο των παραγόντων που πρότεινε επιβεβαιώθηκε, δηλαδή για την τέλεση οικονομικών εγκλημάτων όπως η απάτη απαιτούνται τα στοιχεία: ένα άτομο με κίνητρο, η ευκαιρία και η δικαιολόγηση της πράξης από τον δράστη της.[608]

Η σημασία της ευκαιρίας τονίζεται από την Κραμβιά - Καπαρδή ως η ευνοϊκότερη συνθήκη από τους τρεις προαναφερθέντες παράγοντες για την τέλεση του οικονομικού εγκλήματος, κατά συνέπεια το αποτελεσματικότερο μέσο για την πρόληψη της απάτης είναι η μείωση ή η εξαφάνιση της ευκαιρίας για την διάπραξή της. Η ύπαρξη της κατάλληλης ευκαιρίας συνδέεται με την απουσία ή την έλλειψη εσωτερικού ελέγχου, που σύμφωνα με έρευνα της ACFE (Association of Certified Fraud Examiners) το 2010 αποτελεί τον κυριότερο παράγοντα (σε ποσοστό 38%) που διευκολύνει την εμφάνιση της απάτης.[609] Έτσι η μείωση των εγκληματικών ευκαιριών προέρχεται κυρίως μέσω της ανάπτυξης εσωτερικών συστημάτων ελέγχου σε συνδυασμό με την ύπαρξη εξωτερικών ελεγκτών.[610]

Από την παράθεση των παραπάνω απόψεων της Κραμβιά - Καπαρδή διαπιστώνεται η υιοθέτηση από την συγγραφέα βασικών θέσεων των «εγκληματικών ευκαιριών», τόσο από την πλευρά της περιστασιακής πρόληψης του εγκλήματος, όσο και από την άποψη των καθημερινών δραστηριοτήτων. Αν και η ίδια δεν κάνει άμεσα αναφορά στη θεωρία των καθημερινών δραστηριοτήτων, οι ομοιότητες των θέσεων είναι προφανείς: Το «άτομο με κίνητρο» της Κραμβιά - Καπαρδή είναι ο «δράστης με κίνητρο» των Felson και Cohen, η ύπαρξη της ευκαιρίας στα πρόσωπα εύπιστων ατόμων τα καθιστά «κατάλληλους στόχους», ενώ η έλλειψη επιτήρησης και τακτικού ελέγχου αφορά άμεσα την «απουσία ικανών φυλάκων».

7.4. Το ζήτημα της επιλογής μεθόδου μελέτης του ηλεκτρονικο - οικονομικού εγκλήματος

Η σημασία των λεπτομερειών του τρόπου δράσης, όχι μόνο των εγκληματιών αλλά και των όσων τους περιβάλλουν όπως πιθανά θύματα, φύλακες κλπ, θα πρέπει να ληφθεί υπόψη για το σχηματισμό του προτύπου της εγκληματικής ευκαιρίας που εκμεταλλεύεται ο πιθανός δράστης. Συνεπώς η καταλληλότερη ερευνητική μέθοδος για το πώς δομούνται οι εγκληματικές ευκαιρίες του εγκλήματος λευκού περιλαιμίου είναι η μελέτη περίπτωσης (case study) η οποία μας επιτρέπει να εστιάσουμε στο πώς και στις διαδικασίες της διάπραξης.[611]

Στις περιπτώσεις μελέτης του εγκλήματος του λευκού περιλαιμίου οι ποσοτικές έρευνες παρουσιάζουν αρκετές δυσκολίες εμφανίζοντας αντιφατικά αποτελέσματα.[612] Για το λόγο

[607] Λάζος Γρηγόρης (2001), σσ. 56 -60

[608] Βλ. Κραμβιά- Καπαρδή Μαρία (2001), σσ. 145-147 και Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σ.48

[609] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος, (2011), σσ. 48-49

[610] Κραμβιά- Καπαρδή Μαρία (2001), σ. 147

[611] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.187

[612] Coleman James.W. (1995), σ. 373, βλ. και παρακάτω για τη δόμηση της εγκληματικής ευκαιρίας στις βιομηχανίες.

αυτό, οι Clinard και Yeager πρότειναν τη χρήση πιο εκλεπτυσμένων και ποιοτικών μεθόδων μελέτης[613]. Η επιλογή της μελέτης περίπτωσης υπό το πρίσμα των «εγκληματικών ευκαιριών» ως καταλληλότερης μεθόδου διερεύνησης των εγκλημάτων λευκού περιλαιμίου συνάδει και με το γεγονός ότι τα εγκλήματα αυτά παρουσιάζουν μικρή θεατότητα και μεγάλο σκοτεινό αριθμό. Έτσι θα πρέπει να εξετάζουμε τα λίγα περιστατικά που αποκαλύπτονται ως μη μεμονωμένα και μάλλον αντιπροσωπευτικά του συνόλου τους εφόσον οι τρόποι διάπραξης τους δεν εμφανίζουν σημαντικές διαφορές. Όπως έδειξαν οι Calavita και Pomell κατά τη κρίση του ΄80 υπήρχαν πολλά παραδείγματα τέτοιων εγκλημάτων, που επαναλαμβάνονταν. Συνεπώς, όπως πρότειναν οι Benson και Madensen μπορούμε να επισημάνουμε τις ευκαιριακές δομές και τις συνθήκες διαμόρφωσης των προτύπων αυτών των εγκλημάτων.[614]

Δεν είναι λίγοι οι μελετητές στο πεδίο του εγκλήματος του λευκού περιλαιμίου, μηδέ του Sutherland εξαιρουμένου, που χρησιμοποίησαν τη μελέτη περίπτωσης (case study) ως μέθοδο προσέγγισης του φαινομένου: Sutherland (1949) για το επιχειρηματικό έγκλημα για εγκλήματα δημιουργίας τραστ, Geis 1977, Reuter 1993, Simpson 2001, για περιβαλλοντικά εγκλήματα από τους Block & Bernard 2002, εγκλήματα στην αγορά φαρμάκων του Vaughan 1983, λογιστικές απάτες των McLean & Elkind 2003, παραβιάσεις κανόνων ασφάλειας σε χώρους εργασίας των Aulette and Michalowski 1993, παραβιάσεις κανόνων ασφάλειας καταναλωτικών αγαθών των Mintz 1995, Cullen 2006 [615]

Οι μελέτες αυτές εστίασαν στο «πως» διαπράττεται αυτό το είδος εγκλήματος και στην οπτική της ευκαιριακής δομής του. Οι θεωρίες για τη δόμηση των «εγκληματικών ευκαιριών», όπως αυτές που εξετάζουμε εδώ, των καθημερινών δραστηριοτήτων, του εγκληματικού προτύπου, σε συνδυασμό με την μέθοδο μελέτης περίπτωσης παρέχουν στους μελετητές ξεκάθαρο θεωρητικό πλαίσιο δίνοντας τη δυνατότητα εξέτασης μιας συγκεκριμένης μεταβλητής, που θα προέρχεται από τη μια ή την άλλη οπτική των «εγκληματικών ευκαιριών», σε σχέση με ένα από τα είδη του εγκλήματος. Ακόμα παρέχουν την δυνατότητα διερεύνησης των επιδράσεων που ασκούν αιτιώδεις παράγοντες, όπως οι αλλαγές στο νομικό πλαίσιο, στη διαμόρφωση των ευκαιριών διάπραξης οικονομικού εγκλήματος. Τέλος δεν θα πρέπει να αγνοηθεί η σημασία της εφαρμογής της μελέτης περίπτωσης στο πλαίσιο της προσέγγισης των «εγκληματικών ευκαιριών» στον τομέα της πρόληψης και του ελέγχου των εγκλημάτων αυτών.[616]

Η εστίαση του αντικειμένου μελέτης στις εγκληματικές ευκαιρίες καθιστούν το έγκλημα του λευκού περιλαιμίου από «περιφερειακή» μορφή εγκλήματος σε κομμάτι της καθημερινής ζωής και την αντιμετώπισή του εφικτή με τις ίδιες σχεδόν μεθόδους που χρησιμοποιούνται και στο έγκλημα του δρόμου. [617]

[613] Βλ. Coleman James.W. (1995), σ. 373

[614] Benson Michael L. & Madensen Tamara D. (2007), σ.615

[615] Βλ. Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.189, αναφορά για μελέτη περίπτωσης

[616] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.190

[617] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σ.189

ΚΕΦΑΛΑΙΟ 8. ΤΟ ΕΓΚΛΗΜΑΤΙΚΟ ΠΡΟΤΥΠΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟ – ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στο κεφάλαιο αυτό θα εξετάσουμε τα στοιχεία που συντελούν στη διαμόρφωση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος σύμφωνα με τις θεωρίες της περιβαλλοντικής εγκληματολογίας για τη διαμόρφωση των «εγκληματικών ευκαιριών» που αποτελούν το θεωρητικό πλαίσιο της παρούσας διατριβής.

8.1. Διάκριση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος και του κοινού εγκλήματος

Υπάρχουν πολλές διαφορές μεταξύ του οικονομικού εγκλήματος που τελείται με ηλεκτρονικά μέσα από τη μια πλευρά και του συμβατικού εγκλήματος από την άλλη, τόσο στη διάπραξη όσο και στη δίωξη τους.

Οι βασικές διαφορές έχουν σχέση με το πλαίσιο δράσης: τον τρόπο, το χρόνο και τον τόπο τέλεσης του εγκλήματος. Αυτά τα στοιχεία καθιστούν πολύ δύσκολη την ανίχνευση, τη σύλληψη και την ποινική δίωξη του δράστη του ηλεκτρονικο-οικονομικού εγκλήματος με το ισχύον νομικό σύστημα.

Τις περισσότερες φορές, ο εγκληματίας μπορεί να βρίσκεται μακριά από τη θέση όπου πραγματοποιείται το έγκλημα. Οι επιτιθέμενοι μπορούν να επιλέξουν τη θέση που βρίσκονται όταν πρόκειται να διαπραχτεί το έγκλημα επειδή η τέλεση του ηλεκτρονικο-οικονομικού εγκλήματος δεν απαιτεί φυσική παρουσία του δράστη. Ένα απλό πρόγραμμα μπορεί να γραφτεί από τον επιτιθέμενο και να εισαχθεί οποιαδήποτε στιγμή στο δίκτυο κάποιας επιχείρησης. Το πρόγραμμα μπορεί να οριστεί με χρονοπρογραμματισμό να εκτελεστεί οποιαδήποτε στιγμή επιλέγει ο δράστης. Υπάρχει μια ομοιότητα με μια ωρολογιακή βόμβα, αλλά το μικρό πρόγραμμα είναι πολύ ευκολότερο να κρύβεται και να μεταμφιέζεται μέσα στο δίκτυο. Δεν είναι ακόμα απαραίτητο για το πρόγραμμα για να είναι μέσα στο δίκτυο, θα μπορούσε να αποσταλεί από οποιαδήποτε μέρος της γης μέσω ενός υπολογιστή συνδεδεμένου με το Διαδίκτυο.

Κατά την κλοπή των πληροφοριών, οι επιτιθέμενοι έχουν διάφορες επιλογές από όπου μπορούν πραγματικά να κλέψουν τα δεδομένα. Κατ' αρχάς, μπορούν να κλέψουν από τον κεντρικό υπολογιστή, δεύτερο από το συνοδευτικό κεντρικό υπολογιστή, που κρατά ένα πλήρες αντίγραφο του κύριου κεντρικού υπολογιστή, τρίτο κατά τη μεταφορά των δεδομένων μεταξύ δύο σημείων, και τέταρτο από ιστοσελίδες, οι οποίες παρουσιάζουν τα δεδομένα στον τελικό χρήστη. Δεν έχει σημασία ποια μέθοδο θα επιλέξει ο δράστης δεδομένου ότι υπάρχει μια μεγάλη πιθανότητα ότι η επίθεση θα περάσει απαρατήρητη επειδή οι πληροφορίες δεν δημοσιεύονται αμέσως. Ένα συμβατικό έγκλημα, η κλοπή μετρητών παραδείγματος χάριν, θα παρατηρηθεί την αμέσως επόμενη φορά που θα καταμετρηθούν τα χρήματα. Η κλοπή ψηφιακών δεδομένων είναι διαφορετική περίπτωση. Όλες οι πληροφορίες βρίσκονται ακόμα στον κεντρικό υπολογιστή και φαίνονται άθικτες γιατί ο δράστης κάνει αντίγραφο των δεδομένων.

Τα θύματα του οικονομικού κυβερνο-εγκλήματος είναι συνήθως οργανισμοί, επιχειρήσεις και οι πελάτες τους, των οποίων τα συστήματα δέχονται επιθέσεις. Σε περίπτωση κλοπής δεδομένων, τα στοιχεία θα μπορούσαν να αφορούν αυστηρά την επιχείρηση ή θα μπορούσε να είναι μια βάση δεδομένων πελατών με στοιχεία όπως τους αριθμούς κοινωνικής ασφάλισης, πληροφορίες πιστωτικών καρτών, διευθύνσεις αποστολής και άλλες λεπτομέρειες. Επομένως οι οργανισμοί μπορούν να υποστούν σημαντικές απώλειες υπό τη

μορφή χαμένων πελατών ή/και κλεμμένων εμπιστευτικών πληροφοριών. Οι πελάτες μπορούν επίσης να υποστούν οικονομικές και άλλες απώλειες, όταν κλέβεται η ταυτότητά τους.

Οι επιτιθέμενοι - χάκερ μπορούν να είναι ειδικοί στον τομέα όπου κάνουν το έγκλημά τους, εμπειρογνώμονες ασφάλειας υπολογιστών, προγραμματιστές, ειδικοί διαδικτύου. Αφ' ετέρου οι επιχειρήσεις στηρίζονται στην εργασία υπαλλήλων τους, όπως οι παραπάνω, για να προστατεύουν τα δίκτυα τους. Ακόμα οι επιτιθέμενοι μπορούν να ενεργούν σε οργανωμένη ομάδα, τα μέλη της οποίας μοιράζονται πληροφορίες χωρίς να αποκαλύπτεται η ταυτότητα τους στο διαδίκτυο, καθιστώντας έτσι το στόχο της επιβολής νόμου ακόμα δυσκολότερο. Το ίδιο το διαδίκτυο προσφέρει περισσότερες ευκαιρίες για τους επιτιθεμένους να επικοινωνούν χωρίς να αποκαλύπτεται η ταυτότητα τους και τους δίνει ένα μεγάλο πλεονέκτημα έναντι των αρχών.[618]

Ο Λάζος διακρίνει μάλιστα μια ακόμα ποιοτική διαφορά μεταξύ πληροφορικού και μη πληροφορικού εγκλήματος η οποία αφορά το «μόνιμο και αυτόματο των αποτελεσμάτων» του εγκλήματος. Από τη στιγμή που διαπιστώνει κάποιο κενό ασφαλείας στο δίκτυο υπολογιστών και το λογισμικό του, ο εισβολέας τείνει να επαναλαμβάνει τη δράση του, συχνά με αυτόματο τρόπο εγκαθιστώντας κάποιο κακόβουλο πρόγραμμα το οποίο εκτελεί αυτόματα τις εντολές ακόμα και στην περίπτωση που ο δράστης διακόπτει την πράξη της παραβίασης.[619]

Ο Τσουραμάνης διακρίνει τα ψηφιακά εγκλήματα από τα παραδοσιακά ως προς τα εξής χαρακτηριστικά:

- Τα ψηφιακή εγκλήματα τελούνται από μακρινή απόσταση.
- "Τόπος" τέλεσής τους είναι ο αποκαλούμενος κυβερνοχώρος.
- Ο εντοπισμός τους είναι πιο περίπλοκος από τεχνολογική άποψη.
- Τα αναμενόμενα κέρδη είναι μεγάλα ενώ ο κίνδυνος ανακάλυψης μικρός.
- Ο αριθμός των θυμάτων τους είναι πολύ μεγαλύτερος.
- Οι οικονομικές απώλειες για τα θύματά τους είναι πολύ μεγαλύτερες από αυτές των θυμάτων των παραδοσιακών εγκλημάτων.
- Παρουσιάζουν πολύ σημαντικό "σκοτεινό αριθμό".

Τα τελευταία τέσσερα από τα αυτά τα χαρακτηριστικά τους μας επιτρέπουν, σύμφωνα με τον Τσουραμάνη να εντάξουμε τα ψηφιακά εγκλήματα στην κατηγορία των οικονομικών εγκλημάτων.[620]

Το εγκληματικό πρότυπο λοιπόν του ηλεκτρονικο-οικονομικού εγκλήματος διαφέρει σημαντικά από αυτό του κοινού εγκλήματος και από την άποψη της ευκαιριακής του δομής. Η εγκληματική πορεία των δραστών είναι διαφορετική, η εμπλοκή στην εγκληματική δραστηριότητα πραγματοποιείται σε διαφορετική περίοδο της ζωής των δραστών όπως και τα κοινωνικά τους χαρακτηριστικά είναι διαφορετικά.

Όσον αφορά την διάκριση εγκλήματος λευκού περιλαιμίου και κοινού εγκλήματος οι Piquero και Benson σημειώνουν, παρά το γεγονός ότι οι καταδικασμένοι ως εγκληματίες λευκού περιλαιμίου δεν διέθεταν και τόσο σημαντική κοινωνική θέση[621], εντούτοις διαφέρουν σημαντικά σε σχέση με αυτούς του κοινού εγκλήματος. Οι διαφορές εστιάζονται στο ότι οι εγκληματίες με το λευκό περιλαίμιο προέρχονται από διαφορετικό κοινωνικό

[618] Nykodym Nick, Taylor Robert, & Vilela Julia (2005)
[619] Λάζος Γρηγόρης (2001), σσ. 47-48
[620] Τσουραμάνης Χρήστος (2006)
[621] Βλ. και παραπάνω για τα χαρακτηριστικά του δράστη με λευκό περιλαίμιο.

υπόβαθρο, πιο προνομιούχο και λιγότερο προβληματικό, σε σχέση με τους δεύτερους, δεν μοιράζονται κοινό κοινωνικό χώρο. Μια ακόμα σημαντική διαφορά έχει να κάνει με την εγκληματική «καριέρα» ως προς τη διάρκεια αλλά και τον χρόνο έναρξης και λήξης της. Οι εγκληματίες με το λευκό περιλαίμιο ξεκινούν την εγκληματική τους καριέρα σε αρκετά μεγαλύτερη ηλικία, με μέση ηλικία έναρξης τα 35 έτη, έναντι πρώτης σύλληψης κατά την εφηβική ηλικία για αυτούς που διαπράττουν κοινό έγκλημα δρόμου. Οι πρώτοι διαθέτουν εγκληματική καριέρα που διαρκεί περισσότερο, αλλά με μικρότερη συχνότητα συλλήψεων, με μέση διάρκεια τα 14 έτη σε σχέση με τα 5 έτη των δεύτερων. Ενδιαφέρον παρουσιάζει και ο χρόνος λήξης της εγκληματικής «καριέρας», με μέση ηλικία τελευταίας σύλληψης για έγκλημα λευκού περιλαιμίου τα 43, έναντι 30 για τους κοινούς εγκληματίες.[622]

8.2. Ο ρόλος της τεχνολογίας στη δόμηση της εγκληματικής ευκαιρίας για το ηλεκτρονικο-οικονομικό έγκλημα

Η αλματώδης εξέλιξη της τεχνολογίας τις τελευταίες δεκαετίες δημιουργεί παγκοσμίως οικονομικές και πολιτισμικές ευκαιρίες που πριν δεν ήταν διαθέσιμες. Οι αποστάσεις εκμηδενίζονται και οι επιρροές είναι πλέον παγκόσμιες. Η εφαρμογή της πληροφορικής τεχνολογίας, όχι μόνο στην οικονομία αλλά και στην καθημερινή ζωή, αλλάζει ριζικά τις κοινωνικές σχέσεις και δημιουργεί νέες διεξόδους και τρόπους εφαρμογής στο έγκλημα και κυρίως το οικονομικό που εκσυγχρονίζεται και από παραδοσιακό μετατρέπεται σε ηλεκτρονικό. Η αυξανόμενη εξάρτηση των σύγχρονων επιχειρήσεων και οργανισμών από τα συστήματα πληροφορικής και υπολογιστών τις κατέστησε περισσότερο ευάλωτες στο ηλεκτρονικό έγκλημα. Από την άλλη πλευρά δεν είναι μόνο οι νέες μορφές εγκλήματος που τελούνται με στόχο ή μέσω των ηλεκτρονικών υπολογιστών και κυρίως του διαδικτύου αλλά ταυτόχρονα, πάλι μέσω της χρήσης αυτών ανακαλύπτονται και οι δράστες τους.[623]

Σχεδόν οποιοδήποτε έγκλημα που μπορεί να διαπραχτεί στον πραγματικό κόσμο μπορεί επίσης να διαπραχτεί στον εικονικό αλλά, αναμφίβολα, μερικά εγκλήματα έχουν «αναζωογονηθεί» μέσω του ηλεκτρονικού περιβάλλοντος. Αυτό έχει επιτρέψει στις υπάρχουσες μορφές παραβατικότητας να πραγματοποιηθούν σε ευρύτερη κλίμακα, αποτελεσματικότερα, γρηγορότερα, με μεγαλύτερη ευκολία απόκρυψης και συνακόλουθα με μεγαλύτερη δυσκολία ανίχνευσης.

8.3. Το εγκληματικό πρότυπο του ηλεκτρονικο-οικονομικού εγκλήματος από τη άποψη των «εγκληματικών ευκαιριών»

Οι Hamid Jahankhani και Ameer Al-Nemrat χρησιμοποίησαν τις θεωρίες των «εγκληματικών ευκαιριών» από την οπτική της περιβαλλοντικής εγκληματολογίας για την προσέγγιση της θυματοποίησης στο διαδίκτυο. [624]

Για το τμήμα της εργασίας τους που αφορά τη θεωρία των Brantingham για τις ευκαιρίες και τα κίνητρα των δραστών αναφέρουν ότι τα σημαντικότερα σημεία της για τη μελέτη του διαδικτυακού εγκλήματος είναι:

- Η φύση των κινήτρων ποικίλει μεταξύ των δραστών. Για τους χάκερ επισημαίνουν ότι αυτοί πιστεύουν πως το μοίρασμα των πληροφοριών δεν είναι κάτι κακό, ως εκ τούτου οι χάκερ θεωρούν ότι έχουν υποχρέωση να μοιραστούν τις πληροφορίες που βρίσκουν με τους

[622] Piquero Nicole & Benson Michael L. (2004)
[623] Χάιδου Ανθοζωή (2003), σ. 105.
[624] Jahankhani Hamid & Al-Nemrat Ameer (2011)

άλλους ανθρώπους και ότι πρέπει να διευκολύνουν την πρόσβαση των ανθρώπων όπου αυτό είναι δυνατό.[625]

- Το αρχικό βήμα του επίδοξου δράστη είναι να αναγνωρίσει τα ίχνη του πιθανού θύματος, το όνομα, τη διεύθυνση, τον τηλεφωνικό αριθμό του, τις IP του κλπ. αναζητώντας πληροφορίες σε διάφορους ιστότοπους, όπως το Google.
- Ο δράστης χρησιμοποιεί σημάδια για να εντοπίσει, ανάμεσα στον όγκο των πληροφοριών που αποκτά για το στόχο του, τα ενεργά συστήματα που είναι διαθέσιμα σε αυτόν μέσω του διαδικτύου.
- Ο δράστης διαμορφώνει ένα πρότυπο σκηνικό για τη διάπραξη του εγκλήματος με βάση την εμπειρία του, τα σημάδια και με βάση το οποίο αποφασίζει αν θα επιτεθεί και πότε. Κάποιες μορφές κυβερνοεπιθέσεων απαιτούν ιδιαίτερες τεχνικές γνώσεις από το δράστη, όπως το να ξεπεράσει το τείχος προστασίας, ενώ κάποιες άλλες όχι, όπως οι επιθέσεις μέσω των μέσων κοινωνικής δικτύωσης.
- Μετά την διαμόρφωση του αρχικού εγκληματικού προτύπου η συμπεριφορά του δράστη στο εξής αυτοενισχύεται.
- Ανάλογα με κάθε είδος στόχου διαμορφώνεται και διαφορετικό εγκληματικό πρότυπο.[626]

8.3.1. Η δόμηση του «κοινού τόπου»

Ένα από τα βασικά χαρακτηριστικά των οικονομικών εγκλημάτων του λευκού περιλαιμίου, όπως και των ηλεκτρονικών εγκλημάτων, είναι ότι τα δυο εμπλεκόμενα μέρη, δράστης και θύμα, μπορεί να βρίσκονται σε φυσική απόσταση μεταξύ τους και δεν απαιτείται η *άμεση επαφή* δράστη και θύματος, όπως συμβαίνει για τα παραδοσιακά εγκλήματα «δρόμου». Τα ηλεκτρονικο-οικονομικά εγκλήματα μπορούν να τελούνται από πολλούς δράστες και σε πολλά μέρη ταυτόχρονα, χωρίς να είναι απαραίτητο οι δράστες να έρχονται σε επαφή με τα θύματα ή να γνωρίζουν ακόμα και την ταυτότητα των θυμάτων τους.[627]

Ο Yar θεωρεί τον «κυβερνοχώρο ως ένα χωρο-χρονικά αποδιοργανωμένο και ασυνεχές περιβάλλον» και εξ αυτού δημιουργούνται προβλήματα κατά την εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων για τα εγκλήματα στον κυβερνοχώρο.[628]

Αντίθετα, άλλοι όπως ο Pratt, θεωρούν ότι το ζήτημα της φυσικής εγγύτητας του δράστη με το κατάλληλο θύμα εξουδετερώνεται στον κυβερνοχώρο και το ψηφιακό περιβάλλον παρέχει αμέτρητες εγκληματικές ευκαιρίες σε πιθανούς δράστες. Αυτό γιατί η φυσική επαφή του δράστη με το θύμα είναι αναγκαία αλλά όχι ικανή συνθήκη θυματοποίησης γιατί μπορούν να χρησιμοποιούνται ποικίλοι τρόποι προσέγγισης του στόχου από τον δράστη όπως μέσω έντυπων (εφημερίδες, ταχυδρομείο, διαφημίσεις) ή ψηφιακών μέσων π.χ. τηλεόραση, τηλέφωνο, διαδίκτυο.[629]

Ο Castells θεωρεί ότι ο κυβερνοχώρος «δημιουργεί ένα κοινό κοινωνικό περιβάλλον το οποίο επεκτείνει τον παραδοσιακό κόσμο και αντανακλά τις κοινωνικο-οικονομικές και πολιτιστικές του διαστάσεις». Τα διαφορετικά κοινωνικά και δημογραφικά χαρακτηριστικά των διαφορετικών χρηστών του διαδικτύου αντανακλώνται στα διαφορετικά ενδιαφέροντα,

[625] Βλ. Jahankhani Hamid & Al-Nemrat Ameer (2011) αναφορά στον Chance, 2005
[626] Jahankhani Hamid & Al-Nemrat Ameer (2011)
[627] Benson Michael L. & Madensen Tamara D. (2007), σ.615
[628] Yar Majid, M. (2005)
[629] Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010)

τις διαφορετικές επιλογές που κάνουν στις καθημερινές διαδικτυακές τους δραστηριότητες.[630]

Ο πιθανός δράστης συναντά και αλληλεπιδρά με τα υποψήφια θύματα από απόσταση μέσω κάποιου **δικτύου** συναλλαγών. Η έννοια του ***κοινού τόπου*** περιλαμβάνει όλους τους τρόπους, τα δίκτυα επικοινωνίας που επιτρέπουν την αλληλεπίδραση μεταξύ δράστη με κίνητρο και στόχου-θύματος και προσφέρουν έναν «κοινό χώρο» συνάντησης.[631] Εφόσον δράστες και θύματα αποτελούν μέρος του ίδιου δικτύου, η έννοια της συνύπαρξής τους στον ίδιο «χώρο» έχει δομηθεί. Ειδικότερα για την περίπτωση των ηλεκτρονικο-οικονομικών εγκλημάτων αυτά τελούνται μέσω υπολογιστών που είναι συνδεδεμένοι μεταξύ τους σε δίκτυα επιχειρήσεων ή στο διαδίκτυο προσφέροντας ευκαιρίες για κλοπή εμπιστευτικών δεδομένων, πληροφοριών, κεφαλαίων και άλλων ευαίσθητων αρχείων χωρίς τη φυσική διάρρηξη κάποιου χώρου. Τα δίκτυα, εκτός από την πρόσβαση στους πιθανούς στόχους, προσφέρουν στο δράστη κάποια μορφή απόκρυψης πράγμα που δεν συμβαίνει κατά την φυσική επαφή.[632]

Ο ψηφιακός εγκληματίας, όπως και αυτός του λευκού περιλαιμίου μπορούν να πλήξουν ταυτόχρονα πολλαπλά θύματα-στόχους εξ αποστάσεως χωρίς καν να γνωρίζουν την ταυτότητα των θυμάτων τους. Τα δίκτυα παρέχουν στο δράστη τον κατάλληλο «χώρο» αρκεί και το θύμα – στόχος να συμμετέχει στο ίδιο δίκτυο. Ευκαιρίες για εγκληματική δράση συνιστούν τα δίκτυα υπολογιστών επιχειρήσεων όπου περιέχονται αρχεία, φάκελοι, κεφάλαια, πολύτιμες πληροφορίες τα οποία μπορούν να αποτελέσουν στόχο με απομακρυσμένη πρόσβαση παρέχοντας στο δράστη και την απαραίτητη μυστικότητα και κάλυψη.[633]

Έτσι ο κυβερνοχώρος και άλλα ψηφιακά δίκτυα ή μέσα με τα οποία αλληλεπιδρούν οι πιθανοί δράστες με τους πιθανούς στόχους συνιστούν την έννοια του **χώρου** κατά τη δόμηση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος.

8.3.2. Οι «οδοί – μονοπάτια» του ηλεκτρονικο-οικονομικού εγκλήματος και η «καταλληλότητα» του στόχου - θύματος

Οι νέες τεχνολογίες, που έχουν γίνει προσφιλή εργαλεία για τους ηλεκτρονικούς εγκληματίες και αποτελούν τα **μονοπάτια** τα οποία χρησιμοποιούν για να αποκτήσουν την απαραίτητη εγγύτητα στο στόχο, κατά τη δόμηση του προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος, αφορούν:

- Ευρυζωνικές συνδέσεις. Σε σχέση με τις συνδέσεις μέσω τηλεφώνου (dial up) προσφέρουν μεγαλύτερη δυνατότητα για εισβολή στο δίκτυο εφόσον ο υπολογιστής παραμένει συνεχώς συνδεδεμένος στο (εξωτερικό) δίκτυο και η IP (Internet Protocol address) είναι συνήθως στατική.
- Ασύρματα δίκτυα. Προσφέρουν στους πιθανούς εισβολείς τη δυνατότητα να εισέλθουν στο δίκτυο του χρήστη απομακρυσμένα, χωρίς να απαιτείται η φυσική σύνδεση μέσω κάποιου καλωδίου.
- Φορητά συστήματα υπολογιστών, όπως λάπτοπ, τάμπλετ, «έξυπνα τηλέφωνα» (smart-phones) που προσφέρουν απομακρυσμένη πρόσβαση. Η φορητότητα και

[630] Jahankhani Hamid & Al-Nemrat Ameer (2011), σσ. 181-197

[631] Όπως πρότειναν οι Eck και Clarke, βλ. Benson, Michael, Tamara D. Madensen, & John E. Eck (2009), σ. 179

[632] Benson Michael L. & Madensen Tamara D. (2007), σσ. 615-616

[633] Benson Michael L. & Madensen Tamara D. (2007), ό.π.

ματαφερσιμότητα δίνει την δυνατότητα πρόσβασης στο δίκτυο από παντού, όχι μόνο για τον νόμιμο χρήστη αλλά και τον παράνομο.

- Διαδικτυακές εφαρμογές, όπως Java, ActiveX, Flash κλπ. που χρησιμοποιούν ενεργό περιεχόμενο (active content) και οι οποίες παρέχουν οπτικά εφέ, κίνηση, φωτογραφίες, βίντεο στις ιστοσελίδες που επισκέπτεται ο χρήστης αλλά και δυνατότητα στους εγκληματίες να αναπτύξουν κακόβουλους κώδικες μέσω αυτών.
- Προγράμματα αποστολής ηλεκτρονικών μηνυμάτων και προγράμματα άμεσων μηνυμάτων που υποστηρίζουν πρωτόκολλα HTML και script. Εκτός από τους κινδύνους εκτέλεσης προγραμμάτων script κίνδυνοι υπάρχουν και από τα περιεχόμενα των συνημμένων που μπορεί να περιλαμβάνουν κακόβουλο κώδικα.
- Ηλεκτρονικό εμπόριο και e-banking. Οι διαδικτυακές συναλλαγές, εμπορικές ή τραπεζικές, συναλλαγές με πιστωτικές κάρτες αφορούν κυκλοφορία χρήματος και ως εκ τούτου προσελκύουν το ενδιαφέρον των δραστών με κίνητρο.
- Καινούργια λειτουργικά συστήματα, όπως νέες εκδόσεις των Windows που συνήθως περιέχουν κενά ασφάλειας, ατέλειες και σφάλματα (bugs) όπως και μικρή εξοικείωση των χρηστών σχετικά με τις νέες δυνατότητες τους .
- Η τυποποίηση και ομοιομορφία διευκολύνει τους εγκληματίες, όπως όταν όλοι οι χρήστες χρησιμοποιούν το ίδιο λειτουργικό σύστημα, τον ίδιο περιηγητή ιστοσελίδων (internet explorer), το ίδιο πρόγραμμα ηλεκτρονικής αλληλογραφίας, κλπ. γιατί απλά δεν χρειάζεται να μάθουν τον τρόπο λειτουργίας και τις πιθανές ευπάθειες πολλών διαφορετικών προγραμμάτων. [634]

Σημαντικά «μονοπάτια» που χρησιμοποιούν οι διαδικτυακοί εγκληματίες, ιδιαίτερα για τη διάπραξη απάτης, επίσης αποτελούν και οι ηλεκτρονικές πλατφόρμες και εφαρμογές που έχουν σχέση με τα **κινητά τηλέφωνα** νέας τεχνολογίας (τα λεγόμενα smartphones), οι υπηρεσίες cloud (νέφους) και τα μέσα κοινωνικής δικτύωσης. Η χρήση των οδών αυτών προτιμάται από τους πιθανούς δράστες για να «συναντήσουν» ευάλωτους στόχους επειδή συχνά παρουσιάζεται έλλειψη ικανού ελέγχου και ειδικότερα επαρκών μεθόδων ταυτοποίησης του χρήστη τέτοιων υπηρεσιών μέσω κινητού τηλεφώνου σε συνδυασμό με επίδειξη γενικότερα ριψοκίνδυνης διαδικτυακής συμπεριφοράς.

Για το 2013, όπως αναφέρει η Norton στην ετήσια έκθεσή της, το ένα τρίτο των χρηστών κινητής τηλεφωνίας έχουν πέσει θύματα, οι μισοί δεν λαμβάνουν κάποιο βασικό μέτρο προστασίας, μόνο το 26% των χρηστών κινητής τηλεφωνίας έχει εγκαταστήσει κάποιο πρόγραμμα προστασίας, ενώ το 57% δεν γνωρίζει καν την ύπαρξη τέτοιων μέτρων. Τα παραπάνω στοιχεία δικαιολογούν την ελκυστικότητα της κινητής τηλεφωνίας ως κατάλληλο στόχο των διαδικτυακών απατεώνων.[635]

8.3.3. Η δόμηση της «εγγύτητας»

Βασικό στοιχείο στη διαμόρφωση της εγκληματικής ευκαιρίας και τη δόμηση του εγκληματικού προτύπου του ψηφιακού-οικονομικού εγκλήματος αποτελεί, η εγγύτητα, η έκθεση του στόχου σε πιθανούς δράστες, η ύπαρξη ενός κοινού τόπου όπου ο δράστης με κίνητρο συναντά ελκυστικούς και κατάλληλους στόχους. Την εγγύτητα αυτή προσφέρει η καθημερινή διαδικτυακή συμπεριφορά των χρηστών επειδή υπάρχουν κάποιες

[634] Shinder Debra Littlejohn (2002), σ.63
[635] Όπως αναφέρει η Norton στην έκθεσή της για το 2013, βλ. Paganini Pierluigi (2014)

συγκεκριμένες συμπεριφορές που, όπως στον φυσικό κόσμο έτσι και στον κυβερνοχώρο, εκθέτουν τους χρήστες σε κίνδυνο θυματοποίησης περισσότερο από κάποιες άλλες.[636]

Τα συστήματα των ανυποψίαστων χρηστών παρουσιάζονται ευάλωτα σε επιθέσεις δραστών με κίνητρο κυρίως λόγω ριψοκίνδυνης διαδικτυακής συμπεριφοράς και επιβλαβών συνηθειών (δραστηριοτήτων ρουτίνας) επιβεβαιώνοντας την προσέγγιση των καθημερινών δραστηριοτήτων.

Ο στόχος καθίσταται κατάλληλος και αναγνωρίσιμος και λόγω της φυσικής και χρονικής εγγύτητας του θύματος με τον δράστη[637]. Η **«εγγύτητα»**, στην περίπτωση των παραδοσιακών εγκλημάτων αφορά την φυσική εγγύτητα (πρόσβαση) του πιθανού δράστη στους στόχους του στον γεωγραφικό χώρο, ενώ στον ψηφιακό η «εγγύτητα» επιτυγχάνεται με την αλληλεπίδραση των χρηστών μέσω της χρήσης της σύγχρονης τεχνολογίας, των κατάλληλων ψηφιακών δικτύων και του κυβερνοχώρου.[638] Η ειδοποιός διαφορά στην περίπτωση του ψηφιακού εγκλήματος είναι το γεγονός ότι το υποψήφιο θύμα βρίσκεται σε φυσική εγγύτητα όχι με τον δράστη αυτοπροσώπως αλλά με τα εργαλεία και τα μέσα που χρησιμοποιεί ο δράστης.

Από την πλευρά του δράστη λοιπόν η εγγύτητα με το στόχο του επιτυγχάνεται με ψηφιακά εργαλεία όπως κακόβουλα προγράμματα, ιοί κλπ. με οποία ο δράστης (ιδιαίτερα ο χάκερ) μπορεί να αποκτήσει πρόσβαση στο στόχο του, που μπορεί να είναι ένα μεγάλο φάσμα υπολογιστικών συστημάτων (υπολογιστές, λογαριασμοί, προσωπικά δεδομένα κλπ.) για να τα βλάψει ή να κλέψει δεδομένα εξ αποστάσεως[639]. Η πρόσβαση, η εγγύτητα αυτή δεν είναι απαραίτητο να αποτελεί ένα χρονικά μεμονωμένο περιστατικό αλλά να έχει εξακολουθητικό χρονικά χαρακτήρα επειδή το κακόβουλο λογισμό μπορεί να είναι για μεγάλο διάστημα εγκατεστημένο στον υπολογιστή-στόχο.[640]

Από την άλλη πλευρά ιδιαίτερα καθοριστικός είναι και ο ρόλος των ίδιων των θυμάτων γιατί με την καθημερινή διαδικτυακή συμπεριφορά τους μπορεί να συμβάλλουν στη θυματοποίησή τους φέροντας τους σε ψηφιακή εγγύτητα με τους πιθανούς δράστες.[641]

Όπως στο πραγματικό περιβάλλον συγκεκριμένες καθημερινές δραστηριότητες συνδέονται με κίνδυνο έκθεσης και θυματοποίησης των ατόμων[642], αντίστοιχα στο ψηφιακό περιβάλλον η **«έκθεση»** των θυμάτων στους πιθανούς δράστες με κίνητρο εκφράζεται με την επίδειξη ριψοκίνδυνης διαδικτυακής συμπεριφοράς και δραστηριότητας και συνδέεται με την χρονική διάρκεια αυτών των δραστηριοτήτων. [643]

Ιδιαίτερα η εγγύτητα και η έκθεση των πιθανών θυμάτων σε δράστες με κίνητρο στο ψηφιακό περιβάλλον εκφράζεται, σύμφωνα με τις προσεγγίσεις των «εγκληματικών ευκαιριών», με ορισμένες καθημερινές ψηφιακές δραστηριότητες που τα καθιστούν κατάλληλους στόχους. Τέτοιες δραστηριότητες αποτελούν, η χρήση του e-banking, οι διαδικτυακές αγορές, ο χρόνος που αφιερώνουν οι χρήστες στο διαδίκτυο χωρίς λήψη των κατάλληλων μέσων προστασίας που θα λειτουργούν ως «ικανοί φύλακες».[644] Ακόμα, η

[636] Bossler Adam, & Holt Thomas (2009), ό.π.
[637] Holt Thomas J. & Bossler Adam (2013)
[638] Reyns, Brandford. W., Henson Billy. & Fisher Bonnie. S. (2011)
[639] Holt Thomas J. & Bossler Adam (2013)
[640] Βλ. αναφορά στον Taylor et.al. 2006 στο Bossler Adam, & Holt Thomas (2009)
[641] Holt Thomas J. & Bossler Adam (2013)
[642] Mustaine Elizabeth E. & Tewksbury Richard (1998)
[643] Holt Thomas J. & Bossler Adam (2013)
[644] βλ. και παραπ. υποσημειώσεις για Holt Thomas J. & Bossler Adam (2009), Pratt et. Al. (2010), Choi (2008) κλπ.

συμμετοχή των ίδιων των χρηστών σε παράνομες ή ριψοκίνδυνες δραστηριότητες, το κατέβασμα πειρατικού υλικού, όπως λογισμικό, ταινίες, μουσικά ή άλλα αρχεία που παραβιάζουν τους νόμους περί πνευματικής ιδιοκτησίας, η παρακολούθηση πορνογραφικού υλικού διαδικτυακά, η παράνομη χρήση της σύνδεσης ίντερνετ κάποιου άλλου, αυξάνουν την πιθανότητα προσβολής από κάποιο βλαβερό ιό ή πρόγραμμα με το οποίο χάκερ αποκτούν πρόσβαση ή έλεγχο του υπολογιστή του θύματος.[645]

Ριψοκίνδυνη διαδικτυακή συμπεριφορά των χρηστών αποτελεί ακόμα η χρήση των κινητών τηλεφώνων εντός του χώρου εργασίας (σε ποσοστό 49%) επηρεάζοντας την ασφάλεια όλων των δικτύων των επιχειρήσεων οι οποίες παραδέχονται ότι σε ποσοστό 36% δεν διαθέτουν κάποιο τρόπο αντιμετώπισης του ζητήματος.

Στο χώρο των μέσων κοινωνικής δικτύωσης, ριψοκίνδυνη συμπεριφορά συνιστούν η μη αποσύνδεση των χρηστών από το δίκτυο (ποσοστό 39%), η αποκάλυψη των εμπιστευτικών δεδομένων του χρήστη σε τρίτους (25%), η αποδοχή αιτημάτων από αγνώστους (33%).[646]

Όσον αφορά την χρήση υπηρεσιών cloud, το 24% των χρηστών διαθέτει κοινό λογαριασμό για προσωπικές και για επαγγελματικές δραστηριότητες, το 18% μοιράζεται τα προσωπικά του αρχεία με φίλους. Οι υπηρεσίες cloud καθίστανται με τον τρόπο αυτό ελκυστικός στόχος για τους χάκερ επειδή συγκεντρώνουν ένα σύνολο πολλαπλών υπηρεσιών αρχείου σε ένα μέρος.[647]

Ακόμα και η απλή αλληλεπίδραση με φίλους ή συνεργάτες που επιδεικνύουν παράνομη ή γενικά επικίνδυνη διαδικτυακή συμπεριφορά συνιστά έκθεση σε κίνδυνο και για τους υπόλοιπους.[648]

Όπως είδαμε παραπάνω, σύμφωνα με την πρόσφατη[649] έρευνα του Παντείου Πανεπιστημίου για την θυματοποίηση και τον φόβο του εγκλήματος στο διαδίκτυο βρέθηκε ότι όλοι σχεδόν οι χρήστες που έχουν πέσει θύματα έκαναν χρήση του διαδικτύου καθημερινά.

Ακόμα, σύμφωνα με την ίδια έρευνα του Παντείου, η πλειονότητα των συμμετεχόντων στο δείγμα (25%) δήλωσε ότι έχει δεχτεί απειλή, παρενόχληση ή άλλη μορφή εκβιασμού στο διαδίκτυο, ενώ το 15,2% έχει υποστεί κλοπή προσωπικών του δεδομένων.[650]

Συνοπτικά, ***ριψοκίνδυνη διαδικτυακή συμπεριφορά*** που **εκθέτει** τους χρήστες, τους καθιστά ευάλωτους και κατάλληλους στόχους φέρνοντάς τους σε εγγύτητα με πιθανούς δράστες μπορεί να συνιστούν διάφορες καθημερινές συνήθειες στο διαδίκτυο όπως[651]:

- συμμετοχή των χρηστών σε «δωμάτια» επικοινωνίας (chat rooms) με άλλους χρήστες,
- αποδοχή αγνώστων ως «φίλους» στα μέσα κοινωνικής δικτύωσης,
- συχνή πραγματοποίηση διαδικτυακών συναλλαγών για αγορά προϊόντων μέσω δημοπρασιών ή ηλεκτρονικών καταστημάτων,
- συχνή χρήση του e-banking,
- εμπλοκή του ίδιου του θύματος σε παράνομες διαδικτυακές δραστηριότητες όπως χρήση ευρυζωνικής σύνδεσης για κατέβασμα δωρεάν ή πειρατικού λογισμικού ή αρχείων, συμμετοχή σε δραστηριότητες hacking, επίσκεψη άγνωστων ιστοσελίδων με

[645] Holt Thomas J. & Bossler Adam (2013)
[646] Όπως αναφέρει η Norton στην έκθεσή της για το 2013, βλ. Paganini Pierluigi (2014)
[647] Paganini Pierluigi, ό.π.
[648] Holt Thomas J. & Bossler Adam (2008)
[649] Βλ. και παραπάνω
[650] Zarafonitou Christina & Koumentaki Evangelia (2014)
[651] Choi Kyung-shick (2008) και Bossler Adam, & Holt, Thomas (2009)

αμφιλεγόμενο περιεχόμενο και θέαση απαγορευμένου υλικού όπως πορνογραφικό υλικό.[652]

- κλικάρισμα σε εικόνες,
- κοινοποίηση προσωπικών πληροφοριών και δεδομένων,
- άνοιγμα ύποπτων emails (spam) κλπ.[653]

Οι παραπάνω συμπεριφορές και δραστηριότητες συνιστούν την καθημερινή ρουτίνα πολλών χρηστών του διαδικτύου οι οποίες όμως όσο συχνότερα επιδεικνύονται τόσο περισσότερο τους εκθέτουν και τους φέρνουν σε «εγγύτητα» με δράστες που έχουν κίνητρο να τους θυματοποιήσουν.[654]

8.3.4. Η δόμηση της «ελκυστικότητας» του στόχου

Για το θέμα της **ελκυστικότητας ή καταλληλότητας** του στόχου για τους πιθανούς δράστες οι Cohen και Felson, χρησιμοποίησαν τα αρχικά VIVA (value, inertia, visibility, accessibility)[655] για να περιγράψουν ως κατάλληλο τον στόχο-θύμα που διαθέτει μεγαλύτερη «αξία», «φορητότητα» (ευκολία μεταφοράς), «θεατότητα» και «προσβασιμότητα» σε σχέση με άλλους. Στην περίπτωση των ηλεκτρονικών εγκλημάτων κάποιες περιστάσεις ή πληροφορίες σχετικά με το στόχο-θύμα το καθιστούν πιο επιθυμητό σε πιθανούς δράστες. Τέτοια στοιχεία μπορεί να αποτελούν το πλήρες όνομα του θύματος, διευθύνσεις του ηλεκτρονικού του ταχυδρομείου, προσωπικές φωτογραφίες, βίντεο, πληροφορίες για ενδιαφέροντα και δραστηριότητες στο χώρο και το χρόνο που δημοσιοποιούνται σε ιστοσελίδες (κοινωνικής δικτύωσης κυρίως) και άλλα προσωπικά στοιχεία που προσελκύουν το ενδιαφέρον των δραστών. [656]

Άλλοι ελκυστικοί, από άποψη φορητότητας και προσβασιμότητας, στόχοι μπορεί να είναι διάφορα αρχεία μουσικής, εικόνων, ταινιών και προγράμματα που μπορεί κανείς εύκολα και «δωρεάν» να κατεβάσει από το διαδίκτυο.

Από την άποψη των δημογραφικών χαρακτηριστικών της ελκυστικότητας του στόχου οι έρευνες διαπίστωσαν ότι το γυναικείο φύλο είναι σε μεγαλύτερο κίνδυνο θυματοποίησης από ψηφιακές επιθέσεις, γεγονός που μπορεί να οφείλεται στο ότι οι άνδρες διαθέτουν πιο πολλές δεξιότητες για τη χρήση των ψηφιακών τεχνολογιών[657]. Όσον αφορά το επίπεδο της απασχόλησης όσοι διαθέτουν πλήρη απασχόληση είναι πιο πιθανοί στόχοι επιθέσεων.

Όπως αναφέρθηκε σε άλλο σημείο, σύμφωνα με την έρευνα του Παντείου Πανεπιστημίου για την θυματοποίηση και τον φόβο του εγκλήματος στο διαδίκτυο[658] βρέθηκε ότι η πλειονότητα των θυμάτων έχει θυματοποιηθεί επανειλημμένα (πάνω από 5 φορές) πράγμα που επιβεβαιώνει την άποψη ότι οι δράστες χρησιμοποιούν «οδούς» και προτιμούν στόχους που ήδη έχουν δοκιμάσει και γνωρίζουν.[659]

---

[652] Holt Thomas & Bossler Adam (Dec.(2008)

[653] Βλ. παραπ. για την εφαρμογή των θεωριών εγκληματικών ευκαιριών στην ανάλυση των ηλεκτρονικο-οικονομικών εγκλημάτων όπου γίνεται αναφορά σε Holtfreter, Reisig et.al.(2008), Choi Kyung-shick (2008) και Kigerl Alex (2012).

[654] Holtfreter Kristy, Reisig Michael D., & Pratt Travis C. (2008) και Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010)

[655] Cohen, Lawrence & Felson Marcus (1979), σ. 590

[656] Reyns, Brandford. W., Henson Billy. & Fisher Bonnie. S. (2011)

[657] Bossler Adam, & Holt Thomas J. (2009)

[658] Zarafonitou Christina & Koumentaki Evangelia (2014)

[659] Βλ. παραπ. Θεωρία εγκληματικών προτύπων και Farrell Graham, Clark Ken, Ellingworth Dan, Pease Ken (2005)

8.3.5. Η δόμηση της έννοιας των «ικανών φυλάκων»

Αν και δεν προκύπτει η πρωτοκαθεδρία κάποιου στοιχείου έναντι των υπολοίπων, το σημαντικότερο ίσως από τα τρία παραπάνω στοιχεία που συντελούν στη διαμόρφωση της εγκληματικής ευκαιρίας σύμφωνα με τη θεωρία L-RAT αποτελεί η **«έλλειψη ικανής φύλαξης».** Όπως σημειώνουν οι Grabosky και Smith πολλά από τα κυβερνοεγκλήματα λαμβάνουν χώρα λόγω της απουσίας ικανής φυσικής φύλαξης.[660]

Η έλλειψη «ικανών φυλάκων» όσον αφορά το ψηφιακό περιβάλλον εμφανίζεται με την μορφή:

- έλλειψης μέτρων ασφάλειας του υπολογιστή από τους κινδύνους προσβολής,
- έλλειψης ενημέρωσης των χρηστών για τους κινδύνους αυτούς και για την ανάγκη λήψης μέτρων ασφάλειας και άμυνας έναντι αυτών, [661]
- έλλειψης εξειδικευμένων γνώσεων και δεξιοτήτων σχετικά με την χρήση των ψηφιακών τεχνολογιών. [662]
- αδυναμίας επιβολής του νόμου από πλευράς διωκτικών αρχών,
- απουσίας «διαχειριστών χώρου» όπως γονεϊκού ή σχολικού ελέγχου στις διαδικτυακές δραστηριότητες των παιδιών ή επιτηρητών, ελεγκτών, μάνατζερ κλπ. σε χώρους εργασίας επιχειρήσεων.
- ευάλωτων συστημάτων υπολογιστών και δικτύων και
- έλλειψης προθυμίας καταγγελίας των εγκλημάτων στις αρχές.

Περισσότερα για την ύπαρξη των ικανών φυλάκων στην περίπτωση των ψηφιακών οικονομικών εγκλημάτων εξηγούνται παρακάτω στο ζήτημα της αντιμετώπισης τους.

8.3.6. Ο ρόλος των κινήτρων για τη διάπραξη ηλεκτρονικο – οικονομικού εγκλήματος

Σύμφωνα με ειδικούς που χρησιμοποιούν στρατηγικές πρόληψης του εγκλήματος στο πλαίσιο των προσεγγίσεων των «εγκληματικών ευκαιριών», για να τελεστεί ένα έγκλημα απαιτείται η συνέργια τριών παραγόντων.

Το πρώτο στοιχείο είναι το **κίνητρο**, ο λόγος για τον οποίο κάποιος τελεί το ηλεκτρονικό έγκλημα, παραβίαση κλπ. Το δεύτερο είναι τα διαθέσιμα ***μέσα***, τα εργαλεία για την τέλεση και το τρίτο είναι η κατάλληλη ***ευκαιρία*** η οποία συνίσταται στην εύρεση του ελκυστικού στόχου που διαθέτει κάποιο κενό ασφαλείας, εγγύτητα στον δράστη, αξία, ευκολία απόκτησης, ματαφερσιμότητα.[663]

Παρά το γεγονός ότι τα κίνητρα του δράστη δεν ήταν αρχικά στο επίκεντρο του ενδιαφέροντος των προσεγγίσεων για τη δόμηση των «εγκληματικών ευκαιριών», επειδή εστιάζουν στο πώς και όχι στο γιατί[664], θεωρούνται από το σύνολο τους ως σημαντικά, ιδιαίτερα με την προσχώρηση σε αυτές και της προσέγγισης της «ορθολογικής επιλογής», για το ποιες συμπεριφορές και ποιοι στόχοι κρίνονται από τον πιθανό δράστη ως κατάλληλοι ή επιθυμητοί και ποιοι όχι παίζοντας ρόλο στη δόμηση των προτύπων των εγκληματικών ευκαιριών.

[660] Bossler Adam, & Holt Thomas (2009)
[661] Jahankhani Hamid & Al-Nemrat Ameer (2011)
[662] Holt Thomas J. & Bossler Adam (2013)
[663] Shinder Debra Littlejohn (2002), σσ., 353-354
[664] Όπως είδαμε παραπάνω και για την θεωρία των καθημερινών δραστηριοτήτων αρχικός στόχος των θεωριών αυτών δεν ήταν να μελετήσουν τα κίνητρα των δραστών, τα οποία παίρνουν ως δεδομένα, αλλά το πώς οι κοινωνικές δομές μετατρέπουν τις εγκληματικές ροπές σε δράση.

Η θεωρία των καθημερινών δραστηριοτήτων των Felson και Cohen, αναγνώρισε τη σημασία των κινήτρων του δράστη περιλαμβάνοντάς τα στο πρώτο από τα αναγκαία στοιχεία που δομούν την εγκληματική ευκαιρία: τον «δράστη με δυνατότητα, θέληση και κίνητρο να διαπράξει το έγκλημα» (motivated offender).[665]

Οι θεωρητικοί της «Ορθολογικής επιλογής», εξέτασαν την εγκληματική δράση όπως κάθε κοινωνική δράση, δηλαδή ως «υπολογιστική» που προκαλείται από ορθολογικά κίνητρα. Ο δράστης δηλαδή αναμένει κάποια ανταμοιβή ή όφελος ως κίνητρο στην ευκαιρία διάπραξης κάποιας εγκληματικής δραστηριότητας. Ως προς την ορθολογικότητα των κινήτρων του λοιπόν ο δράστης δεν διαφοροποιείται από τον μη δράστη όμως, λόγω της υποκειμενικής διάστασής του, το κίνητρο είναι διαφορετικό για τον κάθε δράστη.[666]

Η προσέγγιση της ορθολογικής επιλογής πιστεύει, όπως είδαμε παραπάνω, ότι ο δράστης δρα σκόπιμα με κίνητρο να αποκομίσει κάποιο όφελος, οικονομικό ή άλλο όπως κύρος, διασκέδαση, σεξουαλική ικανοποίηση, κυριαρχία. [667]

Η εξέταση των κινήτρων του δράστη είναι σημαντική από διάφορες απόψεις. Πρώτα γιατί σε πολλά, κυρίως αγγλοσαξονικά, συστήματα απονομής δικαιοσύνης το κίνητρο αποτελεί ένα από τα τρία στοιχεία (εκτός από τα μέσα και την ευκαιρία[668]) που απαιτούνται για τη στοιχειοθέτηση της ενοχής κάποιου πιθανού δράστη σε δίκη. Δεύτερο επειδή είναι καίριας σημασίας για τον προσδιορισμό του προφίλ ενός δράστη κατά το στάδιο των ερευνών για την επισήμανση του από τις διωκτικές αρχές. [669]

8.3.7. Η «καταλληλότητα των εγκληματικών ευκαιριών» για τη διάπραξη ηλεκτρονικο – οικονομικού εγκλήματος

Σημαντικό στοιχείο στη διαμόρφωση του εγκληματικού προτύπου για το παραδοσιακό έγκλημα του λευκού περιλαιμίου αποτελεί η ύπαρξη της εγκληματικής ευκαιρίας. Η κατάχρηση, για παράδειγμα δεν θα μπορούσε να τελεστεί χωρίς την απαραίτητη πρόσβαση του υπαλλήλου – δράστη στο λογαριασμό ή τα κεφάλαια του πιθανού θύματος. Η χειραγώγηση μετοχών, η συμμετοχή σε καρτέλ χειραγώγησης τιμών των προϊόντων μπορεί να γίνει κυρίως από άτομα που έχουν τη θέση του χρηματιστή, του υψηλόβαθμου στελέχους κλπ. δηλαδή από αυτά που κατέχουν την κατάλληλη θέση. Για την ύπαρξη λοιπόν της εγκληματικής ευκαιρίας παραδοσιακά ήταν απαραίτητο κάποιο επαγγελματικό status.

Η ευρύτατη διάδοση του διαδικτύου επιτρέπει πλέον την πρόσβαση στις εγκληματικές ευκαιρίες που αυτό προσφέρει όχι μόνο στα προνομιούχα κοινωνικά στρώματα αλλά και στις ευρύτερες μάζες πληθυσμού (εκδημοκρατισμός του διαδικτύου).

Οι Grabosky και Walkley θεωρούν την εξάπλωση της πληροφορικής τεχνολογίας ως βασικό παράγοντα της αύξησης των δραστών με κίνητρο. Η ανάπτυξη των διαδικτυακών συναλλαγών, του ηλεκτρονικού εμπορίου, των ηλεκτρονικών δημοπρασιών, των χρηματιστηριακών συναλλαγών, των υπηρεσιών διαδικτυακής αποθήκευσης αρχείων και δεδομένων (τύπου cloud) έχουν δημιουργήσει ελκυστικούς στόχους και εγκληματικές ευκαιρίες σε δράστες με κίνητρο.

---

[665] Βλ. Cohen, Lawrence και Felson, Marcus (1979)

[666] Βλ. παραπάνω για θεωρία ορθολογικής δραστηριότητας ή επιλογής.

[667] Jahankhani Hamid & Al-Nemrat Ameer (2011), σσ. 188-189

[668] «να βρίσκεται στο κατάλληλο μέρος την κατάλληλη στιγμή».

[669] Shinder, Debra Littlejohn (2002), σ.113

Από την άλλη πλευρά η έλλειψη ικανών φυλάκων - και ο ρόλος της στη δημιουργία των εγκληματικών ευκαιριών του ηλεκτρονικο-οικονομικού εγκλήματος - παρουσιάζεται και στον παγκόσμιο ψηφιακό ιστό, όπως και στο παραδοσιακό έγκλημα του λευκού περιλαιμίου. Η έλλειψη «ικανών φυλάκων» όσον αφορά τον χώρο του διαδικτύου εμφανίζεται με την μορφή αδυναμίας επιβολής του νόμου από πλευράς διωκτικών αρχών, έλλειψη ενημέρωσης των χρηστών για την ανάγκη λήψης μέτρων ασφάλειας και άμυνας έναντι των διαδικτυακών κινδύνων, ευάλωτα συστήματα υπολογιστών και δικτύων όπως και έλλειψη προθυμίας καταγγελίας των εγκλημάτων στις αρχές. [670]

Οι Scraton και South αναγνωρίζουν την κοινωνική και επαγγελματική θέση ως διαφορετικούς τύπους **ευκαιριών** που μπορεί να προσφέρονται για τη διάπραξη αδικημάτων. Κάνουν συσχέτιση των εγκλημάτων που διαπράττονται από εργαζόμενους με χαμηλές αμοιβές και των πιεστικών εργασιακών συνθηκών. Ισχυρίζονται μάλιστα ότι οι εργαζόμενοι στα χαμηλότερα κλιμάκια της επιχείρησης υφίστανται μεγαλύτερο έλεγχο και παρακολούθηση και όταν διαπράττουν αδικήματα αυτά γίνονται λιγότερο ανεκτά από τα αντίστοιχα των υψηλότερων στελεχών.[671]

Η Susan Shapiro αποδίδει τη διάπραξη εγκληματικών πράξεων στη διαφορετική κατανομή εμπιστοσύνης μεταξύ των υπαλλήλων. Οι υπάλληλοι που πιθανά απολαμβάνουν μεγαλύτερης εμπιστοσύνης από την επιχείρηση, έχουν περισσότερες ευκαιρίες για να καταχρώνται αυτή την εμπιστοσύνη.[672]

Η Shapiro επίσης διέκρινε διάφορες τεχνικές που χρησιμοποιούν οι δράστες για να αποκτήσουν και να εκμεταλλευτούν την εμπιστοσύνη των θυμάτων τους κατά την διαμόρφωση της εγκληματικής τους ευκαιρίας. Τέτοιες τεχνικές περιλαμβάνουν την παραπληροφόρηση σχετικά με τα αληθινά κίνητρα της χορήγησης κεφαλαίων σε αναπτυσσόμενες χώρες, χάλκευση ερευνητικών δεδομένων, παραποίηση των αποτελεσμάτων ιατρικών εξετάσεων και ερευνών από φαρμακευτικές εταιρείες κλπ. [673]

Παρόμοιες τεχνικές κατάχρησης εμπιστοσύνης σύμφωνα με τους Grabosky και Walkley εφαρμόζονται και στον ψηφιακό χώρο. Η διαφορά είναι ότι ενώ στον πραγματικό κόσμο η εμπιστοσύνη βασίζεται στην φυσική επαφή δράστη και θύματος, στον ψηφιακό αυτό πραγματοποιείται μέσω των διαδικασιών επικοινωνίας.

Έτσι τα στοιχεία που χαρακτηρίζουν την διαμόρφωση του μοτίβου εμπιστοσύνης στον ψηφιακό χώρο είναι η **απουσία φυσικής επικοινωνίας** και αλληλεπίδρασης, με εξ αποστάσεως επικοινωνία και η ανωνυμία. Για παράδειγμα οι phishers χρησιμοποιούν το όνομα γνωστών και καταξιωμένων εταιρειών για να προσεγγίσουν και να αποκτήσουν την εμπιστοσύνη θυμάτων προκειμένου να τους αποσπάσουν εμπιστευτικές πληροφορίες σχετικά με τους τραπεζικούς λογαριασμούς τους. Η οικοδόμηση εμπιστοσύνης γίνεται μέσω email, συμμετοχής σε δωμάτια συνομιλίας (chat rooms), αποστολής ενημερωτικών φυλλαδίων κλπ.

Η εξαπάτηση και παραπλάνηση των θυμάτων σχετικά με την πραγματική ταυτότητα του δράστη και των προθέσεών του στηρίζεται σε μεγάλο βαθμό και στην **ανωνυμία** που παρέχει το ψηφιακό περιβάλλον. Η ανωνυμία στον κυβερνοχώρο επιτρέπει στους ψηφιακούς δράστες την δυνατότητα να παρέχουν παραπλανητικά στοιχεία για την ταυτότητά τους, τη φύση της συναλλαγής ή τις αληθινές προθέσεις τους, προκειμένου να πείσουν τα υποψήφια θύματα

[670] Grabosky Peter & Walkley Sascha (2007), σσ. 358-375
[671] Backhouse James & Gurpreet Dhillon (1995)
[672] Shapiro Susan (1990)
[673] Shapiro Susan (1990)

τους, όπως παιδιά για να τους συναντήσουν, αγοραστές προϊόντων μέσω διαδικτυακών δημοπρασιών, επενδυτές μετοχών, κάτοχους τραπεζικών λογαριασμών, άτομα για να παρενοχλήσουν, να εκβιάσουν κλπ. [674]

Η κατάχρηση της εμπιστοσύνης του θύματος από τον δράστη κατέχει κεντρική σημασία στη διαμόρφωση του εγκληματικού προτύπου και τη δημιουργία της εγκληματικής ευκαιρίας για τον ψηφιακό δράστη όπως και για τον παραδοσιακό.

Ο Coleman ασχολήθηκε, όπως είδαμε παραπάνω, με την εξήγηση της εγκληματικής συμπεριφοράς του λευκού περιλαιμίου ως έναν σύνθετο συνδυασμό ***κινήτρων*** *και* ***ευκαιριών***. Εκτός από τα κίνητρα θα πρέπει να υπάρχει και η ανάλογη ευκαιρία, χωρίς αυτήν δεν μπορεί να υπάρξει έγκλημα ανεξάρτητα από τη δύναμη που μπορεί να ασκεί το κίνητρο στο άτομο. Κανένα κίνητρο δεν είναι αρκετό για να εξηγήσει μια συμπεριφορά παρά μόνο σε συνδυασμό με τη μελέτη των ευκαιριών που είναι διαθέσιμες σε άτομα που κατέχουν θέσεις ισχύος. Η δομή του βιομηχανικού καπιταλισμού και η φύση του ανταγωνισμού των επιχειρήσεων επιτρέπουν στα στελέχη τους τη δικαιολόγηση και εκλογίκευση των συμπεριφορών που είναι δύσκολο να αντισταθούν στα οφέλη που αναμένονται από αυτές όταν τους παρουσιάζονται ελκυστικές ευκαιρίες για κέρδη. Στις περισσότερες περιπτώσεις τα κίνητρα των στελεχών είναι η επιθυμία για οικονομικό κέρδος, η επιθυμία να παρουσιάζονται ως επιτυχημένοι στα μάτια των άλλων ή ο φόβος της απώλειας των κεκτημένων.[675]

Η ευκαιρία, σύμφωνα με τον Coleman αποτελεί «την πιθανή πορεία μιας δράσης που διευκολύνεται από ένα ιδιαίτερο σύνολο κοινωνικών συνθηκών που ο δράστης ενσωματώνει στο ατομικό του σύστημα διαθέσιμων συμπεριφορών».[676]

Η πιθανή συμπεριφορά μετατρέπεται σε ευκαιρία όταν το άτομο αποκτά επίγνωση για αυτή και εμπίπτει στην κατηγορία των δράσεων που πραγματικά επιθυμεί να πράξει. Μια ευκαιρία θεωρείται κατάλληλη ή όχι αν τη δούμε από την πλευρά του δράστη. Αν πολλοί τη βλέπουν ως τέτοια, τότε μπορούμε να πούμε ότι είναι ελκυστική ευκαιρία με καθολική έννοια.[677]

Κάθε κοινωνική κατηγορία διαθέτει ποικιλία ευκαιριών που δομούν τη συμπεριφορά τους. Η κατανομή των ευκαιριών σε συνδυασμό με τα κίνητρα διαμορφώνουν ένα ιδιαίτερο σκηνικό για την διάπραξη οικονομικού εγκλήματος. Οι εκλογικεύσεις, που αποτελούν σημαντικότατο κομμάτι των κινήτρων, σχηματίζονται από τη μια ως απάντηση στο πλαίσιο συγκριμένης ευκαιριακής δομής και από την άλλη κάθε ευκαιρία απαιτεί και μια συμβολική κατασκευή για τη ψυχολογική προετοιμασία του δράστη και τη δημιουργία των απαραίτητων εκλογικεύσεων εκ μέρους του. Όμως, σύμφωνα με τον Coleman, ενώ το κίνητρο ενέχει μια υποκειμενική διάσταση λόγω του ότι είναι αποτέλεσμα ατομικής νοητικής κατασκευής, η ευκαιρία έχει μια αντικειμενική διάσταση λόγω του γεγονότος ότι σχηματίζεται από τις κοινωνικές συνθήκες. [678]

Η καταλληλότητα ή η ελκυστικότητα μιας ευκαιρίας έχει πιο αντικειμενική διάσταση από το κίνητρο και δομείται, σύμφωνα με τον Coleman από τέσσερεις παράγοντες: α) την αντίληψη του δράστη για το προσδοκώμενο όφελος, β) την αντίληψη του δράστη για τους πιθανούς κινδύνους ανακάλυψης, σύλληψης και τιμωρίας και τη συνεκτίμηση των κινδύνων με τα οφέλη, γ) τη συνάφεια της ευκαιρίας ως προς τις ιδέες, τις εκλογικεύσεις και τα πιστεύω

[674] Grabosky Peter & Walkley Sascha (2007), ό.π.
[675] Βλ. και παραπάνω για τα κίνητρα
[676] Coleman James.W. (1987), σ.156
[677] Coleman James.W. (1987), όπ.
[678] Coleman James.W. (1987), σ.171

του πιθανού δράστη, δ) την συνεκτίμηση της συγκεκριμένης εγκληματικής ευκαιρίας με άλλες πιθανές ευκαιρίες (για νόμιμη συμπεριφορά) που παρουσιάζονται στην αντίληψη του δράστη. Έτσι δεν είναι όλες οι ευκαιρίες ισοδύναμες, η καταλληλότητα της ευκαιρίας ουσιαστικά δομείται από την αλληλεπίδραση του κινήτρου του δράστη με τις δομικές συνθήκες της ευκαιρίας.[679]

Πολλοί έχουν ευκαιρία διάπραξης κάποιου οικονομικού ή άλλου εγκλήματος, κάποιοι όμως έχουν πιο **ελκυστικές ευκαιρίες** από κάποιους άλλους. Η κατανομή αυτών των ευκαιριών διαφέρει σημαντικά ανάμεσα στα δύο φύλα, στα διάφορα επαγγέλματα, τους οργανισμούς και τις βιομηχανίες.[680]

Συναφής με την παραπάνω εκτίμηση του Coleman, είναι και αυτή του Cook στο πλαίσιο του ρόλου της ορθολογικής επιλογής σε σχέση με τη δόμηση της εγκληματικής ευκαιρίας. Έτσι ο εγκληματίας, επιδιώκοντας υψηλές ανταμοιβές με αντάλλαγμα ένα μικρό κόστος με όρους ρίσκου ή προσπάθειας που απαιτείται να καταβάλλει, επιλέγει την **ευκαιρία** με βάση τα παρακάτω χαρακτηριστικά: α) την **εγγύτητα**, όπου προτιμώνται στόχοι που βρίσκονται κοντά στα μέρη που δραστηριοποιείται παρά αυτοί που βρίσκονται μακριά, β) τις υψηλές **ανταμοιβές**, όφελος σε χρήματα ή αντικείμενα αξίας, γ) την ύπαρξη **ευάλωτου στόχου** – θύματος με αδυναμία υπεράσπισης ή προστασίας του, δ) το **κόστος** που εκφράζεται με την πιθανότητα σύλληψης και τη βαρύτητα της ποινής.[681]

Οι διάφορες ποσοτικές έρευνες έχουν καταλήξει σε αντιφατικά μεταξύ τους αποτελέσματα όσον αφορά την επίδραση του είδους της αγοράς στο οποίο ανήκει μια βιομηχανία για τη δόμηση της εγκληματικής ευκαιρίας. Κάποιες συμφωνούν ότι υψηλότερες πιθανότητες εμπλοκής σε εγκληματικές δραστηριότητες, όπως απάτη, βιομηχανική κατασκοπεία, παραπλανητική διαφήμιση, εμφανίζουν οι βιομηχανίες που ανήκουν σε ανταγωνιστικές αγορές, ενώ άλλες ότι αντίθετα τέτοιες πιθανότητες είναι μεγαλύτερες σε ολιγοπωλιακές αγορές που εφαρμόζουν εναρμονισμένες πρακτικές και συμφωνίες για τον προσδιορισμό των τιμών. Σε αυτές τις περιπτώσεις, οι ποσοτικές έρευνες είναι αρκετά δύσκολο να είναι αντιπροσωπευτικές, οπότε οι Clinard και Yeager πρότειναν τη χρήση πιο εκλεπτυσμένων μεθόδων μελέτης. Τέτοιες μέθοδοι είναι οι μελέτες περίπτωσης (case studies) που επιτρέπουν την εξέταση των ιδιαίτερων συνθηκών που ευνοούν την εμφάνιση συγκεκριμένων μορφών εγκλήματος λευκού περιλαιμίου σε συγκεκριμένα είδη βιομηχανιών.[682]

Ένας άλλος παράγοντας που τείνει να ευνοεί την εμφάνιση εγκληματικών ευκαιριών στις βιομηχανίες, είναι σύμφωνα με τους Clinard και Yeager, η ύπαρξη αυστηρού νομοθετικού πλαισίου σχετικά με τη λειτουργία τους. Έτσι οι βιομηχανίες που τα προϊόντα και η λειτουργία τους παρουσιάζουν μεγαλύτερες επιπτώσεις στο κοινωνικό σύνολο, την υγεία του πληθυσμού, το φυσικό περιβάλλον ελέγχονται με αυστηρότερη νομοθεσία αλλά και παρουσιάζουν μεγαλύτερα ποσοστά παραβίασής της.

Τα ερευνητικά δεδομένα επίσης δίνουν ενδείξεις για μετάδοση των παράνομων πρακτικών από την μια επιχείρηση στην άλλη. Αυτό αποδίδεται όχι μόνο στη διασπορά των κινήτρων και των εκλογικεύσεων, αλλά και των ανάλογων ιδιαίτερων μεθόδων που απαιτούνται για την εκμετάλλευση της εγκληματικής ευκαιρίας. Μια επιχείρηση που θέλει να ανταγωνιστεί τις ομοειδείς της επιχειρήσεις που χρησιμοποιούν παράνομες πρακτικές για να μειώσουν το

[679] Coleman James.W. (1994), σσ.171-172
[680] Coleman James.W. (1995), σσ. 360-381
[681] Cook Philip (1986)
[682] Coleman James.W. (1995), σ. 373

κόστος και τις τιμές τους θα αναγκαστεί πιθανότατα και η ίδια να μετέλθει τέτοιων πρακτικών.[683]

Στην περίπτωση των οργανισμών τα ευρήματα των Clinard και Yeager έδειξαν ότι πιο πιθανό να εκμεταλλευτούν τις εγκληματικές ευκαιρίες είναι οι εταιρείες με κέρδη σε φθίνουσα πορεία, με πενιχρά οικονομικά αποτελέσματα και οικονομικά προβλήματα. Όμως οι σύγχρονες επιχειρήσεις και οργανισμοί έχουν πιο πολύπλοκη οργάνωση, με πολλά τμήματα και εσωτερικό καταμερισμό της εργασίας που δεν διαθέτουν μόνο ένα στόχο αλλά πολλούς επιμέρους στόχους που ανατίθενται για επίτευξη σε κάθε τμήμα. Η επιδίωξη του κάθε συγκεκριμένου στόχου από τους υπεύθυνους των τμημάτων και η ανάλογη πίεση που τους ασκείται από την ανώτερη διοίκηση για την επίτευξη τους, μπορεί να συνδέεται με την απόφαση για εμπλοκή τους σε εγκληματικές δραστηριότητες.[684] Αυτό συμβαίνει επειδή η στοχοθεσία υπερβολικά υψηλών στόχων που πολύ δύσκολα επιτυγχάνονται με νόμιμα μέσα μπορεί να οδηγήσει μερικά στελέχη στη χρήση παράνομων. Ακόμα η κατανομή των ευθυνών ανάμεσα στα διάφορα τμήματα, το προσωπικό και τους προϊστάμενους τους, φέρει ως αποτέλεσμα τελικά να μην αναλαμβάνει κανείς από αυτούς την ευθύνη για τις συνέπειες των δράσεων της επιχείρησης. Η πολυπλοκότητα των στόχων και των ευθυνών ανάμεσα στα ημιανεξάρτητα τμήματα των οργανισμών δημιουργεί πολλούς αυτόνομους δράστες και συνακόλουθα αυξάνει την πιθανότητα διάπραξης εγκλημάτων.[685]

Η κατανομή των εγκληματικών ευκαιριών και το ύψος των εγκληματικών κερδών διαφέρει και ανάμεσα στα διαφορετικά επαγγέλματα. Επαγγέλματα που προσφέρουν ευκαιρίες για δωροδοκία και διαφθορά είναι αυτά των δημόσιων λειτουργών, των αστυνομικών και των πολιτικών, ενώ για κατάχρηση αυτά των λογιστών και κάποιων υπαλλήλων σε επιχειρήσεις και για απάτη τα επαγγέλματα που ασχολούνται με εμπορικές και οικονομικές δραστηριότητες όπως οι πωλητές και τα ανώτερα διοικητικά στελέχη όπως και οι αμειβόμενοι με ποσοστά επί των πωλήσεων υπάλληλοι σε σχέση με τους μισθωτούς.[686] Οι υπάλληλοι με ειδική πρόσβαση και γνώση ιδιαίτερων και ευαίσθητων στόχων, όπως υπάλληλοι εμπορικών καταστημάτων, μηχανικοί, τεχνικοί, νοσοκόμες είναι πιο πιθανό να διαπράξουν κλοπή.[687]

Το φύλο, σύμφωνα με τον Coleman αποτελεί ένα σημαντικό παράγοντα εγκληματικότητας. Στον τομέα του εγκλήματος του λευκού περιλαιμίου, σε έρευνα της Kathleen Daly διαπιστώθηκε ότι οι γυναίκες διέφεραν από τους άνδρες στο ότι υπο-αντιπροσωπεύονταν και εμφανίζονταν πιο νέες, χαμηλότερου μορφωτικού επιπέδου, κοινωνικού status, εισοδήματος, ενώ τα εγκλήματά τους ήταν λιγότερο αποδοτικά σε οικονομικό όφελος και λιγότερο εκλεπτυσμένα από αυτά των ανδρών.[688]

8.3.8. Η εκτίμηση του αναμενόμενου κόστους από πλευράς δράστη ως στοιχείο ορθολογικότητας

Όσον αφορά τις περιπτώσεις των ηλεκτρονικών επιθέσεων η δόμηση του προτύπου της εγκληματικής ευκαιρίας επηρεάζεται και από το στοιχείο της, έστω και περιορισμένης, ορθολογικότητας του δράστη. Ιδιαίτερα για την εκτίμηση του αναμενόμενου κόστους από την πλευρά των δραστών, οι διάφορες έρευνες δεν μπορούν να επιβεβαιώσουν ή να απορρίψουν

[683] Coleman James.W. (1995), ό.π.
[684] Coleman James.W. (1995), σσ. 376-377
[685] Coleman James.W. (1987), σ.179
[686] Coleman James.W. (1987), σ.σ.153-183
[687] Coleman James.W. (1995), σ.377
[688] Coleman James.W. (1995), σ.378

το ρόλο της γνώσης του νόμου[689] ή της αυστηρότητας της ποινής ως παράγοντα αποτροπής του εγκληματία, ενώ από την άλλη πλευρά η βεβαιότητα της ποινής διαπιστώνεται, ότι μπορεί να παίξει τέτοιο ρόλο. Η γνώση μάλιστα του δικαίου γενικότερα από το κοινό δεν θα πρέπει να θεωρείται καθόλου αυτονόητη και δεδομένη. Οι διάφορες έρευνες διαπιστώνουν ανομοιογένεια του βαθμού γνώσης και πληροφόρησης των πολιτών για τους νόμους ανάμεσα στα διάφορα είδη αδικημάτων. Συχνά δε, διαπιστώνεται άγνοια νόμου ακόμα και από εκείνους που αποτελούν αποδέκτες των νόμων. Ακόμα και όσοι γνωρίζουν τους νόμους που αφορούν την επαγγελματική τους ενασχόληση, αποκτούν την γνώση και πληροφόρηση αυτή στο πλαίσιο της γενικότερης κοινωνικοποίησης τους για τους κανόνες συμπεριφοράς και την προσβολή των έννομων αγαθών και όχι ως αποτέλεσμα πληροφόρησης των ειδικών νόμων που τους αφορούν.[690]

Από την πλευρά των δραστών η εκτίμηση της βεβαιότητας της ποινής δεν αποτελεί μια εύκολη διαδικασία που απαιτεί γνώση των νομικο-τεχνικών διαδικασιών της ποινικής δίωξης την οποία διαθέτουν οι τεχνολογικά πιο έμπειροι από αυτούς. Η πληροφόρηση και η αντίληψη των πιθανών εμπλεκομένων με την ηλεκτρονική εγκληματικότητα για τις πιθανότητες ποινικής δίωξης και επιβολής ποινών προέρχεται κυρίως από την ενημέρωση που παρέχεται από τα μέσα μαζικής ενημέρωσης. Πιο συγκεκριμένα τα μέσα διαδραματίζουν σημαντικό ρόλο στην διαμόρφωση της αντίληψης για την πιθανότητα έλλειψης δίωξης και καταδικασιμότητας με το να αναφέρουν ειδήσεις για συλλήψεις και διώξεις ατόμων που διαπράττουν ηλεκτρονικές επιθέσεις.[691]

Ο Guitton διακρίνει τον πληθυσμό των ηλεκτρονικών δραστών σε κατηγορίες ανάλογα με την επίγνωση της πιθανότητας δίωξης τους.

Η πρώτη κατηγορία αφορά τους δράστες που γνωρίζουν τον κίνδυνο (πιθανότητα) ποινικής τους δίωξης αλλά παρόλα αυτά προβαίνουν στη δράση τους δρώντας όχι ορθολογικά, αλλά παρορμητικά, επιδιώκοντας μάλιστα την επισήμανσή τους με κίνητρο την «αναγνώριση» των άλλων, την αντιμετώπιση της πρόκλησης να καταφέρουν να παραβιάσουν πολύπλοκα πληροφοριακά συστήματα και δεδομένα και να υπερηφανεύονται για τα «κατορθώματα» τους αυτά. Η πιθανότητα επισήμανσης και ποινικής δίωξης λειτουργεί κάθε άλλο παρά αποτρεπτικά για αυτούς τους δράστες, όπως είναι κατά κύριο λόγο οι χάκερ που ανήκουν στην παραβατική υποκουλτούρα. Σε πολλές περιπτώσεις η πρόσληψή τους ως ειδικοί ασφάλειας επιχειρήσεων ή εκπρόσωποι της δίωξης που χρησιμοποιούνται για την επισήμανση άλλων χάκερ λειτουργεί ως πρόσθετο κίνητρο διάπραξης του εγκλήματος.

Η δεύτερη κατηγορία είναι αυτή των πιθανών δραστών, που αντιλαμβανόμενοι τις πιθανότητες ποινικής τους δίωξης και εκτιμώντας ορθολογικά την εγκληματική ευκαιρία, αποτρέπονται τελικά από την τέλεση της παράνομης πράξης. Για αυτούς η αυστηροποίηση των ποινών και του κοινωνικού ελέγχου θα λειτουργήσει θετικά ως προς την μείωση της καταλληλότητας της εγκληματικής ευκαιρίας.

Στην τρίτη κατηγορία δραστών περιλαμβάνονται όσοι δεν γνωρίζουν τις διαδικασίες άσκησης ποινικής δίωξης και κατά συνέπεια δεν επηρεάζονται από την βεβαιότητα ή την αυστηρότητα των ποινών. Η μείωση της εγκληματικής ευκαιρίας για την κατηγορία αυτή συνίσταται στις προσπάθειες για «σκλήρυνση» των πιθανών στόχων ώστε αυτοί να καταστούν λιγότερο ευάλωτοι με τη λήψη πρόσθετων μέτρων ασφάλειας ή με την διάδοση

[689] Βλ. Λαμπροπούλου Έφη (1999), σσ. 248 -253
[690] Βλ. Λαμπροπούλου Έφη (1999), ό.π.
[691] Guiton Clement, (2012)

και εμπέδωση κοινωνικών αξιών καλής διαδικτυακής συμπεριφοράς μέσω της εκπαίδευσης, της καμπάνιας ενημέρωσης του κοινού κλπ.[692]

Για την μελέτη των οικονομικών εγκλημάτων που τελούνται με ηλεκτρονικά μέσα, που αποτελούν το αντικείμενο της παρούσας διατριβής, το ενδιαφέρον εστιάζεται στις παραπάνω κατηγορίες στο βαθμό που σε κάποιες περιπτώσεις το κίνητρο των δραστών είναι οικονομικό.

Παρά το ότι τα κίνητρα δομούνται στη βάση των νοηματοδοτήσεων που πραγματοποιούν τα δρώντα υποκείμενα, στις παραπάνω διαπιστώσεις για τα κίνητρα και τις ευκαιρίες είναι εμφανής η επίδραση της, περιορισμένης έστω, ορθολογικότητας του δράστη στα εξής σημεία:

Η ορθολογικότητα στα κίνητρα φανερώνεται από τα ευρήματα για επιδίωξη οικονομικού οφέλους που αποτελεί ένα από τα ουσιαστικότερα κίνητρα του εγκλήματος λευκού περιλαιμίου, το φόβο της απώλειας των ήδη κεκτημένων, των υψηλών απολαβών ή της κοινωνικής θέσης. Το κίνητρο της επιδίωξης του ατομικού οικονομικού οφέλους αποτελεί το συνδετικό κρίκο που διασυνδέει τις επιμέρους θεωρητικές προσεγγίσεις που προέρχονται από διαφορετικές σχολές, όπως την κλασική, τη θετικιστική και τη σχολή της συμβολικής αλληλεπίδρασης.

Η ορθολογικότητα στη δόμηση της ευκαιρίας είναι εμφανής στη στάθμιση των αναμενόμενων κερδών και του πιθανού κόστους, που αφορά τον κίνδυνο επισήμανσης και επιβολής ποινής, απώλεια γοήτρου κλπ, και τη στάθμιση της ευκαιρίας αυτής σε σχέση με άλλες εναλλακτικές ευκαιρίες δράσης.

Η θεωρία της ορθολογικής επιλογής, εκτός από τα κίνητρα του δράστη μας διαφωτίζει για τη διαδικασία λήψης της εγκληματικής απόφασης επειδή η επιλογή της εγκληματικής δράσης συνδέεται με δυο είδη (ορθολογικών) αποφάσεων, ένα για την αρχική εμπλοκή του και ένα για το γεγονός, δηλαδή για την συνέχιση ή τη διακοπή της δράσης του. Ο ηλεκτρονικο-οικονομικός δράστης περνά την ίδια διαδικασία όπως για μια παραδοσιακή ληστεία. Θα πρέπει να συλλέξει πληροφορίες για το στόχο του, όπως διεύθυνση, αριθμό λογαριασμού κλπ., να ανοίξει διόδους προσέγγισης και να δημιουργήσει κενά ασφαλείας για να αποκτήσει πρόσβαση ώστε να κλέψει, να καταστρέψει ή να ελέγξει και τέλος να καλύψει τα ίχνη μετά την επίθεση ώστε να αποφύγει τη σύλληψη.[693]

Άρα, για την διακρίβωση των εγκληματικών δομών που συνθέτουν τις ευκαιρίες για ψηφιακά εγκλήματα τύπου λευκού περιλαιμίου, εφαρμόζοντας τις θεωρίες «εγκληματικών ευκαιριών» απαιτείται η συνεξέταση των στοιχείων: του πιθανού δράστη, του ελκυστικού στόχου, του κατάλληλου δικτύου, των επαγγελματικών δομών που επιτρέπουν την επικοινωνία (εγγύτητα) μεταξύ δράστη και στόχου και την ύπαρξη ικανών φυλάκων.[694]

[692] Guiton Clement (2012)
[693] Jahankhani Hamid & Al-Nemrat Ameer (2011), σσ. 188-189
[694] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), ό.π., σ.179

ΚΕΦΑΛΑΙΟ 9. ΝΟΜΟΘΕΤΙΚΗ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ - ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΑΠΟ ΤΟΝ ΕΠΙΣΗΜΟ ΚΟΙΝΩΝΙΚΟ ΕΛΕΓΧΟ: ΑΥΞΗΣΗ ΤΟΥ ΚΟΣΤΟΥΣ - ΜΕΙΩΣΗ ΤΟΥ ΟΦΕΛΟΥΣ ΓΙΑ ΤΟΝ ΔΡΑΣΤΗ

Η αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος, όπως και του κοινού εγκλήματος, κινείται σε δυο γενικές κατευθύνσεις, την πλευρά της πρόληψης και την πλευρά της καταπολέμησης, κυρίως μέσω της ποινικής καταστολής.

Η πρόληψη που προτείνεται αφορά την εφαρμογή των προσεγγίσεων των «εγκληματικών ευκαιριών» - και ιδιαίτερα την στρατηγική της περιστασιακής πρόληψης του εγκλήματος - που εξετάστηκαν παραπάνω. Η πρόληψη, δηλαδή η αποτροπή ή τουλάχιστον η ελαχιστοποίηση του ηλεκτρονικο-οικονομικού εγκλήματος συνίσταται στη διαχείριση του άμεσου περιβάλλοντος του δράστη[695], με τρόπο ώστε να μειωθούν οι εγκληματικές ευκαιρίες και να αυξηθεί η πιθανότητα ανακάλυψής του.[696]

Η καταπολέμηση μέσω της ποινικής καταστολής προέρχεται από την εφαρμογή των θεωριών της ορθολογικής επιλογής (R.C.T) και ιδιαίτερα των κλασικών και των οικονομολογικών απόψεων, που συνίστανται στην αύξηση του αναμενόμενου κόστους και ρίσκου από πλευράς δράστη, με την έμφαση εδώ να βρίσκεται στην αύξηση της πιθανότητας επιβολής αυστηρότερων ποινών.

Παρά τις διάφορες ερευνητικές προσπάθειες να παρέχουν μια γενικευμένη θεωρία αποτροπής της παρέκκλισης, το κοινό στοιχείο που συνδέει τις διαφορετικές προσεγγίσεις είναι οι καταβολές που τους κληρονόμησαν οι κλασικοί[697], στις ιδέες των οποίων - περί αυστηρότητας των ποινών - στηρίζεται ακόμα και σήμερα, λιγότερο ή περισσότερο, το αμερικάνικο σύστημα απονομής της δικαιοσύνης. Στο πλαίσιο αυτό οι ερευνητικές προσπάθειες επικεντρώνονται στην επίδραση της βαρύτητας και της βεβαιότητας των ποινών (στοιχείο της θεωρίας της γενικής πρόληψης) πάνω στην εγκληματική συμπεριφορά και χρησιμοποιούν την ορθολογική επιλογή ως βασικό μεθοδολογικό εργαλείο.[698]

Ιδιαίτερα για την αποτροπή των οικονομικών εγκλημάτων, όπως του λευκού περιλαιμίου, κατά της περιουσίας, τα επιχειρησιακά εγκλήματα κλπ., ο φόβος της ποινής μπορεί να λειτουργήσει αποτρεπτικά, αν και μπορεί η εγκληματική δραστηριότητα εν μέρει να μεταφέρεται σε άλλο είδος εγκλήματος[699] ή οι εγκληματίες να επιδιώξουν να λάβουν καλύτερα μέτρα κάλυψης της δράσης τους. Πιο αποτρεπτικά λειτουργεί η γενική πρόληψη στην περίπτωση των περιστασιακών εγκλημάτων.[700]

Αξίζει πάντως να σημειωθεί ότι τα ερευνητικά δεδομένα ως προς την αποτρεπτική ικανότητα και αποτελεσματικότητα συνηγορούν μάλλον στην πλευρά της έμφασης στην

[695] όπως είναι κυρίως τα δίκτυα υπολογιστικών συστημάτων.

[696] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626

[697] Beccaria και Bentham

[698] Βλ. αναφορά στον Gibbs, 1975 στο Piliavin Irving, Rosemary Gartner, Craig Thornton & Ross L. Matsueda, (1986), σσ. 101-119

[699] Όπως θα δούμε όμως παρακάτω αρκετές έρευνες δεν επιβεβαίωσαν μετατόπιση της εγκληματικότητας, αλλά διαπίστωσαν αντίθετα «διασπορά της ωφέλειας», βλ. αναφορές στους Barr & Pease 1990, Ekblom 1988, Gabor 1990, στο Goldstein Arnold P., ό.π., στο Clarke Ronald V. Editor (1997), σ.28, στο Jeffery C. Ray & Zahm Diane L (2008), σ.337 και στο Goldstein, ό.π., σσ.129-130

[700] Λαμπροπούλου Έφη (1994), σ.128

πρόληψη δηλαδή την αύξηση του ρίσκου ανακάλυψης του δράστη παρά στην καταστολή, την πιθανότητα επιβολής αυστηρής ποινής. [701]

Σε κάθε περίπτωση η αποτελεσματική αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος, σε επίπεδο πρόληψης και ελέγχου, όπως και του παραδοσιακού, προϋποθέτει την συνεργασία των κρατικών αρχών με τους ιδιωτικούς φορείς αλλά και τους μη κερδοσκοπικούς οργανισμούς. [702]

Στο κεφάλαιο αυτό εξετάζονται οι προσπάθειες νομοθετικής αντιμετώπισης του ηλεκτρονικο-οικονομικού εγκλήματος και τις δυσκολίες που παρουσιάζει η αντιμετώπισή της.

9.1. Νομοθετική αντιμετώπιση του ηλεκτρονικο–οικονομικού εγκλήματος

Οι τεχνολογικές αλλαγές συντελούν στη δημιουργία νέων μορφών συμπεριφοράς που προηγουμένως δεν θεωρούνταν παράνομες και αυτές οδήγησαν σε νομοθετική ρύθμιση για τον έλεγχο της εν λόγω συμπεριφοράς. Οι τηλεπικοινωνιακές παραβάσεις είναι ένας τομέας που πρόσφατα αποτέλεσε αντικείμενο νομοθετικών ελέγχων σε όλο τον κόσμο, αν και ούτε αυτοί οι έλεγχοι θεωρούνται επαρκείς να ρυθμίσουν το πρόβλημα αποτελεσματικά.

Οι νομοθεσίες των κρατών, ακόμη και αν αυτά ανήκουν σε υπερεθνικούς οργανισμούς όπως η Ε.Ε., διαφέρουν μεταξύ τους ως προς την ακριβή περιγραφή των ψηφιακών εγκλημάτων. Αυτό μπορεί να συνεπάγεται σημαντικές δυσκολίες στην αποτελεσματική δίωξη εγκλημάτων που πραγματοποιούνται σε διαφορετικές χώρες, εκτός αν αποδειχθούν επιτυχείς οι παράλληλες προσπάθειες εναρμόνισης των νομοθεσιών.[703] Σε αυτό το πλαίσιο, τα διεθνή νομικά όργανα πρέπει να στοχεύσουν στην εναρμόνιση των ορισμών του εγκλήματος από τις εσωτερικές νομοθεσίες και την καθιέρωση ενός κοινά αποδεκτού ορισμού των σχετικών παραβάσεων. Είναι αυτονόητο ότι αυτός ο στόχος συνεπάγεται μια αναθεώρηση των νόμων σε πολλούς τομείς της εθνικής νομοθεσίας, όπως το νομικό καθεστώς προστασίας των προσωπικών δεδομένων και η ηλεκτρονική επιτήρηση.

Τα διάφορα νομοθετικά μέτρα, παγκοσμίως, κινούνται στην κατεύθυνση που προτείνουν οι προσεγγίσεις για τη δόμηση των «εγκληματικών ευκαιριών» για αύξηση του κόστους και μείωση του οφέλους από την διάπραξη του εγκλήματος για τον πιθανό δράστη.

9.1.1. Διεθνής νομοθεσία

Σχετικά με τις νομοθετικές προσεγγίσεις του ηλεκτρονικού εγκλήματος από τα ποινικά συστήματα των διαφόρων κρατών, η Νομική Επιτροπή της Μ. Βρετανίας (British Law Commission) διαπιστώνει την υιοθέτηση τριών βασικών τάσεων:

α) την εξελικτική, όπου το ηλεκτρονικό έγκλημα αντιμετωπίζεται με το ισχύον νομοθετικό πλαίσιο, με έννοιες που απλά διευρύνονται κατά περίπτωση για να περιλαμβάνουν και ορισμένες περιπτώσεις ηλεκτρονικού εγκλήματος.

β) Νομοθετήματα που σχεδιάζονται ειδικά για ηλεκτρονικά εγκλήματα αλλά εντάσσονται στο ευρύτερο νομοθετικό πλαίσιο.

γ) Νόμοι που θεσπίζονται για την συνολική αντιμετώπιση του ηλεκτρονικού εγκλήματος.[704]

Αρχικά οι νομοθεσίες των περισσότερων χωρών (ΗΠΑ, Μ.Βρετανία, Αυστραλία κλπ) αντιμετώπιζαν το δράστη ηλεκτρονικού εγκλήματος με βάση το υπάρχον νομοθετικό πλαίσιο

[701] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626
[702] Grabosky Peter. (2009), σσ.129-171
[703] Pocar Fausto, ό.π.
[704] Λάζος Γρηγόρης (2001), σ. 46-47

συμπεριλαμβάνοντάς το στις γενικότερες κατηγορίες, είτε του οργανωμένου εγκλήματος και οργανωμένης απάτης (Πολιτεία της Αριζόνα)[705] είτε της πνευματικής ιδιοκτησίας (Φλόριντα) είτε του οικονομικού εγκλήματος (Μ. Βρετανία).

Μετά το ΄80 δημιουργήθηκαν νομοθετήματα για την κάλυψη των κενών στην αντιμετώπιση του πληροφορικού εγκλήματος. Το 1986 το αμερικανικό Κογκρέσο θέσπισε το νόμο για «την Απάτη και Προσβολή των Ηλεκτρονικών Υπολογιστών» (Computer Fraud And Abuse Act, U.S. Public Law, 1986)) που προέβλεπε τρία κακουργήματα και τρία πλημμελήματα. Τα τρία κακουργήματα αφορούν:

1) τη σκόπιμη μη εξουσιοδοτημένη ή υπέρβαση εξουσιοδοτημένης πρόσβασης σε υπολογιστές με σκοπό την πρόκληση βλάβης στις ΗΠΑ ή την ωφέλεια ξένης χώρας
2) την πρόσβαση σε υπολογιστή ομοσπονδιακού συμφέροντος με σκοπό την εξαφάνιση των ΗΠΑ και την απόκτηση αξιών εκτός από τον υπολογιστή καθαυτό.
3) Τη σκόπιμη, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή, με σκοπό την αλλαγή, την αλλοίωση ή την καταστροφή πληροφοριών ομοσπονδιακού ενδιαφέροντος ή την παρεμπόδιση της αξιοποίησης αυτών των πληροφοριών.

Οι ποινές που προβλέπονται για το δράστη κυμαίνονται από χρηματικά πρόστιμα μέχρι δεκαετή φυλάκιση με ανώτατο όριο την εικοσαετή.

Τα δύο πλημμελήματα αφορούν επίσης σε ομοσπονδιακά συμφέροντα και το τρίτο με τη παράνομη διακίνηση κωδικών πρόσβασης που επηρεάζει το εμπόριο. Οι ποινές για αυτά δεν ξεπερνούν τη φυλάκιση του ενός έτους.

Στη Μ. Βρετανία η ποινική αντιμετώπιση του πληροφορικού εγκλήματος παίρνει μορφή με το «Νόμο κακής χρήσης των Ηλεκτρονικών Υπολογιστών» (Computer Misuse Act) του 1990. Αυτό προβλέπει:

«1. ένα πρόσωπο είναι ένοχο προσβολής αν: α. αποκτά πρόσβαση σε πρόγραμμα ή δεδομένα αποθηκευμένα σε υπολογιστή β. η πρόσβαση αυτή είναι χωρίς εξουσιοδότηση και γ. είναι σκόπιμη αυτή η πρόσβαση.

2. Ο σκοπός του προσώπου που διαπράττει την παραπάνω προσβολή δεν είναι απαραίτητο να κατευθύνεται προς:

α. κάποιο ειδικό πρόγραμμα ή δεδομένα

β. πρόγραμμα ή δεδομένα ειδικού τύπου

γ. πρόγραμμα ή δεδομένα αποθηκευμένα σε συγκεκριμένο υπολογιστή».

Έτσι δημιουργούνται τρία νέα εγκλήματα εκ των οποίων τα δύο αφορούν τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή ή δεδομένα και το τρίτο με τη συνειδητή και σκόπιμη αλλαγή του περιεχομένου των δεδομένων ενός υπολογιστή. [706]

Ο Γερμανικός Ποινικός Κώδικας προσαρμόστηκε στις νέες μορφές εγκληματικότητας το 1986 με το «2^{ο} Νόμο για την καταπολέμηση της οικονομικής εγκληματικότητας» που περιλαμβάνει διατάξεις οι οποίες αφορούν άμεσα:

α) το hacking, τη μετάδοση ιών, τη χωρίς άδεια απόκτηση δεδομένων. [707]

β) τη παραποίηση δεδομένων[708]

γ) τη δολιοφθορά Η/Υ.[709]

[705] Λάζος Γρηγόρης (2001), σσ. 61-67
[706] Λάζος Γρηγόρης. (2001), σ. 70
[707] Αργυρόπουλος Ανδρέας (2001), σσ. 57-58
[708] Αργυρόπουλος Ανδρέας (2001), σ.86
[709] Αργυρόπουλος Ανδρέας (2001), σσ.111-112

9.1.2. Διεθνείς προσπάθειες νομικής συνεργασίας

Η παγκοσμιοποίηση του ηλεκτρονικο-οικονομικού εγκλήματος απαιτεί διακρατικό συντονισμό και συνεργασία για την αντιμετώπισή του. Τέτοιες προσπάθειες συνιστούν η Σύμβαση του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα στη Βουδαπέστη το 2001, η Συνθήκη των Ηνωμένων Εθνών ενάντια στο Οργανωμένο Έγκλημα το 2000 στο Παλέρμο, η σύνοδος των G8 για το Διεθνές Οργανωμένο Έγκλημα στο Χάλιφαξ το 1995, η συνθήκη του Μάαστριχτ το 1992, η λειτουργία της Europol και της Interpol κλπ.

Για τη διεθνή (νομική) συνεργασία στην καταπολέμηση του κυβερνοεγκλήματος οι ειδικοί μελετητές Grabosky και Broadhurst πρότειναν τα εξής βασικά στοιχεία:

α) Αύξηση της ευαισθητοποίησης και επαγρύπνησης σε θέμα ασφάλειας με παροχή απαραίτητου εξοπλισμού στους ειδικούς για τη διασφάλιση των συναλλαγών.

β) Βελτίωση του συντονισμού και της συνεργασίας μεταξύ του συστήματος ποινικής δικαιοσύνης και των φορέων του δημόσιου και του ιδιωτικού τομέα.

γ) Διασφάλιση ότι η τεχνολογία θα διευκολύνει την δυνατότητα των αρχών να ερευνούν και να θεσπίζουν νόμους για την αντιμετώπιση του εγκλήματος.

δ) Διεύρυνση της ποινικοποίησης των συμπεριφορών.

ε) Ενδυνάμωση των διεθνών συμβάσεων για την αναγνώριση των απειλών, του διεθνή χαρακτήρα τους και της ανάγκης για εναρμόνιση των νομοθεσιών.

στ) Ανάπτυξη δεξιοτήτων για τα εγκληματολογικά εργαστήρια ώστε να συνεργάζονται επιχειρησιακά με τις αρχές των διαφόρων κρατών.[710]

9.1.2.1. *Συνθήκη του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα στη Βουδαπέστη.*[711]

Η Συνθήκη της Βουδαπέστης αποσκοπεί στην αντιμετώπιση του Ηλεκτρονικού Εγκλήματος μέσω της εναρμόνισης των εθνικών νομοθεσιών, της βελτίωσης των διερευνητικών τεχνικών και τη διεύρυνση της συνεργασίας μεταξύ των κρατών. Η Συνθήκη, που αποτελεί την πρώτη Διεθνή Συνθήκη για το κυβερνοέγκλημα, υπεγράφη τον Νοέμβριο του 2001 και τέθηκε σε ισχύ τον Ιούλιο του 2004. Επίσης, ένα πρόσθετο Πρωτόκολλο που αφορά στη ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που τελείται με πληροφορικά συστήματα υπεγράφη το 2003 και τέθηκε σε ισχύ το Μάρτιο του 2006.[712]

Στη Συνθήκη της Βουδαπέστης υπάρχουν ορισμοί, κατηγοριοποιήσεις και ρυθμίσεις για τα ηλεκτρονικά εγκλήματα:

α. κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων ηλεκτρονικών υπολογιστών.

β. που σχετίζονται με τους υπολογιστές όπως η απάτη με ηλεκτρονικό υπολογιστή και η πλαστογραφία.

γ. σχετικά με το περιεχόμενο, όπως το αδίκημα της παιδικής πορνογραφίας.

δ. που σχετίζονται με τη καταπάτηση πνευματικής ιδιοκτησίας.

Σύμφωνα με την Σύμβαση οι χώρες - μέλη θα πρέπει να νομοθετήσουν μέτρα για την καθιέρωση ως ποινικά αδικήματα συμπεριφορών που σχετίζονται με την κακή χρήση υπολογιστών.

Η Σύμβαση του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα στη Βουδαπέστη το 2001 έχει τριπλό σκοπό:

[710] Broadhurst Roderic (2006), σσ. 408-433
[711] Convention on Cybercrime, Budapest, 23.XI.(2001)
[712] Κύρωση της Σύμβασης της Βουδαπέστης και του πρόσθετου Πρωτοκόλλου (2014)

(ι) τον καθορισμό κοινά αποδεκτών ορισμών για συγκεκριμένα είδη εγκλήματος σχετικά με υπολογιστές έτσι ώστε να μπορούν να εναρμονιστούν οι εθνικές νομοθεσίες.

Προς την κατεύθυνση αυτή, του εναρμονισμού και της κάλυψης των νομικών κενών στις εθνικές νομοθεσίες, κινούνται οι προσπάθειες των θεσμών της Ευρωπαϊκής Ένωσης όπως του Συμβουλίου της Ευρώπης, της Europol και του Ευρωπαϊκού Νομικού Δικτύου (European Judicial Network). Με τον τρόπο αυτό ακόμα και οι τοπικές αρχές δίωξης του εγκλήματος θα δρουν περισσότερο διεθνο-κεντρικά και λιγότερο εθνοκεντρικά.

(ιι) τον καθορισμό και συντονισμό κοινών δυνάμεων για την διερεύνηση και δίωξη των κυβερνοεγκλημάτων. Ένα από τα σημαντικότερα θέματα που θίγει η συνθήκη είναι αυτό της δικαιοδοσίας και του καθορισμού του γεωγραφικού τόπου όπου τελέστηκε το έγκλημα για την εφαρμογή της ανάλογης νομοθεσίας υποχρεώνοντας τις χώρες –μέλη να συντονιστούν όταν τα θύματα προέρχονται από διαφορετικές χώρες.

(ιιι) τον συνδυασμό παραδοσιακών και σύγχρονων μεθόδων διεθνούς συνεργασίας και ανάπτυξη δικτύου αλληλο-υποστήριξης με επικοινωνία επί εικοσιτετραώρου βάσεως για την ποινική δίωξη του ηλεκτρονικού εγκλήματος σε σταθερή βάση. Τέτοιοι μέθοδοι περιλαμβάνουν για παράδειγμα την έρευνα, σε πραγματικό χρόνο, την ανακάλυψη και την διατήρηση των ψηφιακών δεδομένων ως αποδεικτικά στοιχεία.

Η συνθήκη προβλέπει την ευρύτερη δυνατή συνεργασία των μελών της για την ελαχιστοποίηση των εμποδίων που θα προκύπτουν από την ταχύτατη ροή των πληροφοριακών δεδομένων στην προσπάθεια αναζήτησης αποδεικτικών στοιχείων.[713]

9.1.2.2. Μέτρα για την πρόληψη και καταπολέμηση της απάτης στην Ευρωπαϊκή Ένωση

Την κύρια ευθύνη για την πρόληψη και καταπολέμηση της απάτης στην Ευρωπαϊκή Ένωση έχουν τα κράτη-μέλη σε συνεργασία με την Ευρωπαϊκή Επιτροπή και τα αρμόδια κοινοτικά όργανα, το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο Υπουργών, το Ελεγκτικό Συνέδριο, το Ευρωπαϊκό Δικαστήριο και τη Διοικητική Μονάδα Συντονισμού της Καταπολέμησης της Απάτης (UCLAF).

Η Ε.Ε. από το 1994 ακολουθεί επίσημη στρατηγική καταπολέμησης της απάτης με προτεραιότητες την ενίσχυση του έργου που γίνεται επιτόπου, την ενίσχυση της εταιρικής σχέσης, τη βελτίωση της κοινοτικής νομοθεσίας και τον εναρμονισμό των εθνικών νομοθεσιών.

Δυο βασικά νομοθετικά κείμενα που θέσπισε το Ευρωπαϊκό κοινοβούλιο το 1995, αφορούν το μεν πρώτο τους «Ελέγχους και Διοικητικές Κυρώσεις» και το δεύτερο την «Ποινική Προστασία των οικονομικών της Ένωσης». Στα κείμενα αυτά ορίζεται η έννοια της «παρατυπίας» που είναι ευρεία και περιλαμβάνει από την απλή παράλειψη από αμέλεια ή λάθος, μέχρι πράξεις από βαριά αμέλεια ή δόλο που επιφέρουν συνέπειες στον Ευρωπαϊκό προϋπολογισμό.

Στον τομέα των κοινοτικών πιστώσεων υιοθετείται, σε συνεργασία με τις εθνικές κυβερνήσεις, το πρόγραμμα με τον κωδικό SEM 2000 που αναφέρεται στην ενίσχυση της διαχείρισης των δημοσιονομικών της Ένωσης, τη διάθεση κοινοτικών πόρων με μεγαλύτερη διαφάνεια και ασφάλεια.

Ο Κανονισμός 2185 του 1996 παρέχει το νομικό πλαίσιο για την διενέργεια των επιτόπιων ελέγχων και επαληθεύσεων στο πλαίσιο πρόληψης και καταπολέμησης της απάτης, αποσαφηνίζει τον τρόπο, τη μέθοδο και τα πρόσωπα με τα οποία διενεργούνται οι έλεγχοι,

[713] Broadhurst Roderic (2006), ό.π.

αποσκοπεί στη παροχή βοήθειας από τη Ευρωπαϊκή Επιτροπή στα κράτη μέλη για την προστασία των οικονομικών συμφερόντων της Ε.Ε.[714]

Η Σύμβαση κατά της Διαφθοράς του Συμβουλίου της Ευρώπης[715] υιοθετεί μια ευρεία έννοια για τη διαφθορά που περιλαμβάνει την ενεργητική και παθητική δωροδοκία οποιουδήποτε αξιωματούχου, το ξέπλυμα χρήματος, φορολογικά αδικήματα σχετιζόμενα με διαφθορά, διασυνοριακές δωροδοκίες, τη δωροδοκία ιδιωτών και την «εμπορία επιρροής».[716]

9.1.2.3. Η σύνοδος των G8 για το Διεθνές Οργανωμένο Έγκλημα

Η ομάδα των οκτώ περισσότερο βιομηχανικά ανεπτυγμένων χωρών[717] του κόσμου ανέπτυξε πρωτοβουλία κάνοντας 40 προτάσεις για την αύξηση της αποτελεσματικότητας της συνεργασίας των κρατών για την καταπολέμηση της διεθνούς εγκληματικότητας. Οι προτάσεις αυτές, που υιοθετήθηκαν από 40 ακόμα κράτη το 2004, δίνουν προτεραιότητα στην ανάπτυξη διασυνοριακής υποστήριξης, όπως αμοιβαία νομική βοήθεια, συνεργασία αστυνομικών αρχών, έκδοση κρατουμένων. Ακόμα σε συνδυασμό με την έναρξη ισχύος των αποφάσεων της συνθήκης του Ευρωπαϊκού Συμβουλίου το 2004, πρότειναν την αύξηση της παραγωγής νομοθετημάτων που ποινικοποιούν περιπτώσεις κακοχρησίας υπολογιστών στις εθνικές νομοθεσίες και το συντονισμό των προσπαθειών για την αντιμετώπιση του εγκλήματος υψηλής τεχνολογίας. [718]

9.1.2.4. Η Ευρωπαϊκή Ένωση, η Συνθήκη του Μάαστριχτ και η Europol

Η Συνθήκη του Μάαστριχτ που υπογράφηκε από τις χώρες – μέλη της Ε.Ε. το 1992 περιλαμβάνει τη δημιουργία υπερεθνικών ιδρυμάτων και οργανισμών που θα αντιμετωπίζουν τις εγκληματικές δραστηριότητες με συνδυασμένη δράση των κρατών, κοινές οδηγίες, θέσεις και κατευθύνσεις. Η συνδυασμένη δράση θα βασίζεται στην υιοθέτηση των αποφάσεων του Ευρωπαϊκού Συμβουλίου για το κυβερνοέγκλημα και των συνθηκών της Ε.Ε. για την παροχή αμοιβαίας υποστήριξης σε νομικά θέματα μεταξύ των μελών.

Στην κατεύθυνση αυτή η Europol [719], θεσμός της Ε.Ε, δίνει έμφαση στην συνεργασία των αστυνομικών αρχών των χωρών – μελών για την καταπολέμηση του οργανωμένου εγκλήματος ενώ πιο πρόσφατα περιελήφθη και αυτή του κυβερνοεγκλήματος. Η συνεργασία μεταξύ των κρατών περιλαμβάνει την ανταλλαγή πληροφοριών και στοιχείων, τη δημιουργία εκθέσεων σχετικά με τις τάσεις και τα πρότυπα της εγκληματικότητας, παροχή τεχνικής υποστήριξης για διενεργούμενες έρευνες στο πλαίσιο της Ε.Ε. [720]

Πρόσφατα μεγάλη επιχείρηση της Europol, σε συνεργασία με το FBI και 16 ευρωπαϊκές χώρες με χρήση σύγχρονων τεχνικών μέσων, είχε αποτέλεσμα το κλείσιμο 400 «σκοτεινών» ιστοσελίδων και 17 συλλήψεις. Οι ιστοσελίδες αυτές δραστηριοποιούνται σε παράνομες πωλήσεις ναρκωτικών, όπλων, περιεχόμενου παιδικής πορνογραφίας και κακοποίησης, ενώ φιλοξενούν πλήθος εξτρεμιστικών οργανώσεων και δεν εμφανίζονται στις κλασικές μηχανές

[714] Κανονισμός (Ευρατόμ, ΕΚ) αριθ. 2185/96 του Συμβουλίου της 11ης Νοεμβρίου 1996 σχετικά με τους ελέγχους και εξακριβώσεις που διεξάγει επιτοπίως η Επιτροπή με σκοπό την προστασία των οικονομικών συμφερόντων των Ευρωπαϊκών Κοινοτήτων από απάτες και λοιπές παρατυπίες, ανακτήθηκε από http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:31996R2185

[715] Στρασβούργο, Νοέμβριος 1998 (CM[98]18 1).

[716] Levi M., (2001), σσ. 303-305.

[717] Γαλλία, Γερμανία, ΗΠΑ, Ηνωμένο Βασίλειο, Ιαπωνία, Ιταλία, Καναδάς, Ρωσία.

[718] Broadhurst Roderic (2006), ό.π.

[719] (European Police Office) Ευρωπαϊκή Αστυνομία

[720] Broadhurst Roderic (2006), ό.π.

αναζήτησης στο διαδίκτυο λειτουργώντας μέσω δικτύων όπως του Tor, το οποίο καθιστά «αόρατα» τα ίχνη των χρηστών του.[721]

9.1.2.5. Ο Ο.Ο.Σ.Α

Στον τομέα της διαδικτυακής ασφάλειας και καταπολέμησης του κυβερνοεγκλήματος, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης με 30 μέλη εξέδωσε το 1997 σειρά κατευθυντήριων γραμμών που δίνουν έμφαση στις τεχνολογίες κρυπτογράφησης και τα μέσα με τα οποία τα κράτη–μέλη θα συντονίζουν την πολιτική τους σε σχέση με την κρυπτογράφηση και θα σταθμίζουν την ισορροπία μεταξύ ιδιωτικότητας και ανάγκης επιβολής του κοινωνικού ελέγχου. Μετά την 11 Σεπτεμβρίου του 2001 οι κατευθυντήριες γραμμές του Οργανισμού εστιάζουν στην αντιμετώπιση της κυβερνο-τρομοκρατίας, των ιών, του hacking και ανάλογων επιθέσεων. Οι γραμμές αυτές είναι ενδεικτικές της πρόθεσης για συναίνεση μεταξύ των χωρών για τα θέματα της διαδικτυακής ασφάλειας, αλλά δεν συνιστούν για αυτές κάποια μορφή νομικής δέσμευσης. [722]

Βασισμένη στις κατευθύνσεις του Ο.Ο.Σ.Α είναι η Financial Action Task Force (Ομάδα Οικονομικής δράσης) που ιδρύθηκε από την σύνοδο των G7 στο Παρίσι το 1989 και η οποία με τη σειρά της εξέδωσε 40 συστάσεις για την καταπολέμηση του ξεπλύματος μαύρου χρήματος σε τρία επίπεδα: της ποινικής νομοθεσίας, της νομοθεσίας των τραπεζών και της διεθνούς συνεργασίας.

9.1.2.6. Το Παγκόσμιο Φόρουμ του ΟΟΣΑ για τη Διαφάνεια και την Ανταλλαγή Πληροφοριών

Την 1η Νοεμβρίου 2014 στο Βερολίνο και στο πλαίσιο του Παγκόσμιο Φόρουμ του ΟΟΣΑ υπογράφηκε το Παγκόσμιο Πρότυπο του ΟΟΣΑ από 52 κράτη[723,] μεταξύ των οποίων και η Ελλάδα, για αυτόματη ανταλλαγή χρηματοοικονομικών πληροφοριών, με στόχο την καταπολέμηση της φοροδιαφυγής και της φορολογικής απάτης και την ενίσχυση της διαφάνειας. Οι χώρες- μέλη του ΟΟΣΑ δεσμεύονται για πρώτη ανταλλαγή πληροφοριών το 2017.[724]

Η συμφωνία προβλέπει ότι οι τράπεζες θα κοινοποιούν αυτόματα στη χώρα όπου πληρώνει ο κάτοχος ενός λογαριασμού τους φόρους του, το όνομα και τη διεύθυνσή του, τον αριθμό φορολογικού μητρώου, το ποσό της κατάθεσης, το ύψος των τόκων και την πληρωμή μερίσματος από μετοχές. Εκτός από τα στοιχεία των λογαριασμών φυσικών προσώπων θα κοινοποιούνται και στοιχεία νομικών προσώπων όπως εταιρείες και ιδρύματα. [725]

9.1.2.7. Η Interpol

Η Ιντερπόλ (International Criminal Police Organization,) δηλαδή η Διεθνής αστυνομία, με αρχηγείο στη Λυών και 181 χώρες μέλη, συντονίζει τη δράση της με τις αστυνομίες των κρατών στον τομέα της ανταλλαγής πληροφοριών, της ανάπτυξης κοινής δράσης και την ανταλλαγή μεθόδων και καλών πρακτικών για την αντιμετώπιση διαφόρων κατηγοριών εγκλημάτων. Ειδικότερα για το έγκλημα σχετικά με την πληροφορική τεχνολογία η Ιντερπόλ συστήνει διεθνή μαθήματα για την απόκτηση ειδικών γνώσεων και παρέχει οδηγίες για τους

[721] Μαζάνης Χρήστος, (2014)
[722] Broadhurst Roderic (2006, ό.π.
[723] Περιλαμβάνονται σχεδόν όλα τα κράτη της ΕΕ όπως και χώρες φορολογικοί παράδεισοι όπως το Λίχτενσταϊν, οι Παρθένοι Νήσοι, οι Βερμούδες και τα Νησιά Κάιμαν. Την συμφωνία δεν έχουν υπογράψει οι ΗΠΑ, Κίνα και Ελβετία.
[724] http://www.sportandbusiness.gr/economia/item/37406-sto-pagkosmio-foroum-tou-oasa-gia-tin-katapolemisi-tis-forodiafygis-o-g-xardoyvelis
[725] Κουπαράνης Παναγιώτης (2014)

αστυνομικούς ερευνητές που εργάζονται πάνω σε αυτό το θέμα. Ακόμα υποστήριξε τη δημιουργία ομάδων εργασίας ειδικών σε τοπικό επίπεδο οι οποίες συναντώνται τακτικά για την ανταλλαγή καλών πρακτικών. Ιδιαίτερη έμφαση δόθηκε και στην αντιμετώπιση της πλαστογραφίας και παραχάραξης με τη δημιουργία ιστοσελίδας, για το Παγκόσμιο Σύστημα Ταξινόμησης της Πλαστογραφίας Καρτών, η οποία παρέχει στους - ανά - τον - κόσμο ειδικούς τη δυνατότητα να ενημερώνονται και να αποκτούν πληροφορίες που θα τους βοηθούν στις έρευνές τους. Στο σύστημα αυτό έχουν πρόσβαση και ειδικά στελέχη του τραπεζικού συστήματος, αρμόδια για τις χρεωστικές και πιστωτικές κάρτες, για ανταλλαγή πληροφοριών με τους ειδικούς της δίωξης σχετικά με απάτες. Με τον τρόπο αυτό αναδεικνύεται ο ρόλος της συνεργασίας δημόσιου και ιδιωτικού τομέα στον τομέα της πρόληψης και αντιμετώπισης του ηλεκτρονικο-οικονομικού εγκλήματος.[726]

9.1.3. Ελληνική νομοθεσία

Στην Ελληνική νομοθεσία δεν υπάρχουν ειδικές διατάξεις για τα ηλεκτρονικά εγκλήματα. Ο κύριος όγκος των περιπτώσεων, που έχουν διωχθεί για εγκλήματα που διαπράττονται γενικά με ηλεκτρονικούς υπολογιστές μέχρι σήμερα αντιμετωπίστηκαν με το Ν. 1805/1988 ο όποιος ενσωμάτωσε τα άρθρα 370Β και 386Α του ποινικού κώδικα. Το άρθρο 370 παρ.2 αφορά την παράνομη αντιγραφή και διείσδυση σε συστήματα και επικοινωνίες υπολογιστών και το άρθρο 386Α του Ποινικού Κώδικα για την απάτη με υπολογιστή, προβλέπει ότι «τιμωρείται ως έγκλημα διακινδύνευσης η πρόσβαση σε στοιχεία που έχουν αποθηκευτεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα επικοινωνιών»[727]. Συγκεκριμένα με το άρθρο 3 του νόμου 1805/1988 προστέθηκαν τρία νέα άρθρα στον Ποινικό Κώδικα, το άρθ. 370Β, 370Γ και 386Α. Σύμφωνα με το άρθ. 370Β του Ποινικού Κώδικα, «όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα ηλεκτρονικών υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι. Αν ο δράστης εργάζεται στην υπηρεσία του κατόχου των στοιχείων, όπως και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά τα ανωτέρω πράξη τιμωρείται με κάθειρξη μέχρι δέκα ετών».

Σύμφωνα με το άρθρο 370Γ παρ. 1 του Ποινικού Κώδικα, «όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα ηλεκτρονικών υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μηνών και με χρηματική ποινή εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών».

Σύμφωνα με τα άρθρα 386 και 386Α του Ποινικού Κώδικα, «όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλον τρόπο, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση

[726] Broadhurst Roderic (2006), ό.π.
[727] Λάζος Γρηγόρης (2001) σ. 73

τουλάχιστον δύο ετών. Επιβάλλεται δε κάθειρξη μέχρι δέκα ετών, αν ο υπαίτιος διαπράττει απάτες (κατά τον ανωτέρω τρόπο) κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσόν των πέντε εκατομμυρίων (5.000.000) δραχμών, ή, εάν ανεξαρτήτως της κατ' επάγγελμα ή κατά συνήθεια τέλεσης η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσόν των είκοσι πέντε εκατομμυρίων (25.000.000) δραχμών». Σύμφωνα με το άρθρο 13στ του Ποινικού Κώδικα, κατ' επάγγελμα τέλεση του εγκλήματος συντρέχει, όταν από την επανειλημμένη τέλεση της πράξης ή από την υποδομή που έχει διαμορφώσει ο δράστης με πρόθεση επανειλημμένης τέλεσης της πράξης προκύπτει σκοπός του δράστη για πορισμό εισοδήματος. Κατά συνήθεια τέλεση του εγκλήματος συντρέχει, κατά το ανωτέρω άρθρο του Ποινικού Κώδικα, όταν από την επανειλημμένη τέλεση της πράξης προκύπτει σταθερή ροπή του δράστη προς τη διάπραξη του συγκεκριμένου εγκλήματος ως στοιχείο της προσωπικότητας του δράστη.

Τα αδικήματα που σχετίζονται με τη χρήση των υπολογιστών αντιμετωπίζονται με το νόμο 2121/1993 για την πνευματική ιδιοκτησία, που περιέχονται και διατάξεις σχετικές με τα προγράμματα ηλεκτρονικών υπολογιστών, τις βάσεις δεδομένων και φωτογραφιών, όπως τροποποιήθηκε και εναρμονίσθηκε με την Οδηγία 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου[728]. Ακόμα, τα σχετικά με τη χρήση υπολογιστών αδικήματα αντιμετωπίζονται με το νόμο 3037/2002 για τον ηλεκτρονικό τζόγο, τον 2225/94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και τους νόμους 2246/1994[729] και 2774/1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στις τηλεπικοινωνίες, σε συνδυασμό με τον Ν. 2472/97 για την «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».[730]

Τα εγκλήματα του κυβερνοχώρου τελούνται με απαραίτητη προϋπόθεση τη χρήση τηλεπικοινωνιών, σταθερής ή κινητής τηλεφωνίας. Ο νόμος 2246/26-10-1994 ψηφίστηκε για την οργάνωση και εν γένει λειτουργία του τομέα τηλεπικοινωνιών και ρυθμίζει θέματα σχετικά με το Διαδίκτυο. Προσδιόριζε συγκεκριμένα ότι φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι τα φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού. Σύμφωνα με το άρθ. 2 παρ. 3 Ν. 2246/1994 συνιστάται η Εθνική Επιτροπή Τηλεπικοινωνιών, η οποία έχει τεχνικές, νομικές και προανακριτικές αρμοδιότητες, γνωμοδοτεί για την έκδοση των κωδίκων δεοντολογίας, επιβάλλει διοικητικά πρόστιμα και ελέγχει γενικώς την ομαλή και ορθή λειτουργία του τομέα τηλεπικοινωνιών. Εν μέρει αντικαταστάθηκε από το ν.2867/2000 για την Οργάνωση και λειτουργία του τομέα των τηλεπικοινωνιών εκτός από το τμήμα που αφορά την παροχή ταχυδρομικών υπηρεσιών και την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων.

Σύμφωνα με το άρθρο 1 του νόμου 2225/1994 ιδρύεται η Εθνική Επιτροπή Προστασίας Απορρήτου των Επικοινωνιών, της οποίας αποστολή είναι και η προστασία του απορρήτου της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης. Υπό τις προϋποθέσεις του νόμου 2225/1994 είναι δυνατή η παρακολούθηση ανταλλαγής ηλεκτρονικής αλληλογραφίας (e-mail). Π.χ. ο Α εκβιάζει τον Β με την αποστολή e-mail, ο Β καταγγέλλει την εκβίαση στην αστυνομία και η αστυνομία ζητά από τον πάροχο (Internet

[728] Χρυσοπούλου Σοφία & Λεφάκης Παναγιώτης (2015)
[729] Καπαρδή Μαρία, Καπαρδής Ανδρέας, Κουράκης Νέστορας (2001), σ. 344
[730] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2014)

Service Provider) να παρακολουθήσει την ανταλλαγή e-mail. Ο πάροχος δεν δικαιούται να επικαλεστεί το απόρρητο των επικοινωνιών.[731]

Σύμφωνα με το νόμο 2774/1999 σε συνδυασμό με τον 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) προβλέπονται ποινικές κυρώσεις για όποιον προβαίνει σε διασύνδεση αρχείων χωρίς να τη γνωστοποιήσει στην αρμόδια αρχή και για όποιον χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών, ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο.

Αυτή είναι μία γενική διάταξη, που αποσκοπεί πράγματι στην προστασία προσωπικών δεδομένων, αλλά δεν καλύπτει τα γνήσια εγκλήματα κυβερνοχώρου, αφού η διασύνδεση αρχείων ή η επέμβαση σε δεδομένα, ή η διάδοση δεδομένων, η επεξεργασία και ανακοίνωσή τους μπορεί να πραγματοποιηθεί και χωρίς τη βούληση και γνώση του κατόχου ηλεκτρονικού υπολογιστή ή του χρήστη του Διαδικτύου. Π.χ. ένας κατευθυνόμενος από το δράστη ηλεκτρονικός «ιός» (virus) προσβάλλει το σύστημα και χρησιμοποιεί όλες τις ηλεκτρονικές διευθύνσεις (e-mail) φίλων, γνωστών του κ.λπ., που έχει αποθηκεύσει ο ανυποψίαστος κάτοχος και χρήστης του Διαδικτύου, προκειμένου να αποστείλει ο δράστης σε αυτούς ευαίσθητα προσωπικά δεδομένα. Η χρήση συγκεκριμένων κωδίκων για τη μετατροπή δεδομένων με σκοπό την ανάγνωσή τους αποσκοπεί στην προστασία των δεδομένων αυτών (κρυπτογραφία). Με την κρυπτογραφία αποτρέπεται δηλαδή η πρόσβαση σε δεδομένα από μη εξουσιοδοτημένα πρόσωπα. Προς τούτο έχει διαμορφωθεί ένας ιδιαίτερος επιστημονικός κλάδος, η διαχείριση ασφάλειας δικτύων.

Άλλοι νόμοι και προεδρικά διατάγματα σχετικά με το ηλεκτρονικό έγκλημα αποτελούν:

- Ν. 2819/2000, «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων».
- Ν. 3115/2003, «Αρχή Διασφάλισης του απορρήτου των επικοινωνιών».
- Ν. 3431/2006, «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις».
- Ν. 3471/2006, «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».
- Ν. 3917/2011, «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».
- Π.Δ. 150/2001, «Ηλεκτρονικές Υπογραφές».
- Π.Δ. 131/2003, «Ηλεκτρονικό εμπόριο κλπ. - Υπηρεσίες της Κοινωνίας της Πληροφορίας».
- Π.Δ. 47/2005, «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».[732]

Το νομοσχέδιο για την εγκληματικότητα στο διαδίκτυο και τους ηλεκτρονικούς υπολογιστές, με το οποίο κυρώνεται η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον

[731] Αγγελής Ιωάννης (2000), σ. 680
[732] Νομοθεσία για το Ηλεκτρονικο Έγκλημα (2015)

Κυβερνοχώρο βρίσκεται[733] στο τελικό στάδιο ολοκλήρωσης από το ελληνικό Υπουργείο Δικαιοσύνης.

Όπως αναφέρεται στην ανακοίνωση του υπουργείου Δικαιοσύνης, με τις διατάξεις του νομοσχεδίου:

1. Εναρμονίζονται οι εθνικές νομοθεσίες σε ότι αφορά την ποινικοποίηση συγκεκριμένων μη νομίμων συμπεριφορών, όπως είναι η παράνομη πρόσβαση σε σύστημα υπολογιστή, η διάδοση υλικού παιδικής πορνογραφίας και η τέλεση αδικημάτων μέσω ηλεκτρονικού υπολογιστή. Η ποινική αντιμετώπιση για τα εγκλήματα αυτά στο διαδίκτυο, θα καλύπτεται από την ποινική νομοθεσία, όπως ήδη ισχύει. Επίσης το απόρρητο στο διαδίκτυο θα αίρεται μόνο στις περιπτώσεις που προβλέπει η ισχύουσα ποινική νομοθεσία, χωρίς πρόσθετες ειδικές διατάξεις.

2. Συμπληρώνονται οι δικονομικές διατάξεις, που ισχύουν στα συμβαλλόμενα μέρη ώστε να βελτιωθεί η δυνατότητα των αστυνομικών αρχών να διεξάγουν τις έρευνές τους σε «πραγματικό χρόνο» (real time) και να διασφαλίζουν και συλλέγουν τα απαραίτητα αποδεικτικά στοιχεία στην εθνική επικράτεια πριν αυτά χαθούν οριστικά.

3. Προσαρμόζονται οι κανόνες, που περιέχονται στις συμβάσεις του Συμβουλίου της Ευρώπης, σχετικά με την έκδοση και τη δικαστική συνδρομή.

4. Με τις διατάξεις του νομοσχεδίου θα τιμωρούνται οι κάθε είδους παρεμβολές σε δεδομένα και συστήματα υπολογιστή και τα διενεργούμενα μέσω συστημάτων ηλεκτρονικών υπολογιστών αδικήματα. Ιδιαίτερα αυστηρή αντιμετώπιση γίνεται στα μέσω του διαδικτύου τελούμενα αδικήματα παιδικής πορνογραφίας.

5. Με τις δικονομικές διατάξεις του νομοσχεδίου διευκολύνεται η διακρίβωση των αδικημάτων που τελούνται μέσω του διαδικτύου με τη διασφάλιση της διατήρησης και την αποτροπή καταστροφής των ιχνών και αποδεικτικών στοιχείων που καταγράφονται, στο διαδίκτυο, κατά την τέλεση των αδικημάτων αυτών.

Συγκεκριμένα, ο πάροχος (διαδικτυακής σύνδεσης) θα είναι υποχρεωμένος να προβαίνει άμεσα στις απαραίτητες τεχνικές διαδικασίες που απαιτούνται για την αποτροπή καταστροφής των ιχνών και των αποδεικτικών στοιχείων αυτών και να αναφέρει άμεσα στις εισαγγελικές αρχές και στην ΑΔΑΕ για τις δικές τους ενέργειες.

6. Τέλος, με τις ρυθμίσεις του σχεδίου σε συνδυασμό με εκείνου για το απόρρητο των επικοινωνιών, που ταυτόχρονα προωθεί το υπουργείο Δικαιοσύνης, θα διασφαλίζεται ο πολίτης από αδικήματα και επιθέσεις στην προσωπικότητά του, που γίνονται μέσω των σύγχρονων ηλεκτρονικών συστημάτων.[734]

Παρόλα αυτά η συνθήκη δεν είχε ακόμα ψηφιστεί από την Ελληνική Βουλή κατά το χρόνο συγγραφής της παρούσας διατριβής (Απρίλιος 2015)[735].

Όσον αφορά την καταπολέμηση της παιδικής πορνογραφίας ισχύει ο νόμος 3625/2007, που περιλαμβάνει:

1. Την κύρωση και εφαρμογή του Προαιρετικού Πρωτοκόλλου στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική

[733] βλ. σχετική Ερώτηση στη Βουλή, τον Αύγουστο του 2013 των βουλευτών Ασημίνα Ξηροτύρη-Αικατερινάρη και Ιωάννη Πανούση, στο http://www.xirotiri.gr/koinobouleitikos-elegxos/erotiseis/ake/kirosi-tis-simbasis-tis-boudapestis-kai-tou-prosthetou-protokollou.html, ανακτήθηκε Νοέμβριος 2014

[734] Πηγή Εφημερίδα Ελεύθερος Τύπος, http://www.e-tipos.com/newsitem?id=27413 , 28/2/(2008)

[735] Ο συγγραφέας συμβουλεύτηκε και τον δικηγόρο κο. Μπουρμά ο οποίος του επιβεβαίωσε ότι η κύρωση της Σύμβασης και η ψήφιση του σχετικού νομοσχεδίου ακόμα εκκρεμεί.

πορνογραφία, που ενσωματώνεται στο εσωτερικό μας Δίκαιο και προσαρτάται στη Διεθνή Σύμβαση για τα Δικαιώματα του Παιδιού, στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών (άρθρα 17).

2. Μια σειρά νέων διατάξεων, με τις οποίες εναρμονίζεται η Ελληνική νομοθεσία με το περιεχόμενο του παραπάνω πρωτοκόλλου και με άλλα διεθνή νομοθετήματα, για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών και της παιδικής πορνογραφίας, σε μια σειρά κατηγοριών (σεξουαλικός τουρισμός, ασέλγεια μεταξύ συγγενών, παιδική πορνογραφία στο διαδίκτυο, διανομή και χρήση υλικού παιδικής πορνογραφίας μέσω συστήματος Η/Υ ή με τη χρήση Διαδικτύου, προστασία της ιδιωτικής ζωής του ανηλίκου κλπ.).

3. Ορισμένες νέες ρυθμίσεις για τα προσωπικά δεδομένα, στην περίπτωση εγκλημάτων κατά της κοινωνίας και τη λειτουργία των καμερών κατά τη διάρκεια συγκεντρώσεων, εφόσον επίκειται σοβαρός κίνδυνος για τη δημόσια ασφάλεια και μόνον κατόπιν εντολής εκπροσώπου της εισαγγελικής αρχής.

Η εφαρμογή των παραπάνω διατάξεων άρχισε από τις 24/12/2007, με τη δημοσίευση του νόμου 3625/2007 στην Εφημερίδα της Κυβερνήσεως (Τεύχος Ά, Αρ. φύλλου 290, 24/12/07). Σύμφωνα με το Άρθρο 14 του Προαιρετικού Πρωτοκόλλου, η εφαρμογή του αρχίζει ένα μήνα αργότερα, δηλαδή στις 24/01/2008.[736]

9.1.4. Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος αποτελεί αυτοτελή υπηρεσία της Ελληνικής Αστυνομίας με αντικείμενο «τη διερεύνηση, εξιχνίαση και δίωξη εγκλημάτων σε βάρος του δημοσίου και την Εθνικής Οικονομίας ή έχουν τα χαρακτηριστικά του οργανωμένου οικονομικού εγκλήματος, όπως και οποιοδήποτε έγκλημα διαπράττεται με τη χρήση του διαδικτύου».

Η δίωξη οικονομικού και ηλεκτρονικού εγκλήματος της ΕΛ.ΑΣ. έχοντας πρόσβαση στα αρχεία της αστυνομίας ή άλλων υπηρεσιών και φορέων, ανταλλάσσει στοιχεία με υπηρεσίες του Υπουργείου Οικονομικών. Χρησιμοποιεί λογισμικό για την ανάλυση εγκληματολογικών πληροφοριών, τη μελέτη και διερεύνηση σοβαρών υποθέσεων οικονομικού και ηλεκτρονικού εγκλήματος στην Ελλάδα. Μετά τη συλλογή προανακριτικού υλικού ενημερώνει και τις φορολογικές αρχές για την επιβολή των αντίστοιχων διοικητικών παραβάσεων.[737]

9.2. Δυσκολίες Αντιμετώπισης – «Αδυναμία ικανών φυλάκων»

Υπάρχουν μερικές ιδιαιτερότητες του ηλεκτρονικού εγκλήματος που το καθιστούν ένα πολύπλοκο θέμα μελέτης. Αρχικά, είναι ένα σχετικά νέο φαινόμενο για τους φορείς του επίσημου κοινωνικού ελέγχου ενώ πολλοί από αυτούς δεν έχουν ακόμα εξοικειωθεί με αυτό. Αφετέρου, οι ορισμοί του ηλεκτρονικού εγκλήματος δεν είναι σαφείς και ομοιόμορφοι στις διάφορες χώρες. Ακόμα χαρακτηρίζεται από μια απόσταση μεταξύ του δράστη και του θύματος που μπορεί να υπερβαίνει τα εθνικά σύνορα μιας χώρας. Αυτό εγκυμονεί κινδύνους και παρέχει εγκληματικές ευκαιρίες. Η μεγάλη κινητικότητα ατόμων, κεφαλαίων, πληροφοριών και ιδεών δημιουργεί νέες δυνατότητες για το έγκλημα και νέες προκλήσεις για τους φορείς του επίσημου κοινωνικού ελέγχου. Οι πιθανότητες της ανίχνευσης και η υποβολή καταγγελίας στην περίπτωση των ηλεκτρονικο-οικονομικών εγκλημάτων είναι πολύ

[736] Ευσταθίου Άννα (2008)
[737] Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (2014)

χαμηλότερες από τα περισσότερα παραδοσιακά εγκλήματα. Η φύση των στοιχείων είναι πολύ διαφορετική από τα παραδοσιακά εγκλήματα.

Οι δυσκολίες αντιμετώπισης του ηλεκτρονικο-οικονομικού εγκλήματος και λόγω του παγκόσμιου χαρακτήρα του ηλεκτρονικο-οικονομικού εγκλήματος, αποτελούν κατά κάποιο τρόπο «έλλειψη ικανών φυλάκων» που δημιουργούν το κατάλληλο σκηνικό εγκλήματος χωρίς την ύπαρξη αποτελεσματικού ελέγχου, καθιστώντας τον στόχο πιο ευάλωτο, αυξάνοντας την πιθανότητα επιτυχούς ολοκλήρωσης της δράσης και συνακόλουθα την ελκυστικότητα της ευκαιρίας για τον δράστη.

Η έλλειψη «ικανών φυλάκων» στον ψηφιακό χώρο έχει λοιπόν τη μορφή αδυναμίας επιβολής του νόμου από πλευράς διωκτικών αρχών, της έλλειψης ενημέρωσης των χρηστών για τα μέτρα προστασίας απέναντι στους ψηφιακούς κινδύνους, τα ευάλωτα ψηφιακά συστήματα υπολογιστών, της απροθυμίας των θυμάτων για καταγγελία των εγκλημάτων στις διωκτικές αρχές.[738]

Όπως προκύπτει και από την παγκόσμια έρευνα της PricewaterhouseCoopers (PwC), παρατηρείται απροθυμία συνεργασίας με τις διωκτικές αρχές. Μόλις το 4,5% αυτών που δήλωσαν ότι έχουν πληγεί από οικονομικό έγκλημα προέβησαν σε δικαστικά μέτρα ή ειδοποίησαν τις αρχές για υπαιτίους εντός(9%) ή εκτός της εταιρίας (14%).[739]

Αυτές οι δυσκολίες περιγράφονται παρακάτω.

9.2.1. Ο Παγκόσμιος χαρακτήρας του ηλεκτρονικού εγκλήματος

Η παγκοσμιοποίηση της πληροφορικής τεχνολογίας παρέχει τη δυνατότητα στις εγκληματικές δραστηριότητες να είναι διεθνείς μη γνωρίζοντας όρια και σύνορα.

Οι κυβερνήσεις αντιμετωπίζουν πρόβλημα να ελέγξουν την ηλεκτρονική συμπεριφορά στα σύνορα τους, πόσο μάλλον εκτός αυτών. Ο αχανής χαρακτήρας του παγκόσμιου διαδικτυακού ιστού καθιστά το νομοθετικό του έλεγχο σχεδόν απίθανο. Άλλωστε οι τεχνολογικές εξελίξεις είναι τόσο γρήγορες που πάντα βρίσκονται πιο μπροστά σε σχέση με τις όποιες νομοθετικές προσπάθειες[740].

Ο παγκόσμιος και ανώνυμος χαραχτήρας του ηλεκτρονικού εγκλήματος, η ευρηματικότητα, η χρήση ισχυρών δικτύων Η/Υ δίνει τη δυνατότητα στον οργανωμένο εγκληματία να προσβάλλει τα εθνικά δίκτυα πληροφοριών και ασφάλειας.[741] Συχνά και το κόστος της δίωξης είναι δυσανάλογα μεγάλο.

Το ψηφιακό χάσμα καθιστά τις αναπτυσσόμενες χώρες λιγότερο ικανές στον τομέα υποστήριξης ψηφιακών τεχνολογιών για να αντιμετωπίσουν απειλές. [742]

Πρόσθετα προβλήματα ανακύπτουν από τη δυσκολία άσκησης της εθνικής κυριαρχίας πάνω στην κυκλοφορία κεφαλαίων και πληροφοριών. Από τις διασυνοριακές μεταφορές μέσω του διαδικτύου προκύπτουν θέματα νομικής δικαιοδοσίας για το που έχει διαπραχθεί το έγκλημα και ποια χώρα είναι αρμόδια να δικάσει την υπόθεση. Για παράδειγμα η υπόθεση κατά την οποία ένα ηλεκτρονικό μήνυμα που φαίνεται να ξεκινά από την Ελλάδα περιέχει παραπλανητικές πληροφορίες για την εξέλιξη της τιμής μιας μετοχής στο χρηματιστήριο του Λονδίνου, στην πραγματικότητα μπορεί να στέλνεται από τη Ρωσία. Επιπρόσθετα υπάρχει έλλειψη διεθνούς συναίνεσης για το τι συνιστά εγκληματική συμπεριφορά. Αυτό που

[738] Grabosky Peter & Walkley Sascha (2007), σσ. 358-375
[739] PwC, PricewaterhouseCoopers, (2014)
[740] Αγγελής Ιωάννης (2000), σσ., 675-686
[741] Wahlert Glenn (1998)
[742] Broadhurst Roderic (2006)

αποτελεί έγκλημα στο Μπαγκλαντές, προστατεύεται ως έννομο αγαθό στην Φιλαδέλφεια των ΗΠΑ.[743]

Όπως εξετάστηκε και παραπάνω, ο κυβερνοχώρος παρουσιάζει ασυνέχεια σε σχέση με τον γεωγραφικό χώρο.[744] Ο τόπος ή η χώρα διάπραξης του εγκλήματος δεν είναι απαραίτητο να συμπίπτει με τη χώρα διαμονής του δράστη. Ένας δράστης από την Ρουμανία μπορεί να έχει εγκαταστήσει βλαβερό λογισμικό και να ελέγχει υπολογιστές και δίκτυα (π.χ. μέσω botnets) που βρίσκονται στις ΗΠΑ και από εκεί να εξαπολύει επιθέσεις (στέλνοντας spam) σε όλο τον κόσμο.[745]

9.2.2. Προβλήματα Νομικής αντιμετώπισης

Παρά τη θέσπιση ή τον εκσυγχρονισμό των νομοθεσιών τους μέχρι τη δεκαετία του΄90, οι βιομηχανικά αναπτυγμένες χώρες δεν κατάφεραν να περιορίσουν το ηλεκτρονικό έγκλημα. Ο στόχος των νομοθετών για μείωση του χάσματος μεταξύ νόμου και τεχνολογίας δεν έχει επιτευχθεί επειδή:

1. Δεν υπάρχει σαφής και ενιαίος ορισμός για το ηλεκτρονικό έγκλημα.
2. Σε πολλές νομοθεσίες οι νόμοι είναι ανεπαρκείς για να καλύψουν την φύση των εγκλημάτων που διαπράττονται.
3. Πολλές χώρες δεν έχουν κυρώσει διεθνείς συμβάσεις για την αντιμετώπιση των ψηφιακών εγκλημάτων με αποτέλεσμα την έλλειψη εναρμονισμού των εθνικών νομοθεσιών.[746]
4. Τα θύματα επιχειρήσεις δεν καταγγέλλουν εύκολα τις παραβιάσεις που τους γίνονται κυρίως για λόγους δυσφήμησης, χρονοβόρων διαδικασιών, δυσκολίας απόδειξης αλλά και για να μην συνεχίσουν να δέχονται επιθέσεις.[747]
5. Μεγάλος «σκοτεινός αριθμός» ηλεκτρονικο-οικονομικής εγκληματικότητας, ακόμα και όταν τα θύματα καταγγέλλουν το έγκλημα οι επίσημες στατιστικές απεικονίζουν περισσότερο τις προτεραιότητες της αστυνομίας και λιγότερο την πραγματική έκταση του εγκλήματος.[748]
6. Οι ενάγοντες συχνά δεν είναι ειδικευμένοι στους Η/Υ.
7. Οι δικαστές δεν έχουν χρήσιμα νομικά προηγούμενα ως οδηγό των αποφάσεων τους.[749]
8. Οι δικηγόροι από τη μεριά τους ούτε αυτοί έχουν σχετικές γνώσεις και εμπειρία.[750]
9. Υπάρχουν μεγάλες διαφορές στη σχετική νομοθεσία μεταξύ των διαφόρων χωρών. Αρκετές χώρες, ιδιαίτερα της Ανατολικής Ευρώπης και της Ασίας διαθέτουν ελλιπή ή χαλαρότερη νομοθεσία σχετικά με τα ηλεκτρονικά εγκλήματα. Ειδικά η Ρωσία έχει αναφερθεί ως χώρα που κατά το παρελθόν έχει επιδείξει ανοχή σε κυβερνοεγκληματίες, λόγω διαφθοράς (κυρίως δωροδοκίας) κρατικών λειτουργών.[751]
10. Η φύση των ποινών διαφέρει από χώρα σε χώρα και από πολιτεία σε πολιτεία (ειδικά για τις ΗΠΑ).[752]
11. Προβλήματα από παραβιάσεις της προσωπικότητας και των δικαιωμάτων του ατόμου.

[743] Grabosky Peter.N. (1998)
[744] βλ. Yar Majid (2005), ό.π.
[745] Kigerl Alex (2012)
[746] Smith Russell, Grabosky Peter & Urbas Gregor. (2004), σ.63
[747] Λάζος Γρηγόρης (2001), ό.π. σσ. 212-213
[748] Broadhurst Roderic (2006), σσ. 408-433.
[749] Λάζος Γρηγόρης (2001), ό.π. σσ. 212-213
[750] Λάζος Γρηγόρης (2001), σσ. 211 – 220
[751] Βλ. αναφορά στον Barham (2008) που γίνεται από τον Kigerl Alex (2012), ό.π.
[752] Pocar Fausto (2004), ό.π.

12. Τα νέα είδη εγκληματικότητας, όπως η επιθέσεις με ιούς, η DoS (Denial of Service, άρνηση υπηρεσίας), αντιμετωπίζονται από πολλές χώρες με «τρομο-νόμους» ειδικά μετά την «11η Σεπτεμβρίου».

Τα τελευταία χρόνια οι κυβερνήσεις των δυτικών χωρών, λόγω και των οικονομικο – πολιτικών εξελίξεων, επιδεικνύουν μεγαλύτερη εγρήγορση σε κάποιες κατηγορίες ηλεκτρονικών και ηλεκτρονικο-οικονομικών εγκλημάτων. Στο πλαίσια αυτό, έχουν θεσπίσει νόμους και διαθέσει πόρους για την δίωξη ατόμων που διακινούν και κατέχουν υλικό παιδικής πορνογραφίας ή για περιπτώσεις παραβίασης πνευματικών δικαιωμάτων και ψηφιακής πειρατείας.[753]

9.2.3. Αδυναμίες των διωκτικών και δικαστικών αρχών για την άσκηση δίωξης

Ο εντοπισμός, η σύλληψη, η ποινική δίωξη και η καταδίκη των δραστών αποτελεί συχνά δύσκολη υπόθεση. Υπάρχει η δυσκολία καθορισμού της χώρας που είναι αρμόδια για την άσκηση της δίωξης, ακόμα κι όταν αυτό ξεκαθαριστεί έπειτα απαιτείται η συνεργασία των υπόλοιπων χωρών για την συγκέντρωση στοιχείων και την έκδοση του δράστη. Εκτός αυτού υπάρχει και η δυσκολία εντοπισμού, επισήμανσης και αναγνώρισης του δράστη, επειδή υπάρχουν πολλοί τρόποι απόκρυψης της πραγματικής ταυτότητας κάποιου μέσω τεχνικών κρυπτογράφησης, χρήσης διακομιστών μεσολάβησης (proxy servers) που κρύβουν την αληθινή IP (Internet Protocol address), χρήση ψεύτικου ονόματος, υπηρεσίες αποστολής ανώνυμων email κλπ. [754]

Η αστυνομική διερεύνηση του ηλεκτρονικο-οικονομικού εγκλήματος απαιτεί άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Τα στελέχη της αστυνομίας, των δικαστικών αρχών - εισαγγελία, δικαστές - αλλά και οι δικηγόροι, δεν έχουν πάντοτε την ικανότητα να απαντήσουν στο ψηφιακό έγκλημα, δεν διαθέτουν τις απαραίτητες γνώσεις, εμπειρία και εξοικείωση με την τεχνολογία της πληροφορικής, δεν έχουν το λεγόμενο «επίπεδο άνεσης». Αποτέλεσμα αυτών είναι οι εισαγγελείς να ασκούν την ποινική δίωξη βασιζόμενοι στα όσα αναγράφονται στην μήνυση ή το διαβιβαστικό της διωκτικής αρχής[755] και οι δικαστές να ερμηνεύουν τους ποινικούς νόμους με τη παραδοσιακή νομική.

Ένα άλλο σημείο που εγείρει δυσκολίες αποτελεί η απόκτηση των απαραίτητων αποδεικτικών στοιχείων. Το αντικείμενο του εγκλήματος και τα αποδεικτικά στοιχεία μπορεί να βρίσκονται αποθηκευμένα σε πολλούς υπολογιστές που βρίσκονται σε διάφορες χώρες. Πολλές φορές απαιτείται η κατάσχεση από την αστυνομία ολόκληρων υπολογιστικών συστημάτων και διερεύνηση σκληρών δίσκων μεγέθους αρκετών terabyte, πράγμα που απαιτεί ατελείωτες ανθρωποώρες και τεράστια δαπάνη. [756]

Συχνά τίθεται και ζήτημα παραβίασης ατομικών δικαιωμάτων κατά τη προσπάθεια των διωκτικών αρχών να συγκεντρώσουν αποδεικτικά στοιχεία. Ακόμα και όταν οι διωκτικές αρχές καταφέρνουν να εντοπίσουν τα ίχνη κάποιων που χρησιμοποιούν ιστοσελίδες με εγκληματικό π.χ. παιδοφιλικό περιεχόμενο, πώς θα μπορέσουν να διακρίνουν τον κοινό εγκληματία από τον αθώο εγκληματολόγο που πραγματοποιεί την έρευνα του για το φαινόμενο; [757]

Έχει σημειωθεί ακόμα και το φαινόμενο οι δικαστές να τιμωρούν το εργαλείο του εγκλήματος, τον Η/Υ διατάσσοντας την φυσική καταστροφή του, ενώ στα άτομα – δράστες να

[753] Smith Russell, Grabosky Peter & Urbas Gregor. (2004), σ.85
[754] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σσ.60-62
[755] Κολιώνη Κωνσταντίνα (2006), σ.57
[756] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σ.62
[757] Grabosky Peter (1998)

επιβάλλουν κυρίως χρηματικές ποινές (πρόστιμα, αποζημιώσεις), υποχρεωτική κοινοτική εργασία ή ψυχιατρική θεραπεία σε νοσηλευτικά ιδρύματα[758].

Συνηθέστερες δυσκολίες για την άσκηση ποινικής δίωξης από τις δικαστικές αρχές συνιστούν: η έλλειψη αρκετών αποδεικτικών στοιχείων, η αδυναμία τεκμηρίωσης της πρόθεσης, η έλλειψη αρμοδιότητας, που ανήκει σε αρχές άλλης χώρας, άγνωστος ή ανήλικος δράστης, έλλειψη μαρτύρων κλπ.[759]

Οι μάρτυρες δεν είναι εύκολο να ταξιδέψουν για να παραστούν σε δικαστήρια ξένων χωρών.

Ακόμα κάποια από τα θύματα δεν αντιλαμβάνονται καν ότι έχουν δεχθεί κάποιου είδους επίθεση, όπως οι περιπτώσεις ψεύτικων διαδικτυακών εράνων ή όταν το αντιλαμβάνονται ο δράστης πλέον έχει σβήσει τα ίχνη του και εξαφανιστεί.

Πολλές από τις περιπτώσεις διαδικτυακής απάτης έχουν να κάνουν με πολύ μικρά ποσά. Πρόκειται για απάτες τύπου «σαλάμι» σύμφωνα με τις οποίες το συνολικό κέρδος για τον απατεώνα προέρχεται από την εξαπάτηση πολλών, αλλεπάλληλων θυμάτων. Με τον τρόπο αυτό «επιμερίζεται» το κόστος της απάτης σε μικρότερα ποσά, έτσι ώστε δεν συμφέρει τα θύματα να κάνουν μηνύσεις επειδή τα δικαστικά έξοδα υπερβαίνουν τα απολεσθέντα λόγω απάτης ποσά.[760]

Ακόμα και όταν κάποιος καταδικάζεται για ψηφιακό έγκλημα η ποινή είναι σχετικά ελαφριά εφόσον τα εγκλήματα αυτά δεν περιέχουν φυσική βία ή άμεση επαφή με το θύμα και στους δράστες αναγνωρίζεται συχνά κάποιο ελαφρυντικό, όπως: το νεαρό της ηλικίας, η συνεργασία με την αστυνομία, ο πρότερος έντιμος βίος και οι πολλές πιθανότητες επανένταξης.[761]

Σε επίπεδο φυσικής φύλαξης, η αδυναμία των αρχών συνίσταται στο ότι δεν θα μπορούσε να τοποθετηθεί και από ένας αστυνομικός σε κάθε υπολογιστή ή ίντερνετ καφέ. Όπως όμως εξετάστηκε παραπάνω, θα μπορούσαν να τοποθετηθούν φυσικοί ή ψηφιακοί επιτηρητές χώρου.

9.2.4. Δυσκολίες στη δίωξη του ηλεκτρονικο-οικονομικού εγκλήματος σε σχέση με το παραδοσιακό.

Η απόδειξη διάπραξης του εγκλήματος ή ακόμα και κατοχής παράνομου υλικού είναι δυσκολότερη από αυτή των παραδοσιακών εγκλημάτων, λόγω των παρακάτω παραγόντων:

1. Έλλειψη ορατότητας των αποδεικτικών στοιχείων του εγκλήματος, επειδή αυτά είναι αποθηκευμένα και κωδικοποιημένα στα αποθηκευτικά μέσα των υπολογιστών.

2. Μεταμφίεση του εγκλήματος. Παραποίηση των αποδείξεων, κάλυψη των ιχνών.[762]

3. Κάλυψη των δραστών με την ανωνυμία που τους προσφέρει η χρήση των δικτύων και ειδικά του διαδικτύου.[763]

3. Εξάλειψη των αποδείξεων. Με προγράμματα διαγράφονται τα δεδομένα, τα ίχνη, οι αποδείξεις που κρυπτογραφούνται και κωδικοποιούνται.[764]

[758] Dreyfus Suelette (1998)
[759] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σσ.83, Βλ. Διάγραμμα 9 στον Πίνακα διαγραμμάτων.
[760] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σ.60
[761] Smith Russell, Grabosky Peter & Urbas Gregor (2004), σ.65
[762] McClure Stuart & Scambray Joel (1999)
[763] Kigerl Alex (2012)
[764] Sieber Ulrich. (1986), σσ.139-142.

4. Ύπαρξη μεγάλου αριθμού δεδομένων. Πολυπλοκότητα των ενεργειών του δράστη που έχει εμπειρία και ειδικές γνώσεις. Ο χάκερ μπορεί κλέψει όσα δεδομένα θέλει ή μπορεί να διαβάσει.[765]

Σύμφωνα με τους υπεύθυνους του τμήματος δίωξης ηλεκτρονικού εγκλήματος της Θεσσαλονίκης οι δυσκολίες στη δίωξη τέτοιων εγκλημάτων και η έκταση που έχει λάβει το φαινόμενο οφείλονται στα εξής αίτια:

- Το Ίντερνετ είναι αχανές
- Ελλιπή μέτρα ασφάλειας
- Μη εναρμονισμένη νομοθεσία μεταξύ των κρατών
- Περιορισμένες γνώσεις χρηστών σε θέματα ασφάλειας
- Ευκολία διάπραξης εγκλημάτων
- Πεποίθηση του δράστη περί της ύπαρξης ανωνυμίας
- Δύσκολος εντοπισμός των δραστών (γεγονός που οφείλεται στην δυσκολία εντοπισμού και ανάλυσης των ψηφιακών ιχνών που αφήνουν οι δράστες).[766]

[765] Λάζος Γρηγόρης, ό.π., σσ. 219-220.

[766] http://www.saferinternet.gr/Portals/0/docs/conference_speeches/Antonis_Papantoniou.pdf, Απρίλιος (2008)

ΚΕΦΑΛΑΙΟ 10. ΠΡΟΛΗΨΗ ΚΑΙ ΕΛΕΓΧΟΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟ-ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΩΝ ΠΡΟΣΕΓΓΙΣΕΩΝ ΤΩΝ ΕΓΚΛΗΜΑΤΙΚΩΝ ΕΥΚΑΙΡΙΩΝ

Στο κεφάλαιο αυτό θα εξετάσουμε τους τρόπους αντιμετώπισης του ηλεκτρονικο-οικονομικού εγκλήματος σε επίπεδο πρόληψης και αποτροπής εφαρμόζοντας τις θεωρίες της περιβαλλοντικής εγκληματολογίας για τη δόμηση των «εγκληματικών ευκαιριών», δηλαδή προτείνονται τρόποι ενίσχυσης των «ικανών φυλάκων», «θωράκισης» του στόχου και αύξησης των πιθανοτήτων σύλληψης του δράστη. Όπως είδαμε, οι παραβάτες αποθαρρύνονται περισσότερο από την πιθανότητα σύλληψης και καταδίκης παρά από την μεγαλύτερη αυστηρότητα των ποινών.

Όπως ισχύει και στις παραδοσιακές μορφές εγκληματικότητας, η πρόληψη είναι η καλύτερη πολιτική. Η ενημέρωση των χρηστών για τους κινδύνους θυματοποίησης που διατρέχουν από πλημμελή συμπεριφορά στο διαδίκτυο μπορεί να αποδειχθεί πιο αποτελεσματική από την εστίαση στην καταστολή και στις ποινές.[767]

Ο έλεγχος και η αποτροπή του εγκλήματος στο πλαίσιο των «εγκληματικών ευκαιριών» απαιτούν τη διακρίβωση των συγκεκριμένων χαρακτηριστικών και των συνθηκών που συνδέονται με το ηλεκτρονικο-οικονομικό έγκλημα. Ο τρόπος με τον οποίο δομούνται οι εγκληματικές ευκαιρίες στο άμεσο περιβάλλον των δραστών, έπειτα η αναγνώριση και η εκτίμηση από αυτούς των συγκεκριμένων ευκαιριών που τους παρουσιάζονται εξετάζονται από τις βασικές θεωρίες για τη δόμηση των εγκληματικών ευκαιριών, την θεωρία των καθημερινών δραστηριοτήτων ρουτίνας (RAT), την θεωρία των εγκληματικών προτύπων και τη στρατηγική περιστασιακής πρόληψης του εγκλήματος που βασίζεται στη θεωρία της ορθολογικής επιλογής.[768]

Όπως αναφέρθηκε και παραπάνω[769] οι συγκεκριμένες θεωρίες, αν και αρχικά χρησιμοποιήθηκαν για τη μελέτη του παραδοσιακού εγκλήματος, έχουν πεδίο εφαρμογής στην μελέτη των σύγχρονων μη βίαιων μορφών εγκληματικότητας όπως το ηλεκτρονικο-οικονομικό έγκλημα, μετά όμως την απαραίτητη προσαρμογή τους

10.1. Η εφαρμογή της θεωρίας «καθημερινών δραστηριοτήτων (L-RAT) για την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος

Στο επίπεδο εφαρμογής η θεωρία **των καθημερινών δραστηριοτήτων** σε συνδυασμό με αυτή του τρόπου ζωής (L-RAT, Lifestyle - Routine Activities Theory) έχουν να συνεισφέρουν αρκετά για τον έλεγχο (πρόληψη και αντιμετώπιση) του ηλεκτρονικο-οικονομικού εγκλήματος.

Στην αρχική εκδοχή της θεωρίας RAT η εστίαση γίνεται στον τρόπο ζωής και τις καθημερινές δραστηριότητες των ατόμων, ενώ αργότερα ο Felson έδωσε περισσότερη έμφαση στο χώρο.[770] Η τοποθέτηση σε αυτή την βάση επιτρέπει τον έλεγχο του χώρου πιο εύκολα από ότι τον έλεγχο των ατόμων, τόσο σε επίπεδο εγκληματολογικής μελέτης όσο και σε επίπεδο κοινωνικής προληπτικής πολιτικής. Τα θύματα – στόχοι μπορούν να θωρακιστούν

[767] Bossler Adam & Holt Thomas (2013) και Jahankhani Hamid & Al-Nemrat Ameer (2011)
[768] Benson Michael L., Madensen Tamara D., & Eck John E. (2009), σσ. 175–194
[769] Βλ. το οικείο κεφάλαιο για την εφαρμογή των αντίστοιχων θεωριών στο ηλεκτρονικό και οικονομικό έγκλημα.
[770] Felson Marcus (1987)

και να γίνουν λιγότερο ελκυστικοί, η φύλαξη να αυξηθεί και να γίνει πιο αποτελεσματική, η προσφορά δραστών με κίνητρο και η εγκληματική ευκαιρία να μειωθεί, μέσω αποτελεσματικών προσπαθειών ελέγχου του χώρου.[771]

Γενικότερα στο ψηφιακό περιβάλλον η πιθανότητα εμφάνισης της εγκληματικής ευκαιρίας για κάποιον δράστη με κίνητρο μπορεί να μειωθεί, και συνακόλουθα η πιθανότητα αποκάλυψης του μπορεί να αυξηθεί, με την χρήση πιο **«ικανής φύλαξης»** σε τρία επίπεδα ελέγχου:

(1) Σε επίπεδο φυσικής φύλαξης και επίσημου κοινωνικού ελέγχου, μέσω της ενίσχυσης του ρόλου και της ικανότητας των υπηρεσιών δίωξης του εγκλήματος και των δικαστικών αρχών για να προστατεύουν αποτελεσματικά τους χρήστες από τους διαδικτυακούς κινδύνους. Στην κατεύθυνση αυτή μπορεί να γίνουν προσπάθειες μείωσης των αδυναμιών που παρουσιάζουν οι διωκτικές αρχές[772] ως προς:

α) τον εντοπισμό δραστών και αδικημάτων, με την ενίσχυση των αρχών δίωξης με εξειδικευμένο προσωπικό που θα έχει τις απαραίτητες γνώσεις και εξοπλισμό.

β) την άσκηση ποινικής δίωξης, με την επικαιροποίηση των εθνικών νομοθεσιών και εναρμονισμό τους με τις διεθνείς νομοθετικές προσπάθειες ώστε να καλύπτονται νομοθετικά κενά.[773]

(2) Σε επίπεδο κοινωνικής φύλαξης και ανεπίσημου κοινωνικού ελέγχου. Η «κοινωνική φύλαξη» αφορά τη συμβολή της παρουσίας ατόμων ή ομάδων στην αποτροπή της εγκληματικής δραστηριότητας μέσω της παρακολούθησης του χώρου ή της προστασίας που προσφέρουν. Στην περίπτωση των παραδοσιακών εγκλημάτων το ρόλο αυτό παίζουν οι γονείς, οι δάσκαλοι, οι φίλοι, ενώ στην περίπτωση του ψηφιακού χώρου αναλαμβάνουν συλλογικότητες δημόσιου ή ημι-δημόσιου χαρακτήρα, οργανισμοί ιδιωτικών δικτύων, επαγγελματίες πληροφορικής τεχνολογίας. Ακόμα, όπως αναφέρθηκε και παραπάνω, ο συγχρωτισμός με παραβατικές ομάδες αυξάνει την έκθεση των ατόμων σε κινδύνους θυματοποίησης, τους φέρνει σε εγγύτητα με πιθανούς δράστες, μειώνει την αποτρεπτική ικανότητα του ανεπίσημου ελέγχου και την πιθανότητα παροχής βοήθειας από φίλους. Στις περιπτώσεις αυτές τα άτομα μπορούν να συνεισφέρουν στην αυτο-προστασία τους και την αύξηση της ικανής φύλαξης τους αποφεύγοντας το συγχρωτισμό με τέτοιες ομάδες, δηλαδή την εμπλοκή των ιδίων με παράνομες ψηφιακές δραστηριότητες.[774]

(3) Σε επίπεδο θωράκισης, «σκλήρυνσης» του στόχου[775] με την ενίσχυση των φυσικών μέσων ασφάλειας, όπως τη χρήση αντιβιοτικών προγραμμάτων και ασπίδων προστασίας σε υπολογιστές, κινητά τηλέφωνα, «ταμπλέτες» για την αντιμετώπιση των χάκερ ή άλλων ψηφιακών εγκληματιών.[776] Όπως αναφέρουν οι Grabosky και Smith πολλά από τα ψηφιακά εγκλήματα τελούνται λόγω της απουσίας φυσικής φύλαξης με τη μορφή προγραμμάτων antivirus.[777]

Οι έρευνες εμφανίζουν μάλλον αντιφατικά συμπεράσματα σχετικά με την αποτελεσματικότητα της χρήσης προγραμμάτων προστασίας των υπολογιστών για την αποτροπή των επιθέσεων. Αντίθετα τα ερευνητικά ευρήματα συμφωνούν ως προς την

[771] Sherman Lawrence, Gartin Patrick & Buerger Michael (1989)
[772] Βλ. και παρακάτω τις αδυναμίες των διωκτικών και δικαστικών αρχών.
[773] Jahankhani Hamid & Al-Nemrat Ameer (2011), σσ. 181- 197
[774] Βλ. Zhang, 2001, όπως αναφέρουν οι Bossler, Adam & Holt Thomas. (2009)
[775] Βλ. και παρακάτω για την εφαρμογή της περιστασιακής πρόληψης του εγκλήματος για την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος.
[776] Jahankhani Hamid & Al-Nemrat Ameer (2011), ό.π.
[777] Βλ. Grabosky και Smith, 2001, όπως αναφέρουν οι Bossler Adam & Holt Thomas (2009)

αντίστοιχη αποτελεσματικότητα της ύπαρξης ειδικών γνώσεων και δεξιοτήτων από πλευράς χρηστών υπολογιστικών συστημάτων επειδή οι γνώσεις αυτές βοηθούν στην αναγνώριση και την αποφυγή της έκθεσής τους σε κινδύνους. [778]

Ουσιαστικό ρόλο στη μείωση της θυματοποίησής τους διαδραματίζει η ενίσχυση της ενημέρωσης και εκπαίδευσης των χρηστών για τους κινδύνους και της συνειδητοποίησης της ανάγκης λήψης μέτρων αυτοπροστασίας τους.[779]

Γενικά, παρά το γεγονός ότι η απόλυτη προστασία από τους ηλεκτρονικούς κινδύνους δεν είναι πρακτικά εφικτή[780], η παρουσία ικανών φυλάκων των στόχων του ηλεκτρονικο-οικονομικού εγκλήματος, μπορεί να επιτυγχάνεται μειώνοντας την ανωνυμία, τοποθετώντας διευθυντές ή «διαχειριστές», φυσικούς ή ψηφιακούς επιτηρητές χώρου, όπως διαχειριστές υπολογιστικών συστημάτων, ηλεκτρονικά μέσα παρακολούθησης χώρων και δραστηριοτήτων των υπαλλήλων μιας επιχείρησης, χρήση προγραμμάτων προστασίας υπολογιστών (αντιικά και τείχη προστασίας), γονεϊκό έλεγχο των δραστηριοτήτων των παιδιών (με φυσική παρουσία), ομάδες διαδικτυακών φυλάκων κλπ.[781]

Τα παραπάνω τρία επιμέρους στοιχεία της ικανής φύλαξης, ο επίσημος, ο ανεπίσημος κοινωνικός έλεγχος και η θωράκιση του στόχου δεν πρέπει να θεωρούνται αποτελεσματικά όταν λαμβάνονται μεμονωμένα και αποσπασματικά. Η ύπαρξη ή και η επιβολή του νόμου, αν και προσδιορίζει το πλαίσιο θεμιτής συμπεριφοράς, δεν αρκεί από μόνη της. Όμοια η ύπαρξη ομάδων επιτήρησης, ελέγχου και προστασίας, η ενημέρωση των χρηστών για την νομοθεσία και τη λήψη των κατάλληλων μέτρων ασφάλειας για την προστασία τους δεν επαρκεί. Αντίθετα απαιτείται συνδυασμός όλων των παραπάνω στοιχείων για την δόμηση μιας ικανής φύλαξης.[782]

10.2. Η εφαρμογή των «εγκληματικών προτύπων» στην αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος

Από την πλευρά της η θεωρία των **εγκληματικών προτύπων** μας προσφέρει την εξήγηση της κατανομής των εγκλημάτων, γιατί τα εγκληματικά γεγονότα έχουν την τάση να συγκεντρώνονται στο χώρο και το χρόνο και ότι οι εγκληματίες λαμβάνουν γνώση των ευκαιριών στη διάρκεια των νόμιμων ενασχολήσεων τους. Όπως είδαμε στην παρουσίαση της θεωρίας, οι δράστες κινούμενοι σε γνώριμους για αυτούς κόμβους και μονοπάτια επισημαίνουν και επιλέγουν τους πιθανούς στόχους τους κατά τη διάρκεια των νόμιμων καθημερινών ασχολιών τους και μάλιστα σχετικά κοντά στον τόπο κατοικίας τους. Τα μονοπάτια που χρησιμοποιούν οι δράστες οικονομικών εγκλημάτων για να κινούνται ανάμεσα στους κόμβους περιλαμβάνουν την επιχείρηση στην οποία εργάζονται και τα δίκτυά της που καθιστούν εφικτή την επικοινωνία με άλλους και την εκτέλεση των νόμιμων εργασιακών τους καθηκόντων και διαμορφώνουν το πρότυπο δραστηριοτήτων τους. Κατά την διάρκεια των καθημερινών επαγγελματικών ενασχολήσεων τους και της αλληλεπίδρασης τους με άλλους ανθρώπους (πελάτες, συνεργάτες κλπ.) οι δράστες, που μπορεί να είναι

[778] Holt Thomas J. & Bossler Adam (2013)
[779] Jahankhani Hamid & Al-Nemrat Ameer (2011)
[780] Jahankhani Hamid & Al-Nemrat Ameer (2011)
[781] Grabosky Peter & Walkley Sascha, (2007)
[782] Jahankhani Hamid & Al-Nemrat Ameer (2011), ό.π. Βλ. και Παράρτημα «ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΟΝΤΕΛΟ των Jahankhani & Al-Nemrat».

«εκμεταλλευτές της ευκαιρίας» ή «ανταποκρινόμενοι σε προβλήματα»[783], αντιλαμβάνονται και εκμεταλλεύονται τις εγκληματικές ευκαιρίες.

Έτσι για μια αποτελεσματικότερη αντιμετώπιση των ηλεκτρονικο-οικονομικών εγκλημάτων απαιτείται ο εντοπισμός και η επισήμανση των κόμβων, των μονοπατιών και των εγκληματικών ευκαιριών που παρουσιάζονται για τους πιθανούς δράστες. Μετά την επισήμανση ακολουθεί η εφαρμογή των ρυθμίσεων αυτών που θα εμποδίζουν την εμφάνιση των ευκαιριών δηλαδή την δυνατότητα των ατόμων να δρουν παρασιτικά τελώντας παράνομες πράξεις στο πλαίσιο της κατά τα άλλα νόμιμης απασχόλησης τους. Αν αλλάξει η δόμηση της ευκαιρίας, ώστε η εκμετάλλευσή της να είναι πιο ριψοκίνδυνη για τον δράστη, τότε είναι πιο πιθανό το συγκεκριμένο έγκλημα να μειωθεί. Στην κατεύθυνση αυτή θα βοηθήσει μια αυστηροποίηση των νομοθετικών ρυθμίσεων και η γνωστοποίηση της, η ενημέρωση και πληροφόρηση των επαγγελματιών αλλά και του ευρύτερου κοινού για τις παράνομες διαδικτυακές και οικονομικές συμπεριφορές, ο μεγαλύτερος εσωτερικός έλεγχος από πλευράς επιχειρήσεων και οργανισμός για τις ενέργειες των υπαλλήλων τους κατά την άσκηση των καθηκόντων τους.[784]

Όπως είδαμε παραπάνω, οι προσεγγίσεις των «εγκληματικών ευκαιριών» και ειδικότερα η πλευρά της περιστασιακής πρόληψης του εγκλήματος, η οποία στην ουσία εφαρμόζει τις απόψεις των περιβαλλοντικών θεωριών στην αντιμετώπιση του εγκληματικού γεγονότος, εστιάζουν στην αλλαγή των περιβαλλοντικών συνθηκών και την μείωση των εγκληματικών ευκαιριών και όχι στα χαρακτηριστικά του ατόμου.

10.3. Η εφαρμογή της «περιστασιακής πρόληψης του εγκλήματος» για την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος

Όπως πρότεινε ο Clarke, συνδυάζοντας την άποψη της ορθολογικής επιλογής, για τα οφέλη και τα κόστη, με την περιστασιακή πρόληψη του εγκλήματος**,** η αποτελεσματική άσκηση πρόληψης του εγκλήματος αποτελείται από μέτρα που συντείνουν στην εξάλειψη της εγκληματικής ευκαιρίας και σχετίζονται με την αντίληψη του δράστη για την προσπάθεια, το ρίσκο, τα οφέλη, τις ευκαιριακές προκλήσεις και τις εκλογικεύσεις που κάνει.[785]

Τα μέτρα πρόληψης θα πρέπει να έχουν στόχο:

α) συγκεκριμένα είδη εγκλήματος, όπως το ηλεκτρονικο-οικονομικό έγκλημα,

β) τη διαχείριση του άμεσου περιβάλλοντος με συστηματικό και διαρκή τρόπο,

γ) την αύξηση της πιθανότητας να εκλάβουν οι πιθανοί εγκληματίες τη διάπραξη του εγκλήματος ως υπερβολικά δύσκολη, κοπιαστική, ριψοκίνδυνη, μη δικαιολογήσιμη και κοστοβόρο διαδικασία[786].

Τα μέτρα θα πρέπει να κινούνται στις εξής κατευθύνσεις:

1. **Αύξηση της απαραίτητης προσπάθειας** για την διενέργεια του εγκλήματος. Αυτό μπορεί να επιτευχθεί με **θωράκιση του στόχου** - θύματος (target hardening), έλεγχο και παρεμπόδιση της πρόσβασης ή εκτροπή του από τον στόχο και τα απαραίτητα μέσα-εργαλεία τέλεσης του εγκλήματος. Βέβαια η απαγόρευση της πρόσβασης σε πιθανούς στόχους δεν

[783] "crisis responders" και "opportunity takers", Βλ. παραπάνω την διάκριση των τριών εγκληματικών προτύπων από τους Piquero και Weisburd ως προς την εγκληματική πορεία των δραστών του λευκού περιλαιμίου, στο Piquero Nicole & Weisburd David (2009), σσ. 153-171

[784] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626

[785] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626

[786] Goldstein Arnold P. (1994), σσ.121-122

αποτελεί πάντα εφικτή λύση επειδή θα μπορούσε να παρεμποδίσει την ομαλή άσκηση και των νόμιμων επαγγελματικών καθηκόντων. Για παράδειγμα δεν είναι δυνατό να εμποδιστεί η πρόσβαση του υπαλλήλου σε υπολογιστή ή η επαφή του με πελάτες γιατί αυτό αποτελεί εργαλείο στη διάρκεια της εργασίας του.[787] Θα μπορούσε όμως να περιοριστεί η πρόσβαση του συγκεκριμένου υπολογιστή σε τμήμα του δικτύου ή των αρχείων της επιχείρησης, ακόμα και στο διαδίκτυο για το κομμάτι εκείνο που δεν εμπίπτει στα καθήκοντα του υπαλλήλου.[788]

Πιο εφικτός στόχος της πρόληψης στο πλαίσιο της «θωράκισης» της άμυνας του στόχου – θύματος είναι αυτό της ενημέρωσής του για τους κινδύνους που διατρέχει λόγω της διαδικτυακής του συμπεριφοράς. Όπως είδαμε[789] υπάρχουν κάποιες συμπεριφορές των χρηστών του διαδικτύου, όπως το κατέβασμα παράνομων προγραμμάτων και αρχείων, οι διαδικτυακές συναλλαγές, το e-banking κλπ. που τους καθιστούν ευάλωτους στόχους, τους φέρουν σε «εγγύτητα» με πιθανούς δράστες και αυξάνουν την έκθεσή τους σε εγκληματικές ευκαιρίες. Κατά συνέπεια η άσκηση μιας αποτελεσματικής πολικής πρόληψης του ηλεκτρονικο-οικονομικού εγκλήματος θα πρέπει οπωσδήποτε να περιλαμβάνει εκστρατείες ενημέρωσης και διαπαιδαγώγησης των χρηστών (καταναλωτών, μαθητών, γονέων, δασκάλων, στελεχών) για τους πιθανούς κινδύνους στο διαδίκτυο, την ανάγκη τροποποίησης της καθημερινής τους διαδικτυακής συμπεριφοράς και τους κατάλληλους τρόπους αντιμετώπισης των κινδύνων, π.χ. χρήση προγραμμάτων προστασίας (αντιβιοτικών, ασπίδες/τείχη προστασίας, χρήση ασφαλών διακομιστών, μείωση της χρήσης πιστωτικών καρτών ή χρήση προπληρωμένων καρτών για τις ηλεκτρονικές τους συναλλαγές κλπ.[790] Με τον τρόπο αυτό η ενίσχυση των ικανών φυλάκων κάνει τον πιθανό στόχο πιο δυσκατάβλητο.

Τα μέτρα πρόληψης, που παρουσιάζονται παρακάτω και προτείνονται από διάφορους φορείς, όπως η Ευρωπαϊκή Ένωση με τα προγράμματα Safer Internet, οι υπηρεσίες δίωξης ηλεκτρονικού και οικονομικού εγκλήματος, οργανώσεις ή άλλοι ειδικοί, κινούνται ακριβώς σε αυτή την κατεύθυνση της ενημέρωσης και εκπαίδευσης του κοινού ώστε να καθίσταται ως λιγότερο ευάλωτος στόχος.

2. **Αύξηση της πιθανότητας επισήμανσης και σύλληψης**, πριν, κατά ή μετά την τέλεση της πράξης. Όπως έχει αναφερθεί παραπάνω, η πιθανότητα επισήμανσης και σύλληψης μπορεί να λειτουργεί πιο αποτρεπτικά για τον πιθανό δράστη από ότι η αυστηρότητα των ποινών. Ο κίνδυνος επισήμανσης για τον δράστη μπορεί να αυξηθεί με ενίσχυση των ικανών φυλάκων, με την αύξηση της φυσικής ή της ηλεκτρονικής παρακολούθησης χώρων και δραστηριοτήτων (για παράδειγμα των υπαλλήλων της επιχείρησης), ενίσχυση των εσωτερικών ελέγχων με την τοποθέτηση «διαχειριστών του χώρου» ή των δικτύων εκπαιδευμένων για την αναγνώριση της απάτης, χρήση εξωτερικών ελεγκτών, όπως ορκωτών λογιστών, μείωση της «ανωνυμίας». Η εκπαίδευση των διαχειριστών χώρου στην αναγνώριση της απάτης ή άλλων παράνομων δραστηριοτήτων αυξάνει την πιθανότητα επισήμανσης και λειτουργεί αποτρεπτικά για τον πιθανό δράστη.[791]

3. **Μείωση των αναμενόμενων κερδών** από την εγκληματική ενέργεια.

Η μείωση των αναμενόμενων κερδών του δράστη συμβάλλει με τη σειρά της στην μετατροπή ή/και εξάλειψη της εγκληματικής ευκαιρίας. Ως μέσα για τον σκοπό αυτόν προτείνεται, από τη σκοπιά της περιστασιακής πρόληψης του εγκλήματος, η εφαρμογή

[787] Benson Michael L. & Madensen Tamara D (2007), ό.π.
[788] Benson Michael L. & Madensen Tamara D. (2007), ό.π.
[789] βλ. την εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων
[790] Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010)
[791] Clarke Ronald V. (1997), σσ. 20-22

κάλυψης ή απομάκρυνσης του στόχου, η επισήμανση και οριοθέτηση των δικαιωμάτων χρήσης και ιδιοκτησίας (π.χ. αναγραφή ονόματος χρήστη και υπογραφή), η άρνηση του οφέλους που προκύπτει από την τέλεση του εγκλήματος.[792]

4. **Μείωση της δυνατότητας του δράστη να σχηματίσει εκλογικεύσεις** για να δικαιολογήσει την δράση του. Όπως αναφέρθηκε[793] ο δράστης χρησιμοποιεί εκλογικεύσεις, π.χ. «δεν ήξερα ότι απαγορεύεται», για να θεωρηθεί η πράξη του δικαιολογημένη και μη εγκληματική. Η αφαίρεση από τον δράστη της δυνατότητας να εξουδετερώνει το αίσθημα ντροπής ή ενοχής πιθανά θα τον περιορίσει από την τέλεση του εγκλήματος. Έτσι προτείνεται η θέσπιση και γνωστοποίηση κανόνων (δεοντολογίας, ορθής χρήσης, επαγγελματικό καθηκοντολόγιο), οδηγιών χρήσης, ανάρτηση ενημερωτικών πινακίδων για την ευαισθητοποίηση της συνείδησης των ατόμων και τη διευκόλυνση της συμμόρφωσής τους.[794]

5. **Μείωση των περιβαλλοντικών προκλήσεων και περιστασιακών συνθηκών** που ευνοούν τη διάπραξη μη προσχεδιασμένου εγκλήματος. Αν και τα περισσότερα ηλεκτρονικο-οικονομικά εγκλήματα έχουν πιο ορθολογική διάσταση κινήτρων και λιγότερο συναισθηματική, η μείωση των προκλήσεων του περιβάλλοντος μπορεί να επιτυγχάνεται με τη μείωση των συναισθηματικών και ψυχολογικών ερεθισμάτων[795], αλλά κυρίως με την προσπάθεια ώστε να καταστεί ο στόχος λιγότερο ελκυστικός δηλαδή να γίνει ακύρωση του οφέλους (denying benefits) για το δράστη από την διάπραξη του εγκλήματος.[796] Για παράδειγμα η απενεργοποίηση των κλεμμένων συσκευών κινητής τηλεφωνίας από τις εταιρείες- παρόχους τις καθιστά άχρηστες και αφαιρεί το αναμενόμενο κέρδος από τον κλέφτη. Τέτοια περίπτωση συνιστά η πρόσφατη απόφαση της ΕΕΕΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων) σύμφωνα με την οποία οι εταιρείες κινητής τηλεφωνίας υποχρεούνται να απενεργοποιούν, μέσω του κωδικού IMEI, τις συσκευές κινητών τηλεφώνων που δηλώνονται κλεμμένες από τους χρήστες τους. Έτσι το κλεμμένο κινητό θα είναι άχρηστο και δεν θα μπορεί να χρησιμοποιηθεί ή να μεταπωληθεί αφού δεν θα ενεργοποιείται με άλλη κάρτα SIM.[797] Αυτό συνιστά «άρνηση οφέλους» για τον δράστη ο οποίος αποτρέπεται να κλέψει επειδή μόνο κόστος θα έχει η δράση του και κανένα όφελος.

Η κάθε μια από τις παραπάνω κατευθύνσεις πρέπει να εφαρμοστεί για την αποτελεσματικότερη, κατά το δυνατό, αντιμετώπιση της ηλεκτρονικο-οικονομικής εγκληματικότητας.[798]

Η πρόληψη αλλά και η εξιχνίαση του ηλεκτρονικού εγκλήματος απαιτούν διεθνή, διακρατική συνεργασία, εναρμόνιση των νομοθεσιών των διαφόρων κρατών και την εμπλοκή δημόσιου και ιδιωτικού τομέα. Παρατηρούμε ότι σε πολλές από αυτές τις προσπάθειες εμπεριέχονται αρκετές από τις πέντε κατευθύνσεις που πρότεινε ο Clarke για την περιστασιακή πρόληψη του εγκλήματος.[799] Ενδεικτικό αποτελεί ότι σε πολλές νομοθεσίες και κανονισμούς περιλαμβάνονται κάποιες από αυτές τις πέντε βασικές αρχές –κατευθύνσεις. [800]

[792] Clarke Ronald.V. (1997), σσ. 21-23
[793] Βλ. παραπάνω για τις «τεχνικές εξουδετέρωσης» Sykes & Matza.
[794] Benson Michael L. & Madensen Tamara D. (2007), ό.π.
[795] Benson Michael L. & Madensen Tamara D. (2007), ό.π
[796] Clarke Roland (1997), σ. 23
[797] http://www.express.gr/news/finance/757931oz_20140926757931.php3, Σεπτέμβριος 2014
[798] Benson Michael L. & Madensen Tamara D. (2007), βλ. και ΔΙΑΓΡΑΜΜΑ 5 για τις «25 τεχνικές παρέμβασης για το περιστασιακό έγκλημα».
[799] Βλ. παραπάνω
[800] Benson Michael L. & Madensen Tamara D. (2007), σσ. 609-626

Τα προληπτικά μέτρα περιλαμβάνουν προσπάθειες βελτίωσης του άμεσου περιβάλλοντος ώστε να μειωθούν οι εγκληματικές ευκαιρίες καθιστώντας δυσκολότερη την επαφή του πιθανού δράστη με τον ευάλωτο στόχο και να ευρεθούν οι «ικανοί φύλακες».

Όπως είδαμε κατά την εφαρμογή της θεωρίας των καθημερινών δραστηριοτήτων στα εγκλήματα του κυβερνοχώρου, η έννοια του χώρου διευρύνεται για να περιλάβει τα δίκτυα υπολογιστών και το διαδίκτυο ως τους πιθανούς τρόπους ή «μέρη» όπου ο δράστης προσεγγίζει τα θύματά του.[801]

Έτσι, με βάση την περιστασιακή πρόληψη του εγκλήματος και τη μείωση των εγκληματικών ευκαιριών, μια καίρια παρέμβαση για την αντιμετώπιση του ηλεκτρονικο-οικονομικού εγκλήματος θα πρέπει οπωσδήποτε να περιλαμβάνει και την τροποποίηση των χαρακτηριστικών των δικτύων, που ανάμεσα στα άλλα παρέχουν στον δράστη και την απαραίτητη κάλυψη (ανωνυμία), για τον δραστικό περιορισμό της πρόσβασης του δράστη στους πιθανούς στόχους, είτε άψυχους (ψηφιακά αρχεία, συστήματα κλπ.) είτε έμψυχους.

Αυτή η τροποποίηση περιλαμβάνει αρχικά τη θωράκιση του στόχου ώστε αυτός να καταστεί δυσκατάβλητος, με τον έλεγχο της πρόσβασης στο στόχο ή στα απαραίτητα μέσα που απαραίτητα για την διενέργεια της εγκληματικής δράσης. Ένα δεύτερο καίριο σημείο παρέμβασης αποτελεί η κατάλληλη ενημέρωση και εκπαίδευση των πιθανών θυμάτων ώστε να καταστούν αυτά περισσότερο δύσπιστα στις προσπάθειες κάθε είδους απόπειρας απάτης εναντίον τους .[802]

10.4. Πρακτικά μέτρα για την πρόληψη του ηλεκτρονικο-οικονομικού εγκλήματος – Μείωση των εγκληματικών ευκαιριών

Όπως σημειώθηκε παραπάνω, η τέλεση ενός εγκλήματος, σύμφωνα με τις προσεγγίσεις των «εγκληματικών ευκαιριών», απαιτεί την σύμπραξη τριών στοιχείων:

1. Το κίνητρο που κινητοποιεί τον δράστη, όπως χρήμα, φήμη, διασκέδαση, σεξ, κλπ.

2. Τα μέσα ή τα εργαλεία που χρησιμοποιεί ο ικανός δράστης για να προσεγγίσει και να καταβάλλει τον στόχο του, όπως κακόβουλα προγράμματα για να εισβάλει στο σύστημα – στόχο.

3. Η ευκαιρία για την διάπραξη του εγκλήματος που εκμεταλλεύεται ο δράστης, όπως η απουσία ικανής φύλαξης και η ελκυστικότητα του στόχου.

Μια προσεκτική εξέταση των παραπάνω παραγόντων που συναποτελούν το «τρίγωνο του εγκλήματος», θα μας οδηγήσει στο συμπέρασμα ότι οι προσπάθειες παρέμβασης για την πρόληψη και την αποτροπή του εγκλήματος θα πρέπει να εστιάσουν περισσότερο στο τρίτο στοιχείο, την ύπαρξη της ευκαιρίας. Αυτό γιατί ούτε η απάλειψη ή η αλλοίωση του κινήτρου του δράστη ούτε των μέσων (εργαλείων, προγραμμάτων, γνώσεων) που αυτός διαθέτει είναι εφικτή από τους φορείς πρόληψης και αντιμετώπισης. Η αλλοίωση της εγκληματικής ευκαιρίας είναι πιο εφικτός στόχος αντεγκληματικής πολιτικής στην προσπάθεια αποτροπής του εγκλήματος. Από πλευράς χρηστών αυτό συνίσταται στην λήψη μέτρων προστασίας “σκλήρυνσης” των συστημάτων τους και, πιθανώς, αλλαγής των καθημερινών δραστηριοτήτων τους. Εφόσον κανείς δεν μπορεί να αλλάξει τα κίνητρα και τα διαθέσιμα

[801] βλ. Benson, Michael, Tamara D. Madensen, & John E. Eck (2009), σ. 179 και κεφάλαιο 4, §4, αναφορά στους Eck και Clarke, βλ. Benson, Michael, Tamara D. Madensen, & John E. Eck (2009), σ.179

[802] Benson Michael L. & Madensen Tamara D (2007), σσ. 609-626

μέσα του δράστη, τουλάχιστον μπορεί να αλλοιώσει τη δόμηση της ευκαιρίας και τα χαρακτηριστικά που καθιστούν ευάλωτους τους στόχους.[803]

Τα μέτρα πρόληψης, εφαρμόζοντας τις θεωρίες των «εγκληματικών ευκαιριών» (κυρίως των καθημερινών δραστηριοτήτων και την περιστασιακή πρόληψη του εγκλήματος) στοχεύουν στη μείωση των εγκληματικών ευκαιριών μέσω της ενίσχυσης των ικανών φυλάκων (θωράκιση των στόχων, αύξηση της πιθανότητας επισήμανσης του δράστη), μείωση των αναμενόμενων κερδών του δράστη.

Στην κατεύθυνση αυτή κινούνται τα μέτρα για την εκπαίδευση των παιδιών και των εφήβων που ανέπτυξε η Ευρωπαϊκή Ένωση, οι συμβουλές των διωκτικών αρχών και των ειδικών για τους τρόπους προστασίας από το ηλεκτρονικο και οικονομικό έγκλημα, τα μέτρα κοινωνικής πολιτικής και διαπαιδαγώγησης που παρουσιάζονται παρακάτω.

10.4.1. Μέτρα για ασφαλή πλοήγηση στο διαδίκτυο από την Ευρωπαϊκή Ένωση

Ο βαθμός διείσδυσης του Διαδικτύου εξακολουθεί να σημειώνει σημαντική αύξηση στις χώρες της Ευρωπαϊκής Ένωσης (ΕΕ). Παράλληλα, εξακολουθεί να αναπτύσσεται το δυνητικά επιβλαβές περιεχόμενο, ιδίως για τα παιδιά, όπως και το παράνομο περιεχόμενο. Η Ευρωπαϊκή Ένωση αναγνωρίζοντας τους κινδύνους που ελλοχεύουν στο διαδίκτυο, ιδιαίτερα για παιδιά και νέους έχει καταρτίσει διάφορα προγράμματα δράσης για πληροφόρηση και εκπαίδευση όλων των εμπλεκομένων.

Πρόγραμμα για την ασφαλή πλοήγηση στο διαδίκτυο για παιδιά και εφήβους

Η διασφάλιση ενός αυστηρού πλαισίου λειτουργίας του Διαδικτύου για παιδιά και εφήβους απασχολεί την Ευρωπαϊκή Ένωση από το 1996, οπότε και ξεκίνησε η προσπάθεια ανάπτυξης ενός πανευρωπαϊκού δικτύου πληροφόρησης και εκπαίδευσης σχετικά με τους κινδύνους αλλά και τα μέτρα που μπορούν να συμβάλουν στην προστασία από τις αρνητικές πλευρές του Διαδικτύου.

Με την απόφαση υπ' αριθμό 276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Ιανουαρίου 1999, δημιουργείται ένα πολυετές κοινοτικό πρόγραμμα δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα. Το πρόγραμμα δράσης είχε τετραετή διάρκεια (από την 1η Ιανουαρίου 1999 έως την 31η Δεκεμβρίου 2002) και προϋπολογισμό ύψους 25 εκατ. ευρώ.

Γενικός στόχος. Το πρόγραμμα δράσης «Safer Internet» στοχεύει στην ενθάρρυνση της δημιουργίας ενός ευνοϊκού περιβάλλοντος για την ανάπτυξη της βιομηχανίας που σχετίζεται με το Διαδίκτυο, μέσω της προώθησης της ασφαλούς χρήσης του Διαδικτύου και της καταπολέμησης του παράνομου και επιβλαβούς περιεχομένου.

Γραμμές δράσης. Το πρόγραμμα διαρθρώνεται γύρω από τους άξονες:

α) Δημιουργία ασφαλέστερου περιβάλλοντος. Για τον σκοπό αυτό δημιουργείται ευρωπαϊκό δίκτυο με ανοικτές γραμμές επικοινωνίας (hotlines), με την ενθάρρυνση της αυτορρύθμισης και εκπόνηση κωδίκων δεοντολογίας. Πρόκειται για αποδέκτες καταγγελιών του κοινού σχετικά με σελίδες με παράνομο περιεχόμενο. Οι καταγγελίες, έπειτα από διεξοδική διερεύνηση, διαβιβάζονται στην αρμόδια υπηρεσία, για παράδειγμα στην αστυνομία, που αναλαμβάνει τον περαιτέρω χειρισμό του θέματος.

[803] Shinder Debra Littlejohn (2002), σσ., 254-255

β) Τεχνικά μέσα άσκησης του γονικού ελέγχου- ανάπτυξη συστημάτων φιλτραρίσματος και διαβάθμισης αναδεικνύοντας κυρίως τα πλεονεκτήματα αυτών των διαδικασιών και διευκολύνοντας μια διεθνή συμφωνία σχετικά με το σχεδιασμό ενός συστήματος διαβάθμισης.

γ) Δράσεις συνειδητοποίησης και πληροφόρησης, που αφορούν γονείς και εκπαιδευτικούς, κυβερνητικούς φορείς και τη βιομηχανία που αναπτύσσεται σε σχέση με το Διαδίκτυο σχετικά με τον αποτελεσματικότερο τρόπο προστασίας των ανηλίκων από την έκθεσή τους σε περιεχόμενο που θα μπορούσε να βλάψει την ανάπτυξή τους. Ειδικά, όσον αφορά τους γονείς και εκπαιδευτικούς, ιδρύθηκε από την Ευρωπαϊκή Επιτροπή το «Κέντρο Ανταλλαγής των Εμπειριών Συνειδητοποίησης για την Ασφαλέστερη Χρήση του Διαδικτύου» (Safer Internet For Knowing και Living - SIFKaL[804]), το οποίο έχει στόχο την ορθή ενημέρωσή τους σχετικά με τις νέες τεχνολογίες, τα προτερήματα και τα μειονεκτήματά τους.[805]

δ) δράσεις υποστήριξης για την αξιολόγηση των νομικών συνεπειών, το συντονισμό με τις ανάλογες διεθνείς πρωτοβουλίες και την αξιολόγηση του αντίκτυπου των κοινοτικών μέτρων.[806]

Πρόγραμμα Safer Internet Plus (2005-2008)

Το πρόγραμμα Safer Internet Plus (2005-2008) διαδέχεται το σχέδιο δράσης Safer Internet (1999-2004). Το πεδίο εφαρμογής του νέου προγράμματος επεκτείνεται στα νέα μέσα επικοινωνίας (όπως π.χ. βίντεο), ρητός σκοπός δε του νέου προγράμματος είναι η καταπολέμηση του ρατσισμού και των ανεπίκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα («spam»). Σε σχέση με το προηγούμενο πρόγραμμα, επικεντρώνεται περισσότερο στους τελικούς χρήστες, όπως γονείς, εκπαιδευτικοί και παιδιά.

Με την απόφαση αριθ. 854/2005/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2005, καθιερώνεται πολυετές κοινοτικό πρόγραμμα για την προαγωγή της ασφαλέστερης χρήσης του Διαδικτύου και νέων επιγραμμικών τεχνολογιών.[807]

Δημιουργήθηκαν ανοικτές γραμμές επικοινωνίας έκτακτης ανάγκης (hotlines) ώστε το κοινό να έχει τη δυνατότητα να επισημαίνει περιπτώσεις παράνομου περιεχομένου και οι πληροφορίες να διαβιβάζονται στο αρμόδιο για ανάληψη δράσης όργανο [π.χ. στον πάροχο υπηρεσιών Διαδικτύου (ISP) ή στην αστυνομία.

Αντιμετώπιση ανεπιθύμητου και επιβλαβούς περιεχομένου

Προαγωγή ασφαλέστερου περιβάλλοντος, για τον περιορισμό της ροής ανεπιθύμητου, επιβλαβούς και παράνομου περιεχομένου.

Ευαισθητοποίηση. Οι δράσεις ευαισθητοποίησης λαμβάνουν υπόψη τα συναφή ζητήματα όπως η προστασία των καταναλωτών, η προστασία των δεδομένων και η ασφάλεια πληροφοριών και δικτύων (ιοί, ανεπίκλητα μηνύματα κ.λπ.).[808]

[804] http://www.sifkal.org/index.htm, Απρίλιος (2008)
[805] http://www.e-yliko.gr/safety/svirus3.htm, Ιούνιος (2007)
[806] http://europa.eu/scadplus/leg/el/lvb/l24190.htm, Απρίλιος (2008)
[807] Βλ. σχετικά με την "καθιέρωση πολυετούς κοινοτικού προγράμματος για προαγωγή ασφαλέστερης χρήσης του Ίντερνετ και νέων επιγραμμικών τεχνολογιών", *Επίσημη Εφημερίδα Ευρωπαϊκής Ένωσης Eur-Lex, αριθ. L 149 της 11/06/2005 σ. 0001 – 0013*, ανακτήθηκε από http://eurlex.europa.eu/search.html?type=expe http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1410535642525&uri=CELEX:32005D0854 rt&qid=1410535642525, Αύγουστος 2014
[808] http://europa.eu/scadplus/leg/el/lvb/l24190b.htm, Απρίλιος (2008)

10.4.2. Η πρόληψη του ηλεκτρονικο-οικονομικού εγκλήματος από τις διωκτικές αρχές.

Οι διωκτικές αρχές πολλών χωρών δαπανούν μεγάλα χρηματικά ποσά για την απόκτηση τεχνολογικού εξοπλισμού, την εκπαίδευση του προσωπικού, την ενημέρωση του κοινού με σκοπό την πρόληψη και καταπολέμηση του εγκλήματος. Ειδικότερα από τις αρχές λαμβάνονται τα πιο κάτω μέτρα για το οικονομικό - ηλεκτρονικό έγκλημα:

1. Δημιουργία ειδικών τμημάτων που ασχολούνται με το οικονομικό και το ηλεκτρονικό έγκλημα και στελεχώνονται με άτομα που διαθέτουν γνώσεις και εμπειρία στα λογιστικά, νομικά, οικονομικά και τους ηλεκτρονικούς υπολογιστές
2. Επιμόρφωση των στελεχών με συμμετοχή τους σε σεμινάρια και διεθνή συνέδρια.
3. Προμήθεια του κατάλληλου τεχνολογικού εξοπλισμού.
4. Ενημέρωση του κοινού για την πρόληψη τέτοιων αδικημάτων
5. Κάλυψη των κενών στη νομοθεσία και εναρμόνιση στις νομοθεσίες των διαφόρων χωρών.
6. Συνεργασία και σύναψη συμφωνιών σε διεθνές επίπεδο για την καταπολέμηση αυτού του είδους εγκλήματος.

Τρόποι εντοπισμού διαδικτυακών δραστών από τις διωκτικές αρχές- Αύξηση της πιθανότητας ανακάλυψης του δράστη

Μέσω των ηλεκτρονικών υπολογιστών και κυρίως του διαδικτύου δεν εμφανίζονται μόνο οι νέες μορφές εγκλήματος αλλά ταυτόχρονα, πάλι μέσω της χρήσης αυτών ανακαλύπτονται και οι δράστες τους.

Παρά τις δυσκολίες εντοπισμού των δραστών του ηλεκτρονικού εγκλήματος, που είδαμε παραπάνω, υπάρχουν και οι αντίθετες απόψεις που υποστηρίζουν ότι η περίφημη «ανωνυμία» στο διαδίκτυο δεν ισχύει στο βαθμό που νομίζουμε. Στις περισσότερες μορφές μεταφοράς δεδομένων ή επικοινωνίας μέσω του διαδικτύου επικρατεί το μοντέλο «πελάτης-πάροχος» (client-server), μια αρχιτεκτονική που επιβάλλει τον κεντρικό έλεγχο της πληροφορίας σε όλες τις δικτυακές μορφές επικοινωνίας που καθιστά δυνατό το «trackback» δηλαδή την ανίχνευση και τον εντοπισμό.[809]

Με ποιούς τρόπους όμως γίνεται εφικτός ο εντοπισμός, όχι μόνο των δραστών, αλλά και οποιουδήποτε χρήστη. Αρχικά, για να συνδεθεί κανείς στο Internet, θα πρέπει να αποκτήσει ένα πακέτο πρόσβασης ή να δικαιούται πρόσβαση μέσω κάποιου εκπαιδευτικού οργανισμού και να δηλώσει τα πραγματικά του στοιχεία (ονοματεπώνυμο, κατοικία, τηλέφωνο) σε έναν ISP (Internet Service Provider, ο πάροχος διαδικτυακών υπηρεσιών) ή άλλο φορέα. Στη συνέχεια και κάθε φορά που συνδέεται στο Διαδίκτυο, ο ISP καταγράφει το σημείο σύνδεσης, τη χρησιμοποιούμενη διεύθυνση IP (που είναι μοναδική), τη διάρκεια σύνδεσης, το μέγεθος των διακινούμενων δεδομένων και τις αιτήσεις του π.χ. για να «κατεβάσει» αρχεία, για σύνδεση σε Web sites κ.λ.π.[810] Το πιο σημαντικό είναι πως, βάσει νόμων, ο ISP είναι υποχρεωμένος να διατηρεί τα παραπάνω στοιχεία και να τα διαθέτει σε οποιαδήποτε αρχή, εφόσον του ζητηθούν.[811]

Έλεγχος για τις online δραστηριότητες υπάρχει σε όλα τα επίπεδα: στα e-mail που στέλνονται ή λαμβάνονται, στις επαφές στα δίκτυα instant messaging, στα αρχεία που

[809] Abernathy William & Lee Tien (2003)
[810] http://www.all-nettools.com
[811] Section 2703(c) of the Electronic Communications Privacy Act (ECPA), February 2006, in www.epic.org/ privacy/anonymity/#legal

κατεβάζονται μέσω FTP/Web αλλά και μέσω των εφαρμογών διαμοιρασμού αρχείων μεταξύ διαδικτυακών κοινοτήτων χρηστών (P2P/Peer to Peer- file sharing). Ακόμα και στις μορφές υποτιθέμενης ελεύθερης επικοινωνίας, υπάρχει τουλάχιστον ένα κομβικό σημείο ελέγχου, αυτό του ISP. Καθ' όλη τη διάρκεια της σύνδεσης στο Internet ίχνη αφήνονται παντού.[812] Έτσι η ανακάλυψη των ηλεκτρονικών δραστών, αργά ή γρήγορα, καθίσταται πιθανή υπόθεση. Μπορούμε να βρούμε «οτιδήποτε για τον οποιονδήποτε στο ίντερνετ».[813] Οι τελευταίες επιτυχίες της υπηρεσίας δίωξης του ηλεκτρονικού εγκλήματος της Ελληνικής Αστυνομίας (εξάρθρωση κυκλώματος ηλεκτρονικής παιδικής πορνογραφίας, ανακάλυψη και διάσωση νέου που ήθελε οδηγίες και στήριξη μέσω του διαδικτύου για να αυτοκτονήσει), επιβεβαιώνουν σε σημαντικό βαθμό αυτή την άποψη.

10.4.3. Η πρόληψη του ηλεκτρονικού εγκλήματος από τα άτομα – χρήστες των ψηφιακών τεχνολογιών. Ενίσχυση των «ικανών φυλάκων»

Η πρώτη γραμμή προστασίας του απλού χρήστη ενάντια στο έγκλημα μέσω του διαδικτύου είναι η αυτοπροστασία.

Αποτελέσματα των πιο πρόσφατων ερευνών, των Bossler και Holt, έδειξαν ότι αυτοί που κινδυνεύουν λιγότερο από θυματοποίηση στο διαδίκτυο είναι οι πιο έμπειροι και με υψηλότερου επιπέδου ψηφιακές δεξιότητες χρήστες. Οι γνώστες της πληροφορικής τεχνολογίας μπορούν πιο εύκολα να διακρίνουν τους ψηφιακούς κινδύνους, να τους επισημαίνουν και να τους αποφεύγουν. Οι ψηφιακές γνώσεις, οι δεξιότητες και η εμπειρία λειτουργούν ως ατομικοί ικανοί φύλακες που προστατεύουν τους χρήστες των τεχνολογιών από έκθεση σε πιθανούς κινδύνους.[814]

Καθοριστική σημασία στον τομέα της πρόληψης και της ενίσχυσης των «ικανών φυλάκων» έτσι αποκτά η ενημέρωση των χρηστών και η εκπαίδευσή τους σχετικά με τις νέες τεχνολογίες. Προσπάθειες ενημέρωσης των χρηστών πρέπει να εστιάσουν στους πιθανούς κινδύνους από την επίδειξη επικίνδυνης διαδικτυακής συμπεριφοράς από πλευράς τους, που όπως εξετάστηκε σε άλλο σημείο[815], συνιστούν το παράνομο κατέβασμα αρχείων, θέαση πορνογραφικού υλικού κλπ.

Λαμβάνοντας υπόψη την περιορισμένη ικανότητα των κυβερνήσεων να ελέγξουν το έγκλημα στον κυβερνοχώρο, η πρώτη γραμμή υπεράσπισης βρίσκεται στην άσκηση συνετής συμπεριφοράς από τα πιθανά θύματα. Ακριβώς όπως το πρώτο βήμα στον έλεγχο της διάρρηξης είναι να κλειδωθούν οι πόρτες και τα παράθυρα κάποιου, έτσι και στην ηλεκτρονική διάρρηξη πρέπει να τηρηθούν οι βασικές αρχές της ασφάλειας πληροφοριών.[816]

Γενικά, όπως υποδεικνύεται και από τα αποτελέσματα ερευνών που εξετάσαμε παραπάνω (όπως του Choi), τα άτομα – χρήστες των διαδικτυακών υπηρεσιών θα πρέπει να θωρακίζονται για να μην αποτελούν ευάλωτους στόχους, να ενημερώνουν τα προγράμματα προστασίας του υπολογιστή τους, να εξακριβώνουν ότι τα προγράμματα αυτά είναι ανοικτά κατά την πλοήγησή τους στο διαδίκτυο και να αλλάζουν τακτικά τους κωδικούς πρόσβασης.[817]

[812] Abernathy William & Lee Tien (2003)
[813] Givens Beth (2009)
[814] Bossler Adam, & Holt Thomas (2013), ό.π.
[815] Βλ. για τον «ρόλο του στόχου - θύματος στην διάπραξη του κυβερνοεγκλήματος»
[816] Grabosky Peter (1998)
[817] Choi Kyung-shick (2008a)

10.4.3.1. Τρόποι Προστασίας των χρηστών από ιούς

Οι διαχειριστές ιστοσελίδων που ειδικεύονται σε θέματα ασφάλειας ηλεκτρονικών υπολογιστών και ασφαλούς πλοήγησης στο διαδίκτυο συμβουλεύουν όσον αφορά την προστασία των ηλεκτρονικών υπολογιστών από ιούς. Μερικά από τα μέτρα αυτά που κρίνονται σημαντικά για την ασφάλεια κάθε χρήστη είναι:

Χρήση προγραμμάτων antivirus, anti-spyware και firewall, για προστασία του ηλεκτρονικού υπολογιστή από ιούς και επιθέσεις μη επιτρεπτής πρόσβασης σε αρχεία και δεδομένα.

Τήρηση αντίγραφων ασφαλείας και δημιουργία δίσκου για αποκατάσταση ζημιών (back up) από ιούς.

Να αποφεύγεται το άνοιγμα ηλεκτρονικών μηνυμάτων με επισυναπτόμενα αρχεία ή έγγραφα από γνωστούς ή αγνώστους αποστολείς, είτε μέσω ηλεκτρονικής αλληλογραφίας είτε μέσω άλλων μέσων.

Τακτική ενημέρωση του λειτουργικού συστήματος (Windows) του Η/Υ ώστε να καλύπτονται τα όποια κενά ασφαλείας έχουν εντοπιστεί.[818]

Απενεργοποίηση της επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που αποστέλλονται μέσω προγραμμάτων συνομιλίας (irc chat) στο διαδίκτυο.

Απενεργοποίηση του ανοίγματος java ή Active X εφαρμογών στον Internet Browser.

Επιλογή της πλήρους εμφάνισης των τύπων αρχείων στον Η/Υ.

Για την αντιμετώπιση του spam χρησιμοποιούνται τα «φίλτρα spam» που ενεργοποιούνται μέσα από το πρόγραμμα για e-mail.[819]

10.4.3.2. Τρόποι Προστασίας καταναλωτών από την ηλεκτρονικο-οικονομική απάτη στο πλαίσιο θωράκισης του στόχου

Οι απάτες που διενεργούνται σε βάρος των απλών καταναλωτών – χρηστών των ψηφιακών υπηρεσιών έχουν όμοια χαρακτηριστικά δόμησης της εγκληματικής ευκαιρίας – προτύπου του εγκλήματος της απάτης:

Ο δράστης α) προσεγγίζει το υποψήφιο θύμα του ενημερώνοντάς το για κάποια προσφορά προϊόντος ή ευκαιρία, β) έπειτα προσπαθεί, με ψεύτικους ισχυρισμούς, να πείσει το θύμα ότι πρόκειται για νόμιμη και μοναδική ευκαιρία, γ) ώστε να του αποσπάσει χρήματα ή τη συναίνεση του για κάποια υπηρεσία.

Με σκοπό την θωράκιση του στόχου, η πρόληψη στην περίπτωση απάτης καταναλωτών, μπορεί να εστιάσει στο δεύτερο σημείο, στην προσπάθεια δηλαδή του δράστη να πεισθεί το υποψήφιο θύμα ότι πρόκειται για νόμιμη συναλλαγή ή πραγματική επαγγελματική ευκαιρία. Προκειμένου να καταστεί δυσκολότερο να ξεγελαστούν τα θύματα θα πρέπει να γίνει προσπάθεια ενημέρωσης και εκπαίδευσής τους σχετικά με τους πιθανούς κινδύνους που διατρέχουν στο πλαίσιο της διαδικτυακής, καταναλωτικής ή επαγγελματικής, συμπεριφοράς τους.[820]

[818] Βλ. http://www.sch.gr/virus/%CE%A3%CE%B5%CE%BB%CE%AF%CE%B4%CE%B1-2#content, ανακτήθηκε Σεπτέμβριος 2014

[819] http://www.e-crime.gr/security_tips.htm, http://www.efpolis.gr/, Σεπτέμβριος 2014

[820] Benson Michael L. & Madensen Tamara D. (2007), ό.π.

10.4.3.3. Μέτρα πρόληψης και προστασίας για τους χρήστες ηλεκτρονικών τραπεζικών υπηρεσιών (e-banking)

Πολλοί είναι εκείνοι που προσπαθούν εν αγνοία των χρηστών να εγκαταστήσουν μέσω του Internet ή του ηλεκτρονικού ταχυδρομείου στον υπολογιστή κακόβουλα προγράμματα (Viruses, Worms, Trojan Horses, Spyware κ.α.)

Ορισμένα από αυτά είναι δυνατόν να υποκλέψουν προσωπικά στοιχεία και κωδικούς, να καταστρέψουν αρχεία και προγράμματα και γενικότερα να βλάψουν την λειτουργία του υπολογιστή.

Οι τράπεζες ενημερώνουν τους πελάτες τους, που χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες της τράπεζας για τους κινδύνους χρήσεως των ηλεκτρονικών συστημάτων, με σκοπό να τους βοηθήσουν να πραγματοποιήσουν με ασφάλεια τις ηλεκτρονικές τους συναλλαγές και προτείνουν διάφορα μέτρα πρόληψης και προστασίας.[821]

10.4.4. Η πρόληψη του ηλεκτρονικο-οικονομικού εγκλήματος από επιχειρήσεις και οργανισμούς: Παρεμπόδιση των δραστών -«Θωράκιση» των πιθανών στόχων

Οι παράγοντες της αγοράς μπορούν να ασκήσουν έλεγχο των λειτουργιών τους. Οι κύριοι τρόποι που προτείνονται για την πρόληψη της ηλεκτρονικής απάτης από επιχειρήσεις και οργανισμούς συνοψίζονται στα ακόλουθα:

1. Διαχείριση του ελέγχου της απάτης.[822] Καθιέρωση αρχών, από τις επιχειρήσεις, για ηθική στη χρήση των τεχνολογικών πληροφοριών.
2. Ανάπτυξη πολιτικών ασφαλείας των ηλεκτρονικών υπολογιστών, βελτίωση του λογισμικού τους, καθημερινός έλεγχος της λειτουργίας των συστημάτων τους.
3. Ο ΟΟΣΑ προτείνει στις επιχειρήσεις να προσέχουν την ασφάλεια και προστασία του δικτύου υπολογιστών τους από φυσικές καταστροφές όπως οι υπερτάσεις ηλεκτρικού ρεύματος από κεραυνούς, οι πλημμύρες, οι σεισμοί, η ζέστη, η υγρασία κλπ. (ΟΟΣΑ,Guidelines For the Security Of Information Systems, 1992) [823]
4. Έλεγχος προσωπικού. Να διασφαλίζουν ότι στις ανώτερες θέσεις απασχολείται υπεύθυνο και αξιόπιστο προσωπικό.
5. Να δίνουν προσοχή στα σημεία ελέγχου ταυτότητας - κωδικών ασφαλείας (password). Να χρησιμοποιούν προηγμένη κρυπτογράφηση, ηλεκτρονικές υπογραφές και πολύπλοκους συνδυασμούς αριθμών – γραμμάτων, να προτρέπουν τους πελάτες τους σε συχνή αλλαγή των κωδικών τους, να αρνούνται την πρόσβαση σε χρήστες μετά από συνεχείς αποτυχημένες προσπάθειες με λάθος κωδικούς. Τελευταία προτείνεται η χρήση έξυπνων καρτών και ηλεκτρονικών βιομετρικών προσδιοριστικών χαρακτηριστικών για τον έλεγχο της ταυτότητας των πελατών τους[824].
6. Έλεγχος της χρήσης των ηλεκτρονικών υπολογιστών από τους υπαλλήλους τους μέσω λογισμικού όπου θα καταγράφει τη χρήση των υπολογιστών και του διαδικτύου από αυτούς και συνακόλουθα τη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα της επιχείρησης.

[821] Στο παράρτημα παραθέτονται οι συμβουλές που δίνουν οι τράπεζες στους πελάτες τους – χρήστες διαδικτυακών τραπεζικών υπηρεσιών. Βλ. Παράρτημα: «Μέτρα Ασφάλειας e-banking»
[822] Καϊτσάς Δημήτρης (2004), σσ. 68-70.
[823] Λάζος Γρηγόρης (2001), σ. 223.
[824] Καϊτσάς Δημήτρης (2004), σ. 75

7. Δεδομένου ότι οι μεγάλες οργανώσεις αρχίζουν να υπολογίζουν την ευπάθειά τους στην ηλεκτρονική κλοπή ή το βανδαλισμό, αναμένονται να ασφαλίζονται ενάντια στις πιθανές απώλειες. Έτσι είναι προς όφελος των ασφαλιστικών εταιρειών να απαιτήσουν τις κατάλληλες προφυλάξεις ασφάλειας εκ μέρους των ασφαλισμένων τους[825].
8. Κάποιες εταιρίες εφαρμόζουν τη ρήση «αν δεν μπορείς να τους νικήσεις, πήγαινε μαζί τους» ή καλύτερα «πάρ' τους με το μέρος σου». Έτσι προσλαμβάνουν πρώην χάκερ συνδυάζοντας το τερπνό μετά του ωφελίμου: από τη μια τους εξουδετερώνουν ως πιθανό κίνδυνο για τη εταιρεία τους και από την άλλη τους χρησιμοποιούν για να δοκιμάζουν τα συστήματα των εταιριών που εισβάλουν και να εντοπίζουν πιθανές αδυναμίες της ασφάλειας των πληροφοριακών τους κέντρων[826].

10.4.4.1. Η Πρόληψη της απάτης σε επιχειρήσεις

Η απάτη συνιστά ζημιά ξένης περιουσίας που πλήττει τα ταμεία των μεγάλων, κυρίως, επιχειρήσεων και αποτελεί στοιχείο του επιχειρηματικού τους κινδύνου. Η αντιμετώπισή της είναι δύσκολη υπόθεση και με υψηλό κόστος, μπορεί όμως να γίνει προσπάθεια ελαχιστοποίησης της ζημιάς που προκαλείται στις επιχειρήσεις. Η γενική φιλοσοφία της πρόληψης της απάτης από τις επιχειρήσεις συνίσταται στη δημιουργία ενός περιβάλλοντος που θα δυσκολεύει - αν όχι αποτρέπει - τους πιθανούς δράστες, πράγμα που απαιτεί συνδυασμό παραγόντων όπως σαφώς προσδιορισμένα συστήματα ελέγχου και πρακτικές που σχετίζονται με τη διαχείριση των ανθρώπινων πόρων της επιχείρησης.

Όπως είδαμε, η απάτη στις επιχειρήσεις στις περισσότερες περιπτώσεις είναι αποτέλεσμα του συνδυασμού κινήτρου –ευκαιρίας – εκλογίκευσης. Εφαρμόζοντας το κατάλληλο μοντέλο διοίκησης θα μπορούσαν να καταπολεμηθούν τα παραπάνω αίτια της απάτης. Οι Κραμβία-Καπαρδή και Τσολάκης υποστηρίζουν ότι η καλλιέργεια μιας επιχειρησιακής κουλτούρας η οποία θα λαμβάνει υπόψη τις ανάγκες των εργαζομένων βελτιώνοντας το ηθικό τους, στο πλαίσιο ενός συμμετοχικού (δημοκρατικού) προτύπου διοίκησης, θα βοηθούσε στον περιορισμό του κινήτρου της απάτης. Η ευκαιρία διάπραξης μπορεί να αντιμετωπιστεί με τη δημιουργία τμήματος εσωτερικού ελέγχου με ρόλο την πρόληψη των κινδύνων απάτης.[827]

Σύμφωνα με τον Κληρίδη ιδιαίτερη προσοχή, για την πρόληψη της απάτης στις επιχειρήσεις, οφείλει να επιδεικνύεται στους εξής παράγοντες[828]:

1) Γνώση των κινδύνων από την επιχείρηση. Εφιστάται η προσοχή των διοικούντων της επιχείρησης να λαμβάνουν υπόψη ότι ο πιθανός δράστης στοχεύει όχι μόνο στα μετρητά, αλλά και σε οτιδήποτε έχει αξία όπως περιουσιακά στοιχεία, εμπορικά δικαιώματα, μυστικά, λογαριασμούς πελατών κλπ.
2) Καθορισμός σαφών πολιτικών της επιχείρησης σε θέματα απάτης. Να γίνεται ξεκάθαρο στον πιθανό δράστη μιας απάτης ότι θα διώκεται διοικητικά και ποινικά.
3) Κλίμα που δυσχεραίνει την τέλεση της απάτης. Η φιλοσοφία της επιχείρησης και το περιβάλλον μέσα σε αυτή να φαίνεται ότι είναι αντίθετο στην απάτη, ότι τηρούνται οι κανόνες και ξεκάθαρες επιχειρηματικές πρακτικές.
4) Αποτελεσματικότητα των συστημάτων εσωτερικού ελέγχου. Να διασφαλίζεται η αποτελεσματικότητα των συστημάτων ελέγχου στο πλαίσιο της επιχείρησης με τον

[825] Grabosky Peter.N. (1998)
[826] Χάιδου Ανθοζωή (2003), σ. 105
[827] Κραμβία –Καπαρδή Μαρία, Τσολάκης Χρίστος (2011), σσ. 286-319
[828] Κληρίδης Τάκης (2001), σσ. 243-254

συνεχή εκσυγχρονισμό, ανασκόπηση και εξέταση του τρόπου που λειτουργούν στην πράξη τα συστήματα ελέγχου. Πιο συγκεκριμένα:

- Τα ανώτερα στελέχη να μην παρακάμπτουν τους υπευθύνους ελέγχου.
- Οι ελεγκτές να μην έχουν επαφή και σχέσεις με τους ελεγχόμενους.
- Να διασφαλίζεται ικανός χρόνος για την διενέργεια σωστών ελέγχων.

5) Αποτελεσματική διαχείριση του ανθρώπινου δυναμικού. Ιδιαίτερη προσοχή απαιτείται στην πολιτική προσλήψεων και διαχείρισης του προσωπικού, επειδή το μεγαλύτερο ποσοστό εγκλημάτων κατά της επιχείρησης διαπράττεται από στελέχη της και εργαζόμενους σε αυτή. Το έκτακτο και εποχικό προσωπικό, οι καθαρίστριες, οι κλητήρες, οι μηχανικοί συντήρησης συνήθως δεν ελέγχονται επαρκώς.
6) Αξιολόγηση των ενδείξεων για απάτη. Όπως αναφέρει ο Κληρίδης[829], παρά το γεγονός ότι οι περισσότερες απάτες αποκαλύπτονται συμπτωματικά, έρευνες έχουν δείξει ότι σε πολλές εταιρείες που έπεσαν θύματα απάτης είχαν προηγηθεί προειδοποιητικές ενδείξεις, όμως δεν έλαβαν τα κατάλληλα μέτρα.

Οι καταστάσεις – ενδείξεις απάτης που πρέπει να λαμβάνονται υπόψη και να διερευνώνται άμεσα από τους διοικούντες της επιχείρησης [830] διακρίνονται:[831]

Α. Σε απλά «προειδοποιητικά σήματα για ύπαρξη προσωρινά αυξημένου κινδύνου» όπως είναι:

- Αυταρχική διοίκηση. Η αυταρχική άσκηση εξουσίας στο πλαίσιο της επιχείρησης μπορεί να οδηγήσει στην παράκαμψη της λειτουργίας ελέγχου, σε απόκρυψη πληροφοριών και συγκάλυψη της απάτης.
- Προσωπικό με χαμηλό αίσθημα ικανοποίησης σημαίνει πιθανότητα το προσωπικό αυτό να μην διενεργεί αποτελεσματικό έλεγχο και να εμφανίζει τάσεις αντεκδίκησης.
- Συχνές αλλαγές προσωπικού, μπορεί να είναι ένδειξη παράτυπων δραστηριοτήτων της επιχείρησης. Το προσωπικό μπορεί να παραιτείται λόγω ανησυχίας του για εμπλοκή της επιχείρησης σε παράνομες δραστηριότητες. Για αυτό απαιτείται αιτιολόγηση των λόγων αποχώρησης των υπαλλήλων ή στελεχών της επιχείρησης.
- Απομακρυσμένες εγκαταστάσεις, όπως αποθήκες, γραφεία κλπ. όπου ο έλεγχος και η επίβλεψη είναι πιο χαλαρά.
- Ο εντοπισμός μιας μικρής απάτης είναι πιθανή ένδειξη και για άλλες μεγαλύτερες απάτες. Οι δράστες χρησιμοποιούν το τρυκ μιας μικρής απάτης για δοκιμή πριν επιχειρήσουν την τελική μεγαλύτερη απάτη.

Β. Σε προειδοποιήσεις για «αυξημένο κίνδυνο» απάτης και συγκεκριμένα «γεγονότα ενδεικτικά απάτης», όπως:

- Ύπαρξη ανώνυμων επιστολών που καταγγέλλουν περιπτώσεις απάτης. Θα πρέπει να γίνεται σωστή αξιολόγηση τέτοιων επιστολών που οι αποστολείς τους μπορεί να είναι χαμηλόβαθμοι υπάλληλοι, πελάτες, προμηθευτές.
- Αλλαγή τρόπου ζωής που υποδεικνύει ασυμφωνία μεταξύ εισοδήματος και δαπανών απόκτησης περιουσιακών στοιχείων του ατόμου. Ύπαρξη υπερβολικών δαπανών που δεν δικαιολογούνται από την οικονομική κατάσταση του δράστη, π.χ. πολυτελή αυτοκίνητα, βίλλες κ.ά.

[829] Πρώην Υπ. Οικονομικών της Κύπρου.
[830] Βλ. και παραπ. «*ενδείξεις για απάτη στους δημόσιους οργανισμούς*».
[831] Κληρίδης Τάκης (2001), σσ. 243-254

- Η μη λήψη άδειας διακοπών από υπαλλήλους, μπορεί να σημαίνει την συνακόλουθη προσπάθεια αποφυγής του κινδύνου εντοπισμού, από αντικαταστάτες, περιπτώσεων απάτης που ακόμη δεν έχουν συγκαλυφτεί.
- Παράλογη, ασυνήθιστη συμπεριφορά, όπως υπάλληλος που αρνείται προαγωγή η οποία συνεπάγεται αλλαγή καθηκόντων του. [832]
- Η ύπαρξη οικονομικών προβλημάτων που αντιμετωπίζει ο δράστης.[833]

Τα στοιχεία που προδίδουν και καθιστούν τους εγκληματίες του λευκού περιλαιμίου πιο εύκολα ανακαλύψιμους από τις αρχές, σύμφωνα με τη Shinder είναι:

- Εισοδήματα, περιουσία και τρόπος ζωής που δεν συνάδει με τη νόμιμη απασχόληση του ατόμου.
- Ασυνήθιστες συναλλαγές με μεγάλα χρηματικά ποσά.
- Η ύπαρξη πολλών διαφορετικών τραπεζικών λογαριασμών σε διάφορες χώρες.
- Η ύπαρξη πολλών επιχειρήσεων καταχωρημένων στην ίδια έδρα.
- «Εικονικές» εταιρείες που δε διαθέτουν κεφάλαια ή δεν παρουσιάζουν κανένα αποτέλεσμα παραγωγικής δραστηριότητας.[834]

Σύμφωνα με μελέτη του ερευνητικού κέντρου στρατηγικού μάνατζμεντ της Μινεσότα το διάστημα 1988-1998, οι επιχειρήσεις που εμφάνισαν τα λιγότερα περιστατικά οικονομικού εγκλήματος ήταν αυτές που διέθεταν:

- Άτομα εκτός επιχείρησης να συμμετέχουν στο Διοικητικό Συμβούλιο.
- Ξεκάθαρες πολιτικές και διαδικασίες, έτσι ώστε όσο πιο σαφή είναι τα όρια μεταξύ των καθηκόντων που επιτελεί ο κάθε υπάλληλος/στέλεχος και οι κανόνες στους οποίους οφείλει να συμμορφώνεται, τόσο λιγότερο πιθανό είναι να υπερβεί κάποιος αυτά τα όρια.
- Μεγαλύτερη επικοινωνία μεταξύ των διαφορετικών τμημάτων της επιχείρησης, πράγμα που καθιστά δυσκολότερη την απόκρυψη κάποιου εγκλήματος.
- Σύστημα επιβράβευσης της απόδοσης των εργαζομένων, οι τελευταίοι να αισθάνονται ότι η αξία τους αναγνωρίζεται από την επιχείρηση ώστε να καταγγέλλουν ευκολότερα συναδέλφους τους που διενεργούν απάτες εναντίον της.[835]

Σύμφωνα με την έρευνα της PcW (Price waterhouse Coopers) για το 2011 τα κύρια μέσα με τα οποία οι οργανισμοί ενημερώνουν και εκπαιδεύουν τους εργαζομένους τους, για τους κινδύνους του ηλεκτρονικού[836] εγκλήματος, στην Ελλάδα αλλά και διεθνώς, αποτελούν τα emails, οι αφίσες, οι παρουσιάσεις, τα σεμινάρια και η ηλεκτρονική εκπαίδευση. Παρόλα αυτά επισημαίνεται η ανάγκη περαιτέρω εσωτερικής εκπαίδευσης για την πρόληψη αυτού του είδους εγκλήματος. Σχετικά με τη διενέργεια διαδικασιών για την αξιολόγηση του

[832] Κληρίδης Τάκης (2001), σσ. 243-254.
[833] Κραμβιά – Καπαρδή Μαρία & Τσολάκης Χρίστος (2011), σ.41
[834] Shinder Debra Littlejohn (2002), σ. 122
[835] Schnatterly Karen (2002)
[836] Σύμφωνα με τον ορισμό που χρησιμοποίησε η PwC για την έρευνα, ως *έγκλημα στον κυβερνοχώρο* ή *ηλεκτρονικό έγκλημα*, όρισε «ένα οικονομικό αδίκημα που διαπράχθηκε με τη χρήση υπολογιστή και του Internet, όπως είναι η μετάδοση ιών, το παράνομο "κατέβασμα" αρχείων (downloading) και η κλοπή προσωπικών δεδομένων, όπως στοιχεία τραπεζικών λογαριασμών. Ο ορισμός αυτός δεν περιλαμβάνει την απάτη "ρουτίνας", όπου ένας υπολογιστής είναι ένα από τα μέσα που χρησιμοποιήθηκαν για την τέλεση απάτης και περιλαμβάνει μόνο εκείνα τα οικονομικά εγκλήματα όπου ένας υπολογιστής ή το Internet ή τα ηλεκτρονικά μέσα και συσκευές είναι τα στοιχεία που κυρίως χρησιμοποιήθηκαν για την τέλεση απάτης και όχι τυχαία»

κινδύνου απάτης, τα αποτελέσματα της εν λόγω έρευνας, για την Ελλάδα το 2011 δείχνουν ότι το 52% των στελεχών ακολουθεί τις διαδικασίες από μία και έως πάνω από τέσσερεις φορές το χρόνο ενώ το 34% δεν διενεργεί καθόλου έλεγχο. [837]

Σε περιπτώσεις κλοπής, κατάχρησης ή απάτης από υπαλλήλους, τα προληπτικά μέτρα που μπορούν να λάβουν οι επιχειρήσεις αφορούν, όχι μόνο τεχνικές ηλεκτρονικής παρακολούθησης μέσω καμερών κ.λπ., αλλά και ένα γενικότερο σύστημα διοίκησης που περιλαμβάνει τη δημιουργία καλύτερων εργασιακών συνθηκών, κλίματος εμπιστοσύνης, ικανοποίησης, κατανόησης, συνεργασίας μεταξύ διοίκησης και εργαζομένων, παροχής κινήτρων και αναγνώρισης της προσφοράς των δεύτερων από τους πρώτους.

Όσον αφορά την αντιμετώπιση των διαπιστωμένων περιπτώσεων, μέχρι πρόσφατα η πιο συνηθισμένη πρακτική των επιχειρήσεων ήταν να μην κάνουν επίσημη καταγγελία του υπαλλήλου τους αλλά να το αντιμετωπίζουν εσωτερικά και εξωδικαστικά. Οι λόγοι είναι η αποφυγή δυσφήμησης και απώλειας του καλού ονόματος της επιχείρησης από τη γνωστοποίηση ότι αυτή απασχολεί και υποθάλπει ανέντιμους υπαλλήλους. Οι οικονομικές απώλειες από τις κλοπές αντιμετωπίζονταν ως στοιχεία που περιελάμβαναν στα έξοδα τους.

Λόγω όμως του ύψους των απωλειών και της σοβαρότητας των παραβάσεων, ολοένα και περισσότερες επιχειρήσεις πλέον καταγγέλλουν και ασκούν ποινικές διώξεις για τέτοιες περιπτώσεις υπαλλήλων σε ποσοστό 40%, ενώ από ένα άλλο 20% ζητείται η αποκατάσταση των ζημιών.

10.4.4.2. Αντιμετώπιση των υπαίτιων του οικονομικού εγκλήματος από τις επιχειρήσεις

Σύμφωνα με την παραπάνω έρευνα της PcW (για την Ελλάδα), όσον αφορά την αντιμετώπιση των υπαίτιων (είτε εσωτερικών είτε εξωτερικών) οικονομικών εγκλημάτων για το 2011, οι οργανισμοί έδειξαν πολύ μικρότερη ανοχή σε σχέση με το 2009, π.χ. απέλυσαν τους υπαίτιους που βρίσκονταν μέσα στην επιχείρηση σε ποσοστό: 36% για το 2009 και 70% για το 2011, κατέθεσαν αγωγές ή κινήθηκαν δικαστικά 23% για το 2009 και 80% για το 2011. Για τους εξωτερικούς υπαίτιους προέβησαν σε διακοπή συνεργασίας σε ποσοστό 14% για το 2009 και 80% για το 2011 ενώ κινήθηκαν δικαστικά σε ποσοστό 27% και 80% αντίστοιχα. Σημειωτέον ότι τα παραπάνω ποσοστά για την Ελλάδα ήταν σε διπλάσιο μέγεθος σε σχέση με τα αντίστοιχα σε διεθνές επίπεδο.[838]

10.4.5. Πρόληψη του Ξεπλύματος Παράνομου Χρήματος

Το ξέπλυμα παράνομου ή «μαύρου» χρήματος συνίσταται στην προσπάθεια του οικονομικού εγκληματία να παρουσιάσει ως νόμιμα τα χρηματικά ποσά ή περιουσιακά στοιχεία που προήλθαν από παράνομη δραστηριότητα ώστε να αποφύγει τον εντοπισμό του και την κατάσχεση του παράνομου οφέλους.

Η κατάργηση διασυνοριακών ελέγχων, κυρίως στα εσωτερικά σύνορα της Ε.Ε σε συνδυασμό με τη χρησιμοποίηση σύγχρονων τεχνικών και από μεριάς εγκληματιών, διευκολύνουν τη γρήγορη και ανεμπόδιστη μεταφορά χρημάτων - όχι μόνο προερχόμενων από νόμιμες αλλά και από παράνομες δραστηριότητες - από χώρα σε χώρα χωρίς να γίνεται αντιληπτό από τις αρχές.

[837] Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014, βλ. και Πίνακα 13.
[838] Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014, βλ. και Πίνακα 14.

Οι τράπεζες, ως οργανισμοί συγκέντρωσης και αποθήκευσης πλούτου, διατρέχουν μεγαλύτερο κίνδυνο από το ξέπλυμα χρήματος από κάθε άλλο οργανισμό ή επιχείρηση. Μέσω των τραπεζών το παράνομο χρήμα μεταφέρεται εύκολα και γρήγορα σε πολλούς διαφορετικούς λογαριασμούς καθιστώντας τον εντοπισμό του αρχικού καταθέτη –εγκληματία πολύ δύσκολο.

Για τους λόγους αυτούς οι τράπεζες εκτός από τη νομοθεσία, τη συνεργασία με τις διωκτικές και φορολογικές αρχές (κυρίως για την εφαρμογή του «πόθεν έσχες») και με όλους τους οργανισμούς που εμπλέκονται στην αγορά χρήματος, απαιτείται να τηρούν κάποιες στοιχειώδεις διαδικασίες προφύλαξης και αποτροπής ενεργειών που έχουν στόχο το ξέπλυμα χρήματος μέσω των τραπεζικών λειτουργιών. [839] Ταυτόχρονα απαιτείται διακρατική συνεργασία για ανταλλαγή πληροφοριών σχετικά με τραπεζικούς λογαριασμούς που τηρούν πολίτες μιας χώρας σε τράπεζες κάποιας άλλης.

10.5. Μέτρα κοινωνικής πολιτικής

Παράλληλα με τα παραπάνω μέτρα ειδικής (κατά περίπτωση) πρόληψης θα μπορούσαν να ληφθούν μέτρα με ευρύτερο κοινωνικό και οικονομικό χαραχτήρα. Τέτοια μέσα πρόληψης συνδέονται με τη λειτουργία του κοινωνικο-οικονομικού συστήματος και εντάσσονται στη λογική της καταπολέμησης των συνθηκών που ευνοούν τη δημιουργία εγκληματικών ευκαιριών όχι μόνο για εγκλήματα οικονομικής φύσης και άλλων αντικοινωνικών συμπεριφορών. Τέτοια μέτρα μπορούν να είναι:

- Περιορισμός στην υπέρμετρη διαφήμιση που οδηγεί στην υπερκατανάλωση και την τεχνητή δημιουργία αναγκών προβάλλοντας τα ηδονιστικά χαρακτηριστικά των εμπορευμάτων.
- Καλύτερη πληροφόρηση του καταναλωτικού κοινού σχετικά με τις ιδιότητες, τα χαρακτηριστικά και την καταλληλότητα ή την επικινδυνότητα κάποιων προϊόντων.[840]
- Καλλιέργεια και καθιέρωση κώδικα δεοντολογίας στις συναλλαγές.
- Ενημέρωση και ευαισθητοποίηση του κοινού για τα οικονομικά εγκλήματα, ώστε να αυξηθεί ο αριθμός καταγγελιών για τέτοιου είδους εγκλήματα.
- Βελτίωση των συνθηκών και όρων διαβίωσης και εργασίας.
- Βελτίωση των νομοθετικών ρυθμίσεων.
- Ανάπτυξη ή βελτίωση του κλίματος επικοινωνίας μεταξύ εργοδοτών και εργαζομένων στους χώρους εργασίας οργανισμών και επιχειρήσεων.

10.5.1. Ενημέρωση - Διαπαιδαγώγηση για τη χρήση υπολογιστών

Όπως αναφέρει ο Λάζος, οι «τεχνο-εγκληματολόγοι υποστηρίζουν ότι η μόνη αποτελεσματική λύση απέναντι στο ηλεκτρονικό έγκλημα είναι η ηθική διαπαιδαγώγηση και η ανάπτυξη μιας κυβερνο-ηθικής μέσω της καθημερινής πράξης και επαφής με την ηλεκτρονική τεχνολογία». Σημαντικό ρόλο στη μετάδοση και διάδοση αυτής της ηθικής καλούνται να παίξουν τα ΜΜΕ για την ενημέρωση και εκπαίδευση του κοινού. Η διαπαιδαγώγηση μπορεί να γίνει και μέσω του εκπαιδευτικού συστήματος όπου τα παιδιά θα μάθουν από νωρίς τι επιτρέπεται και τι απαγορεύεται στον κυβερνο-χώρο [841].

[839] Για τα μέτρα που μπορούν να λαμβάνουν οι τράπεζες στην κατεύθυνση αυτή βλ. Φιλίππου Α. (2001), σσ.270-280.
[840] Κουράκης Νέστορας (1998), σσ. 304-308
[841] Λάζος Γρηγόρης (2001), σσ . 231-232

Ο όρος "cyber-netiquette" περιγράφει το φαινόμενο που, ενώ δεν είναι άμεσα σχετικό με τον έλεγχο των περισσότερο επιθετικών μορφών ηλεκτρονικού εγκλήματος, συμβάλλει σε έναν βαθμό ευταξίας στον κυβερνοχώρο. Τα ηθικά πρότυπα μπορούν να έχουν σημαντική συμβολή στην ασφάλεια του κυβερνοχώρου. Για τους απλούς χρήστες της πληροφορικής - και σε μερικές τουλάχιστον υπο-κοινότητες του κυβερνοχώρου - παρατηρείται η ανάπτυξη κανόνων ηθικής που χρησιμεύουν στο να αποτραπούν μερικές, τουλάχιστον χαμηλού επιπέδου, κυβερνο-παρανομίες.

10.5.2. Ανωνυμία ή έλεγχος στο ίντερνετ. Περιορισμοί που πρέπει να τίθενται κατά την εφαρμογή των μέτρων πρόληψης και αντιμετώπισης.

Η φύση του διαδικτύου και η πρόσβαση σε αυτό συχνά μπορεί να δημιουργεί στα άτομα το αίσθημα ότι οι όποιες δραστηριότητες τους στον ψηφιακό χώρο είναι αόρατες. Αυτό μπορεί να οδηγεί ορισμένους να κάνουν πράξεις που δεν θα πραγματοποιούσαν δημόσια στο πραγματικό περιβάλλον επειδή αυτές οι πράξεις θα κρίνονταν ανήθικες ή παράνομες. [842]

Η προστασία των προσωπικών δεδομένων είναι ένα από τα πιο σημαντικά αγαθά της σύγχρονης δυτικής κοινωνίας. Όπως και στην πραγματική ζωή, έτσι και στο Internet, η ανωνυμία μπορεί να εκληφθεί ως η ιδιαίτερη ανάγκη του ανθρώπου να διατηρήσει τον προσωπικό του «χώρο». Σε ένα δίκτυο δεδομένων, ο «χώρος» αποκτά το δυσδιάκριτο ορισμό της ιδιωτικής φύσης κάποιων συγκεκριμένων πληροφοριών για το κάθε άτομο.[843] Η ανωνυμία ενός χρήστη στο Internet σημαίνει ότι κανείς δεν είναι σε θέση να εντοπίσει την ταυτότητα του, πέραν αυτών στους οποίους ο ίδιος την έχει αποκαλύψει. Δυστυχώς ή ευτυχώς, το Internet έχει εξαρχής σχεδιαστεί με ολοκληρωτικά διαφορετικό σκεπτικό. Όπως είδαμε και παραπάνω, ο εντοπισμός των χρηστών μέσω της IP που τους παρέχουν οι πάροχοι σύνδεσης στο διαδίκτυο (ISPs) δεν αποτελεί πλέον αδύνατη υπόθεση.

Οι απόψεις, για το αν θα πρέπει να εξασφαλίζεται νομικά και τεχνικά η ανωνυμία των χρηστών του Internet, διίστανται. Ακόμα και το συνταγματικό-νομικό πλαίσιο, εθνικό και διεθνές, δεν ξεκαθαρίζει αν η διατήρηση της ανωνυμίας στο Internet αποτελεί δικαίωμα ή όχι των πολιτών [844]. Το τελευταίο διάστημα μάλιστα, οι διαμάχες μεταξύ αυτών που διεκδικούν το δικαίωμα στη online ανωνυμία και αυτών που επιδιώκουν ακριβέστερη ταυτοποίηση των χρηστών του Internet είναι πιο έντονες από ποτέ.

Οι διαδικτυακές οργανώσεις[845] υπεράσπισης των δικαιωμάτων του χρήστη του Internet προσπαθούν να πείσουν, πέρα από τις διάφορες κυβερνητικές αρχές και τους πολλούς ανεξάρτητους οργανισμούς πολιτών, για την αντιμετώπιση online κινδύνων π.χ. καταπολέμηση του κυβερνο-εγκλήματος, της παιδικής πορνογραφίας, των διαφόρων μορφών προπαγάνδας κλπ., για το ορθό του δικαιώματος στην ανωνυμία. Με τα τρέχοντα δεδομένα, οι ισχύοντες μηχανισμοί ελέγχου είναι τόσο χαλαροί, που επιτρέπουν σε διάφορους επιτήδειους να στέλνουν χιλιάδες spam και fraud mails, να στήνουν διαδικτυακές επιχειρήσεις ακόμα και να μεταπωλούν online απαγορευμένα και ελεγχόμενα φάρμακα και όχι μόνο.

[842] Jahankhani Hamid & Al-Nemrat Ameer (2011), ό.π.
[843] Berman Jerry & Bruening Paula (2001), σσ. 306-18
[844] Electronic Frontier Fountation,"Anonymity", February 2006, http://www.eff.org/anonymity.htm
[845] http://www.eff.org , www.epic.org, www.efga.org, www.privacyrights.org, www.aclu.org, www.ipc.org www.rightoprivacy.com, www.privacy.org/ipc, www.computerprivacy.org, www.bigbrotherinside.org, www.privacy.org.

Ένας πιο αυστηρός έλεγχος της ταυτότητας των χρηστών του Internet θα είχε ως αποτέλεσμα την πιο αποτελεσματική καταπολέμηση όλων αυτών των κινδύνων, αλλά από την άλλη θα στερούσε από τη συντριπτική πλειονότητα των χρηστών την ψευδαίσθηση της ελευθερίας της έκφρασης, όπως για παράδειγμα, τη δυνατότητα να μπει ο χρήστης σε ένα forum και να υποστηρίξει ακόμα και την πιο ακραία άποψη, γνωρίζοντας ότι κανείς ή λίγοι θα είναι αυτοί που θα γνωρίζουν ποιος είναι στην καθημερινότητα του.[846]

Από την άλλη, η ελευθερία έκφρασης μπορεί και αυτή υπό συνθήκες να αποτελέσει πρόβλημα για την κοινωνία. Διαδικτυακές οργανώσεις που απαρτίζονται από ανθρώπους με εχθρική προς τους άλλους στάση ζωής, όπως ακραίες σεξουαλικές συμπεριφορές, πολιτικές, ιδεολογικές, θρησκευτικές και φυλετικές πεποιθήσεις και τα οποία σχηματίστηκαν χάρη στην ανωνυμία των μελών τους, με δεδομένο ότι η «ψηφιακή κοινωνική κατακραυγή» δεν έχει σε καμιά περίπτωση τις ίδιες επιπτώσεις με την κοινωνική αποδοκιμασία, αποκτούν οντότητα, προβάλλονται και το χειρότερο καλλιεργούν συνειδήσεις. Ο λόγος τους φθάνει σε άτομα με χαμηλές αντιστάσεις (παιδιά, εφήβους, απαίδευτους, εύπιστους), τα οποία οφείλουν να προφυλαχθούν από την κακή χρήση της ανωνυμίας. Το οξύμωρο είναι πως αυτοί που υπερασπίζονται το δικαίωμα της ανωνυμίας στο Internet αλλά και αυτοί που αντιτίθενται σε αυτό, επικαλούνται τα ίδια κίνητρα, τους ίδιους λόγους: την προστασία του πολίτη, της δημοκρατίας και της ελευθερίας. Όπως διαπιστώνουμε, το θέμα «ανωνυμία στο Internet» δεν είναι τεχνικό ή απλά νομικό, έχει πολιτικές προεκτάσεις και συχνά καταλήγει σε ιδεολογικό αδιέξοδο.

Κατά την εφαρμογή των μέτρων πρόληψης και αντιμετώπισης της ηλεκτρονικο-οικονομικής εγκληματικότητας θα πρέπει πάντα να λάβουμε υπόψη μας και τους κινδύνους προσβολής της ιδιωτικής μας ζωής και των συνταγματικά κατοχυρωμένων ατομικών δικαιωμάτων που εγκυμονεί η χρήση των ηλεκτρονικών μεθόδων πρόληψης και καταστολής όπως είναι οι κάμερες παρακολούθησης σε δημόσιους και άλλους χώρους, η εισβολή στο σύστημα οικιακών υπολογιστών, η χρήση ηλεκτρονικών προσωπικών δεδομένων και άλλες αυθαιρεσίες με το πρόσχημα της ανακάλυψης πιθανών εγκληματικών ενεργειών. Τελικά είναι ζήτημα του τι είδους κοινωνία και κράτος επιδιώκουμε: μια κοινωνία «ελέγχου και ασφάλειας» ή μια κοινωνία «δικαίου και προστασίας ελευθεριών». Η ισορροπία ανάμεσα στα δυο δεν είναι ούτε εύκολη ούτε αυτονόητη.

Η τεχνολογία είναι ένα μέσο που ανάλογα με τη χρήση που του γίνεται μπορεί να ωφελήσει ή να βλάψει. Το αν θα συμβεί το πρώτο ή το δεύτερο εξαρτάται από το ποιος χρησιμοποιεί αυτό το μέσο, με ποιο τρόπο και για ποιο σκοπό. Η συνθήκη Σένγκεν, οι «τρομονόμοι», τα μέτρα που λαμβάνονται για την – δήθεν – ασφάλεια των πολιτών, ειδικά μετά το χτύπημα στους δίδυμους πύργους στη Ν. Υόρκη και στο Λονδίνο και τα συστήματα παρακολούθησης (όπως το ECHELON και οι περιπτώσεις υποκλοπών τηλεφωνικών συνδιαλέξεων - όπως οι πρόσφατα αποκαλυφθείσες μέσω δικτύου κινητής τηλεφωνίας στη χώρα μας[847]), αποτελούν μάλλον προάγγελους μιας περισσότερο αστυνομοκρατούμενης κοινωνίας με αύξηση των μηχανισμών ελέγχου και παρακολούθησης των πολιτών με συνακόλουθη περιστολή προσωπικών ελευθεριών και δικαιωμάτων. Η σύγχρονη τεχνολογία, δυστυχώς μπορεί να αποτελέσει επίκουρο και τέτοιων πρακτικών.

[846] Privacy international, "Freedom of Expression", ανακτήθηκε από www.privacyinternational.org/index.shtml, Ιανουάρ. (2007)
[847] Βλ. Παράρτημα: «Περίπτωση τηλεφωνικών υποκλοπών».

ΚΕΦΑΛΑΙΟ 11. ΣΥΜΠΕΡΑΣΜΑΤΑ - ΣΥΖΗΤΗΣΗ

Η παγκοσμιοποίηση και το νεοφιλελεύθερο οικονομικό περιβάλλον, οι υπερεθνικοί πολιτικο–οικονομικοί συνασπισμοί κρατών, όπως η Ευρωπαϊκή Ένωση και οι εξελίξεις της τεχνολογίας τις τελευταίες δεκαετίες, δημιουργούν οικονομικές και πολιτισμικές ευκαιρίες που πριν δεν ήταν διαθέσιμες. Οι αποστάσεις εκμηδενίζονται, από άποψη χρόνου διάνυσης και οι επιρροές είναι παγκόσμιες.

Η εισαγωγή νέων τεχνολογιών συναλλαγών και η εφαρμογή της πληροφορικής τεχνολογίας, όχι μόνο στην οικονομία, αλλά και στην καθημερινή ζωή, έχει αλλάξει ριζικά τις κοινωνικές σχέσεις και δημιουργεί νέα πρότυπα για το έγκλημα και κυρίως το οικονομικό που εκσυγχρονίζεται και από παραδοσιακό μετατρέπεται σε ηλεκτρονικό. Η αυξανόμενη εξάρτηση των σύγχρονων επιχειρήσεων και οργανισμών από τα συστήματα πληροφορικής και υπολογιστών τις κατέστησε περισσότερο ευάλωτες στο ηλεκτρονικό έγκλημα. Όλοι αυτοί οι παράγοντες, που από τη μια έδωσαν ώθηση στην οικονομική δραστηριότητα και αύξησαν τους οικονομικούς δείκτες, από την άλλη δημιούργησαν νέες ευκαιρίες και προοπτικές για παραδοσιακές αλλά και για καινοφανείς παράνομες οικονομικές δραστηριότητες.

Τις τελευταίες δεκαετίες εμφανίζεται μια ιδιαίτερη μορφή οικονομικού εγκλήματος που χρήζει διερεύνησης και η οποία προσδιορίζεται από το αντικείμενο της αξιόποινης πράξης ή και από τα μέσα τέλεσης που αποτελεί το ηλεκτρονικό -οικονομικό έγκλημα.

Οι σύγχρονες θεωρητικές και ερευνητικές προσπάθειες, λαμβάνοντας υπόψη τις νέες συνθήκες και προκλήσεις της ψηφιακής εποχής, καλούνται να εκτιμήσουν εμπειρικά το φαινόμενο αποτυπώνοντας την έκτασή του, τα χαρακτηριστικά, τον τρόπο τέλεσής του, τόσο με ποσοτικά όσο και με ποιοτικά δεδομένα. Καλούνται ακόμα να διατυπώσουν σύγχρονες θεωρητικές οπτικές για τη μελέτη του εγκλήματος και να αναζητήσουν απαντήσεις πάνω στους παράγοντες που το προκαλούν ώστε να μπορέσουν να προτείνουν λύσεις.

Το αντικείμενο του ανά χείρας πονήματος αποτέλεσε το ηλεκτρονικο-οικονομικό έγκλημα από την οπτική των νεότερων προσεγγίσεων για τη δόμηση των εγκληματικών ευκαιριών. Πιο συγκεκριμένα στόχο της παρούσας διατριβής αποτέλεσε η εφαρμογή των θεωριών της ορθολογικής επιλογής, των καθημερινών δραστηριοτήτων, των εγκληματικών προτύπων και η στρατηγική της περιστασιακής πρόληψης του εγκλήματος, για την κατασκευή του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος. Οι προσεγγίσεις αυτές βοηθούν να εστιάσουμε περισσότερο στο εγκληματικό γεγονός καθαυτό, στον τρόπο που αυτό συμβαίνει παρά στις γενεσιουργές αιτίες του. Η οπτική που υιοθετούν επιτρέπει τη μελέτη και την κατανόηση του «πώς» συμβαίνουν και του γιατί τα εγκλήματα δεν κατανέμονται ομοιόμορφα στον χώρο και τον χρόνο αλλά διαφοροποιούνται. Η διαφοροποίηση αυτή οφείλεται κυρίως στην ύπαρξη των διαφορετικών κατάλληλων ευκαιριών που παρουσιάζονται στους δράστες και οι οποίες δομούν το εγκληματικό πρότυπο. Αν και μέχρι τώρα, οι παραπάνω θεωρητικές προσεγγίσεις, εφαρμόστηκαν στη μελέτη και στον αποτελεσματικότερο σχεδιασμό της αποτροπής του κοινού εγκλήματος, μέσω της αλλαγής του εγκληματικού προτύπου δηλαδή των δομών που συνθέτουν την εγκληματική ευκαιρία (δράστης, θύμα, τόπος, χρόνος, νόμος), προτάθηκε από την παρούσα μελέτη, να εφαρμόζονται πλέον και στη διερεύνηση και την αντιμετώπιση των ηλεκτρονικο-οικονομικών εγκλημάτων.

Το αντικείμενο της παρούσας διατριβής διερευνήθηκε κυρίως με τη μέθοδο της συστηματικής βιβλιογραφικής ανασκόπησης. Από την κριτική ανάλυση σχετικών μελετών από

την υπάρχουσα βιβλιογραφία, για τη διακρίβωση των ερευνητικών μας ερωτημάτων, προκύπτει συνοπτικά η παρακάτω σύνθεση αποτελεσμάτων που αφορούν τη διαμόρφωση του εγκληματικού προτύπου του ηλεκτρονικο-οικονομικού εγκλήματος.

Η διερεύνηση της πρώτης από τις επιμέρους υποθέσεις της μελέτης μας, που αφορά το βαθμό συσχέτισης του ηλεκτρονικού εγκλήματος με το οικονομικό έγινε αντιπαραβάλλοντας τα χαρακτηριστικά τους και διακρίνοντας τα ηλεκτρονικά εγκλήματα σε δυο μεγάλες βασικές κατηγορίες. Πρώτα, τα γνήσια ηλεκτρονικά, δηλαδή αυτά που δεν θα μπορούσαν να τελεστούν αν δεν υπήρχε το ηλεκτρονικό περιβάλλον που παρέχει ο υπολογιστής, τα ψηφιακά δίκτυα, το διαδίκτυο, οι τηλεπικοινωνίες κλπ, όπως είναι η μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικούς υπολογιστές, η δολιοφθορά συστημάτων ηλεκτρονικών υπολογιστών με τη διασπορά κακόβουλου λογισμικού, οι επιθέσεις άρνησης υπηρεσιών ηλεκτρονικού υπολογιστή κλπ. Στη δεύτερη ευρύτερη κατηγορία εξετάστηκαν τα οικονομικά εγκλήματα που προϋπήρχαν και χρησιμοποιούν τον υπολογιστή ή και το διαδίκτυο ως μέσο ή εργαλείο που διευκολύνει την διάπραξη τους, όπως οι διάφορες εμπορικές και οικονομικές απάτες στο διαδίκτυο, οι απάτες με επιταγές, οι απάτες με πιστωτικές κάρτες, οι χρηματοοικονομικές απάτες όπως οι πυραμίδες και οι επενδυτικές απάτες, η παράνομη μεταφορά κεφαλαίων, το ξέπλυμα μαύρου χρήματος στο διαδίκτυο, η βιομηχανική κατασκοπεία και άλλες μορφές οικονομικού εγκλήματος που τελούνται με σύγχρονα μέσα όπως με τη χρήση ηλεκτρονικών υπολογιστών και που απαρτίζουν το ηλεκτρονικο-οικονομικό έγκλημα.

Η συνεξέταση των χαρακτηριστικών του εγκληματικού προτύπου του ηλεκτρονικού με αυτά του οικονομικού εγκλήματος οδήγησε στο συμπέρασμα ότι οι αυτές οι δυο μορφές εγκληματικότητας μοιράζονται σημαντικότατο τμήμα κοινού τόπου. Πιο συγκεκριμένα:

Τα περισσότερα από τα είδη της οικονομικής εγκληματικότητας βρίσκουν νέα μέσα (διόδους) διάπραξης μέσω των ηλεκτρονικών υπολογιστών και του κυβερνοχώρου. Ελάχιστα είναι τα σύγχρονα οικονομικά εγκλήματα που δεν χρησιμοποιούν τη ψηφιακή τεχνολογία. Από την άλλη πλευρά, τα περισσότερα από τα ηλεκτρονικά εγκλήματα αποκτούν οικονομικό χαρακτήρα, έχουν οικονομικό στόχο και κίνητρα, έτσι ώστε να εντάσσονται στις σύγχρονες μορφές των οικονομικών εγκλημάτων. Ακόμα, πολλές από τις κατηγορίες του ηλεκτρονικού εγκλήματος παρουσιάζουν σημαντικά κοινά στοιχεία με τα παραδοσιακά εγκλήματα λευκού περιλαιμίου. Οι δράστες τους, αν και δεν είναι απαραίτητο να ανήκουν στα μεσαία ή ανώτερα στρώματα, διαθέτουν εξειδικευμένες γνώσεις και εμπειρία σε θέματα τεχνολογίας, διαπράττουν τα εγκλήματα τους χωρίς χρήση φυσικής βίας, κυρίως κατά τη διάρκεια νόμιμης ενασχόλησης, διαφεύγουν της σύλληψης ή αποφεύγουν την καταδίκη. Γενικά διαθέτουν πολλά από τα χαρακτηριστικά των εγκληματιών του λευκού περιλαιμίου, σε βαθμό που μελετητές όπως ο Grabosky, θεωρούν ότι τα ηλεκτρονικο-οικονομικά εγκλήματα είναι «τύπου λευκού περιλαιμίου. Ο μεγάλος «σκοτεινός αριθμός» αυτών των εγκλημάτων, λόγω χαμηλής θεατότητας, μειωμένου αριθμού καταγγελιών, εξωδικαστικής διευθέτησης στο πλαίσιο των επιχειρήσεων, που καλλιεργούν τον ανταγωνισμό -και μεταξύ των στελεχών τους- και διαθέτουν ελαστικότερους εσωτερικούς κυρωτικούς μηχανισμούς σε σχέση με τις ποινές που επιβάλλονται από τον επίσημο κοινωνικό έλεγχο, η έλλειψη συγκεκριμένου θύματος και η απροσδιοριστία του οικονομικού έννομου αγαθού που προσβάλλεται, έχουν ως αποτέλεσμα να αποτελούν μειοψηφία εκείνοι οι δράστες που τελικά ελέγχονται από τους μηχανισμούς του επίσημου κοινωνικού ελέγχου. Από τους δράστες που επισημαίνονται, λίγοι συλλαμβάνονται, λιγότεροι διώκονται ποινικά και ελάχιστοι είναι όσοι τελικά καταδικάζονται,

είτε επειδή μπορούν να προσλάβουν ικανότατους και ακριβούς συνηγόρους υπεράσπισης είτε και λόγω απροθυμίας των δικαστών να καταδικάσουν ανθρώπους «υπεράνω κάθε υποψίας» που δεν ανταποκρίνονται στο καθιερωμένο εγκληματικό στερεότυπο.

Για το δεύτερο ερευνητικό ερώτημα, οι έρευνες που εξετάσαμε διαπίστωσαν ότι ο κίνδυνος θυματοποίησης του ατόμου σχετίζεται με το τι κάνει, με ποιες δραστηριότητες ασχολείται, με το αν αυτές οι δραστηριότητες το φέρουν σε εγγύτητα με πιθανούς δράστες και με το αν και πώς προστατεύει τον εαυτό του.

Το κύριο χαρακτηριστικό στον ψηφιακό χώρο είναι η απουσία φυσικής επικοινωνίας και φυσικής αλληλεπίδρασης, η εξ αποστάσεως επικοινωνία και η ανωνυμία (ή η αίσθηση της ανωνυμίας). Το ψηφιακό περιβάλλον παρέχει τον απαιτούμενο «χώρο» που διασυνδέει πιθανούς δράστες με κατάλληλα θύματα – στόχους. Στη διάρκεια των συνηθισμένων ψηφιακών δραστηριοτήτων τους οι δράστες συναντούν την κατάλληλη εγκληματική ευκαιρία κινούμενοι σε γνώριμα «κομβικά» σημεία, όπως δίκτυα επικοινωνίας, διαδίκτυο, δωμάτια συζητήσεων (chat rooms) ή άλλα ψηφιακά μέσα που χρησιμοποιούν καθημερινά.

Σημαντικός παράγοντας στη διαμόρφωση της εγκληματικής ευκαιρίας είναι η εγγύτητα (proximity) του στόχου σε πιθανούς δράστες, σύμφωνα με τη θεωρία των καθημερινών δραστηριοτήτων και του τρόπου ζωής, L-RAT. Το να βρίσκεται κανείς σε επαφή, φυσική ή ψηφιακή, σε κοινά δίκτυα με παραβάτες εμπλεκόμενος και ο ίδιος σε παραβατικές συμπεριφορές αυξάνει τον κίνδυνο θυματοποίησης. Έτσι, μεγαλύτερο κίνδυνο θυματοποίησης διατρέχουν οι χρήστες που επιδεικνύουν πλημμελή διαδικτυακή συμπεριφορά περνώντας πολλές ώρες σε ριψοκίνδυνες διαδικτυακές δραστηριότητες, χωρίς τη λήψη απαραίτητων μέτρων προστασίας που λειτουργούν ως ικανοί φύλακες του υπολογιστή τους. Πολλές από τις έρευνες διαπίστωσαν ότι έχει σημασία για τη θυματοποίηση ο χρόνος που περνά κανείς ασχολούμενος με ψηφιακές δραστηριότητες και κυρίως το ποιες είναι αυτές οι δραστηριότητες και που διαδραματίζονται.[848] Ριψοκίνδυνες ψηφιακές συμπεριφορές βρέθηκε ότι αποτελούν η επίσκεψη σε άγνωστες ιστοσελίδες, το κατέβασμα αρχείων μουσικής, βίντεο ή δωρεάν προγραμμάτων, το κλικάρισμα σε εικόνες. Στο τμήμα που αφορά την θυματοποίηση από την οικονομική εγκληματικότητα μέσω ψηφιακής τεχνολογίας (καθαρά ηλεκτρονικο-οικονομικό έγκλημα), ριψοκίνδυνη καθημερινή ψηφιακή δραστηριότητα αποτελεί η αυξημένη συχνότητα οικονομικής δραστηριότητας, όπως συναλλαγές εξ αποστάσεως μέσω ίντερνετ, τηλεφώνου, e-banking, e-mail που συνδέονται με αυξημένη έκθεση των χρηστών στον κίνδυνο θυματοποίησης: όσο περισσότερες ώρες περνάει κανείς στο διαδίκτυο και όσο περισσότερες διαδικτυακές συναλλαγές πραγματοποιεί, τόσο πιο αυξημένη είναι η πιθανότητα να γίνει στόχος διαδικτυακής απάτης.

Επίσης, όσον αφορά τα ατομικά χαρακτηριστικά, βρέθηκε ότι οι νέοι, οι άνδρες, οι ιδιοκτήτες ακινήτου και οι πιο μορφωμένοι αφιερώνουν μεγαλύτερο χρόνο στο διαδίκτυο, ενώ περισσότερες αγορές πραγματοποιούν οι πιο εύρωστοι οικονομικά, οι παντρεμένοι, οι ιδιοκτήτες σπιτιών και οι πιο μορφωμένοι.

Σε επίπεδο χωρών διαπιστώθηκε, από τον Kigerl, ότι στις πλουσιότερες χώρες, με καλύτερη τεχνολογία και περισσότερους ειδικούς πληροφορικής τεχνολογίας, το μέγεθος των χρηστών του ίντερνετ σχετίζεται θετικά με την εμφάνιση κυβερνοεγκλήματος, επειδή η ύπαρξη πολλών χρηστών συνδέεται τόσο με την πληθώρα κατάλληλων στόχων όσο και πιθανών δραστών.[849] Όσο πιο πολλούς χρήστες διαδικτύου διαθέτει και πιο πλούσια είναι

[848] Mustaine Elizabeth E. & Tewksbury Richard (1998)
[849] Kigerl Alex (2012)

μια χώρα σε επίπεδο κατά κεφαλήν εισοδήματος, τόσο πιο αυξημένους δείκτες κυβερνο-εγκληματικής δραστηριότητας παρουσιάζει.

Στο πλαίσιο του τρίτου ερωτήματος διερευνήθηκε το στοιχείο της ορθολογικότητας ως προς το κίνητρο που ενεργοποιεί τη δράση των ηλεκτρονικο – οικονομικών εγκληματιών. Υποθέσαμε ότι τα άτομα, όπως σε κάθε άλλη ανθρώπινη συμπεριφορά, έτσι και κατά την παράνομη δράση τους σταθμίζουν την καταλληλότητα μιας εγκληματικής ευκαιρίας στην βάση του σχήματος «αναμενόμενο κέρδος έναντι αναμενόμενου κόστους». Ακόμα υποθέσαμε ότι οι δράστες των ηλεκτρονικο-οικονομικών εγκλημάτων λειτουργούν με περιορισμένη ορθολογικότητα, ως προς το κίνητρο για την επιλογή του στόχου τους, με βάση την υποκειμενική εκτίμησή τους για το αναμενόμενο όφελος σε σχέση με το αναμενόμενο κόστος.

Σύμφωνα με τα ευρήματα της βιβλιογραφικής μας έρευνας, σημαντικά για τη διάπραξη του ηλεκτρονικο-οικονομικού εγκλήματος είναι τα κίνητρα για ικανοποίηση αναγκών όπως απόκτηση πλούτου, χρήματος, φήμης, ατομικής επιτυχίας, με αναμενόμενο όφελος την «αποφυγή της πτώσης» από το κοινωνικό status, δηλαδή την διατήρηση των κεκτημένων από τα μέλη της μεσαίας τάξης, όπως του τρόπου ζωής και της επαγγελματικής θέσης. Τα παραπάνω κίνητρα αποτελούν αξίες - στόχους που θέτει στα μέλη της η σύγχρονη (δυτική) κοινωνία, η οικονομία της αγοράς και η κουλτούρα του ανταγωνισμού που καλλιεργείται στις επιχειρήσεις και που εξάρει την επιδίωξη του μέγιστου οφέλους.

Αναμενόμενα κόστη για τον πιθανό εγκληματία αποτελούν θυσίες σε χρόνο, κόπο, χρήμα, ο κίνδυνος επισήμανσης και καταδίκης, με συνακόλουθη απώλεια επαγγελματικής θέσης και κύρους για την υποπερίπτωση των εγκληματιών του λευκού περιλαιμίου.

Ο δράστης υπολογίζει ορθολογικά τα οφέλη και τα κόστη, με βάση την προσπάθεια που απαιτείται και τους πιθανούς κινδύνους που συνεπάγεται η διάπραξη του εγκλήματος, τις ανταμοιβές, τις ευκαιρίες που ευνοούν τη δράση και τις εκλογικεύσεις που κάνει πριν προβεί στην τέλεση του εγκλήματος. [850]

Η ορθολογικότητα - ή μη - της απόφασης του πιθανού δράστη να τελέσει αδίκημα πρέπει να θεωρείται υποκειμενική και περιορισμένη. Το στοιχείο της υποκειμενικότητας σημαίνει ότι ο δράστης δεν κάνει πάντα τις καλύτερες δυνατές επιλογές και η ορθολογικότητά του δεν είναι απόλυτη αλλά σχετική και «περιορισμένη». Η ορθολογικότητα περιορίζεται από τα πληροφοριακά δεδομένα, το χρόνο, τις εναλλακτικές επιλογές που διαθέτει, τις ευκαιρίες που παρουσιάζονται και που διαφέρουν σε κάθε άτομο και σε κάθε δεδομένη χρονική στιγμή. Για τα ηλεκτρονικά εγκλήματα τύπου λευκού περιλαιμίου θεωρείται ότι μπορεί να εφαρμοστεί το στοιχείο της «περιορισμένης» ορθολογικότητας.

Το έγκλημα είναι πιο πιθανό να τελεστεί όταν διαθέτει ευκολία διάπραξης, χαμηλό κίνδυνο επισήμανσης, υψηλό αναμενόμενο όφελος, δικαιολογία και ευνοείται από τις ευκαιρίες που παρουσιάζονται περιστασιακά.[851] Τα χαρακτηριστικά αυτά όπως διαπιστώσαμε ισχύουν και για τα ηλεκτρονικο-οικονομικά εγκλήματα.

Εκτός από το *κίνητρο* απαιτείται η εμφάνιση και της κατάλληλης *ευκαιρίας* και να γίνουν οι απαραίτητες *εκλογικεύσεις* από πλευράς του δράστη. Ο τρόπος κατανομής των ευκαιριών σε σχέση με τα κίνητρα συναποτελούν το ιδιαίτερο σκηνικό για τη διάπραξη του ηλεκτρονικο-οικονομικού εγκλήματος. Οι εκλογικεύσεις αποτελούν απαραίτητο συμπλήρωμα των κινήτρων και σχηματίζονται στο πλαίσιο της ευκαιριακής εγκληματικής δομής ως απάντηση

[850] Cornish Derek και Clarke Roland (1986)
[851] Benson Michael L., Madensen Tamara D., & Eck John E. (2009)

και ως συμβολική κατασκευή για τη ψυχολογική προετοιμασία του δράστη για την άρση των όποιων επιφυλάξεων εκ μέρους του. Το κίνητρο ως αποτέλεσμα ατομικής νοητικής κατασκευής αποτελεί την υποκειμενική διάσταση του εγκληματικού προτύπου, ενώ η ευκαιρία την αντικειμενική διάσταση γιατί δομείται από τις κοινωνικές συνθήκες.[852]

Τα ορθολογικά στοιχεία που δομούν την εγκληματική ευκαιρία αποτελούν η εγγύτητα του στόχου στον δράστη, η ύπαρξη ευάλωτου στόχου που δεν διαθέτει επαρκή φύλαξη, το υψηλό αναμενόμενο όφελος και ο χαμηλός κίνδυνος σύλληψης και επιβολής ποινής.

Αξιοσημείωτο είναι ότι οι δράστες, όπως διαπίστωσαν οι έρευνες[853], λειτουργώντας ορθολογικά, προτιμούν να πλήξουν στόχους την καταλληλότητα των οποίων έχουν ήδη διαπιστώσει από προηγούμενη δράση παρά να αναζητούν νέους, αμφίβολης καταλληλότητας στόχους. Από την πλευρά του θύματος η προηγούμενη θυματοποίηση αυξάνει την πιθανότητα επαναλαμβανόμενης θυματοποίησης.

Το τέταρτο ερώτημα της έρευνας αφορούσε, αφενός το αν η έλλειψη ικανών φυλάκων, δημιουργεί κατάλληλες εγκληματικές ευκαιρίες και συνδέεται με τον κίνδυνο θυματοποίησης και αφετέρου αν η ύπαρξή τους, και με ποια μορφή, αποτελεί αποτελεσματικότερο μέσο πρόληψης της ηλεκτρονικο-οικονομικής εγκληματικότητας. Το κατάλληλο υπόβαθρο στον τομέα αυτό παρέχει η *στρατηγική της περιστασιακής πρόληψης του εγκλήματος* η οποία συνδυάζει τις προσεγγίσεις της περιβαλλοντικής εγκληματολογίας για τη δόμηση των «εγκληματικών ευκαιριών» στο ζήτημα της αντιμετώπισης. Στο επίπεδο της πρόληψης τα διάφορα μέτρα έχουν στόχο τη μείωση του ηλεκτρονικο-οικονομικού εγκλήματος μέσω τεχνικών που επηρεάζουν και αλλοιώνουν τη δόμηση της εγκληματικής ευκαιρίας, την απόφαση των πιθανών δραστών για δράση και καθιστούν την εμπλοκή τους σε αυτό λιγότερο πιθανή.

Το ενδιαφέρον για αποτελεσματικότερη και λιγότερο δαπανηρή, από άποψη διαθέσιμων πόρων, πρόληψη και αντιμετώπιση, εστιάστηκε στη λήψη μέτρων που θα θωρακίζουν το στόχο – θύμα, θα το καθιστούν λιγότερο ευάλωτο, άρα και λιγότερο ελκυστικό, το έγκλημα λιγότερο προσοδοφόρο, θα αυξάνουν την φύλαξη και την πιθανότητα επισήμανσης του δράστη, ώστε αυτός είτε να αποτρέπεται είτε να συλλαμβάνεται ευκολότερα. Υπό την οπτική αυτή η πιθανότητα εμφάνισης της εγκληματικής ευκαιρίας μπορεί να μειωθεί και να αυξηθεί η πιθανότητα αποκάλυψης του δράστη με τη χρήση πιο «ικανής φύλαξης» στα διάφορα επίπεδα ελέγχου:

Πρώτα σε επίπεδο φυσικής φύλαξης ή επίσημου κοινωνικού ελέγχου, η αντιμετώπιση μπορεί να γίνεται μέσω της ενίσχυσης του ρόλου, της αποτελεσματικότητας και της ικανότητας των υπηρεσιών δίωξης του εγκλήματος και των δικαστικών αρχών, τον εκσυγχρονισμό και εναρμονισμό των κρατικών νομοθεσιών με τις διεθνείς συμβάσεις, την ενίσχυση των αρχών δίωξης με προσωπικό που έχει τις απαραίτητες γνώσεις και εξοπλισμό.

Δεύτερο, σε επίπεδο ανεπίσημου κοινωνικού ελέγχου. Το ρόλο ικανών φυλάκων μπορούν να αναλαμβάνουν φορείς και πάροχοι τηλεπικοινωνιών, επαγγελματίες πληροφορικής τεχνολογίας.

Τρίτο, σε επίπεδο θωράκισης, «σκλήρυνσης» του στόχου και αυτοελέγχου, η πιθανότητα εμφάνισης της ευκαιρίας μειώνεται με την ενίσχυση των φυσικών μέσων ασφάλειας, όπως τη χρήση αντιβιοτικών προγραμμάτων και ασπίδων προστασίας σε ψηφιακές συσκευές που

[852] Coleman James (1987)
[853] Farrell Graham, Clark Ken, Ellingworth Dan, Pease Ken (2005)

συνδέονται στο διαδίκτυο για την αντιμετώπιση των ψηφιακών εγκληματιών.[854] Στο ζήτημα αν ως «ικανοί ψηφιακοί φύλακες θεωρούνται προγράμματα προστασίας του υπολογιστή, όπως αντιικά, τείχη προστασίας και αντικατασκοπευτικά, τα αποτελέσματα των υπό εξέταση ερευνών ήταν αντιφατικά. Κάποιες έρευνες, όπως του Choi επιβεβαίωσαν την αποτελεσματικότητα της ύπαρξης τέτοιων προγραμμάτων[855] ενώ άλλες, όπως του Ngo, όχι[856]. Θα πρέπει πάντα να έχουμε υπόψη ότι η αποτελεσματικότητα του κάθε μέτρου προστασίας διαφέρει ανάλογα με το είδος της απειλής που αυτό καλείται να αντιμετωπίσει.

Η εγγύτητα, δηλαδή ο συγχρωτισμός με παραβατικές ομάδες (συμμετέχοντας σε chat-rooms), η εμπλοκή των ίδιων των χρηστών σε παράνομη ή ριψοκίνδυνη συμπεριφορά («κατεβάζοντας» παράνομα αρχεία), σύμφωνα με τα συμπεράσματα ερευνών των Bossler και Holt, αυξάνει την έκθεσή τους σε πιθανούς δράστες. Όπως προκύπτει από τα συμπεράσματα των ερευνών η μείωση των οικονομικά ριψοκίνδυνων συμπεριφορών, μέσω κατάλληλων προγραμμάτων ενημέρωσης του κοινού, κυρίως των χρηστών των ψηφιακών μέσων, θα οδηγήσει και στη μείωση των πιθανοτήτων θυματοποίησης για τις περιπτώσεις ηλεκτρονικο-οικονομικών εγκλημάτων.[857] Έτσι προτείνεται τα άτομα να εκπαιδεύονται και να ενημερώνονται από ειδικούς για να μπορούν αυτοπροστατεύονται και να αποφεύγουν διαδικτυακές και οικονομικές συμπεριφορές που τα εκθέτουν σε κινδύνους.[858]

Τα μέτρα αυτά, για την προστασία από το οικονομικό και το ηλεκτρονικό - οικονομικό έγκλημα, μπορούν να κατηγοριοποιηθούν σε μέτρα κοινωνικής πολιτικής ή νομοθετικά μέτρα που λαμβάνονται κυρίως από τις κυβερνήσεις (σε συνεργασία με την Ευρωπαϊκή Ένωση, για τις χώρες-μέλη) και σε ειδικά μέτρα πρόληψης και ασφάλειας που μπορούν να παίρνουν άτομα και επιχειρήσεις.

Σύμφωνα με τα παραπάνω αποτελέσματα θεωρούμε ότι επιβεβαιώνονται σε μεγάλο βαθμό οι επιμέρους ερευνητικές υποθέσεις της μελέτης μας και ως εκ τούτου το ηλεκτρονικο-οικονομικό έγκλημα έχει ευκαιριακή δομή και το γενικό του πρότυπο διατυπώνεται με συντομία ως εξής:

«Οι δράστες με κίνητρο, όταν συναντούν την κατάλληλη ευκαιρία στο πλαίσιο της καθημερινής τους ενασχόλησης σε ψηφιακό περιβάλλον, κάνουν τις απαραίτητες εκλογικεύσεις και, σταθμίζοντας το αναμενόμενο όφελος σε σχέση με το κόστος, παίρνουν την ορθολογική απόφαση να θυματοποιήσουν εξ αποστάσεως στόχους που δεν διαθέτουν ικανή φύλαξη».

Η διερεύνηση του φαινομένου της ηλεκτρονικο-οικονομικής εγκληματικότητας δυσχεραίνεται από την ύπαρξη του σκοτεινού αριθμού, τη δυσκολία επισήμανσης, εξιχνίασης και δίωξης των ηλεκτρονικών και οικονομικών εγκλημάτων και τη δυσκολία τήρησης στατιστικών αρχείων καταγραφής από τις διωκτικές αρχές. Οι παράγοντες αυτοί, συνοδεύονται από τη σχετική έλλειψη ικανοποιητικού αριθμού αξιόπιστων ερευνών και μελετών πάνω στο θέμα και αποτέλεσαν σημαντικούς περιορισμούς και δυσκολίες για την παρούσα μελέτη.

Περιορισμούς της βιβλιογραφικής μας έρευνας αποτέλεσαν συγκεκριμένα, η έλλειψη σχετικών εμπειρικών ερευνών από την ελληνική βιβλιογραφία, το γεγονός ότι οι

[854] Jahankhani Hamid και Al-Nemrat Ameer (2011)
[855] Choi Kyung-shick (2008a) και (2008b)
[856] Ngo Fawn (2011)
[857] Holtfreter, Reisig, και Pratt (2008)
[858] Bossler Adam & Holt Thomas (2009)

περισσότερες από τις προϋπάρχουσες μελέτες της ξενόγλωσσης βιβλιογραφίας εξαντλούνται ως επί το πλείστον σε ποσοτικές έρευνες που βασίζονται σε δείγματα φοιτητών και όχι γενικού πληθυσμού[859], γεγονός που περιορίζει, σε ένα βαθμό, την αξιοπιστία τους και την ικανότητά τους να παρέχουν γενικεύσιμα συμπεράσματα.

Δυσκολίες αντιμετωπίστηκαν και στο επίπεδο της οριοθέτησης των εννοιών και των μορφών του οικονομικού και του ηλεκτρονικού εγκλήματος όπως και της μεταξύ τους σχέσης, λόγω της έλλειψης ενιαίων ορισμών και θεωρητικών προσεγγίσεων.

Η παρούσα διατριβή, δεδομένων των δυσκολιών αυτών, συνέβαλε με τη σύνθεση στοιχείων από την κείμενη βιβλιογραφία στο θέμα της μελέτης, της πρόληψης και της αντιμετώπισης της σύγχρονης ηλεκτρονικο-οικονομικής εγκληματικότητας.

Στο θεωρητικό πλαίσιο της παρούσας διατριβής χρησιμοποιήθηκε ως ενοποιημένη θεωρία η σύνθεση των προσεγγίσεων της περιβαλλοντικής εγκληματολογίας για τη δόμηση των «εγκληματικών ευκαιριών», αναδεικνύοντας την περαιτέρω συμβολή που μπορεί να παρέχουν στην εγκληματολογική σκέψη ως το κατάλληλο μεθοδολογικό εργαλείο στην μελέτη, όχι μόνο του παραδοσιακού, αλλά και του σύγχρονου ηλεκτρονικο-οικονομικού εγκλήματος.

Στον τομέα της έρευνας του σύγχρονου ηλεκτρονικού-οικονομικού εγκλήματος, υπάρχουν πολλές πλευρές του φαινομένου που μένει ακόμα να διερευνηθούν. Ειδικότερα, απαιτείται περαιτέρω μελέτη του φαινομένου τόσο σε επίπεδο ποιοτικών όσο και ποσοτικών ερευνών (θυματολογικών και όχι μόνο) οι οποίες όμως θα χρησιμοποιούν πιο αντιπροσωπευτικά δείγματα του γενικότερου πληθυσμού και όχι μόνο δείγματα φοιτητών ή καταδικασμένων.

~~~~~~

[859] Το ίδιο συμβαίνει και με τη μοναδική μέχρι τώρα, σχετική με το θέμα, από την ελληνική βιβλιογραφία: Zarafonitou Christina & Koumentaki Evangelia (2014)
~~~~~~

ΒΙΒΛΙΟΓΡΑΦΙΑ

Abernathy William & Lee Tien (2003), "Biometrics: Who's Watching You?", Electronic Frontiers Foundation, ανακτήθηκε από https://www.eff.org/wp/biometrics-whos-watching-you , Ιανουάριος 2013

Αγγελής Ιωάννης (2000), «Διαδίκτυο (Internet) και ποινικό δίκαιο, Έγκλημα στον κυβερνοχώρο», *Ποινικά Χρονικά* (9), Δίκαιο και Οικονομία, Αθήνα, Π.Ν. Σάκκουλας

Αγγελής Ιωάννης (2001), «Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το ελληνικό δίκαιο», *Ποινική Δικαιοσύνη* (12), σσ. 1293-1301

Adler Freda, Mueller Gerhard, Laufer William (1998), *Criminology*, 3rd ed., McGraw-Hill, Boston

Akers Ronald L. (1990-1991), " Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken", *The Journal Of Criminal Law & Criminology*, 81 (3), σσ. 653-676

Αργυρόπουλος Ανδρέας (2001), *Ηλεκτρονική Εγκληματικότητα*, Σάκκουλα, Αθήνα-Κομοτηνή

Αριστοτέλης, *Ηθικά Νικομάχεια* (χ.χ), Ζαμπα Κ. μεταφρ., τόμος Α΄, Βιβλιοθήκη Φέξη Αρχαίων Ελλήνων Συγγραφέων, ανακτήθηκε από www.gutenberg.net, Ιούν. 2014

Backhouse James & Gurpreet Dhillon, (1995), "Managing computer crime: a research outlook", *Computers & Security*, 14 (7), σσ. 645-651.

Bahrani Mahmoud (2012), "The economics of crime with Gary Becker" ανακτήθηκε από http://chicagomaroon.com/2012/05/25/the-economics-of-crime-with-gary-becker, Φεβρ.2014

Bartol Curt (1999), *Criminal Behaviour: A Psychosocial Approach* (5th Edition), Upper Saddle River, NJ Prentice-Hall.

Beccaria, Cesare (1986), «On Crimes and Punishment. Indianapolis», Hackett, Translation of Dei delitti e delle pene (1797), ανακτήθηκε από http://www.criminology.fsu.edu/crimtheory/beccaria.htm, Ιανουάρ. 2014 (βλ. και *www.thefederalistpapers.org)*

Becker Gary S. (1968), "Crime and Punishment: An Economic Approach", *Journal of Political Economy*, 76, σσ.169-217

Becker Gary S. (1976), *The Economic Approach to Human Behaviour* , University of Chicago Press, Chicago

Becker Gary S. (1981), *A Treatise on the Family,* Cambridge, Mass, Harvard University Press

Becker Gary S. (1993), "Nobel Lecture: The Economic Way of Looking at Behavior", *The Journal of Political Economy*, 101 (3), σσ. 385-409

Benson Michael L. & Madensen Tamara D. (2007), "Situational Crime Prevention and White-Collar Crime" στο Pontell Henry N., Geis Gilbert, ed's, *International Handbook of White-Collar and Corporate Crime*, New York, σσ. 609-626

Benson Michael, Madensen Tamara D., & Eck John E. (2009), "White-Collar Crime from an Opportunity Perspective" στο *The Criminology of White-Collar Crime*, Simpson, Sally S., Weisburd, David (Eds.), Springer, New York, σσ. 175–194.

Bentham, Jeremy (1789), «The Principles of Morals and Legislation» (Chapter I), ανακτήθηκε από http://www.constitution.org/jb/pml.htm, Απρ. 2014

Bentham, Jeremy (1931),*Theory of Legislation*, New York, Harcourt, Brace

Berman Jerry & Bruening Paula (2001), "Is privacy still possible in the twenty-first century?", Social Research, 68 (1), σσ. 306-18.

BloomBecker Buck (1997), "Computer Crime and Abuse", στο Hollinger Richard C. (editor,) *Crime, deviance and the computer*, Aldershot Hants, England, Dartmouth.

Blumer Herbert (1966), "Sociological Implications of the Thought of George Herbert Mead", *American Journal of Sociology*, 71 (5), σσ. 535-544

Bossler, Adam & Buruss George (2011) "The general theory of crime and computer hacking: Low self-control hackers?" στο T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology -driven crime: Social dynamics and implications,* Hershey, PA: Information Science Reference, σσ.38-67

Bossler Adam, Holt Thomas, & May David (2012), «Predicting online harassment victimization among a juvenile population», *Youth & Society*, 44, σσ. 500-523

Bossler Adam , & Holt Thomas (2009), "On-line Activities, Guardianship, & Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology*, 3, σσ. 400–420.

Bottoms Antony & Wiles Paul (2002), *Environmental Criminology,* in Morgan Rod, Mike Maguire & Robert Reiner, eds. *The Oxford handbook of criminology*, Oxford University Press, *3rd ed,* σσ. *620*–656

Box Steven (1983), *Power Crime and Mystification*, Routledge, N.York.

Braithwaite John (1989) "Criminological Theory and Organizational Crime", Justice Quartely, 3 (3), στο Nelken David (ed.) *White- Collar Crime*, Darmouth, Aldershot, 1994, σσ.187-213

Braithwaite John (1985), "White Collar Crime", *Annual Review of Sociology*,11, σσ. 1-21

Brantigham Patricia L. & Brantigham Paul J. (2008), "Environment, Routine, and Situation: Toward A Pattern Theory of Crime", στο *Routine Activity And Rational Choice*, Ronald V. Clarke & Marcus Felson Ed's, Advances in Criminological Theory, 5, Second printing σσ. 259-294.

Brantigham Patricia L. & Brantigham Paul J. (1993), "Nodes, Paths And Edges: Considerations On The Complexity Of Crime And The Physical Environment*", Journal of Environmental Psychology*, 13, σσ. 3-28

Brent Michael (χ.χ), "The Routine Activities Theory In Delinquency", ανακτήθηκε από http://www.ehow.com/info_8462976_routine-activities-theory-delinquency.html, Ιαν. 2014

Broadhurst Roderic (2006), "Developments in the global law enforcement of cyber-crime", *Policing: An International Journal of Police Strategies and Management*, 29 (2), σσ. 408-433.

Brunet, James R. (2002), "Discouragement of crime through civil remedies: An application of a reformulated routine activities theory", *Western Criminology Review*, 4, σσ. 68-79

Burden Kit, & Palmer Creole (2003), "Cyber Crime, A new breed of criminal?", *Computer Law & Security Report*, 19 (3), σσ. 222-227

Burke Roger Hopkins (2009), «An Introduction to Criminological Theory», Willan Publishing, Devon, UK ανακτήθηκε από uploadkon.ir/uploads/An_Introduction_to_Criminological_Theory.pdf, Ιούλιος 2014

Γιωτοπούλου-Μαραγκοπούλου Αλίκη (1984), *Εγχειρίδιο Εγκληματολογίας*, Νομική Βιβλιοθήκη, Αθήνα

Center for problem oriented policing (2014), «A Theory of Crime Problems» ανακτήθηκε από http://www.popcenter.org/learning/pam/help/theory.cfm, Ιαν. 2014

Choi Kyung-shick, (2008α) "Structural Equation Modeling Assessment Of Key Causal Factors in Computer Crime Victimization", Dissertation, Indiana University of Pennsylvania, Μάη 2008

Choi Kyung-shick (2008b), «Computer Crime Victimization and Integrated Theory: An Empirical Assessment», *International Journal of Cyber Criminology* (IJCC) ISSN: 0974 – 2891 January-June 2008, 2 (1), σσ . 308–333 ανακτήθηκε από http://www.cybercrimejournal.com/Choiijccjan2008.htm, Μαρτ. 2014

Clarke Ronald V. (1995), "Situational Crime Prevention", *Crime and Justice*, 19, The University of Chicago Press σσ. 91-150

Clarke Ronald V., editor (1997) "Situational Crime Prevention Successful Case Studies", Second Edition, School of Criminal Justice Rutgers University, Harrow and Heston, Publishers, ανακτήθηκε από www.popcenter.org/library/reading/PDFs/scp2_intro.pdf, Φεβρ. 2014

Clarke Ronald. & Cornish Derek. (1987), "Understanding Crime Displacement: An Application Of Rational Choice Theory", *Criminology*, 25 (4), November 1987, σσ. 933–948

Clarke Ronald V. & Cornish Derek , Author(s) (1985), «Modeling Offenders' Decisions: A Framework for Research and Policy», *Crime and Justice*, 6, σσ. 147-185

Clarke Ronald V. & Cornish Derek (2002), "Crime As A Rational Choice", στο Cote Suzette, *Criminological Theories*, Sage Publications, Th. Oaks, London, N.Delhi

Clarke Ronald V. & Felson Marcus Eds (2008), "Introduction in Routine Activity And Rational Choice", *Advances In Criminological Theory*, 5, Second printing

Clarke Ronald V. (1999), «Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods», *Police Research Series*, Paper 112, Policing and Reducing Crime Unit, Research Development and Statistics Directorate, London, Home Office.

Cohen Lawrence & Felson Marcus (1979), "Social change and crime rate trends: a routine activity approach*", American Sociological Review*, 44, σσ. 588–608

Coleman James W. (1987b), «Προς μια Ενοποιημένη Θεωρία για το Έγκλημα Λευκού Περιλαιμίου», Μετάφρ. Δρόσος Λ., *American Journal of Sociology*, 93

Cook Philip T. (1986), «The Demand and Supply of Criminal Opportunities», Crime and Justice, 7 σσ. 1-27, University of Chicago Press, ανακτήθηκε από http://www.jstor.org/stable/1147515?origin=JSTOR-pdf, Μάρτ.2014

Coleman James W. (1994), "Toward an integrated theory of white-collar crime", American Journal of Sociology, 93, 1987, στο Nelken David (ed.) *White- Collar Crime*, Darmouth, Aldershot, 1994

Coleman James W. (1995), "Motivation and Opportunity, Understanding the Causes of White-Collar Crime" στο Geis G., Meier R., Salinger L., *White-collar crime, Classic and Contemporary Views,* 3rd ed., N.York, σσ. 360-381

Cornish Derek B. (1993), "Theories of Action in Criminology: Learning Theory and Rational Choice Approaches" στο Clarke, Ronald Victor Gemuseus, and Marcus Felson, eds. , *Routine activity and rational choice*, 5, Transaction Publishers, σσ. 351-382

Cornish Derek B., & Clarke Ronald V., editors (1986), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, New Brunswick, New Jersey

Cote Suzette (2002), *Criminological Theories*, Sage Publications, Th. Oaks, London, N.Delhi,

Cusson Maurice (2002), *Σύγχρονη Εγκληματολογία*, Ηρώ Σαγκουνίδου-Δασκαλάκη (μετφρ.), Αθήνα, Νομική Βιβλιοθήκη

Δασκαλάκης Ηλίας (1985), *Η Εγκληματολογία της Κοινωνικής Αντίδρασης*, Αθήνα- Κομοτηνή, Σάκκουλα

Dreyfus Suelette (1998), "Computer Hackers", paper at the conference: Internet Crime held in Melbourne, Φεβρ. 1998

Drucker Peter (1969), *The Age of Discontinuity*, Harper and Row, New York.

Dunbar Nicholas, Martinuzzi Elisa (2012), "Goldman Secret Greece Loan Shows Two Sinners as Client Unravels", Bloomberg, Personal Finance , March 2012, ανακτήθηκε από http://www.bloomberg.com/news/2012-03-06/goldman-secret-greece-loan-shows-two-sinners-as-client-unravels.html, Ιούλιος 2014

Eck John E. (1994), "Drug Markets & Drug Places: A Case-Control Study of the Spatial Structure of Illicit Drug Dealing." PhD diss., Univ. of Maryland, College Park. edited by G. Browning, Halcli, & F. Webster, Sage Publications, 2000

Δημόπουλος Χαράλαμπος (1988), *Η Εγκληματολογική Προβληματική των Σύγχρονων Οικονομικών Εγκλημάτων*, Αθήνα – Κομοτηνή, εκδ. Σάκκουλα

Ελληνίδης Χρίστος (2001), «Ασφάλεια και έγκλημα μέσω ηλεκτρονικών υπολογιστών», στο Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν.(επιμ.), *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση,* Αθήνα, εκδ. Σάκκουλα

Emerson Richard M. (1976), «Social Exchange Theory», *Annual Review of Sociology* (2), σσ. 335-362

Etzioni - Halevy, Eva (1999), *Κοινωνιολογική θεωρία της ανάπτυξης*, Επιμ.: Κύρτσης, Α., Μεταφρ.: Αθανασίου, Κ., Παρασκευόπουλος Θ., Νήσος, Αθήνα

Ευρωπαϊκή Επιτροπή, Βρυξέλλες, 27.3.(2013): «Κανονισμός του ευρωπαϊκού κοινοβουλίου και του συμβουλίου σχετικά με τον οργανισμό της Ευρωπαϊκής Ένωσης για τη συνεργασία και την κατάρτιση στον τομέα της επιβολής του νόμου (Ευρωπόλ)», ανακτήθηκε από www.europarl.europa.eu/meetdocs/..._/com_com(2013)0173_el.pdf, Απρίλιος 2014

Ζαραφωνίτου Χριστίνα (1996), *Η προστασία του περιβάλλοντος από εγκληματολογική σκοπιά,* Τετράδια Εγκληματολογίας Ι, Νομική Βιβλιοθήκη, Αθήνα

Ζαραφωνίτου Χριστίνα (2001), «Ο φόβος του εγκλήματος. Ενδοαστεακή κατανομή της εγκληματικότητας και κοινωνικές αναπαραστάσεις του φαινομένου στο εσωτερικό της ελληνικής πρωτεύουσας», *Ποινική Δικαιοσύνη*, 2, σσ. 186-196

Ζαραφωνίτου Χριστίνα (2002), *Ο φόβος του εγκλήματος. Εγκληματολογικές προσεγγίσεις και προβληματισμοί με βάση την εμπειρική διερεύνηση του φαινομένου στο εσωτερικό της Αθήνας,* Σάκκουλα, Αθήνα - Κομοτηνή 2002.

Ζαραφωνίτου Χριστίνα (2004), *Εμπειρική Εγκληματολογία*, β΄έκδ., Νομική Βιβλιοθήκη, Αθήνα

Farrell Graham, Ken Clark, Dan Ellingworth & Ken Pease (2005), «Of Targets And Supertargets: A Routine Activity Theory Of High Crime Rates», *Internet Journal of Criminology* (IJC)

Fattah Ezzat (2008), "The Rational Choice/Opportunity Perspectives as a Vehicle for Integrating Criminological and Victimological Theories" στο Clarke Ronald V. & Felson

Marcus Eds (2008), *Routine Activity And Rational Choice. Advances In Criminological Theory,* Second printing, σ.σ.225-259

Felson Marcus (1986), "Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes", στο Derek B. Cornish, Ronald V. Clarke (editors), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, New Brunswick, New Jersey

Felson Marcus (1986), "Routine Activities, Social Controls, Rational Decisions, and Criminal Outcomes" στο Derek B. Cornish, Ronald V. Clarke (editors),*The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, New York.

Felson Marcus (1987), "Routine Activities And Crime Prevention In The Developing Metropolis", *Criminology*, 25, σσ. 911-932

Felson Marcus & Clarke Roland (1997), *Business and Crime Prevention*, Monsey, New York: Criminal Justice Press.

Felson Marcus & Clarke Roland. (1998*), Opportunity makes the thief*, Editor: Barry Webb, Police Research Group, London: Home Office.

Felson Marcus & Cohen Lawrence E. (1980), "Human Ecology and Crime: A Routine Activity Approach", *Human Ecology*, 8 (4)

File Thom (2013), "Computer and Internet Use in the United States." *Current Population Survery Reports*, 20-568. U.S. Census Bureau, Washington, DC., ανακτήθηκε από http://www.census.gov/en.html, Νοέμβριος 2014

Freiberg Arie (1991), "Sentencing White-Collar Criminals", *Australian Institute of Judicial Administration* (AIJA), Melbourne, σσ. 1-19

Friedrichs David (2010),*Trusted Criminals: White Collar Crime in Contemporary Society*, 4rth ed. Wadsworth

Geis Gilbert , Meier Robert, &Salinger Lawrence (ed's) (1995), *White-collar crime, Classic and Contemporary View*, 3rd ed., N.York,

Geis Gilbert, & Pontell Henry N., ed's (2007), *International Handbook of White-Collar and Corporate Crime*, New York.

Gibbons Don C. (1977), *Society, Crime and Criminal Careers*, Prentice-Hall, Englewood Cliffs, N.J.

Gibbs Carole, Cassidy Michael B., & Rivers Louie (2013), "A Routine Activities Analysis of White-Collar Crime in Carbon Markets", *Law & Policy*, 35 (4), σσ. 341-374

Givens Beth (2009), "True or False? You Can Find Out Anything About Anybody on the Net", ανακτήθηκε από https://www.privacyrights.org/ar/cybercon.htm, Αύγουστος 2014

Goldstein Arnold P. (1994),*The Ecology Of Aggression*, Plenum Press, N. York

Gottfredson Michael R. & Hindelang Michael J. (1981), "Sociological Aspects of Criminal Victimization", *Annual Review of Sociology*, 7, σσ. 107-128

Grabosky Peter N. (1998),"Crime and Technology in the Global Village", paper at the conference: Internet Crime held in Melbourne in 1998.

Grabosky Peter N. (2009), "Globalization & White-Collar Crime", στο Sally S. Simpson και David Weisburd Editors, *The Criminology of White-Collar Crime*, Springer, σσ.129-171

Grabosky Peter N & Smith Russell (1998), *Crime In The Digital Age*, Transaction Publishers – The Federation Press, Australia

Grabosky Peter N. & Walkley Sascha (2007), "Computer Crime and White-Collar Crime" στο Geis Gilbert, Pontell Henry N. ed's, *International Handbook of White-Collar and Corporate Crime,* New York, σσ. 364-375

Groff Elizabeth (2008), "Simulation for Theory Testing and Experimentation: An Example Using Routine Activity Theory and Street Robbery", *Security Journal*, 21 (1-2), σσ. 95-116

Guiton Clement (2012), "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence", *International Journal of Cyber Criminology*, July – December 2012, 6 (2) , σσ. 1030–1043

Hallam Baker Phillip (2005), "Prevention strategies of cyber crime", *Network Security*, 2005, 10, Elsevier Science Publishers, σσ. 12-15

Hawley Amos (1950), *Human Ecology*, Ronald Press, N. York

Helmkamp James C., Townsend Kitty J. &Sundra Jenny A. (2014), "How Much Does White Collar Crime Cost?", National White Collar Crime Center Training and Research Institute, ανακτήθηκε από https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=167026, Ιούνιος 2014

Harcourt Bernard E. (2013), «Beccaria's On Crimes and Punishments: A Mirror on the History of the Foundations of Modern Criminal Law», University of Chicago

Hirschi Travis & Gottfredson Michael R. (1987), "Causes of White-Collar Crime", *Criminology*, 25, σσ. 949-971

Hollinger Richard C., ed. (1997a), *Crime, deviance and the computer*, Aldershot Hants, England: Dartmouth

Hollinger Richard (1997b), "Hackers: Computer Heroes or Electronic Highwaymen?", στο Hollinger Richard C. (editor), *Crime, deviance and the computer*, Aldershot Hants, England: Dartmouth

Hollinger R., Lanza-Kaduce L. (1997), "The Case Of Computer Crime Laws", στο Hollinger Richard C. (editor) *Crime, deviance and the computer,* Aldershot Hants, England, Dartmouth.

Holt Thomas J. & Bossler Adam M. (2008), «Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization», *Deviant Behavior*, 30 (1), σσ. 1-25

Holt Thomas J. & Bossler Adam M. (2013), «Examining the Relationship Between Routine Activities and Malware Infection Indicators», *Journal of Contemporary Criminal Justice*, 29(4), σσ. 420 – 436

Holtfreter Kristy, Michael D. Reisig, & Travis C. Pratt (2008), ''Low Self-control, Routine Activities and Fraud Victimization'', *Criminology*, February 2008, 46, (1), σσ. 189–220

Homans George (1961), *Social Behavior: Its Elementary Forms*, New York: Harcourt Brace Jovanovich

Hutchings Alice & Hennessey Hayes (1992), "Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?, Current Issues", *Criminal Justice*, 20 (3), σσ. 1–20

Ιωαννίδης Χρήστος (2001), «Νομικά ζητήματα αναφορικά με εγκλήματα λευκού κολάρου» στο Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν. (επιμ.) , *Οικονομικά Εγκλήματα στην Κύπρο*: *Μια πολυθεματική προσέγγιση*, Αθήνα , εκδ. Σάκκουλα

Jahankhani Hamid & Al-Nemrat Ameer (2011), "Cybercrime Profiling and Trend Analysis" στο Babak Akhgar, Simeon Yates, Editors, *Intelligence Management*, Springer-Verlag, London σσ. 181- 197

Jeffery C. Ray & Zahm Diane L. (2008), "Crime Prevention through Environmental Design, Opportunity Theory, and Rational Choice Models" στο Ronald V. Clarke and Marcus Felson Eds, *Routine Activity And Rational Choice*, Advances in Criminological Theory, 5, Second printing

Jeffery, C.Ray. (1993), "Obstacles to the development of research in crime and delinquency", *Journal of Research in Crime & Delinquency*, 30, σσ. 491-497

Καϊτατζή – Γουίτλοκ Σοφία (2003), *Η επικράτεια των πληροφοριών*, Αθήνα, Κριτική

Καϊτσάς Δημήτρης (2004), « Ο ρόλος της τεχνολογίας στο οργανωμένο οικονομικό έγκλημα που διαπράττεται στην Ευρώπη», Διδακτορική διατριβή που εγκρίθηκε από το Πάντειο Π.Κ.Π.Ε

Καπαρδή Μαρία, Καπαρδής Ανδρέας, Κουράκης Νέστορας (2001), *Οικονομικά Εγκλήματα στην Κύπρο: μια πολυθεματική προσέγγιση*, Αθήνα, εκδ. Σάκκουλα

Καπαρδής Ανδρέας (2001), «Οικονομικά Εγκλήματα: Μια Γενική Θεώρηση», στο Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν.(επιμ.), *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση,* Αθήνα, εκδ. Σάκκουλα

Κατσουλάκος Γιάννης (2001), *Νέα Οικονομία, Διαδίκτυο και Ηλεκτρονικό Εμπόριο*, Εκδ. Κέρκυρα, Αθήνα.

Kigerl Alex (2012), «Routine Activity Theory and the Determinants of High Cybercrime Countries», *Social Science Computer Review*, 30: 4, σσ. 470-486, ανακτήθηκε από http://ssc.sagepub.com/content/30/4/470, Φεβρ. 2014

Κληρίδης Τάκης (2001), «Η Ανακριτική Λογιστική και Πρόληψη της Απάτης», στο: Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν. (επιμ.), *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση*, Αθήνα , εκδ. Σάκκουλα, σσ. 243-254.

Κολιώνη Κωνσταντίνα (2006), «Έγκλημα και Διαδίκτυο», Μεταπτυχιακή εργασία, Πάντειο Παν/μιο, Αθήνα

Κουράκης Νέστορας (1998), *Τα Οικονομικά Εγκλήματα*, β΄ εκδ., Αθήνα- Κομοτηνή, Σάκκουλα

Κουράκης Νέστορας (2004), «Ηλεκτρονικά Εγκλήματα και Εγκλήματα στο Διαδίκτυο», στο Λάζος Γ., *Οικονομική Εγκληματικότητα ΙΙ*, Σημειώσεις Πάντειο Παν/μιο

Κούρος Κωνσταντίνος (2008), άρθρο στην *Αστυνομική Ανασκόπηση* , Σεπτέμβριος - Οκτώβριος 2005, Τεύχος 233 ανακτήθηκε από http://www.ydt.gr/main/Article.jsp?ArticleID=83890, Δεκέμβριος 2008

Κούρος Κωνσταντίνος (2014), «Ηλεκτρονικό Έγκλημα», ανακτήθηκε από http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN, Αύγουστος 2014

Κραμβιά- Καπαρδή Μαρία (2001), «Απόσπαση Χρημάτων με Απάτη και Δόλο: Αιτιολόγηση, Δράστες και Modus Operandi», στο: Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν. (επιμ.), *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση*, εκδ. Σάκκουλα, Αθήνα

Κραμβία –Καπαρδή Μαρία, Τσολάκης Χρήστος (2011), *Οικονομικά εγκλήματα στις επιχειρήσεις,* Αθήνα, Κριτική

Κυριαζή Νότα (2002), *Η κοινωνιολογική έρευνα : Κριτική επισκόπηση των μεθόδων και των τεχνικών*, Ελληνικά Γράμματα, Αθήνα

Λάζος Γρηγόρης (2001), *Πληροφορική και Έγκλημα*, Αθήνα, Νομική Βιβλιοθήκη

Λάζος Γρηγόρης (2004), «Οικονομική Εγκληματικότητα ΙΙ», Σημειώσεις, Πάντειο Πανεπιστήμιο

Λάζος Γρηγόρης (2013), «Οικονομική Εγκληματικότητα: Σημειώσεις και Φάκελλος», Πάντειο Πανεπιστήμιο

Λαμπροπούλου Έφη (1994), *Κοινωνικός Έλεγχος του Εγκλήματος*, Αθήνα, Παπαζήση

Λαμπροπούλου Έφη (1999), *Κοινωνιολογία του Ποινικού Δικαίου και των Θεσμών της Ποινικής Δικαιοσύνης*, Αθήνα, Ελληνικά Γράμματα

Λαμπροπούλου Έφη (2009), «Η Σχολή του Σικάγου και η νεανική παραβατικότητα», στο: Η *Κοινωνιολογία της Σχολής του Σικάγου*, Τάτσης Ν. & Θανοπούλου Μ. (εκδ.), Παπαζήσης, Αθήνα 2009, σσ. 259-285

Langton Lynn & Piquero Nicole Leeper (2007), "Can general strain theory explain white-collar crime?", *Journal of Criminal Justice*, 35, 1, Ιαν.- Φεβρ. 2007, σσ. 1-15.

Lanier, Mark M. & Stuart Henry (1994), "Preparing for Jobs in Academia and Research and Experiences of Graduate School", στο St. Henry (ed.), *InSide Jobs: A Realistic Guide to Criminal Justice Careers for College Graduates*, Salem WI: Sheffield

Λέανδρος Νίκος (2005), *Πολιτική Οικονομία του Διαδικτύου. Το Διαδίκτυο: Ανάπτυξη και Αλλαγή,* Αθήνα, εκδ. Καστανιώτης

Levi Michael (1989), "Fraudulent Justice? Sentencing the Business Criminal" στο Carlen P., Cook D. (eds), *Paying for Crime*, Keynes: Open University Press, σσ.86-109 .

Levi Michael (2001) «Διαφθορά και Ξέπλυμα Παράνομου Χρήματος; Μερικές Οικονομικές και Νομικές Διαστάσεις», στο Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν. (επιμ.), *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση,* Αθήνα , εκδ. Σάκκουλα, σσ. 303-305.

Linden Rick (2007), "Situational Crime Prevention: Its Role in Comprehensive Prevention Initiatives", *Revue de l' IPC Review*, 1, Μάρτ. 2007, σσ. 139 - 159

Mac Millan, "International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime", ανακτήθηκε από: http://www.uncjin.org/Documents/EighthCongress.html, Ιούλιος 2014

Madriz Esther (1996), "The Perception Of Risk In The Workplace: A Test Of Routine Activity Theory", *Journal of Criminal Justice*, 24, 5, σσ. 407-418

Maguire Mike, Rod Morgan & Robert Reiner (1994), *The Oxford handbook of criminology*, Oxford University Press,

Mars Gerald (1974), "Dock pilferage: A case study in occupational theft" in Rock P. & McIntosh M. (Eds.), *Deviance and social control,* London: Tavistock, σσ. 209-228

Μαυράκης Εμμανουήλ (2004), «Θεωρία Χρησιμότητας και Συμπεριφοράς του Καταναλωτή», Σημειώσεις Παραδόσεων, ΤΕΙ Κρήτης, Ηράκλειο ανακτήθηκε από http://www.sdo.teicrete.gr/Micro_Mavrakis.pdf, Ιαν. 2014

Maslow Abraham H. (1943), "A Theory of human motivation", Psychological Review, 50(4), Jul. 1943, σσ. 370-396, ανακτήθηκε από http://psychclassics.yorku.ca/Maslow/motivation.htm, Μάιος 2014

Massey James L., Krohn Marvin D. & Bonati Lisa M. (1989) " Property crime and the routine activities of individuals", *Journal of Research in Crime & Delinquency*, 26, σσ. 378-400

McClure Stuart & Scambray Joel (1999), «How hackers cover their tracks», ανακτήθηκε από http://edition.cnn.com/TECH/computing/9901/25/hacktracts.idg, Αύγουστος 2014

McGrew Tony, Hall Stuart Held & David Held (Eds) (1992), Modernity and its Futures: Understanding Modern Societies, Book IV, Polity Press, Cambridge

McLaughlin Eugene & Muncie John, (2013), *Criminological Perspectives. Essential Readings*, Third Edition SAGE Publications, London

McQuade Samuel C. (ed.) (2009), *Encyclopedia of cybercrime*, Greenwood Press, London

Meier Robert F. & Short James F. Jr. (1995), "The Consequences of White-Collar Crime", στο Geis G., Meier R., Salinger Lawrence*, White-collar crime, Classic and Contemporary Views*, 3rd ed., N.York

Messner Steven, & Richard Rosenfeld (1994), *Crime and the American dream*, Wadsworth, Belmont

Miethe Terance D., Mark C. Stafford, & Scott Long (1987), "Social differentiation in criminal victimization: A test of routine activities/lifestyles theories" , *American Sociological Review*, 52, σσ. 184-194

Morrow Jordan, (2014), "Routine Activity Theory", στο http://criminology.wikia.com/wiki/Routine_Activity_Theory, Ιανουάριος 2014

Μυλωνόπουλος Χρήστος (2000), *Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο*, Σειρά Ποινικά, Εκδ. Σάκκουλα

Muncie John (2006), *Criminology*, 1, Sage Publications, London

Mustaine Elizabeth E. & Tewksbury Richard (1998), ''Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures'', Criminology, 36, number 4, σσ. 829-857

Navarro Jordana & Jasinski Jana (2012), "Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences" , *Sociological Spectrum: Mid-South Sociological Association,* 32 (91), σσ. 81-94

Nelken David (1994), "White-Collar Crime", στο Maguire M. et.al.(eds), *Oxford Handbook of Criminolog*y, Oxford University Press

Newman Graeme R., & Clarke Ronald V. (2003), *Super-highway Robbery: Preventing E-Commerce Crime*. Cullompton, Devon, Willan, N.Y.

Ngo Fawn T. (2011), «Cybercrime Victimization: An examination of Individual and Situational level factors» στο *International Journal of Cyber Criminology*, 5, 1, January - July 2011, σσ. 773–793 ανακτήθηκε από http://www.cybercrimejournal.com/ngo2011ijcc.pdf., Μαρτ.2014

Nykodym Nick, Taylor Robert, & Vilela Julia (2005), «Criminal profiling and insider cyber crime», *Digital Investigation*, 2 (4), December, σσ. 261-267

Osgood, D. Wayne, Wilson Janet , O'Malley Patrick, Bachman Jerald & Johnston Lloyd, (1996), "Routine activities and individual deviant behavior", *American Sociological Review* 61, σσ. 635-655

Paganini Pierluigi (2013), "2013 – The Impact of Cybercrime", ανακτήθηκε από http://resources.infosecinstitute.com/2013-impact-cybercrime, Ιούνιος 2014

Park Robert E. & Burgess Ernest W. (1921), *Introduction to the Science of Sociology*, The University Of Chicago Press Chicago.

Parker Donn (1987), "Information Crime and Security", *Computer Fraud and security Bulletin*, 9, (5)

Parker Donn (1997), "Computer abuse", στο Hollinger Richard C. (editor), *Crime, deviance and the computer*, Aldershot Hants, England: Dartmouth, σσ.23-33

Parker Donn (2000), "Fighting Computer Crime", Wiley, ανακτήθηκε από http://legal.practitioner.com/computer-crime/computercrime_1.htm, Ιούλιος 2014

Parker Donn (2007), "The Dark Side of Computing: SRI International and the Study of Computer Crime", *IEEE Annals of the History of Computing*, Ιαν. - Μαρτ. 2007

Parsi Boetig Brian R. (2004), "Marcus K. Felson: The Routine Activity Theory", ανακτήθηκε από http://www.criminology.fsu.edu/crimtheory/2004/felson.doc, Ιαν. 2014

Piliavin Irving, Gartner Rosemary, Thornton Craig & Matsueda Ross L., Author(s) (1986), "Crime, Deterrence, and Rational Choice", *American Sociological Review*, 51, No. 1, Feb. 1986, σσ. 101-119, ανακτήθηκε από http://www.jstor.org/stable/2095480?origin=JSTOR-pdf, Ιαν. 2014

Pires Stephen & Clarke Ronald V. (2011), "Are Parrots CRAVED?", *Journal of Research in Crime and Delinquency*, 49 (1), σσ. 122-146

Piquero Nicole & Benson Michael L. (2004), "White-Collar Crime and Criminal Careers: Specifying a Trajectory of Punctuated Situational Offending", Journal of Contemporary Criminal Justice, 20 (148), σσ. 148-165

Piquero Nicole & Weisburd David (2009), "Developmental Trajectories of White-Collar Crime" στο Simpson, Sally S. & Weisburd, David (Eds.),*The Criminology of White-Collar Crime*, Springer, New York σσ. 153-171

Pocar Fausto (2003),"New Challenges For International Rules Against Cyber-Crime", paper at the International Conference on Crime and Technology: New Frontiers for Legislation, Law Enforcement and Research, held in Courmayeur (Italy) on 28–30 November 2003

Pocar Fausto (2004), "New Challenges for International Rules Against Cyber Crime", *European Journal on Criminal Policy and Research,* 10, σσ. 27-34

Pontell Henry, & Geis Gilbert, Ed's (2007), *International Handbook of White-Collar and Corporate Crime*, Springer, N.York

Popp, Ann Marie (2012), "The effects of exposure, proximity, and capable guardians on the risk of bullying victimization ", *Youth Violence and Juvenile Justice,* 10 (4), σσ. 315-332

Pratt Travis C., Holtfreter Kristy & Reisig Michael D. (2010), "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory", *Journal of Research in Crime and Delinquency*, August 2010, 47 (3), σσ. 267-296

Pratt Travis C., Cullen Francis T., Sellers Christine S., Winfree Thomas Jr., L., Madensen Tamara D., Daigle Leah E., Fearn Noelle E. & Gau Jacinta M. (2010), "The Empirical Status of Social Learning Theory: A Meta-Analysis", Justice Quarterly, 27 (6), Dec. 2010, σσ. 765- 802

Quinney Earl R. (1963),"Occupational structure and criminal behavior: Prescription violation by retail pharmacists", Social Problems, 11, σσ. 179–185

Reed Gary E & Yeager Peter Cleary (1996), "Organizational Offending and Neoclassical Criminology: Challenging The Reach of A General Theory of Crime", *Criminology*, 34, Nr.3, σσ. 357-377.

Reyns Bradford W., Henson Billy & Fisher Bonnie S. (2011), «Being Pursued Online: Applying Cyber-Lifestyle-Routine Activities Theory To Cyberstalking Victimization», *Criminal Justice and Behavior*, 38, σσ. 1149-1169.

Roderick J. Lawrence (2001), «Human Ecology», στο Tolba M.K. (Ed.), *Our Fragile World*, Eolss Publishers, Oxford.

Schnatterly Karen (2002), «Detection and Prevention of White Collar Crime», *Strategic Management Research Center*, University of Minnesota Review, 5 (1)

Schoepfer Andrea & Piquero Nicole (2006),"Exploring white-collar crime and the American dream: A partial test of institutional anomie theory", *Journal of Criminal Justice*, 34 (3), σσ. 227-235

Scott John (2000), «Rational Choice Theory», στο Browning G., Halcli and Webster F. eds, Understanding Contemporary Society: Theories of The Present, Sage Publications, ανακτήθηκε από http://www.soc.iastate.edu/Sapp/soc401rationalchoice.pdf

Sieber Ulrich (1986),*The international Handbook of Computer Crime*, J. Wiley & Sons Ltd., Portsmouth

Simpson Sally S. & Weisburd David (Eds.) (2009),*The Criminology of White-Collar Crime*, New York, Springer

Shapiro, S. P. (1990). Collaring the Crime Not the Criminal: Reconsidering the Concept of White-Collar Crime. *American sociological review*, *55*(3), σ.σ. 346-365.

Shapiro Susan P. (2002), "White-collar Crime", *International Encyclopedia of the Social & Behavioral Sciences*, σ.σ. 2941-2945

Sherman Lawrence W., Gartin Patrick R. & Buerger Michael E. (1989), "Hot Spots Of Predatory Crime: Routine Activities And The Criminology Of Place", *Criminology*, 27 (1) , σσ.27-55

Shinder Debra Littlejohn, Tittel Ed. (2002), *Scene of cybercrime Computer Forensics Handbook*, Syngress Publishing

Shover Neil (2007), "Generative Worlds of White-Collar Crime" στο Pontell Henry, Geis Gilbert (eds*.) International Handbook of White-Collar and Corporate Crime*, Springer, N.York, σσ. 81-97

Slapper Gary & Tombs Steve (1999), *Corporate Crime*, Longman, London

Smith Russell, Grabosky Peter & Urbas Gregor (2004), *Cyber Criminals on Trial*, Cambridge University Press

Σοφός Θεμιστοκλής (2014), «Το έγκλημα στον κυβερνοχώρο και η νομοθετική πρόβλεψη», ανακτήθηκε από http://www.sofos.com.gr/news3.html, Οκτ. 2014

Spiegel Henry W., Hubbard Ann, Ed's (1991), *The Growth of Economic Thought*, Ed.3. Duke University

Σπινέλλη Καλλιόπη (2005), *Εγκληματολογία. Σύγχρονες και παλαιότερες κατευθύνσεις.* Εκδ. Σάκκουλα, Αθήνα

Σταμέλος Γιώργος & Δακοπούλου Αθανασία (2007), *Η διατριβή στις κοινωνικές επιστήμες: από το σχεδιασμό στην υλοποίηση*, Αθήνα, Μεταίχμιο.

Stephens Gene (1995), "Crime in cyberspace", *Futurist*, 29 (5), σσ. 24-29

Sutherland Edwin (1940) "White-collar criminality", *American Sociological Review*, 5

Sutherland Edwin (1945), Is "White-Collar Crime" Crime?", *American Sociological Review*, 10, σσ. 132-139

Sutherland Edwin (1983), "White Collar Crime: The Uncut Version", *American Journal of Sociology*, 91 (6), May, 1986

Sutton David (2014), «Ronald V. Clarke» ανακτήθηκε από http://www.criminology.fsu.edu/crimtheory/clarke.htm, Ιαν. 2014

Sykes Gresham M. & Matza David (1957), «Techniques of Neutralization: A Theory of Delinquency», *American Sociological Review*, 22, 6, σσ. 664- 670

Tappan Paul (1947), "Who Is the Criminal?", *American Sociological Review*, 12, σσ. 96 – 102

Trasler Gordon (2008),"Conscience, Opportunity, Rational Choice, and Crime", στο Clarke R., Felson M., Eds, *Routine Activity and Rational Choice, Advances in Criminological Theory*, 5, σσ. 305-322

Taylor Iris (2005), «Consumer Watch: Internet auctions top fraud list», ανακτήθηκε από http://www.crime-research.org/news/30.01.2005/934, Απρίλιος 2008

Τσουραμάνης Χρήστος (2006), «Η ψηφιακή (ηλεκτρονική) εγκληματικότητα στο πλαίσιο της θεωρίας της καθημερινής δραστηριότητας», Ομιλία στην 1η Συνάντηση Ελλήνων Εγκληματολόγων, 9 – 11 Ιουνίου 2006, Μυτιλήνη, Παν/μιο Αιγαίου.

Τσουραμάνης Χρήστος, (2005), *Ψηφιακή Εγκληματικότητα, Η (Αν)ασφαλής Όψη Του Διαδικτύου,* Κατσαρός, Αθήνα

Vila Bryan (1994), «A General Paradigm for Understanding Criminal Behavior: Extending Evolutionary Ecological Theory», Criminology, 32, σσ. 311-351

Wahlert Glenn (1998),"Crime in Cyberspace", paper at the conference: Internet Crime, held in Melbourne in 1998

Walden Ian (2003), "Crime and Security in Cyberspace", Cambridge Review of International Affairs, 18:1, σσ. 51- 68

Watson Business Systems Ltd, Publisher (2014), A Guide To Computer Crime, ανακτήθηκε από: http://legal.practitioner.com/computer-crime/computercrime_1.htm, Ιούλιος 2014

Wheeler Stanton, Weisburd David, & Bode Nancy (1982), "Sentencing the white collar offender: Rhetoric and reality", *American Sociological Review*, 47, σσ. 641–659

Williams Katherine (1991), *Textbook on Criminology*, London, Blackstone Press

Wilsem van, Johan (2013), «Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization», Journal of Contemporary Criminal Justice 29,(4), σσ. 437 –453

Wilson, R. and J. Backhouse (2006), ''Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective.'' *European Journal for Information Systems*, 15, σσ. 403–414.

Winston Gordon C., (1989), "Imperfectly Rational Choice", *Journal of Economic Behavior and Organization*, Elsevier, North-Holland, 12, σσ. 67-86

Wortley Richard & Mazerolle Lorrain eds. (2011), *Environmental Criminology and Crime Analysis,* N.Y, Routledge.

Yar Majid (2005), «The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory», *The European Journal of Criminology*, 2(4), σσ. 407-28

Φιλίππου Ανδρέας (2001), «Το Ξέπλυμα Παράνομου Χρήματος και οι Τράπεζας», στο: Καπαρδή Μ., Καπαρδής Α., Κουράκης Ν.(επιμ.) , *Οικονομικά Εγκλήματα στην Κύπρο: Μια πολυθεματική προσέγγιση*, Αθήνα , εκδ. Σάκκουλα, σ.σ. 270-280.

Χάιδου Ανθοζωή (2003), *Εγκληματολογικά Κείμενα*, Νομική Βιβλιοθήκη, Αθήνα

Χατζής Αριστείδης (2010), "Τα Οικονομικά του Εγκλήματος" στον Τιμητικό Τόμο Καλλιόπης Δ. Σπινέλλη: *Εγκληματολογικές Διεπιστημονικές Προσεγγίσεις*, Αθήνα-Κομοτηνή, Εκδ. Σάκκουλα, σσ. 455-467

Χρυσοπούλου Σοφία & Λεφάκης Παναγιώτης (2015), *Η προσβολή της πνευματικής ιδιοκτησίας στο διαδίκτυο,* ανακτήθηκε Ιανουάριος 2015, από http://aeiforia.or.auth.gr

Zarafonitou Christina & Koumentaki Evangelia (2014), *Victimisation and insecurity of undergraduate students while using internet*, 14th Annual Conference of the ESC, Prague, 10-13 September 2014, ανακτήθηκε από http://criminology.panteion.gr, Νοέμβριος 2014

«Το Βήμα» (2000), 16/02/2000, σελ. Δ.14-46

ΠΗΓΕΣ ΑΠΟ ΙΣΤΟΣΕΛΙΔΕΣ

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2014), Ν. 2472/97, ανακτήθηκε από http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#4 , Οκτ. 2014

Australian Government (2004), “What is e-crime”, ανακτήθηκε από http://www.netalert.net.au, Ιούν. 2012

Center for problem oriented policing (2014), “A Theory of Crime Problems” ανακτήθηκε από http://www.popcenter.org/learning/pam/help/theory.cfm, Ιαν. 2014

Check Fraud (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

Computer & Information Science (2008), ανακτήθηκε από http://csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm, Απρίλιος 2008

Convention on Cybercrime (2001), Budapest, 23.XI.2001, ανακτήθηκε από http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, Σεπτέμβριος 2014

Credit Card Fraud (2007), ανακτήθηκε από www.nw3c.org , Σεπτ. 2007

Δήμα Μαρία (2015), «Εισαγγελέας: Στο εδώλιο 64 για τα «μαύρα ταμεία» της Siemens» ανακτήθηκε από http://www.efsyn.gr/arthro/eisaggeleas-sto-edolio-64-gia-ta-mayra-tameia-tis-siemens Μάρτιος 2015

Disaster Fraud (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

Electronic Frontier Fountation (2006), “Anonymity”, ανακτήθηκε από http://www.eff.org/anonymity.htm, Φεβρ. 2006

ΕΛ.ΣΤΑΤ.(2014), http://www.statistics.gr/portal/page/portal/ESYE/PAGE-themes?p_param=A1901&r_param=SFA20&y_param=2012_00&mytabs=0, Οκτώβριος 2014

Embezzlement/Employee Theft (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

Ευσταθίου Άννα (2008) http://www.iatronet.gr/ygeia/psyxiki-ygeia/article/5038/ragdaia-afxisi-istoxwrwn-paidikis-pornografias.html, ανακτήθηκε Οκτ. 2014

Federal Trade Commission (2006) Consumer Fraud and Identity Theft Complaint Data, January-December 2006, ανακτήθηκε από http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf , Σεπτ. 2006

Global Economic Crime Survey (2011), http://www.pwc.com/gr/en/surveys/economic-crime-2011.jhtml, Νοέμβριος 2014

Health Care Fraud (2007), ανακτήθηκε από www.nw3c.org , Ιανουάρ. 2007

Ιγνατιάδης Βασίλης (2011), http://www.ethnos.gr, ανακτήθηκε Δεκ. 2011

Internet Fraud (2007), ανακτήθηκε από www.nw3c.org , Σεπτ. 2007

Internet Gambling (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

Insurance Fraud (2007), ανακτήθηκε από www.nw3c.org , Ιούν. 2007

Καραμανώλη Εύα (2014) «Πρόστιμο στη ΓΓΠΣ για διαρροή φορολογικών δεδομένων», ανακτήθηκε από http://www.kathimerini.gr/788568/article/oikonomia/ellhnikh-oikonomia/prostimo-sth-ggps--gia-diarroh-forologikwn-dedomenwn, Νοεμβρ. 2014

Καταγγελίες - Στατιστικά στοιχεία (2014), safeline, http://www.safeline.gr/kataggelies/statistika-stoiheia?set=1, Νοέμβριος 2014

Κατωμέρης Κώστας (2015), http://www.efsyn.gr/arthro/enohos-gia-notheysi-eggrafoy-o-g-papakonstantinoy, ανακτήθηκε Μάρτιος 2015

Κέντρο ΠΛΗ.ΝΕ.Τ. Περ. Ενότητας Φλώρινας (2014) , ανακτήθηκε από http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html, Νοέμβρ. 2014

Κορδεράς Δημήτρης (2015), «Infobank Hellastat - RSA/EMC - FEDEX: Τάσεις, ευκαιρίες και προκλήσεις για το e-commerce, μέσα από 3 έρευνες», MarketingWeek Online, ανακτήθηκε από http://www.marketingweek.gr/default.asp?pid=9&la=1&cID=8&arID=53928, Μαρτ. 2015

Κουπαράνης Παναγιώτης, (2014), «Η φοροδιαφυγή στο στόχαστρο του ΟΟΣΑ», http://www.dw.de/ Νοέμβ. 2014

Κύρωση της Σύμβασης της Βουδαπέστης και του πρόσθετου Πρωτοκόλλου (2014), http://www.xirotiri.gr/koinobouleitikos-elegxos/erotiseis/ake/kirosi-tis-simbasis-tis-boudapestis-kai-tou-prosthetou-protokollou.html, ανακτήθηκε Νοέμβριο 2014

Κωνσταντινόπουλος Γιώργος, (2008), ανακτήθηκε από: http://www.enet.gr/online/online_obj?pid=25&tp=T&id=95593724, Απρίλιος 2008

Μαζάνης Χρήστος, (2014), «Λουκέτο σε 400 ιστοσελίδες», http://www.zougla.gr/kosmos/article/pragmatopi8ike-i-megaliteri-epixirisi-sto-diadiktio--eklisan-400-istoselides-1096440, Νοέμβριος 2014

Μαυραγάνης Κώστας (2015), « Ευάλωτα σε αεροπειρατείες από χάκερ μέσω Wi-Fi τα σύγχρονα αεροπλάνα», ανακτήθηκε από HuffPost Greece, http://www.huffingtonpost.gr/2015/04/16/hacker-aeropeirateia_n_7076188.html , Απρίλ.2015

Money laundering (2006), ανακτήθηκε από www.nw3c.org, Μάη 2006

Mortgage Fraud (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

National White Collar Crime Center and Federal Bureau of Investigation (2007), IC3 2006 Internet Crime Report, ανακτήθηκε από http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf, Σεπτ. 2007

Νομοθεσία για το Ηλεκτρονικό Έγκλημα (2015), ανακτήθηκε από www.e-crime.gr/p/links.html, Ιούνιος 2015

Οδηγίες από το Υπουργείο Προστασίας του Πολίτη: (2010)-11-23, ανακτήθηκε από http://blogs.sch.gr/internet-safety/archives/222, Νοέμβρ. 2014

Organized Crime (2007), ανακτήθηκε από www.nw3c.org, Σεπτ. 2007

Privacy international (2007), "Freedom of Expression", ανακτήθηκε από www.privacyinternational.org/index.shtml, Ιανουάρ. 2007

Purcell Kristen (2011), http://www.pewinternet.org/2011/08/09/search-and-email-still-top-the-list-of-most-popular-online-activities, ανακτήθηκε Νοέμβρ. 2014

PwC (PriceWaterhouseCoopers) (2014), "Τα οικονομικά εγκλήματα στην Ελλάδα", ανακτήθηκε από http://www.euro2day.gr/news/economy/article/556792/pwc-ta-oikonomika-egklhmata-sthn-ellada.html, Νοέμβριος 2014

Securities/Investment Fraud (2007), ανακτήθηκε από www.nw3c.org, Ιανουάρ. 2007

The Internet Crime Complaint Center (2007), ανακτήθηκε από www.ic3.gov , Σεπτ. 2007

Review of the Roots of Youth Violence (2014): Literature Reviews, 5 (Chapter 3), ανακτήθηκε από http://www.children.gov.on.ca/htdocs/English/topics/youthandthelaw/roots/5/chapter03_rational_choice.aspx, Ιανουάρ. 2014

Telemarketing Fraud (2006), ανακτήθηκε από www.nw3c.org, Σεπτ. 2006

US Department of Justice (1998), Reasons for Declining Prosecutions in Computer Crime Cases, Source, Matthew Scherb (2004), Northwestern University, published in Granick et al (2003), http://www.securitymanagement.com/library/NACDL_computer0503.pdf, ανακτήθηκε Νοέμβριο 2014

Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (2014), http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1763&Itemid=378, Δεκέμβριος 2014

ΙΣΤΟΣΕΛΙΔΕΣ

http://europa.eu
www.europarl.europa.eu
http://www.europol.europa.eu
http://eur-lex.europa.eu
http://en.wikipedia.org
http://financial-dictionary.thefreedictionary.com
http://virus.gr
http://www.abcsearch.com
http://www.all-nettools.com
http://www.asanet.org
http://www.astynomia.gr
http://www.cbsnews.com, July, 2007
http://www.census.gov
http://www.children.gov.on.ca
http://www.cosmo.gr
http://www.criminology.fsu.edu
http://www.dart.gov.gr
http://www.epic.org
http://www.e-crime.gr
http://www.efsyn.gr
http://www.euro2day.gr
http://www.express.gr
http://www.e-yliko.gr
http://www.ethnos.gr
http://www.europol.europa.eu
http://www.geocities.com
http://www.kathimerini.gr
http://www.lifo.gr
http://www.marketingweek.gr
http://www.news.gr
http://www.newsbomb.gr
http://www.newsnowgr.com
http://www.pewinternet.org
http://www.popcenter.org
http://www.pwc.com
http://www.safeline.gr
http://www.saferinternet.gr
http://www.sch.gr
http://www.sdo.teicrete.gr
http://www.sifkal.org
http://www.simerini.com.cy
http://www.thanko.eu
http://www.the-dma.org
http://www.tovima.gr
http://www.xirotiri.gr
http://www.viadiplomacy.gr

ΠΑΡΑΡΤΗΜΑ

1. Περίπτωση τηλεφωνικών υποκλοπών.

«Υποκλοπές Καραμανλή: Ένταλμα σύλληψης για υπάλληλο της αμερικανικής πρεσβείας»

Δημοσίευση ιστοσελίδας news.gr [860] :

«Σε έναν πρώην υπάλληλο της πρεσβείας των ΗΠΑ οδήγησε η έρευνα των δικαστικών αρχών για το σκάνδαλο των τηλεφωνικών υποκλοπών τόσο σε βάρος του πρώην πρωθυπουργού Κώστα Καραμανλή όσο και μελών της κυβέρνησής του.

Πριν από λίγο ο ανακριτής Δημήτρης Φούκας που χειρίζεται την υπόθεση εξέδωσε ένταλμα σύλληψης για τον αμερικανό πρώην υπάλληλο της πρεσβείας William Β. ο οποίος φέρεται να είχε πρωταγωνιστικό ρόλο στην υπόθεση.

Το συγκεκριμένο πρόσωπο το οποίο φέρεται να ήταν επιχειρησιακό στέλεχος του κλιμακίου της CIA στην Αθήνα από τα μέσα της δεκαετίας του 90 εμφανίζεται από τα στοιχεία της έρευνας να αγόρασε τον Ιούνιο του 2004 από κατάστημα κινητής τηλεφωνίας στον Πειραιά, 4 συσκευές κινητών τηλεφώνων, οι τρεις από τις οποίες χρησιμοποιήθηκαν ως καρτοκινητά σκιές στην υπόθεση των τηλεφωνικών υποκλοπών.

Από την άρση του απορρήτου που ακολούθησε προέκυψε, σύμφωνα με πληροφορίες, ότι η μια τηλεφωνική σύνδεση ενεργοποιήθηκε και σε άλλη συσκευή στην οποία ενεργοποιήθηκε και δεύτερη σύνδεση με στοιχεία συνδρομητή "Πρεσβεία ΗΠΑ Βασ. Σοφίας 91". Μάλιστα, ο κατηγορούμενος φέρεται , μόλις ήρθε στο φως της δημοσιότητας η υπόθεση να έφυγε από την Ελλάδα για να επιστρέψει τον Αύγουστο του 2005 με διπλωματική πλέον ιδιότητα ως πρώτος γραμματέας της πρεσβείας των ΗΠΑ.

Οι πληροφορίες θέλουν τη σύζυγο του να έκανε τις αγορές των τηλεφωνικών συσκευών.

Σύμφωνα με πληροφορίες ο συγκεκριμένος κατηγορούμενος είχε συνεργασία με τις ελληνικές υπηρεσίες κυρίως σε θέματα αντιμετώπισης τρομοκρατίας με πλέον χαρακτηριστική τη συμμετοχή του σε επιχείρηση με την κωδική ονομασία "δίχτυ" η οποία αφορούσε στην απομάκρυνση μεγάλης ποσότητας εκρηκτικών από την πρεσβεία του Ιράκ το 2003. Ελέγχεται ακόμα η πιθανή εμπλοκή του και στο σχέδιο "Πυθία" που φέρεται να αφορούσε σε σχέδιο δολοφονίας του πρώην πρωθυπουργού Κωνσταντίνου Καραμανλή.

Το καλοκαίρι, ο δικηγόρος του είχε έρθει σε επαφή με τον κ. Φούκα προκειμένου να τον ενημερώσει ότι ο πελάτης του πρόκειται να προσέλθει και να συνεργαστεί με την ανάκριση, δίνοντας ενδεχομένως χρήσιμες πληροφορίες. Ωστόσο αυτό δεν έγινε. Έκτοτε ο ανακριτής συγκέντρωσε και άλλα στοιχεία, τα οποία οδήγησαν στον εντοπισμό κτηρίου στα Νότια Προάστια όπου είχε τοποθετηθεί κεραία από τους δράστες των υποκλοπών, και προφανώς ήταν το "στρατηγείο" τους. Στο ίδιο σημείο μάλιστα φαίνεται να λειτουργούσε στο παρελθόν και δεύτερη κεραία, η οποία ήταν - όπως εκτιμάται - κεραία υποδοχής πληροφοριών».

[860] http://www.news.gr/ellada/koinonia/article/208374/ypoklopes-karamanlh-entalma-syllhpshs-gia-ypallhlo.html, Μάρτ. 2015

2. Επενδυτικές/επαγγελματικές ευκαιρίες με εργασία από το σπίτι

Παρατίθεται παραπλανητικό μήνυμα [861]:

Συναλλαγή Συναλλάγματος, η μεγαλύτερη και πιο συναρπαστική αγορά στον κόσμο σου προσφέρει αμέτρητες ευκαιρίες!

Η ισοτιμία του Ευρώ έναντι του Δολαρίου αλλάζει διαρκώς, συνήθως με μικρές μεταβολές. Καθημερινές διακυμάνσεις γύρω στο 1% είναι σχετικά συνηθισμένες. Στο Forex, όταν επενδύσεις με 1:100 μόχλευση, αλλαγές όπως για παράδειγμα 1,2% μετατρέπονται σε 120% κατά τη διάρκεια μιας μέρας, ή σε μερικές ώρες ή λεπτά! Μπορείς να κερδίσεις απεριόριστα ποσά, αλλά αν η ισοτιμία του συναλλάγματος κινηθεί αντίθετα στη συναλλαγή σου, τότε δεν μπορείς να χάσεις παραπάνω από την αρχική σου επένδυση.

Πάρτε μια γεύση του Forex: Αυτό το παράδειγμα δείχνει τι μπορεί να συμβεί σε μια επένδυση, αν ανοίξεις μια συναλλαγή σε EUR/USD:

Τιμή ανοίγματος: 1.3600 **Η επένδυση σας: $100.00**

Τιμή:	Πραγματική Μεταβολή:	Μεταβολή μόχλευσης:	Κέρδος / Απώλειες:
1.3746	1.074%	107.4%	$107.40

[861] http://ads2.easy-forex.com/camp/landing/reporter-LP/ef/GR/index.html?gid=86825&subid=2467887

3. Απάτη με email και με πρόσχημα την προσφορά εργασίας

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους πολίτες για την αποστολή απατηλών μηνυμάτων ηλεκτρονικού ταχυδρομείου σχετικά με δήθεν χορήγηση δανείων, σε μεγάλο αριθμό χρηστών του διαδικτύου:[862]

«Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συστήνει και προτρέπει τους χρήστες του διαδικτύου να μην αποστέλλουν προσωπικά δεδομένα ή οικονομικά στοιχεία

Για τη **διακίνηση** μέσω διαδικτύου ενός παραπλανητικού ηλεκτρονικού μηνύματος (**e-mail)**, με το οποίο προσφέρονται δήθεν ευκαιρίες απασχόλησης και θέσεις εργασίας (σε διευθυντικά πόστα), ακόμη και στη χώρα μας, με υψηλές αποδοχές, προειδοποιεί η **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος** της Ελληνικής Αστυνομίας.

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους χρήστες του διαδικτύου, ότι αυτού του είδους τα μηνύματα έχουν ως σκοπό να πείσουν με απατηλό τρόπο («ψάρεμα»), όσους αναζητούν εργασία, να αποστείλουν:

- είτε τα προσωπικά τους στοιχεία και δεδομένα (ταυτότητα, διαβατήριο, αριθμό φορολογικού μητρώου – Α.Φ.Μ. κ.λπ.)
- είτε προσωπικά τους οικονομικά δεδομένα (αριθμούς τραπεζικών λογαριασμών, προσωπικούς κωδικούς (PIN numbers), αριθμούς πιστωτικών καρτών, πληροφορίες καρτών ATM κ.λπ.)
- είτε να ζητηθεί να προκαταβάλουν ένα ποσό προκειμένου να καταλάβουν τη δήθεν προσφερόμενη θέση εργασίας. Μάλιστα στην τελευταία περίπτωση ζητούν τα χρηματικά ποσά να αποστέλλονται μέσω εταιρειών ταχυμεταφοράς χρημάτων και όχι μέσω τραπεζικών λογαριασμών.

Με αφορμή τη διακίνηση του εν λόγω μηνύματος (email), παρακαλούνται οι πολίτες να είναι ιδιαίτερα προσεκτικοί στην περίπτωση που λάβουν, μέσω του διαδικτύου, τέτοιου είδους μηνύματα, για την αποφυγή πιθανής εξαπάτησης.

Επιπλέον, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συστήνει και προτρέπει τους χρήστες του διαδικτύου να μην αποστέλλουν προσωπικά δεδομένα ή οικονομικά στοιχεία σε άγνωστα άτομα και να διασταυρώνουν την ύπαρξη των εταιρειών, που προσφέρουν τις θέσεις εργασίας και να επικοινωνούν με αυτές, ώστε να επαληθεύουν το περιεχόμενο των αγγελιών.

Ειδικότερα, συνίσταται:

- Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη, επαγγελματία ή γραφείου εύρεσης εργασίας και μέσω δεύτερης πηγής ή του τηλεφωνικού καταλόγου και στη συνέχεια να απευθύνεστε στον εργοδότη απευθείας.
- Να μην εμπιστεύεστε όσους, μέσω διαδικτύου, σας ζητούν χρήματα εκ των προτέρων για να σας βρουν δουλειά ή να σας προσφέρουν μια θέση εργασίας.
- Ποτέ να μην δεχθείτε να πληρώσετε για "αποκλειστικές" πληροφορίες για θέσεις εργασίας ή για να πάρετε κάποια συγκεκριμένη θέση.
- Να αξιολογούνται προσεκτικά τα στοιχεία επαφής, που δίνονται σε αγγελίες εργασίας μέσω διαδικτύου ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες ή κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας. Επίσης να δίνεται προσοχή στη σύνταξη του κειμένου, όπου εάν υπάρχουν πολλά ορθογραφικά λάθη και άλλες ανακρίβειες, αυτό αποτελεί συνηθισμένη ένδειξη που παραπέμπει σε ψεύτικη αγγελία εργασίας.
- Να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον περιηγητή (browser) αντί να χρησιμοποιείτε υπερσυνδέσμους (links) όταν ελέγχετε τις πηγές των θέσεων εργασίας.

862 http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=44846&Itemid=13, Σεπτέμβριος 2014

- Να δημιουργήσετε διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν λογαριασμό για όλες τις μη προσωπικές επικοινωνίες σας.
- Να δίνετε ιδιαίτερη προσοχή όταν απευθύνεστε σε εταιρείες που βρίσκονται έξω από τη Χώρα μας ή γίνεστε αποδέκτης μηνυμάτων από φερόμενες εταιρείες του εξωτερικού.

Εάν κάποια «ευκαιρία» ή θέση εργασίας υπόσχεται υπερβολικά υψηλές αποδοχές, οι οποίες μάλιστα σε σύντομο χρονικό διάστημα θα διπλασιαστούν, μάλλον πρόκειται για παραπλανητικό – απατηλό μήνυμα. το οποίο πρέπει να ελεγχθεί.

Υπενθυμίζεται ότι για ανάλογα περιστατικά, οι πολίτες μπορούν να επικοινωνούν με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας:

- Τηλεφωνικά στους αριθμούς 11012 και 210-6476464
- Στέλνοντας e-mail στα ccu@cybercrimeunit.gov.gr, 11012@hellenicpolice.gr»

4. Ψηφιακή Απάτη στη Θεσσαλονίκη [863]

<Χάκερ «τρύπησαν» το ηλεκτρονικό σύστημα τράπεζας>

«Κατάφεραν να διεισδύσουν στο λογισμικό σύστημα και, αλλάζοντας τις ισοτιμίες, έκαναν εικονικές συναλλαγές, αποκομίζοντας συνολικά πάνω από 300.000 ευρώ. Συνελήφθησαν δύο 21χρονοι Έλληνες φοιτητές. Καταζητείται Βρετανός συνεργός τους. Με μια απίστευτης σύλληψης... παρέμβαση στις συναλλαγματικές ισοτιμίες ευρώ -στερλίνας, τρεις νεαροί «ποντικοί» του Διαδικτύου στη Θεσσαλονίκη «έσπασαν» το σχετικό λογισμικό της CITIBANK και έβαλαν στους τραπεζικούς λογαριασμούς τους309.000 ευρώ. Η απάτη όμως ανακαλύφθηκε από την τράπεζα και η Δίωξη Ηλεκτρονικού Εγκλήματος έβαλε τέλος στην παράνομη δραστηριότητα των τριών φοιτητών, περνώντας χειροπέδες στους δύο από αυτούς. Πρόκειται για δύο Έλληνες, 21 ετών, φοιτητές Ιατρικής και Οδοντοτεχνικής αντίστοιχα, ενώ καταζητείται ο τρίτος συνεργός τους, βρετανικής υπηκοότητας, επίσης 21 ετών. Οι τρεις crackers κατάφεραν να διεισδύσουν μέσω Διαδικτύου στο λογισμικό σύστημα συναλλαγματικών ισοτιμιών της τράπεζας και με μια παρέμβαση στη μέθοδο επεξεργασίας των δεδομένων που καθορίζουν τις ισοτιμίες πέτυχαν να εμφανίζεται το ευρώ και η βρετανική λίρα με την ίδια ισοτιμία (1 προς 1).

Στη συνέχεια προχωρούσαν σε εικονικές συναλλαγές, μετατρέποντας σε λίρες διάφορα χρηματικά ποσά που είχαν σε ευρώ. Αμέσως μετά μετέτρεπαν πάλι τις λίρες σε ευρώ, αλλά με την πραγματική ισοτιμία τους (0,85 λίρες προς 1 ευρώ) και καρπώνονταν τη διαφορά. Με αυτή τη μέθοδο κατάφεραν μέσα σε μία εβδομάδα να κάνουν εικονικές συναλλαγές ύψους 1.650.000 ευρώ και να αποκομίσουν συνολικά 309.102,38 ευρώ από τη διαφορά της ισοτιμίας. Η «πειρατεία» ανακαλύφθηκε κατά τη διαδικασία εσωτερικού ελέγχου της CITIBANK, η οποία προσέφυγε στη Δίωξη Ηλεκτρονικού Εγκλήματος.

Εξειδικευμένα στελέχη της τελευταίας εντόπισαν στη Θεσσαλονίκη τα ηλεκτρονικά «ίχνη» των τριών νεαρών και κλιμάκιο της υπηρεσίας μετέβη στην πόλη την περασμένη Παρασκευή, όπου συνέλαβε τους δύο Έλληνες. Σε έρευνες που έγιναν στα σπίτια τους βρέθηκαν δύο φάκελοι που περιείχαν τραπεζικά έγγραφα (αναλύσεις λογαριασμών και βεβαιώσεις εκτέλεσης εντολών για χρηματιστηριακές ή εξωχρηματιστηριακές συναλλαγές), δύο υπολογιστές, δύο πιστωτικές κάρτες της τράπεζας και 11.300 ευρώ, 19.915 δολάρια ΗΠΑ, 10.130 ελβετικά φράγκα, 1.080 δολάρια Καναδά και 100 δολάρια Αυστραλίας.

Επένδυσαν σε μετοχές. Από την αστυνομική έρευνα προέκυψε ότι οι δράστες έχουν επενδύσει μεγάλα χρηματικά ποσά σε μετοχές και αμοιβαία κεφάλαια διαφόρων τραπεζών, χωρίς να αιτιολογούν την προέλευση των χρημάτων. Για τον λόγο αυτόν ενημερώθηκε η Επιτροπή για το «ξέπλυμα» μαύρου χρήματος. Οι συλληφθέντες παραπέμφθηκαν στον εισαγγελέα, ο 21 ετών Βρετανός συνεργός τους καταζητείται, ενώ συνεχίζεται η έρευνα για να διαπιστωθεί το συνολικό ποσό της ηλεκτρονικής απάτης.

Αργά το βράδυ οι νεαροί με τη σύμφωνη γνώμη εισαγγελέα και ανακριτή αφέθηκαν ελεύθεροι με περιοριστικούς όρους και χρηματική εγγύηση 10.000 ευρώ ο καθένας. Οι δράστες ομολόγησαν την πράξη τους και υποστήριξαν ότι θα επιστρέψουν τα χρήματα στην τράπεζα».

[863] Ιγνατιάδης Βασίλης http://www.ethnos.gr, Ανακτήθηκε 20/12/2011

5. α. Μήνυμα Phishing προς πελάτες διαδικτυακών τραπεζικών συναλλαγών

Ημερομηνία: 31 Jan 2008 12:31:29 +0200 [12:31:29 EET]
Από: Piraeus Bank <IbankV2Email@piraeusbank.gr>
Προς:
Θέμα: Voucher Code #11245325932

Αγαπητε πελατη

Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.

Δωροεπιταγη code: 11245325932

για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου παραπανω.

Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.

Copyright © winbank 2008

5. β. Σας ήρθε mail που λέει ότι έχετε επιστροφή φόρου; [864]

Την προσοχή των πολιτών εφιστά η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, για διάφορα μέιλ που φτάνουν τις τελευταίες ημέρες στα mailbox πολλών χρηστών και στα οποία ενημερώνονται οι χρήστες ότι έχουν επιστροφή από την εφορία. Συγκεκριμένα αναφέρεται και ποσό, συνήθως 452,03 ευρώ. Βεβαίως στη συνέχεια παροτρύνονται προκειμένου να πάρουν τα χρήματα να δώσουν κωδικούς και αριθμούς λογαριασμών. Όπως ενημερώνει η Δίωξη: Στη συνέχεια, εφόσον ο παραλήπτης ανταποκριθεί, του ζητούν να καταχωρήσει σε ειδική φόρμα ευαίσθητες προσωπικές πληροφορίες, όπως ονοματεπώνυμο, διεύθυνση κατοικίας, αριθμό τηλεφώνου, αριθμό τραπεζικού λογαριασμού, ΑΦΜ, αριθμό πιστωτικής κάρτας κ.ά.

Επισημαίνεται ότι τα μηνύματα αυτά χρήζουν μεγάλης προσοχής, καθότι χρησιμοποιούν το λογότυπο της Γενικής Γραμματείας Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών και παρουσιάζονται εξαιρετικά αληθοφανή. Καλούνται οι χρήστες που λαμβάνουν τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου να μην απαντούν να μην καταχωρούν και να μην στέλνουν προσωπικά δεδομένα καθότι σε καμία περίπτωση δεν είναι αληθινά. Επισημαίνεται ότι κανένας Οργανισμός ή Φορέας δεν ζητά πληροφορίες, όπως αριθμούς πιστωτικών καρτών, αριθμούς τραπεζικών λογαριασμών κ.λπ., μέσω ηλεκτρονικού ταχυδρομείου. Υπενθυμίζεται ότι για ανάλογα περιστατικά, οι πολίτες μπορούν να επικοινωνούν με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας: Τηλεφωνικά: 111 88 Στέλνοντας e-mail στο: ccu@cybercrimeunit.gov.gr Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones) με λειτουργικό σύστημα ios-android: CYBERKID

Πηγή: www.lifo.gr

[864] http://www.lifo.gr/now/digital-life/56957

6. Σύλληψη για διακίνηση πορνογραφίας στο διαδίκτυο

Η Δίωξη Ηλεκτρονικού Εγκλήματος συνέλαβε 36χρονο από την Κάρπαθο που φέρεται να συμμετείχε σε διεθνές κύκλωμα παιδεραστών και κατηγορείται για πορνογραφία ανηλίκων και σεξουαλικό τουρισμό.

Ο 36χρονος συνελήφθη στο πλαίσιο διεθνούς έρευνας για τη διακίνηση παιδικής πορνογραφίας.

Σύμφωνα με την αστυνομία, ο συλληφθείς χρησιμοποιούσε διάφορα ψευδώνυμα και διακινούσε υλικό στο διαδίκτυο, ενώ παράλληλα διαφήμιζε σε παιδεραστές το ξενοδοχείο του, υποσχόμενος δωρεάν διακοπές στην Κάρπαθο με μοναδικό αντάλλαγμα να ασελγήσει στα ανήλικα παιδιά τους.

Ο συλληφθής οδηγήθηκε στον εισαγγελέα Ρόδου. [865]

7. Σύλληψη κυκλώματος παραχαρακτών

«Στα ίχνη κυκλώματος παραχαρακτών» [866]

«Ένας 30χρονος συνελήφθη, ενώ διεξάγονται έρευνες για τον εντοπισμό και άλλων μελών.

Στα ίχνη διεθνούς κυκλώματος παραχάραξης τραπεζικών καρτών βρίσκονται οι αστυνομικές αρχές στη Θεσσαλονίκη μετά τη σύλληψη αλλοδαπού ο οποίος κατείχε 120 κλωνοποιημένες κάρτες ανάληψης χρημάτων από ΑΤΜ.

Σύμφωνα με την αστυνομία, αστυνομικοί της Ασφάλειας συνέλαβαν ένα 30χρονο Ρουμάνο έξω από υποκατάστημα τράπεζας στη Θεσσαλονίκη την ώρα που επιχειρούσε να αποσπάσει χρήματα από το μηχάνημα αυτόματης ανάληψης χρησιμοποιώντας πλαστή κάρτα.

Σε έρευνα που πραγματοποιήθηκε στο δωμάτιο του ξενοδοχείο όπου είχε καταλύσει ο 30χρονος μαζί με έναν ομοεθνή του ο οποίος διέφυγε και αναζητείται.

Στις αποσκευές τους βρέθηκαν άλλες 113 κλωνοποιημένες κάρτες, όπως επίσης και 32.450 ευρώ τα οποία προέρχονται από αναλήψεις.

Από την Ασφάλεια συνεχίζονται οι έρευνες για τον εντοπισμό και των άλλων μελών του κυκλώματος».

[865] Δημοσίευση 7 Απριλίου (2008) , http://tech.pathfinder.gr/tech/lawnet/609095.html

[866] Πηγή ιστοσελίδα εφημερίδος «Το Έθνος» http://www.ethnos.gr/article.asp?catid=11424&subid=2&tag=8400&pubid=820496 , 11/4/(2008)

8. Οδηγίες από το Υπουργείο Προστασίας του Πολίτη

Η Ελληνική Αστυνομία εξέδωσε τις παρακάτω απλές οδηγίες για Ασφαλή Πρόσβαση στο Διαδίκτυο και προστασία από την παραβίαση των προσωπικών δεδομένων, απάτες, απειλές ή άλλες εγκληματικές ενέργειες: [867]

«1. Όταν λαμβάνετε email από τράπεζες, να είστε γενικά καχύποπτοι και να γνωρίζετε ότι μια τράπεζα δε θα έστελνε ποτέ ένα μήνυμα προσκαλώντας τους πελάτες της να συμπληρώσουν τα στοιχεία τους σε μια ιστοσελίδα.

2. Εάν έχετε οποιαδήποτε αμφιβολία σχετικά με τον αποστολέα, είναι προτιμότερο πριν απαντήσετε στο email να επικοινωνήσετε με την εταιρεία – αποστολέα για να εξακριβώσετε ότι δεν πρόκειται για περίπτωση απάτης.

3. Μην ακολουθείτε links από email ή ιστοσελίδες αλλά πάντα να πληκτρολογείτε τις διευθύνσεις που σας ζητάνε να επισκεφθείτε.

4. Πριν από κάθε ηλεκτρονική συναλλαγή, να ελέγχετε ότι η ηλεκτρονική διεύθυνση στην οποία βρίσκεστε αρχίζει με «https://» και όχι απλά «http://». Έτσι διασφαλίζετε ότι χρησιμοποιείτε ασφαλή σύνδεση web (http secure).

5. Μην απαντάτε σε μηνύματα ηλεκτρονικού ταχυδρομείου εάν δεν γνωρίζετε τον αποστολέα. Για να μην γεμίζει η διεύθυνση ηλεκτρονικού ταχυδρομείου σας με άχρηστα διαφημιστικά μηνύματα, διαγράψτε τα πριν καν τα διαβάσετε.

6. Καλό είναι να υπάρχει στον υπολογιστή σας ένα λογισμικό προστασίας από ιούς (antivirus). Το λογισμικό αυτό μπορεί να προστατεύσει από ιούς ή λογισμικά υποκλοπής (spyware). Πολλές φορές τα phishing μηνύματα παραπέμπουν σε ιστοσελίδες που εγκαθιστούν στον υπολογιστή σας λογισμικά υποκλοπής, τα οποία καταγράφουν κάθε πληροφορία που εισάγεται από αριθμούς λογαριασμών και πιστωτικών καρτών μέχρι και κωδικών πρόσβασης, ακόμα και μετά την έξοδο του χρήστη από την ιστοσελίδα.

7. Μπορείτε επίσης να εγκαταστήσετε στο ηλεκτρονικό σας ταχυδρομείο ένα ψηφιακό φίλτρο που να μπλοκάρει την ανεπιθύμητη αλληλογραφία.

8. Μην αγοράζετε ποτέ προϊόντα που διαφημίζονται σε spam email ούτε να πλοηγείσθε στα links που περιέχονται σε αυτά, επειδή τα περισσότερα από αυτά είναι απάτες. 9. Να χρησιμοποιείτε δύο λογαριασμούς ηλεκτρονικού ταχυδρομείου. Ο ένας να αποτελεί τον προσωπικό σας λογαριασμό και ο άλλος να χρησιμοποιείται για οποιαδήποτε άλλη δραστηριότητα στο διαδίκτυο (οικονομικές συναλλαγές, εγγραφή σε Forum κλπ). 10. Μην αποθηκεύετε κωδικούς πρόσβασης, αριθμούς ταυτότητας, αριθμούς πιστωτικής κάρτας, στοιχεία για τα μέλη της οικογένειάς σας ή άλλα προσωπικά στοιχεία στον υπολογιστή σας.

11. Να μην εμπιστεύεσθε άγνωστα άτομα κατά τη διάρκεια συζητήσεων σε chat room και να μην δίνετε τα προσωπικά σας στοιχεία.

12. Σε περίπτωση που δέχεστε απειλές από άτομα κατά τη διάρκεια των διαδικτυακών σας συζητήσεων, διακόψτε αμέσως επικοινωνία μαζί τους και επικοινωνήστε απευθείας με τα Τμήματα Δίωξης Ηλεκτρονικού Εγκλήματος των Διευθύνσεων Ασφαλείας Αττικής και Θεσσαλονίκης, κατά περίπτωση».

[867] Οδηγίες από το Υπουργείο Προστασίας του Πολίτη: (2010)-11-23, ανακτήθηκε από http://blogs.sch.gr/internet-safety/archives/222, Νοέμβριος 2014

9. Τάσεις, ευκαιρίες και προκλήσεις για το e-commerce, μέσα από 3 έρευνες[868]

«Τρεις ιδιαίτερα ενδιαφέρουσες έρευνες για το e-commerce που είδαν τις τελευταίες ημέρες το φως της δημοσιότητας, τόσο στην Ελλάδα, όσο και στο εξωτερικό, παρουσιάζουν με ιδιαίτερα ανάγλυφο τρόπο τη δυναμική της εν λόγω λειτουργίας, τις ευκαιρίες και τις προκλήσεις που καλείται να αντιμετωπίσει στο παγκοσμιοποιημένο περιβάλλον.

Οι έρευνες αυτές δημοσιοποιήθηκαν από την Info-bank Hellastat, η οποία αφορά στην Ελλάδα, καθώς και από τις RSA-Τμήμα Ασφαλείας της EMC και FedEx, οι οποίες είναι διεθνείς.

IBHS: Αύξηση 10% των online αγορών το 2014 στην Ελλάδα

Ο κλάδος των ηλεκτρονικών αγορών στην χώρα μας εμφανίζει σημαντική ανάπτυξη λόγω των χαμηλότερων τιμών σε σχέση με τα συμβατικά καταστήματα, ενώ οι καταναλωτές σταδιακά εξοικειώνονται περισσότερο με την τεχνολογία, αναφέρει μελέτη της IBHS. Βάσει στοιχείων του ELTRUN, το 2013 οι συνολικές πωλήσεις των ελληνικών και ξένων e-shops σε Έλληνες καταναλωτές διαμορφώθηκαν σε 3,2 δισ. ευρώ, σημειώνοντας άνοδο 25% από το 2012. Η αγορά εκτιμάται ότι ενισχύθηκε περαιτέρω το 2014, καθώς οι καταναλωτές αύξησαν κατά περίπου 10% τον αριθμό των προϊόντων και υπηρεσιών που αγόρασαν διαδικτυακά. Οι online καταναλωτές το 2013 ανήλθαν σε περίπου 2,2 εκατ. (από 1,9 εκατ. το 2012), αποτελώντας μόνο το 35% των χρηστών του διαδικτύου, σε σχέση με 70% στη Δυτική Ευρώπη. Επιπλέον, μόνο το 60%-65% των αγορών πραγματοποιούνται από ελληνικά sites, με τους Ευρωπαίους καταναλωτές να προτιμούν τα εθνικά sites για το 90% των αγορών τους.

Τα ελληνικά e-shops έχουν υλοποιήσει διαχρονικά σημαντική αναβάθμιση σε τομείς όπως η ασφάλεια των συναλλαγών, οι εναλλακτικοί τρόποι πληρωμής, η λειτουργικότητα και φιλικότητα της ιστοσελίδας και οι υπηρεσίες υποστήριξης. Σύμφωνα με το ELTRUN, για το 2014 το 70% των e-shops αναφέρει αναλυτικά τους όρους χρήσης των συναλλαγών (61% το 2012), ενώ αύξηση 68% εμφανίζει το ποσοστό όσων αναφέρουν ξεκάθαρα την πολιτική προστασίας προσωπικών δεδομένων (60% το 2012). Αντιθέτως, το 10% κρίνεται επισφαλές ως προς την ασφάλεια των συναλλαγών λόγω έλλειψης εταιρικής πληροφόρησης. Η αντικαταβολή αποτελεί τον πιο συνηθισμένο τρόπο πληρωμής, καθώς εφαρμόζεται στο 91% των e-shops.

Τέλος, το 81% παρέχει δυνατότητα χρήσης πιστωτικής κάρτας και το 72% χρεωστικής, ποσοστά ιδιαίτερα αυξημένα σε σχέση με το 2012. Σύμφωνα με τον Χρυσόστομο Κάτση, Διευθύνοντα Σύμβουλο της Infobank Hellastat, «ο κλάδος έχει περιθώρια για ακόμα μεγαλύτερη ανάπτυξη, δεδομένων των οικονομικών συνθηκών που επικρατούν στην Ελλάδα και του χαμηλού –συγκριτικά με άλλες ευρωπαϊκές χώρες- αριθμού των online αγοραστών. Πάντως, απαραίτητη προϋπόθεση για ακόμα μεγαλύτερη διείσδυση των ηλεκτρονικών συναλλαγών στην καταναλωτική συμπεριφορά των Ελλήνων αποτελεί η αύξηση της εμπιστοσύνης των καταναλωτών στα e-shops, κάτι που θα επιτευχθεί μέσω βελτίωσης της ασφάλειας των συναλλαγών».

RSA: Από το διαδίκτυο το 26-50% του συνολικού τζίρου

Περνώντας στο διεθνές περιβάλλον, ιδιαίτερο ενδιαφέρον παρουσιάζει πρόσφατη έρευνα της RSA (το τμήμα ασφαλείας της EMC), η οποία αφορούσε στην ασφάλεια στον κυβερνοχώρο και διεξήχθη σε συνεργασία με την εταιρεία ερευνών J.Gold Associates, με τη συμβολή της εταιρείας TeleSign. Η έρευνα είχε τίτλο «Ηλεκτρονικό εμπόριο μέσω mobile

[868] Κορδεράς Δημήτρης (2015)

συσκευών: Φίλος ή εχθρός;» και αξιολογεί τις νέες τάσεις, αλλά και τον οικονομικό αντίκτυπο του ηλεκτρονικού εμπορίου μέσω mobile συσκευών. Σε αυτή συμμετείχαν 250 μεσαίες αλλά και μεγάλες επιχειρήσεις και οργανισμοί της Βόρειας Αμερικής, οι οποίες είχαν κατά μέσο όρο έσοδα ύψους 2,54 δισεκατομμυρίων δολαρίων. Η έρευνα φέρνει στο φως τις ευρύτερες επιπτώσεις των υποθέσεων που σχετίζονται με απάτες μέσω κινητών τηλεφώνων, με το μέσο όρο των ερωτηθέντων να έχουν υποστεί απώλειες της τάξεως των 92,3 εκατομμυρίων δολαρίων ανά έτος.

Τέσσερα είναι τα βασικά ευρήματα της έρευνας: Το πρώτο αναφέρει ότι το 1/3 των οργανισμών δήλωσε ότι το εύρος των εσόδων που αποκομίζουν από το διαδίκτυο ανέρχεται στο ύψος του 26-50% του συνολικού τους τζίρου. Στη συνέχεια, το 25% των ερωτηθέντων δηλώνει ότι το 11-25% των εσόδων τους προέρχεται από εφαρμογές για mobile συσκευές, ενώ το 50% αναμένει τα έσοδα που προέρχονται από τις συγκεκριμένες συσκευές να αυξηθούν κατά 11-50% τα επόμενα 3 χρόνια. Τέλος, το 30% των οργανισμών προβλέπει αύξηση 51-100% των εσόδων που προέρχονται από mobile συσκευές. Τα στοιχεία υποδηλώνουν ότι το διαδίκτυο και το mobile κανάλι αποτελούν πλέον βασική πηγή εσόδων. Τα συγκεκριμένα, μεγάλα ποσοστά, καθιστούν απαραίτητη για τις εταιρείες την εύρεση λύσεων για την προστασία των εσόδων τους από ενδεχόμενες απάτες. Ο μεγάλος αριθμός απωλειών, υποδεικνύει την ύπαρξη ενός ιδιαιτέρως σοβαρού προβλήματος το οποίο δεν αντιμετωπίζεται κατάλληλα από τα υπάρχοντα συστήματα και τις σχετικές διαδικασίες.

Επιπλέον, καθώς η πλειονότητα των εταιρειών προσδοκά στη συνεχή αύξηση αυτών των εσόδων, προκύπτει επιτακτική ανάγκη για διασφάλιση των συναλλαγών. Η μελέτη δείχνει επίσης ότι η πλειοψηφία των εταιρειών διατηρεί μια λανθασμένη αντίληψη σχετικά με το θέμα της ασφάλειας: 2/3 των ερωτηθέντων πιστεύουν ότι είναι κατάλληλα εξοπλισμένοι για να εντοπίσουν γρήγορα και να αντιμετωπίσουν οποιαδήποτε διαδικτυακή επίθεση που μπορεί να επηρεάσει τις ιστοσελίδες τους. Ωστόσο, το 59% όσων ρωτήθηκαν, δήλωσαν πως έχουν χάσει έως και 25% των εσόδων της εταιρείας λόγω δραστηριοτήτων εξαπάτησης. Οι δραστηριότητες μέσω mobile συσκευών αναπτύσσονται με γεωμετρική πρόοδο, αυξάνοντας τον κίνδυνο της απάτης. Για τον λόγο αυτό, οι εταιρείες πρέπει να ενισχύσουν τα πρωτόκολλα ασφαλείας τους, καθώς και τις διαδικασίες login και authentication». Marketing Week (Τ. 1458)

10. Πρόστιμο στη ΓΓΠΣ για διαρροή φορολογικών δεδομένων [869]

«Διαρροή προσωπικών δεδομένων του συνόλου των Ελλήνων φορολογουμένων προς εταιρείες εμπορίας προσωπικών δεδομένων συνέβαινε επί τουλάχιστον δώδεκα χρόνια, λόγω ανεπάρκειας των μέτρων ασφαλείας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων του υπουργείου Οικονομικών. Το γεγονός, το οποίο σημειωτέον δεν αμφισβητείται ούτε από τη Γενική Γραμματεία Πληροφοριακών Συστημάτων, διαπίστωσε η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και επέβαλε πρόστιμο 150.000 ευρώ στο υπουργείο Οικονομικών, ζητώντας παράλληλα την ισχυροποίηση των μέτρων ασφαλείας για την προστασία των φορολογουμένων. Στην Αρχή προσέφυγε εκ νέου η Γενική Γραμματεία Πληροφοριακών Συστημάτων, ζητώντας μείωση του προστίμου και πίστωση χρόνου για τη συμμόρφωση με την απόφαση, ωστόσο η προσφυγή απορρίφθηκε (απόφαση 117/2014).

Σύμφωνα με τα όσα περιλαμβάνονται στην απόφαση της Αρχής, πλήθος απόρρητων προσωπικών δεδομένων που αφορούν το σύνολο των φορολογουμένων στην Ελλάδα, όπως είναι τα Ε1, Ε9, στοιχεία για το ΕΤΑΚ, τα τέλη κυκλοφορίας κτλ., διέρρευσαν σε εταιρείες εμπορίας δεδομένων προσωπικού χαρακτήρα. Όπως επισημαίνεται μάλιστα στην απόφαση, η διαρροή, η οποία αποδίδεται στα ελλιπή μέτρα ασφαλείας της Γ.Γ., είναι «πρωτοφανούς έκτασης, αφού αφορά στο σύνολο των φορολογουμένων στην Ελλάδα, για ιδιαίτερα μακρύ χρονικό διάστημα». Η όλη υπόθεση αποκαλύφθηκε κατά τη διάρκεια ελέγχων της Αρχής σε εταιρείες εμπορίας προσωπικών δεδομένων, που έγιναν το 2012. Στο πλαίσιο των ερευνών διαπιστώθηκε ότι οι εταιρείες είχαν στη διάθεσή τους αναλυτικά στοιχεία δηλώσεων φορολογίας εισοδήματος, έντυπα Ε1 και Ε9, στοιχεία για το ΕΤΑΚ και την έκτακτη εισφορά, για το ύψος των τελών κυκλοφορίας αλλά και για το ποιοι φορολογούμενοι έκαναν περαίωση το 2010.

Ιδιαίτερα ενδιαφέρον είναι το γεγονός ότι, όπως χαρακτηριστικά αναφέρεται στην απόφαση της Αρχής, η Γενική Γραμματεία δεν αμφισβητεί τα πραγματικά δεδομένα της διαρροής προσωπικών δεδομένων φορολογουμένων αλλά και τις παραβάσεις που της αποδίδονται».

[869] Καραμανώλη Εύα (2014)

11. Ποιοι δίνουν άσυλο στους επίορκους [870]

«Τα Υπηρεσιακά Συμβούλια που θα εφαρμόσουν το νέο αυστηρότερο πειθαρχικό δίκαιο για τους δημοσίους υπαλλήλους δεν έχουν συγκροτηθεί, αν και μεσολάβησαν 11 μήνες από την ψήφιση του νόμου. Ευθύνες αποδίδονται σε υπουργούς, δικαστικούς και συνδικαλιστές, που στερούνται πολιτικής βούλησης. Ασπίδα προστασίας εξακολουθεί να καλύπτει τους επίορκους.

Σωρεία καταγγελιών για το σύστημα συμφερόντων που δημιουργεί ασπίδα προστασίας στους επίορκους υπαλλήλους προκάλεσε η αποκάλυψη του «Έθνους της Κυριακής» με τη λίστα των 1.301 δημοσίων υπαλλήλων για τους οποίους έχουν ασκηθεί διώξεις για σοβαρά ποινικά αδικήματα, ενώ η πολιτική ηγεσία του Υπ. Διοικητικής Μεταρρύθμισης «αγνοεί» την τύχη των συγκεκριμένων υποθέσεων.

Ο πρώην υπουργός Επικρατείας επί κυβέρνησης Λ. Παπαδήμου και επίτιμος αντιπρόεδρος του Συμβουλίου της Επικρατείας Γ. Σταυρόπουλος, ο οποίος ήταν από τους εμπνευστές του νέου πειθαρχικού δικαίου στο Δημόσιο, μιλώντας σε επιστημονική ημερίδα, επέρριψε ευθύνες στην κυβέρνηση, επειδή 11 μήνες μετά την ψήφιση του νέου νόμου δεν έχουν συσταθεί ακόμη τα πειθαρχικά συμβούλια με πλειοψηφία δικαστικών λειτουργών. Άφησε αιχμές για την απροθυμία των δικαστών να συμμετάσχουν στα νέα πειθαρχικά.

Αναφερόμενος στο μακροχρόνιο καθεστώς ατιμωρησίας που έριχνε στα «μαλακά» τους επίορκους, ο Γ. Σταυρόπουλος ήταν ιδιαίτερα καυστικός κάνοντας λόγο για κομματικούς δεσμούς μεταξύ των υπουργών που όριζαν με απόφασή τους τον πρόεδρο και την πλειοψηφία των μελών στα πειθαρχικά με αποτέλεσμα την «προστασία» των επίορκων με απαλλακτικές αποφάσεις και χαμηλές πειθαρχικές ποινές. Ο πρώην υπουργός επέκρινε και την ΑΔΕΔΥ ότι δεν αντιδρούσε στο φαινόμενο αυτό, αλλά και ότι αντιδρούσε στην ψήφιση του νέου αυστηρότερου πειθαρχικού δικαίου.

Ο Γενικός Επιθεωρητής Δημόσιας Διοίκησης Λ. Ρακιντζής δήλωσε στο «Εθνος» ότι τώρα αρχίζει να ξεκαθαρίζεται το τοπίο των επίορκων και, αναφερόμενος στη λίστα που δημοσίευσε το «Εθνος της Κυριακής», σημείωσε ότι τώρα γίνεται έλεγχος για να διαπιστωθεί εάν υπηρετούν ακόμα στο Δημόσιο ή εάν έχουν εκδοθεί τελεσίδικες δικαστικές αποφάσεις για τα αδικήματα που κατηγορούνται.

«Χρειάζεται να υπάρχει πολιτική βούληση για να επιταχυνθούν οι πειθαρχικές διαδικασίες», σημείωσε ο Λ. Ρακιντζής και τόνισε ότι χρειάζεται να επανέλθει στον Γενικό Επιθεωρητή Δημόσιας Διοίκησης το δικαίωμα να ασκεί ένσταση στα πρωτοβάθμια πειθαρχικά συμβούλια, προκειμένου να αποφευχθούν εσφαλμένες αποφάσεις.

«Η επίσπευση της πειθαρχικής διαδικασίας στο Δημόσιο αλλά και η επιτάχυνση των δικαστικών αποφάσεων είναι αναγκαίες, καθώς μέχρι να τελεσιδικήσουν οι αποφάσεις των δικαστηρίων μπορεί να φτάσουν μέχρι και τα 8 χρόνια».

Αξίζει να σημειωθεί ότι οι υπηρεσίες του Γενικού Επιθεωρητή είχαν καταγράψει και απέστειλαν στο υπουργείο Διοικητικής Μεταρρύθμισης τη λίστα με τις ποινικές διώξεις που έχουν ασκηθεί σε 1.301 επίορκους υπαλλήλους από το 2007 έως και το 2012.

Να τιμωρηθούν άμεσα οι υπάλληλοι που κατηγορούνται για σοβαρά πειθαρχικά και ποινικά αδικήματα, αναφέρει στο «Εθνος» ο πρόεδρος της ΑΔΕΔΥ Κ. Τσικρικάς, επισημαίνοντας ότι η πειθαρχική διαδικασία θα πρέπει να σεβαστεί τις διατάξεις του Συντάγματος και του δημοσιοϋπαλληλικού κώδικα. Κατηγορεί το υπουργείο Διοικητικής

[870] Ποιοι δίνουν άσυλο στους επίορκους, ανακτήθηκε από http://www.ethnos.gr/article.asp?catid=22768&subid=2&pubid=63795095# , Μάρτιος 2015

Μεταρρύθμισης ότι κάνοντας λόγο για 7.000 ή 10.000 υποθέσεις επίορκων «στοχοποιεί τους δημοσίους υπαλλήλους και εξισώνει τα πραγματικά σοβαρά περιστατικά παραβατικότητας, εκείνα δηλαδή που χρήζουν άμεσης εκδίκασης και επιβολής ακόμα και της αυστηρότερης των ποινών (απόλυση), με ήσσονος σημασίας ζητήματα, τα οποία μάλιστα στις περισσότερες περιπτώσεις συνδέονται με αναπόδεικτες παραπομπές υπαλλήλων στα πειθαρχικά συμβούλια».

Ο κ. Τσικρικάς καταγγέλλει την κυβέρνηση για λαϊκισμό και ισοπεδωτικές λογικές με τις οποίες «καταργείται το τεκμήριο της αθωότητας, υπονομεύεται η Δικαιοσύνη και η ίδια η Δημοκρατία!», ενώ καλεί τους εργαζομένους να συμμετάσχουν στο συλλαλητήριο που διοργανώνει η ΑΔΕΔΥ την Τετάρτη στις 19 Μαρτίου στην Αθήνα, «ενάντια στις απολύσεις και την αντιμετώπιση της κυβερνητικής αυθαιρεσίας σε βάρος των δημοσίων υπαλλήλων».

«Εδώ και τώρα να τιμωρηθούν οι επίορκοι», δηλώνει στο «Εθνος» ο πρόεδρος της ΠΟΕ-ΟΤΑ Θ. Μπαλασόπουλος και επισημαίνει: «Το υπ. Διοικητικής Μεταρρύθμισης να σταματήσει τα επικοινωνιακά παιχνίδια που στοχοποιούν τους δημοσίους υπαλλήλους, αναφέροντας αυθαίρετα αριθμούς, ενώ την ίδια στιγμή, έναν χρόνο μετά την ψήφιση του νόμου δεν έχει καταφέρει να συγκροτήσει τα νέα πειθαρχικά συμβούλια με πλειοψηφία δικαστών».

ΝΙΚΟΣ Β. ΤΣΙΤΣΑΣ

ΚΕΡΑΥΝΟΙ ΑΠΟ ΤΟΝ Γ. ΣΤΑΥΡΟΠΟΥΛΟ ΓΙΑ ΤΑ ΜΑΚΡΟΧΡΟΝΙΑ ΦΑΙΝΟΜΕΝΑ ΟΛΙΓΩΡΙΑΣ

Κάνουν τα «στραβά μάτια» υπουργοί και προϊστάμενοι

Νέα εμπλοκή στη συγκρότηση και λειτουργία των πρωτοβάθμιων πειθαρχικών συμβουλίων για τους επίορκους υπαλλήλους του Δημοσίου και των ΝΠΔΔ προκαλεί η άρνηση των δικαστών του Ελεγκτικού Συνεδρίου (ΕΣ) να συμμετάσχουν σε αυτά, καθώς θεωρούν αντισυνταγματικές τις σχετικές ρυθμίσεις του νέου πειθαρχικού δικαίου των δημοσίων υπαλλήλων.

Την ίδια στιγμή, στο πλαίσιο επιστημονικής ημερίδας, ο συντάκτης του νέου αυστηροποιημένου πειθαρχικού δικαίου Γ. Σταυρόπουλος (επίτιμος αντιπρόεδρος ΣτΕ, πρώην υπουργός) επέκρινε δριμύτατα την επί 11 σχεδόν μήνες μη εφαρμογή του, τις υπόκωφες αντιδράσεις προκειμένου να «παγώσει», περιγράφοντας με γλαφυρό τρόπο τι συνέβαλε στην επί χρόνια απογοητευτική εικόνα της ατιμωρησίας, με πειθαρχικές ποινές που αθώωναν ή έριχναν τους επίορκους «στα μαλακά».

Η γενική συνέλευση της Ένωσης Δικαστών του ΕΣ έκρινε ότι οι πάρεδροι ΕΣ δεν μπορούν για συνταγματικούς λόγους να συμμετάσχουν στα πρωτοβάθμια πειθαρχικά, γιατί, κατά παράβαση του Συντάγματος και της αρχής της δικαστικής ανεξαρτησίας, δεν εξασφαλίστηκε από την πολιτεία η προηγούμενη συγκατάθεση των δικαστών του ΕΣ, προκειμένου να ανατεθούν σε αυτούς διοικητικά καθήκοντα.

Ο ν. 4057/12 προβλέπει ότι στα 3μελή πρωτοβάθμια προεδρεύει δικαστικός λειτουργός (πάρεδρος ΕΣ ή εφέτης, πρόεδρος πρωτοδικών ή αντίστοιχου βαθμού εισαγγελέας) με 2ετή θητεία αποκλειστικής απασχόλησης και ειδική αποζημίωση. Οι άλλες δικαστικές ενώσεις δεν έχουν αρνηθεί τη συμμετοχή δικαστών, η οποία είχε «παγώσει» όμως στη διάρκεια των κινητοποιήσεων.

Οι δικαστές του ΕΣ υποστηρίζουν επίσης ότι δεν είναι επιτρεπτό η κρίση των πρωτοβάθμιων πειθαρχικών, που εκφέρεται υπό την προεδρία δικαστικού λειτουργού, να ελέγχεται σε β' βαθμό από δευτεροβάθμιο πειθαρχικό όπου προεδρεύει μέλος του Νομικού Συμβουλίου του Κράτους (ΝΣΚ). Υπογραμμίζουν ακόμα ότι δεν είναι νοητή η απειλή

πειθαρχικών διώξεων σε βάρος δικαστικών λειτουργών για την εκτέλεση μη δικαστικών καθηκόντων (όπως είναι τα πειθαρχικά υπαλλήλων).

Η άρνηση αυτή σημαίνει, πάντως, ότι πρέπει να αλλάξουν οι συνθέσεις πειθαρχικών όπου έχουν οριστεί δικαστές του ΕΣ, ενώ αντίθετα η πρόεδρος της Ενωσης Δικαστών και Εισαγγελέων αρεοπαγίτης Β. Θάνου - Χριστοφίλου διαβεβαίωσε ότι δεν υπάρχουν στον κλάδο της αντιρρήσεις για συμμετοχή στα πειθαρχικά.

Ιδιαίτερα αποκαλυπτική για τα μακρόχρονα φαινόμενα ατιμωρησίας, τα πειθαρχικά που έριχναν «στα μαλακά» τους επίορκους, αλλά και τις έντονες αντιδράσεις στη λειτουργία του νέου αυστηρότερου πειθαρχικού δικαίου, ήταν η ομιλία του Γ. Σταυρόπουλου, βαθύ γνώστη του αντικειμένου, αφού επί χρόνια προήδρευε στο ΣτΕ και για τέτοιες υποθέσεις, ενώ ήταν ο πρόεδρος της νομοπαρασκευαστικής επιτροπής για την αυστηροποίηση του πειθαρχικού με τον ν. 4057/12.

Ο επίτιμος αντιπρόεδρος ΣτΕ και πρώην υπουργός επέκρινε την επί χρόνια συχνή αδιαφορία υπουργών και προϊσταμένων διεύθυνσης απέναντι σε πιθανά πειθαρχικά παραπτώματα υφισταμένων τους. Άλλοτε κάνουν «τα στραβά μάτια» -τόνισε- και δίνουν συνήθως την εντύπωση ότι δεν έχουν διάθεση να πολεμήσουν τη διαφθορά στον χώρο ευθύνης τους επιλαμβανόμενοι μετά από καταγγελία ή δημοσιοποίηση του περιστατικού.

Χαρακτήρισε απογοητευτική την πρακτική των ΕΔΕ, μίλησε για «ξεχασμένα πορίσματα», καθυστερήσεις και παραγραφές, αλλά και για την απογοητευτική αδυναμία της Δικαιοσύνης να αντιμετωπίσει αποτελεσματικά και σε εύλογο χρόνο τα φαινόμενα παραβατικής συμπεριφοράς, δείχνοντας κάποιες φορές ανεξήγητη επιείκεια ή εμμονή σε τυπολατρικές ακυρώσεις.

Ιδιαίτερα καυστικός ήταν ο Γ. Σταυρόπουλος για τα πειθαρχικά προ του ν. 4057/12, αφού η πλειοψηφία ανήκε σε υπαλλήλους που με τον ορισμό τους αποκτούσαν διευθυντικό βαθμό, χωρίς διαδικασία επιλογής και ήταν φυσικό να οφείλουν χάρη στον υπουργό. Μίλησε για προφανή κομματικό δεσμό με τον υπουργό που όριζε τον πρόεδρο του πειθαρχικού και για έλλειψη αμεροληψίας των υπολοίπων εκλεγμένων που, αν και ανήκαν σε διαφορετικές συνήθως παρατάξεις, εξυπηρετούσαν με συνέπεια τους κομματικούς ψηφοφόρους και συνεννοούνταν άψογα μεταξύ τους, παρά τις πολιτικές διαφορές. Αποτέλεσμα ήταν οι απαλλακτικές αποφάσεις ή οι πολύ χαμηλές πειθαρχικές ποινές.

«Ήταν όλοι έτσι ευχαριστημένοι -είπε- αφού οι εγκαλούμενοι υπάλληλοι, ανεξαρτήτως πολιτικής απόχρωσης, αθωώνονταν ή "έπεφταν στα μαλακά" κι έτσι ο υπουργός εξασφάλιζε και με τον τρόπο αυτόν συνδικαλιστική ειρήνη στο υπουργείο και η διαφθορά καλά κρατούσε, διαχρονικά και διακομματικά»!

Ιδιαίτερα επέκρινε το γεγονός ότι η ΑΔΕΔΥ δεν αντιδρούσε στο φαινόμενο αυτό, αλλά και στο ότι εκδηλώθηκε «μέγιστη, κυρίως υπόκωφη αντίδραση» στο νέο πειθαρχικό, καθώς οι δημοσιοϋπαλληλικές οργανώσεις μεθόδευσαν και ακόμα μεθοδεύουν τη μη εφαρμογή.

Αρχικά έκαναν ό,τι μπορούσαν για να μην προωθηθεί στη Βουλή, στη συνέχεια να μην ψηφιστεί και να μην εφαρμοστεί ως νόμος, υποστηρίζοντας μάλιστα στην αρμόδια κοινοβουλευτική επιτροπή ότι το παλαιό πειθαρχικό λειτουργούσε άψογα και οι δημόσιοι υπάλληλοι δεν διαπράττουν πειθαρχικά παραπτώματα.

Υπογράμμισε ότι 11 μήνες μετά την έναρξη ισχύος του νέου νόμου (4057/12) το βασικό εργαλείο για την καταπολέμηση της διαφθοράς στον χώρο των υπαλλήλων του Δημοσίου, τα νέα πρωτοβάθμια πειθαρχικά συμβούλια, φαίνεται ότι δεν έχουν λειτουργήσει ακόμα και η εφαρμογή του νόμου προχωρά με μεγάλες δυσκολίες και εσωτερικές αντιδράσεις».

ΑΛΕΞΑΝΔΡΟΣ ΑΥΛΩΝΙΤΗΣ 11/3/2013

Η λίστα με τους 1.301 επίορκους που εμπλέκονται σε 2.200 σκάνδαλα

«Την περιβόητη λίστα με τους επίορκους που παρέδωσαν οι υπηρεσίες του Γενικού Επιθεωρητή Δημόσιας Διοίκησης στο υπουργείο Διοικητικής Μεταρρύθμισης εδώ και περίπου δύο εβδομάδες αποκάλυψε χτες το «Εθνος της Κυριακής». Στην κατάσταση περιλαμβάνονται 2.200 ποινικές διώξεις για σοβαρά αδικήματα που κατηγορούνται ότι διέπραξαν 1.301 υπάλληλοι από το 2007 μέχρι και το 2012.

Χαρακτηριστικό στοιχείο του κομφούζιου που επικρατεί με τους επίορκους στο Δημόσιο είναι το γεγονός ότι η κυβέρνηση δεν γνωρίζει εάν οι συγκεκριμένοι υπάλληλοι έχουν απομακρυνθεί από τις θέσεις τους ή εάν έχουν ληφθεί τελεσίδικες αποφάσεις από τα ελληνικά δικαστήρια. Από την πλευρά του υπουργείου Διοικητικής Μεταρρύθμισης δεν υπήρχε επίσημη αντίδραση για το δημοσίευμα.

Σύμφωνα με τη λίστα των επίορκων, η μεγαλύτερη ομάδα υπαλλήλων στους οποίους έχουν ασκηθεί ποινικές διώξεις για σοβαρά αδικήματα αφορά την Τοπική Αυτοδιοίκηση (δήμοι, νομαρχίες, περιφέρειες και δημοτικές επιχειρήσεις), όπου ο αριθμός των υπαλλήλων που διώκονται από το 2007 μέχρι το 2012 αγγίζει τους 619, που αντιστοιχεί στο 47% των περιπτώσεων ενώ περιλαμβάνονται 128 εφοριακοί, 62 γιατροί και 56 δάσκαλοι».

12. Δικαστική απόφαση για έγκλημα λευκού πριλαιμίου με ηλεκτρονικά μέσα (υπόθεση cd με «λίστα Λαγκάρντ)

«Ποινή - χάδι για Παπακωνσταντίνου» [871]

« Το δικαστήριο αναγνώρισε στον πρώην υπουργό το ελαφρυντικό του πρότερου έντιμου βίου.

Ο πρώην υπουργός Οικονομικών Γιώργος Παπακωνσταντίνου κρίθηκε ένοχος -κατά πλειοψηφία- για νόθευση εγγράφου σε βαθμό πλημμελήματος για τη γνωστή υπόθεση της λίστας Λαγκάρντ. Το ειδικό δικαστήριο έκρινε πως ο πρώην υπουργός έκανε «λαθροχειρία», αφαιρώντας τα ονόματα τριών συγγενικών του προσώπων (εξαδέλφες), ωστόσο, το κακούργημα μετατράπηκε σε πλημμέλημα. Σύμφωνα με την απόφαση του δικαστηρίου με την πράξη της νόθευσης ο πρώην υπουργός είχε σκοπό να διαφυλάξει τη πολιτική του υπόσταση.

Η ποινή που του επιβλήθηκε είναι φυλάκιση ενός έτους με τριετή αναστολή. Επίσης, αποφασίστηκε να πληρώσει ο ίδιος τα έξοδα του δικαστηρίου, ωστόσο να του επιστραφεί η εγγύηση των 30.000.

Επίσης, το ειδικό δικαστήριο ομόφωνα αθώωσε τον κ. Παπακωνσταντίνου για το αδίκημα της απόπειρας απιστίας στην υπηρεσία. Την απόφαση, μετά από 13 μέρες ακροαματικής διαδικασίας, ανακοίνωσε σήμερα (Τρίτη) το απόγευμα ο πρόεδρος του Ειδικού Δικαστηρίου Νικόλαος Πάσσος.

Τρία μέλη τους δικαστηρίου είχαν την άποψη ότι ο κ. Παπακωνσταντίνου θα πρέπει να κηρυχθεί ένοχος για κακούργημα στην υπόθεση της νόθευσης εγγράφου, ενώ μία δεύτερη μειοψηφία -συμπεριλαμβανομένου και του προέδρου Ν. Πάσσου- είχε την άποψη να πρέπει να κηρυχθεί αθώος.

Η υπεράσπιση του κατηγορουμένου ζήτησε από το δικαστήριο να του αναγνωρίσει το ελαφρυντικό του πρότερου εντίμου βίου, κάτι που τελικά έκαναν δεκτό οι δικαστές, παρά την αντίθετη άποψη της εισαγγελέως, Ξένης Δημητρίου η οποία λαμβάνοντας τον λόγο τόνισε ότι ο κατηγορούμενος πρώην υπουργός, πρόσωπο με περγαμηνές και προσόντα -όπως είπε-, δεν δικαιούται το συγκεκριμένο ελαφρυντικό «γιατί είναι ευφυής και δεν θα έπρεπε να βάλει αυτή τη χώρα σε αυτή την περιπέτεια».

«Αυτή η δίκη δεν είναι δίκη του κ. Παπακωνσταντίνου, είναι μια δίκη για τον ελληνικό λαό, τον οποίο ευτέλισε και διέσυρε, και κόστισε πολλά εκατομμύρια. Ακριβώς γιατί έχει αυτά τα προσόντα, για αυτό δεν δικαιούται το ελαφρυντικό του προτέρου εντίμου βίου», ανέφερε η εισαγγελέας που πρότεινε να του επιβληθεί ποινή φυλάκισης 4 ετών.

Από την πλευρά τους οι συνήγοροι του πρώην υπουργού Οικονομικών πρότειναν να του επιβληθεί το ελάχιστο της ποινής.

«Το δικαστήριο υποχρεούται κατ' εκτίμηση να προσδιορίσει το ύψος της ζημιάς...»

Υπενθυμίζεται πως ορισμένους από τους ισχυρισμούς των τριών δικηγόρων του πρώην υπουργού Οικονομικών Γιώργου Παπακωνσταντίνου, αντέκρουσε η εισαγγελέας της έδρας Ξένη Δημητρίου, σε μια δευτερολογία της μετά την ολοκλήρωση των αγορεύσεων των συνηγόρων υπεράσπισης. Ανέφερε δε ότι το ύψος της ζημιάς που προκλήθηκε από τους τρεις λογαριασμούς των συγγενικών προσώπων του πρώην υπουργού πρέπει να προσδιοριστεί από το Ειδικό Δικαστήριο, και αυτό (το ύψος της ζημιάς) θα καθορίσει εάν οι κατηγορίες σε βάρος του κ. Παπακωνσταντίνου θα είναι σε βαθμό κακουργήματος ή πλημμελήματος.

[871] Κατωμέρης Κώστας (2015)

Η ζημιά πρέπει να είναι βέβαιη και οριστική, προσέθεσε η εισαγγελική λειτουργός και τόνισε ότι το δικαστήριο υποχρεούται κατ' εκτίμηση να προσδιορίσει το ύψος της ζημιάς, δηλαδή τα χρήματα που χάνει το ελληνικό Δημόσιο. Η κ. Δημητρίου υποστήριξε πως το γεγονός ότι η ΔΟΥ εξέδωσε προσωρινές πράξεις καταλογισμού δεν επηρεάζει την εξέλιξη και δεν παίζει κανένα ρόλο το ότι οι συγγενείς του κατηγορουμένου έχουν προσφύγει στα Διοικητικά Δικαστήρια, επικαλούμενη η κυρία Δημητρίου αποφάσεις του Αρείου Πάγου επ' αυτού του θέματος, που επιλύουν το ζήτημα υπέρ των θέσεων της.

Ο εκ των συνηγόρων υπεράσπισης, Τάκης Βασιλακόπουλος, είχε τονίσει ότι δεν μπορεί να επιβληθεί ποινή κάθειρξης με μόνη την προσωρινή βεβαίωση της ΔΟΥ για το ύψος της ζημιάς που προκλήθηκε στο Δημόσιο, ενώ επανέλαβε τις αιχμές κατά του πρώην επικεφαλής του ΣΔΟΕ. «Φταίει ο κατηγορούμενος που ο κ. Διώτης έσπασε το αρχικό στικάκι που του είχε δώσει;» αναρωτήθηκε συνήγορος υπεράσπισης προσθέτοντας πως «όλο ανακολουθίες είναι ο κ. Διώτης», και έκλεισε τονίζοντας και πάλι πως «κάποιος του την έστησε».

Για παραγραφή, λόγω διάλυσης της Βουλής, έκανε λόγο συνήγορος του Γ. Παπακωνσταντίνου»

Κατωμέρης Κώστας Συντάκτης: efsyn.gr

13. Άσκηση δίωξης για υπόθεση διαφθοράς (ξέπλυμα μαύρου χρήματος)

«Εισαγγελέας: Στο εδώλιο 64 για τα «μαύρα ταμεία» της Siemens»[872]

«Την προκαταρκτική εξέταση για την υπόθεση είχε διενεργήσει πριν από 8 χρόνια ο σημερινός εισαγγελέας Οικονομικού Εγκλήματος, Παναγιώτης Αθανασίου.

Στην πρότασή του 2.368 σελίδων προς το αρμόδιο δικαστικό συμβούλιο ο εισαγγελέας ζητά να παραπεμφθούν για τα αδικήματα της ενεργητικής και παθητικής δωροδοκίας με τις επιβαρυντικές διατάξεις του νόμου 1608/50 και για ξέπλυμα βρόμικου χρήματος (νομιμοποίηση εσόδων από εγκληματική δραστηριότητα), ενώ παράλληλα ο εισαγγελικός λειτουργός εκτιμά ότι οι «μίζες» αγγίζουν το ποσό των 69.942.000 ευρώ, όση και η ζημιά που υπολογίζεται ότι υπέστη το ελληνικό Δημόσιο.

Την προκαταρκτική εξέταση για την υπόθεση είχε διενεργήσει πριν από 8 χρόνια ο σημερινός εισαγγελέας Οικονομικού Εγκλήματος, Παναγιώτης Αθανασίου.

Ανάμεσα στους κατηγορούμενους που προτείνει ο εισαγγελέας να καθίσουν στο εδώλιο περιλαμβάνονται και 17 Γερμανοί υπήκοοι, ενώ επισημαίνεται ότι για τη διερεύνηση της υπόθεσης έπρεπε να ανοίξουν εκατοντάδες τραπεζικοί λογαριασμοί και να ερευνηθούν οι διαδρομές του μαύρου χρήματος.

Ειδικότερα ο Γαληνός Μπρης ζητά να παραπεμφθούν:

- 19 κατηγορούμενοι για ενεργητική δωροδοκία με την επιβαρυντική περίσταση του νόμου 1608/50 που επισύρει ποινική ισόβιας κάθειρξης και για ξέπλυμα βρόμικου χρήματος.
- 14 κατηγορούμενοι, πρώην στελέχη του ΟΤΕ για παθητική δωροδοκία, επίσης με τον νόμο περί καταχραστών και ξέπλυμα βρόμικου χρήματος.
- 8 κατηγορούμενοι υπάλληλοι εταιρίας συμβούλων για απλή συνέργεια σε παθητική δωροδοκία.
- 14 κατηγορούμενοι για άμεση συνέργεια σε παθητική δωροδοκία και ξέπλυμα βρόμικου χρήματος.
- 8 κατηγορούμενοι για άμεση συνέργεια σε ενεργητική δωροδοκία και ξέπλυμα βρόμικου χρήματος.
- Μία κατηγορούμενη για ξέπλυμα βρόμικου χρήματος.

Το συνολικό κόστος της επίμαχης σύμβασης υπολογίζεται σε 236 δισ. δραχμές και κατά την έρευνα διαπιστώθηκε ότι τα μεγάλα χρηματικά ποσά χρησιμοποιήθηκαν προκειμένου να δωροδοκηθούν κρατικοί αξιωματούχοι, με σκοπό να ανατεθεί η ψηφιοποίηση του ΟΤΕ στη SIEMENS (σύμβαση 8002), χωρίς να υπολογίζονται οι πραγματικές ανάγκες του Οργανισμού Τηλεπικοινωνιών Ελλάδος ή να προστατευτούν τα συμφέροντά του».

Συντάκτης: Μαρία Δήμα, 24.11.2014,

[872] Δήμα Μαρία (2015)

14. Απάτη με αναπάντητες κλήσεις-παγίδες σε κινητά τηλέφωνα

« Οι αριθμοί υψηλής χρέωσης που δεν πρέπει να απαντάμε» [873]

ΔΗΜΟΣΙΕΥΣΗ «το Βήμα»: 28/01/2014

«Ένα νέο κόλπο για να κερδίζουν χρήματα, φουσκώνοντας τους λογαριασμούς των χρηστών κινητής τηλεφωνίας στην Ελλάδα και τον υπόλοιπο κόσμο έχουν εφεύρει οι επιτήδειοι. Τους τελευταίους μήνες, μεγάλος αριθμός συνδρομητών κινητής τηλεφωνίας σχεδόν όλων των εταιρειών στην Ελλάδα έχει δεχθεί αναπάντητες κλήσεις ή κάποιο SMS από κάποιον άγνωστο αριθμό του εξωτερικού.

Σύμφωνα με τους εκπροσώπους των εταιρειών, τρεις είναι οι ομάδες αριθμών του εξωτερικού από τους οποίους έχουν δεχθεί αναπάντητες κλήσεις έλληνες συνδρομητές. Οι περισσότερες κλήσεις έχουν γίνει από τους αριθμούς +375602605281, +37127913091 και +3598920111, καθώς και από άλλους αριθμούς που αρχίζουν από +375 ή +371 ή +359. Το συνηθέστερο, όπως αναφέρουν Τα Νέα, είναι οι αναπάντητες κλήσεις να γίνονται τις νυχτερινές ώρες, όταν ο ανυποψίαστος χρήστης κοιμάται ή έχει το τηλέφωνό του κλειστό. Μόλις ο χρήστης δει στο κινητό του την αναπάντητη κλήση, η πρώτη του κίνηση είναι να καλέσει για να δει ποιος τον έχει ζητήσει. Έτσι πέφτει στην παγίδα, αφού οι αριθμοί αυτοί συνήθως είναι εξαιρετικά υψηλής χρέωσης και λίγα δευτερόλεπτα κλήσης αρκούν για να τον χρεώσουν από 10 έως 25 ευρώ.

Το +375 είναι ο διεθνής κωδικός της Λευκορωσίας, το +371 είναι ο κωδικός για τη Λετονία, ενώ το +359 είναι από τη γειτονική Βουλγαρία».

[873] http://www.tovima.gr/society/article/?aid=561594, ανακτήθηκε Μάρτιος 2015

15. Ειδικές συμβουλές από την Ελληνική Αστυνομία για αποφυγή εξαπάτησης πολιτών

Με αφορμή περιστατικά εξαπάτησης πολιτών, σε διάφορες περιοχές της χώρας, από επιτήδειους που προσεγγίζουν κυρίως άτομα τρίτης ηλικίας και με διάφορα προσχήματα και τεχνάσματα τους αποσπούν χρηματικά ποσά, η Ελληνική Αστυνομία συνιστά[874]:

- Να μην πείθεστε εύκολα από άτομα, τα οποία σας "πλησιάζουν" ως γνωστοί συγγενικών - φιλικών προσώπων.
- Να είστε ιδιαίτερα επιφυλακτικοί σε άγνωστα άτομα που επιχειρούν με διάφορα προσχήματα και τεχνάσματα να εισέλθουν στην οικία σας.
- Εφόσον άγνωστο άτομο εισέλθει στην οικία σας με οποιαδήποτε πρόφαση (π.χ. διεξαγωγή έρευνας, πώληση κάποιου προϊόντος, ανάγκη να πραγματοποιήσουν μια κλήση κ.λπ.), να μην επιτρέπετε να μεταβαίνει σε άλλους χώρους του σπιτιού σας, πέραν αυτών που χρειάζεται και ποτέ να μην χάνετε την οπτική επαφή μαζί του.
- Στην περίπτωση αυτή, να προσέχετε τα προσωπικά σας αντικείμενα, προκειμένου να αποφευχθεί το ενδεχόμενο αφαίρεσής τους με τη μέθοδο της απασχόλησης.
- Να είστε ιδιαίτερα επιφυλακτικοί όταν άγνωστοι προσπαθήσουν να σας πείσουν για την καταβολή χρηματικού ποσού, με το πρόσχημα επείγουσας ανάγκης συγγενικού - φιλικού προσώπου (π.χ. νοσηλεία σε νοσοκομείο). Το ίδιο μπορεί να προσπαθήσουν και τηλεφωνικά. Για τους ίδιους λόγους να μην ενδίδετε σε προτροπές για συνάντηση (ραντεβού κ.λπ.).
- Σε περιπτώσεις που άγνωστοι επικαλούνται έκτακτη ανάγκη γνωστού -συγγενικού σας προσώπου, να επιδιώκετε πάντα οι ίδιοι να επικοινωνείτε τηλεφωνικά με το γνωστό-συγγενικό σας πρόσωπο, προς επιβεβαίωση των όσων επικαλούνται. Η επικοινωνία να γίνεται με δικό σας τηλέφωνο και κατόπιν δικής σας πρωτοβουλίας και να μην δέχεστε να μιλάτε με άτομο, το οποίο κάλεσαν οι άγνωστοι.
- Σε κάθε περίπτωση, να δηλώνετε ότι δεν πρόκειται να παραδώσετε χρήματα, εάν δεν εμφανιστούν οι γνωστοί-συγγενείς σας.
- Να μην δέχεστε σε καμία περίπτωση άγνωστα άτομα να σας οδηγήσουν σε Πιστωτικό Κατάστημα ή ΑΤΜ για ανάληψη χρηματικού ποσού.
- Να μην πείθεσθε εύκολα σε ευκαιριακές αγορές προϊόντων που σας προτείνουν άγνωστα άτομα, ιδιαίτερα δε δίχως να δείτε πρώτα τα προϊόντα αυτά.
- Να μην πείθεστε από άγνωστους, οι οποίοι εμφανίζονται ως υπάλληλοι Δημόσιας Υπηρεσίας ή άλλου φορέα για την επιδιόρθωση κάποιου τεχνικού προβλήματος, εάν δεν τους έχετε εσείς προηγουμένως καλέσει.
- Να μην πείθεστε όταν άγνωστοι σας ζητούν να καταβάλλετε χρήματα για οφειλές γνωστών ή συγγενικών προσώπων σε δημόσιες υπηρεσίες ή σε καταστήματα-εταιρείες για αγορά αγαθών-προσφορά υπηρεσιών.
- Επισημαίνεται ότι από νοσοκομεία ή από δημόσιες υπηρεσίες δεν χρησιμοποιείται η πρακτική υπάλληλοί τους να μεταβαίνουν σε οικίες ή σε δημόσιους χώρους και να ζητούν από πολίτες την καταβολή χρημάτων για υπηρεσίες που παρέχουν.
- Να έχετε πάντα διαθέσιμους τους τηλεφωνικούς αριθμούς, με τους οποίους πρέπει να επικοινωνήσετε σε περίπτωση ανάγκης (Αστυνομία, Πυροσβεστική, Νοσοκομεία, στενοί συγγενείς κ.α.).
- Προσπαθήστε να συγκρατήσετε τα χαρακτηριστικά των δραστών, καθώς και τα οχήματα με τα οποία κινούνται (αριθμό κυκλοφορίας, μάρκα οχήματος, χρώμα κ.λπ.), για να βοηθήσετε το έργο των διωκτικών αρχών.

874

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=9876&Itemid=619&lang, ανακτήθηκε Νοέμβρ. 2014

- Να ενημερώνετε πάντα τις αστυνομικές Αρχές, ακόμη και σε περίπτωση απόπειρας απάτης σε βάρος σας.

Οι δράστες χρησιμοποιούν συνήθως την εξής **μεθοδολογία** :

- **Απάτη με τη μέθοδο προσέγγισης εκ μέρους συγγενικού προσώπου** (κυρίως σε βάρος ηλικιωμένων ατόμων)

Οι δράστες επιλέγουν κυρίως ηλικιωμένους ανθρώπους, για τους οποίους πληροφορούνται με οποιανδήποτε τρόπο τα στοιχεία ταυτότητας τόσο των ιδίων, όσο και προσφιλών συγγενικών τους προσώπων, συνήθως των παιδιών ή των εγγονιών τους.

Τους προσεγγίζουν «δήθεν» ως απεσταλμένοι των συγγενών τους και με το πρόσχημα άμεσης και επείγουσας ανάγκης χρημάτων, επιδιώκουν να τους αποσπάσουν μεγάλα χρηματικά ποσά. Η προσέγγιση συνήθως γίνεται κατά την έξοδο ή λίγο πριν την είσοδο στην κατοικία τους, έξω από Τράπεζες ή εμπορικά καταστήματα κ.λπ.

Οι τεχνικές, που χρησιμοποιούν οι δράστες για να πείσουν τους ηλικιωμένους να τους δώσουν τα χρήματα για λογαριασμό των οικείων τους, είναι ο αιφνιδιασμός και η παρουσίαση μιας αληθοφανούς οικονομικής ανάγκης που πρέπει να ικανοποιηθεί χωρίς αναβολή. Με τον τρόπο αυτό, αλλά και με την αναφορά σε συγγενικά πρόσωπα με ιδιαίτερη οικειότητα, επιδιώκουν να κερδίσουν την εμπιστοσύνη και να μην αφήσουν περιθώρια δεύτερης σκέψης. Σε αρκετές περιπτώσεις, οι δράστες για να ισχυροποιήσουν τα επιχειρήματά τους, προσποιούνται πως τηλεφωνούν στα οικεία πρόσωπα για να επιβεβαιώσουν την οικονομική ανάγκη, πλην όμως οι ηλικιωμένοι μέσα στην αναστάτωση τους δεν αντιλαμβάνονται ότι συνομιλούν με συνεργούς των δραστών και όχι με τους συγγενείς τους.

Οι λόγοι που επικαλούνται οι δράστες για να αποσπάσουν χρήματα είναι συνήθως η εξόφληση ενός χρέους, η πληρωμή ασφαλιστηρίων συμβολαίων, η αγορά ηλεκτρικών συσκευών, ανταλλακτικών αυτοκινήτων κ.λπ., για λογαριασμό «δήθεν» συγγενικών προσώπων.

Τα χρηματικά ποσά, που ζητούν οι δράστες κυμαίνονται από μερικές εκατοντάδες έως αρκετές χιλιάδες Ευρώ, ποσά τα οποία μεταβάλλονται και προσαρμόζονται ανάλογα με τη δεκτικότητα και ευπιστία των ηλικιωμένων. Ενδεικτικά αναφέρεται πως στο παρελθόν δράστες έχουν μεταφέρει με αυτοκίνητο ηλικιωμένους ακόμα και σε Τράπεζες, προκειμένου να αναλάβουν μεγάλα χρηματικά ποσά και να τους τα παραδώσουν.

- **Απάτη με τη μέθοδο νοσηλείας συγγενικού προσώπου**

Οι δράστες επιλέγουν συνήθως ηλικιωμένους και πληροφορούνται με οποιανδήποτε τρόπο τα στοιχεία ταυτότητας τόσο των ιδίων, όσο και προσφιλών συγγενικών τους προσώπων, συνήθως των παιδιών τους.

Ακολούθως, επικοινωνούν τηλεφωνικώς μαζί τους κυρίως τις νυχτερινές ώρες (συνήθως μετά τα μεσάνυχτα) και εκμεταλλευόμενοι την αναστάτωση που προκαλείται, τους αναγγέλλουν ότι ένας στενός συγγενής τους (π.χ. γιος, κόρη, γαμπρός ή νύφη) εισήχθη εσπευσμένα σε κάποιο νοσοκομείο, λόγω τροχαίου ατυχήματος ή κάποιου άλλου εκτάκτου λόγου και απαιτούν χρήματα για να γίνει άμεσα κάποια ιατρική πράξη, συνήθως χειρουργική επέμβαση.

Οι δράστες ζητούν από τους ηλικιωμένους να μεταβούν αμέσως σε συγκεκριμένο σημείο (που νωρίτερα οι ίδιοι έχουν επιλέξει ως κατάλληλο, συνήθως κοντά στο σπίτι τους), όπου τους «αναμένει» άνθρωπος του νοσοκομείου π.χ. ένας νοσηλευτής ή υπάλληλος του ΕΚΑΒ, για να παραλάβει τα χρήματα και να τα παραδώσει το ταχύτερο δυνατό στους γιατρούς.

Οι ηλικιωμένοι χρησιμοποιούν συνήθως την ίδια τηλεφωνική συσκευή στην οποία δέχθηκαν την κλήση για να καλέσουν στο κινητό τηλέφωνο το συγγενικό τους πρόσωπο, που «δήθεν» νοσηλεύεται σε κρίσιμη κατάσταση. Όμως, μέσα στη σύγχυση τους δεν αντιλαμβάνονται ότι η «γραμμή» είναι ακόμη ανοιχτή με τους δράστες, οι οποίοι δεν τερμάτισαν την προηγούμενη κλήση. Οι δράστες προσποιούνται ότι απαντούν στην κλήση

των θυμάτων και «επιβεβαιώνουν» την άσχημη είδηση, παριστάνοντας για παράδειγμα κάποιον τραυματιοφορέα που κρατάει το κινητό του νοσηλευόμενου.

- **Απάτη με τη μέθοδο πώλησης κατασχεμένων από την Τράπεζα ακινήτων ή οχημάτων σε συμφέρουσα τιμή**

Οι δράστες εμφανίζονται συνήθως ως δικηγόροι Τραπεζών, οι οποίες προτίθενται να προχωρήσουν σε πλειστηριασμό κατασχεμένων ακινήτων και αυτοκινήτων. Με τη χρήση πλαστών εγγράφων και συνήθως με το πρόσχημα ότι οι ίδιοι ελέγχουν τη διενέργεια των πλειστηριασμών, πείθουν ότι μπορούν να μεσολαβήσουν στην κατακύρωση του πλειστηριαζόμενου αντικειμένου σε πολύ χαμηλή τιμή και αποσπούν έτσι μεγάλα χρηματικά ποσά.

Έχει παρατηρηθεί ότι μέλη αυτών των εγκληματικών ομάδων για να γίνονται περισσότερο πιστευτοί μισθώνουν πολυτελή διαμερίσματα και ακριβά αυτοκίνητα, προκειμένου να τα παρουσιάζουν ως προοριζόμενα για εκποίηση από τις Τράπεζες.

Είναι χαρακτηριστικό το γεγονός ότι οι δράστες «αλιεύουν» υποψήφιους συναλλασσόμενους, ακόμα και μέσα από τον κύκλο γνωριμιών άλλων ατόμων που έχουν εξαπατήσει, πριν αυτά αντιληφθούν την απάτη.

- **Απάτη με τη μέθοδο της απασχόλησης σε ΑΤΜ** (συνήθως σε βάρος ηλικιωμένων ατόμων)

Οι δράστες προσεγγίζουν ένα άτομο τη στιγμή που πραγματοποιεί συναλλαγή σε ΑΤΜ και χωρίς να γίνουν αντιληπτοί υποκλέπτουν οπτικά το «PIN» κατά την πληκτρολόγησή του, ενώ στη συνέχεια περιμένουν να ολοκληρωθεί η συναλλαγή.

Τη στιγμή της εξόδου της κάρτας από το ΑΤΜ ένας από τους δράστες ρίχνει στα πόδια του συναλλασσόμενου ένα χαρτονόμισμα και τον προτρέπει να το πάρει με το πρόσχημα ότι του έπεσε από τη τσέπη.

Οι δράστες εκμεταλλεύονται το χρονικό διάστημα που ο συναλλασσόμενος απασχολείται με το πεσμένο χαρτονόμισμα και αφαιρούν την κάρτα του από το στόμιο εξόδου του ΑΤΜ, τοποθετώντας στη θέση της μία άλλη.

Μετά την αποχώρηση του συναλλασσόμενου, που δεν έχει αντιληφθεί τη αλλαγή της κάρτας, οι δράστες αφαιρούν το υπόλοιπο του λογαριασμού».

16. Εθνικό Black Out στην Τουρκία
Ατύχημα, σαμποτάζ ή κυβερνοεπίθεση;

Δημοσίευση http://www.viadiplomacy.gr, στις 31 Μαρτίου 2015 [875]

«Την απόλυτη εξάρτηση των σύγχρονων βιομηχανικών κοινωνιών και την τρωτότητα αυτών σε ατυχήματα ή ακόμη και υπονομευτικές δράσεις επιβεβαιώνει το σημερινό εθνικό Black Out που συνέβη στην Τουρκία. Συνολικά 24 μεγάλες πόλεις της χώρας αντιμετώπισαν πλήρη διακοπή του ηλεκτρικού ρεύματος από τις πρωινές ώρες μέχρι και το μεσημέρι.

Πιο συγκεκριμένα οι διακοπές συνέβησαν στην Κωνσταντινούπολη, στο Τσανάκαλε, στη Σμύρνη, στο Αιδίνι, στη Μούγλα στο Ντενιζλί, στην τουριστική Αττάλεια, στα Άδανα, στο Γκαζιαντέπ, στη Σανλιούρφα, στο Μαρντίν, στο Ντιαρμπεκίρ, στο Σίιρτ, στη Μούς, στο Ερζερούμ, στο Ιγκντίρ, στη Σαμψούντα, στο Μπαρντίν, στο Ζογκουλάκ, στο Κοτσάελι, στην Άγκυρα, στο Μπολού, στο Εσκισεχίρ και στην Προύσα, ενώ συνολικά 44 επαρχίες της Τουρκίας έχουν μείνει χωρίς ηλεκτρισμό.

Σύμφωνα με τα τουρκικά ΜΜΕ το εθνικό Black Out ξεκίνησε στις 07.40 το πρωί και εξαπλώθηκε σε ολόκληρη τη χώρα, κυρίως όμως στις περιφερειακές περιοχές της χώρας δηλ. στις επαρχίες που βρίσκονται στην Μαύρη θάλασσα, στο Αιγαίο και στην νοτιοανατολικές επαρχίες όπου κατοικεί η πλειονότητα του Κουρδικού πληθυσμού. Επιπλέον Black Out αντιμετώπισε η καρδιά της βιομηχανικής περιοχής της Τουρκίας το Ιζμίτ και το Κοτσάελι καθώς και η πρωτεύουσα Άγκυρα.

Η εξάπλωση του προβλήματος προκαλεί πολλά ερωτηματικά διότι γεωγραφικά οι περιοχές αυτές δεν βρίσκονται σε μικρή απόσταση η μια από την άλλη, ενώ ειδικά για την νοτιοανατολικές περιοχές το ζήτημα γίνεται πιο περίπλοκο αφού στην ευρύτερη περιοχή λειτουργούν πολλά υδροηλεκτρικά εργοστάσια στους ποταμούς Τίργη και Ευφράτη που τροφοδοτούν με ηλεκτρικό ολόκληρη τη χώρα.

Οι αρχικές εκτιμήσεις ανέφεραν ότι πρόκειται για ένα ατύχημα που συνέβη στο σύστημα της εταιρείας «Turkish Electricity Conduction Company» (TEİAŞ), ενώ δεν έχουν επιβεβαιωθεί οι πληροφορίες για έκρηξη σε εργοστάσιο ηλεκτροπαραγωγής στην περιοχή Κοτσαέλι.

Όπως αναφέρει ανακοίνωση του υπουργείου Ενέργειας της Τουρκίας το πρόβλημα εντοπίζεται στην κεντρική μονάδα διανομής ηλεκτρικής ενέργειας και πιθανότατα προέρχεται από την περιοχή του Αιγαίου.

875 http://www.viadiplomacy.gr/ethniko-black-out-stin-tourkia-atichima-sampotaz-i-kivernoepithesi/, ανακτήθηκε Απρίλιο 2015

Αποτέλεσμα του Black Out ήταν η διακοπή της λειτουργίας του Τραμ, του Μετρό στην Κωνσταντινούπολη, του υποθαλάσσιου τούνελ Marmaray που συνδέει σιδηροδρομικά τις ανατολικές με τις δυτικές ακτές του Βοσπόρου, ενώ προβλήματα υπάρχουν και στις πτήσεις πάνω από την Τουρκία καθώς όσα αεροπλάνα βρίσκονται στην φάση της προσγείωσης στα τουρκικά αεροδρόμια κάνουν κύκλους καθώς δεν μπορούν να προσγειωθούν.

Συνολικά 11 από τους 16 δέκτες επικοινωνιών εναέριας κυκλοφορίας του εθνικού δικτύου δεν λειτουργούν με αποτέλεσμα να μην μπορούν τα αεροσκάφη να προσεγγίσουν τα αεροδρόμια.

Επιπλέον το σύνολο των εργοστασίων στις βιομηχανικές περιοχές του Κοτσάελι και του Ιζμίτ διέκοψαν τις εργασίες τους, ενώ σοβαρά προβλήματα προκλήθηκαν και στις βιομηχανικές περιοχές των υπολοίπων επαρχιών όπου η παροχή διεκόπη. Σύμφωνα με το υπουργείο έχει ήδη ξεκινήσει η αποκατάσταση της βλάβης, ενώ σταδιακά η παροχή ηλεκτρισμού αρχίζει να αποκαθίσταται σε ορισμένες περιφέρειες της Άγκυρας.

Πάντως ο Τούρκος πρωθυπουργός Αχμέτ Νταβούτογλου δήλωσε νωρίτερα σήμερα το πρωί ότι ερευνώνται όλα τα ενδεχόμενα της τρομοκρατικής ενέργειας ή ακόμη και της κυβερνοεπίθεσης.

Το συγκεκριμένο περιστατικό φέρνει στην επιφάνεια το μεγάλο ζήτημα της τρωτότητας των σύγχρονων κοινωνιών σε περιστατικά σαν και αυτά. Κυκλοφοριακό χάος, διακοπή της λειτουργίας των εργοστασίων, σοβαρά προβλήματα ασφάλειας στην αεροπλοΐα, οικονομική ζημιά σε επιχειρήσεις και καταστήματα, πλήρη αδρανοποίηση του μηχανισμού ασφαλείας του κράτους κλπ. αποτελούν μερικά μόνο από τα αποτελέσματα μιας εθνικής διακοπής παροχής ηλεκτρισμού.

Η ψηφιοποίηση και διασύνδεση των ζωτικών υποδομών μιας κοινωνίας που ακολουθεί τα δυτικά πρότυπα λειτουργίας, μπορεί να προσφέρει σημαντικές διευκολύνσεις στην λειτουργία ενός κράτους και μίας οργανωμένης κοινωνίας όμως εμπεριέχει πολλές αδυναμίες μερικές από τις οποίες αντιμετώπισαν σήμερα οι Τούρκοι.

Η απουσία εναλλακτικών αναλογικών, χαμηλής τεχνολογικής εξάρτησης συστημάτων για την διατήρηση της λειτουργίας των βασικών υποδομών ενός κράτους όπως το σύστημα Εναέριας Κυκλοφορίας, η παροχή νερού, η λειτουργία της Αστυνομίας, της Πυροσβεστικής, των Νοσοκομείων, των Κέντρο Συντονισμού των Δημοσίων Υπηρεσιών Κοινής Ωφέλειας, των τηλεπικοινωνιών κλπ αποτελεί τεράστιο λάθος σε μια εποχή που οι απειλές έχουν λάβει πλέον πολλές και διαφορετικές μορφές.

Και αν όλα αυτά που συνέβησαν στην Τουρκία έλαβαν χώρα εν καιρώ ειρήνης, διερωτάται κανείς ποιες θα ήταν οι επιπτώσεις από ένα νέο εθνικό Black Out σε περίπτωση που η χώρα βρισκόταν σε κρίση με γείτονες της ή υπάρχει υψηλό ενδεχόμενο εξαπόλυσης τρομοκρατικών επιθέσεων.

Στο σημείο αυτό αξίζει να σημειωθεί ότι το τουρκικό κράτος είναι καλύτερα προετοιμασμένο από κάθε άλλη γειτονική χώρα της περιοχής για περιστατικά σαν και αυτά, αφού για τρείς δεκαετίες βρίσκεται σε εμπόλεμη κατάσταση με το PKK η δράση του οποίου δεν περιορίζεται μόνο στις ανατολικές επαρχίες της χώρας.

Επιπλέον ο τομέας ασφάλειας και προστασίας κρίσιμων υποδομών αποτελεί ένα από τα θεμέλια του τουρκικού συστήματος εσωτερικής ασφαλείας και έχουν δαπανηθεί τεράστια ποσά για την αναβάθμιση και σωστή λειτουργία των υποδομών.

Επομένως το σόκ που υπέστη σήμερα η τουρκική κοινωνία δεν θα πρέπει να μας ξενίζει αφού το μέγεθος και η έκταση του Black Out είναι πρωτόγνωρο και ανάλογο έχει να συμβεί από την εποχή που η χώρα αντιμετώπιζε την οικονομική της κατάρρευση το 1999-2000.

Εάν δε τελικά το σημερινό περιστατικό αποτελεί προϊόν κυβερνοεπίθεσης τότε δημιουργούνται πολλά ερωτηματικά διότι η Τουρκία διαθέτει μία από τις μεγαλύτερες σε μέγεθος και καλύτερα εξοπλισμένη διοίκηση για κυβερνοεπιθέσεις και κυβερνοάμυνα στην περιοχή με χιλιάδες αναλυτές.

Ο τομέας του κυβερνοπολέμου αποτελεί αντικείμενο της κρατικής υπηρεσίας πληροφορικής και επικοινωνιών ICTA (Information and Communication Technologies

Authority), του τουρκικού ΓΕΕΘΑ της κρατικής εταιρείας τηλεπικοινωνιακού υλικού Aselsan, της κρατικής εταιρείας στρατιωτικού λογισμικού Havelsan και του κρατικού ερευνητικού ιδρύματος TUBITAK.

Μάλιστα πριν από ένα χρόνο το τουρκικό κράτος έθεσε σε υπηρεσία την Διοίκηση Κυβερνοπολέμου (Cyber Warfare Command), μέσα στις εγκαταστάσεις του τουρκικού ΓΕΕΘΑ, ενώ παράλληλα με την νέα Διοίκηση πρόσφατα ιδρύθηκε το Κέντρο Αντιμετώπισης σε Κυβερνο-απειλών (Center for Response to National Cyber Threats).

Όπως ανέφεραν Ισραηλινά ΜΜΕ πέρσι, η Τουρκία δεν έχει περιοριστεί μόνο στην ανάπτυξη των κρυπτοσυστημάτων και του σχετικού λογισμικού για την κάλυψη των Εθνικών αναγκών, αλλά έχει ξεκινήσει και εξαγωγή της τεχνογνωσίας στην Χαμάς, γεγονός που έχει ενοχλήσει σφόδρα τους Ισραηλινούς.

Επομένως εάν το σημερινό Black Out δεν οφείλετο σε έκρηξη σε σταθμό παραγωγής ρεύματος ή σε κάποια βλάβη στο σύστημα διαμονής το οποίο διέκοψε την τροφοδοσία σε επαρχίες που βρίσκονται στις βόρειες δυτικά και νότιες ακτές της Τουρκίας και στα ανατολικά της σύνορα, αλλά σε κυβερνοεπίθεση τότε δημιουργούνται πολλά ερωτηματικά για τον υπαίτιο της σημερινής κατάστασης στην Τουρκία, αλλά και για τις δυνατότητες του τουρκικού κράτους να αμυνθεί στις νέες απειλές παρα τις επενδύσεις του σε αυτό τον τομέα».

17. Θύμα απάτης επιχείρηση στην Κρήτη

« Έχασε 450.000 ευρώ σε μία μέρα» [876]

«Ακόμη ένα πρωτοφανές χτύπημα από χάκερ καλείται να αντιμετωπίσει η Δίωξη Ηλεκτρονικού Εγκλήματος, σε συνεργασία με το FBI και την Europol. Τη στιγμή που η επίθεση σε Έλληνες χρήστες iPhone βρίσκεται σε εξέλιξη από τη Μεγάλη Πέμπτη, οι επιτήδειοι άρχισαν να χακάρουν και ελληνικές εταιρείες (μικρές και μεγάλες).

Στην υπηρεσία κατά του ηλεκτρονικού εγκλήματος έχει σημάνει συναγερμός, ενώ το τηλεφωνικό κέντρο της έχει πάρει φωτιά. Έλληνες επιχειρηματίες διαπιστώνουν ότι έχουν υποστεί οικονομική ζημιά, αφού χάκερ καταφέρνουν να διεισδύουν στην εσωτερική τους αλληλογραφία και να τους αποσπούν μεγάλα χρηματικά ποσά.

Αποκτούν τα ψηφιακά δεδομένα της εταιρείας με ένα email

Όπως εξηγούν αξιωματικοί οι οποίοι συμμετέχουν στην επιχείρηση εντοπισμού των ηλεκτρονικών ιχνών των δραστών, χρειάζεται πολλή προσοχή και εξονυχιστικός έλεγχος στα εισερχόμενα email των λογιστηρίων.

Αποκτούν τον έλεγχο των ψηφιακών δεδομένων μιας εταιρείας και αποσπούν χρηματικά ποσά «Αυτοί οι χάκερ εντοπίζουν μικρές και μεγάλες εταιρείες στην Ελλάδα, και στέλνουν αρχικά ένα ενημερωτικό email σε αυτές, προσποιούμενοι τους πελάτες προμηθευτές ή νέους πελάτες. Στη συνέχεια το στέλεχος της εταιρείας ανοίγει το email και τότε σκάει η βόμβα διείσδυσης (electronic bomb). Αυτό έχει ως αποτέλεσμα να εξαπλωθεί άμεσα σε όλο το δίκτυο της εταιρείας-θύμα ένας ιός, με συνέπεια ο χάκερ να μπορεί πια να ελέγχει όλα τα ηλεκτρονικά της αρχεία. Ουσιαστικά ελέγχει όλο το δίκτυό της σαν να είναι δικό του» επισημαίνουν ειδικοί της Δίωξης στην ηλεκτρονική μας εφημερίδα.

Ένας άλλος τρόπος με τον οποίο χτυπούν τα ηλεκτρονικά αρχεία των εταιρειών και αποσπούν χρήματα είναι η αποστολή ενός email με τα λογότυπα της εταιρείας-θύμα σε μια συνεργαζόμενη επιχείρηση. Στο συγκεκριμένο ηλεκτρονικό ταχυδρομείο γράφουν πως η εταιρεία (το θύμα) αλλάζει τον λογαριασμό της και δίνουν τον λογαριασμό που έχουν φτιάξει αυτοί.

Στέλνουν τα χρήματα σε τράπεζες του εξωτερικού

Αφού λοιπόν οι χάκερ αποκτήσουν τον έλεγχο του λογιστηρίου, αλλάζουν άμεσα ένα ψηφίο στον αριθμό λογαριασμού που η μητρική εταιρεία πληρώνει τους προμηθευτές της. Αυτό έχει ως αποτέλεσμα τα χρήματα να στέλνονται σε άλλους τραπεζικούς λογαριασμούς του εξωτερικού, δίχως ο λογιστής ή ο ιδιοκτήτης να αντιληφθούν τίποτα.

Εισπράττουν τα ποσά χρησιμοποιώντας πολίτες «μουλάρια» (mules).

Χρησιμοποιούν άνεργους πολίτες για να εισπράττουν τα χρήματα. Εξαιρετικό ενδιαφέρον έχει ο τρόπος με τον οποίο οι δράστες καταφέρνουν να εισπράξουν τα χρήματα, αφού -όπως εξηγούν αξιωματικοί της ΕΛ.ΑΣ.- χρησιμοποιούν άνεργους πολίτες από την Ελλάδα και το εξωτερικό.

«Βάζουν αγγελίες στο διαδίκτυο, όπου ζητούν συνεργάτες στην Ευρώπη για να ανοίξουν τραπεζικό λογαριασμό στο όνομά τους. Στη συνέχεια τους λένε πως θα βάζουν εκεί κάποια χρήματα και ο συνεργάτης θα παίρνει ένα ποσοστό αυτών. Συνήθως είναι το 10% του ποσού. Αυτοί οι συνεργάτες λέγονται “μουλάρια” (mules), διότι δεν γνωρίζουν ότι αποτελούν μέλη εγκληματικής οργάνωσης. Απλώς εκμεταλλεύονται τη δυστυχία τους. Στην Ελλάδα έχουμε πολλές περιπτώσεις. Είχαν βγάλει ένα σωρό χρήματα με αυτόν τον τρόπο χωρίς να γνωρίζουν ότι τα ποσά ήταν κλεμμένα» διευκρινίζουν οι Αρχές.

[876] Δημοσίευση στο http://www.ekriti.gr/, ανακτήθηκε Απρίλιο 2015

Επιχείρηση στην Κρήτη έχασε σε μία ημέρα 450.000 ευρώ FBI, Europol και Δίωξη Ηλεκτρονικού Εγκλήματος έχουν στήσει γιγαντιαία επιχείρηση, προκειμένου να μπορέσουν να εντοπίσουν άμεσα τα ηλεκτρονικά ίχνη των δραστών, πριν προκαλέσουν μεγαλύτερες οικονομικές ζημιές σε εταιρείες στη χώρα μας.

Ενδεικτικό της κατάστασης είναι το γεγονός ότι μια γνωστή εταιρεία που εδρεύει στην Κρήτη έχασε μέσα σε μία ημέρα 450.000 ευρώ. Υπολογίζεται ότι η ζημιά στη χώρα μας μέχρι στιγμής αγγίζει τα 7 εκατ. ευρώ.

«Μέχρι στιγμής οι έρευνες εστιάζονται σε χώρες της πρώην Σοβιετικής Ένωσης, διότι από εκεί φέρονται να δρουν οι συγκεκριμένοι χάκερ, παρόλο που τα κλεμμένα χρήματα τα μεταφέρουν σε τράπεζες ευρωπαϊκών χωρών» προσθέτει ανώτατος αξιωματικός που συμμετέχει στην επιχείρηση.

Άμεσοι τρόποι προστασίας

Σύμφωνα με τη Δίωξη Ηλεκτρονικού Εγκλήματος, οι εμπορικές εταιρείες, προκειμένου να διασφαλίσουν τα ψηφιακά δεδομένα τους, αλλά και να προστατεύσουν τις τραπεζικές συναλλαγές τους, καλούνται να εντείνουν την προσοχή τους στις διαδικασίες πληρωμών που γίνονται μέσω των τραπεζικών ιδρυμάτων και να τηρούν τις ακόλουθες διαδικασίες:

- να επαληθεύουν συνεχώς την ορθή διεύθυνση ηλεκτρονικού ταχυδρομείου των εταιρειών - επιχειρήσεων με τις οποίες πραγματοποιείται η επικοινωνία για επερχόμενες συναλλαγές
- σε περίπτωση που απαιτείται αποστολή χρημάτων με οποιονδήποτε τρόπο, θα πρέπει να πραγματοποιούν επαλήθευση των στοιχείων αποστολής και με άλλον τρόπο, πλην του ηλεκτρονικού ταχυδρομείου (τηλέφωνο, διαδικτυακή συνομιλία κ.τ.λ.)
- να επαληθεύουν τις συναλλαγές απευθείας με τους τραπεζικούς οργανισμούς στους οποίους πρόκειται να γίνει η μεταφορά των χρημάτων.
- να τηρούν δεύτερο ή επιπρόσθετο κωδικό ασφαλείας κατά τη διαχείριση των λογαριασμών ηλεκτρονικών ταχυδρομείων που λαμβάνουν-αποστέλλουν ευαίσθητα ή τραπεζικά δεδομένα.
- να ενημερώνουν συνεχώς τα προγράμματα προστασίας και ασφάλειας των πληροφοριακών συστημάτων
- οι αρμόδιοι υπάλληλοι να είναι ιδιαίτερα προσεκτικοί στις διαδικασίες πληρωμών μέσω των τραπεζικών ιδρυμάτων.»

18. Ευάλωτα σε αεροπειρατείες από χάκερ μέσω Wi-Fi τα σύγχρονα αεροπλάνα

«Λίγο καιρό μετά την τραγωδία του μοιραίου αεροσκάφους της Germanwings στις Άλπεις, το ζήτημα της ασφαλείας πτήσεων επανεξετάζεται λεπτομερώς, με πολλούς να επισημαίνουν την ανάγκη για αυξημένες ψυχολογικές εξετάσεις στα πληρώματα, ενώ ποτέ δεν «ξεχνιέται» η απειλή της τρομοκρατικής ενέργειας. Ωστόσο, όπως φαίνεται, τα μοντέρνα αεροπλάνα αντιμετωπίζουν μια νέα απειλή: αυτή της αεροπειρατείας από χάκερ.

Όπως αναφέρεται σε σχετικό δημοσίευμα του Wired, σύμφωνα με αναφορά του US Government Accountability Office, εξακολουθεί να τίθεται το ζήτημα της τρωτότητας των σύγχρονων αεροσκαφών σε hacking, επτά χρόνια μετά την πρώτη προειδοποίηση της Federal Aviation Administration προς την Boeing για το Dreamliner, το οποίο, όπως είχε αναφερθεί είχε πρόβλημα στο Wi-Fi που το καθιστούσε ευάλωτο σε χάκερ.

Τόσο το 787 Dreamliner όσο και τα Airbus A350 και A380 έχουν δίκτυα Wi-Fi για επιβάτες πυο χρησιμοποιούν το ίδιο δίκτυο όπως τα συστήματα avionics των αεροσκαφών, κάτι που αυξάνει την πιθανότητα ένας χάκερ να πάρει τον έλεγχο του συστήματος πλοήγησης, ή ακόμα και του αεροσκάφους συνολικά, μέσω του δικτύου του αεροσκάφους.

Ένας τέτοιος χάκερ-αεροπειρατής θα έπρεπε να παρακάμψει το firewall που διαχωρίζει το σύστημα Wi-Fi από το σύστημα avionics, ωστόσο τα firewalls δεν είναι απόρθητα. Ειδικοί του χώρου της ασφαλείας επισημαίνουν εδώ και χρόνια ότι ο μόνος σίγουρος τρόπος προστασίας είναι η φυσική απομόνωση/ διαχωρισμός των δύο συστημάτων (μέσω «κενού αέρος»- air gap, όπως αποκαλείται αυτού του είδους ο διαχωρισμός) έτσι ώστε ο εισβολέας να μην μπορεί να περάσει από το ένα στο άλλο, είτε βρίσκεται αλλού είτε είναι στο ίδιο το αεροπλάνο.

Το πρόβλημα, σύμφωνα με την αναφορά, έγκειται στο ότι τα Wi-Fi συστήματα στα αεροπλάνα συνδέονται με τον «έξω κόσμο», οπότε και ανοίγει ο δρόμος για κακόβουλη δραστηριότητα εξ αποστάσεως. «Ένας ιός ή malware (κακόβουλο λογισμικό) που έχει τοποθετηθεί σε ιστοσελίδες που επισκέπτονται οι επιβάτες θα μπορούσε να παρέχει την ευκαιρία σε έναν κακόβουλο εισβολέα να αποκτήσει πρόσβαση στα συστήματα των αεροσκαφών μέσω των μολυσμένων συσκευών». [877]

Δημοσιεύθηκε: 16/04/2015

[877] Μαυραγάνης Κώστας (2015)

19. Σύλληψη δημιουργών κακόβουλου λογισμικού

Δηλώσεις από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για τη σύλληψη δύο ημεδαπών - δημιουργών του κακόβουλου λογισμικού με την κωδική ονομασία "Lecpetex" που μόλυνε παγκοσμίως εκατοντάδες χιλιάδες ηλεκτρονικούς υπολογιστές.[878]

Δηλώσεις Εκπροσώπου Τύπου:

«Καλημέρα σας,

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στο πλαίσιο πολύμηνης συστηματικής και εμπεριστατωμένης έρευνας, κατάφερε να εξιχνιάσει την παράνομη διαδικτυακή δράση, δύο (2) ημεδαπών, οι οποίοι δημιούργησαν και χρησιμοποίησαν με άνομους σκοπούς (Cracking), το παγκοσμίως διαδεδομένο κακόβουλο λογισμικό με την κωδική ονομασία "Lecpetex".

Πρόκειται για δύο ημεδαπούς, ηλικίας 31 και 27 ετών, οι οποίοι συνελήφθησαν με την αυτόφωρη διαδικασία, χθες (2-7-2014) το πρωί, σε περιοχές της Αττικής. Σε βάρος τους σχηματίστηκε δικογραφία, για σύσταση και συμμετοχή σε εγκληματική οργάνωση-συμμορία, απάτη με υπολογιστή, παραβίαση απορρήτου υπολογιστών, καθώς και παράβαση της νομοθεσίας για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ειδικότερα, η διερεύνηση της υπόθεσης ξεκίνησε μετά από κατάλληλη αξιοποίηση διαδικτυακών αναρτήσεων και πληροφοριών σχετικά με τη δραστηριότητα Ελλήνων hackers στο διαδίκτυο, οι οποίοι τους τελευταίους μήνες, με την χρήση κακόβουλου λογισμικού, είχαν παραβιάσει μεγάλο αριθμό υπολογιστικών συστημάτων, κυρίως μέσω ιστοσελίδας κοινωνικής δικτύωσης (social media).

Για τα παραπάνω, ενημερώθηκαν οι εισαγγελικές Αρχές, οι οποίες εξέδωσαν σχετικές Διατάξεις και Βουλεύματα για την άρση του απορρήτου των επικοινωνιών. Ακολούθησε πολύμηνη, μεθοδική - συστηματική ψηφιακή διαδικτυακή έρευνα, από ειδικά καταρτισμένους αστυνομικούς της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, στο πλαίσιο της οποίας ταυτοποιήθηκε και διακριβώθηκε η εγκληματική δράση των δύο συλληφθέντων.

Ειδικότερα, από την ψηφιακή διερεύνηση της υπόθεσης προέκυψε ότι οι δύο εμπλεκόμενοι, ήταν οι δημιουργοί του κακόβουλου λογισμικού με την διεθνή κωδική ονομασία "Lecpetex", το οποίο διέδιδαν κυρίως μέσω ιστοσελίδας κοινωνικής δικτύωσης (social media), μολύνοντας μεγάλο αριθμό υπολογιστικών συστημάτων παγκοσμίως.

Αξίζει να σημειωθεί ότι η διαχειρίστρια εταιρεία της ιστοσελίδας κοινωνικής δικτύωσης για να αντιμετωπίσει τις σημαντικές δυσλειτουργίες, που προκαλούσε στα υπολογιστικά της συστήματα ο συγκεκριμένος ιός, άλλαξε πολλές φορές την πολιτική απορρήτου της, εισάγοντας ειδικούς μηχανισμούς ασφαλείας για το σύνολο των χρηστών της, με συνέπεια να επηρεάζεται έτσι η συνολική εύρυθμη λειτουργία του δικτύου της.

Τους μηχανισμούς αυτούς, πολλές φορές κατάφεραν να υπερκεράσουν οι συλληφθέντες, χρησιμοποιώντας προηγμένες τεχνικές και λογισμικό, επιτυγχάνοντας έτσι να προσβάλουν τους μηχανισμούς ανάπτυξης και τα συστήματα, όχι μόνο της συγκεκριμένης σελίδας κοινωνικής δικτύωσης, αλλά και άλλων διαδικτυακών εταιρειών ανά τον κόσμο, καθιστώντας έτσι, τον ιό, μία από τις σοβαρότερες απειλές παγκοσμίως σε επίπεδο κακόβουλου λογισμικού.

Τις λεπτομέρειες σχετικά με τη μεθοδολογία δράσης και τα επιμέρους στοιχεία και δεδομένα της υπόθεσης, θα σας παρουσιάσει ο Προϊστάμενος της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, Ταξίαρχος κ. Εμμανουήλ Σφακιανάκης».

Δηλώσεις Ταξίαρχου Εμμανουήλ Σφακιανάκη:

«Πρόκειται για την πλέον σημαντική υπόθεση που έχει χειριστεί η Δίωξη Ηλεκτρονικού Εγκλήματος, με σοβαρές επιπτώσεις στο παγκόσμιο διαδικτυακό υπολογιστικό σύστημα. Καταφέραμε να αποτρέψουμε μια σημαντική απειλή για την ασφάλεια των ηλεκτρονικών υπολογιστών, που προκάλεσε μεγάλα προβλήματα σε εκατομμύρια χρήστες του διαδικτύου, σε όλο τον κόσμο.

[878] http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=42947&Itemid=1333

Αναφορικά με την μεθοδολογία δράσης τους, αυτή συνίστατο στην αποστολή προσωπικών μηνυμάτων στους χρήστες της σελίδας κοινωνικής δικτύωσης (social media), στα οποία επισύναπταν το κακόβουλο λογισμικό ως συνημμένο αρχείο. Με αυτόν τον τρόπο, αποσκοπούσαν στην εξαπάτηση των χρηστών, ώστε να ανοίξουν το αρχείο, το οποίο στη συνέχεια μόλυνε τον υπολογιστή τους.

Σημειώνεται ότι οι δράστες χρησιμοποιούσαν - αξιοποιούσαν τη διαδικτυακή πλατφόρμα της σελίδας κοινωνικής δικτύωσης, καθώς το κακόβουλο λογισμικό τους, μέσω της ικανότητας που είχε να αυτοδιαδίδεται, κατάφερνε να μολύνει όλες τις επαφές - φίλους του αρχικά προσβαλλόμενου χρήστη αποστέλλοντας τους αυτόματα, παρόμοια κακόβουλα μηνύματα. Με αυτόν τον τρόπο επεκτεινόταν γεωμετρικά ο αριθμός των μολυσμένων υπολογιστών, σε παγκόσμια κλίμακα.

Εναλλακτικά, οι δράστες διαμοίραζαν το κακόβουλο λογισμικό με τη χρήση ειδικών προγραμμάτων διαμοιρασμού αρχείων Peer 2 Peer, μέσω των οποίων διέθεταν δωρεάν «σπασμένες» εκδόσεις δημοφιλών παιχνιδιών, τραγουδιών και κινηματογραφικών ταινιών, στις οποίες όμως είχαν επισυνάψει το κακόβουλο λογισμικό. Αυτό είχε ως αποτέλεσμα, οι χρήστες που «κατέβαζαν» (free download) τα αρχεία αυτά, να μολύνουν τους ηλεκτρονικούς υπολογιστές τους.

Όπως προκύπτει από διεθνή έρευνα, η παραπάνω παράνομη δραστηριότητα που πλέον παρατηρείται στο μεγαλύτερο μέρος των χρηστών του διαδικτύου και μέσω της οποίας οι χρήστες αυτού κατεβάζουν δωρεάν από διάφορες ιστοσελίδες παιχνίδια, λογισμικό, τραγούδια, ταινίες, προκαλεί ετησίως ζημιά στα υπολογιστικά τους συστήματα (PC, Laptop, κ.α.) η οποία ξεπερνά το 1,5 δις ευρώ και αυτό οφείλεται σε διάφορες δυσλειτουργίες (ζημιές) που προκαλούνται στα υπολογιστικά τους συστήματα από το κακόβουλο λογισμικό.

Σημειώνεται ότι είναι μεγάλος ο αριθμός των χρηστών του διαδικτύου, οι οποίοι δελεάζονται από τις ευκαιρίες που τους παρέχει το «ελεύθερο κατέβασμα αρχείων» (free downloading) και αγνοούν τους ενδεχόμενους κινδύνους και τις ζημιές που μπορεί να προκαλέσουν στα υπολογιστικά τους συστήματα.

Όπως προέκυψε από την εξέλιξη της έρευνας, οι δράστες χρησιμοποιούσαν τον ιό για συγκεκριμένους ιδιοτελείς σκοπούς, που αφορούν κυρίως:

- Στη χρήση της υπολογιστικής ισχύος των μολυσμένων μηχανημάτων (εκατοντάδων χιλιάδων) για την παραγωγή εικονικού διαδικτυακού χρήματος (bitcoin mining). Συγκεκριμένα το κακόβουλο λογισμικό, μετά την εγκατάσταση του, χρησιμοποιούσε τους προσβαλλόμενους ηλεκτρονικούς υπολογιστές, για να παράγουν ψηφιακά-εικονικά νομίσματα (bitcoin) και
- Στην υποκλοπή ηλεκτρονικών πορτοφολιών (wallets). Οι δράστες με τη χρήση του ιού, υπέκλεπταν τους κωδικούς πρόσβασης ηλεκτρονικών πορτοφολιών τα οποία περιείχαν ψηφιακά-εικονικά νομίσματα (bitcoins) και τα μετέφεραν σε άλλα ηλεκτρονικά πορτοφόλια, τα οποία βρίσκονταν υπό τον έλεγχό τους.

Τα διαδικτυακά εικονικά νομίσματα (bitcoins) που συνέλεγαν οι δράστες: α) τα προωθούσαν σε εξειδικευμένες υπηρεσίες μείξης (mixing services), μέσω ειδικού δικτύου (TOR) στο οποίο οι χρήστες του διαδικτύου αποκτούν πρόσβαση μόνο με τη χρήση εξειδικευμένου λογισμικού. Με τον τρόπο αυτό απέκρυπταν τα ίχνη προέλευσης των παράνομων κερδών που είχαν προέρθει από την παραγωγή bitcoins και από τα ηλεκτρονικά πορτοφόλια που είχαν υποκλέψει και β) τα μετέτρεπαν σε ευρώ με τη χρήση των υπηρεσιών ειδικών ηλεκτρονικών ανταλλακτηρίων τα οποία διατίθενται στο διαδίκτυο, εισπράττοντας, τελικώς, τα παράνομα κέρδη.

- Στην υποκλοπή κωδικών πρόσβασης πάσης φύσεως. Συγκεκριμένα με τη χρήση του ιού υπέκλεπταν τους κωδικούς πρόσβασης από ηλεκτρονικά ταχυδρομεία και λογαριασμούς πάσης φύσεως (e-banking, Paypal κ.ά.) και τους καταχωρούσαν σε βάση δεδομένων. Χαρακτηριστικό παράδειγμα αποτελεί η υποκλοπή από τους δράστες, κωδικού ασφαλείας (password) διεύθυνσης ηλεκτρονικού ταχυδρομείου του

Υπουργείου Εμπορικής Ναυτιλίας, στο οποίο οι δράστες απέκτησαν πρόσβαση στο περιεχόμενό του.

Επισημαίνεται ότι από την εξέλιξη της έρευνας, οι δράστες το τελευταίο χρονικό διάστημα, σχεδίαζαν την υλοποίηση δικής τους υπηρεσίας νομιμοποίησης εσόδων από παράνομες δραστηριότητες, με τη μείξη ψηφιακών-εικονικών νομισμάτων (bitcoin mixing service), την οποία σκόπευαν να διαθέτουν μέσω του δικτύου TOR.

Σε συντονισμένες έρευνες που πραγματοποιήθηκαν στις οικίες των δύο ημεδαπών, παρουσία Εισαγγελικού Λειτουργού και ειδικότερα από τον έλεγχο που πραγματοποιήθηκε στους ηλεκτρονικούς υπολογιστές τους, βρέθηκαν:

- ο πηγαίος κώδικας του κακόβουλου λογισμικού, τον οποίο χρησιμοποιούσαν προκειμένου να μολύνουν τα υπολογιστικά συστήματα των θυμάτων,
- ο λογαριασμός που διατηρούσαν στην υπηρεσία μείξης ψηφιακών εικονικών νομισμάτων (bitcoin mixing services) “bitcoin fog” (στην TOR διεύθυνση), με σκοπό να αποκρύψουν τα ίχνη προέλευσης των ψηφιακών εικονικών νομισμάτων (bitcoins),
- ο λογαριασμός που διατηρούσαν στο ηλεκτρονικό ανταλλακτήριο “Kraken” (στη διεύθυνση “www.kraken.com”) για τη μετατροπή των bitcoins σε κανονικό νόμισμα (π.χ. ευρώ), καθώς και το ιστορικό αναλήψεων από την εν λόγω υπηρεσία,
- φάκελος στον οποίο ήταν αποθηκευμένα είκοσι έξι χιλιάδες εξακόσια δέκα (26.610) αρχεία με κλεμμένους διάφορους κωδικούς πρόσβασης χρηστών του διαδικτύου από διάφορες υπηρεσίες που αυτοί χρησιμοποιούσαν,
- φάκελος στον οποίο ήταν αποθηκευμένα 114 αρχεία με υποκλαπέντα ηλεκτρονικά πορτοφόλια,
- δείγμα του πηγαίου κώδικα τον οποίο ανέπτυσσαν για την κατασκευή δικής τους υπηρεσίας μείξης ψηφιακών εικονικών νομισμάτων (bitcoin mixing service).

Τα κατασχεθέντα ψηφιακά πειστήρια θα αποσταλούν στη Διεύθυνση Εγκληματολογικών Ερευνών, για περαιτέρω εργαστηριακή τους εξέταση, από την οποία αναμένεται να προκύψουν με ακρίβεια τα υπολογιστικά συστήματα τα οποία είχαν υπό τον έλεγχο τους, καθώς και τα οικονομικά οφέλη που είχαν αποκτήσει.

Οι δύο συλληφθέντες με δικογραφία που σχηματίστηκε σε βάρος τους, οδηγούνται στην Εισαγγελία Πρωτοδικών Αθηνών.»

20. Μέτρα Ασφάλειας e-banking

Η «τράπεζα»[879] δίνει μερικές χρήσιμες συμβουλές και απλές οδηγίες, στους χρήστες των ηλεκτρονικών υπηρεσιών της για να συμβάλλουν και οι ίδιοι στην ασφάλεια των προσωπικών τους στοιχείων.

«1) ΕΞΑΣΦΑΛΙΣΗ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Για την μέγιστη δυνατή εξασφάλιση του απορρήτου της μεταφοράς των δεδομένων, που ανταλλάσσονται μεταξύ των δύο πλευρών (Τράπεζας - Πελάτη) χρησιμοποιούμε το πρωτόκολλο κρυπτογράφησης SSL 128bit, που θεωρείται απαραβίαστο για τις εφαρμογές στο διαδίκτυο. Το σύστημα έχει πιστοποιηθεί από την εταιρία Verisign, η οποία ειδικεύεται σε θέματα ασφάλειας συναλλαγών.

2) ΑΝΑΓΝΩΡΙΣΗ ΧΡΗΣΤΗ

Ο χρήστης για να αναγνωριστεί από την υπηρεσία e-banking που του επιτρέπει την πρόσβαση του στο σύστημα, θα πρέπει να διαθέτει τον Κωδικό Πελάτη (user name) και τον Μυστικό Κωδικό Πελάτη (password).

3) ΥΠΟΧΡΕΩΤΙΚΗ ΑΛΛΑΓΗ ΚΩΔΙΚΩΝ

Με την πρώτη εισαγωγή στο σύστημα e-banking, είναι υποχρεωτική η αλλαγή Μυστικού Κωδικού Πελάτη (password).

Σε τακτά χρονικά διαστήματα, ελέγχεται η τελευταία φορά που αλλάξατε τον Μυστικό Κωδικό Πελάτη (password) σε σχέση με το μέγιστο επιτρεπόμενο διάστημα και εάν έχει ξεπεραστεί, το σύστημα σας υποχρεώνει να τον αλλάξετε.

4) ΑΠΟΣΥΝΔΕΣΗ ΑΠΟ ΤΗΝ ΥΠΗΡΕΣΙΑ E- BANKING

Μετά την πάροδο 20 λεπτών από την είσοδο του χρήστη στο e-banking, γίνεται αυτόματη αποσύνδεσή του από το σύστημα.

5) ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ ΚΩΔΙΚΩΝ

Εάν εισάγετε τον Μυστικό Κωδικό Πελάτη (password) τρεις (3) φορές λάθος, τότε απενεργοποιείται αυτόματα και δεν σας επιτρέπεται η πρόσβαση στο e-banking.

Απενεργοποίηση της χρήσης του e-banking μετά από μεγάλο διάστημα αδράνειας.

Έχει οριστεί ένα διάστημα αδράνειας με την πάροδο του οποίου ο χρήστης απενεργοποιείται και πρέπει να επικοινωνήσει με την Τράπεζα για να παραλάβει τον καινούργιο Μυστικό Κωδικό Πελάτη (password). Στη συνέχεια, το σύστημα θα τον αντιμετωπίσει ως νέο χρήστη.

6) ΑΡΙΘΜΟΙ TAN

Πρόσθετος Κωδικός Ασφαλείας που απαιτείται για την εκτέλεση συγκεκριμένων συναλλαγών σας (εγχρήματων και ασφαλείας).

Κάθε φορά που χρησιμοποιείτε ένα TAN παύει να ισχύει. Για να εκτελέσετε άλλη συναλλαγή πρέπει να εισάγετε καινούριο.

Το σύστημα απενεργοποιεί (μπλοκάρει) αυτόματα τη λίστα σας μετά από τρεις (3) συνεχόμενες προσπάθειες εισαγωγής λανθασμένου TAN.

7) ΕΛΕΓΧΟΣ ΙΣΤΟΣΕΛΙΔΑΣ

Πριν από την εισαγωγή των προσωπικών σας κωδικών πρέπει να είστε πάντα βέβαιοι ότι έχετε συνδεθεί με το αυθεντικό site της Τράπεζας. Η Τράπεζα έχει προμηθευτεί πιστοποιητικό αυθεντικότητας στο διαδίκτυο , που εμφανίζεται κάθε φορά που επισκέπτεστε την ιστοσελίδα εισόδου του συστήματός της με το εικονίδιο (κλειδαριά στο κάτω μέρος της οθόνης).

Ποτέ μην κάνετε σύνδεση μέσω (link) που περιέχει την σελίδα της x bank, πιθανόν κάποιος κακόβουλος να θέλει να υποκλέψει προσωπικά σας στοιχεία.

ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΠΕΛΑΤΗ

Μην παρασυρθείτε από παραπλανητικά τηλεφωνήματα η e-mail.

Η Τράπεζα δεν πρόκειται ποτέ να σας ζητήσει να αποκαλύψετε αριθμούς λογαριασμών, καρτών η προσωπικών σας στοιχείων (Μυστικό Κωδικό Πελάτη - password, TAN κλπ).

[879] Σκόπιμα δεν αναφέρουμε όνομα.

Η Υπηρεσία της Τράπεζας το μόνο που μπορεί να σας ζητήσει είναι τον Κωδικό Πελάτη (user name) για να μπορέσει να σας εξυπηρετήσει, μετά από δικό σας τηλεφώνημα προς την Τράπεζα. Μη δίνετε λοιπόν ποτέ τους κωδικούς σας σε τρίτους.

Ο Μυστικός Κωδικός Πρόσβασης αλλάζει από εσάς, όποτε το επιθυμείτε. Επίσης, αποφεύγετε να χρησιμοποιείτε τους ίδιους επαναλαμβανόμενους χαρακτήρες (π.χ. 11111, κλπ.) είτε γνωστούς χαρακτήρες από τρίτους, όπως π.χ. η ημ/νία γεννήσεώς σας.

Μην αφήνετε «ανοιχτό» το παράθυρο της συναλλαγής σας, εάν δεν βρίσκεστε κοντά στον υπολογιστή σας.

Να ακολουθείτε πάντα τις οδηγίες που δίνονται, προκειμένου είτε να συνδεθείτε είτε να αποσυνδεθείτε από το e-banking. Ειδικότερα, όταν θέλετε να αποσυνδεθείτε να επιλέγετε πάντα το «ΕΞΟΔΟΣ» και να μην αποσυνδέεστε κλείνοντας απλά τη σύνδεση με το Internet.

Φροντίστε να έχετε λάβει τα κατάλληλα μέτρα προστασίας του υπολογιστή σας, ώστε να μην είναι ευάλωτος σε προσπάθειες υποκλοπής προσωπικών σας στοιχείων από τρίτους.

Προστατέψτε τον υπολογιστή σας εγκαθιστώντας αυτόματο πρόγραμμα ελέγχου ιών (antivirus) για την σύνδεση σας στο internet, ώστε να μην είσθε υποχρεωμένοι να ενεργοποιείτε και να ενημερώνετε το (antivirus).

Εάν δεν περιλαμβάνεται στο λειτουργικό του συστήματος σας, μπορείτε να εγκαταστήσετε το πρόγραμμα (firewall). Το πρόγραμμα αυτό δημιουργεί ένα τείχος προστασίας και προστατεύει τον υπολογιστή σας από κακόβουλες επιθέσεις.

Επίσης υπάρχει και το λογισμικό (anti-spyware) της Microsoft για προστασία από υποκλοπές.»[880]

[880] https://ebanking.atticabank.gr/BOA_EBANKdemo/security.jsp

21. Η ψηφιακή προστασία της ιδιωτικής ζωής ανάμεσα στα ανθρώπινα δικαιώματα.

Ο αντίκτυπος των αποκαλύψεων Σνόουντεν. Κατάθεση ψηφίσματος και στον ΟΗΕ. [881]

«Εάν η κατάσταση συνεχίσει ανεξέλεγκτη» δήλωσε ο Γερμανός πρέσβης, Harald Braun, «κινδυνεύουμε να ζήσουμε οργουελικές καταστάσεις, όπου κάθε βήμα των πολιτών θα παρακολουθείται και θα καταγράφεται με σκοπό να αποτραπούν πιθανά εγκλήματα».

Αυξάνεται το διεθνές ενδιαφέρον για το θέμα της προστασίας της ιδιωτικής ζωής στο Διαδίκτυο, το οποίο συζητήθηκε εκτενώς στην τελευταία συνεδρίαση του ΟΗΕ, την περασμένη Τρίτη, όπου και περιγράφεται πλέον ως ανθρώπινο δικαίωμα. Μάλιστα, ο Οργανισμός Ηνωμένων Εθνών με ψήφισμά του την Τρίτη κάλεσε όλες τις χώρες-μέλη του να προστατεύουν το δικαίωμα της ιδιωτικής ζωής των πολιτών τους στον τομέα των ψηφιακών επικοινωνιών αλλά και να τους προσφέρουν λύσεις, αν νιώσουν ότι η ιδιωτική τους ζωή εκεί παραβιάζεται. Το εν λόγω μέτρο έγινε αποδεκτό από την πλειοψηφία της Επιτροπής Ανθρωπίνων Δικαιωμάτων της Γενικής Συνέλευσης και ήταν αποτέλεσμα έντονων διαπραγματεύσεων που πραγματοποιήθηκαν κεκλεισμένων των θυρών.

Μετά το ψήφισμα της Τρίτης το θέμα αναμένεται να πάει στο Συμβούλιο Ανθρωπίνων Δικαιωμάτων στη Γενεύη, το οποίο θα συνέλθει την ερχόμενη άνοιξη, ενώ οι υποστηρικτές του πιέζουν τον ΟΗΕ να στείλει έναν ειδικό απεσταλμένο. Οι χώρες που πρωτοστάτησαν στη θέσπιση του μέτρου ψηφιακής προστασίας της ιδιωτικής ζωής ήταν η Γερμανία και η Βραζιλία, των οποίων οι ηγέτες, η καγκελάριος Άνγκελα Μέρκελ και η Ντίλμα Ρούσεφ αντίστοιχα, εξέφρασαν την οργή τους για τα στοιχεία που έφεραν στο φως οι αποκαλύψεις Σνόουντεν σχετικά με την παρακολούθησή των επικοινωνιών τους από τις αμερικανικές μυστικές υπηρεσίες. «Εάν η κατάσταση συνεχίσει ανεξέλεγκτη» δήλωσε ο Γερμανός πρέσβης, Harald Braun, «κινδυνεύουμε να ζήσουμε οργουελικές καταστάσεις, όπου κάθε βήμα των πολιτών θα παρακολουθείται και θα καταγράφεται με σκοπό να αποτραπούν πιθανά εγκλήματα». Το ψήφισμα υποστηρίχθηκε από 65 χώρες-μέλη αλλά όχι από τις Ηνωμένες Πολιτείες, την Αυστραλία, τη Βρετανία, τον Καναδά και τη Νέα Ζηλανδία, που αποτελούν μια συμμαχία αντικατασκοπείας γνωστή και ως FIVE EYES. Το ψήφισμα της Τρίτης προτρέπει για πρώτη φορά στην ιστορία τις κυβερνήσεις να «παρέχουν στα άτομα των οποίων το δικαίωμα στην ιδιωτική ζωή έχει παραβιαστεί παράνομα ή αυθαίρετα την πρόσβαση σε αποτελεσματικά ένδικα μέσα». Μάλιστα, το κείμενο του ψηφίσματος για πρώτη φορά περιλαμβάνει ρητά μια αναφορά που δεν περιορίζεται μόνο στο περιεχόμενο κάθε επικοινωνίας μέσω Internet αλλά επεκτείνει το όριο του τι ορίζεται ως «ηλεκτρονικά προσωπικά δεδομένα» και στη συλλογή των metadata, τα οποία περιλαμβάνουν την ημερομηνία και την ώρα που στάλθηκε ένα email ή τη διάρκεια τηλεφωνημάτων. Τα παραπάνω είναι εμφανή σημάδια ότι οι αποκαλύψεις του πρώην εποχικού υπαλλήλου της NSA, Έντουαρντ Σνόουντεν, το περασμένο καλοκαίρι είχαν παγκόσμιο αντίκτυπο, ώστε σήμερα να συζητιούνται σε επίπεδο αρχηγών χωρών, χαράσσοντας μια νέα παγκόσμια πολιτική για την προστασίας της ιδιωτικής ζωής στον online κόσμο. Άλλωστε, ο ίδιος ο «πατέρας» του World Wide Web, σερ Τιμ Μπέρνερς Λι, ήταν ο πρώτος που αποκάλεσε πριν από λίγους μήνες «ήρωα» τον Σνόουντεν –έναν άνθρωπο που ακόμα ζει σε καθεστώς «φυγά»– και, απ' ό,τι φαίνεται, είχε πολλούς καλούς λόγους να το κάνει, αναγνωρίζοντας τη μακροπρόθεσμη συνεισφορά του στη θέσπιση ενός νέου, παγκόσμιου χάρτη ψηφιακών ατομικών δικαιωμάτων.

Πηγή: www.lifo.gr (29.11.2014)

[881] http://www.lifo.gr/team/spyrosvj/53454

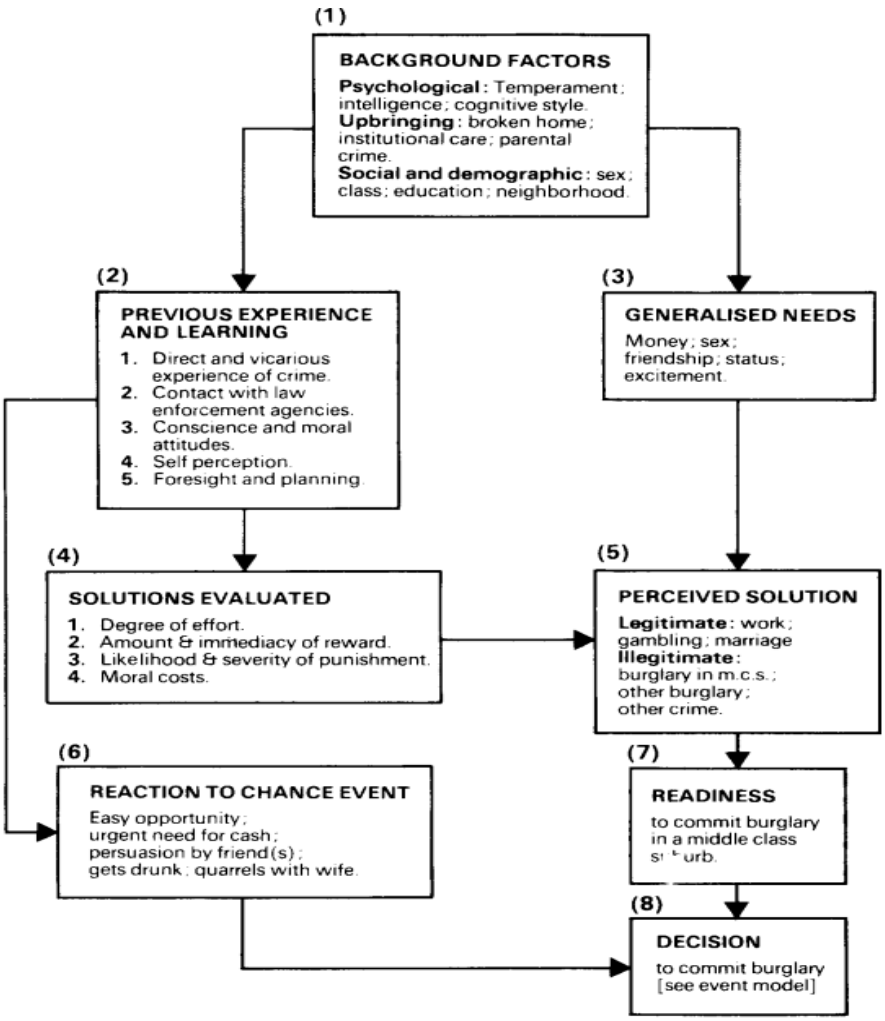
22. Συντομογραφίες της διαδικτυακής επικοινωνίας

AFK	Away From the Keyboard
asl	Age/Sex/Location
BBL	Be Back Later
b/f	Boyfriend
BRB	Be Right Back
BTW	By The Way
CU	See You
CYA	See Ya
DL Download	DLC Download Content
FAQ	Frequently Asked Question
F2F	Face To Face
FYI	For Your Information
GAL	Get A Life
g/f	Girlfriend
IC	I See
IDK	I don't know
IM	Instant Message
IMO	In My Opinion
IRL	In Real Life
JK	Just Kidding
LOL	Laughing Out Loud
kk	O. K.
L8R	Later
Sum1	Someone
np	No Problem
OMG	Oh My Gosh
OT	Off Topic
PPL	People
PLZ	Please
RL	Real Life
SMS	Short Message Service
THX	Thanks!
TTYL	Talk To You Later
WB	Welcome Back
WTGP?	Want To Go Private? [882]

[882] Πηγή http://diadiktio.wikispaces.com

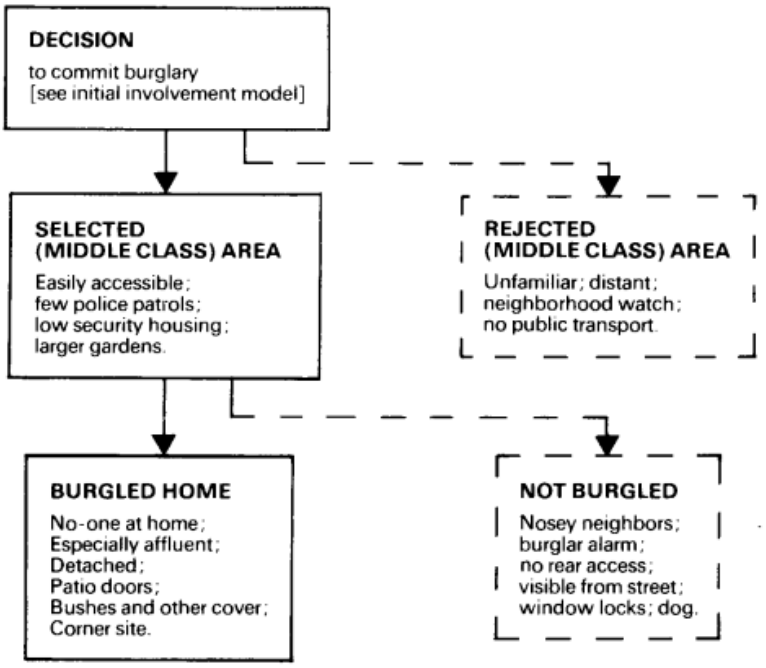
ΔΙΑΓΡΑΜΜΑΤΑ – ΠΙΝΑΚΕΣ

ΔΙΑΓΡΑΜΜΑ 1. ΑΡΧΙΚΗ ΕΜΠΛΟΚΗ (των Clarke R.V. και Cornish D.) [883]



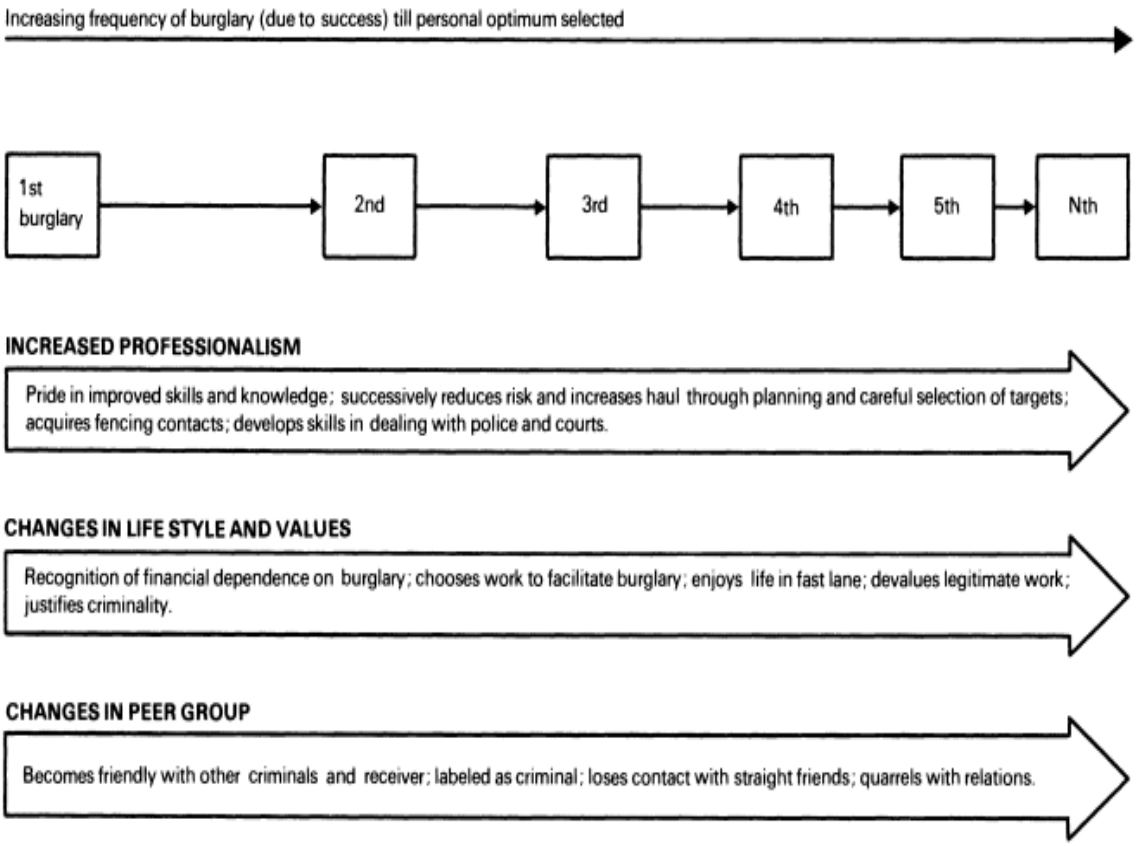
[883] Βλ. Clarke Ronald V. & Cornish Derek B. (1985), FIG. 1. Initial involvement model (example: burglary in a middle-class suburb

ΔΙΑΓΡΑΜΜΑ 2. ΜΟΝΤΕΛΟ ΓΕΓΟΝΟΤΟΣ (των Clarke R.V. και Cornish D.) [884]



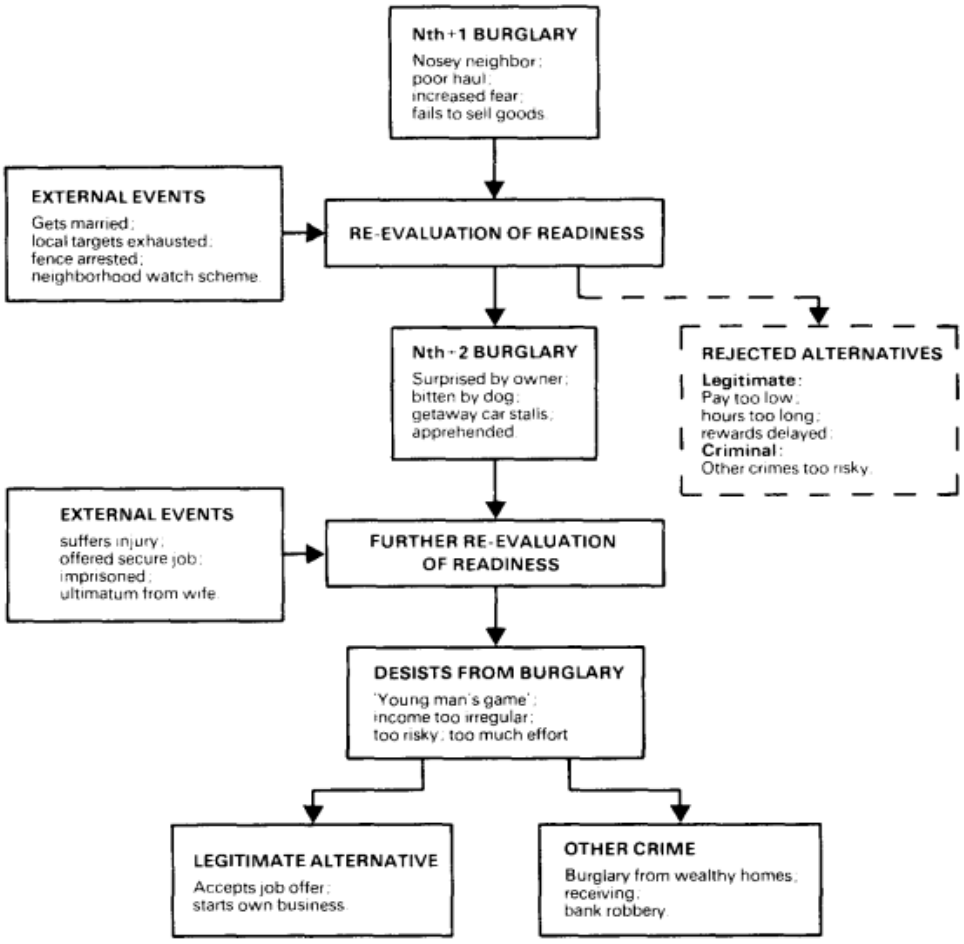
[884] Βλ Clarke Ronald V. & Cornish Derek B. (1985), FIG. 2. Event model (example: burglary in a middle-class suburb), σ.169

ΔΙΑΓΡΑΜΜΑ 3. ΜΟΝΤΕΛΟ ΣΥΝΕΧΙΣΗΣ ΕΜΠΛΟΚΗΣ (των Clarke R.V. και Cornish D.) [885]



[885] Βλ Clarke Ronald V. & Cornish Derek B. (1985), FIG. 3. Continuing involvement model (example: burglary in a middle class suburb), σ.171

ΔΙΑΓΡΑΜΜΑ 4. ΜΟΝΤΕΛΟ ΠΑΥΣΗΣ ΤΗΣ ΔΡΑΣΗΣ (των Clarke R.V. και Cornish D.) [886]



[886] Βλ. Clarke Ronald V. & Cornish Derek B. (1985), FIG. 4.-Desistance model (example: burglary in a middle-class suburb), σ.172

ΔΙΑΓΡΑΜΜΑ 5. «25 ΤΕΧΝΙΚΕΣ ΠΑΡΕΜΒΑΣΗΣ ΓΙΑ ΤΟ ΠΕΡΙΣΤΑΣΙΑΚΟ ΕΓΚΛΗΜΑ» [887]

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
1. Target harden • Steering column locks • Anti-robbery screens • Tamper-proof packaging	**6. Extend guardianship** • Take routine precautions: go out in group at night, leave signs of occupancy, carry phone • "Cocoon" neighborhood watch	**11. Conceal targets** • Off-street parking • Gender-neutral phone directories • Unmarked bullion trucks	**16. Reduce frustrations and stress** • Efficient queues and polite service • Expanded seating • Soothing music/muted lights	**21. Set rules** • Rental agreements • Harassment codes • Hotel registration
2. Control access to facilities • Entry phones • Electronic card access • Baggage • screening	**7. Assist natural surveillance** • Improved street lighting • Defensible space design • Support whistleblowers	**12. Remove targets** • Removable car radio • Women's refuges • Pre-paid cards for pay phones	**17. Avoid disputes** • Separate enclosures for rival soccer fans • Reduce crowding in pubs • Fixed cab fares	**22. Post instructions** • "No Parking" • "Private Property" • "Extinguish camp fires"
3. Screen exits • Ticket needed for exit • Export documents • Electronic merchandise tags	**8. Reduce anonymity** • Taxi driver IDs • "How's my driving?" decals • School uniforms	**13. Identify property** • Property marking • Vehicle licensing and parts marking • Cattle branding	**18. Reduce emotional arousal** • Controls on violent pornography • Enforce good behavior on soccer field • Prohibit racial slurs	**23. Alert conscience** • Roadside speed display boards • Signature for customs declarations • "Shoplifting is stealing"
4. Deflect offenders • Street closures • Separate bathrooms for women • Disperse pubs	**9. Utilize place managers** • CCTV for double-deck buses • Two clerks for convenience stores • Reward vigilance	**14. Disrupt markets** • Monitor pawn shops • Controls on classified ads • License street vendors	**19. Neutralize peer pressure** • "Idiots drink and drive" • "It's OK to say NO" • Disperse troublemakers at school	**24. Assist compliance** • Easy library checkout • Public lavatories • Litter bins
5. Control tools/weapons • "Smart" guns • Disable stolen cell phones • Restrict spray paint sales to juveniles	**10. Strengthen formal surveillance** • Red light cameras • Burglar alarms • Security guards	**15. Deny benefits** • Ink merchandise tags • Graffiti cleaning • Speed humps	**20. Discourage imitation** • Rapid repair of vandalism • V-chips in TVs • Censor details of modus operandi	**25. Control drugs and alcohol** • Breathalyzers in pubs • Server intervention • Alcohol-free events

[887] Benson Michael L., Madensen Tamara D. (2007), «Twenty-five techniques of situational preventions»

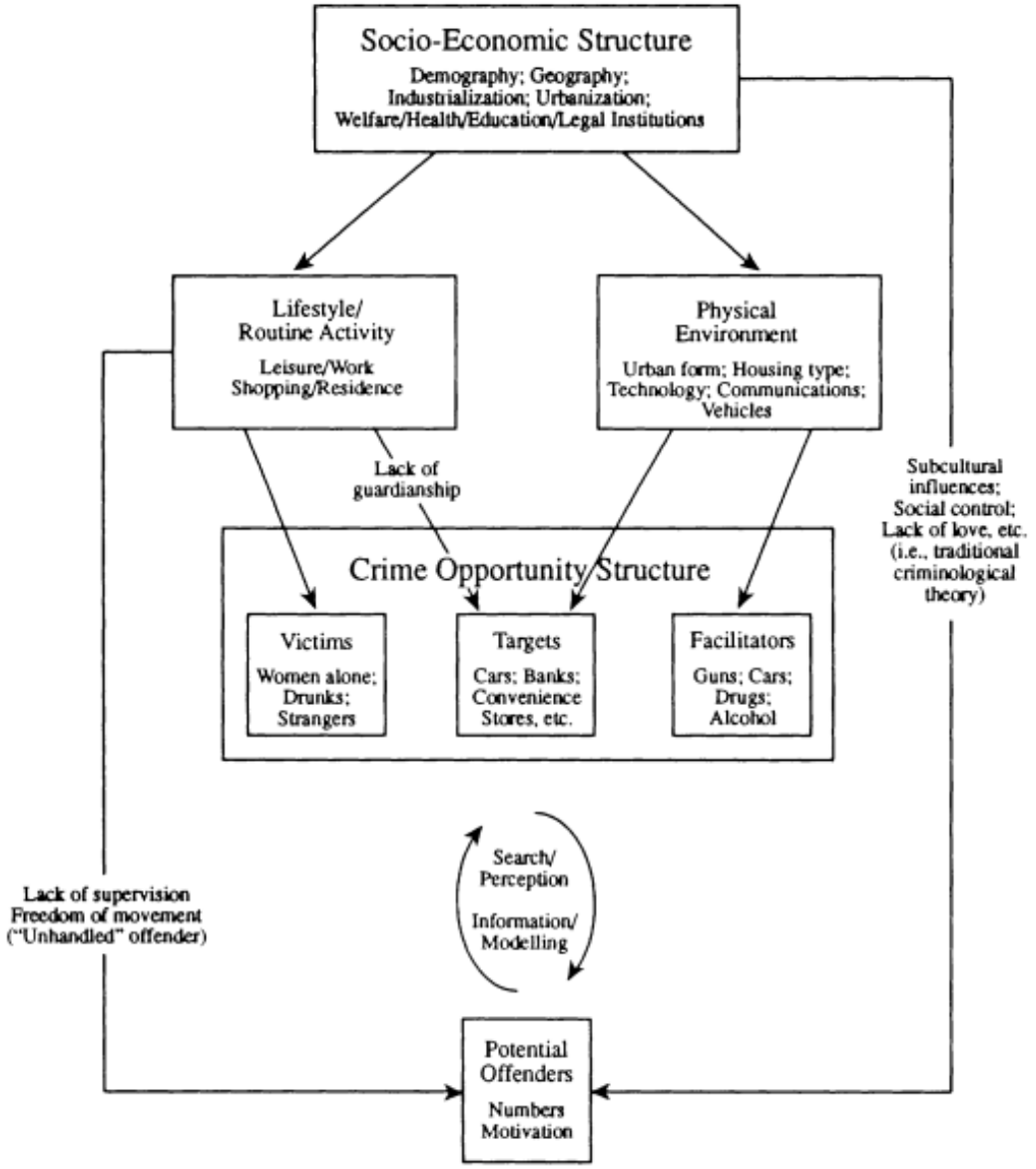
ΔΙΑΓΡΑΜΜΑ 6. ΥΠΟΛΟΓΙΖΟΜΕΝΟ ΚΟΣΤΟΣ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

ΕΙΔΟΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ	ΕΚΤΙΜΩΜΕΝΟ ΚΟΣΤΟΣ	ΠΟΣΟΣΤΟ ΕΠΙ ΤΟΥ ΑΕΠ	ΠΗΓΗ
ΠΑΓΚΟΣΜΙΩΣ			
ΠΕΙΡΑΤΕΙΑ	1 -16 ΔΙΣ $	0,008% -0,02%	IMB
ΔΙΑΚΙΝΗΣΗ ΝΑΡΚΩΤΙΚΩΝ	600 ΔΙΣ $	5 %	UNODC
ΠΑΓΚΟΣΜΙΑ ΔΙΑΔΙΚΤΥΑΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	300 ΔΙΣ -1 ΤΡΙΣ $	0,4% - 1,4 %	ΔΙΑΦΟΡΕΣ

Πηγή (TrendMicro) [888]

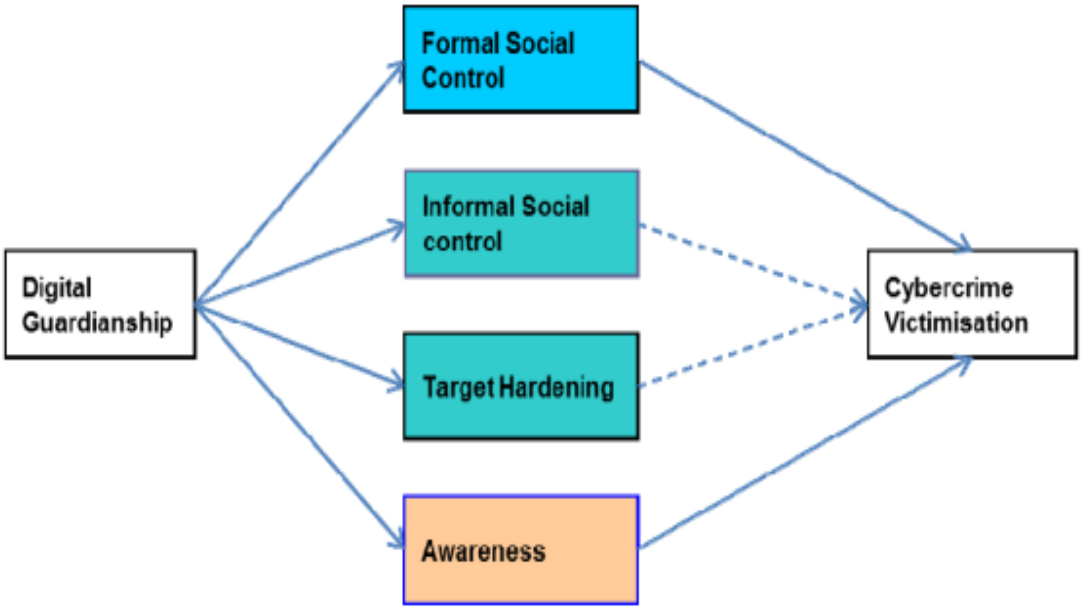
[888] Paganini Pierluigi (2014)

ΔΙΑΓΡΑΜΜΑ 7. Η ΕΥΚΑΙΡΙΑΚΗ ΔΟΜΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ - R.CLARKE[889]



[889] Clarke Ronald V. (1995)

ΔΙΑΓΡΑΜΜΑ 8. ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΟΝΤΕΛΟ ΤΩΝ JAHANKHANI AND AL-NEMRAT ΓΙΑ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΨΗΦΙΑΚΩΝ ΙΚΑΝΩΝ ΦΥΛΑΚΩΝ[890]



[890] Jahankhani Hamid & Al-Nemrat Ameer (2011)

ΠΙΝΑΚΑΣ 1. ΛΟΓΟΙ ΜΗ ΑΣΚΗΣΗΣ ΠΟΙΝΙΚΗΣ ΔΙΩΞΗΣ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ [891]

ΛΟΓΟΙ ΜΗ ΑΣΚΗΣΗΣ ΠΟΙΝΙΚΗΣ ΔΙΩΞΗΣ (Declination Reason)	**Αριθμός περιπτώσεων (Number)**	**Ποσοστό μη άσκησης δίωξης (Declination)**	**Ποσοστό συνολικών δικαστικών αποφάσεων (Total Dispositions)**
Έλλειψη αποδείξεων για εγκληματική πρόθεση (Lack of evidence of criminal intent)	27	13.78%	10.67%
Αδύναμα ή ανεπαρκή αποδεικτικά στοιχεία (Weak or insufficient admissible evidence)	34	17.35%	13.44%
Ο ύποπτος διώκεται από διαφορετικές αρχές δίωξης (Suspect to be prosecuted by other Authorities)	23	11.73%	9.09%
Μη προφανές ομοσπονδιακό αδίκημα (No federal offense evident)	21	10.71%	8.30%
Ελάχιστο ομοσπονδιακό ενδιαφέρον ή έλλειψη αποτρεπτικής ισχύος (Minimal federal interest or no deterrent value)	19	9.69%	7.51%
Άγνωστος ύποπτος (No known suspect)	17	8.67%	6.72%
Ανήλικος ύποπτος (Juvenile suspect)	10	5.10%	3.95%
Υπηρεσιακό αίτημα (Agency request)	10	5.10%	3.95%
Αστικές, διοικητικές ή άλλες ποινικές εναλλακτικές (Civil, administrative, or other disciplinary alternatives)	6	3.06%	2.37%
Προβλήματα δικαιοδοσίας (Jurisdiction or venue problems)	5	2.55%	1.98%
Εξωδικαστικά εναλλακτικά μέτρα (Pre-trial diversion completed)	5	2.55%	1.98%
Έλλειψη ερευνητικών ή ανακριτικών πηγών (Lack of investigative or prosecutive resources)	4	2.04%	1.60%
Προβλήματα μαρτύρων (Witness problems)	3	1.53%	1.19%
Ο ύποπτος διώκεται για άλλες κατηγορίες (Suspect being prosecuted on other charges)	3	1.53%	1.19%
Άλλα αίτια (Other)	13	6.63%	5.15%
Η υπηρεσιακή πολιτική διαφέρει από τις εισαγγελικές οδηγίες [Office policy (fails to meet prosecutive guidelines)]	6	3.06%	2.37%

[891] US Department of Justice (1998)

ΠΙΝΑΚΑΣ 2. ΔΗΜΟΓΡΑΦΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΧΡΗΣΤΩΝ ΙΝΤΕΡΝΕΤ ΣΤΙΣ ΗΠΑ [892]

	% of adults who use the internet	
	June 2000	August 2011
All adults (age 18+)	**47%**	**78%**
Men	50	80
Women	45	76
Race/ethnicity		
White, Non-Hispanic	49	80
Black, Non-Hispanic	35	71
Hispanic^	40	68
Age		
18-29	61	94
30-49	57	87
50-64	41	74
65+	12	41
Household income		
Less than $30,000/yr	28	62
$30,000-$49,999	50	83
$50,000-$74,999	67	90
$75,000+	79	97
Educational attainment		
No high school diploma	16	43
High school grad	33	71
Some College	62	88
College +	76	94

^ Note: In the 2000 survey, this included only English-speaking Hispanics. In the 2011 survey, this included both English- and Spanish-speaking Hispanics.

All differences are statistically significant except for those between blacks and Hispanics in 2011.

Sources: The Pew Research Center's Internet & American Life Project's May 2000 Tracking Survey conducted May 19-June 21, 2000. N=2,117adults age 18 and older. Interviews were conducted in English. // The Pew Research Center's Internet & American Life Project's August Tracking Survey conducted July 25-August 26, 2011. N=2,260 adults age 18 and older, including 916 interviews conducted by cell phone. Interviews were conducted in both English and Spanish.

More: http://pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx

[892] http://www.pewinternet.org/2012/04/13/digital-differences, Νοέμβριος 2014

ΠΙΝΑΚΑΣ 3. ΧΡΗΣΗ ΙΝΤΕΡΝΕΤ ΚΑΤΑ ΦΥΛΗ, ΕΘΝΟΤΗΤΑ, ΕΠΙΠΕΔΟ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΗΛΙΚΙΑ ΣΤΙΣ ΗΠΑ ΑΠΟ 2000 ΕΩΣ 2011 [893]

Household Internet Use by Race and Ethnicity, Education, and Age: 2000–2011

(In thousands)

Year	Race and ethnicity							
	Total number of households and percent of households with Internet use							
	White alone, non-Hispanic		Black alone		Asian alone		Hispanic	
2000	78,719	46.1	13,171	23.6	3,457	56.2	9,565	23.6
2001	80,734	55.2	13,304	31.1	4,081	67.5	10,476	32.2
2003	81,857	59.9	13,746	36.0	4,009	66.7	12,023	36.0
2007	83,294	66.9	14,730	45.3	4,576	75.2	13,619	43.4
2009	83,810	73.3	15,254	54.5	4,625	80.5	13,799	52.8
2010	83,613	74.9	15,357	58.1	4,744	82.6	14,142	59.1
2011	83,148	76.2	15,369	56.9	4,795	82.7	14,222	58.3
Year	Educational attainment							
	Total number of households and percent of households with Internet use							
	Less than high school		High school degree[1]		Some college		Bachelors degree or more	
2000	17,402	11.7	32,278	29.9	27,883	49.0	27,684	66.0
2001	17,463	18.0	33,469	39.7	29,410	57.7	28,765	75.2
2003	16,972	20.2	34,377	43.1	30,320	62.6	31,457	78.3
2007	13,978	24.0	33,099	49.5	30,434	68.9	33,302	84.0
2009	13,711	32.2	32,990	57.5	31,050	74.7	34,910	88.5
2010	13,257	35.5	33,008	60.4	31,549	77.2	35,156	89.2
2011	13,183	36.9	33,060	61.2	31,586	77.3	35,301	89.9
Year	Age							
	Total number of households and percent of households with Internet use							
	Under 35 years		35–44 years		45–55 years		55 years and older	
2001	13,892	54.0	15,066	62.7	13,418	60.9	12,655	33.9
2003	15,251	56.8	15,572	65.3	14,922	65.1	16,108	40.7
2007	16,993	57.7	16,400	71.8	17,504	70.7	21,824	50.2
2009	19,150	67.0	17,249	77.8	18,982	75.8	26,558	58.2
2010	19,988	75.7	17,606	81.5	19,089	77.3	28,267	60.4
2011	19,745	75.9	17,400	81.9	19,083	77.9	29,274	61.7

[893] File Thom (2013)

ΠΙΝΑΚΑΣ 4. ΑΝΑΦΕΡΟΜΕΝΗ ΧΡΗΣΗ Η/Υ ΚΑΙ ΙΝΤΕΡΝΕΤ ΚΑΤΑ ΣΥΓΚΕΚΡΙΜΕΝΑ ΑΤΟΜΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ [894]

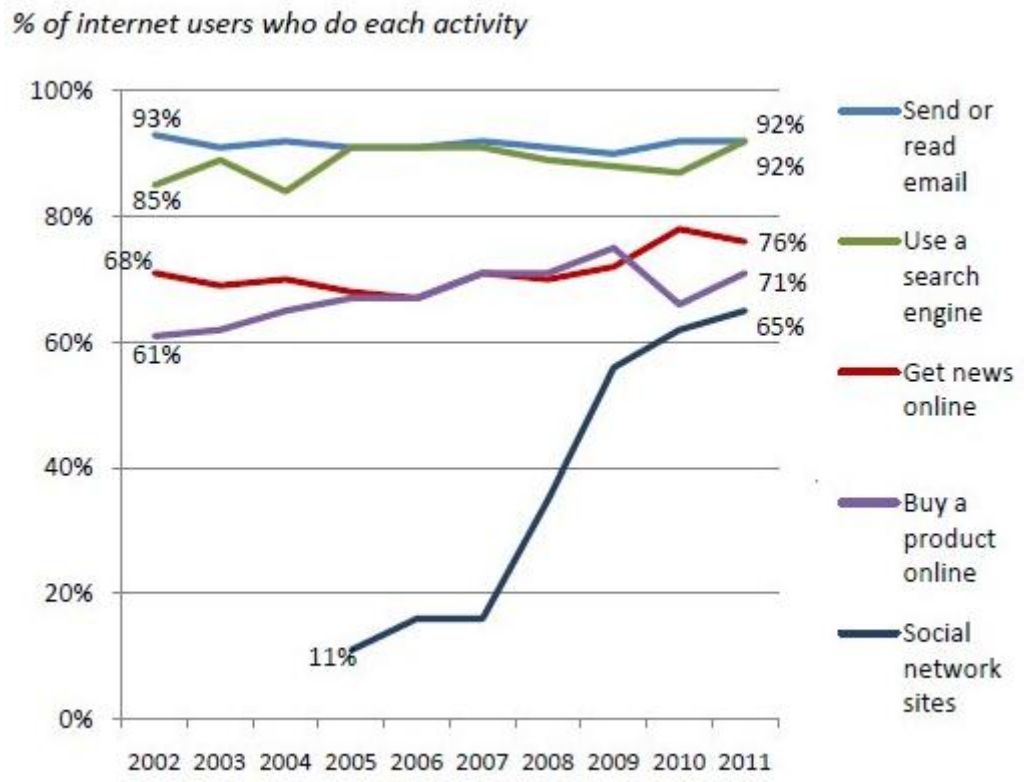
Reported Computer and Internet Use, by Selected Individual Characteristics: 2011

(In thousands)

Selected characteristics	Total	Lives in a home with at least one computer		Accesses the Internet from some location	
		Number	Percent	Number	Percent
Individuals 3 years and older	**293,414**	**235,066**	**80.1**	**204,596**	**69.7**
Age					
3–17 years	62,138	51,720	83.2	37,419	60.2
18–34 years	71,210	58,965	82.8	58,378	82.0
35–44 years	39,478	33,883	85.8	32,144	81.4
45–64 years	80,947	66,016	81.6	58,630	72.4
65 years and older	39,641	24,481	61.8	18,026	45.5
Race and Hispanic origin					
White alone	233,672	190,751	81.6	166,238	71.1
White non-Hispanic alone	190,318	161,471	84.8	142,827	75.0
Black alone	37,117	25,337	68.3	22,370	60.3
Asian alone	13,891	12,383	89.1	10,194	73.4
Hispanic (of any race)	47,114	32,032	68.0	25,648	54.4
Sex					
Male	143,780	116,120	80.8	99,739	69.4
Female	149,635	118,946	79.5	104,857	70.1
Household income					
Less than $25,000	70,352	39,901	56.7	35,020	49.8
$25,000–$49,999	76,985	58,396	75.9	49,070	63.7
$50,000–$99,999	89,514	82,408	92.1	71,509	79.9
$100,000–$149,000	33,157	31,862	96.1	28,810	86.9
$150,000 and more	23,407	22,499	96.1	20,187	86.2
Region					
Northeast	52,720	43,692	82.9	37,698	71.5
Midwest	63,575	51,395	80.8	45,620	71.8
South	108,353	83,546	77.1	72,694	67.1
West	68,766	56,433	82.1	48,585	70.7
Total 15 years and older	**243,689**	**194,096**	**79.6**	**177,808**	**73.0**
Employment status					
Employed	140,696	121,198	86.1	114,744	81.6
Unemployed	14,711	11,324	77.0	11,126	75.6
Not in labor force	88,282	61,575	69.7	51,937	58.8
Total 25 years and older	**201,475**	**158,535**	**78.7**	**142,374**	**70.7**
Educational attainment					
Less than high school graduate	24,960	12,703	50.9	7,864	31.5
High school graduate or GED	61,952	43,897	70.9	36,358	58.7
Some college or associate's degree	53,255	44,869	84.3	42,980	80.7
Bachelor's degree or higher	61,308	57,066	93.1	55,171	90.0

[894] File Thom (2013)

ΠΙΝΑΚΑΣ 5. ΠΟΣΟΣΤΑ ΧΡΗΣΤΩΝ ΚΑΤΑ ΕΙΔΟΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ [895]



[895] File Thom (2013)

ΠΙΝΑΚΑΣ 6. ΔΗΜΟΓΡΑΦΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΧΡΗΣΤΩΝ ΚΑΤΑ ΕΙΔΟΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ [896]

Online activities, by demographics

% of internet users age 18+ within each group who do the following activities online

	Search	Email	Buy a product	Use social network sites	Bank online
Date of survey	May 2011	Aug 2011	May 2011	Aug 2011	May 2011
All adults	92%	91%	71%	64%	61%
Men	93	89	69	63	65
Women	91	93	74	66	57
Race/ethnicity					
White, Non-Hispanic	93	92	73	63	62
Black, Non-Hispanic	91	88	74	70	67
Hispanic (English- and Spanish-speaking)	87	86	59	67	52
Age					
18-29	96	91	70	87	61
30-49	91	93	73	68	68
50-64	91	90	76	49	59
65+	87	86	56	29	44
Household income					
Less than $30,000/yr	90	85	51	68	42
$30,000-$49,999	91	93	77	65	65
$50,000-$74,999	93	94	80	61	74
$75,000+	98	97	90	66	80
Educational attainment					
No high school diploma	81	69	33	63	32
High school grad	88	87	59	60	47
Some College	94	95	74	73	66
College +	96	97	87	63	74

Sources: The Pew Research Center's Internet & American Life Project Tracking Surveys, May & August 2011. Interviews were conducted by landline and cell phone, in both English and Spanish.

[896] http://www.pewinternet.org/2012/04/13/digital-differences/#fn-188-40, Νοέμβριος 2014

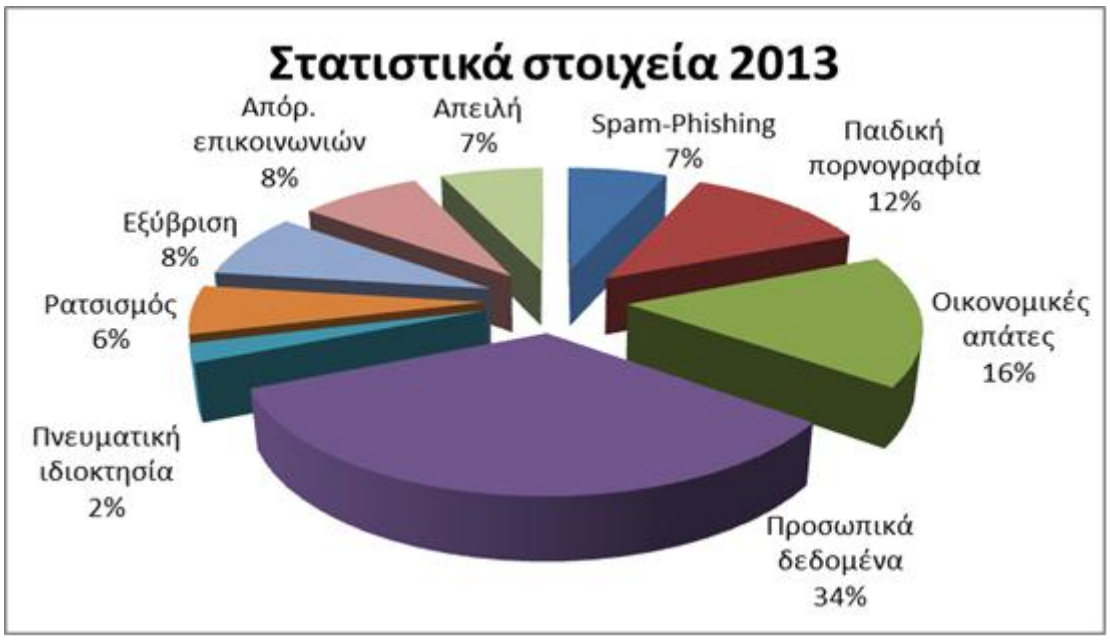
ΠΙΝΑΚΑΣ 7. ΛΟΓΟΙ ΠΡΟΣΒΑΣΗΣ ΑΝΑ ΑΣΧΟΛΙΑ ΧΡΗΣΤΗ (ΕΛΛΑΔΑ)[897]

Χρήση διαδικτύου- κυριότεροι λόγοι πρόσβασης ανά ασχολία χρήστη - 1ο τρίμηνο 2013.						
Κυριότεροι προσωπικοί λόγοι χρήσης του internet	**ΟΛΑ ΤΑ ΑΤΟΜΑ (16-74 ΕΤΩΝ)** που έκαναν χρήση διαδικτύ-ου	**ΑΣΧΟΛΙΑ ΧΡΗΣΤΗ**				
		ΜΑΘΗΤΗΣ/ ΦΟΙΤΗΤΗΣ	ΜΙΣΘΩΤΟΣ	ΑΥΤΟΑΠΑΣΧΟΛΟΥΜΕΝΟΣ/ ΒΟΗΘΟΣ ΣΤΗΝ ΟΙΚΟΓ. ΕΠΙΧΕΙΡΗΣΗ	ΑΝΕΡΓΟΣ	ΜΗ ΟΙΚΟΝΟΜΙ- ΚΑ ΕΝΕΡΓΑ ΑΤΟΜΑ
Επικοινωνία						
Αποστείλατε ή λάβατε ηλεκτρονικά μηνύματα	**76,6**	17,2	40,7	13,9	18,8	9,3
Συμμετείχατε σε ιστοσελίδες κοινωνικής δικτύωσης	**60,3**	22,3	36,5	12,3	21,3	7,5
Αναζήτηση πληροφοριών και on-line υπηρεσιών						
Διαβάσατε online ειδήσεις	**77,1**	13,0	41,8	14,4	17,8	13,0
Αναζητήσατε πληροφορίες υγείας	**56,0**	12,1	42,6	14,4	17,5	13,4
Αναζητήσατε πληροφορίες για κάποια επίσημη βαθμίδα εκπαίδευσης	**34,8**	27,6	37,6	10,5	18,0	6,3
Αναζητήσατε πληροφορίες για προϊόντα και υπηρεσίες	**83,4**	15,6	41,1	14,5	18,0	10,9
<<Κατεβάσατε>> λογισμικό	**23,5**	22,4	43,0	12,5	17,4	4,7
Συμμετοχή και έκφραση γνώμης για κοινωνικά και πολιτικά θέματα						
Αποστείλατε τη γνώμη σας για θέματα κοινωνικά ή πολιτικά σε ιστοσελίδες	**13,6**	11,1	46,1	15,9	14,8	12,1

[897] ΕΛ.ΣΤΑΤ. (2014)

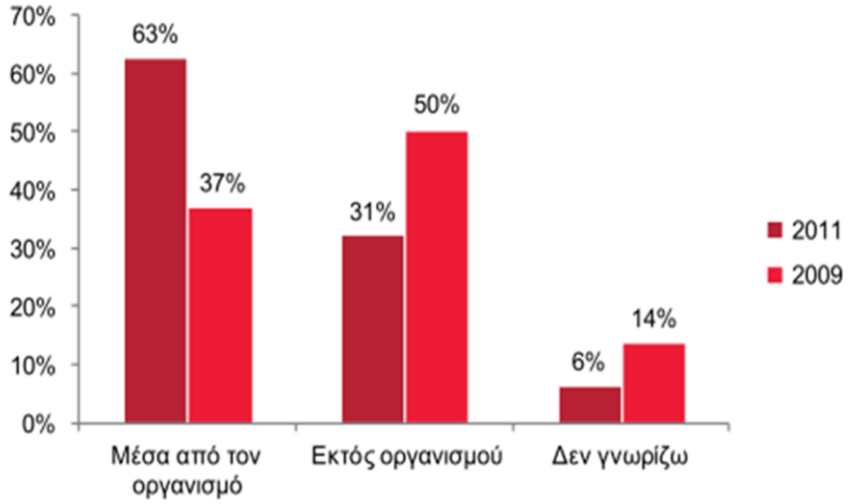
Λάβατε μέλος σε online διαβουλεύσεις ή ψηφοφορίες για τον καθορισμό κοινωνικών ή πολιτικών θεμάτων	**8,9**	9,2	51,6	15,4	14,7	9,1
Γνώση / μόρφωση						
Συμμετείχατε σε online εκπαιδευτικά προγράμματα	**7,0**	20,5	43,5	10,5	19,5	5,9
Συμβουλευτήκατε ηλεκτρονικές εγκυκλοπαιδιες (wikis) με σκοπό τη γνώση για οποιοδήποτε θέμα	**53,3**	20,8	40,0	12,7	17,5	9,0
Επαγγελματική ζωή						
Αναζητήσατε εργασία ή αποστείλατε αιτήσεις για εύρεση εργασίας	**26,7**	13,9	27,8	8,4	46,4	3,5
Συμμετείχατε σε ιστοσελίδες επαγγελματικής δικτύωσης. Στο Linkedin, στο Xing κλπ.)	**6,9**	15,3	45,6	18,5	18,8	1,8
Άλλες online υπηρεσίες						
Κάνατε χρήση υπηρεσιών για ταξίδια και καταλύματα	**38,1**	13,2	44,6	15,7	16,0	10,5
Πουλήσατε αγαθά ή υπηρεσίες, π.χ. μέσω δημοπρασιών	**5,9**	13,5	41,6	14,8	27,4	2,7
Τηλεφωνήσατε ή πραγματοποιήσατε βιντεοκλήσεις	**43,3**	20,4	37,6	13,2	19,2	9,7
Πραγματοποιήσατε τραπεζικές συναλλαγές	**17,9**	6,9	47,0	24,1	14,7	7,3
ΠΗΓΗ: Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας από τα Νοικοκυριά, έτους 2013						

ΠΙΝΑΚΑΣ 8. ΚΑΤΑΓΓΕΛΙΕΣ ΠΟΥ ΑΦΟΡΟΥΣΑΝ ΠΑΡΑΝΟΜΟ ΠΕΡΙΕΧΟΜΕΝΟ Η' ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΟ 2013 [898]



[898] Καταγγελίες - Στατιστικά στοιχεία, safeline, http://www.safeline.gr/kataggelies/statistika-stoiheia?set=1, Νοέμβριος 2014

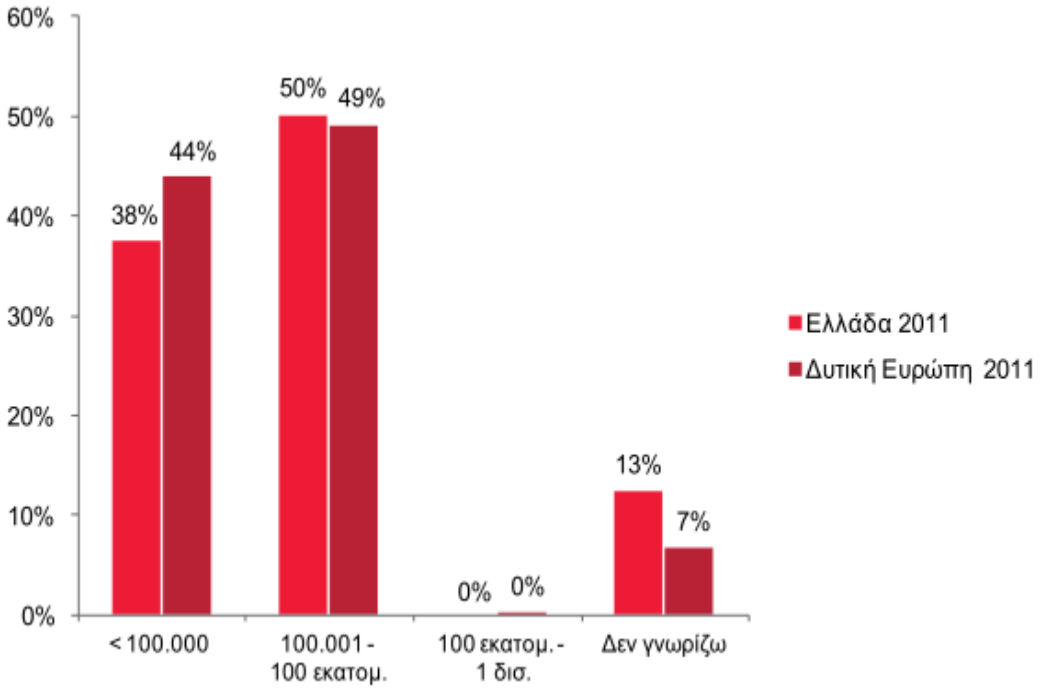
ΠΙΝΑΚΑΣ 9. ΟΙ ΥΠΑΙΤΙΟΙ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΗΝ ΕΛΛΑΔΑ



Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011 [899]

[899] Global Economic Crime Survey (2011)

ΠΙΝΑΚΑΣ 10. ΤΟ ΚΟΣΤΟΣ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ



Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011 [900]

[900] Global Economic Crime Survey (2011)

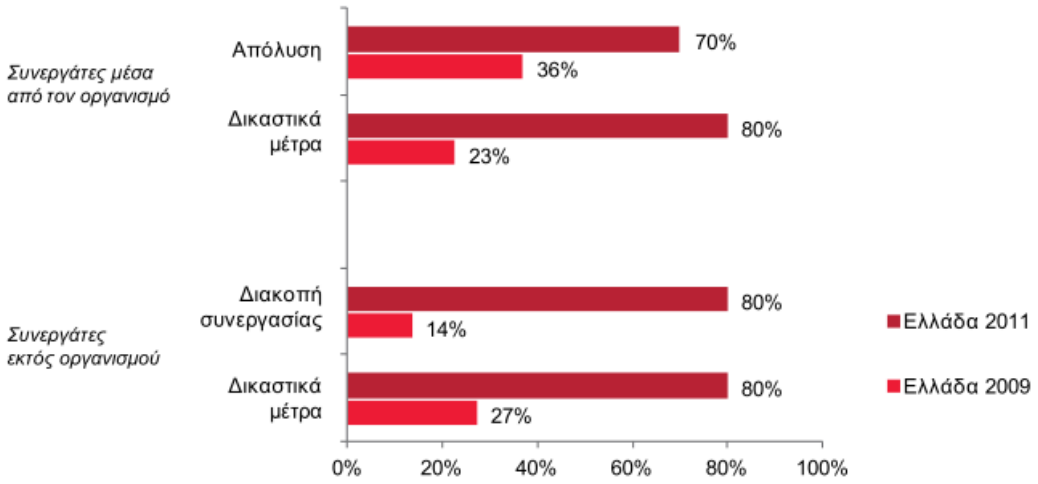
ΠΙΝΑΚΑΣ 11. «ΠΑΡΑΠΛΕΥΡΕΣ» ΑΠΩΛΕΙΕΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΤΟ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

Παράγοντες	Ελλάδα 2011	Δυτική Ευρώπη 2011
Εταιρική φήμη	31%	17%
Ηθικό των εργαζομένων	25%	23%
Επιχειρησιακές σχέσεις	19%	18%
Σχέσεις με ρυθμιστικές αρχές	6%	11%
Τιμή μετοχής	0%	1%

Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011 [901]

[901] Global Economic Crime Survey (2011)

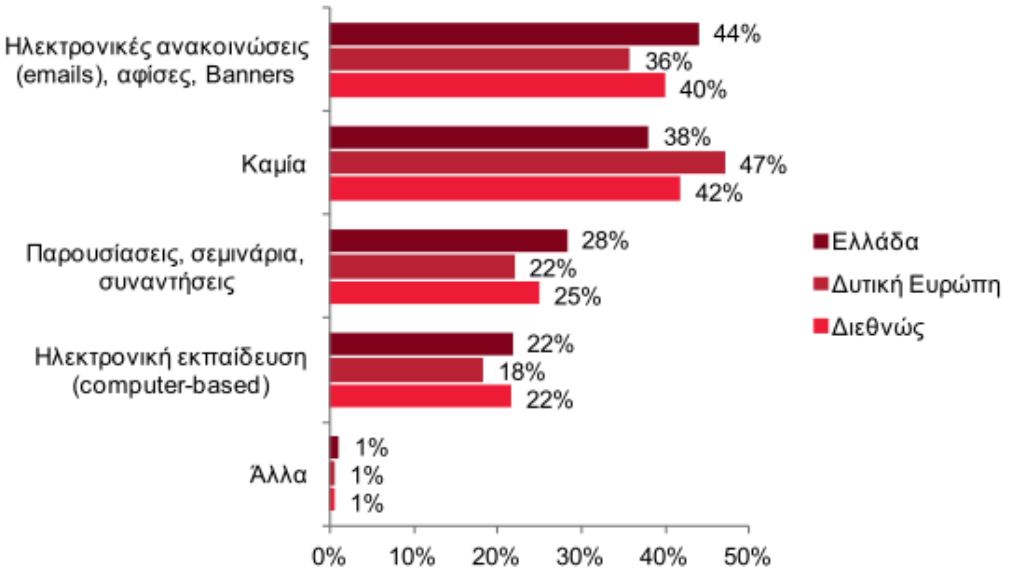
ΠΙΝΑΚΑΣ 12. ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΟ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΤΟΥΣ ΔΡΑΣΤΕΣ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ



Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011 [902]

[902] Global Economic Crime Survey (2011)

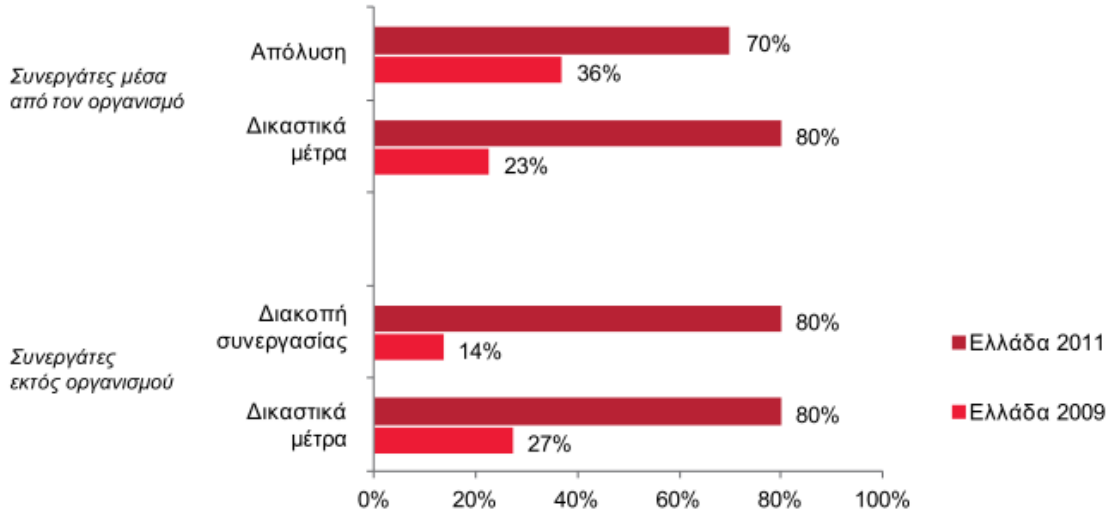
ΠΙΝΑΚΑΣ 13. ΤΡΟΠΟΙ ΕΝΗΜΕΡΩΣΗΣ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΑΠΟ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΓΙΑ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΑΠΟ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ



Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011 [903]

[903] Global Economic Crime Survey (2011)

ΠΙΝΑΚΑΣ 14. ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΥΠΑΙΤΙΩΝ ΟΙΚΟΝΟΜΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΑΠΟ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ



Πηγή: Παγκόσμια Έρευνα για το Οικονομικό Έγκλημα, Νοέμβριος 2011[904]

~~~~~~~~~~~~~~~~

[904] Global Economic Crime Survey (2011)
~~~~~~~~~~~~~~~~