Η ΨΗΦΙΑΚΗ (ΗΛΕΚΤΡΟΝΙΚΗ) ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ "ΘΕΩΡΙΑΣ ΤΗΣ ΚΑΘΗΜΕΡΙΝΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ" ("ROUTINE ACTIVITY THEORY").

Στον επίλογο του βιβλίου του «**Ψηφιακός κόσμος**» που εκδόθηκε το 1995, ο Nicholas Negroponte γράφει κατά λέξη τα εξής:

«Είμαι εκ φύσεως αισιόδοξος. Εντούτοις, κάθε τεχνολογία ή δώρο της επιστήμης έχει και μια σκοτεινή πλευρά. Ο ψηφιακός κόσμος δεν αποτελεί εξαίρεση σ'αυτό τον κανόνα. Η επόμενη δεκαετία θα γνωρίσει περιπτώσεις κατάχρησης πνευματικής ιδιοκτησίας και εισβολής στην προσωπική μας ζωή. Θα γνωρίσουμε ψηφιακούς βανδαλισμούς , πειρατείες λογισμικού και κλοπές δεδομένων……»

Παρατηρώντας τη διάδοση που έχουν σήμερα τα ψηφιακά (ηλεκτρονικά) εγκλήματα που αναφέρονται παραπάνω, βλέπουμε πως ο συγγραφέας και καθηγητής του Μ.Ι.Τ. δικαιώθηκε απόλυτα στις προβλέψεις του αυτές..

Ποιο είναι όμως το ψηφιακό έγκλημα; Ποιος το διαπράττει; Ποια θα μπορούσε να είναι η ερμηνευτική του προσέγγιση; Απάντηση στα ερωτήματα αυτά θα προσπαθήσσουμε να δώσουμε στη συνέχεια.

Ετσι, ως **ψηφιακό έγκλημα (digital crime)** θα μπορούσε να θεωρηθεί *κάθε παράνομη πράξη για τη διάπραξη,αλλά και για την αντιμετώπιση της οποίας θεωρείται απαραίτητη η γνώση της ψηφιακής τεχνολογίας*.

Τα ψηφιακά εγκλήματα διαφέρουν από τα παραδοσιακά εγκλήματα στα εξής χαρακτηριστικά σημεία:

- Διαπράττονται συνήθως από μακρινή απόσταση,

- Ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος,
- Αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη τους,
- Ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος
- Οι οικονομικές απώλειες που προξενούνται στα "ψηφιακά" θύματα είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων και
- Στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμμία επίσημη αρχή δηλ. ο "σκοτεινός αριθμός" τους είναι ιδιαίτερα σημαντικός.

Τα τέσσερα δε τελευταία από τα παραπάνω χαρακτηριστικά τους πιστεύουμε ότι τα κατατάσσουν στο χώρο των **οικονομικών εγκλημάτων.**

"Τόπος" τέλεσής τους είναι ο αποκαλούμενος **κυβερνοχώρος.**

Το σύνολο επομένως, *των ψηφιακών εγκλημάτων που τελούνται στον κυβερνοχώρο (cyberspace) συνιστούν την* **ψηφιακή ή ηλεκτρονική εγκληματικότητα (digital criminality).**

Ποια είναι όμως ειδικότερα τα ψηφιακά εεγκλήματα;

Κατά τη γνώμη μας, τα ψηφιακά εγκλήματα, θα μπορούσαμε να τα χωρίσουμε σε **δύο** μεγάλες κατηγορίες με κριτήριο τα μέσα τέλεσης και εξιχνίασής τους. Έτσι έχουμε,

α.- Τα **γνήσια** ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, **αποκλειστικά και μόνο** με τη χρήση της ψηφιακής τεχνολογίας και

β.- Τα **παραδοσιακά ε**γκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, **τόσο με την υποστήριξη της ψηφιακής τεχνολογίας όσο και χωρίς τη βοήθειά της**.

Με βάση τη διάκριση αυτή στην **πρώτη** από τις παραπάνω κατηγορίες θεωρούμε ότι μπορεί να υπαχθούν :

1.- Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking),

2.- Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ,

3.- Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης "επίθεσης άρνησης παροχής υπηρεσιών" (Denial of service attack – DoS)

4.- Η διασπορά κακόβουλων προγραμμάτων (όπως, ιών (virus), σκουληκιών (worms), Δούρειων Ιππων (Trojan Horses – Trojans), dialers κλπ.) και

5.- Η πειρατεία λογισμικού δηλ.προγραμμάτων Η/Υ που αφορά την παράνομη αντιγραφή τους και τη στη συνέχεια διάθεσή τους στην αγορά – και μέσω του Διαδικτύου - σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου.

Στη **δεύτερη** κατηγορία των παραδοσιακών εγκλημάτων που τελούνται **και με τη χρήση της ψηφιακής τεχνολογίας,** πιστεύουμε ότι μπορεί να υπαχθούν :

1.- Διάφορα **κοινά** εγκλήματα. Σαν τέτοια μπορούμε να αναφέρουμε π.χ. την *κλοπή ενός Η/Υ ή τμημάτων του* – μνήμης, μητρικής κλπ.- ή *περιφερειακών* του – εκτυπωτών, σκάνερς κλπ.- Στην κατηγορία αυτή ανήκουν επίσης και εγκλήματα που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου (e–mail) ή ιστοσελίδων (websites), όπως *απάτες (π.χ. Νιγηριανή απάτη, "ψάρεμα¨/phishing mail), εξυβρίσεις, εκβιασμοί, δυσφημίσεις, πωλήσεις απαγορευμένων προϊόντων (ναρκωτικών, μη εγκεκριμένων φαρμάκων), παροχή υπηρεσιών call-girls, η κυκλοφορία πορνογραφικού υλικού* – που αφορά κυρίως ανηλίκους (παιδική πορνογραφία) – καθώς *και η παρενόχληση χρηστών με ανεπιθύμητα διαφημιστικά μηνύματα (spamming)*. Εδώ υπάγονται επίσης, κατά τη γνώμη μας και οι *προσβολές της πνευματικής ιδιοκτησίας, οι*

*ανταλλαγές πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου μεταξύ τρομοκρατικών οργανώσεων αλλά και συμμοριών του οργανωμένου εγκλήματος καθώς και το ηλεκτρονικό ξέπλυμα βρώμικου χρήματος***.**

2.- **Η κατασκοπεία** είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική και

3.- **Οι υποκλοπές** τηλεφωνικών συνομιλιών που έχουν σαν συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων.

Λαμβάνοντας στη συνέχεια υπόψη την παραπάνω διάκριση των ψηφιακών εγκλημάτων, σε γνήσια και σε παραδοσιακά που τελούνται με τη χρήση της ψηφιακής τεχνολογίας, θα πρέπει να πούμε πως ιδιαίτερη κατηγορία εγκληματικής συμπεριφοράς, που χρήζει παραπέρα ανάλυσης, αποτελεί εκείνη την οποία επιδεικνύει **ο δράστης των γνήσιων ψηφιακών εγκλημάτων**. Αυτός δραστηριοποιείται αποκλειστικά στον κυβερνοχώρο και αυτός χρησιμοποιεί αποκλειστικά και μόνο την ψηφιακή τεχνολογία για να παραβεί το νόμο. Τα από εγκληματολογική άποψη χαρακτηριστικά των δραστών των παραδοσιακών εγκλημάτων – εκβιαστών, απατεώνων, τρομοκρατών κλπ. – είναι ήδη γνωστά και δεδομένα και δεν αλλάζουν από το γεγονός ότι αλλάζει ο τόπος – "κυβερνοχώρος/Διαδίκτυο" - και το μέσο εκδήλωσης - "ψηφιακή τεχνολογία" - της εγκληματικής τους συμπεριφοράς. Με βάση τις παραπάνω σκέψεις μας θα θεωρήσουμε λοιπόν, **ως ψηφιακό εγκληματία εκείνον που διαπράττει τα γνήσια ψηφιακά εγκλήματα.**

Ο ψηφιακός αυτός εγκληματίας είναι γνωστός τόσο στο ευρύ κοινό όσο και στη βιβλιογραφία αλλά και στα ΜΜΕ κυρίως ως **Hacker** αλλά και ως C**racker (σπάστης)** ή C**yberpunk (κεβερνοπάνκ)**.

Ο **Donn Parker** (1998), ειδικός σε θέματα ασφάλειας Η/Υ υποστηρίζει για τους ψηφιακούς εγκληματίες τις ακόλουθες απόψεις:

- Οι άνθρωποι αυτοί διαφέρουν μεταξύ τους ανάλογα με τις δεξιότητες, τη γνώση, τους πόρους και τα κίνητρά τους.

- Οι ψηφιακοί εγκληματίες μπορούν να έχουν διαφορετικά επίπεδα ικανοτήτων που στηρίζονται στη βασική τους εκπαίδευση, τις κοινωνικές τους αλληλεπιδράσεις και στην εμπειρία τους στη χρήση των ηλεκτρονικών υπολογιστών.
- Υπάρχουν τρεις κατηγορίες ψηφιακών εγκληματιών: οι κατασκευαστές εργαλείων, οι χρήστες εργαλείων και οι συγγραφείς προγραμμάτων.
- Τα κίνητρά τους περιλαμβάνουν την πλεονεξία, την ανάγκη (για να λύσουν τα προσωπικά τους προβλήματα, όπως η πληρωμή χρεών από τυχερά παιχνίδια), την αδυναμία να κατανοήσουν τη ζημιά που προξενούν σε άλλους, την προσωποποίηση των υπολογιστών (τους θεωρούν ως αντιπάλους τους σε ένα παιχνίδι) και το σύνδρομο του Robin Hood (που τους κάνει να βλέπουν τις εταιρίες τόσο πλούσιες ώστε η οικονομικές ζημιές που τους προκαλούν να δικαιολογούνται ηθικά).
- Πολλοί από αυτούς θεωρούν ότι η απλή εισβολή σε συστήματα Η/Υ, ο βανδαλισμός τους ή η προφανής παραβίαση της εμπιστευτικότητάς τους είναι ένα αβλαβές και ηθικά αποδεκτό χόμπι.
- Μερικοί πάλι θεωρούν ότι η εισβολή σε συστήματα Η/Υ έχει και τη θετική της πλευρά με την έννοια ότι με τον τρόπο αυτό συμβάλλουν στη βελτίωση της ασφάλειάς τους.
- Οι περισσότεροι ενεργοί ψ.έ. είναι νέοι άνδρες, ηλικίας 12 έως 24 ετών.
- Πολλοί γονείς ανήλικων ψ.έ. δεν έχουν καμία ιδέα για το τι κάνουν τα παιδιά τους με τον ακριβό εξοπλισμό υπολογιστών που τους έχουν κάνει δώρο.

- Μερικοί υποστηρικτές των ψ.έ. κατηγορούν τα θύματα τους για τα ανεπαρκή μέτρα ασφάλειας που έχουν λάβει και ελαχιστοποιούν τα ηθικά ζητήματα που τυχόν προκύπτουν.
- Μερικοί τέλος, υποστηρικτές των χάκερ περιγράφουν τις επιθέσεις τους ως δικαιολογημένες διαμαρτυρίες ή ως άμεση δράση ενάντια στους εχθρούς του περιβάλλοντος ή της κοινωνίας γενικά.

Ένα συνηθισμένο slogan των hackers που είναι το ότι « **Η γνώση αποτελεί δύναμη** » και το οποίο αποδίδεται στον Αγγλο φιλόσοφο και πολιτικό του 17ου αιώνα **Francis Bacon**, εκφράζει με τον καλύτερο τρόπο τις αντιλήψεις τους. Η γνώση είναι βέβαιο ότι δίνει τη μεγαλύτερη δύναμη σ' όσους την κατέχουν και μάλιστα στη σημερινή εποχή με τις χιλιάδες βάσεις δεδομένων τις οποίες διαχειρίζονται κυβερνητικοί οργανισμοί και επιχειρήσεις και για την πρόσβαση των οποίων είναι απαραίτητο το Internet. Ιδού λοιπόν ο χώρος στον οποίο ο hacker θα ξεδιπλώσει σήμερα τις απεριόριστες - όπως υποστηρίζει - ικανότητές του!

Υποστηρίζεται ότι μια επιχείρηση ή ένας οργανισμός που είναι τα συνήθη **θύματα** των ψηφιακών εγκληματιών, μπορούν να αναζητήσουν τους ψ.έ. που έχουν τη δυνατότητα να προσβάλλουν τα συστήματά τους, σε μία από τις ακόλουθες πέντε κατηγορίες ατόμων :

α.- Στους φοιτητές Πανεπιστημίων και Κολεγίων καθώς και στους μαθητές της μέσης εκπαίδευσης.

β.- Ανάμεσα στους υπαλλήλους τους,

γ.- Σε εκείνους που κινούνται στον υπόκοσμο των Η/Υ,

δ.- Σε παλιούς εγκληματίες από τον κόσμο των ναρκωτικών και του οργανωμένου εγκλήματος και τέλος

ε.- Στους επαγγελματίες που έχουν ως αντικειμενό τους τη βιομηχανική κυρίως, κατασκοπεία και οι οποίοι εργάζονται για λογαριασμό των ανταγωνιστών τους.

Θα πρέπει να σημειώσουμε ακόμη πως η **επικινδυνότητα** των ψ.έ. εξαρτάται από τα **κίνητρά** τους.

Η σύγχρονη πρακτική θέλει ένα αρκετά μεγάλο αριθμό από τους σημερινούς ψ.έ. να έχει οικονομικά κίνητρα πράγμα που αυτόματα αυξάνει και τον επικίνδυνο χαρακτήρα τους.

- Η προληπτική αποτροπή του μεγαλύτερου αριθμού των ψηφιακών εγκλημάτων είναι δύσκολη, ανεξαρτήτως του πόσο λεπτομερειακούς νόμους και πόσο αυστηρούς ελεγκτικούς μηχανισμούς δημιουργεί ένα κράτος ή πόσο προηγμένη τεχνολογία διαθέτει. Πέραν της αναποτελεσματικότητας μιας τέτοιας προσέγγισης, οι ζημιές για τη δημοκρατία, το εμπόριο και την εξέλιξη της τεχνολογίας, θα μπορούσαν να ήταν πολύ μεγάλες. Η αποτελεσματική εξιχνίαση των ψηφιακών εγκλημάτων και η σωστή απόδοση δικαιοσύνης, είναι η καταλληλότερη προσέγγιση και για την αποτροπή τους. Προς αυτήν την κατεύθυνση, οι διωκτικές αρχές είναι επιφορτισμένες με το έργο να προστατέψουν τους φιλόνομους πολίτες, οδηγώντας τους συστηματικούς παραβάτες στη δικαιοσύνη.

Σχετικά με την ερμηνευτική προσέγγιση της εγκληματικής αυτής συμπεριφοράς της οποίας το ιδιάζον χαρακτηριστικό είναι η υλοποίησή της στον κυβεερνοχώρο και εφόσον δεχθούμε πως οι εγκληματογόνοι παράγοντες της εικονικής πραγματικότητας του κυβερνοχώρου δεν παρουσιάζουν σημαντικές διαφορές από τους αντίστοιχους παράγοντες που επικρατούν στον υλικό κόσμο, έχουμε την άποψη πως και η ερμηνεία της μπορεί να θεμελιωθεί με βάση κάποια από τις θεωρίες που χρησιμοποιούνται για την θεμελίωση της αντίστοιχης συμπεριφοράς που καταγράφεται και στον υλικό κόσμο.

Σαν τέτοια επιλέξαμε αυτή που είναι γνωστή ως η "θεωρία της καθημερινής δραστηριότητας" (Routine Activity Theory), την οποία διετύπωσαν οι Larry Cohen και Marcus Felson, tto 1979 (βλ. σχετ. μ.ά. **Felson M., (2003), Crime and Everyday Life, 3rd ed., London, Sage)**.
Σύμφωνα με αυτήν, όπως είναι γνωστό, ένα έγκλημα – κυρίως κατά της ιδιοκτησίας – που αποτελεί ένα καθημερινό φαινόμενο, συμβαίνει όταν υπάρξει σύμπτωση στο χρόνο και στον τόπο των ακόλουθων τριών παραγόντων:

- ενός πιθανού δράστη ("a likely offender)
- ενός κατάλληλου στόχου ("a suitable target") και
- της απουσίας των απαραίτητων για την αποτροπή του εγκλήματος μέτρων φύλαξης ("the absence of a capable guardian against crime")

Με βάση τα παραπάνω υποθέτουμε πως και το ψηφιακό έγκλημα αποτελεί ένα βασικό στοιχείο της καθημερινότητας του κυβερνοχώρου, το γεγονός δε που το ευνοεί, αποτελεί ένα συνδυασμό της ταυτόχρονης ύπαρξης των ακόλουθων τριών "παραγόντων":
α.- ενός δράστη (hacker,cracker) με τις κατάλληλες τεχνολογικές γνώσεις και τα απαραίτητα κίνητρα (π.χ. οικονομικό κέρδος, επίδειξη γνώσεων) για να διαπράξει ένα ψηφιακό έγκλημα,
β.- ενός κατάλληλου στόχου – θύματος, όπως είναι το πληροφοριακό σύστημα μιας επιχείρησης, μιας τράπεζας, ενός γνωστού οργανισμού, ή ενός απλού ιδιώτη – χρήστη, γνωστού ή οικονομικά εύρωστου και
γ.- η απουσία ή η ανεπάρκεια των μέσων προφύλαξης/πρόληψης, όπως τα συνήθη μέτρα ασφαλείας (δηλ. τα "τείχη προστασίας", η κρυπτογράφηση των δεδομένων και κατά κύριο λόγο τα λεγόμενα αντιικά προγράμματα) που έχει τη δυνατότητα ναα λάβει προκειμένου να προστατεύσει το πληροφοριακό του σύστημα το υποψήφιο θύμα.

Θα πρέπει δε να παρατηρήσουμε πως όσον αφορά την άσκηση μιας αποτελεσματικής αντεγκληματικής πολιτικής στην συγκεκριμένη περίπτωση των ψηφιακών εγκλημάτων η οποία έχει να κάνει με τον "έλεγχο" του καθενός από τους παράγοντες αυτούς πως,

α.- Ο πρώτος αφορά τη σχέση ανθρώπου – Η/Υ και τη στάση και τις απόψεις του πρώτου για τη λειτουργία και την αποστολή που επιτελεί ο δεύτερος. Για το λόγο αυτό ο παράγων αυτός θα πρέπει να θεωρηθεί αστάθμητος και έτσι ο άμεσος και προληπτικός έλεγχός του φαντάζει αρκετά δύσχερής.

β.- Ο δεύτερος δηλ. το πληροφοριακό σύστημα – πιθανό θύμα είναι αναγκαίο "κακό". Τα οφέλη που προκύπτουν από τη χρήση του είναι προφανή και πλέον αδιαμφισβήτητα, ιδίως εφόσον πρόκειται για τη συμβολή του συστήματος στην λειτουργία επιχειρήσεων και οργανισμών που αφορούν δραστηριότητες όπως π.χ. το ηλεκτρονικό εμπόριο, το ηλεκτρονικό ταχυδρομείο, την ηλεκτρονική μάθηση από απόσταση, την τηλειατρική, τις τηλεδιασκέψεις κλπ που θεωρούνται απαραίτητες στις εμπορικές και μη συναλλαγές της σημερινής ψηφιακής εποχής.

γ.- Ο τρίτος όμως από τους παραπάνω παράγοντες είναι εκείνος που αν προσεχθεί ιδιαίτερα θα μπορέσει να συμβάλλει στη μείωση των ψηφιακών εγκλημάτων. **Η λεπτομερής και ακριβής τήρηση των κατάλληλων μέτρων ασφαλείας όπως π.χ. των αντιικών προγραμμάτων, των "τειχών προστασίας" και της κρυπτογράφησης των δεδομένων, όλων μαζί ή και του καθενός ξεχωριστά, αποτελεί το μόνο μέσο περιορισμού των επιτυχημένων επιθέσεων που μπορεί να δεχθεί ένα πληροφοριακό σύστημα είτε το υποψήφιο θύμα είναι ιδιώτης ή επιχείρηση ή οργανισμός.** Μιλάμε φυσικά για "μείωση" και "περιορισμό" και όχι για ολοσχερή εξάλειψη της συγκεκριμένης απειλής μια και η ψηφιακή εγκληματικότητα όπως και η παραδοσιακή, απλά και μόνο μπορεί να περιορισθεί και όχι να εξαληφθεί εντελώς. Εξάλλου,

όπως έχει προσφυώς λεχθεί ο μόνος εντελώς ασφαλής Η/Υ είναι αυτός που δεν είναι στην πρίζα. Εμείς θα προσθέταμε, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις που αφορούν τους φορητούς Η/Υ και τα ασύρματα δίκτυα και εφόσον δεν είναι συνδεδεμένος και σε κανένα δίκτυο……