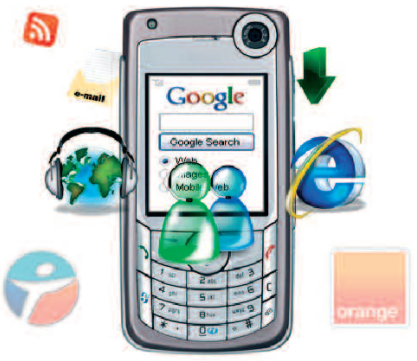
ΗΛΕΚΤΡΟΝΙΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

διερευνώντας το έγκλημα στον κυβερνοχώρο

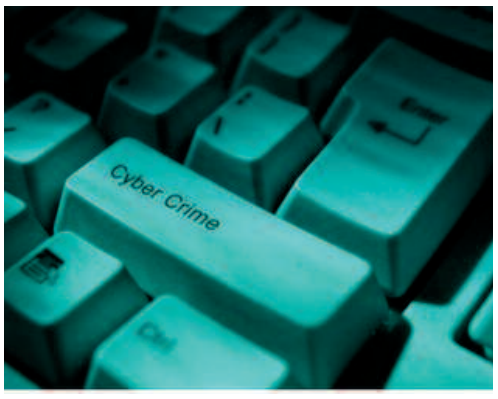
του Γιώργου Χλαπουτάκη

Η είσοδος των ηλεκτρονικών υπολογιστών και του Παγκόσμιου Ιστού στην καθημερινότητα και στα χέρια του κάθε πολίτη, ανεξαρτήτως , εθνικότητας και τόπου διαμονής , έφερε την δύναμη της γνώσης και της ενημέρωσης στον κόσμο. Όπως είναι λογικό το έγκλημα ακολούθησε, όπως και ο νόμος και η Αστυνομία και η Εγκληματολογία. Καλώς ορίσαμε, λοιπόν, στην εποχή του ηλεκτρονικού εγκλήματος και της Ηλεκτρονικής Εγκληματολογίας.

Απο την στιγμή της αρχικής τους επινόησης, οι ηλεκτρονικοί υπολογιστές βρήκαν άπειρες χρήσεις σε εξίσου άπειρα πεδία χρήσης. Η τρομερή πρόοδος της επιστήμης και της τεχνολογίας κατέληξε στην δραστικότατη μείωση του μεγέθους των συσκευών που κάνουν χρήση της τεχνολογίας αυτής και, συγχρόνως, την εξίσου δραστικότατη αύξηση των δυνατοτήτων τους



Εν έτει 2008, βλέπουμε τηλεόραση, και τις φωτογραφίες απο την τελευταία μας εκδρομή, διαβάζουμε την εφημερίδα μας, πάμε στην τράπεζα,ψωνίζουμε ρούχα και δώρα για εμάς και τους δικούς μας, μιλάμε με τους φίλους μας, επισκεπτόμαστε συγγενείς και φίλους σε διαφορετικά μέρη, συνάπτουμε τις επαγγελματικές συμφωνίες μας, παρουσιάζουμε την δουλειά μας, φτιάχνουμε το πρωϊνό μας γεύμα μέσω του Internet και των συσκευών που μας επιτρέπουν να συνδεθούμε με τον Παγκόσμιο Ιστό. Με άλλα λόγια, έχουμε γίνει μια κοινωνία που εξαρτάται πλέον, σε καθημερινή βάση και με πολλαπλούς τρόπους, απο τους ηλεκτρονικούς υπολογιστές και το Internet για την διεκπεραίωση των επαγγελματικών, προσωπικών και διαπροσωπικών συναλλαγών μας.



Ιστορικά μιλώντας, το έγκλημα, οι αυτουργοί του και οι ενέργειες που διαπράττουν, ακολουθούν σταθερά την τεχνολογία και πολλές φορές την προάγουν.Είναι, επομένως, λογικό στην σημερινή εποχή να βλέπουμε το ολοένα και αυξανόμενο φαινόμενο της διάπραξης εγκληματικών ενεργειών με την χρήση ηλεκτρονικών υπολογιστών ή/και την χρήση του Internet. Εξίσου λογικό, λοιπόν, είναι να αναγκαστεί και η διεθνής εγκληματολογική και αστυνομική κοινότητα να προσαρμοστεί στην νέα αυτή πραγματικότητα, με περεταίρω εκπαίδευση και κατάρτιση στην μεταφορά αυτή των εγκλημάτων απο την φυσική πραγματικότητα στην «εικονική πραγματικότητα» του κυβερνοχώρου.

ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΑ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΚΛΗΜΑΤΟΛΟΓΙΑΣ	
1984	*Πρόγραμμα Μαγνητικού Υλικού του FBI*
1993	*1ο Παγκόσμιο Συνέδριο σε Στοιχεία Ηλ. Υπολογιστών*
1995	*Δημιουργία του Παγκόσμιου Οργανισμού Αποδεικτικών Στοιχείων Ηλ. Υπολογιστών (IOCE)*
1997	*Κλήση του IOCE και της G8 για πρότυπα*
1998	*Η G8 δίνει την εποπτεία του θέματος στον IOCE και το πρώτο Συμπόσιο Εγληματολογίας της INTERPOL για το θέμα του Ηλ. Εγκλήματος*
1999	*1ο Παγκόσμιο Συνέδριο Προηγημένου Εγκλήματος και Εγκληματολογίας (IHCFC) και σχέδια προτύπων παρουσιάζονται στο G8*
2000	*Πρώτο Εργαστήριο Ηλ. Εγκληματολογίας του FBI*

Όπως βλέπουμε στον παραπάνω πίνακα, λοιπόν, η Ηλεκτρονική Εγκληματολογία, ώς επιστήμη, είναι αρκετά νέα στον χώρο της Εγκληματολογίας (που ουσιαστικά υπάρχει απο τον 18ο με 19ο αιώνα), και είναι ουσιαστικά μείγμα κλασσικής Εγκληματολογίας και Επιστήμης Ηλ. Υπολογιστών.

Στο σημείο αυτό, ίσως θα ήταν καλύτερο να εξηγήσουμε τί πραγματικά ενοούμε όταν χρησιμοποιούμε τους ορισμούς «ηλεκτρονικό έγκλημα», «ηλεκτρονικά στοιχεία» και «ηλεκτρονική εγκληματολογία».

Ξεκινώντας με τον όρο «ηλεκτρονικά στοιχεία», ο Eoghan Casey, απο τους προτοπόρους της Ηλεκτρονικής Εγκληματολογίας ορίζει στο βιβλίο του οτι αποτελούνται απο «οποιαδήποτε δεδομένα, αποθηκευμένα σε ή μεταδιδόμενα μέσω Ηλ. Υπολογιστή που είτε υποστηρίζουν ή καταρρίπτουν μια θεωρία που αφορά τον τρόπο διάπραξης ενός εγκλήματος, είτε αφορούν συγκεκριμένα κρίσιμα στοιχεία του εγκλήματος όπως πρόθεση ή άλλοθι» (Casey 2004).

Με δεδομένο τον παραπάνω όρο, λοιπόν, «ηλεκτρονικό στοιχείο» μπορεί πχ. να θεωρηθεί ένα έγγραφο που γράφτηκε στον κειμενογράφο Microsoft Word, ένας πίνακας οικονομικών στοιχείων του Excel, μια διαδικτυακή σελίδα που είδε , ένα παιχνίδι που εγκατέστησε ή κατέβασε απο το Internet, μια εικόνα που κατέβασε κάποιος , κ.ο.κ.. Οτιδήποτε δηλαδή περιέχεται ή μεταφέρθηκε με οποιοδήποτε μέσο ή τρόπο σε έναν υπολογιστή.

Επομένως, «Ηλεκτρονική Εγκληματολογία» είναι ο κλάδος της Επιστήμης της Εγκληματολογίας που ασχολείται με την «χρήση ειδικών τεχνικών και τεχνολογιών για την αποκατάσταση, επικύρωση και ανάλυση ηλεκτρονικών δεδομένων όταν μια νομική υπόθεση περιλαμβάνει θέματα που έχουν σχέση με την αναδημιουργία της χρήσης , την ανάλυση των δεδομένων που αφήνει πίσω η χρήση ενός ηλ. Υπολογιστή, την επικύρωση των δεδομένων αυτών μέσω τεχνικών αναλύσεων ή την εξήγηση τεχνικών γνωρισμάτων των δεδομένων και της χρήσης του ηλ. Υπολογιστή».

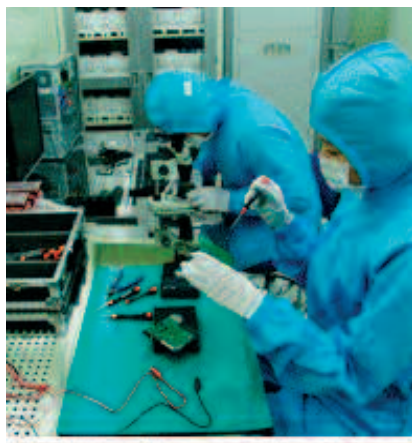
Ο Angus Marshall (Marshall 2008) στο βιβλίο του «Ηλεκτρονική Εγκληματολογία», πολύ σωστά αναφέρει οτι η ηλεκτρονική εγκληματολογία διαφέρει ώς κλάδος απο τους υπόλοιπους κλάδους που απαρτίζουν το πεδίο της γενικότερης Εγκληματολογίας στο οτι το είδος των αποδεικτικών στοιχείων υπο έρευνα είναι προϊόν ανθρώπινης ιδιοφυϊας. Εμβαθύνοντας, αναφέρει οτι αντίθετα με τα στοιχεία που αφήνει μια βιολογική οντότητα σε μια σκηνή εγκλήματος, τα ηλεκτρονικά στοιχεία είναι εφήμερα απο την άποψη του οτι βασίζονται σε μια τεχνολογία που αλλοιώνεται και ανανεώνεται με τρομακτικό ρυθμό.

Ο ορισμός «Ηλεκτρονικό Εγκλημα» αφέθηκε τελευταίος απλούστατα γιατί είναι ο πιό πολύπλοκος και συνάμα ο πιό παρανοημένος και παρερμηνευμένος. Και αυτό γιατί αυτή την στιγμή δεν υπάρχει κάποιος πλήρης και πλήρως αποδεκτός ορισμός της συγκεκριμένης έννοιας.

Παραδείγματος χάριν, η Ευρωπαϊκή Κοινότητα, σύμφωνα με την Συνθήκη κατά του Ηλεκτρονικού Εγκλήματος (ETS No. 185) ορίζει το Ηλεκτρονικό ΄Εγκλημα ώς «οποιαδήποτε εγκληματική ενέργεια διεπράχθη εναντίον ή με την βοήθεια ενός ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών», ενώ ο ορισμός που δίνει η Βρεττανική Αστυνομία (BBC News, 2001) είναι «η χρήση ηλ. υπολογιστή ή δικτύου ηλ. Υπολογιστών για την διάπραξη εγκλήματος».

Στην Ελλάδα, σύμφωνα με άρθρο του Κωσταντίνου Κούρου στην "Αστυνομική Ανασκόπηση", ο ορισμός που δίδεται είναι ο εξής "Ως «Ηλεκτρονικό ΄Εγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου."

Παρόμοιους ορισμούς που βασίζονται στα πλαίσια των παραπάνω βλέπουμε λίγο-πολύ και σε κάθε άλλη χώρα του κόσμου.



Τα πιό συνηθισμένα εγκλήματα που καλείται, λοιπόν να αντιμετωπίσει η Ηλεκτρονική Εγκληματολογία μπορούνε να χωριστούνε με διάφορους τρόπους, σε κάθε έναν απο τους οποίους ο υπολογιστής και το internet κατέχουν έναν ή και περισσότερους ρόλους.

Άν τα χωρίσουμε, πχ. σε τύπους εγκλημάτων, μπορούμε να μιλήσουμε για εγκλήματα παράνομης διείσδυσης σε ηλ. Υπολογιστές και δίκτυα (cracking), εγκλήματα παράνομης απόκτησης προσωπικών δεδομένων (phishing), παράνομης επίθεσης σε υπολογιστές και δίκτυα υπολογιστών με σκοπό την άρνηση εξυπηρέτησης (Denial/Distributed Denial of Service επιθέσεις), διάδοσης ιών ηλ. Υπολογιστών, πειρατείας ιδιόκτητου υλικού/λογισμικού, μουσικής και video (copyright crime), εγκλήματα κατοχής και διάδοσης συγκεκριμένων ειδών πορνογραφίας, με ιδιέταιρη έμφαση σε υλικό παιδικής πορνογραφίας, εγκλήματα απάτης πιστωτικών καρτών (Credit Card Fraud), και εγκλήματα εκβιασμού, δυσφήμησης, καταδίωξης, όπως επίσης και εγκλήματα κυβερνο-τρομοκρατίας.

Είναι σημαντικό, σε αυτό το σημείο, να ειπωθεί οτι τα περισσότερα απο αυτά τα εγκλήματα είναι εγκλήματα που διαπράττονται και διαπράττονταν ανέκαθεν στον κόσμο, χωρίς την βοήθεια ή την χρήση ηλ. Υπολογιστη.

Αυτό μας δείχνει οτι η διάπραξη των περισοτέρων αυτών εγκλημάτων δεν προήλθε απο την χρήση ηλ. Υπολογιστή ή του Internet αλλά απλά μεταφέρθηκαν εκεί για λόγους ευκολίας μετάδοσης, ανωνυμίας και εύρους διάδοσης, πράγμα που είναι λογικό και φυσιολογικό.

Σε κάθε ένα απο αυτά τα εγκλήματα, ανάλογα με το είδος και τον τρόπο χρήσης του ηλ. Υπολογιστή και του Internet, μπορούμε να διαχωρίσουμε τον ρόλο του ηλ. Υπολογιστή ανάλογα με τον τρόπο με τον οποίον χρησιμοποιήθηκε. Αυτό επιτρέπει τόσο την απλούστερη έρευνα και διαχείρηση των υπολογιστών που έχουν μεταφερθεί σε ένα αστυνομικό εργαστήριο για ανάλυση όσο και την ευκολότερη ταξινόμηση των αποδεικτικών στοιχείων πρό της παρουσίασης τους σε δικαστήριο, καθώς επίσης και την ευκολότερη κατάταξη της επικινδυνότητας του εγκληματία σύμφωνα με τα ευρήματα της έρευνας.

Σύμφωνα με τον Casey, λοιπόν, μπορούμε να διαχωρίσουμε τον ρόλο του ηλ. Υπολογιστή σε εγκλήματα στα οποία ο υπολογιστής είναι το αντικείμενο, το υποκείμενο, το εργαλείο και το σύμβολο του εγκλήματος.

Πληρέστερο σύνδεσμο μεταξύ των εγκλημάτων και του είδους και τρόπου χρήσης του ηλ. Υπολογιστή μας δίνει ο Marshall, όμως, όπως βλέπουμε στον παρακάτω πίνακα.

Ρόλος ηλ. Υπολογιστή στο έγκλημα					
	Μάρτυρας	Εργαλείο	Σύνεργος	Προστάτης	Θύμα
Ανοιχτό	ΑΜ	ΑΕ	ΑΣ	ΑΠ	ΑΘ
Κλειστό	ΚΜ	ΚΕ	ΚΣ	ΚΠ	ΚΘ

Ο Marshall (Marshall, 2008; Bryant & Marshall, 2008), λοιπόν, χωρίζει τον υπολογιστή σε Ανοιχτό (συνδεδεμένο στο Internet) και Κλειστό (αυτόνομο) σύστημα. Ένα ανοιχτό σύστημα, αναφέρει, είναι πολύ πληρέστερη πηγή πληροφοριών και εγκληματολογικών στοιχείων απο ένα κλειστό, και άρα και πιο ενδιαφέρον για τον ερευνητή.

Επίσεις, κατηγοριοποιεί τον υπολογιστή, ανάλογα με τον ρόλο που εκπληρώνει σε ένα έγκλημα, σε Μάρτυρα (έμμεσος σύνδεσμος που μπορεί να περιέχει στοιχεία για το έγκλημα), Εργαλείο (άμμεσος σύνδεσμος, χρησιμοποιούμενος απο τον εγκληματία για την διάπραξη του εγκλήματος), Σύνεργος(άμεσος σύνδεσμος και απαραίτητος για την διάπραξη του συγκεκριμένου εγκλήματος), Προστάτης (προστατεύει το θύμα απο τον εγκληματία, πχ. σύστημα ανίχνευσης εισβολής), και Θύμα (στόχος του εγκληματία κατά την διάπραξη του εγκλήματος).

Παραδείγματος χάρην, σε μια υπόθεση απλής παράνομης αντιγραφής CD/DVD στην οποία ο υπολογιστής δεν ήταν συνδεδεμένος σε δίκτυο υπολογιστών, μπορούμε να πούμε οτι ο υπολογιστής είναι Κλειστός Μάρτυρας (ύπαρξη καταγραφής της διαδικασίας αντιγραφής στο λογισμικό αντιγραφής), Κλειστός Σύνεργος (χωρίς τον υπολογιστή και το πρόγραμμα αντιγραφής δεν θα γινόταν η αντιγραφή), και Κλειστός Προστάτης (το CD/DVD που αντεγράφει περιείχε πρόγραμμα προστασίας αντιγραφής).

Έως τώρα, έχουμε αναφερθεί στους τύπους του ηλεκτρονικού εγκλήματος και στους ρόλους τους οποίους μπορεί να κατέχει ένας ηλ. Υπολογιστής σε αυτά. Το στοιχείο στο οποίο δεν έχουμε μέχρι τώρα αναφερθεί, και το οποίο είναι ίσως το σημαντικότερο πρόβλημα που αντιμετωπίζει η Επιστήμη της Ηλεκτρονικής Εγκληματολογίας, είναι η τοποθεσία. Συγκεκριμένα, η τοποθεσία του θύματος, και του θύτη, και η τοποθεσία των υπολογιστών των δύο παραπάνω, η τοποθεσία του εγκλήματος, δηλαδή.

Για τους αναγνώστες που δεν έχουν σχέση με το αστυνομικό επάγγελμα: Ένας Έλληνας εγκληματίας, διαμένων στην Ελλάδα, διαπράττει κάποιο έγκλημα μέσω Internet εναντίον μιας Αμερικάνικης επιχείρησης και αναμεταδίδει το έγκλημα μέσω Αγγλίας, Γαλλίας, Ρωσσίας, Ινδίας, Κίνας και Λιθουανίας. Πού (σε ποιά χώρα) ακριβώς λαμβάνει τόπο η επίθεση; Στην Ελλάδα, στην οποία βρίσκεται ο θύτης, στην Αμερική που βρίσκεται το θύμα, ή στην Αγγλία, στην Γαλλία, στην Ρωσσία, στην Ινδία, στην Κίνα και στην Λιθουανία; Ακόμα και άν, σε ένα ουτοπικό σύμπαν, μπορούσαμε να εντοπίσουμε την ακριβή διαδρομή που πήρε η επίθεση, ποιανής χώρας το νομικό σύστημα θα χρησιμοποιήσουμε; Και είμαστε σύγουροι οτι το νομικό σύστημα πχ της Γαλλίας και της Ινδίας κρίνει την συγκεκριμένη πράξη του θύτη ώς επίθεση;

Η επιστήμη της Ηλεκτρονικής Εγκληματολογίας, αν και απο τις σχετικά καινούργιες και λιγότερο ώριμες επιστήμες στον κόσμο, είναι σίγουρα απο τις πιό ενδιαφέρουσες και απαραίτητες για την εποχή της ελεύθερης και απεριόριστης πληροφόρησης την οποία διανύουμε. Κάποτε, στην αρχή της επανάστασης που προκάλεσε η είσοδος του ηλεκτρονικού υπολογιστή και του Internet στην ζωή του απλού πολίτη, υπήρχε η ελπίδα και η θέληση για έναν τόπο χωρίς νόμους, περιορισμούς και σύνορα. Πλέον, ο κόσμος είναι διαφορετικός και ο Παγκόσμιος Ιστός το καινούργιο μέσο για την διάπραξη εγκλημάτων εικονικών μεν αλλά με προεκτάσεις στον φυσικό κόσμο. Η αστυνόμευση του, λοιπόν, είναι πλέον απαραίτητη, άν όχι αναγκαία.

Ο Γιώργος Χλαπουτάκης (g.chlapoutakis@tees.ac.uk)
είναι φοιτητής διδακτορικού σε Ηλεκτρονική Εγκληματολογία & Ασφάλεια Δικτύων και Ειδικός Καθηγητής Ηλεκτρονικής Εγκληματολογίας στο Πανεπιστήμιο του Teesside στην Αγγλία.

Βιβλιογραφία

Bryant R., Marshall A., (2008), "Investigating Digital Crime: Chapter 12 – Criminological & Motivational Perspectives", John Wiley & Sons, Ltd., Oxford, UK

Casey E., (2004), "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Second Edition", Elsevier Academic Press, London, UK

Marshall A., (2008), "Digital Forensics: Digital Evidence in Criminal Investigations", John Wiley & Sons, Ltd., Oxford, UK

Κούρος Κ.Γ., (2005), "Ηλεκτρονικό Έγγλημα", Αστυνομική Ανασκόπηση, Τεύχος 233/2005, (http://www.ecfpo.gr/forum/viewtopic.php?p=592&sid=bcb80d1581c5289c12daf7d66162ba85), Τελευταία αναφορά: 17/11/2008

BBC News, (2001), "Life of Crime: Part 5 – Cybercrime", BBC, UK, (http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm), Τελευταία αναφορά: 17/11/2008