«**Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του**»

Ιάκ. Φαρσεδάκης
Ομοτ. Καθηγητής Εγκληματολογίας Παντείου Πανεπιστημίου
19/5/2009

Το διαδίκτυο αποτελεί ένα **πολύ χρήσιμο εργαλείο**. Προσφέρει φθηνή και εύκολη πρόσβαση, ανά πάσα στιγμή, σε μια εκτεταμένη δεξαμενή πληροφοριών. **Εν τούτοις, με ένα δισεκατομμύριο χρήστες ανά την υφήλιο, με πρόσβαση σε 75 εκατομμύρια ιστοσελίδες, είναι δυνατό να επιτρέψει και μια παράνομη, ακόμη και επιθετική χρήση του, πράγμα που συμβαίνει καθημερινά, ολοένα και πιο συχνά.**
Αυτή είναι η **σκοτεινή πλευρά** του διαδικτύου. Δεν πρέπει να είναι κανείς αφελής για να το αρνηθεί, ούτε κινδυνολόγος για να υπερβάλλει σχετικά με τις απειλές που προέρχονται από την κακή χρήση του.
Το κυβερνοέγκλημα αναπτύσσεται ιδιαίτερα σε περιόδους οικονομικών κρίσεων και οικονομικής ύφεσης.

Φαίνεται, πάντως, πως οι άνθρωποι περνούν ευκολότερα σε μια εγκληματική δραστηριότητα στο διαδίκτυο, από ότι στον φυσικό κόσμο.
Το κυβερνοέγκλημα κατέστη η πιο προσοδοφόρα και επωφελής για τους εγκληματίες δραστηριότητα. Σε μια ειδική επιτροπή του αμερικανικού Κογκρέσου ειδικοί κατέθεσαν πως ξεπέρασε σε κέρδη και το εμπόριο των ναρκωτικών. Το ίδιο δηλώθηκε και από το FBI που υπολόγισε τα ανά την υφήλιο κέρδη από αυτό σε ένα τρισεκατομμύριο δολάρια.
Και ο σκοτεινός αριθμός σε αυτή την περίπτωση, όπως είναι φυσικό, είναι πολύ μεγάλος. Υπολογίζεται ότι μόνο το 15% αναφέρεται στις Αρχές.
Το 74% διαπράχθηκε μέσω ηλεκτρονικών μηνυμάτων και το υπόλοιπο μέσω ιστοσελίδων.

Χαρακτηριστικό παράδειγμα για να αντιληφθεί κανείς το **μέγεθος του προβλήματος**, μόνο σε ένα τομέα, αυτόν της παιδικής πορνογραφίας, είναι εκείνο της λεγόμενης **επιχείρησης «Ore» στη Βρετανία**. Μετά από την αποστολή από το FBI λεπτομερειών για 7300 θεωρούμενους ως Βρετανούς κατόχους πιστωτικών καρτών που βρέθηκαν εγγεγραμμένοι σε πορνογραφική ιστοσελίδα, οργανώθηκε επιχείρηση και **συνελήφθησαν 1300 άτομα**, μεταξύ των οποίων **δάσκαλοι, κοινωνικοί λειτουργοί, λειτουργοί παροχής φροντίδων υγείας, γιατροί, στρατιώτες και 50 αστυνομικοί**.

Η ορολογία που χρησιμοποιείται, συχνά διαφέρει:
Κυβερνοέγκλημα
Ηλεκτρονικό έγκλημα
Έγκλημα υψηλής τεχνολογίας
Έγκλημα με χρήση ηλεκτρονικών υπολογιστών
Η Ευρωπαϊκή Σύμβαση του Συμβουλίου της Ευρώπης δεν περιλαμβάνει ακριβή ορισμό.
Απλώς απαριθμεί τις διάφορες διατάξεις και τα πεδία που επιβάλλουν μια νέα νομοθεσία.

Ι. Οι υπολογιστές είναι <u>ευάλωτοι</u>:

Γιατί διαθέτουν μεγάλη ικανότητα αποθήκευσης σε μικρό χώρο.
Υπάρχει ευχέρεια πρόσβασης (λόγω της πολύπλοκης τεχνολογίας που χρησιμοποιείται, είναι, π.χ. δυνατή η κρυφή εγκατάσταση μιας «λογικής βόμβας»).
Εξαιτίας της πολυπλοκότητας, μια που τα λειτουργικά συστήματα συντίθενται από εκατομμύρια κώδικες, είναι δυνατό να υπάρχουν ανθρώπινα λάθη κατά τη σύνταξή τους και οι κυβερνοεγκληματίες επωφελούνται από αυτά.
Λόγω ανθρώπινης αμέλειας (που είναι συνυφασμένη με την ανθρώπινη φύση) για την αποτελεσματική προστασία τους.
Λόγω απώλειας του αποδεικτικού υλικού, αφού τα δεδομένα καταστρέφονται, ενώ, συχνά, οι δράστες δρουν εκτός τοπικής περιοχής αρμοδιότητας των διωκτικών Αρχών όπου βρίσκεται ο προσβαλλόμενος υπολογιστής.
Γιατί διαθέτουν μεγάλη ικανότητα αποθήκευσης σε μικρό χώρο.
Υπάρχει ευχέρεια πρόσβασης (λόγω της πολύπλοκης τεχνολογίας που χρησιμοποιείται, είναι, π.χ. δυνατή η κρυφή εγκατάσταση μιας «λογικής βόμβας»).
Εξαιτίας της πολυπλοκότητας, μια που τα λειτουργικά συστήματα συντίθενται από εκατομμύρια κώδικες, είναι δυνατό να υπάρχουν ανθρώπινα λάθη κατά τη σύνταξή τους και οι κυβερνοεγκληματίες επωφελούνται από αυτά.
Λόγω ανθρώπινης αμέλειας (που είναι συνυφασμένη με την ανθρώπινη φύση) για την αποτελεσματική προστασία τους.
Λόγω απώλειας του αποδεικτικού υλικού, αφού τα δεδομένα καταστρέφονται, ενώ, συχνά, οι δράστες δρουν εκτός τοπικής περιοχής αρμοδιότητας των διωκτικών Αρχών όπου βρίσκεται ο προσβαλλόμενος υπολογιστής.

ΙΙ. ΜΟΡΦΕΣ
Το έγκλημα στο διαδίκτυο περιλαμβάνει πολλές μορφές:
(Ενδεικτικά):

Παράνομη πρόσβαση στα δεδομένα άλλων και κλοπή δεδομένων
Αποστολή ιών σε άλλους χρήστες
Απάτες
Κλοπή/Υπεξαίρεση ταυτότητας
Ξέπλυμα χρήματος
Βιομηχανική κατασκοπεία
Παράνομη οργάνωση και συμμετοχή σε τυχερά παιχνίδια
Παράνομη πώληση αντικειμένων
Παράνομη διακίνηση τοξικοεξαρτησιογόνων ουσιών
Πειρατεία λογισμικού
Δυσφημήσεις
Παρενόχληση (σεξουαλική και άλλη: βομβαρδισμός με ηλεκτρονικά μηνύματα)
Προσβολές με ανήθικο και επιθετικό περιεχόμενο (πορνογραφία, ρατσισμός)

Πορνεία
Κυβερνοτρομοκρατία (και πρόκληση σε τέλεση τρομοκρατικών πράξεων)

ΙΙΙ. ΠΡΟΣΒΟΛΕΣ
(Ειδικότερα)

Πρόσβαση χωρίς άδεια σε ιδιωτικό δίκτυο.
Αλλαγή του περιεχομένου της ιστοσελίδας άλλου.
Παρεμπόδιση πρόσβασης τρίτων σε συγκεκριμένη ιστοσελίδα.
Βομβαρδισμός με μηνύματα μέχρι σημείου να εξουδετερωθεί η δυνατότητα κανονικής πρόσβασης.
Ταυτόχρονη αποστολή μέσω ειδικού προγράμματος πολλών μηνυμάτων, με στόχο την αχρήστευση του συστήματος.

Αποστολή ιών, σκουληκιών, δουρείων ίππων, λογικών βομβών, για τη διαγραφή αρχείων, δυσχέρανση λειτουργίας του συστήματος, κ.λπ.
Παράνομη αντιγραφή κινηματογραφικών ταινιών, μουσικών έργων, κ.λπ.
Παράνομες πωλήσεις (απαγορευμένων αντικειμένων, φαρμάκων, πλαστογραφημένων, πώληση παλαιών υπερυπολογιστών δυναμένων να παραβιάσουν κρυπτογραφημένους κώδικες, κ.λπ.).
Ξέπλυμα χρήματος με χρήση της δυνατότητας, μέσω του διαδικτύου, μεταφοράς κεφαλαίων, E-banking, κ.λπ.).
Κυβερνοτρομοκρατία (με προσβολή συστημάτων στρατιωτικού κ.λπ. περιεχομένου).
Κλοπές χρόνου χρήσης του διαδικτύου.
Παράνομη εισβολή με στόχο τον έλεγχο της ιστοσελίδας άλλου.

Κλοπή/ Υπεξαίρεση ταυτότητας
Θεωρείται ως το Έγκλημα της νέας χιλιετίας. Είναι το ταχύτερα αναπτυσσόμενο οικονομικό (και πιθανώς όχι μόνο οικονομικό) έγκλημα στον κόσμο. Αυξάνεται κατά 33% ετησίως στις ΗΠΑ.

1. **<u>με συλλογή και χρήση</u> προσωπικών πληροφοριών για το άτομο: όνομα, αριθμός τηλεφώνου, ημερομηνία γεννήσεως, διεύθυνση κατοικίας/εργασίας, αριθμό αστυνομικής ταυτότητας/διαβατηρίου, αριθμό κοινωνικής ασφάλισης, αριθμό πιστωτικής κάρτας, συνθηματικό πιστωτικής κάρτας, αριθμό άδειας οδήγησης και κάθε άλλη πληροφορία που επιτρέπει την ταυτοποίηση του ατόμου.**

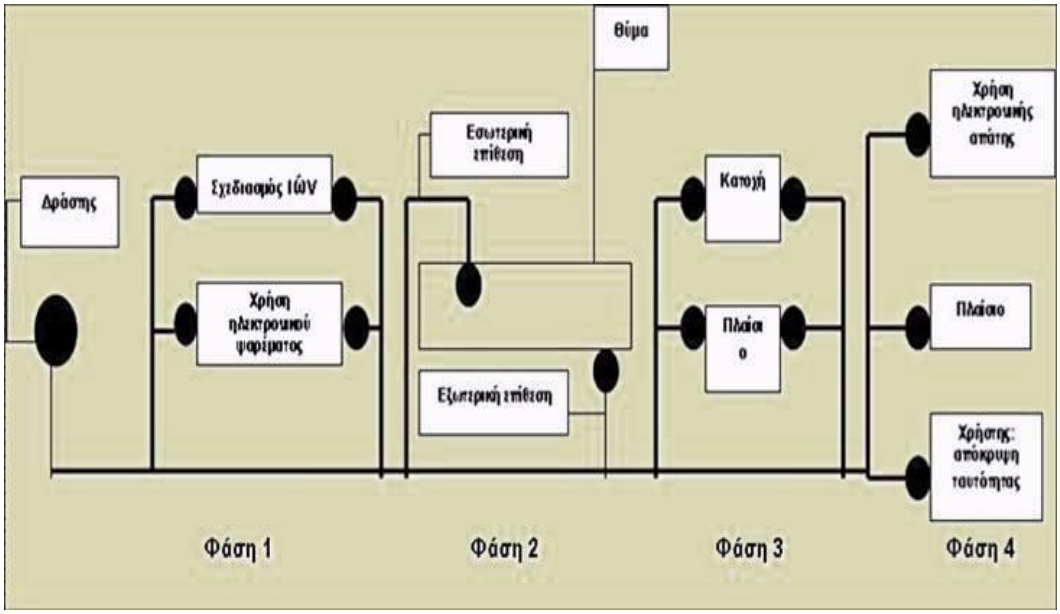
<u>Σε συνδυασμό με πιθανή πλαστογράφηση</u> (αν χρειάζεται) πιστοποιητικών (γεννήσεως, μετανάστευσης, κ.λπ.),
<u>Με στόχο</u> τον έλεγχο των τραπεζικών λογαριασμών ή το άνοιγμα νέων, την μεταφορά κεφαλαίων, την αίτηση για δανεισμό, την αγορά αγαθών ή υπηρεσιών, την λήψη διαφόρων βοηθημάτων από το κράτος, κ.λπ.

Κλοπή/ Υπεξαίρεση ταυτότητας

2. <u>με δημιουργία (πλήρως ή μερικώς) νέας ταυτότητας</u>, συνδυάζοντας διάφορα από τα συλλεγέντα στοιχεία.

Αυτή η σύνθετη κλοπή ταυτότητας είναι πολύ δύσκολο να ανιχνευθεί και διωχθεί.

<u>Το modus operandi των δραστών είναι εξαιρετικά ευρηματικό</u>. <u>Έχουν καταφέρει να πλαστογραφήσουν ακόμη και δακτυλικά αποτυπώματα</u>.



IV. ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΙΕΣ

Έφηβοι
(παιχνίδι, περιέργεια, ανάγκη αυτοεπιβεβαίωσης, αναγνώριση από τους συνομηλίκους, κ.λπ.)

Οργανωμένοι προσβολείς
(για πολιτικούς, θρησκευτικούς, κλπ. λόγους)

Επαγγελματίες προσβολείς
(χρησιμοποιούνται για να παραβιάζουν κώδικες ανταγωνιστών επιχειρηματιών κ.ά.)

Δυσαρεστημένοι υπάλληλοι

Σεξουαλικά διεστραμμένοι

V. ΠΡΟΣΤΑΣΙΑ

1. <u>Αυτοπροστασία</u>

Με το να παραμένει κανείς ανώνυμος
Με το να μη δίδει ποτέ στοιχεία της ταυτότητάς του σε αγνώστους
Με το να μην απαντά σε μηνύματα αγνώστων
Με το να μελετήσει όλα τα σχετικά με την προστασία στο διαδίκτυο της ιδιωτικής του ζωής
Με τη χρήση ειδικών ηλεκτρονικών φραγμάτων
Με τη συχνή αλλαγή συνθηματικού

Με τη χρήση της λεγόμενης ασφαλούς πλοήγησης
Με τον συχνό έλεγχο για ιούς
Με τη χρήση φίλτρων για τα ηλεκτρονικά μηνύματα που δέχεται

2. <u>Προστασία από ειδικούς οργανισμούς</u>
Ορισμένες χώρες έχουν δημιουργήσει ειδικούς οργανισμούς που σε συνεργασία με τράπεζες, πιστωτικά ιδρύματα γενικότερα, παρόχους υπηρεσιών στο διαδίκτυο και άλλους εμπλεκόμενους επιχειρούν να θέσουν κανόνες αυτορρύθμισης και προστασίας των χρηστών.

3. <u>Προστασία από τα Κράτη</u>
Με τη δημιουργία ειδικών Υπηρεσιών για την ανίχνευση, διερεύνηση και δίωξη των παραβατών και με
Τη θέσπιση ειδικών νόμων, όπου αυτό καθίσταται αναγκαίο

4. <u>Σε διεθνές επίπεδο</u>
Με την ανάπτυξη της διεθνούς συνεργασίας
Με τη θέσπιση της σχετικής με το κυβερνοέγκλημα Ευρωπαϊκής Σύμβασης (του Συμβουλίου της Ευρώπης) που κατέστη διεθνής, με τη δυνατότητα που δόθηκε και σε μη ευρωπαϊκά κράτη να γίνουν μέλη της, πράγμα που έγινε σε ευρεία κλίμακα.
Με την εφαρμογή της διεθνούς Σύμβασης του Ο.Η.Ε. για το οργανωμένο έγκλημα, κάθε φορά που πρόκειται για οργανωμένη μέσω του διαδικτύου εγκληματική δραστηριότητα.

Η Ευρωπαϊκή Ένωση έχει αναπτύξει διάφορα νομικά εργαλεία που αναφέρονται στο θέμα των πληροφοριών σχετικά με την ταυτότητα του ατόμου (Οδηγία 95/46/ΕC) ή που προβλέπουν την ποινικοποίηση ορισμένων μορφών απάτης και σχετιζομένων με το διαδίκτυο εγκλημάτων, όπως για την παράνομη πρόσβαση σε συστήματα ηλεκτρονικών υπολογιστών (Απόφαση-Πλαίσιο Ευρωπαϊκού Συμβουλίου 2001/413/JHA και Απόφαση-Πλαίσιο Ευρωπαϊκού Συμβουλίου 2005/222/JHA, αντίστοιχα), ενώ, στα πλαίσιά της, διεξάγεται μεγάλη έρευνα σχετικά με τις ποινικές συνέπειες της κλοπής/υπεξαίρεσης ταυτότητας.

VI. ΔΙΑΚΥΒΕΡΝΗΤΙΚΟΙ ΟΡΓΑΝΙΣΜΟΙ
που εμπλέκονται σε ή έχουν ενδιαφέρον γι' αυτό το πεδίο:

International Organization for Migration (IOM, θέματα διαμετακόμισης και μετανάστευσης)
Council of Europe (ζητήματα κυβερνοεγκλήματος, συμπεριλαμβανομένης της εφαρμογής των όρων της Σύμβασης του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα)
European Commission: Διεύθυνση Δικαιοσύνης, Ελευθερίας και Ασφάλειας (ζητήματα ταυτότητας και ιδιωτικότητας) – ENISA (European Network and Information Security Agency).
Asia Pacific Economic Cooperation (APEC) σε συνεργασία με OECD (κυβερνοέγκλημα και ζητήματα «κακόβουλου λογισμικού» (malware)
Interpol & Europol (γενική εφαρμογή του νόμου και καταχώρηση κλεμμένων διαβατηρίων)

G8 "Roma" (ζητήματα τρομοκρατίας) & ομάδες "Lyon" (εγκληματικά ζητήματα)
ITU, λαμβάνοντας υπόψη την παράλληλη διαδικασία της Ειδικής Ομάδας Εμπειρογνωμόνων για την Ασφάλεια στον Κυβερνοχώρο στο πλαίσιο της ITU Global Cybersecurity Agenda
International Chamber of Commerce
UN Development Programme
Ομάδα ηλεκτρονικού εγκλήματος "24/7"
International Civil Aviation Organization (ICAO, διαβατήρια και ταξιδιωτικά έγγραφα)
Organization for Security and Cooperation in Europe (OSCE)
Southeast European Cooperative Initiative (SECI) (εντός του γενικότερου πλαισίου της καταπολέμησης του διασυνοριακού εγκλήματος στην περιοχή)
World Society of Victimology (ζητήματα θυμάτων)
World Intellectual Property Organization (WIPO, εμπορικά σήματα και άλλα στοιχεία εταιρικής ταυτότητας)
UN Commission on International Trade Law (UNCITRAL, ζητήματα εμπορικής/εταιρικής ταυτότητας, γενικά συμφέροντα ιδιωτικού τομέα)
UN Department of Peacekeeping Operations
UN Human Rights Committee και άλλοι διεθνείς οργανισμού για τα Δικαιώματα του Ανθρώπου

VII. ΕΝΔΕΙΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΔΙΕΘΝΩΣ. ΑΝΑΠΤΥΞΗ ΕΙΔΙΚΗΣ ΔΙΔΑΣΚΑΛΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΑΠΟ ΤΟ KOREAN INSTITUTE OF CRIME: ΕΙΚΟΝΙΚΟ FORUM ΕΝΑΝΤΙΑ ΣΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Διδακτέα Ύλη
Α. Εισαγωγικό μάθημα για στελέχη του συστήματος απονομής της ποινικής δικαιοσύνης

0. Εισαγωγή στο εισαγωγικό μάθημα

1. Κατανοώντας τις τεχνολογίες πληροφορίας και επικοινωνίας (ICT)
- **Κατανοώντας τις τάσεις στις τεχνολογίες πληροφορίας και επικοινωνίας (ICT) και στο κυβερνοέγκλημα την εποχή της πληροφορίας**
- **Δομή του διαδικτύου και ψηφιακό χάσμα**
- **Τα ευάλωτα σημεία των τεχνολογιών πληροφορίας και επικοινωνίας (ICT)**
- **Τεχνολογίες πληροφορίας και επικοινωνίας (ICT) και διαδικτυακή ασφάλεια**
- **Μορφές συμπερίληψης και παράνομης πρόσβασης**
- **Ηλεκτρονικό εμπόριο και μορφές ηλεκτρονικής πληρωμής**
- **Ψηφιακές αποδείξεις και ηλεκτρονική Εγκληματολογία σε μη ειδικούς**

2. Κατανοώντας τους νόμους του κυβερνοχώρου
- **Εγκληματικότητα και ορισμοί του κυβερνοεγκλήματος**
- **Τύποι του κυβερνοεγκλήματος (Ι) – Κυβερνο-βία**

Τύποι του κυβερνοεγκλήματος (ΙΙ) –Αντι-κοινωνικά σχόλια στον κυβερνοχώρο
Τύποι του κυβερνοεγκλήματος (ΙΙΙ) – Κυβερνοεγκλήματα κατά της περιουσίας
Τύποι του κυβερνοεγκλήματος (IV) – Κυβερνοέγκλημα και εγκλήματα διαδικτυακών τραπεζικών συναλλαγών (e-banking)
Τύποι του κυβερνοεγκλήματος (V) – Κυβερνοτρομοκρατία
Δικαιοδοσία – Οι ρόλοι της εθνικής και διεθνούς επιβολής της νομοθεσίας
Διεθνής συνεργασία στον έλεγχο του κυβερνοεγκλήματος
Συμβατότητα διεθνών συμβάσεων για το κυβερνοέγκλημα με τους εθνικούς νόμους
Αμοιβαία νομική βοήθεια: μέθοδοι και προβλήματα – Διαδικασίες και πρακτικές της on-line συνεργασίας για τις υπηρεσίες επιβολής του νόμου
Ψηφιακό αποδεικτικό υλικό, διαφύλαξη και παρουσίασή του σε μη Εγκληματολόγους

Β. Προχωρημένα μαθήματα για ειδικούς

0. Εισαγωγή στο μάθημα για ειδικούς

3. Διερεύνηση του κυβερνοεγκλήματος – Διαδικασίες και Τεχνικές

Τεχνικές διερεύνησης του κυβερνοεγκλήματος (Ι)
Τεχνικές διερεύνησης του κυβερνοεγκλήματος (ΙΙ)
Σύστημα διερεύνησης και διαδικασία των προηγμένων χωρών
Ποινική διαδικασία και ψηφιακές αποδείξεις
Modus operandi στο κυβερνοέγκλημα και τεχνικές διερεύνησης (Ι) – Ιοί, χάκινγκ και botnet. Modus operandi στο κυβερνοέγκλημα και τεχνικές διερεύνησης (ΙΙ)– Ηλεκτρονική ανεπιθύμητη παρακολούθηση και ηλεκτρονικός βανδαλισμός
Modus operandi στο κυβερνοέγκλημα και τεχνικές διερεύνησης (ΙΙΙ) – Ηλεκτρονική απάτη και ψάρεμα
Modus operandi στο κυβερνοέγκλημα και τεχνικές διερεύνησης (IV) – Ηλεκτρονικό εμπόριο και τραπεζικές συναλλαγές
Διαφύλαξη και παρουσίαση των ψηφιακών αποδείξεων
Έλεγχος του κυβερνοεγκλήματος και αυτοματοποιημένα συστήματα
Διαδικτυακή ασφάλεια
Ομάδες καταγραφής περιστατικών – Προτεραιότητες και Ενίσχυση Ομαδικού πνεύματος
Διερευνώντας Καλές Πρακτικές – Μελέτες περίπτωσης
Πρακτική εκπαίδευση – Ασκήσεις

4. Η διερεύνηση του κυβερνοεγκλήματος – Ηλεκτρονική Εγκληματολογία

Κατανόηση και εφαρμογή των κανόνων των ψηφιακών αποδείξεων
Απόκτηση φωτογραφιών χρήσιμων στα εγκληματολογικά εργαστήρια και διαφύλαξη ψηφιακών αποδείξεων
Έλεγχος με χρησιμοποίηση εργαστηριακών εργαλείων (CFTT)
Αναλυτικές διαδικασίες και εγκληματολογικές τεχνικές (Ι) – Ανάλυση Προγράμματος
Αναλυτικές διαδικασίες και εγκληματολογικές τεχνικές (ΙΙ) – Διαδικτυακή Ανάλυση

Αναλυτικές διαδικασίες και εγκληματολογικές τεχνικές (III) – Ανάλυση Βάσης Δεδομένων
Αναλυτικές διαδικασίες και εγκληματολογικές τεχνικές (IV) – Ψηφιακή Ανάλυση αποδείξεων
Έρευνα ηλεκτρονικής αλληλογραφίας
Ανάλυση λέξεων-κλειδιών
Ανάλυση διαδικτυακής δραστηριότητας
Μηχανισμοί κρυπτογράφησης και στενογραφίας
Ηλεκτρονικοί κίνδυνοι ασφάλειας και αντιμετώπιση (I)
Ηλεκτρονικοί κίνδυνοι ασφάλειας και αντιμετώπιση (II)

5. **On-line ειδικά σεμινάρια. Ζητ/ήματα και αντικείμενα.**

Ιδιωτικότητα και προστασία δεδομένων
Ανηθικότητα και προσβλητικό/ρατσιστικό υλικό
On-line παιχνίδια και τζόγος
Εκτίμηση των πιθανών απειλών από την ασύρματη τεχνολογία
Biomatrix / εφαρμογές βιοπληροφορικής στον κυβερνοχώρο
Ηλεκτρονική πνευματική ιδιοκτησία
Κυβερνοτρομοκρατία – Μελέτη Περίπτωσης
Ειδικά θέματα από τους συμμετέχοντες – Ανοικτό forum για ειδικές περιπτώσεις

VIII. ΠΡΟΛΗΨΗ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ που σχετίζονται με την ΨΗΦΙΑΚΗ ΤΑΥΤΟΤΗΤΑ: ΜΙΑ ΜΗΤΡΑ

[Πίνακας του Jonathan J. Rusch, Department of Justice (Draft 17/04/2009)]

Στόχοι	Άτομα	Εκδότες ταυτοτήτων (π.χ. Κυβερνητικές υπηρεσίες), Εκδότες πιστωτικών καρτών	Επικοινωνίες και Μεταδότες δεδομένων ταυτότητας (π.χ. ISPs/Hosting sites, Carriers)	Κύριοι και ενδιάμεσοι τόποι αποθήκευσης/διατήρησης δεδομένων (π.χ. Πιστωτικά ιδρύματα, κυβερνητικές υπηρεσίες)	Χρήστες δεδομένων ταυτότητας (π.χ. έμποροι αγαθών και υπηρεσιών, grantors of program benefits)	Κυβερνήσεις (υπηρεσίες επιβολής του νόμου)

Η προστασία των δεδομένων από τους εγκληματίες	Βελτίωση των μέτρων ασφάλειας που σχετίζονται με τα δεδομένα των χρηστών	Βελτίωση των μέτρων ασφάλειας που σχετίζονται με δεδομένα του εκδότη Επισήμανση και έλεγχος της πρόσβασης στις διαδικτυακές πηγές και στα δεδομένα του κατόχου πιστωτικών καρτών Κανονικός έλεγχος των συστημάτων ασφάλειας και διαδικασίες	Σαφείς όροι της χρήσης κυβερνητικής απάτης και εγκλημάτων που σχετίζονται με θέματα ψηφιακής ταυτότητας Διευκόλυνση του κλεισίματος μη εγκεκριμένων τόπων αποθήκευσης/διατήρησης δεδομένων Υιοθέτηση μεθόδων επαλήθευσης της ηλεκτρονικής αλληλογραφίας	Βελτίωση των μέτρων ασφάλειας σχετικών με των τόπων αποθήκευσης/διατήρησης Επισήμανση και έλεγχος της πρόσβασης στις διαδικτυακές πηγές και στα δεδομένα του κατόχου πιστωτικών καρτών Κανονικός έλεγχος των συστημάτων ασφάλειας και διαδικασίες	Βελτίωση των μέτρων ασφάλειας που σχετίζονται με τα δεδομένα των χρηστών Επισήμανση και έλεγχος της πρόσβασης στις διαδικτυακές πηγές και στα δεδομένα του κατόχου πιστωτικών καρτών Κανονικός έλεγχος των συστημάτων ασφάλειας και διαδικασίες Υιοθέτηση μεθόδων επαλήθευσης της ηλεκτρονικής αλληλογραφίας	Υιοθέτηση οδηγιών και κανονισμών, ώστε να τεθούν ποιοτικά πρότυπα για την ασφάλεια των δεδομένων Χρήση εκπαιδευτικών μεθόδων για την πληροφόρηση των ατόμων σχετικά με την προστασία των δεδομένων που σχετίζονται με την ψηφιακή ταυτότητα Κατασταλτική δράση κατά προσπαθειών απόκτησης δεδομένων ταυτότητας για εγκληματικούς σκοπούς Γνωστοποίηση τρεχουσών τάσεων και τεχνικών

Περιορισμός της αξίας των κλαπέντων ή υπεξαιρεθέντων δεδομένων	Χρήση έγκαιρων αναφορών προς εκδότες, υπηρεσίες εφαρμογής του νόμου, κ.ά. Χρήση των ηλεκτρονικών φραγών	Μείωση της χρήσης της κοινωνικής ασφάλειας/ Αριθμοί κοινωνικής ασφάλειας Χρήση αριθμών μίας φοράς που αφορούν σε ατομικές συναλλαγές Αλλαγή των ατομικών δεδομένων ψηφιακής ταυτότητας, αναγκαία για τη μείωση του κινδύνου Χρήση δημόσιων εκπαιδευτικών ιστοσελίδων και αποστολή προειδοποιητικών μηνυμάτων προειδοποίησης για τις διάφορες απάτες	Κλείσιμο ιστοσελίδων που φιλοξενούν επιχειρήσεις δημιουργίας δεομένων ταυτότητας Δημιουργία των 24/7 σημείων των επαφών για διευκόλυνση/επίσπευση αναγνώρισης και κλεισίματος ιστοσελίδων συνδεόμενων με εγκλήματα περί την ταυτότητα Υιοθέτηση διαδικασιών που δημιουργούν ανάχωμα στην παράβαση Χρήση δημόσιων εκπαιδευτικών ιστοσελίδων και αποστολή προειδοποιητικών μηνυμάτων προειδοποίησης για τις διάφορες απάτες	Έγκαιρη αναφορά σε άτομα των οποίων τα δεδομένα είναι αποκτημένα με ακατάλληλο τρόπο και σε εκδότες Υιοθέτηση διαδικασιών που δημιουργούν ανάχωμα στην παράβαση Χρήση δημόσιων εκπαιδευτικών ιστοσελίδων και αποστολή προειδοποιητικών μηνυμάτων προειδοποίησης για τις διάφορες απάτες	Έγκαιρη αναφορά σε άτομα των οποίων τα δεδομένα είναι αποκτημένα με ακατάλληλο τρόπο και σε εκδότες Υιοθέτηση διαδικασιών που δημιουργούν ανάχωμα στην παράβαση Χρήση δημόσιων εκπαιδευτικών ιστοσελίδων και αποστολή προειδοποιητικών μηνυμάτων προειδοποίησης για τις διάφορες απάτες	Διευκόλυνση των επαφών με νόμιμους μεταδότες και ενδιαμέσους για αναζήτηση κλεισίματος Χρήση δημόσιων εκπαιδευτικών ιστοσελίδων και αποστολή προειδοποιητικών μηνυμάτων προειδοποίησης για τις διάφορες απάτες

Περιορισμός του ύψους των απωλειών που συνδέονται με κατοχή χωρίς άδεια δεδομένων	Αυξημένη πρόσβαση στη χρήση και χρήση μηχανισμών ταυτοποίησης	Εγκαιρη ενημέρωση των θυμάτων	Χρήση μηχανισμών επανακατεύθυνσης	Έγκαιρη ενημέρωση στα θύματα	Έγκαιρη ενημέρωση των εκδοτών	Χρήση μηχανισμών επανακατεύθυνσης (π.χ. Μετά την επιβολή του νόμου)
Ελαχιστοποίηση των αποφάσεων που στηρίζονται σε λανθασμένη θεώρηση του θύματος ως δράστη	Έγκαιρη αναφορά θυματοποίησης στις Υπηρεσίες εφαρμογής του νόμου Χρήση «διαβατηρίων» κλοπής ταυτότητας και μηχανισμοί διόρθωσης των λανθασμένων δεδομένων που περιέχονται στα αρχεία της αστυνομίας	Ολοκληρωμένες επιχειρήσεις, πρόληψης των κινδύνων, πρόληψης της απάτης και θέσπιση μέτρων ασφαλείας	Δημιουργία διαδικασιών για την επαλήθευση της ταυτότητας του θύματος ενάντια σε εξωτερικές πηγές δεδομένων	Ολοκληρωμένες επιχειρήσεις, πρόληψης των κινδύνων, πρόληψης της απάτης και θέσπιση μέτρων ασφαλείας	Ολοκληρωμένες επιχειρήσεις, πρόληψης των κινδύνων, πρόληψης της απάτης και θέσπιση μέτρων ασφαλείας	Χρήση «διαβατηρίων» κλοπής ταυτότητας Χρήση των φακέλων κλοπής ταυτότητας του Εθνικού Κέντρου Πληροφοριών για την Εγκληματικότητα ή αντίστοιχων βάσεων δεδομένων της αστυνομίας Υιοθέτηση τεχνολογικών για τη διευκόλυνση της ταχύτατης επαλήθευσης της ταυτότητας του θύματος

ΙΧ. ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ

Υπάρχουν διάφορα ζητήματα που έχουν σχέση με την **αρχειοθέτηση των δεδομένων και την κρυπτογράφησή** τους. Όλα τα τελευταία χρόνια παρατηρείται **μια διελκυστίνδα μεταξύ των ενεργών πολιτών που υπερασπίζονται την ελευθερία διακίνησης ιδεών στο διαδίκτυο και της κεντρικής εξουσίας**, σχετικά με τη δυνατότητα ή μη χρήσης της κρυπτογραφίας και αποκρυπτογράφησης των μηνυμάτων, προκειμένου να εξιχνιασθούν και τιμωρηθούν τυχόν διαπραττόμενες εγκληματικές πράξεις.

Σύντομα, η **δυνατότητα διαπίστωσης της ταυτότητας μέσω ραδιοσυχνοτήτων (RFID)** θα είναι γεγονός. Και η ελάχιστη κίνησή μας θα παρακολουθείται. Το γεγονός ότι, ήδη, η δυνατότητα παγκόσμιας ηλεκτρονικής παρακολούθησης έχει δημιουργήσει σημαντικά ζητήματα, όπως προκύπτει από την Έκθεση Campbell στο Ευρωκοινοβούλιο για το σύστημα Echelon, κάθε άλλο παρά μας καθησυχάζει. **Απαιτείται εγρήγορση**, αλλά και ιδιαίτερη εφευρετικότητα, προκειμένου να εξευρεθεί τρόπος να καταστεί συμβατή, **η προστασία των δικαιωμάτων των πολιτών τόσο από την κεντρική εξουσία, όσο και από τις πιθανές προσβολές τους από τους κυβερνοεγκληματίες**.