Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ
ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

3ο Συνέδριο
για την Ασφαλή Πλοήγηση στο Διαδίκτυο
2014

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΕΚΔΟΤΙΚΟΣ ΟΙΚΟΣ Α.Α. ΛΙΒΑΝΗ

ΕΛΛΗΝΙΚΗ ΑΣΤΥΝΟΜΙΑ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Τι αναμένεται στο μέλλον;

Ας ρίξουμε μια ματιά στο μέλλον, στα θέματα που αναμένεται να μας καταπλήξουν τα επόμενα χρόνια:

- Η ταχύτητα του Internet αυξάνεται
- Όλα θα είναι ασύρματα και συνδεδεμένα
- Δημιουργείται το Internet των πραγμάτων
- Οι προσωπικές βιντεοδιασκέψεις, καθώς και αυτές μέσω υπολογιστή, θα είναι η ταχύτερα αναπτυσσόμενη επαγγελματική υπηρεσία μέσω διαδικτύου,
- Έξυπνες συσκευές που διασυνδέονται μεταξύ τους μέσω του Internet. Υπολογίζεται ότι το 2020, 50 δισεκατομμύρια έξυπνες συσκευές στην Ευρώπη θα διασυνδέονται μεταξύ τους.
- Οι υπολογιστές γίνονται πιο γρήγοροι
- Οι υπολογιστές γίνονται μικρότεροι
- Η ηλεκτρονική πρώτη ύλη γίνεται όλο και πιο μικρή, επιτρέποντας την ανάπτυξη μικροσκοπικών υπολογιστών.
- Ο οπτικός υπολογιστής θα κυκλοφορήσει
- Ο χημικός υπολογιστής βρίσκεται επίσης μέσα στις δυνατότητες
- Η τεχνολογία λογισμικού εξελίσσεται
- Grid Computing - In the cloud computing
- Η τεχνητή νοημοσύνη των υπολογιστών αναπτύσσεται.

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

3ο Συνέδριο
για την Ασφαλή Πλοήγηση στο Διαδίκτυο
2014

Το Αρχηγείο της Ελληνικής Αστυνομίας και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συνιστά ΝΑΙ στο διαδίκτυο και τις νέες τεχνολογίες!

ISBN: 978-960-14-2938-0

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Πέμπτη 6 Φεβρουαρίου 2014

3ο Συνέδριο
για την Ασφαλή Πλοήγηση στο Διαδίκτυο

Προφυλάξου και προστάτευσε τους δικούς σου ανθρώπους από το cyber-bullying, την κλοπή και εκμετάλλευση των προσωπικών δεδομένων και άλλους κινδύνους.

Μπες τώρα κι εσύ στο **www.astynomia.gr** και παρακολούθησε ζωντανά σε live streaming το συνέδριο για το διαδίκτυο και τους κινδύνους του.

ΠΕΡΙΣΣΟΤΕΡΕΣ ΠΛΗΡΟΦΟΡΙΕΣ:
www.astynomia.gr, ccu@cybercrimeunit.gov.gr, τηλ.: 11012

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

AEGEAN · OLYMPIC · Hertz · 99,5 · Bold Ogilvy & Mather · Εκπαιδευτήρια ΓΕΙΤΟΝΑ · cyta · Eurobank · nova · hol · ΟΤΕ · COSMOTE · POSTBANK · vodafone · VISA · WIND

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Πρόσκληση

Το Αρχηγείο της Ελληνικής Αστυνομίας, με αφορμή
*την **«Παγκόσμια ημέρα ασφαλούς πλοήγησης στο διαδίκτυο»**,*
σας προσκαλεί στο συνέδριο το οποίο διοργανώνεται
από την ΥΠ.Ο.Α.Δ.Η.Ε./Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
*και θα πραγματοποιηθεί την **Πέμπτη 6 Φεβρουαρίου 2014** στο ξενοδοχείο*
***Athenaeum Intercontinental Athens**, Λ. Συγγρού 89-93.*

***Ώρα** έναρξης: **09:30**.*

***Πέρας** προσέλευσης: **09:00**.*

Η πρόσκληση είναι προσωπική και η προσκόμιση του δελτίου ταυτότητας
θα διευκόλυνε τη διαπίστευση εισόδου.

Χορηγός Επικοινωνίας

ΠΡΟΓΡΑΜΜΑ ΣΥΝΕΔΡΙΟΥ

Ενότητα 1η: "Οι δράσεις της Ελληνικής Αστυνομίας σχετικά με το Διαδίκτυο		Ενότητα 2η: "Το Διαδίκτυο στη ζωή μας: τι μέλλει γενέσθαι"	
09:30–10:00	**ΧΑΙΡΕΤΙΣΜΟΙ** Υπουργός Δημοσίας Τάξεως και Προστασίας του Πολίτη κ. Νικόλαος Δένδιας Αρχηγός Ελληνικής Αστυνομίας Αντιστράτηγος κ. Νικόλαος Παπαγιαννόπουλος Διευθυντής Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος Ταξίαρχος κ. Βασίλειος Κοντογιάννης	**11:30–12:45**	**Συντονιστής:** Ταξίαρχος Εμμανουήλ Σφακιανάκης, Υποδιευθυντής Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος
			«ΚΥΒΕΡΝΟΧΩΡΟΣ: Εξέλιξη και Αναδυόμενες Απειλές» Αστυνομικός Υποδιευθυντής Αριστείδης Μούρτος, Διευθυντής Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος
10:00–10:45	**«Απολογισμός δράσεων της Ελληνικής Αστυνομίας σχετικά με το Διαδίκτυο»** Υποστράτηγος Εμμανουήλ Σφακιανάκης, Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος		**«Διαδίκτυο: δυνατότητες της τεχνολογίας – προστασία του πολίτη»** Καθηγητής Ιωάννης Σ. Βενέρης, Εθνικό Μετσόβιο Πολυτεχνείο
10:45–11:00	Ερωτήσεις		**«Διαδικτυακά Ανθρωποκυκλώματα»** Καθηγητής Εμμανουήλ Ι. Γιαννακουδάκης, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών
11:00–11:10	Μουσικό διάλειμμα		
11:10–11:30	Διάλειμμα για καφέ		**«Η ενσωμάτωση νεώτερων τεχνολογικών εφαρμογών στο διαδίκτυο και οι επιδράσεις τους στην υγεία και την ανθρώπινη συμπεριφορά»** Δρ. Κωνσταντίνος Σιώμος, Ψυχίατρος παιδιών και εφήβων – Πρόεδρος της Ελληνικής Εταιρείας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο
			«1984–2014: Οι μελλοντικές τεχνολογίες παρακολούθησης βρίσκονται ήδη εδώ» Δρ. Ιωσήφ Ανδρουλιδάκης, Ερευνητής, Πανεπιστήμιο Ιωαννίνων
			«Διαδίκτυο@2014, τάσεις και εξελίξεις» κ. Μιχαήλ Μπλέτσας, Ερευνητής / Διευθυντής Πληροφορικής, MIT Media Lab, Τεχνολογικό Ινστιτούτο της Μασαχουσέτης
		12:45–13:00	Ερωτήσεις
		13:00–13:30	Ελαφρύ γεύμα

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΑΙΡΕΤΙΣΜΟΙ

Το 3ο Συνέδριο Ασφαλούς Πλοήγησης, που πραγματοποιήθηκε την 6-02-2014 στο Ξενοδοχείο Athenaeum Intercontinental Athens, τίμησαν με την παρουσία τους ο τέως Υπουργός Δημόσιας Τάξης και Προστασίας του Πολίτη, κ. Νίκος Δένδιας.

Παρευρέθηκαν ακόμα ο τέως Αρχηγός της Ελληνικής Αστυνομίας, Αντιστράτηγος Νικόλαος Παπαγιαννόπουλος, ο τέως Γενικός Επιθεωρητής Αστυνομίας Νοτίου Ελλάδας, ο τέως Αντιστράτηγος Σπυρίδων Παπασπύρου και άλλοι Αξιωματικοί του Σώματος.

Το Συνέδριο παρακολούθησαν εκπρόσωποι της πολιτικής, οικονομικής και πνευματικής ζωής της χώρας, επιχειρηματίες, διευθύνοντες σύμβουλοι, Δικαστές, Εισαγγελείς, Καθηγητές Νομικών Επιστημών, Δικηγόροι, Φοιτητές Νομικής και Αξιωματικοί των Ενόπλων Δυνάμεων και των Σωμάτων Ασφαλείας, καθώς και περίπου διακόσια (200) παιδιά – μαθητές πρωτοβάθμιας εκπαίδευσης, από δημόσια και ιδιωτικά Σχολεία της Αττικής.

Μεταξύ των παρισταμένων ήταν ο Προϊστάμενος της Εισαγγελίας Εφετών Αθηνών κ. Εμμανουήλ Ρασιδάκης, η Προϊσταμένη της Εισαγγελίας Πρωτοδικών Αθηνών κα. Παναγιώτα Φάκου, οι Αντεισαγγελείς του Αρείου Πάγου κα. Ξένη Δημητρίου και κ. Νικόλαος Παντελής, οι Αντεισαγγελείς Εφετών κ.κ. Παναγιώτης Αθανασίου και Μπρης Γαλινός, ο Εισαγγελέας Πρωτοδικών Αθηνών κ. Ιωάννης Δραγάτσης, ο Πρόεδρος και Διευθύνων Σύμβουλος ΟΤΕ–COSMOTE κ. Μιχαήλ Τσαμάζ, ο Συνήγορος του Καταναλωτή κ. Ευάγγελος Ζερβέας και ο Πρόεδρος του Ε.Σ.Ρ. κ. Ιωάννης Λασκαρίδης, Αντιπρόεδρος Αρείου Πάγου ε.τ..

Η διοργάνωση, που πραγματοποιήθηκε με αφορμή τον εορτασμό της Παγκόσμιας Ημέρας Ασφαλούς Πλοήγησης στο Διαδίκτυο, περιελάμβανε δύο (2) θεματικές ενότητες. Πραγματοποιήθηκαν παρουσιάσεις από διακεκριμένους και εξειδικευμένους επιστήμονες, από την Ελλάδα και το εξωτερικό, σε θέματα που αφορούν στην Ασφαλή Πλοήγηση στο Διαδίκτυο.

Συγκεκριμένα οι δύο θεματικές ενότητες που αναπτύχθηκαν ήταν:

- **1η ενότητα – «Οι δράσεις της Ελληνικής Αστυνομίας σχετικά με το διαδίκτυο»**, κατά την οποία παρουσιάσθηκε το πρόγραμμα των δράσεων στο πεδίο ενημέρωσης μαθητών, γονέων και άλλων ενδιαφερόμενων φορέων, για τα θετικά και αρνητικά του Διαδικτύου και συνακόλουθα τους κινδύνους που ελλοχεύουν κατά την πλοήγησή τους σε αυτό. Κατά τη διάρκεια της ενότητας αυτής, παρουσιάστηκε το έργο της Ελληνικής Αστυνομίας στον τομέα αυτό μέχρι και σήμερα, καθώς επίσης και το πρόγραμμα των μελλοντικών δράσεων για το 2014. Επιπλέον, προβλήθηκε το τηλεοπτικό **«spot» της νέας εκστρατείας ενημέρωσης για το 2014**.
- **2η ενότητα – «Το Διαδίκτυο στη ζωή μας: τι μέλλει γενέσθαι»**, στο πλαίσιο της οποίας αναπτύχθηκαν οι δυνατότητες που παρέχονται μέσω του διαδικτύου, αποτελώντας πηγή γνώσης, μάθησης, επικοινωνίας, διασκέδασης, ενημέρωσης, ενώ σκοπός της ενότητας αυτής ήταν να αναδειχθεί η σημαντικότητα του Διαδικτύου στην καθημερινότητα του σύγχρονου ανθρώπου.

Ο **τέως Υπουργός Δημόσιας Τάξης και Προστασίας του Πολίτη, κ. Νίκος Δένδιας**, στην ομιλία του, χαιρετίζοντας τις εργασίες του συνεδρίου, τόνισε τα ακόλουθα: *«Αυτό το οποίο γίνεται είναι μία πάρα πολύ σημαντική προσπάθεια, την οποία κάνει η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και ειδικά στο θέμα ο Υποστράτηγος Μανώλης Σφακιανάκης. Τι κάνει; Προσπαθεί να εκπαιδεύσει τα παιδιά, να ευαισθητοποιήσει και τους γονείς ως προς τους κινδύνους, αλλά και τις ευκαιρίες που έχει αυτός ο τεράστιος καινούργιος κόσμος, το διαδίκτυο. Αυτόν τον κόσμο τον οποίο δεν μπορούμε πια να αγνοήσουμε. Είναι ένα κομμάτι της ζωής όλων μας. Ζούμε όλοι με κάτι τέτοιο κοντά μας, μαζί μας, όλη μέρα. Παλιά, όταν εμείς ήμασταν παιδιά, παίζαμε στην πλατεία, οι γονείς μας ήξεραν με ποιον παίζουμε, ήξεραν τους γονείς του, εάν κάναμε κάτι στραβό, μας έλεγαν όχι με αυτόν, όχι με εκείνον, όχι τούτο, όχι το άλλο.*

Εσείς τώρα μπαίνετε σε έναν κόσμο που οι γονείς σας δεν ξέρουν με ποιον μιλάτε ή με ποιον παίζετε, δεν μπορούν να το ξέρουν και γι αυτό δεν μπορούν να σας προστατέψουν από αυτό. Πρέπει λοιπόν εσείς παιδιά να ξέρετε, να μάθετε τους κανόνες που θα προστατεύετε τον εαυτό σας. Αυτός ο καινούργιος κόσμος είναι γεμάτος ευκαιρίες, αλλά είναι και γεμάτος κινδύνους.

Οι ευκαιρίες είναι περισσότερες, αλλά οι κίνδυνοι είναι μεγάλοι και σημαντικοί. Και ο Μανώλης Σφακιανάκης και η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος είναι εδώ για να σας προστατέψουν, να σας μάθουν να προστατεύεστε από αυτούς τους κινδύνους. Για εμένα είναι πολύ συγκινητικό ότι σε μία παρόμοια εκδήλωση στα Γρεβενά –θα σας δείξω (ζωγραφιά μαθητών)– αυτό το έφτιαξαν κοριτσάκια 4 χρονών και μου το έδωσαν. Τι δείχνει; Δείχνει πάνω και θα το δείτε, τους αστυνομικούς σαν αγγέλους που προστατεύουν από τον κακό διάβολο. Θα το θυμάμαι και θα το κρατάω στη ζωή μου. Θα το αφήσω στην Ελληνική Αστυνομία όταν θα φύγω. Είναι ο πιο ωραίος τρόπος που κάποιος φαντάστηκε και είδε το ρόλο της Αστυνομίας στη ζωή του.

Πιστεύω λοιπόν ότι αξίζει αυτή η προσπάθεια, αξίζει αυτός ο στόχος, αξίζει αυτό το οποίο σαν γνώση σας δίνουν αυτές οι εκδηλώσεις. Επίσης γίνεται και κάτι άλλο μαζί. Αμέσως μετά η συνάδερφος η κα Έλενα Ράπτη, Βουλευτής Θεσσαλονίκης, θα σας πει για μία μεγάλη καμπάνια που κάνει το Συμβούλιο της Ευρώπης και την οποία η ίδια την "τρέχει" σε όλη την Ελλάδα, με πολύ μεγάλη προσπάθεια, για την σεξουαλική κακοποίηση των παιδιών και επίσης για το πως μπορούμε να προστατευτούμε και από αυτό.

Ας μην κοροϊδευόμαστε. Η περιουσία μας, η ζωή μας, το μέλλον μας είναι τα παιδιά μας. Και αξίζει να κάνουμε ό,τι μπορούμε για να προστατέψουμε αυτή τη νέα γενιά που είναι και η ελπίδα της πατρίδα μας. Σας ευχαριστώ πολύ».

Η **Έλενα Ράπτη, βουλευτής της ΝΔ στην Α' Θεσσαλονίκης και μέλος της Ελληνικής Αντιπροσωπείας στην Κοινοβουλευτική Συνέλευση του Συμβουλίου της Ευρώπης, μέλος του Δικτύου Κοινοβουλευτικών για τον τερματισμό της σεξουαλικής κακοποίησης των παιδιών και συντονίστρια της εκστρατείας «ΕΝΑ στα ΠΕΝΤΕ» του Συμβουλίου της Ευρώπης στην Ελλάδα**, στην ομιλία της τόνισε τα ακόλουθα: *Κυρίες και κύριοι, είναι χαρά και τιμή να βρίσκομαι σήμερα εδώ σε αυτό το πολύ σημαντικό συνέδριο της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο, μετά από την πολύ ευγενική πρόσκληση του Υποστράτηγου κ. Μανώλη Σφακιανάκη. Γνωρίζω πως υπάρχουν εξαίρετοι αστυνομικοί που πλαισιώνουν όλο το επιχειρησιακό πρόγραμμα της Υποδιεύθυνσης, ωστόσο θα ήθελα να σταθώ στην παρουσία του κ. Σφακιανάκη που ηγείται αυτού του πολύ ευαίσθητου τομέα και που πραγματικά τιμά την Ελληνική Αστυνομία.*

Πώς ξεκίνησε η συνεργασία μας;

Ως μέλος του Δικτύου Κοινοβουλευτικών για τον τερματισμό της σεξουαλικής κακοποίησης των παιδιών και συντονίστρια της εκστρατείας «ΕΝΑ στα ΠΕΝΤΕ» του Συμβουλίου της Ευρώπης στην Ελλάδα ζήτησα από τον τέως Αρχηγό της Ελληνικής Αστυνομίας, Αντιστράτηγο κ. Νικόλαο Παπαγιαννόπουλο και τον κ. Σφακιανάκη να με συμπεριλάβουν στις πρωτοβουλίες ενημέρωσης για τους κινδύνους στο διαδίκτυο. Επιθυμία μου να ενημερώνω παράλληλα για την πρόληψη της παιδικής σεξουαλικής κακοποίησης, τόσο στις εβδομαδιαίες διαδικτυακές συνδέσεις (τηλεδιασκέψεις) με τις σχολικές κοινότητες, όσο και στις ημερίδες-διαλέξεις της προγραμματισμένης περιοδείας σε πόλεις της επικράτειας με στόχο την ενημέρωση για τους κινδύνους στο διαδίκτυο. Ο κ. Σφακιανάκης λόγω της πλούσιας γνώσης και εμπειρίας του αποτελεί πλέον ένα σημείο αναφοράς στα θέματα των κινδύνων του διαδικτύου και θέλω να τον επαινέσω και δημόσια για τη διαρκή προθυμία του να μεταδώσει αυτή την εμπειρία σε όλους και κυρίως στη νεότερη γενιά που αποτελεί από τη θέση της την πιο ευάλωτη ομάδα στο χώρο του ηλεκτρονικού εγκλήματος. Ακολούθησα τον κ. Σφακιανάκη σε πάνω από 10 ελληνικές πόλεις μέσα σε διάστημα λίγων μηνών, ενημερώνοντας για την παιδική σεξουαλική κακοποίηση και διανέμοντας το σχετικό ενημερωτικό υλικό του Συμβουλίου της Ευρώπης. Η ανταπόκριση του κόσμου ήταν τόσο μεγάλη που απέδειξε ότι τέτοιες εκδηλώσεις είναι αναγκαίες για την ενημέρωση και την προστασία των πολιτών. Θέλω να τονίσω πως η πρωτοβουλία της υπηρεσίας δίωξης ηλεκτρονικού εγκλήματος λειτούργησε ως βάση για τη διεύρυνση της ενημερωτικής μας καμπάνιας σε ολόκληρη την χώρα. Αποτέλεσε ένα όχημα που μετέφερε το μήνυμα ενάντια στην σεξουαλική κακοποίηση στην κοινωνία, μου έδωσε την ευκαιρία να παρουσιάσω το θέμα σε πολίτες, παιδιά και γονείς, ενώ λειτούργησε αθροιστικά στη δυναμική της όλης προσπάθειας. Αυτή η κοινή συνέργεια ενημέρωσης δεν θα μπορούσε να μείνει στα όρια της χώρας μας. Την παρουσίασα στις ομιλίες απολογισμού που είχα την ευκαιρία να κάνω στις ευρωπαϊκές συνόδους του συμβουλίου της Ευρώπης και σε ειδικές θεματικές εκδηλώσεις. Ιδιαίτερα μάλιστα στη Γενεύη, οι αναφορές στις κοινές μας δράσεις αποτέλεσαν το μεγαλύτερο μέρος του απολογισμού και πρόβαλαν την εξαιρετική πρωτοβουλία του κ Σφακιανάκη αποσπώντας τα εύσημα όλων των ευρωπαίων συναδέλφων.

Κυρίες και κύριοι,

Εύχομαι η πρωτοβουλία του κ. Σφακιανάκη να συνεχιστεί και σε άλλες πόλεις της Ελλάδας, γιατί είδα τη θερμή υποδοχή και τη μεγάλη της απήχηση σε ολόκληρη την ελληνική κοινωνία. Μπορώ μάλιστα να σας μεταφέρω αιτήματα πολιτών που μας καλούν καθημερινά ζητώντας μας να μεσολαβήσουμε ώστε ο κ. Σφακιανάκης να οργανώσει ανάλογες εκδηλώσεις και στις δικές τους πόλεις. Αυτό από μόνο του νομίζω πως επιβεβαιώνει με τον πιο αδιαμφισβήτητο τρόπο την υψηλή αξία της πρωτοβουλίας αυτής. Το μόνο που θα είχα να προσθέσω ως επίλογο αυτής της σύντομης δικής μου παρέμβασης είναι πως το τμήμα του κ. Σφακιανάκη είναι μια σπουδαία υπηρεσία και οι πρωτοβουλίες του αποτελούν σημαντική κοινωνική προσφορά την οποία πρέπει πολιτεία και πολίτες να στηρίξουμε με όλες μας τις δυνάμεις. Σας ευχαριστώ.

Ενότητα 1η:
«Οι δράσεις της Ελληνικής Αστυνομίας σχετικά με το Διαδίκτυο»

«Απολογισμός δράσεων της Ελληνικής Αστυνομίας σχετικά με το Διαδίκτυο»

Υποστράτηγος **Εμμανουήλ Σφακιανάκης**,
Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Είναι μεγάλη τιμή για την Ελληνική Αστυνομία και τη Δίωξη Ηλεκτρονικού Εγκλήματος που όλοι εσείς έχετε έρθει σήμερα για να τιμήσετε τον αγώνα μας και να τιμήσετε τους ανθρώπους που δουλεύουν για εσάς. Η Δίωξη Ηλεκτρονικού Εγκλήματος έχει εξειδικευμένους αξιωματικούς που δουλεύουν 24 ώρες το 24ωρο και είναι ακατάπαυστα δίπλα σας. Δουλεύουν με πολλή αγάπη για να είστε εσείς πάνω από όλα ασφαλείς.

Σήμερα είναι η παγκόσμια ημέρα ασφαλούς διαδικτύου. Είναι η μέρα μας. Εμείς νοιαζόμαστε για το διαδίκτυο. Το διαδίκτυο διευκολύνει κατά πολύ την ζωή μας. Όμως, υπάρχουν και οι κίνδυνοι. 98% τα θετικά του διαδικτύου και 2% είναι οι κίνδυνοι.

Το Υπουργείο Δημοσίας Τάξης και το Αρχηγείο της Ελληνικής Αστυνομίας έχουν φτιάξει μια Υπηρεσία η οποία είναι κόσμημα για την Ευρώπη και αποτελείται από αξιωματικούς – επιστήμονες με μεταπτυχιακά και διδακτορικά, οι οποίοι συνθέτουν το παζλ της Δίωξης Ηλεκτρονικού

Εγκλήματος. Μιλάμε πλέον για επιστημονική αστυνομία. Όλοι όσοι δουλεύουν στη Δίωξη Ηλεκτρονικού Εγκλήματος κάνουν αυτό που αγαπάνε.

Το να γνωρίζουμε τους κανόνες ασφαλούς πλοήγησης είναι πολύ σημαντικό. Σε αυτούς τους κανόνες θα αναφερθούμε σήμερα. Θα δείτε πώς η Δίωξη Ηλεκτρονικού Εγκλήματος σας προστατεύει από τις κακοτοπιές του Διαδικτύου. Περνάμε λοιπόν στην παρουσίασή μας.

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος ξεκίνησε να λειτουργεί το 2011. Είναι αυτοτελής Υπηρεσία της Ελληνικής Αστυνομίας. Εποπτεύεται απευθείας από τον Αρχηγό της Ελληνικής Αστυνομίας και έχει δικαιοδοσία στο σύνολο της Επικράτειας. Η έδρα της είναι στη Γενική Αστυνομική Διεύθυνση, στη Λεωφόρο Αλεξάνδρας 173, στην Αθήνα. Το ανθρώπινο δυναμικό μας: 42 αξιωματικοί γενικών καθηκόντων, αξιωματικοί ειδικών καθηκόντων, 59 λοιποί βαθμοφόροι και 76 άτομα (λοιπό προσωπικό). Σύνολο 262 άτομα. Οι ειδικότητες που έχει προσλάβει η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι οι εξής:

- Ειδικότητα Τραπεζικών Εφαρμογών (15 άτομα)
- Ειδικότητα Χρηματοοικονομικής (14 άτομα)
- Φοροτεχνικοί (13 άτομα)
- Διερεύνηση Ψηφιακών Πειστηρίων (12 άτομα)
- Λογιστική (11 άτομα)
- Μηχανικοί Η/Υ (7 άτομα)
- Μηχανικοί Τηλεπικοινωνιών (6 άτομα)
- Ηλεκτρολόγοι Μηχανικοί και Μηχανικοί Η/Υ (5 άτομα)
- Δικηγόροι (2 άτομα)

Οι αρμοδιότητες της Υπηρεσίας μας είναι οι εξής:

- **Διαχείριση πληροφοριών – καταγγελιών**
- **Παρακολούθηση** εξελίξεων οικονομικού & ηλεκτρονικού εγκλήματος
- **Μελέτες, προτάσεις** για νέες τάσεις οικονομικού & ηλεκτρονικού εγκλήματος

Επίσης, ασχολούμαστε με την **Έρευνα** και **Δίωξη** εγκλημάτων:

- σε βάρος συμφερόντων του **Δημοσίου**, της **Εθνικής Οικονομίας & Ασφαλιστικών Οργανισμών** του Δημοσίου
- με χαρακτήρα **οργανωμένου οικονομικού εγκλήματος**
- τελούμενα με χρήση του **διαδικτύου** ή άλλων μέσων **ηλεκτρονικής επικοινωνίας & ψηφιακής αποθήκευσης.**

Συνεργαζόμαστε επίσης με διάφορους φορείς και υπηρεσίες.

Έχουμε στενή συνεργασία με τους Εισαγγελείς. Στο σημείο αυτό θα ήθελα να ευχαριστήσω τους Εισαγγελείς, δηλαδή τους ανθρώπους που είναι δίπλα μας καθημερινά. Με τους ανθρώπους αυτούς επικοινωνούμε διαρκώς, για να ενσκύψουν πάνω σε κάθε υπόθεση και να παραγγείλουν τις ενέργειες μας. Εμείς δε λειτουργούμε αυτόβουλα. Πρώτα, ακούμε τον πολίτη, λαμβάνουμε την καταγγελία του και στη συνέχεια ενημερώνουμε τους Εισαγγελείς. Είναι τιμή μας να έχουμε δίπλα μας σε αυτόν τον αγώνα τους Εισαγγελείς. Στο σημείο αυτό, θα ήθελα να ευχαριστήσω την κα Κουτζαμάνη, την Πρόεδρο του Αρείου Πάγου, τον κο Τέντε, γενικό Συντονιστή και πρώην Εισαγγελέα του Αρείου Πάγου, τον κο Σανιδά, πρώην Εισαγγελέα του Αρείου Πάγου, την κα Δημητρίου, Αντιεισαγγελέα του Αρείου Πάγου, τον κο Αγγελή, Εισαγγελέα της Eurojust, τον κο Ορνεράκη, την κα Φάκου, την κα Ράικου, και γενικά όλους τους Εισαγγελείς, οι οποίοι ήταν και είναι

κοντά μας. Οι Εισαγγελείς μας συνδράμουν στον δύσκολο αγώνα μας για την αντιμετώπιση των εγκλημάτων και ειδικά της παιδικής πορνογραφίας.

Εδώ θα ήθελα να κάνω ειδική μνεία στον κο Κορρέ, τον Εισαγγελέα, ο οποίος μας βοήθησε σε υπόθεση εκούσιας απαγωγής 13χρονης. Η ανήλικη ήταν εξαφανισμένη για 2 μήνες από το σπίτι της στον Πειραιά. Ο κος Κορρές ήταν εκτός υπηρεσίας, αλλά παρόλα αυτά, γύρισε στο πόστο του, μας βοήθησε να διεκπεραιώσουμε την υπόθεση και να βρούμε την ανήλικη. Η υπόθεση αυτή και ο εντοπισμός της ανήλικης με έκανε πραγματικά να συγκινηθώ και ήταν μια ψυχική ανάταση για τον υποστράτηγο Εμμανουήλ Σφακιανάκη. Για μια ακόμα φορά, ευχαριστώ τους Εισαγγελείς και τους δικαστές.

Επιπλέον, στενή συνεργασία έχουμε με την Ε.Υ.Π., με τη Γενική Γραμματεία Πληροφοριακών Συστημάτων, με την Europol, με την Interpol, με το Λιμενικό Σώμα και γενικά με τις Αστυνομικές Αρχές. Αν δεν είχαμε αυτές τις συνεργασίες, δε θα είχαμε αποτρέψει 880 περίπου συνανθρώπους μας από την αυτοκτονία. Στο σημείο αυτό, θα ήθελα να ευχαριστήσω όλους τους αστυνομικούς ανά τη χώρα, είναι καθοριστική η βοήθεια τους στην πρόληψη των αυτοκτονιών.

Όσον αφορά τα στατιστικά μας, έχουμε δεχτεί 14.895 καταγγελίες, 4.017 επώνυμες και 10.879 ανώνυμες. Έχουμε χειριστεί 7201 υποθέσεις, 5906 δικογραφίες και 423 αυτόφωρα. Η ζημία του δημοσίου ανέρχεται στα 35.501.665,81€, ενώ η ζημία τρίτων στα 3.232.565,12€.

Στο σημείο αυτό, θα ήθελα να σας παρουσιάσω τα αποτελέσματα των υποθέσεων μας. Μέχρι σήμερα, έχουμε 2.038 κατηγορούμενους, εκ των οποίων οι 1.280 έχουν εντοπιστεί από την Οικονομική Αστυνομία, ενώ οι 758 από τη Δίωξη Ηλεκτρονικού Εγκλήματος. Οι 196 ήταν κατηγορούμενοι για υποθέσεις παιδικής πορνογραφίας.

Οι συλληφθέντες είναι 907, 699 από την Οικονομική Αστυνομία και 208 από τη Δίωξη Ηλεκτρονικού Εγκλήματος, ενώ οι 93 έχουν συλληφθεί για παιδική πορνογραφία τα τελευταία τρία χρόνια. 75 άτομα έχουν προφυλακιστεί με 265 άτομα να έχουν περιοριστικούς όρους.

Περνάμε τώρα σε ένα μεγάλο κεφάλαιο, στις Δράσεις Ασφαλούς Πλοήγησης, τις οποίες κάνει η Υπηρεσία μας. Η πρώτη από αυτές είναι οι τηλεδιασκέψεις, στις οποίες δεχόμαστε τις ερωτήσεις των παιδιών από όλη τη χώρα.

Κάποιες από τις απορίες των παιδιών είναι οι ακόλουθες:

- Έχουν υπάρξει αυτοκτονίες στην Ελλάδα λόγω του Cyberbullying;
- Πώς μπορούμε να καταπολεμήσουμε τον εθισμό στο internet;
- Πόσες αυτοκτονίες γίνονται το χρόνο στην Ελλάδα;
- Τί ποσοστό του πληθυσμού που χρησιμοποιεί το internet το κάνει επαγγελματικά;
- Πόσοι άνθρωποι στον κόσμο πέφτουν θύματα καθημερινά εξαιτίας της κακής χρήσης του internet;
- Υπάρχει περίπτωση η Αστυνομία να ζητήσει διακρίβωση στοιχείων ηλεκτρονικά;

Αυτές είναι οι ερωτήσεις που δεχόμαστε από τα παιδιά μέσω τηλεδιασκέψεων που γίνονται στην Υπηρεσία μας. Τα παιδιά από όλα τα σχολεία της χώρας μας υποβάλλουν τις ερωτήσεις τους, νιώθουν πολύ άνετα να συνομιλούν με αξιωματικούς της Υπηρεσίας μας κι έτσι είναι πολύ κοντά στο Ηλεκτρονικό Έγκλημα και την Ελληνική Αστυνομία.

Προχωράμε τώρα στην Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης, με αφορμή την οποία κάνουμε σήμερα το συνέδριο μας και σας παρουσιάζουμε τους κανόνες ασφαλούς πλοήγησης. Στο 1ο και 2ο Συνέδριο, το 2012 και το 2013 αντίστοιχα, είχαμε 100 περίπου ομιλητές, νομικούς και Εισαγγελείς, και 35.000 αιτήσεις για να συμμετέχουν στα Συνέδρια μας και περισσότερα από 30.000

άτομα παρακολούθησαν τα Συνέδρια μας μέσω live streaming, και όλα τα Μέσα Μαζικής Επικοινωνίας ήταν παρόντα στο Συνέδριο μας.

Παρακάτω, μπορείτε να δείτε τις αφίσες ασφαλούς πλοήγησης, που είχαμε φτιάξει για τα προηγούμενα συνέδρια μας.

Προχωράμε στις Ημερίδες που έχουμε κάνει. Τα τελευταία χρόνια έχουμε κάνει 89 ημερίδες, σε 33 πόλεις της επικράτειας, όπως η Ηγουμενίτσα, Γρεβενά, Πρέβεζα, Πάτρα, Τρίπολη κλπ.

Διαφημιστικό Σποτ Ημερίδων

Ενδεικτικές φωτογραφίες ημερίδων

Στη συνέχεια, θα σας παρουσιάσω την αφίσα των ημερίδων μας με σύνθημα «Μη τσιμπάς»

Αφίσα Ημερίδων

Μπαίνουμε στις καινοτόμες δράσεις της Υπηρεσίας μας. Έχουμε προβεί στην ανάπτυξη του site www.cyberkid.gr, έναν ιστότοπο με παιχνίδια και συμβουλευτικό χαρακτήρα. Περιλαμβάνει συμβουλές τόσο για τα παιδιά, όσο και για τους γονείς.

Έχουμε επίσης προβεί και στη δημιουργία ενημερωτικών φυλλαδίων που περιλαμβάνουν συμβουλές για την ασφαλή πλοήγηση στο διαδίκτυο, τα οποία έχουν συγγράψει αξιωματικοί – επιστήμονες της Υπηρεσίας μας.

Η επόμενη καινοτόμα δράση της Υπηρεσίας μας είναι οι τηλεδιασκέψεις, κατά τη διάρκεια των οποίων συνδεόμαστε με πολλά σχολεία παράλληλα και ενημερώνουμε τους μαθητές για την ασφάλεια στο διαδίκτυο.

Στόχος μας είναι η Ασφαλής Πλοήγηση να καθιερωθεί ως μάθημα σε όλα τα σχολεία.

Στο σημείο αυτό, πρέπει να σας πω ότι η Υπηρεσία μας δίνει μεγάλη βαρύτητα στην αντιμετώπιση του bullying, και για αυτό έχει προβεί στην παραγωγή ειδικού τηλεοπτικού σποτ, στιγμιότυπο από το οποίο θα δείτε στη συνέχεια.

Μέσα από ειδική αντιμετώπιση επιδιώκουμε να σταματήσουμε το bullying στα παιδιά. Θα ήθελα να παροτρύνω όλα τα παιδιά που βιώνουν τέτοιες καταστάσεις να απευθυνθούν άμεσα στο γονείς και τους εκπαιδευτικούς του σχολείου τους. Εμείς υποστηρίζουμε τη διαχείριση τέτοιων καταστάσεων μέσα από το σχολείο. Η Αστυνομία έπεται. Είναι ό,τι χειρότερο γονείς και παιδιά να πηγαίνουν στα δικαστήρια. Συμβουλευτικά, συνδράμουμε κι εμείς σε αυτές τις καταστάσεις. Το bullying στα παιδιά πρέπει να σταματήσει.

Σας ευχαριστώ που με ακούσατε κι ευχαριστώ και τους χορηγούς μας. Ένα μεγάλο ευχαριστώ στους χορηγούς μας, γιατί χωρίς αυτούς δε θα μπορούσαμε να υλοποιήσουμε κανένα συνέδριο και καμία καμπάνια.

Ενότητα 2η:
«Το Διαδίκτυο στη ζωή μας:
τι μέλλει γενέσθαι»

«Εισαγωγή συντονιστή ενότητας»

Υποστράτηγος **Εμμανουήλ Σφακιανάκης**
Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Θα ήθελα να σας καλωσορίσω στο 2ο μέρος του συνεδρίου μας, όπου ομιλητές είναι διακεκριμένοι επιστήμονες. Οι επιστήμονες αυτές θα σας εκφράσουν ανησυχίες και σκέψεις σχετικά με το μέλλον του διαδικτύου και θα σας παρουσιάσουν τις μελλοντικές εξελίξεις, προτείνοντας λύσεις που θα σας θωρακίσουν από τις παγίδες του διαδικτύου. Ας τους ακούσουμε προσεκτικά, για να φύγουμε από εδώ σοφότεροι!

«ΚΥΒΕΡΝΟΧΩΡΟΣ: Εξέλιξη και Αναδυόμενες Απειλές»

Αστυνομικός **Υποδιευθυντής Αριστείδης Μούρτος,**
Τέως Διευθυντής Δίωξης Ηλεκτρονικού Εγκλήματος

Καλησπέρα σας. Θα ήθελα και εγώ με την σειρά μου ως Δ/ντης ΥΔΗΛΕ, και ανοίγοντας τη δεύτερη αυτή ενότητα, να σας ευχαριστήσω για την ανταπόκριση που δείξατε και παρευρίσκεστε σήμερα στις εργασίες αυτού του Συνεδρίου.

Αισθάνομαι ιδιαίτερη χαρά και τιμή που έχω την ευκαιρία να μιλήσω σε ακροατήριο σαν το σημερινό, στο οποίο παρευρίσκονται εκπρόσωποι του Πολιτικού χώρου, της Δικαστικής Εξουσίας, Ακαδημαϊκοί, Επιχειρηματίες, Δημοσιογράφοι, τεχνολόγοι και πολίτες. Κυβερνοχώρος και Αναδυόμενες Απειλές.

Αυτός ο εικονικός-τεχνολογικός κόσμος – ο κυβερνοχώρος – είναι ένας κόσμος που εξαρτόμαστε κάθε μέρα και περισσότερο. Είναι το υλικό, το λογισμικό, οι Η/Υ και τα κινητά που έχουν γίνει συνυφασμένα με την καθημερινότητα μας. Είναι τα ευρυζωνικά και τα ασύρματα δίκτυα γύρω μας, τα τοπικά δίκτυα στα σχολεία, τα νοσοκομεία και τις επιχειρήσεις. Είναι το διαδίκτυο που μας έχει διασυνδέσει με τον υπόλοιπο κόσμο.

Αντιλαμβανόμαστε λοιπόν ότι ο κυβερνοχώρος είναι πραγματικός. Το ίδιο όμως και είναι οι κίνδυνοι που έρχονται με αυτόν. Όλοι μας πλέον γνωρίζουμε ότι οι παρεισφρήσεις-επιθέσεις σε δίκτυα και Η/Υ, αποτελούν σοβαρές απειλές τόσο στην εθνική ασφάλεια, την οικονομία όσο και σε απλές δραστηριότητες της καθημερινότητας μας.

Όλοι ξέρουμε ότι αυτές οι απειλές αυξάνονται... Θεωρώ ότι δεν χρειάζεται να ξοδέψω το χρόνο εξιστορώντας ξανά γνωστά πράγματα.

Επέλεξα συνοπτικά να αναφερθώ στην σημερινή πραγματικότητα-έκταση του φαινομένου και κυρίως στην εξέλιξη-τάσεις που παρουσιάζει ο κυβερνοχώρος και στις τεχνολογικές προκλήσεις που διαφαίνεται να παρουσιάσει στο μέλλον (οπτική Δίωξης). Δε θα αναλυθούν οι τεχνολογικές δυνατότητες, θα παρουσιαστούν συνοπτικά οι τεχνολογικές τάσεις και μέσω αυτών θα διαφανούν οι μέλλουσες απειλές και προκλήσεις.

Ο κυβερνοχώρος (cyberspace) είναι ο δυνητικός χώρος μέσα στον οποίο κυκλοφορούν τα ηλεκτρονικά δεδομένα των Η/Υ παγκοσμίως. Αυτός είναι ο ορισμός που έδωσε η Ευρωπαϊκή Επιτροπή το 2011. Σχεδόν όλα είναι στον κυβερνοχώρο. Τα κράτη και οι κρίσιμες Υποδομές εξαρτώνται όλο και περισσότερο από τα δίκτυα. Αυτό συνιστά μία «ηλεκτρονική Αχίλλειο φτέρνα ».

Τα θύματα όλων όσων συμβαίνουν στον κυβερνοχώρο ανέρχονται στα 378.000.000 ετησίως, ενώ καθημερινά έχουμε πάνω από 1.000.000 θύματα. Ενδιαφέρον είναι το γεγονός ότι τα θύματα όλων όσων συμβαίνουν στον κυβερνοχώρο ανέρχονται στα 12 το δευτερόλεπτο.

Πώς είναι όμως διαμορφωμένη η σημερινή πραγματικότητα;

- Σχεδόν 1/2 χρήστες SMARTPHONE/TABLET κοιμούνται με τις συσκευές τους σε απόσταση του "χεριού τους".
- Σχεδόν 1/2 χρήστες δεν χρησιμοποιούν μέτρα προστασίας και προφύλαξης (Passwords, Security Software ή Back Up).
- Μόνο το 26% έχει λογισμικό για Mobile Security με αυξημένους μηχανισμούς προστασίας
- 57% δεν γνωρίζει ότι υπάρχουν τέτοια λογισμικά προγράμματα

Πόσο σοβαρά παίρνουμε την επικινδυνότητα των Wi-Fi;
Όχι και τόσο σοβαρά, αν λάβουμε υπόψη τα ακόλουθα:

- 56% Πρόσβαση σε λογαριασμούς Κοινωνικών Δικτύων
- 29% Πρόσβαση σε Τραπεζικό λογαριασμό
- 3/10 Δεν κάνουν πάντα LOG OFF μετά από χρήση δημοσίων ελεύθερων WI-FI συνδέσεων
- 54% Πρόσβαση σε λογαριασμό E-MAIL
- 29% Αγορές ON-LINE
- 39% Δεν παίρνουν κανένα ειδικό μέτρο για προστασία όταν χρησιμοποιούν δημόσια WI-FI

Το 2014 αναμένεται να υπάρξει εστίαση στους τομείς:

- Προστασία της ιδιωτικής ζωής
- Έξυπνες συσκευές – Android – Κινητά
- Προηγμένα κακόβουλα λογισμικά – hi-tech malware
- BYOD – 4G δίκτυα
- CLOUD αρχιτεκτονικές
- ATM / POS

Επίσης, σημειώνεται ραγδαία η εξάπλωση των τεχνολογιών που έχουν ως βάση τα Υπολογιστικά Συστήματα Νέφους. Με τα συστήματα αυτά, παρέχεται η δυνατότητα σε χρήστες να χρησιμοποιούν υπηρεσίες και υπολογιστικούς πόρους που είναι απομακρυσμένοι. Ταυτόχρονα, τα συστήματα αυτά αποτελούν σοβαρό στόχο αφού θέτουν ένα ακόμη σημείο για επίθεση. Οι απειλές της Cloud τεχνολογίας είναι πλέον απτές και ορατές. 24% των χρηστών αποθηκεύουν επαγγελματικά και προσωπικά δεδομένα στον ΙΔΙΟ online Storage λογαριασμό.

Οι σοβαρές απειλές ασφάλειας είναι οι εξής:

- Παραβίαση Δεδομένων – data breaches
- Απώλεια Δεδομένων – data lost
- Πρόσβαση στα διαπιστευτήρια – access to credentials – account hijacking
- Ανασφαλείς διεπαφές – insecure interfaces and APIs
- Άρνηση Εξυπηρέτησης – Denial of service
- Κακόβουλοι εσωτ. χρήστες, λογισμικό – malicious insiders
- Διαχείριση Δεδομένων – Data Handling
- Κατάχρηση Σύννεφου – Cloud abuse
- Ευπάθειες Τεχνολογίας – tech vulnerabilities

Σήμερα αρκετοί οργανισμοί προκειμένου να δώσουν την δυνατότητα εργασίας και επικοινωνίας στα στελέχη τους και όταν είναι εκτός του χώρου εργασίας έχουν αναπτύξει συστήματα πρόσβασης στα δεδομένα της εκάστοτε εταιρείας με τη χρήση των προσωπικών συσκευών των υπαλλήλων. Η συγκεκριμένη τεχνολογία έχει επικρατήσει με το Bring your own device.

Έχουν όμως ληφθεί όλα τα απαραίτητα μέτρα που απαιτούνται προκειμένου να υπάρχει η διασφάλιση ότι δεν θα υπάρχει κάποια είδος διαρροή αυτών των εταιρικών δεδομένων?

Έχουν αναπτυχθεί τα κατάλληλα εργαλεία και οι πολιτικές ασφαλείας που θα είναι ικανές να περιφρουρήσουν τις επικοινωνίες με τις συσκευές εκτός των τειχών της εταιρείας?

Σήμερα παρατηρείται μία γεωμετρική αύξηση τέτοιων δυνατοτήτων και παράλληλα χρήσης από τις εταιρείες... και δυστυχώς τα κρούσματα παράνομης παρείσφρησης συνεχώς αυξάνονται.

Προκειμένου να ελαχιστοποιηθεί το κόστος επικοινωνίας, η χρήση της τεχνολογίας VOIP έχει αποτελέσει σημαντικό εργαλείο ιδιαίτερα σε μεγάλες επιχειρήσεις (telecommunication, banking, retail).

Έχουμε όμως λάβει υπόψιν μας τις πιθανές απειλές που υπάρχουν;

Πρόσφατα ερευνητικές ομάδες πανεπιστημίων (AUEB κ. Γρίτζαλης) έχουν αναπτύξει εργαλεία προκειμένου να αντιμετωπίσουν Απειλές Denial of Services. (αδυναμία λειτουργίας)

Ο λόγος είναι ότι παρατηρήθηκε ότι υπάρχει η δυνατότητα αποστολής μαζικών κλήσεων (bot) οι οποίες δεν θα μπορούν να διακριθούν από τις πραγματικές κλήσεις. Σήμερα έχουν γίνει τα πρώτα βήματα για τον διαχωρισμό και την αντιμετώπιση του φαινομένου, είναι όμως μία περιοχή που θα αποτελέσει πρόκληση για την Υπηρεσία μας.

Τα συστήματα πληρωμών με την χρήση καρτών αποτελούν μία πολύ χρήσιμη και ασφαλή διαδικασία πληρωμής υπηρεσιών και αγαθών. Η ανάγκη διασφάλισης των πολιτών για τις συναλλαγές τους έχει ενεργοποιήσει το σύνολο των εμπλεκομένων για ολοένα και πιο σύγχρονα μέτρα προστασίας.

Ο λόγος της συνεχούς επαγρύπνησης είναι προφανής.

Η χρήση των νέων τεχνολογιών έχει γίνει εργαλείο και για τους κακόβουλους χρήστες που έχουν ως σκοπό να διαπεράσουν τα συστήματα ελέγχου και να παρεισφρήσουν στα τραπεζικά δεδομένα των πολιτών και των οργανισμών με σκοπό το οικονομικό όφελος. Κάθε αντικείμενο είτε παράγει κάποια μορφή πληροφορίας είτε όχι, θα έχει πάνω του κάποιες πληροφορίες.

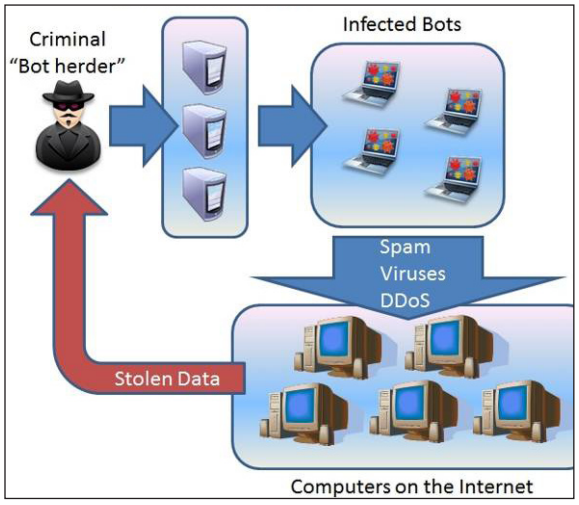
Για παράδειγμα μπορούμε να δούμε τα ρούχα στα καταστήματα. Σήμερα με την χρήση των ετικετών RFID γίνεται ο έλεγχος αντικλεπτικού συστήματος καθώς και η πληρωμή στα ταμεία. Επιπλέον αρκετές εταιρείες έχουν αναπτύξει συστήματα εφοδιασμού με βάση τι έχει περάσει από το ταμείο. Επιπλέον, κάθε έξυπνη ηλεκτρονική συσκευή έχει πλέον δυνατότητα διασύνδεσης με το www. Η ύπαρξη ενός τεράστιου συνόλου από αντικείμενα που θα έχουν άγνωστες πολλές φορές δυνατότητες μπορεί να αποτελέσει ένα εν δυνάμει κακόβουλο στρατό από επιτιθέμενα αντικείμενα που εν αγνοίας τους θα εκτελούν εντολές άλλων. Στα επόμενα χρόνια θα αλλάξει ο τρόπος επιλογής των ρούχων μας. Θα αναζητάμε στο κάθε προϊόν που αγοράζουμε την εφαρμογή (app) που έχει αναπτύξει η εταιρία που τα παράγει ώστε να είμαστε on-line.

Στην χώρα μας ακούμε πολύ συχνά τον όρο ηλεκτρονική διακυβέρνηση, και οι περισσότεροι έχουν την αντίληψη ότι πρόκειται για τον εκσυγχρονισμό του κράτους και τις υπηρεσίες που προσφέρει.

Λογικό είναι να έχουμε αυτήν την εικόνα. Σκεφτείτε όμως οι ηλεκτρονικές υπηρεσίες δεν είναι μόνο αυτές που καθημερινά βλέπουμε σαν πολίτες αλλά και αρκετές άλλες, που σύντομα πι-

θανώς θα υλοποιηθούν και στη χώρα μας. Πχ. Αυτοματοποιημένο σύστημα καταγραφής ιατρικού ιστορικού, διαχείριση επικοινωνιών και εγγράφων δημόσιων οργανισμών (Government community cloud.)

Τελευταία, παρατηρείται μια τάση να προσφέρεται το έγκλημα ως Υπηρεσία (Crime as a Service).



Τί σημαίνει όμως αυτό; Οργανωμένες ομάδες προσφέρουν παράνομες υπηρεσίες επί πληρωμή.

Σημαντικός είναι ο ρόλος των "botnets". Τα botnets είναι διαθέσιμα προς πώληση σε όποιον ενδιαφέρεται (χωρίς να έχει τεχνικές γνώσεις) να πράττει επιθέσεις στον κυβερνοχώρο. Οι εγκληματίες δεν περιορίζονται στις δικές τους τεχνικές γνώσεις για την εφαρμογή των σχεδίων τους. Μια νέα αγορά: έχει ήδη δημιουργηθεί...Botnets-as-a-Service (BaaS).

Τί είναι το Bitcoin

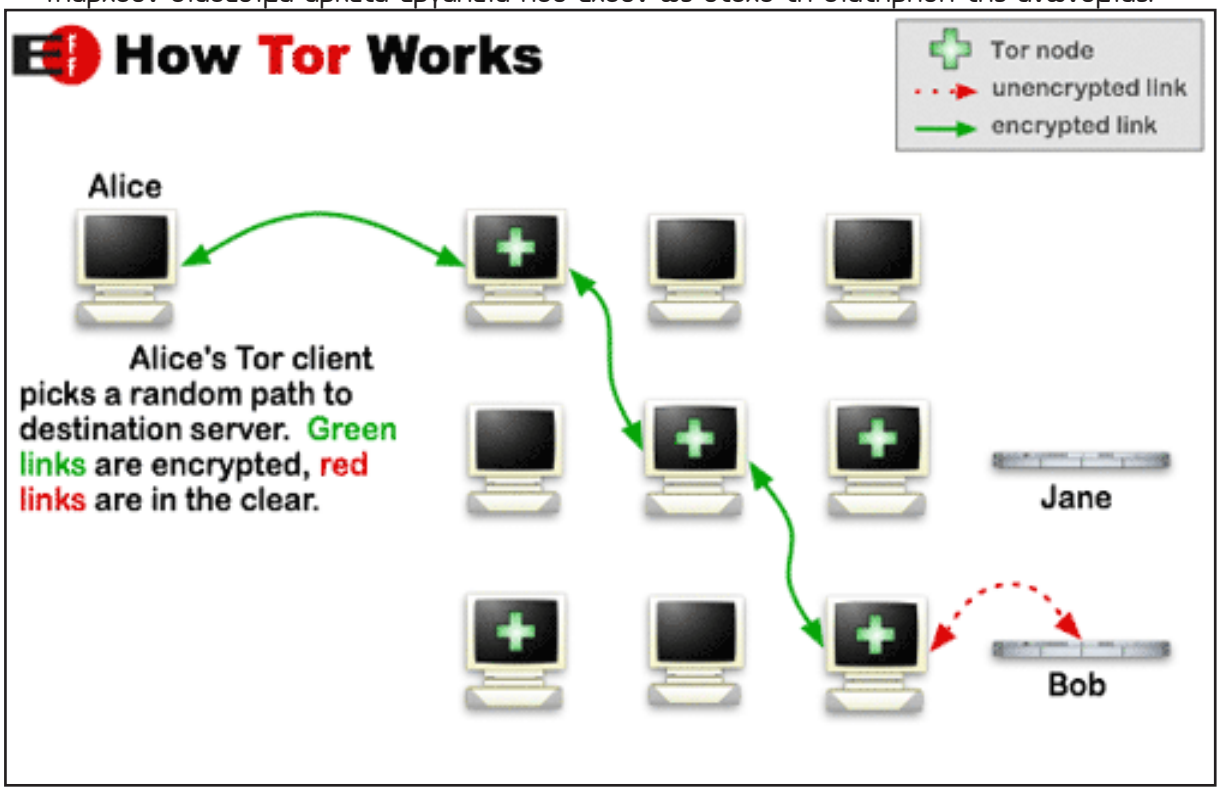
Αποκεντροποιημένο (decentralized) σύστημα μεταφοράς εικονικών χρημάτων. Δεν είναι συνδεδεμένο σε τραπεζικό σύστημα ή επίσημη αρχή. Οι χρήστες στέλνουν και λαμβάνουν bitcoins έχοντας λογισμικό πορτοφόλι σε Η/Υ, κινητό ή στο διαδίκτυο. Οι δοσοληψίες δεν μπορούν να εντοπιστούν εύκολα, έτσι αποτελούν εργαλείο παράνομης διακίνησης κεφαλαίων. Το νόμισμα είναι δημοφιλή στο «dark net», που μεταξύ άλλων διευκολύνει παιδική πορνογραφία, ναρκωτικά, όπλα, κλπ. Πρόσφατα πανεπιστημιακό ίδρυμα έκανε δεκτό το bitcoin ως τρόπο πληρωμής. Στον Καναδά υπάρχει είδη ATM. Ομάδα του NBA δέχεται παραγγελίες με βάση το εικονικό νόμισμα. Οι εξελίξεις είναι ταχύτατες αλλά ακόμα και τα πιο σύγχρονα κράτη στο κόσμο αδυνατούν να δώσουν με ασφάλεια κάποιες πληροφορίες για τον τρόπο αντιμετώπισης τυχόν παράνομων δραστηριοτήτων με την χρήση εικονικών χρημάτων.

robot-network: αριθμός Η/Υ που έχει μολυνθεί από κακόβουλο λογισμικό (malware) και έχει μετατραπεί σε zombie. Ο ιδρυτής ελέγχει απομακρυσμένα τους Η/Υ και ονομάζεται «bot master»

Τον τελευταίο χρόνο έχουν εξαπλωθεί, έχουν αντοχή, κρύβονται σε TOR και εστιάζουν σε νέους στόχους.

Εργαλεία Ανωνυμίας

Υπάρχουν διαθέσιμα αρκετά εργαλεία που έχουν ως στόχο τη διατήρηση της ανωνυμίας.



Παράδειγμα τέτοιων εργαλείων είναι το λογισμικό Tor.

Με τη χρήση του πραγματοποιούνται κρυπτογραφημένες συνδέσεις και μέσα από ένα δίκτυο συσκευών επιτυγχάνεται η διατήρηση της διαδικτυακής ανωνυμίας.

Υπάρχουν "λειτουργικά συστήματα" που έχουν ως αποκλειστικό σκοπό την πλήρη απόκρυψη της ταυτότητας του χρήστη. Έχουν δυνατότητα να εκτελούνται χωρίς να απαιτείται η εγκατάσταση για τη χρήση τους.

Μετάβαση από IPv4 σε IPv6

Κρίνεται αναγκαία από διεθνής οργανισμούς (Internet Engineering Task Force/IETF) καθώς δεν επαρκούν οι ηλεκτρονικές διευθύνσεις (IPv4).

Ηλεκτρονικό Ίχνος = IP διεύθυνση + χρονοσήμανση

IPv4: ο εντοπισμός του δράστη είναι δυσχερέστερος καθώς γίνεται χρήση τεχνολογιών NAT που επιτρέπουν καταχώρηση της ίδιας ηλεκτρονικής διεύθυνσης σε πολλαπλές συσκευές.

IPv6: Είναι πιο σύγχρονο. Περιέχει πρωτόκολλα που εξασφαλίζουν την προστασία της ιδιωτικής ζωής και την ασφάλεια.

Συμπέρασμα

Δεν μπορούμε να σταματήσουμε κάθε επίθεση...

...μπορούμε να εξασφαλίσουμε την ασφάλεια πληροφοριών, συστημάτων και δικτύων μας.

Στα επόμενα έτη, θα αντιμετωπίσουμε πολυπλοκότερες και νέες μεθόδους παρείσφρυσης, τεχνικές hacking. Οι εγκληματίες ανακαλύπτουν συνεχώς και εκμεταλλεύονται τις ευπάθειες στο λογισμικό και δίκτυά μας. Έχουν γίνει περισσότερο επαγγελματιές: Είναι οργανωμένοι... δικτυωμένοι... μοιράζονται εργαλεία, κλεμμένα στοιχεία, και τεχνογνωσία.

Σε απάντηση, εμείς θα συνεχίσουμε να αναπτύσσουμε τεχνικές δεξιότητες και εργαλεία ώστε να αποτρέψουμε τις παρεισφρύσεις και να περιορίσουμε τη ζημία. Αλλά δεν θα είμαστε σε θέση να μηδενίσουμε-εξαλείψουμε όλες τις ευπάθειες. Δεν μπορούμε να σταματήσουμε κάθε επίθεση.

Κυρίες και Κύριοι, Δεν έχω τις απαντήσεις για το πώς θα χτίσουμε καλύτερες αρχιτεκτονικές ασφάλειας από αυτές που χρησιμοποιούνται σήμερα, αλλά αισθάνομαι την ανάγκη να δηλώσω, ότι οι συζητήσεις πρέπει να αρχίσουν σήμερα-τώρα. Αλλωστε οι λύσεις ανήκουν κυρίως στους Ακαδημαικούς, στους τεχνολόγους, τον Ιδιωτικό τομέα.

Σας προτρέπω λοιπόν, να αναλογιστείτε γνωρίζοντας τη φυσική εξέλιξη των πραγματων, αν υπάρχει ανάγκη και απαίτηση να αναπτυχθούν δικτυακά περιβάλλοντα τέτοια, που να απαιτούν λιγότερη υπεράσπιση, και να στηρίζονται περισσότερο στην ταυτοποίηση του χρήστη, ανακάλυψη των δραστών κάθε κυβερνοαπειλής-κυβερνοεπίθεσης. Αλλωστε πρέπει να αντιληφθούμε ότι πίσω από κάθε παρείσφρυση είναι κάποιο ατομο υπέυθυνο, είτε βρίσκεται στην Ελλάδα ή Ευρώπη ή Αμερική, κλπ.

Ενα ανοιχτό έθνος δεν μπορεί να κλείσει τα συστήματα στον κυβερνοχώρο για το φόβο των κυβερνοαπειλών. Είναι μονοδρομος. Πρέπει να συνεχίσουμε προς τα εμπρός, ανεξάρτητα αν οι αντίπαλοί μας είναι επικίνδυνοι. Γνωρίζουμε ότι θέλουν τα χρήματά μας, την ιδιοκτησία μας, τα μυστικά μας. Μαζί, μπορούμε να στραφούμε ενάντια τους και να υποστηρίξουμε-εξασφαλίσουμε την ασφάλεια των πληροφοριών, των δικτύων και της κρίσιμης υποδομής μας. Σας ευχαριστώ.

«Διαδίκτυο: δυνατότητες της τεχνολογίας – προστασία του πολίτη»

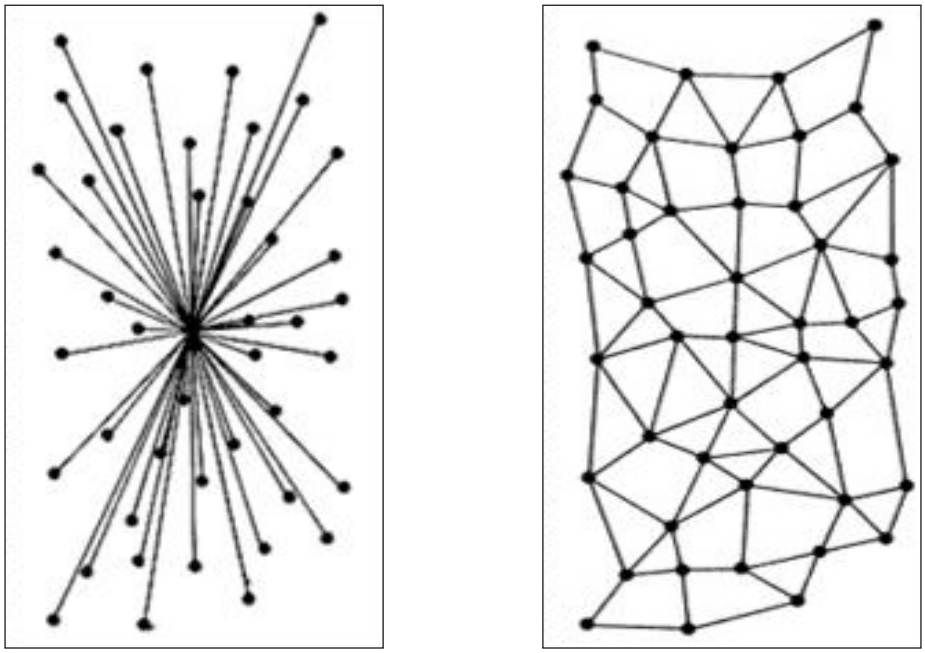
Καθηγητής **Ιωάννης Σ. Βενέρης**,
Εθνικό Μετσόβιο Πολυτεχνείο

Εδώ εξετάζουμε τη δημιουργία, ανάπτυξη και κρίση του Διαδικτύου και του Παγκόσμιου Ιστού.

Διακρίνουμε δύο περιόδους, που συμβολικά αποκαλούμε «Περίοδος της (σχετικής) αθωότητας» και «Περίοδος του Φόβου».

Η περίοδος της (σχετικής) αθωότητας: οι απαρχές και η έκρηξη –2013

Το Διαδίκτυο (που είναι ένα υπερσύνολο του Παγκόσμιου Ιστού) ξεκίνησε στην εποχή του Ψυχρού Πολέμου, ως τρόπος εξασφάλισης της λειτουργίας των πολεμικών υπολογιστικών συστημάτων των ΗΠΑ (του Υπ Άμυνας, των ΑΕΙ και ΕΙ, άλλων κυβερνητικών υπηρεσιών) σε περίπτωση επίθεσης από το Σύμφωνο της Βαρσοβίας, με πυραύλους, βομβαρδισμό ή δολιοφθορά. Ο βασικός στόχος ήταν να αποφευχθεί συντριπτικό πλήγμα με την καταστροφή ενός ή περισσότερων κέντρων υπολογιστών ή κόμβων δικτύου (Εικόνα 1).



Εικόνα 1 Η γενική ιδέα για ένα δίκτυο ΗΥ με πολλαπλές οδεύσεις. Το δίκτυο να λειτουργεί, ακόμη κι αν σημαντικά μέρη δεν λειτουργούν, λόγω βλάβης ή επίθεσης. Κάθε κόμβος ή γραμμή που δεν λειτουργεί να μπορεί να παρακαμφθεί

Η επεξεργασία της γενικής ιδέας έγινε υπο την αιγίδα της Advanced Research Projects Agency (ARPA, U.S. Department of Defence), και στις 1/6/1968 υπεγράφη το σχετικό συμβόλαιο (Εικόνα 2).

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

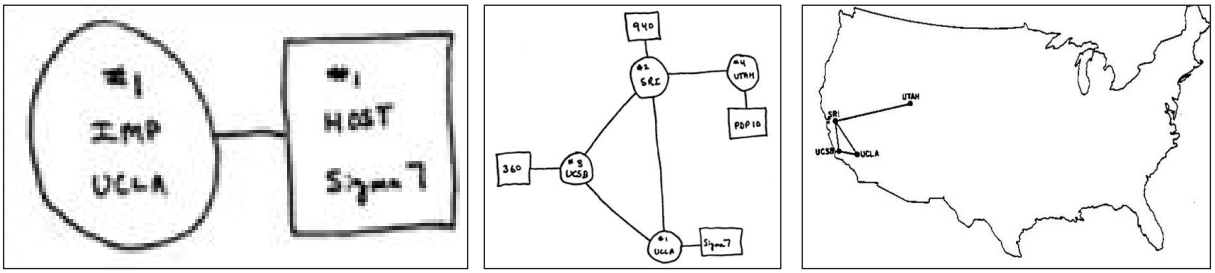
A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

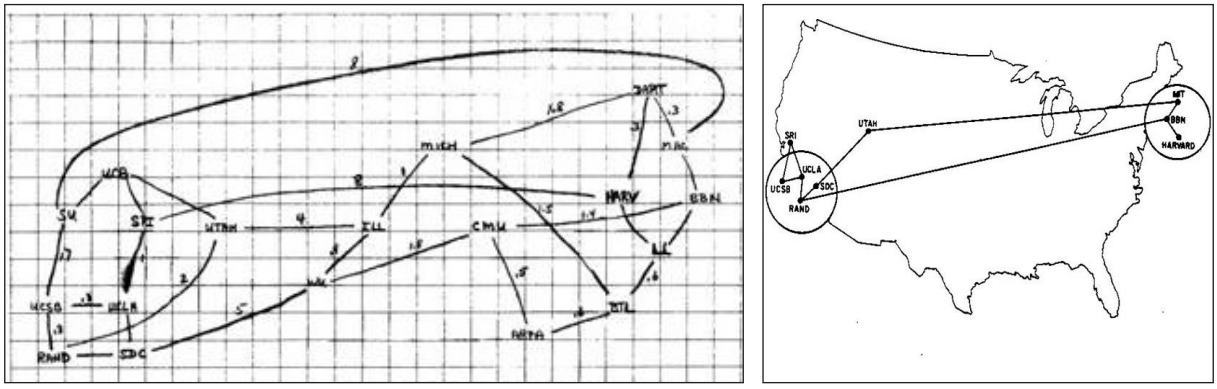
Εικόνα 3 ARPA, Συμβόλαιο ανάπτυξης δικτύου ΗΥ: οι απαρχές του Internet (τότε ARPAnet)

Μέχρι τις 9-12-1969 είχε γίνει ο πρώτος σχεδιασμός και οι πρώτες διασυνδέσεις (Εικόνα 4).

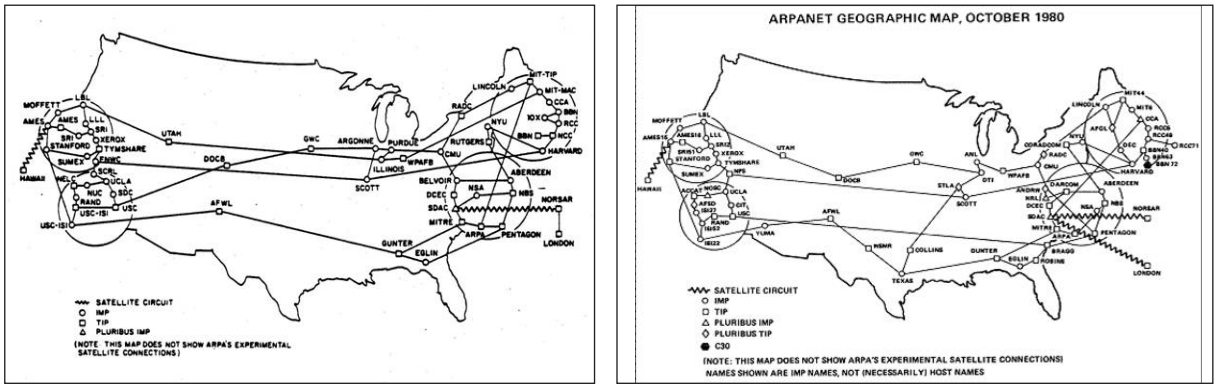


Εικόνα 4 Τα πρώτα βήματα για το ARPAnet: 9-12-1969

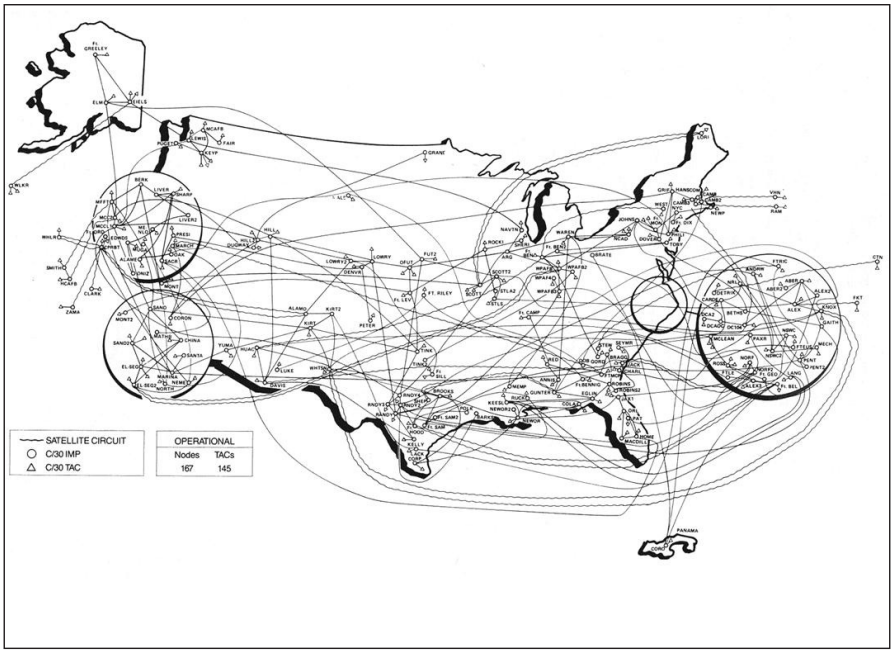
Η ανάπτυξη ήταν γρήγορη (Εικόνα 5)



Εικόνα 5 ARPAnet 6/1970

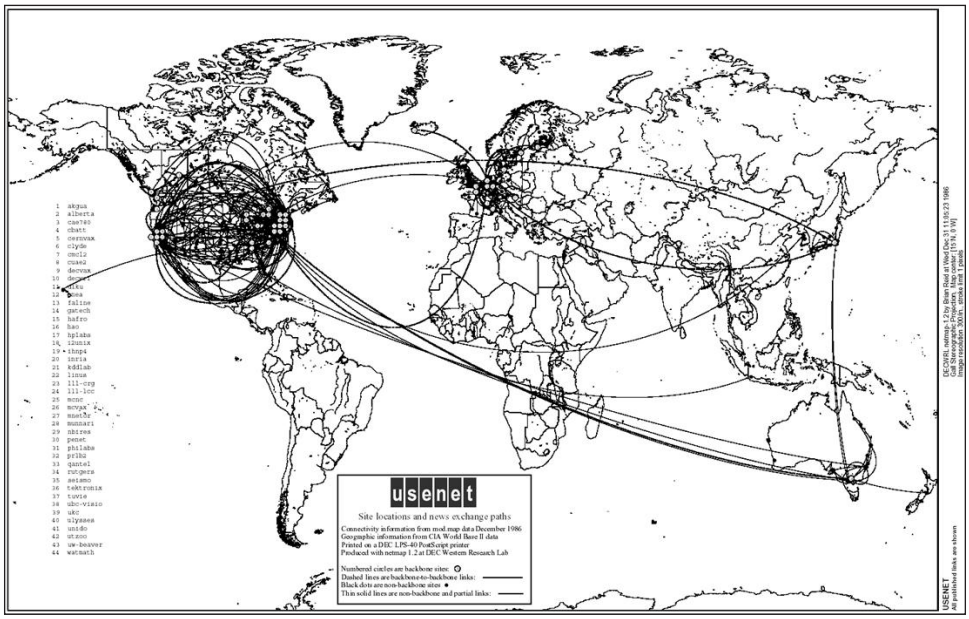


Το 1984 το στρατιωτικό MILnet αποσπάται από το ARPAnet (Εικόνα 6)



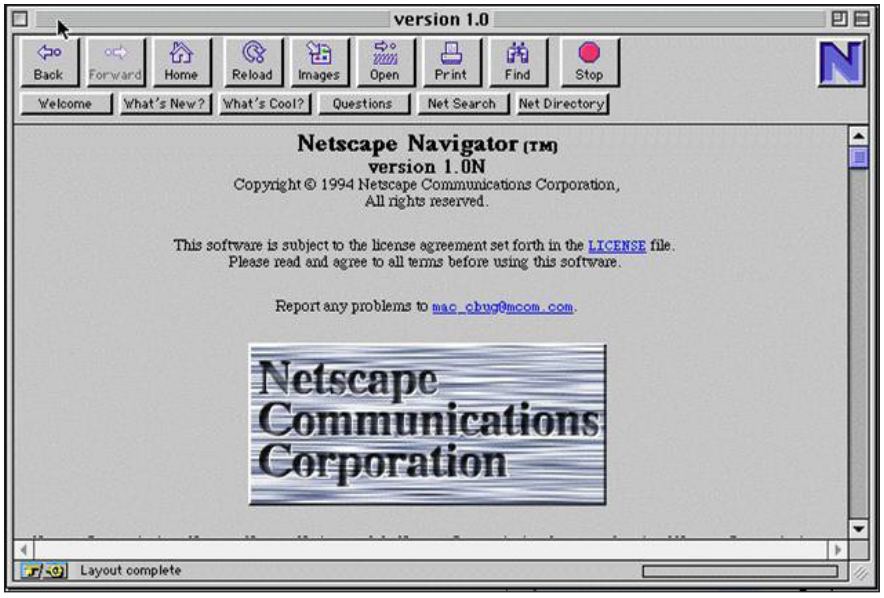
Εικόνα 6 1984: το στρατιωτικό MILnet αποσπάται από το ARPAnet

Η νέα υπηρεσία χρηστών, το USEnet αναπτύσσεται επίσης ραγδαία (Εικόνα 7).



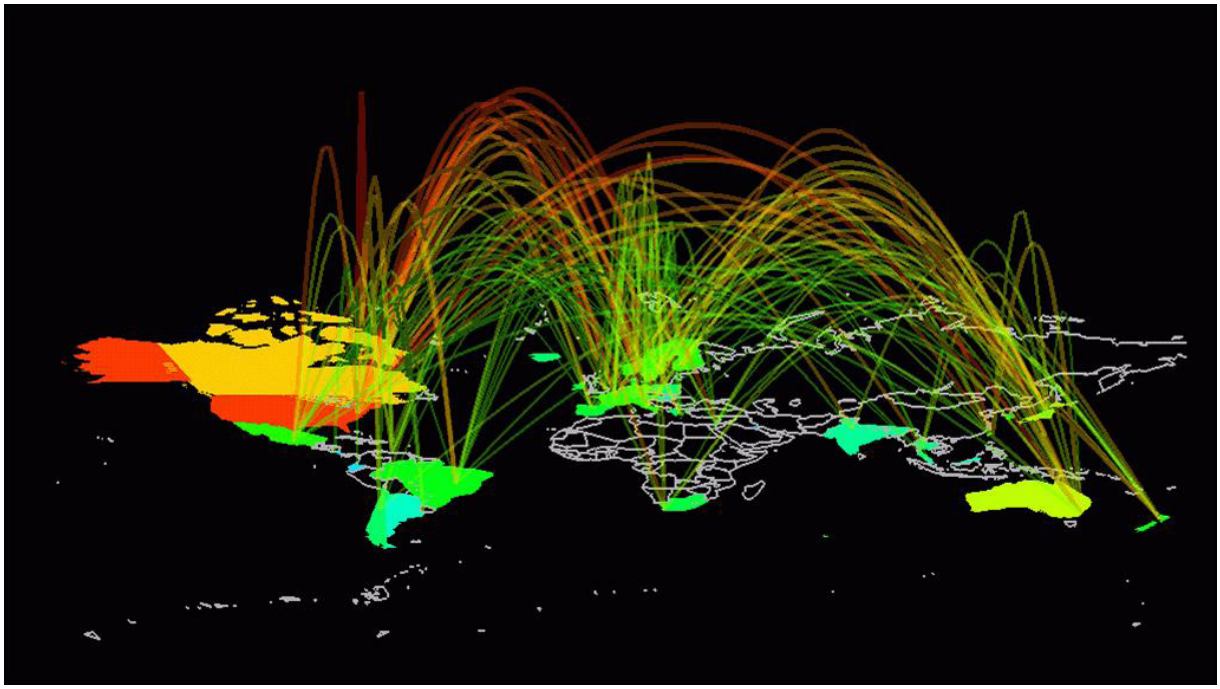
Εικόνα 7 Η νέα υπηρεσία χρηστών USEnet

Το 1994 κάνει την εμφάνισή του ο Παγκόσμιος Ιστός, το World-Wide Web, που είναι μία από τις υπηρεσίες του Internet, αν και σήμερα οι περισσότεροι ταυτίζουν, κακώς, τα δύο. Μαζί έρχεται η γλώσσα περιγραφής ιστοσελίδων με υπερσυνδέσμους, η HTML (Hyper Text Markup Language), και το πρωτόκολλο μεταφοράς ιστοσελίδων μέσω του Internet, HTTP (Hyper Text Transfer Protocol). Εμφανίζεται επίσης ειδικό πρόγραμμα 'πλοήγησης' στις ιστοσελίδες, το Netscape Navigator (Εικόνα 8).

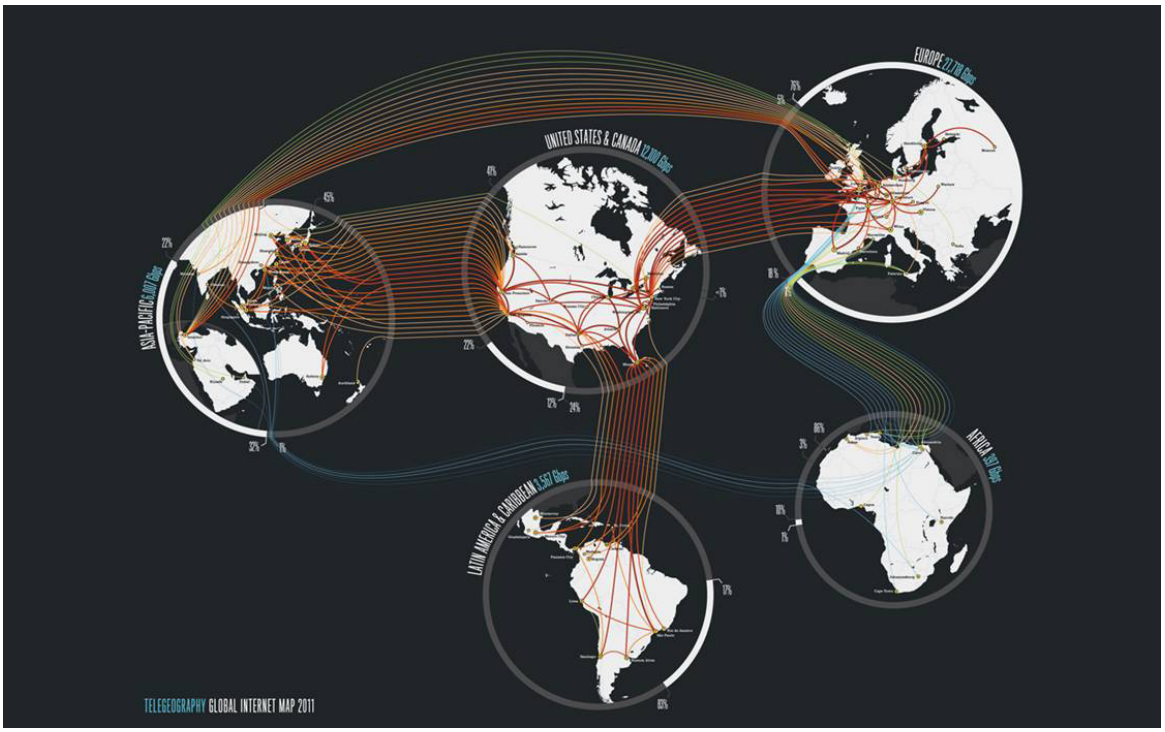


Εικόνα 8 Netscape Navigator: πρόγραμμα 'πλοήγησης' στις ιστοσελίδες

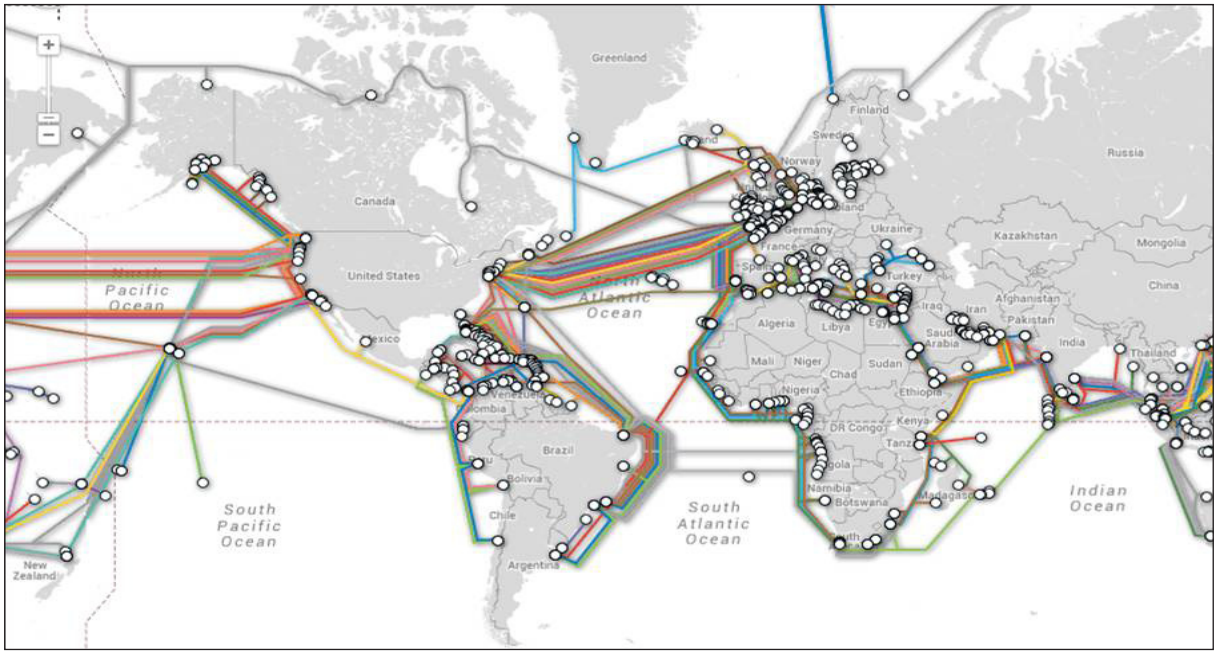
Σε μερικά χρόνια επακολουθεί η έκρηξη (Εικόνα 9 – Εικόνα 15)!



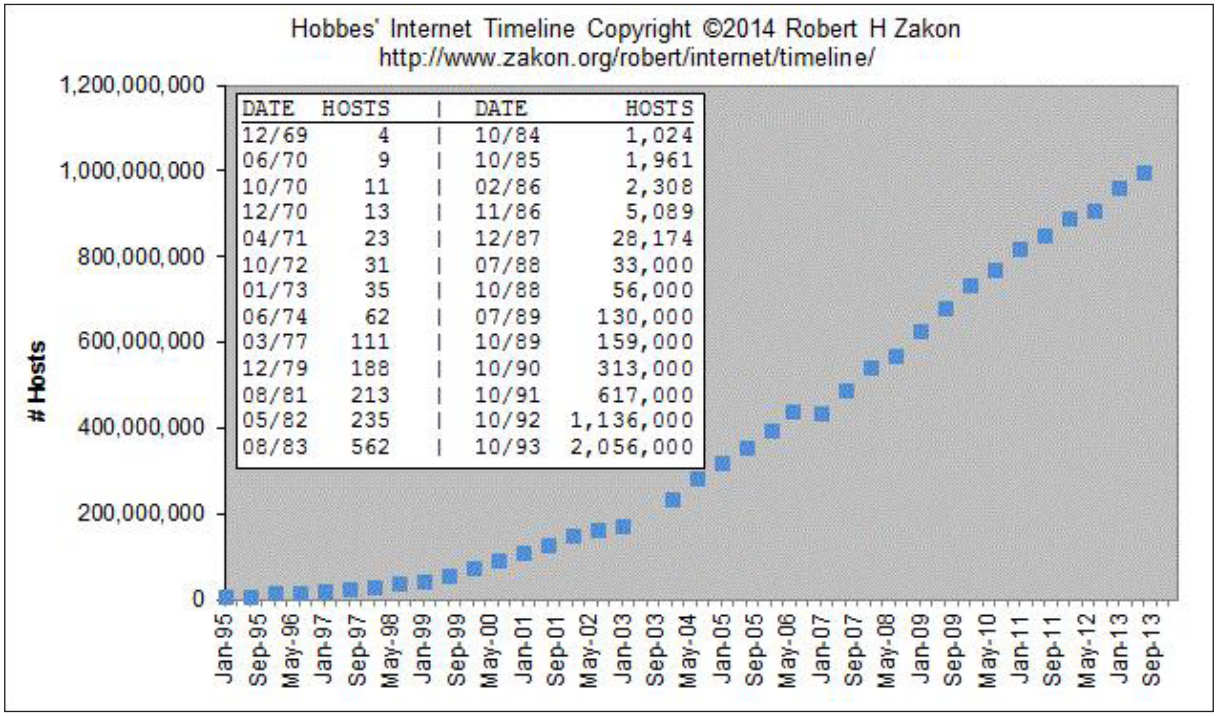
Εικόνα 9 Η έκρηξη!



Εικόνα 10 Η έκρηξη: τα βασικά κυκλώματα

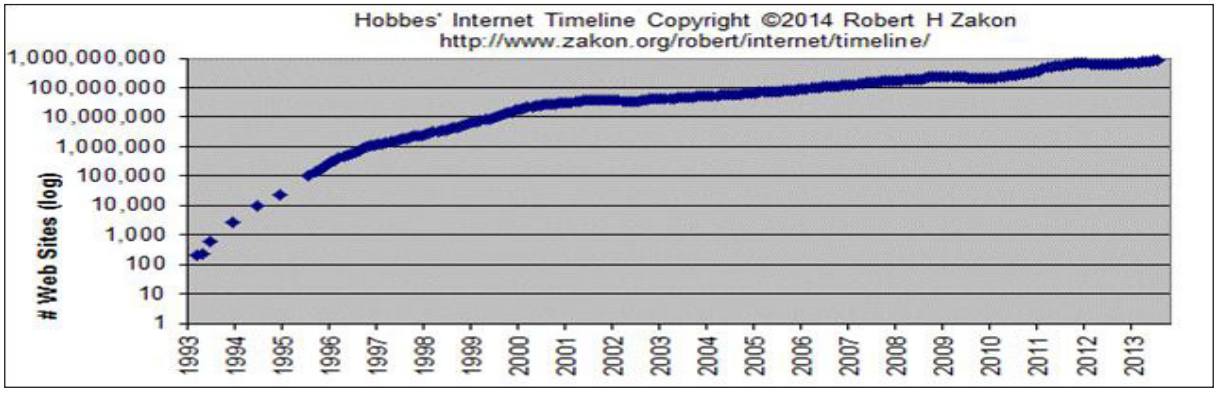


Εικόνα 11 Η έκρηξη: τα υποθαλάσσια καλώδια

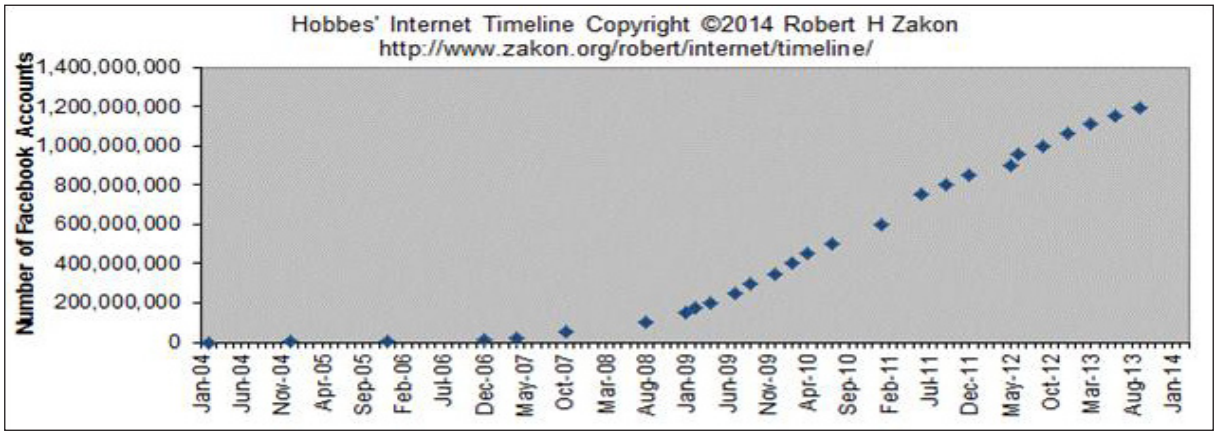


DATE	HOSTS	DATE	HOSTS
12/69	4	10/84	1,024
06/70	9	10/85	1,961
10/70	11	02/86	2,308
12/70	13	11/86	5,089
04/71	23	12/87	28,174
10/72	31	07/88	33,000
01/73	35	10/88	56,000
06/74	62	07/89	130,000
03/77	111	10/89	159,000
12/79	188	10/90	313,000
08/81	213	10/91	617,000
05/82	235	10/92	1,136,000
08/83	562	10/93	2,056,000

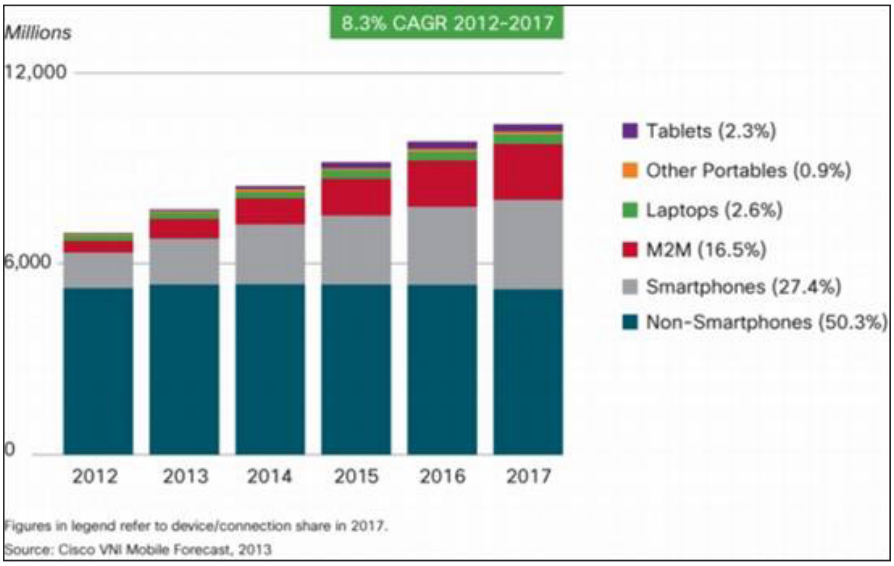
Εικόνα 12 Η έκρηξη: αριθμός συνδεδεμένων εξυπηρετητών (HY)



Εικόνα 13 Η έκρηξη: πλήθος ιστοτόπων



Εικόνα 14 Η έκρηξη: πλήθος λογαριασμών Facebook



Εικόνα 15 Δισεκατομμύρια συσκευές (όχι μόνο ΗΥ) συνδέονται στο Διαδίκτυο

Η περίοδος του φόβου: 2013 – 2014

Η περίοδος του φόβου χαρακτηρίζεται από δύο ισχυρές και επικίνδυνες για την ασφάλεια του πολίτη τάσεις:

α. Την ανάδυση του 'Μυστικού Ιστού', όπως τον έχουν αποκαλέσει και που θεωρείται ο διαδικτυακός χώρος εντός του οποίου γίνονται ενέργειες διακίνησης ναρκωτικών, πορνογραφίας και πορνείας, έως και συμβολαίων θανάτου και τρομοκρατίας (Εικόνα 16).

Εικόνα 16 Ο Φόβος του «Μυστικού Ιστού»

β. Τη μαζική παρακολούθηση και καταγραφή ιδιωτικών επικοινωνιών και διαδικτυακής δραστηριότητας πολύ μεγάλων αριθμών πολιτών, διεθνώς, από κρατικές υπηρεσίες. Μαζικές είναι και οι αποκαλύψεις των σχετικών επίσημων στοιχείων ().

Εικόνα 17 Οι αποκαλύψεις

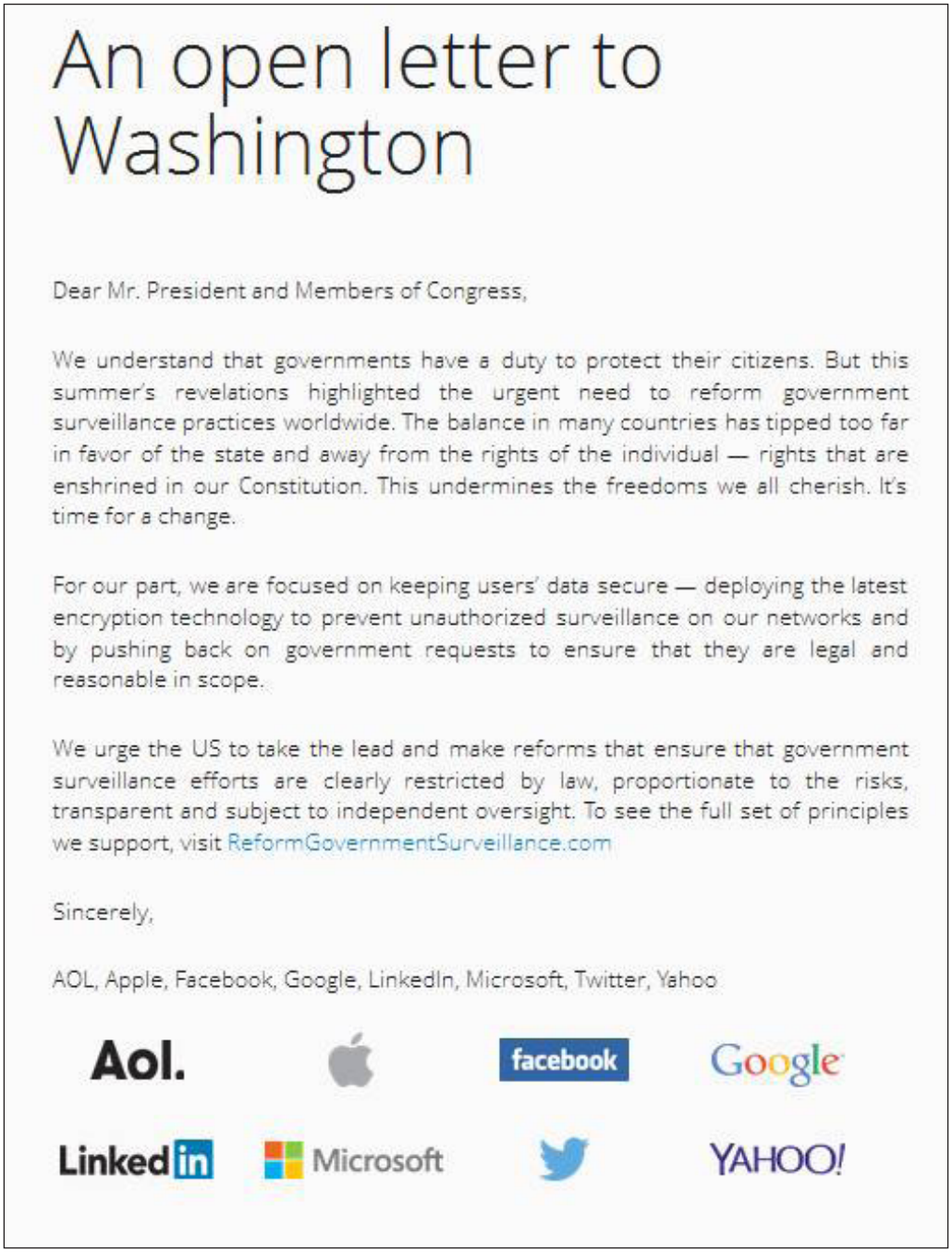
Η παράνομη αυτή δραστηριότητα φθάνει στο υψηλότατο επίπεδο (Εικόνα 18).

Εικόνα 18 Ο σύμμαχος ... 'ακούει' τη σύμμαχο

Μετά τις αποκαλύψεις, οι 'γίγαντες' του Διαδικτύου αντιδρούν. AOL, Apple, Facebook, Google, Linkedin, Microsoft, Yahoo, ενώνουν τις δυνάμεις τους και απαιτούν από τις Αρχές και την Κυβέρνηση των ΗΠΑ ουσιώδεις μεταρρυθμίσεις όσον αφορά στις παρακολουθήσεις (Εικόνα 19).

Εικόνα 19 Η εξέγερση των 'γιγάντων' εναντίον των παρακολουθήσεων από τις Κυβερνητικές Υπηρεσίες των ΗΠΑ

Απευθύνουν μάλιστα σχετική ανοικτή επιστολή προς τον Πρόεδρο και το Κογκρέσσο των ΗΠΑ (Εικόνα 20).



An open letter to Washington

Dear Mr. President and Members of Congress,

We understand that governments have a duty to protect their citizens. But this summer's revelations highlighted the urgent need to reform government surveillance practices worldwide. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual — rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It's time for a change.

For our part, we are focused on keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope.

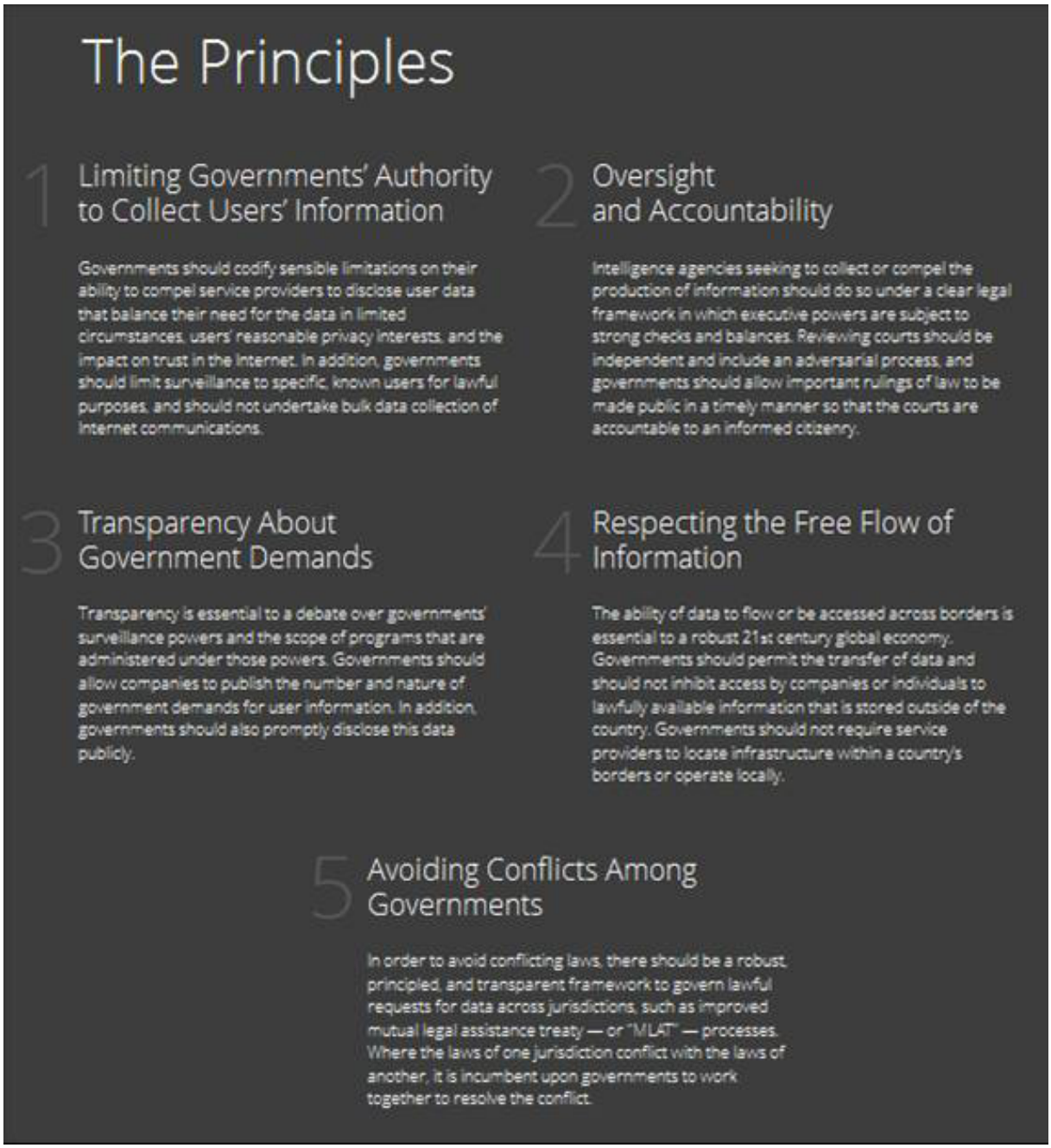
We urge the US to take the lead and make reforms that ensure that government surveillance efforts are clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight. To see the full set of principles we support, visit ReformGovernmentSurveillance.com

Sincerely,

AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo

Εικόνα 20 Ανοικτή επιστολή των μεγάλων εταιριών προς τον Πρόεδρο και το Κογκρέσσο των ΗΠΑ

Οι θέσεις τους είναι σαφείς (Εικόνα 21):
Περιορισμοί στη συλλογή προσωπικών δεδομένων
Λογοδοσία
Διαφάνεια
Σεβασμός της ελεύθερης διακίνησης των πληροφοριών



Εικόνα 21 Οι βασικές θέσεις των μεγάλων εταιριών

Υπό τις συνθήκες αυτές έρχεται η μεγάλη έκπληξη: ένας ειδικός που εργάζεται σε ιδιωτικές εταιρίες που συνεργάζονται με τις Κρατικές Υπηρεσίες των ΗΠΑ για τις παρακολουθήσεις αποκαλύπτει μεγάλο όγκο εγγράφων που δείχνουν τί συμβαίνει. Από τις ΗΠΑ χαρακτηρίζεται 'προδότης', ενώ Νορβηγοί πολιτικοί τον προτείνουν Υποψήφιο για το Νόμπελ Ειρήνης (Εικόνα 22)!

Εικόνα 22 Ο Snowden που αποκαλύπτει πληθώρα στοιχείων για τις παρακολουθήσεις προτείνεται υποψήφιος για το Νόμπελ Ειρήνης

Μέσα την καταιγίδα αυτών των αποκαλύψεων επανατοποθετείται και η υπόθεση που αναστάτωσε τη χώρα μας (). Σχετικά έγγραφα αποκαλύπτονται από το Γερμανικό περιοδικό Der Spiegel και αναπαράγονται στη χώρα μας.

Τί πήγε τόσο 'στραβά';

Έκ γενετής προβλήματα στο σχεδιασμό του Διαδικτύου και των υπηρεσιών του

Η διάδοση του Διαδικτύου ανέδειξε σοβαρά, 'εκ γενετής' θα λέγαμε, τεχνικά προβλήματα του σχεδισμού του, όπως:

- Το ARPANET συνέδεε αρχικώς υπολογιστές μόνο σε πανεπιστήμια, ερευνητικά κέντρα και

κυβερνητικές υπηρεσίες.
- Οι χρήστες και οι χώροι ήταν 'ελεγχόμενοι'.
- Κανείς δεν υποψιαζόταν *πόσοι*, και κυρίως *ποιοί*, θα ήταν οι μελλοντικοί χρήστες...!
- Οι υπηρεσίες ήταν λίγες και 'βασικές': email, e-newsgroups, remote login (πρόσβαση σε απομακρυσμένους ΗΥ), ftp (μεταφορά αρχείων).
- Ο 'εχθρός' (ΕΣΣΔ) ήταν μακρυά... ενώ η επίθεση αναμενόταν με υλικά μέσα, με πυραύλους...

Ας δούμε συνοπτικώς ορισμένα από αυτά τα προβλήματα:

α. IP: Internet Protocol – διευθύνσεις
- 'Ειλικρίνεια': Δεν ελέγχεται αν οι διευθύνσεις που εμπεριέχονται στα 'πακέτα' δεδομένων είναι αληθείς και αντιστοιχούν σε/στον πραγματικό αποστολέα, άρα
- IP 'spoofing': ένας χρήστης μπορεί να δημιουργήσει μηνύματα (packets) με όποιες IP διευθύνσεις επιθυμεί:
  - νομίμως, για δοκιμές
  - παρανόμως για να 'πλημμυρίσει' (DoS) ένας εξυπηρετητής με εισερσόμενα μηνύματα, 'διαφόρων' αποστολέων, χωρίς να φαίνεται ο πραγματικός.

β. TCP/IP, το 'θεμέλιο'
- Καθορίζει την επικοινωνία μεταξύ ΗΥ, που καθένας έχει όνομα-διεύθυνση, αλλά και
- Η πρόσβαση γίνεται μέσα από 'θύρες', που είναι λογικές θύρες, αριθμημένες (πχ Port 80). Τέτοιες 'θύρες' μπορεί να μείνουν 'ανοιχτές', να προσβληθούν από επίθεση, και να επιτρέψουν πρόσβαση στον ΗΥ.
- Αν κάποιος στείλει μηνύματα με ψευδή IP του ΗΥ_αποστολέα, ή προσποιούμενος αληθή διεύθυνση, ο ΗΥ_παραλήπτης θα προσπαθεί να απαντήσει, αλλά επιβεβαίωση δεν θα παίρνει... Η συσσώρευση τέτοιων ανοιχτών επικοινωνιών εγκλωβίζει τον ΗΥ_παραλήπτη (DoS attack).
- Το ίδιο μπορεί να γίνει, με συνεχείς κλήσεις *ping* (που γίνονται με ειδικό λογισμικό για να διαπιστωθεί αν ένας ΗΥ λειτουργεί και απαντά), στις οποίες ο ΗΥ_παραλήπτης προσπαθεί να απαντήσει και εγκλωβίζεται.

γ. SMTP: το πρωτόκολλο του email
- Θεωρεί ότι η επικοινωνία γίνεται μεταξύ *χρηστών*, όχι μεταξύ υπολογιστών. Δηλ., ποιός είναι ο χρήστης, ΚΑΙ που (=σε ποιό ΗΥ) βρίσκεται: όνομα – διεύθυνση. (Επειδή όμως δεν είναι real time, χρειάζεται ένα mailbox address.)
- Text-based: αρχικώς, μπορούσε να μεταφέρει μόνο κείμενα.
- Αρχικώς, δεν υπήρχαν domain names, άρα δεν μπορούσαμε να γράψουμε abc@ijkl.xyz.
- Επέτρεπε email 'Spoofing': όποιος θέλει μπορεί να προσποιηθεί ότι αποστέλει μηνύματα ως κάποιος άλλος! Γιατί; Επειδή ήταν βέβαιοι ότι κανείς διαπιστευμένος χρήστης της εποχής της αθωότητας δεν θα έκανε κάτι τέτοιο, αφού οι χρήστες και οι χώροι ήταν ελεγχόμενοι!

δ. Έλεγχος πρόσβασης
- δομή και μορφή συνθηματικών (user name, passwords)

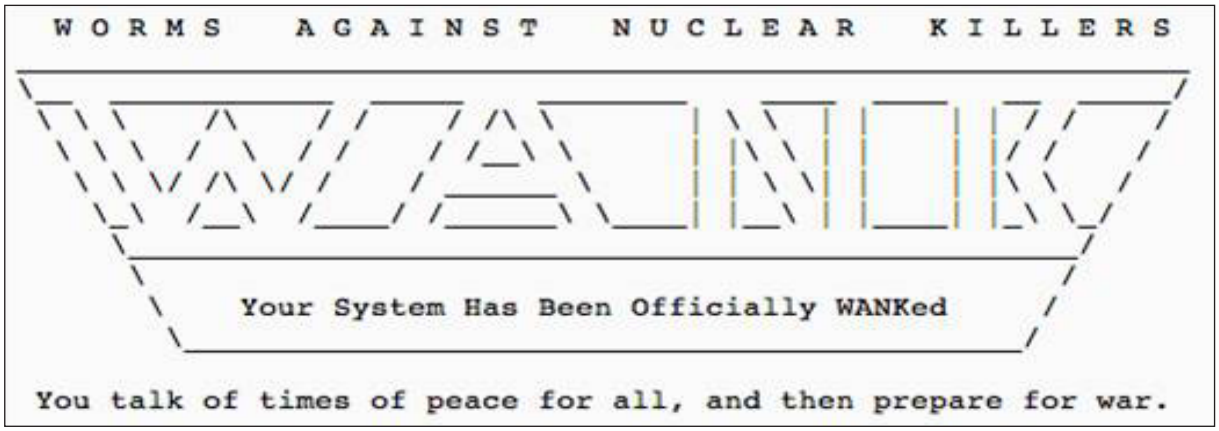
- περιορισμένος έλεγχος αναγνώρισης και δικαιωμάτων πρόσβασης χρηστών στο σύστημα
- εύκολη, μη ελεγχόμενη, πρόσβαση μέσω τηλεφωνικών (dial up) συνδέσεων, ενώ οι αριθμοί τηλεφώνου πρόσβασης ανακοινώνονταν σε ευρύ κύκλο ατόμων

Πολλά άλλα τέτοια 'εκ γενετής' προβλήματα θα μπορούσαν να αναφερθούν. Ένα εύλογο ερώτημα είναι γιατί δεν αντιμετωπίστηκαν εγκαίρως, όταν διαπιστώθηκαν. Η απάντηση δεν μπορεί να είναι άλλη από το ότι η τεράστια επιχειρηματική δραστηριότητα που αναπτύχθηκε σε σχέση με το Διαδίκτυο δεν επέτρεπε να σταματήσει η λειτουργία του Διαδικτύου για να ανασχεδιαστούν οι λειτουργίες του. Η διάδοση των προσωπικών υπολογιστών έκανε τα πράγματα πολύ χειρότερα. Αφενός, εισήλθαν μαζικά στο Διαδίκτυο νέοι χρήστες, χωρίς κατάρτιση, άρα εύκολα θύματα απατεώνων. Αφετέρου, έδωσε σε κάθε λογής παράνομο πρόσβαση σε ένα απίστευτο πριν μερικά χρόνια όγκο πληροφοριών και συστημάτων.

Τα αποτελέσματα:
- Παραβιάσεις κεντρικών συστημάτων
- Παραβιάσεις προσωπικών ΗΥ

Παραδείγματα πρώιμων διαδικτυακών επιθέσεων

Η τεχνολογία των διαδικτυακών επιθέσεων αναπτύχθηκε πολύ νωρίς. Θα αναφέρουμε ορισμένους χαρακτηριστικούς 'σταθμούς':
- 1967: διαπιστώνονται ορισμένα προβλήματα και η (D)ARPA δημιουργεί την Task Force on computer security
- 1970: RAND Report για το ίδιο θέμα
- 1980–: Οι *προσωπικοί υπολογιστές* εμφανίζονται και αυξάνουν ραγδαία τον αριθμό των 'αγνώστων' χρηστών.
- 1988: 'Σκώληξ' (worm) του Morris. Ο πρώτος 'ιός', λογισμικό δηλαδή που μπορεί να προσβάλει υπολογιστικά συστήματα και να αυτοαναπαραχθεί, αν και αρχικώς δεν είχε κακόβουλους στόχους.
- 1989: WANK 'σκώληξ' με πολιτική 'στόχευση' (Εικόνα 23)



Εικόνα 23 WANK ένας 'σκώληξ' με πολιτική στόχευση

Και ορισμένα στοιχεία πρώϊμων επιθέσεων:

- Εμφανίζονται οι crackers, δηλαδή κακόβουλοι χάκερς (Chaos –Γερμανία, Warelords –ΗΠΑ, 414 –ΗΠΑ)
- 1994: Ρώσσοι κράκερς κλέβουν διαδικτυακά $10 εκ. από τη Citibank και τα 'κρύβουν' σε διάφορους προορισμούς.
- Οι χάκερς γίνονται θέμα στον κινηματογράφο (πχ Sneakers, 1992)
- 1996: χάκερς παραποιούν τις ιστοσελίδες της CIA και της ΠΑ των ΗΠΑ. 250000 επιθέσεις σε συστήματα του Υπ 'Αμυνας, από τις οποίες το 65% επιτυχείς.
- 1998: 'ιός' τύπου 'Δούρειου Ίππου' (trojan, Cult of Dead Cow)

Απειλές για τον πολίτη:

Παραβίαση της 'ουδετερότητας' του Διαδικτύου

- **end-to-end**: κάθε 'τερματική' συσκευή συνδέεται με κάθε άλλη στο δίκτυο
- **best effort**: κάθε διαδικτυακός πάροχος κάνει το καλύτερο δυνατόν για να εξασφαλίσει την επικοινωνία end-to-end
- **innovation without permission**: καθένας μπορεί να εισάγει καινοτομίες στο διαδίκτυο χωρίς να ζητά την άδεια κανενός.

Όλες οι αρχές αυτές μαζί ορίζουν την ουδετερότητα του διαδικτύου που είναι ουσιώδης τόσο για την ανάπτυξη της τεχνολογίας, όσο και για την εξασφάλιση των δημοκρατικών αρχών και της ελευθερίας επικοινωνίας.

Υπονόμευση της 'ουδετερότητας' του διαδικτύου

Επιπλέον στοιχεία της 'ουδετερότητας':

- Όλη η 'κυκλοφορία' εντός του διαδικτύου είναι ισότιμη, ανεξαρτήτως: αποστολέα, παραλήπτη, περιεχομένου, ή τεχνολογίας μεταφοράς δεδομένων (πρωτόκολλα, ή μέσα).
- Οποιαδήποτε διαφοροποίηση ή απόκλιση από την αρχή της ισοτιμίας μπορεί να γίνει μόνο για τεχνικούς λόγους (πχ αντιμετώπιση φόρτου), και πρέπει να είναι:
  - Προσωρινή
  - Αναλογική
  - Στοχευμένη
  - 'Διαφανής'
  - Σύμφωνη με τους νόμους (προστασία δεδομένων, δικαιωμάτων πολίτη, κλπ)

Τεχνολογίες διαδικτύου: τα παράδοξα: απειλή ή/και προστασία

- Η ίδια τεχνολογία που μπορεί να απειλεί, συχνά, με άλλη χρήση, μπορεί να προστατεύει!
- Η τεχνολογία που χρησιμοποιείται για παράνομους σκοπούς μπορεί να έχει αναπτυχθεί από νόμιμους, ή/και κρατικούς φορείς!
- Οι κρατικοί φορείς μπορεί να χρησιμοποιούν νόμιμα ή/και παράνομα νόμιμη τεχνολογία!
- Οι πάροχοι μπορούν να ελέγχουν τις επικοινωνίες, και να 'κλειδώνουν' (domain name blocking) ανεπιθύμητες ιστοσελίδες, ακόμη και χωρίς δικαστική απόφαση, είτε για προστασία, είτε για λογοκρισία!

Ανωνυμία

Το πλαίσιο της ανωνυμίας

Οι τεχνολογίες **ανωνυμίας** επιδιώκουν να αντιμετωπίσουν τέτοιες απειλές για τα δικαιώματα του πολίτη.

Η ανωνυμία στο Διαδίκτυο ενδιαφέρει:

- Τους πολίτες, για την προστασία τους από κακόβουλους 'παρατηρητές', που παρακολουθούν τη δραστηριότητά τους με σκοπό να τους επωφεληθούν, ή από κρατικές υπηρεσίες που έχουν εκφύγει των δημοκρατικών αρχών (παρακολούθηση, λογοκρισία, κα). Η προστασία της ανωνυμίας – ιδιωτικότητας αφορά τόσο στον αποστολέα, όσο και στον παραλήπτη.
- Τις κρατικές υπηρεσίες, για την εξασφάλιση του απορρήτου των επικοινωνιών τους.
- Τους πάσης φύσεως παραβάτες του ποινικού κώδικα (εμπόριο ναρκωτικών και άλλων απαγορευμένων προϊόντων, διακίνηση 'μαύρου' χρήματος, λαθρεμπόριο, εκβιασμούς, trafficking, κλπ).

Σημαντικές επισημάνσεις:

- Η χρησιμοποίηση τεχνολογιών ανωνυμίας δεν πρέπει να καθιστά τον πολίτη ... ύποπτο!
- Ανώνυμες είναι οι σημαντικότερες ψηφοφορίες!
- Η ανώνυμη κοινοποίηση πληροφοριών για καταστάσεις που βλάπτουν τη δημοκρατία θεωρείται στοιχείο της δημοκρατίας.
- Τεχνολογίες ανωνυμίας έχουν ενσωματωθεί σε βασικά προγράμματα πλοήγησης στον Ιστό.
- Ακόμη και στα απλά τηλεφωνήματα, η απόκρυψη δεν συνομολογεί παρανομία ή όχληση. Πχ, μια κλήση για πληροφορίες σε ένα σινεμά ή μιά εταιρία δεν θέλουμε να δώσει και τον αριθμό μας, ώστε να αποφύγουμε μελλοντική όχληση, ή αναζήτηση προσωπικών στοιχείων μας.

Η ανωνυμία μπορεί να αξιοποιηθεί για την προστασία των δικαιωμάτων του πολίτη:

- Εξασφάλιση της ανωνυμίας και του απόρρητου των προσωπικών δεδομένων κατά τη χρήση διαδικτυακών υπηρεσιών.
- Είναι απαραίτητη προκειμένου να προστατευτεί ο πολίτης από την παρακολούθηση της ιδιωτικής ζωής του.
- Αφορά: email, αναζητήσεις, αγορές, τοποθεσία, κλπ. Τόσο για τα δεδομένα, όσο και για τα μετα-δεδομένα

Οι πάροχοι υπηρεσιών έχουν επίσης σημαντικό ρόλο για την προστασία των δικαιωμάτων του πολίτη.

Δεν πρέπει να:

- επεξεργάζονται τα στοιχεία αποστολέα-παραλήπτη, παρά μόνο για τεχνικούς λόγους
- 'διαβάζουν' το περιεχόμενο των μηνυμάτων, παρά μόνο σε περιπτώσεις: δικαστικής εντολής, στοχευμένης αναζήτηση στοιχείων επίθεσης (πχ συνημμένα που φέρουν ιούς), αλλά ποτέ σε μαζική κλίμακα, χωρίς στόχευση
- να πωλούν τα στοιχεία επικοινωνίας των συνδρομητών σε διαφημιστικές ή άλλες εταιρίες, ούτε να τα διαθέτουν σε Κρατικές Υπηρεσίες χωρίς δικαστική εντολή.

Ενώ οφείλουν να:

- μεριμνούν για την παρεμπόδιση διακίνησης μηνυμάτων με απόκρυψη ή παραποίηση στοι-

χείων αποστολέα.

- ελέγχουν και διακόπτουν ιστοσελίδες που διακινούν πληροφορίες με απαγορευμένο (πχ παιδική πορνογραφία) ή επικίνδυνο περιεχόμενο (πχ μέθοδοι φόνου ή αυτοκτονίας)
- διαφυλάσσουν τα στοιχεία των συνδρομητών τους από υποκλοπή, ιδίως μαζική υποκλοπή.
- παρεμποδίζουν συκοφαντικά, υβριστικά, κλπ σχόλια, σε ανοικτά blogs
- Επειδή συνήθως η IP του χρήστη είναι γνωστή στον πάροχο, ενισχύεται η τάση χρησιμοποίησης τεχνολογιών ανωνυμίας από τους χρήστες.

Η ανωνυμία είναι σημαντική κατά την πλοήγηση στον Ιστό, επειδή οι πάροχοι σχετικών υπηρεσιών εφαρμόζουν τεχνικές 'ανώδυνης' παρακολούθησης. Παραδείγματα:

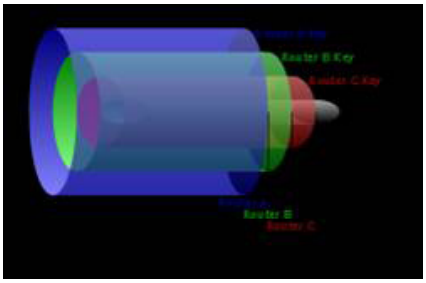
- 'Cookies': ο πιό συνήθης τρόπος. Μικρά αρχεία, συνήθως χωρίς κακόβουλο περιεχόμενο, με τα οποία οι πάροχοι συλλέγουν στοιχεία χρηστών.
- Οι στοχευμένες διαφημίσεις αποδεικνύουν την παρακολούθηση, αξιοποιώντας (βλ About Google Ads):
  - τις αναζητήσεις μας
  - το περιεχόμενο των μηνυμάτων email
  - τις αγορές μας
  - τη θέση μας
- Botnets (ro-Bot – net-work)
  - Νόμιμη χρήση: για τη διαχείριση διαύλων Internet Relay Chat (IRC), και την προστασία τους από ανεπιθύμητους χρήστες (Παράδειγμα: eggdrop).
  - Παράνομη χρήση: εγκατάσταση σε ΗΥ που η ασφάλειά τους έχει παραβιαστεί, και μετατροπή τους σε φορέα (bot, zombie): μαζικής διακίνησης μηνυμάτων (spam), επιθέσεων τύπου DoS, κλπ, μέσω νόμιμων οδών (όπως IRC, HTTP). Μπορούν να περάσουν τον έλεγχο του ΗΥ στον αποστολέα του bot.
  - Τρόπος εγκατάστασης: ο ίδιος ο χρήστης μπορεί να παραπλανηθεί για να εκτελέσει κακόβουλο λογισμικό, που ο οδηγήθηκε να κατεβάσει στον ΗΥ του!, ίσως μέσω trojan που ήρθε με μήνυμα email.

Τεχνολογίες ανωνυμίας

Βασικές τεχνολογίες έχουν αναπτυχθεί από κρατικούς φορείς και επίσημα ερευνητικά κέντρα!

Παράδειγμα, η τεχνολογία 'onion', που ονομάζεται έτσι επειδή προσομοιάζει στα διαδοχικά στρώματα του ... Κρεμμυδιού (υπάρχει και τεχνολογία 'σκόρδου'!).

Αναπτύχθηκε από το Ναυτικό των ΗΠΑ (Naval Research Lab) και στη συνέχεια χρηματοδοτήθηκε από το Electronic Frontier Foundation.



Τώρα αναπτύσσεται από την The Tor Project.

Υπάρχουν αρκετές άλλες τεχνολογίες ανωνυμίας, όπως οι λεγόμενες peer-to-peer (p2p), που μπορούν να δημιουργούν εναλλακτικά δίκτυα:

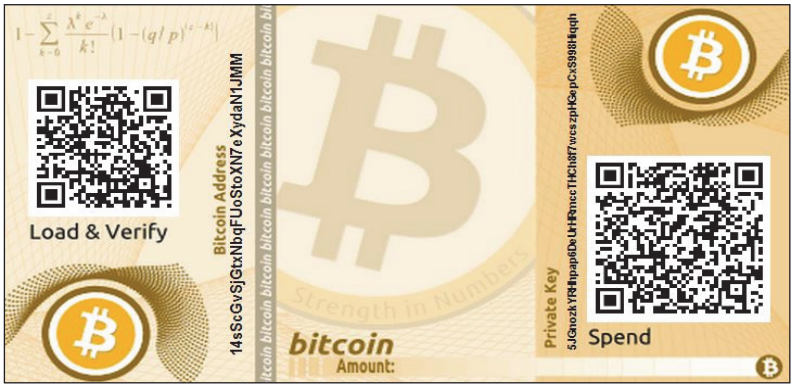
I2P

napster

Για την ανωνυμία των συναλλαγών έχει αναπτυχθεί και το ψηφιακό χρήμα, όπως το διαδεδομένο 'bitcoin', το οποίο:

bitcoin

- είναι κρυπτογραφημένο
- δεν ταυτοποιούνται οι συναλλασσόμενοι
- χρησιμοποιείται σε συστήματα p2p
- συνδυάζεται με 'ψηφιακό πορτοφόλι'
- αξιοποιεί το QR
- χρησιμοποιήθηκε στο Silk Road για 'μαύρες' αγορές, και το FBI κατέσχεσε, όταν το έκλεισε, 144000 bitcoins εκτιμώμενης αξίας $28.5
- κυκλοφορούν μεταλλικά και χάρτινα bitcoins



Ανωνυμία μέσω Κρυπτογραφίας: απόρρητο των μηνυμάτων

Η Κρυπτογραφία είναι πανάρχαιο μέσο διαφύλαξης μυστικών.

Διακρίνουμε:

- Τη νόμιμη χρήση: προστασία απόρρητων προσωπικών, εταιρικών, ή κρατικών δεδομένων. Προστατεύει την ελευθερία και τη δημοκρατία. Δίνει στους πολίτες τεχνικά μέσα που έχουν και οι κρατικές υπηρεσίες.
- Την παράνομη χρήση: κρυπτογράφηση πληροφοριών για παράνομες πράξεις, ώστε να αποφευχθεί ο εντοπισμός και η τιμωρία.

Έχουν αναπτυχθεί πολλές τεχνολογίες κρυπτογράφησης ψηφιακών επικοινωνιών, αρκετές από τις οποίες είναι προσιτές για το ευρύ κοινό, ενώ άλλες αξιοποιούνται κυρίως από κρατικές Υπηρεσίες.

Παρακολουθήσεις, υποκλοπές, επεξεργασία προσωπικών και εταιρικών δεδομένων

Τα συστήματα παρακολουθήσεων που έχουν αναπτυχθεί καλύπτουν όλο το φάσμα των ψηφιακών επικοινωνιών. Ορισμένα είναι εξειδικευμένα σε ένα είδος επικοινωνίας, άλλα σε περισσότερα, άλλα είναι συνδυαστικά.

Ορισμένα παραδείγματα ακολουθούν.

Σύστημα υποκλοπής κινητών τηλεφώνων: GSM/LI

Το σύστημα υποκλοπής επικοινωνιών κινητών τηλεφώνων αναπτύχθηκε επισήμως και κατά παραγγελία των Αρχών της ΕΕ (EUR-Lex-31996G1104) μαζί με την τεχνολογία GSM από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιών –ETSI. Αναφέρεται συνήθως με τον ευφημιστικό όρο Lawful interception –LI

- Επεκτείνεται για φωνή και δεδομένα, VoIP, καθώς και για ενσύρματες επικοινωνίες.
- Περιλαμβάνει όλες τις απαραίτητες λειτουργίες για την υποκλοπή.
- Ο πάροχος δεν είναι απαραίτητο να γνωρίζει την υποκλοπή.
- Στη χώρα μας γνωρίσαμε τη χρήση του σε επικοινωνίες υψηλού Κρατικού επιπέδου.

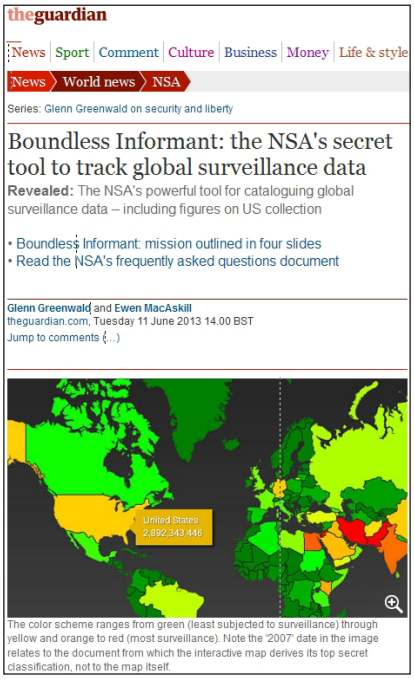
Συστήματα συλλογής και ανάλυσης δεδομένων τηλεφωνικών κλήσεων

- **ECHELON**: ΗΠΑ
  Από τα αρχαιότερα συστήματα παρακολούθησης και καταγραφής τηλεφωνικών κλήσεων, φαξ και μεταφοράς δεδομένων πολιτών από όλες τις χώρες. Συμμετείχαν: ΗΠΑ, Βρετανία, Αυστραλία, NZ, Καναδάς (τα '5 Μάτια') με δεκάδες 'σταθμούς' ανα τον κόσμο
- **Fairview και MAINWAY**: ΗΠΑ
  Μάλλον η σύγχρονη εκδοχή του Echelon, για συλλογή δεδομένων για πολίτες άλλων χωρών.
- **Frenchelon**: Γαλλία
  Παρόμοιο πρόγραμμα

Συστήματα συνδυασμένης ανάλυσης και οπτικοποίησης προσωπικών δεδομένων διαδικτύου και τηλεφωνικών κλήσεων: Boundless Informant

Η ύπαρξη του συστήματος αυτού αποκαλύφθηκε πολύ πρόσφατα (6/2013). Πρόκειται για προηγμένο σύστημα ταξινόμησης και οπτικοποίησης δεδομένων υποκλοπών, με μεγάλες δυνατότοτητες

επεξεργασίας. Αναφέρεται ότι μόνο τον Μάρτιο του 2013 επεξεργάστηκε 3 δις στοιχείων επικοινωνιών στις ΗΠΑ. Έκανε αίσθηση ότι χρησιμοποιείται κυρίως για δεδομένα υποκλαπέντα από Αμερικανούς πολίτες.

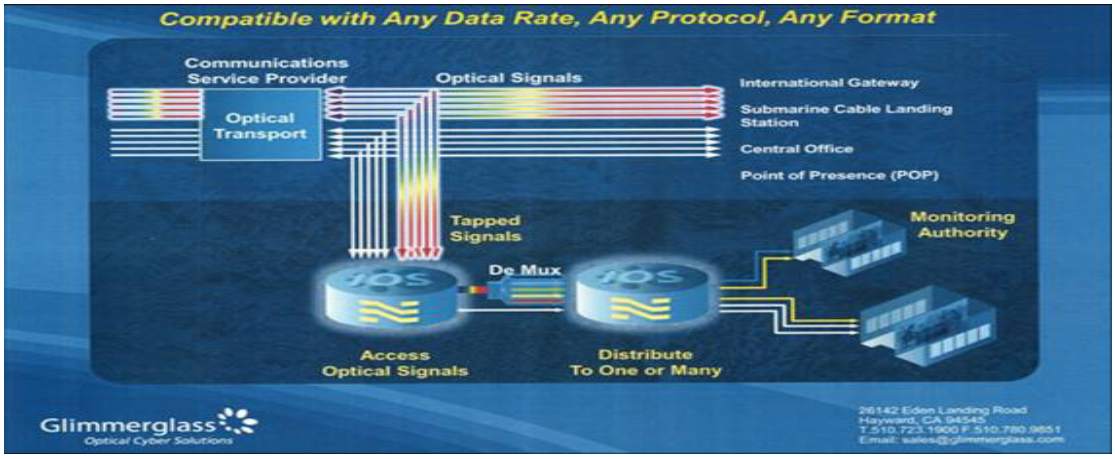


Εικόνα 24 Το σύστημα ταξινόμησης και οπτικοποίησης επικοινωνιών Boundless Informant

Συστήματα υποκλοπής δεδομένων από γραμμές οπτικών ινών

Tempora: Βρετανία, ΗΠΑ

Υποκλέπτει δεδομένα οπτικές ίνες. Συλλέγει email, FB, ιστορικό αναζητήσεων, τηλεφωνικές κλήσεις. (80% των δεδομένων που μεταδίδονται μέσω διεθνών κυκλωμάτων οπτικών ινών διέρχονται μέσω ΗΠΑ.)



Εικόνα 25 Σύστημα TEMPORA για συλλογή δεδομένων από κυκλώματα οπτικών ινών

Συστήματα παρακολούθησης και λογοκρισίας

Golden Shield (Great fireWall) Κίνα

- Αποτρέπει την πρόσβαση σε συγκεκριμένες IP, URL και DNS, ή παραπέμπει σε άλλες
- Αναλύει το περιεχόμενο των 'πακέτων' δεδομένων, αναζητώντας λέξεις 'κλειδιά'. Περιλαμβάνει αναζητήσεις, email, FTP, HTTP.
- Για 30' παρεμποδίζει επανάληψη επικοινωνιών που 'φιλτραρίστηκαν' ως άνω.

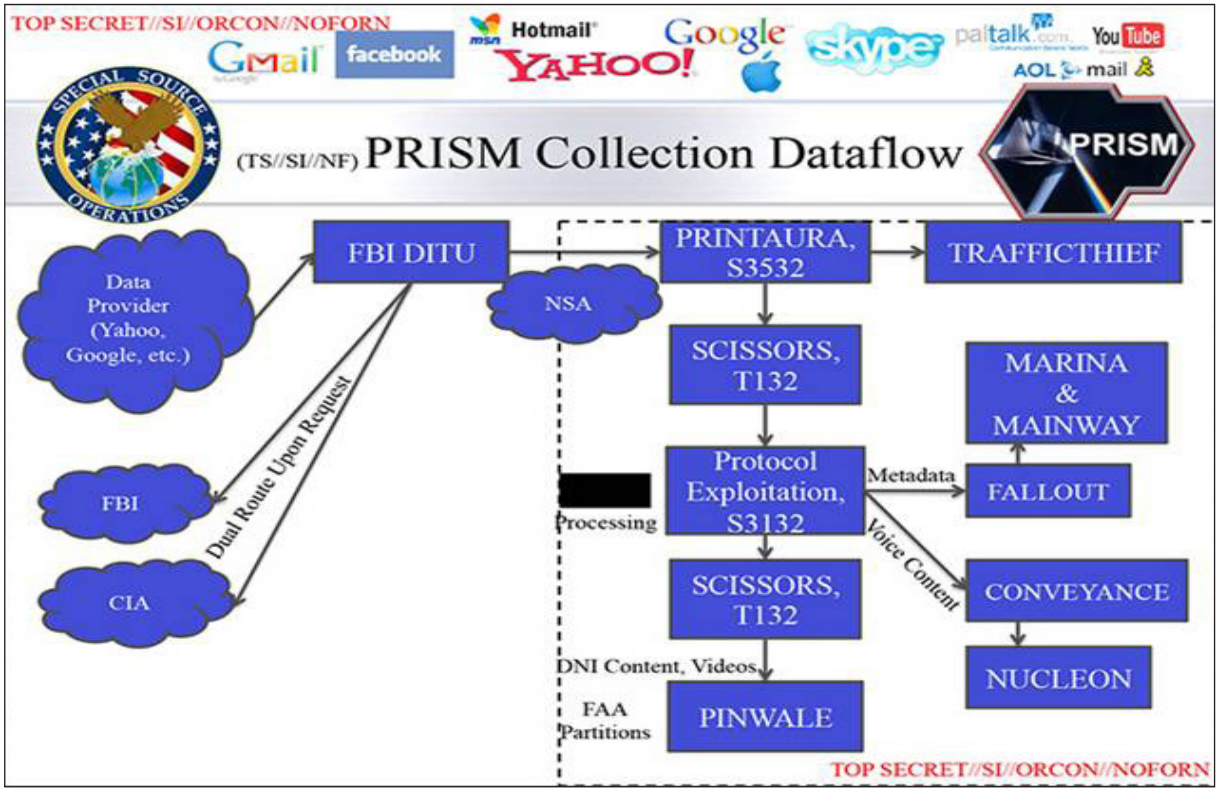
Project 6, ή P6

Διεθνής βάση προσωπικών δεδομένων ατόμων ύποπτων ως 'τζιχαντιστών

- Έδρα: Γερμανία, συνεργασία ΗΠΑ
- Συλλέγει φωτογραφίες, αριθμούς πινακίδων αυτοκινήτων, ιστορικό αναζήτησης στον Ιστό, μεταδεδομένα τηλεφωνικών κλήσεων

Συστήματα συλλογής δεδομένων Internet: ΗΠΑ, Ινδία

- **PRISM**: ΗΠΑ
  πρόγραμμα τύπου data mining. Προεδρία Bush (Protect America Act, SIGAD US-984XN). Συλλέγει δεδομένα από πηγές όπως Google, Skype, με δικαστικές αποφάσεις. Μπορεί να στοχεύει κρυπτο- επικοινωνίες, καθώς και αποθηκευμένα δεδομένα που απορρίφθηκαν από 'φίλτρα' παρόχων.
- **CMS**
  Όμοιο πρόγραμμα στην Ινδία



Εικόνα 26 Το σύστημα PRISM (ΗΠΑ)

Συστήματα καταγραφής και ανάλυσης προσωπικών διαδικτυακών δεδομένων

Narus Semantic Traffic Analyzer

Κάθε ΗΥ αυτού του τύπου μπορεί να αναλύσει (deep packet inspection) 10Gb 'πακέτων' IP και 2.5Gb δεδομένων και μηνυμάτων email το δευτερόλεπτο. Στη συνέχεια 'ανακατασκευάζει' την πληροφορία και τη μεταδίδει σε κεντρικό ΗΥ για αποθήκευση και ανάλυση. Αναφέρεται ότι δεκάδες τέτοιοι ΗΥ λειτουργούν σε εγκαταστάσεις τηλεπικοινωνιακών εταιριών.

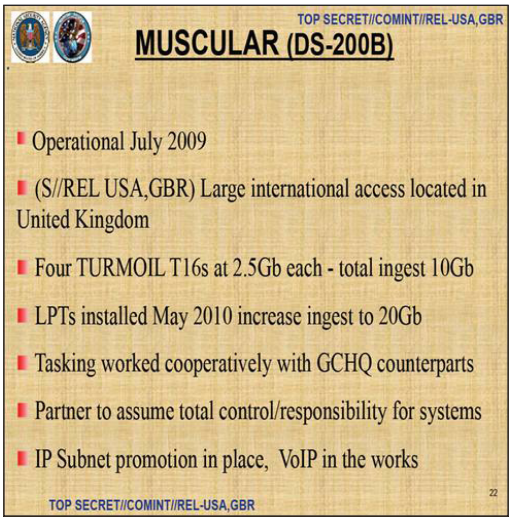
Συστήματα συλλογής και ανάλυσης προσωπικών διαδικτυακών δεδομένων: ΗΠΑ

- **XKeyscore**: Λογισμικό αναζήτησης πληροφοριών σε μεγάλες βάσεις δεδομένων που περιέχουν μηνύματα email, συζητήσεις (chats), αριθμούς τηλεφώνου, πρόσβασης (log-ins), ιστορικό αναζήτησης στον Ιστό και άλλες διαδικτυακές δραστηριότητες φυσικών προσώπων ή εταιρικών φορέων.
- **Pinwale**: γιγάντια βάση δεδομένων κυβερνητικών υπηρεσιών των ΗΠΑ, κυρίως για αποθήκευση μηνυμάτων email.
- **Marina**: σύστημα αποθήκευσης και ανάλυσης 'μεταδεδομένων' από τον Ιστό.

Συστήματα συλλογής και ανάλυσης προσωπικών διαδικτυακών δεδομένων: ΗΠΑ – Βρετανία

- **MUSCULAR** (DS-200B)

  Με βάση τη Βρετανία, το πρόγραμμα υποκλέπτει πληροφορίες από τους κεντρικούς διαύλους μεταφοράς δεδομένων που συνδέουν τα κέντρα δεδομένων των Yahoo και Google.
- Σε συνδυασμό με το DS-300 ('**Incenser**') υπολογίζεται ότι έχουν συλλέξει την περίοδο 2012-13 στοιχεία για 14 bis επικοινωνίες.



Εικόνα 27 Το σύστημα MUSCULAR για την υποκλοπή δεδομένων των Yahoo και Google.

Συστήματα συλλογής και ανάλυσης προσωπικών δεδομένων μεσω κινητών τηλεφώνων: DISHFIRE, PREFER: USA-UK

Αναλύει πληροφορίες από:

- Vcards, και συνδέει ονόματα, διευθ. email, αρ. τηλ., και φωτογραφίες

- Γεω-πληροφορίες, για τοποθεσίες και περιαγωγή χρηστών, και τόπους συναντήσεων
- Αναπάντητες κλήσεις
- Αλλαγές SIM και κινητού τηλ.
- Πληροφορίες ταξιδίων (διαδρομές, αλλαγές)
- Συναλλαγές (πιστωτικές, μεταφορές, κινήσεις λογαριασμών
- Passwords

Utah, USA: το 'στοιχειωμένο' Κέντρο Δεδομένων

Για την αποθήκευση και ανάλυση όλων αυτών των δεδομένων κατασκευάστηκε στις ΗΠΑ Κέντρο Δεδομένων με κόστος $12 δις. Το Κέντρο σχεδιάστηκε να συγκεντρώσει πληροφορίες από περίπου **30 τρις** επικοινωνίες δεδομένων που έχουν συλλεγεί τα τελευταία 12 χρόνια περίπου.
Για κάποιο λόγο όμως, παρουσιάζονται συνεχώς ηλεκτρικές βλάβες και δεν έχει μέχρι σημερά ουσιαστικώς τεθεί σε λειτουργία.

Σύστημα παρακολούθησης επικοινωνιών: Ρωσία

SORM

(CORM – Система Оперативно-Розыскных Мероприятий – System for Operative Investigative Activities)

Σύστημα παρακολούθησης τηλεφωνικών και διαδικτυακών επικοινωνιών, ενσύρματων και ασύρματων, καθώς και συναλλαγών μέσω πιστωτικών καρτών

Παιχνίδια/υπηρεσίες – παγίδες

Ένας πολίτης που επιθυμεί να χρησιμοποιήσεις υπηρεσίες ανωνυμίας μπορεί να καταστεί ως εκ τούτου στόχος παρακολούθησης, με την υποψία ότι 'κάτι έχει να κρύψει'.

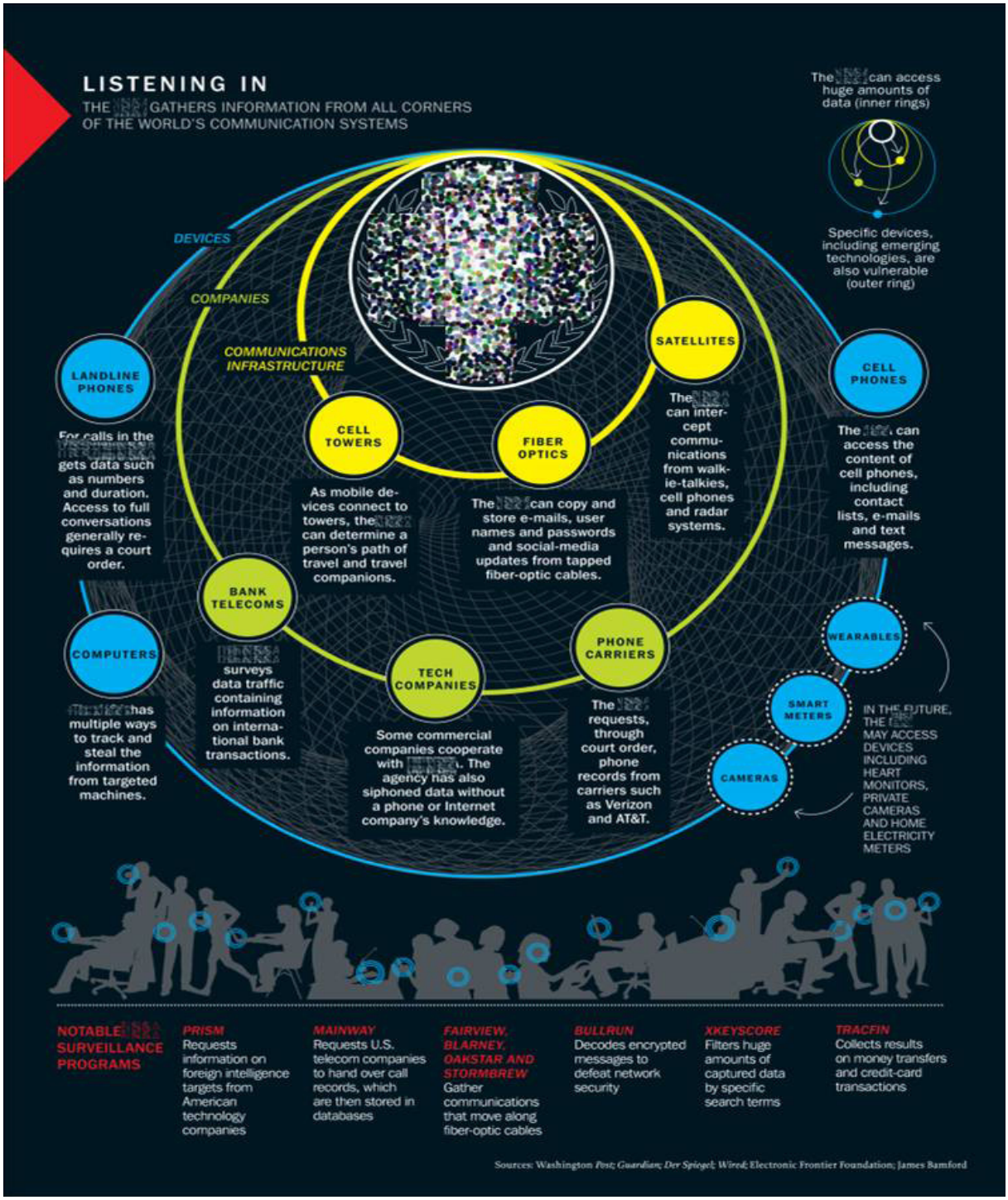
Για τον εντοπισμό και παρακολούθηση τέτοιων προσπαθειών ανωνυμίας έχουν αναπτυχθεί 'ελεγχόμενες' υπηρεσίες ψευδο-ανωνυμοποίησης, οι οποίες καταγράφουν όλα τα στοιχεία των 'ανώνυμων' επικοινωνιών και των χρηστών.

Επίσης, αναφέρεται ότι για τον ίδιο σκοπό έχουν αξιοποιηθεί δημοφιλή διαδικτυακά παιχνίδια (Εικόνα 28).

Εικόνα 28 Αξιοποίηση δημοφιλών διαδικτυακών παιχνιδιών για παρακολουθήσεις

Η 'μεγάλη εικόνα': το Σύστημα των παρακολουθήσεων

Τα επιμέρους εξειδικευμένα συστήματα παρακολουθήσεων συγκροτούν πλέον ένα γιγάντιο και πολυπλόκαμο Σύστημα (Εικόνα 29).



Εικόνα 29 ΤΟ Σύστημα παρακολουθήσεων

Τεχνολογίες ευρείας χρήσης που μπορεί να αξιοποιούνται στην παρακολούθηση

Ορισμένες διαδικτυακές τεχνολογίες προφανούς κοινωνικής χρησιμότητας μπορούν να αξιοποιούνται για σκοπούς παρακολουθήσεων. Ορισμένα παραδείγματα ακολουθούν.

Location-based Services

Πρόκειται για τεχνολογίες που αποσκοπούν στην παροχή υπηρεσιών με βάση την τοποθεσία του χρήστη:

- Το 'τυρί': ο χρήστης 'διευκολύνεται' να βρεί τί υπάρχει γύρω του. Μπορεί μάλιστα να αφήσει 'σχόλια' και 'συστάσεις'.
- Η 'φάκα': Τα συστήματα γνωρίζουν που είναι και πώς κινείται ο χρήστης, με συνδυασμό GPS, GSM, GoogleMaps, κλπ. Οι πληροφορίες αυτές μπορεί να αξιοποιηθούν από τρίτους, και όχι μόνο από τον ίδιο τον χρήστη.

Internet of Things –IoT

Αναφέρεται σε κάθε αντικείμενο που μπορεί να αποκτήσει 'ταυτότητα' (IP) και να απεικονιστεί στο Διαδίκτυο.

- Περιλαμβάνονται τεχνολογίες όπως: RFID, barcode, QR code, digital 'watermarks', κλπ
- Η ταυτότητα του αντικειμένου μπορεί να συνδέεται με ταυτότητες άλλων αντικειμένων, με στοιχεία προσώπων, μετακινήσεων, κλπ. Με τον τρόπο αυτόν ένας πολίτης μπορεί να συσχετιστεί με τα αντικείμενα που κατέχει, αλλά και μέσω αυτών να προκύψουν πολλά συνδυαστικά στοιχεία.
- Θεωρείται ένας από τους λόγους που οι 4.3 δις διευθύνσεις του IPv4 (32-bit) κρίνεται ότι θα εξαντληθούν, και απαιτήθηκε η προώθηση του IPv6 (128-bit).

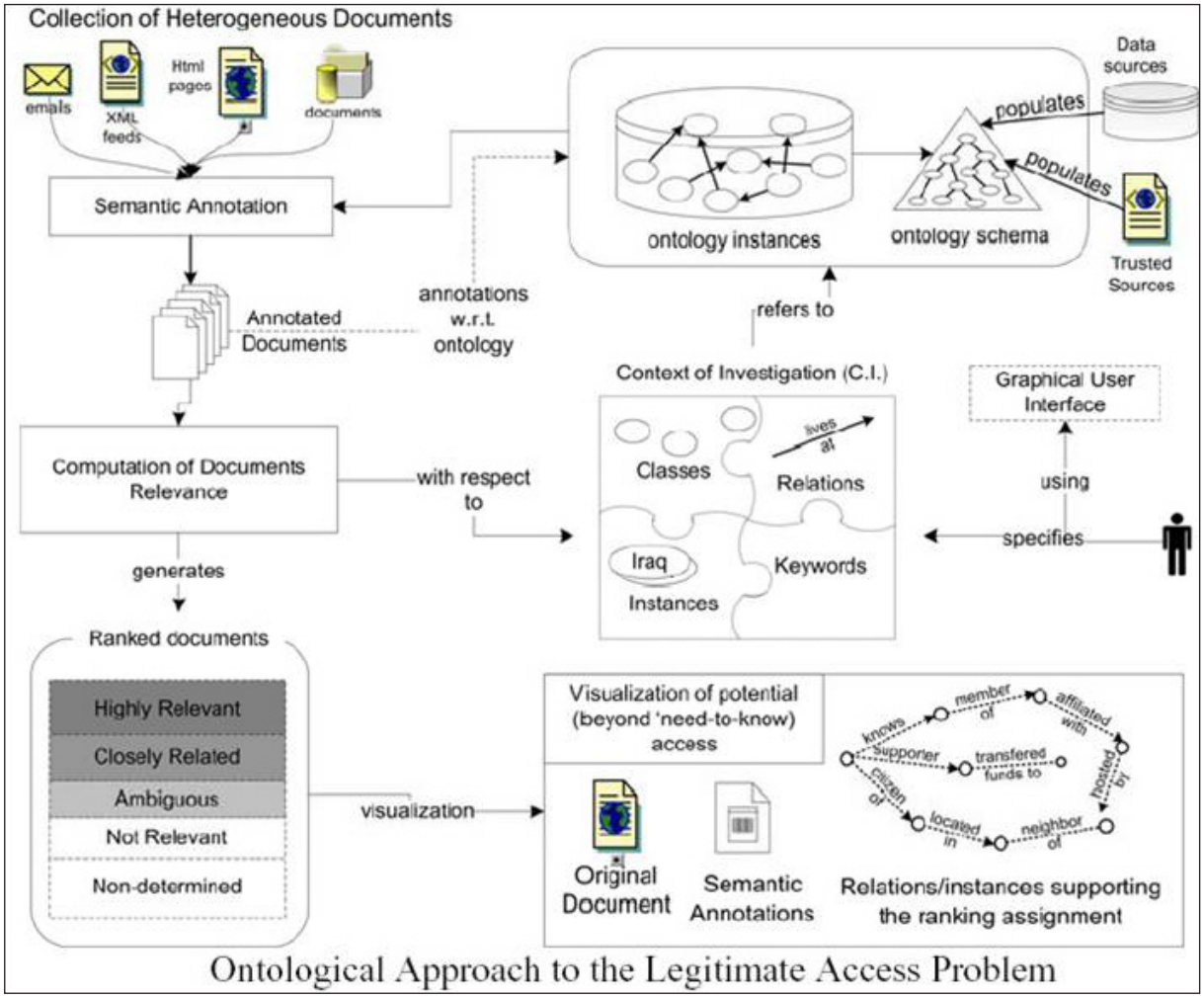
Σημασιολογικός Ιστός

Η τεχνολογία αυτή ξεκινά από μια ουσιώδη διαπίστωση:

ο Ιστός –www γεμίζει με τεράστιο όγκο ασύνδετων πληροφοριών, όπως είδαμε. Η αυτόματη επεξεργασία τους σε βάθος δεν είναι εφικτή. Η διαδεδομένη HTML μπορεί να χρησιμοποιηθεί μόνο για τη δημιουργία ιστοσελίδων και για τη δημιουργία σχέσεων μεταξύ τους μέσω υπερσυνδέσμων.

Για την αντιμετώπιση του ζητήματος προτείνεται η αξιοποίηση της γνωστής από τους αρχαίους Έλληνες φιλοσόφους μέθοδος των οντολογικών ιεραρχιών 'είδους – γένους', οι οποίες με κατάλληλες γλώσσες προγραμματισμού μπορεί να γίνουν αναγνώσιμες από 'αυτόματες μηχανές' λογισμικού. Νέες γλώσσες δημιουργούνται (RDF, OWL) για το Web 3.0. Κάτι τέτοιο θα καταστήσει εφικτή την επικοινωνία μηχανής-με-μηχανή (HY-HY).

Ελλοχεύει όμως ο κίνδυνος η μαζική επεξεργασία δεδομένων (data mining) θα γίνει πιό εύκολη, τόσο για αντιδημοκρατικές πρακτικές (πχ λογοκρισία), όσο και για την παρανομία (συλλογή προσωπικών δεδομένων), εντοπισμός γνωριμιών (FoF).



Εικόνα 30 Οντολογία και Σημασιολογικός Ιστός

Πηγές πληροφόρησης για θέματα παραβίασης ψηφιακών δικαιωμάτων

Από τον Ιστό:

- https://www.privacyinternational.org/
  Βρετανική οργάνωση για την προώθηση της προστασίας της ιδιωτικότητας
- https://www.eff.org/
  Οργάνωση στις ΗΠΑ για την προστασία των δικαιωμάτων στον 'ψηφιακό κόσμο'
- http://cryptome.org/
  Οργάνωση στις ΗΠΑ που αποκαλύπτει ντοκουμέντα για παραβιάσεις
- http://wikileaks.org/
  Η πολυσυζητημένη σελίδα που ανάρτησε πλήθος αποκαλυπτικών ντοκουμέντων

Για όλες τις σχετικές τεχνολογίες, συγκεντρωτική και συγκροτημένη πηγή γνώσεων αποτελεί το βιβλίο μου:

Βενέρης, Γιάννης (2010) *Μίμησις Πληροφορική: Έννοιες και Τεχνολογίες*, Εκδ. Τζιόλας.

«Διαδικτυακά Ανθρωποκυκλώματα»

Καθηγητής **Εμμανουήλ Ι. Γιαννακουδάκης**,
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Η πρόβλεψη του μέλλοντος της τεχνολογίας του Διαδικτύου είναι για τους ονειροπόλους που εικάζουν τις εξελίξεις από την οπτική τους και τις εμπειρίες τους, οι οποίες ενδεχομένως δεν καλύπτουν κατ' ανάγκη ούτε καν τις στοιχειώδεις λειτουργίες του Διαδικτύου. Όταν ο ειδικός καλείται να προβλέψει το μέλλον, θα πρέπει να είναι σε θέση να αποδείξει ότι αυτό που προβλέπει δεν είναι μόνο εφικτό, αλλά και πραγματοποιήσιμο μέσα σε ένα εύλογο χρονικό διάστημα, στηριζόμενος στη δική του ερευνητική προσπάθεια και στη διεθνή βιβλιογραφία.

Θα προσπαθήσω να καλύψω αυτό το ζήτημα από τη δική μου άποψη και τις δικές μου εμπειρίες[1], αφού μελετώ το αντικείμενο για περισσότερα από 40 χρόνια τώρα. Τα θέματα που θα καλυφθούν περιλαμβάνονται συνοπτικά στους εξής τομείς: α) Ουδετερότητα, β) Ταξιδιώτες στο χρόνο, γ) Ανθρωποκυκλώματα. Ωστόσο, υπάρχουν πολύ σοβαρά προβλήματα που μπορούμε και πρέπει άμεσα να αντιμετωπίσουμε, όπως είναι η ανάγκη για υψηλές ταχύτητες μετάδοσης δεδομένων[2], βιολογική – φωτονική αποθήκευση[3], η ποιότητα της παρεχόμενης πληροφόρησης, καθώς και η ανωνυμία των χρηστών.

Ουδετερότητα

Η ουδετερότητα του διαδικτύου είναι ένα θέμα που σίγουρα πρέπει να μας απασχολήσει στο μέλλον, καθότι έχει άμεση σχέση με το Δικαίωμα πρόσβασης στην αναρτημένη πληροφορία. Ένα από τα προβλήματα σχετίζεται με το εύρος των υπηρεσιών ενός πάροχου, καθώς και με τις δικαιοδοσίες που έχει, όπως εξηγείται παρακάτω. Έστω ότι ένας χρήστης εξυπηρετείται από τον πάροχο ISP_1, ο οποίος έχει συνάψει ειδική συμφωνία με τη διεύθυνση του ιστότοπου PAG_X, σύμφωνα με την οποία όλοι οι πελάτες του ISP_1 έχουν πρόσβαση στο PAG_X με υψηλές ταχύτητες μέσω της σύνδεσης που προσφέρει ο ISP_1. Τώρα, εάν υπάρχει ένας ιστότοπος, έστω PAG_Y, που είναι ανταγωνιστής του PAG_X, τότε ο πάροχος ISP 1 ενδέχεται να παρεμποδίζει την πρόσβαση των χρηστών στον ιστότοπο PAG_Y ή ακόμη και να μην επιτρέπει την πρόσβαση των χρηστών στις ιστοσελίδες PAG_Y. Το σενάριο αυτό δεν είναι καθόλου τυχαίο και καθόλου θεωρητικό. Υπάρχουν στοιχεία που επιβεβαιώνουν τον προβληματισμό που προκύπτει από το προαναφερόμενο σενάριο.

Το πρόβλημα ίσως είναι πιο σοβαρό, διότι ενδέχεται ο πάροχος να έχει την απόλυτη εξουσία ως προς τους ιστότοπους στους οποίους θα έχει πρόσβαση ένας χρήστης / πελάτης αυτού. Επίσης, σε ορισμένες αγορές, ενδέχεται ο χρήστης να μην έχει επιλογή παρόχου, όπου για παράδειγ-

1. Γιαννακουδάκης Ε. Ι., *Η αθέατη πλευρά της πληροφορικής*, Εκδόσεις Γκιούρδας, 2006
2. Dave Lee, *Fastest ever broadband passes speed test*, BBC, http:// www.bbc.co.uk/ news/ technology-25840502, 2014
3. Γιαννακουδάκης Ε. Ι., *Επιστημονικές περιπλανήσεις*, Παπασωτηρίου 2014

μα οι χρήστες σε ένα γεωγραφικό σημείο (π.χ. Πατήσια) έχουν πρόσβαση στο διαδίκτυο μόνο μέσω συγκεκριμένου παρόχου.

Ένας άλλος τομέας που πρέπει να μας απασχολήσει αφορά την πλατφόρμα μέσω της οποίας πραγματοποιείται η σύνδεση στο διαδίκτυο, όπως για παράδειγμα, Smartphones, Video game consoles, Tablets, κ.λπ., δεδομένου ότι οι περισσότερες πλατφόρμες αποτελούν πνευματική ιδιοκτησία πολυεθνικών συμφερόντων. Με άλλα λόγια, η κατασκευαστική εταιρεία ενδέχεται να θέτει περιορισμούς και όρους πρόσβασης στο διαδίκτυο. Σε τελική ανάλυση, αυτό σημαίνει ότι οι χρήστες τέτοιων συσκευών θα έχουν διαφορετική εμπειρία, όταν συνδέονται στο διαδίκτυο, πράγμα που μπορεί να οδηγήσει σε δυσκολίες στην επικοινωνία τους με άλλους χρήστες. Αν αυτή η τάση συνεχιστεί, μπορεί να γίνει δύσκολο να έχουμε μια ουσιαστική συζήτηση για το Διαδίκτυο, διότι η άποψη του κάθε ατόμου θα διαμορφωθεί από τις συσκευές που χρησιμοποιεί. Με άλλα λόγια, αυτό που πρέπει να αποφύγουμε με κάθε τρόπο είναι ένας πύργος της Βαβέλ.

Ταξιδιώτες στο χρόνο

Παρότι το θέμα αυτό ακούγεται ουτοπικό, ο πειραματισμός απέδειξε ότι είναι μια αξιόλογη άσκηση που μπορεί να οδηγήσει σε έξυπνα εργαλεία για την ανίχνευση χρηστών εκτός νόρμας, όπως εξηγείται παρακάτω. Το πραγματικό πρόβλημα που αποτελεί αντικείμενο έρευνας σχετίζεται με την ταξινόμηση των χρηστών του Διαδικτύου και την πρόβλεψη της συμπεριφοράς αυτών, συμπεριλαμβανομένων των κινήτρων τους, τις προθέσεις, τα σχέδια, τους στόχους και τους σκοπούς.

Η έννοια του «ταξιδιώτη του χρόνου» αναφέρεται στην περίπτωση κατά την οποία κάποιος χρήστης του διαδικτύου διακρίνεται από τη δυνατότητα να αναζητήσει πληροφορίες που αφορούν ένα θέμα το οποίο ενδέχεται να είναι α) απόρρητο (Top secret), όπου μόνο συγκεκριμένα, συνήθως ελάχιστα άτομα κατέχουν τη σχετική γνώση, β) παντελώς άγνωστο στην επιστημονική κοινότητα, γ) γνώση που αναφέρεται σε μελλοντικό γεγονός / πληροφορία με εκατό τοις εκατό πιθανότητα να συμβεί. Για να κυνηγήσουν τους ταξιδιώτες του χρόνου στο διαδίκτυο, δύο ερευνητές[4] επινόησαν τρεις δαιμόνιες προσεγγίσεις αναζήτησης:

1. Αναζήτηση στο Google και το Twitter (Hashtags) για τυχόν αναφορές στον κομήτη ISON και στον Πάπα Francis τα τελευταία επτά χρόνια. Και οι δύο όροι επινοήθηκαν πολύ πρόσφατα (Ο Πάπας Francis είναι ο πρώτος Πάπας που ονομάζεται Francis, ενώ δεν υπήρξε άλλος κομήτης με το όνομα ISON), οπότε κάθε αναφορά πριν από την άφιξή τους το 2013, θα μπορούσε να θεωρηθεί ως ένδειξη πρόγνωσης από άτομα με «υπερφυσικές» ικανότητες.
2. Κοιτάζοντας μέσα από ένα αρχείο καταγραφής των αναζητήσεων στην ιστοσελίδα της NASA, προσπάθησαν να δουν αν ένας ταξιδιώτης του χρόνου είχε ψάξει για τον κομήτη ISON πριν ανακαλυφθεί.
3. Αυτή ήταν μακράν η πιο φαεινή προσέγγιση, η οποία ήταν ένα απλό αίτημα / ένσταση από τους ερευνητές, ζητώντας από έναν ταξιδιώτη του χρόνου να τους στείλει ένα άμεσο μήνυμα που μεταδόθηκε πριν από το αρχικό αίτημα / συμβάν.

Δυστυχώς, καμία από αυτές τις αναζητήσεις δεν εμφάνισε κάποιον ταξιδιώτη του χρόνου – ή ακριβέστερα, δεν βρήκαν καμία πληροφορία που να είχε σταλεί πίσω στο χρόνο από το μέλλον. Ωστόσο, καταλήγουμε σε ποικίλα συμπεράσματα από αυτό το πείραμα σχετικά με το σχεδι-

4. Robert Nemiroff and Teresa Wilson, Michigan Technological University, *Searching the Internet for evidence of time travelers*, Research paper: arXiv:1312.7128, 2013

ασμό των μηχανών αναζήτησης νέας γενιάς, που προσφέρουν μια ποικιλία υπηρεσιών και περιλαμβάνουν: α) τον εντοπισμό προγραμματισμένων / προγραμματιζόμενων τρομοκρατικών ενεργειών, β) την ταξινόμηση της προσωπικότητας των χρηστών και τη διάγνωση παραγόντων με μετρήσεις εκτός των αποδεκτών ορίων (εκτός νόρμας), γ) ταξινόμηση των αντικοινωνικών πρακτικών αναζήτησης.

Ανθρωποκυκλώματα

Την ανάγκη για εξελιγμένους τρόπους επικοινωνίας έρχεται να καλύψει μια εντυπωσιακή ανακάλυψη, που αξιοποιεί το ανθρώπινο σώμα ως αγωγό για τη μετάδοση ψηφιακών σημάτων. Πρόκειται για το προσωπικό δίκτυο (Personal Area Network – PAN***5***,***6***), που παρέχει τη δυνατότητα σε ένα άτομο να επικοινωνήσει με άλλα, μόνο με μια χειραψία***7***, με την οποία δημιουργείται ο απαιτούμενος κύκλος μετάδοσης δεδομένων μέσω του εδάφους.

Για παράδειγμα, οι αριθμοί τηλεφώνων ενός κινητού μπορεί να αντιγράφονται σε ένα άλλο κινητό ή σε φορητό υπολογιστή με μία μόνο χειραψία. Επίσης, με μία χειραψία ο άνθρωπος θα είναι σε θέση να ενημερώνεται από έναν εμπειρογνώμονα πάνω σε συγκεκριμένα θέματα, όπως επίσης και ένας μαθητής θα παίρνει μαθήματα από το δάσκαλό του μέσω ενός ανθρωποκυκλώματος. Εδώ, αναφερόμαστε σε ανθρωποκυκλώματα που δημιουργούνται μέσω του διαδικτύου και εξυπηρετούν συγκεκριμένους σκοπούς, όπως εξηγούμε παρακάτω.

Ο ανθρώπινος εγκέφαλος καταναλώνει κατά μέσο όρο 20 Watt, ενώ το ανθρώπινο σώμα στο σύνολό του εκπέμπει ενέργεια που είναι ίση με αυτήν που εκπέμπει ένας λαμπτήρας των 60 Watt***8***. Επομένως, η ενέργεια είναι αρκετή για να λειτουργήσει το προαναφερόμενο κύκλωμα. Για όσους ενδιαφέρονται για τις τεχνικές λεπτομέρειες***9***, σημειώνουμε ότι το προαναφερόμενο βιοκύκλωμα στηρίζεται σε κλίμακα της τάξεως των 10 Fem-to-Farads, ενώ το ηλεκτρικό ρεύμα που διαπερνά το ανθρώπινο σώμα μετράται σε NanoAmber (δισεκατομμυριοστά του Amber). Ο πομπός λειτουργεί σε λιγότερα από 500 KHz και θεωρητικά έχει ταχύτητα μετάδοσης 1Mbit/sec, με πρακτικό όριο γύρω στα 100 Kbit/sec.

Η σύνδεση εγκεφαλικών νευρώνων που δίνουν τις σχετικές με την κίνηση εντολές (π.χ. για την κίνηση χεριών, ποδιών, κ.λπ.) με εξειδικευμένα ηλεκτρονικά νανοκυκλώματα (τσιπ) παρέχουν τη δυνατότητα περαιτέρω επεξεργασίας των υποκείμενων εγκεφαλικών σημάτων. Είναι πλέον εφικτό τα τσιπ αυτά να συνδεθούν με ρομποτικούς μηχανισμούς κατά τρόπον ώστε να ενεργοποιούνται με τη λήψη των σημάτων και να αναπαράγουν τις ίδιες κινήσεις***10***.

Επίσης, ερευνητικά αποτελέσματα καθώς και πειράματα που διεξήχθησαν***11***, απέδειξαν ότι είναι δυνατόν να συνδεθούν διαφορετικά είδη ζώων (π.χ. άνθρωπος με ζώο). Συγκεκριμένα, ένα άτομο-πομπός δύναται να στέλνει σήματα μέσω του διαδικτύου σε έναν πίθηκο-δέκτη, ο οποίος με τη σειρά του κουνάει το σχετικό με το σήμα μέλος του σώματός του.

5. T G Zimmerman, *Personal area networks: Near-field intrabody communication*, IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 609-617, 1996
6. Pun S H, Gao Y M, Mak P U, Du M, Vai M I, *Modeling for intra-body communication with bone effect*, Proc IEEE Eng Med Biol Soc, 2009:693-6, 2009
7. Γιαννακουδάκης Ε. Ι., *Η αθέατη πλευρά της πληροφορικής*, Εκδόσεις Γκιούρδας, 2006
8. Elia M, *Organ and tissue contribution to metabolic rate*, In: Energy Metabolism: Tissue Determinants and Cellular Corollaries, Edited by Kinney and Tucker, Raven Press, pp. 61-77, 1992
9. Željka Lučev, Igor Krois, Mario Cifrek, *Intrabody Communication in Biotelemetry*, Wearable and Autonomous Biomedical Devices and Systems for Smart Environment, Lecture Notes in Electrical Engineering, Vol. 75, pp. 351-368, 2010
10. Miguel A L Nicolelis, *Neuroengineering – Mind in Motion*, Scientific American, September 2012
11. Γιαννακουδάκης Ε. Ι., *Επιστημονικές περιπλανήσεις*, Παπασωτηρίου 2014

Φανταστείτε τώρα δύο άτομα συνδεδεμένα, κατά τρόπον ώστε όταν το ένα άτομο κινεί το δεξί του χέρι και γράφει ένα άλλο άτομο αναπαραγάγει την ίδια ακριβώς κίνηση. Φανταστείτε επίσης ότι το άτομο-πομπός δύναται να βρίσκεται στην άλλη άκρη του κόσμου, συνδεδεμένο μέσω του διαδικτύου με κάποιο άλλο άτομο-δέκτη, το οποίο υπακούει τυφλά στις εντολές που δέχεται, όποιες και αν είναι αυτές...

Μια καταπληκτική εφαρμογή είναι, φυσικά, η σύνδεση ενός πεπειραμένου δασκάλου-πομπού με ένα μικρό παιδί-δέκτη, το οποίο μαθαίνει να γράφει και όχι μόνο....

«Η ενσωμάτωση νεώτερων τεχνολογικών εφαρμογών στο διαδίκτυο και οι επιδράσεις τους στην υγεία και την ανθρώπινη συμπεριφορά»

Δρ. **Κωνσταντίνος Σιώμος**,
Ψυχίατρος παιδιών και εφήβων
Πρόεδρος της Ελληνικής Εταιρείας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο

Περίληψη

Η πληροφορική και το Internet προσφέρουν την δυνατότητα εικονικοποίησης (Virtualization) διαδικασιών, αντικειμένων και μορφών ζωής που παρουσιάζονται ζωντανά χωρίς να υπάρχουν πραγματικά. Η τεχνολογία αυτή δημιουργεί πολλές δυνατότητες σε τομείς όπως η επιστημονική και βιομηχανική έρευνα, η εκπαίδευση, η ιατρική και η ψυχαγωγία.

Η επόμενη εξέλιξη είναι αυτή της επαυξημένης πραγματικότητας (augmented reality) προσθέτοντας επί πρόσθετες πληροφορίες στην πραγματικότητα, με τέτοιο τρόπο που ο άνθρωπος να βιώνει αυτές τις επί πλέον πληροφορίες, ως αναπόσπαστο μέρος της πραγματικότητας.

Η εικονικοποίηση και η επαυξημένη πραγματικότητα, ιδίως στο Διαδίκτυο, δυνητικά μπορούν να οδηγήσουν τους ανθρώπους στην απομάκρυνσή τους από τον πραγματικό κόσμο, τις πραγματικές σχέσεις με σημαντικές επιπτώσεις στην κοινωνική ζωή και την ψυχολογία του ανθρώπου.

Το άρθρο αυτό στοχεύει να προσφέρει στον αναγνώστη μία επισκόπηση της διαθεσιμότητας της εικονικοποίησης και επαυξημένης πραγματικότητας και ρίχνει μία ματιά στις αναμενόμενες μελλοντικές εξελίξεις, ώστε ο ψηφιακός πολίτης να διαμορφώσει την δική του προσωπική άποψη για την χρησιμότητα της τεχνολογίας και να ανακαλύψει τους τρόπους αντιμετώπισης της επιρροής της στην καθημερινότητα του.

Ορισμός της εννοίας Virtualization – Εικονικοποίηση

"Η μεταφορά ενός αντικειμένου, ενός μηχανισμού ή μίας μορφής ζωής σε μία παρουσίαση από υπολογιστές, συνήθως διαδραστική"

Μερικά παραδείγματα αποτελούν

- Παρουσιάσεις εικονικών κτιρίων
- Εικονικά μοντέλα στην έρευνα & ανάπτυξη
- Εικονικά μουσεία και άλλα αξιοθέατα
- Virtual Computers
- Εικονικά καταστήματα ένδυσης
- VR/AR Gaming

Εδώ υπάρχουν πλέον άπειρα παραδείγματα. Από προσομοιωτές που δίνουν την δυνατότητα να ζήσεις την εμπειρία να πετάς με αεροπλάνο ή να οδηγήσεις ένα αυτοκίνητο φόρμουλα 1 κλπ. Το συναρπαστικό εδώ είναι ότι στον εικονικό κόσμο όλα είναι δυνατά και με την ρεαλιστική προσομοίωση είναι σαν να είσαι "μέσα στο παιχνίδι".

Augmented Reality – Επαυξημένη Πραγματικότητα

Ενώ στην εικονική πραγματικότητα εξομοιώνεται κάτι που μας είναι οικείο από την πραγματικότητα, το «Augmented Reality» είναι το φαινόμενο όπου με τεχνητά μέσα προστίθεται κάτι στην πραγματικότητα που βιώνουμε. Κάτι που δεν υπάρχει αλλά που γίνεται αντιληπτό από τον άνθρωπο ως υπαρκτό.

Τι αναμένεται στο μέλλον;

Οι εξελίξεις στην εικονικοποίηση και στην επαυξημένη πραγματικότητα εξαρτώνται από την διαθέσιμη τεχνολογία και από την δημιουργικότητα του ανθρώπου.

- Η ταχύτητα του Internet αυξάνεται
- Όλα θα είναι ασύρματα και συνδεδεμένα
- Δημιουργείται το Internet των πραγμάτων

Έξυπνες συσκευές που διασυνδέονται μεταξύ τους μέσω του Internet. Υπολογίζεται ότι το 2020, 50 δισεκατομμύρια έξυπνες συσκευές στην Ευρώπη θα διασυνδέονται μεταξύ τους.

- Οι υπολογιστές γίνονται πιο γρήγοροι
- Οι υπολογιστές γίνονται μικρότεροι

Η ηλεκτρονική πρώτη ύλη γίνεται όλο και πιο μικρή, επιτρέποντας την ανάπτυξη μικροσκοπικών υπολογιστών.

- Ο οπτικός υπολογιστής θα κυκλοφορήσει

Λειτουργώντας με την ταχύτητα του φωτός. Γενικά είναι αναμενόμενο ότι η αρχιτεκτονική των υπολογιστών θα αλλάξει δραστικά, μίας που η τωρινή βασίζεται σε ιδέες από την εποχή πριν από 60 χρόνια. Ο χημικός υπολογιστής βρίσκεται επίσης μέσα στις δυνατότητες

- Η τεχνολογία λογισμικού εξελίσσεται
- Grid Computing – In the cloud computing
- Η τεχνητή νοημοσύνη των υπολογιστών αναπτύσσεται.

Ανεξαρτητοποίηση των τεχνολογικών συσκευών από τον άνθρωπο–Τεχνητή νοημοσύνη

Όλο και περισσότερες εργασίες που τώρα καθοδηγούνται από τον άνθρωπο, θα αρχίζουν να γίνονται απευθείας μέσω της αναπτυσσόμενης τεχνητής νοημοσύνης των συσκευών. Για παράδειγμα σε μία στιγμή κινδύνου ο υπολογιστής του αυτοκινήτου και τα φρένα του θα συνεννοούνται πολύ πιο γρήγορα μεταξύ τους χωρίς την μεσολάβηση του οδηγού. Η συνεννόηση μεταξύ διεργασιών φυσικά θα γίνει κατά μεγάλο μέρος μέσω του Internet, και θα δούμε την εξέλιξη ανεξάρτητης εικονικής ζωής εκεί. Το Avatar σας για παράδειγμα στο Second Life δεν θα χρειάζεται εσάς για καθοδήγηση αλλά θα συνεχίζει τις δραστηριότητές του και όταν απουσιάζεστε εσείς, με δική του πρωτοβουλία.

Αναμενόμενα παραδείγματα εικονικοποίησης

- Humanoids – Robots με ανθρώπινη εμφάνιση και συμπεριφορά μέσω τεχνητής νοημοσύνης

θα βρίσκουν όλο και περισσότερη εφαρμογή. Για εργασίες, ιδίως επαναλαμβανόμενες βαρετές ή επικίνδυνες. Στη βιομηχανία, για στρατιωτικούς σκοπούς – ένα humanoid μπορεί να θεωρηθεί αναλώσιμο, μία ανθρώπινη ζωή όχι. Η ρομποτική εξελίσσεται πολύ γρήγορα. Σύντομα θα υπάρχουν humanoids με εμφάνιση και κίνηση όπως εκείνη στον άνθρωπο.

- Βελτίωση της Εικονικής Πραγματικότητας
- Όλο και περισσότερη Εικονική Πραγματικότητα – Virtual Reality
- Όλο και περισσότερη Επαυξημένη Πραγματικότητα – Augmented Reality

Θα περπατάτε στον δρόμο φορώντας τα έξυπνα γυαλιά σας ή τους φακούς επαφής σας, με υψηλής ταχύτητας σύνδεση Internet και GPS. Σε ό, τι κοιτάτε θα προστίθεται επί πλέον πληροφορία σε εικόνα και ήχο, ή η πραγματική εικόνα θα αλλοιώνεται.

Θα κάθεστε για παράδειγμα σ' ένα παγκάκι και δίπλα σας θα κάθεται ένα avatar (δικής σας επιλογής ή όχι) που δεν θα ξεχωρίζει από πραγματικό άνθρωπο και με τον οποίο μπορείτε να συζητήσετε κανονικότατα. Ή μία έξυπνη εφαρμογή θα παραμορφώνει την εικόνα των αντικειμένων που κοιτάτε ή τον ήχο που ακούτε ώστε να μπορείτε να δημιουργήσετε το δικό σας 'look and feel' του κόσμου.

Η επαυξημένη πραγματικότητα μαζί με τον Κυβερνοχώρο θα δημιουργήσουν μία παράλληλη ζωή στην πραγματική ζωή, οδηγώντας ορισμένους ανθρώπους σε μεγάλη εξάρτηση από την τεχνολογία.

Δυσμενείς εξελίξεις

Κάθε τεχνολογική εξέλιξη έχει την αρνητική πλευρά της. Η εικονική και επαυξημένη πραγματικότητα εδώ δεν αποτελούν εξαίρεση. Ο Κυβερνοχώρος καθίσταται μία παράλληλη διάσταση της ζωής επηρεάζοντας σχεδόν όλους τους ανθρώπους. Όλοι θα έχουμε κάτι σημαντικό εκεί και θα βιώνουμε το άγχος της συνεχούς παρουσίας μας εκεί.

Η βιομηχανία παραγωγής του κακόβουλου λογισμικού φυσικά ακολουθεί την τεχνολογική εξέλιξη από κοντά. Θα υπάρχουν Ιοί που θα μολύνουν και θα αναλαμβάνουν τον έλεγχο εικονικής ζωής (avatars) όπως και η κλοπή εικονικής ταυτότητας θα γίνει ένα συνηθισμένο φαινόμενο. Όλα αυτά με σκοπό την κλοπή πληροφοριών προς πώληση, το Cyberbullying, την απάτη ή την απoπλάνηση κλπ. Το ηλεκτρονικό έγκλημα, η ασφάλεια στο διαδίκτυο, η προστασία των προσωπικών μας δεδομένων και τα φαινόμενα εξάρτησης από την τεχνολογία είναι τα ζητήματα που ζητούν επίλυση στην ψηφιακή εποχή.

Και σε έναν κόσμο όπου τα πάντα στην καθημερινότητα θα βασίζονται στο Internet, ένα από τα μεγαλύτερα προβλήματα που θα προκύψουν θα είναι απλά το γεγονός ότι κάποια στιγμή δεν θα μπορείτε να συνδεθείτε!

Συμπεράσματα

Η εικονικοποίηση και η επαυξημένη πραγματικότητα θα έχουν μία σημαντική επιρροή στην λειτουργία της ψηφιακής κοινωνίας. Η εξάρτηση του ανθρώπου από την τεχνολογία θα αποδειχθεί καθολική. Ο χρόνος που οι άνθρωποι θα περνάνε σε σύνδεση με το διαδίκτυο προοδευτικά θα γίνει πολύ περισσότερος από τον χρόνο εκτός σύνδεσης.

Αυτό σημαίνει ότι προοδευτικά η επικοινωνία μέσω των κοινωνικών δικτύων θα αντικαταστήσει σε ένα μεγάλο μέρος την πρόσωπο με πρόσωπο επικοινωνία. Βρισκόμαστε σε μία εποχή ραγδαίας τεχνολογικής εξέλιξης. Αλλά όπως η ιστορία διδάσκει η εξέλιξη αυτή θα έχει θετικές και αρνητικές επιρροές. Η σοφή εφαρμογή της τεχνολογίας προς όφελος του συνόλου, είναι και θα παραμένει το καθήκον του ανθρώπου στην αρχή της ψηφιακής εποχής που διανύουμε.

ΒΙΒΛΙΟΓΡΑΦΙΑ

4. Σιώμος ΚΕ. (2008). *Εθισμός των εφήβων στους Η/Υ και το διαδίκτυο: Ψυχιατρικά συμπτώματα και διαταραχές ύπνου. Διδακτορική Διατριβή*, Ιατρική Σχολή, Πανεπιστήμιο Θεσσαλίας.
5. Σιώμος Κ– Φλώρος Γ. (2011). *Έρευνα–Πρόληψη–Αντιμετώπιση των Κινδύνων στη Χρήση του Διαδικτύου*. Εκδόσεις Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο, [συλλογικό έργο).
6. Σφακιανάκης Ε. – Σιώμος Κ. –Φλώρος Γ. (2012). *Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου*. Εκδόσεις Λιβάνη.
7. Σιώμος Κ– Φλώρος Γ. (2013). *Οφέλη και κίνδυνοι στη χρήση του διαδικτύου*. Εκδόσεις Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο, (συλλογικό έργο).

«1984–2014: Οι μελλοντικές τεχνολογίες παρακολούθησης βρίσκονται ήδη εδώ»

Δρ. **Ιωσήφ Ανδρουλιδάκης**,
Ερευνητής, Πανεπιστήμιο Ιωαννίνων

Ήδη από το 1948 ο George Orwell είχε φανταστεί έναν κόσμο απόλυτης παρακολούθησης στο πασίγνωστο μυθιστόρημά του "1984", από το οποίο προέκυψε και ο όρος «μεγάλος αδερφός». Από τότε, έχουν γίνει δεκάδες αποκαλύψεις για παρακολουθήσεις μεμονωμένων προσώπων ή ομάδων, καθιστώντας το φαινόμενο «τετριμμένο» και ίσως «δεδομένο». Η ρήση, εξάλλου, του Scott McNealy, CEO της τότε Sun Microsystems, το 1999: «You have zero privacy anyway. Get over it!» μαρτυρούσε ότι το αγαθό της ιδιωτικότητας είχε ήδη εκλείψει εδώ και πολλά χρόνια από τον ψηφιακό κόσμο.

Μεγαλύτερο ενδιαφέρον, ωστόσο, παρουσιάζουν οι μαζικές παρακολουθήσεις μεγάλης κλίμακας. Μια από τις πρώτες τέτοιες αποκαλύψεις ήταν αυτή για το δίκτυο ECHELON, το οποίο αποκαλύφθηκε από τη Margaret Newsham το 1988. Το δίκτυο αυτό από τη δεκαετία του '60 χρησιμοποιούταν από συμμαχία 5 κρατών (Αυστραλία, Καναδά, Νέα Ζηλανδία, Ηνωμένο Βασίλειο, ΗΠΑ) για την υποκλοπή στρατιωτικών και διπλωματικών πληροφοριών από τη Σοβιετική Ένωση και το ανατολικό μπλοκ. Με την πάροδο του χρόνου η χρήση του επεκτάθηκε καθιστώντας το ένα σύστημα καθολικών υποκλοπών τόσο προσωπικών όσο και εμπορικών επικοινωνιών.

Φτάνοντας στις μέρες μας, δεν υπάρχει πλέον καμία αμφιβολία ότι βρισκόμαστε σε ένα καθεστώς καθολικής παρακολούθησης όπου το σύνολο σχεδόν των ηλεκτρονικών επικοινωνιών υποκλέπτονται μαζικά και συστηματικά. Οι αποκαλύψεις των «Wikileaks» από τον Julian Assange το 2011 και το «Global surveillance disclosure» από τον Edward Snowden το 2013 συνθέτουν ένα ιδιαίτερα ζοφερό τοπίο όσον αφορά στην ιδιωτικότητα. Πράγματι, το μυθιστόρημα του George Orwell να έχει γίνει πλέον πραγματικότητα ως προς το κομμάτι του «μεγάλου αδερφού». Η συνεργασία μεταξύ κρατών, υπηρεσιών, κατασκευαστών, τηλεπικοινωνιακών παρόχων και παρόχων υπηρεσιών, καθιστά δυνατή την παρακολούθηση οποιουδήποτε. Το πλαίσιο και οι κανόνες αυτής της συνεργασίας δεν είναι απολύτως γνωστά, σύμφωνα όμως με τις αποκαλύψεις, τις περισσότερες φορές είναι επωφελή για όλους τους εμπλεκόμενους. Από την άλλη πλευρά, οι εταιρείες και πάροχοι των οποίων τα προϊόντα και οι υπηρεσίες έχουν εμπλακεί στις αποκαλύψεις περί μαζικών υποκλοπών σπεύδουν να διαψεύσουν τα στοιχεία και να αρνηθούν την οποιαδήποτε εμπλοκή στα σχετικά σκάνδαλα.

Στις μέρες μας, λοιπόν, λαμβάνει χώρα καθολική παρακολούθηση του συνόλου σχεδόν των ηλεκτρονικών επικοινωνιών, με απόλυτο έλεγχο τόσο των υπολογιστών όσο και των σταθερών και κινητών τηλεφώνων. Τις περισσότερες φορές, αυτό γίνεται εν κρυπτώ, χωρίς ο χρήστης να μπορεί να αντιληφθεί το παραμικρό. Οι υποκλοπές γενικώς πραγματοποιούνται σε πραγματικό χρόνο με τα δεδομένα να αναλύονται και αξιοποιούνται άμεσα. Όμως ακόμα και αν δεν προκύπτει κάποια άμεση πληροφορία, τα δεδομένα αποθηκεύονται και διατηρούνται για μελλοντική χρήση.

Από τεχνικής πλευράς, υλοποιούνται συστήματα και μέθοδοι παθητικής αλλά και ενεργής φύσης. Μια παθητική υποκλοπή πραγματοποιείται χωρίς καμία επέμβαση–παρέμβαση στο υπό παρακολούθηση σύστημα. Τυπικό παράδειγμα αποτελεί η υποκλοπή ραδιοκυμάτων. Τα ραδιοκύματα ταξιδεύουν ελεύθερα και είναι σχετικά εύκολο να ληφθούν και καταγραφούν ακόμα και σε μεγάλες αποστάσεις. Κατόπιν, ανάλογα με το είδος της κρυπτογράφησης (ή και την απουσία της πολλές φορές) μπορεί να γίνει η αποκρυπτογράφηση και να προκύψει το περιεχόμενο της επικοινωνίας. Αντιθέτως, υποκλοπές με ενεργό τρόπο, απαιτούν την τροποποίηση είτε του εξοπλισμού είτε των πρωτοκόλλων επικοινωνίας. Ένα σχετικό παράδειγμα είναι η εγκατάσταση κακόβουλου λογισμικού σε κάποιον υπολογιστή ή η τοποθέτηση ενός πλαστού–ελεγχόμενου ασύρματου σημείου πρόσβασης (access point) σε κάποιον δημόσιο χώρο. Όπως είναι λογικό, οι παθητικές μέθοδοι είναι πρακτικά αδύνατο να εντοπισθούν σε αντίθεση με τις ενεργές οι οποίες αφήνουν συγκεκριμένα ίχνη.

Υποκλοπή με ενεργό τρόπο αποτελεί και η εγκατάσταση μιας ηλεκτρονικής διάταξης–κοριού. Το ενδιαφέρον στοιχείο, σύμφωνα με τις αποκαλύψεις Snowden, είναι ότι οι μυστικές υπηρεσίες φροντίζουν να κατασκευάζουν τις διατάξεις αυτές με εμπορικά ηλεκτρονικά εξαρτήματα, τα οποία βρίσκονται ευρέως διαθέσιμα στην αγορά. Παράλληλα, σε περίπτωση που οι διατάξεις επικοινωνούν με τον υποκλοπέα (για να στείλουν π.χ. το περιεχόμενο μιας υποκλαπείσας ομιλίας), αυτό γίνεται πάντα με ισχυρή κρυπτογράφηση. Έτσι, ακόμα και στην περίπτωση που οι διατάξεις αυτές ανακαλυφθούν, δεν υπάρχουν στοιχεία που να οδηγούν στην ταυτότητα του υποκλοπέα.

Εκτός από τα δίκτυα σταθερής και κινητής τηλεφωνίας, το Διαδίκτυο βρίσκεται και αυτό υπό «επιτήρηση». Είναι γνωστό εδώ και πολλά χρόνια εξάλλου ότι το Διαδίκτυο δεν εγγυάται την ασφάλεια των πληροφοριών που διακινούνται μέσα από αυτό. Αυτό που ήταν λιγότερο γνωστό μέχρι τις πρόσφατες αποκαλύψεις, είναι το γεγονός ότι μέσα από ένα εκτεταμένο δίκτυο ελεγχόμενων ή/και επιμολυσμένων υποδομών (π.χ. στις εγκαταστάσεις των παρόχων), μέσων μετάδοσης (π.χ. καλωδίων οπτικών ινών), δρομολογητών, εξυπηρετητών και υπολογιστών, είναι δυνατή η παρακολούθηση του συνόλου σχεδόν των πακέτων δεδομένων που διακινούνται σήμερα στο Διαδίκτυο. Βεβαίως εκτός από την πληροφορία που διακινείται, υπάρχει και πληροφορία που βρίσκεται ήδη αποθηκευμένη. Η πρόσβαση και σε αυτή την πληροφορία είναι εφικτή, με τη συνεργασία των παρόχων υπηρεσιών με διάφορους βαθμούς νομιμότητας.

Η λαθρανάγνωση των πακέτων πληροφορίας τα οποία διακινούνται στο Διαδίκτυο είναι τετριμμένη τεχνική. Πιο εντυπωσιακή είναι η έγχυση/εισαγωγή πλαστών πακέτων ελέγχου των πρωτοκόλλων επικοινωνίας και η αντικατάσταση των γνησίων πακέτων με πλαστά τα οποία καταφτάνουν ταχύτερα από τα αυθεντικά στον χρήστη. Αυτό είναι δυνατό με χρήση πλαστών/ελεγχόμενων εξυπηρετητών που βρίσκονται εγγύτερα στον χρήστη σε σχέση με τον γνήσιο εξυπηρετητή. Πράγματι, αν αναλογισθεί κανείς πόσοι κόμβοι μεσολαβούν για την επικοινωνία μεταξύ ενός υπολογιστή και ενός εξυπηρετητή τότε πάντα υπάρχει περιθώριο για κάποιον ενδιάμεσο «ελεγχόμενο» κόμβο.

Συνεχίζοντας στο τεχνικό κομμάτι των ενεργών υποκλοπών, η παγίδευση του λογισμικού διαδραματίζει και αυτή σημαντικό ρόλο. Μέχρι πρόσφατα γνωρίζαμε ότι είναι σχετικά εύκολο να εγκατασταθεί σε κάποιον υπολογιστή κακόβουλο λογισμικό το οποίο να υποκλέπτει τις επικοινωνίες και τα προσωπικά δεδομένα του χρήστη. Οι σύγχρονες μέθοδοι όμως, αποφεύγουν το λογισμικό σε επίπεδο λειτουργικού συστήματος και κατεβαίνουν ένα βήμα παρακάτω, παγιδεύοντας το λογισμικό που εκτελείται στο υλισμικό του υπολογιστή (firmware). Πράγματι υπάρχουν ήδη

στοιχεία για παγιδευμένο BIOS ή για επιθέσεις μέσω του System Management Mode. Καθώς η υποκλοπή αυτή λαμβάνει χώρα έξω από το λειτουργικό σύστημα, η ανίχνευσή της είναι εξαιρετικά δύσκολη. Και βέβαια, στο στόχαστρο δε μπαίνουν μόνον οι υπολογιστές. Το ίδιο συμβαίνει και με τα κινητά τηλέφωνα, τις κάρτες (U)SIM, τους δρομολογητές, και κάθε είδους εξοπλισμό πληροφορικής και τηλεπικοινωνιών. Ακόμα και στους σκληρούς δίσκους, είναι γνωστό ότι το ενσωματωμένο λογισμικό ελέγχου τους μπορεί να φιλοξενήσει και αυτό κακόβουλο λογισμικό.

Πέρα από τεχνικές παρακολούθησης λογισμικού υπάρχουν φυσικά και οι επεμβάσεις σε επίπεδο υλισμικού. Πάντα σύμφωνα με τα στοιχεία που είδαν το φως της δημοσιότητας, υπάρχει ήδη υλισμικό παγίδευσης, διαθέσιμο για δεκάδες εμπορικά προϊόντα. Προφανώς απαιτείται φυσική παρέμβαση, και αντικατάσταση/ενσωμάτωση ηλεκτρονικών κυκλωμάτων. Φαίνεται και ίσως είναι δύσκολο να παραβιάσει κάποιος τη φυσική ασφάλεια μιας εταιρείας, να αποκτήσει πρόσβαση στις εγκαταστάσεις της, να ξεβιδώσει υπολογιστές και να τοποθετήσει μικροκυκλώματα στις μητρικές κάρτες και στους σκληρούς δίσκους. Αναλογισθείτε όμως, πόσο απλούστερο είναι η ίδια διαδικασία να γίνει κατά τη μεταφορά των υπολογιστών και των εξαρτημάτων όταν γίνεται η αγορά τους, στη διαδρομή μέχρι να φτάσουν στον τελικό χρήστη. Με τον τρόπο αυτό, οι υπολογιστές καταφθάνουν με μια μικρή καθυστέρηση, ήδη παγιδευμένοι!

Από τεχνικής πλευράς, και πάλι, μπορούν να παγιδευθούν οι δίαυλοι επικοινωνίας όπως το PCI, το I2C bus αλλά και δίαυλοι ελέγχου και δοκιμών όπως το JTAG. Οι θύρες εισόδου και εξόδου όπως το USB, η κάρτα δικτύου, τα πληκτρολόγιο αλλά ακόμα και το καλώδιο της οθόνης μπορούν να φιλοξενήσουν υλισμικό υποκλοπών. Το υλισμικό αυτό, θα πρέπει με κάποιον τρόπο να μεταδώσει τα υποκλαπέντα δεδομένα στον δημιουργό του. Αυτό μπορεί να γίνει με διάφορους τρόπους, μέσω του ιδίου του δικτύου του υπολογιστή (σταθερού ή ασύρματου), μέσω ασύρματων πομποδεκτών, μέσα από τα ηχεία του υπολογιστή (με υπέρηχους), ακόμα και με την ανάκλαση μικροκυματικής ακτινοβολίας.

Κλείνοντας, με αφορμή τη μέθοδο υποκλοπών με ανάκλαση μικροκυματικής ακτινοβολίας, θα κάνουμε μια σημαντική παρατήρηση. Όπως αναφέρει και ο τίτλος, οι τεχνολογίες που περιγράφηκαν μπορεί να φαντάζουν εξωτικές και «μελλοντικές», ιδιαίτερα στον απλό χρήστη. Κάθε άλλο, όμως: η ανάκλαση μικροκυματικής ακτινοβολίας είναι γνωστή από τη δεκαετία του '50, ενώ αν παρατηρήσει κανείς τα έγγραφα που παρουσίασε ο Snowden, πολλά από τα συστήματα που περιγράφονται αναφέρουν ημερομηνίες διάθεσης από το 2008–2009. Χωρίς υπερβολή, με δεδομένη την ασταμάτητη εξέλιξη της τεχνολογίας, οι δυνατότητες των πραγματικά μελλοντικών συστημάτων υποκλοπών θα είναι τρομακτικές.

Τι μπορεί να γίνει λοιπόν; Ο έλεγχος των μαζικών υποκλοπών και των καθολικών παρακολουθήσεων και η προστασία μπορεί να επιτευχθεί μόνο με μια ευρεία συνεργασία Πολιτικής, Δικαιοσύνης, Βιομηχανίας, Ακαδημίας, Δημοσιογραφίας και Κοινωνίας. Δυστυχώς ή ευτυχώς, η τεχνολογία από μόνη της δε μπορεί να δώσει τη λύση!

Συμβουλές για τους γονείς!

• Προτιμήστε να τοποθετήσετε τον υπολογιστή σας σε χώρους όπως είναι το σαλόνι, και όχι στο υπνοδωμάτιο του παιδιού. Έτσι, θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.

• Κάντε την πλοήγηση στο Διαδίκτυο οικογενειακή δραστηριότητα. Χρησιμοποιήστε τον υπολογιστή μαζί με τα παιδιά σας.

• Ενημερώστε τα παιδιά σας για τους κινδύνους που ελλοχεύουν όταν συνομιλούν με αγνώστους μέσω chatrooms.

• Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.

• Διδάξτε τα να μη δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα, ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ωράρια σχολείου, ονόματα φίλων κ.λπ.).

• Μη δίνετε στα παιδιά την πιστωτική σας κάρτα για να τη χρησιμοποιήσουν σε διαδικτυακές συναλλαγές.

• Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου. Διδάξτε τα να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν μπορεί, να είναι επικίνδυνοι.

• Χρησιμοποιήστε τα λεγόμενα «φίλτρα», που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητά sites (βία, πορνογραφία).

• Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.ά., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.

• Μείνετε κοντά στα παιδιά σας και εμπλακείτε σε κάθε δική τους διαδικτυακή δραστηριότητα, με τον ίδιο τρόπο που κάνετε για τις δραστηριότητες του σχολείου.

• Μιλήστε με το παιδί σας και κάντε το να συνειδητοποιήσει ότι, αν προκύψει κάτι ξαφνικό ή ενοχλητικό στο Διαδίκτυο, πρέπει να κλείσει την ηλεκτρονική σελίδα.

Διαδίκτυο

Το διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο. Η λέξη διαδίκτυο προέρχεται από τις λέξεις Διασύνδεση Δικτύων και αναφέρεται σε ένα σύνολο υπολογιστών και δικτύων που συνδέονται μεταξύ τους σε ένα παγκόσμιο δίκτυο έτσι ώστε να μπορούν να επικοινωνούν και να μοιράζονται πληροφορίες. Στα Αγγλικά η λέξη Internet προέρχεται από τις λέξεις International Network που σημαίνει Διεθνές Δίκτυο Υπολογιστών.

Το διαδίκτυο παρομοιάζεται με «υπερλεωφόρο πληροφοριών». Καθημερινά διακινούνται πλήθος δεδομένων με οποιαδήποτε μορφή - κείμενα , εικόνες , ήχοι, μουσική, βίντεο - φέρνοντας στην οθόνη του υπολογιστή μας ένα τεράστιο αριθμό ψηφιακών πηγών πληροφόρησης. Σε αυτή όμως την παγκόσμια Κοινωνία της Πληροφορίας είναι πολύ δύσκολο έως ακατόρθωτο να υπάρχει ένα είδος ελέγχου της ποιότητας, της εγκυρότητας και της καταλληλότητας των πληροφοριών που φτάνουν στον υπολογιστή μας. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος λέει "Ναι Στο Διαδίκτυο και τις Νέες Τεχνολογίες", ενώ παράλληλα θεωρεί υποχρέωσή της να ενημερώνει τους πολίτες για τους κινδύνους του διαδικτύου και για τους τρόπους που μπορούν να μας βοηθήσουν να προστατέψουμε τους εαυτούς μας και να «σερφάρουμε» με ασφάλεια στο διαδίκτυο.

Δράσεις Δίωξης Ηλεκτρονικού Εγκλήματος

Ημερίδες Ασφαλούς Πλοήγησης: Διοργανώνονται ημερίδες σε όλη την Ελληνική Επικράτεια, έχοντας ως στόχο την ενημέρωση μαθητών, γονέων και εκπαιδευτικών για τα φαινόμενα διαδικτυακής βίας, τους κινδύνους που ελλοχεύουν στις ιστοσελίδες κοινωνικής δικτύωσης και γενικά την πρόληψη και την αντιμετώπιση των κινδύνων που σχετίζονται με τις νέες τεχνολογίες.

Διοργάνωση συνεδρίων σε πανευρωπαϊκό επίπεδο: με αφορμή τον εορτασμό της Παγκόσμιας Ημέρας Ασφαλούς Πλοήγησης στο Διαδίκτυο, πραγματοποιούνται από την Υπηρεσία μας συνέδρια σχετικά με Ασφαλή Πλοήγηση στο Διαδίκτυο τα οποία περιελάμβαναν παρουσιάσεις από διακεκριμένους και εξειδικευμένους σε θέματα που αφορούν στην Ασφαλή Πλοήγηση στο Διαδίκτυο, επιστήμονες της Ελλάδας και του εξωτερικού.

Ενημερωτικά συνέδρια σε μαθητές ειδικών σχολείων: Στόχος είναι η ενημέρωση της ευαίσθητης ομάδας των παιδιών, για τους κινδύνους που κρύβει το διαδίκτυο και για τους τρόπους αντιμετώπισης των προκλήσεων του ψηφιακού κόσμου, καθώς είναι ύψιστης σημασίας η ισότιμη συμμετοχή των μαθητών αυτών, στην κοινωνία της γνώσης και των σύγχρονων τεχνολογιών.

Τηλεδιασκέψεις: Πραγματοποιούνται, κάθε εβδομάδα (Τρίτη και Πέμπτη), με ιδιαίτερη επιτυχία ενημερώσεις σε σχολεία ανά την επικράτεια, μέσω της υιοθέτησης της τεχνολογίας των τηλεδιασκέψεων με παράλληλη σύνδεση σε πολλαπλά σημεία.

Τηλεοπτικά «σποτ»: Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προχώρησε στην παραγωγή και προβολή μέσω ραδιοφωνικών και τηλεοπτικών σταθμών πανελλαδικής εμβέλειας, τριών τηλεοπτικών «σποτ» στο πλαίσιο της εκστρατείας πληροφόρησης ευαίσθητων κοινωνικών ομάδων για την προστασία τους από τις παγίδες του διαδικτύου.

Ιστότοπος cyberkid.gr: Παρέχονται χρήσιμες πληροφορίες και συμβουλές σχετικά με το πως μπορεί να εκμεταλλευτεί όλη η οικογένεια τα θετικά των σύγχρονων τεχνολογιών που μας περιβάλλουν και φυσικά του διαδικτύου. Δημιουργήθηκε πρόσφατα η ενότητα «Ψηφιακή Αλάνα», όπου τα παιδιά μπορούν να παίζουν τα αγαπημένα τους ηλεκτρονικά παιχνίδια με απόλυτη προστασία από τους κινδύνους που παραμονεύουν στο διαδίκτυο.

Εφαρμογές Cyberkid για φορητές συσκευές (APPS): Δημιουργήθηκε με σκοπό να ενημερώνει καθημερινά τους γονείς και τα παιδιά κάθε οικογένειας για την ασφαλή πλοήγηση στο διαδίκτυο και τους κινδύνους που ελλοχεύουν σε αυτό. Δίνει την δυνατότητα άμεσης επικοινωνίας με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος μέσω της γραμμής CYBER ALERT, ενώ υπάρχει η δυνατότητα ψυχαγωγίας μέσω των διαφόρων παιχνιδιών.

Χορηγοί Έκδοσης

ISBN 978-960-14-2938-0