ΝΕΕΣ ΠΡΟΚΛΗΣΕΙΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

-

Η ΠΡΟΟΠΤΙΚΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

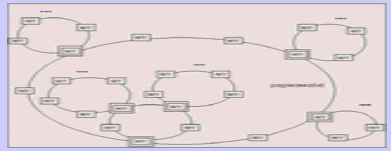
Γ. ΠΑΓΚΑΛΟΣ

Καθ. Πολυτεχνικής Σχολής ΑΠΘ

Εθνικός εκπρόσωπος FP7 / SECURITY

11 - 4 - 2008

Ι. ΤΟ ΝΕΟ ΠΕΡΙΒΑΛΛΟΝ

Το νέο περιβάλλον:  +  + 

- **Ηδη:**
  - πάνω από 1.100.00 ευρυζωνικες συνδέσεις στην Ελλάδα - (KIN > 5*Η/Υ)
  - αξία κλάδου τηλεπικοινωνίες + Πληροφορική στην Ελλάδα 2008: 23 δις Ε
  - 58% επιχειρήσεων μέχρι και 5% προυπ/μου στις ΤΠΕ
  - ρυθμός αύξησης κινητών > των Η/Υ (παγκόσμια)
- **Νέα πραγματικότητα: Πληροφορικη + Δικτυα + Επικοινωνιες (Στ+Κιν).**

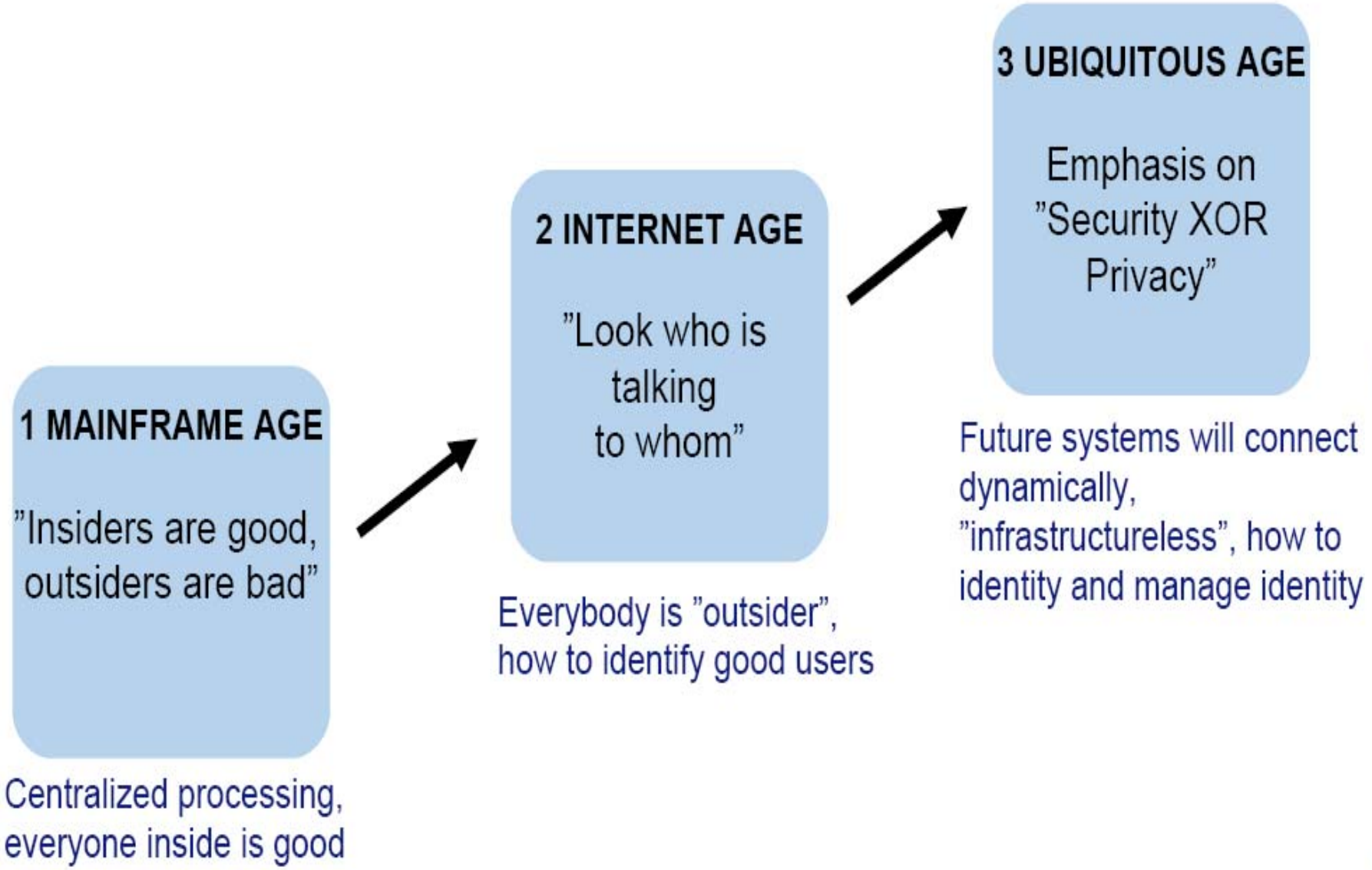
  (Fast ιντερνετ, πολυμεσικες υπηρεσίες, νέες υπηρεσίες, ενιαίος λογαρ/μος…)
- **Λέξη-κλειδί: Σύγκλιση (τεχνολογική / υπηρεσιών)**
- **Τάση για Λ.Σ. ανοικτής αρχιτεκτονικής και στα κινητά (SYMBIAN+MICROSOFT ήδη > 10%)**
- **Νέα κινητά: μικροί (ατελείς) Η/Υ (μέγεθος, κόστος, κλπ)**
- **Νέες εφαρμογές: π.χ. Χρήση κινητών για ηλεκτρονικές πληρωμές**
  - Ήδη (Ασία) / Γαλλία ('payez mobile', και 3 δίκτυα - VISA / MASTER)
  - Εγκατάσταση τεχνολογίας NFC στις κάρτες SIM και σύνδεση με τραπ. λογ. Χρήστη (ήδη: LG L600V, Motorola L7, etc)

➔ Η ασφάλεια ΒΑΣΙΚΟ ΠΡΟΒΛΗΜΑ / ΠΡΟΥΠΟΘΕΣΗ

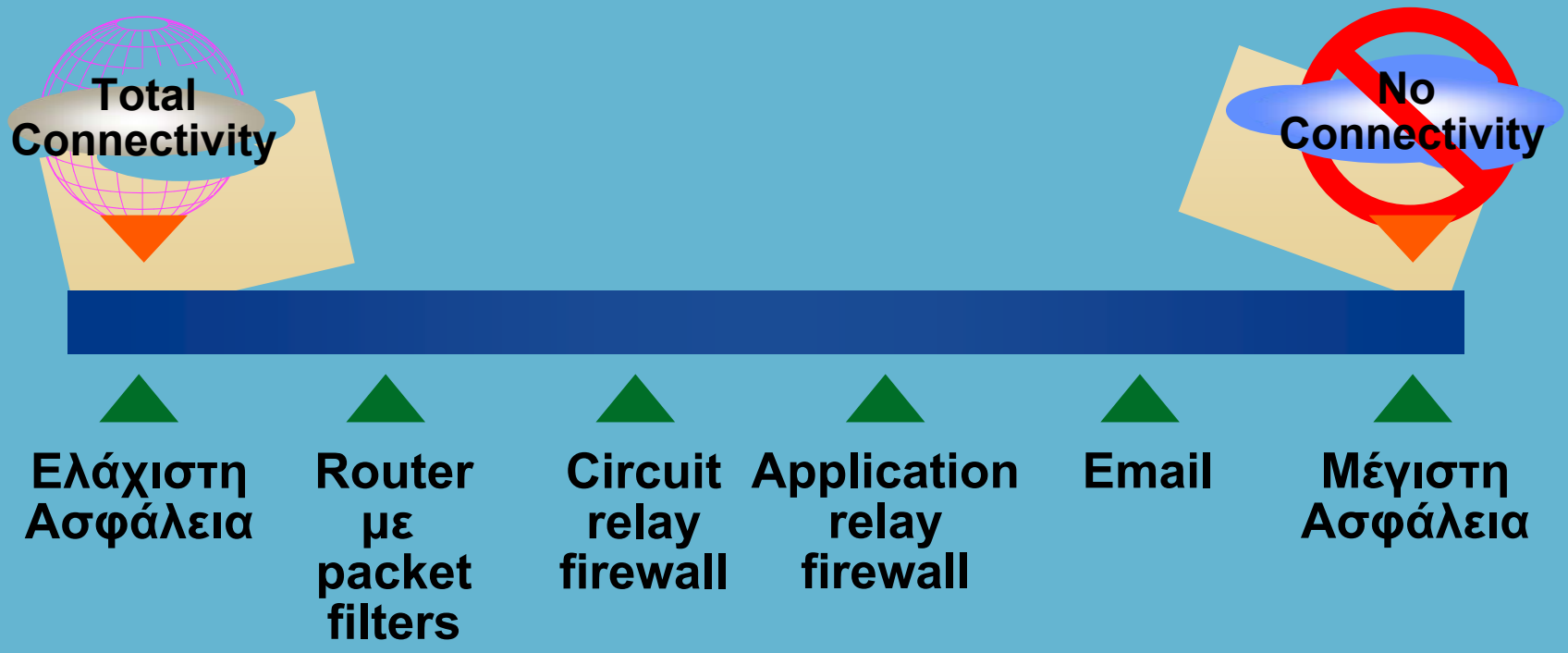
Το νέο περιβάλλον: ΑΠΕΙΛΕΣ

(attacks today: some Facts)

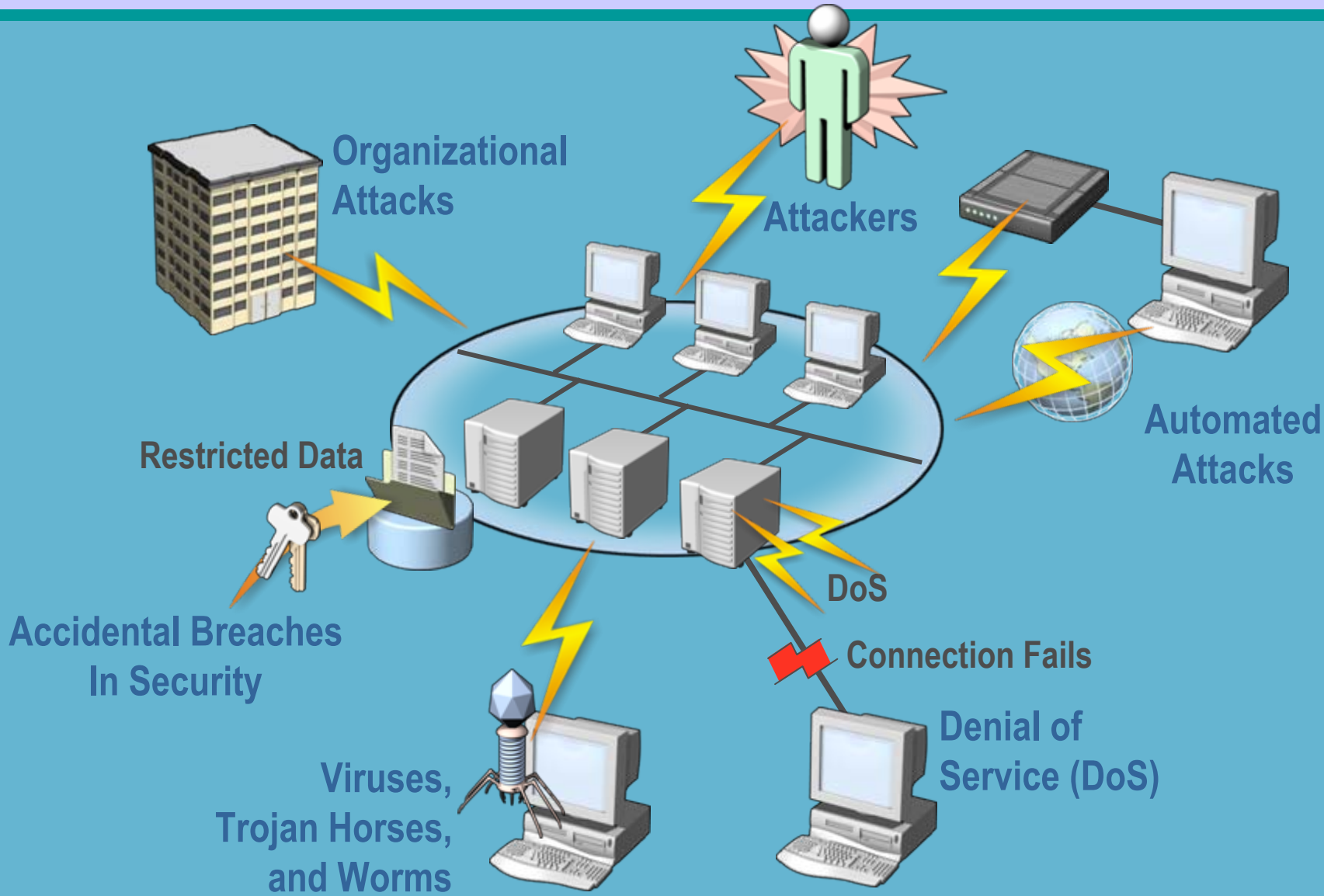
EVOLUTION OF COMPUTING PARADIGMS



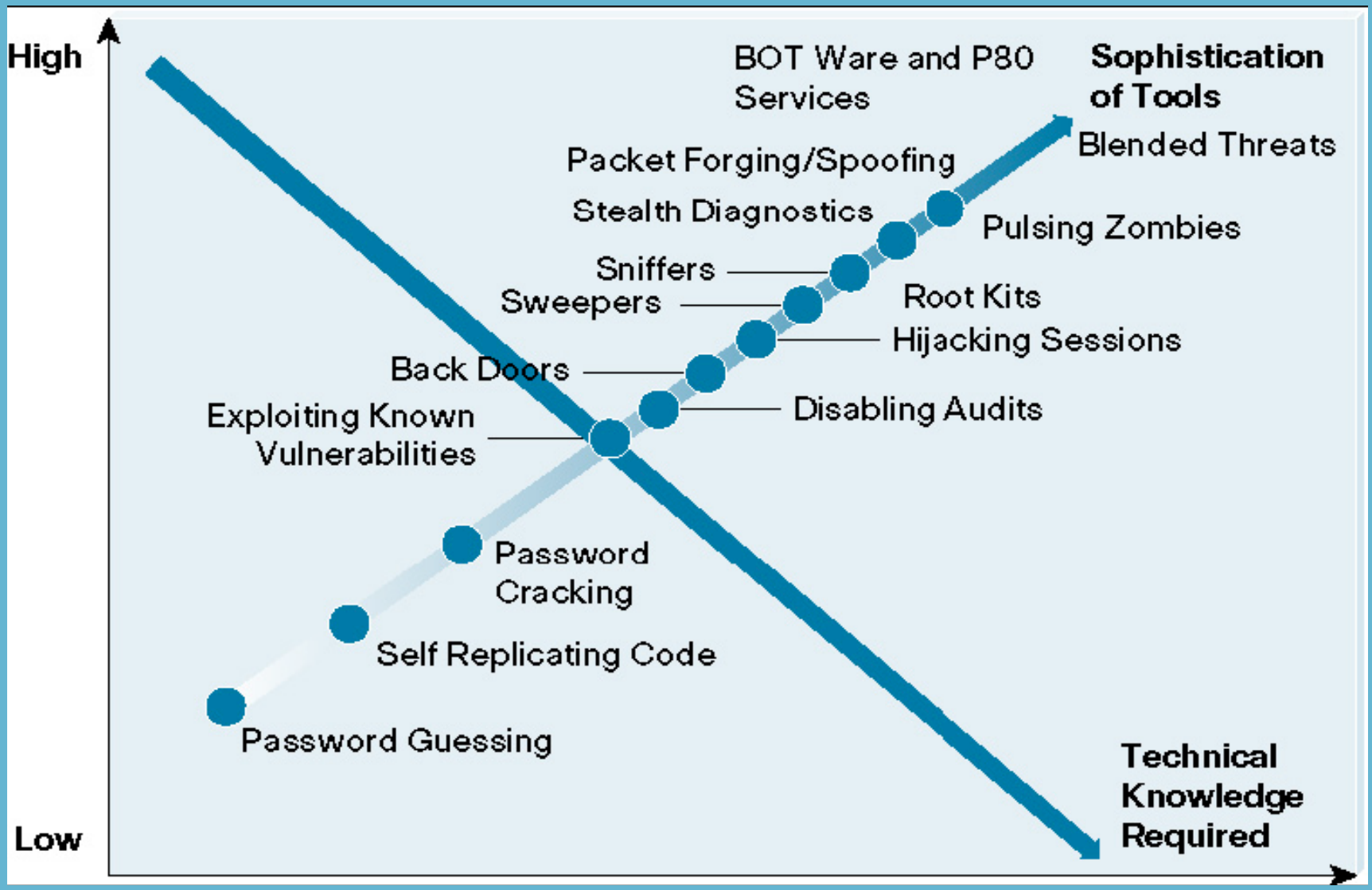
Συνδεσιμότητα σε σχέση με την Ασφάλεια:



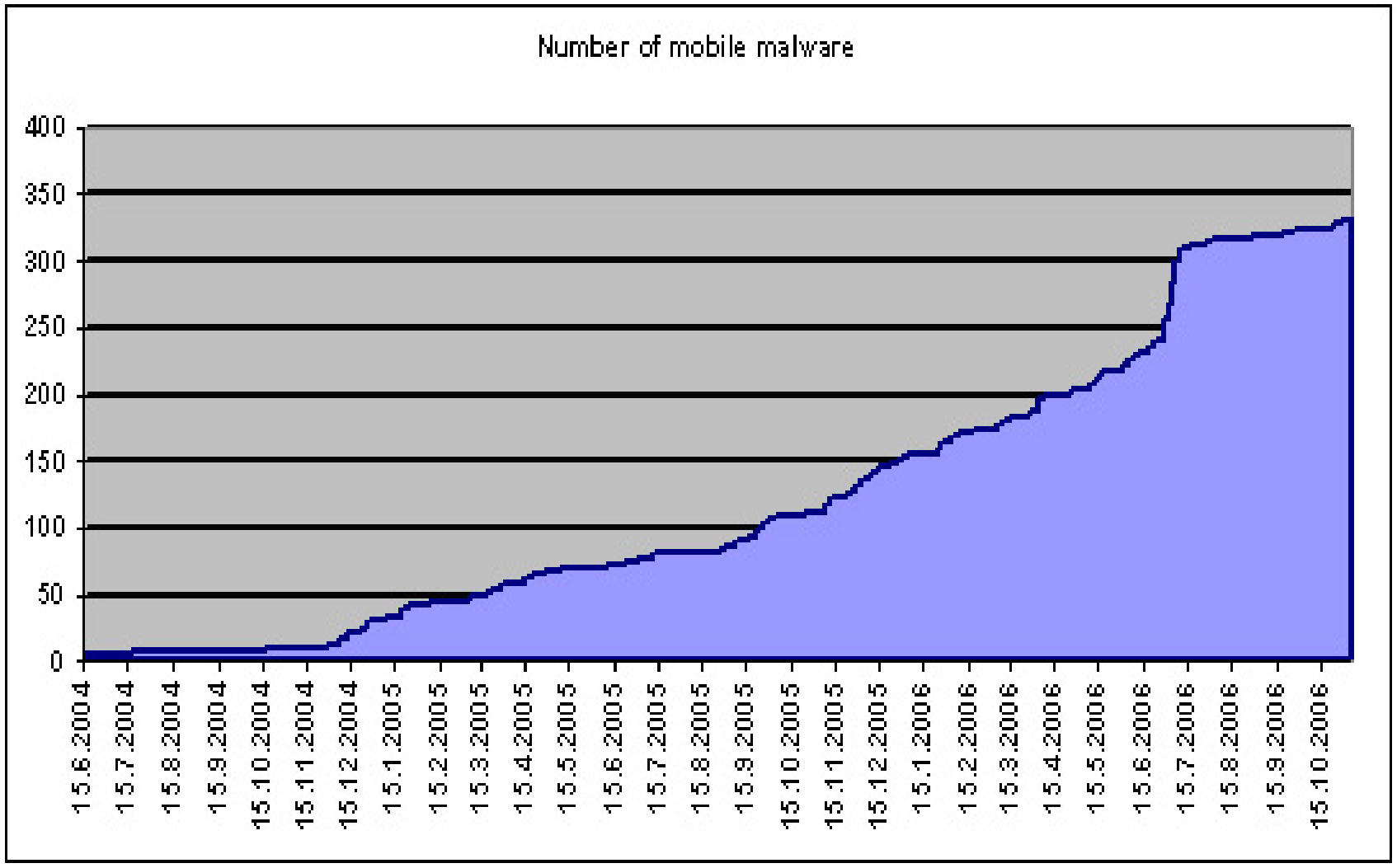
Συνηθισμένοι Τύποι Επιθέσεων σε δίκτυα – Η/Υ: :



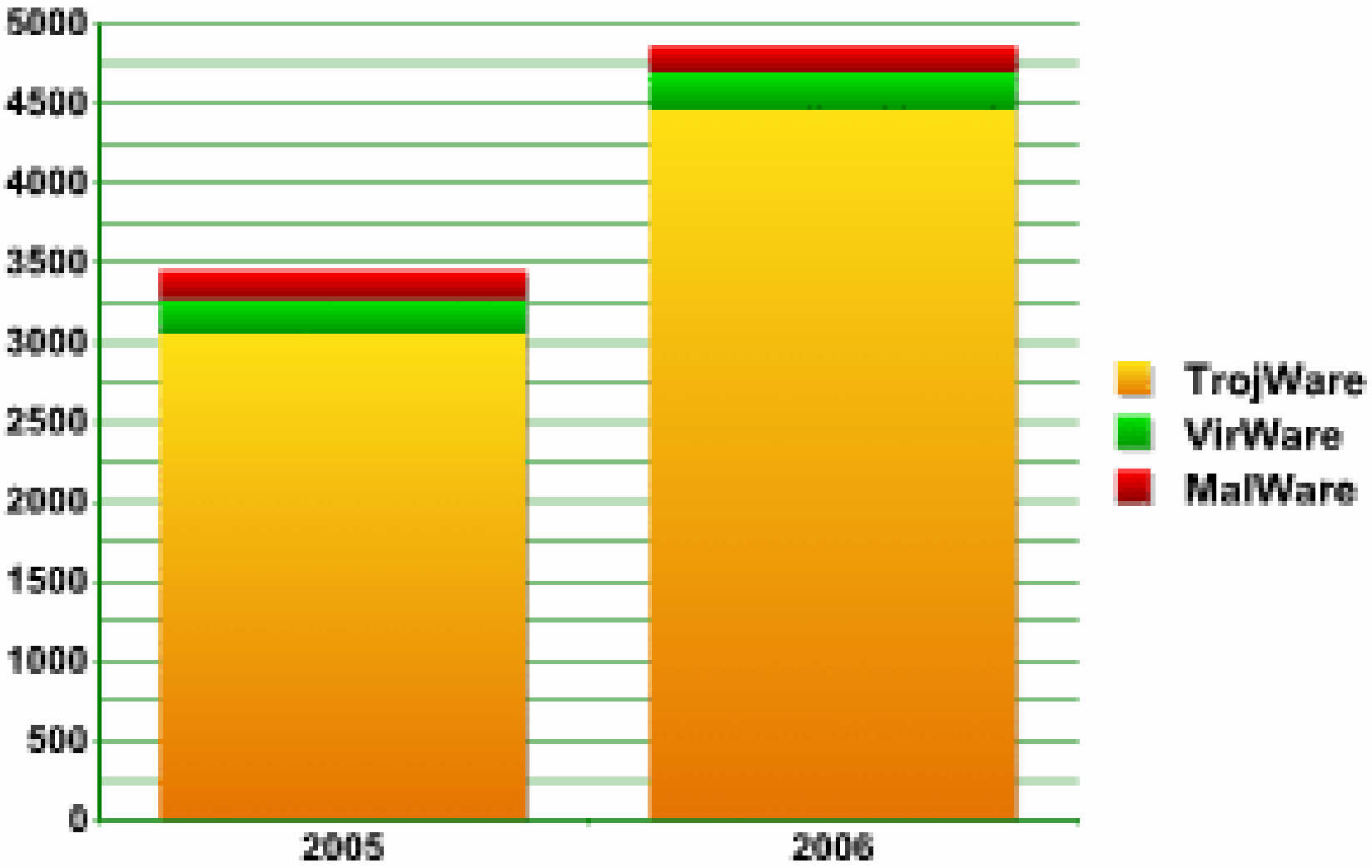
Επιθέσεις στα δίκτυα επικοινωνιών:



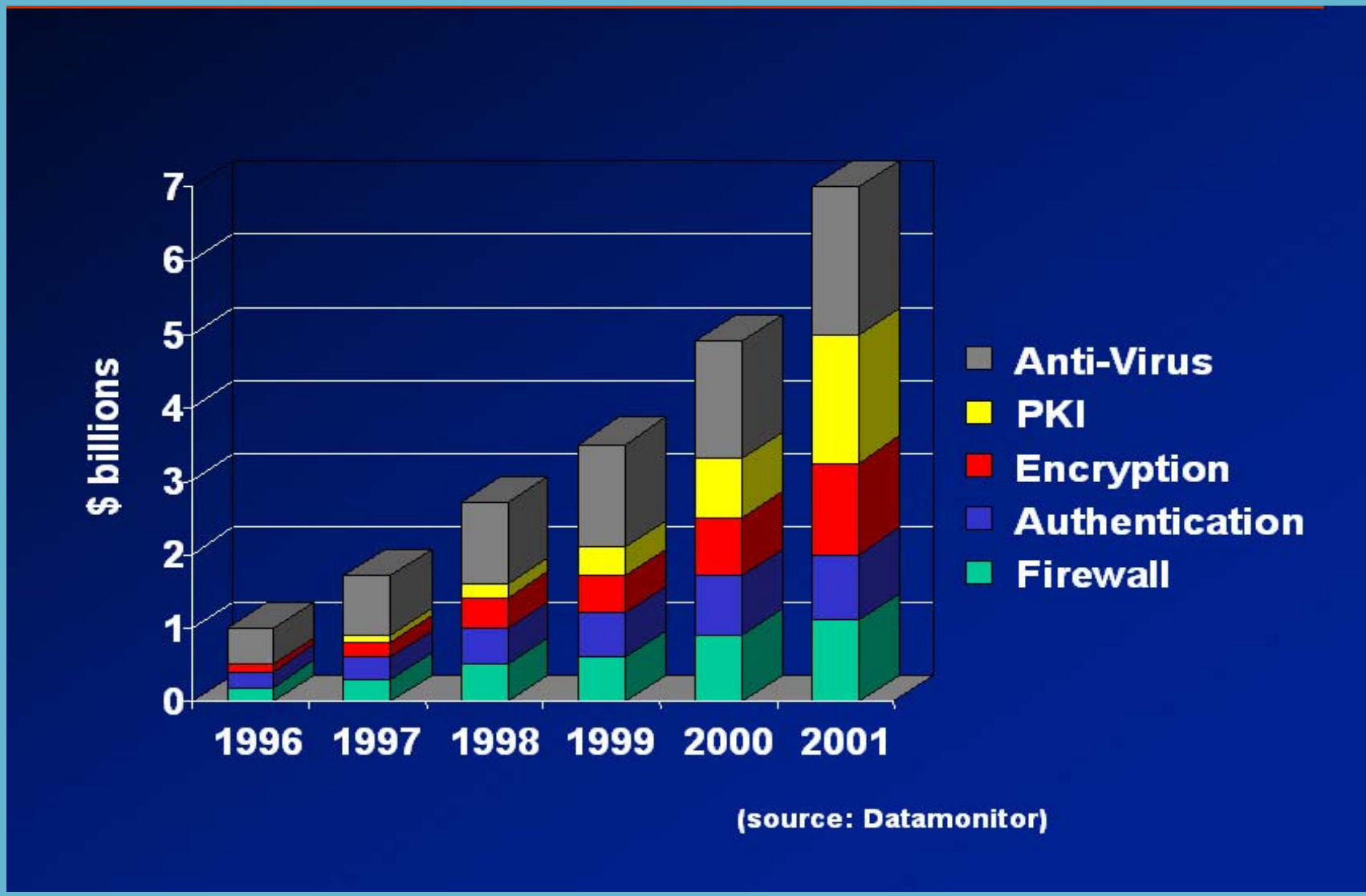
Ρυθμός αύξησης αριθμού malware στα δίκτυα κινητων:



Μέσος αριθμός νέων malicious programs ανά μήνα



ΤΟ ΚΟΣΤΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ:



Η ηλεκτρονικη επικοινωνια εισάγει πολλούς νέους κινδύνους:

Identification is the Challenge

"On the Internet, nobody knows you're a dog..."

II.
ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

Πολύ σύντομα:

- Τα δίκτυα σταθερής και κινητής τηλεφωνίας θα **αντιμετωπίζουν τις ίδιες επιθέσεις** με τα δίκτυα IP (που εξυπηρετούν Internet, e-mail, κλπ εφαρμογές).
- Η ικανότητα παροχής ασφαλών δικτύων για την υποστήριξη πολυμέσων υπηρεσιών θα αποτελεί τον **βασικό παράγοντα διαφοροποίησης** ανάμεσα σε manufacturers, integrators, network operators, και service providers.
- Η ασφάλεια θα αποτελεί μια από τις πιο **βασικές προϋποθέσεις** για την επιτυχή ανάπτυξη των δικτύων επόμενης γενιάς (: φωνή, πολυμέσα και specialist functions)

III.
ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΚΕΥΩΝ

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΚΕΥΩΝ

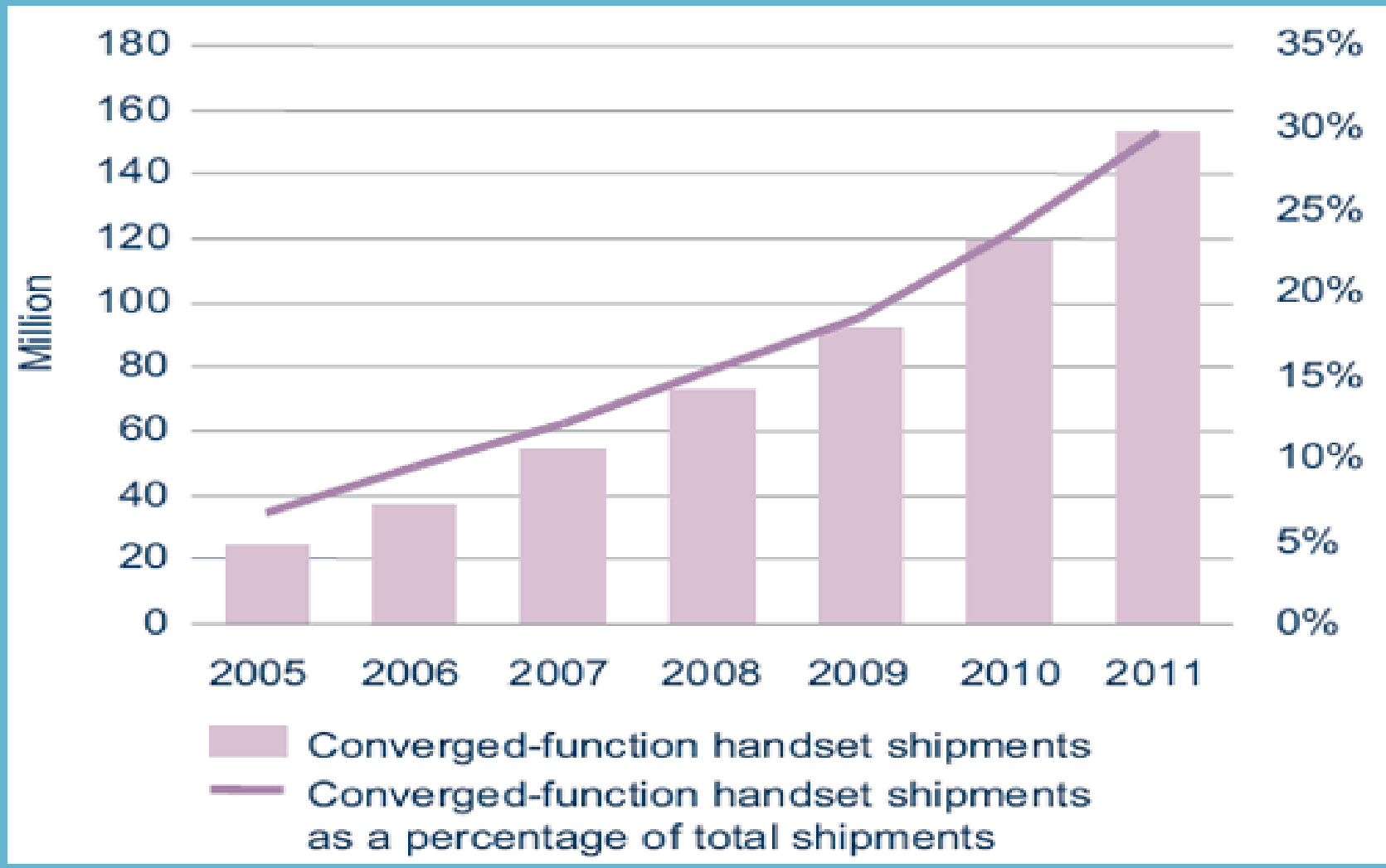
- Τα κινητά νέας γενεάς (converged-function handsets) θα κυριαρχήσουν μέχρι το 2011 (*Analysis Research)*.

- Τα νέα κινητά αποτελούν μεγάλη πρόκληση από άποψη ασφαλείας, λόγω:
  - Αυξημενων δυνατοτητων διασυνδεσης (connectivity),
  - Αυξημενου ογκου αποθηκευμενων δεδομενων (data stored)
  - Μεγαλη δυνατοτητα να ‘μολυνουν’ ιδιωτικα και εταιρικα δικτυα
  - Περιορισμενων ενσωματωμενων μηχανισμων αμυνας (μεγεθος/κοστος)

- Παρατηρειται συνεχης αύξηση των malware για κινητά

Converged-function handsets in developed markets

(Source: Analysis Research, 2006)



Το προβλημα:

- Τα σύγχρονα κινητά (smartphones) είναι στην ουσία μικροί, φορητοί υπολογιστές
- Είναι συνεπώς ευάλωτοι στους ιδίους κινδύνους: viruses, spam, phishing, κλπ.
- Οι αναγκαίοι περιορισμοί σε όγκο / βάρος / κόστος κάνουν τα συστήματα αυτά πιο ευάλωτα,
  και την ενσωμάτωση μηχανισμών άμυνας δυσκολότερη
- Η χρήση VoIP στα δίκτυα φορέων σε συνδυασμό με την απουσία επαρκών μηχανισμών άμυνας θα εισάγει και νέα προβλήματα ασφαλείας (next generation of phone hacking).

ΣΥΜΠΕΡΑΣΜΑ:

- Η σύγκλιση των τεχνολογιών φέρνει νέους κινδύνους ασφάλειας (integrated risk).
- Παρατηρείται ήδη συνεχής αύξηση των επιθέσεων σε κινητά τηλέφωνα (Juniper Research) .
- Με τον αριθμό των κινητών να είναι ήδη ΥΠΕΡ-ΠΕΝΤΑΠΛΑΣΙΟΣ από αυτόν των PC's, <u>το πρόβλημα ασφαλειας όλο και θα μεγαλώνει.</u>
- Οι προκλησεις αυτές ολο και θα μεγαλωνουν.
  Πιο συγκεκριμένα:…

IV.
ΟΙ ΝΕΕΣ ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Α. Τεχνολογικές εξελίξεις

1. Νέα συστήματα κινητών επικοινωνιών (πέραν της 3ης γενιάς)

- **Σε επίπεδο υπηρεσιών, σημαίνει:**

την παροχή νέων, ποιοτικών υπηρεσιών, όπως:

- **διαδραστικών επικοινωνιών πολυμέσων και κινητής τηλεόρασης (DVB-H),**
- **δυνατότητα πρόσβασης στις νέες υπηρεσίες μέσω ασύρματων ευρυζωνικών δικτύων (WLAN hotspots, WiMAX),**

με τρόπο που να εξασφαλίζεται:

- **η διαλειτουργικότητα με τα υπάρχοντα δίκτυα**
- **η λειτουργία διαφανώς προς το χρήστη (seamless operation)**

- **Σε επίπεδο εξοπλισμού χρήστη, σημαινει:**

τερματικά «πέραν της 3ης γενιάς» (PDAs, smart-phones),
που είναι στην πραγματικότητα προσωπικοί υπολογιστές-μινιατούρες, με:

- **ευέλικτο λογισμικό,**
- **επαρκή αποθηκευτικό χώρο, και**
- **διεπαφές πρόσβασης στα ασύρματα δίκτυα,**

ώστε να υποστηρίζουν τις νέες υπηρεσίες.

Νέα συστήματα κινητών επικοινωνιών πέραν της 3ης γενιάς …

- **Σε επίπεδο δικτυων πυρήνα (core networks), σημαινει:**

  την επικράτηση αμιγούς τεχνολογίας Διαδικτύου (all-IP networks)

- **Δηλαδη:**
  την ενοποίηση όλων των διακριτών δικτύων σε ένα, τεχνολογίας IP
  (π.χ. Βρετανική BT: όλο της το δίκτυο σε αμιγές δίκτυο IP).

- **=>**

  θεαματικές επιπτώσεις, τόσο στο τεχνολογικό όσο και στο επιχειρηματικό μοντέλο παροχής ενοποιημένων υπηρεσιών
  (και, τελικώς, στο κόστος των παρερχόμενων υπηρεσιών).

Νέα συστήματα κινητών επικοινωνιών πέραν της 3ης γενιάς …

- **Σε επιπεδο τεχνολογιων και πρότυπων, σημαινει:**
- **Την αυξημενη χρήση των ανοιχτών τεχνολογιών και προτύπων, σε βάρος των ιδιοταγών (proprietary),**
- **Σκοπός: η διασφάλιση της διαλειτουργικότητας σε έναν απελευθερωμένο και λιγότερο καθετοποιημένο επιχειρηματικό χώρο.**

  (Σε συνδιασμο με την γενικευμένη χρήση της τεχνολογίας IP σε επίπεδο δικτύου).

Β.
Αλλαγές στο επιχειρηματικό μοντέλο

Απελευθέρωση και οριζόντια διάρθρωση των αγορών των επικοινωνιών

- Βασική πολιτική της ΕΕ είναι η ελεύθερη παροχή / διακίνησή υπηρεσιών και προϊόντων και η λειτουργία του ανταγωνισμού.
- Αυτο, σε συνδυασμό με τις τεχνολογικές εξελίξεις, οδηγει σε:
  - περισσότερο οριζόντια διάρθρωση των αγορών, με διαχωρισμό των παρόχων δικτύων, υπηρεσιών, περιεχομένου.
  - Την ευρυτερη υιοθετηση πρακτικων 'outsourcing'

    (π.χ. εταιρία κινητής τηλεφωνίας μπορεί να αναθέσει την υπηρεσία καρτοκινητής τηλεφωνίας ή τη χρέωση ή ακόμη και την ασφάλεια των συστημάτων της σε άλλη εταιρία ως outsourcing).

V.
Επιπτώσεις των εξελίξεων στην ασφάλεια

Επιπτώσεις των εξελίξεων στην ασφάλεια:

- Οι εξελίξεις αυτές αναμένεται να επηρεάσουν ριζικά και το μοντέλο ασφάλειας στο νέο τοπίο.
- Η πολιτική ασφάλειας στο συγκεκριμένο χώρο θα πρέπει να είναι μια δυναμική διαδικασία κατανόησης και προσαρμογής του εξελισσόμενου περιβάλλοντος.
- Με αυτή την έννοια, η ασφάλεια είναι *διαδικασία* παρά *κατάσταση* (a process rather than a state).
- Μερικοί από τους αναδυόμενους κινδύνους είναι:

1. Κίνδυνοι των συστημάτων «πέραν της 3ης γενιάς»

- Η εξέλιξη των τερματικών σε μικρούς Η/Υ, σε συνδυασμό και με τη σύνδεσή τους σε ανοιχτά δίκτυα τεχνολογίας IP, τους δίνει πολλαπλές δυνατότητες
- Τους κληροδοτεί όμως και όλες τις αδυναμίες ασφάλειας και τους κινδύνους προσβολών των PCs: viruses, e-mail spam, warms, phishing (SmiShing), κλπ
- Καθώς δε η φορητή συσκευή:
  - θα χρησιμοποιείται όλο και περισσότερο για ευαίσθητες συναλλαγές και αποφάσεις (e-banking, decision support), και
  - θα διατηρεί περισσότερα προσωπικά / εμπιστευτικά δεδομένα,

  οι κίνδυνοι επιθέσεων θα αυξάνουν
- Είναι δε διαπιστωμένο ότι ο χρήστης είναι ο πιο αδύνατος κρίκος στην αλυσίδα ασφάλειας των πληροφοριών

2. Κίνδυνοι στο ανοιχτό, ενοποιημένο περιβάλλον

- Έως τώρα, η αδιαφάνεια και η μυστικότητα ήταν βασικο όπλο άμυνας στις επιθέσεις (security by obscurity).
- Από την άλλη πλευρά, τα ανοιχτά συστήματα (δηλ. συστήματα με γνωστά τα πρωτόκολλα επικοινωνίας, λογισμικό, και αλγ. κρυπ/σης):
  - εκτίθενται μεν σε όλους τους γνωστούς κινδύνους,
  - υποκεινται όμως και εξαντλητικο ελέγχο των μηχανισμών άμυνας από μια τεράστια ανοιχτή κοινότητα.
- Για την καλύτερη ασφάλεια, λοιπόν (και διαλειτουργικότητα), η τάση είναι προς τη χρήση ανοιχτών αλγορίθμων και μηχανισμών.

3. Η ασφάλεια στο νέο περιβάλλον - διαχυση ευθυνης

- **Οι τεχνολογικες εξελιξεις και η οριζόντια διάρθρωση της αγοράς συνιστα ένα εντελώς νέο τοπίο, με νέες προκλήσεις ασφάλειας.**
- **Το πρόσφατο συμβάν προσβολής στο δίκτυο της εταιρίας Vodafone, ανέδειξε π.χ το πρόβλημα της διάχυσης της ευθύνης μεταξύ των μερών (παρόχου, προμηθευτή εξοπλισμού, κλπ).**
- **Το σχετικό νομικό πλαίσιο χρήζει αντίστοιχης προσαρμογής.**

VI.
Βασικές αρχές για την ασφάλεια συστημάτων και πληροφοριών

- **το κλειδί της επιτυχίας ειναι μια δυναμική πολιτική ασφάλειας, διαρκώς προσαρμοζόμενη στα νέα δεδομένα**

- **Μερικές γενικά αποδεικτές σχετικές αρχές, ανεξάρτητες τεχνολογίας και επιχειρηματικών μοντέλων, είναι:**

1. Αρχή της απλότητας

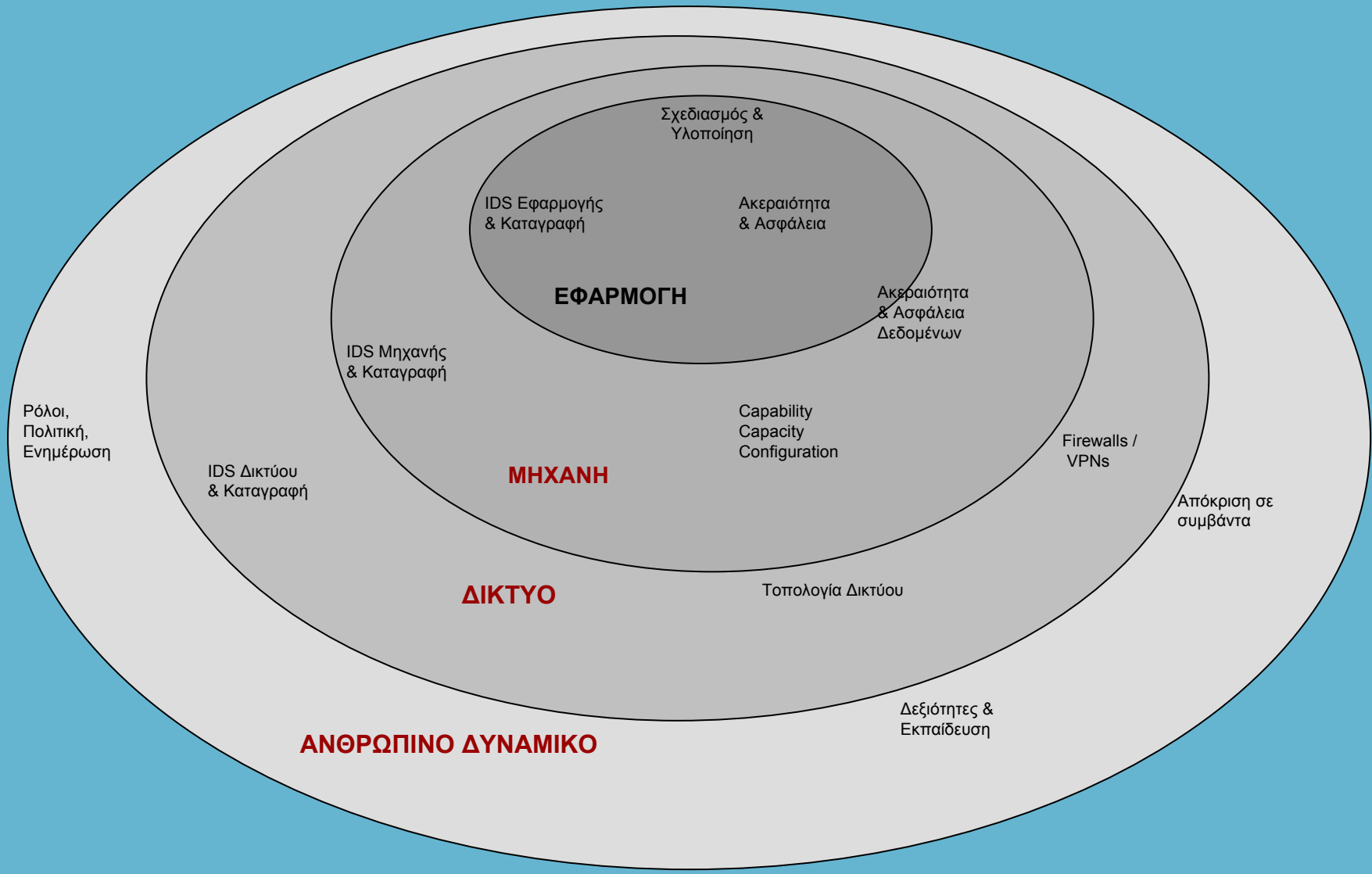
- **Είναι γνωστό ότι η πολυπλοκότητα είναι εχθρός της ασφάλειας.**
- **Σε κάθε περίπτωση, λοιπόν, θα πρέπει να προτιμώνται τα απλούστερα δυνατά συστήματα και μηχανισμοί που θα προσφέρουν τον επιθυμητό βαθμό ασφάλειας.**

2. Αρχή των πολλαπλών γραμμών άμυνας (Defense in-depth)

- **<u>Η οργάνωση της ασφάλεια σε επάλληλες γραμμές άμυνας</u> με ανεξάρτητους μηχανισμούς προστασίας και όχι σε μία μόνο (έστω και ισχυρή) περίμετρο, έχει προφανή πλεονεκτήματα.**

- **Π.χ., σε αντιστοιχία με τα τέσσερα διακριτά εμπλεκόμενα μέρη:**
  - **το Ανθρώπινο Δυναμικό,**
  - **το Δίκτυο,**
  - **τη Μηχανή, και**
  - **την εφαρμογή**

Επάλληλες γραμμές άμυνας και στοιχεία προστασίας



3. Αρχή του ελαχίστου δικαιώματος (least privilege)

- **Σε κάθε εμπλεκόμενο μέρος θα πρέπει να δίνονται <u>τα ελάχιστα απαραίτητα δικαιώματα ενεργειών</u> (πρόσβασης, διαχείρισης κλπ).**

3. Αρχή της ποικιλομορφίας μηχανισμών και συστημάτων (diversity of defense)

- **Π.χ.: χρήση συστημάτων διαφορετικών κατασκευαστών με διαφορετικά λειτουργικά συστήματα:**
- **(προσβολή με έναν ιό, για παράδειγμα, είναι απίθανο να συμβεί ταυτόχρονα σε δύο διαφορετικής κατασκευής λογισμικά).**

4. Αρχή της ασφάλειας σε αστοχία (fail-safe)

- **Για τις κρίσιμες υπηρεσίες, θα πρέπει να διασφαλίζεται ότι πιθανή αστοχία συστημάτων δεν θα έχει επίπτωση στην ποιότητα της προσφερόμενης υπηρεσίας.**
- **Π.χ.: η χρήση δύο παράλληλων συστημάτων, ενός κύριου και ενός εφεδρικού.**

5. Αρχή της στενωπού (choke point) για τη διέλευση πιθανών επιθέσεων

- **Η πρόσβαση στο Δίκτυο, τις Μηχανές και τις Εφαρμογές επιτρέπεται μέσω περιορισμένου αριθμού interfaces, η φύλαξη των οποίων μπορεί να διασφαλισθεί με επάρκεια και αποτελεσματικότητα.**

VII
ΔΙΑΔΙΚΑΣΙΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

- **Εφόσον το περιβάλλον ασφάλειας αλλάζει συνεχώς, είναι απαραίτητο να παίρνονται έγκαιρα μέτρα για την θωράκιση από άποψη ασφάλειας**

- **Αυτό περιλαμβάνει ενέργειες όπως:**
  - **Η εκτίμηση του σημερινού καθώς και (κυρίως) του επιθυμητού νέου επιπέδου ασφάλειας (security gap)**
  - **Ο προσδιορισμός των μεθόδων προστασίας που απαιτούνται για τη μετάβαση στο επιθυμητό νέο επίπεδο ασφάλειας**
  - **Ο προσδιορισμός των πολιτικών, τεχνολογιών και μέτρων ασφάλειας που μπορεί να τις ικανοποιήσει**
  - **Ο τρόπος αξιολόγησης (evaluation) του νέου περιβάλλοντος ασφαλείας**

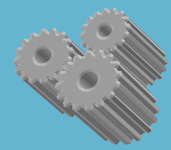
  κλπ.

Security Research

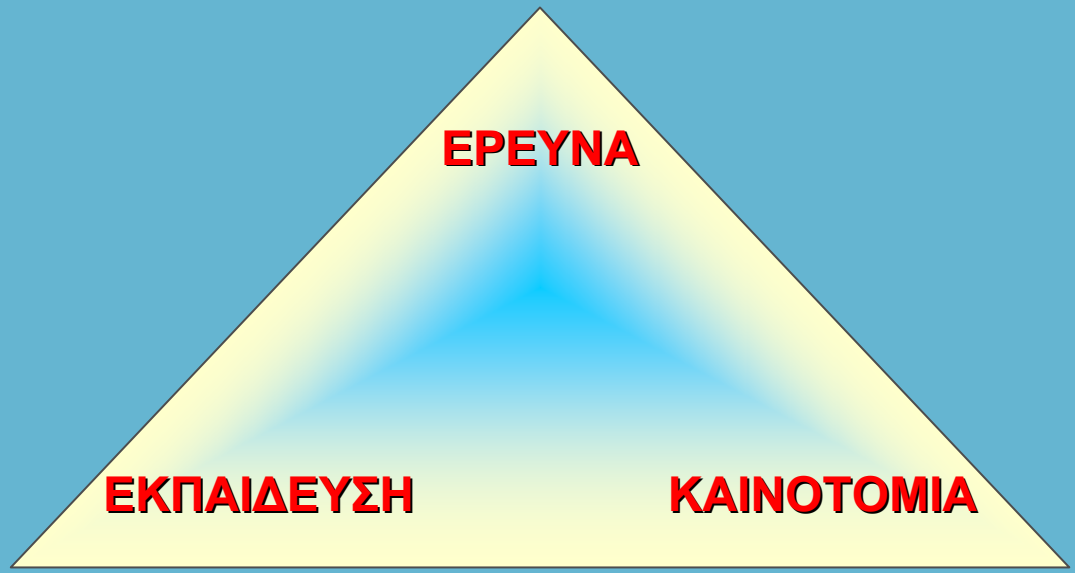
SEVENTH FRAMEWORK PROGRAMME

VIII.
Δράσεις της Ε. Ένωσης για την Ασφάλεια των Επικοινωνιών
-
Η έρευνα στον τομέα της Ασφάλειας στο 7ο Π.Π.

Ι. ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ 7ο Π.Π. (2007 - 20013)



7ο ΠΠ: Ενεργοποίηση του Γνωστικού Τριγώνου



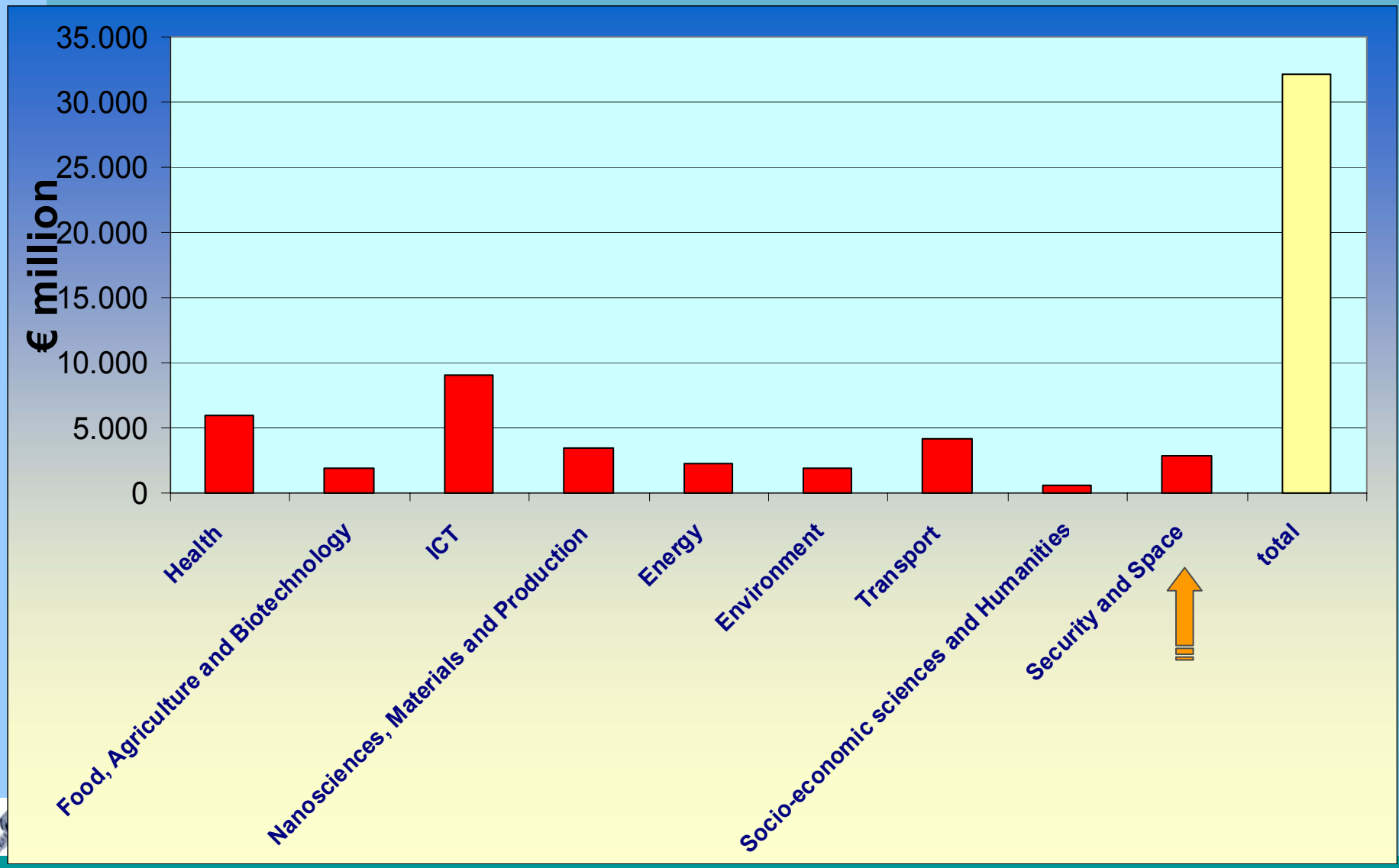
Για μια Ευρώπη Παγκόσμια Ανταγωνιστική
που βασίζεται στην Οικονομία της Γνώσης

ΘΕΜΑΤΙΚΟΙ ΤΟΜΕΙΣ 7ου Π.Π.:

1. ΥΓΕΙΑ
2. ΤΡΟΦΙΜΑ, ΓΕΩΡΓΙΑ, ΒΙΟΤΕΧΝΟΛΟΓΙΑ
3. ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΑΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ
4. ΝΑΝΟΕΠΙΣΤΗΜΕΣ, ΝΑΝΟΤΕΧΝΟΛΟΓΙΑ
5. ΕΝΕΡΓΕΙΑ
6. ΠΕΡΙΒΑΛΛΟΝ + ΚΛΙΜΑΤΙΚΕΣ ΑΛΛΑΓΕΣ
7. ΜΕΤΑΦΟΡΕΣ + ΑΕΡΟΝΑΥΠΗΓΙΚΗ
8. ΚΟΙΝΩΝΙΚΟ-ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΣΤΗΜΕΣ
9. ΔΙΑΣΤΗΜΑ
10. ΑΣΦΑΛΕΙΑ

ΚΑΤΑΝΟΜΗ ΠΡΟΥΠΟΛΟΓΙΣΜΟΥ 7ΟΥ ΠΠ

ΠΡΟΓΡΑΜΜΑ «ΣΥΝΕΡΓΑΣΙΑ»



ΙΙ. ΑΣΦΑΛΕΙΑ:
ΣΤΟΧΟΙ ΚΑΙ ΣΚΟΠΙΜΟΤΗΤΑ ΔΡΑΣΗΣ

ΔΙΑΠΙΣΤΩΣΗ:

- Η ασφάλεια είναι σήμερα ένα πολύ σοβαρό πρόβλημα, σε τοπικό, αλλά και διεθνές επίπεδο.
- Η ασφαλεια είναι ένα από τα νεοτερα δικαιωματα του πολιτη
- Η Ευρώπη θα πρέπει συνεπώς να επενδύσει σε νέες δράσεις και σε μια νέα νοοτροπία απέναντι στην ασφάλεια.
- **Στόχος:**

  Να κινητοποιηθεί το ανεκμετάλλευτο δυναμικό της ¨Ευρωπαϊκής ερευνητικής κοινότητας¨ και της "Ευρωπαϊκής βιομηχανίας ασφάλειας" ώστε να αντιμετωπιστούν οι σημερινές και μελλοντικές προκλήσεις.

Η ΠΡΟΚΛΗΣΗ ΓΙΑ ΤΗΝ Ε.Ε:

Να προσαρμοστεί στο νέο περιβάλλον, παραμένοντας ταυτόχρονα συνεπής προς τις θεμελιώδεις αξίες και στόχους της Ένωσης.

(security: … service to the society
… α modern human right)

Η ΑΝΤΙΜΕΤΩΠΙΣΗ:

1. ΑΝΑΔΕΙΞΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΝΑΝ ΑΠΌ ΤΟΥΣ 10 ΒΑΣΙΚΟΥΣ ΘΕΜΑΤΙΚΟΥΣ ΤΟΜΕΙΣ ΤΟΥ 7ου Π.Π.

2. ΔΙΑΤΗΡΗΣΗ ΤΩΝ ΕΠΙ ΜΕΡΟΥΣ ΔΡΑΣΕΩΝ ΑΣΦΑΛΕΙΑΣ ΣΤΟΥΣ ΥΠΟΛΟΙΠΟΥΣ ΤΟΜΕΙΣ

ΠΡΟΥΠΟΛΟΓΙΣΜΟΣ ΓΙΑ ΤΟΝ ΤΟΜΕΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ (10):

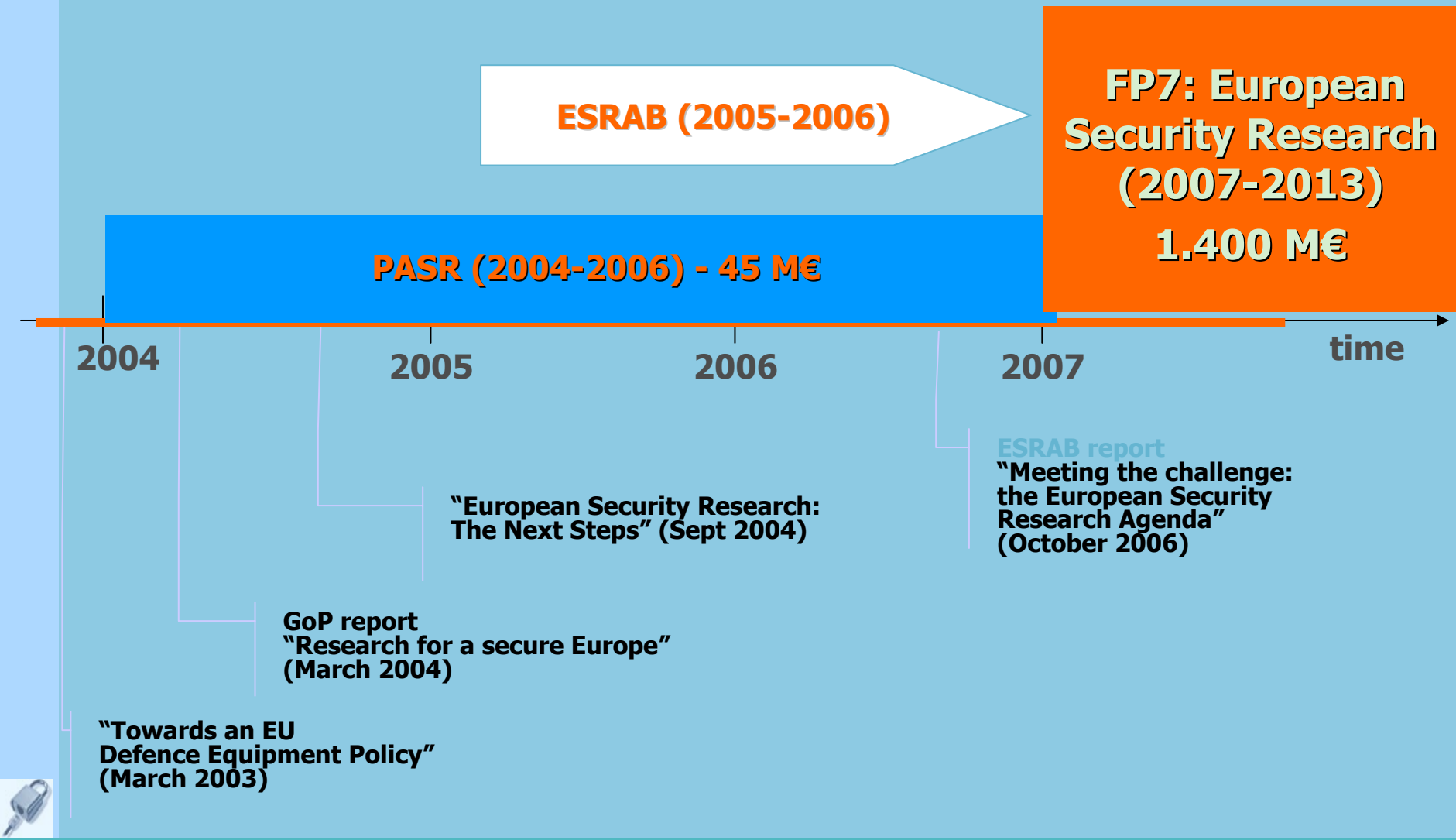
- ~ 2 ΔΙΣΕΚΑΤΟΜΥΡΙΑ ΕΥΡΩ !

Η ΝΕΑ ΟΠΤΙΚΗ:

- **Όχι πλέον διαχωρισμός σε:**
  - **Πολιτική και Στρατιωτική ασφάλεια**
- **Αλλά διαχωρισμός σε:**
  - **Παραγωγούς τεχνογνωσίας & συστηματων ασφάλειας (ερευνητική κοινότητα, βιομηχανία ασφάλειας)**

    και
  - **Μεγάλους χρήστες (επικοινωνίες, ηλεκτρονικό εμπόριο, δημ. τάξη, στρατός, κλπ)**

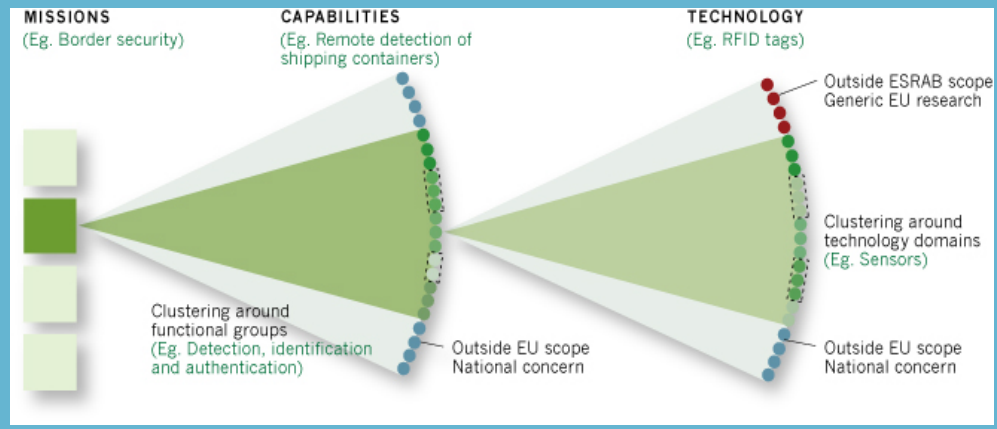
Διαχρονική Εξέλιξη:



ΤΟΜΕΙΣ ΠΡΟΤΕΡΑΙΟΤΗΤΑΣ:

ΒΑΣΗ: ΤΟ 'ESRAB REPORT':

missions ==> capabilities ==> technologies



Θεματικές περιοχές της δράσης Security:

/ FP7: 2007-13

- **4 Βασικές περιοχές (security missions / activities):**
- **3 Οριζόντιες δράσεις (cross cutting activities):**

Θεματικές περιοχές της δράσης Security (2007-13)

1. Ενίσχυση της ασφάλειας των πολιτών
   (Security of citizens)

2. Ασφάλεια υπηρεσιών κοινής ωφέλειας & υποδομών
   (Security of infrastructures and utilities)

3. Ευφυής παρακολούθηση & ασφάλεια συνόρων
   (Intelligent surveillance and border security)

4. Αποκατάσταση της ασφάλειας σε περιπτώσεις *κρίσεων*
   (Restoring security and safety in case of crisis)

Οριζόντιες δράσεις:
(cross cutting activities)

5. **Ασφάλεια διασυνδεδεμένων και διαλειτουργικών συστ/των**
   (Security systems integration, interconnectivity and interoperability)

6. **Ασφάλεια και κοινωνία**
   (Security & Society)

7. **Έρευνα σε θέματα ασφάλειας**
   (Security Research coordination and structuring)

ΑΣΦΑΛΕΙΑ ΣΕ ΑΛΛΟΥΣ ΤΟΜΕΙΣ ΤΟΥ 7ου Π.Π.:
ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ICT Technology Pillars:

- Nano-electronics, photonics and integrated micro/nano-systems
- Ubiquitous and unlimited capacity communication networks
- Embedded systems, computing and control
- Software, Grids, security and dependability
- Knowledge, cognitive and learning systems
- Simulation, visualisation, interaction and mixed realities

Σχήματα Χρηματοδότησης:

Συνεργατικά έργα
(Collaborative projects)

- Πολύ Μεγαλα → **Demonstration projects (30-40 M€)**
- Μεγαλα → **Integration projects (10-25 M€)**
- Μικρα εως Μεσαία → **Capability projects (2-5 M€)**

In the missions

for Security and society

Δρασεις υποστηριξης και συντονισμου
(Coordination and support actions)

Studies, networks, supporting actions

for Security research coordination and structuring

Απολογισμός και Συμπεράσματα από την πρώτη Ελληνική συμμετοχή

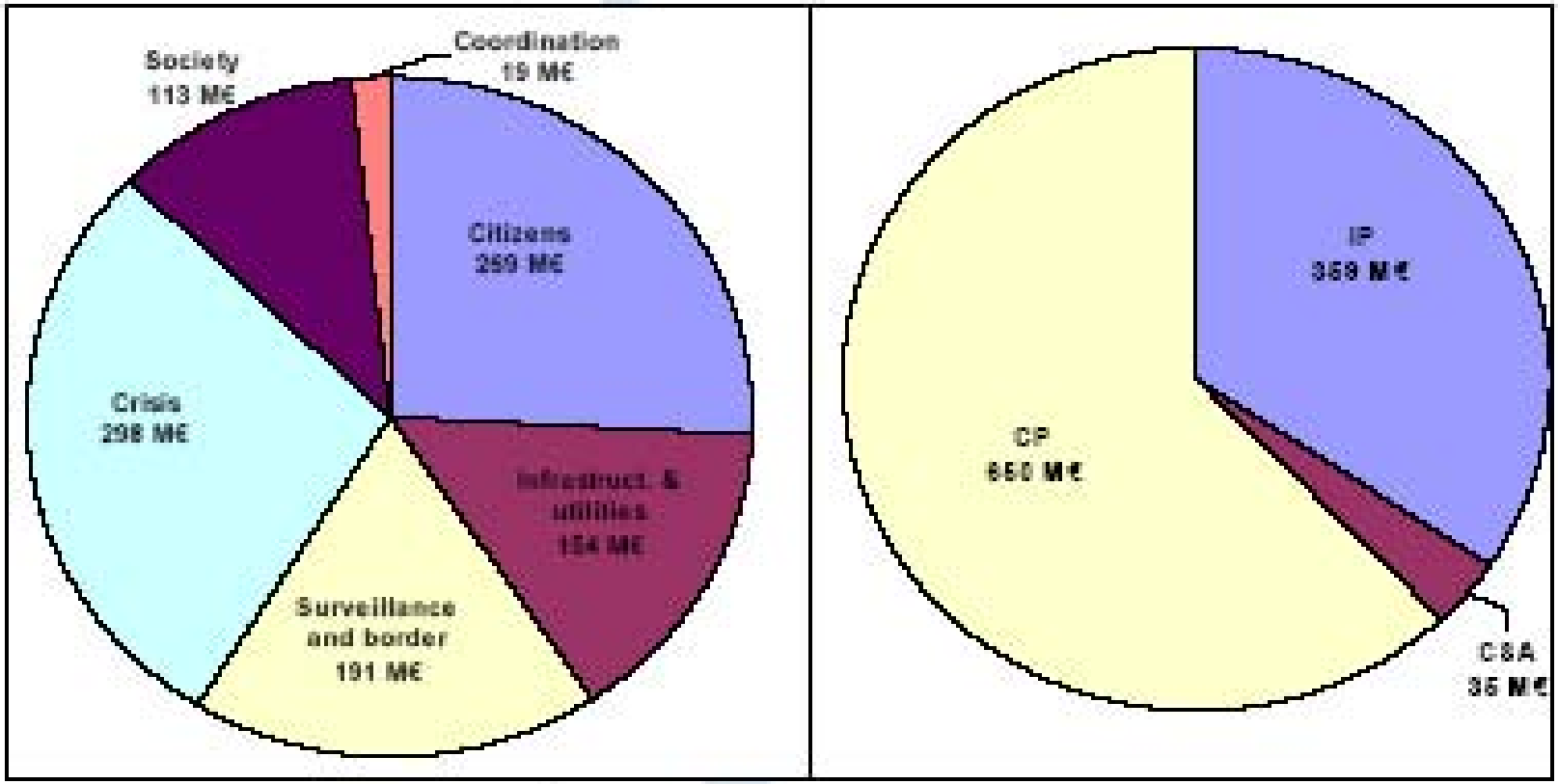
Security theme in FP7 2007 – 2013

- **4 Security missions / activities**:
  1. Security of citizens
  2. Security of infrastructure and utilities
  3. Intelligent surveillance and border security
  4. Restoring security and safety in case of crisis

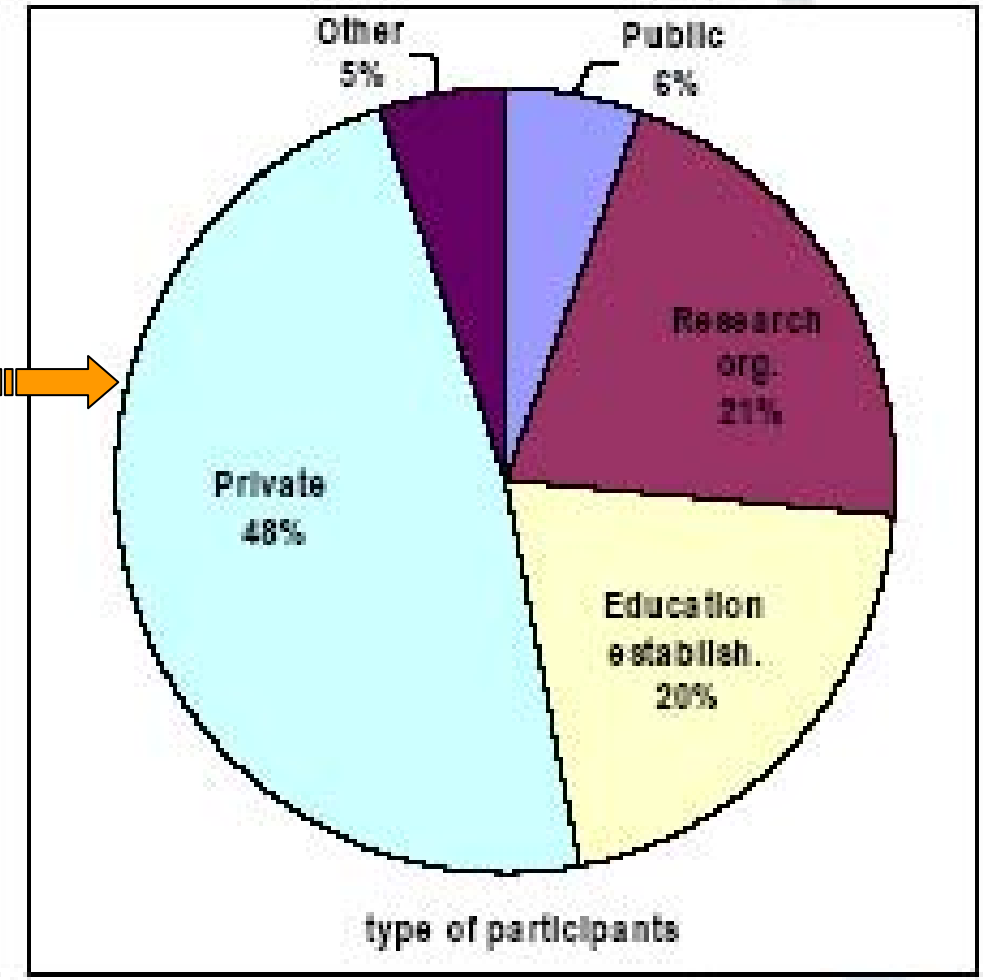
- **3 Cross cutting activities**:
  5. *Security systems integration, interconnectivity and interoperability* – **not open in 1st call**
  6. Security and Society
  7. Security Research coordination and structuring

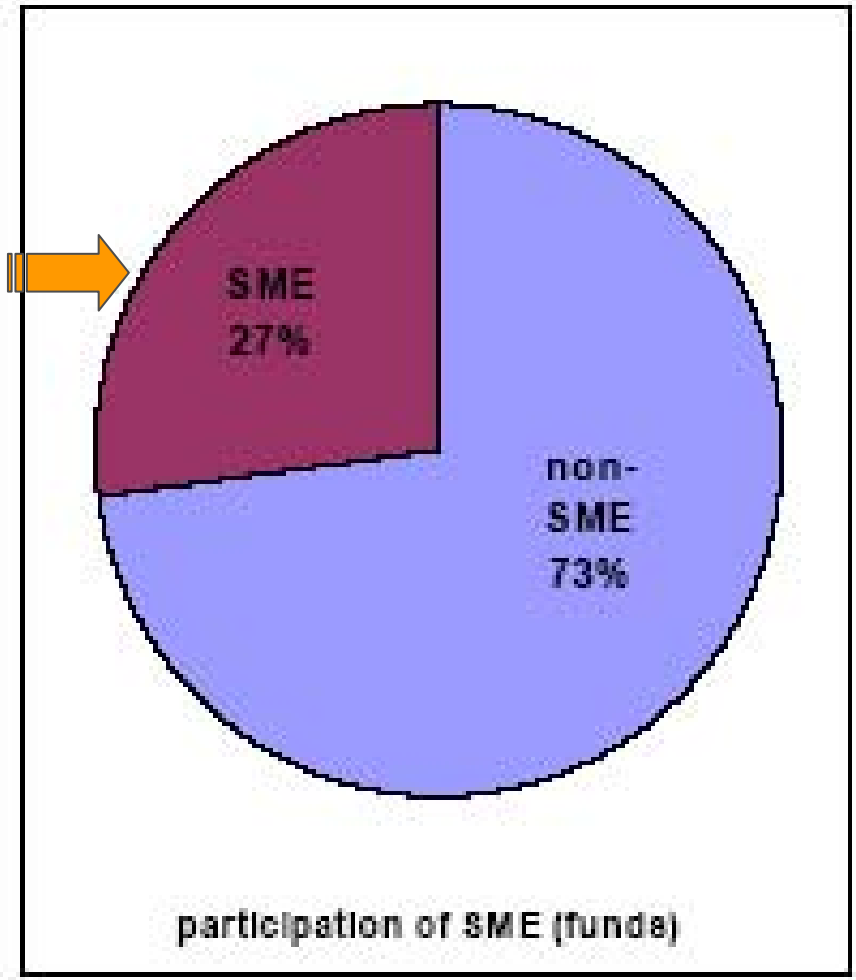
High over-subscription

- 325 eligible proposals
- Requested EU contribution : 1.046 M€

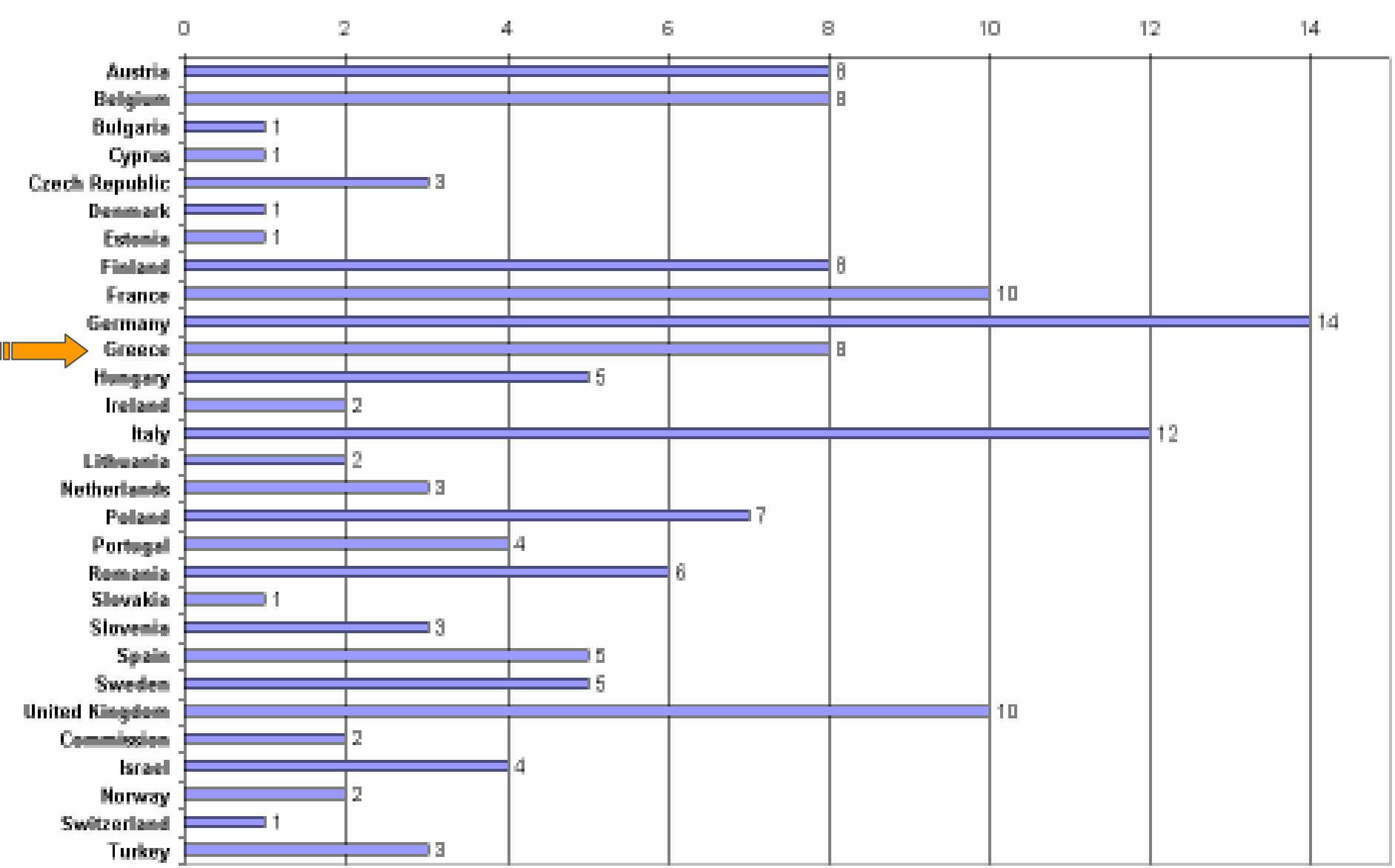


Statistics on participants





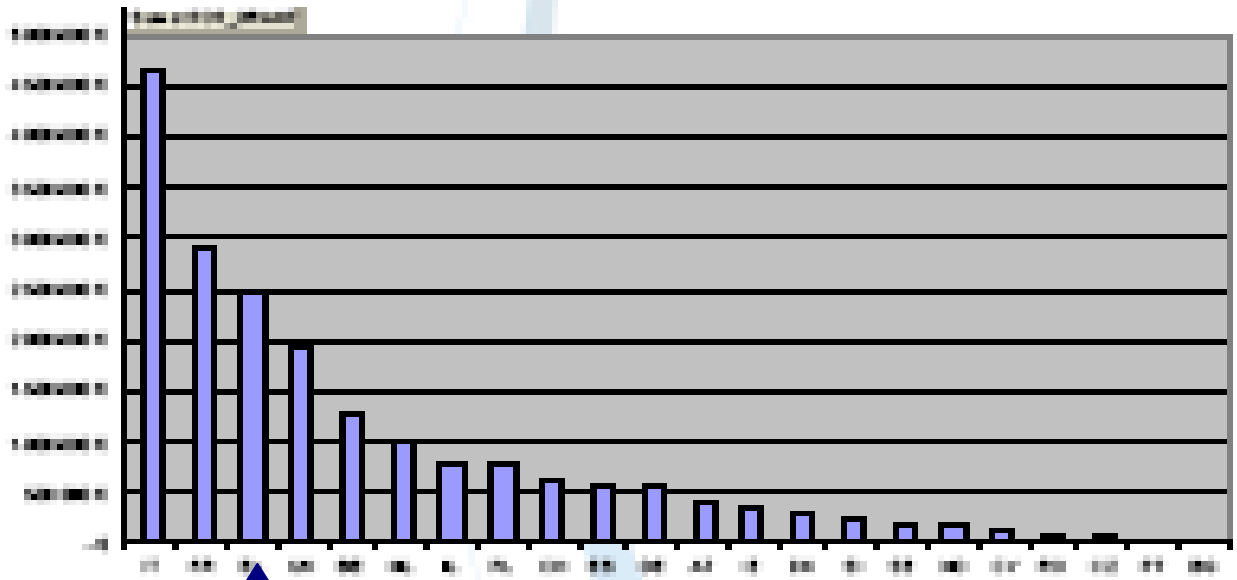
Overview of Experts' nationality



ΕΠΙΔΟΣΕΙΣ ΧΩΡΩΝ:

	All proposals		Retained proposals	
	EC Contr. (M€)	%	EC Contr. (M€)2	%
AT	20.7	2.0%	4.1	2.5%
BE	26.7	2.5%	3.2	2.0%
BG	9.2	0.9%	0.4	0.2%
CY	6.3	0.6%	0.1	0.1%
CZ	14.2	1.3%	1.8	1.1%
DE	116.1	11.0%	16.8	10.4%
DK	23.8	2.3%	1.6	1.0%
EE	2.4	0.2%	1.0	0.6%
EL	42.2	4.0%	5.3	3.3%
ES	68.7	6.5%	10.5	6.5%
FI	26.3	2.5%	7.2	4.5%
FR	106.7	10.1%	21.3	13.2%
HU	14.6	1.4%	0.9	0.6%
IE	9.0	0.9%	0.7	0.4%
IT	137.6	13.1%	14.3	8.9%
LT	4.2	0.4%	0.1	0.1%
LU	1.5	0.1%	0.3	0.2%
LV	0.9	0.1%	0.6	0.4%
MT	0.5	0.0%	0.2	0.1%
NL	50.6	4.8%	5.3	3.3%
PL	29.1	2.8%	13.5	8.4%
PT	17.6	1.7%	1.1	0.7%
RO	19.9	1.9%	0.9	0.5%
SE	51.5	4.9%	12.1	7.5%
SI	8.1	0.8%	1.0	0.6%
SK	5.5	0.5%	3.3	2.1%
UK	144.9	13.8%	18.8	11.7%
CH	14.8	1.4%	0.6	0.4%
HR	1.9	0.2%	0.9	0.6%
IL	31.9	3.0%	6.5	4.0%
IS	0.4	0.0%	0.0	0.0%
NO	16.6	1.6%	3.8	2.4%
TR	21.5	2.0%	2.3	1.5%

Countries statistics (2/2)



ΟΙ ΝΕΟΙ ΚΑΝΟΝΕΣ ΤΟΥ FP7:

- **Ετησια Προγράμματα Εργασίας (WorkPrograms)**
  (όλα τα calls του έτους σε ένα doc)
- **Έμφαση στο impact**
- **Ίδια δομή έργων για όλα τα themes**
  (format, key notions, document structure, rules for cross-cutting issues etc.)
- **Ειδικότερα για το Security WP:**
  - Βάση οι συστάσεις του ESRAB
  - Αξιοποίηση της εμπειρίας του PASR
  - Συνδυασμός πολιτικών & τεχν/κών απαιτήσεων

Σημαντικά θέματα για το FP7-SEC-2007-1

Υποβολή προτάσεων:

- Περιορισμός: No classified proposals in this call
- Χρημματ/ση: All topics open for 75% funding
- Σημαντικό: End user involvement
- Νεα έννοια: Sensitive and classified actions
- Νέο: Security Aspects Letter
- Συμμετοχή: All topics open for int. coop/tion
- Τρόπος: Electronic submission of proposals

Επιλογή προτάσεων:

- Evaluation by experts from supply and demand side
- Single step evaluation
- Hearings for successful (demonstration / integration) projects

ΣΥΜΠΕΡΑΣΜΑ …

- Ο τομέας της ασφάλειας έχει αποκτήσει πολύ μεγάλη σημασία και έχει δημιουργηθεί ένα εντελώς νέο περιβάλλον σε ευρωπαϊκό επίπεδο
- Η ασφάλεια είναι ένας από τους 10 βασικούς τομείς δράσης του 7ου ΠΠ, με πρωτόγνωρο προϋπολογισμό (και σε πολλούς άλλους τομείς του)
- Η ασφαλεια των επικοινωνιων περιλαμβανεται στους τομεις που υποστηριζονται
- Οι δραστηριοποιουμενοι φορεις στην Ελλαδα μπορουν να συμμετεχουν για την βελτιωση (σαν παραγωγοι ή χρηστες)
- Οι επικοινωνιες εχουν ουτως ή αλλως υπερτοπικη διασταση (EU)
- Τα έργα όμως στον τομεα αυτό είναι συνήθως σύνθετα και η δημιουργία συνεργασιών δυσκολότερη (➔ χρειάζεται συστηματική προσπάθεια)
- Δημιουργούνται έτσι νέες μεγάλες ευκαιρίες & προοπτικές

Πληροφορίες:

(E.E.):

- **Ιντερνετ (EU Security research websites):**
  - http://ec.europa.eu/enterprise/security
  - http://cordis.europa.eu/security
  - http://cordis.europa.eu/fp7/calls/

- **Helpdesk:**
  - entr-pasr@ec.europa.eu

(NCP):

PRAXIS:
Ζαλοκώστα 4, Αθήνα / Πλ. Μοριχόβου 1, Θεσσαλονίκη
Τηλ: 210 36 07 690, 2310 55 27 91
e-mail: ncp@help-forward.gr, http://www.help-forward.gr

ΕΥΧΑΡΙΣΤΩ
ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ

Γ. Πάγκαλος
Εθν. Εκπρόσωπος SECURITY / FP7