

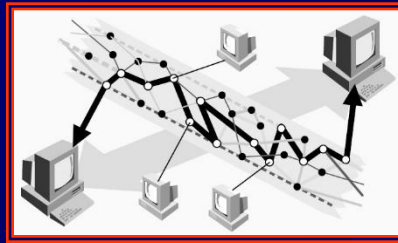


Security and Civic Disobedience in Cyberspace

Dimitris Gritzalis

April 2004

Ασφάλεια και Πολιτική Ανυπακοή στον Κυβερνοχώρο



Δημήτρης Γκοιτζαλης

Αναπλ. Καθηγητής Ασφάλειας στις ΤΠΕ

Τμήμα Πληροφορικής

Οικονομικό Πανεπιστήμιο Αθηνών

Cosmo: The world isn't run by weapons anymore, or energy, or money, it's run by little ones and zeroes, little bits of data. It's all just electrons.

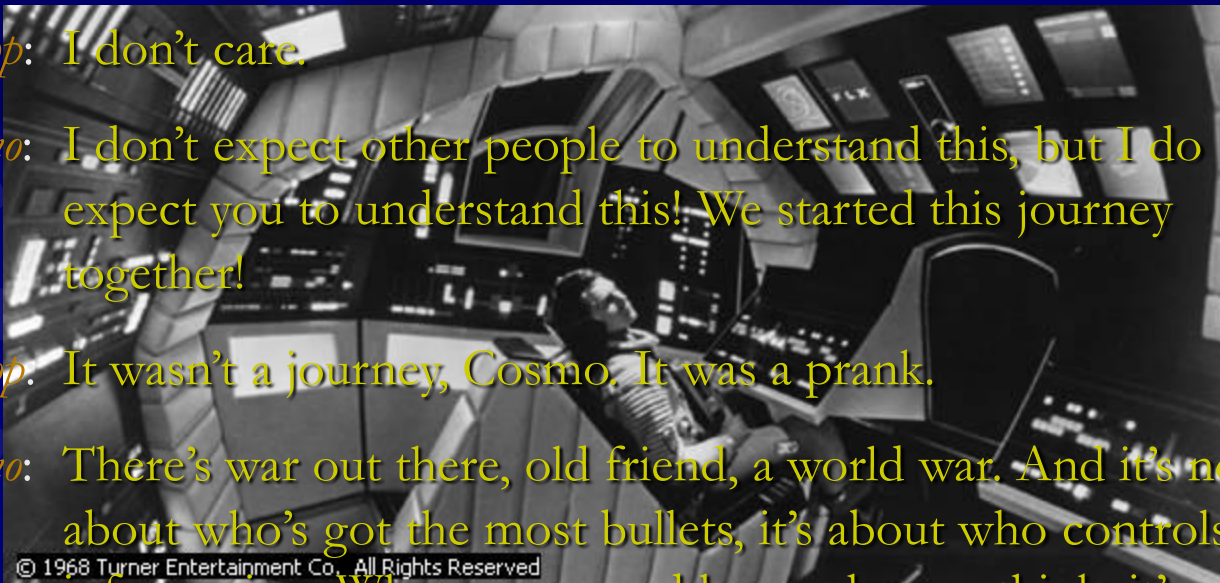
Bishop: I don't care.

Cosmo: I don't expect other people to understand this, but I do expect you to understand this! We started this journey together!

Bishop: It wasn't a journey, Cosmo. It was a prank.

Cosmo: There's war out there, old friend, a world war. And it's not about who's got the most bullets, it's about who controls the information. What we see and hear, what we think, it's all about the information!

Bishop: If I were you, I would destroy that thing...



© 1968 Turner Entertainment Co. All Rights Reserved

Sneakers (1992)

Οι τέσσερις ασυνέχειες (Mazlish)

Η Γη δεν είναι το κέντρο του σύμπαντος (Κοπέρνικος).

Ο άνθρωπος δεν κατέχει προνομιακή θέση στο σύστημα της δημιουργίας (Darwin).

Η συνείδηση, από μόνη της, δεν μπορεί να καταστήσει τον άνθρωπο κύριο του κόσμου (Freud).

Ο άνθρωπος δεν μπορεί να θεωρήσει τον εαυτό του ανώτερο, από όλες τις απόψεις, από κάθε μορφής υλικό αντιειμένο.



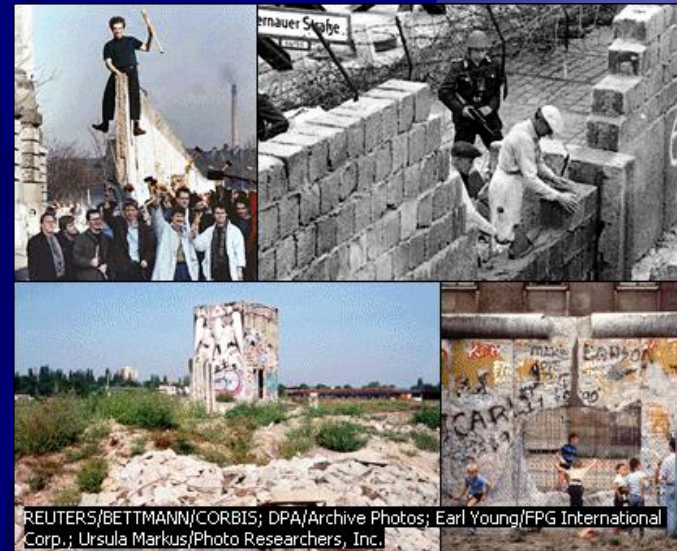
Η αρχή:
Επανάσταση των Μπολσεβίκων
(Οκτώβρης 1917)



Η αρχή:
Εναρξη του 2ου Παγκόσμιου
Πόλεμου (Ιούλιος 1914)

ΤΠ&Ε στα τέλη του “σύντομου” 20ου αιώνα

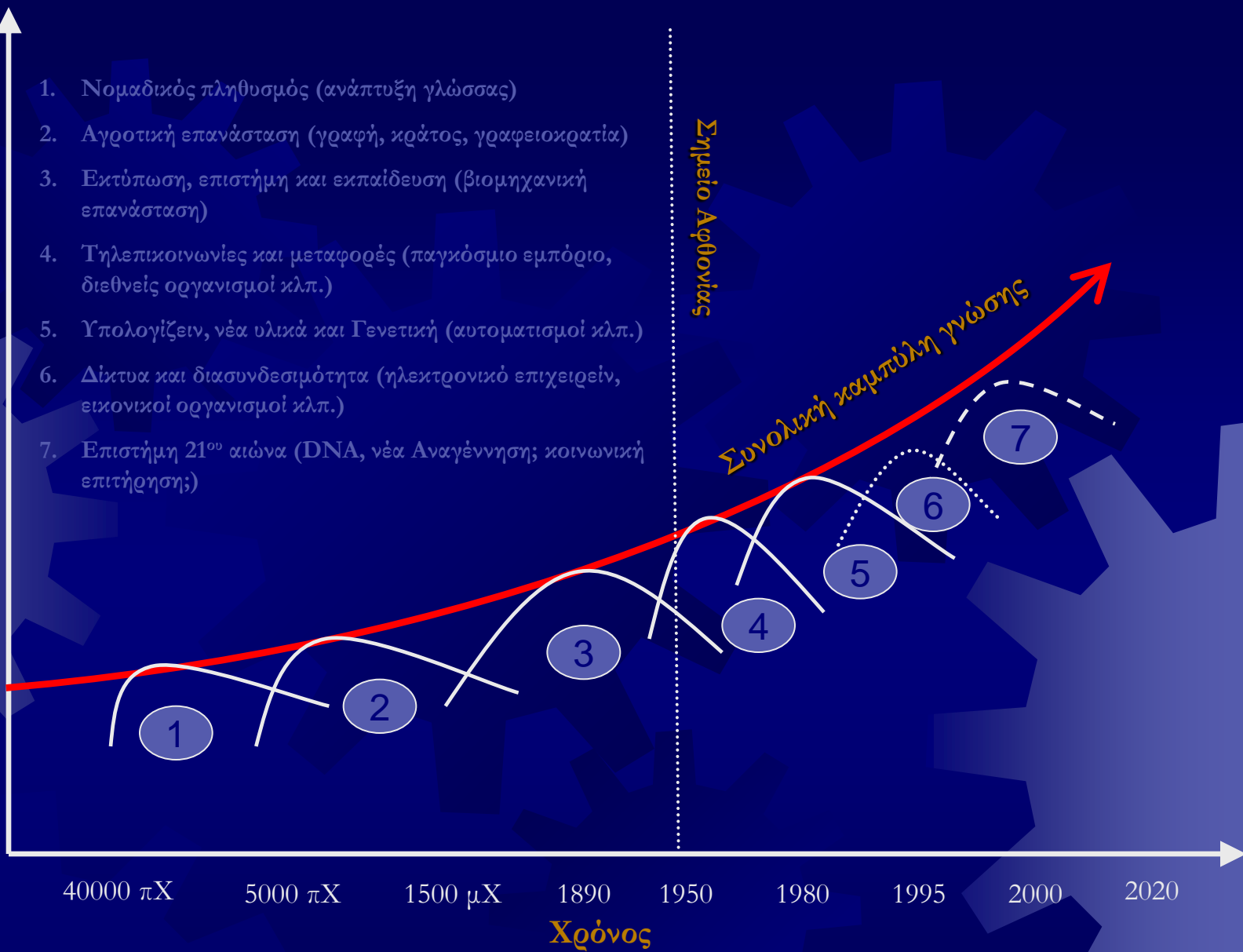
Το τέλος:
Πτώση του τείχους του Βερολίνου
(Νοέμβρης 1989)



REUTERS/BETTMANN/CORBIS; DPA/Archive Photos; Earl Young/FPG International Corp.; Ursula Markus/Photo Researchers, Inc.

Απαραίτητη μάθηση από ένα μέσο ενήλεια
προκειμένου να γίνει ενεργό μέλος της κοινωνίας

1. Νομαδικός πληθυσμός (ανάπτυξη γλώσσας)
2. Αγροτική επανάσταση (γραφή, κράτος, γραφειοκρατία)
3. Εκτύπωση, επιστήμη και εκπαίδευση (βιομηχανική επανάσταση)
4. Τηλεπικοινωνίες και μεταφορές (παγκόσμιο εμπόριο, διεθνείς οργανισμοί κλπ.)
5. Υπολογίζεин, νέα υλικά και Γενετική (αυτοματισμοί κλπ.)
6. Δίκτυα και διασυνδεσιμότητα (ηλεκτρονικό επιχειρείν, εικονικοί οργανισμοί κλπ.)
7. Επιστήμη 21^{ου} αιώνα (DNA, νέα Αναγέννηση; κοινωνική επιτήρηση;)



Τέλη 20ου αιώνα: Αναγκαία γνώση για ενεργή κοινωνική συμμετοχή

ERA: European Research Area

FP6, Eureka, COST, National RTD Programmes

... towards a
Single Market for Research

eEurope

Broadband access, e-business, e-government, **security**, skills, e-health, ...

Lisbon Strategy

"EU: Largest knowledge-based economy by 2010"

Enlargement

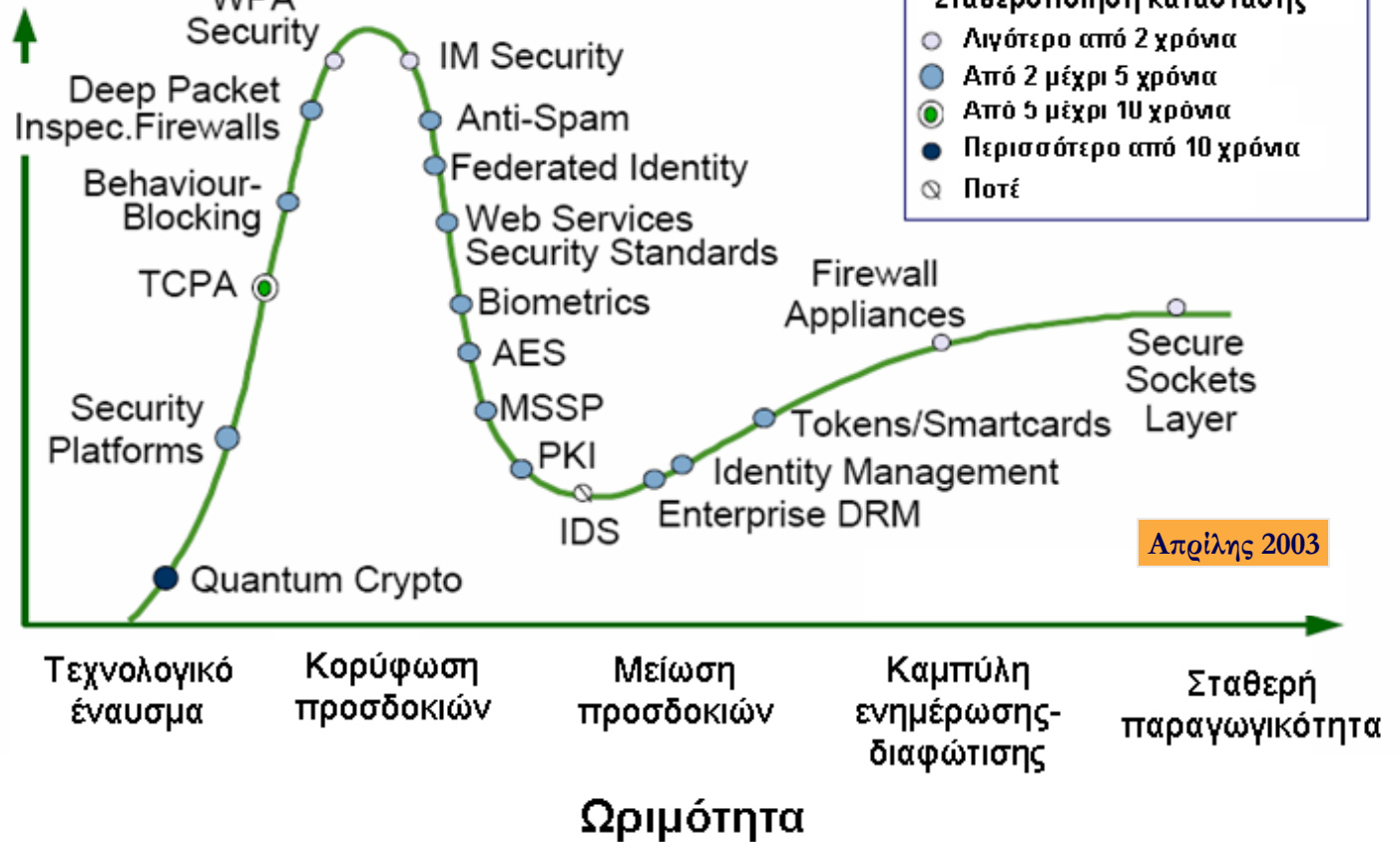
The candidate countries are full partners in FP5.

Other policies

Single Market, Single Currency, Security of Europeans, Sustainable Development, ...

Τέλη 20ου αιώνα: Οράματα της κοινοτικής νομοδότησης...

Ορατότητα



Τέλη 20ου αιώνα: Εξέλιξη Τεχνολογιών Ασφάλειας στις ΤΠ&Ε

Κατακερματισμένη αλυσίδα αξίας	Στοιχεία αξίας										
	Συσκευές «πάνω» στο άτομο 1	Ασφάλεια συσκευών τελικού χρήστη 2	Ασφάλεια επιπέδου μεταφοράς 3	Ασφάλεια εγκαταστάσεων 4	Διαχείριση Ασφάλειας 5	Φορείς Εμπιστοσύνης 6	Ασφάλεια Περιεχομένου 7	Διαχείριση συναλλαγών 8	Credit Assurance 9	Κοινοβουλευτικές Πολιτικές Ασφάλειας 10	
Υπηρεσίες		Παροχείς λύσεων, System Integrators						MSFDC			
Λογισμικό • Εφαρμογές • Εργαλεία • Δεικ. Συστήματα				Network Associates		Verisign		CyberCash			
				Microsoft				Cylink			
						Cylink, Frontier, BBN, HP, TIS					
Υλικό	Atally, Spyrus, Datakey										
	PC/SC Workgroup										
Πρότυπα			Cisco	ICSA			Internet Mail Consortium	OBI			
					W3CF, IEFT		Cylink	SET Workgroup			

Τέλη 20ου αιώνα: Επιχειρηματικό Οικοσύστημα Ασφάλειας

Ασφάλεια στις ΤΠ&Ε: Κύματα και μορφότυποι

- 60's** (Primitive Computing): **Security...?**
- 70's** (Mainframe Computing): **Needed-to-few security**
- 80's** (Personal Computing): **Added-on security**
- 90's** (Networked Computing): **Built-in security**
- 00's** (Ambient Intelligence?): **Security-to-start-with**



Ζούμε σε μια εποχή ειδικών κάθε τύπου, στους οποίους απευθυνόμαστε για κάθε επιμέρους πρόβλημα. Οι ειδικοί, όμως, είναι εντελώς αναρμόδιοι για όλα όσα είναι ξένα προς την επιστήμη τους και κατά κανόνα δεν ξέρουν να σκέφτονται με τρόπο διεπιστημονικό. Συνεπώς, δεν είναι σε θέση να αντιμετωπίσουν σφαιρικά προβλήματα.

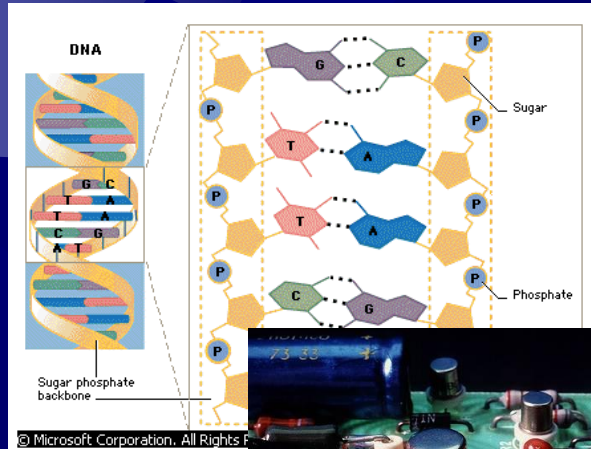
Ε. Μορέν, *La Repubblica*



Science Source/Photo Researchers, Inc.

Γέννηση:
A. Turing:
On computable numbers (1937)

ΤΠ&Ε: Από τη γέννηση ως τη μετάλλαξη τους



Μετάλλαξη:
Human Genome Project
(Ιούνιος 2000)



H. Schneebell/Science Source/Photo Researchers, Inc.

Μετάλλαξη:
World Trade Centre
(Σεπτέμβριος 2001)



ΤΠ&Ε και παγκοσμιοποιημένη οικονομία

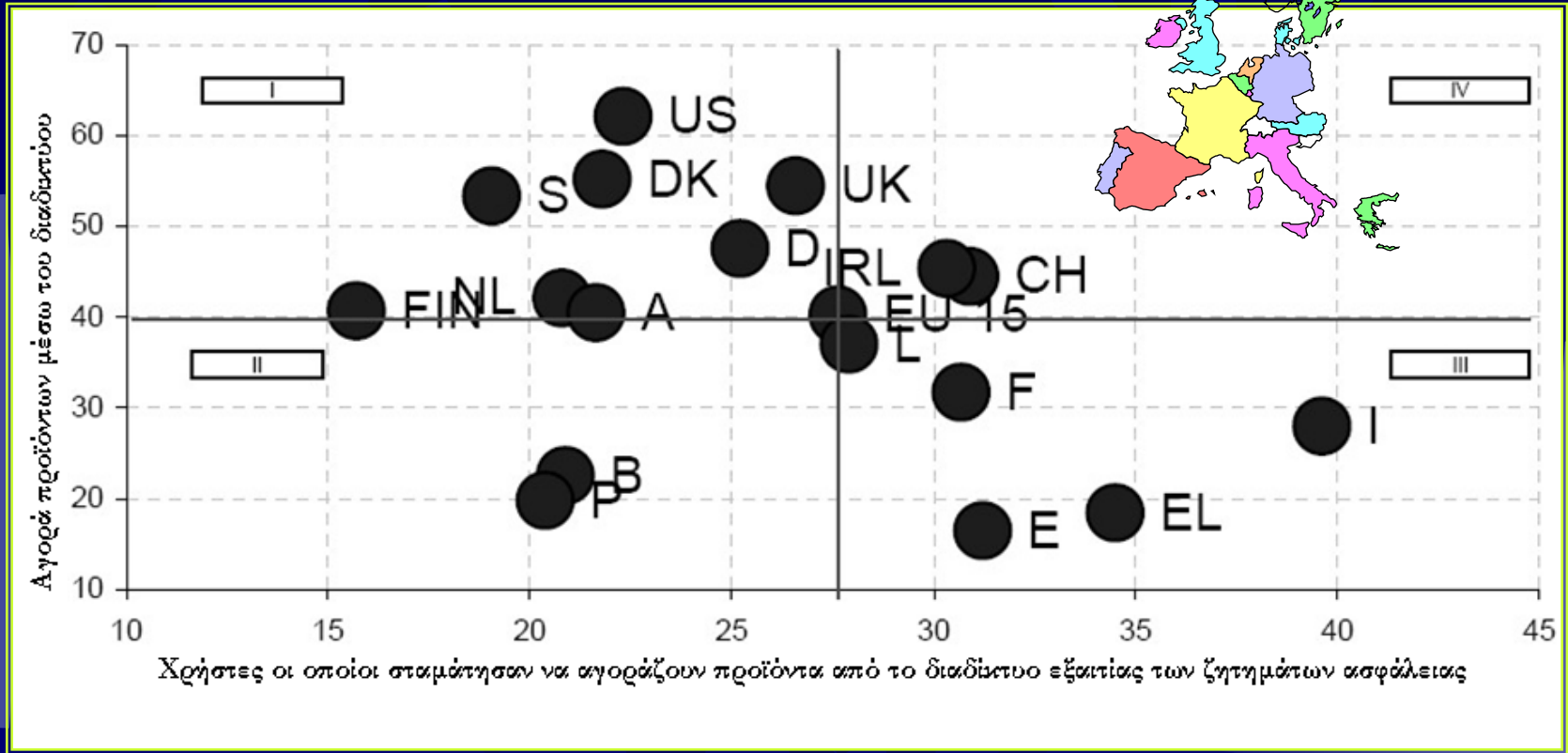


Ασφάλεια: Διαπλοκή και αλληλεπίδραση

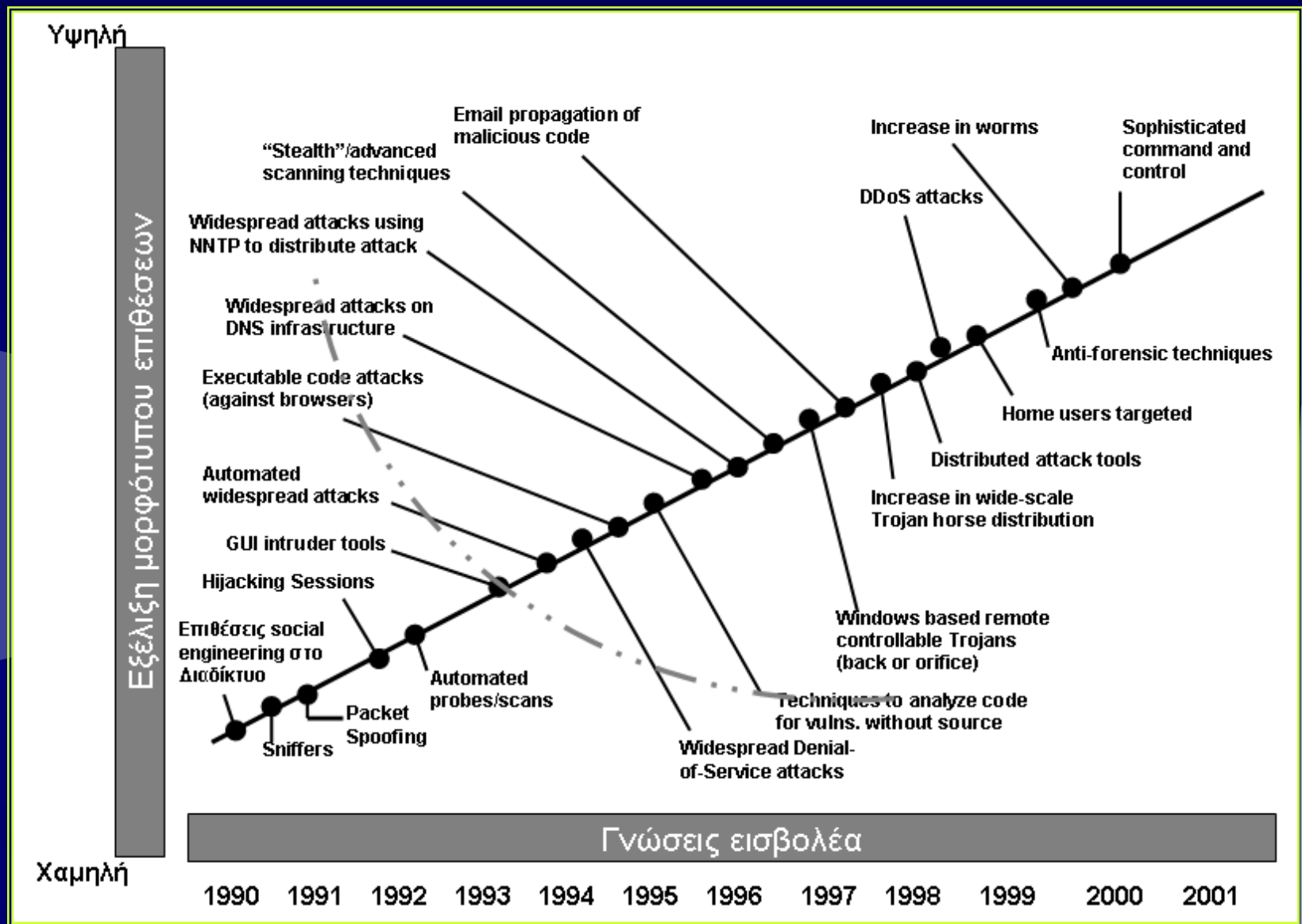


Σχετική Πυκνότητα Απειλών κατά τους επόμενους 12 μήνες	Μέση Τιμή				
	Χαμηλό		Μέση	Υψηλή	
	1	2	3	4	5
Ισομορφικό λογισμικό			●		
Ανάρμοστη συμπεριφορά εργαζομένων			●		
Κατανομημένες Επιθέσεις Μη Παροχής Υπηρεσιών			●		
Απώλεια πληροφοριών και δεδομένων που σχετίζονται με τους πελάτες μιας επιχείρησης			●		
Ερασιτέχνες hackers			●		
Κλοπή πληροφοριών			●		
Προμηθευτές – Σύμβουλοι με πρόσβαση στα Π.Σ. μιας επιχείρησης			●		
Ανάρμοστη συμπεριφορά όσο αφορά τα Π.Σ. πρώην εργαζομένων μιας επιχείρησης			●		
Φυσικές καταστροφές			●		
Ανάρμοστη συμπεριφορά από εταιρικούς συνεργάτες μιας επιχείρησης			●		
Επιθέσεις που οφείλονται στον ανταγωνισμό			●		
Δικτυακή διαμαρτυρία			●		
Κυβερνοτρομοκρατία προκαλούμενη από ξένες χώρες			●		
Κυβερνοτρομοκρατία προκαλούμενη από το εσωτερικό μιας χώρας			●		
Μη πυρηνική τρομοκρατική επίθεση			●		
Κυβερνοπόλεμος			●		
Κατασκοπεία μεταξύ κρατών			●		

Εκτίμηση έντασης απειλών κατά ΠΣ και κρίσιμων υποδομών (2004)



Ασφάλεια και καταναλωτισμός-in-context



Αρχές 21ου αιώνα: Ωρίμανση μορφώτων ιομορφικών προσβολών

Ο μορφότυπος του hacker...

50's: Εποχή του προγραμματισμού Η/Υ



Οι hackers είναι οι δεξιοτέχνες του προγραμματισμού. Διαθέτουν πλατειά περιθώρια αυτενέργειας και τεχνοκρατικής δημιουργίας. Το αποτέλεσμα της δουλειάς τους θεωρείται τέχνηργο και οι ίδιοι χαίρουν γενικής αποδοχής. Είναι προσόν να είσαι hacker, ακόμη και για τα λεξικά...

Ο μορφότυπος του hacker...

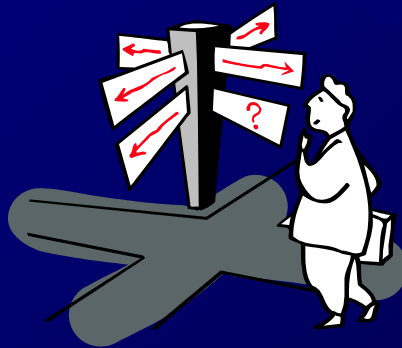
60's: Εποχή της επιστημονικής διοίκησης



Οι αρμοδιότητες μεταφέρονται από τους προγραμματιστές στην ενδιάμεση κλάση των γραφειοκρατών-διαχειριστών. Οι μεθοδολογίες και τα εμπειρικά πρότυπα τυποποιούνται. Οι hackers προσπαθούν να διατηρήσουν στο επίκεντρο την επιδεξιότητα, σε βάρος της τυποποίησης και της γραφειοκρατίας. Είναι ενοχλητικό για κάποιους γραφειοκράτες νάσαι hacker.

Ο μορφότυπος του hacker...

70's-80's: Εποχή του αντινομικού τεχνολογικού ριζοσπαστισμού



Η Πληροφορική ειλαμβάνεται από διανοούμενους ως μέσο για τη διάχυση της εξουσίας σε ευρύτερα κοινωνικά στρώματα. Άλλοι τη θεωρούν μέσο (παράνομου) πλουτισμού. Η παραδοσιακή εξουσία αμύνεται. Οι hackers δρουν ως αντινομιστές “τεχνοχίπις”, στηρίζοντας την πλατειά χρήση της Πληροφορικής, από όσο το δυνατόν περισσότερους πολίτες. Συγκρούονται με το Κράτος. Είναι παράνομο νάσαι hacker, γράφει το λεξικό!

Ο μορφότυπος του hacker...

90's: Εποχή της παγκοσμιοποίησης



Η διαδικτύωση συνδέει τους επαγγελματίες των ΤΠΕ (και όχι μόνον) όπου γής. Γεωγραφικά σύνορα καταλύονται. Πολιτικές διεκδικήσεις παγκοσμιοποιούνται και η πολιτική ανυπακοή διευρύνεται. Η δυνατότητα συνεργατικής δημιουργίας των δεξιοτεχνών δημιουργεί νέες προοπτικές, τόσο επιστημονικής, όσο και πολιτικής δράσης. Τώρα είναι trendy νάσαι hacker ή hacktivist...

Ο μορφότυπος του hacker...

00's: Εποχή της αβεβαιότητας



Μετά τις 11/9, η τρομοϋστερία και η τρομολαγνεία κυριαρχούν. Η διανόηση αφυπνίζεται αργά. Οι πολιτικές διεκδικήσεις περιορίζονται. Η πολιτική ανυπακοή εξοστρακίζεται. Οι hackers θεωρούνται υπό εγκύβλαψη “τρομοκρατές” ή “στρατοκράτες-εθνικιστές”. Είναι αμφίσημο νάσαι ειδικός σε θέματα ασφάλειας στις ΤΠΕ...

Διλήμματα που μας αφορούν...



Οι ειδικοί στην Ασφάλεια στις ΤΠ&Ε
καλούνται συχνά να ενεργήσουν
κινούμενοι:

ανάμεσα στον έπαινο και στο ανάθεμα,
ανάμεσα στη δημοσιότητα και στην ανωνυμία,
ανάμεσα στην αξιοπρέπεια και στον εξευτελισμό,
ανάμεσα στην ευαισθητοποίηση και στον ωχαδερφισμό,
ανάμεσα στον τεχνοκρατισμό και στην επιστήμη,
ανάμεσα στον ελιτισμό και στην περιθωριοποίηση,
ανάμεσα στη δημοκρατία και στον αυταρχισμό,
και συχνά:

ανάμεσα στη συνείδηση και στο νόμο.



Η μόνη υποχρέωση που έχω το δικαίωμα να εκπληρώνω είναι το να πράττω, ανά πάσα στιγμή, αυτό που θεωρώ σωστό.

H. Thoreau, *Αντίσταση στην πολιτική εξουσία*

The political criminal of today must needs be the hero, the martyr and the saint of the new age. No new faith has ever been considered within the law by those in power. Never can a new idea move within the law. Progress is ever renewing, ever becoming, ever changing, never is it within the law.

E. Goldman, *Απολογία*

Νομίζεις πως μια πόλη μπορεί να εξακολουθήσει να υπάρχει και να αποφύγει την ανατροπή, αν οι δικαστικές αποφάσεις της δεν έχουν ισχύ και μπορούν να αγνοηθούν από τους πολίτες;

Πλάτων, *Κρίτων*

Η βαθύτερη ανανέωση της κοινωνίας είναι η διαμόρφωση μιας νέου τύπου δημο-κρατικής διακυβέρνησης και η εγγύηση του δικαιώματος της ανυπακοής σε όποιον διαφωνεί με αυτό που συμβαίνει, όταν αυτό είναι εκτός της συμφωνίας όπου στηρίζεται η κοινή διαβίωση και επιβίωση των πολιτών.

N. Κοτζιάς, *Το δικαίωμα της ανυπακοής*

References

1. Denault M., Gritzalis D., Karagiannis D., Spirakis P., "Intrusion detection: Evaluation and performance issues of the SECURENET system", *Computers & Security*, Vol. 13, No. 6, pp. 495-508, October 1994.
2. Doulas A., Mavroudakos K., Gritzalis D., Katsikas S., "Design of a neural network for recognition and classification of computer viruses", *Computers & Security*, Vol. 14, No. 5, pp. 435-448, 1995.
3. Gritzalis D., *Secure Electronic Voting*, Springer, USA 2003.
4. Gritzalis D., "Principles and requirements for a secure e-voting system", *Computers & Security*, Vol. 21, No. 6, pp. 539-556, 2002.
5. Gritzalis D., "Embedding privacy in IT applications development", *Information Management and Computer Security*, Vol. 12, No. 1, pp. 8-26, 2004.
6. Gritzalis D., Theoharidou M., Kalimeri E., "Towards an interdisciplinary information security education model", in *Proc. of the 4th World Conference on Information Security Education*, 2005.
7. Gritzalis D., Katsikas S., "Towards a formal system to system authentication protocol", *Computer Communications*, Vol. 19, No. 8, pp. 954-961, 1996.
8. Lekkas D., Gritzalis D., Cumulative Notarization for Long-term Preservation of Digital Signatures, *Computers & Security*, Vol. 23, No. 5, pp. 413-424, 2004.
9. Spinellis D., Gritzalis D., "PANOPTIS: Intrusion detection using process accounting records", *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, 2002.
10. Spirakis P., Katsikas S., Gritzalis D., Allegre F., Darzentas J., Gigante C., Karagiannis D., Putkonen H., Spyrou T., "SECURENET: A Network-oriented intrusion prevention and detection intelligent system", in *Proc. of the 10th International Information Security Conference*, 1994.