



Future steps for securing Critical ICT Infrastructures

Dimitris Gritzalis

October 2007

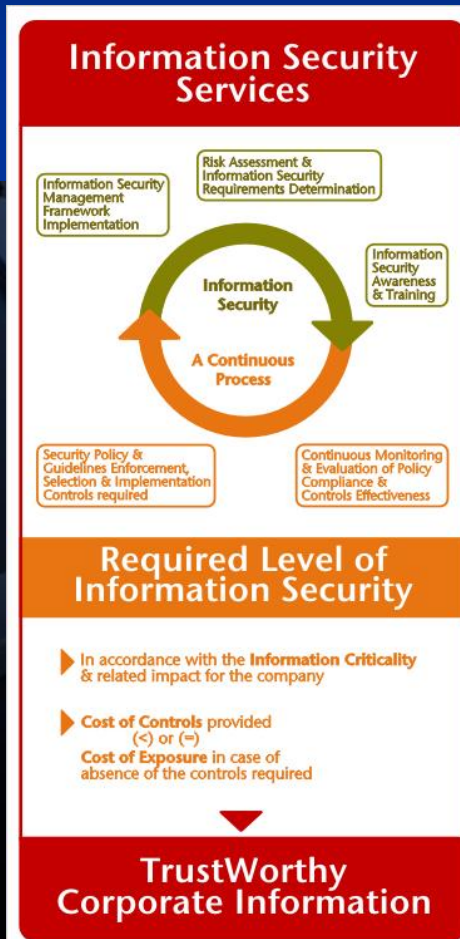
Από το πρόσφατο παρελθόν...
(Ασφάλεια Πληροφοριακών Συστημάτων)
...στο προσεχές μέλλον
(Προστασία Κρίσιμων Πληροφοριακών
Υποδομών)

Καθηγητής Δημήτρης Γκρίτζαλης (dgrit@aueb.gr, www.cis.aueb.gr)

Ερευνητική Ομάδα Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών



Ασφάλεια Πληροφοριακών Συστημάτων



- POLICY
- STRATEGY
- STANDARDS
- PROCEDURES
- GUIDELINES
- S/W FUNCTIONS



Νέοι όροι – νέες στοχεύσεις

■ ΥΠΟΔΟΜΗ:

Πλέγμα αλληλοεξαρτώμενων δικτύων και συστημάτων που παρέχει αξιόπιστη ροή προϊόντων, υπηρεσιών και αγαθών, για τη λειτουργία διοίκησης, οικονομίας, κοινωνίας και άλλων υποδομών.

■ ΚΡΙΣΙΜΗ ΥΠΟΔΟΜΗ:

Υποδομή μεγάλης κλίμακας, υποβάθμιση, διακοπή ή δυσλειτουργία της οποίας έχει σοβαρή επίπτωση στην υγεία, ασφάλεια ή ευμάρεια των πολιτών ή στην ομαλή λειτουργία διοίκησης ή οικονομίας.



Νέοι όροι – νέες στοχεύσεις

■ ΚΡΙΣΙΜΗ ΠΛΗΡΟΦΟΡΙΑΚΗ ΥΠΟΔΟΜΗ:

Πληροφοριακό Σύστημα υποστηριζόμενο από ΤΠΕ, που αποτελεί το ίδιο κρίσιμη υποδομή ή είναι προϋπόθεση για τη λειτουργία άλλων τέτοιων υποδομών.

■ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΗΣ ΠΛΗΡΟΦΟΡΙΑΚΗΣ ΥΠΟΔΟΜΗΣ:

Δράσεις των κατόχων, κατασκευαστών, χρηστών, διαχειριστών, ερευνητικών ιδρυμάτων, Διοίκησης και κανονιστικών αρχών, για τη διατήρηση της ποιοτικής λειτουργίας της υποδομής σε περίπτωση επιθέσεων, ατυχημάτων, σφαλμάτων, όσο και για την ταχεία ανάκαμψη της υποδομής μετά από τέτοιο γεγονός.



Κρίσιμες Υποδομές και ευπάθειες: Φαινόμενα συγκέντρωσης

- Συγκέντρωση **ενέργειας** (εγκαταστάσεις παραγωγής ηλεκτρισμού, φράγματα, εύφλεικτα υλικά, τοξικές ουσίες, ειρηνητικά κλπ.).
- Συγκέντρωση **πληθυσμού** (μεγα-πόλεις, μητροπόλεις, περιφερειακά κέντρα).
- Συγκέντρωση **εξουσίας** (οικονομικής και πολιτικής, ειδικά στις ΤΠΕ και στη βιομηχανία τροφίμων).

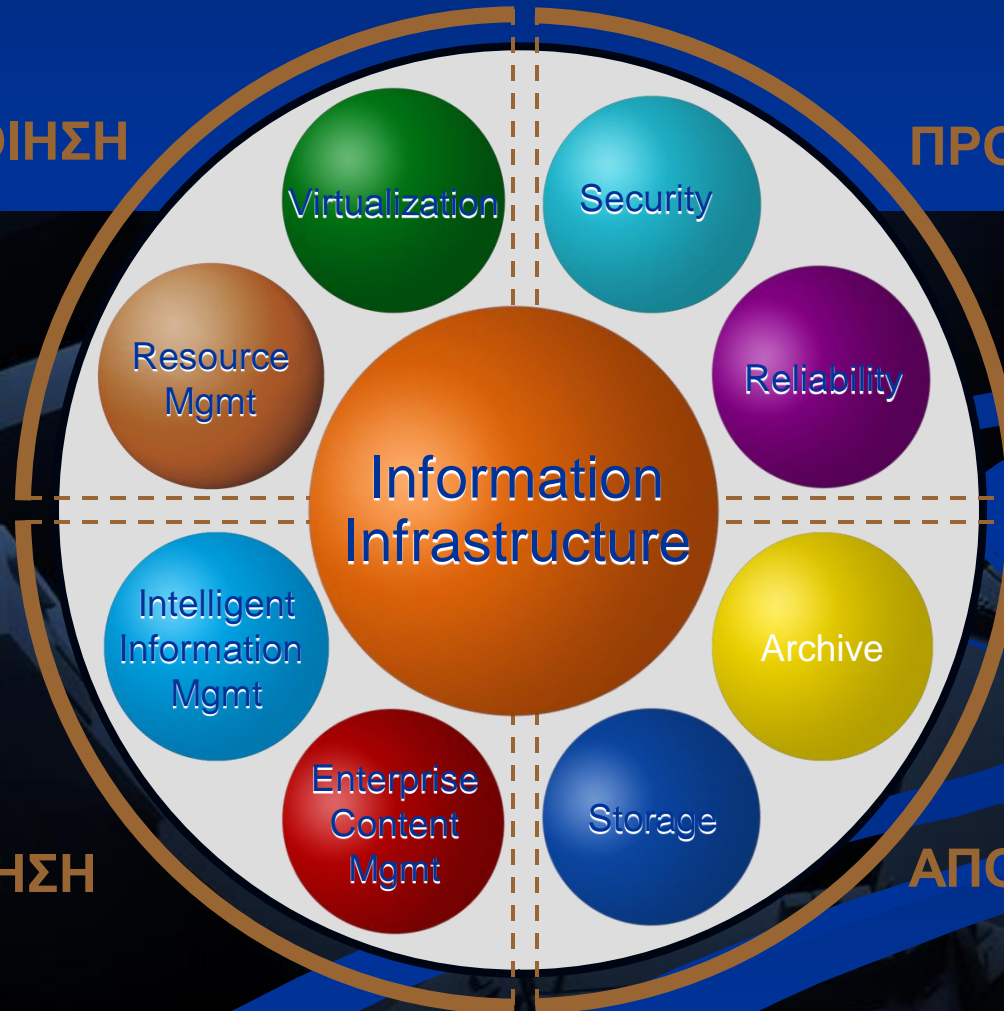
...οι συγκεντρώσεις οικονομικής και πολιτικής εξουσίας ευνοούν τη συγκέντρωση ενέργειας (συνήθως μέσω της απελευθέρωσης αγορών), η οποία τείνει να συμβαίνει σε περιοχές με πολύ μεγάλο πληθυσμό.



Μια νέα πληροφοριακή πλατφόρμα αναδύεται...

ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ

ΠΡΟΣΤΑΣΙΑ

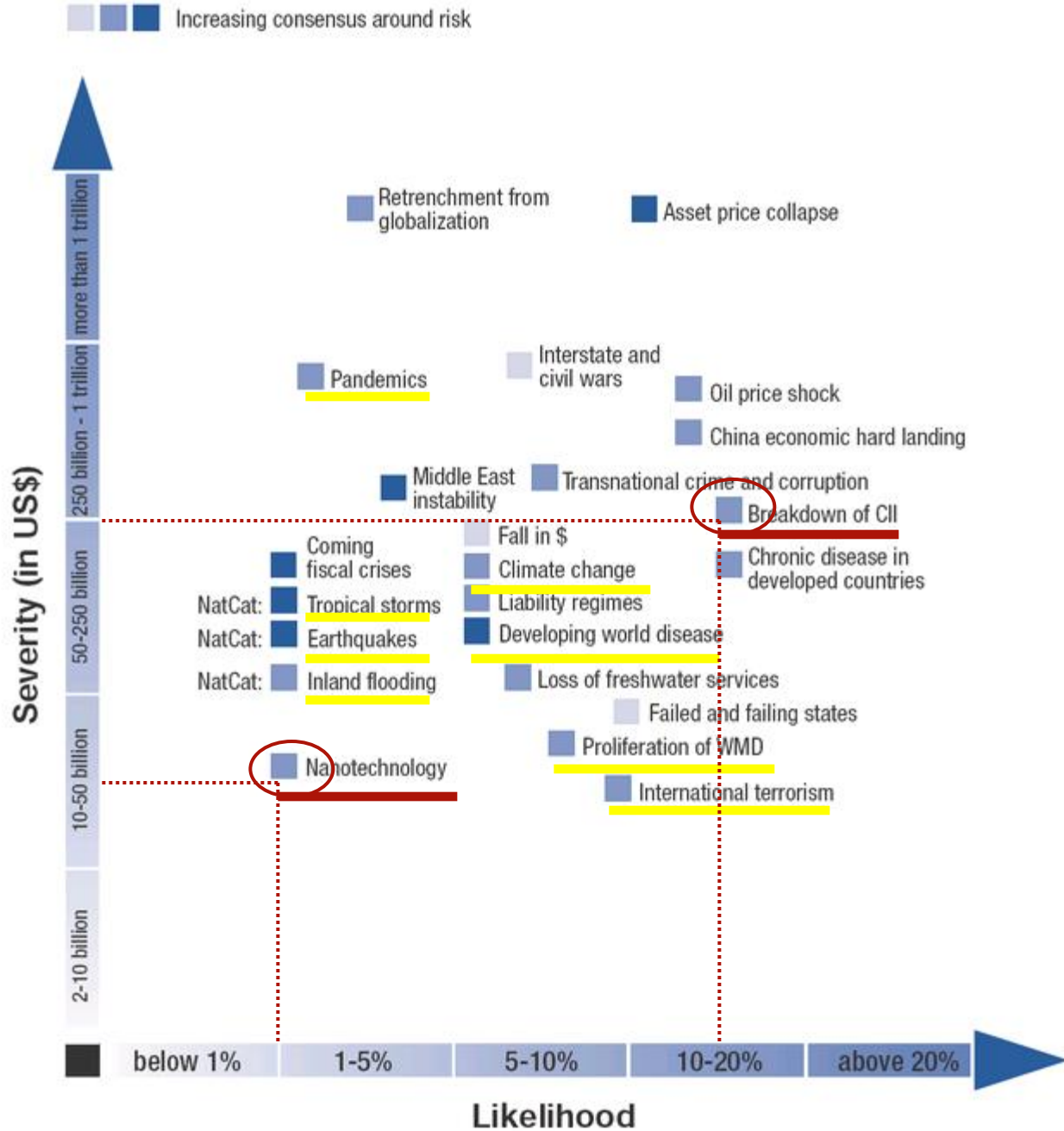


ΑΞΙΟΠΟΙΗΣΗ

ΑΠΟΘΗΚΕΥΣΗ



World Economic Forum (2008)
 Core Global Risks: Likelihood with Severity by Economic Loss



Κρίσιμες Υποδομές που κινδυνεύουν: Η περίπτωση των ΗΠΑ

■ Agriculture and Food

- 1.9M farms

- 87,000 food processing plants

■ Water

- 1,800 federal reservoirs

- 1,600 treatment plants

■ Public Health

- 5,800 registered hospitals

■ Chemical Industry

- 66,000 chemical plants

■ Telecomm

- 2B miles of cable

■ Energy

- 2,800 power plants

- 300K production sites

■ Transportation

- 120.000 miles railroads

- 590,000 highway bridges

- 2M miles of pipeline

- 250 ports

■ Banking and Finance

- 6,600 FDIC institutions

■ Postal and Shipping

- 300M delivery sites

■ Key Assets

- 5,800 historic buildings

- 104 nuclear power plants

- 80K dams

- 3,000 government facilities

- 460 skyscrapers

Το σύνολο των
Κρίσιμων Υποδομών
εξαρτάται από τη χρήση
Υποδομών ΤΠΕ



Νέα απειλή - νέες εξαρτήσεις



Οικονομικές διαστάσεις προστασίας Κρίσιμων Πληροφοριακών Υποδομών

Commercially Global
Telecommunications
Industry Revenue
(2005)

\$10¹² - Trillion

**Μέσο κόστος
ενός ICBM**

\$10⁹ - Billion

Satellite
Benefits (2002)

\$638M

~\$10-50M

12 year service
cost of a
\$100M Satellite

\$53M

\$10⁶ - Million

42 TV

\$2000

\$10³ - Thousand



Σύγκριση Κρισιμότητας Υποδομών

		Electricity	Gas	Railways	ICT	Urban Water	Satellite Systems	
Infrastructure characteristics	Complexity	Physical	Red	Green	Yellow	Red	Green	Red
		Organisational	Red	Green	Yellow	Red	Green	Red
		Speed of change	Yellow to Red	Green	Yellow	Yellow	Yellow	Yellow
	Dependence (interconnectedness)	On other infrastructures	Yellow	Green	Red	Red	Yellow	Red
		For other infrastructures	Red	Green	Yellow	Red	Yellow	Red
		Intra-infrastructure	Yellow	Green	Yellow	Yellow	Green	Red
		ICT control	Yellow to Red	Yellow	Red	Red	Yellow	Yellow
	Vulnerability	External impact*	Red	Red	Yellow	Green	Yellow	Red
		Technical/human failure	Yellow	Green	Yellow	Red	Green	Yellow
		Cyber attacks	Yellow	Yellow	Yellow	Red	Yellow	Yellow to Red
		Terrorist target	Red	Yellow	Red	Yellow	Red	Yellow to Red
	Market environment	Degree of liberalisation	Yellow to Red	Yellow to Red	Yellow	Green	Yellow	Yellow
		Adequacy of control	Red	Yellow	Yellow	Yellow	Green	Yellow
		Speed of change	Yellow	Green	Yellow	Yellow	Yellow	Red

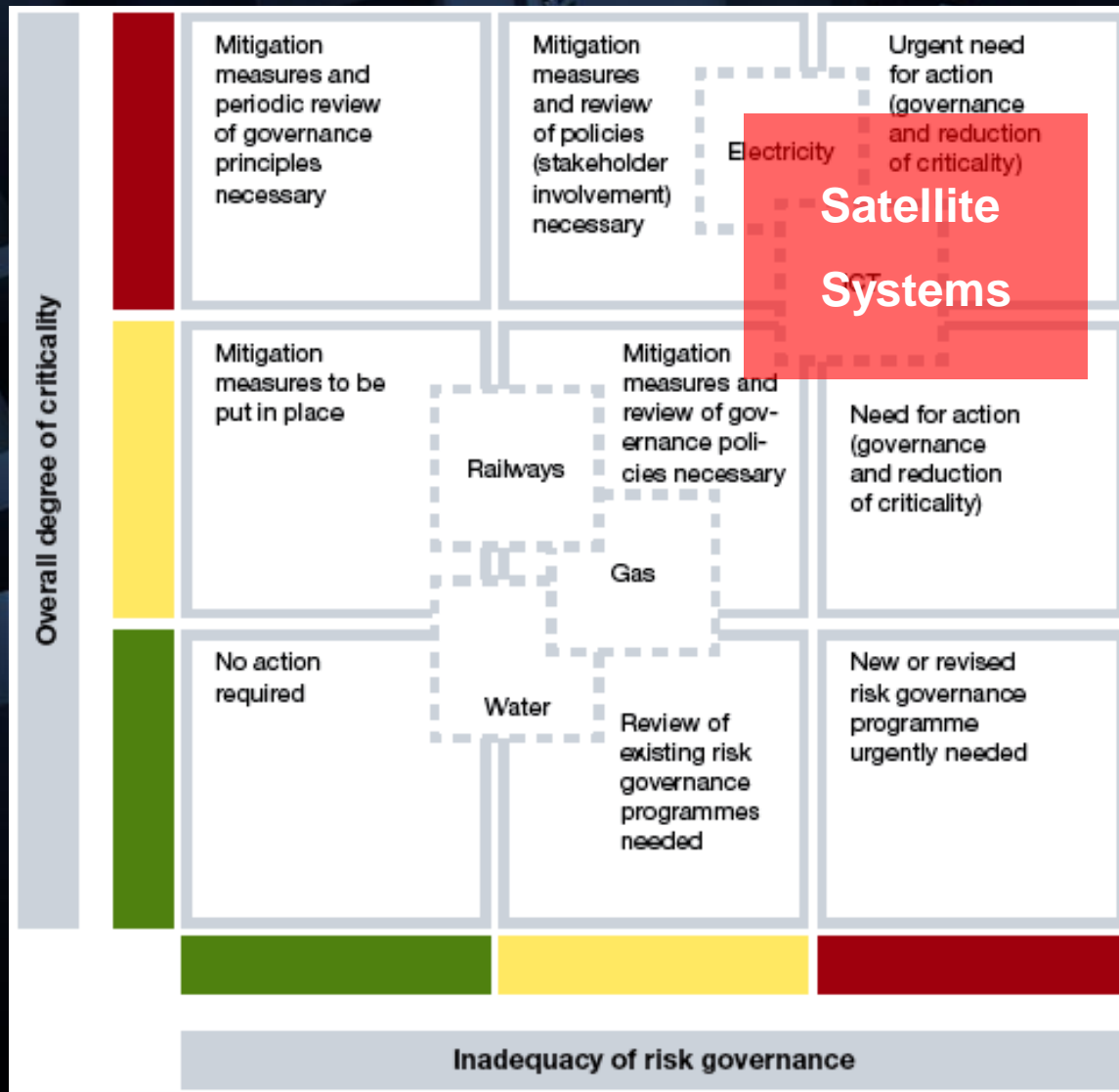
Colors are used to judge the performance level;

red corresponds to the worst, green to an adequate performance with regard to the considered criterion, transitions indicate changes.



Κρισιμότητα Υποδομής vs.

Αναταλληλότητα Διαχείρισης Επικινδυνότητας



Πρώτα συμπεράσματα

- Μεγάλο μέρος κρίσιμων υποδομών ανήκει στον ιδιωτικό τομέα, που - όπως και ο δημόσιος - είναι επιρρεπής σε σφάλματα, αστοχίες και συχνή αδυναμία ικανοποίησης των απαιτήσεων των πολιτών-πελατών.
- Οι πιθανές επιπτώσεις ατυχημάτων, σφαλμάτων και αστοχιών είναι διεθνείς και γεωγραφικά ειτενεείς.
- Το πλήθος των κρίσιμων υποδομών αυξάνεται και η αλληλεξάρτησή τους, καθώς και η εξάρτηση άλλων από αυτές διευρύνεται.
- Οι υποδομές ΤΠΕ τείνουν, ταχύτατα και διεθνώς, να καταστούν υποδομές-υποδομών.
- Η επιδίωξη για ανάπτυξη ασφαλών ολοκληρωμένων πληροφοριακών συστημάτων δίνει τη θέση της στην ανάπτυξη ασφαλών πληροφοριακών υποδομών.
- Μια νέα επιστημονική περιοχή πιθανώς αναδύεται: **Critical Infrastructures Management and Engineering**



References

1. Gritzalis D., *Secure Electronic Voting*, Springer, USA 2003.
2. Gritzalis D., "Embedding privacy in IT applications development", *Information Management and Computer Security*, Vol. 12, No. 1, pp. 8-26, 2004.
3. Gritzalis D., "Principles and requirements for a secure e-voting system", *Computers & Security*, Vol. 21, No. 6, pp. 539-556, 2002.
4. Lekkas D., Gritzalis D., Cumulative Notarization for Long-term Preservation of Digital Signatures, *Computers & Security*, Vol. 23, No. 5, pp. 413-424, 2004.
5. Lekkas D., Gritzalis D., "e-Passports as a means towards the first world-wide Public Key Infrastructure", in *Proc. of the 4th European PKI Workshop*, pp. 34-48, Springer, 2007.
6. Gritzalis D., Katsikas S., Keklikoglou J., Tomaras A., "Data security in medical information systems: The Greek case", *Computers & Security*, Vol. 10, No. 2, pp. 141-159, April 1991.
7. Spinellis D., Gritzalis D., "A domain-specific language for intrusion detection", in *Proc. of the 1st ACM Workshop on Intrusion Detection and Prevention Systems (WIDS -2000)*, Greece, 2000.
8. Tsoumas V., Papagiannakopoulos P., Dritsas S., Gritzalis D., "Security-by-Ontology: A knowledge-centric approach", in *Proc. of the 21st International Information Security Conference*, pp. 99-110, 2006.
9. Theoharidou M., Stougiannou E., Gritzalis D., "A CBK for Information Security and Critical Infrastructure Protection", in *Proc. of the 5th IFIP Conference on Information Security Education*, pp. 49-56, Springer, 2007.
10. Theoharidou M., Xidara D., Gritzalis D., "A Common Body of Knowledge for Information Security and Critical Information and Communication Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, Vol. 1, No. 1, pp. 81-96, 2008.

