

A collection of items including a chessboard, medals, a compass, and glasses. The chessboard is in the top left corner, featuring a blue and brown checkered pattern with several pieces. Below it are two medals: one with a red ribbon and a white star, and another with a blue ribbon and a white star. A compass is in the bottom left corner, and a pair of glasses is in the bottom center. The background is a light-colored, textured surface.

# **Organizing the Protection of Critical ICT Infrastructures**

---

**Dimitris Gritzalis**

June 2003

A collection of medals and a compass on a wooden surface. The medals include a red ribbon with a circular emblem, a blue ribbon with a circular emblem, and a silver star-shaped medal with a central emblem. A pair of glasses is also visible. A compass is in the bottom left corner.

Ημερίδα  
Ασφάλεια Δικτύων και Πληροφοριών  
Υπουργείο Μεταφορών & Επικοινωνιών, Ιούνιος 2003

# Οργάνωση της Προστασίας των Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών

---

**Δημήτρης Α. Γκρίτζαλης**

Αναπληρωτής Καθηγητής Ασφάλειας στις ΤΠΕ

Τμήμα Πληροφορικής

Οικονομικό Πανεπιστήμιο Αθηνών

# Κοινωνία της Πληροφορίας και Παγκοσμιοποιημένη Οικονομία



# Κρίσιμες Υποδομές

Οι κρίσιμες υποδομές αναφέρονται και αφορούν στους οργανισμούς, τα δίκτυα πληροφοριών και επικοινωνιών και τα δίκτυα διανομής, τα οποία διασφαλίζουν τη διαρκή διανομή των αγαθών και των υπηρεσιών που είναι απαραίτητες για την εθνική άμυνα και οικονομία, τη δημόσια υγεία και ευμάρεια και την ασφάλεια των πολιτών.

Περιλαμβάνουν: Δημόσιο και Ιδιωτικό τομέα.

Περιλαμβάνουν συστήματα των τομέων: Γεωργία, Διατροφή, Υδρευση, Δημόσια Υγεία, Επείγουσες Υπηρεσίες, Δημόσια Διοίκηση, Εθνική Άμυνα, Πληροφορική, Ενέργεια, Μεταφορές, Επικοινωνίες, Χρηματοοικονομικά, Χημική Βιομηχανία, Ταχυδρομεία.

Κοινό πεδίο αναφοράς: Κυβερνοχώρος.

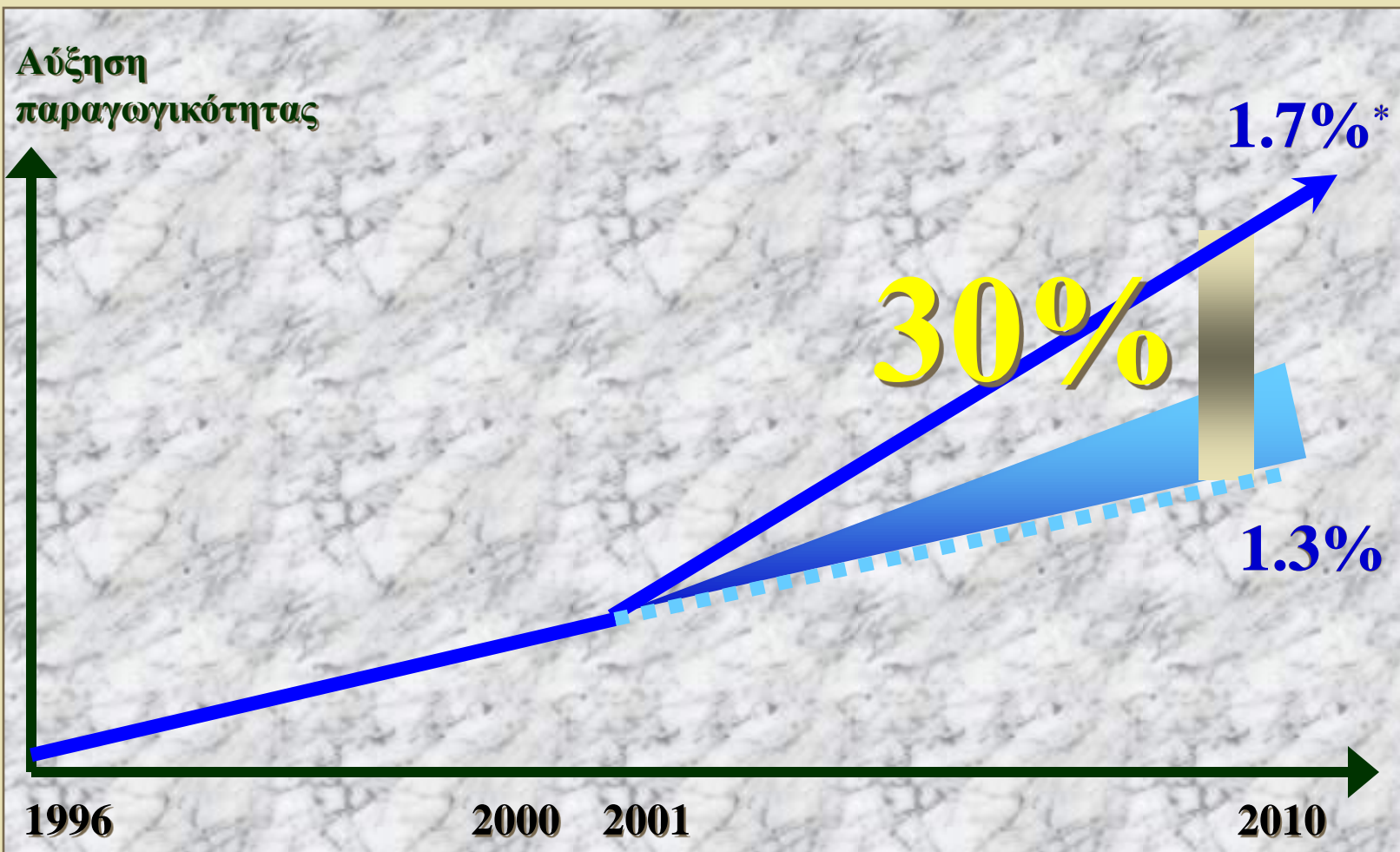


# Βασικές διαπιστώσεις

- ✓ Η προστασία των κρίσιμων υποδομών είναι αναγκαία για την εθνική ασφάλεια
- ✓ Οι κρίσιμες υποδομές εξαρτώνται από τις ΤΠΕ
- ✓ Αρκετές κρίσιμες υποδομές αλληλεξαρτώνται
- ✓ Μερικές κρίσιμες υποδομές ανήκουν στον ιδιωτικό τομέα
- ✓ Η προστασία κρίσιμων υποδομών προϋποθέτει συνεργασία δημόσιου-ιδιωτικού τομέα



# Web-enabled εφαρμογές και βελτίωση της ανταγωνιστικότητας στην ΕΕ



\* Εκτιμήσεις του ΟΟΣΑ (1992-2001)



# Βασικοί στόχοι προστασίας Π&Ε Υποδομών

Κυβερνο-επιθέσεις

- ◆ Προληπτική προστασία των κρίσιμων υποδομών
- ◆ Περιορισμός των ευπαθειών των κρίσιμων υποδομών
- ◆ Περιορισμός των συνεπειών από επιθέσεις

Π&Ε Υποδομές

Κοινωνία της Πληροφορίας



# Διαπλοκή και αλληλεπίδραση

“Tears without action are irrelevant”  
B. Williams, Nobel Ειρήνης

“Αφήστε όλα τα λουλούδια ν' ανθίσουν”  
Mao Zedong

Εθνική  
Ασφάλεια

Οργάνωση και  
διαχείριση

Προστασία  
Κρίσιμων  
Υποδομών

Επιχειρηματική  
συνδρομή

Κομβικές  
Υποδομές

Κουλτούρα



# Δράσεις και προτεραιότητες\*

- 1 Εθνικό **σύστημα αντίδρασης** στις κυβερνοεπιθέσεις.
- 2 Πρόγραμμα **μείωσης απειλών και ευπαθειών** των κρίσιμων Π&Ε υποδομών.
- 3 **Ενημέρωση και εκπαίδευση** στην αντιμετώπιση κυβερνοεπιθέσεων.
- 4 Ασφάλεια **κυβερνητικού πυρήνα** του κυβερνοχώρου.
- 5 **Συντονισμός** εθνικής ασφάλειας και ασφάλειας κυβερνοχώρου.

\* U.S. White House, *The National Strategy to Secure Cyberspace*, February 2003.



# ① Εθνικό σύστημα αντίδρασης στις κυβερνοεπιθέσεις

- ✓ Τακτική και στρατηγική ανάλυση κυβερνοεπιθέσεων
- ✓ Εθνική διαχείριση περιστατικών ανασφάλειας
- ✓ Ανάπτυξη σχεδίων ανάκαμψης από καταστροφή και συνέχισης της λειτουργίας των Π&Ε υποδομών
- ✓ Ασκήσεις συνέχισης της λειτουργίας των Π&Ε υποδομών μετά από κυβερνο-επιθέσεις
- ✓ Συντονισμός δημόσιου και ιδιωτικού τομέα
- ✓ Διάχυση πληροφόρησης μεταξύ δημόσιου-ιδιωτικού τομέα



## ② Πρόγραμμα περιορισμού των απειλών και ευπαθειών των εθνικών Π&Ε υποδομών

---

- ✓ **Θεσμικό πλαίσιο** για την πρόληψη και την καταστολή του κυβερνοεγκλήματος
- ✓ **Αποτίμηση επικινδυνότητας** εθνικών Π&Ε υποδομών
- ✓ Ανάπτυξη προηγμένων **τεχνικών ασφάλειας** στο Διαδίκτυο
- ✓ **Ανάπτυξη ασφαλών** Πληροφοριακών Συστημάτων και εφαρμογών λογισμικού
- ✓ **Χρηματοδότηση της E&TA** στην Ασφάλεια στις ΤΠΕ
- ✓ **Φυσική προστασία** εθνικών Π&Ε υποδομών



### ③ Πρόγραμμα ενημέρωσης και εκπαίδευσης στην αντιμετώπιση κυβερνο-επιθέσεων

---

- ✓ Ανάπτυξη εθνικού προγράμματος ενημέρωσης και ευαισθητοποίησης σε θέματα Ασφάλειας στις ΤΠΕ
- ✓ Ανάπτυξη προγραμμάτων εκπαίδευσης και εξειδίκευσης στην Ασφάλεια στις ΤΠΕ
- ✓ Ενδυνάμωση των υπαρχόντων προγραμμάτων εκπαίδευσης στην Ασφάλεια στις ΤΠΕ
- ✓ Προώθηση πιστοποίησης επαγγελματικής κατάρτισης στην Ασφάλεια στις ΤΠΕ



## ④ Ασφάλεια κυβερνητικού πυρήνα του Κυβερνοχώρου

- ✓ Διαρκής αποτίμηση επικινδυνότητας κυβερνητικών Π&Ε υποδομών
- ✓ Βελτίωση διαδικασιών αυθεντικοποίησης και εξουσιοδότησης χρηστών κυβερνητικών Π&Ε υποδομών
- ✓ Προστασία των ασύρματων κυβερνητικών τοπικών επικοινωνιακών δικτύων
- ✓ Βελτίωση ασφάλειας στις διαδικασίες υπεργολαβιών, outsourcing και προσλήψεων
- ✓ Υποστήριξη πρωτοβουλιών ανταλλαγής πληροφοριών και εμπειριών

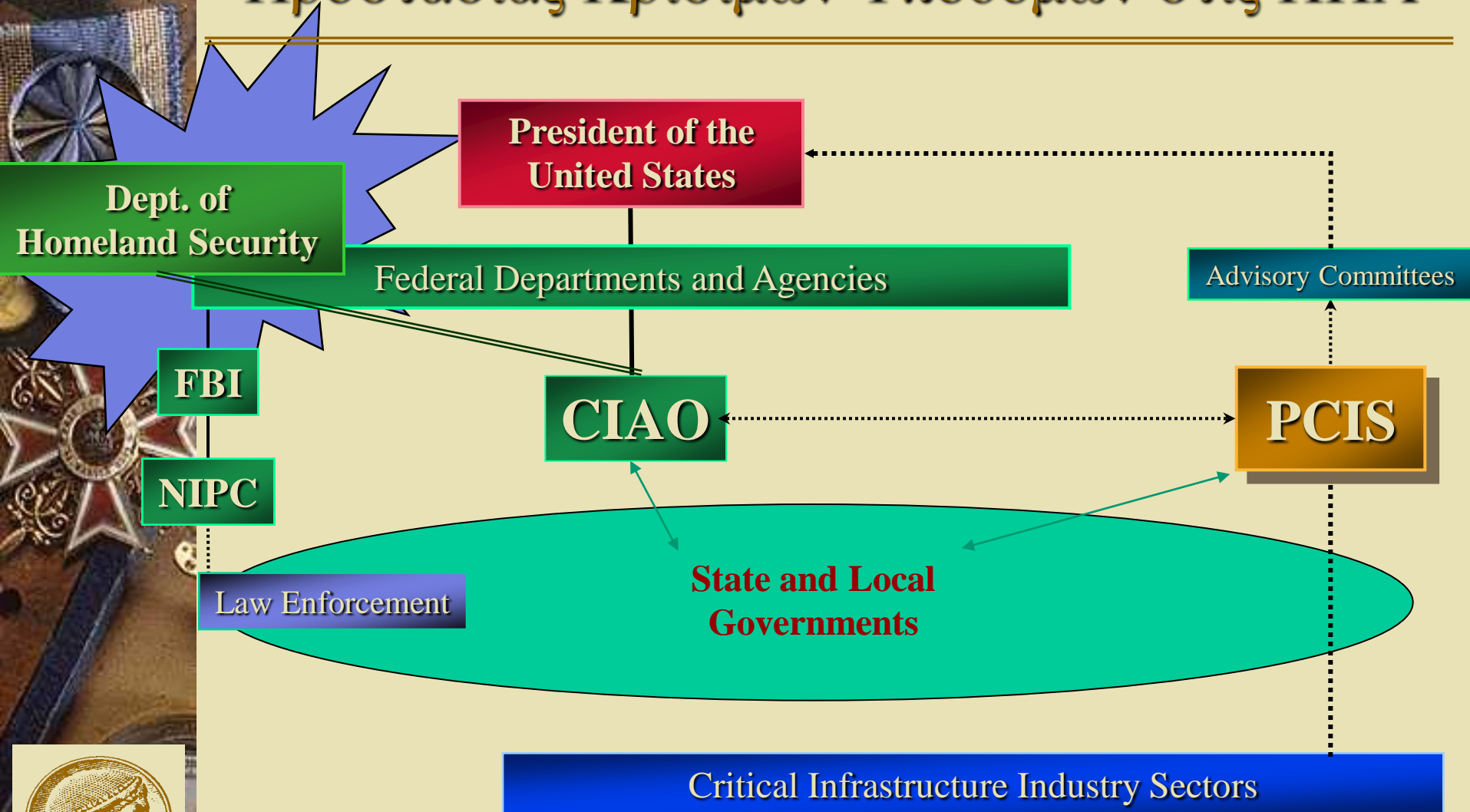


## 5 Συντονισμός Εθνικής Ασφάλειας και Ασφάλειας Κυβερνοχώρου

- ✓ Βελτίωση αποτελεσματικής αντίδρασης σε κυβερνοεπιθέσεις
- ✓ Συντονισμός δράσης αρμόδιων υπηρεσιών
- ✓ Συμμετοχή σε σχετικούς οργανισμούς και fora
- ✓ Προώθηση “κουλτούρας ασφάλειας”
- ✓ Ανάπτυξη δικτύων εποπτείας-προειδοποίησης για κυβερνοεπιθέσεις
- ✓ Προώθηση διακρατικής συνεργασίας



# Οργανωτικές πρωτοβουλίες Προστασίας Κρίσιμων Υποδομών στις ΗΠΑ



# Πρωτοβουλίες και δράσεις στην Ελλάδα

- ✓ Μεμονωμένα έργα (1997+)
- ✓ Εκπαιδευτικές πρωτοβουλίες (ΑΕΙ)
- ✓ Συμμετοχή σε σημαντικά διεθνή έργα Ε&ΤΑ
- ✓ Συνδρομή Ε.Π. “Κοινωνία της Πληροφορίας”
  
- ☹ Ελλειψη εθνικού σχεδιασμού
- ☹ Αποσπασματικότητα και έλλειψη συνεργειών
- ☹ Εσωστρέφεια ιδιωτικού τομέα
- ☹ Αμελητέες χρηματορροές για Ε&ΤΑ
  
- ? ΟΑ 2004: Υποδομές και δράσεις ασφάλειας



# Επίμετρο

- ◆ Η προστασία των κρίσιμων υποδομών είναι ...**κρίσιμη!**
- ◆ Οι αναγκαίες τεχνολογίες είναι **διαθέσιμες** σε αρκετό βαθμό.
- ◆ Οι φορείς της εκπαίδευσης, έρευνας και ανάπτυξης είναι ανοικτοί σε **συνεργασίες**.
- ◆ Οι στρατηγικοί στόχοι και προτεραιότητες είναι **σαφείς**

## Αλλά:

- ◆ Η αναγκαία οργανωτική υποδομή **απουσιάζει**.
- ◆ Η γόνιμη πολιτική βούληση **αναζητείται/αναμένεται...**





## 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, 1994.
2. Doulas A., Mavroudakis 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., "A baseline security policy for distributed healthcare information systems", *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
6. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
7. Iliadis J., Gritzalis D., Spinellis D., Preneel B., Katsikas S., "Evaluating certificate status information mechanisms", in *Proc. of the 7<sup>th</sup> ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, October 2000.
8. Katsikas S., Spyrou T., Gritzalis D., Darzentas J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
9. Lambrinouidakis C., Gritzalis D., Katsikas S., "Building a reliable e-voting system: Functional requirements and legal constraints", in *Proc. of the 13<sup>th</sup> International Workshop on Database & Expert Systems Applications*, pp. 435-446, 2002.
10. Spinellis D., Gritzalis D., " PANOPTIS: Intrusion detection using process accounting records", *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, 2002.