

A collection of military 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 two silver Maltese crosses with central emblems. A pair of gold-rimmed glasses is also visible. A circular compass is in the bottom left corner.

# Protecting Critical ICT Infrastructures

**Dimitris Gritzalis**

May 2003

1ο Πανελλήνιο Συνέδριο  
Προστασία της Κρίσιμης Υποδομής της χώρας  
ΕΚΕΦΕ Δημόκριτος, Μάης 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 two silver Maltese crosses with central emblems. A pair of gold-rimmed glasses lies across the scene. In the bottom left corner, a circular compass is visible. The background is a light-colored, textured surface.

# Ασφάλεια Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών

Υπεροψία. Αλλαζονεία. Τραγωδία. Μετά;

**Δημήτρης Γκρίτζαλης**  
Επ. Καθηγητής Ασφάλειας στις ΤΠΕ  
Τμήμα Πληροφορικής  
Οικονομικό Πανεπιστήμιο Αθηνών

# Κοινωνία της Πληροφορίας και Παγκοσμιοποιημένη Οικονομία



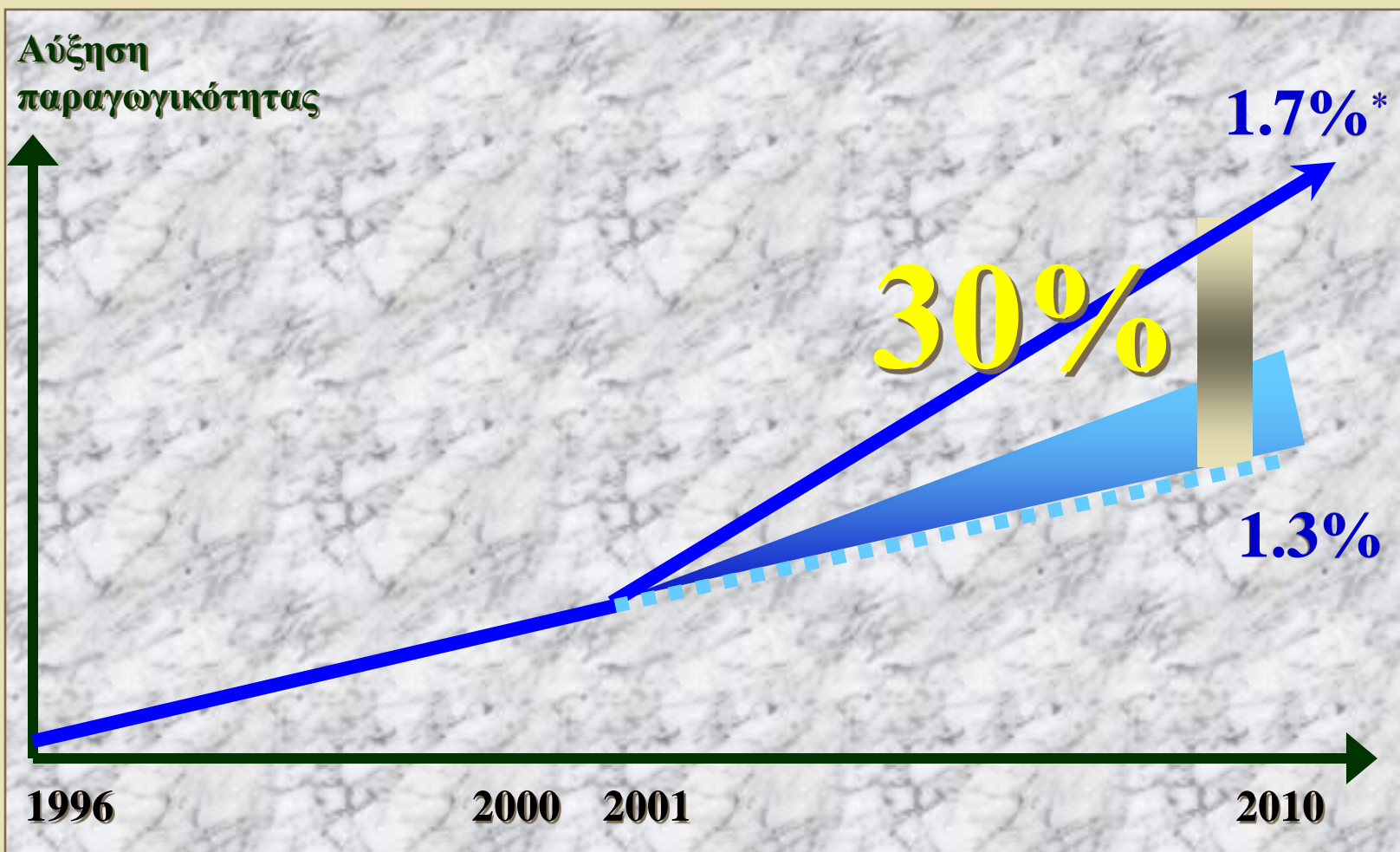


## Υποδομές - ΤΠΕ - Ασφάλεια

---

- ✓ Η προστασία των υποδομών είναι απαραίτητη για την εθνική ασφάλεια
- ✓ Οι υποδομές εξαρτώνται από τις ΤΠΕ
- ✓ Πολλές υποδομές εξαρτώνται η μία από την άλλη
- ✓ Ορισμένες κρίσιμες υποδομές ελέγχονται από τον ιδιωτικό τομέα
- ✓ Η προστασία κρίσιμων υποδομών προϋποθέτει συνεργασία δημόσιου-ιδιωτικού τομέα

# Αξιοποίηση δικτυο-εφαρμογών και βελτίωση της ανταγωνιστικότητας στην ΕΕ



\* Εκτιμήσεις του ΟΟΣΑ (1992-2001)

# Στόχοι προστασίας Π&Ε Υποδομών

Κυβερνο-επιθέσεις

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

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

Ασφάλεια  
Κρίσιμων  
Υποδομών

Επιχειρηματική  
Συνδρομή

Υποδομές  
Κλειδιά


Ιστορία και  
Πολιτισμός



## Δράσεις - Προτεραιότητες\*

- 1 Εθνικό **σύστημα αντίδρασης** στις κυβερνο-επιθέσεις.
- 2 Πρόγραμμα **περιορισμού των απειλών και ευπαθειών** των εθνικών Π&Ε υποδομών.
- 3 Πρόγραμμα **ενημέρωσης και εκπαίδευσης** στην αντιμετώπιση κυβερνο-επιθέσεων.
- 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 κυβερνο-επιθέσεις

---

- ✓ Τακτική και στρατηγική ανάλυση κυβερνο-επιθέσεων
- ✓ Εθνική διαχείριση περιστατικών ανασφάλειας
- ✓ Ανάπτυξη σχεδίων ανάκαμψης από καταστροφή και συνέχισης της λειτουργίας των Π&Ε υποδομών
- ✓ Ασκήσεις σχεδίων συνέχισης της λειτουργίας των δημόσιων 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 κυβερνο-εγκλήματος
- ✓ **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
- ✓ Ενθάρρυνση της χρήσης μεθόδων **ψηφιακού ελέγχου και εποπτείας**



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

---

- ✓ Ανάπτυξη εθνικού προγράμματος **ενημέρωσης και ευαισθητοποίησης** σε θέματα Ασφάλειας στις ΤΠΕ
- ✓ Υποστήριξη ανάπτυξης **προγραμμάτων εκπαίδευσης και εξειδίκευσης** στην Ασφάλεια στις ΤΠΕ
- ✓ Αύξηση της **αποτελεσματικότητας** των υπαρχόντων προγραμμάτων εκπαίδευσης στην Ασφάλεια στις ΤΠΕ
- ✓ Προώθηση διαδικασιών **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
- ✓ Ενθάρρυνση σχετικών πρωτοβουλιών σε τοπικό επίπεδο, ειδικά για ανταλλαγή πληροφοριών και εμπειριών

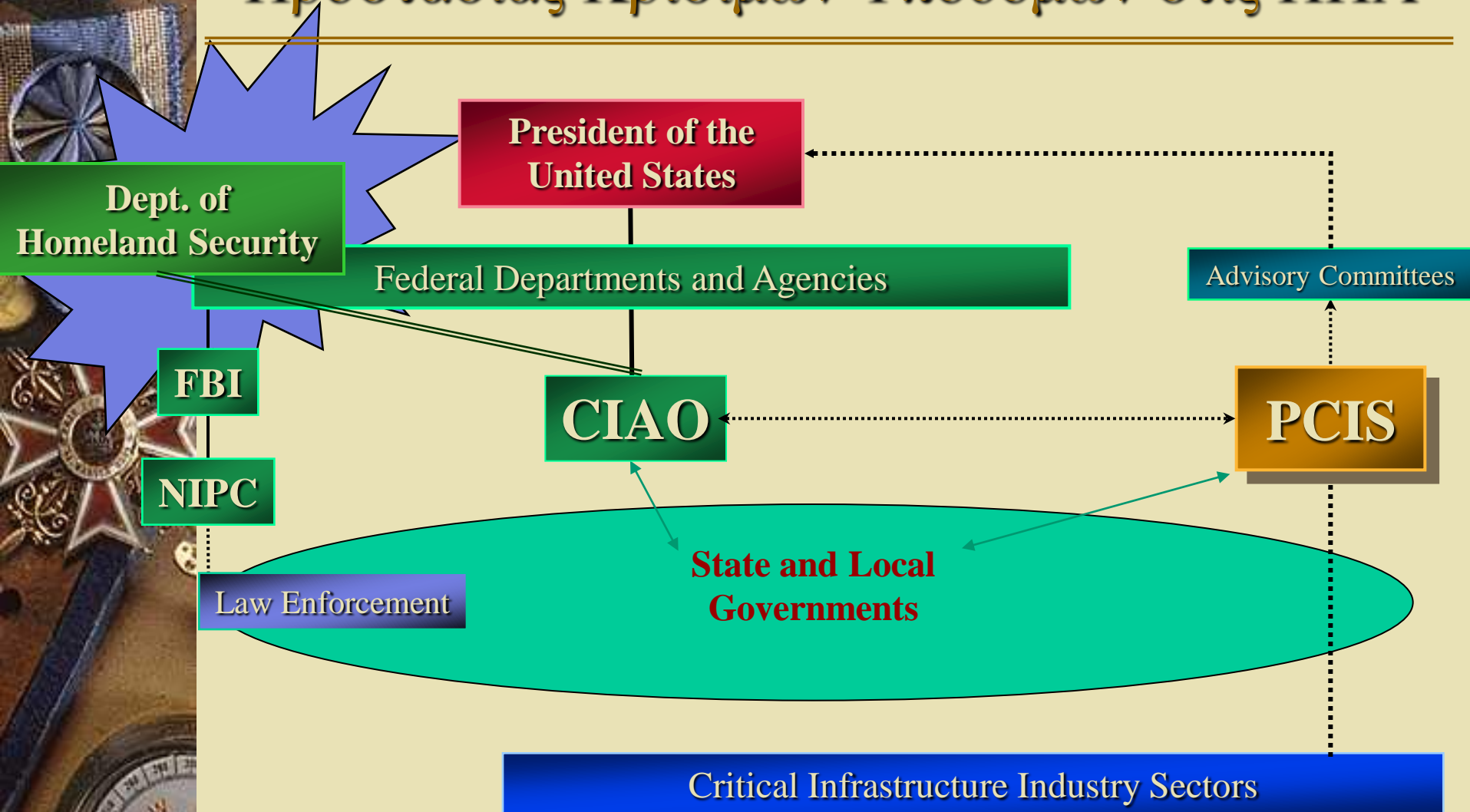


## 5 Συντονισμός Εθνικής Ασφάλειας και Ασφάλειας Κυβερνοχώρου

---

- ✓ Βελτίωση δυνατοτήτων **αποτελεσματικής αντίδρασης** σε κυβερνο-επιθέσεις
- ✓ **Συντονισμός** της δράσης των αρμόδιων υπηρεσιών
- ✓ Συμμετοχή σε διεθνείς οργανισμούς και fora για την προώθηση μιας “**κουλτούρας ασφάλειας**”
- ✓ Ανάπτυξη εθνικών και διεθνών **δικτύων εποπτείας και προειδοποίησης** κυβερνο-επιθέσεων
- ✓ Προώθηση **διακρατικής συνεργασίας** στα σχετικά ζητήματα

# Υπό εξέλιξη οργανωτικές πρωτοβουλίες Προστασίας Κρίσιμων Υποδομών στις ΗΠΑ









# Partnership for Critical Infrastructure (PCIS)





# Κομβικά πεδία Ε&ΤΑ: INFOSEC & Προστασία Κρίσιμων Υποδομών

---

-  Inter-Enterprise Security
-  Adaptive Anomaly-based Security Monitoring
-  Audit Records-Logs Analysis
-  Information System Reconstitution
-  Distributed Information System Security for Information Sharing
-  Interdependence Analysis

# Σχετικές πρωτοβουλίες στην Ελλάδα

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



## 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. Doumas 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. Gritzalis D., "A digital seal solution for deploying trust on commercial transactions", *Information Management & Computer Security*, Vol. 9, No. 2, pp. 71-79, 2001.
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. Spinellis D., Gritzalis D., "A domain-specific language for intrusion detection", in Proc. of the *1<sup>st</sup> ACM Workshop on Intrusion Detection and Prevention Systems (WIDS -2000)*, November 2000.