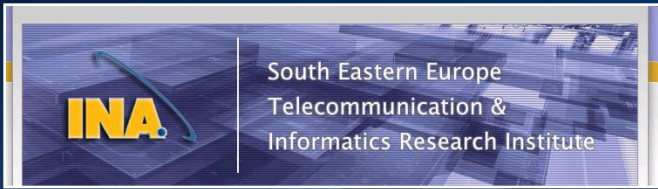




**Critical ICT Infrastructure
Protection in Public
Administration: The case of Greece**

Dimitris Gritzalis, Ioanna Sambrakou

November 2008



4th Regional Electronic Security Forum
Θεσσαλονίκη, Νοέμβρης 2008

Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης

Δημήτρης Γκρίτζαλης (dgrit@aueb.gr)

Οικονομικό Πανεπιστήμιο Αθηνών και e-Government Forum (Ο.Ε. CICIP)

Ιωάννα Σαμπράκου (i.samprakou@yme.gov.gr)

Υπουργείο Μεταφορών και Επικοινωνιών και e-Government Forum (Ο.Ε. CICIP)

Ομάδα Εργασίας e-Government Forum:

Προστασία Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης (CICIP)

Σύνθεση Ομάδας Εργασίας:

Σπύρος Καρούσος	Κοινωνία της Πληροφορίας Α.Ε. (Συντονιστής)
Δημήτρης Γκριτζαλής	Οικονομικό Πανεπιστήμιο Αθηνών (Εισηγητής)
Αλέξανδρος Ζαχαρής	Εκπρόσωπος ΣΕΠΕ
Μαριάνθη Θεοχαρίδου	Οικονομικό Πανεπιστήμιο Αθηνών
Πάνος Κοτζανικολάου	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
Δημήτρης Λέικας	Πανεπιστήμιο Αιγαίου
Νίκος Μήτρου	Εθνικό Μετσόβιο Πολυτεχνείο
Δέσποινα Πολέμη	Πανεπιστήμιο Πειραιώς
Ιωάννα Σαμπράκου	Υπουργείο Μεταφορών και Επικοινωνιών
Βικτωρία Σκουλαρίδου	Ελληνική Αστυνομία
Βασίλης Τσούμας	Ernst & Young

Λειτουργικό Πλαίσιο:

Κοινωνία της Πληροφορίας Α.Ε., e-Government Forum (www.e-governmentforum.gr)

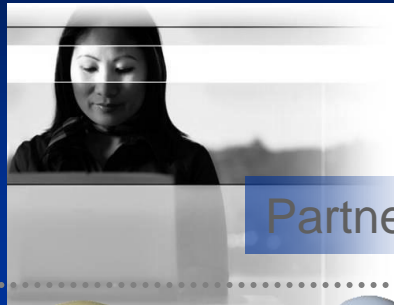
Νέοι όροι - νέες επιδιώξεις - νέοι κίνδυνοι

- **Υποδομή (Infrastructure):** Πλέγμα αλληλοεξαρτώμενων δικτύων και συστημάτων που παρέχει αξιόπιστη ροή προϊόντων, υπηρεσιών και αγαθών, για τη λειτουργία της Δ.Δ., της Οικονομίας, της Κοινωνίας ή άλλων υποδομών.
- **Κρίσιμη Υποδομή: (Critical Infrastructure):** Υποδομή μεγάλης κλίμακας, της οποίας τυχόν υποβάθμιση, διακοπή ή δυσλειτουργία έχει σοβαρή επίπτωση στην υγεία, ασφάλεια ή ευμάρεια των πολιτών ή στη λειτουργία Δ.Δ. ή/και Οικονομίας.
- **Πληροφοριακή και Επικοινωνιακή Υποδομή (ΠΕΥ):** Υποδομή που αποσκοπεί στην παροχή πληροφοριών, υπηρεσιών επικοινωνίας ή άλλων e-υπηρεσιών.
- **Κρίσιμη ΠΕΥ (Critical Information and Communication Infrastructure):** Πληροφοριακό και επικοινωνιακό σύστημα που είναι κρίσιμη υποδομή ή αποτελεί προϋπόθεση για τη λειτουργία άλλων τέτοιων υποδομών.
- **Προστασία Κρίσιμης ΠΕΥ (Critical Information and Communication Infrastructure Protection):** Ενέργειες των κατόχων, κατασκευαστών, χρηστών, διαχειριστών, ερευνητικών ιδρυμάτων, Δ.Δ. και κανονιστικών/ρυθμιστικών αρχών, για την διασφάλιση της ποιοτικής λειτουργίας της υποδομής σε περίπτωση επιθέσεων, ατυχημάτων και σφαλμάτων και για την τυχόν ανάκαμψή της, σε εύλογο χρόνο.

ΤΠΕ στη Δημόσια Διοίκηση: Πακτωλός ή παγίδα;



Customers



Partners



Employees

Applications

quotes

video

contracts

SOPs

presentations

images

manuals

manuals

RFID

specs

Όγκος δεδομένων

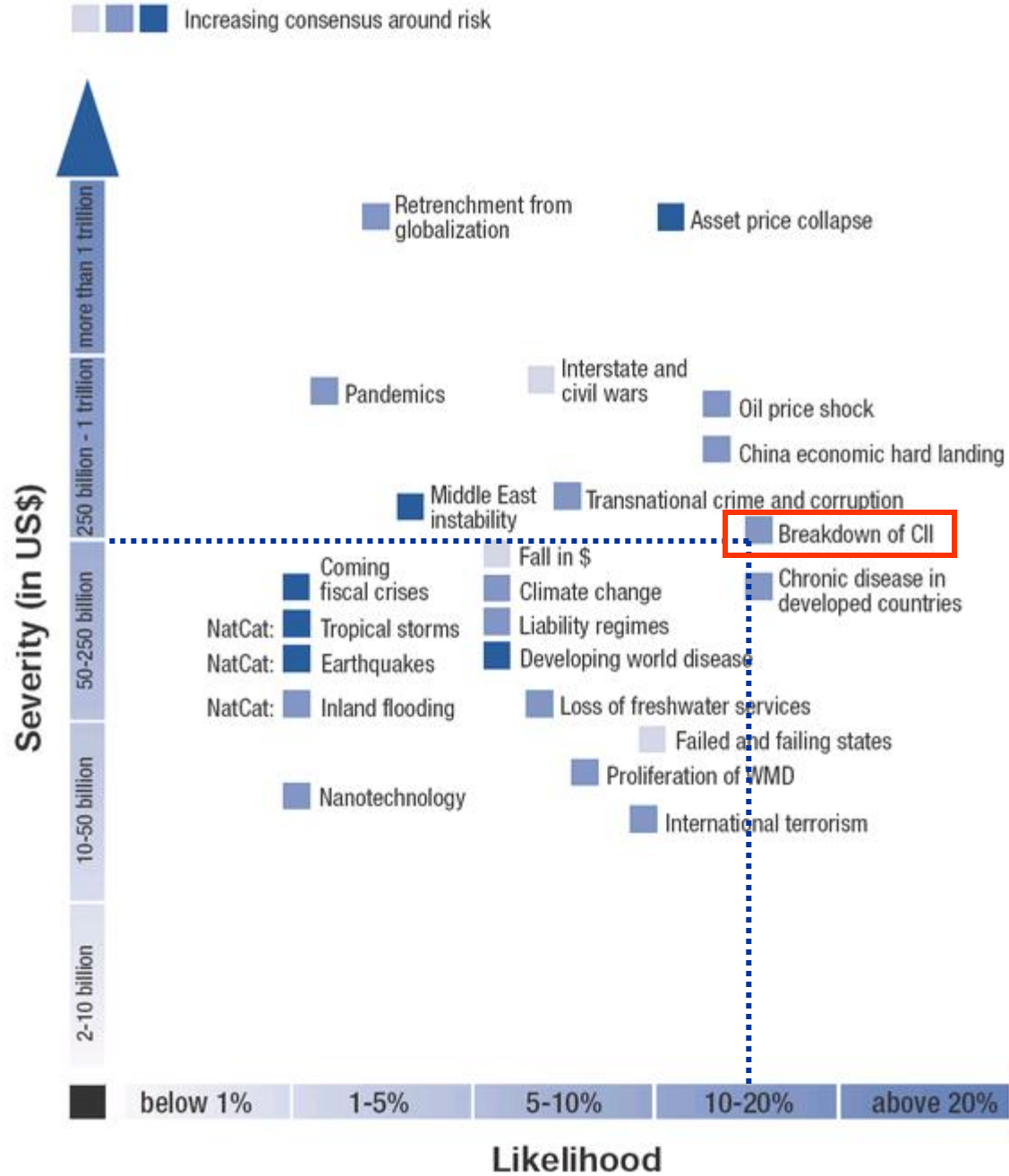
75% ετήσια αύξηση

Από Gigabytes σε Petabytes
σε 10 μόλις χρόνια

Πολυπλοκότητα διαδικασιών
Εκατοντάδες εφαρμογές και formats
Περίπλοκοι διακομιστές και δίκτυα
Νέοι κανόνες και κανονισμοί
Νέες απειλές και ευπάθειες

World Economic Forum (2008)

Core Global Risks: Likelihood with Severity by Economic Loss

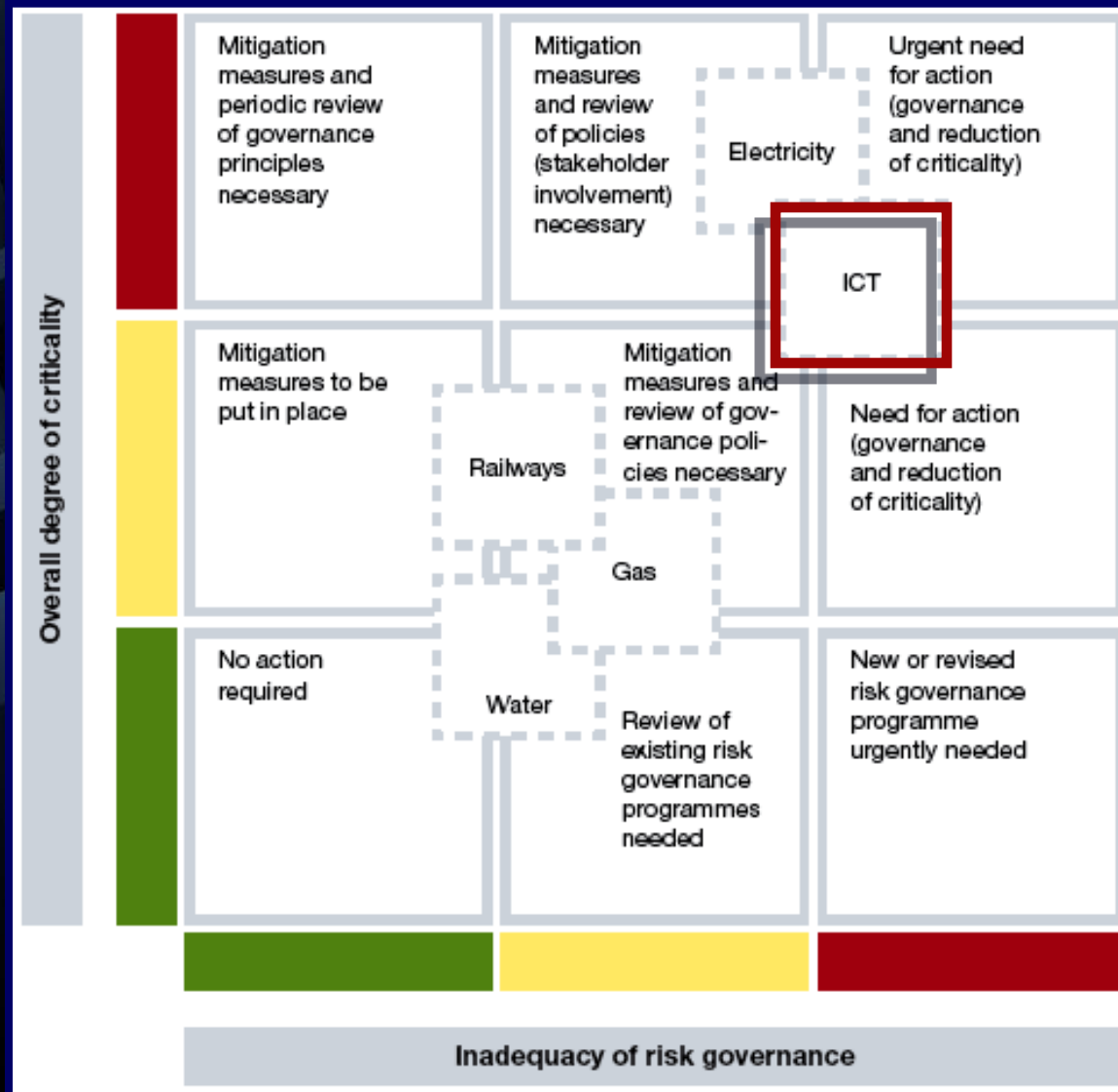


Οριζόντια σύγκριση κρυσιμότητας εθνικών υποδομών

		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.

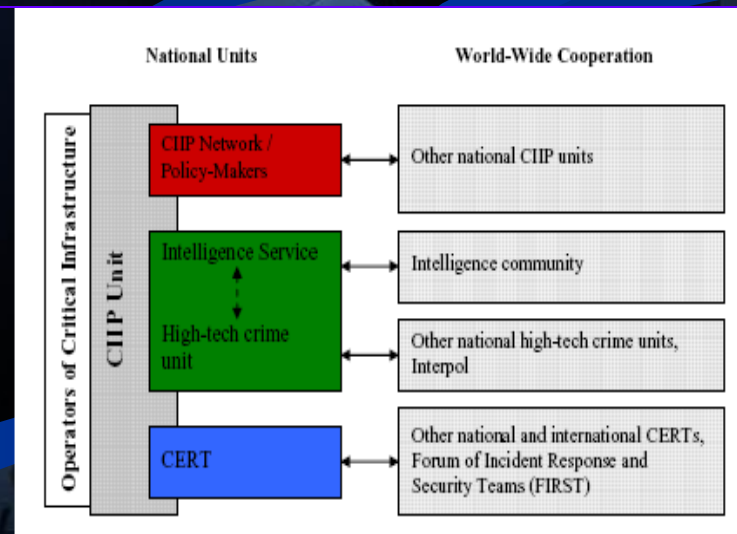
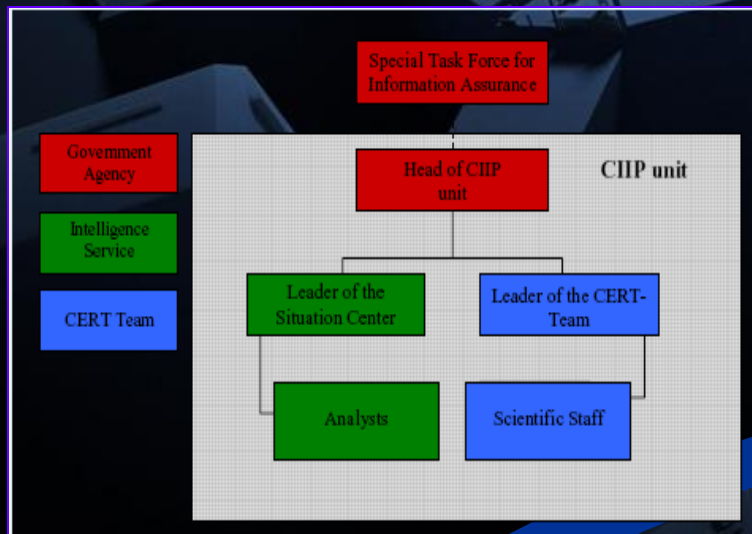
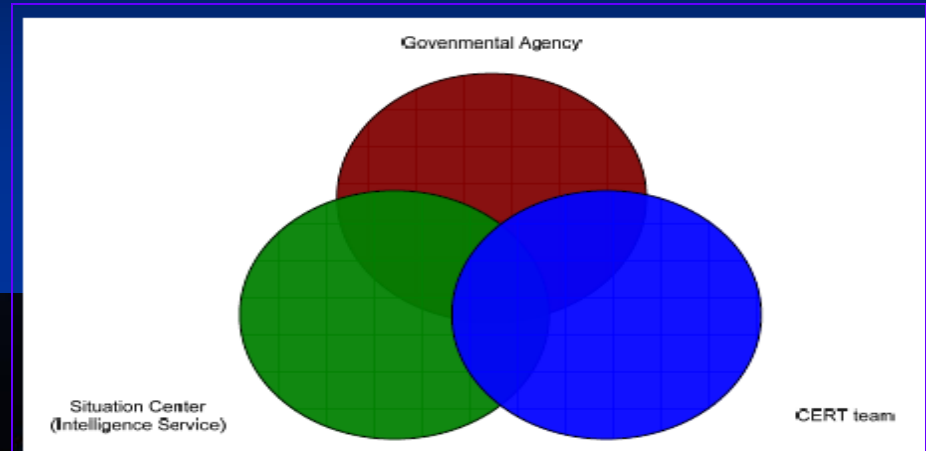
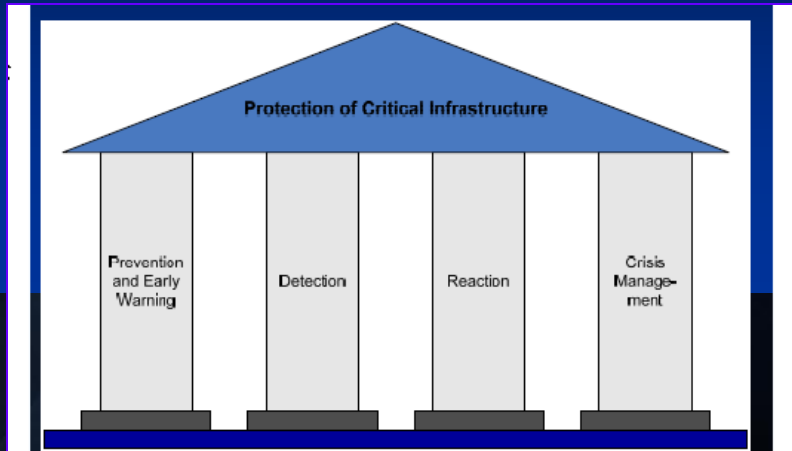
Κρισιμότητα Υποδομής vs. Ακαταλληλότητα Διαχείρισης Επικινδυνότητας



Μεθοδολογία της Ο.Ε. CICIP



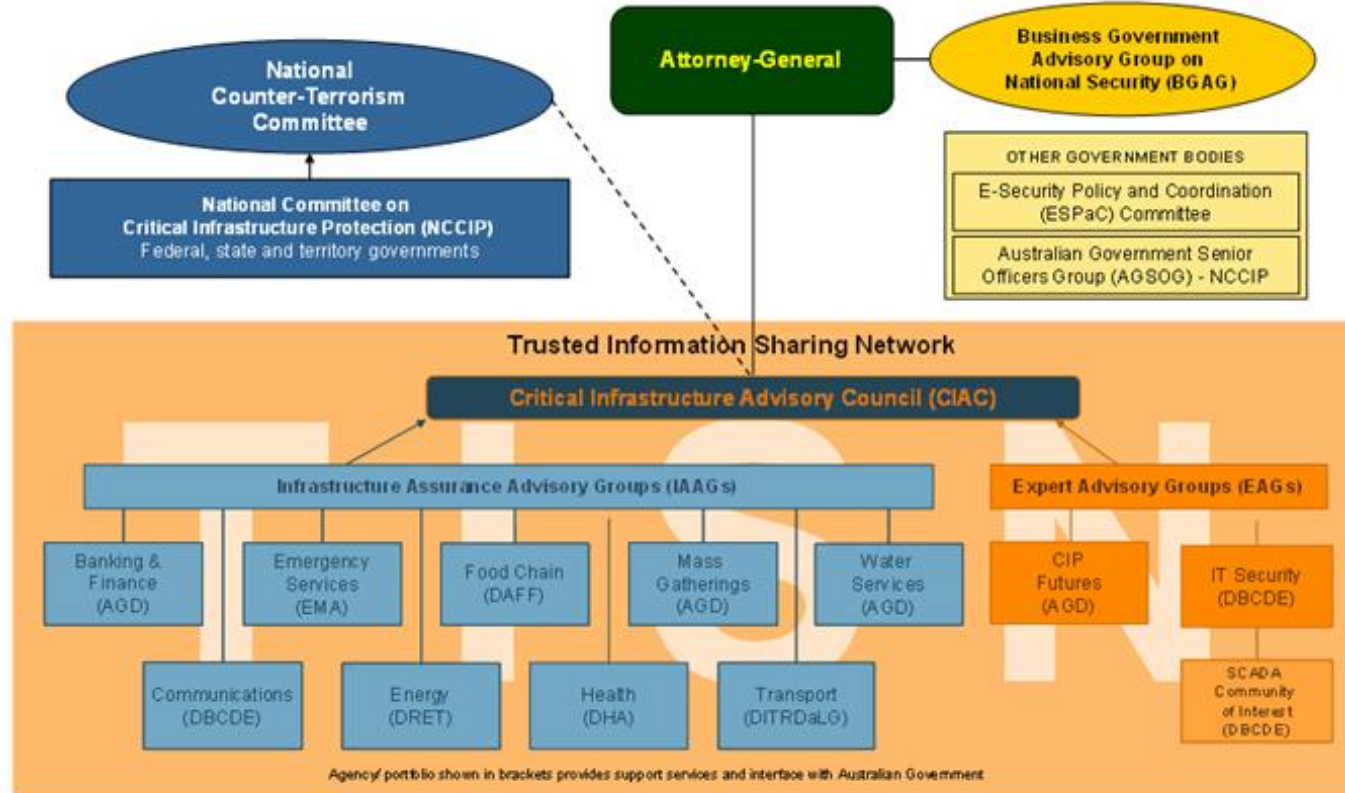
Διδάγματα και καλές πρακτικές...



Διεθνή οργανωτικά σχήματα και δομές

ΑΥΣΤΡΑΛΙΑ

Australia's Critical Infrastructure Protection Arrangements



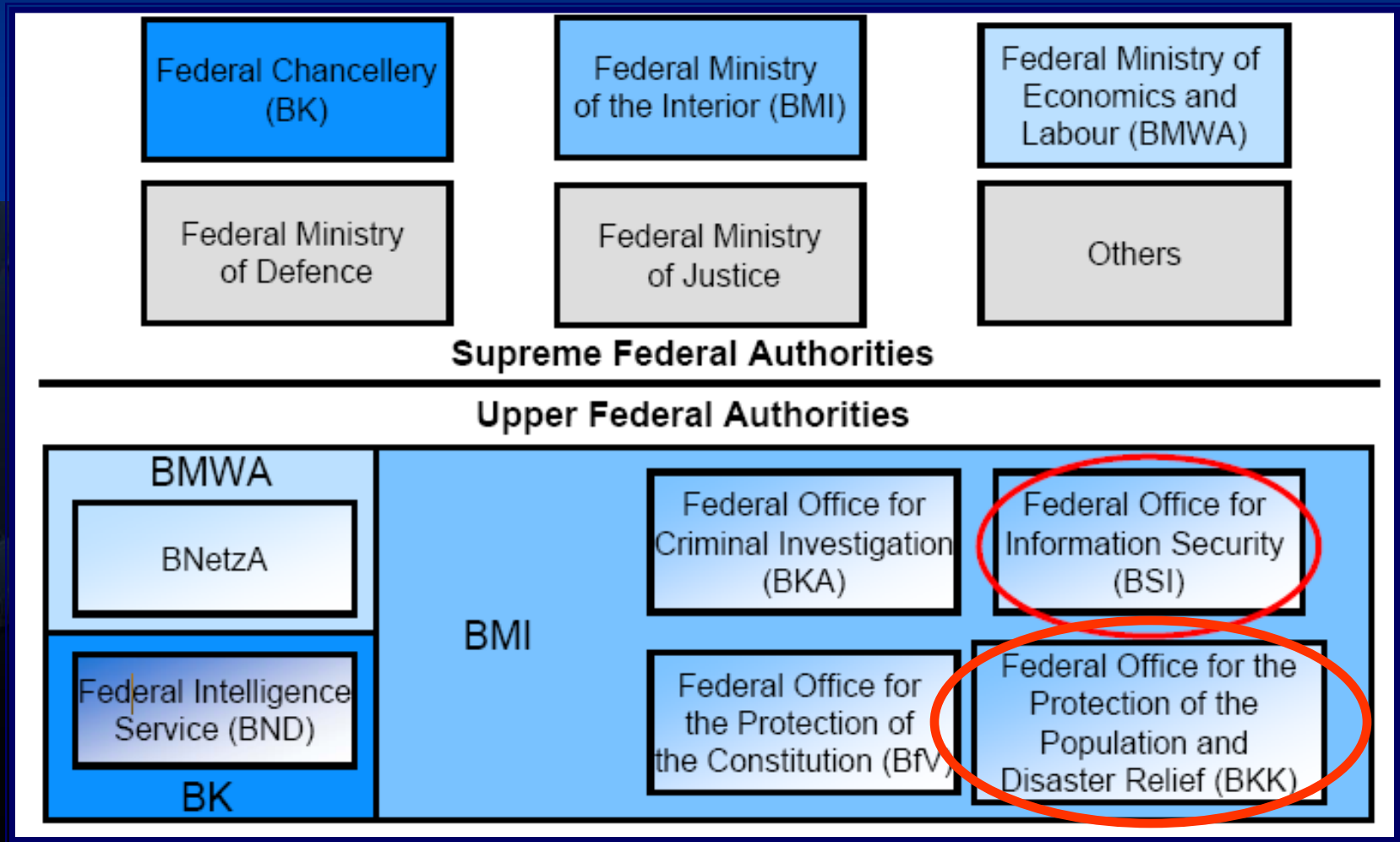
December 2007

Legend:

AGD	Attorney-General's Department
EMA	Emergency Management Australia
DAFF	Department of Agriculture, Fisheries and Forestry
DBCDE	Department of Broadband, Communications and the Digital Economy
DRET	Department of Resources, Energy and Tourism
DHA	Department of Health and Ageing
DITRD&LG	Department of Infrastructure, Transport, Regional Development and Local Government

Διεθνή οργανωτικά σχήματα και δομές

ΓΕΡΜΑΝΙΑ



Εμπλεκόμενοι ελληνικοί φορείς

(με τον ένα ή τον άλλο τρόπο/βαθμό/έκταση/ένταση)

- Υπουργείο Εσωτερικών (Ελληνική Αστυνομία, Εθνική Υπηρεσία Πληροφοριών, Διεύθυνση Πολιτικού Σχεδιασμού Έκτακτης Ανάγκης, Υπηρεσία Ανάπτυξης Πληροφορικής)
- Υπουργείο Εθνικής Άμυνας (ΓΕΕΘΑ)
- Υπουργείο Μεταφορών και Επικοινωνιών
- Υπουργείο Οικονομίας και Οικονομικών (Ομάδα Δράσης για την Ψηφιακή Ασφάλεια)
- Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ)
- Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)
- Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ)
- Τράπεζα της Ελλάδας
- Κέντρο Μελετών Ασφάλειας (ΚΕΜΕΑ)
- Ινστιτούτο Ερευνών/Μελετών Τηλεπικοινωνιών και Πληροφορικής Χωρών Νοτιοανατολικής Ευρώπης (ΙΝΑ)
- Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας ΕΔΕΤ (GRNET-CERT)
- Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης (ΕΦΤΑ)
- Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδος (ΣΕΠΕ)
- Ελληνικός Κόμβος Ασφαλούς Διαδικτύου SafeNetHome Plus
- SafeLine
- ...

Επικαλύψεις αρμοδιοτήτων ορισμένων σχετικών ελληνικών φορέων

ΦΟΡΕΑΣ	ΣΧΕΤΙΚΟ ΠΕΔΙΟ ΔΡΑΣΗΣ	ΡΟΛΟΙ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ			
		Ρυθμίσεις, κανονισμοί	Έλεγχοι εφαρμογής θεσμικού πλαισίου	Παροχή προϊόντων-υποδομών ασφαλείας	Πιστοποίηση προϊόντων και υπηρεσιών ασφαλείας
ΑΠΠΔ	Προστασία προσωπικών δεδομένων	✓	✓		✓ (?)
ΑΔΑΕ	Προστασία απορρήτου των επικοινωνιών	✓	✓		✓
ΕΕΤΤ	Ρύθμιση θεμάτων τηλεπικοινωνιών	✓	✓	✓ (?)	✓
ΕΦΤΑ	Πρόληψη τηλεπικοινωνιακής απάτης	✓		✓	
GRNET – CERT	Προϊόντα/υπηρεσίες ασφάλειας συστημάτων			✓	

Κριτήρια επιλογής κρίσιμων υποδομών της Δ.Δ.

Επίπτωση Κριτήριο	Πολύ υψηλή	Υψηλή	Μέτρια	Χαμηλή	Πολύ χαμηλή
Επηρεαζόμενος πληθυσμός	>100,000	10,000-100,000	1,000-10,000	100-1,000	<100
Οικονομική επίπτωση	>100 x 10 ⁶ €	10-100 x 10 ⁶ €	1-10 x 10 ⁶ €	0,1-1 x 10 ⁶ €	<0,1 x 10 ⁶ €
Ένταση διασυννοριακότητας	Ευρύτερη της Ευρωπαϊκής Ένωσης	Ευρωπαϊκή Ένωση	Εθνική	Περιφερειακή	Τοπική
Αλληλεξάρτηση	Καταλυτική επίδραση σε άλλες υποδομές/τομείς	Σημαντική επίδραση σε άλλες υποδομές/τομείς	Μέτρια επίδραση σε άλλες υποδομές/τομείς	Μικρή επίδραση σε άλλες υποδομές/τομείς	Επίδραση σε μία υποδομή/τομέα
Ανάκαμψη Π.Ε.Υ.	Υψηλό κόστος σε πολλούς τομείς, μακρύς χρόνος ανάκαμψης (μήνες - χρόνια)	Υψηλό κόστος, μακρύς απαιτούμενος χρόνος ανάκαμψης (βδομάδες - μήνες)	Μέσο κόστος, σημαντικός χρόνος ανάκαμψης (μέρες - βδομάδες)	Χαμηλό κόστος, μικρός απαιτούμενος χρόνος ανάκαμψης (ώρες - μέρες)	Αμελητέο κόστος, μικρός απαιτούμενος χρόνος ανάκαμψης (ώρες)
Ενόχληση της κοινής γνώμης	Διεθνής αποδοκιμασία	Περιορισμός κυβερνητικής αξιοπιστίας σε διεθνές επίπεδο	Μετριασμός κυβερνητικής αξιοπιστίας σε εθνικό επίπεδο	Αρνητική δημοσιότητα περισσότερων του ενός κυβερνητικών οργανισμών/φορέων	Αρνητική δημοσιότητα ενός κυβερνητικού οργανισμού/φορέα
Εφαρμογή πολιτικής και λειτουργία Δ.Δ.	Σοβαρή παρεμπόδιση ή διακοπή της ανάπτυξης/εφαρμογής κυβερνητικών πολιτικών	Υποβάθμιση της διαπραγματευτικής και συναλλακτικής δυνατότητας της κυβέρνησης	Παρεμπόδιση της αποτελεσματικής ανάπτυξης/εφαρμογής κυβερνητικών πολιτικών	Υπονόμευση της σωστής διαχείρισης ή λειτουργίας μιας δημόσιας υπηρεσίας	Ανεπαρκής λειτουργία μιας δημόσιας υπηρεσίας
Προσωπική ασφάλεια	Απώλεια πολλών ανθρώπινων ζωών	Απώλεια ανθρώπινης ζωής	Σοβαρός τραυματισμός πολλών προσώπων	Μικροτραυματισμοί πολλών προσώπων	Μικροτραυματισμός ενός προσώπου
Επίπτωση στην ιδιωτικότητα	Αποκάλυψη απόρρητων δεδομένων που επηρεάζουν μείζονες κυβερνητικές πολιτικές	Παραβίαση νομοθεσίας και σοβαρή ενόχληση πολλών προσώπων	Παραβίαση νομοθεσίας και σοβαρή ενόχληση ενός προσώπου	Μικρή ενόχληση πολλών προσώπων	Μικρή ενόχληση ενός προσώπου
Επηρεασμός του κοινού για τις ΤΠΕ	Απαξίωση των ΤΠΕ από το κοινωνικό σύνολο	Αρνητικός επηρεασμός του κοινωνικού συνόλου	Κλονισμός της εμπιστοσύνης του κοινωνικού συνόλου	Απογοήτευση επιμέρους ομάδων του πληθυσμού	Απογοήτευση μεμονωμένων πολιτών

Εντοπισμός κρίσιμων¹ υποδομών της Δ.Δ.

Κριτήριο	Πληροφοριακή και Επικοινωνιακή Υποδομή ²	Εθνικό Δίκτυο Δ.Δ. ΣΥΖΕΥΞΙΣ	Ο.Π.Σ. Κέντρων Εξυπηρέτησης Πολιτών	Κέντρα Δεδομένων (Data Centers) ΚτΠ Α.Ε.	Ολοκληρωμένο Σύστημα Φορολογίας TaxisNET
Επηρεαζόμενος πληθυσμός	Πολύ υψηλή	Πολύ υψηλή	Πολύ υψηλή	Πολύ υψηλή	Πολύ υψηλή
Οικονομική επίπτωση	Χαμηλή	Χαμηλή	Χαμηλή	Χαμηλή	Πολύ υψηλή
Ένταση διασυννοριακότητας	Υψηλή	Υψηλή	Υψηλή	Υψηλή	Πολύ υψηλή
Αλληλεξάρτηση	Πολύ υψηλή	Μέτρια	Μέτρια	Υψηλή	Υψηλή
Ανάκαμψη	Χαμηλή/Μέτρια	Χαμηλή	Χαμηλή	Υψηλή	Χαμηλή
Ενόχληση της κοινής γνώμης	Υψηλή	Μέτρια	Μέτρια	Μέτρια	Μέτρια
Εφαρμογή πολιτικής και λειτουργία Δ.Δ.	Μέτρια	Χαμηλή	Χαμηλή	Μέτρια	Μέτρια
Προσωπική ασφάλεια	Πολύ χαμηλή	Πολύ χαμηλή	Πολύ χαμηλή	Πολύ χαμηλή	Πολύ χαμηλή
Επίπτωση στην ιδιωτικότητα	Υψηλή	Υψηλή	Υψηλή	Υψηλή	Υψηλή
Επηρεασμός του κοινού για τις ΤΠΕ	Υψηλή	Υψηλή	Υψηλή	Πολύ υψηλή	Υψηλή

Χαμηλή

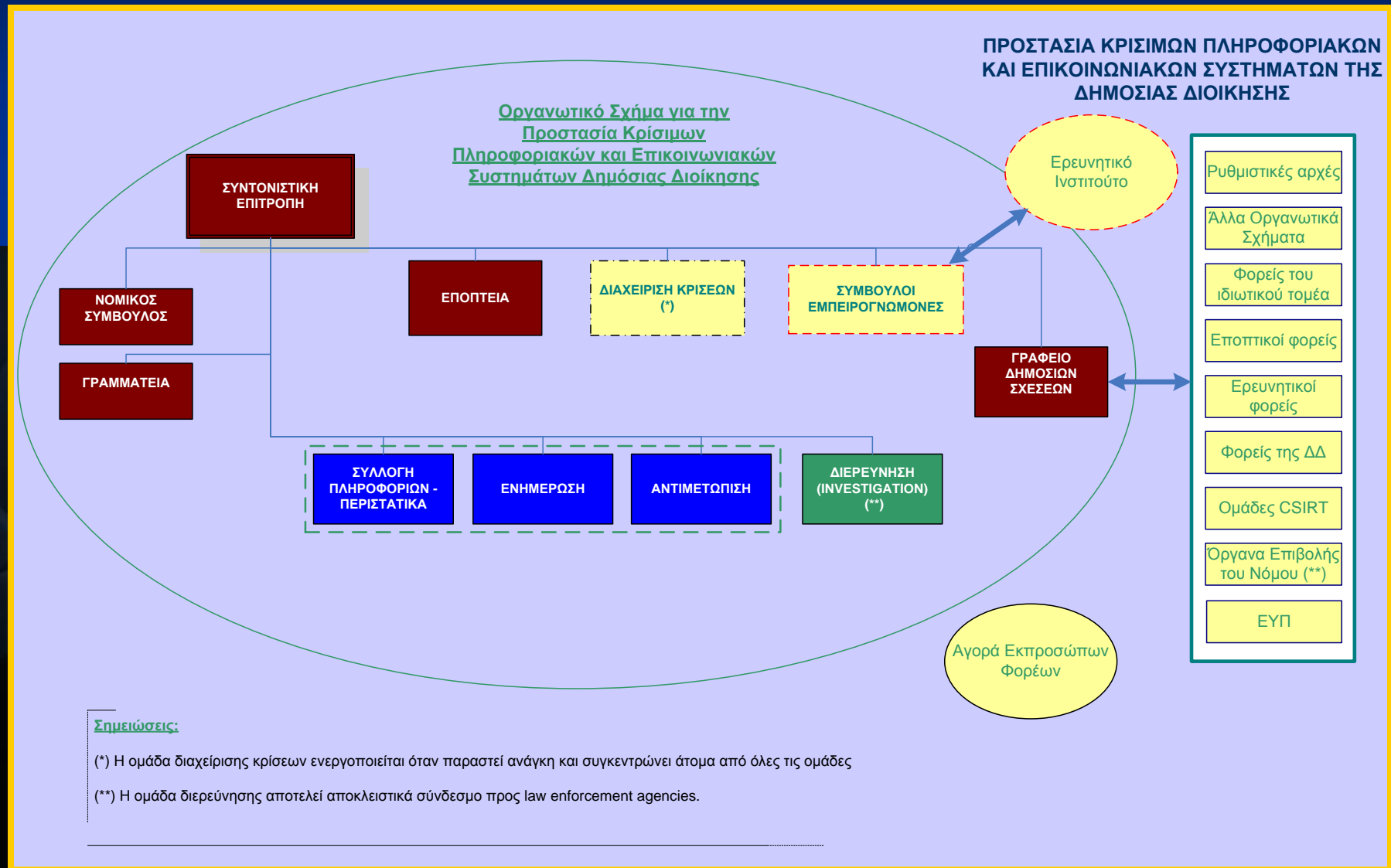
Μέτρια

Υψηλή

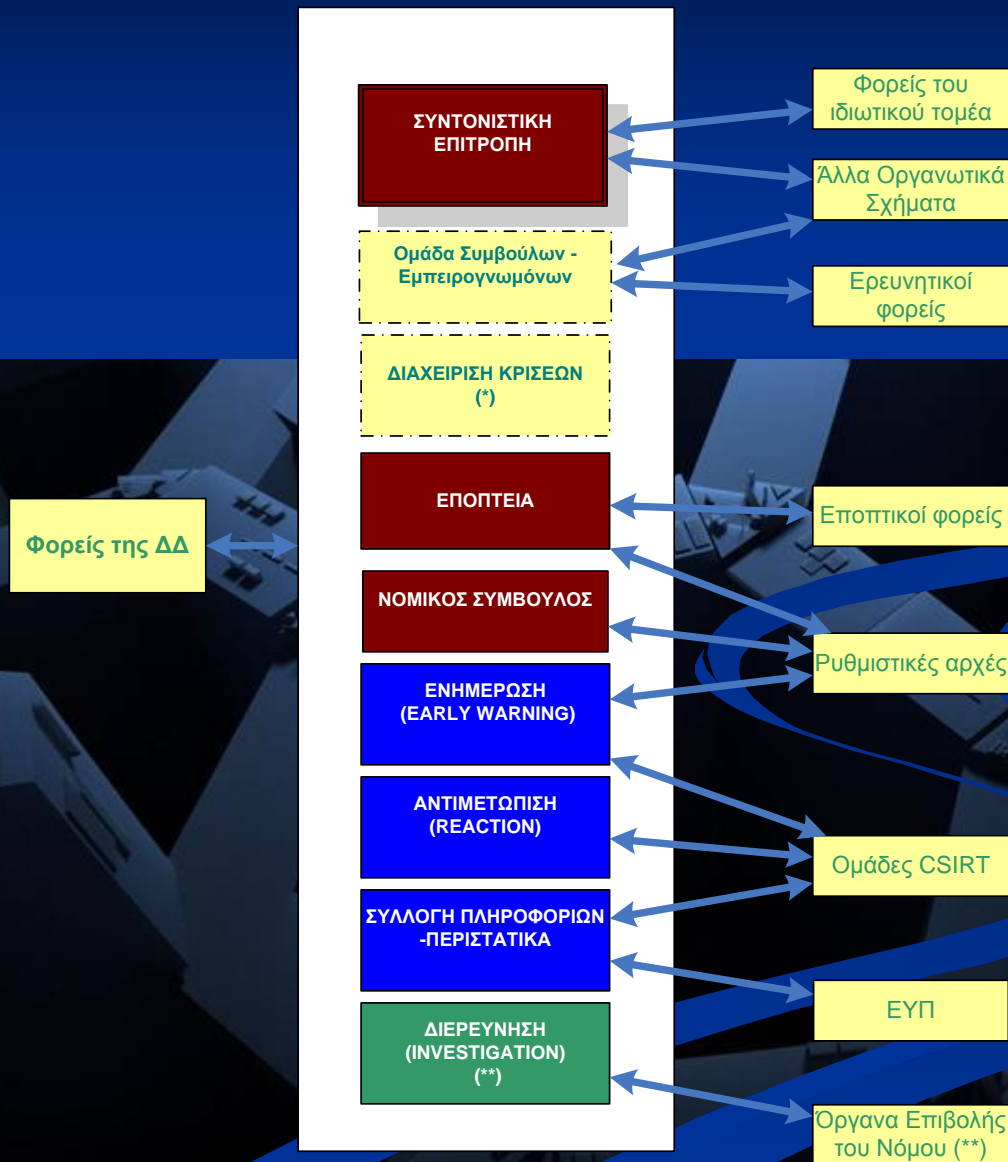
¹ Αναφέρεται σε ήπια κρίσιμότητα (soft criticality) και δεν αφορά υποδομές εθνικής ασφαλείας (ΥΕΘΑ, ΥΠΙΕΞ, ΕΥΠ κλπ.).

² Βέργη Ε., Παππάς Θ., *Εξέλιξη των 20 βασικών υπηρεσιών ηλεκτρονικής διακυβέρνησης στην Ελλάδα*, Παρατηρητήριο για την Κοινωνία της Πληροφορίας, Αθήνα, Νοέμβρης 2007.

Δομή ενός φορέα για την προστασία των κρίσιμων υποδομών της ελληνικής Δ.Δ.



Διασυνδέσεις του φορέα με αρμόδιους φορείς



Προτεινόμενες πρωτοβουλίες

ΒΑΣΙΚΕΣ ΠΑΡΑΜΕΤΡΟΙ			
ΠΑΡΕΜΒΑΣΗ	Κατηγορία	Προτεραιότητα	Πιθανό χρηματοδοτικό σχήμα
Ίδρυση Φορέα Προστασίας Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης	Θεσμική (εισήγηση Συμβουλίου e-Government Forum)	Υψηλή	Κρατικός Προϋπολογισμός
Ίδρυση Ερευνητικού Ινστιτούτου Προστασίας Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών	Θεσμική (πρόταση Συμβουλίου e-Government Forum)	Υψηλή	Ε.Π. Υπουργείου Παιδείας Ε.Π. Υπουργείου Ανάπτυξης (Γενική Γραμματεία Έρευνας και Τεχνολογίας)
Ασφάλεια Πολυκέντρου Δεδομένων της Κοινωνίας της Πληροφορίας Α.Ε.	Διαχειριστική (απόφαση ΚτΠ Α.Ε.)	Πολύ υψηλή	Ε.Π. Κοινωνία της Πληροφορίας Ε.Π. Ψηφιακή Σύγκλιση
Εντοπισμός Κρίσιμων Ελληνικών Υποδομών	Διαχειριστική (απόφαση ΚτΠ ΑΕ)	Υψηλή	Ε.Π. Διοικητική Μεταρρύθμιση Ε.Π. Ψηφιακή Σύγκλιση
Τεχνολογική υποδομή Φορέα Προστασίας Κρίσιμων Πληροφοριακών και Επικοινωνιακών Υποδομών της Δημόσιας Διοίκησης	Διαχειριστική (απόφαση ΚτΠ Α.Ε.)	Υψηλή	Ε.Π. Ψηφιακή Σύγκλιση

References

1. Doulas A., Mavrouidakis 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.
2. Dritsas S., Tsoumas B., Dritsou V., Konstantopoulos P., Gritzalis D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, Vol. 32, No. 2, pp. 203-212, 2009.
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., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
6. Gritzalis D., "A digital seal solution for deploying trust on commercial transactions", *Information Management & Computer Security*, Vol. 9, No. 2, pp. 71-79, 2001.
7. Iliadis J., Gritzalis D., Spinellis D., Katsikas S., "Developing secure web-based medical applications", *Medical Informatics*, Vol. 24, No. 1, pp. 75-90, 1999.
8. Spinellis D., Iliadis J., Gritzalis D., Katsikas S., "Trusted Third Party services for deploying secure telemedical applications over the WWW", *Computers & Security*, Vol. 18, No. 7, pp. 627-639, 1999.
9. Theoharidou M., Marias J., Dritsas S., Gritzalis D., "The Ambient Intelligence Paradigm: A review of security and privacy strategies in leading economies", in *Proc. of the 2nd IET Conference on Intelligent Environments*, Vol. 2, pp. 213-219, 2006.
10. 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.
11. 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.