

National Critical Infrastructure Protection: Towards an Holistic Strategy



P. Kotzanikolaou

June 2016

Προστασία Εθνικών Κρίσιμων Υποδομών: Προς μία Ολιστική Στρατηγική



Επίκουρος Καθηγητής Παναγιώτης Κοτζανικολάου

Τμήμα Πληροφορικής | Πανεπιστήμιο Πειραιώς
(Εξωτερικός Συνεργάτης INFOSEC Laboratory, ΟΠΑ)

pkotzani@unipi.gr



Η ανάγκη για μία Εθνική Στρατηγική Προστασίας ΚΥ: Παρούσα κατάσταση

Πρακτικοί λόγοι

- Ανάγκη για ολιστική προστασία υποδομών ζωτικής σημασίας
- Πρόληψη, αποφυγή και έγκαιρη ανάκαμψη
- Διαχείριση απειλών και κινδύνων
- Ανάγκη συμμόρφωσης με Ευρωπαϊκές Οδηγίες
- Ανάγκη συντονισμού σε εθνικό επίπεδο

Παρούσα Κατάσταση

- Απουσία στρατηγικού σχεδιασμού
- Αποσπασματική αντιμετώπιση
- Αρκετές μεμονωμένες δράσεις χωρίς επαρκή συντονισμό



Η ανάγκη για μία Εθνική Στρατηγική Προστασίας ΚΥ: Στόχοι και περιορισμοί

Στόχοι Προτεινόμενης Στρατηγικής

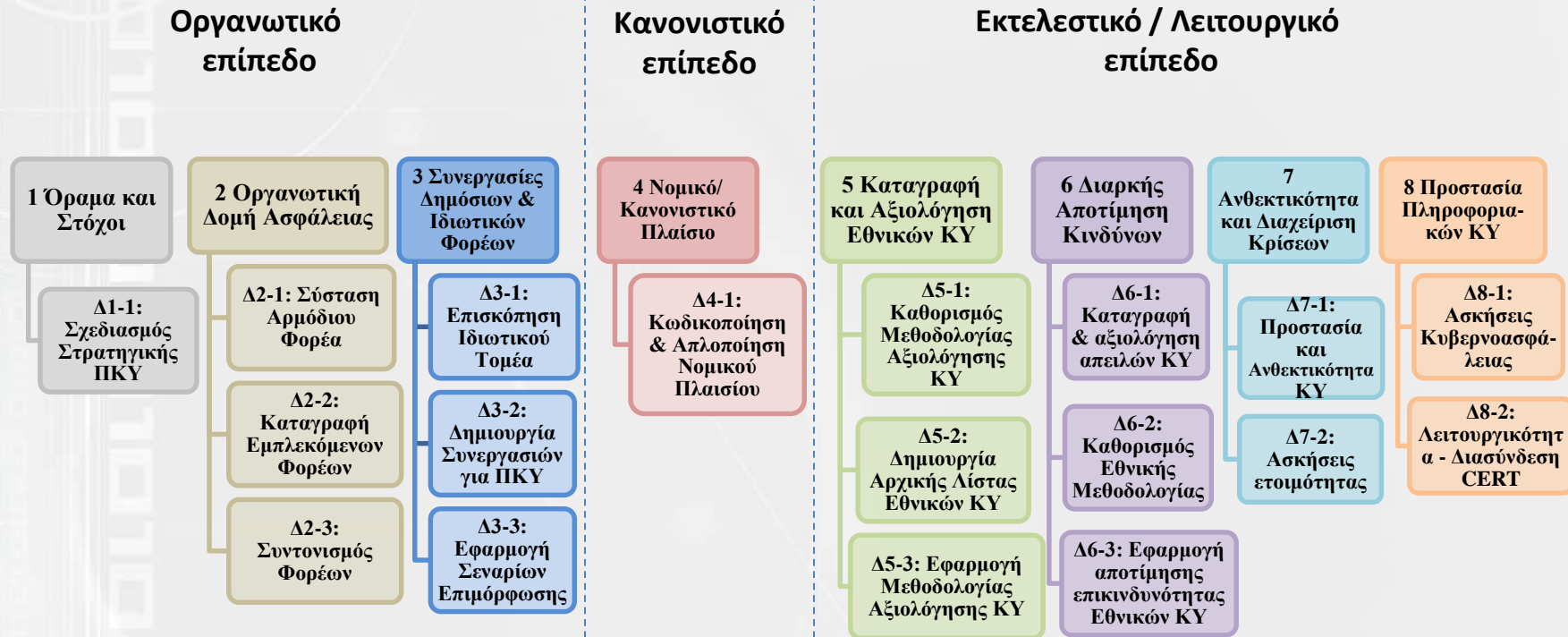
- Καθορισμός συγκεκριμένων **τομέων προτεραιότητας** με βάση τη διεθνή πρακτική
- Πρόταση πρακτικών και **εφαρμόσιμων Δράσεων** εφαρμογής
- Αξιοποίηση υφιστάμενων Δράσεων
- Ένταξη αποτελεσμάτων της μελέτης με σαφή και δομημένο τρόπο
- Πρόταση ρεαλιστικού **Σχεδίου Εφαρμογής** (Action Plan)

Περιορισμοί Προτεινόμενου Σχεδίου

- Χρήση μόνο δημόσια προσβάσιμων πληροφοριών
- Ο αρμόδιος φορέας θα έχει (όπου απαιτείται) τη δυνατότητα για:
 - πρόσβαση σε διαβαθμισμένη πληροφορία
 - αποδοτικότερο συντονισμός δράσεων φορέων



Παρουσίαση Σχεδίου Στρατηγικής: Συνοπτική παρουσίαση Δράσεων



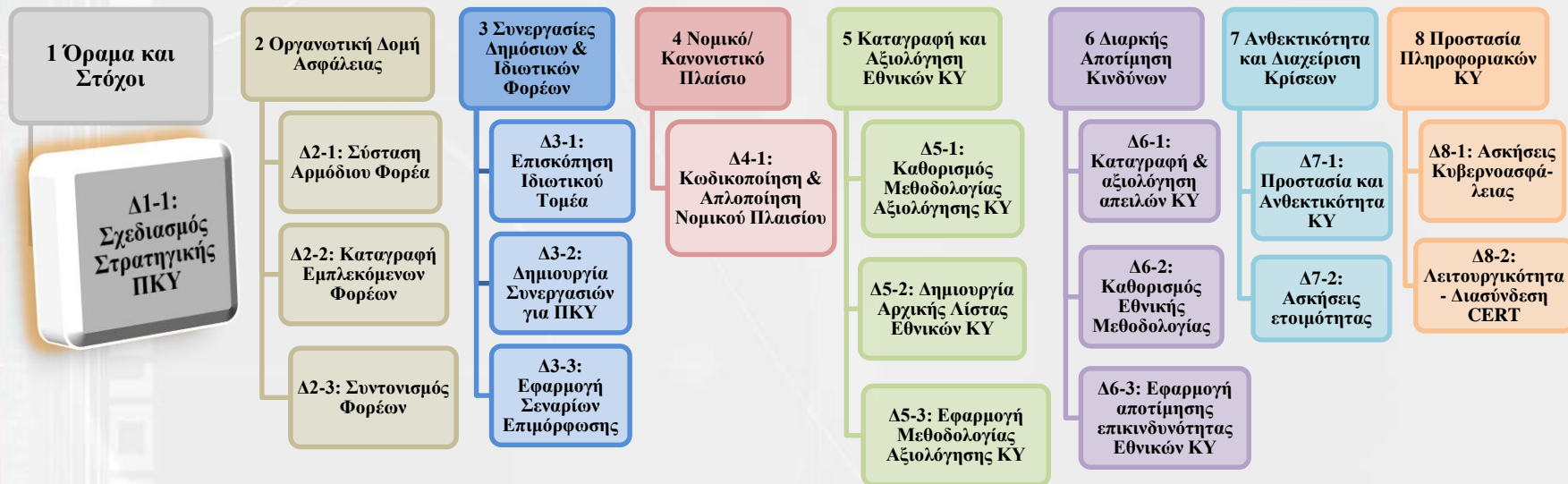
Συνοπτική παρουσίαση Δράσεων ανά Τομέα Προτεραιότητας



Ενδεικτική παρουσίαση κυριότερων Δράσεων ανά Τομέα Προτεραιότητας



Όραμα και Στόχοι: Σχεδιασμός Στρατηγικής Προστασίας ΚΥ



Δράση 1-1: Σχεδιασμός Στρατηγικής Προστασίας Εθνικών ΚΥ

Περίληψη Δράσης:

- Καθορισμός Τομέων Προτεραιότητας, Δράσεων Υλοποίησης και Σχεδίου Εφαρμογής

Εκτιμώμενος Χρόνος Εφαρμογής:

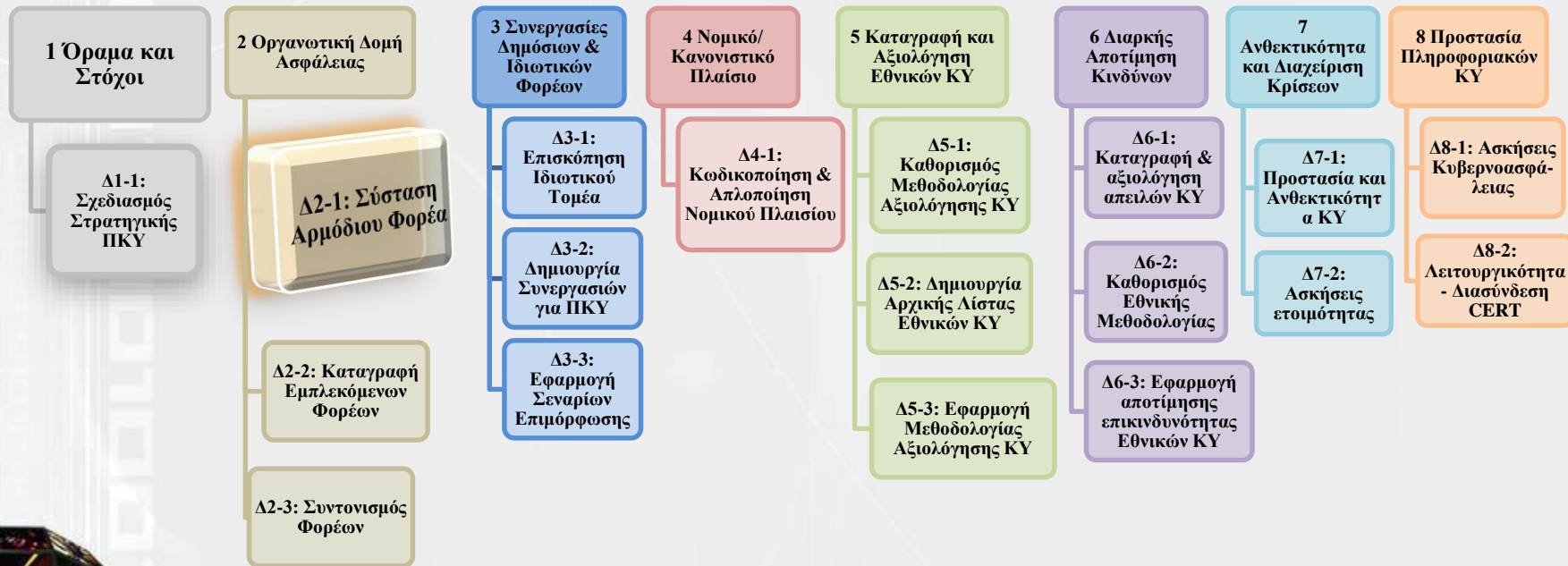
- Φάση Α (άμεσης προτεραιότητας)

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης:

- Το **Παραδοτέο Π3** της μελέτης (συνοπτικά παρουσιάζεται εδώ) μπορεί να αποτελέσει ένα σχέδιο μίας Ολιστικής Στρατηγικής



Οργανωτική Δομή: Σύσταση Αρμόδιου Φορέα



Δράση 2-1: Σύσταση Αρμόδιου Φορέα

Περίληψη Δράσης:

- Ένταξη της αρμοδιότητας του Συντονισμού για την Προστασία των ΚΥ σε φορέα, πολύ υψηλά στην διοικητική ιεραρχία (ει δυνατόν φορέας υπαγόμενος απευθείας στον Πρωθυπουργό)

Εκτιμώμενος Χρόνος Εφαρμογής:

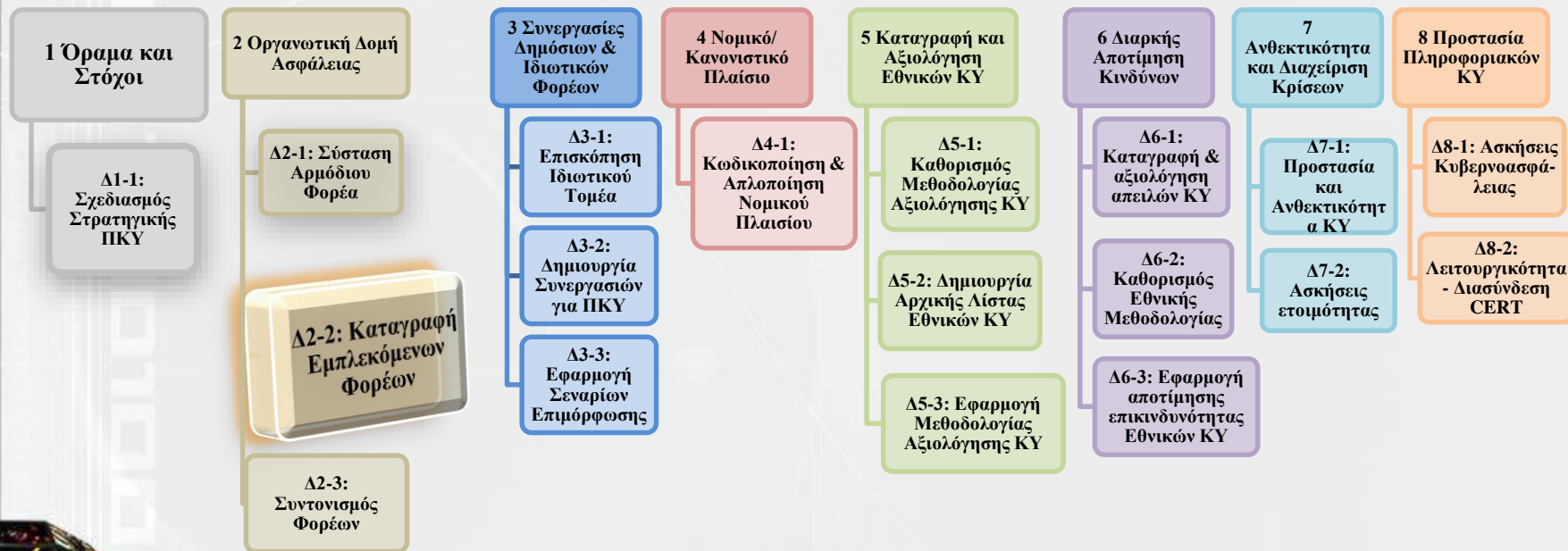
- Φάση Α (άμεσης προτεραιότητας)

Αξιοποίηση υφιστάμενων Δράσεων:

- Η νέο-ιδρυθείσα Γενική Γραμματεία Ψηφιακής Πολιτικής, θα μπορούσε να αποτελέσει τον αρμόδιο φορέα



Οργανωτική Δομή: Καταγραφή Εμπλεκόμενων Φορέων



Δράση 2-2: Καταγραφή Φορέων

Περίληψη Δράσης:

- Η καταγραφή όλων των εμπλεκόμενων φορέων με αρμοδιότητες οι οποίες άπτονται των θεμάτων ΠΚΥ
- Βέλτιστος καταμερισμός των αρμοδιοτήτων, επίλυση επικαλύψεων, διευκόλυνση παρακολούθησης και συντονισμού των δράσεων

Εκτιμώμενος Χρόνος Εφαρμογής:

- Φάση Α (άμεσης προτεραιότητας)

Αξιοποίηση υφιστάμενων Δράσεων:

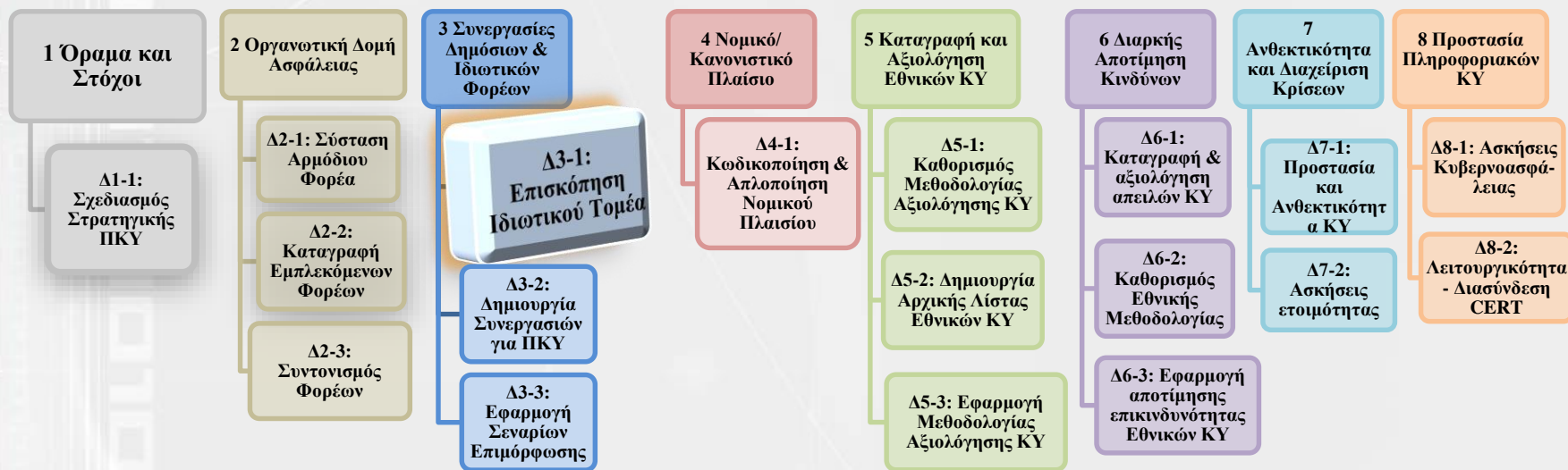
- Αρκετές δράσεις φορέων του Δημοσίου Τομέα

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης:

- Το **Παραδοτέο Π1, Κεφ.3.2** της μελέτης περιλαμβάνει μία αρχική καταγραφή



Συνεργασίες Δημόσιων-Ιδιωτικών Φορέων: Επισκόπηση Ιδιωτικού Τομέα



Δράση 3-1: Επισκόπηση Ιδιωτικού Τομέα

Περίληψη Δράσης:

- Εκτενής καταγραφή των κατόχων/διαχειριστών (ενδεχόμενων) ΚΥ
- Συνήθως (αλλά όχι μόνο) είναι φορείς του Ιδιωτικού Τομέα

Εκτιμώμενος Χρόνος Εφαρμογής:

- Φάση Α (άμεσης προτεραιότητας)

Αξιοποίηση υφιστάμενων Δράσεων:

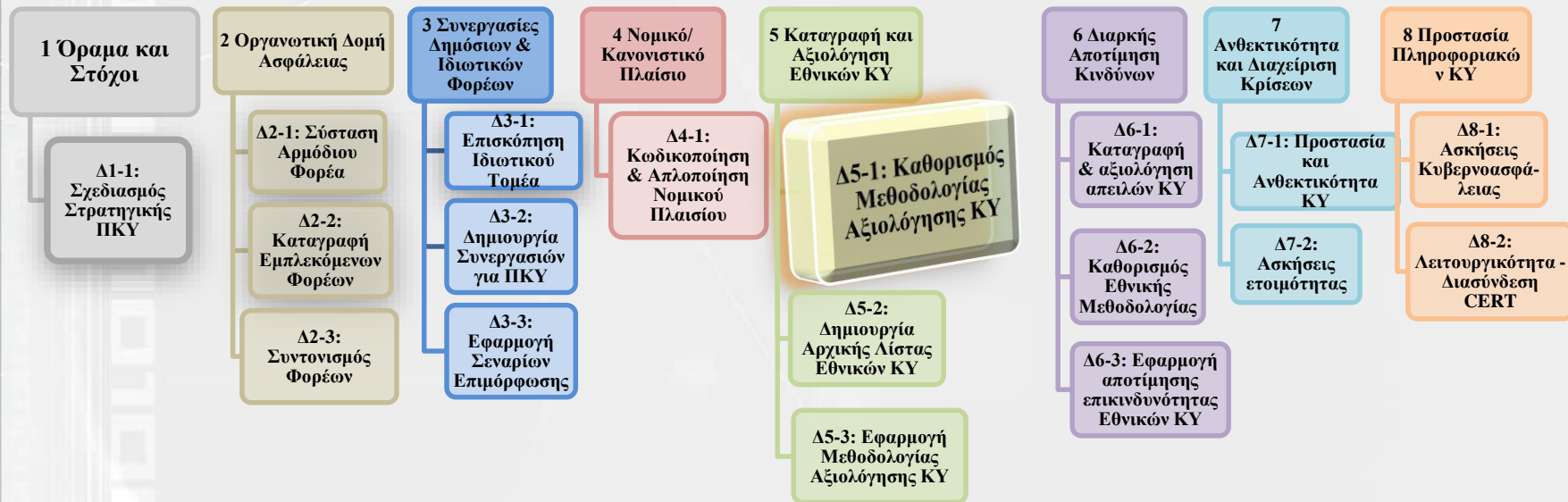
- Αρκετές δράσεις ρυθμιστικών φορέων (π.χ. ΡΑΕ, ΑΔΑΕ, ΕΕΤΤ κτλ)

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης:

- Το **Παραδοτέο Π1, Κεφ.4** έχει γίνει μία αρχική καταγραφή για τους τομείς της Ενέργειας, των ΤΠΕ και των Μεταφορών



Καταγραφή και Αξιολόγηση ΚΥ: Μεθοδολογία Αξιολόγησης ΚΥ



Δράση 5-1: Επισκόπηση Ιδιωτικού Τομέα

Περίληψη Δράσης:

- Καθορισμός Εθνική μεθοδολογίας προσδιορισμού και αξιολόγησης των ΚΥ, σύμφωνα με τις Ευρωπαϊκές οδηγίες και τις καλές πρακτικές

Εκτιμώμενος Χρόνος Εφαρμογής:

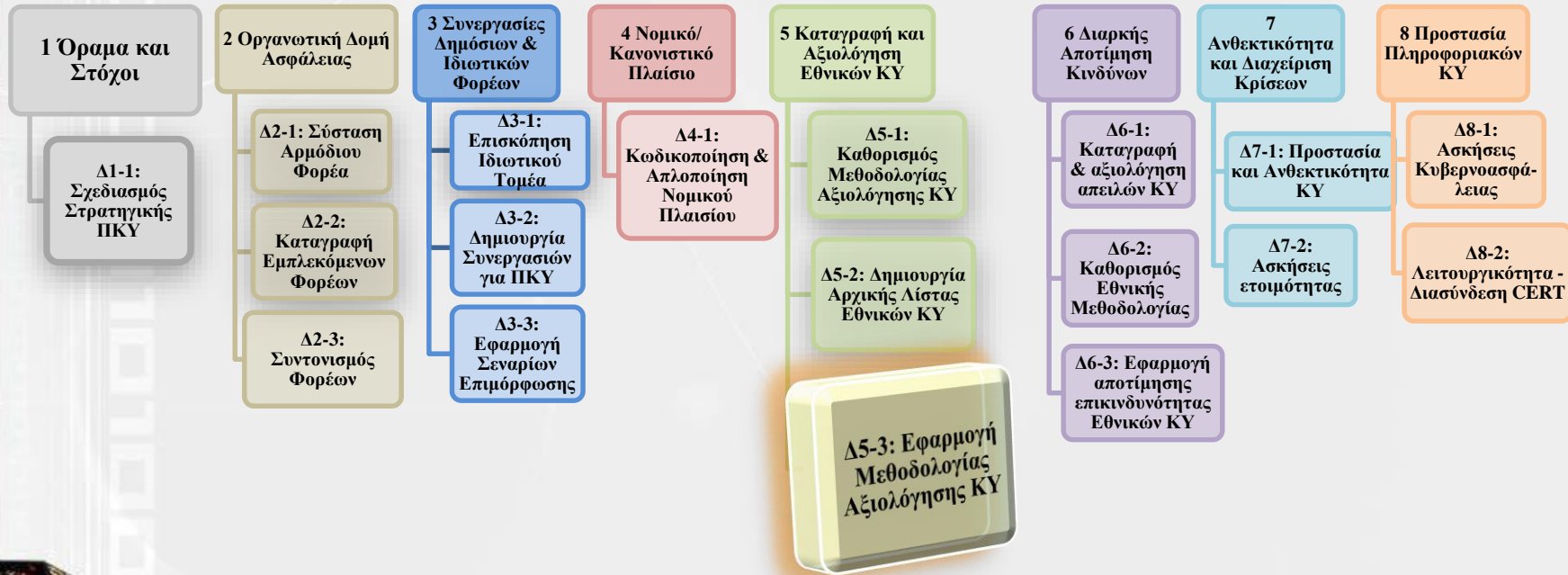
- Φάση Α (άμεσης προτεραιότητας)

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης:

- Το **Παραδοτέο Π2, Κεφ.3** προτείνει μία τέτοια μεθοδολογία (αναλύθηκε στην προηγούμενη παρουσίαση)



Καταγραφή και Αξιολόγηση ΚΥ: Εφαρμογή Μεθοδολογίας Αξιολόγησης



Δράση 5-3: Εφαρμογή Μεθοδολογίας Αξιολόγησης Εθνικών ΚΥ

Περίληψη Δράσης:

- Εφαρμογή της μεθοδολογίας που προσδιορίστηκε στην Δράση 5-1, με σκοπό τον προσδιορισμό των κρίσιμων τομέων, υποτομέων, υποδομών και υπηρεσιών

Εκτιμώμενος Χρόνος Εφαρμογής:

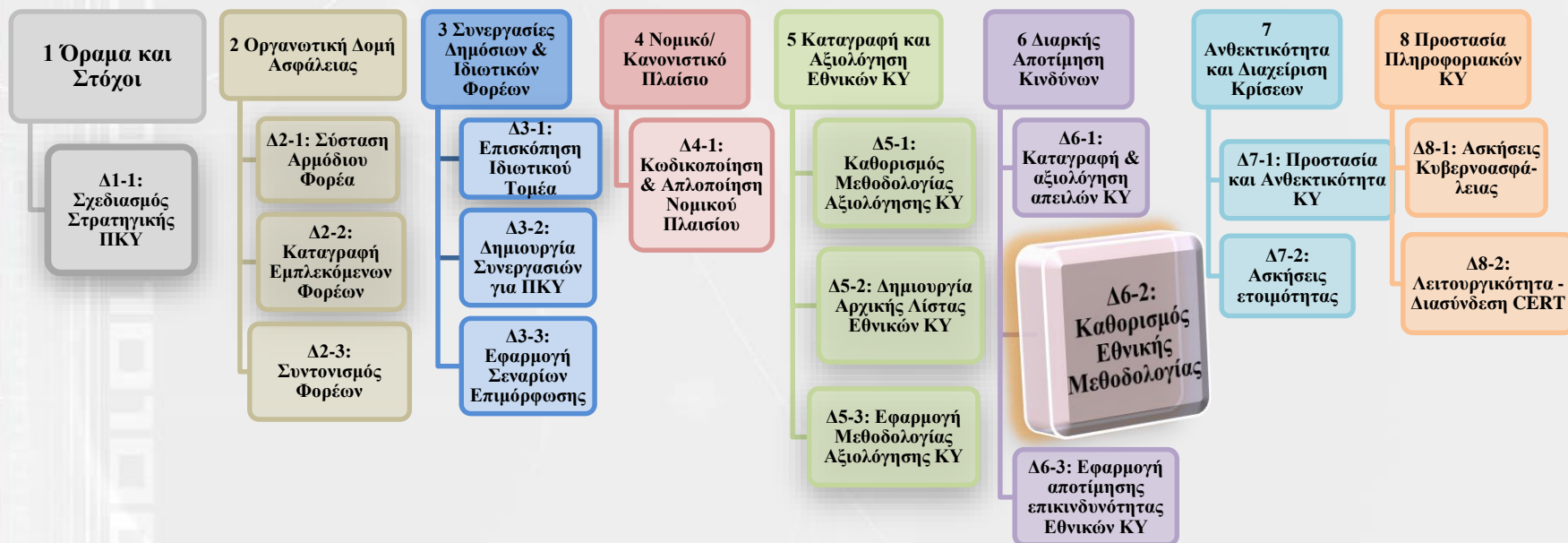
- Φάση Α/Β

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης:

- Το **Παραδοτέο Π2, Κεφ.3** παρουσιάζει μία ενδεικτική εφαρμογή, όπου ήταν δυνατό, της προτεινόμενης μεθοδολογίας σε τρεις βασικούς τομείς ΚΥ (Ενέργεια, ΤΠΕ, Μεταφορές).



Διαρκής Αποτίμηση Κινδύνων: Καθορισμός Εθνικής Μεθοδολογίας Αποτίμησης Κινδύνων



Δράση 6-2: Καθορισμός Εθνικής Μεθοδολογίας Αποτίμησης Κινδύνων

Περίληψη Δράσης:

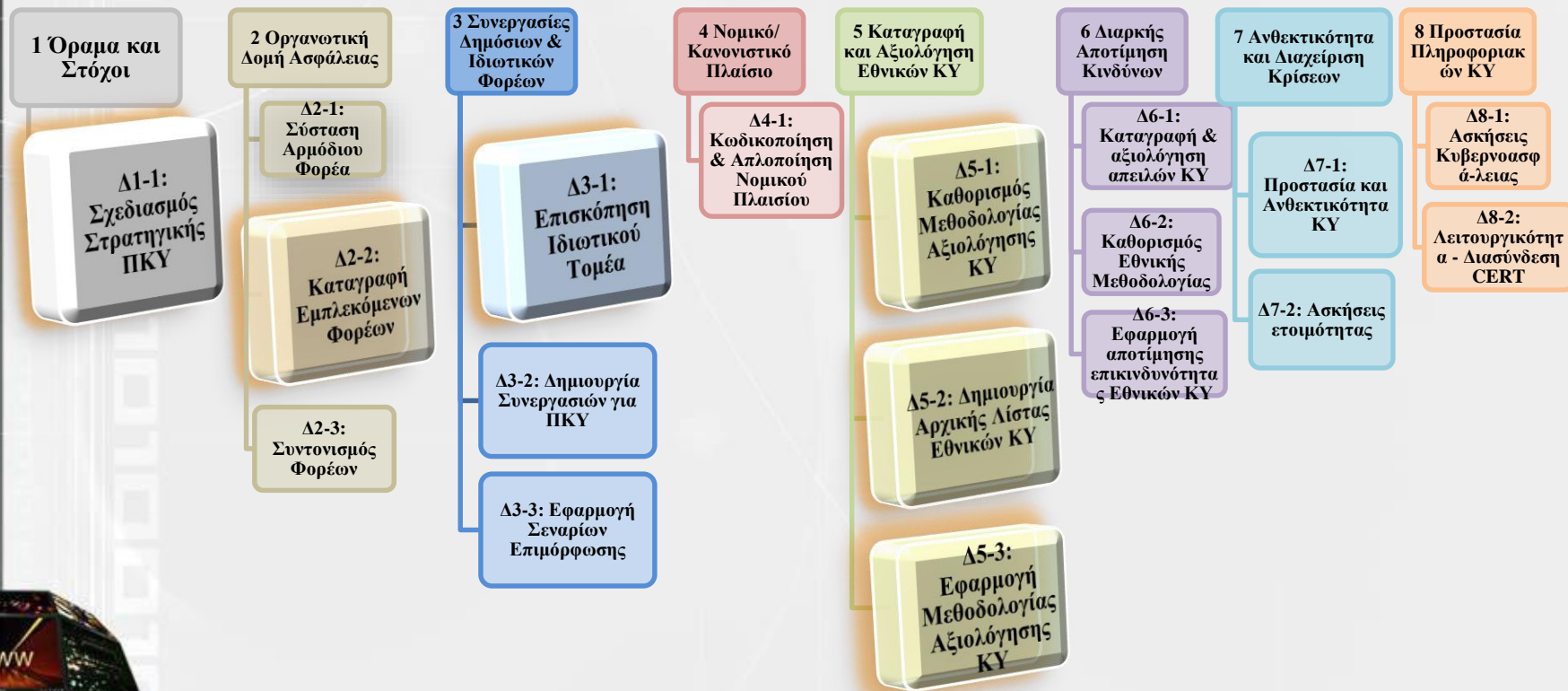
- Προσδιορισμός Εθνικής Μεθοδολογίας Αποτίμησης Επικινδυνότητας ΚΥ
- Σκοπός είναι ο προσδιορισμός των βέλτιστων μέτρων ασφάλειας για τις πιθανές απειλές

Εκτιμώμενος Χρόνος Εφαρμογής:

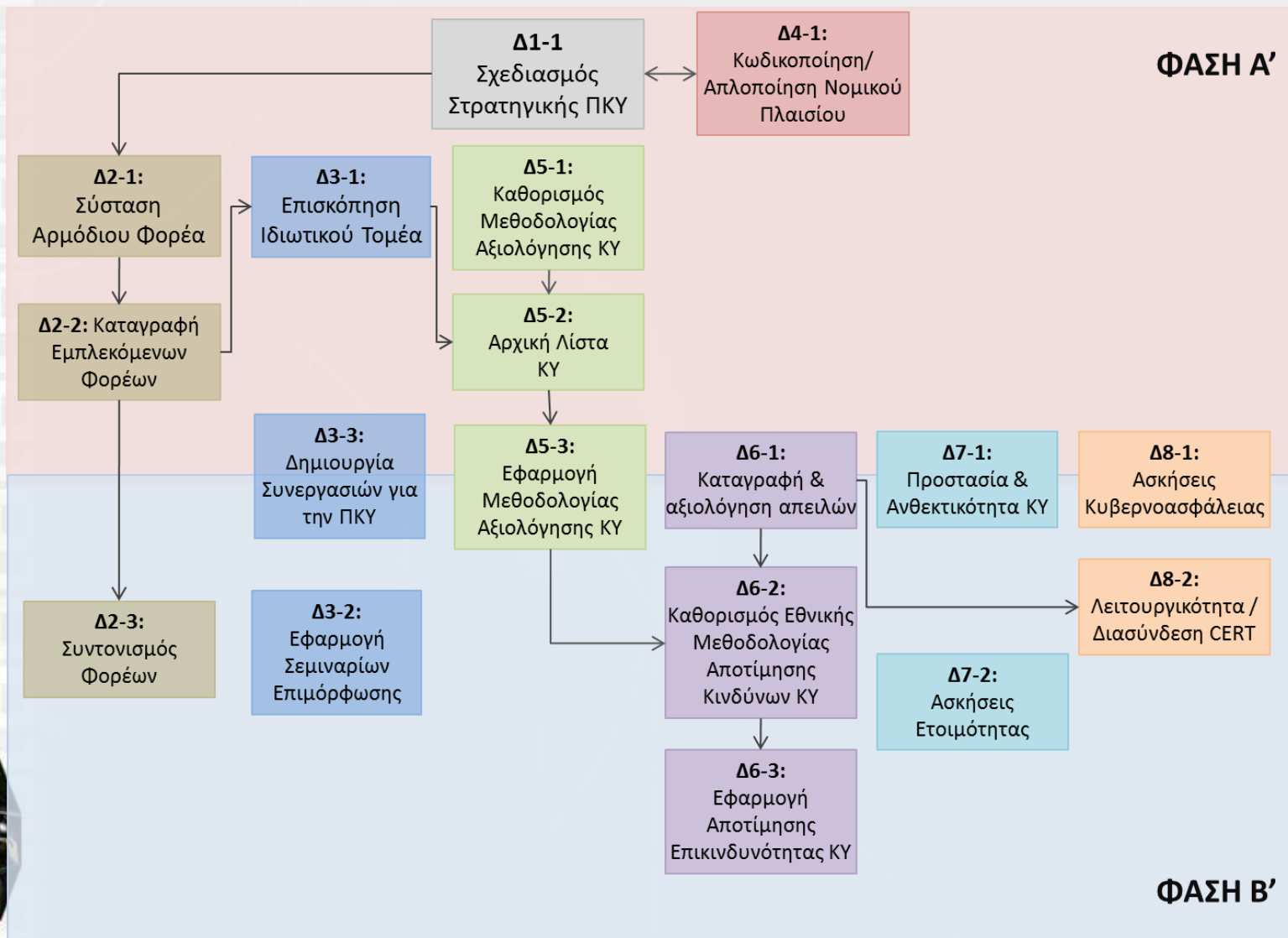
- Φάση Β



Συνεισφορά μελέτης στις προτεινόμενες Δράσεις



Σχέδιο Εφαρμογής (Action Plan)



Αναφορές

1. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", Proc. of the 6th International Workshop on Critical Infrastructure Security, pp. 107-118, Springer, Greece, 2011.
2. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", Critical Information Infrastructure Protection and Resilience in the ICT Sector, pp. 151-170, IGI Global, 2013.
3. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Assessing n-order dependencies between critical infrastructures", International Journal of Critical Infrastructure Protection, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, Proc. of the 7th IFIP Inter-national Conference on Critical Infrastructure Protection, pp. 171-182, Springer, USA, 2013.
5. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-base critical infrastructure dependency analysis for large-scale and cross-sectoral failures", International Journal of Critical Infrastructure Protection, Vol. 12, pp. 46-60, 2016.
6. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", International Journal of Critical Infrastructure Protection, Vol. 10, pp. 34-44, 2015.
7. Stergiopoulos G., Theocharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in Critical Infrastructure Protection IX, pp. 25-40, Springer, 2016.
8. Theocharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", International Journal of Risk Assessment and Management, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
9. Theocharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", Computers & Security, Vol. 29, No. 6, pp. 643-658, 2010.
10. Theocharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in Proc. of the 7th IEEE Inter-national Conference in Global Security, Safety and Sustainability, pp. 171-178, Springer, Greece, 2012.
11. ENISA (2014). R. Mattioli, C. Levy-Bencheton. Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report, December 2014. Retrieved from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis/methodologies-for-the-identification-of-ciis/at_download/fullReport
12. ENISA (2015). Stocktaking, Analysis and Recommendations on the protection of CIIs. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis>
13. Klaver, M. H. A., Luijff, H. A. M., & Nieuwenhuijsen, A. H. (2011). RECIPE: Good practices manual for CIP policies, for policy makers in Europe.