06.2016

διαΝΕΟσις
ΟΡΓΑΝΙΣΜΟΣ ΕΡΕΥΝΑΣ & ΑΝΑΛΥΣΗΣ

Ολιστική Προστασία Κρίσιμων Υποδομών

Μέρος Γ'
Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Ομάδα έργου

Επιστημονική Ομάδα

Δημήτρης Γκρίτζαλης
B.Sc, M.Sc., Ph.D., Καθηγητής, Επιστημονικός Διευθυντής INFOSEC Laboratory, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Πάνος Κοτζανικολάου
B.Sc., Ph.D., Επίκουρος Καθηγητής, Τεχνικός Διευθυντής, Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς

Μάνος Μάγκος
B.Sc., Ph.D., Επίκουρος Καθηγητής,Έμπειρος Ερευνητής, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Γιώργος Στεργιόπουλος
B.Sc., M.Sc., Ph.D., Διδάκτορας Πληροφορικής, Ερευνητής INFOSEC Laboratory, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Γεωργία Λύκου
B.Sc., MBA, M.Sc., Υποψήφια Διδάκτορας Πληροφορικής, Ερευνήτρια INFOSEC Laboratory, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Ομάδα Διαχείρισης

Μίνα Καραγιάννη
B.Sc., M.Sc., Υπεύθυνη Συντονισμού, Διαχείρισης & Επικοινωνίας INFOSEC Laboratory, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Εύα Γούμενου
B.Sc., M.Sc., Διαχειρίστρια Έργου, Ειδικός Λογαριασμός Κονδυλίων Έρευνας Οικονομικού Πανεπιστημίου Αθηνών (ΕΛΚΕ/ΟΠΑ)

Τα αναφερόμενα στο παρόν πόνημα απηχούν, αυστηρά και μόνον, τις προσωπικές απόψεις των μελών της Επιστημονικής Ομάδας. Δεν εκφράζουν, κατ' ανάγκην, ούτε δεσμεύουν με οποιονδήποτε τρόπο κάποιο άλλο φυσικό ή νομικό πρόσωπο.

Η ακρίβεια των περιεχομένων του κειμένου ελέγχθηκε με βάση τους διαθέσιμους πόρους και τα διαθέσιμα μέσα κατά το χρόνο της συγγραφής του. Παρά ταύτα, τυχόν σποραδικές αποκλίσεις από τα κατά περίπτωση ισχύοντα δεν μπορούν να αποκλειστούν και, εάν υπάρχουν, βαρύνουν αποκλειστικά και μόνο τα μέλη της Επιστημονικής Ομάδας.

Περιεχόμενα

ΕΠΙΤΕΛΙΚΗ ΣΥΝΟΨΗ..... 7

Α ΕΙΣΑΓΩΓΗ..... 11

Α1. Στόχοι..... 14

Α2. Περιορισμοί..... 15

Α3. Δομή του Μέρους Γ' της Μελέτης..... 16

Β ΕΠΙΣΚΟΠΗΣΗ ΣΤΡΑΤΗΓΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΣΤΗΝ ΕΕ..... 18

Β1. Ευρωπαϊκή Θεώρηση Προστασίας ΚΥ..... 19

Β2. Καλές Πρακτικές στην ΕΕ..... 21

Β2.1. Οργανωτικό Επίπεδο..... 22

Β2.2. Κανονιστικό Επίπεδο..... 24

Β2.3. Εκτελεστικό/Λειτουργικό Επίπεδο..... 25

Γ ΤΟΜΕΙΣ ΠΡΟΤΕΡΑΙΟΤΗΤΑΣ ΟΛΙΣΤΙΚΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΚΥ..... 30

Γ1. Όραμα/Στόχοι/Σχέδιο Δράσης..... 31

Γ2. Οργανωτική Δομή Διοίκησης Ασφάλειας ΚΥ..... 32

Γ3. Συνεργασία Δημόσιων και Ιδιωτικών Φορέων..... 33

Γ4. Νομικό/Κανονιστικό Πλαίσιο..... 35

Γ5. Καταγραφή και Αξιολόγηση Εθνικών ΚΥ..... 36

Γ6. Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ..... 38

Γ7. Ανθεκτικότητα ΚΥ και Διαχείριση Κρίσεων..... 40

Γ8. Προστασία Πληροφοριακών ΚΥ..... 42

Δ ΠΡΟΤΑΣΗ ΟΛΙΣΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΕΘΝΙΚΩΝ ΚΥ..... 46

Δ1. Όραμα και Στόχοι..... 47

Δ1.1. Δράση 1-1: Σχεδιασμός Στρατηγικής Προστασίας ΚΥ της Ελλάδας..... 47

Δ2. Οργανωτική Δομή Διοίκησης Ασφάλειας ΚΥ....48
Δ2.1. Δράση 2-1: Σύσταση Αρμόδιου Φορέα για την Προστασία των Εθνικών ΚΥ....48
Δ2.2. Δράση 2-2: Καταγραφή των Εμπλεκόμενων Φορέων....49
Δ2.3. Δράση 2-3: Συντονισμός Δράσεων των Εμπλεκόμενων Φορέων....49
Δ3. Συνεργασίες Δημόσιων και Ιδιωτικών Φορέων....50
Δ3.1. Δράση 3-1: Καταγραφή Κατόχων/Διαχειριστών ΚΥ....50
Δ3.2. Δράση 3-2: Δημιουργία Συνεργασιών για την Προστασία των ΚΥ....50
Δ3.3. Δράση 3-3: Εφαρμογή Σεναρίων Επιμόρφωσης....51
Δ4. Νομικό/Κανονιστικό Πλαίσιο....53
Δ4.1. Δράση 4-1: Κωδικοποίηση, Καταγραφή και Απλοποίηση Νομικού Πλαισίου....53
Δ5. Καταγραφή και Αξιολόγηση Εθνικών ΚΥ....54
Δ5.1. Δράση 5-1: Καθορισμός Μεθοδολογίας Προσδιορισμού και Αξιολόγησης ΚΥ....54
Δ5.2. Δράση 5-2: Δημιουργία Αρχικής Λίστας Εθνικών Κρίσιμων Τομέων, Υποτομέων και Υπηρεσιών....55
Δ5.3. Δράση 5-3: Εφαρμογή Μεθοδολογίας Προσδιορισμού και Αξιολόγησης ΚΥ....56
Δ6. Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ....57
Δ6.1. Δράση 6-1: Καταγραφή και Αξιολόγηση Απειλών για τις Εθνικές ΚΥ....57
Δ6.2. Δράση 6-2: Καθορισμός Εθνικής Μεθοδολογίας Αποτίμησης Επικινδυνότητας Εθνικών ΚΥ....57
Δ6.3. Δράση 6-3: Εφαρμογή Αποτίμησης Επικινδυνότητας στις Εθνικές ΚΥ....58
Δ7. Ανθεκτικότητα ΚΥ και Διαχείριση Κρίσεων....59
Δ7.1. Δράση 7-1: Προστασία και Ανθεκτικότητα των ΚΥ....59
Δ7.2. Δράση 7-2: Ασκήσεις Ετοιμότητας και Διαχείρισης Κρίσεων....59
Δ8. Προστασία Πληροφοριακών ΚΥ....60
Δ8.1. Δράση 8-1: Ασκήσεις Κυβερνο-ασφάλειας....60
Δ8.2. Δράση 8-2: Πλήρης Λειτουργικότητα και Διασύνδεση Ελληνικών CERT....60
Δ9. Συνοπτική Παρουσίαση Δομής Προτεινόμενης Πολιτικής Προστασίας Εθνικών ΚΥ....61

Ε ΣΧΕΔΙΟ ΔΡΑΣΗΣ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΟΛΙΣΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΕΘΝΙΚΩΝ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ.....64

ΣΤ ΣΥΜΠΕΡΑΣΜΑΤΑ.....67

ΕΝΝΟΙΟΛΟΓΙΚΗ ΟΡΙΟΘΕΤΗΣΗ.....69
ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ/ΠΙΝΑΚΩΝ.....72
ΒΙΒΛΙΟΓΡΑΦΙΑ/ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ.....74

Ακρωνύμια

ΑΔΑΕ	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
ΕΕ	Ευρωπαϊκή Ένωση
ENISA	European Network and Information Security Agency
Κ-Μ	Κ-Μ
PPP	Public Private Partnerships
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΕΕΘΑ	Γενικό Επιτελείο Εθνικής Άμυνας
ΔΔ	Δημόσια Διοίκηση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΚΥ	Ευρωπαϊκές Κρίσιμες Υποδομές
ΕΛΑΣ	Ελληνική Αστυνομία
ΕΠΠΥΖΣ	Ευρωπαϊκό Πρόγραμμα για την Προστασία Υποδομών Ζωτικής Σημασίας (EPCIP)
ΕΥΠ	Εθνική Υπηρεσία Πληροφοριών
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΚΕΜΕΑ	Κέντρο Μελετών Ασφάλειας
ΟΛΙΚΥ	Ολιστική Προστασία Κρίσιμων Υποδομών: Ανθεκτικότητα & Προστασία Διασυνδέσεων
ΠΚΥ	Προστασία Κρίσιμων Υποδομών (CIP)
ΠΣ	Πληροφοριακά Συστήματα
ΠΣΕΑ	Πολιτική Σχεδίαση Έκτακτης Ανάγκης
ΡΑΕ	Ρυθμιστική Αρχή Ενέργειας
ΡΑΣ	Ρυθμιστική Αρχή Σιδηροδρόμων
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΥΑΠ	Υπηρεσία Ανάπτυξης Πληροφορικής
ΥΔΤ	Υπουργείο Δημόσιας Τάξης
ΥΖΣ	Υποδομές Ζωτικής Σημασίας
ΥΠΑ	Υπηρεσία Πολιτικής Αεροπορίας
ΥΠΕ	Υποδομές Πληροφορικής και Επικοινωνιών
ΥΠΕΣ	Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΥΠΖΣ	Υποδομές Πληροφορίας Ζωτικής Σημασίας
ΥΠΟΜΕΔΙ	Υπουργείο Υποδομών, Μεταφορών και Δικτύων

Επιτελική Σύνοψη

Τα Μέρη Α' και Β' της επιστημονικής μελέτης εστίασαν στην καταγραφή της παρούσας κατάστασης στην Ελλάδα σχετικά με την προστασία των Κρίσιμων Υποδομών, σε σχέση και με το ευρωπαϊκό γίγνεσθαι (Μέρος Α'), καθώς και στην πρόταση μιας μεθοδολογίας αξιολόγησης των ΚΥ (Μέρος Β').

Ειδικότερα, στο Μέρος Α' της έρευνας πραγματοποιήθηκε μια επισκόπηση των καλών ευρωπαϊκών πρακτικών για τον εντοπισμό των υποψήφιων ΚΥ, καθώς και για την αξιολόγηση της κρισιμότητας τόσο των ενδεχόμενων κρίσιμων υπηρεσιών, ανά τομέα/υποτομέα όσο και των αγαθών που απαρτίζουν μια κρίσιμη υπηρεσία. Επιπλέον, έγινε καταγραφή των υποψήφιων ΚΥ στους επιλεγμένους τομείς Ενέργειας, Μεταφορών και Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) –όπου επικεντρώνεται η Οδηγία 114/2008/ΕΚ– ως υποψήφιων ευρωπαϊκών ΚΥ (ΕΚΥ).

Στο Μέρος Β' ορίστηκε μια γενική μεθοδολογία αξιολόγησης των υποψήφιων ΚΥ και ορίστηκαν κριτήρια αξιολόγησης, ενώ η προτεινόμενη μεθοδολογία εφαρμόστηκε ενδεικτικά στους τρεις τομείς που καταγράφηκαν στο Μέρος Α'.

Σκοπός του Μέρους Γ' της μελέτης είναι η πρόταση μιας γενικής και εφαρμόσιμης εθνικής πολιτικής για την προστασία των Κρίσιμων Υποδομών της χώρας.

Οι βασικοί στόχοι της προτεινόμενης πολιτικής είναι:

- Να λάβει υπόψη τις βέλτιστες πρακτικές και τις υφιστάμενες πολιτικές άλλων χωρών, οι οποίες έχουν ήδη εκπονήσει και εφαρμόσει αντίστοιχες πολιτικές προστασίας των Κρίσιμων Υποδομών τους.

- Να λάβει υπόψη τη σχετική νομοθεσία, τις εθνικές ιδιαιτερότητες, το πλαίσιο λειτουργίας και τα συγκεκριμένα χαρακτηριστικά των Κρίσιμων Υποδομών της Ελλάδας.

- Να αξιοποιήσει και να εντάξει στην προτεινόμενη πολιτική πιθανές υφιστάμενες δράσεις, οι οποίες ενδεχομένως ήδη εφαρμόζονται από φορείς

που εμπλέκονται στους τομείς της πολιτικής προστασίας και ανθεκτικότητας των Κρίσιμων Υποδομών.

- Να αξιοποιήσει και να εντάξει στην προτεινόμενη πολιτική τα αποτελέσματα των Μερών Α' και Β' της μελέτης, με σαφή και δομημένο τρόπο.

- Να προτείνει ένα ρεαλιστικό σχέδιο εφαρμογής (action plan) της προτεινόμενης πολιτικής.

Δεδομένων των περιορισμών της ομάδας μελέτης, τόσο η προτεινόμενη πολιτική όσο και το σχέδιο εφαρμογής δεν μπορούν να θεωρηθούν ως οριστικές και ανελαστικές προτάσεις άμεσης εφαρμογής, τουλάχιστον όπως εμφανίζονται στην παρούσα μορφή τους. Φιλοδοξία της ερευνητικής ομάδας είναι η προτεινόμενη πολιτική να αποτελέσει χρήσιμο οδηγό για τον εκάστοτε αρμόδιο φορέα και να λειτουργήσει καταλυτικά για την εκπόνηση και άμεση εφαρμογή μιας Ολιστικής Πολιτικής Προστασίας των Κρίσιμων Υποδομών και μιας Ολοκληρωμένης Πολιτικής Κυβερνοασφάλειας της χώρας, εν γένει.

Το περιεχόμενο του Μέρους Γ' της μελέτης δομείται ως εξής:

Στην Ενότητα Α, **«Εισαγωγή»**, αναλύονται οι βασικοί στόχοι και οι περιορισμοί του Μέρους Γ'.

Στην Ενότητα Β, **«Επισκόπηση Στρατηγικών Προστασίας Κρίσιμων Υποδομών στην Ε.Ε.»**, αναλύονται οι πολιτικές και η στρατηγική που εφαρμόζεται σε χώρες της Ε.Ε., λαμβάνοντας υπόψη τις καλές πρακτικές αυτών των χωρών και οι οποίες μελετήθηκαν στην Ενότητα Β του Μέρους Α'.

Στην Ενότητα Γ, **«Τομείς Προτεραιότητας μιας Ολιστικής Στρατηγικής Προστασίας ΚΥ»**, ορίζονται οι κύριοι τομείς προτεραιότητας, οι οποίοι θα πρέπει, σύμφωνα με τη μελέτη των πρακτικών άλλων χωρών που διερευνήθηκαν, να αποτελέσουν τους κύριους άξονες μιας Εθνικής Στρατηγικής Προστασίας ΚΥ.

Στην Ενότητα Δ, **«Πρόταση Ολιστικής Πολιτικής Προστασίας Εθνικών ΚΥ»**, προδιαγράφεται ένα σχέδιο μιας Ολιστικής Πολιτικής Προστασίας των ΚΥ της χώρας μας. Το προτεινόμενο σχέδιο πολιτικής βασίζεται στους τομείς προτεραιότητας που ορίστηκαν στην προηγούμενη ενότητα και επιπρόσθετα ορίζει συγκεκριμένες και εφαρμόσιμες δράσεις για τη σταδιακή και δομημένη υλοποίηση της προτεινόμενης πολιτικής. Βασικό στοιχείο του προτεινόμενου σχεδίου είναι η προσπάθεια να ληφθούν υπόψη και να ενταχθούν στην προτεινόμενη πολιτική όλες οι σχετικές υφιστάμενες δράσεις του δημόσιου και του ιδιωτικού τομέα, αλλά και οι προτάσεις που έγιναν στα Μέρη Α' και Β' της μελέτης.

Στην Ενότητα Ε, **«Σχέδιο Δράσης για την Προστασία των Εθνικών ΚΥ»**, προτείνεται ένα γενικό Σχέδιο Δράσης (generic Action Plan), με σκοπό την παροχή οδηγιών ως προς τα στάδια και τις χρονικές προτεραιότητες υλοποίησης των δράσεων της προτεινόμενης πολιτικής.

Στην Ενότητα ΣΤ συνοψίζονται τα **βασικά συμπεράσματα του έργου.**

Τα βασικότερα συμπεράσματα που προέκυψαν από την εκπόνηση του παρόντος μέρους της μελέτης είναι τα εξής:

- Τα βασικά θεμέλια μιας πολιτικής Ολιστικής Προστασίας ΚΥ είναι ο καθορισμός ενός δομημένου πλαισίου προστασίας και ασφάλειας των Κρίσιμων Υποδομών.

- Ένα τέτοιο πλαίσιο προϋποθέτει την υιοθέτηση στρατηγικών στόχων (Όραμα), των οποίων η επίτευξη θα στηρίζεται σε αυστηρά καθορισμένους Τομείς Προτεραιότητας.

- Οι βασικοί τομείς προτεραιότητας μιας Στρατηγικής Ολιστικής Προστασίας των ΚΥ είναι:

Σε **Οργανωτικό** επίπεδο:

Καθορισμός Οράματος και Μετρήσιμων Στόχων
Καθορισμός Οργανωτικής Δομής Διοίκησης για την προστασία Κρίσιμων Υποδομών
Καθορισμός Συνεργασιών Κράτους και Ιδιωτικών Φορέων

Σε **Κανονιστικό** επίπεδο:

Καθορισμός του σχετικού Νομικού και Κανονιστικού Πλαισίου

Σε **Εκτελεστικό/Λειτουργικό** επίπεδο:

Καταγραφή και Αξιολόγηση Εθνικών ΚΥ
Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ
Διαχείριση Ανθεκτικότητας ΚΥ και Διαχείριση Κρίσεων
Προστασία Πληροφοριακών ΚΥ

- Οι τομείς Προτεραιότητας της Πολιτικής υλοποιούνται μέσα από συγκεκριμένες και εφαρμόσιμες δράσεις (actions), οι οποίες θα πρέπει να είναι σαφώς ορισμένες και να έχουν μετρήσιμους στόχους. Δεδομένου τούτου, το Μέρος Γ' εμπεριέχει έναν σαφή καθορισμό ανάλογων δράσεων.

- Η υλοποίηση της Πολιτικής Προστασίας Κρίσιμων Υποδομών επιτυγχάνεται μέσω ενός Σχεδίου Δράσης, το οποίο θέτει ένα σαφές και ορισμένο χρονοδιάγραμμα εκτέλεσης των επιμέρους δράσεων. Το προτεινόμενο στο Μέρος Γ' σχέδιο θα μπορούσε να αποτελέσει ένα χρήσιμο οδηγό για την αρμόδια Αρχή, ώστε να καθορίσει ένα ρεαλιστικό Σχέδιο Δράσης.

ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Εισαγωγή

Α. Εισαγωγή

Ο προσδιορισμός και η αξιολόγηση των εθνικών ΚΥ αποτελούν ευρωπαϊκή προτεραιότητα. Αυτό αποδεικνύεται, τόσο από μια σειρά θεσμικών ευρωπαϊκών κειμένων και πρωτοβουλιών, όσο και από την ουσιαστική εφαρμογή εθνικών στρατηγικών προστασίας των ΚΥ από τα περισσότερα Κ-Μ της Ευρωπαϊκής Ένωσης, τα οποία αντιμετωπίζουν μοναδικές προκλήσεις στον τομέα της πολιτικής προστασίας των ΚΥ (CIP).

Στη διάρκεια των τελευταίων ετών, η Ευρωπαϊκή Επιτροπή έχει υιοθετήσει μια σειρά από πρωτοβουλίες σε αυτόν τον τομέα, συμπεριλαμβανομένων των Οδηγιών και εγγράφων επικοινωνίας για την προώθηση της βελτίωσης της ετοιμότητας, της ασφάλειας και της ανθεκτικότητας. Ωστόσο, μια σειρά από εκκρεμή προβλήματα, τα οποία αναφέρονται παρακάτω, παραμένουν (CEPS, CIP REPORT):

- Τα Κ-Μ βρίσκονται σε διαφορετικό βαθμό ωριμότητας σε σχέση με την ανάπτυξη μιας ολοκληρωμένης στρατηγικής προστασίας των ΚΥ.

- Αν και υπάρχουν ψήγματα συνεργασίας μεταξύ των Κ-Μ της Ευρωπαϊκής Ένωσης, δεν υπάρχει συνολικό πλαίσιο συνεργασίας σε επίπεδο Ευρωπαϊκής Ένωσης.

- Οι εταιρικές σχέσεις και συνεργασίες μεταξύ των εμπλεκόμενων φορέων στην προστασία των ΚΥ είναι διαφορετικές ανά χώρα, ανάλογα με τις ιδιαιτερότητες τόσο της χώρας όσο και των ΚΥ της.

- Οι Κρίσιμες Υποδομές της Ευρωπαϊκής Ένωσης είναι διάσπαρτες γεωγραφικά και συχνά εμφανίζουν αλληλεξαρτήσεις, οι οποίες ενίοτε επηρεάζουν έναν αριθμό Κ-Μ.

Η προστασία των ΚΥ στη χώρα μας απέχει σημαντικά από το ευκταίο επίπεδο, τόσο τυπικά όσο και επί της ουσίας. Η Ελλάδα παραμένει μια από τις ελάχιστες χώρες στην Ευρωπαϊκή Ένωση η οποία έχει μεν τυπικά ενσωματώσει τη σχετική Ευρωπαϊκή Οδηγία (114/ 2008/ΕΚ) στην εθνική της νομοθεσία, ωστόσο δεν διαθέτει κάποια στρατηγική προστασίας των εθνικών ΚΥ.

Με βάση τα συμπεράσματα του Μέρους Α' της μελέτης, η απουσία αφενός της καταγραφής και της αξιολόγησης/ιεράρχησης των εθνικών ΚΥ και αφετέρου των σχετικών διασυνδέσεων και αλληλεξαρτήσεων οδηγεί σε αποσπασματικά και ελλιπή μέτρα προστασίας των ΚΥ. Παρότι υπάρχουν μέτρα ασφάλειας για την προστασία των φυσικών υποδομών και των πληροφοριακών συστημάτων, τα οποία υλοποιούνται από μεγάλους οργανισμούς, όπως οι Χειριστές (Operators) των ΚΥ, στο πλαίσιο της Πολιτικής Ασφάλειας κάθε οργανισμού, είναι σαφές ότι η εφαρμογή μεμονωμένων Σχεδίων Ασφάλειας χωρίς εθνική στρατηγική ασφάλειας των ΚΥ δεν επαρκεί. Αυτό οφείλεται σε πολλούς λόγους, όπως:

- Η απουσία συστηματικής καταγραφής και ιεράρχησης των εθνικών ΚΥ οδηγεί σε αποσπασματική και *ad hoc* αξιολόγηση των διασυνδέσεων των ΚΥ. Συνεπώς υπάρχει μια αδυναμία ουσιαστικής αξιολόγησης των αλληλεξαρτήσεων μεταξύ των ΚΥ, η οποία έχει ως συνεπακόλουθο την αδυναμία ολιστικής αξιολόγησης των πιθανών συνεπειών από την προσβολή μιας ΚΥ.

- Το «άθροισμα» των μεμονωμένων Πολιτικών Ασφάλειας των διαχειριστών των ΚΥ δεν μπορεί να προσφέρει επαρκή προστασία των εθνικών ΚΥ. Διότι όσο αποτελεσματική και αν είναι μια Πολιτική Ασφάλειας ενός οργανισμού για την προστασία των κινδύνων ασφάλειας που αφορούν τον οργανισμό, δεν στοχεύει (δεν οφείλει να το κάνει, λόγω του εύρους της) στην προστασία κινδύνων ασφάλειας που ενδεχομένως να εκδηλωθούν σε εξωτερικούς οργανισμούς, φορείς ή στο ευρύτερο κοινωνικό σύνολο.

- Η διεθνής βιβλιογραφία, όσο και η πραγματικότητα, έχουν δείξει ότι λόγω των αλληλεξαρτήσεων μεταξύ των ΚΥ η εκδήλωση μιας απειλής ή αστοχίας σε μια ΚΥ πολύ συχνά οδηγεί σε διαδοχικές συνέπειες (cascading impact) στις διασυνδεδεμένες ΚΥ, οι οποίες –με τη σειρά τους– προκαλούν νέες συνέπειες στις δικές τους διασυνδεδεμένες ΚΥ, οδηγώντας σε αθροιστικές συνέπειες μεγάλης κλίμακας. Τέτοια φαινόμενα μπορούν συστηματικά να υποδειγματοποιηθούν μόνο μέσα από μια ολιστική προσέγγιση ασφάλειας.

Σε εθνικό επίπεδο υπάρχουν αρκετοί και σημαντικοί φορείς, οι οποίοι αναφέρθηκαν αναλυτικά στην Ενότητα Γ του Μέρους Α' της μελετης και έχουν αρμοδιότητες σχετικές με την προστασία των ΚΥ, όπως είναι το ΚΕΜΕΑ, η ΠΣΕΑ και το ΓΕΕΘΑ. Επιπλέον, Ανεξάρτητες και Ρυθμιστικές Αρχές ανά τομέα (π.χ. ΑΔΑΕ, ΑΠΔΠΧ, ΕΕΤΤ, ΡΑΕ, ΔΕΔΙΕ, ΡΑΣ κ.λπ.) διαθέτουν σχετική τεχνογνωσία και, αν δεν διαδραματίζουν ήδη, ενδέχεται να διαδραματίσουν αξιοσημείωτο ρόλο στον προσδιορισμό και στην προστασία των εθνικών ΚΥ.

Στο Μέρος Β' της μελέτης περιγράφηκε μια μεθοδολογία αξιολόγησης των πιθανών εθνικών ΚΥ, συνοδευόμενη από την πρακτική εφαρμογή της σε κρίσιμους τομείς, υποτομείς και υπηρεσίες. Η προτεινόμενη μεθοδολογία περιλάμβανε –με τη μορφή καλώς ορισμένων βημάτων– όλες τις ανα-

γκαίες διαδικασίες εντοπισμού και αξιολόγησης των ΚΥ που πρέπει να εφαρμοστούν από τους εκάστοτε αρμόδιους εθνικούς φορείς, στο πλαίσιο μιας εθνικής στρατηγικής προστασίας των εθνικών ΚΥ. Επιπλέον, περιλάμβανε, κατάλληλα κριτήρια αξιολόγησης, καθώς και αντίστοιχες κλίμακες για κάθε κριτήριο, με σκοπό τη στοιχειοθετημένη ένταξη υποδομών σε επίπεδα κρισιμότητας. Η μεθοδολογία εφαρμόστηκε στην πράξη για την αξιολόγηση ορισμένων κρίσιμων υπηρεσιών, ανά υποτομέα. Η εφαρμογή των κριτηρίων αξιολόγησης έγινε σε τρεις τομείς σημαντικού εθνικού ενδιαφέροντος, που επελέγησαν ως οι πιο κρίσιμοι για τη χώρα μας (Ενέργεια, Μεταφορές και ΤΠΕ).

Στο παρόν μέρος της μελέτης αξιολογούνται τα βασικά συμπεράσματα που προέκυψαν από την εφαρμογή κριτηρίων αξιολόγησης των ΚΥ και γίνεται μια επισκόπηση των στρατηγικών που εφαρμόζονται σε άλλες χώρες της Ε.Ε., με στόχο τη διαμόρφωση μιας πρότασης ολιστικής πολιτικής ασφάλειας των ΚΥ. Οι βασικοί στόχοι του Μέρους Γ' αναλύονται στην επόμενη ενότητα, όπου περιγράφεται το γενικό πλαίσιο στο οποίο εντάσσεται η χάραξη Στρατηγικής και Προτάσεων Ολιστικής Προστασίας των εθνικών ΚΥ. Επίσης, περιγράφονται οι υφιστάμενοι περιορισμοί και η δομή του.

Α1. Στόχοι

Το παρόν αποτελεί το Γ' Μέρος της μελέτης. Οι βασικοί στόχοι του είναι:

- Η επισκόπηση των βέλτιστων πρακτικών και κάποιων επιλεγμένων πολιτικών προστασίας ΚΥ χωρών που έχουν ήδη εκπονήσει ή/και εφαρμόσει πολιτικές προστασίας Κρίσιμων Υποδομών.

- Η πρόταση βασικών στρατηγικών στόχων και προτεραιοτήτων που θα πρέπει να διαθέτει μια τομεακή Στρατηγική Ολιστικής Προστασίας των εθνικών ΚΥ.

- Η περιγραφή και η ανάλυση μιας πρότασης για μια Ολιστική Πολιτική Προστασίας των ΚΥ της χώρας μας, μέσω τεχνικών, λειτουργικών και οργανωτικών οδηγιών και προτάσεων. Βασικοί στόχοι της προτεινόμενης πολιτικής είναι:

  Να αξιοποιήσει και να εντάξει πιθανές υφιστάμενες δράσεις, οι οποίες ενδεχομένως ήδη εφαρμόζονται από διάφορους φορείς που εμπλέκονται στους διάφορους τομείς της πολιτικής προστασίας και ανθεκτικότητας των ΚΥ.

  Να αξιοποιήσει και να εντάξει στην προτεινόμενη πολιτική τα αποτελέσματα των προηγούμενων παραδοτέων του έργου, με σαφή και δομημένο τρόπο.

  Να προτείνει ένα ρεαλιστικό σχέδιο εφαρμογής (action plan) της προτεινόμενης πολιτικής.

Α2. Περιορισμοί

Η παρούσα πρόταση σχεδιάστηκε και υλοποιήθηκε, λαμβάνοντας υπόψη μία σειρά από περιορισμούς που αφορούν τόσο τα δεδομένα/πληροφορίες που η μελέτη αυτή κλήθηκε να επεξεργαστεί, όσο και τη γνώση που καλείται να πράξει. Οι περιορισμοί αυτοί είτε προέκυψαν κατά τη διεξαγωγή της έρευνας είτε αυτο-επιβλήθηκαν εκ προοιμίου, εξαιτίας της φύσης και του αντικειμένου της διεξαχθείσας μελέτης.

Στο σημείο αυτό πρέπει να τονιστεί ότι επ' ουδενί η ερευνητική ομάδα δεν επιθυμεί να υποκαταστήσει τους εντεταλμένους και αρμόδιους εθνικούς φορείς, οι οποιοι καλούνται να εμπλακούν στο σχεδιασμό, στη χάραξη της στρατηγικής και στην υλοποίηση του εθνικού προγράμματος προστασίας των εθνικών ΚΥ.

Η προτεινόμενη Πολιτική Ασφάλειας ΚΥ θα διέπεται από γενικά αλλά ευπροσάρμοστα μέτρα ασφάλειας (όπως είναι τεχνικές και οργανωτικές οδηγίες ασφάλειας) και θα λαμβάνει υπόψη τόσο προβλήματα ασφάλειας των ΚΥ όσο και την εθνική και ευρωπαϊκή νομοθεσία.

Α3. Δομή του Μέρους Γ' της Μελέτης

Το Μέρος Γ' της μελέτης δομείται ως εξής:

Στην Ενότητα Α, **«Εισαγωγή»**, αναλύονται οι βασικοί στόχοι και περιορισμοί του που ισχύουν για το Μέρος Γ' της μελέτης..

Στην Ενότητα Β, **«Επισκόπηση Στρατηγικών Προστασίας Κρίσιμων Υποδομών στην Ε.Ε.»**, γίνεται στοχευμένη επισκόπηση των πολιτικών και της στρατηγικής που εφαρμόζονται από άλλες χώρες της Ε.Ε., λαμβάνοντας υπόψη και τις καλές πρακτικές αυτών των χωρών, και οι οποίες μελετήθηκαν στην Ενότητα Β του Μέρους Α' της μελέτης.

Στην Ενότητα Γ, **«Τομείς Προτεραιότητας μιας Ολιστικής Στρατηγικής Προστασίας ΚΥ»,** παρουσιάζονται συγκεκριμένοι τομείς προτεραιότητας, οι οποίοι, σύμφωνα και με τη μελέτη των πρακτικών άλλων χωρών που διερευνήθηκαν, προτείνεται να αποτελέσουν τους κύριους άξονες μιας Ολιστικής Πολιτικής Προστασίας των εθνικών ΚΥ.

Στην Ενότητα Δ, **«Πρόταση Ολιστικής Πολιτικής Προστασίας Εθνικών ΚΥ»**, προδιαγράφεται ένα σχέδιο μιας Ολιστικής Πολιτικής Προστασίας των ΚΥ της χώρας μας. Το προτεινόμενο σχέδιο πολιτικής βασίζεται στους τομείς προτεραιότητας που ορίστηκαν στην προηγούμενη ενότητα και επιπρόσθετα ορίζει συγκεκριμένες και εφαρμόσιμες δράσεις, με σκοπό τη σταδιακή και δομημένη υλοποίηση της προτεινόμενης πολιτικής. Σημαντικό στοιχείο του προτεινόμενου σχεδίου είναι η συνειδητή προσπάθεια να ληφθούν υπόψη και να ενταχθούν στην προτεινόμενη πολιτική όλες οι σχετικές υφιστάμενες δράσεις του δημόσιου και του ιδιωτικού τομέα, καθώς επίσης και οι σχετικές προτάσεις που έγιναν στα προηγούμενα παραδοτέα του έργου.

Στην Ενότητα Ε, **«Σχέδιο Δράσης για την Προστασία των Εθνικών ΚΥ»**, προτείνεται ένα γενικό Σχέδιο Δράσης (generic Action Plan), με σκοπό την παροχή οδηγιών ως προς τα στάδια και τις χρονικές προτεραιότητες υλοποίησης των δράσεων της προτεινόμενης πολιτικής.

Στην Ενότητα ΣΤ συνοψίζονται τα **βασικά συμπεράσματα** του έργου.

ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Επισκόπηση Στρατηγικών Προστασίας Κρίσιμων Υποδομών στην Ε.Ε.

Β

Β. Επισκόπηση Στρατηγικών Προστασίας Κρίσιμων Υποδομών στην Ε.Ε.

Σε αυτή την ενότητα γίνεται μια επισκόπηση των εθνικών στρατηγικών και δράσεων άλλων χωρών της Ε.Ε. αναφορικά με τη χάραξη μιας πολιτικής προστασίας των Κρίσιμων Υποδομών τους, χρησιμοποιώντας την υπάρχουσα βιβλιογραφία/δικτυογραφία και αξιοποιώντας δημόσιες πηγές. Επιπλέον, αναφέρονται οι καλές πρακτικές χωρών της Ε.Ε. σε διάφορους τομείς προτεραιότητας σχετικά με την προστασία των εθνικών ΚΥ τους.

Β1. Ευρωπαϊκή Θεώρηση Προστασίας ΚΥ

Η βασική αρχή για την προστασία των κρίσιμων υποδομών, διατυπωμένη τόσο στην Πράσινη Βίβλο (EU Commission, 2005) περί ενός Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών (EPCIP), όσο και σε ύστερα θεσμικά κείμενα (EU Commission, 2006; EU Council, 2007), είναι ότι κάθε Κ-Μ (Κ-Μ) είναι υπεύθυνο να αναπτύξει ένα εθνικό πρόγραμμα προστασίας των ΚΥ που διαθέτει. Προς αυτή την κατεύθυνση, έχει κατά καιρούς προταθεί ένα σύνολο από γενικές αρχές και οδηγίες, τόσο σε θεσμικό επίπεδο (π.χ. EU Council, 2008; 2008b; EU Commission, 2012, 2013) όσο και από τους εκάστοτε αρμόδιους διεθνείς φορείς για την προστασία των ΚΥ (ENISA, 2014).

Από τη διεθνή εμπειρία, την ευρωπαϊκή βιβλιογραφία (π.χ. Luiijf, 2003; Nečesal & Lukáš, 2011; Novotný et al., 2015), τα ευρωπαϊκά θεσμικά κείμενα (π.χ. Hammerli & Renda, 2010; Klaver et al., 2011, ENISA, 2014; ENISA, 2015), τις διαθέσιμες στρατηγικές και διεθνείς πρακτικές σε επίπεδο Κ-Μ (π.χ. FRG, 2009; FC, 2009, 2009b; UK, 2010; SG, 2011; MSB, 2011, 2014; FOCP, 2013), η Προστασία των ΚΥ σε εθνικό επίπεδο γίνεται κατανοητή ως μια αλληλεπίδραση των διαφόρων τομέων προτεραιότητας που συμβάλλουν σε μια αποτελεσματική στρατηγική ολιστικής προστασίας των ΚΥ. Οι εν λόγω τομείς δράσης είναι:

Όραμα/Στόχοι: Η ανάπτυξη κάθε στρατηγικής Προστασίας ΚΥ προϋποθέτει την κατάρτιση των στρατηγικών στόχων (Όραμα), που αναλύονται σε επιμέρους μετρήσιμους στόχους.

Διοίκηση Ασφάλειας ΚΥ: Η δομή της διοίκησης/διακυβέρνησης αφορά τον καθορισμό των αρμόδιων και εντεταλμένων φορέων για την προστασία των ΚΥ, τον καθορισμό ρόλων και αρμοδιοτήτων ανά φορέα και, τέλος, το πλαίσιο συνεργασίας μεταξύ δημόσιων και ιδιωτικών φορέων.

Συνεργασίες Δημόσιου-Ιδιωτικού Τομέα: Κάθε εθνικό πρόγραμμα προστασίας προϋποθέτει τη συνεργασία των εμπλεκόμενων μερών (EU Commission, 2005), και πιο συγκεκριμένα τη συνεργασία δημόσιου-ιδιωτικού τομέα (Public-Private Partnership, PPP), συμπεριλαμβανομένων των δημόσιων φορέων και των κατόχων/χειριστών των ΚΥ.

Ανταλλαγή Πληροφοριών: Η ανταλλαγή πληροφοριών αναφέρεται στην ενημερότητα των απειλών/ευπαθειών, στην εξασφάλιση έγκαιρης προειδοποίησης προς τους εμπλεκόμενους φορείς και γενικότερα στην αλληλοενημέρωση και στην επαρκή γνώση των κινδύνων και των απειλών.

Νομοθετικό/Κανονιστικό πλαίσιο: Η θέσπιση νόμων αποτελεί σημαντικό εργαλείο για την εξασφάλιση, μεταξύ άλλων, ότι οι δημόσιοι και ιδιωτικοί φορείς ανταποκρίνονται στους ρόλους και στις αρμοδιότητές τους, καθώς και ότι τηρούν συγκεκριμένα πρότυπα ασφάλειας.

Προσδιορισμός και Αξιολόγηση Εθνικών ΚΥ: Ο προσδιορισμός και η αξιολόγηση των εθνικών κρίσιμων στοιχείων (τομέων, υποτομέων, υπηρεσιών και συγκεκριμένων υποσυστημάτων) αποτελούν προϋπόθεση για την υλοποίηση των πολιτικών προστασίας των εθνικών ΚΥ. Σημαντικό κριτήριο για την κατηγοριοποίηση των ΚΥ αποτελεί, μεταξύ άλλων, ο βαθμός και η σπουδαιότητα των διασυνδέσεων και αλληλεξαρτήσεων μεταξύ των ΚΥ.

Αποτίμηση Κινδύνων: Πρωταρχικό στοιχείο της στρατηγικής προστασίας ΚΥ είναι η μεθοδική αξιολόγηση των απειλών και η αποτίμηση των συνεπαγόμενων κινδύνων ασφάλειας των εθνικών ΚΥ.

Διαχείριση Κινδύνων και Κρίσεων: Τα μέτρα απόκρισης σε περιστατικά ασφάλειας που συνιστούν έκτακτη ανάγκη εξασφαλίζουν τη συνέχεια λειτουργίας ή τη γρήγορη επανάκαμψη του κρίσιμου στοιχείου.

Β2. Καλές Πρακτικές στην Ε.Ε.

Τα τελευταία χρόνια, σε συνέχεια ή ως επιστέγασμα μίας σειράς θεσμικών ευρωπαϊκών πρωτοβουλιών (EU Commission (2005, 2006, 2012, 2013); EU Council (2007, 2008)), τα περισσότερα Κ-Μ διαθέτουν ή σχεδιάζουν ή βρίσκονται στη φάση του σχεδιασμού συνεκτικών πολιτικών προστασίας ΚΥ (EU Cybersecurity Dashboard, 2014; ENISA, 2014). Η Οδηγία 2008/114 (EU Council, 2008) αναδεικνύει την αναγκαιότητα αξιοποίησης βέλτιστων πρακτικών και μεθόδων για την προστασία των ΚΥ. Σε αυτή την ενότητα θα επισκοπήσουμε ορισμένες καλές πρακτικές στον προσδιορισμό και στην προστασία των ευρωπαϊκών ΚΥ, χρησιμοποιώντας την υφιστάμενη βιβλιογραφία και αξιοποιώντας δημόσιες πηγές.

Πίνακας 1: Αξιολόγηση Ωριμότητας Προστασίας Εθνικών ΚΥ στην Ε.Ε. (EU Dashboard, 2014)

Επίπεδο 0	Απουσία δραστηριοτήτων που σχετίζονται με την προστασία κρίσιμων υποδομών	Κροατία, Ιρλανδία, Πορτογαλία
Επίπεδο 1	Ενσωμάτωση της Οδηγίας 114/2008 για την προστασία των κρίσιμων εθνικών υποδομών στο νομικό πλαίσιο της χώρας. Απουσία περαιτέρω δραστηριοτήτων	Ελλάδα, Βουλγαρία, Δανία, Μάλτα
Επίπεδο 2	Διαμόρφωση εθνικής στρατηγικής για τον προσδιορισμό και το χαρακτηρισμό των εθνικών ΚΥ ή των εθνικών ΠΚΥ	Βέλγιο, Κύπρος, Λετονία, Λιθουανία, Ουγγαρία, Σλοβενία, Σουηδία
Επίπεδο 3	Υλοποίηση ολοκληρωμένου προγράμματος προστασίας των ΥΖΣ, συμπεριλαμβανομένων των ΠΚΥ	Αυστρία, Γαλλία, Γερμανία, Ελβετία, Εσθονία, Ισπανία, Μεγάλη Βρετανία, Ολλανδία, Πολωνία, Ρουμανία, Σλοβακία, Τσεχία, Φινλανδία

Στην παρούσα ενότητα διερευνώνται ορισμένες καλές πρακτικές ανά τομέα προτεραιότητας για την προστασία των ΚΥ. Πιο συγκεκριμένα, προτείνεται να εξεταστούν καλές πρακτικές στους εξής τομείς:

Σε Οργανωτικό επίπεδο:

- Η δημιουργία μιας οργανωτικής δομής αρμόδιων και εντεταλμένων φορέων για την προστασία των εθνικών ΚΥ.

- Η αποδοτική συνεργασία μεταξύ των εμπλεκόμενων φορέων του δημόσιου και ιδιωτικού τομέα, τόσο σε εθνικό όσο και σε διεθνές επίπεδο.

Σε Κανονιστικό επίπεδο:

- Η δημιουργία ενός νομοθετικού πλαισίου που να καλύπτει όλες τις πτυχές της ασφάλειας των εθνικών ΚΥ.

- Η διαμόρφωση προτύπων, πολιτικών και διαδικασιών για την προστασία των εθνικών ΚΥ, σε επίπεδο πρόληψης, ανίχνευσης και απόκρισης σε συμβάντα ασφάλειας.

Σε Εκτελεστικό/Λειτουργικό επίπεδο:

- Ο προσδιορισμός των εθνικών ΚΥ και των αλληλεξαρτήσεών τους.

- Η διαρκής αποτίμηση, καθώς και η διαχείριση κινδύνων και κρίσεων που σχετίζονται με απειλές κατά των εθνικών ΚΥ.

- Η δημιουργία ή η προσαρμογή των απαραίτητων μηχανισμών και εργαλείων ώστε να διασφαλιστεί η ανταλλαγή πληροφοριών με σκοπό την πρόληψη, την ανίχνευση και την άμεση ανταπόκριση σε συμβάντα.

- Η προστασία των Πληροφοριακών Κρίσιμων Υποδομών που υποστηρίζουν τη λειτουργία των εθνικών ΚΥ.

Β2.1. Οργανωτικό Επίπεδο

Οργανωτική Δομή Διοίκησης. Στην Ολλανδία (Luiijf, 2003) ακολουθείται αποκεντρωμένο μοντέλο οργανωτικής δομής για την προστασία των ΚΥ, χωρίς δηλαδή την ύπαρξη κάποιας δημόσιας επιτελικής αρχής που συντονίζει την προστασία των ΚΥ, με κάθε τομέα να αυτορρυθμίζεται ως προς την ασφάλεια των ΚΥ που ανήκουν στο πεδίο ευθύνης του. Παρόμοια, αποκεντρωτικά μοντέλα διοίκησης εφαρμόζονται σε Κ-Μ της Ε.Ε., συμπεριλαμβανομένης της Μεγάλης Βρετανίας (UK, 2010).

Στην Εσθονία (Parliament of Estonia, 2009) εφαρμόζεται ένα πιο συγκεντρωτικό μοντέλο, όπου το Υπουργείο Εσωτερικών συντονίζει την υλοποίηση της στρατηγικής διαχείρισης κρίσεων για την προστασία και την ασφάλεια των κρίσιμων τομέων. Επιπλέον, υπάρχει νομοθετικό πλαίσιο στο οποίο καθορίζονται ρητά οι αρμοδιότητες όλων των εμπλεκόμενων φορέων, για την προστασία των ΚΥ και τη διαχείριση κρίσεων. Στους φορείς συμπεριλαμβάνονται τα αρμόδια υπουργεία για την προστασία της αδιάλειπτης λειτουργίας των ΚΥ στις περιοχές ευθύνης τους, οι φορείς τοπικής αυτοδιοίκησης και οι Κάτοχοι/Χειριστές.

Αναλόγως συγκεντρωτικό είναι και το μοντέλο διοίκησης που εφαρμόζεται στη Γερμανία (FRG, 2011), με το Ομοσπονδιακό Υπουργείο Εσωτερικών να σχεδιάζει τη στρατηγική ΠΚΥ και να συντονίζει την υλοποίησή της.

Συνεργασίες Δημόσιων και Ιδιωτικών Φορέων (Public-Private Partnerships, PPP). Τον Απρίλιο του 2006, το Υπουργείο Εσωτερικών Υποθέσεων της Ολλανδίας, σε συνεργασία με τη Συνομοσπονδία της Ολλανδικής Βιομηχανίας και Υπαλλήλων (VNO-NCW), θεσπίζει το SOVI[1] (Strategisch Overleg Vitale Infrastructuur). Το SOVI αποτελεί ένα συμβουλευτικό σώμα σκοπός του οποίου είναι η δημιουργία μιας πλατφόρμας συνεργασίας μεταξύ της κυβέρνησης και των ιδιωτικών φορέων, στο στρατηγικό πλαίσιο της Προστασίας ΚΥ στην Ολλανδία. Οι δράσεις του SOVI περιλαμβάνουν τακτικές συναντήσεις εργασίας, στις οποίες συμμετέχει ένας αντιπρόσωπος από κάθε κρίσιμο τομέα. Η συμμετοχή στις συναντήσεις είναι προαιρετική (Klaver et al., 2011). Το πρόγραμμα προστασίας ΚΥ της Ολλανδίας (Luiijf et al., 2003, Klaver et al., 2011) δίνει μεγάλη έμφαση στην αποτίμηση των διατομεακών αλληλεξαρτήσεων (intersectoral dependencies). Προς τούτο, διεξάγονται συχνά συναντήσεις εργασίας (workshops), στις οποίες δίνουν το «παρών» δημόσιοι φορείς αλλά και Κάτοχοι/Χειριστές (onwers/operators) ΚΥ από διαφορετικούς κρίσιμους τομείς. Σε αυτές τις συναντήσεις εργασίας –στο πλαίσιο διαφόρων σεναρίων διαχείρισης συμβάντος (π.χ. πανδημία γρίπης, πλημμύρες κ.λπ.)–, μεταξύ άλλων, συζητούνται: Οι επιπτώσεις από τη δυσλειτουργία μιας ΚΥ στις κρίσιμες υπηρεσίες ενός τομέα, οι εξαρτήσεις ενός τομέα από άλλους τομείς, καθώς και ο σχεδιασμός και η αποδοτικότητα υποψήφιων μέτρων για την εξάλειψη των σχετιζόμενων ευπαθειών.

1. www.rijksoverheid.nl/binaries/rijksoverheid/documenten/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi/5vragenoversovi-1.pdf

Ανάλογες δράσεις συνεργασίας προάγονται και στο σχέδιο δράσης για την προστασία των Ζωτικών Υπηρεσιών για την κοινωνία και των ΚΥ στη Σουηδία (MSB, 2014). Στη Φινλανδία, το Δίκτυο Συνεργασίας NESA (National Emergency Supply Agency)[2], ένας οργανισμός υπό το Υπουργείο Απασχόλησης και Οικονομίας, χρηματοδοτεί, υπό προϋποθέσεις και μέσω του ταμείου NESF (National Emergency Supply Fund), επιλεγμένα μέτρα προστασίας ΚΥ που σχετίζονται κυρίως με τη συνέχιση λειτουργίας (business continuity) κρίσιμων υπηρεσιών.

2. http://www.nesa.fi/

Το Κέντρο για την Προστασία των Εθνικών Υποδομών (Centre for the Protection of National Infrastructure, CPNI) στο Ηνωμένο Βασίλειο παρέχει υποστήριξη σε επιχειρήσεις και οργανισμούς που απαρτίζουν την κρίσιμη εθνική υποδομή, αναφορικά με ζητήματα ασφαλείας (βλ. Ενότητα Β.2.4).

Στη στρατηγική ΠΚΥ της Γερμανίας (FRG, 2009) προάγονται, ως πιο σημαντικές, οι συνεργασίες μεταξύ φορέων όπως η κυβέρνηση, τα κρατίδια, η τοπική αυτοδιοίκηση (π.χ. δήμοι), οι Κάτοχοι/Χειριστές (operators), οι επιχειρηματικοί εταίροι (βιομηχανία), η επιστημονική και ερευνητική κοινότητα, οι επιχειρήσεις που δραστηριοποιούνται στην ασφάλεια, οι πολίτες, οι διεθνείς οργανισμοί και τα συναφή ιδρύματα, καθώς και οι εταίροι της Γερμανίας (γείτονες, Ε.Ε., G8, NATO κ.λπ.). Για το σκοπό αυτόν η γερμανική στρατηγική προάγει και συντονίζει Στρογγυλά Τραπέζια (round tables) σε εθνικό επίπεδο, σε επίπεδο κρατιδίων, αλλά και σε επίπεδο αυτοδιοίκησης, με τη συμμετοχή των εμπλεκόμενων φορέων. Επίσης, οι αρμόδιες αρχές

εκδίδουν κείμενα συστάσεων και οδηγιών προς Κατόχους/Χρήστες και λοιπούς εμπλεκόμενους φορείς. Παράδειγμα αποτελεί η σύσταση «Protection of Critical Infrastructures – Baseline Protection Concept»[3] του γερμανικού Υπουργείου Εσωτερικών προς Κατόχους/Χειριστές και τις αρμόδιες κυβερνητικές υπηρεσίες.

3. http://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf

Σε ευρωπαϊκό επίπεδο, η «Ευρωπαϊκή Σύμπραξη Δημόσιου-Ιδιωτικού τομέα για την Ανθεκτικότητα» (European Public Private Partnership for Resilience - EP3R)[4] δρομολογήθηκε ως ένα ευρωπαϊκής κλίμακας πλαίσιο διακυβέρνησης για την ανθεκτικότητα των υποδομών ΤΠΕ και αποσκοπεί στην ενίσχυση της συνεργασίας μεταξύ δημόσιου και ιδιωτικού τομέα σε στρατηγικά θέματα ασφάλειας.

4. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

Β2.2. Κανονιστικό Επίπεδο

Υποχρεώσεις Κατόχων/Χειριστών. Σύμφωνα με τη νομοθεσία περί Επειγουσών Καταστάσεων (Emergency Act), στην Εσθονία (Parliament of Estonia, 2009) το Υπουργείο Εσωτερικών δημοσιεύει οδηγίες για την εκπόνηση –από κάθε Κάτοχο/Χειριστή ΚΥ– αποτιμήσεων επικινδυνότητας και Σχεδίου Επιχειρησιακής Λειτουργίας της κρίσιμης υπηρεσίας την οποία ελέγχει. Κάθε δύο χρόνια, ο Κάτοχος/Χειριστής οφείλει να υποβάλει τα παραπάνω στο Υπουργείο που είναι αρμόδιο για την αντίστοιχη κρίσιμη υπηρεσία. Επίσης, ο Κάτοχος/Χειριστής υποχρεούται να υποβάλει στο αρμόδιο Υπουργείο αναφορά για κάθε συμβάν που επηρεάζει την αδιάλειπτη παροχή της κρίσιμης υπηρεσίας. Ακόμη, παρέχει στο αρμόδιο υπουργείο οποιαδήποτε πληροφορία του ζητηθεί σε σχέση με την κρίσιμη υπηρεσία, συμπεριλαμβανομένων των πιθανών (αλληλο-)εξαρτήσεων με άλλες κρίσιμες εθνικές υπηρεσίες. Επιπλέον, κάθε Κάτοχος/Χειριστής καταρτίζει μία λίστα κρίσιμων, πληροφοριακών αγαθών που υποστηρίζουν την κρίσιμη υπηρεσία. Οι Κάτοχοι είναι υπεύθυνοι για τη διαχείριση των κινδύνων οι οποίοι σχετίζονται με την κρίσιμη υπηρεσία που ελέγχουν, επωμιζόμενοι το κόστος.

Στη Γαλλία (SGDSN, 2015) κάθε Κάτοχος/Χειριστής, σε συνέχεια της πράξης No. 2013-1168 (18 Δεκ. 2013)[5], και των διατάξεων που ακολούθησαν, υποχρεούται, εκτός των άλλων:

5. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825

- Να ορίσει υπευθύνους ασφάλειας τόσο σε κεντρικό όσο και σε τοπικό επίπεδο.

- Να εκπονήσει αποτίμηση επικινδυνότητας για τον προσδιορισμό των κρίσιμων υποσυστημάτων[6] στην περιοχή ευθύνης του, καθώς και να καταστρώσει ένα Σχέδιο Ασφαλούς Λειτουργίας (Plan de Securité Opérateur) για την προστασία τους.

- Να προσδιορίσει τα αγαθά/συστήματα στην περιοχή ευθύνης του που θα αποτελέσουν το αντικείμενο τόσο ενός εσωτερικού σχεδίου προστασίας

6. Στην (Klaver et al., 2011) αναφέρεται ότι προσδιορίστηκαν 220 ζωτικοί διαχειριστές, οι οποίοι προσδιόρισαν περίπου 1.000 κρίσιμα αγαθά/συστήματα.

(Plan Particulier de Protection, PPP), την ευθύνη υλοποίησης του οποίου έχει ο ίδιος ο διαχειριστής, όσο και ενός εξωτερικού σχεδίου προστασίας (Plan de Protection Externe, PPE), την ευθύνη υλοποίησης του οποίου θα έχει ο αρμόδιος δημόσιος φορέας.

Στο πλαίσιο της ίδιας προσέγγισης, και αναφορικά με την προστασία των εθνικών πληροφοριακών ΚΥ (French Strategy, 2015), τα διατάγματα 2015-351 (27 Μαρ. 2015)[7], 2015-350 (27 Μαρ. 2015)[8] και 2015-349 (27 Μαρ. 2015)[9] θεσπίζουν υποχρεώσεις για τους περίπου 200 ζωτικούς διαχειριστές, σε σχέση με την ασφάλεια πληροφοριακών συστημάτων (D. Lebeau-Marianna & E. Roger, 2015).

7. http://legifrance.gouv.fr/eli/decret/2015/3/27/PRMD1502905D/jo/texte
8. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405903
9. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405864

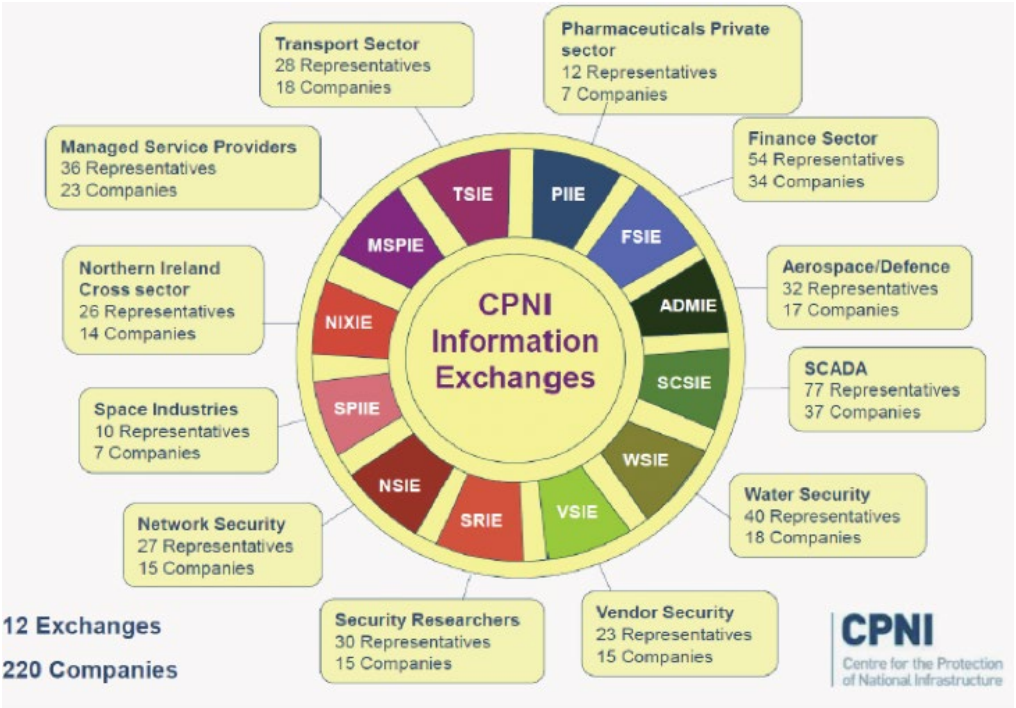
B2.3. Εκτελεστικό/Λειτουργικό Επίπεδο

Ανταλλαγή Πληροφοριών. Στη Μεγάλη Βρετανία το Κέντρο CPNI προσφέρει μια πλατφόρμα ανταλλαγής πληροφοριών σε ζητήματα ΠΚΥ, τόσο σε τομεακό όσο και σε διατομεακό επίπεδο, μεταξύ δημόσιων και ιδιωτικών φορέων (βλ. Σχήμα 1 παρακάτω). Οι πληροφορίες αφορούν ζητήματα απειλών, ευπαθειών, συμβάντων και καλών πρακτικών ΠΚΥ. Σε κάθε κανάλι (information exchange) η ανταλλαγή πληροφοριών γίνεται με ασφάλεια και εμπιστευτικότητα, κάνοντας χρήση πρωτοκόλλων ασφαλούς ανταλλαγής πληροφοριών, όπως το πρωτόκολλο TLP (Traffic Light Protocol)[10].

10. NISCC's Information Exchanges Example Membership Guidelines (March 16, 2007), http://www.uniras.gov.uk/niscc/docs/re-20040601-00395.pdf

Σχήμα 1: Πλατφόρμα Ανταλλαγής Πληροφοριών στο Κέντρο CPNI[11]

11. http://www.cpni.gov.uk/



Σε επίπεδο προτύπων, σημαντική παρόμοια πρωτοβουλία αποτελεί το πρόσφατα διαμορφωθέν πρότυπο ISO/IEC 27010:2015[12] για την ασφαλή ανταλλαγή πληροφοριών σε διατομεακό επίπεδο. Στο πλαίσιο παρεμφερούς πρωτοβουλίας/δράσης στη Μεγάλη Βρετανία, τα σημεία προειδοποίησης, συμβουλών και αναφορών (Warning, Advice and Reporting, WARP)[13] αποτελούν κορμό της στρατηγικής του Κέντρου NISCC (National Infrastructure Security Co-ordination Centre in the United Kingdom) για την προστασία των βρετανικών ΚΥ από ηλεκτρονικές επιθέσεις. Ανάλογη πρωτοβουλία, σε ευρωπαϊκό επίπεδο, αποτελεί η μελέτη (EU Council, 2008) για τη δημιουργία του Δικτύου CIWIN (Critical Infrastructure Warning Information Network)[14], στο πλαίσιο του Ευρωπαϊκού Προγράμματος Προστασίας Κρίσιμων Υποδομών (EPCIP). Το δίκτυο αυτό έχει ως σκοπό την ανταλλαγή πληροφοριών απειλών, ευπαθειών, μέτρων ασφάλειας και στρατηγικών για τη μείωση των κινδύνων στο πλαίσιο της προστασίας ΚΥ.

12. ISO/IEC 27010:2015 Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications (2nd edition). http://www.iso27001security.com/html/27010.html
13. https://www.warp.gov.uk/
14. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

Προστασία Πληροφοριακών ΚΥ. Σημαντική πρωτοβουλία, σε ευρωπαϊκό επίπεδο, για την ανταλλαγή πληροφοριών αποτέλεσε η μελέτη για την ανάπτυξη του Ευρωπαϊκού Συστήματος Συναγερμού και Ανταλλαγής Πληροφοριών (EISAS) (ENISA, 2007b), για τους πολίτες και τις μικρομεσαίες επιχειρήσεις (ΜΜΕ), που θα στηρίζεται στην υλοποίηση βασικών υπηρεσιών σε επίπεδο εθνικών ομάδων CERT/CSIRT και υπηρεσιών διαλειτουργικότητας, ώστε τα εθνικά συστήματα προειδοποίησης (Δράση 41 Ψηφιακού Θεματολογίου)[15] να ενταχθούν στο EISAS. Ανάλογες δράσεις για την ασφάλεια στον κυβερνοχώρο έχουν ληφθεί και στο πλαίσιο ευρωπαϊκών προγραμμάτων (FISHA, NISHA, NEISAS)[16, 17, 18].

15. https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security
16. FISHA: A Framework for Information Sharing and Alerting. http://fisha-project.eu/the-project
17. NISHA: Network for Information Sharing and Alerting http://nisha-network.eu/
18. NEISAS: National & European Information Sharing & Alerting System. http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/neisas_en.htm

Παρόμοιες συνέργειες για τη συνεργασία και την ανταλλαγή πληροφοριών, σε εθνικό ή/και σε ευρωπαϊκό/παγκόσμιο επίπεδο, αποτελούν οι κάτωθι (ENISA, 2015b):

- Στη Γερμανία, η CERT-Verbund[19], με σκοπό τη συνεργασία μεταξύ των ομάδων CERT/CSIRT που δραστηριοποιούνται σε εθνικό επίπεδο.

19. https://www.cert-verbund.de/

- Στην Αυστρία, η CERT.at, σε συνεργασία με την GovCert Austria και την Ομοσπονδιακή Καγκελαρία, για την προστασία των κρίσιμων πληροφοριακών υποδομών σε εθνικό επίπεδο.

- Στην Ολλανδία, η o-IRT-o (operationeel Incident Response Team overleg)[20] αποτελεί, από το 2002, ένα forum συνεργασίας και ανταλλαγής πληροφοριών σχετικών με την απόκριση περιστατικών και τη διαχείριση κρίσεων, όπου σήμερα συμμετέχουν 31 επιχειρήσεις και οργανισμοί.

20. https://www.ncsc.nl/binaries/content/documents/ncsc-nl/organisatie/producten--en-dienstencatalogus-pdc-2013/1/NCSC%2BProducten%2Ben%2BDiensten.pdf

- Στη Μεγάλη Βρετανία, η CiSP (Cyber Information Sharing Partnership)[21] είναι πρωτοβουλία όπου συμμετέχουν περισσότερες από 1.700 επιχειρήσεις και οργανισμοί, με σκοπό την ανταλλαγή πληροφοριών σχετικών με κυβερνο-απειλές και ευπάθειες [22].

21. https://www.cert.gov.uk/cisp/
22. Μέχρι το Φεβρουάριο του 2016 (www.cert.gov.uk/cisp/)

- Το Forum FIRST (Forum for Incident Response and Security Teams) προωθεί τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ ομάδων αντιμετώπισης περιστατικών, με περισσότερα από 300 εγγεγραμμένα μέλη από όλον τον κόσμο.

- Η πρωτοβουλία E-CoAT[23] είναι μια διεθνής συνεργασία Ομάδων Διαχείρισης Περιστατικών Κατάχρησης (Abuse Teams) που ανήκουν σε δικτυακούς/τηλεπικοινωνιακούς Παρόχους.

- Σε ευρωπαϊκό επίπεδο, η Ομάδα EGC (European Government CERTs)[24] αποτελεί άτυπο συνεταιρισμό μεταξύ των εθνικών/κυβερνητικών CERT/CSIRT των K-M με σκοπό τη βελτίωση της συνεργασίας μεταξύ των ομάδων CERT [25].

- Παρόμοιο σκοπό υπηρετεί η ειδική ομάδα TF-CSIRT[26], με στόχο την προώθηση της συνεργασίας μεταξύ των Ομάδων CERT στην Ευρώπη.

23. E-CoAT -- European Coordination of Abuse fighting Teams: http://www.e-coat.org/

24. http://www.egc-group.org/
25. Μέλη του συνεταιρισμού αποτελούν οι ομάδες από Αυστρία, Βέλγιο, Δανία, Φινλανδία, Γαλλία, Γερμανία, Ολλανδία, Νορβηγία, Ισπανία, Σουηδία, Ελβετία, Ηνωμένο Βασίλειο, καθώς και η «θεσμική» CERT-EU (www.egc-group.com).
26. https://www.terena.org/activities/tf-csirt/

Αποτίμηση Κινδύνων. Στην Ολλανδία εφαρμόζεται η μεθοδολογία αποτίμησης εθνικών κινδύνων «Nationale Risico beoordeling»[27] για την αποτίμηση, στο πλαίσιο μιας ολιστικής προσέγγισης (all-hazards approach), των κινδύνων που σχετίζονται με όλες τις κατηγορίες απειλών, συμπεριλαμβανομένων των τεχνικών και μη τεχνικών απειλών, των φυσικών απειλών/καταστροφών (βλ. Σχήμα 3 παρακάτω), καθώς και των απειλών που σχετίζονται με την αδιάλειπτη λειτουργία των εθνικών ΚΥ. Ανάλογη μέριμνα λαμβάνεται στη Σουηδία (MSB, 2011; 2014), στην Ελβετία (FOCP, 2013; FC, 2009, 2009b), καθώς και στη Μεγάλη Βρετανία (UK, 2010; SG, 2011).

27. https://www.nctv.nl/Images/nat.risicobeoordeling-6-definitief_tcm126-571117.pdf&usg=AFQjCNFzpZtWDNKaK0PfRlD8TiFjyc19eg&sig2=GiRFa4AfUh-vljOfOT8f9Q

Σημαντικό στοιχείο στη στρατηγική προστασία των ΚΥ που εφαρμόζεται στη Γερμανία (FRG, 2009) αποτελεί η θεώρηση ότι οι εθνικές ΚΥ εκτίθενται σε μία σειρά από εσωτερικές ή/και εξωτερικές απειλές και κινδύνους, επίσης στο πλαίσιο της ολιστικής προσέγγισης (all-hazards) (βλ. Πίνακας 2 παρακάτω), καθώς κινδυνεύουν και από τις αλληλεπιδράσεις εντός ή μεταξύ των κρίσιμων τομέων, οι οποίες αποτελούν μια ξεχωριστή κατηγορία απειλών που πρέπει να ληφθούν υπόψη.

Πίνακας 2: Ολιστική Προσέγγιση Αποτίμησης Κινδύνων (Γερμανία) (FRG, 2009)

Natural events	Technical failure/ human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in man, animals and plants	Failures in organization inter alia, shortcomings in risk and crisis management, inadequate co-ordination and co-operation	Civil wars and wars
Cosmic events inter alia, energy storms, meteorites and comets		

Επίσης, στο πλαίσιο του Εθνικού Σχεδίου για την προστασία των Πληροφοριακών Υποδομών (Natonal Plan for Information Infrastructure Protection, NPSI), δίνεται ιδιαίτερη σημασία στην προστασία των κρίσιμων πληροφοριακών υποδομών και στην αξιολόγηση των απειλών από τις οποίες κινδυνεύουν, σύμφωνα με διεθνώς αποδεκτούς κανόνες αποτίμησής τους (π.χ. πρότυπο ISO/IEC 2001)[28].

Αντιμετώπιση Περιστατικών και Διαχείριση Κρίσεων. Στη Γερμανία, οι αρμόδιες αρχές εκδίδουν κείμενα συστάσεων και οδηγιών προς Κατόχους/Χρήστες και λοιπούς εμπλεκόμενους φορείς για τη διαχείριση κινδύνων και κρίσεων. Παράδειγμα αποτελεί η Σύσταση «Protecting Critical Infrastructures - Risk and Crisis Management, a guide for companies and government authorities»[29] του γερμανικού Υπουργείου Εσωτερικών προς Κατόχους/Χειριστές καθώς και κυβερνητικές υπηρεσίες.

Επίσης, υπό την αιγίδα της ομοσπονδιακής κυβέρνησης εκτελείται από το 2004 η Άσκηση LÜKEX (Länder übergreifende Krisenmanagement-Übung/Exercise)[30] (FRG, 2009), στην οποία οι Κάτοχοι/Χειριστές διαφόρων κρίσιμων τομέων αλλά και οι δημόσιοι φορείς συνεργάζονται για την αντιμετώπιση περιστατικών ασφάλειας ΚΥ, μέσα από την εκτέλεση συγκεκριμένων σεναρίων διαχείρισης κρίσεων.

Ανάλογες ασκήσεις, στο πεδίο της Προστασίας Πληροφοριακών ΚΥ και της Ασφάλειας στον κυβερνοχώρο, διεξάγονται τόσο σε εθνικό όσο και σε πανευρωπαϊκό, αλλά και οι παγκόσμιο επίπεδο. Παράδειγμα αποτελεί η άσκηση Cyber Europe[31], υπό την αιγίδα του ENISA, καθώς και η άσκηση Cyber Storm[32] στις ΗΠΑ.

28. ISO/IEC 27001 - Information security management. http://www.iso.org/iso/iso27001

29. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Protecting-Critical-Infrastructures.pdf?__blob=publicationFile

30. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Flyer/Flyer_Luekex_10_14.html

31. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

32. https://www.dhs.gov/cyber-storm

ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Τομείς Προτεραιότητας μιας Ολιστικής Στρατηγικής Προστασίας ΚΥ

Γ. Τομείς Προτεραιότητας Ολιστικής Στρατηγικής Προστασίας ΚΥ

Λαμβάνοντας υπόψη τις βέλτιστες πρακτικές, καθώς και την εμπειρία από την εφαρμογή πολιτικών προστασίας ΚΥ άλλων χωρών, προτείνεται η δόμηση των προτεραιοτήτων μιας ολιστικής στρατηγικής για την προστασία των Κρίσιμων Υποδομών της Ελλάδας, σύμφωνα με τους παρακάτω Τομείς Προτεραιότητας.

(1) Σε Οργανωτικό επίπεδο:

Τ.Π.1: Καθορισμός Οράματος και Μετρήσιμων Στόχων
Τ.Π.2: Καθορισμός Οργανωτικής Δομής Διοίκησης
Τ.Π.3: Συνεργασίες Κράτους και Ιδιωτικών Φορέων

(2) Σε Κανονιστικό επίπεδο:

Τ.Π.4: Καθορισμός Νομικού Πλαισίου

(3) Σε Εκτελεστικό/Λειτουργικό επίπεδο:

Τ.Π.5: Καταγραφή & Αξιολόγηση Εθνικών ΚΥ
Τ.Π.6: Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ
Τ.Π.7: Ανθεκτικότητα των ΚΥ και Διαχείριση Κρίσεων
Τ.Π.8: Προστασία Πληροφοριακών ΚΥ

Παρακάτω ακολουθεί αναλυτική περιγραφή των προτεινόμενων Τομέων Προτεραιότητας.

Γ1. Όραμα/Στόχοι/Σχέδιο Δράσης

Το βασικό θεμέλιο μιας πολιτικής Ολιστικής Προστασίας ΚΥ είναι η υιοθέτηση ενός σαφούς στρατηγικού στόχου (Όραμα), το οποίο υλοποιείται μέσα από επιμέρους μετρήσιμους στόχους. Το όραμα και οι στόχοι κοινοποιούνται ευρέως σε όλους τους εμπλεκόμενους φορείς και στην κοινωνία εν γένει. Η υλοποίησή τους επιτυγχάνεται μέσω μιας δομημένης στρατηγικής προστασίας των ΚΥ, σε συνδυασμό με την ισχυρή πολιτική δέσμευση από το κράτος που την εφαρμόζει.

Η Στρατηγική Ολιστικής Προστασίας ΚΥ υλοποιείται μέσω ενός Σχεδίου Δράσης, με σαφή βήματα δράσης, για την αποτελεσματική εφαρμογή των μέτρων και δράσεων, σε ένα σαφώς ορισμένο χρονοδιάγραμμα (βλ. Ενότητα Ε).

Γ2. Οργανωτική Δομή Διοίκησης Ασφάλειας ΚΥ

Βασική προτεραιότητα μιας στρατηγικής προστασίας ΚΥ είναι ο καθορισμός μιας Οργανωτικής Δομής Διοίκησης της ασφάλειας των ΚΥ. Όπως αναλύθηκε στο Μέρος Α' της μελέτης και εν συνεχεία υπογραμμίζεται (βλ. Ενότητα Γ.3), στα ζητήματα της προστασίας των εθνικών ΚΥ εμπλέκονται πολλοί φορείς τόσο του δημόσιου όσο και του ιδιωτικού τομέα, με διαφορετικούς τομείς ευθύνης και διαφορετικούς στόχους και προτεραιότητες. Ο σχεδιασμός μιας Οργανωτικής Δομής Διοίκησης πρέπει να λαμβάνει υπόψη την πολυπλοκότητα του προβλήματος. Ο συντονισμός των αρμόδιων φορέων και ο καθορισμός μιας Οργανωτικής Δομής Διοίκησης της προστασίας των εθνικών ΚΥ είναι, ως εκ τούτου, τομέας άμεσης προτεραιότητας.

Σε ένα **αποκεντρωτικό μοντέλο διοίκησης**, η διοίκηση της ασφάλειας των ΚΥ καταμερίζεται είτε στα αρμόδια υπουργεία είτε στις ρυθμιστικές αρχές ανά τομέα.

Σε ένα **συγκεντρωτικό μοντέλο διοίκησης**, η οργανωτική δομή διοίκησης συντονίζεται από μία επιτελική Δημόσια Υπηρεσία, η οποία τυπικά λειτουργεί σε ανώτατο θεσμικά επίπεδο.

Τα βασικά τυπικά χαρακτηριστικά της Υπηρεσίας-Αρχής είναι:

- Σε οργανωτικό επίπεδο, η Υπηρεσία-Αρχή είναι υπεύθυνη για τη σχεδίαση και την υλοποίηση μιας Ολιστικής Στρατηγικής Προστασίας των ΚΥ. Επίσης, τις διαχειρίζεται και τις υντονίζει με αποδοτικό τρόπο τις απαιτούμενες δράσεις για την προστασία των ΚΥ.

- Σε νομοθετικό/κανονιστικό επίπεδο, η Υπηρεσία-Αρχή καθορίζει τις σαφείς αρμοδιότητες, τις διεπαφές επικοινωνίας και τις σχέσεις συνεργασίας των εμπλεκόμενων φορέων του δημόσιου και του ιδιωτικού τομέα.

- Σε τεχνικό επίπεδο, η Υπηρεσία-Αρχή διαθέτει την απαραίτητη τεχνογνωσία σε θέματα ασφάλειας συστημάτων και υποδομών. Η Υπηρεσία-Αρχή μπορεί να διαδραματίζει τόσο συμβουλευτικό όσο και ελεγκτικό ρόλο (πραγματοποίηση ελέγχων (audits)).

Γ3. Συνεργασία Δημόσιων και Ιδιωτικών Φορέων

Στα περισσότερα Κ-Μ της Ε.Ε., αλλά και σε παγκόσμιο επίπεδο, οι ΚΥ, σε ποσοστό άνω του 80%, ανήκουν και λειτουργούνται από ιδιωτικές εταιρείες (Klaver et al., 2011). Επιπλέον, στο δημόσιο τομέα υπάρχουν δομές και υπηρεσίες οι οποίες έχουν τη δυνατότητα άμεσης πρόσβασης και διαχείρισης περιστατικών ασφάλειας.

Ως εκ τούτου, η συνεργασία των αρμόδιων και εμπλεκόμενων δημόσιων φορέων με τους Κατόχους/Χειριστές (Owners/Operators) των ΚΥ αποτελεί σημαντικό επιμέρους στόχο της στρατηγικής προστασίας των ΚΥ και μπορεί να οδηγήσει στην αύξηση της ενημέρωσης των εμπλεκόμενων φορέων, στην οικοδόμηση εμπιστοσύνης μεταξύ των φορέων, σε μια συναντίληψη των απειλών και κινδύνων, καθώς και στην αποτελεσματικότερη λήψη μέτρων προστασίας των ΚΥ, τόσο σε εθνικό επίπεδο όσο και στο πλαίσιο διεθνών συνεργασιών.

Οι Συνεργασίες Δημόσιων και Ιδιωτικών Φορέων (Public Private Partnerships, PPP) μπορούν να έχουν άτυπη ή/και τυπική υπόσταση, ανάλογα με το βαθμό ελέγχου που ασκεί σε αυτές το κράτος. Ταξινομώντας τις ως προς το βαθμό ελέγχου που ασκεί το κράτος στη συνεργασία, αναφέρονται ενδεικτικά οι ακόλουθες εναλλακτικές:

Κέντρα Ανταλλαγής και Ανάλυσης Πληροφοριών. Τα κέντρα ISAC (Information Sharing and Analysis Centers) ή WARP (Warning, Advice and Reporting Points) αποτελούν κοινότητες ανταλλαγής πληροφοριών μεταξύ των εμπλεκόμενων δημόσιων/ιδιωτικών φορέων σε ζητήματα προστασίας ΚΥ και μπορούν να λειτουργούν είτε ανά τομέα είτε σε διατομεακό επίπεδο. Οι πληροφορίες που ανταλλάσονται αφορούν: (α) Θέματα απειλών, ευπαθειών, επιπτώσεων, αλληλεξαρτήσεων, κινδύνων, (β) Αναφορές περιστατικών ασφάλειας κατά των ΚΥ και (γ) Προειδοποιήσεις, μέτρα και καλές πρακτικές για την προστασία της ασφάλειας των ΚΥ. Επιπλέον, μπορούν να οδηγήσουν στην έγκαιρη αναγνώριση των νέων απειλών.

Χρηματοδότηση Μέτρων Προστασίας ΚΥ. Στο υπόδειγμα αυτό, το κράτος προσφέρει οικονομικά κίνητρα, καλύπτοντας μέρος ή το σύνολο των δαπανών στις οποίες προβαίνει ένας Κάτοχος/Χειριστής ΚΥ (π.χ. Ταμείο NESA – βλ. Ενότητα Β2.1).

Υποχρεωτική Συνεργασία μεταξύ Δημόσιων/Ιδιωτικών Φορέων. Με βάση νόμο, ο Κάτοχος/-Χειριστής ΚΥ αναλαμβάνει συγκεκριμένες δεσμεύσεις έναντι του αρμόδιου φορέα Προστασίας ΚΥ, π.χ., την ανά τακτά χρονικά διαστήματα αποστολή αναφορών αποτίμησης και διαχείρισης επικινδυνότητας, την αποστολή αναφορών συμβάντων, την αποστολή σχεδίων επιχειρησιακής συνέχειας κ.λπ. Η επίτευξη υψηλού επιπέδου ασφάλειας και ετοιμότητας των ΚΥ απαιτεί την υψηλή κατάρτιση του προσωπικού που εργάζεται στις ΚΥ σε θέματα ασφάλειας και προστασίας των ΚΥ, τόσο σε τεχνικό όσο και σε οργανωτικό επίπεδο. Δεδομένου ότι οι Κάτοχοι/Χειριστές ΚΥ είναι φορείς τόσο του δημόσιου όσο και του ιδιωτικού τομέα, η ανάπτυξη των σχετικών ικανοτήτων μπορεί να διευκολυνθεί επιπροσθέτως μέσα από δράσεις Συνέργειας Δημόσιου-Ιδιωτικού τομέα. Ως εκ τούτου, τόσο ο δημόσιος όσο και ο ιδιωτικός τομές, σε συνεργασία και με το συντονισμό της αρμόδιας οργανωτικής δομής προστασίας ΚΥ, θα πρέπει να υποστηρίξουν κατάλληλες δράσεις εκπαίδευσης προσωπικού στα θέματα ασφάλειας ΚΥ. Αυτές μπορεί να πραγματοποιηθούν μέσω του σχεδιασμού κατάλληλων εκπαιδευτικών προγραμμάτων και πιστοποιήσεων, αλλά και της δημιουργίας και κινητικότητας ενός συνόλου ανθρώπινου δυναμικού με τις απαραίτητες εξειδικευμένες γνώσεις.

Είναι σημαντικό, πέρα από το ικανοποιητικό επίπεδο γνώσεων και ικανοτήτων που πρέπει να έχουν οι Κάτοχοι/Χειριστές των ΚΥ για την προστασία τους, να υπάρχει μια αναπτυγμένη κουλτούρα ασφάλειας για τη χρήση των ΚΥ. Αυτή μπορεί να καλλιεργηθεί μέσω της ευαισθητοποίησης του κοινού και των χρηστών για την ορθολογική χρήση των υποδομών αυτών, συντελώντας στον περιορισμό κάποιων κινδύνων.

Γ4. Νομικό/Κανονιστικό Πλαίσιο

Προκειμένου να είναι αποτελεσματική η Οργανωτική Δομή για την προστασία των ΚΥ, πρέπει να υποστηρίζεται από ένα σαφές, δομημένο και εκσυγχρονισμένο νομικό πλαίσιο, το οποίο θα πρέπει:

- Να προδιαγράφει και να οριοθετεί επακριβώς την καθ' ύλην αρμόδια Οργανωτική Δομή η οποία έχει την ευθύνη για τον επιτελικό σχεδιασμό και την παρακολούθηση της εφαρμογής της Πολιτικής Προστασίας ΚΥ.

- Να προσδιορίζει όλους τους βασικούς εμπλεκόμενους φορείς, τόσο του δημόσιου όσο και του ιδιωτικού τομέα, καθώς και τις αρμοδιότητές τους.

- Να συμμορφώνεται πλήρως τόσο με το ευρωπαϊκό ή/και διεθνές νομοθετικό πλαίσιο όσο και με το εθνικό νομικό, το οποίο άπτεται θεμάτων που σχετίζονται με την προστασία ΚΥ, όπως είναι τα θέματα της ασφάλειας δικτύων και πληροφοριών, της προστασίας προσωπικών δεδομένων, της διασφάλισης του απορρήτου των επικοινωνιών και του ηλεκτρονικού εγκλήματος.

- Να λαμβάνει υπόψη σύγχρονες τάσεις και μελλοντικές προκλήσεις ως προς την προστασία των Κρίσιμων Υποδομών και την ασφάλεια στον κυβερνοχώρο.

Γ5. Καταγραφή και Αξιολόγηση Εθνικών ΚΥ

Οποιαδήποτε πολιτική προστασίας ΚΥ έχει ως προαπαιτούμενο βήμα τη συστηματική καταγραφή των εθνικών κρίσιμων στοιχείων, με σκοπό τη μετέπειτα αξιολόγησή τους. Ο καθορισμός της οργανωτικής δομής προστασίας ΚΥ, σε συνδυασμό με τη συνεργασία δημόσιου-ιδιωτικού τομέα, θα βοηθήσει σημαντικά στη συστηματική καταγραφή των κρίσιμων τομέων, υποτομέων και υπηρεσιών για τη χώρα.

Τα περισσότερα κριτήρια αξιολόγησης που αφορούν τις εθνικές και ευρωπαϊκές ΚΥ, καθώς και οι μεθοδολογίες που συνήθως εφαρμόζονται, περιγράφονται μόνον ή κυρίως σε γενικό (generic) επίπεδο. Όπως αναφέρθηκε, η αξιολόγηση της κρισιμότητας των εθνικών ΚΥ πρέπει να γίνει με την ανάπτυξη μιας μεθοδολογίας σε εθνικό επίπεδο, που θα λαμβάνει υπόψη τα ιδιαίτερα χαρακτηριστικά επιμέρους εθνικών τομέων σημαντικού ενδιαφέροντος, και ειδικότερα:

- Περιγραφή μιας δομημένης μεθοδολογίας εντοπισμού και αξιολόγησης των εθνικών ΚΥ.
- Περιγραφή κριτηρίων αξιολόγησης ΚΥ που χρησιμοποιούνται στις διεθνώς εφαρμοσμένες μεθοδολογίες αξιολόγησης ΚΥ.
- Επιλογή των κριτηρίων που θα αξιοποιηθούν για την αξιολόγηση των υποψήφιων εθνικών ΚΥ, σύμφωνα με τη μεθοδολογία εντοπισμού και αξιολόγησης των εθνικών ΚΥ.
- Προσδιορισμό κατάλληλης κλίμακας αξιολόγησης, ανά κριτήριο αξιολόγησης, για την ένταξη των κρίσιμων στοιχείων σε επίπεδα κρισιμότητας.
- Εφαρμογή των επιλεγμένων κριτηρίων σε μία λίστα πιθανών κρίσιμων εθνικών τομέων ή υποτομέων, με σκοπό την ιεράρχησή τους.
- Διασύνδεση και αλληλεξάρτηση των Κρίσιμων Υποδομών. Σημαντικό κριτήριο για την κατηγοριοποίηση των ΚΥ αποτελεί, μεταξύ άλλων, ο βαθμός και η σπουδαιότητα των διασυνδέσεων και αλληλεξαρτήσεων μεταξύ των ΚΥ.

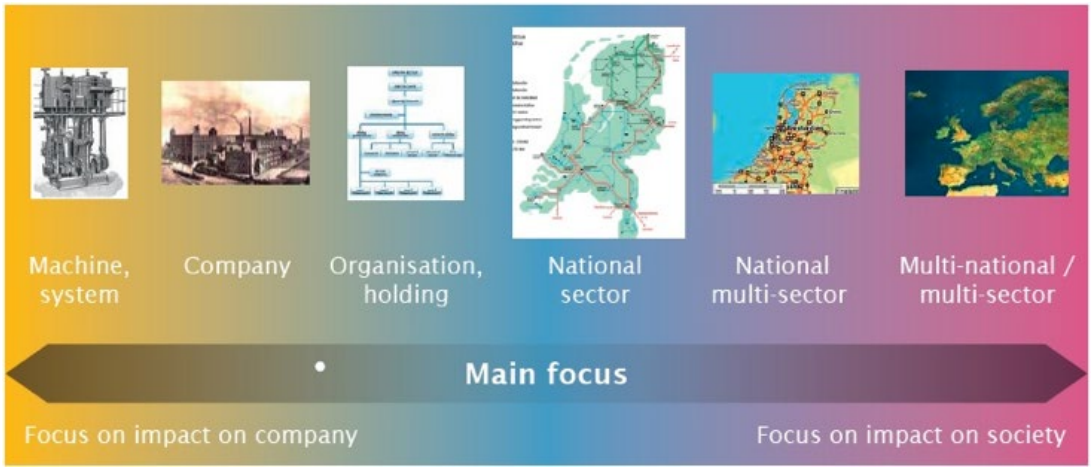
Στόχος μιας μεθοδολογίας αξιολόγησης ΚΥ είναι η κατηγοριοποίηση των εθνικών κρίσιμων στοιχείων ως προς το βαθμό των συνεπειών που αναμένεται να προκαλέσει η εκδήλωση απειλών κατά της ασφάλειας των ΚΥ. Απώτερος στόχος μιας μεθοδολογίας αξιολόγησης ΚΥ είναι η ιεράρχηση της εφαρμογής μέτρων ασφάλειας στις εθνικές ΚΥ, σε συνδυασμό και με την αποτίμηση των απειλών και των κινδύνων των ΚΥ.

Γ6. Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ

Σημαντική προτεραιότητα της στρατηγικής προστασίας ΚΥ είναι η μεθοδολογία αξιολόγησης των απειλών και των συνεπαγόμενων κινδύνων ασφάλειας όλων των κρίσιμων στοιχείων (υποδομών, υπηρεσιών και συστημάτων), όπως αυτά έχουν προσδιοριστεί σύμφωνα με τη μεθοδολογία εντοπισμού και αξιολόγησης ΚΥ (Ενότητα Γ.5).

Η αποτίμηση επικινδυνότητας μπορεί να πραγματοποιηθεί σε ένα ή σε περισσότερα από τα ακόλουθα επίπεδα: Σε επίπεδο υποσυστήματος κρίσιμης υπηρεσίας (βλ. Μέρος Β', Ενότητα Α3.4.), σε επίπεδο υπηρεσίας κρίσιμου τομέα (βλ. Μέρος Β', Ενότητες Α3.2.-Α3.3.), σε επίπεδο ενός ή περισσότερων υποτομέων/τομέων (βλ. Μέρος Β', Ενότητα Α3.1.), σε εθνικό επίπεδο ή σε διεθνές επίπεδο (βλ. Σχήμα 2 παρακάτω).

Σχήμα 2: Επίπεδα Εφαρμογής της Αποτίμησης Επικινδυνότητας ΚΥ (Klaver et al., 2011)



Στην πιο ειδική περίπτωση, η αποτίμηση πραγματοποιείται από τον Κάτοχο/Χειριστή (Operator), λαμβάνοντας υπόψη κυρίως τις επιπτώσεις που θα είχε ένα περιστατικό ασφάλειας στη λειτουργία της επιχείρησης που χειρίζεται ή κατέχει το κρίσιμο υποσύστημα. Στην πιο γενική, ή αλλιώς, ολιστική περίπτωση, κατά την αποτίμηση εθνικών κινδύνων (national risk assessment) λαμβάνονται υπόψη (και) οι επιπτώσεις που θα είχε ένα συμβάν ασφάλειας σε μια ΚΥ για το κοινωνικό σύνολο. Για παράδειγμα, σε μια αποτίμηση εθνικού κινδύνου θα μπορούσε να αξιολογηθεί η επίδραση μιας ΚΥ στην εξέλιξη ενός συμβάντος ή κρίσης. Ενδεικτικά, σε περίπτωση ενός ευρύτερου συμβάντος, όπως είναι μια

φυσική καταστροφή (πλημμύρα, σεισμός κ.λπ.), θα πρέπει να αποτιμηθούν οι επιπτώσεις στο κοινωνικό σύνολο, εξαιτίας μιας πιθανής διακοπής της παροχής ηλεκτρικής ενέργειας. Επιπλέον, θα πρέπει να αξιολογηθούν και οι συνέπειες που θα προκληθούν από πιθανή δυσλειτουργία άλλων διασυνδεδεμένων ΚΥ, οι οποίες εξαρτώνται από την υποδομή παροχής ενέργειας.

Ανεξαρτήτως του επιπέδου στο οποίο θα πραγματοποιηθεί η αποτίμηση επικινδυνότητας, πρέπει να αναπτυχθεί ένα σαφές πλαίσιο αποτίμησης το οποίο να περιλαμβάνει (μεταξύ άλλων):

Αποτίμηση απειλών ασφάλειας (threat assessment)
Αποτίμηση ευπαθειών ασφάλειας (vulnerability assessment)
Αποτίμηση επιπτώσεων (impact assessment)
Αποτίμηση επικινδυνότητας (risk assessment)

Το πλαίσιο αυτό είναι αναγκαίο να συμφωνηθεί και να υιοθετηθεί από όλα τα εμπλεκόμενα μέρη, συμπεριλαμβανομένων των Κατόχων/Χειριστών ΚΥ, και θα πρέπει να λαμβάνει υπόψη τα σχετικά διεθνή πρότυπα ασφάλειας και τις καλές πρακτικές σε διεθνές επίπεδο.

Ως προς το εύρος των απειλών που αξιολογούνται, η μεθοδολογία αποτίμησης μπορεί να λάβει υπόψη μία ή περισσότερες κατηγορίες απειλών, ενώ συχνά ακολουθείται η ολιστική προσέγγιση (all -hazards), όπου λαμβάνονται υπόψη όλες οι κατηγορίες απειλών, περιλαμβανομένων των τεχνικών και μη τεχνικών απειλών, των φυσικών απειλών/καταστροφών κ.λπ.

Μία συγκεκριμένη κατηγορία απειλών, που μπορεί να ληφθεί υπόψη ξεχωριστά, είναι οι απειλές κατά των πληροφοριακών συστημάτων που υποστηρίζουν μια ΚΥ (ή των Πληροφοριακών ΚΥ), στο πλαίσιο της Προστασίας Πληροφοριακών ΚΥ (βλ. και Ενότητα Γ8). Πράγματι, η ολοένα αυξανόμενη διασύνδεση των ΚΥ με πληροφοριακά συστήματα, καθώς και η αυξανόμενη διασύνδεση και αλληλεξάρτηση μεταξύ τους, οδηγούν σε συνεχώς μεγαλύτερη έκθεση των ΚΥ σε νέες –και συχνά παγκόσμιες– απειλές στον κυβερνοχώρο. Ο ρόλος των υποδομών πληροφορίας για τη λειτουργία των ΚΥ είναι αυξανόμενης σημασίας για την πολιτική προστασίας των ΚΥ, καθώς υπάρχει έντονη αλληλεπίδραση μεταξύ της ασφάλειας στον κυβερνοχώρο και της πολιτικής προστασίας των ΚΥ. Η αυξανόμενη εξάρτηση των φυσικών υποδομών ζωτικής σημασίας από τον τομέα των ΤΠΕ και η αυξανόμενη σημασία του Διαδικτύου και των συναφών υπηρεσιών για την Κοινωνία και την Οικονομία τείνουν σταδιακά να αλλάξουν το τοπίο των απειλών.

Η αποτίμηση επικινδυνότητας επιβάλλεται να είναι διαρκής. Αυτό σημαίνει πως κάθε κύκλος επανάληψης της αποτίμησης επικινδυνότητας εμμέσως θα πρέπει να αξιολογεί τα μέτρα προστασίας που εφαρμόστηκαν σε συνέχεια της προηγούμενης αποτίμησης και θα πρέπει συνδέεται με δράσεις ελέγχου της ανθεκτικότητας των ΚΥ.

Γ7. Ανθεκτικότητα ΚΥ και Διαχείριση Κρίσεων

Κάθε σχέδιο Διαχείρισης Κινδύνων για την Προστασία των ΚΥ περιλαμβάνει μία σειρά πολιτικές και μέτρα για τη μείωση της επικινδυνότητας που αφορά τα πιο κρίσιμα εθνικά στοιχεία, όπως αυτά έχουν αναδειχθεί στα (προηγούμενα) στάδια της Καταγραφής και Αξιολόγησης Εθνικών ΚΥ, αλλά και της Αποτίμησης Επικινδυνότητας ΚΥ. Σύμφωνα με την αρχή της αναλογικότητας (proportionality) (FC, 2009), τα μέτρα προστασίας που θα επιλεχθούν θα πρέπει να είναι σύμφωνα με το επίπεδο επικινδυνότητας, τους στόχους προστασίας και τους οικονομικούς στόχους που έχουν τεθεί, καθώς και να λαμβάνουν υπόψη τα ήδη υπάρχοντα μέτρα προστασίας και την ισχύουσα νομοθεσία.

Σύμφωνα με την ολιστική προσέγγιση περί ανθεκτικότητας (resilience) (π.χ. UK, 2010; SG, 2011), τα μέτρα προστασίας για τη μείωση των πιο σημαντικών κινδύνων μπορούν να έχουν είτε προληπτικό/αποτρεπτικό χαρακτήρα είτε να δίνουν έμφαση στην ταχεία απόκριση/αποκατάσταση του κρίσιμου στοιχείου ή της κρίσιμης υπηρεσίας, όταν μια απειλή εκδηλωθεί με επιτυχία. Επιπλέον, τα μέτρα ασφάλειας μπορεί να απευθύνονται είτε σε απλά περιστατικά (incidents) είτε σε κρίσιμα περιστατικά (emergencies).

Η πλειονότητα των μέτρων ασφάλειας τυπικά βασίζονται σε δύο άξονες:

Ανθεκτικότητα – Πρόληψη. Η προστασία των ΚΥ εξαρτάται σημαντικά από την ανθεκτικότητά τους, η οποία νοείται ως η εξασφάλιση της συνέχειας λειτουργίας (business continuity) των πλέον κρίσιμων υποσυστημάτων και υπηρεσιών. Τα λαμβανόμενα μέτρα ασφάλειας στοχεύουν κυρίως στην ενίσχυση των δυνατοτήτων πρόληψης έναντι ενδεχομένων απειλών, όπως κακόβουλων ενεργειών κ.λπ.

Αντιμετώπιση Περιστατικών Ασφάλειας (Incident Response) και Διαχείριση Κρίσεων (Crisis Management). Επίσης σημαντική για την προστασία μιας ΚΥ είναι η λήψη μέτρων για την ανταπόκριση σε περιστατικά ασφάλειας, την ελαχιστοποίηση των συνεπειών/επιπτώσεων, καθώς και την αποκατάσταση των πλέον κρίσιμων και ζωτικών υποσυστημάτων/υπηρεσιών, λαμβάνοντας υπόψη απλά περιστατικά ή/και περιστατικά που μπορεί να οδηγήσουν σε κρίση.

Κατά αναλογία με το στάδιο της αποτίμησης επικινδυνότητας, η διαχείριση κρίσεων μπορεί να εφαρμοστεί σε διαφορετικά επίπεδα: Στο επίπεδο του Κατόχου/Χειριστή, σε επίπεδο ενός ή περισσότερων κρίσιμων τομέων, καθώς και σε εθνικό ή διεθνές επίπεδο. Δεδομένου ότι οι ΚΥ σε μεγάλο ποσοστό λειτουργούν στον ιδιωτικό τομέα, ενδέχεται να είναι απαραίτητη η λήψη συγκεκριμένων νομοθετικών μέτρων για την επιβολή των πολιτικών διαχείρισης κινδύνου.

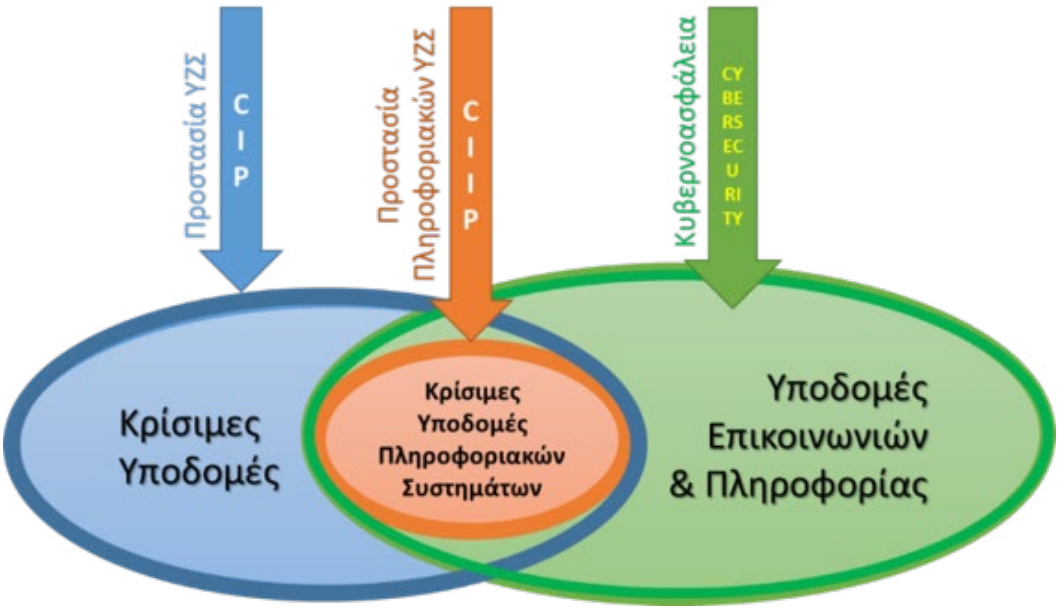
Επίσης, σύμφωνα με την ολιστική προσέγγιση (all-hazards), οι πολιτικές διαχείρισης κρίσεων αναφορικά με τις εθνικές ΚΥ μπορούν να ενσωματωθούν σε μια εθνική στρατηγική διαχείρισης κρίσεων. Έτσι, λοιπόν, εκτός από τις απειλές κατά των ΚΥ, στο στάδιο αυτό μπορεί να εξεταστεί πώς η αδιάλειπτη λειτουργία ενός κρίσιμου υποσυστήματος ή υπηρεσίας εντάσσεται σε μια πολιτική αντιμετώπισης ενός κρίσιμου περιστατικού (π.χ. διαθεσιμότητα δικτύων κινητής και διαδικτυακών υπηρεσιών σε μεγάλες καταστροφές).

Γ8. Προστασία Πληροφοριακών ΚΥ

Σε συνέχεια της ανακοίνωσης της Επιτροπής σχετικά με την Προστασία των Πληροφοριακών Κρίσιμων Υποδομών (Commission 149, 2009), αλλά και του Ψηφιακού Θεματολογίου για την Ευρώπη [συνεπώς και με τη στρατηγική «Ευρώπη 2020» EU Commission (2010)], η επερχόμενη νέα Ευρωπαϊκή Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (ΑΔΠ – NIS) (EU Commission, 2013), η οποία αναμένεται να αποτελέσει εφαλτήριο για την εμπέδωση της ευρωπαϊκής στρατηγικής ασφάλειας του κυβερνοχώρου (Cybersecurity Strategy), θα επικεντρώνεται, εκτός των άλλων, στη βελτίωση της ασφάλειας των κρίσιμων συστημάτων πληροφοριών και δικτύων που υποστηρίζουν κρίσιμες (απαραίτητες) υπηρεσίες, δίνοντας έμφαση στην προστασία κρίσιμων (ζωτικών) υπηρεσιών.

Η Προστασία Πληροφοριακών Κρίσιμων Υποδομών (ΠΠΚΥ/CIIP) αποτελεί, αφενός, αναπόσπαστο κομμάτι της Προστασίας Κρίσιμων Υποδομών (ΠΚΥ/CIP) και, αφετέρου, αναπόσπαστο τμήμα της προστασίας του κυβερνοχώρου (Cybersecurity) (βλ. Σχήμα 3 παρακάτω) (Cavelty and Suter, 2012).

Σχήμα 3: Διάκριση μεταξύ Προστασίας ΥΖΣ και Πληροφοριακών Υποδομών

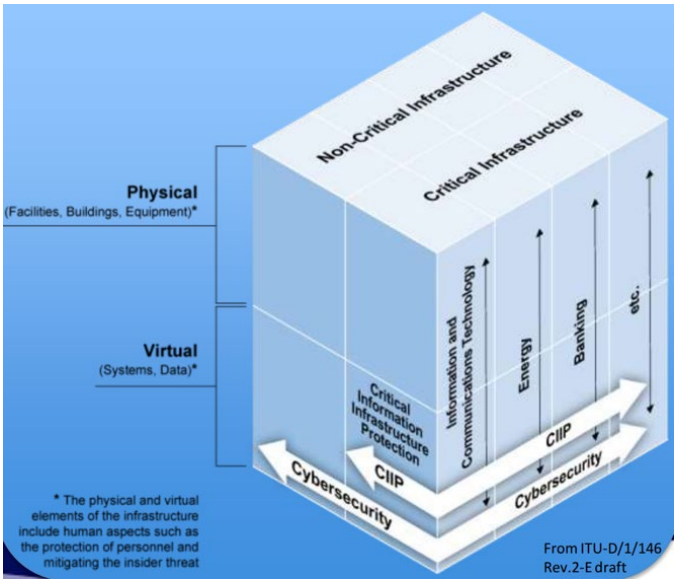


Οι πληροφοριακές ΚΥ μπορεί να περιλαμβάνουν (Hammerli & Renda, 2010): (α) πληροφοριακά/επικοινωνιακά συστήματα υποστηρικτικά της λειτουργίας μιας ΚΥ, (β) συστήματα υποστηρικτικά κυβερνητικών λειτουργιών (government business) και (γ) πληροφοριακές υποδομές που είναι σημαντικές για την εθνική οικονομία. Υπό αυτή τη θεώρηση, η ΠΠΚΥ μπορεί εννοιολογικά να θεωρηθεί ως υποσύνολο της ασφάλειας του κυβερνοχώρου (βλ. Σχήμα 4 παρακάτω).

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), σε πρόσφατη μελέτη του (ENISA, 2015) δίνει γενικές συστάσεις προς τα Κ-Μ της Ε.Ε. για το πώς να βελτιώσουν την προστασία των ΠΚΥ στην Ευρωπαϊκή Ένωση. Οι συστάσεις είναι οι εξής:

Σύσταση 1: Αύξηση θεσμοθετημένης συνεργασίας κράτους με ιδιωτικούς φορείς (PPP).
Σύσταση 2: Εναρμόνιση των δομών διαχείρισης της προστασίας των ΠΚΥ με τις υπάρχουσες εθνικές δομές διαχείρισης κρίσεων και έκτακτης ανάγκης (crisis and emergency management).
Σύσταση 3: Συμμετοχή ή φιλοξενία διεθνών ασκήσεων ετοιμότητας για την προστασία ΚΥ.
Σύσταση 4: Καθιέρωση υποχρεωτικής αναφοράς περιστατικών ασφάλειας από τους Χειριστές (Operators).
Σύσταση 5: Διεξαγωγή εθνικής αποτίμησης κινδύνων (national risk assessment).
Σύσταση 6: Υιοθέτηση βέλτιστων πρακτικών ως προς τη θεσμοθέτηση ενός νομικού πλαισίου για την προστασία των ΠΚΥ σε όλους τους κρίσιμους εθνικούς τομείς.
Σύσταση 7: Κίνητρα στους διαχειριστές των ΠΚΥ για να επενδύσουν σε αποδοτικά μέτρα ασφάλειας.

Σχήμα 4: Προστασία Πληροφοριακών ΚΥ και Ασφάλεια στον Κυβερνοχώρο[33]



33. Protecting Critical Information Infrastructure: An Industry View. Presentation by Matt Broda at the CEPS Task Force, Brussels, 2011.

Η διαρκής αποτίμηση των απειλών στην ασφάλεια πληροφοριών προϋποθέτει μια καλά δομημένη και οργανωμένη παρακολούθηση και αντιμετώπιση των περιστατικών ασφάλειας. Θεωρείται δεδομένο από τους ειδικούς της ασφάλειας ΤΠΕ ότι καμία οργανωτική δομή δεν μπορεί να αποτρέψει πλήρως την εκδήλωση περιστατικών ασφάλειας.

Βασικός τομέας προτεραιότητας μιας Ολιστικής Πολιτικής Προστασίας ΚΥ είναι, κατά συνέπεια, η διαρκής παρακολούθηση και η έγκαιρη αντιμετώπιση των περιστατικών ασφάλειας, ώστε να περιοριστούν οι ενδεχόμενες συνέπειές τους.

Βασική οργανωτική μονάδα προς τη διασφάλιση αυτού του σκοπού είναι οι Ομάδες Αντιμετώπισης Περιστατικών Ασφάλειας (Computer Security Incident Response Teams ή Computer Emergency Response Teams, CSIRT ή CERT). Η οργάνωση και ο συντονισμός των δράσεων αυτών των ομάδων (Εθνικό/Κυβερνητικό CERT και λοιπά CERT) θα οδηγήσουν στον έγκαιρο εντοπισμό και στη μεγαλύτερη δυνατή αποτροπή της εκδήλωσης περιστατικών ασφάλειας με υψηλό βαθμό συνεπειών. Η καλή λειτουργία ενός CERT απαιτεί την ύπαρξη και τη λειτουργία των αναγκαίων υποδομών, τη στελέχωσή τους με επαρκώς καταρτισμένο προσωπικό, αλλά και τη διαρκή εκπαίδευση του προσωπικού. Επιπλέον, απαιτείται η πιστοποίηση του CERT, έτσι ώστε να είναι δυνατή η συμμετοχή τους στις ευρωπαϊκές ομάδες εργασίας.

ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Πρόταση Ολιστικής Πολιτικής Προστασίας Εθνικών ΚΥ

Δ. Πρόταση Ολιστικής Πολιτικής Προστασίας Εθνικών ΚΥ

Στην προηγούμενη ενότητα περιγράφηκαν οι τομείς προτεραιότητας οι οποίοι αξιολογούνται, με βάση τη μελέτη των στρατηγικών ΠΚΥ άλλων χωρών και λαμβάνοντας υπόψη την ελληνική πραγματικότητα, ως οι πλέον σημαντικοί τομείς για το σχεδιασμό μιας στρατηγικής ΠΚΥ της χώρας. Με βάση αυτούς τους τομείς προτεραιότητας, προτείνεται σε αυτή την ενότητα ένα σχέδιο μιας Ολιστικής Πολιτικής Προστασίας των Εθνικών Κρίσιμων Υποδομών.

Σε κάθε τομέα προτεραιότητας θα καθοριστούν συγκεκριμένες δράσεις, για την εφαρμογή των στόχων που ορίζονται σε κάθε τομέα προτεραιότητας. Επιπλέον, για κάθε προτεινόμενη δράση γίνεται μια γενική εκτίμηση ως προς το χρόνο εφαρμογής της. Καθορίζονται δύο φάσεις εφαρμογής:

Φάση Α: Σε αυτήν κατηγοριοποιούνται οι δράσεις των οποίων η εφαρμογή κρίνεται ως άμεσης προτεραιότητας και ταυτόχρονα πληρούνται οι προϋποθέσεις άμεσης εφαρμογής.

Φάση Β: Σε αυτήν κατηγοριοποιούνται είτε δράσεις των οποίων η εφαρμογή προϋποθέτει την πρότερη εφαρμογή άλλων δράσεων, οι οποίες απαιτούν μεγάλο χρόνο εφαρμογής, είτε δράσεις μεταγενέστερου σταδίου ωρίμανσης της Πολιτικής Προστασίας ΚΥ.

Ορισμένες δράσεις εντάσονται και στις δύο φάσεις εφαρμογής, με την έννοια ότι είναι δράσεις οι οποίες απαιτούν αφενός την εφαρμογή άλλων βραχυπρόθεσμων δράσεων και αφετέρου θα πρέπει και οι ίδιες να έχουν εφαρμοστεί πριν την έναρξη άλλων δράσεων της δεύτερης φάσης εφαρμογής.

Επιπλέον, όπου είναι δυνατόν, γίνεται αναφορά σε υφιστάμενες δράσεις, τυπικές ή άτυπες, οι οποίες θα μπορούσαν να αξιοποιηθούν για την εφαρμογή των προτεινόμενων δράσεων ανά τομέα προτεραιότητας.

Τέλος, επισημαίνεται ότι για κάθε προτεινόμενη δράση καταβάλλεται προσπάθεια να αξιοποιηθούν, όπου είναι δυνατόν, τα αποτελέσματα των λοιπών παραδοτέων της παρούσας μελέτης.

Δ1. Όραμα και Στόχοι

Το Όραμα της Στρατηγικής Ασφάλειας μιας Ολιστικής Πολιτικής Προστασίας των Εθνικών ΚΥ πρέπει να είναι η εξασφάλιση της απρόσκοπτης λειτουργίας των ΚΥ οι οποίες υποστηρίζουν ζωτικές υπηρεσίες για το κοινωνικό σύνολο. Προτεραιότητα θα πρέπει να δοθεί στην προστασία της ανθρώπινης ζωής και της υγείας, στην εύρυθμη κοινωνική λειτουργία και στα ανθρώπινα δικαιώματα, στην προστασία του περιβάλλοντος, στην προστασία της ιδιοκτησίας, στην ελεύθερη διακίνηση, στο δικαίωμα στην πληροφορία και στην ενημέρωση.

Δ1.1. Δράση 1-1: Σχεδιασμός Στρατηγικής Προστασίας ΚΥ της Ελλάδας

- Η στρατηγική και οι προτεινόμενες δράσεις πρέπει να εξασφαλίζουν τους εξής στόχους:

- Διατήρηση της ακεραιότητας, της ανθεκτικότητας και της διαθεσιμότητας των ΚΥ.

- Ανάπτυξη μιας ολιστικής προσέγγισης για την προστασία των ΚΥ.

- Αποφυγή δυσάρεστων επιπτώσεων από απειλές και αποτελεσματική αντιμετώπιση έκτακτων περιστατικών, με την αύξηση της ανθεκτικότητας των ΚΥ και της ικανότητας ανάκαμψης σε περίπτωση εμφάνισης απειλής ή κινδύνου.

- Υποστήριξη των στόχων του κράτους για την ανάπτυξη της χώρας, που συμβάλλουν στην ευημερία των πολιτών.

- Ανάπτυξη εμπιστοσύνης από τους πολίτες και επιχειρήσεις/οργανισμούς για την ασφάλεια της λειτουργίας των εθνικών ΚΥ και την εδραίωση ενός ασφαλούς περιβάλλοντος για την κοινωνία.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση Αποτελεσμάτων Παρούσας Μελέτης. Η παρούσα μελέτη (Μέρος Γ') θα μπορούσε να αποτελέσει τη βάση για το σχεδιασμό μιας Εθνικής Στρατηγικής Προστασίας ΚΥ στην Ελλάδα.

Δ2. Οργανωτική Δομή Διοίκησης Ασφάλειας ΚΥ

Με βάση τους τομείς προτεραιότητας που αναλύθηκαν στην προηγούμενη ενότητα, ο καθορισμός μιας σαφούς Οργανωτικής Δομής του κράτους αποτελεί το θεμέλιο για τη δημιουργία και την επιτυχή υλοποίηση μιας Στρατηγικής Ολιστικής Προστασίας των Εθνικών ΚΥ της χώρας μας, με δεδομένες την υφιστάμενη πολυπλοκότητα, την επικάλυψη αρμοδιοτήτων και την αναποτελεσματικότητα που παρουσιάζει η υφιστάμενη διάρθρωση.

Δ2.1. Δράση 2-1: Σύσταση Αρμόδιου Φορέα για την Προστασία των Εθνικών ΚΥ

Για την αποτελεσματικότερη οργάνωση του κράτους στον τομέα προστασίας των ΚΥ, προτείνεται η σύσταση ή η ένταξη σε κατάλληλη Υπηρεσία (π.χ. Γενική Γραμματεία), ει δυνατόν υπαγόμενη στον Πρωθυπουργό, η οποία θα έχει, μεταξύ άλλων, ως αποστολή:

(α) Τη χάραξη και την εποπτεία υλοποίησης της Εθνικής Στρατηγικής, ως προς τις ανάγκες, τους στόχους, τις προτεραιότητες και τον προσανατολισμό της Πολιτικής Προστασίας των Εθνικών ΚΥ, περιλαμβανομένης της πολιτικής Προστασίας των Πληροφοριακών ΚΥ της χώρας.
(β) Την παρακολούθηση και το συντονισμό των σχετικών δράσεων μεταξύ όλων των Υπουργείων και φορέων για την εφαρμογή και τη διασφάλιση της συνεκτικότητας μεταξύ των στρατηγικών Πολιτικής Προστασίας και Διαχείρισης Κρίσεων, της Εθνικής Ψηφιακής Στρατηγικής, καθώς και της Πολιτική Ασφάλειας των Εθνικών ΚΥ.
(γ) Την αξιολόγηση των αποτελεσμάτων από την εφαρμογή της Εθνικής Στρατηγικής και τη διατύπωση σχετικών προτάσεων στα αρμόδια Υπουργεία και φορείς.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση Υφιστάμενων Δράσεων. Η υπό ίδρυση Γενική Γραμματεία Ψηφιακής Πολιτικής θα μπορούσε να αποτελέσει τον αρμόδιο φορέα με τα παραπάνω χαρακτηριστικά.

Δ2.2. Δράση 2-2: Καταγραφή των Εμπλεκόμενων Φορέων

Η καταγραφή όλων των εμπλεκόμενων φορέων με αρμοδιότητες οι οποίες άπτονται των θεμάτων ΠΚΥ είναι σημαντική προϋπόθεση για το βέλτιστο καταμερισμό των αρμοδιοτήτων και την επίλυση επικαλύψεων, καθώς και για τη διευκόλυνση της υλοποίησης παρακολούθησης και συντονισμού των σχετικών δράσεων. Οι εντεταλμένοι φορείς αφορούν κυρίως, αλλά όχι αποκλειστικά, το δημόσιο τομέα (Ανεξάρτητες Αρχές, ρυθμιστικοί φορείς κ.λπ.).

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση Υφιστάμενων Δράσεων. Αρκετές δράσεις φορέων του δημόσιου τομέα.

Αξιοποίηση Αποτελεσμάτων Παρούσας Μελέτης. Στο πλαίσιο της παρούσας μελέτης έχει γίνει καταγραφή των εμπλεκόμενων και αρμόδιων φορέων στην Ελλάδα (βλ. Μέρος Α', Κεφ. Γ2.).

Δ2.3. Δράση 2-3: Συντονισμός Δράσεων των Εμπλεκόμενων Φορέων

Μετά τον καθορισμό του αρμόδιου φορέα, πρέπει να καθοριστεί με σαφήνεια το πλαίσιο συνεργασίας και ανταλλαγής πληροφοριών μεταξύ όλων των εμπλεκόμενων (κρατικών ή ιδιωτικών) φορέων με τη νέα Υπηρεσία, αλλά και των δημοσίων αρχών μεταξύ τους, ώστε ο συντονισμός της στρατηγικής ανταπόκρισης του κράτους στον τομέα της προστασίας των εθνικών ΚΥ να γίνει με αυξημένη αποτελεσματικότητα.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Δ3. Συνεργασίες Δημόσιων και Ιδιωτικών Φορέων

Στον τομέα της προστασίας ΚΥ, η αποτελεσματική συνεργασία κράτους και ιδιωτικού τομέα μπορεί να επιφέρει σημαντικές συνέργειες και να συνδράμει στην οικοδόμηση εμπιστοσύνης μεταξύ των δύο τομέων στα θέματα της ασφάλειας και της προστασίας των ΚΥ.

Δ3.1. Δράση 3-1: Καταγραφή Κατόχων/Διαχειριστών ΚΥ

Πρέπει να γίνει μια εκτενής επισκόπηση, τόσο του ιδιωτικού τομέα όσο και του δημόσιου, για τον εντοπισμό ομάδων και εμπλεκομένων (stakeholders) οι οποίοι μπορούν να συμβάλουν θετικά στην προσπάθεια για αύξηση του επιπέδου ασφάλειας των ΚΥ. Κύριος, αλλά όχι αποκλειστικός, στόχος αυτής της δράσης είναι η καταγραφή των Κατόχων/Διαχειριστών των πιθανών ΚΕΥ.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση Υφιστάμενων Δράσεων. Οι ρυθμιστικοί φορείς διαφόρων τομέων, όπως ενδεικτικά της Ενέργειας (ΡΑΕ), των ΤΠΕ (ΑΔΑΕ, ΑΠΔΠΧ), των Μεταφορών κ.λπ., διατηρούν μητρώα ελεγχόμενων οργανισμών, τα οποία θα μπορούσαν να αξιοποιηθούν για δράσεις φορέων του δημόσιου τομέα.

Αξιοποίηση Αποτελεσμάτων Παρούσας Μελέτης. Στο πλαίσιο της παρούσας μελέτης έχει γίνει καταγραφή των κύριων διαχειριστών για τους τομείς Ενέργειας, ΤΠΕ και Μεταφορών (βλ. Μέρος Α', Κεφ. Δ).

Δ3.2. Δράση 3-2: Δημιουργία Συνεργασιών για την Προστασία των ΚΥ

Πρέπει να δημιουργηθεί ένα πλαίσιο συνεργασίας για την επίτευξη κοινών στόχων ασφάλειας, που θα διευκολύνει την ανταλλαγή πληροφοριών σχετικά με ενδεχόμενες νέες απειλές ή κινδύνους και θα οδηγήσει σε νέες λύσεις για την αποφυγή τους. Το πλαίσιο συνεργασίας μπορεί να περιλαμβάνει:

- Την οργάνωση ενημερωτικών ημερίδων για την Ασφάλεια των ΚΥ, με συμμετοχή προσωπικού υψηλής εξειδίκευσης σε θέματα ασφάλειας τόσο από το δημόσιο όσο και τον ιδιωτικό τομέα, σε συνδυασμό με έγκριτους ερευνητές από την ακαδημαϊκή κοινότητα.

- Την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών που εφαρμόζονται με επιτυχία στις επιμέρους ΚΥ, ώστε να διαδίδονται και να εφαρμόζονται οι καλές πρακτικές –εφόσον είναι εφικτό– και σε άλλες ΚΥ.

- Τη συγκρότηση ομάδων εργασίας από εξειδικευμένο προσωπικό των Χειριστών ΚΥ, με στόχο την αξιολόγηση θεμάτων ασφάλειας ΚΥ, σε συνεργασία με φορείς του κράτους και υπό την αιγίδα μιας επιτελικής συντονιστικής Υπηρεσίας.

- Τη δημιουργία ενός κρατικού Συμβουλίου/Επιτροπής εμπειρογνωμόνων για την Προστασία των Εθνικών ΚΥ, στο οποίο θα συμμετάσχουν στελέχη υψηλού επιπέδου από τον ιδιωτικό και το δημόσιο τομέα, για την εφαρμογή της Στρατηγικής Προστασίας των ΚΥ και την αξιολόγηση των εφαρμοζόμενων μέτρων ασφάλειας.

- Τη συνεργασία με τους αντίστοιχους PPPs σε άλλες χώρες της Ευρωπαϊκής Ένωσης στον ίδιο τομέα, μέσω της ενεργού συμμετοχής σε αντίστοιχες ομάδες εργασίας. Αυτό θα επιφέρει σημαντικές βελτιώσεις στην αποτελεσματική προστασία των ΚΥ, επιτρέποντας τη συνεργασία στην έρευνα και στην καινοτομία στον αντίστοιχο τομέα.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Αξιοποίηση Υφιστάμενων Δράσεων. Υπάρχουν πολλές διάσπαρτες δράσεις φορέων που θα μπορούσαν να αξιοποιηθούν στο πλαίσιο μιας δομημένης στρατηγικής. Όμως απουσιάζει ο απαραίτητος συντονισμός.

Δ3.3. Δράση 3-3: Εφαρμογή Σεναρίων Επιμόρφωσης

Η κατάλληλη κατάρτιση του προσωπικού που εργάζεται στις ΚΥ και η ανάπτυξη ικανοτήτων των στελεχών του δημοσίου στον τομέα της ασφάλειας και προστασίας ΚΥ είναι απαραίτητη προϋπόθεση για την ομαλή λειτουργία των συστημάτων ασφάλειας, καθώς και για τη σωστή υλοποίηση οποιωνδήποτε δράσεων σχετικά με το θέμα.

Αυτό μπορεί να επιτευχθεί μέσα από τη συνεχή επιμόρφωση, κατάρτιση και πιστοποίηση των στελεχών σε εξειδικευμένα θέματα ασφάλειας και προστασίας των ΚΥ. Τα σεμινάρια για την προστασία των ΚΥ μπορεί να είναι μονοθεματικά ή πολυθεματικά και να απευθύνονται σε συγκεκριμένο κλάδο ΚΥ (π.χ. Ενέργεια, Μεταφορές, Τηλεπικοινωνίες, Διαδίκτυο κ.λπ.) ή να είναι πολυκλαδικά, παρέχοντας την ευκαιρία στα στελέχη των ΚΥ να ανταλλάσσουν γνώσεις και εμπειρίες από την εφαρμογή πολιτικών και μέτρων για την αποτελεσματική προστασία των ΚΥ. Η εκπαίδευση μπορεί να γίνεται με φυσική παρουσία σε εκπαιδευτικούς χώρους, στο πεδίο με ασκήσεις ετοιμότητας, με ηλεκτρονικό τρόπο μέσω διαδικτύου (τηλε-εκπαίδευση) ή με συμμετοχή σε ερευνητικά προγράμματα.

Επειδή οι ΚΥ υποστηρίζονται από ηλεκτρονικά και άλλα έξυπνα συστήματα, προτείνεται να διαμορφωθεί ένα εξειδικευμένο πρόγραμμα ενημέρωσης των στελεχών που εμπλέκονται στην προστασία ΚΥ ειδικά για τα θέματα ηλεκτρονικής ασφάλειας, το οποίο θα περιέχει τα ακόλουθα:

- Δημιουργία εκπαιδευτικών σεμιναρίων μικρής διάρκειας σε εργαζομένους στις ΚΥ.

- Δημιουργία εξειδικευμένων σεμιναρίων για κυβερνητικούς χρήστες συστημάτων πληροφορίας που εμπεριέχουν ευαίσθητα δεδομένα ή/και διαβαθμισμένα έγγραφα.

- Προώθηση της ανάπτυξης κουλτούρας ασφάλειας σε όλα τα κυβερνητικά τμήματα και υπηρεσίες του κράτους, καθώς και σε ιδιωτικές επιχειρήσεις.

- Δημιουργία πληροφοριακού υλικού, καθώς και χρήση διαθέσιμου υλικού από εξωτερικές πηγές (π.χ. ENISA), για τους πολίτες σχετικά με τα θέματα ασφαλούς χρήσης του Διαδικτύου, με επικέντρωση στην προστασία προσωπικών δεδομένων, στη σωστή συμπεριφορά στον κυβερνοχώρο κ.ο.κ.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α/Β.

Αξιοποίηση Υφιστάμενων Δράσεων. Μπορούν να αξιοποιηθούν αρκετές δράσεις φορέων, όπως είναι το Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΚΔΔΑ), επιστημονικά συνέδρια και ημερίδες πανεπιστημιακών φορέων κ.λπ..

Δ4. Νομικό/Κανονιστικό Πλαίσιο

Απαιτούνται ο εντοπισμός, η εναρμόνιση και ο εκσυγχρονισμός των υφιστάμενων νομοθετημάτων και κανονιστικών εγκυκλίων, ενώ πρέπει –όπου είναι απαραίτητο, για να καλυφθούν οι ανάγκες της προστασίας των ΚΥ– να προωθηθεί καινούρια, πρωτογενής ή δευτερογενής, νομοθεσία.

Δ4.1. Δράση 4-1: Κωδικοποίηση, Καταγραφή και Απλοποίηση Νομικού Πλαισίου

Η νέα επιτελική Αρχή, που θα συσταθεί, θα είναι αρμόδια να συντονίζει το Νομοθετικό έργο και θα πρέπει να έχει συγκεκριμένες κανονιστικές αρμοδιότητες:

- Να συνεργάζεται με τη Γενική Γραμματεία της Κυβέρνησης, για τη διασφάλιση της νομοθετικής ορθότητας και ποιότητας προτεινόμενων νομοθετικών ρυθμίσεων στον τομέα της αρμοδιότητάς της και να διατυπώνει σχετικές συστάσεις στα Υπουργεία.

- Να εισηγείται σχέδια νόμου ή άλλες κανονιστικές διατάξεις, που αφορούν την προστασία των ΚΥ, αλλά και να παρακολουθεί την ορθή εφαρμογή των νομοθετημάτων αυτών.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Δ5. Καταγραφή και Αξιολόγηση Εθνικών ΚΥ

Απαιτούνται ο συστηματικός εντοπισμός, η καταγραφή και η αξιολόγηση των εθνικών ΚΥ. Στο πλαίσιο των Μερών Α' και Β' της μελέτης, υλοποιήθηκαν τα βασικά βήματα σχετικά με τις δράσεις που προτείνονται σε αυτόν τον τομέα.

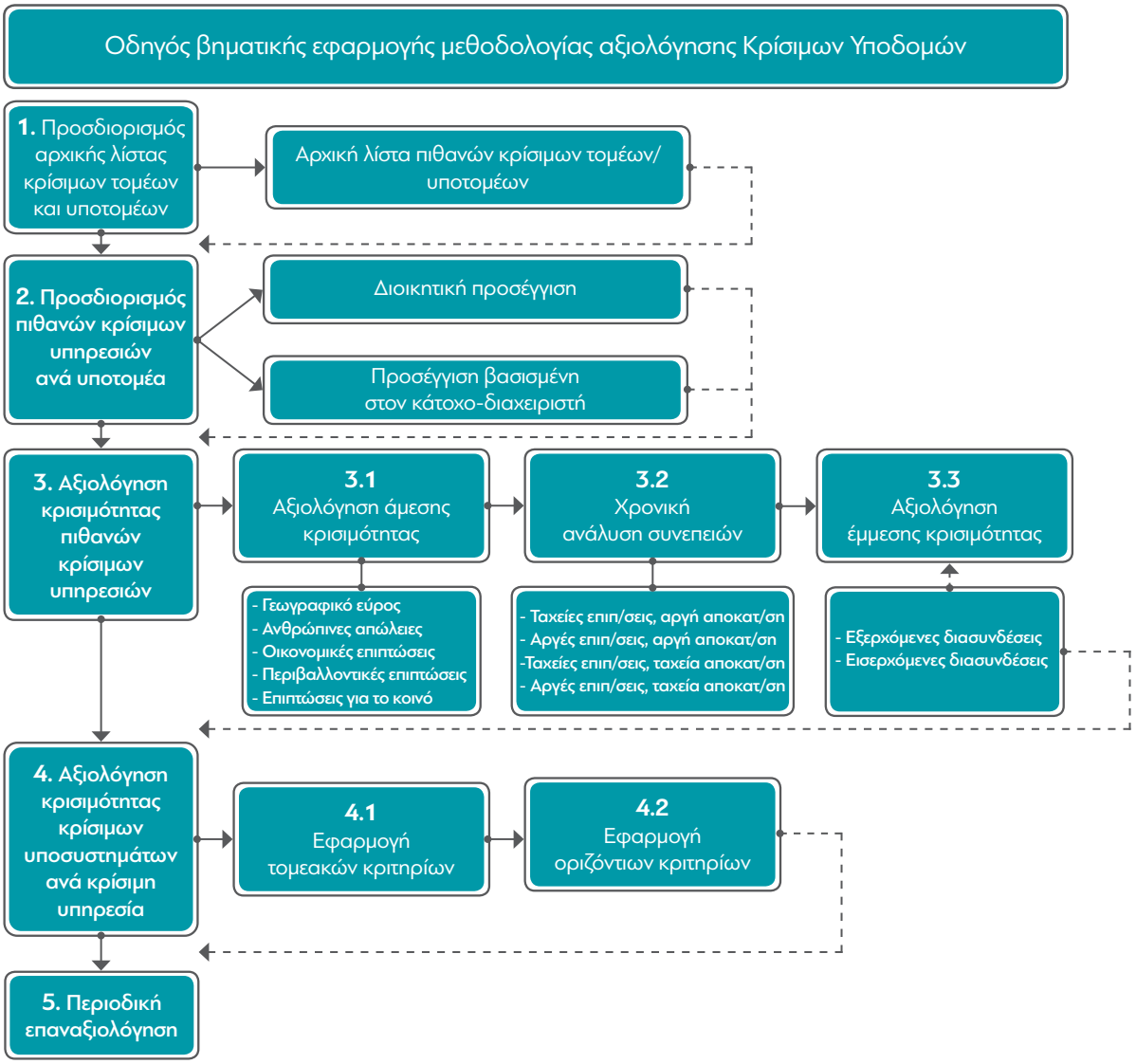
Δ5.1. Δράση 5-1: Καθορισμός Μεθοδολογίας Προσδιορισμού και Αξιολόγησης ΚΥ

Απαραίτητη προϋπόθεση για την προστασία των ΚΥ είναι η διαρκής και συστηματική καταγραφή των κρίσιμων στοιχείων (τομέων, υποτομέων, υπηρεσιών και συστημάτων). Επιπλέον, πρέπει να γίνεται μια διαρκής αξιολόγηση των παραπάνω στοιχείων, με σαφή και δομημένο τρόπο. Προς αυτή την κατεύθυνση, πρέπει να καθοριστεί μια εθνική μεθοδολογία προσδιορισμού και αξιολόγησης των ΚΥ, σύμφωνα με τις Ευρωπαϊκές Οδηγίες και τις καλές πρακτικές. Προτείνεται η συμμετοχή στη δράση αυτή και των Κατόχων/Διαχειριστών των υποψήφιων ΚΥ, με σκοπό τον ακριβέστερο καθορισμό των κριτηρίων αξιολόγησης, κυρίως των τομεακών αλλά και των κριτηρίων διασύνδεσης (βλ. Μέρος Β', Κεφ. Β).

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση αποτελεσμάτων παρούσας μελέτης. Η μεθοδολογία που αναπτύχθηκε στο Μέρος Β' (Κεφ. Α και Β) περιλαμβάνει όλες τις αναγκαίες διαδικασίες εντοπισμού και αξιολόγησης ΚΥ που πρέπει να εφαρμοστούν από τους αρμόδιους εθνικούς φορείς, στο πλαίσιο μιας εθνικής στρατηγικής προστασίας των εθνικών ΚΥ. Περιλαμβάνει, επίσης, κατάλληλα κριτήρια αξιολόγησης, καθώς και αντίστοιχες κλίμακες για κάθε κριτήριο, με σκοπό τη στοιχειοθετημένη ένταξη των υποδομών σε επίπεδα κρισιμότητας. Η μεθοδολογία αυτή μπορεί να αξιοποιηθεί από τον εκάστοτε αρμόδιο εθνικό φορέα, ως οδηγός για τον καθορισμό μιας εθνικής μεθοδολογίας αξιολόγησης των πιθανών εθνικών ΚΥ.

Σχήμα 5: Γενική Περιγραφή Προτεινόμενης Μεθοδολογίας Αξιολόγησης Εθνικών ΚΥ



Δ5.2. Δράση 5-2: Δημιουργία Αρχικής Λίστας Εθνικών Κρίσιμων Τομέων, Υποτομέων και Υπηρεσιών

Το πρώτο βήμα της μεθοδολογίας προσδιορισμού και αξιολόγησης των ΚΥ είναι η δημιουργία μίας Αρχικής Λίστας των Εθνικών Κρίσιμων Υποδομών. Η δράση αυτή είναι απαραίτητη προϋπόθεση για τον προσδιορισμό και την αξιολόγηση των κρίσιμων τομέων, υποτομέων, υποδομών και υπηρεσιών. Χρήσιμη είσοδος για τη δράση αυτή μπορεί να αποτελέσει το αποτέλεσμα της Δράσης 3-1 (Καταγραφή Κατόχων/Διαχειριστών ΚΥ), από την οποία μπορούν να συλλεγούν στοιχεία για τη δημιουργία της αρχικής λίστας υποψήφιων κρίσιμων τομέων/υποτομέων. Προτείνεται οι συγκεκριμένες δράσεις να υλοποιηθούν συνδυαστικά και σε συνεργασία τόσο με τους αρμόδιους

δημόσιους φορείς, όσο και με τους ίδιους τους Κατόχους/Διαχειριστές των υποδομών που ενδεχομένως ανήκουν στον ιδιωτικό τομέα.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α.

Αξιοποίηση Υφιστάμενων Δράσεων. Οι ρυθμιστικοί φορείς διαφόρων τομέων, όπως ενδεικτικά της Ενέργειας (ΡΑΕ), των ΤΠΕ (ΑΔΑΕ, ΑΠΔΠΧ), των Μεταφορών κ.λπ., διατηρούν μητρώα ελεγχόμενων οργανισμών, τα οποία θα μπορούσαν να αξιοποιηθούν για δράσεις φορέων του δημόσιου τομέα.

Αξιοποίηση Αποτελεσμάτων Παρούσας Μελέτης. Στο πλαίσιο της παρούσας μελέτης έχει ήδη γίνει καταγραφή των διαχειριστών για τους τομείς της Ενέργειας, των ΤΠΕ και των Μεταφορών (βλ. Μέρος Α', Κεφ. Δ).

Δ5.3. Δράση 5-3: Εφαρμογή Μεθοδολογίας Προσδιορισμού και Αξιολόγησης ΚΥ

Μετά τον καθορισμό της μεθοδολογίας αξιολόγησης των ΚΥ (βλ. Δράση 5-1) και τον καθορισμό της Αρχικής Λίστας των ΚΥ (βλ. Δράση 5-2), θα πρέπει να γίνει εφαρμογή της μεθοδολογίας, με σκοπό την τεκμηριωμένη αξιολόγηση του επιπέδου κρισιμότητας των υποψήφιων Κρίσιμων Υποδομών, σύμφωνα με τα κριτήρια. Για τις πλέον κρίσιμες υπηρεσίες (βλ. Δράση 5-2) καταρτίζεται λίστα εμπλεκόμενων Κατόχων-Χειριστών, σε συνεργασία με τους οποίους συγκροτείται μία λίστα με τα πιο κρίσιμα υποσυστήματα που υποστηρίζουν την εν λόγω υπηρεσία. Τα υποσυστήματα αυτά αποτελούν την τελική λίστα των εθνικών κρίσιμων υποσυστημάτων (CIP Inventory).

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α/Β.

Αξιοποίηση Αποτελεσμάτων Παρούσας Μελέτης. Η μεθοδολογία που αναπτύχθηκε στο Μέρος Β΄ της μελέτης εφαρμόστηκε ενδεικτικά και στα βήματα, όπου αυτό ήταν εφικτό, στους τομείς της Ενέργειας, των ΤΠΕ και των Μεταφορών (Μέρος Β', Κεφ. Γ).

Δ6. Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ

Όπως προαναφέρθηκε, απαιτούνται ο εντοπισμός και η αξιολόγηση των απειλών, των αδυναμιών και των κινδύνων ασφάλειας των ΚΥ. Οι δράσεις που προτείνονται σε αυτόν τον τομέα περιλαμβάνουν την καταγραφή και την αξιολόγηση των απειλών ασφάλειας, τον καθορισμό μιας εθνικής μεθοδολογίας αποτίμησης επικινδυνότητας και την εφαρμογή της στις ΚΥ.

Δ6.1. Δράση 6-1: Καταγραφή και Αξιολόγηση Απειλών για τις Εθνικές ΚΥ

Το πρώτο βήμα για την αποτίμηση των κινδύνων ασφάλειας που αντιμετωπίζουν οι εθνικές ΚΥ είναι η καταγραφή και η αξιολόγηση των σχετικών απειλών. Σε αυτή τη δράση απαιτείται η στενή συνεργασία των αρμόδιων δημόσιων φορέων με τους ιδιωτικούς φορείς που διαχειρίζονται Κρίσιμες Υποδομές. Η έρευνα, η καταγραφή και η αξιολόγηση των πραγματικών περιστατικών ασφάλειας (επιθέσεων και κυβερνοεπιθέσεων) θα βοηθήσουν στην ουσιαστική μελέτη και αξιολόγηση των απειλών ανά τομέα και υποτομέα. Η δράση αυτή θα πρέπει να είναι διαρκής, ώστε να υπάρχει διαρκής παρακολούθηση για εμφάνιση γνωστών ή νέων απειλών που εμφανίζονται στον εθνικό, στον ευρωπαϊκό και στο διεθνή χώρο. Η δράση αυτή θα πρέπει να αξιοποιήσει και να γίνει σε συνεργασία με το εθνικό και τα άλλα CERT που λειτουργούν στη χώρα (βλ. και Δράση 8-2).

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α/Β.

Δ6.2. Δράση 6-2: Καθορισμός Εθνικής Μεθοδολογίας Αποτίμησης Επικινδυνότητας Εθνικών ΚΥ

Σε συνέχεια της προηγούμενης δράσης, κατ' αναλογία με τη Δράση 5-1, πρέπει να υιοθετηθεί μια Εθνική Μεθοδολογία Αποτίμησης Επικινδυνότητας, για την κατηγοριοποίηση των εθνικών κρίσιμων στοιχείων ως προς τις συνέπειες και τις απειλές κατά της ασφάλειας των ΚΥ, με απώτερο στόχο την ιεράρχηση της εφαρμογής μέτρων ασφάλειας στις εθνικές ΚΥ.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Δ6.2. Δράση 6-3: Εφαρμογή Αποτίμησης Επικινδυνότητας στις Εθνικές ΚΥ

Η εθνική μεθοδολογία αποτίμησης επικινδυνότητας των ΚΥ (βλ. Δράση 6-2) πρέπει να εφαρμόζεται σε τακτά χρονικά διαστήματα, με σκοπό τη διαρκή αξιολόγηση της επικινδυνότητας των απειλών για κάθε συγκεκριμένη ΚΥ, καθώς και την καλύτερη και αποδοτικότερη στόχευση της εφαρμογής των κατάλληλων μέτρων ασφάλειας στις εθνικές ΚΥ.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Δ7. Ανθεκτικότητα ΚΥ και Διαχείριση Κρίσεων

Οι παράγοντες της ασφάλειας (safety and security) θα πρέπει να είναι ενσωματωμένοι στα συστήματα των ΚΥ. Καθ' αυτόν τον τρόπο, τα συστήματα, από τον αρχικό σχεδιασμό και την κατασκευή τους, θα μπορούν να απορροφούν ή να ανθίστανται σε διαταραχές, ελαχιστοποιώντας παράλληλα τις συνέπειες αυτών των διαταραχών.

Επειδή είναι αδύνατον να προβλεφθούν εκ των προτέρων όλοι οι κίνδυνοι και να σχεδιαστούν τα απαιτούμενα μέτρα ασφάλειας, η Ικανότητα Ανάκαμψης των ΚΥ αποτελεί βασικό στοιχείο της ανθεκτικότητας των ΚΥ, καθώς αναφέρεται στη διαδικασία αλλά και στην ταχύτητα της ανάκαμψης.

Η ενίσχυση της ανθεκτικότητας των ΚΥ μπορεί να επιτευχθεί μέσα από την ανάπτυξη νέων εργαλείων διαχείρισης κρίσεων και διαλειτουργικής επικοινωνίας, καθώς και την υιοθέτηση καινοτόμων λύσεων για την προστασία των ΚΥ.

Δ7.1. Δράση 7-1: Προστασία και Ανθεκτικότητα των ΚΥ

Σε συνέχεια του καθορισμού της Λίστας Κρίσιμων Υποσυστημάτων (βλ. Δράση 5-3), οι Κάτοχοι/Χειριστές, στο πλαίσιο που έχει τεθεί από την Οργανωτική Δομή ΠΚΥ, καλούνται να εκπονήσουν Σχέδια Ασφαλούς Λειτουργίας (ΣΑΛ) και Σχέδια Έκτακτης Ανάγκης (ΣΕΑ) για την προστασία τους (Παράρτημα ΙΙ – Οδηγία 114/2008/ΕΚ). Τα σχέδια αυτά εκπονούνται ανά τακτά χρονικά διαστήματα και υποβάλλονται στην αρμόδια επιτελική Αρχή.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α/Β.

Δ7.2. Δράση 7-2: Ασκήσεις Ετοιμότητας και Διαχείρισης Κρίσεων

Η δράση αυτή αφορά τη διοργάνωση, σε τακτικά χρονικά διαστήματα, ασκήσεων ετοιμότητας, τόσο σε επίπεδο μεμονωμένων υποδομών όσο και σε εθνικό επίπεδο. Σκοπός των ασκήσεων είναι, μέσα από διάφορα επεισόδια (σενάρια επιθέσεων), η εξάσκηση των εμπλεκόμενων φορέων σε ζητήματα προετοιμασίας για τον εντοπισμό, την ανάλυση και την αντιμετώπιση περιστατικών ασφάλειας των εθνικών ΚΥ, καθώς και η δοκιμή και η αξιολόγηση της επάρκειας των υφιστάμενων διαδικασιών και μηχανισμών προστασίας των εθνικών ΚΥ της χώρας.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Δ8. Προστασία Πληροφοριακών ΚΥ

Δ8.1. Δράση 8-1: Ασκήσεις Κυβερνο-ασφάλειας

Η δράση αυτή περιλαμβάνει ασκήσεις οι οποίες στοχεύουν στην αύξηση των δεξιοτήτων του προσωπικού των διαχειριστών των ΚΥ, σε θέματα κυβερνοασφάλειας. Τέτοιες ασκήσεις μπορούν να πραγματοποιούνται μεμονωμένα, σε επίπεδο τομέα ή και σε εθνικό επίπεδο, προκειμένου να ενισχύσουν την εμπειρία και την ανάπτυξη των δεξιοτήτων των εμπλεκόμενων στελεχών και των συμμετεχόντων σε αυτές.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Α/Β.

Αξιοποίηση Υφιστάμενων Δράσεων. Η ελληνική εθνική άσκηση κυβερνοάμυνας (ΠΑΝΟΠΤΗΣ), την οποία διοργανώνει σε ετήσια βάση το ΓΕΕΘΑ, σε συνεργασία με πολλούς φορείς του δημόσιου και του ιδιωτικού τομέα, είναι μια σημαντική δράση προς αυτή την κατεύθυνση.

Δ8.2. Δράση 8-2: Πλήρης Λειτουργικότητα και Διασύνδεση Ελληνικών CERT

Η δράση αυτή αποσκοπεί να διασφαλίσει την πλήρη λειτουργικότητα των Φορέων Άμεσης Ανταπόκρισης για περιστατικά και συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRT/CERT), με άμεση προτεραιότητα την πλήρη λειτουργία του κυβερνητικού CSIRT/CERT. Σημαντικό στοιχείο είναι η δραστηριοποίηση όλων των φορέων, κυρίως των Κατόχων/Διαχειριστών ΚΥ, και η καλή συνεργασία τους με τους αρμόδιους φορείς CERT/CIRT, για την άμεση καταγραφή των κυβερνοαπειλών και την έγκαιρη ενημέρωση πιθανών στόχων τέτοιων επιθέσεων.

Εκτιμώμενος χρόνος εφαρμογής: Φάση Β.

Δ9. Συνοπτική Παρουσίαση Δομής Προτεινόμενης Πολιτικής Προστασίας Εθνικών ΚΥ

Στο Σχήμα 6 που ακολουθεί παρουσιάζεται, συνοπτικά, η προτεινόμενη Πολιτική Προστασίας Εθνικών Κρίσιμων Υποδομών. Σε κάθε Τομέα Προτεραιότητας εμφανίζονται συνοπτικά οι προτεινόμενες δράσεις, οι οποίες προτάθηκαν με σκοπό την εφαρμογή των στόχων του εκάστοτε τομέα.

Σημειώνεται ότι οι τομείς προτεραιότητας καλύπτουν το οργανωτικό, το κανονιστικό και το εκτελεστικό/λειτουργικό επίπεδο.

Σχήμα 6: Συνοπτική Παρουσίαση Προτεινόμενου Σχεδίου Ολιστικής Πολιτικής Προστασίας Εθνικών Κρίσιμων Υποδομών

ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Σχέδιο Δράσης για την Προστασία των Εθνικών Κρίσιμων Υποδομών

Ε. Σχέδιο Δράσης για την Εφαρμογή Ολιστικής Πολιτικής Προστασίας των Εθνικών Κρίσιμων Υποδομών

Για να υλοποιηθούν αποτελεσματικά οι δράσεις που αναπτύχθηκαν στην προηγούμενη ενότητα, με βάση τους τομείς προτεραιότητας που ορίστηκαν στην Ενότητα Γ, απαιτείται ένα Σχέδιο Δράσης (Action Plan), το οποίο να ορίζει τις αναγκαίες χρονικές προτεραιότητες και τις εξαρτήσεις μεταξύ των προτεινόμενων επιμέρους δράσεων.

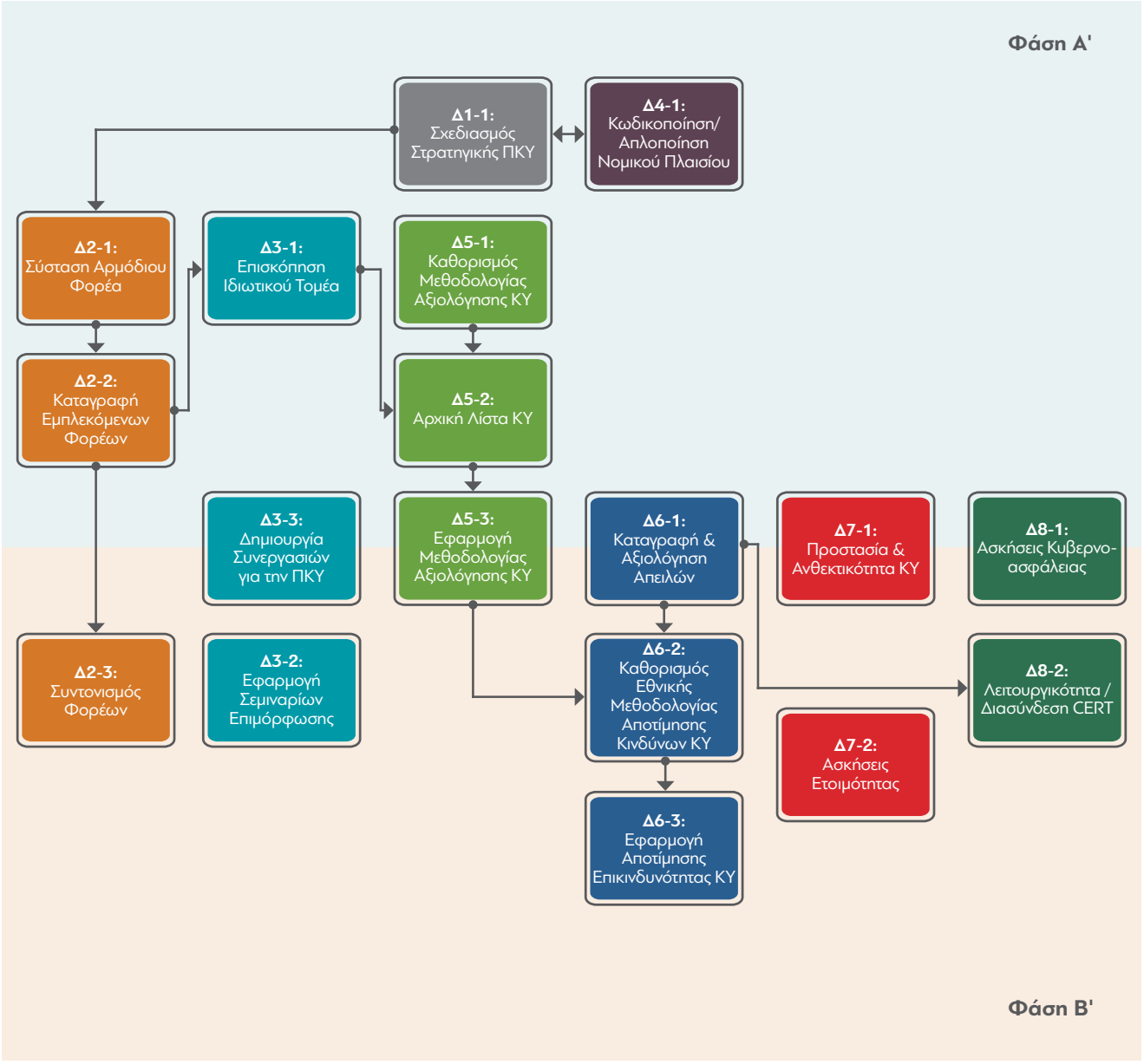
Η ανάπτυξη του Σχεδίου Δράσης θέτει χρονικές προτεραιότητες στις προτεινόμενες δράσεις και επισημαίνει πιθανές εξαρτήσεις μεταξύ των δράσεων για την υλοποίηση της στρατηγικής, με βάση τις αρχές και τις στρατηγικές δραστηριότητες προτεραιότητας. Το Σχέδιο Δράσης θα περιλαμβάνει τις λεπτομέρειες σχετικά με το πώς μπορούν να υποστηριχθούν οι ΚΥ και πώς η εφαρμογή της στρατηγικής θα επιφέρει τα επιθυμητά αποτελέσματα.

Ένα ολοκληρωμένο Σχέδιο Δράσης πρέπει να είναι προϊόν στενής συνεργασίας της εντεταλμένης κρατικής Οργανωτικής Δομής με τους άλλους φορείς του δημοσίου αλλά και του ιδιωτικού τομέα, όπου αυτός εμπλέκεται (κυρίως οι Κάτοχοι/Διαχειριστές ΚΥ).

Στο Σχήμα 7 που ακολουθεί παρουσιάζεται ένας γενικός (generic) οδηγός εφαρμογής, ο οποίος θα μπορούσε να αποτελέσει πυξίδα για την εκπόνηση και την εφαρμογή ενός ρεαλιστικού Σχεδίου Δράσης από τον εκάστοτε αρμόδιο φορέα.

Στο σχήμα αυτό οι δράσεις έχουν ταξινομηθεί στην προτεινόμενη φάση εφαρμογής, όπως ορίστηκε στην προηγούμενη ενότητα. Επιπλέον, έχει γίνει προσπάθεια να οριστούν οι διαφαινόμενες εξαρτήσεις μεταξύ των διαφόρων δράσεων, ανεξαρτήτως του τομέα προτεραιότητας όπου ανήκουν. Για παράδειγμα, σύμφωνα με το προτεινόμενο σχέδιο εφαρμογής, η δημιουργία της αρχικής λίστας ΚΥ (βλ. Δράση Ε2) εξαρτάται τόσο από την επισκόπηση του ιδιωτικού τομέα (βλ. Δράση Γ1) όσο και από τον καθορισμό της μεθοδολογίας αξιολόγησης των ΚΥ (βλ. Δράση Ε2). Αντίστοιχα, ο Σχεδιασμός της Στρατηγικής (βλ. Δράση Α1) εξαρτάται, αλλά και επηρεάζει τον Καθορισμό του Νομικού Πλαισίου (βλ. Δράση Δ1).

Σχήμα 7: Γενικό Σχέδιο Δράσης για την Εφαρμογή της Πολιτικής Προστασίας ΚΥ



ΟΛΙΣΤΙΚΗ ΠΡΟΣΤΑΣΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

Μέρος Γ': Πρόταση Ολιστικής Πολιτικής Προστασίας Και Ανθεκτικότητας Κρίσιμων Υποδομών

Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών, Οικονομικό Πανεπιστήμιο Αθηνών

Ιούνιος 2016

Συμπεράσματα

ΣΤ. Συμπεράσματα

Η ανάγκη για την προστασία των ΚΥ είναι πραγματική, με αντιμαχόμενες τάσεις μεταξύ της απαίτησης για μέγιστη αποτελεσματικότητα στην προστασία των ΚΥ και του υψηλού κόστους επίτευξης μιας υψηλής ανθεκτικότητας των ΚΥ. Οι παραπάνω αντικρουόμενες απαιτήσεις πρέπει να αντιμετωπιστούν μέσα από τη χάραξη μιας κατάλληλης πολιτικής Ολιστικής Προστασίας των ΚΥ.

Τα βασικά θεμέλια μιας πολιτικής Ολιστικής Προστασίας ΚΥ είναι η υιοθέτηση ενός γενικού στρατηγικού στόχου (Όραμα), που αναλύεται σε επιμέρους μετρήσιμους στόχους. Αμφότεροι κοινοποιούνται ευρέως στους χειριστές και στους χρήστες των ΚΥ, ενώ η υλοποίησή τους επιτυγχάνεται μέσω μιας δομημένης Στρατηγικής Προστασίας των ΚΥ, σε συνδυασμό με την ισχυρή πολιτική δέσμευση από το εκάστοτε Κ-Μ που την εφαρμόζει. Η Προστασία των ΚΥ σε εθνικό επίπεδο γίνεται κατανοητή ως μια αλληλεπίδραση κατευθυντήριων οδηγιών, που υιοθετούνται και συμβάλλουν στη δημιουργία μιας αποτελεσματικής Στρατηγικής Ολιστικής Προστασίας των ΚΥ.

Τα βασικότερα συμπεράσματα που προέκυψαν από την εκπόνηση του παρόντος Μέρους Γ' της παρούσας μελέτης ως εξής:

Τα βασικά θεμέλια μιας πολιτικής Ολιστικής Προστασίας ΚΥ είναι ο καθορισμός ενός δομημένου πλαισίου προστασίας και ασφάλειας των Κρίσιμων Υποδομών.

Ένα τέτοιο πλαίσιο προϋποθέτει την υιοθέτηση στρατηγικών στόχων (Οράματος), των οποίων η επίτευξη θα στηρίζεται σε αυστηρά καθορισμένους Τομείς Προτεραιότητας.

Οι βασικοί τομείς προτεραιότητας μιας Στρατηγικής Ολιστικής Προστασίας των ΚΥ είναι:

Σε **Οργανωτικό** επίπεδο:
- Καθορισμός Οράματος και Μετρήσιμων Στόχων
- Καθορισμός Οργανωτικής Δομής Διοίκησης για την Προστασία Κρίσιμων Υποδομών
- Καθορισμός Συνεργασιών Κράτους και Ιδιωτικών Φορέων

Σε **Κανονιστικό** επίπεδο:
Καθορισμός του σχετικού Νομικού και Κανονιστικού Πλαισίου

Σε **Εκτελεστικό/Λειτουργικό** επίπεδο:
Καταγραφή και Αξιολόγηση Εθνικών ΚΥ
Διαρκής Αποτίμηση Επικινδυνότητας ΚΥ
Διαχείριση Ανθεκτικότητας ΚΥ και Διαχείριση Κρίσεων
Προστασία Πληροφοριακών ΚΥ

Οι Τομείς Προτεραιότητας της Πολιτικής υλοποιούνται μέσα από συγκεκριμένες και εφαρμόσιμες δράσεις (actions), οι οποίες θα πρέπει να είναι σαφώς ορισμένες και να έχουν μετρήσιμους στόχους. Στο παρόν μέρος της μελέτης ορίστηκαν συγκεκριμένες και εφαρμόσιμες δράσεις προς αυτή την κατεύθυνση.

Η υλοποίηση της Πολιτικής Προστασίας Κρίσιμων Υποδομών επιτυγχάνεται μέσω ενός Σχεδίου Δράσης, το οποίο θέτει ένα σαφές και ορισμένο χρονοδιάγραμμα εκτέλεσης των επιμέρους δράσεων. Το προτεινόμενο σχέδιο θα μπορούσε να αποτελέσει ένα χρήσιμο οδηγό για την εκάστοτε αρμόδια υπηρεσία, ώστε να καθορίσει πλήρως ένα ρεαλιστικό Σχέδιο Δράσης.

Εννοιολογική Οριοθέτηση

Για την προσέγγιση του ζητήματος που μας απασχολεί αξιοποιούμε μία σειρά εννοιών, τις οποίες ορίζουμε σύμφωνα με τα σχετικά διεθνή πρότυπα και την υπάρχουσα βιβλιογραφία [βλ. Γκρίτζαλης (2004), ISO/IEC73 (2002), ISO/IEC 13335-1(2004), NIST SP 800-30 (2002)]:

Αγαθό (Asset): Ανθρώπινοι ή/και άυλοι πόροι, οι οποίοι είναι ευλόγως σκόπιμο να προστατευθούν, μεταξύ άλλων, λόγω και της εγγενούς σημασίας/χρησιμότητάς τους.

Υποδομή (Infrastructure): Πλέγμα αλληλοεξαρτώμενων δικτύων και συστημάτων που παρέχει αξιόπιστη ροή προϊόντων, υπηρεσιών και αγαθών, για τη λειτουργία της Διοίκησης, της Οικονομίας, της Κοινωνίας ή/και άλλων υποδομών.

Κρίσιμη Υποδομή (ΚΥ) ή **Υποδομή Ζωτικής Σημασίας** (ΥΖΣ) (Critical Infrastructure): Υποδομή μεγάλης κλίμακας, της οποίας τυχόν υποβάθμιση, διακοπή ή δυσλειτουργία έχει σοβαρή επίπτωση στη Δημόσια Υγεία, στην Ασφάλεια και ευμάρεια των πολιτών καθώς και στην ομαλή λειτουργία της Δημόσιας Διοίκησης ή/και της Οικονομίας. Στο παρόν έγγραφο, καθώς και σε όλα τα επιμέρους τμήματα της μελέτης, οι όροι (και τα αντίστοιχα ακρωνύμια) Κρίσιμη Υποδομή (ΚΥ) και Υποδομή Ζωτικής Σημασίας (ΥΖΣ) χρησιμοποιούνται εναλλακτικά ως ταυτόσημοι όροι[34].

34. Με ανάλογο τρόπο χρησιμοποιούνται και στη διεθνή βιβλιογραφία.

Πληροφοριακή και Επικοινωνιακή Υποδομή (ΠΕΥ): Υποδομή που αποσκοπεί στην παροχή πληροφοριών, υπηρεσιών επικοινωνίας ή άλλων ηλεκτρονικών υπηρεσιών μιας ΚΥ, π.χ., για την υποστήριξη της λειτουργίας, τη διαχείριση ή τον έλεγχο της ΚΥ.

Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ): Πληροφοριακά και Επικοινωνιακά αγαθά τα οποία χρησιμοποιούνται για την παροχή ή την υποστήριξη της παροχής μιας υπηρεσίας. Οι ΤΠΕ ενδέχεται να υποστηρίζουν μια Κρίσιμη Υποδομή ή να αποτελούν οι ίδιες μια Κρίσιμη (Πληροφοριακή και Επικοινωνιακή) Υποδομή.

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 ΚΥ (Critical Protection): Ενέργειες των κατόχων, κατασκευαστών, χρηστών, διαχειριστών, ερευνητικών ιδρυμάτων, Δημόσιας Διοίκησης ή/και κανονιστικών/ρυθμιστικών αρχών, για την τήρηση της ποιοτικής λειτουργίας της υποδομής σε περίπτωση επιθέσεων, ατυχημάτων και σφαλμάτων, καθώς και για την ανάκαμψη, σε εύλογο χρόνο, της υποδομής μετά από τέτοια γεγονότα.

Συστατικά ΚΥ (Στοιχεία ΠΕΥ): Δίκτυα επικοινωνίας, λογισμικό, υλικό, υπηρεσίες, ανθρώπινο δυναμικό ή οποιοδήποτε άλλο μέσο αξιοποιείται για την αποτελεσματική διαχείριση μιας ΠΕΥ.

Ακεραιότητα ΚΥ (Integrity): Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφοριακής και επικοινωνιακής υποδομής η οποία αποτελεί συστατικό μιας ΚΥ.

Εμπιστευτικότητα ΚΥ (Confidentiality): Αποφυγή αποκάλυψης των πληροφοριών που διακινούνται σε μια πληροφοριακή και επικοινωνιακή υποδομή η οποία αποτελεί συστατικό μιας ΚΥ, χωρίς την άδεια του ιδιοκτήτη τους.

Διαθεσιμότητα ΚΥ (Availability): Αποφυγή μη εύλογων καθυστερήσεων στην εξουσιοδοτημένη προσπέλαση των πόρων (πληροφοριακών ή οποιασδήποτε άλλης μορφής) μιας ΚΥ.

Ασφάλεια ΚΥ (Information and Communication Infrastructure Security): Τήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των κάθε είδους πόρων μιας ΚΥ[35].

Παραβίαση ΚΥ (Violation): Γεγονός κατά το οποίο προσβλήθηκαν μία ή περισσότερες από τις ιδιότητες –διαθεσιμότητα, εμπιστευτικότητα και ακεραιότητα– μιας ΚΥ.

Απειλή ΚΥ (Threat): Πιθανή ενέργεια ή γεγονός που μπορεί να προκαλέσει την απώλεια κάποιου χαρακτηριστικού της ασφάλειας μιας πληροφοριακής και επικοινωνιακής υποδομής.

Τρωτότητα ΚΥ (Ευπάθεια, Αδυναμία) (Vulnerability): Σημείο μιας ΚΥ που μπορεί να επιτρέψει να συμβεί κάποια παραβίαση.

Επίπτωση (Impact): Απώλεια μιας αξίας, η αύξηση του κόστους ή κάθε άλλη ζημία που θα μπορούσε να προκύψει ως συνέπεια μιας συγκεκριμένης παραβίασης μιας ΚΥ.

35. Για τους οποίους έχουν έννοια οι προαναφερθείσες ιδιότητες.

Πιθανοφάνεια (Ενδεχομενικότητα) (Likelihood): Η πιθανότητα εκδήλωσης μιας απειλής, σταθμισμένη με το βαθμό τρωτότητας του στόχου της απειλής.

Μέσο Προστασίας (Ελεγχος) (Safeguard – Control): Διαδικασία ή τεχνικό μέτρο που επιδιώκει να εμποδίσει μια παραβίαση ή να μειώσει τις επιπτώσεις της σε μια ΚΥ.

Επικινδυνότητα ΚΥ (Διακινδύνευση) (Risk): Το ενδεχόμενο μια δεδομένη απειλή να αξιοποιήσει την τρωτότητα κάποιων αγαθών και να προκαλέσει βλάβη σε μια ΚΥ.

Ανάλυση επικινδυνότητας ΚΥ (Risk analysis): Η συστηματική αξιοποίηση πληροφοριών για την αναγνώριση των πόρων μιας ΚΥ και για την εκτίμηση της επικινδυνότητάς τους.

Διαχείριση επικινδυνότητας ΚΥ (Risk management): Η διαδικασία στάθμισης εναλλακτικών μέσων ασφάλειας, σε συνεννόηση με τους εμπλεκόμενους φορείς και λαμβάνοντας υπόψη τα αποτελέσματα της ανάλυσης επικινδυνότητας και το ισχύον νομικό πλαίσιο, προκειμένου να επιλεγούν τα καταλληλότερα μέσα ασφάλειας μιας ΚΥ.

Σχήματα

Σχήμα 1: Πλατφόρμα Ανταλλαγής Πληροφοριών στο Κέντρο CPNI..... 25
Σχήμα 2: Επίπεδα Εφαρμογής της Αποτίμησης Επικινδυνότητας ΚΥ..... 38
Σχήμα 3: Διάκριση μεταξύ Προστασίας ΥΖΣ και Πληροφοριακών Υποδομών.....42
Σχήμα 4: Προστασία Πληροφοριακών ΚΥ και Ασφάλεια στον Κυβερνοχώρο.....43
Σχήμα 5: Γενική Περιγραφή Προτεινόμενης Μεθοδολογίας Αξιολόγησης Εθνικών ΚΥ..... 55
Σχήμα 6: Σύνοψη Σχεδίου Ολιστικής Πολιτικής Προστασίας Εθνικών ΚΥ..... 62
Σχήμα 7: Γενικό Σχέδιο Δράσης για την Εφαρμογή της Πολιτικής Προστασίας ΚΥ..... 65

Πίνακες

Πίνακας 1: Αξιολόγηση Ωριμότητας Προστασίας Εθνικών ΚΥ στην Ε.Ε. (EU Dashboard, 2014)..... 21
Πίνακας 2: Ολιστική Προσέγγιση Αποτίμησης Κινδύνων..... 28

Βιβλιογραφία/Ηλεκτρονικές Πηγές

Cavelty, M. D., & Suter, M. (2012). "The art of CIIP strategy: tacking stock of content and processes". *In Critical Infrastructure Protection* (pp. 15-38). Springer Berlin Heidelberg.

ENISA (2007) EISAS – European Information Sharing and Alert System. Online: https://www.enisa.europa.eu/publications/eisas-deployment-feasibility-study/at_download/fullReport

ENISA (2014). R. Mattioli, C. Levy-Bencheton. Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report, December 2014. Ανακτήθηκε από: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport

ENISA (2015). Stocktaking, Analysis and Recommendations on the protection of CIIs. https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

ENISA (2015b). Inventory of CERT activities in Europe. https://www.enisa.europa.eu/publications/inventory-of-cert-activities-in-europe

EU Commission (2005). European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, Brussels. Ανακτήθηκε από: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN

EU Commission (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final. Ανακτήθηκε από: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33260&from=EN

EU Commission 149 (2009). European Commission. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". Com(2009) 149 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

EU Commission (2010). European Commission, Europe 2020. A strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels 3.3.2010.

EU Commission (2012). European Commission, staff working document on

the review of the European Programme for Critical Infrastructure Protection (EPCIP), Brussels. Ανακτήθηκε από: http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

EU Commission (2013). European Commission, staff working document on on a new approach to the European Programme for Critical Infrastructure Protection making European Critical Infrastructures more secure), Brussels, Belgium. Ανακτήθηκε από: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

EU Commission (2013b). European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048

EU Council (2007). Council of the European Union, Adoption of the Council Conclusions on a European Programme for Critical Infrastructure Protection. Ανακτήθηκε από: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%207743%202007%20INIT

EU Council (2008). Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', Official Journal L 345, P.0075-0082.

EU Council (2008b). Council of the European Union, Non-Binding Guidelines for the application of the Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels [14808/08]. Ανακτήθηκε από: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015616%202008%20INIT

EU Council (2008c). Proposal for a COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN). COM(2008) 676 final. Ανακτήθηκε από: http://ccpic.mai.gov.ro/docs/COM(2008)676 final CIWIN_EN.pdf

FC (2009). Federal Council's Basic Strategy for Critical Infrastructure Protection, Basis for the national critical infrastructure protection strategy. Confédération Swisse, 18 May, 2009. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.42043.DownloadFile.tmp/grundstrategieski20090518e.pdf (ημερομηνία πρόσβασης: 15-11-2015)

FC (2009b). Critical Infrastructure Protection - Second Report to the Federal Council and Measures for the Period 2009–2011. Federal Office for Civil Protection, 18 May, 2009. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.60516.downloadList.59025.DownloadFile.tmp/2berichtski20090605e.pdf (ημε-

ρομνία πρόσβασης 05. 12.2015).

FOCP (2013). A Method for Risk Analysis of Disasters and Emergencies in Switzerland. Federal Office for Civil Protection, Bern, 2013. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/gefaehrdungen-risiken/nat__gefaehrdungsanlayse.parsysrelated1.91664.DownloadFile.tmp/methodenbericht20133107en.pdf

FRG (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Ministry of the Interior, Federal Republic of Germany. Berlin, June 17, 2009. Ανακτήθηκε από: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

French Strategy (2015). French national digital security strategy. French Republic, 2015. Ανακτήθηκε από: http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (ημερομνία πρόσβασης: 5-12-2015)

Klaver, M. H. A., Luiijf, H. A. M., & Nieuwenhuijsen, A. H. (2011). RECIPE: Good practices manual for CIP policies, for policy makers in Europe. Ανακτήθηκε από: http://repository.tudelft.nl/search/tno/?q=title%3A%22RECIPE%20%3A%20Good%20practices%20manual%20for%20CIP%20policies%2C%20for%20policy%20makers%20in%20Europe%22

Lebau-Marianna, D., & E. Roger (2015). France – three decrees reinforced the safety obligations of Operators of Vital Importance. July 8, 2015. http://www.lexology.com/library/detail.aspx?g=111ccbaf-b3cb-4efa-8fb3-8db74b57c2be (ημερομνία πρόσβασης 01.12. 2015).

Livre Blanc (2013). Défense et sécurité nationale, République Francaise, 2013. Ανακτήθηκε από: http://fr.calameo.com/read/000331627d6f04ea4fe0e (ημερομνία πρόσβασης: 1/12/2015).

Luiijf, E., Burger, H., & Klaver, M. (2003). "Critical infrastructure protection in the Netherlands: A Quick-scan". In *EICAR Conference Best Paper Proceedings* (Vol. 19). EICAR, Denmark.

MSB (2011). A first step towards a national risk assessment. Swedish Civil Contingencies Agency-MSB, Sweden, 2011. On-line: https://www.msb.se/RibData/Filer/pdf/26189.pdf

MSB (2014). Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. Swedish Civil Contingencies Agency (MSB), Risk & Vulnerability Reduction Department. https://www.msb.se/RibData/Filer/pdf/27412.pdf

Nečesal, L., & Lukáš, L. (2011). "Entities of critical infrastructure protection in the Czech Republic". In *Recent Researches in Automatic Control-13th WSEAS International Conference on Automatic Control, Modelling and Simulation*, ACMOS'11.

Novotný, P., Markuci, J., Řehák, D., Almarzouqi, I., & Janušová, L. (2015).

"Proposal of Systems Approach to Critical Infrastructure Determination in European Union Countries". In: *TRANSCOM 2015,* June 2015. http://www.researchgate.net/profile/David_Rehak/publication/279178787_Proposal_of_Systems_Approach_to_Critical_Infrastructure_Determination_in_European_Union_Countries/links/558c40e008ae591c19d9f76f.pdf

Parliament of Estonia (2009) Emergency Act, State Gazette I, 39, 262, 2009. Ανακτήθηκε από: http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=en&sk=et&dok=XXXXX26.htm&query=H%E4daolukorra+seadus&tyyp=X&ptyyp=RT&fr=no&pg=1 (ημερομηνία πρόσβασης: 15.11. 2015).

Renda, A., & Hammerli, B. (2010). Protecting critical infrastructure in the EU. CEPS Task Force Report. http://ccpic.mai.gov.ro/docs/Critical Infrastructure Protection Final A4.pdf

SG (2011). Secure and Resilient: A Strategic Framework for Critical National Infrastructure in Scotland. Edinburgh, UK: The Scottish Government. Ανακτήθηκε από: http://www.gov.scot/Resource/Doc/346469/0115308.pdf

SGDSN (2015). Secrétariat général de la défense et de la sécurité nationale (SGDSN). Organisation des secteurs d'activités d'importance vitale http://www.sgdsn.gouv.fr/site_rubrique70.html (ημερομηνία πρόσβασης: 15/11/2015).

UK (2010). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Ανακτήθηκε από: https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards

διαΝΕΟσις

ΟΡΓΑΝΙΣΜΟΣ ΕΡΕΥΝΑΣ & ΑΝΑΛΥΣΗΣ