ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ

Βρυξέλλες, 17.11.2005
COM(2005) 576 τελικό

ΠΡΑΣΙΝΟ ΒΙΒΛΙΟ

για το Ευρωπαϊκό Πρόγραμμα Προστασίας των Υποδομών Ζωτικής Σημασίας (EPCIP)

(υποβληθέν από την Επιτροπή)

ΠΡΑΣΙΝΟ ΒΙΒΛΙΟ

για το Ευρωπαϊκό Πρόγραμμα Προστασίας των Υποδομών Ζωτικής Σημασίας (EPCIP)

1. ΙΣΤΟΡΙΚΟ

Οι Υποδομές Ζωτικής Σημασίας (ΥΖΣ) είναι δυνατόν να υποστούν ζημίες, να καταστραφούν ή να διακοπεί η λειτουργία τους με εσκεμμένες τρομοκρατικές ενέργειες, φυσικές καταστροφές, αμέλεια, ατυχήματα ή ηλεκτρονική πειρατεία, εγκληματικές ενέργειες και δόλια συμπεριφορά. Για τη διάσωση της ζωής και της περιουσίας των κατοίκων της ΕΕ που κινδυνεύουν από την τρομοκρατία, τις φυσικές καταστροφές και τα ατυχήματα, κάθε διακοπή της λειτουργίας ή χειραγώγηση των ΥΖΣ θα πρέπει, ενόσω τούτο είναι δυνατόν, να είναι μικρής διάρκειας, σπάνια, ελέγξιμη, γεωγραφικά περιορισμένη και ελάχιστα επιζήμια για την ευπραγία των κρατών μελών, των πολιτών τους και της Ευρωπαϊκής Ένωσης. Οι πρόσφατες τρομοκρατικές επιθέσεις στη Μαδρίτη και στο Λονδίνο ανάδειξαν τον κίνδυνο τρομοκρατικών επιθέσεων κατά των ευρωπαϊκών έργων υποδομής. Η απάντηση της ΕΕ πρέπει να είναι ταχεία, συντονισμένη και αποτελεσματική.

Το Ευρωπαϊκό Συμβούλιο του Ιουνίου 2004 ζήτησε από την Επιτροπή να εκπονήσει μια συνολική στρατηγική για την προστασία των ΥΖΣ. Ανταποκρινόμενη η Επιτροπή εξέδωσε στις 20 Οκτωβρίου 2004 την ανακοίνωση «Προστασία των υποδομών ζωτικής σημασίας στην καταπολέμηση της τρομοκρατίας», με σαφείς προτάσεις για την ενίσχυση της πρόληψης, της ετοιμότητας και της αντιμετώπισης τρομοκρατικών επιθέσεων κατά ΥΖΣ.

Τα συμπεράσματα του Συμβουλίου σχετικά με την «Πρόληψη, ετοιμότητα και αντιμετώπιση τρομοκρατικών επιθέσεων» και το «Πρόγραμμα αλληλεγγύης για τις συνέπειες των τρομοκρατικών απειλών και επιθέσεων», το οποίο εξέδωσε το Συμβούλιο τον Δεκέμβριο του 2004, προσυπέγραφαν την πρόθεση της Επιτροπής να προτείνει ένα πρόγραμμα για την προστασία των ΥΖΣ (European Programme for Critical Infrastructure Protection - EPCIP), συμφωνούσαν δε ως προς τη σύσταση από την Επιτροπή ενός δικτύου προειδοποιητικών πληροφοριών για τις ΥΖΣ (Critical Infrastructure Warning Information Network - CIWIN).

Η Επιτροπή διοργάνωσε δύο σεμινάρια και ζήτησε να προταθούν ιδέες και σχόλια από τα κράτη μέλη. Το πρώτο σεμινάριο διεξήχθη στις 6-7 Ιουνίου 2005, με τη συμμετοχή των κρατών μελών. Μετά το σεμινάριο αυτό, τα κράτη μέλη έδωσαν στην Επιτροπή έγγραφα αναφοράς για την προσέγγισή τους στο ζήτημα της προστασίας των ΥΖΣ και σχολίασαν τις ιδέες που είχαν συζητηθεί κατά το σεμινάριο. Τα αποσταλέντα έγγραφα ελήφθησαν τον Ιούνιο και τον Ιούλιο, και αποτέλεσαν τη βάση για την περαιτέρω επεξεργασία του ως άνω ζητήματος. Το δεύτερο σεμινάριο διεξήχθη στις 12-13 Σεπτεμβρίου με σκοπό την προώθηση της συζήτησης των ζητημάτων προστασίας των ΥΖΣ. Στο σεμινάριο αυτό έλαβαν μέρος τόσο τα κράτη μέλη όσο και οι επαγγελματικές τους οργανώσεις. Ως κατάληξη του σεμιναρίου αυτού, η Επιτροπή αποφάσισε να συντάξει την παρούσα πράσινη βίβλο, όπου σκιαγραφούνται οι επιλογές που προτείνονται για το EPCIP.

2. ΣΤΟΧΟΙ ΤΗΣ ΠΑΡΟΥΣΑΣ ΠΡΑΣΙΝΗΣ ΒΙΒΛΟΥ

Βασικός στόχος της πράσινης βίβλου είναι η εξασφάλιση στοιχείων ανάδρασης σχετικά με τις πιθανές επιλογές για το EPCIP, μέσω της εμπλοκής μεγάλου αριθμού ενδιαφερομένων. Η έμπρακτη προστασία των ΥΖΣ απαιτεί επικοινωνία, συντονισμό και συνεργασία τόσο σε εθνικό όσο και σε κοινοτικό επίπεδο μεταξύ όλων των ενδιαφερομένων - κατόχων και διαχειριστών των έργων υποδομής, ρυθμιστικών αρχών, επαγγελματικών οργανώσεων και φορέων, σε συνεργασία με όλες τις κυβερνητικές βαθμίδες και με το κοινό.

Η παρούσα πράσινη βίβλος παρέχει επιλογές ως προς το πώς η Επιτροπή είναι δυνατόν να ανταποκριθεί στο αίτημα του Συμβουλίου για την εκπόνηση του EPCIP και τη σύσταση του CIWIN, αποτελεί δε τη δεύτερη φάση της διαδικασίας διαβουλεύσεων σχετικά με την εκπόνηση του EPCIP. Η Επιτροπή ευελπιστεί ότι, παρουσιάζοντας αυτή την πράσινη βίβλο, θα λάβει συγκεκριμένα στοιχεία ανάδρασης ως προς τις πολιτικές επιλογές που σκιαγραφούνται στο παρόν έγγραφο. Ανάλογα δε με το αποτέλεσμα των διαβουλεύσεων, θα μπορούσε κατά το 2006 να προταθεί μια δέσμη πολιτικών μέτρων για το EPCIP.

3. ΣΚΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ EPCIP

3.1. Ο γενικός του EPCIP

Στόχος του EPCIP θα μπορούσε να είναι η εξασφάλιση επαρκών και ισοδύναμων επιπέδων προστασίας των ΥΖΣ, περιορισμένες στο ελάχιστο αστοχίες και ταχείες και δοκιμασμένες μεθόδους αποκατάστασης σε ολόκληρη την ΕΕ. Το επίπεδο προστασίας δεν είναι δυνατόν να είναι το ίδιο για όλες τις ΥΖΣ, εξαρτάται δε από τις επιπτώσεις τυχόν αστοχίας της εκάστοτε ΥΖΣ. Το EPCIP θα μπορούσε να αποτελέσει μια αδιάλειπτη διαδικασία, ενώ με την τακτική αναθεώρησή του θα λαμβάνονται υπόψη τα νέα ζητήματα και ανησυχίες.

Το EPCIP θα πρέπει να ελαχιστοποιεί, ενόσω τούτο είναι δυνατόν, κάθε αρνητική επίπτωση που είναι δυνατόν να προκύψει για την ανταγωνιστικότητα ενός συγκεκριμένου κλάδου από τις αυξημένες επενδύσεις για την ασφάλεια. Κατά τον υπολογισμό της αναλογικότητας των δαπανών, δεν θα πρέπει να αγνοείται η ανάγκη διατήρησης της σταθερότητας των αγορών, η οποία είναι ζωτικής σημασίας για τις μακροπρόθεσμες επενδύσεις, καθώς και η επίδραση της ασφάλειας στην πορεία των χρηματιστηρίων και στους μακροοικονομικούς δείκτες.

Ερώτημα

Αυτός ο στόχος του EPCIP είναι ο ενδεδειγμένος; Εάν όχι, ποιος θα πρέπει να είναι;

3.2. Από τι θα πρέπει να προστατεύει το EPCIP

Αν και τα μέτρα που λαμβάνονται για τη διαχείριση των συνεπειών των περισσότερων διακοπών λειτουργίας είναι πανομοιότυπα ή παρόμοια, τα μέτρα προστασίας είναι δυνατόν να διαφέρουν ανάλογα με τη φύση της απειλής. Στις απειλές που θα μπορούσαν να μειώσουν σημαντικά την ικανότητα κάλυψης των ουσιωδών αναγκών και της ασφάλειας του πληθυσμού, διατήρησης της τάξης και παροχής των ελάχιστων ουσιωδών υπηρεσιών κοινής ωφέλειας ή ομαλής λειτουργίας της οικονομίας, είναι δυνατόν να συμπεριλαμβάνονται τόσο οι εσκεμμένες επιθέσεις όσο και οι φυσικές καταστροφές. Οι επιλογές είναι:

α) **μια συνολική προσέγγιση για όλες τις απειλές** – Θα μπορούσε να είναι μια περιεκτική προσέγγιση, η οποία να λαμβάνει υπόψη τόσο τις εσκεμμένες επιθέσεις όσο και τις φυσικές

καταστροφές. Τούτο θα εξασφάλιζε τη μέγιστη αξιοποίηση των συνεργειών μεταξύ μέτρων προστασίας, χωρίς όμως να δίνει ιδιαίτερη έμφαση στην τρομοκρατία·

β) **μια συνολική προσέγγιση με προτεραιότητα στην τρομοκρατία** – Θα μπορούσε να είναι μια ευέλικτη προσέγγιση, η οποία να εξασφαλίζει τη διασύνδεση με άλλες μορφές απειλών, όπως εκείνη από εσκεμμένες επιθέσεις και φυσικές καταστροφές, αλλά με προτεραιότητα στην τρομοκρατία. Εάν το επίπεδο των μέτρων προστασίας σε έναν κλάδο της οικονομίας θεωρηθεί επαρκές, οι ενδιαφερόμενοι θα μπορούν να εστιάζουν την προσοχή τους σε απειλές έναντι των οποίων θα εξακολουθούν να είναι ευάλωτοι.

γ) **μια προσέγγιση με έμφαση στις τρομοκρατικές απειλές** – Θα ήταν μια προσέγγιση εστιασμένη στην τρομοκρατία, χωρίς όμως να δίνει ιδιαίτερη προσοχή σε περισσότερο συνήθεις απειλές.

Ερώτημα

Ποια προσέγγιση θα πρέπει να επιλέξει το EPCIP; Γιατί;

4. ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΒΑΣΙΚΕΣ ΑΡΧΕΣ

Προτείνεται, το EPCIP να βασισθεί στις ακόλουθες βασικές αρχές:

- **Επικουρικότητα** – Η επικουρικότητα θα είναι στο κέντρο του EPCIP, με την προστασία των ΥΖΣ να αποτελεί πρωτίστως και κυρίως εθνική αρμοδιότητα. Η κύρια ευθύνη για την προστασία των ΥΖΣ θα ανήκει στα κράτη μέλη και στους κατόχους/διαχειριστές, οι οποίοι θα ενεργούν σε ένα κοινό πλαίσιο. Η Επιτροπή, με τη σειρά της, θα εστιάζει τις δραστηριότητές της σε πτυχές της προστασίας των ΥΖΣ με κοινοτικό διασυνοριακό χαρακτήρα. Η ευθύνη και η λογοδοσία των κατόχων/διαχειριστών ως προς την λήψη αποφάσεων και την εκπόνηση σχεδίων για την προστασία των περιουσιακών τους στοιχείων δεν θα πρέπει να αλλάξει.

- **Συμπληρωματικότητα** – Το κοινό πλαίσιο του EPCIP θα είναι συμπληρωματικό με τα υφιστάμενα μέτρα. Όπου υπάρχουν ήδη κοινοτικοί μηχανισμοί, θα πρέπει να συνεχίσουν να χρησιμοποιούνται και να συμβάλλουν στην εξασφάλιση της συνολικής εφαρμογής του EPCIP.

- **Εμπιστευτικότητα** – Η ανταλλαγή πληροφοριών ως προς την προστασία των ΥΖΣ θα γίνεται σε ένα περιβάλλον εμπιστοσύνης και εμπιστευτικότητας. Τούτο γίνεται αναγκαίο αν ληφθεί υπόψη το ότι συγκεκριμένα στοιχεία σχετικά με τις ΥΖΣ είναι δυνατόν να χρησιμοποιηθούν για την πρόκληση αστοχιών ή ανεπιθύμητων συνεπειών στις ΥΖΣ. Τόσο σε κοινοτικό όσο και σε εθνικό επίπεδο, οι πληροφορίες για τις ΥΖΣ θα διαβαθμίζονται, η δε πρόσβαση σε αυτές θα επιτρέπεται μόνο σε περιπτώσεις δεόντως αιτιολογημένες.

- **Συνεργασία των ενδιαφερομένων** – Όλοι οι ενδιαφερόμενοι, συμπεριλαμβανόμενων των κρατών μελών, της Επιτροπής, των επαγγελματικών ενώσεων, των φορέων τυποποίησης και των κατόχων, διαχειριστών και χρηστών ΥΖΣ (με τους χρήστες να ορίζονται ως οι οργανισμοί που εκμεταλλεύονται και χρησιμοποιούν τις ΥΖΣ για λόγους επαγγελματικούς και για την παροχή υπηρεσιών) έχουν τον δικό τους ρόλο στην προστασία των ΥΖΣ. Όλοι οι ενδιαφερόμενοι θα πρέπει να συνεργάζονται και να συμβάλλουν στην εκπόνηση και στην εφαρμογή του EPCIP ανάλογα με τις εκάστοτε αρμοδιότητες και ρόλους. Οι αρχές

των κρατών μελών θα καθοδηγούν και θα συντονίζουν την ανάπτυξη και την εφαρμογή μιας συνεκτικής εθνικής προσέγγισης για την προστασία των ΥΖΣ στο πλαίσιο της δικαιοδοσίας τους. Οι κάτοχοι, διαχειριστές και χρήστες θα μετέχουν ενεργά τόσο σε εθνικό όσο και σε κοινοτικό επίπεδο. Εάν δεν υπάρχουν πρότυπα κατά τομέα, ή εάν δεν έχουν ακόμη θεσπισθεί διεθνή πρότυπα, οι οργανισμοί τυποποίησης θα μπορούσαν, όπου τούτο ενδείκνυται, να εκδώσουν κοινά πρότυπα.

- **Αναλογικότητα** – Οι στρατηγικές και τα μέτρα για την προστασία θα είναι ανάλογα προς το επίπεδο του εκάστοτε κινδύνου, καθόσον δεν είναι δυνατόν να προστατεύονται όλες οι ΥΖΣ από όλες τις απειλές (π.χ., τα δίκτυα ηλεκτρικής ενέργειας είναι πολύ μεγάλου μεγέθους για να περιφράσσονται ή να φυλάσσονται). Με την εφαρμογή των κατάλληλων τεχνικών διαχείρισης κινδύνων, η προσοχή θα εστιάζεται σε περιοχές μεγαλύτερου κινδύνου, με συνεκτίμηση της απειλής, της σχετικής ζωτικής σημασίας, της αποδοτικότητας, του επιπέδου της εξασφαλιζόμενης ασφάλειας και της αποδοτικότητας των διαθέσιμων στρατηγικών μετριασμού των κινδύνων.

Ερώτημα

Οι ως άνω αρχές είναι αποδεκτές; Είναι μερικές περιττές; Υπάρχουν και άλλες που θα έπρεπε να εξετασθούν; Συμφωνείτε ότι τα μέτρα προστασίας θα πρέπει να είναι ανάλογα προς τον εκάστοτε κίνδυνο, καθόσον δεν είναι δυνατόν να προστατεύονται όλες οι ΥΖΣ από όλες τις απειλές;

5. ΕΝΑ ΚΟΙΝΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΟ EPCIP

Η φθορά ή η απώλεια ενός έργου υποδομής σε ένα κράτος μέλος είναι δυνατόν να έχει αρνητικές επιπτώσεις και σε άλλα τέτοια έργα, καθώς και σε ολόκληρη την ευρωπαϊκή οικονομία. Τούτο γίνεται ολοένα και πιθανότερο, καθώς οι νέες τεχνολογίες (π.χ. το Διαδίκτυο) και η απελευθέρωση των αγορών (π.χ. της ηλεκτρικής ενέργειας και του φυσικού αερίου) σημαίνουν ότι πολλά έργα υποδομής αποτελούν τμήματα ενός ευρύτερου δικτύου. Σε ένα τέτοιο πλαίσιο, τα μέτρα προστασίας είναι τόσο ισχυρά όσο ο πιο αδύναμος κρίκος τους. Τούτο σημαίνει ότι μπορεί να χρειασθεί ένα κοινό επίπεδο προστασίας.

Η αποτελεσματική προστασία απαιτεί επικοινωνία, συντονισμό και συνεργασία σε εθνικό, κοινοτικό (όπου ενδείκνυται) και διεθνές επίπεδο μεταξύ των ενδιαφερομένων. Θα μπορούσε να δημιουργηθεί ένα κοινό κοινοτικό πλαίσιο προστασίας των ΥΖΣ στην Ευρώπη, έτσι ώστε να υπάρχει η βεβαιότητα ότι κάθε κράτος μέλος θα παρέχει επαρκή και ισοδύναμη προστασία των ΥΖΣ του, καθώς και ότι οι κανόνες ανταγωνισμού εντός της κοινής αγοράς δεν θα νοθεύονται. Με σκοπό να υποστηρίξει τις ενέργειες των κρατών μελών, η Επιτροπή σκοπεύει να διευκολύνει τον εντοπισμό, την ανταλλαγή και τη διάδοση των βέλτιστων πρακτικών σε ζητήματα προστασίας των ΥΖΣ, παρέχοντας ένα κοινό πλαίσιο για την προστασία αυτή. Το εύρος αυτού του κοινού πλαισίου θα πρέπει να μελετηθεί.

Το κοινό πλαίσιο για το EPCIP θα περιέχει οριζόντια μέτρα που θα καθορίζουν τις αρμοδιότητες και τις ευθύνες όλων των εμπλεκόμενων στην προστασία των ΥΖΣ, ενώ θα θέτει και τα θεμέλια για επιμέρους προσεγγίσεις κατά τομέα. Το κοινό τούτο πλαίσιο νοείται ως συμπλήρωμα των ισχυόντων κατά τομέα μέτρων της Επιτροπής και των κρατών μελών, έτσι ώστε να παρέχει το μέγιστο δυνατό επίπεδο ασφάλειας των ΥΖΣ που βρίσκονται στην ΕΕ. Θα πρέπει να δοθεί προτεραιότητα στις εργασίες για την επίτευξη συμφωνίας ως προς έναν κοινό κατάλογο ορισμών και τομέων ΥΖΣ.

Επειδή οι τομείς που περιλαμβάνουν ΥΖΣ παρουσιάζουν μεγάλη ποικιλία, θα ήταν δύσκολο να καθορισθούν επακριβώς τα κριτήρια προς χρήση για τον εντοπισμό και την προστασία όλων αυτών των ΥΖΣ σε ένα οριζόντιο πλαίσιο. Τούτο θα πρέπει να γίνει κατά τομέα. Ωστόσο, υπάρχει ανάγκη επίτευξης συναντίληψης ως προς ορισμένα οριζόντια ζητήματα.

Ως εκ τούτου, προτείνεται να επιδιωχθεί η ενίσχυση των ΥΖΣ στην ΕΕ μέσω της δημιουργίας ενός κοινού πλαισίου για το EPCIP (με κοινούς στόχους, μεθοδολογία π.χ. για την αντιπαραβολή και την αξιολόγηση των αλληλεξαρτήσεων), με ανταλλαγή των βέλτιστων πρακτικών και μηχανισμούς παρακολούθησης της συμμόρφωσης. Μερικά από τα στοιχεία που θα μπορούσαν να ενταχθούν σε ένα τέτοιο κοινό πλαίσιο είναι:

- κοινές αρχές προστασίας των ΥΖΣ·
- κοινά αποδεκτοί κώδικες/πρότυπα·
- κοινοί ορισμοί βάσει των οποίων θα μπορούν να συμφωνούνται επιμέρους ορισμοί κατά τομέα (στο παράρτημα 1 εμφαίνονται ενδεικτικά ορισμένοι τέτοιοι ορισμοί)·
- κοινός κατάλογος τομέων ΥΖΣ (στο παράρτημα 2 εμφαίνονται ενδεικτικά ορισμένοι τέτοιοι τομείς)·
- τομείς προτεραιότητας στην προστασία των ΥΖΣ·
- περιγραφή των ευθυνών των εμπλεκομένων·
- κοινά στοιχεία συγκριτικής ανάλυσης·
- μεθοδολογίες για τη σύγκριση και την ιεράρχηση των ΥΖΣ στους διάφορους· τομείς.

Ένα τέτοιο κοινό πλαίσιο θα ελαχιστοποιούσε και τις πιθανότητες νόθευσης του ανταγωνισμού στην εσωτερική αγορά.

Το κοινό πλαίσιο για το EPCIP θα μπορούσε να είναι είτε προαιρετικό είτε υποχρεωτικό – είτε και τα δύο σε συνδυασμό, ανάλογα με το εκάστοτε ζήτημα. Και οι δύο μορφές πλαισίου θα μπορούσαν να συμπληρώνουν τα ισχύοντα τομεακά και οριζόντια μέτρα σε κοινοτικό και σε εθνικό επίπεδο. Ωστόσο, μόνο ένα νομοθετικό πλαίσιο θα μπορούσε να αποτελέσει μιαν ισχυρή και εφαρμόσιμη νομική βάση για τη συνεπή και ομοιόμορφη εφαρμογή των μέτρων προστασίας των ευρωπαϊκών ΥΖΣ, καθώς και για τον σαφή ορισμό των αντίστοιχων αρμοδιοτήτων των κρατών μελών και της Επιτροπής. Μη δεσμευτικά προαιρετικά μέτρα, αν και ευέλικτα, δεν θα μπορούσαν να καθορίσουν με σαφήνεια τις αρμοδιότητες του καθενός.

Ανάλογα με την έκβαση μιας προσεκτικής ανάλυσης, και με τη δέουσα συνεκτίμηση της αναλογικότητας των προτεινόμενων μέτρων, η Επιτροπή είναι δυνατόν να χρησιμοποιήσει διάφορα μέσα, συμπεριλαμβανόμενων των νομοθετικών, στην πρότασή της για το EPCIP. Όπου κρίνεται αναγκαίο, τις προτάσεις θα συνοδεύει και αξιολόγηση των επιπτώσεών τους.

Ερωτήματα

Ένα κοινό πλαίσιο θα συνέβαλλε αποτελεσματικά στην ενίσχυση της προστασίας των ΥΖΣ;

Εάν απαιτηθεί νομοθετικό πλαίσιο, ποια στοιχεία θα πρέπει να περιλαμβάνει;

Συμφωνείτε ότι τα κριτήρια για τον προσδιορισμό των διαφόρων κατηγοριών ευρωπαϊκών ΥΖΣ και των αναγκαίων μέτρων προστασίας τους θα πρέπει να καθορισθούν κατά τομέα;

Ένα κοινό πλαίσιο θα ήταν χρήσιμο για την αποσαφήνιση των αρμοδιοτήτων των εμπλεκομένων; Σε ποιο βαθμό ένα τέτοιο πλαίσιο θα πρέπει να είναι υποχρεωτικό και σε ποιο βαθμό προαιρετικό;

Τι έκταση θα πρέπει να έχει ένα κοινό πλαίσιο; Συμφωνείτε με τον ενδεικτικό κατάλογο όρων και ορισμών του παραρτήματος 1, βάσει του οποίου θα μπορούν να δίδονται (όπου θα ενδείκνυται) επιμέρους ορισμοί κατά τομέα; Συμφωνείτε με τον κατάλογο των ενδεικτικών τομέων ΥΖΣ του παραρτήματος 2;

6. ΚΟΙΝΟΤΙΚΕΣ ΥΠΟΔΟΜΕΣ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ (ΚΥΖΣ)

6.1. Ορισμός των ΚΥΖΣ

Ο ορισμός ενός κοινοτικού έργου υποδομής με ζωτική σημασία θα μπορούσε να δοθεί με γνώμονα τη διασυνοριακή επίδρασή του, οπότε και διαπιστώνεται αν ένα συμβάν θα μπορούσε να έχει σοβαρές επιπτώσεις πέρα από το έδαφος του κράτους μέλους όπου βρίσκεται το έργο αυτό. Ένα άλλο στοιχείο που πρέπει να ληφθεί υπόψη εδώ είναι το ότι τα προγράμματα διμερούς συνεργασίας μεταξύ κρατών μελών στον τομέα αυτόν αποτελούν ένα καθιερωμένο και αποτελεσματικό μέσο διαχείρισης των ΥΖΣ εκατέρωθεν των συνόρων δύο κρατών μελών. Η συνεργασία αυτή θα μπορούσε να συμπληρώσει το EPCIP.

Οι ΚΥΖΣ θα μπορούσαν να περιλαμβάνουν και εκείνους τους φυσικούς πόρους, υπηρεσίες, εγκαταστάσεις της τεχνολογίας της πληροφορίας, δίκτυα και περιουσιακά στοιχεία τα οποία, εάν υποστούν βλάβη ή καταστραφούν, θα έχουν σοβαρή επίπτωση στην υγεία, την ασφάλεια και την οικονομική και κοινωνική ευπραγία:

α) είτε δύο ή περισσοτέρων κρατών μελών – **τούτο θα συμπεριλάμβανε και ορισμένες διμερείς ΥΖΣ (εφόσον συντρέχει περίπτωση)·**

β) είτε τριών ή περισσότερων κρατών μελών – **τούτο θα εξαιρούσε όλες τις διμερείς ΥΖΣ.**

Όταν εξετάζονται τα πλεονεκτήματα καθεμιάς από τις ως άνω επιλογές, είναι σημαντικό να λαμβάνονται υπόψη τα ακόλουθα σημεία:

– Το γεγονός ότι ένα έργο υποδομής χαρακτηρίζεται ΚΥΖΣ δεν σημαίνει ότι θα απαιτήσει οπωσδήποτε πρόσθετα μέτρα προστασίας. Τα υφιστάμενα μέτρα προστασίας, μεταξύ των οποίων και τυχόν διμερείς συμφωνίες μεταξύ κρατών μελών, είναι δυνατόν να είναι απολύτως επαρκή, οπότε και να μη χρειάζεται να αλλάξουν λόγω του ως άνω χαρακτηρισμού.

– Η επιλογή α) είναι δυνατόν να συνεπάγεται μεγαλύτερο αριθμό χαρακτηρισμών.

– Η επιλογή β) είναι δυνατόν να σημαίνει ότι, για τα έργα υποδομής που ενδιαφέρουν μόνο δύο κράτη μέλη, δεν απαιτείται παρέμβαση της Κοινότητας, ακόμη και αν το επίπεδο προστασίας έχει κριθεί ανεπαρκές από ένα από αυτά τα δύο κράτη μέλη και το άλλο έχει αρνηθεί να αναλάβει δράση. Η επιλογή β) θα μπορούσε να οδηγήσει σε πλειάδα διμερών συμφωνιών ή διαφωνιών μεταξύ κρατών μελών. Οι επιχειρήσεις, οι οποίες συχνά δραστηριοποιούνται σε πανευρωπαϊκό επίπεδο, είναι δυνατόν να πρέπει να ενεργήσουν με μια ποικιλία διαφόρων συμφωνιών, πράγμα που είναι πιθανό να οδηγήσει σε πρόσθετα έξοδα.

Ακόμη, αναγνωρίζεται ότι οι ΥΖΣ που προέρχονται ή βρίσκονται εκτός ΕΕ, αλλά διασυνδέονται ή είναι δυνατόν να έχουν άμεση επίδραση στα κράτη μέλη θα πρέπει επίσης να λαμβάνονται υπόψη.

Ερώτημα

Οι ΚΥΖΣ θα πρέπει έχουν δυνητικά σοβαρές διασυνοριακές επιπτώσεις μεταξύ δύο ή περισσοτέρων, ή τριών ή περισσοτέρων κρατών μελών, και γιατί;

6.2. Αλληλεξαρτήσεις

Προτείνεται, κατά τον σταδιακό προσδιορισμό όλων των ΚΥΖΣ να λαμβάνονται υπόψη οι αλληλεξαρτήσειςη. Οι σχετικές μελέτες θα συνέβαλλαν στην αξιολόγηση της δυνητικής επίδρασης των απειλών εναντίον συγκεκριμένων ΥΖΣ, και ιδίως στον προσδιορισμό των κρατών μελών που θα επηρεάζονταν σε περίπτωση μείζονος συμβάντος σε ΥΖΣ.

Θα πρέπει να δοθεί ιδιαίτερη προσοχή στις αλληλεξαρτήσεις μεταξύ και στο πλαίσιο επιχειρήσεων, επαγγελματικών κλάδων, οργάνων με εδαφική δικαιοδοσία και αρχών των κρατών μελών, και ιδίως εκείνων που οφείλονται στις τεχνολογίες της πληροφορίας και της επικοινωνίας. Η Επιτροπή, τα κράτη μέλη και οι κάτοχοι/διαχειριστές ΥΖΣ θα εργασθούν από κοινού για τον προσδιορισμό των αλληλεξαρτήσεων και θα εφαρμόσουν τις κατάλληλες στρατηγικές για την κατά το δυνατόν μείωση των κινδύνων.

Ερώτημα

Πώς είναι δυνατόν να ληφθούν υπόψη οι αλληλεξαρτήσεις;

Γνωρίζετε κάποια μεθοδολογία κατάλληλη για την ανάλυση των αλληλεξαρτήσεων;

Σε ποιο επίπεδο θα πρέπει να γίνεται ο προσδιορισμός των αλληλεξαρτήσεων; Σε κοινοτικό ή/και σε εθνικό;

6.3. Μέτρα εφαρμογής για τις ΚΥΖΣ

Η Επιτροπή θα ήθελε να προτείνει τα ακόλουθα μέτρα εφαρμογής για τις ΚΥΖΣ:

(1) Η Επιτροπή, από κοινού με τα κράτη μέλη, θα καθορίσει τα συγκεκριμένα κριτήρια προς χρήση για τον προσδιορισμό των ΚΥΖΣ κατά τομέα.

(2) Σταδιακός προσδιορισμός και επαλήθευση από την Επιτροπή και τα κράτη μέλη των ΚΥΖΣ κατά το τομέα. Η απόφαση για τον χαρακτηρισμό μιας ΥΖΣ ως ΚΥΖΣ θα λαμβάνεται σε ευρωπαϊκό επίπεδο[1], λόγω της διασυνοριακής φύσης των υποδομών αυτών.

(3) Τα κράτη μέλη και η Επιτροπή θα αναλύουν τα κενά στην ασφάλεια των ΚΥΖΣ κατά τομέα.

(4) Τα κράτη μέλη και η Επιτροπή θα συμφωνούν ως προς τους τομείς/υποδομές προτεραιότητας για ανάληψη δράσης, λαμβάνοντας υπόψη και τις αλληλεξαρτήσεις.

[1] Με την εξαίρεση των αμυντικών ΥΖΣ.

(5) Όπου θα ενδείκνυται για κάθε τομέα, η Επιτροπή και οι βασικοί ενδιαφερόμενοι θα συμφωνούν ως προς τις προτάσεις μέτρων ελάχιστης προστασίας, περιλαμβανόμενων ενδεχομένως και προτύπων.

(6) Μετά την έγκριση των εκάστοτε προτάσεων από το Συμβούλιο, τα αντίστοιχα μέτρα θα τίθενται σε εφαρμογή.

(7) Η τακτική παρακολούθηση θα γίνεται από τα κράτη μέλη και την Επιτροπή. Επανεξέταση (μέτρων και χαρακτηρισμού ΥΖΣ) θα γίνεται εφόσον και οσάκις τούτο θα κρίνεται ενδεδειγμένο.

Ερωτήματα

Ο κατάλογος των μέτρων εφαρμογής ως προς τις ΚΥΖΣ θεωρείται αποδεκτός;

Πώς προτείνετε να γίνεται ο χαρακτηρισμός των ΚΥΖΣ από την Επιτροπή και τα κράτη μέλη; Τα κράτη μέλη διαθέτουν εμπειρογνωμοσύνη, ενώ η Επιτροπή διαθέτει γενική εποπτεία των κοινοτικών συμφερόντων. Θα πρέπει ο χαρακτηρισμός να γίνεται με επίσημη (δεσμευτική) απόφαση;

Υπάρχει ανάγκη για έναν μηχανισμό διαιτησίας στην περίπτωση όπου ένα κράτος μέλος δεν θα συμφωνεί ως προς τον χαρακτηρισμό μιας ΥΖΣ στην επικράτειά του ως ΚΥΖΣ;

Υπάρχει ανάγκη για επαλήθευση των χαρακτηρισμών; Ποιος θα πρέπει να είναι αρμόδιος;

Τα κράτη μέλη θα πρέπει να είναι σε θέση να χαρακτηρίζουν έργα υποδομής σε άλλο κράτος μέλος ή τρίτη χώρα ως ζωτικής σημασίας για τα ίδια; Τι θα πρέπει να γίνεται εάν ένα κράτος μέλος, μια τρίτη χώρα ή ένας επαγγελματικός κλάδος θεωρεί ένα έργο υποδομής σε κράτος μέλος ως ζωτικής σημασίας για τον εαυτό του;

Τι θα πρέπει να γίνεται εάν αυτό το κράτος μέλος δεν συμφωνεί; Χρειάζεται να προβλεφθεί μηχανισμός προσφυγής, και ποιος;

Ένας φορέας λειτουργίας ενός έργου υποδομής θα πρέπει να έχει τη δυνατότητα να προσφύγει κατά χαρακτηρισμού εάν δεν συμφωνεί με τον χαρακτηρισμό ή τον μη χαρακτηρισμό ενός έργου υποδομής, και σε ποιον;

Ποιες μεθοδολογίες θα χρειαζόταν να αναπτυχθούν για τον καθορισμό των τομέων/υποδομών με προτεραιότητα για την ανάληψη δράσης; Υπάρχουν ήδη κατάλληλες μεθοδολογίες που θα μπορούσαν να προσαρμοσθούν στα κοινοτικά δεδομένα;

Πώς μπορεί η Επιτροπή να λάβει μέρος στην ανάλυση των κενών στην ασφάλεια των ΚΥΖΣ;

7. ΕΘΝΙΚΕΣ ΥΠΟΔΟΜΕΣ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ (ΕΥΖΣ)

7.1. Οι ΕΥΖΣ στο EPCIP

Πολλές ευρωπαϊκές επιχειρήσεις λειτουργούν διασυνοριακά, οπότε υπόκεινται σε διαφορετικές υποχρεώσεις ως προς τις ΕΥΖΣ. Ως εκ τούτου, προτείνεται, προς το συμφέρον των κρατών μελών αλλά και ολόκληρης της ΕΕ, κάθε κράτος μέλος να προστατεύει τις ΕΥΖΣ του μέσα σε ένα κοινό πλαίσιο, έτσι ώστε οι κάτοχοι και διαχειριστές σε ολόκληρη την

Ευρώπη να ωφελούνται από τη μη υπαγωγή τους σε ποικίλα και περίπλοκα πλαίσια, τα οποία οδηγούν σε μια πλειάδα μεθοδολογιών και πρόσθετων εξόδων. Έτσι, η Επιτροπή προτείνει, το EPCIP – αν και με κεντρικό αντικείμενο τις κοινοτικές ΥΖΣ – να μην μπορεί να παραλείπει τελείως τις ΕΥΖΣ. Πάντως, θα μπορούσαν να εξετασθούν οι εξής τρεις επιλογές:

α) Οι ΕΥΖΣ εντάσσονται πλήρως στο EPCIP.

β) Οι ΕΥΖΣ τίθενται εκτός του πεδίου εφαρμογής του EPCIP.

γ) Τα κράτη μέλη είναι δυνατόν να χρησιμοποιούν τμήματα του EPCIP κατά την κρίση του και σε συσχετισμό με τις ΕΥΖΣ τους, αλλά δεν έχουν καμία υποχρέωση προς τούτο.

Ερώτημα

Η αποτελεσματική προστασία των ΥΖΣ στην Ευρωπαϊκή Ένωση φαίνεται να απαιτεί τον προσδιορισμό τόσο των ΚΥΖΣ όσο και των ΕΥΖΣ. Συμφωνείτε ότι, αν και το EPCIP θα πρέπει να εστιάζεται στις ΚΥΖΣ, δεν μπορεί να παραλείπει τελείως τις ΕΥΖΣ;

Ποια από τις ως άνω επιλογές θεωρείτε ως την πλέον ενδεδειγμένη για το EPCIP;

7.2. Εθνικά προγράμματα για την προστασία των ΥΖΣ

Βάσει ενός κοινού πλαισίου για το EPCIP, τα κράτη μέλη θα μπορούσαν να αναπτύξουν εθνικά προγράμματα προστασίας των εθνικών τους ΥΖΣ. Τα κράτη μέλη θα ήταν σε θέση να εφαρμόσουν μέτρα περισσότερο περιοριστικά από εκείνα που προβλέπονται στο EPCIP.

Ερώτημα

Είναι επιθυμητό, κάθε κράτος μέλος να εκδίδει εθνικά προγράμματα προστασίας των ΥΖΣ βάσει του EPCIP;

7.3. Ένα ενιαίο εποπτικό όργανο

Η ανάγκη για αποτελεσματικότητα και συνέπεια οδηγεί στην αναγκαιότητα διορισμού από κάθε επιμέρους κράτος μέλος ενός ενιαίου εποπτικού οργάνου, το οποίο να ασχολείται με την εν γένει εφαρμογή του EPCIP. Ως προς αυτό, θα μπορούσαν να εξετασθούν οι εξής δύο επιλογές:

α) Ένα ενιαίο όργανο εποπτείας της προστασίας των ΥΖΣ.

β) Ένα εθνικό σημείο επαφής χωρίς αρμοδιότητες, με την ευθύνη οργάνωσης των κρατών μελών να επαφίεται στα ίδια.

Ένα τέτοιο όργανο θα μπορούσε να συντονίζει, να παρακολουθεί και να εποπτεύει την εφαρμογή του EPCIP εντός της δικαιοδοσίας του, καθώς και να χρησιμεύει ως το κυριότερο θεσμικό σημείο επαφής με την Επιτροπή, τα άλλα κράτη μέλη και τους κατόχους/διαχειριστές ΥΖΣ σε ζητήματα προστασίας των ΥΖΣ. Επίσης, το όργανο αυτό θα μπορούσε να αποτελέσει τη βάση για την εκπροσώπηση της χώρας του στις ομάδες εμπειρογνωμόνων που ασχολούνται με ζητήματα προστασίας των ΥΖΣ, καθώς και να συνδεθεί με το δίκτυο CIWIN. Τα εθνικά όργανα συντονισμού της προστασίας των ΥΖΣ θα μπορούσαν να συντονίζουν τα

ζητήματα προστασίας των ΥΖΣ παρά το ενδεχόμενο να υπάρχουν στο εκάστοτε κράτος και άλλα όργανα ή οντότητες που ασχολούνται με ζητήματα προστασίας των ΥΖΣ.

Ο σταδιακός προσδιορισμός των ΕΥΖΣ θα μπορούσε να γίνεται μέσω της υποχρέωσης των κατόχων και διαχειριστών ΥΖΣ να ενημερώνουν το οικείο εθνικό συντονιστικό όργανο σχετικά με κάθε δραστηριότητα σχετιζόμενη με την προστασία των ΥΖΣ.

Το εθνικό συντονιστικό όργανο θα μπορούσε να είναι αρμόδιο για την έκδοση της επίσημης απόφασης σχετικά με τον χαρακτηρισμό των έργων υποδομής στην περιοχή της δικαιοδοσίας του ως ΕΥΖΣ. Τα σχετικά στοιχεία θα παραμένουν στη διάθεση μόνο του οικείου κράτους μέλους.

Συγκεκριμένες αρμοδιότητες θα μπορούσαν να είναι:

α) ο συντονισμός, η παρακολούθηση και η εποπτεία της εν γένει εφαρμογής του EPCIP σε ένα κράτος μέλος·

β) ο ρόλος του κυριότερο σημείου επαφής σε ζητήματα προστασίας των ΥΖΣ, με:

i. την Επιτροπή,

ii. τα άλλα κράτη μέλη,

iii. του κατόχους/διαχειριστές ΥΖΣ·

γ) η συμμετοχή στον χαρακτηρισμό των κοινοτικών ΥΖΣ·

δ) η έκδοση της επίσημης απόφασης σχετικά με τον χαρακτηρισμό ενός έργου υποδομής στην περιοχή δικαιοδοσίας του ως ΕΥΖΣ·

ε) ο ρόλος της αρχής δικαστικής προσφυγής των κατόχων/διαχειριστών που δεν συμφωνούν ως προς τον χαρακτηρισμό ενός έργου υποδομής ως ζωτικής σημασίας·

στ) η συμμετοχή στην εκπόνηση του προγράμματος προστασίας των ΕΥΖΣ και των επιμέρους κατά τομέα προγραμμάτων προστασίας·

ζ) ο προσδιορισμός των αλληλεξαρτήσεων μεταξύ συγκεκριμένων τομέων ΥΖΣ·

η) η συμβολή στις κατά τομέα προσεγγίσεις της προστασίας των ΥΖΣ μέσω της συμμετοχής σε ομάδες εμπειρογνωμόνων. Οι εκπρόσωποι των κατόχων/διαχειριστών θα μπορούσαν να προσκαλούνται στις σχετικές συζητήσεις. Οι συναντήσεις θα μπορούσαν να γίνονται σε τακτική βάση·

θ) η εποπτεία της διαδικασίας εκπόνησης σχεδίων έκτακτης ανάγκης για τις ΥΖΣ.

Ερωτήματα

Συμφωνείτε ότι τα κράτη μέλη θα πρέπει να είναι αρμόδια μόνο για τον χαρακτηρισμό και τη διαχείριση των ΕΥΖΣ μέσα σε ένα κοινό πλαίσιο του EPCIP;

Είναι επιθυμητό να ορίζεται από κάθε κράτος μέλος ένα συντονιστικό όργανο για την προστασία των ΥΖΣ, με γενική συντονιστική αρμοδιότητα σε ζητήματα προστασίας, ενώ θα

ασκεί και τις υφιστάμενες αρμοδιότητες κατά τομέα (υπηρεσίες πολιτικής αεροπορίας, οδηγία Seveso κλπ.);

Οι προτεινόμενες για ένα τέτοιο συντονιστικό όργανο αρμοδιότητες είναι οι κατάλληλες; Υπάρχουν και άλλες που θεωρείτε αναγκαίες;

7.4. Μέτρα εφαρμογής για τις ΕΥΖΣ

Η Επιτροπή θα ήθελε να προτείνει τα ακόλουθα μέτρα εφαρμογής:

(1) Μέσω του EPCIP, τα κράτη μέλη θα καθορίσουν τα συγκεκριμένα κριτήρια προς χρήση για τον προσδιορισμό των ΕΥΖΣ.

(2) Σταδιακός προσδιορισμός και επαλήθευση των ΕΥΖΣ κατά τομέα από τα κράτη μέλη.

(3) Τα κράτη μέλη θα αναλύουν τα κενά που υπάρχουν στην ασφάλεια των ΕΥΖΣ κατά τομέα.

(4) Τα κράτη μέλη θα καθορίζουν τους τομείς με προτεραιότητα για δράση, λαμβάνοντας υπόψη τις αλληλεξαρτήσεις και τις προτεραιότητες που θα συμφωνούνται σε κοινοτικό επίπεδο, εφόσον θα συντρέχει περίπτωση.

(5) Εφόσον θα συντρέχει περίπτωση, για κάθε τομέα τα κράτη μέλη θα συμφωνούν τα ελάχιστα μέτρα προστασίας.

(6) Τα κράτη μέλη θα είναι υπεύθυνα για την εφαρμογή εκ μέρους των κατόχων/διαχειριστών της περιοχής δικαιοδοσίας τους των αναγκαίων μέτρων εφαρμογής.

(7) Η τακτική παρακολούθηση θα ασκείται από τα κράτη μέλη. Οι αναθεωρήσεις (των μέτρων και του προσδιορισμού των ΥΖΣ) θα πραγματοποιείται όπου και όταν τούτο θα ενδείκνυται.

Ερώτημα

Ο ως άνω κατάλογος μέτρων εφαρμογής για τις ΕΥΖΣ είναι ο ενδεδειγμένος; Υπάρχουν και περιττά μέτρα; Θα πρέπει να προστεθούν και άλλα;

8. Ο ΡΟΛΟΣ ΤΩΝ ΚΑΤΟΧΩΝ, ΤΩΝ ΔΙΑΧΕΙΡΙΣΤΩΝ ΚΑΙ ΤΩΝ ΧΡΗΣΤΩΝ

8.1. Οι ευθύνες των κατόχων, των διαχειριστών και των χρηστών ΥΖΣ

Ο χαρακτηρισμός ενός έργου υποδομής ως ΥΖΣ συνεπάγεται ορισμένες ευθύνες για τους κατόχους και τους διαχειριστές. Θα μπορούσαν να εξετασθούν τέσσερις ευθύνες σχετικά με τις ΕΥΖΣ και τις ΚΥΖΣ:

(1) **Γνωστοποίηση στο όργανο του οικείου κράτους μέλους που είναι υπεύθυνο για την προστασία των ΥΖΣ, του ότι ένα έργο υποδομής είναι δυνατόν να είναι ζωτικής σημασίας.**

(2) **Διορισμός ενός ανώτερου στελέχους ως συνδέσμου ασφαλείας (Security Liaison Officer - SLO) μεταξύ κατόχων /διαχειριστών και της αρχής του κράτους μέλους που είναι αρμόδια για την προστασία των ΥΖΣ.** Ο SLO θα μπορούσε να λαμβάνει μέρος στην εκπόνηση σχεδίων ασφαλείας και έκτακτης ανάγκης, καθώς και να αποτελεί τον κυριότερο σύνδεσμο με το όργανο το αρμόδιο για την προστασία των ΥΖΣ κάθε τομέα στο εκάστοτε κράτος μέλος, εφόσον δε συντρέχει περίπτωση και με τις αρχές που μεριμνούν για την εφαρμογή του νόμου.

(3) **Εκπόνηση, εφαρμογή και ενημέρωση του σχεδίου ασφάλειας των διαχειριστών (Operator Security Plan - OSP).** Στο παράρτημα 3 εμφαίνεται ένας κατάλογος τέτοιων προτεινόμενων σχεδίων.

(4) **Συμμετοχή στην εκπόνηση σχεδίων έκτακτης ανάγκης** για τις ΥΖΣ, από κοινού με τις αρχές πολιτικής προστασίας και εφαρμογής του νόμου στο εκάστοτε κράτος μέλος.

Τα OSP θα μπορούσαν να υποβάλλονται προς έγκριση στην αρχή του κράτους μέλους που είναι αρμόδια για την προστασία των ΥΖΣ κατά τομέα, υπό τη γενική εποπτεία του οικείου εθνικού συντονιστικού οργάνου (NCCB), τόσο για τις ΕΥΖΣ όσο και για τις ΚΥΖΣ, το οποίο θα εγγυάται τη συνέπεια των μέτρων ασφαλείας που λαμβάνονται από τους εκάστοτε κατόχους και διαχειριστές, και από τον αντίστοιχο τομέα εν γένει. Σε αντάλλαγμα, θα δίδονται στους κατόχους και διαχειριστές στοιχεία ανάδρασης και υποστήριξη σε σχέση με τους κινδύνους και την ανάπτυξη βέλτιστων πρακτικών, καθώς και, εφόσον ενδείκνυται, βοήθεια στην αξιολόγηση των αλληλεξαρτήσεων και των αδύναμων σημείων μέσω του εθνικού συντονιστικού οργάνου και, εφόσον ενδείκνυται, της Επιτροπής.

Κάθε κράτος μέλος θα μπορούσε να καθορίζει χρονικό όριο για την εκπόνηση του OSP από τους κατόχους και διαχειριστές των ΕΥΖΣ και των ΚΥΖΣ (στην περίπτωση των ΚΥΖΣ, η Επιτροπή θα μπορούσε επίσης να συμμετέχει), καθώς και να επιβάλλει διοικητικά πρόστιμα όταν οι τιθέμενες προθεσμίες δεν τηρούνται.

Προτείνεται, το κάθε OSP να προσδιορίζει τα περιουσιακά στοιχεία του εκάστοτε κατόχου/διαχειριστή και να καθορίζει τα μέτρα ασφαλείας για την προστασία τους. Το OSP θα μπορούσε να περιγράφει τις μεθόδους και τη διαδικασία που θα ακολουθούνται για την εξασφάλιση της συμμόρφωσης με το EPCIP, τα εθνικά και τα κατά τομέα επιμέρους προγράμματα προστασίας των ΥΖΣ. Ακόμη, το OSP θα μπορούσε να αποτελεί ένα όχημα για την από τη βάση προς τα άνω ρύθμιση της προστασίας των ΥΖΣ, έτσι ώστε ο ιδιωτικός τομέας να έχει μεγαλύτερα περιθώρια δράσης (αλλά και ευθύνες).

Σε ιδιάζουσες περιπτώσεις όπου εμπλέκονται ορισμένα έργα υποδομής όπως τα δίκτυα διανομής της ηλεκτρικής ενέργειας και της πληροφορίας, θα ήταν εξωπραγματικό (από πρακτική και οικονομική άποψη) να αναμένεται από τους κατόχους και διαχειριστές να παρέχουν το ίδιο επίπεδο ασφάλειας για όλα τα περιουσιακά στοιχεία τους. Στις περιπτώσεις αυτές, προτείνεται, οι κάτοχοι και διαχειριστές να μπορούν, από κοινού με τις αρμόδιες αρχές, να προσδιορίζουν τα ζωτικής σημασίας σημεία (κόμβους) ενός υλικού ή ηλεκτρονικού δικτύου στο οποίο θα μπορούσαν να εστιασθούν τα μέτρα ασφαλείας και προστασίας.

Το OSP θα μπορούσε να περιέχει μέτρα ασφαλείας γύρω από τους εξής δύο άξονες:

- **Μόνιμα μέτρα ασφαλείας**, τα οποία θα μπορούσαν να προσδιορίζουν τις απαραίτητες επενδύσεις και μέσα που δεν μπορούν να υλοποιηθούν από τους κατόχους/διαχιεριστές σε σύντομο χρονικό διάστημα. Οι κάτοχοι/διαχειριστές θα μπορούν να παραμένουν σε διαρκή ετοιμότητα κατά πιθανών απειλών χωρίς τούτο να διαταράσσει τις συνήθεις οικονομικές, διοικητικές και κοινωνικές τους δραστηριότητες.

- **Σταδιακά μέτρα ασφαλείας**, τα οποία θα μπορούσαν να τίθενται σε εφαρμογή ανάλογα με ποικίλα επίπεδα απειλής. Έτσι, το OSP θα μπορούσε να προβλέπει διάφορα καθεστώτα ασφαλείας ανάλογα με την πιθανή απειλή στο κράτος μέλος όπου βρίσκεται το εκάστοτε έργο υποδομής.

Προτείνεται, η αδυναμία του κατόχου/διαχειριστή ενός έργου υποδομής να ανταποκριθεί στην υποχρέωσή του να εκπονήσει ένα OSP, να συμβάλει στην ανάπτυξη σχεδίων έκτακτης ανάγκης και να διορίσει έναν SLO, μπορεί να οδηγήσει στην πιθανότητα επιβολή χρηματικής ποινής.

Ερωτήματα

Οι πιθανές ευθύνες των κατόχων/διαχειριστών ΥΖΣ είναι αποδεκτές από την άποψη της αύξησης της ασφάλειας των ΥΖΣ αυτών; Ποιο είναι το πιθανό κόστος τους;

Οι κάτοχοι/διαχειριστές θα πρέπει να υποχρεώνονται να γνωστοποιούν το ότι οι ΥΖΣ τους είναι δυνατόν να είναι ζωτικής σημασίας; Θεωρείτε ότι η ιδέα του OSP είναι χρήσιμη και γιατί;

Οι προτεινόμενες υποχρεώσεις είναι ανάλογες των σχετικών εξόδων;

Τι δικαιώματα θα πρέπει να δοθούν στους κατόχους/διαχειριστές ΥΖΣ από τις αρχές των κρατών μελών και από την Επιτροπή;

8.2. Ο διάλογος με τους κατόχους, διαχειριστές και χρήστες ΥΖΣ

Το EPCIP θα μπορούσε να οδηγήσει τους κατόχους/διαχειριστές σε εταιρικές σχέσεις. Η επιτυχία ενός προγράμματος προστασίας εξαρτάται από τη συνεργασία και τον βαθμό συμμετοχής των κατόχων και διαχειριστών. Στα κράτη μέλη, οι κάτοχοι/διαχιεριστές ΥΖΣ θα μπορούσαν να συμμετέχουν ενεργά στις εξελίξεις μέσω τακτικών επαφών με το εθνικό συντονιστικό όργανο.

Σε κοινοτικό επίπεδο, θα μπορούσαν να δημιουργηθούν χώροι συναντήσεων με σκοπό τη διευκόλυνση της ανταλλαγής απόψεων επί γενικών και συγκεκριμένων ζητημάτων προστασίας των ΥΖΣ. Μια κοινή προσέγγιση της συμμετοχής του ιδιωτικού τομέα στα ζητήματα προστασίας των ΥΖΣ, έτσι ώστε να βρεθούν μαζί όλοι οι ενδιαφερόμενοι του δημόσιου και του ιδιωτικού τομέα, θα έδινε στα κράτη μέλη, στην Επιτροπή και στους επαγγελματικούς κλάδους μια σημαντική βάση επικοινωνίας σχετικά με οποιοδήποτε νέο ζήτημα προστασίας των ΥΖΣ. Οι κάτοχοι, διαχειριστές και χρήστες ΥΖΣ θα μπορούσαν να συμβάλλουν στην επεξεργασία κοινών κατευθυντήριων γραμμών και βέλτιστων πρακτικών, καθώς και, όπου ενδείκνυται, στην ανταλλαγή πληροφοριών. Ένας τέτοιος διάλογος θα διαμόρφωνε και τις μελλοντικές αναθεωρήσεις του EPCIP.

Όπου ενδείκνυται, η Επιτροπή θα μπορούσε να ενθαρρύνει τη δημιουργία κοινοτικών επαγγελματικών/επιχειρηματικών ενώσεων με αντικείμενο την προστασία των ΥΖΣ. Ακόμη δύο, τελευταίοι, στόχοι θα ήταν η εξασφάλιση της διατήρησης της ανταγωνιστικότητας των επαγγελματικών κλάδων και της ενίσχυσης της ασφάλειας των πολιτών της ΕΕ.

Ερώτημα

Πώς θα πρέπει να δομηθεί ο διάλογος με τους κατόχους, διαχειριστές και χρήστες των ΥΖΣ;

Ποιος θα πρέπει να εκπροσωπεί τους κατόχους, διαχειριστές και χρήστες των ΥΖΣ στον διάλογο δημόσιου και ιδιωτικού τομέα;

9. ΜΕΤΡΑ ΥΠΟΣΤΗΡΙΞΗΣ ΤΟΥ EPCIP

9.1. Το σύστημα προειδοποιητικών πληροφοριών για τις ΥΖΣ (Critical Infrastructure Warning Information Network - CIWIN)

Η Επιτροπή έχει αναπτύξει ορισμένα συστήματα ταχείας προειδοποίησης, τα οποία επιτρέπουν τη συγκεκριμένη, συντονισμένη και αποτελεσματική αντιμετώπιση περιπτώσεων έκτακτης ανάγκης, συμπεριλαμβανόμενων εκείνων με τρομοκρατική προέλευση. Στις 20 Οκτωβρίου 2004, η Επιτροπή ανακοίνωσε τη δημιουργία ενός κεντρικού δικτύου στους κόλπους της, το οποίο εξασφαλίζει την ταχεία ροή πληροφοριών μεταξύ όλων των συστημάτων της ταχείας προειδοποίησης της Επιτροπής και των αρμόδιων υπηρεσιών της (ARGUS).

Η Επιτροπή προτείνει τη δημιουργία του CIWIN, το οποίο θα μπορούσε να συμβάλλει στην επεξεργασία των κατάλληλων μέτρων προστασίας μέσω της διευκόλυνσης της ανταλλαγής των βέλτιστων πρακτικών κατά τρόπο ασφαλή, καθώς και παίζοντας τον ρόλο του οχήματος διαβίβασης στοιχείων για τις άμεσες απειλές και συναγερμούς. Το δίκτυο αυτό θα μπορούσε να εξασφαλίζει τη σωστή πληροφόρηση των σωστών προσώπων τη σωστή στιγμή.

Για την ανάπτυξη του CIWIN υπάρχουν οι εξής δυνατές επιλογές:

(1) **Το CIWIN θα έχει τη μορφή χώρου συναντήσεων, περιοριζόμενου στην ανταλλαγή ιδεών για την προστασία των ΥΖΣ και βέλτιστων πρακτικών** για την υποστήριξη των κατόχων και διαχειριστών ΥΖΣ. Ένας τέτοιος χώρος θα μπορούσε να έχει τη μορφή ενός δικτύου εμπειρογνωμόνων και μιας ηλεκτρονικής βάσης για την ανταλλαγή των εκάστοτε πληροφοριών κατά τρόπο ασφαλή. Η Επιτροπή θα αναλάβει έναν σημαντικό ρόλο στη συγκέντρωση και διάδοση των πληροφοριών αυτών. Η επιλογή αυτή δεν θα παρέχει την αναγκαία ταχεία προειδοποίηση για επικείμενες απειλές. Ωστόσο, θα υπάρχει έδαφος για μελλοντική επέκταση του CIWIN.

(2) **Το CIWIN θα είναι ένα σύστημα ταχείας προειδοποίησης (Rapid Alert System - RAS), το οποίο θα συνδέει τα κράτη μέλη με την Επιτροπή.** Η επιλογή αυτή θα αυξήσει την ασφάλεια των ΥΖΣ μέσω της παροχής προειδοποίησης, περιοριζόμενης στις άμεσες απειλές και συναγερμούς. Ο στόχος εδώ είναι η διευκόλυνση της ταχείας ανταλλαγής πληροφοριών περί πιθανών απειλών στους κατόχους/διαχειριστές ΥΖΣ. Το RAS δεν θα περιλαμβάνει ανταλλαγή πληροφοριών μακροπρόθεσμου χαρακτήρα, αλλά θα μπορεί να χρησιμοποιείται για την ταχεία ανταλλαγή πληροφοριών για επικείμενες απειλές κατά συγκεκριμένων ΥΖΣ.

(3) **Το CIWIN θα είναι ένα πολυεπίπεδο σύστημα επικοινωνίας/προειδοποίησης με δύο χωριστές λειτουργίες:** α) σύστημα ταχείας προειδοποίησης (RAS), το οποίο θα συνδέει τα κράτη μέλη με την Επιτροπή, και β) χώρος ανταλλαγής ιδεών και βέλτιστων πρακτικών για την υποστήριξη των κατόχων και διαχειριστών ΥΖΣ, αποτελούμενος από ένα δίκτυο εμπειρογνωμόνων και μια ηλεκτρονική βάση ανταλλαγής δεδομένων.

Ανεξάρτητα από την επιλογή που θα προκριθεί, το CIWIN θα συμπληρώσει τα υφιστάμενα δίκτυα, με τη δέουσα μέριμνα για την αποφυγή αλληλεπικαλύψεων. Μακροπρόθεσμα, το CIWIN θα μπορούσε να συνδεθεί με όλους τους ενδιαφερόμενους κατόχους/διαχειριστές ΥΖΣ σε κάθε κράτος μέλος μέσω, π.χ., του εθνικού συντονιστικού οργάνου. Η προειδοποίηση και οι βέλτιστες πρακτικές θα μπορούν να διοχετεύονται μέσω του οργάνου αυτού, το οποίο θα είναι η μόνη υπηρεσία με άμεση σύνδεση με την Επιτροπή, οπότε και με τα άλλα κράτη μέλη. Τα κράτη μέλη θα είναι σε θέση να χρησιμοποιούν τα υφιστάμενα συστήματα πληροφοριών που διαθέτουν για να δημιουργήσουν τις δικές τους δυνατότητες CIWIN, συνδέοντας τις αρχές τους με τους συγκεκριμένους κατόχους και διαχειριστές. Είναι σημαντικό το ότι τα εθνικά δίκτυα θα μπορούν να χρησιμοποιούνται από τα εθνικά όργανα που είναι αρμόδια για την προστασία των ΥΖΣ και από τους κατόχους/διαχειριστές τους ως αμφίδρομο σύστημα επικοινωνίας.

Θα διεξαχθεί μιας μελέτη με σκοπό τον προσδιορισμό του εύρους και των τεχνικών προδιαγραφών της μελλοντικής διεπαφής του CIWIN με τα κράτη μέλη.

Ερωτήματα

Ποια μορφή θα πρέπει να έχει το δίκτυο CIWIN για την υποστήριξη των στόχων του EPCIP;

Οι κάτοχοι/διαχειριστές των ΥΖΣ θα πρέπει να συνδεθούν στο CIWIN;

9.2. Κοινές μεθοδολογίες

Τα διάφορα κράτη μέλη έχουν διαφορετικά επίπεδα συναγερμού για τις διάφορες περιπτώσεις. Αυτή τη στιγμή, δεν υπάρχει τρόπος να γνωρίζουμε αν, π.χ., ένα «υψηλό» επίπεδο συναγερμού σε ένα κράτος μέλος είναι το ίδιο σε ένα άλλο. Τούτο είναι δυνατόν να καθιστά δυσχερή για τις διακρατικές επιχειρήσεις τον προσδιορισμό των προτεραιοτήτων για τις δαπάνες τους σε μέτρα προστασίας. Ως εκ τούτου, θα ήταν ωφέλιμο να επιχειρηθεί η εναρμόνιση ή ο επαναπροσδιορισμός των διαφόρων επιπέδων συναγερμού.

Για καθένα από τα επίπεδα απειλής, θα μπορούσε να υπάρχει ένα επίπεδο ετοιμότητας, όπου θα είναι δυνατόν να τίθενται σε εφαρμογή κοινά μέτρα ασφαλείας εν γένει και, εφόσον θα ενδείκνυται σε μια συγκεκριμένη περίπτωση, μέτρα σταδιακής εφαρμογής. Τα κράτη μέλη που δεν θα επιθυμούν να εφαρμόσουν ένα μέτρο θα είναι σε θέση να αντιμετωπίσουν μια συγκεκριμένη απειλή με εναλλακτικά μέτρα ασφαλείας.

Θα μπορούσε να εξετασθεί και μια κοινή μεθοδολογία για τον προσδιορισμό και την ταξινόμηση των απειλών, των δυνατοτήτων, των κινδύνων και των αδύναμων σημείων, καθώς και για τη συναγωγή συμπερασμάτων ως προς την πιθανότητα εκδήλωσης και τον βαθμό σοβαρότητας μιας απειλής για βλάβη ενός έργου υποδομής. Η μεθοδολογία αυτή θα μπορούσε να περιλαμβάνει και αξιολόγηση των κινδύνων καθώς και διαβάθμιση των προτεραιοτήτων, όπου οι κίνδυνοι θα μπορούσαν να ορίζονται με γνώμονα την πιθανότητα

υλοποίησής τους, τις επιπτώσεις τους και τη σχέση τους με άλλους επικίνδυνους τομείς ή διαδικασίες.

Ερωτήματα

Πόσο είναι επιθυμητό και εφικτό να εναρμονισθούν ή να επαναξιολογηθούν τα διάφορα επίπεδα συναγερμού;

Θα πρέπει να υπάρχει μια κοινή μεθοδολογία για τον προσδιορισμό και την ταξινόμηση των απειλών, δυνατοτήτων, κινδύνων και αδύναμων σημείων, καθώς και για συναγωγή συμπερασμάτων σχετικά με την πιθανότητα εκδήλωσης και τον βαθμό σοβαρότητας μιας απειλής;

9.3. Χρηματοδότηση

Μετά τη σχετική πρωτοβουλία του Ευρωπαϊκού Κοινοβουλίου (δημιουργία ενός νέου κωδικού στον προϋπολογισμό του 2005 για το πειραματικό σχέδιο «Καταπολέμηση της τρομοκρατίας»), η Επιτροπή αποφάσισε, στις 15 Σεπτεμβρίου, να διαθέσει 7 εκατ. ευρώ για τη χρηματοδότηση ορισμένων ενεργειών για την ενίσχυση της πρόληψης, της ετοιμότητας και της αντιμετώπισης από την ΕΕ των τρομοκρατικών επιθέσεων, συμπεριλαμβανόμενης της διαχείρισης των επιπτώσεών τους για την προστασία των ΥΖΣ και τον έλεγχο της χρηματοδότησης της τρομοκρατίας, των εκρηκτικών και του βίαιου ριζοσπαστισμού. Τα δύο τρίτα και πλέον του ποσού αυτού προορίζονται για την εκπόνηση του ευρωπαϊκού προγράμματος για την προστασία των ΥΖΣ, για την ολοκλήρωση και ανάπτυξη των δυνατοτήτων που απαιτούνται για τη διαχείριση των κρίσεων διακρατικού χαρακτήρα που προκύπτουν από πιθανές τρομοκρατικές επιθέσεις, καθώς και για τα έκτακτα μέτρα που είναι δυνατόν να απαιτηθούν για την αντιμετώπιση σημαντικής απειλής ή επίθεσης. Αναμένεται ότι η χρηματοδότηση θα συνεχισθεί και το 2006.

Από το 2007 έως το 12013, η χρηματοδότηση θα αναληφθεί από το πρόγραμμα-πλαίσιο «Ασφάλεια και Προστασία των Ελευθεριών». Το πρόγραμμα αυτό θα περιλαμβάνει και ένα επιμέρους πρόγραμμα για την «Πρόληψη, ετοιμότητα και τη διαχείριση των συνεπειών της τρομοκρατίας». Με πρόταση της Επιτροπής διετέθησαν 137,4 εκατ. ευρώ για τον εντοπισμό των σχετικών αναγκών και για την κατάρτιση τεχνικών προτύπων για την προστασία των ΥΖΣ.

Το ως άνω πρόγραμμα θα προβλέπει την κοινοτική χρηματοδότηση των σχεδίων που θα υποβάλλονται από εθνικές, περιφερειακές και τοπικές αρχές με σκοπό την προστασία των ΥΖΣ. Το πρόγραμμα εστιάζεται στον εντοπισμό των αναγκών προστασίας και στην παροχή πληροφοριών για την ανάπτυξη κοινών προτύπων και αξιολογήσεων απειλών και κινδύνων με σκοπό την προστασία των ΥΖΣ, καθώς και για την κατάρτιση συγκεκριμένων σχεδίων έκτακτης ανάγκης. Η Επιτροπή θα κάνει χρήση της υφιστάμενης εμπειρογνωμοσύνης, ενώ θα μπορούσε να συμβάλει στη χρηματοδότηση μελετών για τις αλληλεξαρτήσεις σε συγκεκριμένους τομείς. Μετά, θα αποτελεί κυρίως ευθύνη των κρατών μελών ή των κατόχων/διαχειριστών να αναβαθμίσουν την ασφάλεια των ΥΖΣ τους σύμφωνα με τις εντοπιζόμενες ανάγκες. Το ίδιο το πρόγραμμα δεν χρηματοδοτεί την αναβάθμιση της προστασίας των ΥΖΣ. Για την αναβάθμιση αυτή θα μπορούσαν να χρησιμοποιηθούν δάνεια από χρηματοπιστωτικά ιδρύματα των κρατών μελών, σύμφωνα με τις ανάγκες που θα εντοπίζονται μέσω του προγράμματος, καθώς και για την εφαρμογή κοινών προτύπων. Η Επιτροπή θα είναι διατεθειμένη να υποστηρίξει μελέτες κατά τομέα, με σκοπό την

αξιολόγηση των πιθανών οικονομικών επιπτώσεων της αναβάθμισης της ασφάλειας των ΥΖΣ στους επαγγελματικούς κλάδους.

Η Επιτροπή χρηματοδοτεί ερευνητικά σχέδια για την υποστήριξη της προστασίας των ΥΖΣ στο πλαίσιο της προπαρασκευαστικής ενέργειας για την έρευνα στον τομέα της ασφάλειας[2] (2004-2006), έχει δε σχεδιάσει ακόμη περισσότερο σημαντικές ενέργειες στον τομέα της έρευνας για την ασφάλεια στο πλαίσιο της πρότασής της για απόφαση του Συμβουλίου, του Ευρωπαϊκού Κοινοβουλίου σχετικά με το 7ο πρόγραμμα-πλαίσιο για την ΕΤΑ (COM(2005)119 τελικό)[3], καθώς και της πρότασής της για απόφαση του Συμβουλίου σχετικά με το πρόγραμμα «Συνεργασία» για την εφαρμογή του 7ου προγράμματος-πλαισίου (COM(2005)440 τελικό). Η στοχευμένη έρευνα για την παροχή πρακτικών στρατηγικών ή εργαλείων με σκοπό τον μετριασμό των κινδύνων έχει πρώτιστη σημασία για την ασφάλεια των ΥΖΣ της ΕΕ μεσοπρόθεσμα και μακροπρόθεσμα. Όλη η έρευνα για την ασφάλεια, και στον τομέα αυτόν, θα διέπεται από ηθικά κριτήρια, έτσι ώστε να εξασφαλίζεται η συμβατότητα με τον Χάρτη των Θεμελιωδών Δικαιωμάτων. Η ζήτηση για έρευνα αναμένεται με βεβαιότητα ότι θα αυξηθεί, καθώς οι αλληλεξαρτήσεις των έργων υποδομής αυξάνονται.

Ερώτημα

Πώς εκτιμάτε το κόστος και τις επιπτώσεις της εφαρμογής των μέτρων που προτείνονται στην παρούσα πράσινη βίβλο για τη διοίκηση και τους επαγγελματικούς κλάδους; Νομίζετε ότι είναι αναλογικό;

9.4. Αξιολόγηση και παρακολούθηση

Η αξιολόγηση και η παρακολούθηση της εφαρμογής του EPCIP προϋποθέτει μια πολυεπίπεδη διαδικασία, η οποία απαιτεί τη συμμετοχή όλων των ενδιαφερόμενων:

- **Σε κοινοτικό επίπεδο, θα μπορούσε να δημιουργηθεί ένας μηχανισμός αμοιβαίας αξιολόγησης**, στον οποίο τα κράτη μέλη και η Επιτροπή θα εργάζονται από κοινού για την αξιολόγηση της συνολικής εφαρμογής του EPCIP σε καθένα από τα κράτη μέλη. Θα μπορούσαν να συντάσσονται ετήσιες εκθέσεις της Επιτροπής σχετικά με την πρόοδο της εφαρμογής του EPCIP.

- **Η Επιτροπή θα εκθέτει την πρόοδο της εφαρμογής του EPCIP στα κράτη μέλη και στα λοιπά θεσμικά όργανα κάθε ημερολογιακό έτος,** μέσω εγγράφου εργασίας της.

- **Σε επίπεδο κρατών μελών, το εθνικό συντονιστικό όργανο θα μπορούσε να παρακολουθεί τη συνολική εφαρμογή του EPCIP στο πλαίσιο της δικαιοδοσίας της, μεριμνώντας για τη συμβατότητά του με τα εθνικά προγράμματα προστασίας των ΥΖΣ και τα ανάλογα επιμέρους προγράμματα κατά τομέα,** έτσι ώστε να εξασφαλίζει ότι αυτά θα εφαρμόζονται αποτελεσματικά, θα συντάσσει δε ετήσιες εκθέσεις προς το Συμβούλιο και την Επιτροπή.

---

[2] Οι συνολικές πιστώσεις στους προϋπολογισμούς του 2004 και του 2005 ανήλθαν σε 30 εκατ. ευρώ. Για το 2006, η Επιτροπή έχει προτείνει 24 εκατ. ευρώ, και η πρόταση αυτή εξετάζεται από την αρμόδια για τον προϋπολογισμό αρχή.

[3] Η πρόταση της Επιτροπής για τη χρηματοδότηση από τον προϋπολογισμό των δραστηριοτήτων για την ασφάλεια και το διάστημα δυνάμει του 7ου προγράμματος-πλαισίου για την ΕΤΑ αναφέρεται σε 570 εκατ. ευρώ (COM(2005)119 τελικό).

Η εφαρμογή του EPCIP θα είναι μια δυναμική διαδικασία, διαρκώς εξελισσόμενη και αξιολογούμενη τόσο για να παρακολουθεί τις εξελίξεις σε έναν μεταβαλλόμενο κόσμο όσο και για αξιοποιεί τα συναγόμενα συμπεράσματα. Οι αμοιβαίες αξιολογήσεις και οι εκθέσεις παρακολούθησης των κρατών μελών θα μπορούσαν να αποτελούν μέρος των μέσων που θα χρησιμοποιούνται για την αναθεώρηση του EPCIP και να προτείνουν νέα μέτρα για την ενίσχυση της προστασίας των ΥΖΣ.

Οι πληροφορίες των κρατών μελών σχετικά με τις ΕΥΖΣ θα μπορούσαν να διατίθενται στην Επιτροπή με σκοπό την εκπόνηση κοινών αξιολογήσεων των αδύναμων σημείων, σχεδίων διαχείρισης των συνεπειών και κοινών προτύπων προστασίας των ΥΖΣ, καθώς και την κατάταξη κατά προτεραιότητα των ερευνητικών δραστηριοτήτων και, εφόσον θα ενδείκνυται, την κανονιστική ρύθμιση και εναρμόνιση. Οι πληροφορίες αυτές θα ταξινομούνται και θα τηρούνται απόλυτα εμπιστευτικές.

Η Επιτροπή θα μπορούσε να παρακολουθεί τις διάφορες πρωτοβουλίες των κρατών μελών, συμπεριλαμβανόμενων εκείνων που θα προβλέπουν οικονομικές συνέπειες για τους κατόχους/διαχιεριστές που δεν θα είναι σε θέση να επαναλάβουν την παροχή βασικών υπηρεσιών στους πολίτες εντός συγκεκριμένου μέγιστου χρονικού διαστήματος.

Ερώτημα

Ποιας μορφής μηχανισμός αξιολόγησης θα χρειαζόταν για το EPCIP; Ο μηχανισμός αυτός θα ήταν επαρκής;

Οι απαντήσεις θα πρέπει να αποσταλούν ηλεκτρονικά έως την 15η Ιανουαρίου 2006 στην ακόλουθη διεύθυνση: **JLS-EPCIP@cec.eu.int**. Οι απαντήσεις θα τηρηθούν εμπιστευτικές, εκτός εάν ο απαντών ρητά αναφέρει ότι επιθυμεί τη δημοσιοποίησή τους, οπότε θα ενταχθούν στον δικτυακό τόπο της Επιτροπής.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  – Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  – Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  – Environment (effect on the public and surrounding location);

  – Interdependency (between other critical infrastructure elements).

  – Political effects (confidence in the ability of government);

  – Psychological effects (may escalate otherwise minor events).
  both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- Graduated security measures, which may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.