KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 20.10.2004
KOM(2004) 702 endelig

**MEDDELELSE FRA KOMMISSIONEN
TIL RÅDET OG EUROPA-PARLAMENTET**

Beskyttelse af kritisk infrastruktur i forbindelse med bekæmpelse af terrorisme

INDHOLDSFORTEGNELSE

1. INDLEDNING 3

2. TRUSLEN 3

3. KRITISK INFRASTRUKTUR I EU 3

3.1. Hvad er kritisk infrastruktur? 3

3.2. Sikkerhedsforvaltning 5

4. DE HIDTIDIGE FREMSKRIDT I FORBINDELSE MED BESKYTTELSEN AF KRITISK INFRASTRUKTUR PÅ FÆLLESSKABSPLAN 6

5. FORBEDRING AF EU'S EVNE TIL AT BESKYTTE SIN KRITISKE INFRASTRUKTUR 7

5.1. Et EU-program for beskyttelse af kritisk infrastruktur (EPCIP) 7

5.2. Gennemførelsen af EPCIP-programmet 8

5.3. Mål for EPCIP-programmet og resultatindikatorer 9

TEKNISK BILAG 10

1. INDLEDNING

På Det Europæiske Råds møde i juni 2004 blev Kommissionen og den højtstående repræsentant anmodet om at udarbejde en overordnet strategi for beskyttelse af kritisk infrastruktur.

I denne meddelelse gives et overblik over Kommissionens nuværende tiltag for at beskytte kritisk infrastruktur, og der foreslås en række supplerende foranstaltninger for at styrke de eksisterende instrumenter og efterleve det mandat, der blev givet på Det Europæiske Råds møde.

2. TRUSLEN

Risikoen for terrorangreb med katastrofale konsekvenser, der påvirker kritisk infrastruktur, bliver stadig større. Følgerne af et terrorangreb på industrielle kontrolsystemer i forbindelse med kritisk infrastruktur kan variere meget. Det antages generelt, at et vellykket cyberangreb kun vil kræve få, om nogen, menneskeliv, men det kan medføre, at vitale infrastrukturtjenester går tabt. Et vellykket cyberangreb på det offentlige telefonnet kan medføre, at abonnenternes telefoner ikke virker, mens teknikerne reparerer nettet. Et angreb på kontrolsystemet for et kemisk anlæg eller et anlæg for flydende naturgas kan medføre både omfattende tab af menneskeliv og væsentlige materielle skader.

En anden form for katastrofe i forbindelse med svigtende infrastruktur er, når en del af infrastrukturen medfører, at andre dele ophører med at virke og derved skaber en større kædereaktion. Sådanne svigt skyldes synergivirkningen mellem infrastrukturindustrierne. Et eksempel herpå er et angreb på elnettet, hvor eldistributionen afbrydes; derved kan rensningsanlæg og vandværker også risikere at ophøre med at fungere, såvel som turbiner og andre elektriske apparater på disse anlæg.

En kædereaktion kan medføre alvorlige forstyrrelser og dermed omfattende skader på offentlige værker. Strømsvigtene i Nordamerika og Europa de sidste to år har vist, hvor sårbar energiinfrastrukturen er, og at der er behov for at træffe effektive foranstaltninger for at forebygge/afbøde følgerne af et større strømsvigt. Cyberterrorisme kan desuden forøge virkningerne af et fysisk angreb. Et eksempel herpå er et almindeligt bombeangreb på en bygning kombineret med et midlertidigt strøm- eller telefonsvigt. De deraf følgende problemer med at besvare nødopkald, indtil el- og kommunikationssystemerne kan genetableres og anvendes, kan øge antallet af døde og den offentlige panik.

3. KRITISK INFRASTRUKTUR I EU

3.1. Hvad er kritisk infrastruktur?

Kritisk infrastruktur er de fysiske og informationsteknologiske systemer, net, tjenester og anlæg, hvis afbrydelse eller ødelæggelse i alvorlig grad vil påvirke borgernes sundhed, sikkerhed og økonomiske velfærd eller forhindre, at medlemsstaternes regeringer fungerer effektivt. Der findes kritisk infrastruktur i en lang række økonomiske sektorer, herunder bank- og finanssektoren, transport- og distributionssektoren, energisektoren, offentlige værker, sundhedssektoren, fødevareforsyning og kommunikation samt en række vigtige offentlige

tjenester. Visse kritiske elementer i disse sektorer er strengt taget ikke "infrastrukturer", men snarere netværker eller forsyningskæder, der understøtter leveringen af væsentlige produkter eller tjenester. For eksempel afhænger fødevare- og vandforsyningen til større byområder af nogle vigtige systemer, men også af et kompleks net af producenter, forarbejdere, distributører og detailhandlende.

Kritisk infrastruktur omfatter:

- Energianlæg og -netværker (f.eks. strøm-, olie- og gasproduktion, oplagringsanlæg og raffinaderier samt transmissions- og distributionssystemer).

- Kommunikations- og informationsteknologi (f.eks. telekommunikation, radio- og tv-spredning, software, hardware og netværker, herunder Internettet).

- Finanssektoren (f.eks. banker, værdipapirer og investeringer).

- Sundhedsvæsnet (f.eks. hospitaler, sundhedspleje og blodforsyning, laboratorier og medicinalfirmaer, eftersøgning og redning samt beredskabstjenester).

- Fødevarer (f.eks. sikkerhed, produktionsmidler, engrosdistribution og fødevareindustrien).

- Vand (f.eks. dæmningssøer, vandreservoirer, -behandling og -net).

- Transport (f.eks. lufthavne, havne, intermodale systemer, jernbanenet og massetransportsystemer samt trafikkontrolsystemer).

- Produktion, lagring og transport af farligt gods (f.eks. kemiske, biologiske, radiologiske og nukleare stoffer).

- Det offentlige (f.eks. kritiske tjenester, systemer, informationsnetværker, anlæg samt vigtige steder og monumenter af national interesse).

Disse infrastrukturer ejes eller drives af såvel den offentlige som den private sektor. Kommissionen erklærede imidlertid i sin meddelelse 574/2001 af 10. oktober 2001 følgende: "Udgifterne til den styrkelse af visse foranstaltninger, som de offentlige myndigheder har gennemført som følge af angreb, der er rettet mod hele samfundet og ikke blot mod luftfartsbranchens aktører, bør efter Kommissionens opfattelse bæres af staten." Den offentlige sektor spiller derfor en grundlæggende rolle.

Hvad der udgør kritisk infrastruktur, skal defineres på medlemsstatsplan og på EU-plan, og listerne herover skal udarbejdes inden udgangen af 2005.

EU's kritiske infrastrukturer er i høj grad forbundne og indbyrdes afhængige. Virksomhedskonsolideringer, industrielle rationaliseringer, effektiv forretningspraksis såsom just in time-produktion og befolkningskoncentrationen i byområder har alt sammen bidraget til at skabe denne situation. De kritiske infrastrukturer i EU er blevet mere afhængige af almindelig informationsteknologi, herunder Internettet og radionavigation og kommunikation via satellit. Problemerne kan spredes gennem disse indbyrdes afhængige infrastrukturer og forårsage uventede og stadig mere alvorlige svigt i væsentlige tjenester. Infrastrukturernes indbyrdes forbundethed og afhængighed gør dem mere udsatte for svigt og ødelæggelse.

Det er nødvendigt at undersøge kriterierne for at afgøre, hvad der gør en særlig infrastruktur eller en del af en infrastruktur kritisk. Disse kriterier bør baseres på sektorbestemt og kollektiv ekspertise. Der kan foreslås tre elementer til indkredsning af potentielt kritisk infrastruktur:

- Rækkevidde - Tab af en del af en kritisk infrastruktur måles ved størrelsen af det geografiske område, der vil blive påvirket af et sådant tab eller svigt - internationalt, nationalt, territorialt eller lokalt.

- Alvorlighed - Følgernes eller tabets alvorlighed kan vurderes som nul, minimal, moderat eller stor. Blandt de kriterier, der kan anvendes til at vurdere den potentielle alvorlighed er:

    (a) Følger for offentligheden (andel af befolkningen, der påvirkes, tab af menneskeliv, sygdom, alvorlig legemsbeskadigelse og evakuering)

    (b) Økonomisk (virkningen for BNP, betydningen af økonomisk tab og/eller forringelse af produkter eller tjenester)

    (c) Miljømæssigt (virkninger for offentligheden og omgivelserne)

    (d) Indbyrdes afhængighed (mellem andre dele af kritiske infrastrukturer)

    (e) Politisk (tillid til regeringens handlekraft).

- Tidsmæssig virkning - Dette kriterium bruges til at konstatere, hvornår tabet af et element giver alvorlige følger (f.eks. straks, efter 24-48 timer, en uge eller andet).

I mange tilfælde kan de psykologiske virkninger imidlertid få selv mindre begivenheder til at eskalere.

Teknisk bilag indeholder dokumentation for udviklingen for så vidt angår beskyttelsen af de nuværende kritiske infrastrukturer og giver et sektorbaseret overblik over Kommissionens hidtidige resultater. De viser, at Kommissionen har væsentlige erfaringer på området.

3.2. Sikkerhedsforvaltning

For at kunne foretage en analyse af truslen mod medlemsstaternes kritiske infrastruktur, fejlforekomsten og den kritiske infrastrukturs sårbarhed kræves der oplysninger fra en række kilder. Hver sektor og medlemsstat skal indkredse deres kritiske infrastruktur på deres respektive områder i henhold til en metode, der er harmoniseret på EU-plan, og de organisationer eller personer, der har ansvaret for sikkerheden.

Ikke alle infrastrukturer kan beskyttes mod alle trusler. Eltransmissionsnet er f.eks. for store at indhegne eller bevogte. Ved at anvende risikoforvaltningsteknikker kan der fokuseres på højrisikoområderne, idet der tages hensyn til truslen, den relative sårbarhed, den nuværende sikkerhedsgrad, og hvor effektive de til rådighed stående afhjælpningsstrategier er for at sikre den fortsatte drift.

Sikkerhedsforvaltning er en bevidst proces med henblik på at forstå risikoen og træffe beslutning om og gennemføre foranstaltninger for at mindske risikoen til et bestemt niveau, der udgør et acceptabelt risikoniveau til en acceptabel pris. Karakteristisk for denne metode er, at der sker en indkredsning, måling og kontrol af risiciene på et niveau, der står i et rimeligt forhold til det fastsatte niveau.

Beskyttelse af kritisk infrastruktur kræver et konsekvent samarbejdspartnerskab mellem ejere og operatører af kritisk infrastruktur og medlemsstaternes myndigheder. Det er fortsat ejere og operatører, der har hovedansvaret for at forvalte risikoen i forbindelse med fysiske lokaliteter, forsyningskæder samt informationsteknologi- og kommunikationsnet.

Der må udsendes advarsler, råd og oplysninger for at hjælpe de berørte i den offentlige og den private sektor med at beskytte væsentlige infrastruktursystemer. Der kan fra tid til anden opstå særlige risici eller trusler om et terrorangreb, som kræver en øjeblikkelig reaktion. I så tilfælde må medlemsstaternes regeringers og erhvervslivets reaktion være velkoordineret og operationelt målrettet. EU skal under sådanne omstændigheder koordinere de nødvendige politiske reaktioner, og der skal på det grundlag i hvert enkelt tilfælde aftales detaljerede støtteforanstaltninger med parterne.

Selv de bedste planer for og retsforskrifter vedrørende sikkerhedsforvaltning tjener intet formål, hvis de ikke gennemføres korrekt. Erfaringen har vist, at den eneste effektive måde at sikre en korrekt gennemførelse af sikkerhedskrav på er ved, at Kommissionen foretager uafhængige sikkerhedstilsyn.

4. DE HIDTIDIGE FREMSKRIDT I FORBINDELSE MED BESKYTTELSEN AF KRITISK INFRASTRUKTUR PÅ FÆLLESSKABSPLAN

EU-borgerne forventer, at kritiske infrastrukturer fortsætter med at fungere, uanset hvilken organisation der ejer eller driver de enkelte dele heraf. De forventer, at medlemsstaternes regeringer og EU spiller en ledende rolle med at sikre dette. De forventer, at offentlige og private ejere og operatører på alle niveauer samarbejder om at sikre den fortsatte drift af de tjenester, som EU-borgerne er afhængige af.

Som supplement til de foranstaltninger, der er blevet truffet på nationalt plan, har EU allerede truffet en række retlige foranstaltninger vedrørende fastsættelse af minimumsstandarder for beskyttelse af infrastruktur inden for rammerne af de forskellige EU-politikker. Det er navnlig tilfældet inden for transport, kommunikation, energi, arbejdsmiljø og det offentlige sundhedsvæsen. Der er blevet iværksat endnu flere aktiviteter efter de seneste angreb i USA og EU. Dette vil medføre en yderligere forbedring eller udbredelse af de eksisterende foranstaltninger.

Inden for rammerne af Euratom-traktaten er der i årevis blevet gennemført tilsyn for at kontrollere, at nukleare stoffer anvendes korrekt. På strålingsbeskyttelsesområdet findes en lang række retsforskrifter, der finder anvendelse på risici i forbindelse med driften af anlæg og anvendelsen af kilder, der involverer radioaktive stoffer.

Inden for international transport har EU vedtaget forskrifter med henblik på at gennemføre eller styrke aftaler, der er indgået med internationale ledende instanser i fly- og skibssektoren. EU vil fortsat fremme og aktivt deltage i deres aktiviteter på internationalt plan. EU vil opfordre tredjelande, der har økonomiske forbindelser med EU, til at gennemføre disse aftaler. EU har ydet bistand til nogle af dem med henblik på at nå op på et ensartet og konstant sikkerhedsniveau inden og uden for EU's grænser.

Med oprettelsen af agenturer såsom Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) på kommunikationssikkerhedsområdet tages der endnu et skridt fremad. Inden for fly- og skibssikkerhed er der desuden blevet oprettet tilsynstjenester i

Kommissionen med henblik på at overvåge medlemsstaternes gennemførelse af deres sikkerhedslovgivning. Disse tilsyn gør det muligt at afsætte de nødvendige benchmarks og sikre samme gennemførelsesniveau i EU.

Teknisk bilag indeholder dokumentation for udviklingen for så vidt angår beskyttelsen af de nuværende kritiske infrastrukturer og giver et sektorbaseret overblik over Kommissionens hidtidige resultater. De viser, at Kommissionen har væsentlige erfaringer på området.

5. FORBEDRING AF EU'S EVNE TIL AT BESKYTTE SIN KRITISKE INFRASTRUKTUR

5.1. Et EU-program for beskyttelse af kritisk infrastruktur (EPCIP)

I lyset af det store antal potentielle kritiske infrastrukturer og deres særpræg er det umuligt at beskytte dem alle ved hjælp af foranstaltninger på EU-plan. EU skal ved hjælp af subsidiaritetsprincippet koncentrere sin indsats om at beskytte infrastrukturer, der går på tværs af grænserne, og lade medlemsstaterne selv have ansvaret for de øvrige, men inden for fælles rammer.

Der findes allerede adskillige direktiver og forordninger vedrørende midler til påvisning af risikoen for ulykker, udformning af beredskabsplaner i samarbejde med civilforsvaret, regelmæssige øvelser og klare forbindelser mellem de involverede på forskellige niveauer, offentlige myndigheder, centrale organisationer og beredskabstjenester. Der mangler dog på den anden side meget for at beskytte andre energianlæg end nukleare anlæg. Som det fremgår af teknisk bilag, findes der mere eller mindre veludviklede fællesskabsforskrifter vedrørende beskyttelse af kritisk infrastruktur.

Der arbejdes fortsat på de fleste af ovennævnte områder, og der er indgået et samarbejde med medlemsstaternes eksperter og de berørte økonomiske sektorer for at indkredse mulige mangler og de (retlige og andre) foranstaltninger, der kan træffes for at rette op herpå. Der er blevet etableret mange netværker og sikkerhedsudvalg.

Kommissionen vil hvert år i en meddelelse rapportere til de øvrige institutioner om de fremskridt, der er gjort. Den vil for hver sektor analysere udviklingen i EU's arbejde på områderne risikoevaluering, udvikling af beskyttelsesteknikker og igangværende/planlagte retlige foranstaltninger for at indsamle råd. Kommissionen vil i denne meddelelse desuden om nødvendigt foreslå ajourføringer og generelle organisatoriske foranstaltninger, der kræver harmonisering, koordinering eller samarbejde. Denne meddelelse, der omfatter alle sektoranalyser og -foranstaltninger, skal udgøre grundlaget for et EU-program for beskyttelse af kritisk infrastruktur (EPCIP).

Et sådant program skal hjælpe industrien og medlemsstaternes regeringer på alle planer i EU, samtidig med at de enkeltes mandater og ansvarsområder respekteres. Kommissionen mener, at et netværk bestående af medlemsstaternes eksperter inden for beskyttelse af kritisk infrastruktur kan bistå Kommissionen med at udforme programmet – dette informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN) bør snarest muligt etableres i 2005.

Oprettelsen af netværket skal først og fremmest være med til at fremme udvekslingen af oplysninger om fælles trusler og svage punkter og om hensigtsmæssige foranstaltninger og

strategier til mindskelse af risikoen og beskyttelse af kritisk infrastruktur. Medlemsstaterne skal til gengæld herfor sikre, at de relevante oplysninger videreformidles til alle relevante regeringsinstanser og agenturer, herunder beredskabstjenester, og informere industrisektorer, således at de kan informere de berørte ejere og operatører af kritisk infrastruktur gennem et net af kontakter, der etableres i medlemsstaterne.

EPCIP-programmet skal fremme et forum, hvor konkurrencemæssige krav, ansvar og informationsfølsomhed vejes op imod en mere sikker kritisk infrastruktur. Industrien vil omhyggeligt blive hørt i denne proces. Det vil give partnerne flere oplysninger om særlige trusselssituationer, der sætter dem i stand til at træffe foranstaltninger med henblik på at afhjælpe de potentielle følger heraf. Der bør ikke ændres ved det forhold, at det er ejere og operatører, der har ansvaret for deres egne beslutninger om og planer for beskyttelse af deres egne systemer.

Hvis der ikke findes sektorstandarder, eller der endnu ikke er blevet fastlagt internationale standarder, kan Den Europæiske Standardiseringsorganisation (CEN) og andre relevante standardiseringsorganisationer bistå netværket og foreslå ensartede, sektorbaserede og tilpassede sikkerhedsstandarder for alle de forskellige berørte brancher og sektorer. Det vil også være muligt at fremsætte forslag om sådanne standarder på internationalt plan via ISO for at fastsætte hensigtsmæssige og ensartede spilleregler på området.

Der må udvises forsigtighed, når der henvises til nationale sikkerhedstrusler mod kritisk infrastruktur, herunder terrorisme, for at undgå at skabe unødvendig frygt såvel i EU som blandt potentielle turister og investorer. Terrorisme udgør en konstant trussel, men det er de politiske beslutningstageres opgave at opfordre alle til fortsat at leve deres liv så upåvirket heraf som muligt. Det må desuden tilstræbes, at retten til privatlivets fred respekteres både i og uden for EU. Forbrugerne og erhvervslivet må have tillid til, at oplysninger vil blive behandlet korrekt, fortroligt og pålideligt. Det er nødvendigt at afstikke hensigtsmæssige rammer for at sikre, at klassificerede oplysninger forvaltes ordentligt og beskyttes mod ulovlig brug eller offentliggørelse.

Mange af både EU's og medlemsstaternes kritiske infrastrukturer går på tværs af grænserne i EU. Pipelines strækker sig tværs over kontinenter, kabler, der er af vital betydning for informationsteknologitjenester, er gravet ned i havets bund osv. Det betyder, at det er vigtigt med et internationalt samarbejde med henblik på at etablere dynamiske nationale og internationale partnerskaber mellem ejere/operatører af kritisk infrastruktur og regeringer i tredjelande, navnlig for så vidt angår direkte leverandører af energi til EU.

5.2. Gennemførelsen af EPCIP-programmet

For at beskytte kritisk infrastruktur kræves der aktiv deltagelse af ejere og operatører af infrastruktur, lovgivere, erhvervs- og industriorganisationer samt medlemsstaterne og Kommissionen. På grundlag af oplysninger fra medlemsstaterne, der lægges på netværket, vil EPCIP fortsat tilstræbe at indkredse, hvad der udgør kritiske infrastrukturer, analysere, hvor udsatte de er, og hvor indbyrdes afhængige de er, og fremsætte forslag til, hvordan det er muligt at beskytte dem mod og forberede dem på alle former for farer. Dette omfatter at hjælpe industrisektorer med at forstå truslen og konsekvensvariabler i forbindelse med deres risikovurderinger. Medlemsstaternes retshåndhævende myndigheder og civilforsvar skal sikre, at EPCIP-programmet indgår som en integreret del af deres planlægning og bevidstgørelse.

Kommissionens tjenester vil i tæt samarbejde med netværket udvikle yderligere foranstaltninger i form af vedtagelse af lovgivning og/eller videreformidling af oplysninger. Taskforcen af politichefer og Europol skal spille en rolle i forbindelse med videreformidlingen af oplysninger om de relevante sikkerhedsniveauer og efterretnings-oplysninger til medlemsstaternes retshåndhævende myndigheder, som til gengæld skal rådgive ejere og operatører af kritisk infrastruktur i forbindelse med oplysninger om trusler og bistå dem med at udvikle strategier til beskyttelse mod terrorisme.

Medlemsstaternes regeringer skal fortsat opbygge eller videreudvikle databaser med oplysninger om væsentlige kritiske infrastrukturer på nationalt plan og tage ansvar for udviklingen, valideringen og revisionen af de relevante planer for derved at sikre kontinuiteten i tjenester på deres område. Ved udformningen af EPCIP-programmet vil Kommissionen fremsætte forslag til, hvad sådanne databaser mindst skal indeholde og deres format, samt hvordan de skal kobles sammen.

Medlemsstaternes regeringer skal til gengæld videreformidle relevante efterretnings-oplysninger og advarsler til ejere og operatører af kritisk infrastruktur (samt til andre medlemsstater, hvis det er hensigtsmæssigt) samt informere de berørte om, hvilken type reaktion der forventes for hver trussels-/varslingsniveau.

Ejere og operatører af kritisk infrastruktur skal sikre deres systemer på en hensigtsmæssig måde ved aktivt at gennemføre deres sikkerhedsplaner og regelmæssigt foretage tilsyn, gennemføre øvelser, foretage vurderinger og udforme planer. Medlemsstaterne skal kontrollere den overordnede proces, men Kommissionen skal sikre en ensartet gennemførelse i hele EU ved hjælp af hensigtsmæssige tilsynssystemer.

5.3. Mål for EPCIP-programmet og resultatindikatorer

Formålet med EPCIP-programmet og Kommissionens rolle er at sikre et hensigtsmæssigt og ensartet beskyttelsesniveau for kritisk infrastruktur, at mindske de svage punkter mest muligt og at etablere beredskabsordninger, der er afprøvet i hele EU. EPCIP-programmet vil hele tiden blive videreudviklet, og der vil være behov for regelmæssige revideringer for at være på forkant med problemerne i EU.

Hvor vellykket programmet bliver, måles ved hjælp af følgende:

- Medlemsstaternes regeringers indkredsning af kritisk infrastruktur på deres område og udarbejdelse af oversigter herover i henhold til prioriteringen i EPCIP-programmet.

- Virksomhedernes samarbejde inden for de forskellige sektorer og med regeringen med henblik på at udveksle oplysninger og mindske sandsynligheden for begivenheder, der vil skabe omfattende eller langvarige svigt i kritiske infrastrukturer.

- Det Europæiske Fællesskab fastlægger en fælles metode til at løse problemerne med sikkerheden ved kritisk infrastruktur gennem samarbejde med alle offentlige og private aktører.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

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

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

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.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has 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.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

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.