EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 20.10.2004
KOM(2004) 702 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET

Skydd av viktig infrastruktur i kampen mot terrorismen

INNEHÅLLSFÖRTECKNING

1. INLEDNING ... 3

2. HOTET ... 3

3. EUROPAS VIKTIGA INFRASTRUKTUR ... 3

3.1. Vad är viktig infrastruktur ... 3

3.2. Säkerhetsförvaltning ... 5

4. HITTILLSVARANDE FRAMSTEG I SKYDDET AV VIKTIG INFRASTRUKTUR PÅ GEMENSKAPSNIVÅ ... 6

5. ATT FÖRBÄTTRA EU:s FÖRMÅGA ATT SKYDDA VIKTIG INFRASTRUKTUR ... 7

5.1. Det europeiska programmet för skydd av viktig infrastruktur ... 7

5.2. Genomförandet av det europeiska programmet för skydd av viktig infrastruktur ... 8

5.3. Mål och framgångsindikatorer för det europeiska programmet för skydd av viktig infrastruktur ... 9

TEKNISK BILAGA ... 11

1. INLEDNING

Vid sitt möte i juni 2004 uppmanade Europeiska rådet kommissionen och den höge representanten att förbereda en övergripande strategi till skydd för viktig infrastruktur.

Detta meddelande innehåller en genomgång av de åtgärder som kommissionen för närvarande vidtar till skydd för viktig infrastruktur och förslag på ytterligare åtgärder för att stärka befintliga instrument och att efterleva de mandat som Europeiska rådet givit den.

2. HOTET

Risken för terroristattacker med katastrofal effekt på viktig infrastruktur ökar. Följderna av en attack på systemen för kontroll av viktig infrastruktur kan bli mycket varierande. Det anses allmänt att en framgångsrik attack mot våra datasystem skulle förorsaka få, om ens några, dödsfall, men skulle kunna leda till förluster av centrala infrastrukturtjänster. Exempelvis skulle en framgångsrik attack mot datorerna i de offentliga telefonnätens växlar kunna slå ut vissa telefonitjänster medan tekniker startade om och reparerade växelnätet. En attack mot kontrollsystemen i kemikalie- eller naturgasanläggningar skulle kunna leda till stora förluster av människoliv och avsevärd materiell förstörelse.

En annan typ av infrastrukturhaveri med katastrofala följder kan vara ett haveri som gör att andra delar av systemet kollapsar och därmed ger upphov till omfattande kedjereaktioner. Sådana haverier uppstår på grund av de synergieffekter som olika infrastrukturbranscher har på varandra. Ett enkelt exempel är en attack mot elkraftverk som leder till elavbrott där turbiner och annan elapparatur måste stängas av. I sin tur kan detta leda till driftsstopp i renings- och vattenverk.

Kedjereaktioner kan också förorsaka allvarliga störningar om de ger upphov till stora anläggningsskador. Elavbrotten i Nordamerika och Europa de gångna två åren har visat på energiinfrastrukturens sårbarhet och därmed behovet av att finna effektiva åtgärder för att förebygga eller minimera följderna av ett större avbrott i försörjningen. Denna typ av terrorangrepp mot datasystem skulle också kunna göra att följderna av de fysiska attackerna förvärras. Ett exempel på detta är en attack med konventionella bomber mot en byggnad i kombination med ett tillfälligt el- och telefonavbrott. Den försämrade katastrofberedskap som följer till dess att reservsystemen kan användas kan leda till ett ökat antal dödsoffer och omfattande panik.

3. EUROPAS VIKTIGA INFRASTRUKTUR

3.1. Vad är viktig infrastruktur

Viktig infrastruktur är sådana fysiska eller elektroniska system, nät, tjänster och anläggningar som inte kan drabbas av störningar eller förstöras utan att det allvarligt påverkar folkhälsan, medborgarnas allmänna säkerhet och ekonomiska välstånd eller det praktiska arbetet inom medlemsstaternas myndigheter. Den viktiga infrastrukturen omfattar många ekonomiska sektorer, bl.a. bank- och finansvärlden, transport- och distributionssektorn, energisektorn, allmännyttiga tjänster, hälsovården, livsmedelsdistributionen, telekommunikation och centrala myndighetsfunktioner. Vissa viktiga element inom dessa sektorer är inte ”infrastruktur” i

strikt bemärkelse, utan i själva verket nätverk eller distributionskedjor som används för distribution av en viktig produkt eller tjänst. Exempelvis är distributionen av livsmedel eller vatten till våra storstadsregioner inte blott beroende av vissa nyckelfunktioner utan också av ett komplext nät av producenter, bearbetningsföretag, tillverkare, distributörer och återförsäljare.

Den viktiga infrastrukturen omfattar följande:

- Energiinstallationer och distributionsnät (t.ex. kraftnät, olja- och gasproduktion, lager och raffinaderier, överförings- och distributionssystem).

- Kommunikations- och informationsteknik (t.ex. telekommunikation, radio- och tv-sändningssystem, programvara, hårdvara och elektroniska nät inklusive Internet)

- Finanssystem (t.ex. banktjänster, värdepapper och investeringar)

- Hälsovård (t.ex. sjukhus, hälsovårdsinrättningar och blodcentraler, laboratorier och apotek samt räddningstjänsten)

- Livsmedel (t.ex. livsmedelssäkerhet, produktionsmedel, grossistdistribution och livsmedelsindustrin)

- Vatten (t.ex. dammar, reservoarer, reningsanläggningar och försörjningsnät)

- Transport (t.ex. flygplatser, hamnar, intermodala system, järnvägar och andra masstransportnät samt trafikövervakningssystem)

- Produktion, lagring och transport av farligt gods (t.ex. kemiskt, biologiskt, radiologiskt och radioaktivt material)

- Myndigheter (t.ex. viktiga tjänster, inrättningar, informationsnät, fasta tillgångar samt viktiga platser och monument av nationellt intresse)

Denna infrastruktur ägs och sköts av såväl offentliga som privata aktörer. I sitt meddelande 574/2001 av den 10 oktober 2001 förklarade kommissionen följande: ”Då myndigheterna skärper vissa åtgärder som en följd av angreppen mot hela samhället och inte mot aktörerna inom trafikflyget bör ansvaret enligt kommissionens mening ligga på myndigheterna.” Därför är den offentliga sektorn mycket viktig.

Viktiga infrastrukturer måste definieras på medlemsstatsnivå och på EU-nivå och förteckningar över dem bör ha upprättats i slutet av år 2005.

Europas viktiga infrastrukturer är tätt sammankopplade och i högsta grad beroende av varandra. Företagskoncentrationer, industriell rationalisering, effektiv affärspraxis såsom just-in-time-tillverkning och befolkningskoncentrationen till städerna har bidragit till denna situation. Europas viktiga infrastrukturer har blivit mer beroende av gemensam informationsteknik, inklusive Internet och rymdbaserad radionavigation och -kommunikation. Problem kan spridas genom dessa av varandra beroende infrastrukturer, vilket gör att viktiga tjänster drabbas av oväntade och därmed allvarligare haverier. Det faktum att dessa infrastruktursystem är sammankopplade och beroende av varandra gör dem mer utsatta för störningar och haverier.

Det krävs närmare studier av kriterierna för att avgöra vilka faktorer som gör att en viss infrastruktur eller en del av sådan betraktas som viktig. Definitionen av dessa urvalskriterier skall också bygga på såväl sektorsspecifik som kollektiv sakkunskap. Tre faktorer kan anges för att identifiera potentiellt viktig infrastruktur:

- Omfattning – Förlusten av ett viktigt infrastrukturelement bedöms efter vidden av det geografiska område som kan påverkas om detta element slogs ut eller inte vore tillgängligt – internationellt, nationellt, territoriellt eller lokalt.

- Betydelse – Graden av återverkningarna eller förlusten kan bedömas som obefintlig, minimal, måttlig eller omfattande. Bland de kriterier som kan användas till att bedöma den potentiella betydelsen finns följande:

    (a) Allmänna återverkningar (antal människor som drabbas, antal döda, antal personer som insjuknar, antal svårt skadade, evakueringsbehov).

    (b) Ekonomiska återverkningar (BNP-effekt, de ekonomiska förlusternas omfattning och eventuell nedgång i produktionen av varor och tjänster).

    (c) Återverkningar på miljön (påverkan på allmänna och omgivande områden).

    (d) Ömsesidigt beroende (mellan övriga viktiga infrastrukturella element).

    (e) Politiska återverkningar (förtroendet för myndigheternas förmåga).

- Tidsaspekten – Dessa kriterier visar vid vilken tidpunkt förlusten av ett element skulle kunna få allvarliga följder (dvs. omedelbart, efter 24–48 timmar, en vecka eller annat).

I många fall kan emellertid psykologiska effekter göra att händelser som normalt är av mindre betydelse eskalerar.

Den utveckling som för närvarande äger rum vad gäller skyddet av infrastrukturen finns dokumenterad i teknisk bilaga som innehåller en sektorsindelad översikt över vad kommissionen hittills uppnått. Där framgår att kommissionen har samlat avsevärd erfarenhet på detta område.

3.2. Säkerhetsförvaltning

Det krävs information från ett antal källor för att man skall kunna genomföra en hot-, incident- och sårbarhetsanalys avseende medlemsstaternas viktiga infrastrukturelement och storheter som är beroende av dessa. Med hjälp av ett EU-formulär som skall fyllas i av de organisationer eller personer som ansvarar för säkerheten skall varje sektor och medlemsstat identifiera vilken infrastruktur som är viktig där.

All infrastruktur kan inte skyddas mot alla hot. Exempelvis är kraftledningsnät för stora för att skyddas eller bevakas. Genom tillämpning av riskhanteringsmetoder kan fokus inriktas på högriskområden, varvid hänsyn tas till hotet, dess relativa allvar, nivån på det befintliga skyddet och effektiviteten i de strategier som finns för att dämpa återverkningarna så att verksamheten kan fortgå.

Säkerhetsförvaltning är en metod för att genom noggranna överväganden lära sig förstå risker och besluta om och genomföra åtgärder för att minska risken till en definierad nivå. Detta

arbetssätt utmärks av att man identifierar, bedömer och styr risker till en nivå som sammanfaller med ett angivet mål.

För att kunna skydda viktig infrastruktur krävs konsekvent samarbete mellan ägarna och operatörerna av viktig infrastruktur och medlemsstaternas myndigheter. Ansvaret för att riskhanteringen avseende fysisk infrastruktur, distributionskedjor, informationsteknik och kommunikationsnät ligger främst hos ägarna och operatörerna.

Beredskaps-, rådgivnings- och informationsmaterial måste utarbetas för att hjälpa offentliga och privata aktörer att skydda sina centrala infrastruktursystem. Ibland kan särskilda risker för eller hot om terroristattacker uppstå som kräver omedelbara reaktioner. Vid sådana tillfällen krävs en väl samordnad och operationellt fokuserad insats från myndigheternas och branschens sida. Under sådana omständigheter bör EU samordna nödvändiga politiska reaktioner och på grundval därav kommer sedan detaljerade hjälpinsatser att avtalas med berörda parter från fall till fall.

Även den bästa planering och lagstiftning avseende hur säkerhetsförvaltningen skall verkställas är värdelösa om de aldrig genomförs i praktiken. Erfarenheten visar att oberoende inspektioner från kommissionens sida av säkerhetsföreskrifternas genomförande är det enda effektiva instrumentet för att garantera ett korrekt genomförande av säkerhetskraven.

4. HITTILLSVARANDE FRAMSTEG I SKYDDET AV VIKTIG INFRASTRUKTUR PÅ GEMENSKAPSNIVÅ

Europas medborgare förväntar sig att viktig infrastruktur också fortsättningsvis skall fungera, oberoende av vilken organisation som äger eller driver de enskilda delarna. De förväntar sig att medlemsstaternas myndigheter och EU skall spela en ledande roll för att se till att så sker. De förväntar sig att alla myndighetsnivåer samt ägare och operatörer inom den privata sektorn skall samarbeta för att säkerställa kontinuiteten i de tjänster som Europa är beroende av.

Som ett komplement till de åtgärder som vidtas nationellt, har Europeiska unionen redan vidtagit ett antal lagstiftningsåtgärder för att införa minimistandarder till skydd för infrastruktur inom ramen för EU:s olika politikområden. Detta gäller i synnerhet de sektorer som ansvarar för transport, kommunikationer, energi, arbetsmiljö- och arbetarskydd samt folkhälsa. Verksamheten har intensifierats efter de senaste attackerna i USA och Europa. De kommer att medföra ytterligare förbättringar eller en utökning av befintliga åtgärder.

I årtionden har inspektioner utförts inom ramen för Euratomfördraget för att kontrollera att radioaktivt material används i enlighet med reglerna. På strålskyddsområdet finns omfattande lagstiftning som gäller risker med driften av anläggningar och användning av energikällor som innehåller radioaktiva ämnen.

På området internationella transporter antog Europeiska unionen lagstiftning för att genomföra eller stärka de överenskommelser som slutits mellan internationella tillsynsmyndigheter inom luft- och sjöfarten. Europeiska unionen kommer även fortsättningsvis att främja och aktivt delta i deras internationella verksamhet. Den kommer att uppmuntra tredje länder som har ekonomiska förbindelser med EU att verkställa dessa överenskommelser. Den har givit en del av dem visst stöd för att en homogen och konstant säkerhetsnivå skall kunna uppnås inom och bortom EU:s gränser.

Ännu ett steg kommer att tas i och med inrättandet av nya myndigheter såsom Euronet och Europeiska byrån för nät- och informationssäkerhet, vilka skall ansvara för kommunikationssäkerhet. Vad gäller sjö- och luftfartssäkerhet har dessutom tillsynstjänster inrättats inom kommissionen som skall inspektera genomförandet av medlemsstaternas säkerhetslagstiftning på området. Dessa inspektioner ger nödvändigt jämförelsematerial för att säkerställa samma genomförandenivå inom hela unionen.

Den utveckling som för närvarande sker i skyddet av infrastrukturen finns dokumenterad i teknisk bilaga som innehåller en sektorsindelad översikt över vad kommissionen hittills uppnått. Där framgår att kommissionen har samlat avsevärd erfarenhet på detta område.

5. ATT FÖRBÄTTRA EU:S FÖRMÅGA ATT SKYDDA VIKTIG INFRASTRUKTUR

5.1. Det europeiska programmet för skydd av viktig infrastruktur

Med tanke på den stora mängden potentiellt viktig infrastruktur och alla dess särdrag är det omöjligt att skydda alla delar med hjälp av EU-åtgärder. Genom tillämpning av subsidiaritetsprincipen kan EU koncentrera sina ansträngningar till skyddet av infrastruktur som sträcker sig över gränserna och överlåta övriga strukturer till medlemsstaternas ansvar samtidigt som all infrastruktur omfattas av en gemensam ram.

Det finns redan ett stort antal direktiv och förordningar som föreskriver metoder för upptäckt av olycksrisker, utarbetandet av insatsplaner i samarbete med civilförsvaret, regelbundna övningar och tydliga kopplingar mellan olika insatsnivåer, myndigheter, centrala organisationer och räddningstjänsterna. Å andra sidan återstår mycket att göra för att skydda andra energiinstallationer än kärnkraftsanläggningar. Som framgår av teknisk bilaga finns gemenskapslagstiftning på olika utvecklingsnivå till skydd för viktig infrastruktur.

På de flesta ovannämnda områden pågår arbetet och samarbete har etablerats med medlemsstaternas sakkunniga och berörda ekonomiska sektorer för att identifiera eventuella brister och korrigeringsåtgärder som bör vidtas (rättsliga eller andra). Många nätverk och säkerhetskommittéer har inrättats.

I ett särskilt meddelande kommer kommissionen varje kalenderår att rapportera om utvecklingen till övriga institutioner. Den kommer sektorsvis att analysera utvecklingen inom gemenskapens arbete på området riskutvärdering, utveckling av skyddsteknik och pågående eller planerade rättsliga åtgärder i avsikt att samla in råd. Om nödvändigt kommer kommissionen i sitt meddelande dessutom att föreslå uppdateringar och horisontella organisatoriska åtgärder som kräver harmonisering, samordning och samarbete. Detta meddelande, som omfattar alla sektorsindelade analyser och åtgärder, utgör grunden för det europeiska programmet för skydd av viktig infrastruktur.

Ett sådant program syftar till att stötta berörda branscher och medlemsstaternas myndigheter på alla nivåer inom EU, samtidigt som deras respektive mandat och ansvarsområden respekteras. Kommissionen anser att ett nätverk med nationella experter på skydd av viktig infrastruktur skulle kunna bistå kommissionen i utarbetandet av programmet – detta nätverk för varning om hot mot viktig infrastruktur bör inrättas så tidigt som möjligt 2005.

Nätverket bör framförallt verka för att stimulera utbyte av information om gemensamma hot och svaga punkter samt föreslå tillämpliga åtgärder och strategier för att minska riskerna till stöd för skydd av viktig infrastruktur. I gengäld skall medlemsstaterna säkerställa att tillämplig information förs vidare till berörda departement och myndigheter, inklusive räddningstjänsten och berörda organisationer inom drabbade branscher, så att dessa i sin tur kan informera berörda ägare och operatörer av viktig infrastruktur genom ett nätverk av kontakter som byggts upp inom medlemsstaterna.

Det europeiska programmet för skydd av viktig infrastruktur skulle främja ett ständigt verksamt forum där konkurrenstvång, ansvarsfrågor och informationens konfidentialitetsgrad kan vägas mot fördelarna med en säkrare viktig infrastruktur. Fördjupade överläggningar kommer också att hållas med berörda branscher. Det kommer att bidra till framskaffandet av mer information till parterna om specifika hotsituationer så att dessa kan vidta åtgärder för att hantera de eventuella återverkningarna. Ägarnas och operatörernas ansvar för att fatta egna beslut och utarbeta planer för att skydda sina egna tillgångar kommer inte att ändras.

Om det saknas sektorsnormer eller om internationella normer ännu inte har inrättats, kan Europeiska standardiseringkommittén och andra berörda standardiseringsorganisationer bistå nätverket och föreslå enhetliga sektorsnormer och normer som är anpassade till berörda branscher och sektorer. Sådana normer bör också förslås på internationell nivå genom ISO för att inrätta lika villkor i detta avseende.

För att undvika omotiverad oro i EU och bland potentiella turister och investerare måste hänsyn också tas när nationella säkerhetshot, inklusive terroristhot, riktar sig mot viktig infrastruktur. Terrorismen utgör ett konstant hot men det är beslutfattarnas uppgift att uppmana allmänheten att låta livet gå vidare med så små förändringar som möjligt. Hänsyn måste också visas för att säkerställa respekten för privatlivets helgd, såväl inom som utanför unionen. Konsumenter och operatörer måste kunna lita på att informationen kommer att hanteras på ett korrekt, konfidentiellt och pålitligt sätt. Det är nödvändigt att ha en lämplig ram på plats för att säkerställa att konfidentiell information hanteras på vederbörligt sätt och att den skyddas från otillåten användning eller insyn.

Mycket av EU:s och medlemsstaternas viktiga infrastruktur sträcker sig över gränserna inom EU. Distributionsledningar sträcker sig över kontinenter, kablar för informationstekniktjänster dras på havets botten osv. Detta innebär att det internationella samarbetet är ett viktigt inslag i upprättandet av permanenta, dynamiska nationella och internationella partnerskap mellan ägare och operatörer av viktig infrastruktur och tredje länder, i synnerhet direktleverantörer av energiprodukter till unionen.

5.2. Genomförandet av det europeiska programmet för skydd av viktig infrastruktur

Skyddet av viktig infrastruktur kräver ett aktivt deltagande från infrastrukturens ägare och operatörer, lagstiftare, yrkes- och branschorganisationer samt medlemsstaterna och kommissionen. Utifrån den information som tillhandahålls av medlemsstaternas kontaktorgan och nätverket kommer det europeiska programmet för skydd av viktig infrastruktur att ha som mål att fortsätta att identifiera viktig infrastruktur, analysera sårbarhet och ömsesidigt beroende samt lägga fram lösningar för att utarbeta skydd för och beredskap mot alla eventualiteter. Detta skulle inbegripa stöd till branscherna så att de bättre kan förstå hot- och konsekvensvariabler i riskbedömningarna. Medlemsstaternas rättsvårdande myndigheter och

civilförsvarsorganisationer bör se till att det europeiska programmet för skydd av viktig infrastruktur blir en integrerad del av deras arbete för planering och information till allmänheten.

Kommissionen kommer i nära samarbete med nätverket att utveckla ytterligare åtgärder som exempelvis kan bestå av att lagstiftning antas eller information sprids. Arbetsgruppen för polischefer och Europol kommer att spela en roll vid spridningen av information om gällande säkerhetsnivåer och underrättelseuppgifter till medlemsstaternas rättsvårdande myndigheter som i sin tur får lämna rekommendationer och etablera kontakter med ägare och operatörer av viktig infrastruktur angående relevant information om hot, bistå med säkerhetsrådgivning och utarbeta strategier till skydd mot terrorism.

Medlemsstaternas regeringar kommer även fortsättningsvis att bygga upp eller utveckla och underhålla databaser över viktig infrastruktur av vikt för nationen. De kommer också att ansvara för utvecklingen, utvärderingen och översynen av aktuella planer samt för kontinuiteten i tjänsterna i sina länder. Vid utarbetandet av det europeiska programmet för skydd av viktig infrastruktur kommer kommissionen att lägga fram förslag om vilket minimiinnehåll och -format som sådana databaser bör ha och hur de bör sammankopplas med varandra.

Medlemsstaternas regeringar skall i sin tur fortsätta att informera ägare och operatörer av viktig infrastruktur (och andra medlemsstater om så krävs) om relevanta underrättelseuppgifter och varningar samt om den överenskomna typ av reaktion som förväntas för varje hot- eller beredskapsnivå.

Ägare och operatörer av viktig infrastruktur skall säkra sina anläggningar på lämpligt sätt genom att verkställa sina säkerhetsplaner och genomföra regelbundna inspektioner, övningar och bedömningar samt utarbeta planer. Medlemsstaterna skall kontrollera den övergripande processen medan kommissionen skall säkerställa att den verkställs på samma sätt i hela unionen med hjälp av lämpliga inspektionssystem.

5.3. Mål och framgångsindikatorer för det europeiska programmet för skydd av viktig infrastruktur

Målet med det europeiska programmet för skydd av viktig infrastruktur är att säkerställa lämpliga och lika nivåer avseende skyddsåtgärderna för den viktiga infrastrukturen, ett minimalt antal svaga punkter och snabba, testade återhämtningsåtgärder inom unionen. För kommissionens del är detta en skyldighet. Europeiska programmet för skydd av viktig infrastruktur är en del av en fortlöpande och regelbunden översyn som kommer att krävas för att hålla jämna steg med frågorna och problemen inom gemenskapen.

Framsteg skall mätas med hjälp av följande åtgärder:

- Medlemsstaternas officiella identifiering och inventering av viktig infrastruktur på det egna territoriet enligt de prioriteringar som gjorts inom ramen för det europeiska programmet för skydd av viktig infrastruktur.

- Företag som samarbetar inom enskilda sektorer och med berörda myndigheter för att sprida information och minska risken för incidenter som förorsakar omfattande och ihållande störningar i viktig infrastruktur.

- Europeiska gemenskapen föresätter sig att genom samarbete mellan samtliga berörda offentliga och privata aktörer inrätta ett gemensamt förfaringssätt för att hantera säkerheten i fråga om viktig infrastruktur.

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.