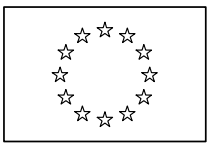

KOMISE EVROPSKÝCH SPOLEČENSTVÍ

V Bruselu dne 20.10.2004
KOM(2004) 702 v konečném znění

SDĚLENÍ KOMISE RADĚ A EVROPSKÉMU PARLAMENTU

Ochrana kritické infrastruktury při boji proti terorismu

OBSAH

1. ÚVOD

Evropská rada na svém zasedání v červnu 2004 požádala Komisi a vysokého představitele o přípravu celkové strategie na ochranu kritické infrastruktury.

Toto sdělení obsahuje přehled opatření, která Komise v současné době provádí v oblasti ochrany kritické infrastruktury, a navrhuje další opatření pro posílení stávajících nástrojů a splnění úloh, které byly Komisi uloženy Evropskou radou.

2. HROZBA

Možnost katastrofických teroristických útoků s dopadem na kritické infrastruktury roste. Následky útoku na průmyslové řídící systémy kritické infrastruktury se mohou značně lišit. Všeobecně se předpokládá, že úspěšný kybernetický útok by si vyžádal málo obětí, pokud vůbec nějaké, ale mohl by vést ke ztrátě životně důležitých infrastrukturních služeb. Například úspěšný kybernetický útok na telefonní ústřednu veřejné telefonní sítě by mohl připravit zákazníky o možnost využívat telefonních služeb po dobu, po kterou budou technici ústřednu obnovovat a opravovat. Útok na řídící systémy chemických zařízení nebo zařízení pro tekutý zemní plyn by mohl vést k větším ztrátám na životech a rovněž ke značným hmotným škodám.

Dalším typem katastrofického selhání infrastruktury by mohl být případ, kdy selhání jedné části infrastruktury vede k selhání jejích dalších částí, což způsobuje rozsáhlý kaskádový efekt. Takové selhání může nastat v důsledku vzájemné provázanosti infrastrukturních odvětví. Jednoduchým příkladem může být útok na elektrárenské podniky, při němž dojde k přerušení dodávek elektrické energie; v takovém případě mohou selhat také čističky odpadních vod a vodárny, protože se může stát, že turbíny a jiné elektrické přístroje v těchto zařízeních přestanou fungovat.

Kaskádové události mohou rovněž vést k rozsáhlým škodám, protože způsobují rozsáhlé výpadky veřejných služeb. Výpadky elektrického proudu v Severní Americe a v Evropě, ke kterým došlo v posledních dvou letech, přinesly důkazy o zranitelnosti energetických infrastruktur a tudíž o potřebě nalézt účinná opatření za účelem prevence a/nebo zmírnění následků vyplývajících z rozsáhlého přerušení dodávek. Tento druh kybernetického terorismu by mohl také vyústit v zesílení dopadů fyzických útoků. Jako příklad je možné uvést konvenční bombový útok na budovu v kombinaci s dočasným přerušením dodávek elektrické energie nebo telefonních služeb. Výsledné ztížení pohotovostní reakce do doby, než jsou zavedeny a uvedeny do provozu záložní systémy dodávek elektrické energie nebo komunikace, může vést ke zvýšení počtu obětí a k veřejné panice.

3. EVROPSKÉ KRITICKÉ INFRASTRUKTURY

3.1. Co je kritická infrastruktura

Kritické infrastruktury se skládají z hmotných zařízení a zařízení informační technologie, sítí, služeb a majetku, jejichž narušení nebo zničení by mělo vážný dopad na zdraví, bezpečnost, zabezpečení nebo hospodářský blahobyt občanů nebo efektivní fungování vlád v členských státech. Kritické infrastruktury se vyskytují v mnoha různých odvětvích hospodářství, včetně

bankovnictví a finančnictví, dopravy a distribuce, energetiky, podniků veřejných služeb, zdravotnictví, dodávek potravin, komunikací a klíčových vládních služeb. Některé důležité prvky v těchto odvětvích nejsou „infrastruktura“ v pravém slova smyslu, nýbrž sítě nebo dodavatelské řetězce, které podporují dodávky důležitých výrobků nebo služeb. Například dodávky potravin nebo vody do našich hlavních městských oblastí závisí na některých klíčových zařízeních, ale také na komplexní síti producentů, zpracovatelů, výrobců, distributorů a maloobchodníků.

Mezi kritické infrastruktury patří:

- Energetická zařízení a sítě (např. elektrická energie, produkce ropy a plynu, skladová zařízení a rafinérie, přenosové a distribuční systémy)

- Komunikační a informační technologie (např. telekomunikace, vysílací systémy, software, hardware a sítě včetně Internetu)

- Finančnictví (např. bankovnictví, cenné papíry a investice)

- Zdravotnictví (např. nemocnice, zdravotnická zařízení a krevní banky, laboratoře a léčiva, pátrací a záchranné služby, pohotovostní služby)

- Potravinářství (např. bezpečnost, výrobní prostředky, velkoobchodní distribuce a potravinářský průmysl)

- Vodní hospodářství (např. přehrady, skladování, úprava a sítě)

- Doprava (např. letiště, přístavy, intermodální zařízení, železniční sítě a sítě veřejné hromadné dopravy, dopravní řídící systémy)

- Výroba, skladování a přeprava nebezpečných výrobků (např. chemických, biologických, radiologických a jaderných materiálů)

- Vláda (např. kritické služby, zařízení, informační sítě, majetek a klíčová státní místa a památky)

Tyto infrastruktury jsou vlastněny nebo provozovány veřejným i soukromým sektorem. Komise však ve svém sdělení 574/2001 ze dne 10. října 2001 uvedla: „Posílení některých bezpečnostních opatření veřejnými orgány v reakci na útoky směřované proti společnosti jako celku a nikoliv na průmyslové subjekty musí být provedeno státem.“ Veřejný sektor proto musí hrát základní úlohu.

Kritické infrastruktury musí být vymezeny na úrovni členských států a na evropské úrovni a příslušné seznamy by měly být sestaveny do konce roku 2005.

Kritické evropské infrastruktury jsou vysoce propojené a vysoce navzájem závislé. K této situaci přispívá konsolidace podniků, racionalizace průmyslu, efektivní obchodní postupy jako např. výroba „v pravý čas“ (just-in-time) a koncentrace obyvatelstva v městských oblastech. Kritické evropské infrastruktury jsou více závislé na společných informačních technologiích, včetně Internetu a kosmické rádiové navigace a komunikace. Prostřednictvím těchto navzájem závislých infrastruktur může docházet k řetězovému hromadění problémů, které mohou způsobovat neočekávané a stále vážnější selhávání nezbytných služeb.

V důsledku své propojenosti a vzájemné závislosti jsou tyto infrastruktury náchylnější k narušení nebo zničení.

Je zapotřebí zkoumat kritéria pro určení faktorů, které způsobují, že určitá infrastruktura nebo prvek infrastruktury jsou kritické. Tato kritéria výběru by měla být rovněž založena na odvětvových a kolektivních odborných poznatcích. Pro určení potenciální kritické infrastruktury lze navrhnout tři faktory:

- Rozsah – ztráta prvku kritické infrastruktury se hodnotí podle velikosti zeměpisné oblasti, která by mohla být jeho ztrátou nebo nedostupností postižena – mezinárodní, vnitrostátní, oblastní/teritoriální nebo místní.

- Závažnost – stupeň dopadu nebo ztráty může být hodnocen jako žádný, minimální, mírný nebo velký. Mezi kritéria, která lze pro hodnocení velikosti použít, patří:

    (a) veřejný dopad (počet dotčených obyvatel, ztráty na životech, onemocnění, vážné zranění, evakuace),

    (b) hospodářský dopad (vliv na HDP, závažnost hospodářské ztráty a/nebo zhoršení kvality výrobků nebo služeb),

    (c) životní prostředí (dopad na veřejnost a okolní oblast),

    (d) vzájemná závislost (mezi jinými prvky kritické infrastruktury),

    (e) politický dopad (důvěra ve schopnost vlády).

- Vliv času – toto kritérium zjišťuje, kdy by mohla mít ztráta prvku vážný dopad (tj. okamžitě, za 24 – 48 hodin, za týden, jindy).

V mnoha případech však mohou být jinak zanedbatelné události vystupňovány psychologickými účinky.

Současný vývoj v oblasti ochrany kritických infrastruktur je popsán v technické příloze, která obsahuje přehled dosud dosažených výsledků Komise podle jednotlivých odvětví. Tyto výsledky ukazují, že Komise získala v této oblasti značné zkušenosti.

3.2. Řízení bezpečnosti

Pro provádění analýz hrozeb, incidentů a zranitelnosti prvků kritické infrastruktury členských států a jejich závislostí jsou zapotřebí informace z mnoha zdrojů. Každé odvětví a členský stát si musí v rámci své příslušné oblasti působnosti a v souladu s harmonizovaným postupem Evropské unie určit infrastrukturu, která je pro ně kritická, a organizace nebo osoby odpovědné za bezpečnost.

Ne všechnu infrastrukturu je možné chránit před všemi hrozbami. Například rozvodné sítě elektrické energie jsou příliš rozsáhlé na to, aby je bylo možné oplotit nebo hlídat. Uplatněním technik řízení rizik lze soustředit pozornost na oblasti největšího rizika, přičemž je nutno vzít v úvahu danou hrozbu, relativní kritičnost, stávající úroveň bezpečnostní ochrany a účinnost dostupných zmírňujících strategií pro zajištění kontinuity provozu.

Řízení rizik je promyšlený proces zjišťování rizika a zvažování a provádění opatření zaměřených na snížení rizika na vymezenou úroveň, která je přijatelnou úrovní rizika za přijatelnou cenu. Tento přístup se vyznačuje určováním, měřením a snižováním rizik na úroveň odpovídající určité předem stanovené úrovni.

Ochrana kritických infrastruktur vyžaduje konzistentní, kooperativní partnerství mezi vlastníky a provozovateli kritických infrastruktur a orgány členských států. Odpovědnost za řízení rizika v rámci hmotných zařízení, dodavatelských řetězců, informačních technologií a komunikačních sítí spočívá zejména na jejich vlastnících a provozovatelích.

Za účelem pomoci zúčastněným subjektům veřejného a soukromého sektoru chránit klíčové systémy infrastruktur je zapotřebí vydávat výstrahy, rady a informace. Čas od času mohou nastat specifická rizika nebo hrozby teroristického útoku, které vyžadují okamžitou reakci. Při těchto příležitostech bude od vlád a průmyslových subjektů členských států vyžadována dobře koordinovaná, operačně zaměřená reakce. Za těchto okolností by Evropská unie měla koordinovat nezbytné politické reakce a na základě tohoto budou se zúčastněnými subjekty případ od případu dohodnuta detailní podpůrná opatření.

I ty nejlepší plány řízení bezpečnosti a právní předpisy, které zajišťují jejich prosazování, jsou bezcenné bez řádného provádění. Zkušenosti ukazují, že jediným účinným nástrojem pro zaručení správného provádění bezpečnostních požadavků jsou nezávislé bezpečnostní kontroly Komise týkající se provádění těchto plánů.

4. DOSAVADNÍ POKROK PŘI OCHRANĚ KRITICKÝCH INFRASTRUKTUR NA ÚROVNI SPOLEČENSTVÍ

Evropané očekávají, že kritické infrastruktury budou dále fungovat bez ohledu na to, jaké organizace vlastní nebo provozují jejich součásti. Očekávají, že při zajištění jejich fungování budou hrát vedoucí úlohu vlády členských států a Evropská unie. Očekávají, že všechny úrovně vlády a soukromí vlastníci a provozovatelé budou spolupracovat za účelem zajištění kontinuity služeb, na kterých Evropané závisí.

Jako doplněk k opatřením, která již byla přijata na vnitrostátní úrovni, přijala Evropská unie řadu legislativních opatření, která stanoví minimální normy pro ochranu infrastruktury v rámci různých politik Evropské unie. Jedná se zejména o oblast dopravy, komunikací, energetiky, zdraví a bezpečnosti při práci a veřejného zdraví. Po nedávných útocích v Americe a v Evropě byla činnost v této oblasti výrazně zintenzívněna a předpokládá se, že povede k dalšímu zlepšení nebo rozšíření stávajících opatření.

Po desetiletí byly prováděny kontroly v rámci Smlouvy o Euratomu za účelem kontroly řádného používání jaderných materiálů. V oblasti radiační ochrany existuje značné množství právních předpisů, které se vztahují na rizika spojená s provozováním zařízení a používáním zdrojů obsahujících radioaktivní látky.

V oblasti mezinárodní dopravy Evropská unie přijala právní předpisy, kterými se provádějí nebo posilují dohody sjednané mezinárodními orgány v oblasti letecké a námořní dopravy. Evropská unie bude jejich činnost na mezinárodní úrovni nadále podporovat a bude se na ní nadále aktivně podílet. Bude vyzývat třetí země, které s ní mají hospodářské vztahy, aby tyto dohody prováděly. Evropská unie poskytla některým z těchto zemí pomoc s cílem dosáhnout jednotné a konstantní úrovně bezpečnosti v rámci hranic Evropské unie i mimo ně.

Dalším krokem je vytvoření agentur, například Evropské agentury pro bezpečnost sítí a informací (European Network and Information Security Agency – ENISA) pro bezpečnost komunikací. Kromě toho v oblastech, jako je bezpečnost letecké a námořní dopravy, byly v rámci Komise vytvořeny kontrolní útvary za účelem kontroly provádění bezpečnostních právních předpisů členskými státy. Tyto kontroly vytvářejí nezbytný srovnávací standard, který zajišťuje stejnou úroveň provádění v Evropské unii.

Současný vývoj v oblasti ochrany kritických infrastruktur je popsán v technické příloze, která obsahuje přehled dosud dosažených výsledků Komise podle jednotlivých odvětví. Tyto výsledky ukazují, že Komise získala v této oblasti značné zkušenosti.

5. ZVYŠOVÁNÍ SCHOPNOSTI EVROPSKÉ UNIE CHRÁNIT KRITICKÉ INFRASTRUKTURY

5.1. Evropský program na ochranu kritických infrastruktur

S ohledem na velký počet potenciálně kritických infrastruktur a jejich zvláštností je nemožné všechny chránit opatřeními na evropské úrovni. Uplatňováním zásady subsidiarity musí Evropa soustředit své úsilí na ochranu infrastruktur, které mají přeshraniční vliv, a ponechat ostatní infrastruktury ve výhradní odpovědnosti členských států, avšak ve společném rámci.

Existuje již mnoho směrnic a nařízení, která stanoví prostředky pro detekci nehod, vytvoření zásahových plánů ve spolupráci s civilní obranou, pravidelná cvičení a jasné vazby mezi jednotlivými zásahovými úrovněmi, veřejnými silami, centrálními organizacemi a pohotovostními službami. Na druhé straně musí být ještě hodně učiněno v oblasti ochrany energetických zařízení jiných než jaderných. Jak je uvedeno v technické příloze, nachází se acquis Společenství o ochraně kritických infrastruktur v různých fázích vývoje.

Ve většině výše uvedených oblastí probíhá příslušná činnost a je vytvořena spolupráce s odborníky členských států a dotčených hospodářských odvětví za účelem určení možných nedostatků a uplatnění nápravných opatření (právních nebo jiných). Bylo vytvořeno mnoho sítí a bezpečnostních výborů.

Komise bude každý rok ve formě sdělení informovat ostatní orgány o pokroku. Provede pro každé odvětví analýzu vývoje činnosti Společenství v oblasti hodnocení rizik, vývoje technik ochrany nebo probíhajících/předpokládaných právních kroků s cílem shromáždit jejich podněty. Pokud to bude nezbytné, Komise v tomto sdělení dále navrhne aktualizace a horizontální organizační opatření, u kterých bude zapotřebí harmonizace, koordinace nebo spolupráce. Toto sdělení, které bude integrovat všechny odvětvové analýzy a opatření, bude představovat základ Evropského programu na ochranu kritických infrastruktur (European Programme for Critical Infrastructure Protection – EPCIP).

Tento program si klade za cíl pomoci průmyslu a vládám členských států na všech úrovních v Evropské unii, přičemž bude respektovat jednotlivé oblasti působnosti a odpovědnosti. Komise zastává názor, že by jí při sestavování tohoto programu mohla pomoci síť sdružující specialisty na ochranu kritických infrastruktur z členských států Evropské unie – tato Varovná informační síť pro kritické infrastruktury (Critical Infrastructure Warning Information Network – CIWIN) by měla být vytvořena co nejdříve v roce 2005.

Vytvoření této sítě by mělo zejména pomoci stimulovat výměnu informací o společných hrozbách a zranitelných místech a vhodná opatření a strategie pro snížení rizik a na podporu ochrany kritických infrastruktur. Členské státy by měly proto zajistit, aby byly příslušné informace předávány všem příslušným vládním útvarům a agenturám, včetně útvarů pohotovostních služeb, a aby byly informovány příslušné orgány průmyslových odvětví, které budou informovat dotčené vlastníky a provozovatele kritické infrastruktury prostřednictvím sítě kontaktů vytvořených v rámci členských států.

Evropský program na ochranu kritických infrastruktur by podpořil zřízení trvalého fóra, v jehož rámci by bylo možné vyvážit na jedné straně omezení daná hospodářskou soutěží, odpovědností a citlivostí informací a na druhé straně výhody bezpečnějších kritických infrastruktur. V rámci tohoto procesu bude úzce konzultován průmysl. Tento přístup pomůže poskytovat více informací o konkrétních hrozbách partnerům, které jim umožní přijmout opatření zaměřená na řešení jejich možných následků. Tím by se však neměla změnit odpovědnost vlastníků a provozovatelů přijímat vlastní rozhodnutí a plány na ochranu svého majetku.

Pokud odvětvové normy neexistují nebo pokud nebyly dosud stanoveny mezinárodní normy, měly by této síti pomáhat Evropský výbor pro normalizaci (CEN) a jiné příslušné normalizační organizace a navrhnout jednotné bezpečnostní odvětvové a upravené normy pro všechny různé zainteresované oblasti a odvětví. Takové normy by také měly být navrženy na mezinárodní úrovni prostřednictvím ISO, aby v tomto ohledu byly vytvořeny rovné podmínky pro všechny.

Při informování o vnitrostátním bezpečnostním ohrožení kritických infrastruktur, včetně terorismu, je třeba postupovat obezřetně, aby se předešlo zbytečným obavám v rámci Evropské unie i obavám potenciálních turistů nebo investorů. Terorismus představuje neustálou hrozbu, ale političtí činitelé by měli povzbuzovat občany k tomu, aby i nadále vedli pokud možno nerušený život. Také je nutné zajistit respektování práv na soukromí, a to v rámci Evropské unie i mimo ni. Spotřebitelé a provozovatelé musí mít jistotu, že s informacemi bude nakládáno přesně, důvěrně a spolehlivě. Je nezbytné disponovat vhodným rámcem, aby bylo zajištěno, že utajované informace jsou řádně spravovány a chráněny před neoprávněným použitím nebo zveřejněním.

Mnoho kritických infrastruktur Evropské unie a členských států překračuje hranice Evropské unie. Potrubí se táhnou napříč kontinenty, kabely nezbytné pro služby informačních technologií jsou uloženy hluboko v mořském dně atd. To znamená, že při vytváření trvalých, dynamických vnitrostátních a mezinárodních partnerství mezi vlastníky/provozovateli kritických infrastruktur a vládami třetích zemí, zejména přímými dodavateli energetických produktů do Evropské unie, hraje důležitou úlohu mezinárodní spolupráce.

5.2. Provádění Evropského programu na ochranu kritických infrastruktur

Ochrana kritických infrastruktur vyžaduje aktivní účast vlastníků a provozovatelů infrastruktur, úřadů, profesních organizací a odvětvových sdružení a členských států a Komise. Na základě informací dodaných členskými státy a uvedenou sítí bude cílem Evropského programu na ochranu kritických infrastruktur identifikovat kritické infrastruktury, analyzovat jejich zranitelnost a vzájemnou závislost a předkládat řešení týkající se ochrany před všemi druhy nebezpečí a přípravy na tato nebezpečí. Součástí tohoto programu by byla rovněž pomoc průmyslovým odvětvím se zjišťováním hrozeb a možných následků v rámci jejich hodnocení rizik. Donucovací orgány členských států a mechanismus civilní ochrany by

měly zajistit, aby Evropský program na ochranu kritických infrastruktur tvořil nedílnou součást jejich plánování a opatření na zvyšování informovanosti.

Útvary Komise budou v úzké spolupráci se sítí vyvíjet další činnost, která by měla spočívat v přijímání právních předpisů a/nebo šíření informací. Na předávání informací o stupních ohrožení a poznatků zpravodajských služeb donucovacím orgánům členských států se bude podílet task force složená z velitelů policie a Europol. Donucovací orgány členských států by měly udržovat kontakty s vlastníky a provozovateli kritických infrastruktur, předávat jim příslušné informace o hrozbách a poskytovat jim rady týkající se ochrany bezpečnosti a vývoje ochranných bezpečnostních strategií proti terorismu.

Vlády členských států budou dále spravovat a/nebo vyvinou a budou udržovat databáze vnitrostátně významných kritických infrastruktur a budou odpovědné za vývoj, validaci a audit příslušných plánů za účelem zajištění kontinuity služeb v rámci jejich působnosti. Při vytváření Evropského programu na ochranu kritických infrastruktur by Komise předložila návrhy minimálního obsahu a formy takových databází a způsobu jejich vzájemného propojení.

Vlády členských států by pokračovaly v informování vlastníků a provozovatelů kritických infrastruktur (a rovněž v případě potřeby ostatních členských států) o poznatcích zpravodajských služeb a výstrahách a o dohodnutých formách reakce na každý stupeň hrozby/výstrahy.

Vlastníci a provozovatelé kritických infrastruktur by zajistili odpovídající zabezpečení svého majetku aktivní implementací svých bezpečnostních plánů a prováděním pravidelných kontrol, cvičení, hodnocení a plánů. Členské státy by měly celý proces řídit, zatímco Komise by měla zajišťovat rovnoměrné provádění v rámci celé Evropské unie prostřednictvím odpovídajících kontrolních systémů.

5.3. Cíle a ukazatele pokroku Evropského programu na ochranu kritických infrastruktur

Cílem Evropského programu na ochranu kritických infrastruktur a úkolem Komise by bylo zajišťovat, aby v rámci celé Evropské unie existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritických infrastruktur, co nejméně jednotlivých bodů selhání a rychlá, vyzkoušená nápravná opatření. Evropský program na ochranu kritických infrastruktur by se neustále vyvíjel a v budoucnu by musel být pravidelně revidován, aby odpovídal problémům a požadavkům v rámci Společenství.

Úspěch by se měřil na základě níže uvedených prvků:

- určení a vytvoření seznamů kritických infrastruktur vládami členských států v rámci jejich působnosti podle stanovených priorit Evropského programu na ochranu kritických infrastruktur;

- spolupráce podniků v rámci odvětví a s vládou za účelem sdílení informací a snížení pravděpodobnosti výskytu incidentů způsobujících rozsáhlé nebo dlouhodobé narušení kritických infrastruktur;

- úsilí Evropského společenství o vytvoření společného přístupu k řešení bezpečnosti kritických infrastruktur prostřednictvím spolupráce všech veřejných a soukromých subjektů.

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.