KOMISIJA EVROPSKIH SKUPNOSTI

Bruselj, 20.10.2004
KOM(2004) 702 končno

# SPOROČILO KOMISIJE SVETU IN EVROPSKEMU PARLAMENTU

## Varovanje kritične infrastrukture v boju proti terorizmu

# KAZALO

## 1. UVOD

Evropski svet junija 2004 je zaprosil Komisijo in visokega predstavnika, da pripravita celovito strategijo varovanja kritične infrastrukture.

To sporočilo vsebuje pregled dejavnosti, ki jih Komisija trenutno izvaja za varovanje kritične infrastrukture, ter predlaga dodatne ukrepe za krepitev obstoječih instrumentov in izpolnitev nalog in pooblastil, ki ji jih je naložil Evropski svet.

## 2. GROŽNJA

Možnost katastrofalnih terorističnih napadov, ki zadevajo kritično infrastrukturo, narašča. Posledice napada na industrijske nadzorne sisteme kritične infrastrukture bi bile lahko zelo raznolike. Na splošno se predpostavlja, da bi uspešen kibernetski napad povzročil malo žrtev, če sploh katero, vendar bi lahko vodil v izgubo ključnih infrastrukturnih storitev. Na primer uspešen kibernetski napad na preklopno omrežje javnih telefonov bi lahko strankam onemogočil dostop do telefonskih storitev, medtem ko bi tehniki ponastavljali in popravljali preklopno omrežje. Napad na nadzorne sisteme kemičnega obrata ali tekočega zemeljskega plina bi lahko povzročil izgubo življenj velikih razsežnosti in tudi veliko materialne škode.

Do druge vrste katastrofalne okvare infrastrukture bi lahko prišlo, če bi en del infrastrukture povzročil okvaro drugih delov, kar bi sprožilo verižno reakcijo. Do takšne okvare bi lahko prišlo zaradi medsebojnih sinergističnih učinkov infrastrukturnih industrij. Enostaven primer bi bil napad na službe za distribucijo električne energije, ki bi oviral distribucijo elektrike, lahko bi odpovedale naprave za čiščenje odplak in vodovodi, saj bi se lahko ugasnile turbine in druge električne naprave v teh obratih.

Verižne reakcije so lahko tudi zelo škodljive in povzročijo obsežne izpade komunalnih storitev. Izpadi elektrike v Severni Ameriki in Evropi v zadnjih dveh letih so dokaz ranljivosti energetskih infrastruktur in posledično potrebe po določitvi učinkovitih ukrepov za preprečevanje/ali omilitev posledic velikih prekinitev dobave. Takšna uporaba kibernetskega terorizma bi lahko tudi ojačila materialne posledice napada. Primer tega bi lahko bil konvencionalen bombni napad s hkratnim izpadom električnih ali telefonskih storitev. Posledično poslabšanje odziva na izredne razmere, dokler se ne bi vzpostavili in uporabili rezervni električni in komunikacijski sistemi, bi lahko povečalo število žrtev in javne panike.

## 3. KRITIČNE INFRASTRUKTURE EVROPE

### 3.1. Kaj je kritična infrastruktura

Kritično infrastrukturo predstavljajo tisti obrati, omrežja, storitve in premoženja fizične in informacijske tehnologije, katerih okvara ali uničenje bi resno vplivalo na zdravje, varnost ali gospodarsko blaginjo državljanov ali na učinkovito delovanje vlad držav članic. Kritične infrastrukture zajemajo številne sektorje gospodarstva, tudi bančništvo in finance, promet in dostavo, energetiko, komunalne storitve, zdravstvo, oskrbo s hrano in komunikacijami, kot tudi ključne državne službe. Nekateri kritični elementi v teh sektorjih strogo rečeno niso „infrastruktura“, temveč so dejansko omrežja ali dobavne verige, ki podpirajo oskrbo s ključnimi proizvodi ali storitvami. Na primer oskrba s hrano ali vodo v naših večjih mestnih

središčih je odvisna od nekaj ključnih obratov, toda tudi od kompleksne mreže proizvajalcev, predelovalcev, izdelovalcev, distributerjev in trgovcev na drobno.

Kritična infrastruktura vključuje:

- Energetske naprave in omrežja (npr. proizvodnja električne energije, nafte in plina, skladišča in rafinerije ter prenosni in distribucijski sistem)
- Komunikacijska in informacijska tehnologija (npr. telekomunikacije, radiodifuzijski sistemi, programska oprema, strojna oprema in omrežja, vključno z internetom)
- Finance (npr. bančništvo, vrednostni papirji in naložbe)
- Zdravstvo (npr. bolnice, zdravstvene ustanove, ustanove za oskrbo s krvjo, laboratoriji in lekarne, službe za iskanje in reševanje, službe za ukrepanje ob izrednih dogodkih)
- Hrana (npr. varnost, proizvodna sredstva, prodaja na debelo in prehrambena industrija)
- Voda (npr. jezovi, skladiščenje, čiščenje in omrežja)
- Prevoz (npr. letališča, pristanišča, intermodalni objekti, železnice, omrežja javnega prevoza, sistemi kontrole prometa)
- Proizvodnja, skladiščenje in prevoz nevarnih snovi (npr. kemične, biološke, radiološke in jedrske snovi)
- Vlada (npr. kritične službe, ustanove, informacijska omrežja, premoženja in ključna nacionalna mesta in spomeniki)

Te infrastrukture imata v lasti in z njimi upravljata tako zasebni kot javni sektor. Kljub temu je Komisija v svojem Sporočilu 574/2001 z dne 10. oktobra 2001 zapisala: „Okrepitev določenih varnostnih ukrepov državnih organov po napadih, usmerjenih proti družbi kot celoti in ne proti industrijskim subjektom, mora biti breme države.“ Javni sektor mora torej odigrati bistveno vlogo.

Kritično infrastrukturo je treba opredeliti na ravni držav članic in na evropski ravni, ti seznami morajo biti sestavljeni do konca leta 2005.

Evropske kritične infrastrukture so izredno povezane in visoko soodvisne. K temu stanju so prispevali gospodarsko združevanje, industrijska racionalizacija, učinkovite poslovne prakse, kot je proizvodnja ravno ob pravem času, ter koncentracija prebivalstva v urbanih območjih. Evropske kritične infrastrukture so postale bolj odvisne od skupnih informacijskih tehnologij, vključno z internetom, vesoljsko radijsko navigacijo in telekomunikacijami. Težave se lahko širijo skozi te soodvisne infrastrukture in pri tem povzročajo nepričakovane in vedno resnejše odpovedi temeljnih javnih služb. Zaradi medsebojne povezanosti in soodvisnosti so te infrastrukture bolj ranljive za motnje ali uničenje.

Potrebno je raziskovati merila za določanje faktorjev, zaradi katerih je določena infrastruktura ali element infrastrukture kritičen. Ta merila za izbor morajo temeljiti tudi na sektorskih in kolektivnih izkušnjah. Za ugotavljanje potencialno kritične infrastrukture se predlaga tri faktorje:

- Domet – Izguba elementa kritične infrastrukture se oceni glede na geografski obseg območja, ki bi bilo prizadeto ob izgubi ali nedostopnosti – mednarodni, državni, pokrajinski/teritorialni ali lokalni.

- Obseg – Stopnja vpliva ali izgube se lahko oceni kot nična, minimalna, zmerna ali velika. Med merili, ki bi se lahko uporabili za oceno potencialnega obsega, so:

    (a) Posledice za prebivalstvo (število prizadetega prebivalstva, izguba življenja, bolezni, resne poškodbe, evakuacija);

    (b) Gospodarstvo (vpliv na BDP, velikost gospodarske izgube in/ali poslabšanja proizvodov ali storitev);

    (c) Okolje (vpliv na javnost in okoliško območje);

    (d) Soodvisnost (med elementi kritične infrastrukture);

    (e) Politične posledice (zaupanje v sposobnost vlade).

- Časovni učinek – To merilo ugotavlja, na kateri točki bi izguba elementa imela resne posledice (t.j. takoj, v 24-48 urah, po enem tednu, drugo).

Toda v mnogih primerih lahko psihološki učinki poslabšajo sicer manj pomembne dogodke.

Obstoječ razvoj varovanja kritične infrastrukture je prikazan v Tehnična Prilogi, ki vsebuje pregled dosedanjih dosežkov Komisije po sektorjih. Glede na te dosežke je Komisija pridobila pomembne izkušnje na tem področju.

### 3.2. Varnostno upravljanje

Za analizo groženj, nezgod in ranljivosti elementov kritične infrastrukture in povezanih elementov v državah članicah so potrebni podatki iz številnih virov. Vsak sektor in vsaka država članica bodo morali določiti infrastrukturo kritičnega pomena, znotraj svoje pristojnosti in v skladu z usklajeno EU formulo in organizacijami ali osebami, zadolženimi za varnost.

Vseh infrastruktur ni mogoče zavarovati pred vsemi grožnjami. Omrežje za prenos električne energije so na primer prevelika, da bi jih ogradili ali varovali. Z uporabo metod obvladovanja tveganja se lahko usmeri pozornost na področja največjega tveganja, ob upoštevanju grožnje, relativne kritičnosti, obstoječe stopnje zaščitnega varovanja in učinkovitost dostopnih strategij za ublažitev za poslovno kontinuiteto.

Varnostno upravljanje je nameren postopek razumevanja tveganj ter odločanja o in izvajanja dejavnosti za zmanjševanje tveganj na določeno stopnjo, ki je sprejemljiva stopnja tveganja ob sprejemljivih stroških. Za ta pristop je značilno ugotavljanje, merjenje in nadzorovanje tveganja do stopnje, ki je sorazmerna s pripisano stopnjo.

Varovanje kritične infrastrukture (CIP) zahteva dosledno partnerstvo na temelju sodelovanja med lastniki in upravljavci kritične infrastrukture ter organi držav članic. Za upravljanje s tveganjem znotraj fizičnih obratov, dobavnih verig, informacijskih tehnologij in komunikacijskih mrež so odgovorni predvsem lastniki in upravljavci.

Potrebno je izdajati opozorila, nasvete in informativna sporočila za pomoč zainteresiranim subjektom v javnem in zasebnem sektorju pri varovanju ključnih infrastrukturnih sistemov. Občasno lahko pride do določenih tveganj ali groženj terorističnega napada, ki zahtevajo takojšnje ukrepanje. V teh primerih bo od držav članic, vlad in industrije potreben dobro usklajen in operativno naravnan odziv. V takšnih okoliščinah bi morala EU usklajevati ustrezne politične odzive in na podlagi tega bodo z zainteresiranimi subjekti dogovorjene podrobne podporne ureditve za vsak primer posebej.

Tudi najboljši načrti varnostnega upravljanja in predpisi, ki silijo v njihovo izvrševanje, so brez vrednosti, če ni pravilnega izvajanja. Izkušnje dokazujejo, da so neodvisni varnostni pregledi izvajanja s strani Komisije edin učinkovit instrument za zagotavljanje pravilnega izvajanja varnostnih zahtev.

## 4. DOSEDANJI NAPREDEK PRI VAROVANJU KRITIČNE INFRASTRUKTURE NA RAVNI SKUPNOSTI

Evropejci pričakujejo, da bodo kritične infrastrukture še naprej delovale ne glede na to, kdo je lastnik ali upravljavec sestavnih delov. Od vlad držav članic in EU pričakujejo vodstveno vlogo pri zagotavljanju tega. Pričakujejo sodelovanje vseh ravni državnih in zasebnih lastnikov in upravljavcev, da se zagotovi kontinuiteta služb, od katerih so Evropejci odvisni.

Kot dopolnilo k ukrepom, ki so bili sprejeti na nacionalni ravni, je Evropska unija že sprejela številne zakonodajne ukrepe, s katerimi je določila minimalne standarde za varovanje infrastrukture v okviru različnih politik EU. To velja zlasti v sektorjih prometa, komunikacij, energetike, zdravja in varnosti pri delu ter javnega zdravstva. Po nedavnih napadih v Ameriki in Evropi so se dejavnosti pospešile. Vodile bodo v nadaljnje izboljšanje in razširitev obstoječih ukrepov.

Že desetletje so se v okviru Pogodbe EURATOM izvajali inšpekcijski pregledi za nadzor pravilne uporabe jedrskih materialov. Na področju zaščite pred sevanjem obstaja obsežna zakonodaja, ki se uporablja za tveganja, povezana z delovanjem obratov in uporabo virov, ki vključujejo radioaktivne snovi.

Na področju mednarodnega prometa je Evropska unija sprejela zakonodajo, ki izvajae in krepi sporazume, ki so jih dosegla mednarodna telesa v letalskem in pomorskem sektorju. Evropska unija bo še naprej spodbujala in aktivno sodelovala pri njihovih dejavnostih na mednarodni ravni. Tretje države, s katerimi ima gospodarske odnose, bo spodbujala k izvajanju teh sporazumov. Nekaterim je nudila pomoč z namenom doseganja homogene in stalne stopnje varnosti znotraj in zunaj meja EU.

Napredek je dosežen tudi z ustanovitvijo agencij za varovanje podatkov kot je Evropska agencija za varovanje omrežij in podatkov (ENISA). Poleg tega so bile v sektorjih, kot je letalska in pomorska varnost, znotraj Komisije ustanovljene inšpekcijske službe za nadzor izvajanja varnostne zakonodaje s strani držav članic. Te inšpekcije določajo potrebno merilo uspešnosti, ki zagotavlja enako stopnjo izvajanja v Uniji.

Obstoječ razvoj varovanja kritične infrastrukture je prikazan v Prilogi 1, ki vsebuje pregled dosedanjih dosežkov Komisije po sektorjih. Glede na te dosežke je Komisija pridobila pomembne izkušnje na tem področju.

## 5. KREPITEV SPOSOBNOSTI EU ZA VAROVANJE KRITIČNE INFRASTRUKTURE

### 5.1. Evropski program za varovanje kritične infrastrukture

Glede na veliko število potencialno kritične infrastrukture in njihovih posebnih značilnosti je nemogoče vse varovati z ukrepi na evropski ravni. Z uporabo načela subsidiarnosti mora Evropa osredotočiti svoja prizadevanja na varovanje infrastruktur s čezmejnim učinkom in prepustiti ostale v pristojnost držav članic, toda v skupnem okviru.

Številne direktive in uredbe že obstajajo, ki določajo načine za zaznavanje nesreč, vzpostavljanje intervencijskih načrtov in sodelovanje s civilno zaščito, redne vaje in jasne povezave med različnimi intervencijskimi ravnmi, javnimi službami, centralnimi organizacijami in službami za ukrepanje ob izrednih dogodkih. Po drugi strani je potrebno še veliko storiti na področju varovanja energetskih naprav, ki niso jedrske. Kot je razvidno iz priloge 1, je pravni red Skupnosti za varovanje kritične infrastrukture na različnih stopnjah razvoja.

Na večini zgoraj omenjenih področij se delo nadaljuje in vzpostavljeno je sodelovanje s strokovnjaki držav članic in zadevnih gospodarskih sektorjev, da se ugotovijo možne pomanjkljivosti in potrebni korektivni ukrepi (pravni in drugi). Vzpostavljene so bile številne mreže in odbori za varnost.

Komisija bo vsako koledarsko leto ostalim ustanovam s sporočilom poročala o napredku. Za vsak sektor bo analizirala napredek dela Skupnosti na področju vrednotenja tveganja, razvoja varnostnih metod ali tekočih/predvidenih pravnih sporov, z namenom zbiranja njihovih nasvetov. Nadalje bo Komisija v tem sporočilu po potrebi predlagala posodobitve in horizontalne organizacijske ukrepe, za katere obstaja potreba po harmonizaciji, uskladitvi ali sodelovanju. To sporočilo, ki bo združevalo vse sektorske analize in ukrepe, bo predstavljalo podlago za Evropski program za varovanje kritične infrastrukture (EPCIP).

Ta program bo poskušal pomagati industriji in vladam držav članic na vseh ravneh EU, ob upoštevanju njihovih individualnih nalog in pooblastil in odgovornosti. Komisija meni, da bi ji pri sestavljanju programa lahko pomagala mreža, ki bi združevala strokovnjake programa pobud Skupnosti iz držav članic EU – ta Informacijska mreža za opozorila o kritični infrastrukturi (CIWIN) mora biti čim prej vzpostavljena v letu 2005.

Vzpostavljanje te mreže bo predvsem pripomoglo s spodbujanjem izmenjave podatkov o skupnih grožnjah in ranljivostih ter ustreznih ukrepih in strategijah za ublažitev tveganja za podporo varovanja kritične infrastrukture. Države članice pa bi poskrbele, da so skozi mrežo kontaktov znotraj države članice ustrezni podatki posredovani vsem ustreznim vladnim službam in agencijam, vključno z organizacijami služb za ukrepanje ob izrednih dogodkih, da so ustrezna industrijska sektorska telesa obveščena in lahko obvestijo prizadete lastnike in upravljavce kritične infrastrukture.

EPCIP bi spodbujal stalen forum, kjer bi se lahko omejitve konkurence, odgovornosti in občutljivosti podatkov uravnotežile s prednostmi bolj varne kritične infrastrukture. V tem postopku se bo redno posvetovalo z industrijo. Partnerjem bo omogočalo razpolaganje z večjo količino podatkov o posameznih grožnjah, kar jim bo omogočalo ukrepati in obravnavati možne posledice. Obveznost in odgovornost lastnikov in upravljavcev za sprejemanje lastnih odločitev in načrtov za varovanje svojega premoženja morata ostati nespremenjeni.

Kjer ne obstajajo sektorski standardi ali še niso bile vzpostavljene mednarodne norme, bi lahko mreži pomagali Evropski odbor za standardizacijo (CEN) in druge ustrezne organizacije in predlagali enotne varnostne standarde in prirejene standarde za vse različne zainteresirane panoge in sektorje. Takšne standarde bi bilo potrebno predlagati tudi na mednarodni ravni z ISO-m, da se vzpostavijo enaki pogoji delovanja.

Ob omembi groženj nacionalni varnosti kritični infrastrukturi, vključno s terorizmom, je potrebna previdnost, da se prepreči neupravičen strah znotraj EU, kot tudi med potencialnimi turisti in vlagatelji. Terorizem predstavlja stalno grožnjo, toda naloga oblikovalcev politike je, da spodbujajo vse, da kar se da nemoteno nadaljujejo s svojimi življenji. Potrebno je zagotoviti tudi spoštovanje pravic do zasebnosti, znotraj in zunaj Unije. Potrošniki in izvajalci morajo imeti zaupanje v to, da bodo podatki obravnavani pravilno, zaupno in zanesljivo. Nujno je potreben ustrezen sistem za zagotavljanje, da se z zaupnimi podatki ravna pravilno in da so varni pred nedovoljeno uporabo ali razkritjem.

Veliko kritične infrastrukture EU in držav članic presega meje EU. Naftovodi potujejo čez cele kontinente; kabli, ključni za storitve informacijske tehnologije, so zakopani globoko na dnu oceanov itd. To pomeni, da je mednarodno sodelovanje nujen sestavni del vzpostavljanja trajnih, dinamičnih nacionalnih in mednarodnih partnerstev med lastniki/upravljavci kritične infrastrukture in vladami tretjih držav, zlasti neposrednimi dobavitelji energentov v Unijo.

### 5.2. Izvajanje EPCIP

Varovanje kritične infrastrukture zahteva aktivno sodelovanje lastnikov in upravljavcev infrastrukture, zakonodajalcev, strokovnih teles, gospodarskih združenj, držav članic in Komisije. Na podlagi podatkov vmesnikov držav članic in mreže, bodo cilji EPCIP nadaljevanje z ugotavljanjem kritične infrastrukture, analiza ranljivost in soodvisnot ter predlaganje rešitev za varovanje pred vsemi nevarnostmi in pripravljenost nanje. To bo vključevalo pomoč industriji pri razumevanju spremenljivk groženj in posledic v svojih ocenah tveganja. Organi kazenskega pregona držav članic in mehanizmi civilne zaščite morajo zagotoviti, da je EPCIP sestavni del njihovega načrtovanja in dvigovanja zavesti.

V tesni usklajenosti z mrežo bodo službe Komisije razvijale nadaljnje aktivnosti, ki vključujejo sprejem zakonodaje in/ali razširjanje informacij. Delovna skupina policijskih načelnikov pri Europolu bi imela vlogo pri razširjanju ustreznih varnostnih in obveščevalnih podatkov organom kazenskega pregona držav članic, ki pa bi svetovali in se povezovali z lastniki in upravljavci kritične infrastrukture glede informacij o grožnjah, pomagali pri zagotavljanju svetovanja o zaščitni varnosti in pri razvoju strategij protiteroristične zaščitne varnosti.

Vlade držav članic bi nadaljevale in/ali razvijale podatkovne baze o nacionalno pomembni kritični infrastrukturi in bile odgovorne za razvoj, potrjevanje in revizijo ustreznih načrtov za zagotavljanje kontinuitete služb v njeni pristojnosti. Ob oblikovanju EPCIP bi Komisija predložila predlog o minimalni vsebini in obliki teh podatkovnih baz in o načinu njihove medsebojne povezanosti.

Vlade držav članic pa bi nadaljevale z obveščanjem lastnikov in upravljavcev kritične infrastrukture (in po potrebi tudi druge države članice) o ustreznih obveščevalnih podatkih in opozorilih, kot tudi o dogovorjeni vrsti odziva, ki je pričakovan za vsako stopnjo grožnje/opozorila zainteresiranim subjektom.

Lastniki in upravljavci kritične infrastrukture bi zagotavljali ustrezno varnost svojega premoženja z aktivnim izvajanjem svojih varnostnih načrtov in izvajanjem rednih inšpekcijskih pregledov, vaj, ocen in načrtov. Države članice bi nadzorovale celoten postopek, medtem ko bi Komisija s primernimi nadzornimi sistemi zagotavljala enako izvajanje v celotni Uniji.

### 5.3. Cilji EPCIP in kazalci napredka

Cilj EPCIP in naloga Komisije bi bilo v celotni Uniji zagotoviti ustrezne in enake stopnje zaščitne varnosti na kritični infrastrukturi, čim manj nezavarovanih točk odpovedi ter hitre in preverjene ukrepe za odpravo posledic. EPCIP bi predstavljal stalen proces in potrebne bodo redne revizije, da bo na tekočem s vprašanji in skrbmi v Skupnosti.

Uspeh se bo meril z:

- ugotavljanjem kritičnih infrastruktur in uvedbo seznamov s strani držav članic znotraj njihovih pristojnosti in v skladu s prednostmi, ki jih bo določil EPCIP;

- sodelovanjem podjetij znotraj sektorjev in z državami z namenom skupne uporabe podatkov in zmanjševanja verjetnosti incidentov, ki bi povzročili široko in dolgo motnjo kritičnih infrastruktur;

- zavezanostjo Evropske skupnosti, da bo vzpostavila skupen pristop k obravnavanju varnosti kritične infrastrukture s sodelovanjem vseh javnih in zasebnih subjektov.

## 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.