COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 20.10.2004
COM(2004) 702 final

COMUNICAÇÃO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU

Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo

ÍNDICE

1. INTRODUÇÃO 3

2. A AMEAÇA TERRORISTA 3

3. INFRA-ESTRUTURAS CRÍTICAS NA EUROPA 3

3.1. Definição de infra-estrutura críticas 3

3.2. Gestão da segurança 5

4. PROGRESSOS REALIZADOS ATÉ AO MOMENTO EM MATÉRIA DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS A NÍVEL COMUNITÁRIO 6

5. REFORÇO DA CAPACIDADE DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS DA UE 7

5.1. Programa Europeu para a Protecção das Infra-estruturas Críticas 7

5.2. Aplicação do PEPIC 9

5.3. Objectivos e indicadores do PEPIC 9

ANEXO TÉCNICO 11

1. INTRODUÇÃO

O Conselho Europeu de Junho de 2004 instou a Comissão e o Alto Representante a prepararem uma estratégia global para proteger as infra-estruturas críticas.

A presente Comunicação apresenta uma perspectiva geral das acções que a Comissão está actualmente a promover em matéria de protecção das infra-estruturas críticas e propõe medidas adicionais para reforçar instrumentos já existentes e cumprir os mandatos conferidos pelo Conselho Europeu.

2. A AMEAÇA TERRORISTA

Os riscos de atentados terroristas catastróficos contra infra-estruturas críticas estão a aumentar. As consequências de um ataque aos sistemas de controlo das infra-estruturas críticas podem variar muito. Considera-se geralmente que um ciber-atentado bem sucedido provocaria poucas ou nenhumas vítimas, embora possa interromper o funcionamento de infra-estruturas essenciais. Por exemplo, um ciber-atentado bem sucedido contra a rede telefónica pública podia privar os clientes de serviço telefónico até que os técnicos restabelecessem e reparassem a rede. Um atentado contra um sistema de controlo de uma instalação química ou de gás liquefeito poderia ocasionar um maior número de vítimas, bem como danos materiais significativos.

Outro tipo de paragem catastrófica de infra-estruturas poderia residir na produção de um efeito em cadeia, em que uma parte da infra-estrutura conduz à paragem de outras partes. Tal paragem podia ocorrer devido às sinergias que existem entre as diferentes infra-estruturas. A título de exemplo poderíamos citar um ataque a instalações eléctricas o que provocaria uma interrupção no fornecimento de electricidade. As estações de tratamento de águas residuais e redes de água também podem parar, devido à falta de alimentação das turbinas e outros aparelhos eléctricos dessas instalações.

Os efeitos em cadeia também podem ser bastante devastadores, causando interrupções de um grande número de serviços de base. Os cortes de electricidade na América do Norte e na Europa durante os últimos dois anos evidenciaram a vulnerabilidade das infra-estruturas energéticas e, consequentemente, a necessidade de encontrar medidas efectivas para prevenir ou atenuar as consequências resultantes de uma importante rotura do abastecimento. Este recurso ao ciber-terrorismo pode também resultar numa amplificação dos efeitos de um ataque físico. Um exemplo disto podia ser um bombardeamento convencional contra um edifício combinado com uma falta temporária de electricidade ou de telefone. As dificuldades de intervenção dos serviços de emergência, até que os sistemas de reserva eléctricos ou de comunicação sejam repostos e utilizados, poderiam aumentar o número de vítimas e o pânico geral.

3. INFRA-ESTRUTURAS CRÍTICAS NA EUROPA

3.1. Definição de infra-estrutura críticas

As infra-estruturas críticas são as instalações físicas e de tecnologia de informação, redes, serviços e bens, os quais, se forem interrompidos ou destruídos, provocarão um sério impacto

na saúde, na protecção, na segurança ou no bem-estar económico dos cidadãos ou ainda no funcionamento efectivo dos governos nos Estados-Membros. As infra-estruturas críticas abarcam vários sectores da economia, incluindo o sector bancário e financeiro, os transportes e a distribuição, a energia, os serviços públicos, a saúde, o abastecimento alimentar e as comunicações, bem como certos serviços administrativos de base. Alguns elementos essenciais destes sectores não são "infra-estruturas" propriamente ditas, mas, de facto, redes ou cadeias de abastecimento que asseguram a entrega de um produto ou a prestação de um serviço essencial. Por exemplo, o abastecimento alimentar ou de água às nossas áreas urbanas mais importantes está dependente de algumas instalações principais, mas também de uma complexa rede de produtores, transformadores, fabricantes, distribuidores e retalhistas.

As infra-estruturas essenciais incluem:

- instalações e redes de energia (por exemplo, energia eléctrica, produção de petróleo e gás, instalações de armazenamento e refinarias, sistema de transmissão e distribuição);

- tecnologia da informação e comunicação (por exemplo, telecomunicações, sistemas de radiodifusão, programas e equipamentos informáticos e redes, incluindo a Internet);

- finanças (por exemplo, actividades bancárias, valores mobiliários e investimento);

- cuidados de saúde (por exemplo, hospitais, centros de assistência médica e bancos de sangue, laboratórios e empresas farmacêuticas, serviços de busca e de primeiros socorros, serviços de urgência);

- alimentação (por exemplo, segurança, alimentar meios de produção, distribuição por grosso e indústria alimentar);

- água (por exemplo, barragens, armazenamento, tratamento e redes);

- transportes (por exemplo, aeroportos, portos, instalações intermodais, redes ferroviárias e redes de transporte de massa, sistemas de controlo de tráfego);

- produção, armazenamento e transporte de mercadorias perigosas (por exemplo, materiais químicos, biológicos, radiológicos e nucleares);

- administração (por exemplo, serviços de base, instalações, redes de informação, bens, sítios e monumentos de importância nacional).

Estas infra-estruturas pertencem ou são exploradas tanto pelo sector público como pelo sector privado. Contudo, na sua Comunicação 574/2001, de 10 de Outubro de 2001, a Comissão declarou: "O reforço de algumas medidas de segurança pelos poderes públicos, na sequência de ataques dirigidos contra a sociedade inteira e não contra os intervenientes do sector do transporte aéreo, deve ser assumido pela autoridade pública". O sector público tem portanto um papel fundamental a desempenhar.

As infra-estruturas críticas devem ser definidas ao nível dos Estados-Membros e a nível europeu e as listas correspondentes deverão ser elaboradas até ao final de 2005.

As infra-estruturas críticas da Europa estão muito interligadas e são interdependentes. A concentração das empresas, a racionalização industrial, práticas empresariais eficientes, tais

como processos de fabrico *just-in-time*, e a concentração de população em áreas urbanas, constituem factores que contribuíram para esta situação. As infra-estruturas críticas da Europa tornaram-se mais dependentes das tecnologias da informação, incluindo a Internet, a radionavegação e a comunicação por satélite. Os problemas podem surgir em cadeia através destas infra-estruturas interdependentes, causando falhas inesperadas e cada vez mais graves dos serviços essenciais. A interligação e a interdependência fazem com que estas infra-estruturas se tornem mais vulneráveis à interrupção dos serviços ou à destruição das instalações.

É conveniente estudar os critérios que permitem considerar como "crítica" uma infra-estrutura ou um determinado elemento de uma infra-estrutura. Estes critérios de selecção devem também basear-se em conhecimentos sectoriais ou colectivos. Três factores podem ser apontados para identificar potenciais infra-estruturas críticas:

- Alcance – a perda de um elemento de infra-estrutura é avaliada em função da extensão da área geográfica que pode ser afectada pela sua perda ou indisponibilidade – internacional, nacional, provincial/territorial ou local;

- Magnitude – o grau do impacto ou da perda pode ser avaliado como Nulo, Mínimo, Moderado ou Elevado. Entre os critérios que podem ser utilizados para avaliar a magnitude potencial encontram-se:

    (a) O impacto no público (número de pessoas afectadas, perda de vidas, doença, prejuízos graves, evacuação);

    (b) Os efeitos económicos (efeitos no PIB, importância das perdas económicas e/ou degradação de produtos ou serviços);

    (c) A incidência ambiental (impacto no público e em áreas vizinhas);

    (d) A interdependência (em relação a outros elementos de infra-estrutura crítica);

    (e) Efeitos políticos (confiança na capacidade do governo);

- Efeitos no tempo – este critério permite verificar até que ponto a perda de um elemento pode ter um impacto grave (ou seja, imediato, 24-48 horas, uma semana, outro).

No entanto, em muitos casos, os efeitos psicológicos podem agravar acontecimentos que em si mesmo seriam de menor importância.

A evolução da situação em matéria de protecção das infra-estruturas críticas consta do Anexo técnico, o qual fornece uma perspectiva sectorial das realizações da Comissão até agora. Estes progressos mostram que a Comissão adquiriu uma experiência considerável nesta matéria.

3.2. Gestão da segurança

Para proceder à análise da ameaça, do incidente e da vulnerabilidade dos elementos das infra-estruturas críticas dos Estados-Membros e dos elementos que delas dependem, é conveniente obter informações de várias fontes. Cada sector e cada Estado-Membro deverão identificar as infra-estruturas que para si são críticas nos seus territórios, segundo uma fórmula harmonizada a nível da UE, bem como as organizações ou pessoas responsáveis pela sua segurança.

Nem todas as infra-estruturas podem ser protegidas contra todas as ameaças. Por exemplo, as redes de transmissão de electricidade são demasiado extensas para poderem ser vedadas ou vigiadas. No entanto, através de técnicas de gestão de risco, a atenção pode concentrar-se em áreas de maior risco, tendo em conta a ameaça, a importância relativa, o nível existente de segurança e a eficácia das estratégias existentes para limitar as incidências e assegurar a continuidade da actividade.

A gestão da segurança é um processo deliberado destinado a determinar o risco e a definir e aplicar acções com vista a reduzir o risco para um nível determinado, isto é, um nível de risco aceitável a um custo aceitável. Esta abordagem consiste em identificar, medir e controlar os riscos, para os manter a um nível correspondente a um nível predeterminado.

A protecção das infra-estruturas críticas (PIC) requer uma parceria coerente, baseada na colaboração entre os proprietários e operadores das infra-estruturas críticas e as autoridades dos Estados-Membros. Os proprietários e os operadores continuam a ser os principais responsáveis pela gestão dos riscos em instalações físicas, cadeias de abastecimento, tecnologias de informação e redes de comunicação.

Devem ser emitidos alertas, avisos e notas informativas para ajudar os parceiros dos sectores público e privado a proteger as suas principais infra-estruturas. Pontualmente, podem surgir riscos ou ameaças específicos de um atentado terrorista, o que exige uma resposta imediata. Nesses casos, será necessária uma resposta bem coordenada e bem orientada por parte dos governos e das empresas dos Estados-Membros. Por seu lado, a UE deveria coordenar as respostas políticas necessárias e, neste contexto, serão acordadas, com as partes interessadas, disposições pormenorizadas de execução numa base individual.

Mesmo os melhores planos de gestão de segurança e a legislação que obriga à sua execução não terão qualquer valor se não forem devidamente aplicados. A experiência mostra que inspecções independentes da Comissão destinadas a verificar a sua aplicação são o único instrumento eficaz susceptível de garantir uma correcta aplicação dos requisitos de segurança.

4. PROGRESSOS REALIZADOS ATÉ AO MOMENTO EM MATÉRIA DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS A NÍVEL COMUNITÁRIO

Os europeus esperam que as infra-estruturas essenciais continuem a funcionar, independentemente das organizações a que pertencem ou que as operam. Consideram também que os governos dos Estados-Membros e a UE devem desempenhar um papel predominante neste contexto. Esperam que os proprietários e os operadores a todos os níveis do sector público e do sector privado colaborarão, a fim de assegurar a continuidade dos serviços de que dependem.

Para complementar as medidas tomadas a nível nacional, a União Europeia já adoptou um certo número de medidas legislativas que estabelecem normas mínimas para a protecção das infra-estruturas no quadro de diferentes políticas comunitárias. É nomeadamente o caso dos transportes, das comunicações, da energia, da saúde e da segurança no trabalho e ainda da saúde pública. Na sequência dos recentes atentados na América e na Europa, foi dado um novo impulso a algumas destas actividades. Estas permitirão continuar a melhorar e a alargar as medidas existentes.

Durante décadas, foram efectuadas inspecções no âmbito do Tratado Euratom, a fim de controlar a utilização apropriada dos materiais nucleares. No domínio da protecção contra as radiações, existe legislação considerável que se aplica aos riscos relacionados com o funcionamento das instalações e a utilização de fontes que envolvem substâncias radioactivas.

No âmbito do transporte internacional, a União Europeia adoptou legislação que permite aplicar ou reforçar os acordos alcançados pelos organismos internacionais de regulamentação dos sectores da aviação e dos transportes marítimos. A União Europeia continuará a promover e a participar activamente nestas actividades a nível internacional e, neste âmbito, encorajará os países terceiros que com ela mantêm relações económicas a aplicarem estes acordos. A UE forneceu assistência a alguns deles, com vista a atingir um nível homogéneo e constante de segurança, tanto no interior, como para além das fronteiras da UE.

A criação de agências, como a Agência Europeia para a Segurança das Redes e da Informação (ENISA), que tem como objectivo a segurança das comunicações, constitui um novo marco. Além disso, em sectores como o da segurança dos transportes aéreos e marítimos, foram criados serviços de inspecção da Comissão para controlar a aplicação da legislação de segurança nos Estados-Membros. Estas inspecções permitem estabelecer as referências necessárias e assegurar um nível de aplicação uniforme em toda a União.

O Anexo técnico inclui informações relativas aos actuais desenvolvimentos em matéria de protecção das infra-estruturas críticas e apresenta uma perspectiva sectorial das realizações da Comissão até agora. Revelam que a Comissão adquiriu uma experiência considerável neste domínio.

5. REFORÇO DA CAPACIDADE DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS DA UE

5.1. Programa Europeu para a Protecção das Infra-estruturas Críticas

Tendo em conta o grande número de potenciais infra-estruturas críticas e as suas próprias particularidades, é impossível protegê-las a todas através de medidas europeias. Aplicando o princípio da subsidiariedade, a Europa deve concentrar os seus esforços na protecção das infra-estruturas de dimensão transnacional e deixar as outras sob a responsabilidade dos Estados-Membros, ainda que no âmbito de um quadro comum.

Existem já numerosas directivas e regulamentos que impõem meios para a detecção de acidentes, para a elaboração de planos de intervenção em colaboração com a protecção civil, para efectuar exercícios regulares e para estabelecer relações claras entre os diversos níveis de intervenção: poderes públicos, organismos centrais e serviços de urgência. Pelo contrário, muito resta ainda a fazer a nível da protecção das instalações energéticas, com excepção das nucleares. Tal como mostra o Anexo técnico, o acervo comunitário em matéria de protecção das infra-estruturas críticas apresenta vários níveis de desenvolvimento.

Na maioria dos domínios acima mencionados, os trabalhos prosseguem e foi instituída uma cooperação com os peritos dos Estados-Membros e os sectores económicos interessados, a fim de identificar eventuais lacunas e as medidas correctivas a introduzir (de carácter jurídico ou outro). Foi criado um grande número de redes e de comités de segurança.

A Comissão informará anualmente as outras instituições dos progressos realizados nesta matéria através de uma comunicação. A Comissão analisará para cada sector os progressos dos trabalhos comunitários em matéria da avaliação do risco, do desenvolvimento de técnicas de protecção ou as acções legais em curso ou previstas, com vista a obter os seus pareceres. Se necessário, a Comissão proporá ainda nesta comunicação actualizações e medidas organizativas de carácter horizontal, que requerem harmonização, coordenação ou cooperação. Esta comunicação, que integrará todas as análises e medidas sectoriais, deverá constituir a base de um Programa Europeu para a Protecção das Infras-estruturas Críticas (PEPIC).

Tal programa deverá ajudar as empresas e os governos dos Estados-Membros a todos os níveis na UE, ao mesmo tempo que respeita as responsabilidades e os mandatos de cada um. A Comissão considera que uma rede que reúna os especialistas dos Estados-Membros da UE em matéria de protecção das infra-estruturas críticas poderia ajudar esta instituição a elaborar o programa. Esta rede de informação sobre alertas nas infra-estruturas críticas deverá ser criada o mais rapidamente possível em 2005.

A criação da rede deveria principalmente contribuir para estimular a troca de informações sobre ameaças e vulnerabilidades partilhadas, bem como medidas e estratégias apropriadas para limitar os riscos e proteger as infra-estruturas críticas. Os Estados-Membros deveriam, por seu turno, assegurar-se que as informações pertinentes são transmitidas a todos os departamentos ministeriais e serviços relevantes, incluindo os serviços de emergência e os sectores industriais que deverão, por sua vez, informar os proprietários e operadores das infra-estruturas críticas através de uma rede de contactos estabelecida nos Estados-Membros.

O PEPIC proporcionaria um fórum permanente em que poderia ser estabelecido o equilíbrio adequado entre as limitações da concorrência, da responsabilidade e da sensibilidade da informação e as vantagens de se dispor de infra-estruturas críticas mais seguras. As empresas seriam estreitamente associadas a este processo. O programa contribuirá para transmitir mais informações aos parceiros sobre as situações específicas de ameaça, o que lhes permitirá tomar medidas para fazer face às suas eventuais consequências. A responsabilidade dos proprietários e operadores na tomada das suas próprias decisões e planos a fim de proteger os seus bens não é afectada.

Quando não existam normas sectoriais ou normas internacionais, o Comité Europeu de Normalização (CEN) e outros organismos de normalização poderiam ajudar a rede e propor normas de segurança uniformes a nível sectorial e adaptadas para todos os sectores interessados. Tais normas deveriam também ser propostas a nível internacional através da ISO, de modo a estabelecer condições uniformes.

As ameaças à segurança das infra-estruturas críticas, incluindo o terrorismo, devem ser evocadas com prudência para não suscitar inquietações inúteis na população da UE, nem entre os turistas e investidores potenciais. O terrorismo é uma ameaça constante, mas os responsáveis políticos devem encorajar os seus concidadãos a prosseguirem as suas vidas o mais normalmente possível. Além disso, deverá ser preservado o direito à vida privada, tanto dentro como fora da União. Os consumidores e os agentes económicos devem estar certos de que as informações serão tratadas de forma correcta, confidencial e fiável. Um quadro apropriado deverá garantir que as informações classificadas são geridas correctamente e protegidas contra qualquer divulgação ou utilização não autorizada.

Uma parte importante das infra-estruturas críticas, tanto da UE como dos Estados-Membros, atravessam as fronteiras da UE. Os oleodutos atravessam continentes, os cabos indispensáveis ao bom funcionamento das tecnologias da informação estão enterrados no fundo dos oceanos, etc. Isto significa que a cooperação internacional desempenha um papel importante no estabelecimento de parcerias nacionais e internacionais permanentes e dinâmicas entre os proprietários e os operadores de infra-estruturas críticas e os governos dos países terceiros, em especial quando se trata de fornecedores directos de produtos energéticos à União.

5.2. Aplicação do PEPIC

A protecção das infra-estruturas críticas requer a participação activa dos proprietários e dos operadores das infra-estruturas, dos órgãos de regulação, das organizações profissionais e das associações industriais, dos Estados-Membros e da Comissão. A partir das informações fornecidas pelos Estados-Membros e colocadas em rede, o objectivo do PEPIC consiste em continuar a identificar as infra-estruturas críticas, analisar a sua vulnerabilidade e a sua interdependência e apresentar soluções que as protejam e preparem para todos os tipos de perigos. Nesta perspectiva, deveria nomeadamente ajudar os sectores industriais a determinar a ameaça terrorista e as suas consequências potenciais para a sua análise do risco. Os serviços responsáveis pela aplicação da lei dos Estados-Membros e o mecanismo de protecção civil deverão integrar o PEPIC nas suas actividades de programação e de sensibilização.

Em estreita coordenação com a rede, os serviços da Comissão desenvolverão novas medidas que passam nomeadamente pela adopção de legislação e/ou pela difusão de informação. A unidade dos chefes da polícia e a Europol teriam um papel a desempenhar na divulgação de informações sobre os níveis de segurança relevantes e outras junto dos serviços responsáveis pela aplicação da lei dos Estados-Membros. Estes deveriam, por sua vez, estabelecer contactos com os proprietários e operadores das infra-estruturas essenciais, tendo em vista aconselhá-los a propósito das informações relativas à ameaça terrorista e contribuir para a adopção de estratégias de protecção contra o terrorismo.

Os governos dos Estados-Membros continuarão a desenvolver e a alimentar bases de dados relativas às infra-estruturas críticas a nível nacional e serão encarregados de elaborar, validar e verificar os planos adequados, assegurando deste modo a continuidade dos serviços sob sua jurisdição. Ao elaborar o PEPIC, a Comissão apresentará sugestões relativamente ao que deve ser o conteúdo mínimo e o formato de tais bases de dados e como se devem interconectar.

Os governos dos Estados-Membros deveriam continuar, por sua vez, a informar os proprietários e operadores das infra-estruturas críticas (tal como os outros Estados-Membros, se apropriado) das informações e dos alertas pertinentes, comunicando-lhes o tipo de resposta definido para cada nível de ameaça ou de alerta.

Os proprietários e os operadores das infra-estruturas críticas assegurarão a segurança adequada aos seus bens, graças à aplicação dos seus planos de segurança e à realização de inspecções regulares, exercícios, avaliações e planos. Os Estados-Membros deveriam controlar o processo a nível geral, enquanto a Comissão deveria assegurar uma aplicação uniforme em toda a União, através de sistemas de inspecção adequados.

5.3. Objectivos e indicadores do PEPIC

O objectivo do PEPIC e o papel da Comissão consistiriam em assegurar a existência de níveis de protecção adequados e uniformes das infra-estruturas críticas, de reduzir ao mínimo as falhas e fornecer no conjunto da União Europeia meios de reacção rápida que tenham sido

testados. O programa estará em constante evolução e será reexaminado regularmente em função da evolução dos problemas e das preocupações da sociedade.

O sucesso deverá ser avaliado com base nos seguintes elementos:

- a identificação e elaboração de inventários pelos governos dos Estados-Membros das infra-estruturas críticas situadas nos seus territórios, de acordo com as prioridades definidas pelo PEPIC;

- a colaboração das empresas no âmbito dos seus respectivos sectores e com o governo para partilhar a informação e para reduzir a probabilidade de incidentes que provocam perturbações frequentes ou prolongadas das infra-estruturas críticas;

- a Comunidade Europeia define uma abordagem comum para tratar do problema da segurança das infra-estruturas críticas graças à colaboração de todos os actores, tanto públicos como privados.

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.