KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 20.10.2004
KOM(2004) 702 endgültig

**MITTEILUNG DER KOMMISSION
AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT**

Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung

INHALTSVERZEICHNIS

1. EINLEITUNG 3

2. DIE BEDROHUNG 3

3. DIE KRITISCHEN INFRASTRUKTUREN EUROPAS 3

3.1. Was versteht man unter kritischen Infrastrukturen? 3

3.2. Sicherheitsmanagement 6

4. BISHERIGE FORTSCHRITTE BEIM SCHUTZ KRITISCHER INFRASTRUKTUREN AUF GEMEINSCHAFTSEBENE 6

5. AUSBAU DES EU-POTENZIALS ZUM SCHUTZ KRITISCHER INFRASTRUKTUREN 7

5.1. Ein Europäisches Programm für den Schutz kritischer Infrastrukturen 7

5.2. Durchführung des EPCIP 9

5.3. Ziele des EPCIP und Fortschrittsindikatoren 10

TECHNICAL ANNEX 11

1. EINLEITUNG

Auf seiner Tagung vom Juni 2004 beauftragte der Europäische Rat die Kommission und den Hohen Vertreter mit der Ausarbeitung einer umfassenden Strategie zum Schutz kritischer Infrastrukturen.

Die vorliegende Mitteilung gibt einen Überblick über die derzeitigen Maßnahmen der Kommission zum Schutz kritischer Infrastrukturen und enthält Vorschläge für zusätzliche Maßnahmen zur Stärkung der bestehenden Instrumente und zur Erfüllung der vom Europäischen Rat erteilten Aufträge.

2. DIE BEDROHUNG

Die Gefahr folgenschwerer Terroranschläge auf kritische Infrastrukturen nimmt zu. Die Folgen von Anschlägen auf Steuersysteme kritischer Infrastrukturen können äußerst vielfältig sein. Es wird allgemein angenommen, dass ein erfolgreicher Cyber-Angriff zwar, wenn überhaupt, nur wenige Opfer fordern, jedoch zum Verlust lebenswichtiger Infrastrukturdienste führen würde. Im Falle eines erfolgreichen Cyber-Angriffs auf das öffentliche Telefonnetz wäre zum Beispiel den Kunden die Möglichkeit zu telefonieren genommen, während die Techniker das Vermittlungsnetz wiederherstellen und reparieren. Ein Angriff auf Steuersysteme von Chemie- oder Flüssigerdgasanlagen könnte mehr Menschenleben fordern sowie zu erheblichen Sachbeschädigungen führen.

Eine andere Art eines folgenschweren Infrastrukturausfalls könnte entstehen, wenn ein Teil der Infrastruktur den Ausfall anderer Teile verursacht und dadurch einen Dominoeffekt auslöst. Ein solcher Ausfall könnte sich durch das Zusammenwirken der Infrastrukturbereiche ergeben. Ein einfaches Beispiel dafür wäre ein Anschlag auf ein Stromversorgungsunternehmen, der eine Unterbrechung der Stromversorgung nach sich zieht; in der Folge könnten auch Abwasserbehandlungsanlagen und Wasserwerke ausfallen, wenn die Turbinen und anderen elektrischen Vorrichtungen in diesen Anlagen zum Stillstand kommen.

Auch Dominoeffekte können zu enormen Schäden führen und umfassende Versorgungsausfälle verursachen. Die Stromausfälle in Nordamerika und Europa in den letzten zwei Jahren haben die Verwundbarkeit der Infrastrukturen im Energiebereich sowie die Notwendigkeit gezeigt, dass zur Verhinderung bzw. Abschwächung der Folgen eines größeren Versorgungsausfalls wirksame Lösungen gefunden werden müssen. Diese Art des Cyber-Terrorismus könnte auch die Folgen eines Angriffs auf ein Gebäude verschärfen. Ein Beispiel dafür wäre ein herkömmlicher Sprengstoffanschlag auf ein Gebäude, verbunden mit einem vorübergehenden Ausfall des Strom- oder Telefonnetzes. Da dies die Hilfseinsätze erschwert, bis Notsysteme für die Stromversorgung und Kommunikation eingerichtet und einsatzbereit sind, könnte es zu einer Erhöhung der Opferzahl und zu allgemeiner Panik kommen.

3. DIE KRITISCHEN INFRASTRUKTUREN EUROPAS

3.1. Was versteht man unter kritischen Infrastrukturen?

Kritische Infrastrukturen sind materielle und informationstechnologische Einrichtungen, Netze, Dienste und Anlagegüter, deren Störung oder Vernichtung gravierende Auswirkungen

auf die Gesundheit, die Sicherheit oder das wirtschaftliche Wohlergehen der Bürger sowie auf das effiziente Funktionieren der Regierungen in den Mitgliedstaaten hätte. Kritische Infrastrukturen sind in vielen Wirtschaftssektoren, u. a. im Bank- und Finanzwesen, im Verkehrs- und Verteilungssektor, in den Bereichen Energie, Versorgungseinrichtungen, Gesundheit, Lebensmittelversorgung und Kommunikation sowie der wichtigen Dienste des Staates zu finden. Bei einigen kritischen Elementen in diesen Sektoren handelt es sich genau genommen nicht um „Infrastruktur", sondern eigentlich um Netze oder Versorgungsketten, die die kontinuierliche Versorgung mit wesentlichen Erzeugnissen oder Dienstleistungen gewährleisten. Die Versorgung unserer Ballungsräume mit Lebensmitteln und Wasser hängt zum Beispiel nicht nur von einigen wichtigen Einrichtungen ab, sondern auch von einem verzweigten Netz von Erzeugern, Be- und Verarbeitern, Herstellern, Verteilern und Einzelhändlern.

Zu den kritischen Infrastrukturen gehören:

- Energieanlagen und -netze (z.B. Strom-, Öl- und Gaserzeugung, Speicheranlagen und Raffinerien, Übertragungs- und Verteilungssysteme)

- Kommunikations- und Informationstechnologien (z.B. Fernmeldewesen, Rundfunksysteme, Software, Hardware und Netze wie das Internet)

- Finanzwesen (z.B. Bankwesen, Versicherungs- und Investmentbereich)

- Gesundheitswesen (z.B. Krankenhäuser, Gesundheits- und Blutversorgungseinrichtungen, Laboratorien und Arzneimittel, Such- und Rettungswesen, Hilfsdienste)

- Lebensmittel (z.B. Sicherheit, Produktionsmittel, Großhandel und Lebensmittelindustrie)

- Wasser (z.B. Stau-, Speicher- und Behandlungsanlagen sowie Netze)

- Verkehr (z.B. Flughäfen, Häfen, intermodale Einrichtungen, Eisenbahnverkehr und öffentliche Nahverkehrsnetze, Verkehrsleitsysteme)

- Erzeugung, Lagerung und Beförderung gefährlicher Güter (z.B. chemische, biologische, radiologische und nukleare Stoffe)

- Staatliche Einrichtungen (z.B. wichtige Dienste, Anlagen, Informationsnetze, Anlagegüter und bedeutende nationale Stätten und Denkmäler)

Diese Infrastrukturen gehören sowohl dem öffentlichen als auch dem privaten Sektor oder werden von diesen betrieben. In ihrer Mitteilung 574/2001 vom 10. Oktober 2001 erklärte die Kommission: „Die Verschärfung einiger dieser Maßnahmen durch staatliche Stellen infolge der Angriffe, die sich gegen die gesamte Gesellschaft und nicht nur gegen die am Luftverkehr Beteiligten richten, muss nach Auffassung der Kommission vom Staat übernommen werden". Der öffentliche Sektor spielt daher eine wesentliche Rolle.

Kritische Infrastrukturen müssen auf Ebene der Mitgliedstaaten und auf europäischer Ebene bestimmt werden, und diese Listen sollten bis Ende 2005 erstellt sein.

Die kritischen Infrastrukturen Europas sind eng miteinander verbunden und in hohem Maße voneinander abhängig. Dies ist u. a. auf Faktoren wie Unternehmenszusammenführungen, die

Rationalisierung der Industrie, effiziente Geschäftspraktiken wie Just-in-time-Fertigung und die Konzentration der Bevölkerung in Ballungsräumen zurückzuführen. Die kritischen Infrastrukturen in Europa sind abhängiger von verbreiteten Informationstechnologien wie dem Internet und der satellitengestützten Funknavigation und –kommunikation geworden. Da diese Infrastrukturen voneinander abhängig sind, können Probleme in Kettenreaktionen aufeinander folgen und unerwartete und immer gravierendere Ausfälle wesentlicher Dienste verursachen. Durch ihre Vernetzung und gegenseitige Abhängigkeit können diese Infrastrukturen leichter gestört oder vernichtet werden.

Die Kriterien zur Bestimmung der Faktoren, die eine bestimmte Infrastruktur oder ein bestimmtes Element einer Infrastruktur kritisch machen, müssen untersucht werden. Diese Auswahlkriterien sollten sich auch auf sektorspezifisches sowie kollektives Expertenwissen stützen. Zur Bestimmung potenziell kritischer Infrastrukturen könnten drei Faktoren herangezogen werden:

- Reichweite – Der Verlust eines kritischen Infrastrukturelements wird anhand der Größe des geografischen Gebietes beurteilt, das durch seinen Verlust oder seine Nichtverfügbarkeit beeinträchtigt wird – auf internationaler, nationaler, Provinz-/Gebiets- oder lokaler Ebene.

- Schwere – Die Auswirkungen oder der Verlust können als gleich null, minimal, mittelschwer oder erheblich bewertet werden. Zur Feststellung der potenziellen Schwere könnten u. a. folgende Kriterien dienen:

    (a) Auswirkungen auf die Allgemeinheit (die Zahl der betroffenen Personen, Todesopfer, Erkrankungen, schwere Verletzungen, Evakuierung);

    (b) Wirtschaftliche Auswirkungen (Auswirkungen auf das BIP, Schwere des wirtschaftlichen Verlusts und/oder Minderung der Qualität von Erzeugnissen oder Dienstleistungen);

    (c) Auswirkungen auf die Umwelt (Auswirkungen auf die Allgemeinheit und auf die Umgebung); und

    (d) Gegenseitige Abhängigkeit (Abhängigkeit der kritischen Infrastrukturelemente untereinander).

    (e) Politische Auswirkungen (Vertrauen in die Fähigkeiten der Regierung);

- Zeitliche Auswirkungen – Anhand dieses Kriteriums wird festgelegt, zu welchem Zeitpunkt der Verlust eines Elements schwerwiegende Auswirkungen haben könnte (z.B. sofort, nach 24-48 Stunden, nach einer Woche, zu einem anderen Zeitpunkt).

In vielen Fällen kann auch die psychologische Wirkung an sich harmlose Ereignisse dramatisieren.

Die derzeitigen Entwicklungen im Bereich des Schutzes kritischer Infrastrukturen sind in Technischer Anhang beschrieben, wo ein Überblick über die bisherigen Fortschritte der Kommission in den verschiedenen Bereichen gegeben wird und aus dem hervorgeht, dass sie bereits umfassende Erfahrungen auf diesem Gebiet gesammelt hat.

3.2. Sicherheitsmanagement

Um die Bedrohung, die Zwischenfälle und die Verwundbarkeit der kritischen Infrastrukturen der Mitgliedstaaten und ihrer Abhängigkeit voneinander zu analysieren muss auf mehrere Informationsquellen zurückgegriffen werden. Alle Sektoren und Mitgliedstaaten müssen innerhalb ihrer jeweiligen Zuständigkeitsbereiche gemäß einem EU-weit harmonisierten Schema die für sie kritischen Infrastrukturen und die sicherheitsverantwortlichen Organisationen und Personen bestimmen.

Nicht alle Infrastrukturen können jedoch vor allen Bedrohungen geschützt werden. Stromnetze zum Beispiel sind zu weitläufig, um umzäunt oder bewacht werden zu können. Durch die Anwendung von Risikomanagement-Techniken kann die Aufmerksamkeit auf die am stärksten gefährdeten Bereiche konzentriert werden, wobei die Bedrohung, die relative Kritikalität, der Grad des Sicherheitsschutzes und die Wirksamkeit der zur Gewährleistung der Geschäftskontinuität verfügbaren Abhilfestrategien berücksichtigt werden.

Sicherheitsmanagement ist ein wohl durchdachter Prozess, in dessen Verlauf Gefahren erkannt werden und Maßnahmen zur Minderung der Gefahr auf ein bestimmtes, annehmbares Ausmaß zu einem akzeptablen Preis beschlossen und durchgeführt werden sollen. Dieser Ansatz besteht in der Feststellung, Messung und Reduzierung der Gefahr auf ein bestimmtes vorgegebenes Ausmaß.

Der Schutz kritischer Infrastrukturen (Critical infrastructure protection - CIP) erfordert eine konstante, kooperative Partnerschaft zwischen den Eigentümern und Betreibern kritischer Infrastrukturen einerseits und den Behörden der Mitgliedstaaten andererseits. Die Verantwortung für das Risikomanagement in technischen Einrichtungen, Versorgungsketten, informationstechnologischen Einrichtungen und Kommunikationsnetzen liegt in erster Linie bei den Eigentümern und Betreibern.

Warnungen, Ratschläge und Informationen müssen verbreitet werden, um die Beteiligten im öffentlichen und im privaten Sektor beim Schutz wichtiger Infrastruktursysteme zu unterstützen. Von Zeit zu Zeit kann es zu gewissen Gefahren oder Bedrohungen durch Terroranschläge kommen, auf die unmittelbar reagiert werden muss. In diesen Fällen müssen die Regierungen und Gewerbetreibenden der Mitgliedstaaten koordiniert und einsatzorientiert reagieren. Dabei sollte die EU die notwendigen politischen Schritte koordinieren und dann mit den Beteiligten die Unterstützungsmaßnahmen im Einzelnen und von Fall zu Fall absprechen.

Die besten Sicherheitsmanagement-Pläne und Rechtsvorschriften zu deren Durchsetzung sind jedoch wertlos, wenn sie nicht richtig umgesetzt werden. Die Erfahrung hat gezeigt, dass unabhängige Kontrollen der Umsetzung der Sicherheitsvorschriften durch die Kommission das einzig wirksame Mittel sind, ihre Einhaltung zu gewährleisten.

4. BISHERIGE FORTSCHRITTE BEIM SCHUTZ KRITISCHER INFRASTRUKTUREN AUF GEMEINSCHAFTSEBENE

Die Bürger Europas erwarten, dass kritische Infrastrukturen stets klaglos funktionieren, egal, welche Einrichtungen Eigentümer oder Betreiber ihrer Bestandteile sind. Sie gehen davon aus, dass es vor allem Aufgabe der Regierungen der Mitgliedstaaten und der EU ist, dies zu gewährleisten. Sie erwarten, dass auf allen Ebenen der Regierungen, der Eigentümer im

Privatsektor und der Betreiber zusammengearbeitet wird, um die Kontinuität der für die europäischen Bürger lebenswichtigen Dienste zu gewährleisten.

Zusätzlich zu den einzelstaatlichen Maßnahmen hat die Europäische Union bereits eine Reihe gesetzgeberischer Maßnahmen ergriffen, durch die im Rahmen der verschiedenen EU-Politiken Mindeststandards für den Schutz von Infrastrukturen festgelegt wurden. Dies ist insbesondere in den Bereichen Verkehr, Kommunikation, Energie, Arbeitsschutz und Gesundheitswesen der Fall. Nach den jüngsten Anschlägen in Amerika und Europa wurden die Aktivitäten verstärkt, was zu einer weiteren Verbesserung bzw. zu einem Ausbau der bestehenden Maßnahmen führen wird.

Seit Jahrzehnten wurden Inspektionen im Rahmen des EURATOM-Vertrags durchgeführt, um die ordnungsgemäße Nutzung nuklearer Stoffe zu kontrollieren. Auf dem Gebiet des Strahlenschutzes gibt es zahlreiche Rechtsvorschriften zu den Gefahren im Zusammenhang mit dem Betrieb von Anlagen und der Nutzung von Energiequellen auf Basis nuklearer Stoffe.

Auf dem Gebiet des internationalen Verkehrs hat die Europäische Union Rechtsvorschriften zur Um- bzw. Durchsetzung der Abkommen erlassen, die von den internationalen Entscheidungsgremien im Luft- und im Seeverkehrssektor geschlossen wurden. Die Europäische Union wird deren Aktivitäten auf internationaler Ebene weiterhin fördern und aktiv daran teilnehmen. Sie wird mit der EU in Wirtschaftsbeziehungen stehende Drittländer dazu anhalten, diese Abkommen umzusetzen. Sie unterstützt einige von ihnen, um innerhalb der EU und über ihre Grenzen hinaus ein homogenes und konstantes Sicherheitsniveau zu erreichen.

Ein weiterer Schritt wurde mit der Einrichtung von Agenturen für Datensicherheit wie der Europäischen Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency - ENISA) gesetzt. Außerdem wurden in Bereichen wie der Flug- und Seeverkehrssicherheit Inspektionsdienste innerhalb der Kommission geschaffen, um die Anwendung der Sicherheitsvorschriften durch die Mitgliedstaaten zu überprüfen. Dank dieser Inspektionen können die notwendigen Richtwerte festgelegt werden, wodurch gewährleistet wird, dass diese Vorschriften in der gesamten Union gleichermaßen angewandt werden.

Die derzeitigen Entwicklungen im Bereich des Schutzes kritischer Infrastrukturen sind in Technischer Anhang beschrieben, wo ein Überblick über die bisherigen Fortschritte der Kommission in den verschiedenen Bereichen gegeben wird und aus dem hervorgeht, dass sie bereits umfassende Erfahrungen auf diesem Gebiet gesammelt hat.

5. AUSBAU DES EU-POTENZIALS ZUM SCHUTZ KRITISCHER INFRASTRUKTUREN

5.1. Ein Europäisches Programm für den Schutz kritischer Infrastrukturen

Da es eine Vielzahl potenziell kritischer Infrastrukturen gibt, die jeweils eigene Besonderheiten aufweisen, können nicht alle durch Maßnahmen auf europäischer Ebene geschützt werden. In Anwendung des Subsidiaritätsprinzips muss die Union ihre Bemühungen auf den Schutz von Infrastrukturen mit grenzüberschreitender Wirkung konzentrieren und die übrigen der alleinigen Verantwortung der Mitgliedstaaten überlassen – wenn auch in einem gemeinsamen Rahmen.

Es gibt bereits zahlreiche Richtlinien und Verordnungen, in denen Mittel zur Erkennung von Unfällen, die Erstellung von Interventionsplänen in Zusammenarbeit mit dem Zivilschutz, regelmäßige Übungen und klar festgelegte Verbindungen zwischen den verschiedenen Interventionsebenen, den öffentlichen Stellen, den zentralen Einrichtungen und den Hilfsdiensten vorgesehen sind. Andererseits ist im Bereich des Schutzes von nicht nuklearen Energieanlagen noch viel zu tun. Wie aus Technischer Anhang zu ersehen ist, befindet sich der gemeinschaftliche Besitzstand im Bereich des Schutzes kritischer Infrastrukturen auf unterschiedlichem Entwicklungsniveau.

In den meisten genannten Bereichen sind Arbeiten im Gange, und es wird verstärkt mit den Sachverständigen der Mitgliedstaaten und den betreffenden Wirtschaftssektoren zusammengearbeitet, um mögliche Mängel festzustellen und (rechtliche oder sonstige) Abhilfemaßnahmen zu ermitteln. Zahlreiche Netze und Sicherheitsausschüsse wurden eingerichtet.

Die Kommission wird die anderen Organe jedes Kalenderjahr in einer Mitteilung über die jeweiligen Fortschritte informieren. Sie wird für jeden Bereich den Fortgang der Gemeinschaftsarbeiten im Hinblick auf Risikoanalyse, Entwicklung von Schutztechniken oder laufende/geplante rechtliche Schritte analysieren, um Stellungnahmen von diesen Organen zu erhalten. Die Kommission wird in dieser Mitteilung gegebenenfalls auch Verbesserungen und organisatorische Maßnahmen auf horizontaler Ebene vorschlagen, die Harmonisierung, Koordinierung und Zusammenarbeit erfordern. Diese Mitteilung, die Analysen und Maßnahmen für alle Bereiche enthält, wird die Grundlage eines Europäischen Programms für den Schutz kritischer Infrastrukturen (EPCIP) bilden.

Mit einem solchen Programm sollen die Wirtschaft und die Regierungen der Mitgliedstaaten EU-weit auf allen Ebenen und unter Beachtung der einzelnen Befugnisse und Verantwortlichkeiten unterstützt werden. Die Kommission ist der Meinung, dass ein Netz aus Experten für den Schutz kritischer Infrastrukturen aus den EU-Mitgliedstaaten die Kommission bei der Erstellung des Programms unterstützen könnte – dieses Warn- und Informationsnetz für kritische Infrastrukturen (Critical Infrastructure Warning Information Network - CIWIN) sollte 2005 so bald wie möglich eingerichtet werden.

Die Einrichtung dieses Netzes sollte vor allem der Förderung des Informationsaustausches über gemeinsame Bedrohungen und Gefährdungen sowie über geeignete Maßnahmen und Strategien zur Risikoverringerung im Hinblick auf den Schutz kritischer Infrastrukturen dienen. Die Mitgliedstaaten würden daher ihrerseits dafür sorgen, dass die entsprechenden Informationen an alle zuständigen Ministerien und sonstigen Institutionen, wie zum Beispiel Hilfsorganisationen, weitergegeben werden und die zuständigen Stellen der jeweiligen Wirtschaftssektoren unterrichten, damit diese ihrerseits die betroffenen Eigentümer und Betreiber kritischer Infrastrukturen durch ein in den Mitgliedstaaten eingerichtetes Kontaktnetz informieren können.

Das EPCIP würde die Einrichtung eines permanenten Forums ermöglichen, in dessen Rahmen auf ein ausgeglichenes Verhältnis zwischen den Zwängen des Wettbewerbs, der Verantwortlichkeit und der Sensibilität von Informationen einerseits und den Vorteilen sichererer kritischer Infrastrukturen andererseits hingearbeitet werden kann. Die Wirtschaft wird in diesen Prozess eng eingebunden werden. Damit könnten den Partnern mehr Informationen über bestimmte Bedrohungssituationen übermittelt werden, anhand derer sie Maßnahmen zur Abwehr möglicher Folgen ergreifen können. An der Verantwortung der

Eigentümer und Betreiber, zum Schutz ihrer Anlagegüter Entscheidungen zu treffen und Pläne zu erstellen, sollte sich nichts ändern.

In Fällen, für die es keine sektorspezifischen Standards oder noch keine internationalen Normen gibt, könnten das Europäische Komitee für Normung (CEN) und andere zuständige Normungsgremien das Netz unterstützen und einheitliche sektorspezifische und angepasste Sicherheitsstandards für alle beteiligten Branchen und Sektoren vorschlagen. Solche Standards sollten auch auf internationaler Ebene von ISO vorgeschlagen werden, um in dieser Hinsicht gleiche Bedingungen zu schaffen.

Vorsicht ist bei der Bekanntmachung nationaler Sicherheitsgefährdungen für kritische Infrastrukturen, wie zum Beispiel durch Terrorismus, geboten, da unnötige Beunruhigung sowohl innerhalb der EU als auch unter potenziellen Touristen oder Investoren vermieden werden muss. Der Terrorismus stellt eine konstante Bedrohung dar, es ist jedoch Aufgabe der politischen Entscheidungsträger, die Allgemeinheit dazu anzuhalten, sich so wenig wie möglich in ihrem gewohnten Tagesablauf beeinträchtigen zu lassen. Auch der Schutz der Privatsphäre muss sowohl innerhalb als auch außerhalb der Union gewährleistet bleiben. Verbraucher und Wirtschaftsbeteiligte müssen die Gewissheit haben, dass Informationen mit Sorgfalt, vertraulich und seriös behandelt werden. Ein entsprechender Rahmen zur Gewährleistung der ordnungsgemäßen Handhabung von Verschlusssachen und ihres Schutzes vor unbefugtem Gebrauch und vor Offenlegung ist erforderlich.

Ein großer Teil der kritischen Infrastrukturen sowohl der EU als auch der Mitgliedstaaten geht über die Grenzen der EU hinaus. Zum Beispiel erstrecken sich Pipelines über ganze Kontinente und wichtige Kabel für die Informationstechnologie sind tief im Meeresgrund versenkt. Das heißt, dass die internationale Zusammenarbeit eine wichtige Komponente beim Aufbau permanenter, dynamischer nationaler und internationaler Partnerschaften zwischen Eigentümern bzw. Betreibern kritischer Infrastrukturen und den Regierungen von Drittländern ist, insbesondere was Lieferanten betrifft, die die Union auf direktem Wege mit Energieerzeugnissen versorgen.

5.2. Durchführung des EPCIP

Der Schutz kritischer Infrastrukturen erfordert die aktive Beteiligung der Eigentümer und Betreiber von Infrastrukturen, der Behörden, der Berufs- und Industrieverbände sowie der Mitgliedstaaten und der Kommission. Das EPCIP hat das Ziel, ausgehend von den durch die Mitgliedstaaten und über das Netz bereitgestellten Informationen laufend kritische Infrastrukturen zu ermitteln, die Gefährdung und gegenseitige Abhängigkeit zu analysieren und Lösungen für den Schutz vor allen Arten von Gefahren und zur Vorbereitung darauf anzubieten. Dies schließt mit ein, die Wirtschaftssektoren im Rahmen ihres Risikomanagements bei der Erkennung der Gefahren und der möglichen Folgen zu unterstützen. Die Strafverfolgungsbehörden der Mitgliedstaaten und das Katastrophenschutzverfahren sollten dafür sorgen, dass das EPCIP zu einem festen Bestandteil der Planung und der Sensibilisierungsmaßnahmen dieser Sektoren wird.

Die Dienststellen der Kommission werden in enger Koordination mit dem Netz weitere Maßnahmen ausarbeiten, die im Erlass von Rechtsvorschriften und/oder der Verbreitung von Informationen bestehen sollten. Die Task Force der Polizeichefs und Europol spielt eine wichtige Rolle bei der Weiterleitung der Informationen über die entsprechenden Sicherheitsstufen und nachrichtendienstlichen Erkenntnisse an die Strafverfolgungsbehörden der Mitgliedstaaten, die ihrerseits mit den Eigentümern und Betreibern kritischer

Infrastrukturen Kontakt aufnehmen und ihnen die entsprechenden Informationen über die Bedrohung übermitteln und Ratschläge zum Sicherheitsschutz und zur Entwicklung von Sicherheitsschutzstrategien im Kampf gegen den Terrorismus geben sollten.

Die Regierungen der Mitgliedstaaten werden Datenbanken über national bedeutende kritische Infrastrukturen weiterführen und/oder entwickeln sowie pflegen und wären verantwortlich für die Entwicklung, Validierung und Prüfung entsprechender Pläne, um die Kontinuität der Dienste ihrer Zuständigkeitsbereiche zu gewährleisten. Bei der Erstellung des EPCIP wird die Kommission Vorschläge zum Mindestinhalt und zur Form solcher Datenbanken machen sowie dazu, wie diese untereinander verbunden sein sollten.

Die Regierungen der Mitgliedstaaten informieren ihrerseits die Eigentümer und Betreiber kritischer Infrastrukturen (sowie gegebenenfalls die Mitgliedstaaten) über die entsprechenden nachrichtendienstlichen Erkenntnisse und Warnungen sowie über die für jede Gefahren- bzw. Alarmstufe vereinbarte Art der Reaktion.

Die Eigentümer und Betreiber kritischer Infrastrukturen sorgen für die entsprechende Sicherheit ihrer Anlagegüter, indem sie ihre Sicherheitspläne aktiv umsetzen und regelmäßige Inspektionen sowie Übungen, Bewertungen und Pläne durchführen. Die Mitgliedstaaten sollten den allgemeinen Ablauf kontrollieren, während die Kommission eine gleichmäßige Umsetzung in der gesamten Union und geeignete Inspektionssysteme gewährleisten sollte.

5.3. Ziele des EPCIP und Fortschrittsindikatoren

Das Ziel der EPCIP und die Aufgabe der Kommission bestünde darin, ein angemessenes und gleichmäßiges Sicherheitsschutzniveau in Bezug auf kritische Infrastrukturen zu gewährleisten, das nur minimale einzelne Fehlerpunkte aufweist, sowie zügige, erprobte Verfahren zur Wiederherstellung der gewohnten Ordnung in der gesamten Union. Das EPCIP wird ein ständiger Prozess sein und muss regelmäßig überprüft werden, um den Problemen und Anforderungen der Gemeinschaft gerecht werden zu können.

Der Erfolg wird gemessen:

- daran, ob und inwieweit die Regierungen der Mitgliedstaaten in ihren jeweiligen Zuständigkeitsbereichen und gemäß den im Rahmen des EPCIP festgelegten Prioritäten kritische Infrastrukturen ermitteln und entsprechende Bestandsverzeichnisse erstellen;

- an der Zusammenarbeit von Unternehmen in den Sektoren und mit der Regierung zum Austausch von Informationen und zur Verringerung der Wahrscheinlichkeit von Zwischenfällen, die weitläufige oder übermäßig lange Beeinträchtigungen kritischer Infrastrukturen verursachen.

- an den Bemühungen der Europäische Gemeinschaft, einen gemeinsamen Ansatz zur Gewährleistung der Sicherheit kritischer Infrastrukturen durch die Zusammenarbeit aller Beteiligten des öffentlichen und des privaten Sektors zu finden.

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.