

**Unterrichtung**  
durch die Bundesregierung

Grünbuch der Kommission der Europäischen Gemeinschaften über ein europäisches

Programm für den Schutz kritischer Infrastrukturen

KOM(2005) 576 endg.; Ratsdok. 14910/05

Übermittelt vom Bundesministerium der Finanzen am 30. November 2005 gemäß § 2 des Gesetzes über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union (BGBl. I 1993 S. 313 ff.).

Die Vorlage ist von der Kommission der Europäischen Gemeinschaften am 17. November 2005 dem Generalsekretär/Hohen Vertreter des Rates der Europäischen Union übermittelt worden.

Hinweis: vgl. AE-Nr. 043358 und Drucksache 354/05 = AE-Nr. 051188

---

Vom Umdruck der fremdsprachigen Anhänge ist abgesehen worden, sie werden als Folgedokument an die Länder verteilt.

## GRÜNBUCH

### ÜBER EIN EUROPÄISCHES PROGRAMM FÜR DEN SCHUTZ KRITISCHER INFRASTRUKTUREN

#### 1. HINTERGRUND

Kritische Infrastrukturen (KI) können sowohl durch Naturkatastrophen, Unfälle und Nachlässigkeit als auch durch Terroranschläge, Manipulierung von Computern, mutwilliges Verhalten und sonstige strafbare Handlungen in ihrem Betrieb gestört, beschädigt oder vernichtet werden. Um Leben und Eigentum der EU-Bevölkerung vor Terroranschlägen, Naturkatastrophen und Unfällen zu schützen, sollten Störungen oder Manipulationen kritischer Infrastrukturen nach Möglichkeit nur ausnahmsweise, für kurze Zeit und örtlich begrenzt auftreten und relativ leicht zu beheben sein, um den Schaden für die Mitgliedstaaten, ihre Bürger und die Europäische Union auf ein Mindestmaß zu begrenzen. Die jüngsten Terroranschläge in Madrid und London haben die terroristische Bedrohung europäischer Infrastruktureinrichtungen deutlich gemacht. Die EU muss darauf rasch, effizient und koordiniert reagieren.

Auf seiner Tagung vom Juni 2004 beauftragte der Europäische Rat die Kommission mit der Ausarbeitung einer umfassenden Strategie für den Schutz kritischer Infrastrukturen. Daraufhin nahm die Kommission am 20. Oktober 2004 die Mitteilung „Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung“ an, in der konkrete Vorschläge zur Stärkung der Prävention, Abwehrbereitschaft und Reaktionsfähigkeit bei terroristischen Anschlägen gegen vitale Infrastrukturen formuliert wurden.

Die Absicht der Kommission, ein „Europäisches Programm für den Schutz kritischer Infrastrukturen (EPSKI)“ vorzuschlagen, wurde vom Rat in seinen Schlussfolgerungen zu Prävention, Abwehrbereitschaft und Reaktionsfähigkeit bei terroristischen Anschlägen sowie in seinem im Dezember 2004 angenommenen „EU-Solidaritätsprogramm zu den Folgen terroristischer Bedrohungen und Anschläge“ gebilligt. Der Rat stimmte überdies der von der Kommission geplanten Einrichtung eines Warn- und Informationsnetzes für kritische Infrastrukturen (WINKI) zu.

Die Kommission hat hierzu zwei Seminare veranstaltet und die Mitgliedstaaten um Vorschläge und Stellungnahmen gebeten. Das erste Seminar zum Thema „Schutz kritischer Infrastrukturen“ fand am 6./7. Juni 2005 unter Beteiligung der Mitgliedstaaten statt. Im Anschluss daran übermittelten die Mitgliedstaaten der Kommission Beiträge zu ihrer eigenen Strategie und Anmerkungen zu den auf dem Seminar erörterten Vorschlägen. Auf der Grundlage der im Juni und Juli eingegangenen Beiträge wurde die Strategie für den Schutz kritischer Infrastrukturen weiter entwickelt. Das zweite Seminar zu diesem Thema fand am 12./13. September statt. An diesem Seminar nahmen außer den Mitgliedstaaten auch Vertreter der Wirtschaft teil. Die Kommission legt jetzt im Anschluss daran dieses Grünbuch vor, in dem die Optionen für ein europäisches Schutzprogramm vorgestellt werden.

#### 2. ZIELSETZUNG

Das Grünbuch dient in erster Linie dazu, möglichst viele Akteure in die Diskussion um das europäische Programm für den Schutz kritischer Infrastrukturen einzubeziehen und ihre

Meinung zu den hier vorgestellten Optionen in Erfahrung zu bringen. Ein effizienter Schutz kritischer Infrastruktureinrichtungen setzt Kommunikation, Koordination und Kooperation sowohl auf nationaler als auch auf EU-Ebene unter Einbeziehung aller Beteiligten voraus – Eigentümer/Betreiber von Infrastrukturen, Behörden, Berufs- und Industrieverbände in Zusammenarbeit mit allen Regierungsebenen und der Öffentlichkeit.

Im Grünbuch werden Optionen vorgestellt, wie die Kommission der Aufforderung des Rates zur Ausarbeitung eines Europäischen Programms für den Schutz kritischer Infrastrukturen (EPSKI) sowie eines entsprechenden Warn- und Informationsnetzes (WINKI) nachkommen kann. Damit wird die zweite Konsultationsphase zur Einführung eines europäischen Schutzprogramms eingeleitet. Die Kommission erhofft sich konkrete Stellungnahmen zu den nachfolgend dargelegten Optionen. Ein EPSKI-Entwurf könnte je nach Ausgang der Konsultation im Laufe des Jahres 2006 vorgelegt werden.

### **3. ZWECK UND ANWENDUNGSBEREICH DES EPSKI**

#### **3.1. Was das EPSKI insgesamt bezwecken soll**

Das EPSKI soll bei kritischen Infrastrukturen unionsweit angemessene, gleiche Sicherheitsschutzstufen gewährleisten, Schwachstellen minimieren und zügige, erprobte Verfahren zur Wiederherstellung normaler Verhältnisse bereitstellen. Das Schutzniveau ist u. U. nicht für alle kritischen Infrastrukturen gleich und kann davon abhängen, wie sich der Ausfall einer KI auswirkt. Das EPSKI ist kein statisches Gebilde, sondern muss regelmäßig überprüft werden, um neuen Problemen und Anforderungen gerecht werden zu können.

Die mit steigenden Sicherheitsinvestitionen u. U. verbundenen negativen Auswirkungen auf die Wettbewerbsfähigkeit eines bestimmten Wirtschaftszweigs sollten durch das EPSKI so weit wie möglich minimiert werden. Die für langfristige Investitionen notwendige Marktstabilität darf ebenso wenig außer Acht gelassen werden wie der Einfluss, den die Sicherheit auf die Aktienmärkte und die makroökonomische Entwicklung ausübt.

#### **Frage**

Ist dies ein für das EPSKI angemessener Zweck? Wenn nein, welchem Zweck sollte das EPSKI dienen?

#### **3.2. Wovon das EPSKI schützen sollte**

Während die Folgenbewältigung bei den meisten Störfällen gleich oder ähnlich ist, können Schutzmaßnahmen je nach Art der Bedrohung unterschiedlich beschaffen sein. Eine Bedrohung, durch die die Fähigkeit, für vitale Bedürfnisse und die Sicherheit der Bevölkerung zu sorgen, die Ordnung aufrechtzuerhalten, eine minimale öffentliche Grundversorgung oder eine funktionsfähige Wirtschaft sicherzustellen, deutlich eingeschränkt wird, kann u. a. ein vorsätzlicher Angriff oder eine Naturkatastrophe sein. Für die Ausgestaltung des EPSKI bieten sich folgende Optionen an:

a) **Ein umfassender Schutz vor Gefahren aller Art** – Berücksichtigt würden sowohl vorsätzliche Angriffe als auch Naturkatastrophen. Damit wäre eine maximale Ausschöpfung der Synergien zwischen Schutzmaßnahmen gewährleistet, ohne dabei allerdings besonders auf den Terrorismus abzustellen;

b) **ein umfassender Schutz vor Gefahren aller Art mit Schwerpunkt Terrorismus** – Dies wäre ein flexiblerer Ansatz, der alle Gefahrentypen berücksichtigt, aber besonders auf den Terrorismus ausgerichtet ist: Stellt sich heraus, dass das Schutzniveau in einem bestimmten Wirtschaftszweig angemessen ist, konzentrieren sich die Akteure auf die Gefahren, vor denen sie nach wie vor unzureichend geschützt sind;

c) **Schutz vor Terrorismus** – Bei einer auf den Terrorismus ausgerichteten Schutzstrategie würden Bedrohungen allgemeinerer Art nicht eigens berücksichtigt.

### Fragen

Welche Strategie sollte im EPSKI verfolgt werden? Warum?

## 4. WESENTLICHE GRUNDSÄTZE

Die Konzeption des EPSKI sollte sich im Wesentlichen an folgenden Grundsätzen orientieren:

- **Subsidiarität** – Subsidiarität steht im Mittelpunkt des EPSKI, denn der Schutz kritischer Infrastrukturen ist zuallererst eine nationale Aufgabe. Hauptverantwortung für den Schutz kritischer Infrastrukturen tragen die Mitgliedstaaten und Eigentümer/Betreiber, die auf einer gemeinsamen Grundlage handeln. Die Kommission konzentriert sich ihrerseits auf die grenzübergreifenden Aspekte. An der Verantwortung der Eigentümer/Betreiber, selbst den Schutz ihrer Anlagen zu planen und darüber zu entscheiden, sollte sich nichts ändern.
- **Komplementarität** – Mit dem EPSKI werden bereits bestehende Maßnahmen ergänzt. Sind auf Gemeinschaftsebene bereits Mechanismen vorhanden, sollten sie weiter genutzt werden, um so zur Umsetzung des EPSKI beizutragen.
- **Vertraulichkeit** – Informationen über den Schutz kritischer Infrastrukturen werden auf der Basis von Vertrauen und Vertraulichkeit ausgetauscht. Dies ist erforderlich, da bestimmte Informationen über eine kritische Infrastruktur dazu benutzt werden können, ihren Betrieb zu stören oder andere untragbare Konsequenzen herbeizuführen. Den Schutz kritischer Infrastrukturen betreffende Informationen werden sowohl auf EU- als auch auf nationaler Ebene als Verschlussache behandelt, zu der nur die Personen Zugang erhalten, die Kenntnis von der Sache nehmen müssen.
- **Mitwirkung der Stakeholder** – Alle Stakeholder einschließlich der Mitgliedstaaten, der Kommission, der Wirtschaftsverbände, Normungsgremien, Eigentümer/Betreiber von Infrastruktureinrichtungen und Nutzer („Nutzer“ sind Organisationen, die eine Infrastruktur gewerblich und zur Erbringung von Dienstleistungen betreiben und nutzen) haben einen Beitrag zum Schutz kritischer Infrastrukturen zu leisten. Alle Stakeholder sollten entsprechend ihren jeweiligen Aufgaben und Zuständigkeitsbereichen zusammenarbeiten und an der Entwicklung und Umsetzung des EPSKI mitwirken. Die Federführung und Koordination bei der Ausarbeitung und Umsetzung eines landesweit kohärenten Konzepts für den Schutz kritischer Infrastrukturen obliegt den Behörden der Mitgliedstaaten innerhalb ihres Zuständigkeitsbereichs. Die Eigentümer/Betreiber und Nutzer der Infrastruktureinrichtungen arbeiten sowohl auf einzelstaatlicher als auch auf EU-Ebene aktiv mit. Normungsorganisationen könnten gegebenenfalls einheitliche Normen für die Bereiche setzen, für die es noch keine internationalen oder sektorspezifischen Normen gibt.

- **Verhältnismäßigkeit** – Die Schutzstrategien und -maßnahmen müssen im Verhältnis zu dem jeweiligen Risiko stehen, da nicht alle Infrastruktureinrichtungen vor allen Risiken geschützt werden können (Stromnetze zum Beispiel sind zu weitläufig, um umzäunt oder bewacht werden zu können). Durch die Anwendung geeigneter Risikomanagement-Techniken kann die Aufmerksamkeit auf die am stärksten gefährdeten Bereiche konzentriert werden, wobei die Bedrohung, die relative Kritikalität, das Kosten-Nutzen-Verhältnis, der Grad des Sicherheitsschutzes und die Wirksamkeit der verfügbaren Risikominimierungsstrategien berücksichtigt werden.

**Frage**

Sind die vorstehenden wesentlichen Grundsätze annehmbar? Sind einige überflüssig? Gibt es weitere Grundsätze, die berücksichtigt werden sollten?

Teilen Sie die Auffassung, dass die Schutzmaßnahmen im Verhältnis zum jeweiligen Risiko stehen müssen, da nicht alle Infrastruktureinrichtungen vor allen Risiken geschützt werden können?

**5. EIN GEMEINSAMER EPSKI-RAHMEN**

Die Beschädigung oder der Ausfall einer Infrastruktureinrichtung in einem Mitgliedstaat kann sich negativ auf andere Mitgliedstaaten und die europäische Wirtschaft insgesamt auswirken. Dies wird umso wahrscheinlicher, als mit den neuen Technologien (z. B. Internet) und der Liberalisierung der Märkte (z. B. der Gas- und Strommärkte) zahlreiche Infrastrukturen in größere Netze eingebunden werden. In diesem Fall ist der Schutz nicht stärker als das schwächste Glied in der Kette der Schutzmaßnahmen. Ein einheitliches Schutzniveau ist daher erforderlich.

Ein effizienter Schutz setzt Kommunikation, Koordination und Kooperation sowohl auf nationaler als auch (gegebenenfalls) auf EU-Ebene und auf internationaler Ebene unter Einbeziehung aller Beteiligten voraus. Für den Schutz kritischer Infrastrukturen in Europa könnte auf EU-Ebene ein gemeinsames Rahmenprogramm aufgelegt werden, das in jedem Mitgliedstaat für angemessene und gleiche Sicherheitsstufen sorgt und sicherstellt, dass der Wettbewerb im Binnenmarkt nicht verfälscht wird. Mit der Bereitstellung eines gemeinsamen Rahmens für den Schutz kritischer Infrastrukturen erleichtert die Kommission die Definition, den Austausch und die Verbreitung bewährter Praktiken und unterstützt so die Arbeit der Mitgliedstaaten. Zu überlegen ist, was dieser allgemeine Rahmen genau umfassen sollte.

Ein gemeinsames EPSKI sollte horizontale Maßnahmen enthalten, die die Zuständigkeit und Verantwortung aller Beteiligten für den Schutz kritischer Infrastrukturen definieren und die Basis für ein sektorspezifisches Vorgehen abgeben. Der gemeinsame Rahmen soll auf Gemeinschaftsebene und in den Mitgliedstaaten bereits bestehende sektorbezogene Maßnahmen ergänzen, um so ein Höchstmaß an Sicherheit für kritische Infrastrukturen in der EU zu gewährleisten. Die Verständigung auf einen gemeinsamen Katalog einschlägiger Definitionen und Sektoren sollte Vorrang haben.

Da die Wirtschaftszweige, die kritische Infrastrukturen aufweisen, sehr unterschiedlich sind, ist es schwierig, in einer sektorübergreifenden Regelung präzise Kriterien für die Ermittlung dieser Infrastrukturen und ihren Schutz vorzuschreiben. Dies sollte für jeden Sektor getrennt erfolgen. Dessen ungeachtet bedarf es einer Verständigung über bestimmte allgemeine Fragen.

Kritische Infrastrukturen sollten in der EU mit Hilfe eines gemeinsamen EPSKI (Festlegung gemeinsamer Ziele, Methoden z. B. für Vergleiche, Interdependenzen) sowie dem Austausch bewährter Praktiken und mit Konformitätskontrollen geschützt werden. Ein solcher gemeinsamer Rahmen umfasst u. a.:

- gemeinsame Grundsätze für den Schutz kritischer Infrastrukturen
- gemeinsam festgelegte Verhaltensweisen/Standards
- gemeinsame Definitionen, auf deren Grundlage sektorspezifische Definitionen festgelegt werden können (Vorschlag siehe Anhang I)
- eine gemeinsame Liste der einschlägigen Sektoren (Vorschlag siehe Anhang II)
- die Festlegung prioritärer Bereiche für den Schutz kritischer Infrastrukturen
- eine Beschreibung der Verantwortungsbereiche aller Beteiligten
- vereinbarte Benchmarks
- Methoden für den Vergleich von Infrastrukturen in verschiedenen Wirtschaftszweigen und die Festlegung von Prioritäten.

Ein solcher gemeinsamer Rahmen würde auch potenzielle Störwirkungen im Binnenmarkt minimieren.

Das EPSKI könnte freiwillig oder verbindlich sein oder beides je nach Regelungsgegenstand. Das Schutzprogramm könnte bestehende sektorspezifische oder sektorübergreifende Maßnahmen auf Gemeinschaftsebene und in den Mitgliedstaaten ergänzen. Aber nur eine rechtliche Rahmenregelung könnte eine starke, durchsetzbare Rechtsgrundlage für eine kohärente, einheitliche Umsetzung der Maßnahmen zum Schutz von kritischen EU-Infrastrukturen abgeben und die Verantwortungsbereiche der Mitgliedstaaten und der Kommission klar voneinander abgrenzen. Nicht verbindliche, freiwillige Maßnahmen wären zwar flexibel, würden aber keine Klarheit darüber schaffen, wer wofür zuständig ist.

Je nachdem, wie die Abwägung im Einzelfall ausfällt, kann die Kommission unter sorgfältiger Beachtung des Verhältnismäßigkeitsprinzips auch Legislativvorschläge in ihren Vorschlag für ein europäisches Schutzprogramm aufnehmen. Für konkrete Vorschläge wird gegebenenfalls eine Folgenabschätzung erstellt.

**Fragen**

Wäre ein gemeinsamer Rahmen zur Stärkung des Schutzes kritischer Infrastrukturen geeignet?

Falls ein rechtlicher Rahmen erforderlich ist, was sollte er enthalten?

Sind Sie auch der Meinung, dass die Kriterien zur Ermittlung der verschiedenen Typen kritischer EU-Infrastrukturen (EUKI) und der hierfür als erforderlich angesehenen Schutzmaßnahmen für jeden Sektor getrennt festgelegt werden sollten?

Wäre ein gemeinsamer Rahmen für die Klärung der Verantwortungsbereiche der einzelnen Beteiligten hilfreich? Inwieweit sollte ein solcher gemeinsamer Rahmen verbindlich bzw. fakultativ sein?

Worauf sollte sich der gemeinsame Rahmen erstrecken? Sind Sie mit der Liste der Begriffsbestimmungen in Anhang I einverstanden, auf deren Grundlage (gegebenenfalls) sektorspezifische Definitionen festgelegt werden können? Sind Sie mit der Liste der einschlägigen Sektoren in Anhang II einverstanden?

## **6. KRITISCHE EU-INFRASTRUKTUREN (EUKI)**

### **6.1. Definition kritischer EU-Infrastrukturen**

Maßgebend für die Definition einer kritischen EU-Infrastruktur ist ihr Potenzial, bei einem Störfall über das Gebiet des Mitgliedstaats, in dem sie sich befindet, hinaus gravierende Wirkungen zu entfalten. Zu berücksichtigen ist auch, dass sich bilaterale Kooperationsvereinbarungen zwischen den Mitgliedstaaten im Umgang mit kritischen Infrastrukturen an der Grenze zwischen zwei Mitgliedstaaten bewährt haben und als Ergänzung des EPSKI anzusehen sind.

Als kritische EU-Infrastrukturen können gelten natürliche Ressourcen, Dienste, informationstechnologische Einrichtungen, Netze und sonstige Infrastruktureinrichtungen, deren Störung oder Vernichtung gravierende Auswirkungen hätte auf die Gesundheit, die Sicherheit oder das wirtschaftliche oder soziale Wohlergehen in entweder

- a) zwei oder mehr Mitgliedstaaten – **dies würde (gegebenenfalls) bestimmte bilaterale kritische Infrastrukturen einschließen** oder
- b) drei oder mehr Mitgliedstaaten – **dies würde alle bilateralen kritischen Infrastrukturen ausschließen.**

Bei Prüfung dieser Optionen ist Folgendes zu beachten:

- Die Einstufung einer Infrastruktur als EUKI bedeutet nicht, dass deshalb zusätzliche Schutzvorkehrungen erforderlich wären. Die bestehenden Schutzvorkehrungen, zu denen auch bilaterale Vereinbarungen zwischen Mitgliedstaaten zählen können, können völlig angemessen sein und würden durch die Einstufung als EUKI nicht berührt.
- Option a) hätte u. U. zur Folge, dass mehr Infrastrukturen als EUKI eingestuft würden.



- Option b) könnte dazu führen, dass die Gemeinschaft bei Infrastruktureinrichtungen, die nur für zwei Mitgliedstaaten von Belang sind, nicht tätig würde, auch wenn einer der beiden Mitgliedstaaten das Schutzniveau als unzureichend ansieht und der andere Mitgliedstaat sich weigert, entsprechende Maßnahmen zu ergreifen. Option b) könnte auch eine Vielzahl bilateraler Vereinbarungen oder das Fehlen von Vereinbarungen zur Folge haben. Die häufig europaweit agierenden Wirtschaftszweige sähen sich dann einem Flickwerk unterschiedlicher Vereinbarungen gegenüber, die zusätzliche Kosten verursachen können.

Kritische Infrastrukturen außerhalb der EU, die mit einem Mitgliedstaat verbunden sind oder die sich unmittelbar in einem Mitgliedstaat auswirken können, sollten ebenfalls berücksichtigt werden.

### **Fragen**

Sollten Infrastrukturen als EUKI eingestuft werden, wenn sie ein Gefahrenpotenzial für zwei oder mehr oder drei oder mehr Mitgliedstaaten darstellen? Warum?

## **6.2. Interdependenzen**

Bei der Ermittlung aller kritischen EU-Infrastrukturen sollten auch Interdependenzen berücksichtigt werden. Einschlägige Studien könnten dazu beitragen, die potenzielle Auswirkung einer Bedrohung bestimmter Infrastrukturen abzuschätzen und festzustellen, welche Mitgliedstaaten bei einem größeren Störfall betroffen wären.

In vollem Umfang berücksichtigt würden Interdependenzen innerhalb und zwischen Unternehmen, Wirtschaftszweigen, geografischen Zuständigkeitsbereichen und mitgliedstaatlichen Behörden, insbesondere wenn sie auf Informations- und Kommunikationstechnologien (IKT) beruhen. Die Kommission, die Mitgliedstaaten und die Eigentümer/Betreiber kritischer Infrastrukturen sollten diese Interdependenzen gemeinsam analysieren und nach Möglichkeit geeignete Strategien zur Risikominimierung verfolgen.

### **Fragen**

Wie kann Interdependenzen Rechnung getragen werden?

Sind Ihnen geeignete Methoden zur Analyse von Interdependenzen bekannt?

Auf welcher Ebene sollten Interdependenzen ermittelt werden – auf EU- und/oder mitgliedstaatlicher Ebene?

## **6.3. Vorgehen in Bezug auf EUKI**

Die Kommission schlägt folgende Vorgehensweise vor:

- (1) Die Kommission legt gemeinsam mit den Mitgliedstaaten die Kriterien für die Definition sektorspezifischer kritischer EU-Infrastrukturen fest.
- (2) Anschließend werden die EUKI von den Mitgliedstaaten und der Kommission in den einzelnen Sektoren anhand dieser Kriterien ermittelt und überprüft. Ob eine bestimmte

kritische Infrastruktur als EUKI einzustufen ist, wird aufgrund des grenzübergreifenden Charakters solcher Infrastrukturen auf EU-Ebene<sup>1</sup> entschieden.

- (3) Die Mitgliedstaaten und die Kommission analysieren die in den einzelnen Sektoren bestehenden Sicherheitslücken bei EUKI.
- (4) Die Mitgliedstaaten und die Kommission legen einvernehmlich unter Berücksichtigung bestehender Interdependenzen die Sektoren/Infrastrukturen fest, die prioritär zu behandeln sind.
- (5) Die Kommission und maßgebliche Stakeholder in den Mitgliedstaaten schlagen gegebenenfalls für jeden Sektor Mindestschutzvorkehrungen vor, zu denen auch Normen zählen können.
- (6) Die Umsetzung dieser Maßnahmen erfolgt nach Annahme der Vorschläge durch den Rat.
- (7) Die Mitgliedstaaten und die Kommission sorgen für eine regelmäßige Kontrolle. Bei Bedarf werden die Maßnahmen und Kriterien angepasst.

### Fragen

Ist die Vorgehensweise in Bezug auf EUKI annehmbar?

Wie sollten die Kommission und die Mitgliedstaaten Ihrer Ansicht nach bei der gemeinsamen Einstufung der EUKI vorgehen, wenn man bedenkt, dass die Mitgliedstaaten über das nötige Sachwissen verfügen, während die Kommission den Überblick darüber hat, was im europäischen Interesse liegt? Sollte dies in Form einer rechtsverbindlichen Entscheidung erfolgen?

Bedarf es eines Schlichtungsverfahrens, wenn ein Mitgliedstaat es ablehnt, eine Infrastruktur in seinem Hoheitsgebiet als EUKI einzustufen?

Ist eine Überprüfung notwendig? Wer sollte für die Überprüfung zuständig sein?

Sollten Mitgliedstaaten die Möglichkeit haben, Infrastrukturen in anderen Mitgliedstaaten oder Drittstaaten als für sie kritisch einzustufen? Wie ist zu verfahren, wenn ein Mitgliedstaat, ein Drittland oder ein Wirtschaftszweig eine Einrichtung in einem Mitgliedstaat als sicherheitskritisch ansieht?

Wie ist zu verfahren, wenn dieser Mitgliedstaat die betreffende Einrichtung nicht als EUKI einstuft? Ist ein Beschwerdeverfahren erforderlich? Wenn ja, in welcher Form?

Sollte Betreibern eine Beschwerdemöglichkeit eingeräumt werden, wenn sie mit der Einstufung als EUKI oder der Nichteinstufung als EUKI nicht einverstanden sind? Wenn ja, an wen sollte sich der Betreiber wenden?

In welcher Weise sollte vorgegangen werden, um die Sektoren/Infrastrukturen zu bestimmen, die prioritär zu behandeln sind? Gibt es bereits geeignete Methoden, die europäischen Anforderungen angepasst werden könnten?

---

<sup>1</sup> Mit Ausnahme von verteidigungsrelevanten Infrastrukturen.

Wie kann die Kommission in die Analyse der Sicherheitslücken bei EUKI einbezogen werden?

## **7. NATIONALE KRITISCHE INFRASTRUKTUREN (NKI)**

### **7.1. Rolle der NKI im EPSKI**

Viele europäische Unternehmen sind in anderen Mitgliedstaaten tätig und unterliegen deshalb unterschiedlichen Auflagen in Bezug auf NKI. Im Interesse der Mitgliedstaaten und der EU insgesamt sollte jeder Mitgliedstaat seine nationalen kritischen Infrastrukturen (NKI) auf der Grundlage einer gemeinsamen Rahmenregelung schützen, damit Eigentümer/Betreiber dieser Infrastrukturen in Europa nicht einer Vielzahl unterschiedlicher Bestimmungen und Methoden mit den daraus resultierenden Zusatzkosten unterliegen. Das EPSKI kann insofern, auch wenn es in erster Linie auf kritische EU-Infrastrukturen ausgerichtet ist, nationale kritische Infrastrukturen nicht völlig außer Acht lassen. Drei Optionen sind hier zu prüfen:

- a) **Vollständige Einbeziehung der NKI in das EPSKI**
- b) **Nichtberücksichtigung der NKI im EPSKI**
- c) **Mitgliedstaaten können das EPSKI auf Wunsch auf NKI anwenden, sind aber nicht dazu verpflichtet.**

#### **Fragen**

Um kritische Infrastrukturen in der Europäischen Union effizient schützen zu können, erscheint eine Einstufung dieser Infrastrukturen als EUKI oder NKI geboten. Sind Sie auch der Meinung, dass das EPSKI zwar in erster Linie auf kritische EU-Infrastrukturen ausgerichtet sein sollte, NKI aber nicht völlig außer Acht gelassen werden können?

Welche Option ist Ihrer Meinung nach für das EPSKI am geeignetsten?

### **7.2. Nationale Programme für den Schutz kritischer Infrastrukturen**

Die Mitgliedstaaten könnten auf der Grundlage eines einheitlichen EPSKI nationale Schutzprogramme für ihre nationalen kritischen Infrastrukturen ausarbeiten. Dabei könnten sie strengere Maßstäbe als im EPSKI anlegen.

#### **Frage**

Halten Sie es für wünschenswert, dass jeder Mitgliedstaat auf der Grundlage des EPSKI ein nationales Programm für den Schutz kritischer Infrastrukturen erstellt?

### **7.3. Eine einzige nationale Aufsichtsbehörde**

In Anbetracht der Effizienz- und Kohärenzanforderungen liegt es nahe, dass jeder Mitgliedstaat eine einzige Aufsichtsbehörde benennt, die für die Umsetzung des EPSKI zuständig ist. Zwei Optionen kommen in Betracht:

- a) eine einzige Aufsichtsbehörde für den Schutz kritischer Infrastrukturen
- b) eine nationale Kontaktstelle ohne Befugnisse; es bleibt den Mitgliedstaaten überlassen, wie sie sich organisieren.

Eine solche Behörde könnte die Umsetzung des EPSKI auf nationaler Ebene koordinieren und kontrollieren, und sie könnte in Angelegenheiten, die den Schutz kritischer Infrastrukturen betreffen, der Kommission, den anderen Mitgliedstaaten und den Eigentümern/Betreibern kritischer Infrastrukturen als Kontaktstelle dienen. Sie könnte die nationalen Vertreter in die Expertengruppen entsenden, die sich mit dem Schutz kritischer Infrastrukturen befassen, und darüber hinaus die Verbindung zum Warn- und Informationsnetz für kritische Infrastrukturen (WINKI) sicherstellen. Eine solche nationale Koordinierungsbehörde für den Schutz kritischer Infrastrukturen (NKBSKI) könnte ungeachtet anderer mitgliedstaatlicher Behörden oder Stellen, die bereits in diesem Bereich tätig sind, die Koordinierung des Schutzes kritischer Infrastrukturen auf einzelstaatlicher Ebene übernehmen.

Würden die Eigentümer/Betreiber von Infrastruktureinrichtungen verpflichtet, der NKBSKI alle Aktivitäten anzuzeigen, die für den Schutz kritischer Infrastrukturen relevant sind, könnten auf diese Weise nach und nach alle nationalen kritischen Infrastrukturen erfasst werden.

Der NKBSKI könnte die Aufgabe zufallen, Infrastrukturen in ihrem Zuständigkeitsbereich rechtsverbindlich als NKI einzustufen. Über diese Information würde allein der betreffende Mitgliedstaat verfügen.

Der Aufgabenbereich dieser Behörde ließe sich wie folgt umreißen:

- a) Koordinierung, Beaufsichtigung und Kontrolle der Umsetzung des EPSKI auf mitgliedstaatlicher Ebene
- b) Kontaktstelle für Angelegenheiten, die den Schutz kritischer Infrastrukturen betreffen, gegenüber
  - i) der Kommission
  - ii. den übrigen Mitgliedstaaten
  - iii) den Eigentümern/Betreibern kritischer Infrastrukturen
- c) Mitwirkung an der Einstufung kritischer EU-Infrastrukturen (EUKI)
- d) Rechtsverbindliche Festlegung einer Infrastruktur in ihrem Zuständigkeitsbereich als NKI
- e) Beschwerdeinstanz für Eigentümer/Betreiber, die mit der Einstufung ihrer Infrastruktur als „kritisch“ nicht einverstanden sind
- f) Teilnahme an der Ausarbeitung des Programms für den Schutz nationaler kritischer Infrastrukturen sowie der sektorspezifischen Schutzprogramme
- g) Aufzeigen von Interdependenzen zwischen KI-Sektoren
- h) Beitrag zu sektorspezifischen Schutzstrategien durch die Beteiligung in Expertengruppen. Vertreter der Eigentümer/Betreiber könnten ebenfalls eingeladen werden und zur Diskussion beitragen. Es könnten regelmäßig Sitzungen abgehalten werden
- i) Beaufsichtigung der Erstellung von Notfallplänen für kritische Infrastrukturen.

**Fragen**

Teilen Sie die Auffassung, dass die Mitgliedstaaten allein für die Einstufung und Verwaltung von NKI auf der Grundlage eines gemeinsamen EPSKI zuständig sein sollen?

Halten Sie es für wünschenswert, in jedem Mitgliedstaat eine Koordinierungsbehörde für den Schutz kritischer Infrastrukturen zu benennen, die für die Koordinierung aller Maßnahmen zum Schutz kritischer Infrastrukturen zuständig ist, ohne jedoch in bestehende sektorbezogene Zuständigkeitsbereiche (Zivilluftfahrtbehörden, Seveso-Richtlinie usw.) einzugreifen?

Halten Sie die vorgeschlagene Aufgabenzuweisung für eine solche Koordinierungsbehörde für angemessen? Gibt es weitere notwendige Aufgaben?

**7.4. Vorgehen in Bezug auf NKI**

Die Kommission schlägt folgende Vorgehensweise vor:

- (1) Die Mitgliedstaaten legen auf der Grundlage des EPSKI die Kriterien für die Definition nationaler kritischer Infrastrukturen fest.
- (2) Anschließend werden die NKI von den Mitgliedstaaten in den einzelnen Sektoren anhand dieser Kriterien ermittelt und überprüft.
- (3) Die Mitgliedstaaten analysieren die in den einzelnen Sektoren bestehenden Sicherheitslücken bei NKI.
- (4) Die Mitgliedstaaten legen unter Berücksichtigung bestehender Interdependenzen und gegebenenfalls der auf EU-Ebene vereinbarten Prioritäten die Sektoren fest, die vorrangig zu behandeln sind.
- (5) Die Mitgliedstaaten vereinbaren gegebenenfalls für jeden Sektor Mindestschutzvorkehrungen.
- (6) Die Mitgliedstaaten sorgen dafür, dass die Eigentümer/Betreiber in ihrem Hoheitsgebiet die notwendigen Umsetzungsmaßnahmen ergreifen.
- (7) Die Mitgliedstaaten sorgen für eine regelmäßige Kontrolle. Bei Bedarf werden die Maßnahmen und Kriterien angepasst.

**Fragen**

Ist die Vorgehensweise in Bezug auf NKI angemessen? Sind manche Maßnahmen überflüssig? Sind weitere Maßnahmen vorzusehen?

**8. ROLLE DER EIGENTÜMER/BETREIBER UND NUTZER KRITISCHER INFRASTRUKTUREN****8.1. Aufgaben der Eigentümer/Betreiber und Nutzer kritischer Infrastrukturen**

Die Einstufung als kritische Infrastruktur bringt für die Eigentümer/Betreiber gewisse Pflichten mit sich. Für Eigentümer/Betreiber einer als NKI oder EUKI eingestuften Infrastruktur kommen folgende vier Pflichten in Betracht:

- (1) Mitteilung an die für den Schutz kritischer Infrastrukturen zuständige mitgliedstaatliche Behörde, dass die Infrastruktur als kritisch eingestuft werden könnte
- (2) **Bestellung eines Sicherheitsbeauftragten, der den Eigentümer/Betreiber gegenüber der zuständigen mitgliedstaatlichen Behörde vertritt.** Der Sicherheitsbeauftragte wird in die Ausarbeitung von Sicherheits- und Notfallplänen einbezogen. Der Sicherheitsbeauftragte ist der Hauptansprechpartner der betreffenden sektorspezifischen Stellen für den Schutz kritischer Infrastrukturen in den Mitgliedstaaten sowie gegebenenfalls der Strafverfolgungsbehörden
- (3) **Ausarbeitung, Umsetzung und Aktualisierung von Sicherheitsplänen für eine bestimmte Infrastruktur:** Ein entsprechendes Muster ist in Anhang III beigefügt
- (4) **Mitwirkung an der Ausarbeitung von Notfallplänen** für kritische Infrastrukturen zusammen mit den zuständigen Zivilschutz- und Strafverfolgungsbehörden der Mitgliedstaaten (nach Aufforderung).

Der Sicherheitsplan könnte der für den betreffenden Sektor zuständigen Behörde für den Schutz kritischer Infrastrukturen, die der Aufsicht der nationalen Koordinierungsbehörde untersteht, zur Genehmigung vorgelegt werden, unabhängig davon, ob es sich um eine NKI oder eine EUKI handelt. Auf diese Weise wäre die Kohärenz der von den Eigentümern/Betreibern und den betreffenden Sektoren allgemein getroffenen Sicherheitsvorkehrungen gewährleistet. Im Gegenzug könnten Eigentümer/Betreiber Informationen und Hilfestellung in Bezug auf sie betreffende Bedrohungen sowie bewährte Praktiken erhalten und gegebenenfalls auch Unterstützung der Koordinierungsbehörde oder der Kommission bei der Beurteilung von Interdependenzen und Schwachstellen.

Jeder Mitgliedstaat könnte den Eigentümern/Betreibern von NKI und EUKI eine Frist für die Erstellung von Sicherheitsplänen setzen (bei EUKI wäre auch die Kommission einzubeziehen) und bei Fristüberschreitung Geldbußen vorsehen.

Im Sicherheitsplan wären die betreffenden kritischen Infrastruktureinrichtungen des Eigentümers/Betreibers genau darzustellen und Sicherheitsvorkehrungen zu ihrem Schutz festzulegen. Ferner wären die Methoden und Verfahren zu beschreiben, die einzuhalten wären, um die Vereinbarkeit mit dem EPSKI, den nationalen sowie etwaigen sektorspezifischen Schutzprogrammen zu gewährleisten. Mit dem Sicherheitsplan lässt sich der Schutz kritischer Infrastrukturen von der Basis aus organisieren, was der Privatwirtschaft mehr Gestaltungsmöglichkeiten lässt (für sie aber auch mehr Verantwortung bedeutet).

Bei bestimmten Infrastrukturen wie Strom- oder IT-Netzen wäre es (sowohl aus praktischer als auch finanzieller Sicht) unrealistisch, von den Eigentümern/Betreibern zu erwarten, dass sie für alle Teile ihrer Infrastruktur ein gleiches Sicherheitsniveau gewährleisten. In diesen Fällen könnten die Eigentümer/Betreiber gemeinsam mit den zuständigen Behörden die kritischen Punkte eines physischen oder IT-Netzes bestimmen, an denen strengere Sicherheitsvorkehrungen ansetzen könnten.

Im Sicherheitsplan könnten zwei Kategorien von Sicherheitsvorkehrungen ausgewiesen werden:

- **Auf Dauer angelegte Sicherheitsvorkehrungen**, die unerlässliche Sicherheitsinvestitionen und Vorkehrungen umfassen, die von den Eigentümern/Betreibern nicht kurzfristig bereitgestellt werden können. Die Eigentümer/Betreiber würden eine ständige Alarmbereitschaft unterhalten, die den regelmäßigen Betrieb der Infrastruktur in wirtschaftlicher, administrativer und sozialer Hinsicht nicht stört.
- **Abgestufte Sicherheitsvorkehrungen**, die entsprechend der jeweiligen Gefahrenstufe aktiviert werden könnten. Im Sicherheitsplan wären somit mehrere Sicherheitsszenarios vorgesehen, die den möglichen Gefahrenstufen in dem Mitgliedstaat angepasst sind, in dem sich die Infrastruktur befindet.

Für den Fall, dass ein KI-Eigentümer/Betreiber seinen Pflichten (u. a. Aufstellung eines Sicherheitsplans, Mitwirkung an der Aufstellung von Notfallplänen, Benennung eines Sicherheitsbeauftragten) nicht nachkommt, könnte die Verhängung einer Geldstrafe vorgesehen werden.

### Fragen

Sind die den Eigentümern/Betreibern kritischer Infrastrukturen auferlegten potenziellen Pflichten im Hinblick auf die dadurch erreichte größere Sicherheit kritischer Infrastrukturen annehmbar? Welche Kosten wären damit voraussichtlich verbunden?

Sollte Eigentümern/Betreibern aufgegeben werden, den Umstand zu melden, dass es sich bei ihrer Infrastruktur um eine kritische Infrastruktur handeln könnte? Halten Sie die Idee eines Sicherheitsplans für nützlich? Warum?

Sind die vorgeschlagenen Pflichten in Bezug auf die damit verbundenen Kosten verhältnismäßig?

Welche Rechte könnten den KI-Eigentümern/Betreibern von der Kommission und den Mitgliedstaaten eingeräumt werden?

## **8.2. Dialog mit den Eigentümern/Betreibern und Nutzern kritischer Infrastrukturen**

Die Eigentümer/Betreiber könnten im Rahmen des EPSKI in Partnerschaften eingebunden werden. Der Erfolg eines Schutzprogramms hängt davon ab, wie intensiv und in welchem Umfang die Eigentümer/Betreiber an dem Programm mitarbeiten. Auf Ebene der Mitgliedstaaten könnten die KI-Eigentümer/Betreiber durch regelmäßige Kontakte mit der Koordinierungsbehörde eng an den Entwicklungen im Bereich des Schutzes kritischer Infrastrukturen beteiligt werden.

Auf EU-Ebene könnten Foren eingerichtet werden, um den Meinungs austausch bei allgemeinen und sektorspezifischen KI-Problemen zu erleichtern. Eine einheitliche Strategie zur Einbeziehung der Privatwirtschaft in die IK-Problematik, die alle Beteiligten aus dem öffentlichen und privaten Bereich zusammenführt, würde den Mitgliedstaaten, der Kommission und der Wirtschaft eine wichtige Plattform bieten, um sich über IK-Fragen jedweder Art auszutauschen. Die KI-Eigentümer/Betreiber und Nutzer könnten in die Ausarbeitung gemeinsamer Leitlinien und bewährter Praktiken sowie gegebenenfalls in den Informationsaustausch einbezogen werden. Ein solcher Dialog würde künftige Anpassungen des EPSKI erleichtern.

Sollte sich dies als sinnvoll erweisen, könnte die Kommission auch Zusammenschlüsse in Industrie und Wirtschaft fördern, die auf den Schutz kritischer EU-Infrastrukturen gerichtet sind. Die beiden Ziele, die es letztlich zu erreichen gilt, sind, dafür zu sorgen, dass die europäische Wirtschaft wettbewerbsfähig bleibt und die EU-Bürger in größerer Sicherheit leben können.

### **Fragen**

In welcher Form sollte der Dialog mit den KI-Eigentümern/Betreibern und Nutzern erfolgen?

Wer sollte die Eigentümer/Betreiber und Nutzer im öffentlich-privaten Dialog vertreten?

## **9. MASSNAHMEN ZUR UNTERSTÜTZUNG DES EPSKI**

### **9.1. Das Warn- und Informationsnetz für kritische Infrastrukturen (WINKI)**

Die Kommission hat eine Reihe von Schnellwarnsystemen eingerichtet, die im Katastrophenfall – auch terroristischen Ursprungs - eine konkrete, koordinierte und effiziente Reaktion ermöglichen. Am 20. Oktober 2004 kündigte die Kommission die Einrichtung eines zentralen Netzes innerhalb der Kommission an (ARGUS), das einen raschen Informationsfluss zwischen allen Schnellwarnsystemen und zuständigen Dienststellen der Kommission sicherstellen soll.

WINKI könnte die Entwicklung geeigneter Schutzmaßnahmen durch den sicheren Austausch bewährter Praktiken fördern und gleichzeitig Informationen über eine unmittelbare Bedrohung oder Alarmmeldungen weiterleiten. Auf diese Weise würde dafür gesorgt, dass die richtigen Leute die richtigen Informationen rechtzeitig erhalten.



Drei Optionen kommen in Betracht:

- (1) WINKI als Forum für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes kritischer Infrastrukturen zur Unterstützung von KI-Eigentümern/Betreibern: Das Forum könnte als Expertennetz und elektronische Plattform für den Austausch relevanter Informationen in einer sicheren Umgebung funktionieren. Bei der Zusammenstellung und Verbreitung dieser Informationen würde die Kommission eine wichtige Rolle spielen. Bei dieser Option wäre es nicht möglich, Warnungen vor einer unmittelbaren Bedrohung zu verbreiten. Eine breitere Ausrichtung des WINKI wäre allerdings in der Zukunft denkbar.
- (2) **WINKI als Schnellwarnsystem zwischen den Mitgliedstaaten und der Kommission:** Mit dieser Option ließe sich die Sicherheit kritischer Infrastrukturen durch die Übermittlung von Warnungen bei unmittelbarer Bedrohung oder Alarmmeldungen erhöhen. Hier ginge es darum, die rasche Übermittlung von Informationen über eine potenzielle Bedrohung an KI-Eigentümer/Betreiber zu erleichtern. Der Austausch von über einen längeren Zeitraum gesammelten nachrichtendienstlichen Erkenntnissen über das Schnellwarnsystem ist nicht vorgesehen. Der Informationsaustausch würde sich auf die rasche Übermittlung von Informationen über eine unmittelbare Bedrohung für eine bestimmte Infrastruktur beschränken.
- (3) **WINKI als Mehrebenen-Kommunikations-/Warnsystem mit zwei verschiedenen Funktionen:** a) Schnellwarnsystem zwischen den Mitgliedstaaten und der Kommission und b) Forum für den Austausch bewährter Praktiken und Ideen im Bereich des Schutzes kritischer Infrastrukturen zur Unterstützung von KI-Eigentümern/Betreibern in Gestalt eines Expertennetzes und einer elektronischen Plattform für den Datenaustausch.

WINKI würde unabhängig davon, welche Option gewählt würde, bestehende Netze ergänzen und doppelten Aufwand vermeiden. Langfristig könnten alle KI-Eigentümer/Betreiber in den Mitgliedstaaten z. B. über die zuständige Koordinierungsbehörde mit WINKI verbunden werden. Alarmmeldungen und bewährte Praktiken könnten über das Netz vermittelt werden, das als einziges direkt mit der Kommission und damit mit allen anderen Mitgliedstaaten verbunden wäre. Die Mitgliedstaaten könnten ihre bestehenden Informationssysteme für den Ausbau eines nationalen WINKI nutzen, das die Behörden mit bestimmten KI-Eigentümern/Betreibern verbindet. Und noch wichtiger, die mitgliedstaatlichen Koordinierungsbehörden und die IK-Eigentümer/Betreiber könnten diese nationalen Netze als duales Kommunikationssystem nutzen.

Welches Spektrum von WINKI abgedeckt werden soll und welche technischen Spezifikationen für die Schnittstelle zu den Mitgliedstaaten erforderlich sind, wird in einer Studie untersucht werden.

#### Fragen

Wie sollte das WINKI beschaffen sein, um die Ziele des EPSKI zu fördern?

Sollten KI-Eigentümer/Betreiber dem WINKI angeschlossen sein?

## 9.2. Einheitliche Methodik

In den Mitgliedstaaten gibt es unterschiedliche Alarmstufen, die unterschiedlichen Situationen entsprechen. Zurzeit gibt es keine Möglichkeit festzustellen, ob „Alarmstufe 1“ in einem Mitgliedstaat der „Alarmstufe 1“ in einem anderen Mitgliedstaat entspricht. Für ein in mehreren Mitgliedstaaten tätiges Unternehmen kann es deshalb schwierig sein, die Ausgaben für Sicherheitsvorkehrungen entsprechend zu gewichten. Eine Harmonisierung oder Vereinheitlichung der verschiedenen Alarmstufen könnte sich als nützlich erweisen.

Jedem Gefährdungsgrad könnte eine Bereitschaftsstufe entsprechen, auf der gemeinsame Sicherheitsvorkehrungen allgemein und gegebenenfalls abgestufte Sicherheitsvorkehrungen ausgelöst werden können. Mitgliedstaaten, die im Fall einer spezifischen Bedrohung eine bestimmte Maßnahme ablehnen, könnten stattdessen alternative Sicherheitsmaßnahmen ergreifen.

Zu erwägen wäre eine einheitliche Methode zur Identifizierung und Einstufung von Gefahren, Risiken, Schwachstellen und Reaktionsmöglichkeiten sowie zur Feststellung, ob die Bedrohung schwer wiegend genug ist, um eine Störung der Infrastruktur als möglich oder wahrscheinlich einzustufen. Hierzu würde eine Risikoeinstufung und Hierarchisierung gehören, bei der Risiken im Hinblick auf die Wahrscheinlichkeit ihres Eintretens, ihre Wirkungen und ihr Verhältnis zu anderen Risikobereichen oder –prozessen definiert werden könnten.

### Fragen

Inwieweit wäre eine Harmonisierung oder Vereinheitlichung der unterschiedlichen Alarmstufen wünschenswert und praktikabel?

Sollte eine einheitliche Methode zur Identifizierung und Einstufung von Gefahren, Risiken, Schwachstellen und Reaktionsmöglichkeiten sowie zur Feststellung, ob die Bedrohung schwer wiegend genug ist, um eine Störung der Infrastruktur als möglich oder wahrscheinlich einzustufen, eingeführt werden?

## 9.3. Finanzierung

Auf Initiative des Europäischen Parlaments (Einfügung einer neuen Haushaltslinie – Pilotprojekt „Bekämpfung des Terrorismus“ in den Haushaltsplan 2005) beschloss die Kommission am 15. September, 7 Mio. EUR für die Finanzierung eines Maßnahmenpakets bereitzustellen, das der Stärkung von Prävention, Abwehrbereitschaft und Reaktion in Bezug auf Terroranschläge in Europa dienen soll. Weitere Bestandteile dieses Pakets sind die Folgenbewältigung, der Schutz kritischer Infrastrukturen, die Terrorismusfinanzierung, Sprengstoffe und Radikalisierung. Mehr als zwei Drittel des Budgets sind für die Ausarbeitung des Europäischen Programms für den Schutz kritischer Infrastrukturen, die Entwicklung und Verbreitung von Fähigkeiten, die nötig sind, um etwa durch Terroranschläge ausgelöste Krisen grenzübergreifenden Ausmaßes bewältigen zu können, sowie für Sofortmaßnahmen bestimmt, die erforderlich sein können, um einer größeren Bedrohung oder einem Anschlag begegnen zu können. Die Finanzierung dürfte auch 2006 weiterlaufen.

Von 2007 bis 2013 wird die Finanzierung aus dem Rahmenprogramm „Sicherheit und Schutz der Freiheitsrechte“ erfolgen. Für das Einzelprogramm „Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten“ hat die Kommission 137,4 Mio. EUR vorgesehen, die für eine Bedarfsanalyse und die Entwicklung einheitlicher technischer Standards für den Schutz kritischer Infrastrukturen eingesetzt werden sollen.

Auf der Grundlage des Programms werden Gemeinschaftsmittel für Projekte nationaler, regionaler und kommunaler Behörden zum Schutz kritischer Infrastrukturen bereitgestellt. Im Mittelpunkt des Programms stehen eine Bedarfsanalyse sowie die Bereitstellung von Informationen für die Entwicklung einheitlicher Standards und Gefahren- und Risikobewertungen im Hinblick auf den Schutz kritischer Infrastrukturen oder zur Ausarbeitung spezieller Notfallpläne. Die Kommission kann vorhandenes Fachwissen einbringen oder zur Finanzierung von Studien beitragen, die sich mit den Interdependenzen in bestimmten Sektoren beschäftigen. Die Verstärkung der Sicherheit kritischer Infrastrukturen anhand der festgestellten Schutzanforderungen ist dann in erster Linie Sache der Mitgliedstaaten oder der Eigentümer/Betreiber. Diese Arbeiten können nicht aus dem Programm finanziert werden. Für die Verstärkung der Sicherheit von Infrastruktureinrichtungen in den Mitgliedstaaten entsprechend den mit Hilfe des Programms ermittelten Sicherheitsanforderungen und die Anwendung einheitlicher Sicherheitsstandards können u.a. Bankkredite in Anspruch genommen werden. Die Kommission ist bereit, sektorspezifische Studien zu unterstützen, um die finanziellen Auswirkungen solcher Sicherheitsinvestitionen in dem betreffenden Wirtschaftszweig zu ermitteln.

Die Kommission finanziert im Rahmen der „Vorbereitenden Maßnahmen zur Sicherheitsforschung“ (2004-2006) Forschungsvorhaben zur Förderung des Schutzes kritischer Infrastrukturen<sup>2</sup>. Für weitere Arbeiten im Bereich der Sicherheitsforschung sind im Kommissionsvorschlag für einen Beschluss des Europäischen Parlaments und des Rates über das siebte Rahmenprogramm der Europäischen Gemeinschaft für Forschung, technologische Entwicklung und Demonstration (KOM(2005) 119 endg.)<sup>3</sup> und im Vorschlag für eine Entscheidung des Rates über das spezifische Programm „Zusammenarbeit“ zur Durchführung des siebten Rahmenprogramm (KOM (2005) 440 endg.). Gezielte Forschungsanstrengungen, die auf praxisnahe Strategien oder Werkzeuge zur Risikominimierung gerichtet sind, sind von größter Bedeutung, um die kritischen Infrastrukturen in der EU mittel- bis langfristig sicherer zu machen. Sicherheitsforschung wird auch in diesem Bereich generell einer Prüfung unter ethischen Gesichtspunkten unterzogen, um die Vereinbarkeit mit der Grundrechtscharta zu gewährleisten. In dem Maße, wie die Interdependenzen von Infrastruktureinrichtungen zunehmen, wird sich auch der Forschungsbedarf erhöhen.

### **Fragen**

Wie schätzen Sie die Kosten und die Wirkungen ein, die sich aus der Umsetzung der in diesem Grünbuch dargelegten Maßnahmen für die Behörden und die Wirtschaft ergeben? Halten Sie diese Kosten für verhältnismäßig?

---

<sup>2</sup> Insgesamt wurden im Haushalt 2004 und 2005 Mittel in Höhe von 30 Mio. EUR ausgewiesen. Für 2006 hat die Kommission eine Mittelausstattung von 24 Mio. EUR vorgeschlagen, die derzeit von der Haushaltsbehörde geprüft wird.

<sup>3</sup> Für Forschungsarbeiten auf der Grundlage des 7. FTE-Rahmenprogramms in den Bereichen Sicherheit und Weltraum hat die Kommission eine Mittelausstattung in Höhe von 570 Mio. EUR vorgeschlagen (KOM(2005) 119 endg.).

#### 9.4. Kontrolle und Bewertung

Die Kontrolle und Bewertung der Umsetzung des EPSKI legt ein Vorgehen auf mehreren Ebenen und die Einbeziehung aller Beteiligten nahe:

- **Auf EU-Ebene könnte ein Begutachtungsverfahren eingeführt werden**, in dem die Mitgliedstaaten und die Kommission gleichberechtigt die Umsetzung des EPSKI in jedem einzelnen Mitgliedstaat gemeinsam bewerten. Die Kommission könnte jährlich über die Fortschritte bei der Umsetzung des EPSKI berichten.
- **Die Kommission könnte den Mitgliedstaaten und den anderen EU-Institutionen jedes Jahr in einer Arbeitsunterlage ihrer Dienststellen über die Fortschritte bei der Umsetzung des EPSKI berichten.**
- Auf Ebene der Mitgliedstaaten könnte die nationale Koordinierungsbehörde mit Hilfe jährlicher Berichte an den Rat und die Kommission die Umsetzung des EPSKI in ihrem Zuständigkeitsbereich überwachen und dafür sorgen, dass das/die nationale(n) Schutzprogramm(e) sowie die sektorspezifischen Schutzprogramme mit dem EPSKI vereinbar sind und alle Schutzprogramme effektiv umgesetzt werden.

Die Umsetzung des EPSKI ist ein dynamischer Prozess, der laufend angepasst und bewertet werden muss, um mit der Entwicklung Schritt zu halten, aber auch um aus Erfahrungen zu lernen. Zur Überprüfung des EPSKI und zur Formulierung neuer Vorschläge für einen besseren Schutz kritischer Infrastrukturen bieten sich u. a. die Begutachtungen der Mitgliedstaaten und der Kommission sowie die Kontrollberichte der Mitgliedstaaten an.

Informationen der Mitgliedstaaten zu bestimmten EUKI könnten der Kommission zur Erstellung einheitlicher Anfälligkeitsbewertungen und Folgenbewältigungspläne sowie einheitlicher Normen für den Schutz kritischer Infrastrukturen, zur Festlegung von Forschungsprioritäten und erforderlichenfalls zur Regelung und Harmonisierung dieses Bereichs zur Verfügung gestellt werden. Diese Informationen würden als Verschlussache eingestuft und streng vertraulich behandelt.

Die Kommission könnte bestimmte Initiativen der Mitgliedstaaten näher verfolgen. Dies gilt insbesondere in den Fällen, in denen Eigentümer/Betreiber, die nicht in der Lage sind, innerhalb einer bestimmten Frist die Grundversorgung für die Bürger wiederherzustellen, finanzielle Folgen zu gewärtigen haben.

#### Fragen

Wie sollte ein Evaluierungsmechanismus für das EPSKI aussehen? Wäre der oben beschriebene Mechanismus ausreichend?

Die Antworten sind bis 15. Januar 2006 elektronisch an folgende E-Mail-Adresse zu richten: **JLS-EPCIP@cec.eu.int**. Die Antworten werden vertraulich behandelt, es sei denn der Einsender erklärt ausdrücklich, dass er ihre Veröffentlichung wünscht. In diesem Fall werden die Antworten auf der Website der Kommission veröffentlicht.