EUROPÄISCHES PARLAMENT

2004 *2009*

Ausschuss für Wirtschaft und Währung

VORLÄUFIG
2006/0276(CNS)

21.3.2007

ENTWURF EINER STELLUNGNAHME

des Ausschusses für Wirtschaft und Währung

für den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

zu dem Vorschlag für eine Richtlinie des Rates über die Ermittlung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern
(KOM(2006)0787 – C6-0053/2007 – 2006/0276(CNS))

Verfasser der Stellungnahme: Harald Ettl

KURZE BEGRÜNDUNG

Gestützt auf das Haager Programm vom 5. November 2005, das sowohl die effiziente Bewältigung von grenzüberschreitenden Krisen als auch den verbesserten Katastrophenschutz und für die Union den Schutz kritischer Infrastrukturen (im Folgenden „SKI“) im Rahmen der Terrorismusbekämpfung umfasst und gestützt auf die Vorarbeiten der Kommission im Rahmen des Grünbuchs vom 17.11.2005 liegt ein Kommissionsvorschlag über anstehende Verbesserungsmaßnahmen des europäischen Krisenmanagements vor.

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 den wichtigen Diensten des Staates zu finden.

Der SKI in der EU ist gemeinsam mit der inneren Sicherheit eine zentrale Frage des europäischen Gesellschaftssystems. Zerstörung von kritischen Infrastrukturen kann aus psychologischer Sicht zum totalen Vertrauensverlust der Öffentlichkeit in der EU führen. Zurzeit haben die EU-Mitgliedsländer auf nationaler Ebene unterschiedlichste Niveaus für ihre Krisenmanagementeinrichtungen. Speziell aus diesem Grund zielt der vorliegende Kommissionsvorschlag darauf ab, kritische europäische Infrastrukturen nach einem gemeinsamen Verfahren zu ermitteln und als solche auszuweisen.

Voraussetzung für aktives Krisenmanagement ist das Aufrechterhalten aller notwendigen Kommunikationssysteme im Bereich IT und Telekomkommunikation. Diese Sektoren weisen eine Querschnittinfrastruktur auf und stellen gleichzeitig eine kritische Infrastruktur für andere kritische Infrastrukturen dar, wie z. B. auch für das Geld-, Finanz- und Versicherungswesen. Einem gezielten Angriff auf das Datennetz der EZB, einer Großbank oder der Frankfurter Börse muss technisch und institutionell schnell entgegengewirkt werden.

Für Großkonzerne ist grenzübergreifendes Arbeiten unumgänglich. Eine europäische Erhebung aus dem Jahr 2000 ergab, dass mehr als die Hälfte relevanter Unternehmen keine Sicherheitsaudits durchführen. Der mögliche Missbrauch von Webservern erleichtert ebenfalls radikalen Aktionismus und ist wesentlicher Bestandteil terroristischer Informationstechnik.

Infrastrukturen mit internationalem Bezug und schlechten Ausweichmöglichkeiten sind im Katastrophenfall jeder Art besonders anfällig. Durch den Stromausfall im europäischen Übertragungsnetz am 4.11.2006 wurde diese Schwachstelle drastisch verdeutlicht. Ebenfalls grenzübergreifend und zwischenstaatlich kann sich die Wasserversorgung durch Grund-, Quell- und fließendes Wasser trotz nationaler Netzausstattung zu einem Versorgungsproblem entwickeln.

Auch schienengebundener Verkehr mit grenzübergreifender Anbindung und Flughäfen mit Flugsicherungsanlagen müssen im Krisenfall auf europäische Logistik für

Gegensteuerungsmaßnahmen zurückgreifen können.

Versicherungen und Rückversicherungsgesellschaften haben sich branchenbedingt seit Jahren mit den Fragen des Risikomanagements beschäftigt. In Richtlinien, wie z. B. im Rahmen der Richtlinien des Maßnahmenpakets „ Solvabilität I“, wurden bereits Fragen des Risikomanagements für Versicherungen sowohl in der Datenfrage als auch vom materiellen Deckungsgrad mitberücksichtigt und müssen in dem Projekt „Solvabilität II“ auf die Ist-Situation der erhöhten Risiken abgestimmt werden. Für Versicherungen ist trotz der notwendigen Verhältnismäßigkeit ein zusätzliches - eventuell auch ein staatliches - Haftungsrisiko in die Überlegungen miteinzubeziehen.

Der Verfasser der Stellungnahme begrüßt und unterstützt die Intention der Kommission, eine Koordinierung der Maßnahmen zum SKI auf europäischer Ebene vorzunehmen. Allerdings muss darauf hingewiesen werden, dass eine Doppelregelung von bestehenden sektoriellen Maßnahmen verhindert werden muss, wie sie zum Beispiel in den Empfehlungen für Wertpapierabwicklungssysteme, für Standards für die Wertpapierverrechnung und -abwicklung in der EU und Standards für die Nutzung von Wertpapierabwicklungssystemen in der EU bei Kreditgeschäften des ESZB vorgesehen sind.

Aus der Kombination der bindenden und nicht bindenden Maßnahmen muss ein realistisches Kosten-Nutzen-Verhältnis für einen europäischen Mehrwert erarbeitet werden.

ÄNDERUNGSANTRÄGE

Der Ausschuss für Wirtschaft und Währung ersucht den federführenden Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, folgende Änderungsanträge in seinen Bericht zu übernehmen:

Vorschlag der Kommission	Abänderungen des Parlaments
	Änderungsantrag 1 Erwägung 5 a (neu)
	(5a) In bestimmten Sektoren gibt es bereits eine Reihe von Maßnahmen, die die Ermittlung, Ausweisung und den Schutz von kritischen Infrastrukturen regeln. Eine künftige EU-weite Regelung darf in diesen Sektoren nicht zu einer Doppelregelung - ohne zusätzlichen Sicherheitsgewinn - führen.

Änderungsantrag 2
Artikel 1

Durch diese Richtlinie wird ein Verfahren zur Ermittlung und Ausweisung kritischer europäischer Infrastrukturen sowie ein gemeinsamer Ansatz für die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, eingeführt.	Durch diese Richtlinie wird ein Verfahren zur Ermittlung und Ausweisung kritischer europäischer Infrastrukturen sowie ein gemeinsamer Ansatz für die Bewertung der Notwendigkeit, ihren Schutz ***vor Gefahren aller Art*** zu verbessern, eingeführt.

Begründung

Die Strategie sollte den Schutz vor Gefahren aller Art verfolgen, einschließlich vor jenen Gefahren, die weder von Terrorismus noch von Naturkatastrophen ausgehen, aber trotzdem die Funktionalität und Integrität der Infrastruktur nachhaltig beeinträchtigen können. Dazu zählen u. a. menschliches Versagen, nicht hinreichend qualifiziertes Personal, Outsourcing unternehmenskritischer Infrastrukturen, Epidemien/Seuchen, zunehmende IT-Abhängigkeit, weltweite Vernetzung von IT-Systemen, politische Unruhen usw.

Änderungsantrag 3
Artikel 5 Absatz 2 Unterabsatz 1

In dem Sicherheitsplan werden die wesentlichen Bestandteile der einzelnen kritischen europäischen Infrastrukturen aufgeführt und einschlägige Sicherheitsmaßnahmen zu ihrem Schutz nach Anhang II festgelegt. In Übereinstimmung mit dem in Artikel 11 Absatz 3 genannten Verfahren können sektorspezifische, den bestehenden Gemeinschaftsmaßnahmen Rechnung tragende Anforderungen an den Sicherheitsplan ***angenommen*** werden.	In dem Sicherheitsplan werden die wesentlichen Bestandteile der einzelnen kritischen europäischen Infrastrukturen aufgeführt und einschlägige Sicherheitsmaßnahmen zu ihrem Schutz nach Anhang II festgelegt. In Übereinstimmung mit dem in Artikel 11 Absatz 3 genannten Verfahren können sektorspezifische, den bestehenden Gemeinschaftsmaßnahmen Rechnung tragende Anforderungen an den Sicherheitsplan ***voll angerechnet*** werden.

Begründung

Versicherungsunternehmen und Banken gehören zu jenen Branchen, welche laufend hohe Summen in Sicherheitsvorkehrungen wie Zugangskontrollen oder die Sicherung von Informationssystemen investieren. Die staatlichen Maßnahmen dürfen bereits bestehende sektorielle Maßnahmen nicht duplizieren. Daher sollte eine künftige Regelung die volle Anrechnung bestehender Sicherheitspläne gewährleisten.

Änderungsantrag 4
Artikel 10 Absatz 3

3. Die Mitgliedstaaten stellen sicher, dass ihnen oder der Kommission übermittelte Informationen über den Schutz kritischer Infrastrukturen zu keinem anderen Zweck als zum Schutz kritischer Infrastrukturen verwendet werden.	3. Die Mitgliedstaaten stellen sicher, dass ihnen oder der Kommission übermittelte Informationen über den Schutz kritischer Infrastrukturen zu keinem anderen Zweck als zum Schutz kritischer Infrastrukturen verwendet werden ***und dass der Grundsatz der Verhältnismäßigkeit aus materieller Sicht und schützenswerte Grundrechte und Institutionen unbedingt mitberücksichtigt werden.***

Begründung

Zu anderen schützenswerten Grundrechten und Institutionen zählen zum Beispiel Datenschutz oder das Telekommunikationsgeheimnis.

Änderungsantrag 5
Anhang I Reihe VII „Finanzsektor“ Spalte „Untersektor“ Nummer 19

19. Infrastrukturen ***und Netze*** für das Clearing und die Abrechnung von ***Zahlungen und*** Wertpapieren	19. Infrastrukturen für das Clearing und die Abrechnung von Wertpapieren

Änderungsantrag 6
Anhang I Reihe VII „Finanzsektor“ Spalte „Untersektor“ Nummer 19 a (neu)

	19a. Zahlungssysteme

Änderungsantrag 7
Anhang I Reihe VII „Finanzsektor“ Spalte „Untersektor“ Nummer 19 b (neu)

	19b. Bank- und Versicherungswesen