Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Bevölkerungsschutz BABS

Erster Bericht an den Bundesrat zum

Schutz Kritischer Infrastrukturen

20.06.2007

Inhaltsverzeichnis

1 Ausgangslage

1.1 Was sind Kritische Infrastrukturen

Infrastrukturen bilden eine zentrale Voraussetzung für das Funktionieren vieler gesellschaftlicher, wirtschaftlicher und politischer Prozesse. Sie lassen sich zu Sektoren zusammenfassen, zu denen beispielsweise Energieversorgung, Verkehrswesen, Informations- und Kommunikationstechnologien, Finanzwesen, Trinkwasser- und Lebensmittelversorgung und Gesundheitswesen gehören. Der Grad der Funktionsfähigkeit von Infrastrukturen beeinflusst die Lebensqualität einer Gesellschaft, die Wertschöpfung der Wirtschaft und die Sicherheit des Staates und seiner Bevölkerung.

Im Allgemeinen bezeichnet man diejenigen Infrastrukturen als kritisch, welche für das Funktionieren des Gesamtsystems oder anderer Infrastrukturen besonders wichtig sind. Die Bedeutung der einzelnen Infrastrukturen hängt jedoch von der jeweiligen Betrachtungsebene ab. Der Einsturz eines Einfamilienhauses ist in erster Linie für die betroffene Familie eine Tragödie. Der Brand in einem Gemeindehaus wiederum hat Auswirkungen auf die gesamte Gemeinde. Die umliegende Region, der Kanton und der Bund sind dadurch jedoch nicht beeinträchtigt. Störungen des zentralen Leitsystems der SBB können zu Ausfällen in der ganzen Schweiz führen – ja sogar mit grenzüberschreitenden Konsequenzen. Die Ausführungen in diesem Bericht beziehen sich auf Infrastrukturen, deren Funktionen und Dienstleistungen primär auf nationaler Ebene von Bedeutung sind.

Der Schutz Kritischer Infrastrukturen (SKI) ist an sich kein neues Thema. Staaten haben schon immer versucht, wichtige Infrastrukturen gegen Naturereignisse, technische Ausfälle, Sabotage bzw. Zerstörungen zu schützen. Auch in Kriegen stellen wirtschaftlich bedeutende Anlagen des Gegners jeweils ein lohnendes Ziel dar, um dessen Rückgrat zu brechen.

Das störungsfreie Funktionieren Kritischer Infrastrukturen ist für westliche Industrienationen mittlerweile zu einer Selbstverständlichkeit geworden. Störungen und Unterbrechungen Kritischer Infrastrukturen haben direkte Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen. Ein wichtiger Standortfaktor der Schweiz ist ein stabiles und qualitativ hoch stehendes Infrastruktursystem. Entsprechend gering ist in der Schweiz die Akzeptanz für eingeschränkte oder nicht verfügbare Dienstleistungen.

1.2 Auftrag des Bundesrates

Im Frühjahr 2004 ersuchte die Geschäftsprüfungsdelegation der eidgenössischen Räte (GPDel) um Auskunft, welche Bedeutung der Sicherheitsausschuss des Bundesrates und die Lenkungsgruppe Sicherheit den Kritischen Infrastrukturen in der Schweiz beimessen. Insbesondere interessierte die Frage, ob und inwiefern bereits geklärt sei, welche Infrastrukturen für das Funktionieren von Gesellschaft, Wirtschaft und Politik unerlässlich seien und ob deren Verletzlichkeit überprüft sowie Schutz- und Sicherheitsmassnahmen evaluiert worden seien.

Das Bundesamt für Bevölkerungsschutz (BABS) wurde durch den Chef VBS, Bundesrat Samuel Schmid, in seiner Funktion als Vorsitzender des Sicherheitsausschusses des Bundesrats mit der Ausarbeitung der verlangten Übersicht beauftragt. Das BABS hatte sich seit 2003 vertieft mit der Thematik befasst und erstellte im Hinblick auf eine Anhörung der GPDel am 5. Juli 2004 einen zusammenfassenden Bericht "Schutz und Sicherheit Kritischer Infrastrukturen in der Schweiz".

In diesem Bericht wurden Lücken und entsprechender Handlungsbedarf festgestellt (v.a. gemeinsames Grundverständnis, Gefährdungsszenarien, Schutzziele, Liste von Kritischen Infrastrukturen und Kompetenzregelungen). Diese wurden im Aussprachepapier an den Bundesrat zusammengefasst. Basierend auf dem Aussprachepapier vom 15. Juni 2005 hat der Bundesrat am 22. Juni 2005 das VBS (BABS) damit beauftragt, *"die koordinative Leitung der Arbeiten zum Thema 'Schutz Kritischer Infrastrukturen' zu übernehmen und - gemäss den Empfehlungen der Ziffer 4 des Aussprachepapiers - zusammen mit den von den Departementen bzw. Ämtern bezeichneten Kontaktpersonen die Arbeiten durchzuführen."* Der vorliegende erste Bericht stellt ein erstes Ergebnis dieses Auftrags dar.

2 Ziele

2.1 Erster Bericht

Die diesem ersten Bericht zugrunde liegenden Ziele sind im Aussprachepapier vom 15. Juni 2005 festgehalten. In einer etappierten und fokussierten Vorgehensweise sollen folgende Teilaspekte bearbeiten werden:

- *Erstellen einer Übersicht der bisherigen Arbeiten im Bereich Schutz Kritischer Infrastrukturen*
- *Identifikation von für die Schweiz relevanten Kritischen Infrastrukturen*
- *Vereinbaren eines Grundsets an Gefährdungsszenarien*
- *Auswahl einer für die Schweiz relevanten Kritischen Infrastruktur und modellhafte Erarbeitung einer Strategie und eines Massnahmenkatalogs*

Der vorliegende Bericht, welcher durch die Zusammenarbeit der in der Arbeitsgruppe SKI vertretenen Bundesstellen breit abgestützt ist, präsentiert erste Ergebnisse dieser Arbeiten und versteht sich als Etappe auf dem Weg zu einer nationalen Strategie zum Schutz Kritischer Infrastrukturen in der Schweiz. Im Bericht werden Arbeitsweise, Problemstellung und Definitionen festgelegt, die für die Schweiz als relevant betrachteten Kritischen Infrastruktursektoren aufgeführt sowie Grundlagen und Rahmenbedingungen der Gefährdungsszenarien dargelegt. Im Weiteren skizziert der Bericht Gefährdungsszenarien und zeigt den Handlungsbedarf sowie das geplante Vorgehen im Bereich Schutz Kritischer Infrastrukturen auf. In den Anhängen zu diesem Bericht werden die bisherigen Arbeiten im Bereich Schutz Kritischer Infrastrukturen (Aktivitäten anderer Staaten, relevante Stellen des Bundes, Entwicklungen in der Schweiz) dargestellt. Da es in einer ersten Etappe wichtig war, sich innerhalb der Arbeitsgruppe, in der Bundesämter aus allen sieben Departementen vertreten sind, auf gemeinsame Definitionen und Rahmenbedingungen zu einigen und das gegenseitige Verständnis zu fördern, musste in diesem Bericht auf die Erarbeitung einer modellhaften Strategie und eines Massnahmenkatalogs zu einer für die Schweiz besonders relevanten Kritischen Infrastruktur verzichtet werden. Dies wird im Rahmen der nächsten Etappe nachgeholt werden.

2.2 Nationale Strategie zum Schutz Kritischer Infrastrukturen

Viele Stellen beim Bund, bei den Kantonen, der Wirtschaft und der Wissenschaft befassen sich – teils unabhängig voneinander und in ihren jeweiligen Kompetenzbereichen – mit dem Schutz Kritischer Infrastrukturen. Die nationale Strategie soll den Dialog und die Zusammenarbeit zwischen diesen Stellen fördern, Synergien nutzen sowie den Austausch von Wissen und Erfahrungen institutionalisiert vorantreiben.

Aufbauend auf diesem ersten Bericht soll eine nationale Strategie erarbeitet werden. Diese Strategie soll gemeinsame Beurteilungsmethoden enthalten und einheitliche Schutzziele definieren. Damit soll eine Grundlage für sektorspezifische und übersektorielle Arbeiten und ein kohärenter Rahmen geschaffen werden, worauf sich Stellen innerhalb und ausserhalb der Bundesverwaltung, welche sich mit dem Schutz Kritischer Infrastrukturen befassen, bei ihren Tätigkeiten abstützen können.

Das Ziel der nationalen Strategie ist die Aufrechterhaltung der Lebensgrundlagen der Bevölkerung. Dies soll mittels folgender Teilziele erreicht werden:

- die Risiken für die Kritischen Infrastrukturen integral analysieren sowie Massnahmen zu deren Minderung vorschlagen;
- die Wechselwirkungen und gegenseitigen Abhängigkeiten der Kritischen Infrastrukturen aufzeigen;
- das Vertrauen, den Informationsaustausch und die Zusammenarbeit zwischen Behörden, Betreibern kritischer Infrastrukturen und der Privatwirtschaft fördern und damit Synergien nutzen;
- geeignete Massnahmen empfehlen, um beim Eintritt von Schadenereignissen die Dauer und die Auswirkungen möglichst gering zu halten.

3 Arbeitsweise

3.1 Arbeitsgruppe Schutz Kritischer Infrastrukturen

Die nationale Strategie zum Schutz Kritischer Infrastrukturen soll in enger Zusammenarbeit mit den zuständigen Ämtern erarbeitet werden. Vorerst wurde eine Arbeitsgruppe (AG SKI) auf der Basis einer offiziellen Anfrage gebildet, in der 18 Bundesstellen (Auflistung gemäss Staatskalender) vertreten sind:

EDA	POLS, DEZA
EDI	MeteoSchweiz, BAG
EJPD	fedpol
VBS	IOS, FST A, armasuisse Immobilien, BABS
EFD	ISB, BIT, BBL
EVD	BWL
UVEK	BAV, BFE, ASTRA, BAKOM, BAFU

Zur Erarbeitung des vorliegenden Berichts hat sich die AG SKI unter der Leitung des BABS drei Mal getroffen und Vorversionen in mehreren Runden konsultiert. Diese Treffen haben ein gemeinsames Grundverständnis gefördert und zu einem einheitlichen Sprachgebrauch der wichtigsten Begriffe (vgl. Ziffer 5) beigetragen. Sie haben zudem die Identifikation des Gefahrenspektrums und der Kritischen Infrastrukturen ermöglicht. Dieser Bericht wurde mehrmals innerhalb der AG SKI konsultiert und berücksichtigt dabei die unterschiedlichen Anliegen der darin vertretenen Bundesämter. In einer nächsten Phase sollen neben der AG SKI gezielt Unterarbeitsgruppen eingesetzt werden, um einzelne Themenbereiche vertieft zu bearbeiten. Die Resultate dieser Unterarbeitsgruppen fliessen zurück in die Arbeiten der AG SKI.

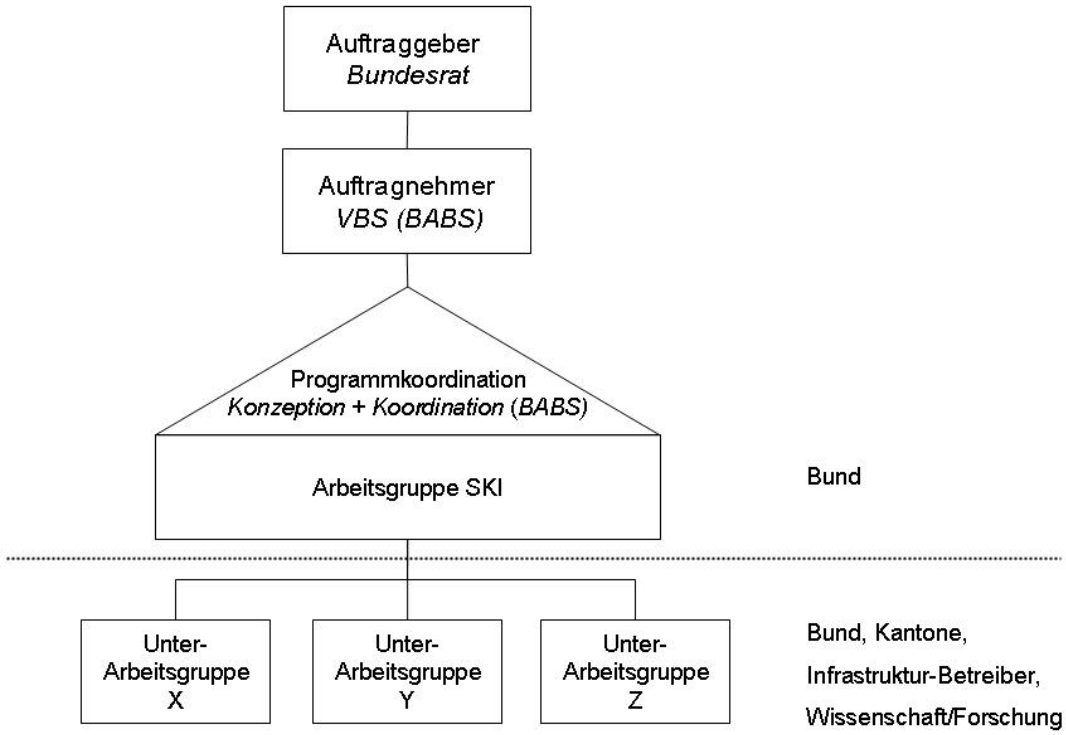

Abbildung 1: Organisation des Programms für den Schutz Kritischer Infrastrukturen

3.2 Partnerschaftliche Zusammenarbeit

Die Zusammenarbeit aller Partner stellt eine wesentliche Voraussetzung für die erfolgreiche Erarbeitung und Umsetzung einer nationalen Strategie zum Schutz Kritischer Infrastrukturen dar. Der Einbezug aller relevanten Bundesstellen, der Wirtschaft (Industrie, Gewerbe, Dienstleistungsbereich usw.) und der Kantone bzw. der zuständigen Behörden ist somit unabdingbar. Im Rahmen der AG SKI findet bereits heute zwischen vielen relevanten Bundesstellen eine Zusammenarbeit statt. Zudem bestehen bereits partnerschaftliche Instrumente zu einzelnen Infrastruktursektoren (z.B. MELANI, SONIA, Infosurance Roundtables; siehe dazu Anhänge 2 und 3). Im Rahmen der Erarbeitung einer nationalen Strategie soll diese auf weitere Partner ausgedehnt werden.

4 Problemstellung

4.1 Einflussfaktoren

Durch Veränderungen der sicherheitspolitischen Lage und der politischen, wirtschaftlichen und technologischen Rahmenbedingungen wird die Bedeutung des Schutzes Kritischer Infrastrukturen weiter steigen. Die folgenden Gründe sind hierfür ausschlaggebend:

- Höhere gegenseitige Abhängigkeiten: Verschiedene Produkte und Dienstleistungen der modernen Gesellschaft sind immer stärker von funktionierenden Infrastrukturen abhängig. Die Bedeutung von Infrastrukturdienstleistungen (z.B. Stromversorgung, Verkehr, Informations- und Kommunikationstechnologien) für das gesellschaftliche,

wirtschaftliche und politische Leben hat gegenüber früher deutlich zugenommen. Dadurch steigt im Ereignisfall auch das Risiko von dominoartigen Effekten.

- Zunehmende Durchdringung mit technischen Systemen: Infrastrukturen sind vermehrt mit technischen Einrichtungen (z.B. Informationstechnologie und Automatisierung der Produktion) ausgerüstet. Diese unterstützen die Produktions- und Überwachungsprozesse; die erhöhte Komplexität kann jedoch eine erhöhte Verletzlichkeit zur Folge haben.
- Wirtschaftliche Entwicklungen: Die Auswirkungen der heutigen wirtschaftlichen Rahmenbedingungen (Produktionsverlagerungen ins Ausland, serienmässige Produktion, Reduktion der Zeitmarge und des Lagerbestands, Liberalisierung und Globalisierung, Abnahme der Vielfältigkeit der Informatik-Produkte) tragen zur Erhöhung der Verletzlichkeit der Infrastrukturen bei.
- Abnahme von Redundanzen: Kostendruck hat zur Abschaffung von zahlreichen Redundanzen (z.B. Stromaggregate, Notvorräte) geführt, was die Verwundbarkeit erhöht und bei Störungen der Infrastrukturen zu längeren Ausfallzeiten führen kann.
- Höhere Konzentration von Werten: Die zunehmende Konzentration von Werten (Immobilien, Mobilien, Kulturgüter usw.) auf Ballungszentren sowie eine gegenüber früher erhöhte Nutzungsintensität führen im Ereignisfall zu höheren Schäden.
- Attraktivität der Ziele: Zivile Einrichtungen erweisen sich als besonders attraktive Ziele bei Terroranschlägen und asymmetrischer Kriegsführung, da sie v.a. aus wirtschaftlichen Gründen nicht im gleichen Ausmass wie militärische Einrichtungen geschützt werden können. Dazu gehören insbesondere Regierungsgebäude, Wirtschafts- und Verkehrsknotenpunkte sowie Energie- und Informationsinfrastrukturen.

4.2 Bedeutung Kritischer Infrastrukturen anhand von Beispielen

Folgende Beispiele verdeutlichen, welche Schäden entstehen können, wenn es bei Kritischen Infrastrukturen zu Beschädigungen oder Ausfällen kommt:

- Naturkatastrophen: Extreme Naturereignisse, welche in jüngster Zeit vermehrt aufgetreten sind und weiter zunehmen dürften, richten bei Kritischen Infrastrukturen grosse Schäden an. Im Sommer 2005 verursachte der Wirbelsturm Katrina in New Orleans nicht nur grosse menschliche Verluste und hohe Sachschäden, sondern legte auch die Produktion, den Import und das Raffinieren von Rohöl sowie die lokale Stromversorgung und die Hafenanlagen (einer der wichtigsten US-Häfen für den Export von Agrarwaren) für mehrere Wochen lahm. Heftige Schnee- und Eisregenfälle zerstörten in Deutschland im November 2005 ca. 70 Hochspannungsmasten. Dadurch waren rund 250'000 Personen bei sehr tiefen Temperaturen für mehrere Tage ohne Strom. Betroffen waren durch die Stromausfälle die allgemeine Versorgung der Bevölkerung sowie der Transportsektor, da viele Zug- und Flugverbindungen ganz ausfielen.
- Grossflächige Blackouts: Am 28. September 2003 kam es in praktisch ganz Italien zu einem Totalausfall der Stromversorgung. Der Gesamtschaden wurde auf ca. 185 Millionen Franken geschätzt (v.a. Verluste in der Lebensmittelindustrie und Wiederinstandsetzungskosten). Es war innerhalb von sieben Wochen der vierte grossflächige Stromausfall – nach denjenigen in den USA, Schweden/Dänemark und London. Diese Vorfälle zeigen die Abhängigkeit der Infrastrukturen von der Stromversorgung auf und verdeutlichen, wie gross die unmittelbaren Folgeschäden sein können.
- Ausfälle einzelner Stromnetze: Am 22. Juni 2005 kam es zu einem landesweiten Ausfall des Stromnetzes der Schweizer Bundesbahnen (SBB). Betroffen davon waren rund 2'000 Züge mit über 200'000 Reisenden. Die sonst als zuverlässig geltenden SBB bezeichneten den erlittenen Imageschaden als gross. Neben dem Imageschaden

entstand ein finanzieller Schaden von ca. 5 Millionen Franken, der vor allem durch Entschädigungszahlungen verursacht wurde.

- Softwareprobleme: In Japan bewirkte die Einführung neuer Software Anfang März 2003 einen landesweiten Ausfall des Flugleitsystems. Mehrere hundert Flüge mussten gestrichen werden. Es dauerte mehrere Tage, bis das System wieder einwandfrei funktionierte.
- Sabotage: Im März und April 2000 drang ein 49jähriger Mann in die durch Computer gesteuerte Wasserversorgung in Queensland (Australien) ein. Mit der erlangten Befehlsgewalt über 300 Kontrollknoten des Trink- und Abwassersystems der Region gelang es ihm, einige Millionen Liter Abwasser in Flüsse, Parks und Erstklasshotels fliessen zu lassen. Dadurch wurde die Meeresfauna stark geschädigt; dies verursachte u.a. hohe finanzielle Ausfälle im Tourismusbereich.
- Terroranschläge: Ereignisse wie die Terroranschläge vom 11. September 2001 zeigen, dass Angriffe vermehrt gegen (zivile) Schwachstellen und Kritische Infrastrukturen gerichtet werden: Beim Einsturz der beiden Türme des World Trade Centers kamen mehr als 2'600 Personen ums Leben. Wichtige Kommunikationsinfrastrukturen wurden zerstört, was auch die Wall Street und das globale Finanzsystem stark beeinträchtigte. Der wirtschaftliche Schaden überstieg alleine in den ersten Monaten nach den Angriffen die Schwelle von 100 Milliarden USD. Die Terroranschläge in Madrid (2004) und London (2005) forderten zusammen einige hundert Tote und mehrere tausend Verletzte. Der gesamte Bahnverkehr wurde für Stunden lahm gelegt. Die Anschläge hatten einschneidende psychologische Auswirkungen und verstärkte Sicherheitsmassnahmen zur Folge.

5 Definitionen

Folgende Definitionen wurden innerhalb der AG SKI erarbeitet. Dabei hat sich die AG SKI auf bestehende Definitionen anderer Staaten und der EU (siehe Anhang 1) abgestützt und diese den schweizerischen Verhältnisse (hinsichtlich Politik, Wirtschaft, Technologie, Kultur, Geographie und Topographie) angepasst. Dies ist zum einen nötig, da es keine allgemein anerkannte Definitionen mit genügender Aussagekraft gibt, und zum anderen, da sich die länderspezifischen Definitionen je nach der Entwicklung des Landes (technologisch und politisch), der Wahrnehmung der Bedeutung der Infrastrukturen (Kultur, Sensibilität und Geschichte) und der Situation des Landes (Geographie und Sicherheitspolitik) unterscheiden.

Die Definitionen setzen den Rahmen für den Schutz Kritischer Infrastrukturen und bieten die Grundlagen für die weiteren Arbeiten. Die Definitionen müssen je nach Bedarf in der nationalen Strategie weiterentwickelt und angepasst werden.

Infrastrukturen
Der Sammelbegriff Infrastrukturen umfasst Personen, Organisationen, Prozesse, Produkte, Dienstleistungen, Informationsflüsse sowie technische und bauliche Anlagen und Einrichtungen, welche einzeln oder vernetzt das Funktionieren der Gesellschaft, der Wirtschaft und des Staates ermöglichen.

Die Infrastrukturen sind in drei Ebenen eingeteilt:
- **Sektoren**: z.B. Energie, Finanzen, Gesundheit
- **Teilsektoren**: z.B. Stromversorgung, Erdölversorgung, Erdgasversorgung
- **Einzelobjekte/Elemente**: z.B. Pumpen, Rohrleitungen, Staudämme, Hochspannungsleitungen, Steuerungssysteme

Kritische Infrastrukturen
Kritische Infrastrukturen sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf Gesundheit, Öffentlichkeit, Umwelt, Politik, Sicherheit, das wirtschaftliche oder soziale Wohlergehen haben.

Kritikalität
Die Kritikalität einer Infrastruktur bezeichnet ihre relative Bedeutung in Bezug auf die Auswirkungen, die eine Störung, ein Funktionsausfall oder eine Zerstörung für die Bevölkerung und ihre Lebensgrundlagen hätte.

Ziel des Schutzes Kritischer Infrastrukturen
Das Ziel des Schutzes Kritischer Infrastrukturen ist es, die Eintretenswahrscheinlichkeit und das Schadensausmass einer Störung, eines Ausfalls oder einer Zerstörung der Kritischen Infrastrukturen zu reduzieren beziehungsweise die Ausfallzeit zu minimieren.

Schutz Kritischer Infrastrukturen und Schutz Kritischer Informationsinfrastrukturen
Es wird zwischen dem Schutz kritischer Infrastrukturen, SKI (Critical Infrastructure Protection, CIP) und dem Schutz kritischer Informationsinfrastrukturen, SKII (Critical Information Infrastructure Protection, CIIP) unterschieden. Der SKI umfasst den Schutz sämtlicher Kritischer Infrastrukturen, während sich der SKII auf den Schutz der Informationsinfrastrukturen beschränkt und einen Teilbereich im Rahmen einer umfassenden Schutzstrategie darstellt.

6 Identifikation der Kritischen Infrastrukturen

Eine erste Identifikation der für die Schweiz relevanten Kritischen Infrastrukturen wurde innerhalb der AG SKI vorgenommen. Die Liste muss im Laufe der Arbeiten zur nationalen Strategie überprüft und durch kritische Einzelobjekte und Infrastrukturelemente verfeinert werden.

Die Einstufung einer Infrastruktur als kritisch bezieht sich auf den gesamten (Teil-)Sektor und nicht auf einzelne Infrastrukturelemente (Bsp. Energie und nicht einzelne Talsperre). Die Auflistung der Sektoren erfolgt alphabetisch und stellt somit keine Gewichtung dar. Es ist vorgesehen, im weiteren Verlauf der Arbeiten eine Gewichtung aufgrund der Bedeutung des Sektors (und seiner Teilsektoren und Infrastrukturelemente) vorzunehmen.

Sektoren	Teilsektoren
Behörden	Parlament, Regierung, Justiz, Verwaltung
	Forschungseinrichtungen
	Nationale Kulturgüter
	Ausländische Vertretungen und Sitze internationaler Organisationen
Chemische Industrie	Produktion, Transport, Lagerung und Verarbeitung chemischer Stoffe
Energie	Stromversorgung
	Erdölversorgung
	Erdgasversorgung
Entsorgung	Abwasser
	Industrie- und Hausabfälle
	Kontrollpflichtige Abfälle
Finanzen	Banken
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Arzneimittel
	Labors
Informations- und Kommunikationstechnologien (IKT)	Telekommunikation
	Informationssysteme und -netze
	Internet
	Instrumentations-, Automations- und Überwachungssysteme
	Rundfunk und Medien
Nahrung	Versorgung mit Lebensmitteln und Gewährleistung der Lebensmittelsicherheit
	Trinkwasserversorgung
Öffentliche Sicherheit, Rettungs- und Notfallwesen	Blaulichtorganisationen (Polizei, Feuerwehr, sanitätsdienstliches Rettungswesen)
	Zivilschutz
	Armee
Verkehr	Strassenverkehr
	Schienenverkehr
	Luftverkehr
	Schifffahrt
	Postwesen und Logistik

Tabelle 1: Kritische Infrastruktursektoren und -teilsektoren der Schweiz

7 Grundlagen und Rahmenbedingungen

7.1 Integrales Risikomanagement

Für den Schutz Kritischer Infrastrukturen wird ein integrales Risikomanagement verwendet. Die Komplexität und die gegenseitigen Abhängigkeiten der Kritischen Infrastrukturen führen dazu, dass ein umfassender Ansatz unabdingbar ist, um einen optimalen Schutz der Kritischen Infrastrukturen zu gewährleisten.

In der Massnahmenplanung soll der Risikomanagement-Kreislauf angewandt werden. Dieser unterstützt die Auswahl von geeigneten Massnahmen und optimiert die Umsetzung der getroffenen Massnahmen für alle Phasen des Risikomanagements. Als Ausgangspunkt der weiteren Arbeiten dient das im Rahmen von KATARISK durch das BABS erarbeitete Konzept (Abbildung 2). Dieses soll v.a. im präventiven Bereich durch bauliche, technische,

organisatorische und rechtliche Massnahmen spezifisch für die Bedürfnisse zum Schutz Kritischer Infrastrukturen angepasst werden.

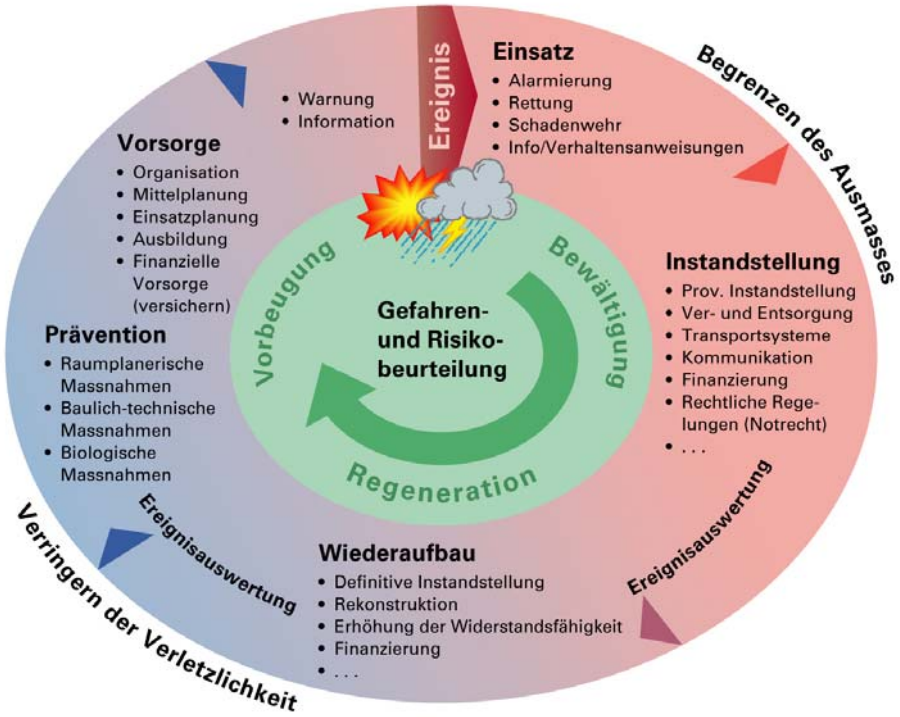

Abbildung 2: Risikomanagement-Kreislauf (BABS 2003)

Das integrale Risikomanagement lässt sich wie folgt auf die Perspektive des Schutzes Kritischer Infrastrukturen anwenden (Abb. 3). Dabei gilt es zu berücksichtigen, dass neben den präventiven und vorsorglichen Massnahmen auch Interventionsmassnahmen eingeplant und vorbereitet werden.

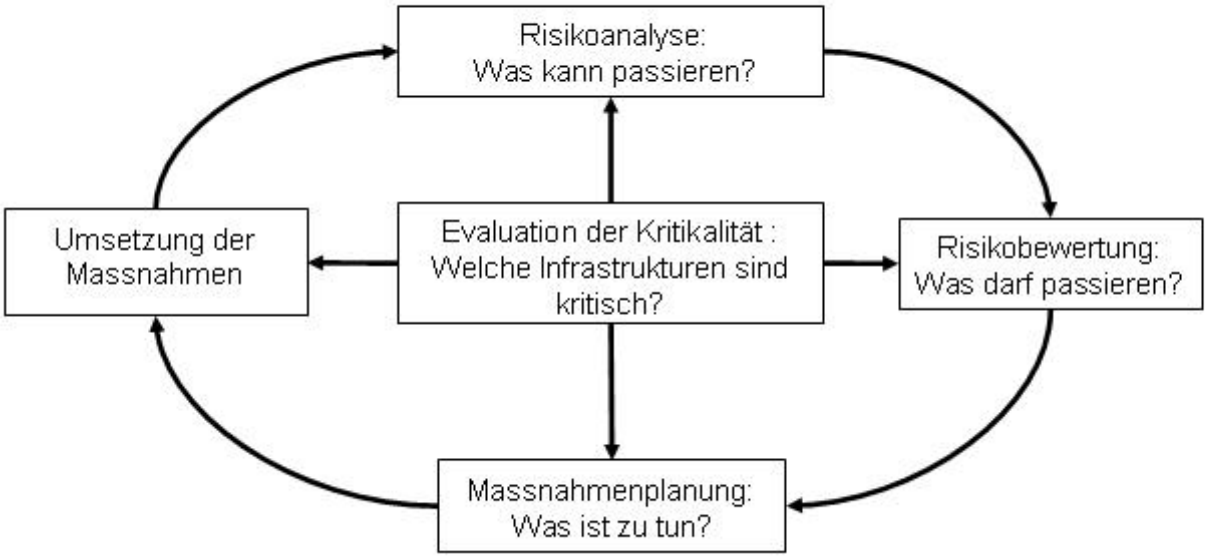

Abbildung 3: Das integrale Risikomanagement aus der Perspektive des Schutzes Kritischer Infrastrukturen

Gesellschaft, Technologien sowie das wirtschaftliche und sicherheitspolitische Umfeld wandeln sich dauernd. Deshalb müssen Risikoanalysen periodisch aktualisiert und Schutzmassnahmen entsprechend angepasst werden. Punktuelle und zeitlich begrenzte Massnahmen sind unzureichend, um einen umfassenden Schutz zu erreichen. Der Schutz Kritischer Infrastrukturen in der Schweiz ist deshalb eine permanente Aufgabe. Nur so lässt sich ein der jeweiligen Risikolage angepasster Schutz wirksam und nachhaltig gewährleisten.

7.2 Schutzziele

Die Schutzziele umschreiben das anzustrebende und finanzierbare Sicherheitsniveau und bestimmen die entsprechenden Schutzmassnahmen. Das Schutzziel selber ist nicht absolut und hängt von der sicherheitspolitischen Lage ab.

Allgemeine Schutzziele lassen sich von der Lagebeschreibung ableiten. Spezifische Schutzziele müssen für jeden Infrastruktursektor (z.B. minimale Stromversorgung im Energiesektor) vereinbart werden. Sie hängen von der Art der Infrastruktur und ihrer Kritikalität ab.

Lagen	Beschreibung der Situation	Allgemeine Schutzziele
Normale Lage	Situation, in der ordentliche Abläufe zur Bewältigung der anstehenden Probleme und Herausforderungen ausreichen.	Im Alltag müssen die Kritischen Infrastrukturen ständig in der Lage sein, die gewohnte Leistung zu erbringen und Alltagsstörungen ohne bemerkbare Folgen zu bewältigen.
Besondere Lage	Situation, in der gewisse Aufgaben mit den normalen Abläufen nicht mehr bewältigt werden können. Im Unterschied zur "ausser-ordentlichen Lage" ist die Funktionsfähigkeit nur sektoriell betroffen. Typisch ist der Bedarf nach rascher Konzentration der Mittel und Straffung der Verfahren.	Das übliche Niveau der Leistungen soll möglichst aufrechterhalten und die Wirtschaft möglichst wenig beeinträchtigt werden. Die Einschränkungen sollen selten, geographisch und zeitlich limitiert sein, eine beschränkte Auswirkung haben und die Konsequenzen jederzeit bewältigbar und unter Kontrolle sein.
Ausserordentliche Lage	Situation, in der in zahlreichen Bereichen und Sektoren normale Abläufe nicht genügen, um die Probleme und Herausforderungen zu bewältigen, beispielsweise bei Naturkatastrophen oder kriegerischen Ereignisse, die das ganze Land schwer in Mitleidenschaft ziehen.	Mit ausserordentlichen Mitteln und ausserordentlichen Massnahmen muss die Instandstellung nach einer gewisser Zeit und Einschränkungen wieder möglich sein. Überlebensnotwendige Dienstleistungen (z.B. Wasser, Lebensmittel, Unterkunft) müssen gewährleistet werden und sind dementsprechend prioritär zu behandeln.

Tabelle 2: Allgemeine Schutzziele für die normale, besondere und ausserordentliche Lage (Lagebeschreibung basierend auf dem sicherheitspolitischen Bericht 2000)

7.3 Gefahrenspektrum

Dem Konzept des integralen Risikomanagements (vgl. Abb. 3) folgend, beginnt die Risikoanalyse mit einer Gefahrenanalyse, welche umfassend ("all hazards approach"-Ansatz) sein soll. Erst nach einer vollständigen Risikoanalyse und -bewertung können Prioritäten gesetzt werden, die sich auf den Schutz vor bestimmten Gefahren beziehen.

Die folgende Gefahrenliste ist nicht abschliessend. Je nach Infrastruktur(-Element) und den dazugehörigen Schutzzielen stehen andere Gefahren im Vordergrund, was eine jeweilige Anpassung erfordert.

Kategorien	**Gefahren**
Naturgefahren	Erdbeben
	Lawine
	Geologische Massenbewegung
	Hochwasser
	Sturm
	Trockenheit
	Extremtemperatur
	Grossbrand
Technische Gefahren	Technischer Ausfall von Systemen
	Menschliches Versagen bei techn. Systemen
	Störfall bei Stau-Anlage
	KKW-Störfall
	Chemischer Störfall
	Verkehrsunfall mit gefährlichen Gütern
Gesellschaftliche Gefahren	Pandemie
	Massenmigration
Gewalt (unterhalb und oberhalb der Kriegsschwelle)	Organisierte Kriminalität
	Sabotage
	Erpressung
	Terrorismus
	Bewaffneter Konflikt

Tabelle 3: Gefahrenliste

8 Gefährdungsszenarien

Szenarien sind unabdingbar für die Risikoanalyse, indem sie mögliche Ereignisse oder Entwicklungen beschreiben und somit ein wichtiges Instrument für die Vorbereitung auf diese Ereignisse darstellen.

Bisherige Studien und Planungsgrundlagen im Bereich Schutz Kritischer Infrastrukturen gehen teilweise von unterschiedlichen Gefährdungsszenarien aus, die oftmals keine Angaben zu Häufigkeit und Auswirkungen auf die Infrastrukturen enthalten. Für eine kohärente Strategie und abgestimmte Massnahmen braucht es ein gemeinsames Grundset an Gefährdungsszenarien.

Klassische Referenzszenarien lassen sich nicht direkt auf die Risikoanalyse zu Kritischen Infrastrukturen übertragen und müssen aus folgenden Überlegungen überarbeitet werden:

- Klassische Szenarien basieren auf einzelnen und isolierten Gefahren und Bedrohungen und ihren allgemeinen Auswirkungen. Die Auswirkungen eines Ereignisses sind aber im

Fall der Kritischen Infrastrukturen wenig voraussehbar, da sie stark von den Wechselwirkungen mit anderen kritischen Infrastrukturelementen abhängen, die gegenüber Gefahren unterschiedlich exponiert sind. Spezifische Gefährdungsszenarien sind dementsprechend nur anwendbar, wenn sie Auswirkungen über breite Regionen (z.B. Pandemie) berücksichtigen und/oder viele kritische Infrastrukturen (z.B. Erdbeben) umfassen. Ein alternativer Ansatz wäre die Erarbeitung von Szenarien, die sich direkt auf den Ausfall bestimmter Kritischer Infrastrukturen (z.B. Ausfall der Stromversorgung) beziehen.

- Klassische Szenarien berücksichtigen jeweils nur ein Ereignis pro Szenario. Es kommt aber immer öfter vor, dass mehrere Ereignisse gleichzeitig auf die Infrastrukturen einwirken und Störungen sowie Ausfälle verursachen. Die Szenarien sollten diese Eventualitäten berücksichtigen.
- Die Interdependenzen zwischen Kritischen Infrastrukturen führen dazu, dass ein sehr komplexes Szenario notwendig wäre, um die weit verzweigten Dominoeffekte realistisch darzustellen. Eine grosse Herausforderung liegt darin, die Szenarien zum einen so zu entwerfen, dass sie überschaubar bleiben, und zum anderen so breit wie möglich zu gestalten, so dass sie alle relevanten Wechselwirkungen berücksichtigen.

Als exemplarische Grundlage für die Erarbeitung der nationalen Strategie sollen vier Szenarien aufdatiert und überarbeitet werden:

- **Erdbeben**: Diese Naturgefahr hat breitflächige Auswirkungen und kann somit als generisches Gefährdungsszenario für die Kritischen Infrastrukturen verwendet werden. Szenarien wurden im Dokument "Einsatzkonzept für den Fall eines Erdbebens in der Schweiz" (BABS, 2004) erarbeitet. Die Auswirkungen auf die Kritischen Infrastrukturen könnten mit der Auswertung der grenzüberschreitenden Erdbebenübung "RHEINTAL" (Oktober 2006) ergänzt werden.
- **Pandemie**: Eine Pandemie würde für viele Kritische Infrastrukturen schwerwiegende Auswirkungen haben. Das Szenario, welches im Rahmen des *Influenza-Pandemieplans Schweiz 2006* unter der Leitung des Bundesamts für Gesundheit (BAG) erarbeitet wurde, könnte bezüglich den Auswirkungen auf die Kritischen Infrastrukturen angepasst werden.
- **Ausfall der Stromversorgung**: Das Szenario eines Ausfalls der Stromversorgung wurde teilweise durch das Bundesamt für wirtschaftliche Landesversorgung (BWL) erstellt. Die Auswirkungen auf andere Kritische Infrastrukturen müssten anhand einer ausführlichen Risikoanalyse weiter erarbeitet werden.
- **Ausfall der Informationsinfrastruktur:** Dieses Szenario wurde 2004 im Rahmen des Projekts "Szenarien- und Expertenpool Risikoanalyse Schweiz" (ETHZ) erarbeitet. Seither erstellt das BWL - zusammen mit Stellen der Verwaltung und Privatwirtschaft - sektorspezifische Risikoanalysen (Szenarien, Risiken, Massnahmen) in den Sektoren Informations- und Kommunikationstechnologien, Finanzen, Energie (Strom), Verkehr, Gesundheit (Spitäler).

9 Weiteres Vorgehen

Aufgrund der Erkenntnisse der Arbeitsgruppe Schutz Kritischer Infrastrukturen (AG SKI) in der ersten Etappe lassen sich für das weitere Vorgehen folgende Empfehlungen ableiten:

9.1 Arbeitsgruppe Schutz Kritischer Infrastrukturen

Das VBS bzw. das BABS führt die koordinative Leitung der Tätigkeiten im Rahmen der Arbeitsgruppe Schutz Kritischer Infrastrukturen (AG SKI) weiter. Die AG SKI hat sich bewährt, um die verschiedenen Interessen der vertretenen Bundesämter einzubringen und

zu einem gemeinsamen Grundverständnis zum Schutz Kritischer Infrastrukturen zu gelangen. Punktuelle Ergänzungen mit Vertretern aus bis anhin nicht beteiligten Bundesstellen (z.B. Stab SiA, DSP, EFV, BAZL, etc.) werden in der zweiten Phase vorgenommen. Andere laufende Projekte des Bundes werden in dieser Phase berücksichtigt. Insbesondere wird die Koordination mit dem "Risikomanagement des Bundes" sichergestellt, so dass Synergien genutzt werden können. Im weiteren Verlauf der Arbeiten sollen neben der AG SKI gezielt Unterarbeitsgruppen eingesetzt werden, um einzelne Themenbereiche (siehe unten) vertieft zu bearbeiten.

9.2 Geplante weitere Etappen

Aufgrund der Vielschichtigkeit der Thematik und der Anzahl der involvierten Ämter ist es notwendig, weiterhin etappiert vorzugehen. Dabei werden gezielt Schwerpunkte gesetzt. Für die zweite Etappe bis Ende 2008 stehen folgende Tätigkeiten im Vordergrund:

- Auswahl eines für die Schweiz besonders relevanten Kritischen Infrastruktursektors und modellhafte Erarbeitung einer Strategie einschliesslich einer Risikoanalyse sowie eines Massnahmenkatalogs (Beispielstudie)
- Vertiefung der Gefährdungsszenarien
- Initiierung von Grundlagenforschung zu relevanten Themen (wie z.B. Interdependenzen zwischen Kritischen Infrastrukturen)
- Förderung der Zusammenarbeit (auf einzelne Infrastruktursektoren bezogen und sektorübergreifend) mit Kantonen und Betreibern Kritischer Infrastrukturen sowie Nachbarländern und internationalen Organisationen im Bereich Schutz Kritischer Infrastrukturen

Aufbauend auf diesen Arbeiten werden im Zeitraum von 2009-2011 folgende Schwerpunkte bearbeitet:

- Erweiterung der Beispielstudie auf andere kritische Infrastruktursektoren
- Erweiterung der Grundlagenforschung zu relevanten Themen in Zusammenarbeit mit akademischen Institutionen und der Privatwirtschaft
- Erarbeitung der nationalen Strategie für den Schutz Kritischer Infrastrukturen mit der Involvierung der Kantone und der Privatwirtschaft
- Erweiterung der Zusammenarbeit mit Nachbarländern und internationalen Organisationen im Bereich Schutz Kritischer Infrastrukturen mit z.B. spezifischen grenzüberschreitenden Risikoanalysen sowie nach Möglichkeit gemeinsamen Übungen

Schliesslich folgen ab 2012 die Umsetzung und Aktualisierung der nationalen Strategie für den Schutz Kritischer Infrastrukturen.

9.3 Personelle Konsequenzen

Auf Stufe Bund werden für die 2. Etappe bis zur nächsten Information des Bundesrates keine zusätzlichen personellen Ressourcen benötigt. Im Verlauf der vorgesehenen dritten Etappe (2009 - 2011) ist jedoch mit einer personellen Verstärkung zu rechnen, um die notwendigen Koordinationstätigkeiten wahrzunehmen.

9.4 Finanzielle Konsequenzen

Auf Stufe Bund werden für die 2. Etappe bis zur nächsten Information des Bundesrates keine zusätzlichen finanziellen Ressourcen benötigt. Die geplanten Forschungsvorhaben werden im Rahmen der bestehenden Forschungskredite abgewickelt. Dabei ist auch zu prüfen, inwiefern Mittel des Nationalfonds und des 7. Forschungsrahmenprogramms der EU (Sicherheit) genutzt werden können.

9.5 Orientierung des Bundesrates

Das VBS informiert den Bundesrat bis im Frühjahr 2009 anhand eines Berichts über die Ergebnisse der zweiten Etappe sowie über das weitere Vorgehen.

Anhang 1 Aktivitäten anderer Staaten zum Schutz Kritischer Infrastrukturen

Seit Mitte der 1990er Jahre befassen sich viele Staaten vermehrt mit dem Schutz Kritischer Infrastrukturen. Im Folgenden wird anhand einiger Beispiele dargestellt, wie andere Staaten dieses Thema bearbeiten.

USA
Die sicherheitspolitische Debatte zur Bedeutung ziviler Kritischer Infrastrukturen begann Mitte der 90er Jahre in den USA. Die bis anhin vorwiegend unter militärischen und wirtschaftlichen Gesichtspunkten geführte Diskussion über den Schutz von Infrastrukturen wurde nun aus einer ganzheitlichen sicherheitspolitischen Betrachtungsweise vorangetrieben. Einer der wichtigsten Meilensteine war 1996 die Einsetzung der *Presidential Commission on Critical Infrastructure Protection* (PCCIP) durch den damaligen Präsidenten Bill Clinton. Es handelte sich um den ersten sicherheitspolitischen Schritt auf Bundesebene, der den Schutz Kritischer Infrastrukturen zum Ziel hatte und dabei besonders die Relevanz von Informationstechniken hervorhob. Der physische Schutz stand nicht unbedingt im Vordergrund der Überlegungen.
Dies änderte sich 2001. Die Terroranschläge vom 11. September 2001 verdeutlichten die physische Verwundbarkeit der USA gegenüber Anschlägen. Der Schutz Kritischer Infrastrukturen wurde von da an vor allem unter den Gesichtspunkten "Homeland Security" und "Schutz vor Terroranschlägen" gesehen. Im Februar 2003 veröffentlichte die US-Regierung das Dokument *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Diese Strategie hat den umfassenden, physischen Schutz Kritischer Infrastrukturen in den USA zum Ziel. Der Wirbelsturm Katrina, welcher die Region von New Orleans in September 2005 verwüstete, zeigte die Verwundbarkeit und mangelnde Vorbereitung gegenüber von Naturgefahren auf. Im Juni 2006 wurde der Bericht *National Infrastructure Protection Plan* veröffentlicht. Darin werden 17 Kritische Infrastrukturen und Schlüssel-Ressourcen aufgeführt.

Kanada
In Kanada bildete der Jahrtausendwechsel den Ausgangspunkt für die Anstrengungen zum Schutz Kritischer Infrastrukturen. Es wurde eine umfassende Risikoanalyse durchgeführt, um die Kritikalität der Infrastrukturen zu erfassen. 2003 wurde das "Department of Public Safety and Emergency Preparedness Canada" (PSEPC) eingereichtet. Das Ministerium koordiniert Ministerien und Behörden, die sich mit Teilaspekten zur Wahrung nationaler Sicherheit befassen. Im Sinne eines partnerschaftlichen Modells arbeitet das PSEPC eng mit weiteren staatlichen Akteuren (inkl. den Provinzen und Territorien) und der Privatwirtschaft zusammen.
In der ersten umfassenden Berichterstattung zur nationalen Sicherheit, hob die kanadische Regierung die Bedeutung des Schutzes Kritischer Infrastrukturen hervor. Das PSEPC hat Ende 2006 einen Entwurf zu einer *National Strategy for Critical Infrastructure Protection* erstellt. Zusätzlich wurden mehrere wissenschaftliche Forschungsprojekte zum Thema der Interdependenzen von Kritischen Infrastrukturen lanciert.

Norwegen
Im September 2003 wurde in Norwegen das Direktorat für Zivilschutz und Notfallvorsorge gegründet (DSB), das dem Ministerium für Justiz und Polizei untersteht. Es koordiniert Massnahmen zum Schutz kritischer Einrichtungen in Kooperation mit anderen Akteuren. Grundsätzlich haben die zuständigen Ministerien die Verantwortung in ihren Bereichen sowohl in normalen wie auch in Krisenzeiten. Für eine umfassende Bewertung der Kritischen Infrastrukturen setzte die norwegische Regierung Ende 2004 eine Kommission ein, welche aus Vertretern verschiedener Infrastruktursektoren besteht. Die Kommission hat ihren Abschlussbericht dem Ministerium für Justiz und Polizei im April 2006 vorgelegt.

Deutschland
In Deutschland lag der Fokus lange Zeit hauptsächlich auf dem Schutz Kritischer Informationsinfrastrukturen. Im Rahmen des deutschen Anti-Terror-Paktes erhielt das Bundesamt für Sicherheit in der Informationstechnik (BSI) finanzielle und personelle Ressourcen. Im BSI analysierte man bis zu den Terroranschlägen vom 11. September 2001 neben den IT- auch die physischen Bedrohungen auf kritische Infrastrukturen. Im Jahr 2004 begann sich das "Monopol" des BSI zu lockern. Im neu gegründeten Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) wurde ein Zentrum Schutz Kritischer Infrastrukturen gegründet, welches sich den physischen Aspekten des Schutzes Kritischer Infrastrukturen widmet. Das Bundeskriminalamt (BKA) wiederum setzt sich mit dem Schutz vor Terroranschlägen und anderen Fragen der Strafverfolgung auseinander. Alle drei Ämter sind Teil des Bundesinnenministerium (BMI).
In Deutschland fehlte bis 2005 eine nationale Strategie für den Schutz Kritischer Infrastrukturen. Für den Bereich der Informationsinfrastrukturen veröffentlichte das BMI den *Nationalen Plan zum Schutz von Informationsinfrastrukturen (NPSI)*. Mit dem Dokument *Schutz Kritischer Infrastrukturen – Basisschutzkonzept* erhielten Unternehmen einen Leitfaden, um ihre Infrastrukturen vor natürlichen Ereignissen ebenso wie vor Terroranschlägen zu schützen. Die staatlichen Institutionen arbeiten verstärkt mit der Wirtschaft zusammen.

Niederlande
In den Niederlanden ist der Schutz Kritischer Infrastrukturen ein wichtiger Bereich der nationalen Sicherheit. Nach den Terroranschlägen vom 11. September 2001 in den USA wurde das niederländische Innenministerium beauftragt, eine umfassende Analyse und Massnahmenplanung vorzunehmen. IT- und physische Aspekte wurden dabei gleichermassen betrachtet. Während der so genannten „Quick Scan Phase“ (2002-2003) wurden insgesamt 11 Infrastruktursektoren und bestehende Interdependenzen untersucht, mittlerweile werden 12 Sektoren als kritisch bewertet. In der nächsten Phase wurden zwischen 2004 und 2005 in jedem Sektor Knotenpunkte und deren geografisch Lage identifiziert, die für das Funktionieren der jeweiligen Sektoren wichtig sind. In der Folge wurden einige Massnahmen zur Verbesserung des Schutzes Kritischer Infrastrukturen ausgearbeitet, welche im September 2005 dem Parlament vorgelegt wurden. Seit 2004 koordiniert das Direktorat für Krisenmanagement, das zum Innenministerium gehört, die Umsetzungsarbeiten. Dabei wird auch eng mit der Privatwirtschaft zusammen gearbeitet.

Schweden
Mitte der 1990er Jahre wurde im Rahmen einer Neubetrachtung der Gesamtverteidigung die Bedrohungslage für Schweden beurteilt. Dabei stellte die Identifikation von Risiken der Informationskriegsführung ein erster Schritt im Zusammenhang der kritischen Infrastrukturen dar. Ende der Neunzigerjahre wurde eine hochrangige Kommission eingesetzt, die sich mit den Verwundbarkeiten und dem Schutz Schwedens befasste. 2001 schlug diese Kommission in ihrem Schlussbericht u.a. Massnahmen zum Schutz Kritischer Infrastrukturen vor. Der Schutz Kritischer Infrastrukturen wird als integrale Aufgabe zur Gewährleistung der nationalen Sicherheit verstanden. Die Initiativen im Bereich des Infrastrukturschutzes gehen in Schweden hauptsächlich von staatlicher Seite aus. Die führende Rolle hatte hierbei die Swedish Emergency Management Agency (SEMA), das schwedische Amt für Notfallplanung, welches 2002 gegründet wurde. In den Richtlinien im Bereich Notfallplanung für 2006 und 2007 wurde die Bedeutung des Schutzes Kritischer Infrastrukturen besonders hervorgehoben sowie Priorität auf Vorsorge-Massnahmen gelegt.

Europäische Union
Viele Jahre lag die Europäische Union (EU) beim Schutz Kritischer Infrastrukturen hinter den Einzelstaaten zurück. Nach ersten Initiativen wie der *Information Infrastructure Dependability Support Initiative (DDSI)* im Jahr 2002 befasst sich die EU mittlerweile weitaus stärker mit dem Thema. Dies resultiert zu einem gewissen Mass auch aus den Erfahrungen der Terroranschläge in den USA. Im Oktober 2004 kündigte die Europäische Kommission den

Start des *European Programme for Critical Infrastructure Protection (EPCIP)* an. Teil dieses Programms sind die Errichtung eines EU *Critical Infrastructure Warning Information Network (CIWIN)*, um die Mitgliedsstaaten bei ihren Vorhaben zum Schutz kritischer Infrastrukturen zu unterstützen sowie die Entwicklung spezifischer Standards durch das European Committee for Standardization (CEN) voranzutreiben. In Anwendung des Subsidiaritätsprinzips soll die EU ihre Bemühungen auf den Schutz von kritischen Infrastrukturen mit grenzüberschreitender Wirkung konzentrieren und die übrigen Infrastrukturen der alleinigen Verantwortung der Mitgliedsstaaten überlassen. Ziel des von der EU-Kommission initiierten Programms ist es, die Kapazitäten zum Schutz Kritischer Infrastrukturen in Europa zu steigern. Berücksichtigt werden alle Gefahren ("all hazards approach"-Ansatz), obwohl der Fokus auf dem Schutz gegen Terroranschläge liegt. Um das Programm voran zu bringen, veröffentlichte die EU im November 2005 ein Grünbuch zu EPCIP. Ziel war es, möglichst viele Akteure in die Diskussion über das europäische Programm zum Schutz Kritischer Infrastrukturen einzubeziehen. Das Grünbuch stellt Optionen vor, wie die Kommission der Aufforderung des Rates zur Ausarbeitung eines detaillierten europäischen Programms für den Schutz Kritischer Infrastrukturen nachkommen kann. Nach verschiedenen Konsultationen (woran die Schweiz teilgenommen hat) wurde Dezember 2006 eine Kommunikation und eine Direktive durch die EU-Kommission verabschiedet. Die Kommunikation legt den Rahmen für den Schutz Europäischer Kritischer Infrastrukturen fest während die Direktive die Identifikation sowie die Risikoanalyse der Europäischen Kritischen Infrastrukturen regelt. Nach offiziellen Konsultationen bei den Mitgliederstaaten sollen die zwei Dokumente voraussichtlich Mitte 2007 durch den Europäischen Rat verabschiedet werden.

Infrastruktur	**USA**	**CDN**	**N**	**D**	**NL**	**EU**	**CH**
Energie	X	X	X	X	X	X	X
Finanzen	X	X	X	X	X	X	X
Gesundheit	X	X	X	X	X	X	X
Information- und Kommunikationstechnologie	X	X	X	X	X	X	X
Lebensmittel	X	X	X	X	X	X	X
Transport	X	X	X	X	X	X	X
Wasser	X	X	X	X	X	X	x
Regierung und Verwaltung	X	X	X	X	X		X
Chemische Industrie	X	X		X	X	X	X
Notfall- und Rettungswesen	X	X	X	X			X
Kulturgüter	X	X		X			x
Post	X				X		x
Landwirtschaft	X	X					
Verteidigung			X		X		x
Rüstungsindustrie	X	X					
Forschung				X		X	x

Tabelle A1.1: Vergleich der Kritischen Infrastruktursektoren in ausgewählten Ländern
(X bezeichnet Infrastruktursektoren;
x bezeichnet Teilsektoren in der Schweiz (siehe Tabelle 1 im Haupttext))

Die obige Tabelle zeigt, dass es zwischen den Ländern unterschiedliche Auffassungen gibt, welche Infrastrukturen als kritisch zu betrachten sind. Diese Unterschiede lassen sich u.a. aufgrund geographischer Begebenheiten, wirtschaftlicher und politischer Ausprägung und historischen und kulturellen Erfahrungen erklären. Gemeinsam ist jedoch, dass sie allesamt die sieben Bereiche Energie, Finanzen, Gesundheit, Informations- und Telekommunikationstechnologie, Lebensmittel, Transport sowie Wasser (in der Schweiz den Sektoren Nahrung und Entsorgung zugeteilt) zu den Kritischen Infrastrukturen zählen.

Tendenziell kann festgestellt werden, dass unter dem Eindruck der Anschläge vom 11. September 2001 die Zahl der Infrastrukturen, die als kritisch bewertet werden, deutlich zugenommen hat. In den USA wurden 1998 fünf Infrastruktursektoren als kritisch eingestuft. 2006 stieg die Zahl auf 17 Kritischen Infrastrukturen und Schlüssel-Ressourcen.

Anhang 2 Schutz Kritischer Infrastrukturen in der Schweiz - Relevante Stellen des Bundes

Im Folgenden werden Grundaufgaben und konkrete Aktivitäten im Bereich Schutz Kritischer Infrastrukturen einiger Bundesstellen aufgeführt. Die Auflistung dient der Illustration und ist nicht abschliessend. Sie widerspiegelt die in der AG SKI vertretenen Ämter und führt sie gemäss Staatskalender auf.

Politisches Sekretariat
Das Politische Sekretariat (POLS, ehemals Zentrum für Internationale Sicherheitspolitik (ZiSP)) befasst sich im Rahmen seiner allgemeinen Zuständigkeit für aussensicherheitspolitische Fragen mit dem Schutz Kritischer Infrastrukturen. Seit 2003 organisiert es im Rahmen des euro-atlantischen Partnerschaftsrats (EAPC) internationale Workshops zu CIP und Civil Emergency Planning, welche nationalen und internationalen Experten aus Verwaltung, Wirtschaft und Wissenschaft als wichtige Plattform des Informationsaustausches dient. Das POLS ist in der ad hoc CIP Working Group des Civil Protection Committee der EAPC und CIP Point of Contact bei der EU (zusammen mit dem BABS) vertreten.

Direktion für Entwicklung und Zusammenarbeit
Die Direktion für Entwicklung und Zusammenarbeit (DEZA) betreibt selbst keine kritischen Infrastrukturen. Die Humanitäre Hilfe hat den Auftrag global mit Vorbeugungs- und Nothilfemassnahmen zur Erhaltung gefährdeten menschlichen Lebens sowie zur Linderung von Leiden beizutragen. Im Umgang mit kritischen Infrastrukturen im Ausland verfügt die DEZA über eine langjährige Erfahrung in der Nothilfe und im Wiederaufbau nach Natur- (Erdbeben, Überschwemmungen oder Dürren) und technologischen Katastrophen (nukleare, biologische und chemische Ereignisse) sowie bei Dammbrüchen und anderen massiven und akuten Zerstörungen in Krisen und Konflikten.

Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz)
Das Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz) erbringt – neben allgemeinen Leistungen für die Öffentlichkeit – für zivile und militärische Einsatzorganisationen Dienstleistungen zur Lagebeurteilung. Unter anderem wird vor Gefahren des Wetters gewarnt, die Überwachung der Radioaktivität in der Atmosphäre sichergestellt und im Ereignisfall die Berechnung der Ausbreitung von Schadstoffen durchgeführt. In besonderen und ausserordentlichen Lagen werden im Rahmen des Koordinierten Bereiches Wetter alle notwendigen Dienstleistungen in Zusammenarbeit mit den Wetterdiensten der Luftwaffe und der Artillerie erbracht. MeteoSchweiz verstärkt derzeit seine Bemühungen, die Aufgabenerfüllung in allen Lagen zu gewährleisten. Zu diesem Zweck wurde eine Projektvoranalyse unter dem Titel *Business Continuity Management (BCM)* erstellt. Erste Massnahmen werden sofort umgesetzt, weitere voraussichtlich im Rahmen eines Projektes ab 2009 angegangen.

Bundesamt für Gesundheit
Die Arbeitsgruppe Influenza des Bundesamts für Gesundheit (BAG) hat einen Pandemieplan für die Schweiz erstellt. Ziel dieses Plans ist es, beim Ausbruch einer Pandemie existenziell notwendige Dienste wie Transport, Kommunikation, Information und Versorgung mit Energie, Trinkwasser und Nahrungsmitteln genügend leistungsfähig zu erhalten, sowie durch gezielte Impfungen bei Polizei, Feuerwehr und beim Gesundheitspersonal Schlüsselfunktionen der Schweiz zu gewährleisten. Später soll dazu eine Prioritätenliste von Impfstoffempfängern erstellt werden, die sowohl die medizinische als auch die gesellschaftlich-politische Ebene berücksichtigt. Dies betrifft auch Betreiber von Kritischen Infrastrukturen. Der Bundesrat hat 2006 den Kauf von acht Millionen Dosen eines Präpandemie-Impfstoffes beschlossen. Ein Konzept für eine Massenimpfung ist in Erarbeitung.

Bundesamt für Polizei
Die Tätigkeiten des Bundesamtes für Polizei (fedpol) umfassen vorbeugende Aufgaben wie den präventiven Staatsschutz und Sicherheitsmassnahmen zum Schutz gefährdeter Personen und Objekte. Andererseits nimmt das Amt auch Aufgaben im Bereich der Strafverfolgung wahr. Im Rahmen der Melde- und Analysestelle Informationssicherung (MELANI) ist das fedpol für den Schutz der kritischen Informationsinfrastrukturen zuständig. MELANI arbeitet eng mit ausgewählten Betreibern von nationalen kritischen Infrastrukturen zusammen. Im Rahmen der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) koordiniert das fedpol die Strafverfolgung im Bereich der Internetkriminalität, welche für den Schutz kritischer Informationsinfrastrukturen eine zentrale Rolle spielt.

Informations- und Objektsicherheit, Stab Chef der Armee
Die Informations- und Objektsicherheit (IOS), Stab Chef der Armee, VBS, bearbeitet diverse Belange der Integralen Sicherheit. Sie liefert dabei Beiträge zur militärischen Sicherheit, aber auch zur Sicherheit der Verwaltung im Inland und teilweise auch im Ausland. Basierend auf kurz-, mittel- und langfristigen Bedrohungsanalysen erarbeitet sie Grundlagen, Vorgaben und Massnahmen in allen Sicherheitsbereichen (Personen, Informationen, Sachwerte und Umwelt) und kontrolliert deren Umsetzung. Sie trägt wesentlich zur systematischen Umsetzung einer optimalen Sicherheitsstrategie bei und hat dabei den Einbezug aller Aspekte der Sicherheit (Security bis Waffenschutz) und über alle Lagen im VBS sicherzustellen. Diese Aufgabe wird durch eine enge Zusammenarbeit mit entsprechenden Stellen des Bundes, der Kantone und Gemeinden, aber auch mit ausländischen Fachstellen sichergestellt.

Führungsstab der Armee
Seit rund 15 Jahren katalogisiert der Territorialdienst in Zusammenarbeit mit den kantonalen Führungsstäben und verschiedenen Bundesämtern die Infrastrukturen von nationaler und regionaler Bedeutung und erstellt einen Katalog der zivilen Objekte zur Sicherstellung existenzieller Bedürfnisse (SEB). Die darin enthaltenen Objektlisten mit rund 700 Objekten dienen den zivilen Partnern als Führungs- und Entscheidungsgrundlage für die Gesuchstellung an den Bundesrat zur subsidiären Unterstützung im Objektschutz durch die Armee. Die katalogisierten Objekte sind nur aus der Sicht von aktiven Gefahren erfasst, d.h. von Gewalteinwirkungen und Inbesitznahme durch terrestrisch vorgetragene Aktionen sowie vor Sabotage. Passive Gefahren wurden bei der Erfassung der Objekte ausgeklammert.
Die Informationsoperationen befassen sich ebenfalls mit der Sicherheit kritischer Infrastrukturen, weil diese für die Sicherstellung des Entscheidfindungsprozesses der Armee wie auch für die von der Armee abhängigen Instanzen zentral sind. Dieser Bereich befasst sich nicht nur mit den physischen Problemstellungen, sondern auch mit allen damit verbundenen relevanten psychologischen und kybernetischen Aspekten. Dazu wurde eine nicht frei verfügbare "Konzeptionsstudie Information Operations" erarbeitet.

armasuisse Immobilien
armasuisse Immobilien führt als Immobilienkompetenzzentrum des VBS das Immobilienmanagement VBS, nimmt die Rolle des Eigentümervertreters wahr und stellt eine moderne Immobilienbewirtschaftung mit hoher Wertschöpfung sicher. Da im Portfolio auch die Verteidigungsinfrastruktur der Armee enthalten ist, sorgt armasuisse Immobilien mit der Studiengruppe Schutz Infrastruktur Militär (SG SIM) im Auftrag des Chefs der Armee und des Rüstungschefs für die Sicherstellung der Grundlagen für Schutzbauten und geschützte Anlagen der Armee.

Bundesamt für Bevölkerungsschutz
Die gesetzlichen Grundlagen des Bevölkerungsschutzes, insbesondere die Konkretisierung der Zielsetzung "Schutz der Bevölkerung und ihrer Lebensgrundlagen", sind im Zusammenhang mit Kritischen Infrastrukturen relevant. Im Herbst 2003 erarbeitete das Bundesamt für Bevölkerungsschutz (BABS) als Arbeitsgrundlage die Konzeptionsstudie "Schutz und Sicherheit von Kritischen Infrastrukturen". Das BABS koordiniert die

interdepartementale Arbeitsgruppe Schutz Kritischer Infrastrukturen (AG SKI), ist CIP Contact Point bei der EU (zusammen mit dem POLS) und vertritt die Schweiz im Civil Protection Committee der EAPC, welche sich ebenfalls mit CIP-Aspekten befasst.
Die Nationale Alarmzentrale (NAZ) ist ein Geschäftsbereich des BABS. Sie spielt eine wesentliche Rolle bei der Bewältigung von schweren Ereignissen, die Auswirkungen auf kritische Infrastrukturen haben können. Im Rahmen der Erdbebenübung "RHEINTAL 06" wurde u.a. die Katastrophenbewältigungskapazität von kritischen Infrastrukturen (Telekom, Gas-, Strom- und Lebensmittelversorgung) beübt.

Informatikstrategieorgan Bund
Das Informatikstrategieorgan Bund (ISB) gehört zum Generalsekretariat des Finanzdepartements und ist Stabsorgan des Informatikrats Bund (IRB). Es ist unter anderem für die Vorgaben und Weisungen des Bundes in Sachen Informationssicherheit zuständig. Eine zentrale Stellung nimmt das ISB im Bereich des Schutzes kritischer Informationsinfrastrukturen ein. So war es massgeblich an der Ausarbeitung des Einsatzkonzepts Information Assurance Schweiz beteiligt. Das ISB ist zuständig für die strategische Leitung der Melde- und Analysestelle Informationssicherung (MELANI) sowie des Sonderstabs Information Assurance (SONIA).

Bundesamt für Informatik und Telekommunikation (BIT)
Die in der Verantwortung des BIT liegenden Infrastrukturen der Informations- und Kommunikationstechnologien (IKT) werden bezüglich Verfügbarkeit, Vertraulichkeit und Integrität breit geschützt. Die Weisung über die Informatiksicherheit in der Bundesverwaltung (WIsB) definiert den Grundschutz, welcher in jedem Fall einzuhalten ist. Darüber hinaus werden bei erhöhtem Schutzbedarf mit einzelnen Kunden spezielle Massnahmen beispielsweise zur Katastrophenvorsorge vereinbart. Die physische Sicherheit wird durch ein Zutritts- und Schliesskonzept mit verschiedenen Sicherheitsstufen umgesetzt. Die Versorgungssicherheit wird soweit möglich mit redundanten Anbindungen oder Reserveaggregaten sichergestellt. Netzwerksicherheit bieten die Firewall- und Proxy-Infrastrukturen, ein effizienter Viren- und Spamschutz und eine fortlaufend verbesserte Segmentierung des Netzwerkes. Sicherheitsvorgaben und Standards sorgen auf System- und Datenbankebene für gehärtete Systeme, deren Umsetzungsgrad mittels Schwachstellenprüfungen zudem periodisch geprüft wird. Erprobte Backup-Konzepte bieten Datensicherheit im Desasterfall. Ein vollwertiger Backup-Standort für das Rechenzentrum des BIT wie auch für andere IKT-Leistungserbringer der Bundesverwaltung befindet sich im Aufbau.

Bundesamt für Bauten und Logistik
Das Bundesamt für Bauten und Logistik (BBL) ist für die räumliche Unterbringung der zivilen Bundesverwaltung zuständig. Bezüglich des Schutzes Kritischer Infrastrukturen achtet das BBL bei Neubauten darauf, dass die jeweils geltenden Erdbebennormen eingehalten werden. Bei Umbauten und Sanierungen werden Schutzmassnahmen bez. Erdbebensicherheit unter der Berücksichtigung der Verhältnismässigkeit der Kosten getroffen. Bei Bauprojekten werden die Sicherheitsanforderungen (Security-Aspekte) mit einem Sicherheitskonzept und detaillierten Massnahmen umgesetzt. Diese stützen sich auf die vom Bundessicherheitsdienst erstellte Risikoanalyse und den Schutzzielen.

Bundesamt für wirtschaftliche Landesversorgung
Das Bundesamt für wirtschaftliche Landesversorgung (BWL) konzentriert seine Versorgungsanstrengungen auf die Bewältigung kurz- und mittelfristiger sektorieller Störungen in den Grundversorgungsbereichen Ernährung, Energie und Heilmittel sowie auf die Infrastrukturbereiche Transporte, Industrie und IKT-Infrastruktur. Primäres Ziel ist es, das Marktangebot bei lebenswichtigen Gütern mittels "Angebotslenkungsmassnahmen" grundsätzlich während sechs Monaten auf einem Niveau von 100 % aufrechtzuerhalten, so insbesondere durch (1) die Freigabe von Pflichtlagern, (2) die Förderung des Imports und (3) Produktionslenkungsmassnahmen. Nach sechs Monaten kann eine hundertprozentige

Marktversorgung unter Umständen nicht mehr gewährleistet werden. In diesem Fall sollen Handel und Konsum durch "Nachfragelenkungsmassnahmen" (Kontingentierung, Rationierung oder ähnliche Massnahmen) eingeschränkt werden können.

Bundesamt für Verkehr
Das BAV ist unter anderem verantwortlich für die Gewährleistung der Verkehrssicherheit im Schienen-, Seilbahn-, Schiffs- und Automobilverkehr, insbesondere durch die Aufsicht über Betrieb, Anlagen und Fahrzeuge der Unternehmungen des öffentlichen Verkehrs. Das BAV ist zudem verantwortlich für die Gewährleistung der Einheit des Rheinregimes im Bereich der technischen und der sicherheitspolitischen Vorschriften im Rahmen der internationalen Zusammenarbeit. Es bereitet die Entscheidungen für eine kohärente Politik im Bereich des öffentlichen Verkehrs, mit Ausnahme der Luftfahrt und des Strassenbaus, sowie im Bereich der Binnenwasserstrassen und der Grossschifffahrt in Verbindung mit dem Meer vor und setzt sie um.
Das BAV führt die Koordination des Verkehrswesens im Ereignisfall (KOVE). Ziel der KOVE ist die Nutzung der Verkehrsinfrastrukturen und Mittel im Hinblick auf Ereignisfälle so abzustimmen, dass nach deren Eintreten ein geregelter Verkehrsablauf gewährleistet werden kann.
Der Direktor BAV ist Vorsitzender des gemischten Ausschusses Landverkehrsabkommen Schweiz / EG. Das BAV vertritt als Gast auf der Fachebene die Schweizer Interessen bezüglich kritischer Infrastrukturen im Landtransport in einer Expertengruppe der EU.

Bundesamt für Energie
Das Bundesamt für Energie (BFE) ist unter anderem zuständig für die Energiegesetzgebung und für Bewilligungsverfahren für Kernanlagen, Hochspannungsleitungen sowie Erdgas- und Erdölpipelines. Die Sektion "Kernenergie" überwacht die Umsetzung der Verpflichtungen der Schweiz im Bereich Kernbrennstoffkreislauf sowie den Schutz von Kernanlagen und Kernmaterialien vor Sabotage. Die BFE-Abteilung "Wasserkraft und Talsperren" befasst sich mit der Nutzbarmachung der Wasserkraft und ihrer Regelung bei den Grenzgewässern und der technischen sowie betrieblichen Sicherheit der Stauanlagen in der Schweiz. Eine vom UVEK eingesetzte Arbeitsgruppe hat im März 2003 ein Paket von Massnahmen zur Verbesserung der Netzstrukturen im Höchstspannungsbereich präsentiert. Damit sollen künftige Blackouts in der Schweiz möglichst vermieden werden.

Bundesamt für Strassen
Das Bundesamt für Strassen (ASTRA) ist die Schweizer Fachbehörde für die Strasseninfrastruktur und den individuellen Strassenverkehr. Es erarbeitet Grundlagen für die nachhaltige Verkehrspolitik des Bundes und entwirft und koordiniert entsprechende Massnahmen auf nationaler und internationaler Ebene. Es sorgt für den Bau, Betrieb und Unterhalt eines sicheren und leistungsfähigen Strassennetzes von nationaler Bedeutung. Im Rahmen eines organisationsweiten Risikomanagements erfolgt die Erfassung und Bewertung der Risiken. Eine Priorisierung der Reduktionsmassnahmen erfolgt mit der Abwägung der Kosten mit dem zu erwartenden Nutzen.

Bundesamt für Kommunikation
Das Bundesamt für Kommunikation (BAKOM) beschäftigt sich im Rahmen seiner Funktion als Aufsichts- und Regulierungsbehörde u.a. mit Fragen der Sicherheit der Informations- und Kommunikationsinfrastruktur sowie mit Fragen des Schutzes Kritischer Infrastrukturen. Hervorzuheben sind v.a.:

- Berichte über die Sicherheitsinteressen der Schweiz an Rundfunk- und Telekommunikationsinfrastrukturen in ausserordentlichen Lagen.
- Mit-Initiant des Roundtable des Vereins Infosurance zum Thema sektorspezifische Risikoanalyse im Bereich Telekommunikation.

Der interdepartementale Ausschuss Informationsgesellschaft (IDA IG) unter Vorsitz des BAKOM hat zwischen 2004 und 2006 die Strategie für eine Informationsgesellschaft in der Schweiz überarbeitet und im Januar 2006 veröffentlicht. Dabei werden als Massnahmen insbesondere 'Sicherheit und Vertrauen' genannt.

Bundesamt für Umwelt

Das Bundesamt für Umwelt (BAFU) hat den Auftrag, den Schutz der Menschen und grosser Sachwerte vor Naturgefahren sowie die Sicherstellung der Trinkwasserversorgung und den Schutz der Umwelt sicherzustellen (Wasserbaugesetz, Waldgesetz, Gewässerschutzgesetz, Umweltschutzgesetzgebung) und übt die Oberaufsicht über die Störfallvorsorge (Störfallverordnung) aus. Dem BAFU obliegt im Bereich Schutz vor Naturgefahren die strategische Führung, gleichzeitig fördert es Schutzmassnahmen und stellt Grundlagen von nationalem Interesse zur Verfügung. Das BAFU erarbeitet und betreut die entsprechende Gesetzgebung auf Bundesebene. Es stellt gesamtschweizerisch einen vergleichbaren Schutz vor Naturgefahren sicher. Neben Hochwasser, Lawinen, Steinschlag, Fels- und Bergstürzen stellen starke Erdbeben ein nicht vernachlässigbares Risiko dar. Auch Trockenheit, Hitze- und Kältewellen können den Lebensraum und Infrastrukturen betreffen.
Vor Extremereignissen gibt es keinen absoluten Schutz. Im Rahmen eines integralen Risikomanagements kommt der Reduktion der Verletzlichkeit von Bauten und Anlagen eine hohe Bedeutung zu (Objektschutz). Den Grossrisiken, welche hohe Schäden verursachen, und dem Schutz der kritischen Infrastrukturen muss im Rahmen der Differenzierung der Schutzziele Rechnung getragen werden.

Anhang 3 Chronologie der Entwicklungen in der Schweiz

In der Schweiz wurde der Begriff "Schutz Kritischer Infrastrukturen" bis etwa 2002 nicht in einem umfassenden Sinn verwendet. Es wurden jedoch bereits vorher diverse Projekte und Massnahmen in Teilbereichen lanciert. Dies geschah allerdings oftmals unter anderen Bezeichnungen und vor allem wenig koordiniert.

Entwicklungen im Bereich Schutz Kritischer Infrastrukturen basierten in den letzten Jahrzehnten in der Schweiz u.a. auf den Anstrengungen des Militärs und des Zivilschutzes (z.B. Schutz militärischer Bauten bzw. Schutzräume gegen Waffenwirkungen), der KKW-Betreiber (baulich-technische und organisatorische Massnahmen), der Betreiber von Wasserkraftanlagen (Überprüfung der Sicherheit), der Polizei (Gebäudesicherheit) und anderer Organisationen.

In chronologischer Reihenfolge werden nachstehend einige wichtige Meilensteine aufgeführt:

1997: Strategische Führungsübung: Die Strategische Führungsübung ’97 der Strategischen Führungsausbildung (SFA) der Bundeskanzlei setzt einen wichtigen Akzent bei den Aktivitäten in der Schweiz. Die Übung hat u.a. aufgezeigt, dass Infrastrukturen und die Gesellschaft von der Sicherheit der Informationsinfrastruktur abhängig sind.

1998: Strategie für eine Informationsgesellschaft Schweiz: In einem Strategiepapier zur "Informationsgesellschaft Schweiz" fordert der Bundesrat, dass die Verfügbarkeit und Nutzung von Informationen auch in ausserordentlichen Lagen sichergestellt werden muss.

1998-1999: Konzept Information Assurance: Im Auftrag des Bundesrates erarbeitet die Koordinationsgruppe Informationsgesellschaft (KIG) das Konzept Information Assurance (IA). Es wird im Juni 2000 genehmigt. Das Konzept legt fest, dass (1) die damalige Stiftung InfoSurance vom Bund finanziell massgeblich unterstützt wird (vgl. weiter unten die Ausführungen zu InfoSurance), (2) die wirtschaftliche Landesversorgung einen Bereich Informations- und Kommunikationsinfrastrukturen (ICT-I) aufbaut und (3) ein Sonderstab Informationssicherheit gebildet wird (vgl. weiter unten Ausführungen zu SONIA).

2000: SIPOL B 2000: Der Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000) nennt explizit mögliche Bedrohungen für die Informatik- und Kommunikationsinfrastruktur der Schweiz.

2001: Übung Informo: Im Rahmen der Übung Informo 2001 werden unter der Führung der SFA die Krisenmanagement-Abläufe in den Bereichen Verkehr/Logistik, Energie, Telekommunikation, Verteidigung, Finanz- und Versicherungswesen und Medien beübt. Der Sonderstab Informationssicherheit (SONIA) wird dabei überprüft. Die Übung zeigt, dass ein partnerschaftlicher Ansatz zwischen Staat und Wirtschaft funktionieren kann.

2001: Bericht IKT-Sicherheitsinteressen in ausserordentlichen Lagen: Der Bericht des Bundesrates an die Sicherheitspolitischen Kommissionen der Eidgenössischen Räte "Sicherheitsinteressen der Schweiz an Rundfunk- und Telekommunikations-Infrastrukturen in ausserordentlichen Lagen" beinhaltet u.a. eine Risikoanalyse im Bereich der Informations- und Kommunikationstechnologien (IKT). Der Bericht wird von einer interdepartementalen Arbeitsgruppe unter der Leitung des BAKOM erarbeitet. Die Analyse führt zu konkreten Massnahmen im IKT-Bereich (z.B. Änderungen der Telecom Gesetzgebung) und beeinflusst spätere Arbeiten zum Thema (z.B. Infosurance Risikoanalyse des Sektors Telecom).

2002: InfoSurance: InfoSurance beginnt mit der sektorspezifischen Analyse von kritischen Infrastrukturen. Insbesondere die Informations- und Kommunikationstechnologieabhängigkeit und Vernetzungen zwischen den einzelnen Infrastrukturen stehen dabei im Zentrum.

2003: MELANI: Der Bundesrat beauftragt im Oktober das Informatikstrategieorgan Bund (ISB) zusammen mit den Betriebspartnern, dem fedpol (DAP) und der Stiftung SWITCH (SWITCH-CERT), eine Melde- und Analysestelle Informationssicherung (MELANI) aufzubauen. MELANI ist seit dem 1. Oktober 2004 operativ.

2003: Grobanalyse zum Schutz und zur Sicherheit Kritischer Infrastrukturen: Im Sommer/Herbst 2003 erarbeitet das Bundesamt für Bevölkerungsschutz (BABS) als Arbeitsgrundlage die Konzeptionsstudie "Schutz und Sicherheit von Kritischen Infrastrukturen". Dabei wird eine Methodik zur Identifikation und Beurteilung Kritischer Infrastrukturen entwickelt. Auf dieser Grundlage wird mit Experten aus verschiedenen Departementen und Bundesämtern eine Grobanalyse durchgeführt. Diese ergibt eine erste Identifikation von sechs kritischen Infrastruktursektoren (Regierung und Verwaltung, Stromversorgung, Kommunikation, Bevölkerungsschutz, Gesundheitsversorgung, Verkehr und Logistik) und von fünf relevanten Szenarien / Gefährdungsannahmen (Erdbeben, erhöhte Radioaktivität, flächendeckende Gesundheitsgefährdung, Ausfall grosser Teile der Informationsinfrastruktur und Extremismus / Terrorismus).

2004: Bericht Erdbebenvorsorge und Lifelines: Der Bericht "Erdbebenvorsorge und Lifelines" des Bundesamt für Umwelt (BAFU) identifiziert die überlebenswichtigen "Lebensadern" (Lifelines), deren Funktion zur Bewältigung eines starken Erdbebens in der Rettungs- und Bewältigungsphase unbedingt erforderlich ist und schlägt Schutzziele sowie entsprechende Massnahmen vor.

Anfang 2005: Risikomanagement des Bundes: Der Bundesrat beschliesst die Einführung eines systematischen Risikomanagements beim Bund. Der Fokus liegt schwergewichtig auf den Auswirkungen der Risiken auf den Bundeshaushalt. Mit der Umsetzung der Risikopolitik sind die Departemente und die Bundeskanzlei betraut. Das EFD (EFV) nimmt verschiedene administrative und koordinierende Aufgaben wahr und ist für die Formulierung und die Umsetzung der Versicherungspolitik des Bundes verantwortlich.“

2005: Als Folge der Unwetter im August 2005 hat der Bundesrat das BABS in Zusammenarbeit mit der PLANAT (Nationale Plattform Naturgefahren) beauftragt, planerische, organisatorische und technische Massnahmen zu prüfen, um Optimierungsmöglichkeiten für die Warnung und Alarmierung (OWARNA) zu erzielen. Dabei haben sich bezüglich der Redundanzen der eingesetzten Alarmierungsmittel und der Stromversorgung kritischer Infrastrukturen einige Schwachstellen gezeigt. Massnahmen sind vertieft zu analysieren.

2005: Koordination der SKI-Aktivitäten: Der Bundesrat beauftragt im Juni 2005 das BABS, die koordinative Leitung der schweizerischen Aktivitäten im Bereich Schutz Kritischer Infrastrukturen wahrzunehmen und in einer ersten Phase u.a. eine Übersicht der bisherigen Arbeiten zu erstellen, relevante Infrastruktursektoren zu identifizieren, ein Grundset an Gefährdungsszenarien darzulegen. Zur Unterstützung dieser Arbeiten wurde 2006 eine interdepartmentale Arbeitsgruppe eingerichtet.

2007: Evaluation MELANI: Aufgrund einer vom Center for Security Studies der ETH Zürich durchgeführten Evaluation entscheidet der Bundesrat am 24. Januar, die Melde- und Analysestelle Informationssicherung (MELANI) definitiv als Bundesstelle weiterzuführen und die dafür notwendigen personellen und finanziellen Ressourcen bereit zu stellen.