

MASTERPLAN Österreichisches Programm zum Schutz Kritischer Infrastruktur¹ (APCIP²)

A: Einleitung

1) Grundlagen und Ziele des Masterplans APCIP

Vor dem Hintergrund einer **zunehmenden Bedrohung durch terroristische Anschläge** sowie einer wachsenden **Abhängigkeit der Bevölkerung** von funktionierenden **Infrastrukturen** gewinnt der Schutz kritischer Infrastrukturen auch in Österreich immer mehr an Bedeutung.

Das Konzept der **Umfassenden Sicherheitsvorsorge**³ legt den Schutz kritischer nationaler Infrastrukturen als Querschnittsaufgabe nicht nur durch die Außen- und Verteidigungspolitik und die Maßnahmen zur „Inneren Sicherheit“, sondern darüber hinaus durch die Wirtschafts-, Landwirtschafts-, Gesundheits-, Verkehrs-, Infrastruktur- und Finanzpolitik sowie die Bildungs- und Informationspolitik fest. Das Programm zum Schutz kritischer Infrastrukturen ist somit voll inhaltlich in das Konzept der Umfassenden Sicherheitsvorsorge eingebettet. Das jährlich erstellte **Sicherheitspolitische Lagebild** unterstreicht ebenfalls die Bedeutung eines funktionierenden Schutzes kritischer Infrastrukturen.

Der Masterplan legt die Grundsätze, Verantwortlichkeiten und die einzelnen Arbeitsschritte zur Entwicklung eines **österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP)** fest und ist damit der Ausgangspunkt für den Umsetzungsprozess auf nationaler Ebene.

Der staatliche Gesamtprozess zur Implementierung und Umsetzung des Masterplans APCIP wird vom **Bundeskanzleramt gemeinsam mit dem Bundesministerium für Inneres unter Einbindung der betroffenen Bundesministerien, der Bundesländer sowie sonstiger Stakeholder** (WKÖ, BAK, zentrale Infrastrukturbetreiber, ...) koordiniert. Die Projektgruppe „Schutz kritischer Infrastruktur“ wurde beim Bundeskanzleramt eingerichtet und hat den Auftrag übernommen, den Masterplan und das österreichische Programm zum Schutz kritischer Infrastrukturen zu erarbeiten.

Der vorliegende Masterplan soll dazu beitragen, das Bewusstsein für das vorhandene Risiko auf allen relevanten Ebenen zu schaffen, die Attraktivität des **Wirtschaftsstandorts Österreich abzusichern** und möglichst **gleiche Wettbewerbsvoraussetzungen** herzustellen.

¹ „Schutz kritischer Infrastrukturen“ und der englische Begriff „Critical Infrastructure Protection“ werden im Masterplan als „Schutz und Sicherung kritischer Infrastrukturen“ verstanden, also in einem weiteren Begriffsfeld. Im Masterplan wird jedoch aus Vereinfachungsgründen nur der Begriff „Schutz“ verwendet.

² APCIP = Austrian Program for Critical Infrastructure Protection

³ Beschluss der Verbindungspersonen zum Nationalen Sicherheitsrates vom 9.10.2005

Ziel des Programms ist es, eine **umfassende Strategie und detaillierte Maßnahmen zum Schutz kritischer Infrastrukturen in Österreich festzulegen** und **die bisher von den zuständigen Ressorts und Infrastrukturbetreibern gesetzten Maßnahmen in ein gemeinsames Gesamtkonzept** zu stellen.

Im Rahmen dieses Programms werden nationale österreichische kritische Infrastrukturen (ACI)⁴ definiert, strategische Ziele festgelegt, Risikofaktoren und wesentliche Akteure beschrieben. Die erforderlichen **Maßnahmen** werden in einem **Aktionsplan** festgelegt und sollen durch eine periodische Evaluierung laufend den gegebenen Notwendigkeiten angepasst werden. Alle österreichischen kritischen Infrastrukturen sollen nach festgelegten Kriterien erfasst, eine Prioritätenreihung vorgenommen sowie die zu erreichenden Sicherungs- und Schutzstandards sowie die nötigen Schutzmassnahmen festgelegt werden.

Die „Optimierung der Sicherheit und der Schutz vernetzter Systeme (Infrastruktur)“ ist ein zentraler Schwerpunkt des nationalen Sicherheitsforschungsprogramms. Die Projekte der Sicherheitsforschung werden Analysen und wichtige Anregungen zur Verbesserung des Schutzes kritischer Infrastruktur liefern.

2) Europäisches Programm zum Schutz kritischer Infrastrukturen (EPCIP⁵)

Vor dem Hintergrund der Terroranschläge in Madrid im März 2004 beauftragte der Europäische Rat im Juni 2004 die Kommission mit der **Ausarbeitung einer umfassenden Strategie für den Schutz kritischer Infrastrukturen**. Die Absicht der Kommission, ein Europäisches Programm zum Schutz kritischer Infrastrukturen vorzulegen, wurde vom Rat im Dezember 2004 angenommen. In der Folge legte die Kommission im Dezember 2005 ein **Grünbuch** über ein Europäisches Programm für den Schutz kritischer Infrastrukturen⁶ vor, in dem verschiedene Optionen für ein solches Programm vorgestellt wurden.

Nach einem umfangreichen Konsultationsverfahren unter Befassung der Mitgliedstaaten und sonstiger Stakeholder legte die Kommission im Dezember 2006 eine **Mitteilung über ein Europäisches Programm für den Schutz kritischer Infrastrukturen**⁷ sowie einen Vorschlag für eine **Richtlinie des Rates über die Ermittlung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern**⁸ vor. Seit Anfang 2007 wird der Vorschlag der Richtlinie in der Ratsarbeitsgruppe PROCIV⁹ beraten. Parallel dazu wurde vom Rat ein spezielles Finanzprogramm für die Periode 2007 -2013 beschlossen.¹⁰

In der **Mitteilung der Kommission** wird insbesondere eine Vorgangsweise für die Ermittlung, Ausweisung und Schutz europäischer Kritischer Infrastrukturen vorgeschlagen. Darüber hinaus wird angeregt, dass **jeder Mitgliedstaat ein nationales Programm zum Schutz seiner kritischen Infrastrukturen erstellt**. In diesem Programm soll das von dem

⁴ ACI = Austrian Critical Infrastructure
ECI = European Critical Infrastructure

⁵ EPCIP = European Program for Critical Infrastructure Protection

⁶ Dok. 576/2005

⁷ Dok 786/2006

⁸ Dok 787/2006

⁹ Rats - Arbeitsgruppe Gruppe Protection Civile

¹⁰ Ratsentscheidung vom 12. Februar 2007, mit der für die Periode 2007 – 2013 ein spezielles Programm „Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks“ als Teil des allgemeinen Programms über Sicherheit und Bewahrung der Freiheiten, eingerichtet wird (2007/124/EG, Euratom) in OJ Nr. L 58/1 vom 24.2.2007

Mitgliedstaat verfolgte Konzept für den Schutz der auf seinem Hoheitsgebiet befindlichen kritischen Infrastrukturen dargelegt werden. Ferner sollen in dem nationalen Programm zumindest folgende Aspekte behandelt werden:

- Die **Ermittlung und Ausweisung kritischer nationaler Infrastrukturen** anhand vorgegebener nationaler Kriterien durch den betreffenden Mitgliedstaat.
- Schaffung eines **Dialogs mit den Eigentümern/Betreibern** kritischer Infrastrukturen.
- Ermittlung **geografischer und sektorspezifischer Abhängigkeiten**.
- Ausarbeitung von **Notfallplänen**.

Die Entwicklung des **Österreichischen Programms zum Schutz kritischer Infrastrukturen** (APCIP) soll so weit wie möglich mit dem EU Programm inhaltlich abgestimmt sein und Vorschläge der EU sowie schon bestehende Regelungen integrieren, um Doppelgleisigkeiten zu vermeiden. Dabei soll auch darauf geachtet werden, dass aus einer möglichen Verzögerung des europäischen Programms kein Nachteil für die Umsetzung des österreichischen Programms resultiert.

3) Bedeutung von Infrastrukturen für eine komplexe Gesellschaft

Eine komplexe Gesellschaft mit einem hohen Grad an **Arbeitsteilung** benötigt eine Vielzahl an Infrastrukturen unterschiedlichster Art, damit ihre Bürger an der Erstellung und der Nutzung von Gütern und Dienstleistungen teilnehmen können. Durch die intensiven Verflechtungen Österreichs in der EU, mit dem Rest Europas aber auch weltweit nützt und benötigt Österreich nicht nur Infrastrukturen innerhalb seines Staatsgebiets, sondern auch Infrastrukturen außerhalb seines Territoriums.

Der Grad der Interaktionen und Verknüpfungen wird auch in Zukunft weiter steigen, der Trend zur **Globalisierung** ist noch lange nicht abgeschlossen. Die verschiedenen Infrastrukturen ermöglichen erst den Austausch von Gütern und Dienstleistungen, sowohl in Österreich selbst als auch im internationalen Zusammenhang. Funktionierende Infrastrukturen tragen nicht nur wesentlich zur öffentlichen Sicherheit und zur staatlichen Stabilität bei, sondern werden für die BürgerInnen zum „Schlüssel“ für die Teilhabe am Wohlstand und an der Gesellschaft insgesamt.

4) Bedrohungslage und All-Hazard-Ansatz

Die Infrastrukturen sollen vor einem breiten Spektrum möglicher Risiken gesichert werden. Hauptansatzpunkt des APCIP ist es, ein Gesamtverständnis für die Interdependenzen innerhalb und zwischen den CIP-Sektoren sowie die damit verbundenen Risiken zu entwickeln. Die Maßnahmen sind aus einem **umfassenden Sicherheitsverständnis** abzuleiten und sollten daher das Risiko krimineller Akte und terroristischer Anschläge genauso berücksichtigen wie Naturgefahren und von Menschen verursachte Katastrophen bzw. technisches Versagen (All-Hazard-Ansatz). Der Schwerpunkt von APCIP liegt auf der Ausweisung bestimmter Unternehmen und öffentlicher Einrichtungen, die als potentiell gefährdet erkannt wurden, als nationale kritische Infrastrukturen.

Eine mangelnde Abstimmung der Unternehmensstrategien der verschiedenen Betreiber und Akteure der Infrastruktur, sowohl innerhalb eines Sektors selbst sowie zwischen den Sektoren, stellt ein weiteres Risiko für das reibungslose Funktionieren der Gütererstellung

und Leistungserbringung dar. Die verschiedenen Risikoquellen – von kriminellen Bedrohungen bis hin zum technischen Versagen - können diese Probleme zusätzlich verstärken.

Der Schwerpunkt des APCIP soll in der Unterstützung zur Implementierung eines Risikomanagements für ausgewählte Bereiche und Wirtschaftssektoren liegen. Maßnahmen der Prävention und Vorsorge stehen dabei im Vordergrund: der **Schwerpunkt liegt bei der „Verringerung der Verletzlichkeit“**.

Katastrophenhilfe und Zivilschutz hingegen gewährleisten einen Schutz vor allgemeinen Gefährdungen wie Erdbeben, Überflutungen, Bränden oder Lawinen. Im Rahmen des Staatlichen Krisen- und Katastrophenmanagements wurden auf Basis umfangreicher gesetzlicher Regelungen ausgereifte Strategien entwickelt. Diese Maßnahmen reichen von der Warnung und dem Einsatz bis zum Wiederaufbau: der Schwerpunkt liegt bei der „Begrenzung des Schadensausmaßes“. **Die Katastrophenhilfe sollte deshalb kein Arbeitsschwerpunkt im APCIP sein.**

Gleichzeitig muss jedoch darauf hingewiesen werden, dass Katastrophenhilfe und Schutz kritischer Infrastruktur in manchen Szenarien gleichzeitig betroffen sind und eine enge Wechselbeziehung dann eintritt, wenn Mittel der Katastrophenhilfe bei der Schadensbewältigung zum Schutz kritischer Infrastrukturen erforderlich sind.

5) Grundsätze

Die Konzeption von APCIP soll sich an folgenden Grundsätzen orientieren:

- **Subsidiarität:** Die Eigentümer und Betreiber kritischer Infrastruktur sind in erster Linie für die Aufrechterhaltung ihrer Geschäftsfähigkeit und den Schutz ihrer Anlagen und Einrichtungen selbst verantwortlich. Nur bei Betrieben, die als ACI eingestuft werden, entsteht ein nationales Interesse an ihrer Versorgungsfunktion. Deshalb sind Politik und Verwaltung für die Gestaltung der Rahmenbedingungen verantwortlich, damit ein klar definiertes Schutzniveau erreicht wird.
- **Komplementarität:** Bestehende Maßnahmen und Pläne sollen weiter genutzt und den neuen Bedrohungen angepasst werden.
- **Vertraulichkeit:** Informationen zu ACI sollen auf Basis von Vertraulichkeit ausgetauscht werden und nur in jener Informationstiefe vorliegen, die die jeweilige Aufgabenstellung erfordert.
- **Kooperation:** Die Zusammenarbeit aller Stakeholder von ACI, d.h. Unternehmen und Interessenverbände, öffentliche Verwaltung und Regulatoren, aber auch Normungsinstitute und Medien haben einen angemessenen Beitrag zur Entwicklung und Umsetzung von APCIP zu leisten.
- **Verhältnismäßigkeit:** Die Maßnahmen und Kosten zur Erhöhung des Schutzniveaus müssen in einem ausgeglichenen Verhältnis zum jeweiligen Risiko und zu den Möglichkeiten zur Gefahrenminderung stehen.

1) Definition österreichischer kritischer Infrastrukturen (ACI)

Komplexe Gesellschaften sind abhängig von der **Funktionsfähigkeit wichtiger Infrastruktur- und Versorgungseinrichtungen im In- und Ausland** und somit vielfältig verwundbar. Daher ist es vordringlich, bestimmte Einrichtungen und Leistungserstellungsprozesse als sensibel zu erkennen und besonders zu schützen. Daran sieht man auch, wie sehr bei dieser Frage innere und äußere Sicherheit ineinander übergehen und deshalb ihre Instrumente miteinander abgestimmt werden müssen.

Kritische Infrastrukturen sind jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben würde.

2) Liste der Sektoren der kritischen Infrastruktur auf europäischer Ebene und Ableitungen für Österreich

Im europäischen Programm werden 11 Sektoren kritischer Infrastrukturen angeführt:

- **Energie**
- **Nuklearindustrie**
- **IKT**
- **Wasser**
- **Lebensmittel**
- **Gesundheit**
- **Finanzen**
- **Transport**
- **Chemische Industrie**
- **Raumfahrt**
- **Forschungseinrichtungen**

Für Österreich sind nicht alle diese Sektoren von gleicher Bedeutung wie für die EU. Nuklearindustrie und Raumfahrt haben keine besondere nationale Bedeutung. Die Schwerpunkte bei der nationalen österreichischen kritischen Infrastruktur (ACI) sollen hingegen auch die **verfassungsmäßigen Einrichtungen**¹¹, die Aufrechterhaltung des **Sozialsystems und der Verteilungssysteme** sowie die **Hilfs- und Einsatzkräfte** umfassen. Die endgültige Liste der ACI-Sektoren wird erst nach Abschluss der Risiko- und Kritikalitätsanalysen festgelegt werden können. Weiters wird es auch zu einer unterschiedlichen Gewichtung der Sektoren auf Bundesebene im Verhältnis zu den Bundesländern und den Gemeinden kommen, da **aus regionaler und lokaler Sicht andere Prioritäten** entstehen.

¹¹ Der Schutz der verfassungsmäßigen Einrichtungen liegt nach SPG in der alleinigen Zuständigkeit der Sicherheitsbehörden

3) Kriterien für die Einstufung kritischer Infrastrukturen

Die **Ermittlung und Ausweisung kritischer österreichischer Infrastrukturen** anhand vorgegebener **Kriterien** ist ein **zentraler Bestandteil des APCIP**. Um die österreichischen kritischen Infrastrukturen (ACI) zu erfassen, sind **Kriterien** festzulegen, die insbesondere folgende **quantitative und qualitative Aspekte**¹² berücksichtigen:

- **Anzahl der betroffenen Bürger** (insbesondere hinsichtlich **gesundheitlicher und sozialer Auswirkungen**)
- **Wirtschaftliche Auswirkungen**
- **Auswirkungen auf die Umwelt**
- **Psychologische Auswirkungen**
- **Politische Auswirkungen**
- **Räumliche Ausdehnung**
- **Zeitliche Dauer**
- **Mangelnde Substitutionsmöglichkeiten** bei der Herstellung gleichwertiger Güter oder der Erbringung gleichartiger Dienstleistungen
- **Interdependenzen** (die Intensität der Abhängigkeiten und Wechselwirkungen zwischen den einzelnen Wirtschaftsbereichen).

Die anhand dieser Kriterien ermittelten kritischen Infrastrukturen werden sodann in einer **Liste nationaler österreichischer kritischer Infrastrukturen** zusammengefasst (Liste ACI).

4) Strategische Ziele

Ein Großteil der kritischen Infrastrukturen befindet sich nicht in staatlicher Hand, wodurch der Staat nur indirekt seiner Schutzfunktion nachkommen kann. Eine Kooperation mit den Besitzern/Betreibern der kritischen Infrastrukturen ist deshalb von Beginn an anzustreben. Darüber hinaus fehlen dem Staat und seinen Organen bestimmte Fähigkeiten und Kapazitäten zum Schutz kritischer Infrastruktur, weshalb auch hier eine enge Kooperation mit der Wirtschaft notwendig ist (z.B. Anbieter von Sicherheitstechnologien).

Grundsätzlich sind die Eigentümer oder Betreiber kritischer Infrastrukturen auch für die Sicherheit ihrer Anlagen und der damit verbundenen Prozesse verantwortlich (vgl. Verbandsverantwortlichkeitsgesetz 2005). Überschreitet jedoch ein Ereignis die „übliche“ Größenordnung, ist auch die öffentliche Hand in das Ereignis involviert, um die negativen Auswirkungen unter Kontrolle zu bringen. Eine Häufung von Störungen oder ein Totalausfall kann dazu führen, dass faktisch oder in der Darstellung durch die Medien eine

¹² Teilweise auf Basis der Mitteilung der EK über ein europäisches Programm zum Schutz kritischer Infrastruktur vom Dezember 2006 (Dok 786/2006)

strategische Schwelle überschritten wird, die neben den Aktivitäten der Verwaltung und dem Einsatz der Hilfs- und Einsatzkräfte auch eine politische Reaktion erfordern.

Das zu erreichende Schutzniveau ist durch einen politischen Kompromiss zwischen Unternehmen und Verwaltung auszuhandeln, die Zumutbarkeit von Maßnahmen für die Unternehmen klar zu definieren und ergänzende notwendige Aktivitäten der öffentlichen Hand in der jeweiligen Verwaltungsebene festzulegen. Solche strategischen Schwellen sowie entsprechende Mitigationsstrategien, dh. eine möglichst frühzeitig anzuwendende Risikominderungsstrategie, sind für die einzelnen Infrastrukturen zu bestimmen.

Dennoch kann auch eine hoch entwickelte Gesellschaft nicht alle Risiken abwehren, die Abgrenzung zwischen dem Selbstschutz der Infrastrukturbetreiber einerseits und der Unterstützung durch die Behörden bzw. der staatlichen Schutzpflicht andererseits ist zentrales Thema des APCIP.

Das strategische Ziel von APCIP ist es, die kritischen Infrastrukturen, die nationale Bedeutung haben zu identifizieren und durch Vorsorgemaßnahmen und Maßnahmen zur Schadensbehebung vor Störung und Zerstörung zu schützen. Dadurch sollen die Bevölkerung, die Grundwerte und die verfassungsmäßigen Einrichtungen geschützt werden. Die Verwundbarkeit kritischer Infrastrukturen gegenüber Naturkatastrophen, menschlichem oder/und technischem Versagen, Terrorismus und organisierter Kriminalität ist so weit wie möglich zu reduzieren. Im Sinne der Wirtschaftlichkeit und Zweckmäßigkeit ist für jede Infrastruktur ein von den jeweils Betroffenen akzeptiertes Schutzniveau zu definieren und zu implementieren.

C: Risikofaktoren

Die für jeden ACI - Sektor zu entwickelnden Maßnahmen zur Umsetzung des APCIP sollen systematisch allen folgend genannten Risikofaktoren entgegenwirken. Die angeführten Details zu den Risikofaktoren sind nicht erschöpfend ausgeführt.

1) Risikofaktor Mensch:

- mangelndes Sicherheitsbewusstsein
- nicht hinreichend qualifiziertes Personal
- menschliches Versagen
- kriminelles Verhalten („workplace violence“, Sabotage, Terroranschläge, OK)
- Weitergabe sensibler Information (Wirtschaftsspionage)

2) Risikofaktor Organisation:

- Konzentration unverzichtbarer Ressourcen
- Outsourcing unternehmenskritischer Infrastrukturen
- Just-in-Time Logistikketten
- Unternehmensbeteiligungen
- Liberalisierung von Teilmärkten

3) Risikofaktor Natur, Umwelt und Technologie:

- Natur- und Klimakatastrophen
- Seuchen und Epidemien
- Technologische Katastrophen

4) Risikofaktor IT:

- Komplexität der Systeme
- Zunehmende IT-Abhängigkeit
- Umfangreiche weltweite Vernetzung von IT-Systemen
- Kurze Innovationszyklen der IT
- Standardisierung der Technik und Komponenten
- Mobile Endgeräte weichen Behörden- und Unternehmensgrenzen auf

5) Risikofaktor Interdependenzen:

- Berücksichtigung von Abhängigkeiten
- Bedachtnahme auf Wechselwirkungen
- Dominoeffekte

D: Akteure

Ein zentraler Aspekt von APCIP ist eine Verstärkung des **Verständnisses für die potentielle Gefährdung von ACI Einrichtungen und Prozessen zu schaffen**, das die politisch und wirtschaftlich Verantwortlichen in die Lage versetzt, vorsorgend zu handeln. Deshalb bedarf es auch einer Einbindung der Infrastrukturbetreiber, der Medien und letztlich auch der Konsumenten. Einseitige von der Verwaltung vorgegebene Lösungen werden alleine nicht zum Erfolg führen.

Wie schon oben festgestellt sind heute die meisten kritischen Infrastrukturen nicht mehr in der öffentlichen Verwaltung verankert, sondern werden von Unternehmen betriebswirtschaftlich geführt. In vielen Branchen gibt es die Institution eines Regulators, der ebenfalls in das Programm einzubinden ist. Gleichzeitig spielt die veröffentlichte Meinung und die Stimmung in der Bevölkerung eine große Rolle bei Versorgungsstörungen oder der Zerstörung von Infrastrukturen. Die Verantwortung der KonsumentInnen in Bezug auf die Sicherheit ist ebenfalls bewusst zu machen.

1) Bundesverwaltung

Verwaltungen, die bestrebt sind, Sicherheitsdefizite in der privaten Wirtschaft zu beseitigen, setzen sich entweder dem Vorwurf zu starker Restriktion oder dem Vorwurf der Untätigkeit aus. Das richtige Gleichgewicht zu finden erfordert Differenzierung, offene Kommunikation mit dem privaten Sektor sowie Plattformen für den Informationsaustausch. In Österreich ist zudem die Aufgaben- und Kompetenzverteilung zwischen Bund und Bundesländern zu berücksichtigen und genau festzulegen, wer welche Aufgaben zu erfüllen hat. Der Masterplan APCIP beschäftigt sich vornehmlich mit den bundesstaatlichen Angelegenheiten.

2) Bundesländer und Gemeinden

Aufgabe von APCIP ist es den Schutz der nationalen kritischen Infrastruktur zu verbessern. Darüber hinaus wird es Aufgabe der Länder und Gemeinden sein, den Schutz kritischer Infrastrukturen auf regionaler und lokaler Ebene wahrnehmen und eigene Programme analog dem der EU und des APCIP entwickeln. Dabei ist zu erwarten, dass die Schwerpunkte naturgemäß anders gesetzt sein werden und sich damit ein enges Netz der Sicherheit bilden wird, das die nationalen und europäischen Anstrengungen komplementär ergänzt.

3) Regulatoren

Die sektorspezifischen Regulatoren sollen in das CIP Programm integriert werden, um die Definition von Standards und die Überprüfung ihrer Einhaltung in der Praxis zu unterstützen. Sollte dieser Prozess nicht möglich sein, wäre angesichts der Interdependenzen die Einrichtung eines „integrierten Regulators für CIP“ zu erwägen.

4) Interessenvertretungen

Die Einbeziehung der Interessenvertretungen sowohl der Wirtschaft, der Arbeitnehmer als auch der Landwirtschaft wird ein erster Schritt sein, ein vertieftes Bewusstsein für Maßnahmen von CIP bei Unternehmen und Konsumenten zu schaffen.

5) Unternehmensleitungen der Infrastrukturbetreiber

Die Unternehmensleitung trägt bei Schadensereignissen das unternehmerische Risiko und auch mögliche Haftungsrisiken. CIP ist eine gesamtunternehmerische Aufgabe, die der Unterstützung aller Ebenen bedarf, besonders der Sicherheitsverantwortlichen und allen voran der Geschäftsführung.

6) Medien

Die Medien spielen in der Informationsgesellschaft die wichtigste Rolle bei der Vermittlung neuer Sachthemen. Deshalb sind Redakteure aus dem Fachbereich Sicherheit von Anfang an über das Projekt CIP umfassend zu informieren.

7) Konsumenten

Die Konsumenten wirken mit ihren Kaufentscheidungen direkt auf die Gestaltung des Waren- und Dienstleistungsangebots ein und somit auch darauf, wie viel „Sicherheit“ diese Produkte bieten (Versorgungssicherheit, Nachhaltigkeit, etc.) und welchen Preis sie dafür bereit sind zu zahlen. Deshalb sind die Konsumenten eine wichtige Anspruchsgruppe für das APCIP.

E: Maßnahmen zum Schutz kritischer Infrastrukturen

Neben der Festlegung der strategischen Ziele, der Grundsätze, der Risikofaktoren und der Akteure ist die Festlegung und Umsetzung konkreter Maßnahmen zum Schutz kritischer Infrastrukturen ein zentraler Schwerpunkt des APCIP. Nach einer exemplarischen Darstellung der wichtigsten Maßnahmen werden im folgenden Aktionsplan die Maßnahmen in Teilziele gebündelt:

1) Intensivierung des Informationsaustauschs

Die **Stärkung des Informationsaustausches** und des **Dialogs mit und zwischen den Betreibern von kritischen Infrastrukturen** ist eines der wesentlichsten Ziele des APCIP. Ansprechpartner sind nicht nur die Betreiber und Eigentümer kritischer Infrastrukturen, sondern auch deren Interessenvertretungen und die zuständigen Regulatoren. Dabei muss vermittelt werden, dass eine moderne, interdependente Wirtschaft möglichst viele verlässliche Wirtschaftspartner benötigt, die Maßnahmen zu CIP umgesetzt haben. Zu diesem Zweck soll eine **Informationsplattform CIP** eingerichtet werden.

2) Erstellen von Sicherheits- und Notfallplänen für ACI

Die bestehenden Sicherheitspläne von Unternehmen, die diese selbst unter Einbindung von Behörden erstellen, und die Notfallpläne der Gebietskörperschaften sollen an die spezifischen Bedrohungen als kritische Infrastruktur angepasst und akkordiert werden. Dabei ist auf funktionierende und erprobte Strukturen für den Einsatz, die Koordination und Kommunikation zu achten. Die Notfallpläne sollen insbesondere Kompetenzen klären, Präventivmaßnahmen ergreifen, die Sicherstellung eines Notbetriebs gewährleisten und bei Bedarf Evakuierungspläne beinhalten.

3) Public-Private-Partnership (PPP)

PPP ist ein Modell der Zusammenarbeit zwischen Hoheitsverwaltung und Privatwirtschaft, wobei die unterschiedlichen Ressourcen und Risikomanagementstrategien sich gegenseitig ergänzen. Bei der IKT Sicherheit gibt es bereits erprobte PPP-Modelle. Anzustreben sind **APCIP-Partnerschaften** für alle genannten Sektoren. Für ein gelungenes PPP Modell bei CIP ist die gegenseitige Integration in Ablaufprozesse notwendig. Dies erfordert die gemeinsame Analyse der relevanten Prozesse, die Identifizierung von Schnittstellen in den Prozessabläufen und die Bestimmung von Ansatzmöglichkeiten für die gegenseitige Prozessintegration. Die Einbindung der ACI - Betreiber in den gesamtstaatlichen Lagebildprozess und in die Risikoanalyse ist dabei ein wichtiger Schritt. Dafür ist die Festlegung von kompetenten Ansprechpartnern auf beiden Seiten unbedingt notwendig.

4) Sicherheitskette (Sicherungs- und Schutzprogramm)

Bei der Planung und Umsetzung von Schutzmaßnahmen sind alle Schritte der gesamten Sicherheitskette zu berücksichtigen, damit alle möglichen Maßnahmen ausgeschöpft und Erfahrungen rückgekoppelt werden. Das **Spektrum der phasenorientierten Maßnahmen** umfasst Prävention, Vorsorge und Vorbereitung, um mögliche negative Auswirkungen auszuschließen bzw. so weit wie möglich einzugrenzen. Hilfeleistungen im Anlassfall sollen die Auswirkungen der Störung bewältigen und die Schäden begrenzen. Nachsorge und Bewertung schließen das Spektrum der Maßnahmen ab. Auf die wirtschaftliche

Ausgewogenheit der Maßnahmen zur Reduzierung des Risikos und in Bezug auf die internationale Wettbewerbsfähigkeit ist zu achten.

Prävention:

Mit einer breiten Palette an Präventionsmaßnahmen lässt sich das Risiko des Eintritts einer Störung sehr früh minimieren und das mögliche Schadensausmaß reduzieren. Dies beginnt bei der Risikoanalyse einer neuen Technologie oder besonderen Entwicklungstendenzen, prüft die Fehlerfreundlichkeit technischer oder organisatorischer Systeme und die Eintrittswahrscheinlichkeit von Störungen, um Überraschungen vorzubeugen, erkennt und behebt strukturelle und prozessuale Ursachen für Sicherheitslücken und – mängel und ergreift eventuell bauliche Maßnahmen.

Vorsorge:

Im österreichischen Konzept der Umfassenden Sicherheitsvorsorge stehen Vorsorgemaßnahmen an oberster Stelle: Schulung der Verantwortlichen, Mittel- und Einsatzplanung, organisations-/sektor-/grenzüberschreitende Übungen.

Vorbereitung durch Warnungen und Informationen, Maßnahmen zur Begrenzung der Störung:

Information der Bevölkerung: das Wissen um die Auswirkungen führt zur Stärkung der Verantwortung. Die aktive Vorbereitung auf Angriffe, Störungen oder Katastrophen schöpft alle Möglichkeiten zur Schadensminimierung aus.

Maßnahmen zur Schadensbewältigung:

Die Folgen eines Schadenseintritts können durch effizientes Krisenmanagement, das Auswirkungen rasch erkennt, bekämpft und reduziert werden. Schadensbegrenzung ist das Ziel. Gleichzeitig ist es besonders wichtig, Hilfs- und Einsatzorganisationen und deren Mittel zu schützen und zu stärken.

Nachsorge:

„Back to normal“, Opfer und Einsatzkräfte versorgen, Schadensbehebung und Wiederaufbau.

Bewertung:

Einheitliches Berichtswesen, „Lessons Learned“, Schlussfolgerungen umsetzen, Rückkopplungsschleife.

5) Physische Schutzmaßnahmen

Das **Spektrum der physischen Schutzmaßnahmen**, die einerseits von den Betreibern selbst und andererseits von der Exekutive oder gemeinsam ergriffen werden können, umfasst

- Personenbezogene Schutzmaßnahmen (wie im § 22 SPG vorgesehen),
- Bauliche und technische Schutzmaßnahmen,
- Organisatorische Schutzmaßnahmen,
- Maßnahmen bei IKT und
- Fähigkeitsplanungen bei den Einsatzkräften.

Besonders die baulichen und technischen Schutzmaßnahmen sind im **Objektschutz** seit Jahren wirksam und werden durch die Erstellung von spezifischen Sicherheits- und

Notfallsplänen für jede kritische Infrastruktur konkretisiert. Diese Erfahrungen des BMI sind für die Erstellung eines wirksamen APCIP von hoher Bedeutung.

Objektschutzmaßnahmen durch die Sicherheitsbehörden und ihre Organe werden in folgenden Fällen durchgeführt:

- Präventivmaßnahmen im Zuge einer direkten Bedrohung gegen das Objekt
- Überwachung aufgrund angeordneter Präventivmaßnahmen nach einer Gefährdungseinschätzung
- Sicherungsmaßnahmen und Ermittlungen nach einem Ereignis (kriminell, terroristisch, Unfall, Naturkatastrophe, ...), insbesondere nach Aufforderung durch Betriebsangehörige oder öffentliche Organe.

6) Freiwillige und gesetzliche Maßnahmen :

Bei den Anreizen zu Investitionen in CIP gibt es eine breite Palette an Maßnahmen, die von F&E Förderung bis hin zu steuerlichen Begünstigungen reichen können. Auch die Überprüfung von als kritisch eingestuften Infrastrukturen anhand von Normen oder die Einführung eines Gütesiegels „geprüfter ACI - Betrieb“ sollen geprüft werden.

Sofortiger Handlungsbedarf entsteht dann, wenn die bisherigen Schutzmaßnahmen zu stark von den neu definierten Sicherheits- und Schutzstandards abweichen und Risiken für die Allgemeinheit nicht mehr in Kauf genommen werden können. In diesem Fall sind gesetzliche Regelungen unvermeidbar.

Die heutigen Schutzmaßnahmen sind durch **Normen und Standards** vorgegeben. Dabei ist einerseits zu berücksichtigen, dass sich diese auf nationaler und europäischer Ebene nicht widersprechen und so weit wie möglich mit internationalen Ansätzen kompatibel sind. Andererseits ist eine Entwicklung zu erwarten, dass erst die Erfüllung vorgegebener Schutzniveaus den Marktzugang ermöglicht (US „Container Security Initiative“).

F: Aktionsplan APCIP¹³

1. Teilziel: Erstellung einer Liste österreichischer kritischer Infrastrukturen (ACI)

- Zusammenstellung der rechtlichen Rahmenbedingungen.
- Erhebung des Ist-Standes der Maßnahmen zur Umsetzung CIP.
- Risikoanalyse im Wirkungsbereich der Bundesministerien.
- Erstellung einer Liste Kritischer Infrastrukturen (Liste ACI).

2. Teilziel: Prioritätenreihung

- Prioritätenreihung der Liste ACI.
- Schaffung von sektorenübergreifenden CI Clustern.

3. Teilziel: Festlegung der Sicherungs- und Schutzstandards

- Festlegung von Standards in Hinblick auf das Schutzniveau je ACI Sektor/Cluster.
- Festlegung eines Verfahrens zur Definition, Einführung, Umsetzung und Weiterentwicklung der Standards.

4. Teilziel: Sicherungs- und Schutzmaßnahmen

- Implementierung der Sicherungs- und Schutzmaßnahmen.

5. Teilziel: Informationsmanagement, Entwicklung von Partnerschaften CIP, Private-Public-Partnerships

- Identifikation von Ansprechpartnern für APCIP bei wesentlichen Infrastrukturbetreibern.
- Einrichtung einer Informationsplattform.
- Einbindung ausgewählter Ansprechpartner in den staatlichen Lagebildprozess.
- Einrichtung von APCIP-Partnerschaften (PPP-Modell).

6. Teilziel: Evaluation und Follow – up

- Evaluierung der Umsetzung des Masterplans.

¹³ Die Arbeitsergebnisse aus Projekten des nationalen Sicherheitsforschungsprogramms (KIRAS) werden so weitgehend wie möglich in das österreichische Programm zum Schutz kritischer Infrastrukturen übernommen.