Sicherheitsinteressen der Schweiz an Rundfunk- und Telekommunikations-Infrastrukturen in ausserordentlichen Lagen

Bericht des Bundesrates an die Sicherheitspolitischen Kommissionen der Eidgenössischen Räte

vom 30. November 2001

Inhaltsverzeichnis

1 AUSGANGSLAGE 3

1.1 Auftrag 3

1.2 Abgrenzung 3

1.3 Vorgehen 4

1.4 Begriffsbildung 5

2 GRUNDLAGEN 6

2.1 Abhängigkeiten und Gefahren in der Informationsgesellschaft 6

2.2 Sicherheitspolitischer Auftrag 6

2.3 Gesetzliche Grundlagen 7

3 SICHERHEITSBEDÜRFNIS 7

3.1 Im Allgemeinen 7

3.2 Im Besonderen 8

4 RISIKEN UND MASSNAHMEN 11

4.1 Methodik der Risikoanalyse 11

4.2 Risikoanalyse und daraus resultierende Massnahmen 12
4.2.1 Technik 13
4.2.1.1 Netzüberlastung *(1)* 13
4.2.1.2 Kritische Pfade und Zentralisierung der Netzintelligenz *(2)* 13
4.2.1.3 Technologische Entwicklung *(3)* 14
4.2.1.4 Ausländische Technologien *(4)* 14
4.2.1.5 Netzbetriebszentren im Ausland *(5)* 14
4.2.1.6 Satelliten-Technologie *(6)* 15
4.2.1.7 Technische Monokultur *(18)* 15
4.2.1.8 Empfangsprobleme *(7)* 15
4.2.2 IT-Branche 15
4.2.2.1 Privatisierung *(8)* 16
4.2.2.2 Aufteilung von Unternehmen *(9)* 16
4.2.2.3 Internationalisierung *(10)* 16
4.2.3 Personal *(11)* 17
4.2.4 Äussere Einwirkungen 18
4.2.4.1 Sabotage *(12)* 18
4.2.4.2 Energieausfall *(13)* 18
4.2.4.3 Zivilisationsunfälle *(14)* 18
4.2.4.4 Naturkatastrophen *(15)* 19
4.2.5 Organisation 19
4.2.5.1 Fehlende Kompatibilität (16) 19
4.2.5.2 Probleme im Bereich VRK-UKW 77 *(17)* 19

4.3 Risiken und Massnahmen im Überblick 20

5 ZUSAMMENFASSENDE ERGEBNISSE 22

Anhänge

Anhang 1: Teilnehmer der Arbeitsgruppe

Anhang 2: Strukturvorgabe

1 AUSGANGSLAGE

1.1 Auftrag

In der politischen Diskussion im Zusammenhang mit den Plänen der Swisscom, ihre Broadcasting-Aktivitäten zu verkaufen, wurde die Frage aufgeworfen, inwieweit der Bund als Hauptaktionär die Verfügungsgewalt über wichtige Informations- und Kommunikations-Infrastrukturen behalten müsse, um die nationalen Sicherheitsinteressen zu gewährleisten. Verschiedene parlamentarische Vorstösse fordern denn auch Massnahmen zur Sicherstellung dieser Sicherheitsbedürfnisse. Der Bundesrat kündigte in deren Beantwortung an, die geltend gemachten Bedürfnisse im Rahmen einer interdepartementalen Arbeitsgruppe zu analysieren sowie Mittel und Wege zu prüfen, wie deren Sicherstellung gewährleistet werden kann. In der Folge wurde eine Arbeitsgruppe unter der Leitung des UVEK (BAKOM) tätig. Der vorliegende Bericht basiert auf den Resultaten dieser Arbeiten.

Schnell zeigte sich, dass die nationalen Sicherheitsinteressen bezüglich der elektronischen Informations- und Kommunikationsinfrastrukturen in ihrem Gesamtzusammenhang zu betrachten sind und man sich nicht auf Teilaspekt wie die Frage des Zugriffs auf solche Infrastrukturen mittels Eigentum am sie betreibenden Unternehmen beschränken kann. In diesem Sinne gilt es, die Risiken, welche diese Infrastrukturen bedrohen, in ihrer Gesamtheit zu erfassen. Darauf gestützt sind Massnahmen zu definieren, welche die entsprechenden Risiken eliminieren resp. vermindern.[1]

Der vorliegende Bericht ist eine Momentanaufnahme der aktuellen Situation. Er darf nicht darüber hinweg täuschen, dass die Risikoanalyse und die daraus resultierende Formulierung von Massnahmen grundsätzlich eine Daueraufgabe der jeweiligen Träger von Sicherheitsbedürfnissen ist.

1.2 Abgrenzung

Krisensituationen im Umfeld der Informationsgesellschaft können die öffentliche Hand und die Privatwirtschaft gleichermassen treffen. Alle Teilnehmer der Informationsgesellschaft tragen letztlich selbst die Verantwortung für die Sicherheit ihrer Informatik- und Kommunikations-Infrastrukturen.[2] Um aber in einer Situation, die sich durch eine grosse Vernetzung charakterisiert, eine Gesamtsystemsicht zu verfolgen, ist das Vorgehen von Staat, Wirtschaft und Wissenschaft zu koordinieren. Vor diesem Hintergrund sind bereits verschiedene staatliche, halbstaatliche oder private Organe geschaffen oder im Aufbau begriffen, die sich mit der Informationssicherheit *im weiteren Sinne* beschäftigen. Im Wesentlichen handelt es sich dabei um die private Stiftung InfoSurance[3], das Milizamt ICT-I[4] und den Sonderstab Informationssicherheit[5]. Im militärischen Bereich beschäftigt sich innerhalb des VBS eine Projektgruppe Information Operations mit dem Informationskrieg und verwandten Themen. Auf Stufe Bund ist zudem die Schaffung eines 'Koordinationsorgans Information Assurance' vorgesehen.[6] Im Juni 2001 organisierte die strategische Führungsausbildung eine Übung INFORMO, anlässlich welcher diese Organe, in erster Linie der Sonderstab, ihre Positionie-

[1] Es sei darauf hingewiesen, dass in manchen Bereichen bereits Massnahmen getroffen wurden. Nachfolgend geht aus dem Zusammenhang hervor, ob es sich um bereits verwirklichte oder noch zu verwirklichende Massnahmen handelt. Diese Unterscheidung ist insbesondere bei der Risikoanlayse (Ziff. 4) von Bedeutung, wo bereits verwirklichte Massnahmen typischerweise entschärfend zu Buche schlagen.

[2] Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000), S. 66.

[3] www.infosurance.ch

[4] Organisatorisch dem Bundesamt für wirtschaftliche Landesversorgung, Bereich Informations- und Kommunikationsinftrastruktur, angegliedert.

[5] Organisatorisch dem Informatikstrategieorgan des Bundes angegliedert.

[6] Dazu ausführlich das Konzept 'Information Assurance' der Koordinationsgruppe Informationsgesellschaft vom 17. Mai 2000.

rung und Funktionsweise testen konnten. Die Resultate werden zur Zeit ausgewertet und dem Bundesrat im Verlaufe des Herbstes vorgelegt.

Bei der diesem Bericht zu Grunde liegenden Fragestellung geht es dagegen *in einem engeren Sinne* um die einschlägigen Sicherheitsbedürfnisse der öffentlichen Hand in ausserordentlichen Lagen, mithin um ihre Bedürfnisse im Rahmen der Krisenbewältigung. Sicherheitsinteressen Privater von landeswichtiger Bedeutung werden vorliegend allenfalls im Rahmen der wirtschaftlichen Landesversorgung mitberücksichtigt. Erfasst werden dabei vor allem Zwischenfälle und Störungen, die auf Grund ihrer Ausdehnung und Intensität geeignet sind, schwere Mangellagen herbeizuführen, denen die Wirtschaft nicht alleine begegnen kann. In der Regel handelt es sich dabei um branchenübergreifende Ereignisse, denen auch branchenübergreifend koordiniert begegnet werden muss.

Generell wird im Zusammenhang mit der Sicherheit im Informations- und Kommunikationsbereich zwischen infrastruktur-relevanten und inhalt-relevant Aspekten unterschieden. Die Verantwortung für inthaltliche Aspekte wird tendenziell dem Endbenutzer bzw. dem Inhaltsproduzenten (z.B. Rundfunkprogrammteile) selbst zugewiesen (z.B. End-zu-End-Chiffrierung), währenddem die Sicherheit bezüglich der Infrastruktur grundsätzlich vom Betreiber der technischen Kommunikationsinfrastruktur zu gewährleisten ist (Aufbau und Betrieb).

1.3 Vorgehen

In einem ersten Schritt wurden durch das BAKOM mögliche Träger von Sicherheitsbedürfnissen in der Bundesverwaltung und im Umfeld der Kantone ausfindig gemacht sowie über den Auftrag und die geplante Vorgehensweise informiert.[7] Bei dieser Gelegenheit wurden die angeschriebenen Stellen gebeten, weitere Bedürfnisträger zu identifizieren und im Rahmen einer Umfrage bereits die ersten inhaltlichen Arbeitsgrundlagen zu liefern. Die Verantwortlichen der kantonalen Sicherheitskooperation wurden schliesslich über die nationale Sicherheitskooperation, welche in der Arbeitsgruppe vertreten war, miteinbezogen. Die Strukturvorgabe[8] sollte den Angefragten dabei einerseits als Arbeitsinstrument dienen, dem BAKOM andererseits aber auch die Auswertung erleichtern. Nach einer ersten Sichtung der eingegangenen Antworten, welche bezüglich Umfang und Konkretisierungsgrad sehr unterschiedlich ausfielen, wurde schliesslich am 27. März 2001 eine erste Plenumssitzung durchgeführt, mit dem Ziel, ein gemeinsames Verständnis über Fragestellung und Vorgehensweise zu erreichen, die bisherigen Ergebnisse zu vervollständigen, zu konkretisieren sowie allfällige Schnittstellen zu erkennen. Diese ersten Erkenntnisse wurden der Arbeitsgruppe mittels einer Informationsnotiz vom 2. April 2001 in aufbereiteter Form zugestellt. Am 16. Mai 2001 fand ein ganztägiger Workshop zur Risikoanalyse mit ausgewählten Exponenten der Arbeitsgruppe statt. Daneben fanden informelle Aussprachen mit einzelnen Mitgliedern der Arbeitsgruppe statt. Mit Schreiben vom 31. Juli 2001 wurde den Mitgliedern der Arbeitsgruppe (neben einigen weiteren interessierten Stellen) die Version 1.0 des Berichts zur Vernehmlassung unterbreitet. Zahlreiche Eingaben lieferten in der Folge konkretisierende oder weitergehende, teilweise aber auch richtig stellende Informationen, welche in die Version 2.0 einflossen. An der 2. Plenumsveranstaltung vom 3. Oktober 2001 wurde der Bericht (Version 2.2), nachdem noch einige inhaltliche Details bereinigt wurden, in der Arbeitsgruppe im Konsens verabschiedet. Einige redaktionelle Änderungen führten schliesslich zur definitiven Version 2.3.

[7] Die Teilnehmer der Arbeitsgruppe sind namentlich in Anhang 1 aufgeführt. Neben den eigentlichen Bedürfnisträgern nahmen auch Vertreter der Grundversorger Einsitz.

[8] Siehe Anhang 2.

1.4 Begriffsbildung

Zwecks einheitlicher Anwendung und somit zur Vermeidung von Missverständnis wurden folgende Begriffsbildungen vorgenommen.

Ausserordentliche Lage:[9]

Situation, in der in zahlreichen Bereichen und Sektoren normale Verwaltungsabläufe nicht genügen, um die Probleme und Herausforderungen zu bewältigen, beispielsweise bei Naturkatastrophen, die das ganze Land schwer in Mitleidenschaft ziehen, oder bei kriegerischen Ereignissen.

> Zur Abgrenzung:
>
> *Normale Lage:* Situation, in der ordentliche Verwaltungsabläufe zur Bewältigung der anstehenden Probleme und Herausforderungen ausreichen.
>
> *Besondere Lage:* Situation, in der gewisse Staatsaufgaben mit den normalen Verwaltungsabläufen nicht mehr bewältigt werden können. Im Unterschied zur „ausserordentlichen Lage„ ist aber die Regierungstätigkeit nur sektoriell betroffen. Typisch ist der Bedarf nach rascher Konzentration der Mittel und Straffung der Verfahren.

Die Aussagen dieses Berichts gelten im Allgemeinen auch für besondere Lagen, besteht zur ausserordentlichen Lage lediglich ein gradueller Unterschied bezüglich Ausdehnung und Intensität des Ereignisses. Auf eine scharfe Trennung zwischen besonderer und ausserordentlichen Lage wird nachfolgend somit verzichtet.

Krise:

Synonym für *besondere* und *ausserordentliche Lagen.*

Sicherheit (im konkreten Zusammenhang):

Minimale Verfügbarkeit (inklusive Integrität) der Informations- und Kommunikations-Infrastrukturen zur Alarmierung, Information und Führung in ausserordentlichen Lagen, um die Entscheidungs- und Handlungsfähigkeit im Bereiche landeswichtiger Interessen zu gewährleisten.[10]

Rundfunk- und Telekommunikationsinfrastruktur (als Teil der Informations- und Kommunikationsinfrastruktur):

Unter diesem Begriff werden für den vorliegenden Bericht Systeme der Rundfunk- und Telekommunikationsnetzwerke, damit im Zusammenhang stehende Computer und andere technische Anlagen verstanden, welche der Übertragung von Daten, Sprache resp. Bild und Ton dienen. In einem weiteren Sinn fällt neben technischen Komponenten auch das zum Aufbau, Betrieb und Unterhalt benötigte Know-how darunter. Nicht gemeint sind dagegen reine Informationsspeicher- und Informationsverarbeitungssysteme bzw. Programmproduktionssysteme für Radio und Fernsehen.

[9] In Anlehnung an den SIPOL B 2000, Anhang 'Umschreibung von Kernbegriffen', S. iii.

[10] In einem weiteren Sinn umfasst die Sicherheit auch inhaltsbezogene Aspekte wie Vertraulichkeit, Authentizität und Verbindlichkeit von Informationen.

2 GRUNDLAGEN

2.1 Abhängigkeiten und Gefahren in der Informationsgesellschaft

Die Informationstechnologie gilt als eine der Schlüsseltechnologien in der heutigen Zeit. Sichere Informations- und Kommunikations-Infrastrukturen stellen nicht nur für die ökonomische Entwicklung sondern auch für die Funktionsfähigkeit der Regierungs- und Verwaltungstätigkeit eine unabdingbare Voraussetzung dar. Diese Abhängigkeit wird in Zukunft noch weiter zunehmen. Mit zunehmender Abhängigkeit steigen aber auch die Gefahren und Risiken. Den Sicherheitskonzepten und der Notfallplanung (contingency planing and disaster recovery) kommen angesichts dieser Entwicklung vorrangige Bedeutung zu.

In ausserordentlichen Lagen kann sich das Informations- und Kommunikationsbedürfnis je nach Situation und Aufgabenbereich gar beträchtlich erhöhen. Im Vordergrund steht hierbei die Informationsbeschaffung, die Einsatzführung im Rahmen der Krisenbewältigung und die Information der Bevölkerung. Die Praxis zeigt, dass Krisen oftmals auch zu Informationskrisen werden. Ursache dafür ist in nicht seltenen Fällen die fehlende oder nur mangelhafte Verfügbarkeit der erforderlichen Infrastruktur.

Vor diesem Umstand erscheint die Sensitivität von Informations- und Kommunikationssystemen je nach Art der ausserordentlichen Lage als logische Konsequenz. Jedenfalls steigt mit zunehmender Komplexität und Abhängigkeit von Systemen auch der Anreiz für Missbräuche oder gezieltes Ausnützen von Schwachstellen, sei es durch einzelne Hacker, kleinere oder grössere Gruppierungen oder gar fremde Staaten. Mannigfach können dabei auch die Motive sein: politisch-ideologisch, religiös, wirtschaftlich, kriminell.

2.2 Sicherheitspolitischer Auftrag

Der Bundesrat hat die Bedeutung von Informations- und Kommunikationsmitteln bereits in seinem Bericht über die Sicherheitspolitik der Schweiz (SIPOL B 2000) erkannt.[11] Dabei unterstreicht er insbesondere die Wichtigkeit der wahrheitsgetreuen, raschen und verständlichen Information der Öffentlichkeit. Je nach Lage verfügt der Bundesrat dazu neben den zivilen Medien auch über den Stab Bundesrat Abteilung Presse und Funkspruch (Stab BR APF). Dieser kommt nach dem Subsidiaritätsprinzip dann zum Einsatz, wenn die zivilen Medien nicht mehr in der Lage sind ihren Informationsautrag zu erfüllen.[12]

Oberstes Ziel des Bundesrates ist es, die Entscheidungs- und Handlungsfähigkeit der Schweiz aufrecht zu erhalten und Rahmenbedingungen zu schaffen, um das Funktionieren der Informationsgesellschaft Schweiz zu gewährleisten. Dabei bedarf es einer Gesamtsystemsicht und eines koordinierten Vorgehens insbesondere bei der Identifikation vitaler nationaler Infrastrukturen, bei der Sensibilisierung, bei der Ausbildung von Experten, bei der permanenten Erfassung und Verfolgung der Risikolage, bei der Früherkennung und Warnung, bei der schnellen Zusammenführung von Entscheidungsträgern sowie beim Aufbau gemeinsamer Sicherheitsinfrastrukturen. Im Weiteren erkennt der Bundesrat, dass ein vollständiger Schutz mit *vertretbarem* Aufwand nicht zu erreichen ist, weshalb basierend auf fundierten Risikoanalysen *angemessene* Sicherheitsmassnahmen zu treffen sind.

In diesen umfassenden sicherheitspolitischen Auftrag fügt sich der unter Ziff. 1.2 abgesteckte Themenbereich des vorliegenden Berichtes als gewichtiger Teil ein.

[11] Siehe Ziff. 3.1.7 und 6.7 SIPOL B 2000.

[12] Art. 2 Abs. 1 der Verordnung über den Stab Bundesrat Abteilung Presse und Funkspruch.

2.3 Gesetzliche Grundlagen

Soweit ersichtlich finden sich bzgl. Informations- und Kommunikations-Infrastrukturen in ausserordentlichen Lagen auf Bundesebene im Wesentlichen folgende, im vorliegenden Kontext relevanten, gesetzlichen Grundlagen:

- Fernmeldegesetz (FMG; SR 784.10), 8. Kapitel: Wichtige Landesinteressen (Art. 47 f.)
- Verordnung über Fernmeldedienste (FDV; SR 784.101.1), 6. Kapitel: Wichtige Landesinteressen (Art. 66 ff.)
- Bundesgesetz über Radio und Fernsehen (RTVG; SR 784.40), Art. 6: Öffentliche Sicherheit, Verbreitungspflichten
- Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (SR 172.010.58)
- Bundesgesetz über die wirtschaftliche Landesversorgung (LVG; SR 531; insbes. Art. 2 und 22 ff.)
- Verordnung über Organisation und Aufgaben der wirtschaftlichen Landesversorgung (SR 531.11)
- Verordnung über die Koordination der Übermittlung im Rahmen der Gesamtverteidigung (SR 501.6)
- Militärgesetz (MG; SR 510.10)
- Verordnung über den Stab Bundesrat Abteilung Presse und Funkspruch (SR 510.109)
- Bundesratsbeschluss vom 27. August 1980 betreffend Vorbereitung der Radioversorgung in Katastrophen-, Krisen- und Kriegsfällen (VRK)
- Verordnung über die Requisition (SR 519.7)
- Verordnung über die Befreiung vom Militärdienst (SR 511.31)
- Verordnung des VBS über die Organisation der Armee (SR 513.11), Art. 17 Abs. 5: Einteilung von Angehörigen der Swisscom in die Telecombrigade
- Verordnungen betreffend Aufgaben und Dienstpflicht der Telecombrigade 40
- Verordnung über den Zivilschutz (ZSV; SR 520.11), 2. Kapitel: Alarmierung der Bevölkerung und Verbreitung von Verhaltensweisen, 9. Kapitel: Übermittlungsnetze (Art. 66 ff.)
- Verordnung über die Nationale Alarmzentrale (SR 732.34), Art. 5 Abs. 1 lit. a: Zusammenarbeit mit SRG.

3 Sicherheitsbedürfnis

3.1 Im Allgemeinen

Die besondere und die ausserordentliche Lage zeichnen sich dadurch aus, dass in gewissen Sektoren normale Verwaltungsabläufe nicht genügen, um die Probleme und Herausforderungen zu bewältigen. Typisch ist der Bedarf nach rascher Konzentration der Mittel und Straffung der Verfahren. Nichtsdestoweniger wird die öffentliche Hand bestrebt sein, ihren Kernaufgaben vollumfänglich nachzukommen. Die Sicherstellung der dazu erforderlichen Infrastruktur gilt dabei als eigentliches Grundbedürfnis, welches demjenigen in ordentlichen Lagen entspricht. Gewisse Träger öffentlicher Aufgaben wie Polizei, Armee, Bevölkerungsschutz und Rettungskräfte sind in ausserordentlichen Situationen typischerweise in erhöhtem Masse gefordert und stellen im Rahmen der Krisenbewältigung an Verfügbarkeit und Vertraulichkeit der dabei eingesetzten Mittel erhöhte Ansprüche. Hinzu kommt, dass die Krisensituation im Vergleich zum 'courant normal' per se einen gesteigerten Informations- und Kommunikationsbedarf bewirkt. Information wird dabei zu einem der wichtigsten Führungsmittel. Daneben ist in ausserordentlichen Situationen aber auch ein ausgeprägtes Informationsbedürfnis seitens der Bevölkerung vorhanden. Hier gilt es insbesondere auch das verfassungsmässige Recht der Informationsfreiheit zu beachten, welches dem Bürger nach neueren Tendenzen in beschränktem Mass auch den Anspruch auf behördliche Information ge-

währt.[13] Um diesen Anforderungen gerecht zu werden, stellen die einzelnen Verwaltungseinheiten hohe Sicherheitsbedürfnisse an die Telekommunikations- und Rundfunk-Infrastrukturen.

Eine absolute Sicherheit ist aus technischen insbesondere aber auch aus wirtschaftlichen Gründen oftmals gar nicht möglich oder zumindest nicht erstrebenswert. Mit der Frage nach der Sicherheit stellt sich somit immer auch die Frage nach dem Restrisiko, welches man gewillt ist einzugehen resp. nicht ausschliessen kann. Insbesondere aus diesem Grund ist eine Gesamtsicht, welche die konkreten Abhängigkeiten und Gefahren aufzeigt, unbedingt erforderlich.

3.2 Im Besonderen

Das Sicherheitsbedürfnis bezieht sich immer auf eine konkrete Einrichtung. Dass diese Ansprüche hoch sind und in Krisensituationen tendenziell noch ansteigen, wurde bereits dargelegt. Im Folgenden wird aufgezeigt, auf welche Infrastrukturen (Netze) die einzelnen Akteure in ausserordentlichen Lagen konkret angewiesen sind, und wer diese Infrastrukturen betreibt.

Wesentlich ist der Umstand, dass im Rahmen der Krisenbewältigung eine umfassende Kommunikation zwischen den verschiedenen Instanzen nur mit den öffentlichen Fix- und Mobilnetzen sichergestellt werden kann. Diese Anschlüsse bilden die Basis der Kommunikation aller beteiligten Stellen (Armee, Zivilschutz, Polizei, Milizorgane, zivile Führung) schlechthin. Damit sie auch in Krisensituationen und im Falle von Überlast der Netze benutzbar sind, wurden sie in den öffentlichen Netzen der Grundversorgerin priorisiert.

Bundesverwaltung generell:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
Basisnetzwerk für die Kommunikation der Bundesverwaltung KOMBV 1-3	Swisscom, Bund (BIT)	
Mobilfunknetz	Swisscom, künftig evtl. auch Orange, Sunrise, 3G Mobile	Im Swisscom-Netz kann heute priorisiert werden.
POLYCOM	Bund, Kantone	Sicherheits- und Rettungsfunknetz (Zellular- und Direct-Modus)
Internet Provider	Diverse	
Allgemeine Rundfunknetze (SRG und andere private Veranstalter)	Swisscom (generell für terrestrische Verbreitung der SRG-Radioprogramme und 98 % der Fernsehprogramme) neben anderen privaten Betreibern, EUTELSAT (französische Gesellschaft) für die Satellitenverbreitung, Kabelbetreiber (CATV-Firmen) für leitungsgestützte Verbreitung.	Art. 6 RTVG (öffentliche Sicherheit, Verbreitungspflicht) Ab NAZ besteht eine Besprechungsmöglichkeit für SRG-Programme zur direkten Warnung und Alarmierung.

[13] Siehe dazu auch BGE 107 Ia 304. Daneben statuieren Art. 10 und 34 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010) eine Informationspflicht des Bundesrates und der Verwaltung gegenüber der Öffentlichkeit.

Auswärtige Angelegenheiten:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
KOMBV4	Swisscom, ausländische Betreiber	
Mobiltelefonie	Swisscom, ausländische Betreiber	
Botschaftsfunk	Bund (EDA und VBS)	Kurzwellenfunk Anbindung an ComCenter EDA über AF-Netz- und Tranet-Anschlüsse (militärische Netze)
Satellitenverbindungen	INMARSAT (britische Gesellschaft)	3 % Beteiligung der Swisscom
KW-Radio (SRI-SRG)	Swisscom im Auftrag SRI-SRG, ausländische Betreiber	(Swiss Radio International), Information von Auslandschweizern und EDA-Personal
Satellitenfernsehen	Swisscom im Auftrag SRI-SRG, ausländische Betreiber	Information von Auslandschweizern und EDA-Personal

Armee:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
AF-Netz	Bund (VBS), Swisscom	Allgemeines, strategisches Führungsnetz (Fest- und Richtstrahlnetz) des Bundes unter Einbindung der Kantone
BBUS-Richtstrahl **BBUS-Kabel**	Bund (VBS) Bund (VBS) / Swisscom	Operative Übertragung Richtstrahl Operative Übertragung Kabel
IMFS und taktische Funknetze	Bund (VBS)	Erfordern den Einsatz von Übermittlungstruppen
TRANET	Bund (VBS)	Datenkommunikationsnetz der Armee und von Teilen der Armeeverwaltung
VULPUS Funk/ VULPUS Telematik	Bund (VBS)	

VRK-UKW 77	Eigentum:
	- Gebäude und Infrastruktur: Swisscom
	- Übertragungsanlagen: Stab BR APF
	Betrieb:
	- Im Normalfall:
	  - ziviler Teil: Swisscom im Auftrag SRG
	  - VRK-Teil: Swisscom im Auftrag Stab BR APF
	- In ausserordentlichen Lagen:
	  - Swisscom im Auftrag NAZ
	  - Ab Mob: Tc Br 40 im Auftrag Stab BR APF (Info Rgt 1)
		Radioversorgung der Bevölkerung in ausserordentlichen Lagen. Ab Bezug Schutzräume mit verstärkter Sendeleistung.
		Subsidiarität
		(zur Zeit noch in Abklärung)

Zivilschutz:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen

VRK-UKW 77	Eigentum:
	- Gebäude und Infrastruktur: Swisscom
	- Übertragungsanlagen: Stab BR APF
	Betrieb:
	- Im Normalfall:
	  - ziviler Teil: Swisscom im Auftrag SRG
	  - VRK-Teil: Swisscom im Auftrag Stab BR APF
	- In ausserordentlichen Lagen:
	  - Swisscom im Auftrag NAZ
	  - Ab Mob: Tc Br 40 im Auftrag Stab BR APF (Info Rgt 1)
		Radioversorgung der Bevölkerung in ausserordentlichen Lagen. Ab Bezug Schutzräume mit verstärkter Sendeleistung.
		Subsidiarität
		(zur Zeit noch in Abklärung)

INFRANET	Swisscom	Ständig betriebsbereites Sicherheitsnetz für Datenübertragung Netz für die Auslösung der ferngesteuerten stationären Sirenen SFI 457

Polizei:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
VULPUS Telematik	Bund (VBS), Swisscom	
WAN EJPD	Bund,Swisscom	
KKPKS-Intranet	Bund,Kantone,Swisscom	
Janus-Intranet	Bund,Kantone,Swisscom	
Internationale Verbindungen		

Wirtschaftliche Landesversorgung:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
öffentliche Fix-und Mobilnetze	Swisscom künftig evtl. auch Orange, Sunrise, 3G Mobile	Anschlüsse können in Swisscom-Netzen prorisiert werden (KWT resp NATEL D Plus).
Satellitenverbindungen	INMARSAT	Verbindung zur Hochseeflotte
Kurzwellenverbindungen	Swissradio	Verbindung zur Hochseeflotte beim Ausfall der Satellitenverbindungen

Kantone:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
POLYCOM	Bund, Kantone	Sicherheits- und Rettungsfunknetz (Zellular- und Direct-Modus)
Verwaltungsnetze	unterschiedlich	Regionalnetze im Gesamtsystem
Verkehrsleitnetze	Kantone und andere	Insbesondere für Nationalstrassen-netz

Zivile Rettungsorganisationen:

Bezeichnung	Eigentümer/Betreiber	Bemerkungen
öffentliche Fix-und Mobilenetze	Swisscom, künftig evtl. auch Orange, Sunrise, 3G Mobile	Anschlüsse können in Swisscom-Netzen prorisiert werden (KWT resp NATEL D Plus).
POLYCOM	Bund, Kantone	Sicherheits- und Rettungsfunknetz (Zellular- und Direct-Modus)

Aus dieser Aufstellung geht hervor, dass die Bedürfnisträger ihre nötigen Kommunikations-Infrastrukturen entweder selbst betreiben oder sie von einem Dienstleister beziehen. Zum Teil werden auch Vorleistungen, die notwendig sind, um Kommunikationsdienste zu produzieren, von privaten Unternehmen bezogen (z.B. Miete von Übertragungskapazität oder von Standorten, die benötigt werden, um ein Übertragungsnetz zu betreiben).

4 RISIKEN UND MASSNAHMEN

Grundsätzlich sind Kommunikations-Infrastrukturen ständig Risiken ausgesetzt. Bereits im ordentlichen Betrieb müssen die Betreiber der entsprechenden Netze umfassende Sicherheitsmassnahmen treffen. Wie der heutige Betrieb zeigt, sind diese Massnahmen auch weitgehend wirksam und die Verfügbarkeit der Infrastrukturen in der Schweiz sehr gross. Mit Bezug auf ausserordentliche Lagen soll jedoch im Folgenden eine grobe Risikoanalyse vorgenommen werden. Im Detail obliegt eine solche Analyse jeweils den einzelnen Bedürfnisträgern. Sie muss regelmässig aktualisiert werden.

4.1 Methodik der Risikoanalyse

Für die Anforderungen des vorliegenden Berichts wurde folgende Methode gewählt: Zunächst werden mögliche Gefahren identifiziert und sodann beurteilt, wie wahrscheinlich es ist, dass diese Ereignisse eintreten und wie hoch der Schaden ist, der dabei entstehen kann. Das Risiko wird somit aus der Eintretenswahrscheinlichkeit und der zu erwartenden Schadenshöhe ermittelt. Es geht dabei um die Eintretenswahrscheinlichkeit des Ereignisses im Rahmen einer ausserordentliche Lage. Wie gross die Wahrscheinlichkeit für das Eintreten der ausserordentlichen Lage selbst ist, wird dagegen nicht berücksichtigt. Von Bedeutung ist im Weiteren, dass bereits verwirklichte Massnahmen bei dieser Beurteilung mitberücksichtigt werden, das heisst in der Regel die Gefahrensituation entschärfen und den Handlungsbedarf somit vermindern.

Aufgrund dieser Überlegungen kann jeder Gefahr in der Risikomatrix (graphische Darstellung) ein Standort zugeordnet werden. Die Darstellung stellt die einzelnen Gefahren wertend zueinander und zeigt *tendenziell* die Erforderlichkeit von allenfalls noch zu treffenden Massnahmen auf.

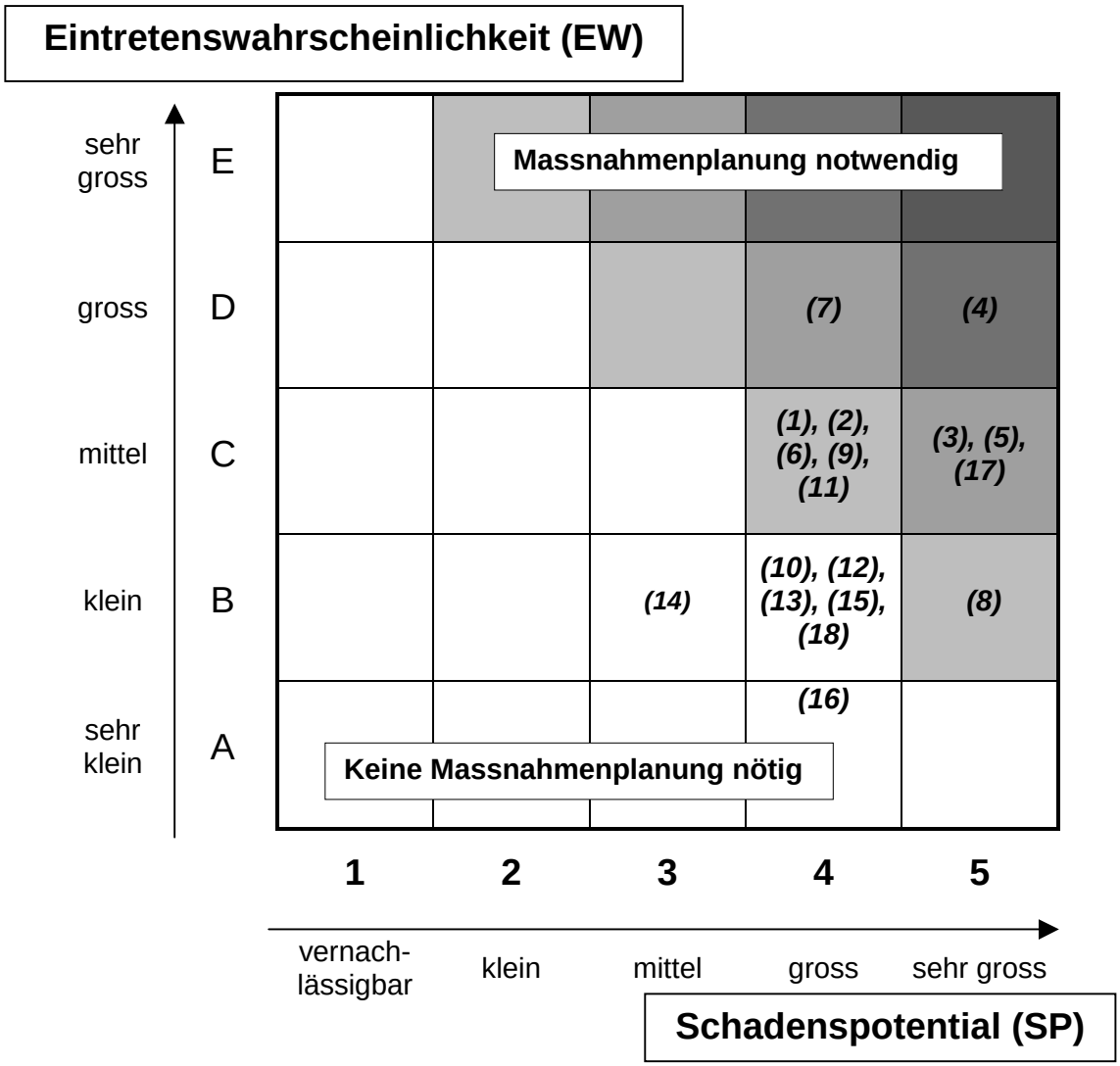

Abbildung 1: Risikomatrix (Die in der Matrix plazierten Nummern stehen für die unter Ziff. 4.2 beschriebenen einzelnen Risiken:

(1) Netzüberlastung, (2) kritische Pfade und Zetralisierung der Netzintelligenz, (3) technologische Entwicklung, (4) ausländische Technologien, (5) Netzbetriebszentren im Ausland, (6) Satelliten-Technologie, (7) Empfangsprobleme, (8) Privatisierung, (9) Aufteilung von Unternehmen, (10) Internationalisierung, (11) Personal, (12) Sabotage, (13) Energieausfall, (14) Zivilisationsunfälle, (15) Naturkatastrophen, (16) fehlende Kompatibilität, (17) Probleme im Bereich VRK-UKW 77 (18) Technische Monokultur.)

Die vorliegende Analyse erhebt nicht den Anspruch auf eine absolute, wissenschaftliche Genauigkeit. Angewandt durch Experten der Bedürfnisträger, erlaubt sie aber eine Selektion der Fälle, in denen staatlicher Handlungsbedarf besteht.

4.2 Risikoanalyse und daraus resultierende Massnahmen

Im Folgenden werden potentielle Gefahren gemäss der vorgehend beschriebenen Methode bewertet und allenfalls mögliche und nötige Massnahmen aufgezeigt. Die Gefahren können

dabei den fünf Kategorien Technik, Personal, IT-Branche, äussere Einwirkungen und Organisation zugeordnet werden.

4.2.1 Technik

Es handelt sich dabei um Risiken, die direkt in der Technik, welche der Infrastruktur zu Grunde liegt, gründen.

4.2.1.1 Netzüberlastung *(1)*

Beschreibung: Durch Überlastung können Netze vorübergehend ausfallen.

Bewertung: Die Netzbetreiber sind aus wirtschaftlichen Überlegungen selber bestrebt, die Netzkapazität nach der Hauptverkehrslast auszubauen. Die Erfahrung zeigt aber, dass es in ausserordentlichen Lagen trotzdem zu Überlastungen kommen kann. Art. 48 FMG (s. auch Art. 71 f. FDV) lässt eine Einschränkung des Fernmeldeverkehrs (Priorisierung) in ausserordentlichen Lagen zu. Dies bringt für die priorisierten Teilnehmer die Verfügbarkeit der entsprechenden Netze. Zu prüfen ist die Priorisierung von netzübergreifendem Verkehr im Rahmen der Interkonnektion.

Die Praxis (Überschwemmung in Brig vom 24. September 1993) hat zudem gezeigt, dass ein öffentlicher Aufruf der Behörden, das Telefonieren auf das Nötigste zu beschränken, durchaus seine Wirkung zeigt.

Das Gesetz sieht bei der Einschränkung des Fernmeldeverkehrs eine Entschädigung der Betroffenen vor, welche aber wenig detailliert geregelt ist.

Risikomatrix: Eintretenswahrscheinlichkeit (ES) mittel, Schadenspotential (SP) gross.

Massnahmen: Pflicht für Betreiber von wichtigen öffentlichen Netzen (Festnetz, Mobilfunknetz, IP-Netz), die Möglichkeit der Priorisierung von bestimmten Kundengruppen zu schaffen, sowie Gewährleistung der Priorisierung im Interkonnektionsbereich. Zudem ist die Frage der Entschädigung klarer zu regeln.

4.2.1.2 Kritische Pfade und Zentralisierung der Netzintelligenz *(2)*

Beschreibung: Bei kritischen Pfaden handelt es sich primär um nicht redundante Netzverbundsschnittstellen oder Kabelkanäle durch 'Nadelöhre'. Infolge des technischen Fortschritts und allenfalls aus Rationalisierungsüberlegungen besteht die Tendenz zur Netzsteuerung durch nicht oder nur mangelhaft redundante, zentrale Server.

Bewertung: Kritische Pfade entstehen überall dort, wo das Verkehrsaufkommen durch einige wenige Netzübergänge oder gar durch die gleichen Kabelkanäle geführt werden. Insbesondere betroffen sind Interkonnektionsschnittstellen unter Festnetzdienstanbieterinnen oder zwischen Mobil- und Festnetzen. Von einem Ausfall der Interkonnektionsschnittstellen wären jeweils alle Kunden einer Fernmeldedienstanbieterin betroffen, die mit anderen Kunden anderer Anbieterinnen kommunizieren möchten. Durch die Beschädigung von Kabelkanälen, in denen die Übertragungsleitungen mehrerer Anbieter im gleichen Kanal geführt werden (z.B. Gotthardtunnel) könnte zum gleichzeitigen Ausfall der Netze verschiedener, wichtiger Anbieter führen. Im Falle der Niederlande weiss man zum Beispiel, dass der Ausfall eines einzigen Knotens die gesamte Internetanbindung des Landes in Frage stellen würde.

Wie die jüngsten Beispiele zeigen, kann eine Störung in einem zentralen Server den Ausfall des ganzen Netzes provozieren, insbesondere wenn der Redundanz dieser Systeme zuwenig Aufmerksamkeit geschenkt wird.

Die gleiche Problematik besteht auch im Bereiche des Rundfunkes, wenn beispielsweise Kabelnetzbetreiber die Anspeisung mit den Grundversorgungsprogrammen ausschliesslich über Satellit vorsehen und zudem keine redundante Energieversorgung aufweisen.

Risikomatrix: EW mittel, SP gross.

Massnahmen: Auferlegung von Verfügbarkeitsvorschriften in Konzessionen. Deklarierungspflicht und in der Folge Erfassung von nichtredundanten Netzelementen im Netzbeschrieb der Konzession, bei meldepflichtigen Telekomanbietern auch im Rahmen der Registrierung.

4.2.1.3 Technologische Entwicklung *(3)*

Beschreibung: Die technische Entwicklung lässt Systeme veralten, bis sie mangels Kompatiblität nicht mehr einsetzbar sind.

Bewertung: Die Entwicklung im ICT-Bereich geht in rasantem Tempo voran. Es besteht hier ein regelrechter (technischer und wirtschaftlicher) Zwang zum technischen Nachvollzug. Systeme müssen stets aufgerüstet oder gar ersetzt werden. Mit dem Problem sind die Verantwortlichen bereits in ordentlichen Lagen konfrontiert. Dabei werden die Grundlagen für die Verfügbarkeit der Infrastruktur in der ausserordentlichen Lage geschaffen. Die Gefahr, dass Systeme während ausserordentlichen Lagen veralten, ist dagegen eher klein. Am gefährdetsten sind somit Systeme die ausschliesslich oder vor allem in der ausserordentlichen Lage benutzt werden (z.B. Infrastruktur VRK-UKW 77). Es kann vorkommen, dass diese in der ordentlichen Lage vernachlässigt werden und in der ausserordentlichen Lage somit nicht mehr oder nur beschränkt verfügbar sind.

Zu bemerken ist, dass die der Konkurrenz ausgesetzten Netzbetreiber einem grossen wirtschaftlichen Druck unterliegen, ihre Netze à jour zu halten.

Als positiv zu werten ist, dass die entsprechenden Technologien durch ihre Weiterentwicklung in der Regel sicherer werden. Dieser Fortschritt führt auf Grund der technischen Möglichkeiten und aus Rationalisierungsbestrebungen aber auch zu einer Zentralisierung der Intelligenz, welche wiederum Gefahren in sich birgt (siehe 4.2.1.2).

Risikomatrix: EW mittel, SP sehr gross.

Massnahme: Sensibilisierung der Verantwortlichen.

4.2.1.4 Ausländische Technologien *(4)*

Beschreibung: Abhängigkeit von Technologien, über welche die Schweiz nicht verfügt.

Bewertung: Es handelt sich hierbei um eine äusserst ernst zu nehmende Abhängigkeit mit grossem Risikopotential, sowohl hinsichtlich der Eintretenswahrscheinlichkeit als auch des Schadensausmasses. Die Handelsbilanz der Schweiz ist in allen Produktsegmenten des ICT-Sektors negativ. Es besteht also eine starke Auslandabhängigkeit, welche auch missbraucht werden kann, um auf die Schweiz oder in der Schweiz angesiedelte Unternehmen politischen oder wirtschaftlichen Druck auszuüben. Die Tatsache, dass die fraglichen Technologien zur Zeit vor allem aus Ländern importiert werden, die der Schweiz wohl gesinnt sind, entschärft die Situation nur beschränkt. In ausserordentlichen Lagen kann sich diese Problematik vor allem im Bereiche der Ersatzteilbeschaffung und teilweise beim second bzw. oft beim third level support bemerkbar machen. Allerdings erscheint gerade auf Grund des rasanten, technischen Fortschrittes eine Lagerhaltung, wie sie in anderen Bereichen der wirtschaftlichen Landesversorgung praktiziert wird, nur beschränkt als erfolgsversprechend, der Aufbau eines entsprechend autarken Industriezweiges gar als unrealistisch. Risikomatrix: EW gross, SP sehr gross.

Massnahmen: Lagerhaltung kaum möglich. Vertragliche Bindung von Lieferanten (in Krisensituationen nur beschränkt durchsetzbar).

Hier ist die Inkaufnahme eines überdurchschnittlichen Restrisikos wohl unvermeidlich.

4.2.1.5 Netzbetriebszentren im Ausland *(5)*

Beschreibung: Wenn Netzbetriebszentren ausschliesslich im Ausland liegen, ist eine Betriebssteuerung aus der Schweiz nicht oder nicht innert nützlicher Frist gewährleistet.

Bewertung: Es handelt sich hierbei um ein Phänomen, das einerseits mit der Internationalisierung der Märkte und andererseits mit ökonomischen Rationalisierungsprozessen zusammenhängt. Tatsächlich führt dies zu einer nicht zu unterschätzenden Abhängigkeit, da im Extremfall Netze aus dem Ausland 'per Knopfdruck' ausser Betrieb gesetzt werden könnten. Risikomatrix: EW mittel, SP sehr gross.

Massnahmen: Rechtliche Verpflichtung der Anbieter, lokale, in der Schweiz gelegene minimale Netzbetreibungszentralen bzw. -netzmanagementwerkzeuge einzurichten, die jederzeit durch Personal in der Schweiz autonom hochgefahren werden können.

4.2.1.6 Satelliten-Technologie *(6)*

Beschreibung: Abhängigkeit von (ausländischen) Satelliten.

Bewertung: Die Technik kommt beispielsweise bei der Anspeisung (Distribution) von Rundfunksendeanlagen oder bei der Telefonie (z.B. Hochseeschifffahrt) zur Anwendung. Die Schweiz verfügt aus primär wirtschaftlichen Überlegungen über keine eigenen Satelliten. Wie die Erfahrung zeigt, ist deren Verfügbarkeit gerade in internationalen Krisen keineswegs gewährleistet. Es handelt sich somit um eine absolute Abhängigkeit, auch wenn der Satelliten-Technik in ausserordentlichen Lagen mit Ausnahme der Hochseeschifffahrt und der Auslandvertretungen bis anhin keine grosse Bedeutung zukam. Gerade in diesen Fällen wurde der Kurzwellen-Funk als Alternative betrachtet. Im Bereiche der Hochseeschifffahrt ist dieser aber aus wirtschaftlichen Überlegungen nicht mehr unumstritten. Risikomatrix: EW mittel, SP gross.

Massnahme: Alternativen sicherstellen (KW-Technik zum Teil fraglich). Hier muss allenfalls ein überdurchschnittliches Restrisiko in Kauf genommen werden.

4.2.1.7 Technische Monokultur *(18)*

Beschreibung: Allgmein ist zu beobachten, dass in der ICT-Branche immer weniger Lieferanten immer mehr Infrastruktur (Hard- und Software) produzieren.

Bewertung: Einerseits können durch technische Monokulturen ganze Verwaltungszweige von einem Lieferanten abhängig werden. Es besteht ein ähnliches Problem wie bei der Auslandabhängigkeit, unter Ziff. 4.2.1.4 beschrieben. Andererseits kann die Situation auch die Verbreitung von fehlerhaften Komponenten begünstigen. Besonders problematisch wird es dann, wenn suboptimale Infrastruktur nicht mehr substituierbar ist. Tendenziell führt aber wohl eher die technische Überlegenheit von Produkten zu Monokulturen. Risikomatrix: EW klein, SP gross.

Massnahmen: Keine Massnahmen erforderlich.

4.2.1.8 Empfangsprobleme *(7)*

Beschreibung: Technische Unzulänglichkeiten beim Empfänger ausserhalb der Verwaltung verhindern den Informationsfluss (insbesondere "Höhrergewohnheiten" im Bereiche des Rundfunks, Nichtverfügbarkeit von portablen Empfangsgeräten).

Bewertung: Die betroffenen Empfänger sind sich der Problematik meistens gar nicht bewusst. Es besteht zudem eine grosse Abhängigkeit von den CATV Betreibern. Risikomatrix: EW gross, SP gross.

Massnahme: Sensibilisierung der betroffenen Bevölkerungskreise.

4.2.2 IT-Branche

Im Zuge der Liberalisierung der betroffenen Märkte, kam es zu tiefgreifenden Veränderungen der ökonomischen Strukturen, welche auch die Verhaltensmuster der Akteure beeinflussen.

4.2.2.1 Privatisierung *(8)*

Beschreibung: Bis 1998 stellte hauptsächlich die staatliche PTT die Netzinfrastruktur zur Verfügung. Mit deren Privatisierung und der Öffnung der Märkte für andere Anbieter hat sich die Situation grundlegend verändert. Private Unternehmen entscheiden naturgemäss nach privatwirtschaftlichen Kriterien und nicht aus sicherheitspolitischer Sicht.

Bewertung: Bisher hat der Bund durch seine gesetzlich vorgeschriebene Aktienmehrheit einen erheblichen Einfluss auf die Geschäftspolitik der Swisscom, auch wenn er die Interessen der Minderheitsaktionäre gemäss aktienrechtlichen Vorgaben gebührend zu berücksichtigen hat. Bei anderen Netzbetreibern ist das nicht der Fall. Bei der Swisscom erhält dieser Umstand allerdings grössere Bedeutung, weil diese nach wie vor den grössten Teil der Netzinfrastruktur (Telekommunikation und Rundfunk) betreibt, mithin auch Anlagen die für die Information und die Kommunikation in ausserordentlichen Lagen von grosser Bedeutung sind.

Gemäss Art. 47 FMG können Betreiber von landeswichtigen Telekommunikations-Infrastrukturen unabhängig von der Eigentümerschaft bereits heute verpflichtet werden, bestimmte Leistungen in ausserordentlichen Situationen zur Verfügung zu stellen und dazu bestimmte Vorkehrungen zu treffen. Eine entsprechende Pflicht kann im Rahmen von Konzessionen, Verträgen oder Verfügungen begründet werden. Dies wurde im Falle der Swisscom auch in mehreren Fällen getan. Die eigentliche Requisition ausserordentlichen Lagen bleibt dabei zusätzlich vorbehalten. Im Bereiche des Rundfunkes ist eine solche grundsätzliche Pflicht dagegen noch nicht vorgesehen. Diese Lücke wurde bei den RTVG-Revisionsarbeiten erkannt und ist in diesem Rahmen zu schliessen.

In diesem Zusammenhang kann nicht ausser Acht gelassen werden, dass auch private Netzbetreiber im Eigeninteresse Sicherheitsansprüche an ihre Netze stellen, welche sich oft mit sicherheitspolitischen Anforderungen decken.

Risikomatrix: EW klein, SP sehr gross.

Massnahmen: Konsequente Anwendung von Art. 47 FMG auf sämtliche bedeutenden Betreiber von Kommunikations-Infrastrukturen. Bedürfnisse regelmässig aktualisieren und mit Leistungserbringern verhandeln, nötigenfalls Auflagen machen. Schaffung einer analogen Regelung für den Rundfunkbereich resp. Ausdehnung der Anwendbarkeit auf den Rundfunkbereich.

4.2.2.2 Aufteilung von Unternehmen *(9)*

Beschreibung: Es geht um die Aufteilung von Unternehmen (Konzentration auf Kerngeschäfte), die in einem Sektor bisher in umfassender Weise tätig waren (Planung, Erstellung, Betrieb), in verschiedene, spezialisierte und verselbständigte Unternehmen.

Bewertung: Eine solche Aufteilung einer Unternehmung, wie sie bei der Swisscom in Umsetzung ist, kann die Koordination von Massnahmen erschweren. Risikomatrix: EW mittel, SP gross.

Massnahmen: Konsequenter Nachvollzug von solchen Unternehmensaufteilungen im regulatorischen Bereich (v.a. bei Konzessionen). Sensibilisierung der betroffenen Entscheidungsträger zu vernetztem und gesamtheitlichem Denken.

4.2.2.3 Internationalisierung *(10)*

Beschreibung: Im Zuge der Liberalisierung der bedeutendsten Telekommunikationsmärkte rund um den Globus entstanden internationale Allianzen zwischen Anbietern. Wirtschaftliche Grösse erscheint als Gebot der Stunde. Es gibt Befürchtungen, ausländische Mehrheitsbeteiligungen an inländischen Netzbetreibern widersprächen schweizerischen Sicherheitsinteressen, zumal der staatliche Zugriff auf ausländische Einheiten von internationale Konzernen schwieriger als auf nationale Unternehmen sein dürfte.

Bewertung: Die Globalisierung ist ein Phänomen, dem sich die Schweiz nicht entziehen kann. Eine ausländische Beteiligung (selbst eine Mehrheitsbeteiligung) stellt per se noch keine Gefahr für die Telekommunikations- und Rundfunkinfrastruktur dar. Die Aussage, es handle sich dabei um einen 'Verkauf ins Ausland', verzerrt die Realität, da sie in diesem Kontext suggeriert, es würde Infrastruktur ins Ausland geschafft. Viele in der Schweiz ansässige Firmen werden über Aktien- oder andere Beteiligungen mehrheitlich aus dem Ausland beherrscht, ohne dass sie damit per se ein Risiko für die Sicherheit in ihrem Tätigkeitsbereich darstellen, dies auch nicht, wenn sie in existentiellen Bereichen wie beispielsweise der Energieversorgung tätig sind.

Die Möglichkeit, dass im Vorfeld einer ausserordentlichen Lage Reserveausrüstung ins Ausland geschafft werden könnte, ist nur schon deshalb von untergeordneter Bedeutung, da die Eratzlagerhaltung bei privaten Anbietern aus Überlegungen der Wirtschaftlichkeit nicht sehr verbreitet sein dürfte.

Zugegebenermassen bietet eine international tätige Unternehmung eine grössere Fläche für 'Angriffe' von verschiedenster Seite (Regulatoren, Konkurrenten, Kunden, Geschädigte, etc.) als eine Unternehmung die lediglich auf einem nationalen Markt auftritt. Dies allerdings als Gefahr für die sicherheitsrelevante Infrastruktur zu bezeichnen, ginge zu weit. Umgekehrt sind grosse, global tätige Firmen in ihrem Bestehen häufig stabiler.

In der Regel verfügen internationale Konzerne über nationale Tochtergesellschaften, welche effektiv als Infrastrukturbetreiber auftreten. Das Wissen, sich als Behörde auch im globalen Umfeld durchsetzen zu können und die internationale Rechtshilfe relativiert die Problematik der Internationalisierung ein Stück weit.

Risikomatrix: EW klein, SP gross.

Massnahmen: Keine Massnahmen erforderlich.

4.2.3 Personal *(11)*

Beschreibung: Es geht hier um die Verfügbarkeit von Fachkräften, welche über das notwendige Know-how verfügen, um die sicherheitsrelevante Infrastruktur zu handhaben.

Bewertung: Es handelt sich dabei um eine äusserst ernst zu nehmende Abhängigkeit mit grossem Risikopotential, insbesondere hinsichtlich des Schadensausmasses. Im Vordergrund steht nicht das Know-how für den Aufbau der Infrastruktur, denn in der Regel besteht diese in ausserordentlichen Lagen schon. Vielmehr geht es um den Betrieb und den Unterhalt von Systemen und Netzen. In diesen Bereichen verfügen die Verantwortlichen auf Benützerseite oft über zu wenig eigenes Know-how, sondern sind auf externes Expertenwissen angewiesen. Aber gerade in ausserordentlichen Lagen ist dieses Wissen unter Umständen nur noch beschränkt verfügbar. Handelt es sich dabei noch um ausländisches Know-how, kann dies die Situation je nach Art der Krise noch zusätzlich erschweren.

Die Eintretenswahrscheinlichkeit und somit das Risiko wächst zudem typischerweise mit der Dauer der Krise.

Inwieweit die im Rahmen des neuen Bundespersonalrechts eingeführte Flexibilität im Bereiche der Entlöhnung für die Rekrutierungsproblematik bei Fachkräften Besserung bringt, kann im Moment noch nicht abgeschätzt werden.

Art. 69 FDV sieht vor, dass Fernmeldedienstanbieterinnen, deren Anlagen oder Dienste in ausserordentlichen Lagen von Bedeutung sind, verpflichtet werden können, sich im Hinblick auf solche Situationen zu organisieren, insbesondere auch das notwendige Personal zur Verfügung zu stellen. Daneben ist im Militärgesetz und den entsprechenden Nebenerlassen die Militarisierung der Swisscom auch in personeller Hinsicht geregelt.

Risikomatrix: EW mittel (zunehmend mit der Dauer der Krise), SP gross.

Massnahmen: Von der Möglichkeit, externes Expertenwissen durch Schaffung von finanziellen und anderen Anreizen zu internalisieren, muss für vom Bund betriebene Infrastrukturen konsequent Gebrauch gemacht werden. Durch interne Bildungsmassnahmen kann das eigene Know-how zusätzlich verbessert werden. Schliesslich muss der vertraglichen Bindung von externen Experten das nötige Augenmerk geschenkt werden. Im Rahmen der Armee XXI ist die Personalverfügbarkeit für die landeswichtige Kommunikation- und Rundspruchversorgung sicherzustellen.

4.2.4 Äussere Einwirkungen

Es handelt sich dabei um Eingriffe Dritter oder um Naturereignisse.

4.2.4.1 Sabotage *(12)*

Beschreibung: Es geht um gezielte Angriffe auf Infrastrukturen (physisch oder virtuell): Hakking, Denial of Services Attacken, Leitungsbeschädigungen, Viren, Frequenzstörungen etc.

Bewertung: Ein gezielter Angriff kann durch Dritte, aber auch durch eigene Mitarbeiter verübt werden. Die Motive können hier von unterschiedlichster Art sein: Wirtschaftliche oder politische Interessen, Rachegefühle, Neugier etc. Angriffe durch eigene Leute nehmen die Betroffenen oftmals gar nicht als solche wahr, Angriffe Dritter erst, wenn es zu spät ist. Im Zuge der Tendenz zur Zentralisierung von Netzintelligenz und unter Berücksichtigung der Existenz von kritischen Pfaden erscheinen gewisse Strukturelemente als besonders sensibel (vgl. dazu auch die Ausführungen unter Ziff. 4.2.1.2). Die meisten dieser Handlungen können bereits heute strafrechtlich sanktioniert werden. Allgemein ist zu beobachten, dass es sich dabei um eine Gefahr handelt, derer man sich in weiten Kreisen sehr wohl bewusst ist und gegen welche vielerorts schon geeignete Massnahmen realisiert wurden oder zumindest geplant sind (Firewalls, Chiffrierung, Härten von sensitiven Anlagen, etc.; vgl. dazu auch die unter Ziff. 1.2 beschriebenen staatlichen und privaten Bemühungen). Risikomatrix: EW klein, SP gross.

Massnahmen: Keine weiteren Massnahmen erforderlich (neben den Massnahmen im Rahmen des Konzeptes 'Information Assurance').

4.2.4.2 Energieausfall *(13)*

Beschreibung: Energieausfälle können zum Zusammenbruch von Netzen und Systemen führen.

Bewertung: Vorübergehende, örtliche Energieausfälle können nie ausgeschlossen werden. Da die meisten Betreiber auf diesen Fall vorbereitet sein dürften (Notstromaggregate), besteht hier wenig Handlungsbedarf. Ein grossflächiger Energieausfall hätte allerdings schon nach kurzer Zeit verheerende Auswirkungen auf Gesellschaft und Staat. Im Rahmen der wirtschaftlichen Landesversorgung sind hier bereits griffige Massnahmen vorgesehen. Risikomatrix: EW klein, SP gross.

Massnahmen: Keine weiteren Massnahmen erforderlich.

4.2.4.3 Zivilisationsunfälle *(14)*

Beschreibung: Atomunfälle, Chemieunfälle, grosse Verkehrsunfälle, etc.

Bewertung: Je nach Art können Zivilisationsunfälle auch die Kommunikations- und Informations-Infrastrukturen, welche gerade nötig wären, um die Krise zu bewältigen, zerstören. Festnetze erscheinen hier besonders anfällig, obschon auch Mobilnetze teilweise von terrestrischen Anlagen abhängig und damit ebenfalls gefährdet sind. In der Regel stehen für sol-

che Situationen genügend Funkmittel zur Verfügung (von Vorteil mit Direct-Mode, neu auch POLYCOM). Risikomatrix: EW klein, SP mittel.

Zur Notwendigkeit der Nutzung der öffentlichen Netze und der Überlastungsproblematik vgl. die Ausführungen unter Ziff. 4.2.1.1.

Massnahmen: Keine weiteren Massnahmen nötig.

4.2.4.4 Naturkatastrophen *(15)*

Beschreibung: Überschwemmungen, Lawinen, Stürme etc.

Bewertung: Naturkatastrophen können auch die Kommunikations- und Informations-Infrastrukturen, welche gerade nötig wären, um die Krise zu bewältigen, zerstören. Festnetze erscheinen hier besonders anfällig, obschon auch Mobilnetze teilweise von terrestrischen Anlagen abhängig und damit ebenfalls gefährdet sind. In der Regel stehen für solche Situationen genügend Funkmittel zur Verfügung (von Vorteil mit Direct-Mode, neu auch POLYCOM). Risikomatrix: EW klein, SP gross.

Zur Notwendigkeit der Nutzung der öffentlichen Netze und der Überlastungsproblematik vgl. die Ausführungen unter Ziff. 4.2.1.1.

Massnahmen: Keine weiteren Massnahmen nötig.

4.2.5 Organisation

4.2.5.1 Fehlende Kompatibilität *(16)*

Beschreibung: Mangels Kompatibilität der Techniken oder mangels standardisierter Schnittstellen können verschieden Benutzerkreise nicht miteinander kommunizieren.

Bewertung: Das Problem ist seit längerem erkannt. Mit der beabsichtigten Einführung von POLYCOM (Tetrapol-Standard) ist im Moment ein gesamtschweizerisches Sicherheits- und Rettungsfunknetz im Aufbau begriffen. Allerdings besteht dieses aus zahlreichen kantonalen Teilnetzen und es ist den Kantonen freigestellt, ob und wann sie diesen Standard einführen. Der Bund koordiniert dabei die Einführung und realisiert die nationale Komponente (v.a. Grenzwacht, Armee). Auch mit dem benachbarten Ausland ist man bestrebt, kompatible Lösungen zu finden. Im Moment werden dort, wo keine Gemeinschaftskanäle zur Verfügung stehen, noch Funkgeräte ausgetauscht. Aber auch im europäischen Raum scheint sich der Tetrapol-Standard bei Sicherheits- und Rettungskräften allgemein durchzusetzen. Risikomatrix: EW sehr klein, SP gross.

Massnahmen: Keine weiteren Massnahmen erforderlich.

4.2.5.2 Probleme im Bereich VRK-UKW 77 *(17)*

Beschreibung: Beim VRK-UKW 77 handelt es sich um ein integriertes, terrestrisch gestütztes, drahtloses Rundfunkverbreitungssystem über UKW. Es stellt landesweit die Radioversorgung in ausserordentlichen Lagen sicher und ist heute das einzige Verbreitungsmittel, welches dem Bundesrat für die Information der Bevölkerung in Schutzräumen zur Verfügung steht. Gebäude und Infrastruktur sind im Eigentum der Swisscom. Die gesetzlichen Grundlagen und Aufträge stammen aus den frühen 80-er-Jahren. Akteure waren damals im Wesentlichen die APF (heute Stab BR APF) und die ehemaligen PTT-Betriebe.

Seither hat sich durch die Marktliberalisierung und den damit verbundenen Reorganisationen vieles verändert, insbesondere im organisatorischen Bereich (Trennung der PTT in Post und Swisscom, Schaffung BAKOM, neues FMG und RTVG, etc.). Die Neuverteilung der Zuständigkeiten und Verantwortlichkeiten wurden dabei gesetzgeberisch nicht oder nur ungenü-

gend nachvollzogen. Neu muss auch die Reorganisation der Armee XXI berücksichtigt werden

Eine früher ins Auge gefasste Veräusserung des Broadcasting-Bereichs durch die Swisscom gibt in breiten Kreisen zu weiteren Bedenken Anlass (vgl. dazu auch 4.2.2.1).

Die Swisscom hat bei der terrestrischen, drahtlosen Rundfunkverbreitung praktisch nach wie vor das Monopol.

Bewertung:

- Regelungslücken

Im Zusammenhang mit den Besitzverhältnissen, dem Unterhalt und der Nutzung der VRK-UKW 77-Sendeanlagen bestehen einige Regelungslücken, welche zum Teil schon vor der Marktliberalisierung vorhanden waren, und in der Folge etliche Ungeklärtheiten auf der Verantwortlichkeitsebene. Betroffene Stellen schienen sich dieser Problematik zum Teil gar nicht bewusst. Der Handlungsbedarf wurde zwischenzeitlich erkannt. Der Stab BR APF, die NAZ, das BAKOM, die Swisscom und die SRG klären insbesondere die Prozessabläufe im Zusammenhang mit der Nutzung der VRK/UKW77-Sendeinfrastruktur durch die SRG ab.

- Veräusserung der Infrastruktur

Es ist geplant, dass die Swisscom den Unternehmensbereich Broadcasting mit den VRK-UKW 77-Sendeanlagen in eine 100% Tochtergesellschaft überführt. Ein Verkauf steht heute nicht zur Diskussion, ist aber in Zukunft zumindest nicht ausgeschlossen. Wohl hat sich die Swisscom gegenüber dem Bund (VBS) vertraglich verpflichtet, die Pflicht zum Betrieb und Unterhalt des VRK-UKW 77-Netzes auf eine allfällige Rechtsnachfolgerin zu übertragen. Sollte diese mangels wirtschaftlichen Interesses die Anlagen ausser Betrieb setzen oder im Unterhalt vernachlässigen, wären Funktionsfähigkeit und Einsatzbereitschaft in ausserordentlichen Lagen eingeschränkt oder verunmöglicht. Entsprechend könnte der Stab BR APF seine Aufgabe nicht mehr wahrnehmen. Die Interventionsmöglichkeiten des Bundes beschränkten sich diesfalls momentan auf vertragsrechtliche Instrumente. Bis zum Inkrafttreten des neuen RTVG fehlt eine gesetzliche Verpflichtung des Eigentümers bzw. des Betreibers der Sendeanlagen, diese einsatzbereit und funktionstüchtig zu halten, oder aber eine Möglichkeit des Bundes, analog zu Artikel 47 FMG (siehe Ziffer 4.2.2.1), den Betreiber der VRK/UKW77-Sendenanlagen zu bestimmten Vorkehrungen zu verpflichten.

Risikomatrix: EW mittel, SP sehr gross

Massnahmen: Schliessen der Regelungslücken (insbesondere in den Bereichen RTVG/FMG und MG) unter Definition der neuen Zuständigkeiten und Festlegung der Abläufe. Im Weiteren ist bei einer allfälligen Veräusserung der Broadcasting-Aktivitäten durch die Swisscom zu gewährleisten, dass sämtliche, in diesem Zusammenhang stehenden Pflichten (einschliesslich der Geheimhaltung) auf den Erwerber übergehen und der Bund seine Interessen gegenüber diesem wirksam durchsetzen kann. Schaffung einer analogen Bestimmung zu Art. 47 FMG im Rahmen der RTVG-Revision (resp. Anwendbarkeit von Art. 47 FMG auch im Rundfunkbereich).

4.3 Risiken und Massnahmen im Überblick

In der folgenden Tabelle werden diejenigen Risiken, welche nach Massnahmen rufen, zusammenfassend dargestellt. Darüber hinaus werden bezüglich der geforderten Massnahmen entsprechende Verantwortlichkeiten zugewiesen.

Risiken	**Massnahmen**	**Verantwortlichkeiten**	**Bemerkungen** (insbesondere massgebende Erlasse)
Netzüberlastung (4.2.1.1)	• Prüfung der Einführung einer Pflicht für sämtliche Fix- und Mobilnetzbetreiber, Priorisierung vornehmen zu können • Gewährleistung der Priorisierung auch im Interkonnektionsbereich • Entschädigungsfrage klarer regeln	• Zuständige Stellen im Rahmen Gesamtverteidigung in Zusammenarbeit mit BAKOM • Verordnungsgeber	FDV
Kritische Pfade und Zentralisierung der Netzintelligenz (4.2.1.2)	• Auflagen bzgl. Verfügbarkeit • Erfassung von nichtredundanten Netzelementen in Konzession oder im Rahmen der Meldepflicht	• BAKOM, evtl. Verordnungsgeber • BAKOM	• Konzessionen, evtl. FDV • Netzbeschrieb
Technologische Entwicklung (4.2.1.3)	Sensibilisierung der Verantwortlichen	Verwaltungsinterne und -externe Kompetenzzentren (VBS, ISB, BIT, InfoSurance)	
Ausländische Technologien (4.2.1.4)	• Lagerhaltung, wo überhaupt sinnvoll • Vertragliche Bindung von Lieferanten	• BIT und Supportstellen in Departementen • Netzbetreiber	***Restrisiko bleibt überdurchschnittlich***
Netzbetriebszentren im Ausland (4.2.1.5)	Schaffung der Pflicht für Betreiber, Netze auch von der Schweiz aus autonom bedienen zu können	• Gesetz- resp. Verordnungsgeber • Prüfung der Einhaltung von Auflage durch BAKOM	FMG und Ausführungsverordnungen
Satelliten-Technologie (4.2.1.6)	Alternativen sicherstellen		KW-Technik zum Teil fraglich ***Restrisiko bleibt überdurchschnittlich***
Empfangsprobleme (Rundfunk) (4.2.1.8)	Sensibilisierung der betroffenen Bevölkerungskreise	• Stab BR APF • Programmveranstalter	
Privatisierung (4.2.2.1)	• Konsequente Anwendung von Art. 47 FMG auf sämtliche bedeutenden Betreiber von Kommunikations-Infrastrukturen • Konsequente Aktualisierung • Strenge Kontrolle • Schaffung einer analogen Bestimmung zu Art. 47 FMG im Rundfunkbereich (resp. Anwendbarkeit von Art. 47 FMG auch im Rundfunkbereich)	• Zuständige Stellen im Rahmen der umfassenden und flexiblen Sicherheitskooperation in Zusammenarbeit mit BAKOM • Gesetzgeber	• Auflagen im Rahmen der Konzessionierung

Aufteilung von Unternehmen (4.2.2.2)	• Konsequenter Nachvollzug im regulatorischen Bereich • Sensibilisierung zu vernetztem und gesamtheitlichen Denken bei den betroffenen Entscheidungsträgern	• BAKOM • Bedürfnisträger	• Auflagen im Rahmen der Konzessionierung
Personal (4.2.3)	• Finanzielle und andere Anreize schaffen, um Fachkräfte zu gewinnen • Allg. Bildungsmassnahmen • Vertragliche Bindung von externen Experten • Requirierung von Personal • Militarisierung und/oder Dienstbefreiung des militärpflichtigen Personals	• Personalverantwortliche Bundesverwaltung • Bundesrat • Verantwortliche im Beschaffungswesen • Zuständige Stellen Armee	• Schaffung von Standardverträgen • Militärgesetz und Verordnungen im Rahmen Armee XXI
Probleme im Bereich VRK-UKW 77 (4.2.5.2)	• Schliessung der Regelungslücken unter Definition der neuen Zuständigkeiten und Abläufe • Bei einer Veräusserung der Infrastruktur durch die Swisscom konsequente Übertragung der Pflichten auf den Erwerber • Schaffung einer analogen Bestimmung zu Art. 47 FMG im Rundfunkbereich (resp. Anwendbarkeit von Art. 47 FMG auch im Rundfunkbereich)	• Gesetz- resp. Verordnungsgeber (Prüfen durch BAKOM und Stab BR APF)	• RTVG, FMG, MG und Verordnung über den Stab Bundesrat Abteilung Presse und Funkspruch sowie Verordnung Tc Br 40

5 ZUSAMMENFASSENDE ERGEBNISSE

Informationstechnologien sind nicht nur Garanten für die ökonomische Entwicklung sondern auch für die Funktionsfähigkeit von Regierung und Verwaltung. Sie sind der Lebensnerv unserer Gesellschaft schlechthin. Diese Abhängigkeit birgt nicht zu unterschätzende Risiken und Gefahren in sich.

In ausserordentlichen Lagen besteht in der Regel ein erhöhter Informations- und Kommunikationsbedarf. Für die Verantwortungsträger sind Informationen nicht nur Entscheidungsgrundlage sondern auch Führungsmittel. Aber auch die Bevölkerung ist in Krisen vermehrt auf Information angewiesen. Die Sicherheitsansprüche an Informations- und Kommunikations-Infrastrukturen in ausserordentlichen Lagen sind somit gross. Eine absolute Sicherheit ist jedoch weder technisch möglich noch wirtschaftlich tragbar.

Befürchtungen, die nationalen Sicherheitsinteressen bzgl. Informations- und Kommunikations-Infrastrukturen könnten nicht mehr gewährleistet sein, sind vor diesem Hintergrund ernst zu nehmen. Der vorliegende Bericht wurde denn auch zum Anlass genommen, mögli-

che Risiken in einer Gesamtsicht aufzuzeigen und dieser bereits umgesetzte, geplante sowie weitere nötige Massnahmen gegenüberzustellen.

Der Katalog von möglichen Ereignissen, welche diesen Sicherheitsinteressen in ausserordentlichen Lagen entgegenstehen, ist gross. Es ist wichtig, die einzelnen Gefahren in ihrem Gesamtzusammenhang zu sehen, um so die wahren Relationen und Abhängigkeiten zu erkennen.

Eine Risikoanalyse zeigt, dass die grössten Risiken, zu deren Minderung oder zur Minderung derer Auswirkungen Massnahmen notwendig sind, in den Bereichen Technologieabhängigkeit, organisatorische Fragen und Verfügbarkeit von qualifiziertem Personal liegen.

Auf Grund des ausgewiesenen Handlungsbedarfs zu erwähnen ist dabei die ausgeprägte Abhängikeit von ausländischen Technologien, welche inländischen Netzen zu Grunde liegen. Aus praktischen Gründen wird aber gerade hier auch künftig ein überdurchschnittliches Restrisiko in Kauf genommen werden müssen. Ähnlich verhält es sich bzgl. Einsatz von Satelliten-Technologie bei der Telekommunikation in den Bereichen Hochseeschifffahrt und auswärtige Angelegenheiten. Auch die rasante, technologische Entwicklung kann sich, sofern sie von den Anwendern nicht konsequent nachvollzogen wird, nachteilig auf die Sicherheit von Netzwerken auswirken. Als weitere Risiken technischer Art, denen mit geeigneten Massnahmen zu begegnen wäre, sind zu erwähnen: Netzüberlastungen mangels Kapazität, kritische Pfade (nicht oder zuwenig redundante Transportwege) und Tendenzen zur Zentralisierung der Netzintelligenz (ein Server steuert das ganze Netz), was zu einer erheblichen Anfälligkeit von Systemen führen kann. Im Bereiche des Rundfunks verdient im Weiteren die Empfangsproblematik erwähnt zu werden. Diesen Risiken ist, sofern sie nicht als mit vernünftigem Aufwand unvermeidbar hinzunehmen sind, im Wesentlichen mit klaren Auflagen im Rahmen der Konzessionierung oder Rechtsetzung und mit nachfolgenden Kontrollen zu begegnen. Daneben soll bei den Betroffenen durch eine hartnäckige Sensibilisierung ein Risikobewusstsein geschaffen werden: Das Kennen einer Gefahr verkleinert diese.

Ein beträchtliches Risiko ist auch in personeller Hinsicht zu orten. So sind die Benützer der IT-Infrastruktur bezüglich Betrieb und Unterhalt oftmals in bedenklichem Ausmass auf externes Know-how angewiesen, welches in ausserordentlichen Lagen unter Umständen nicht verfügbar ist. Dieser Know-how-Abhängigkeit muss mit Massnahmen im Bildungsbereich begegnet werden. Langfristig könnte dabei in beschränktem Mass auch der Technologieabhängigkeit begegnet werden. Dies bedingt einerseits Grundwissen, aufgebaut in der fachlichen Grundausbildung (insbesondere Hochschulen und Fachschulen, Forschung) und andererseits spezialisiertes Fachwissen im Rahmen (der häufig betrieblich organisierten) Weiterbildung. Daneben muss im Rahmen der Personalrekrutierung durch Schaffen von Anreizen wieder vermehrt Expertenwissen in die Verwaltung geholt werden.

Während mit der Technologie- und Know-how-Abhängigkeit wohl ein Stück weit auch gelebt werden muss, kann der Staat insbesondere organisatorischen Risiken mittels geeigneten Massnahmen weitestgehend begegnen. Im Bereiche VRK-UKW 77 sollen daher die im Rahmen der Liberalisierung in organisatorischer Hinsicht entstandenen Regelungslücken (Verantwortlichkeiten und Abläufe) umgehend geschlossen werden.

Ereignisse wie die ausländische Beteiligung an nationalen Betreiberfirmen stellen dagegen weniger eigenständige Risiken dar, da sie mittels Auflagen an die Betreiber in Griff gehalten werden können. Sie sind tendenziell weniger risikobehaftet als andere Gefahren wie eben die Technologie- und Know-how-Abhängigkeit. Als Folge der Internationalisierung muss aber doch geprüft werden, welche regulatorischen Massnahmen gewährleisten, dass für die Schweiz lebenswichtige Netze und Systeme unabhängig der Eigentümer in ausserordentlichen Lagen vom Inland aus gesteuert werden können.

Insgesamt kann festgestellt werden, dass heute die Sicherheit der Kommunikations-Infrastrukturen in ausserordentlichen Lagen - nicht zuletzt auf Grund bereits getroffener Massnahmen - weitgehend gewährleistet ist. Mit Blick auf laufende und zukünftige Entwicklungen sollen aber im Sinne einer wirtschaftlich vertretbaren Optimierung zusätzliche Mass-

nahmen getroffen und in der Folge nach Bedarf auch aktualisiert sowie ergänzt werden. Im Allgemeinen sollen Verantwortungs- und Entscheidungsträger vermehrt und umfassend über Abhängigkeiten und Sicherheitsrisiken informiert werden, um die nötige Sensibilität zu erlangen, Gefahren richtig und rechtzeitig zu begegnen. In diesem Zusammenhang sind auch Veranstaltungen wie die strategische Führungsübung INFORMO und das Engagement des Bundes in der Stiftung InfoSurance von hervorragender Bedeutung. Sie ermöglichen in diesem Bereich den Wissens- und Erfahrungsaustausch zwischen Wirtschaft und Verwaltung. Daneben ist vollumfänglich zu gewährleisten, dass die zur Kommunikation in ausserordentlichen Lagen erforderlichen Leistungen der Betreiber über Art. 47 FMG definiert und sichergestellt werden. Dabei haben die Bedürfnisträger, insbesondere die im Rahmen der umfassenden und flexiblen Sicherheitskooperation zuständigen Stellen, ihren Bedarf an Vereinbarungen und Auflagen laufend zu formulieren. Vereinbarungen könnten von den Bedürfnisträgern direkt mit den Betreibern eingegangen werden, wogegen ComCom und BAKOM Auflagen als Konzessionsbehörde erlassen oder das BAKOM solche im Rahmen der Rechtsetzung beantragt. In der Folge ist die Einhaltung der Vereinbarung und der Auflagen von den besagten Stellen permanent zu überprüfen. Im Rahmen der laufenden Revision des RTVG werden zusätzliche Auflagen im Bereich von Rundfunk und Telekommunikation geprüft. Dabei soll insbesondere eine analoge Bestimmung zu Art. 47 FMG geschaffen, resp. die Anwendbarkeit von Art. 47 FMG auf den Rundfunkbereich ausgedehnt werden. Diese Vorlage wird das Parlament voraussichtlich im Frühjahr 2002 zur Beratung erhalten.

Abschliessend sei zudem nochmals darauf hingewiesen, dass es bei der Optimierung von Sicherheit nicht die alle Probleme lösende 'Supermassnahme' gibt, sondern dass sich eine umfassende Sicherheitskonzeption wie ein Mosaik aus vielen, kleinen Elementen zusammensetzt. Und letztlich muss auch immer wieder die Frage gestellt werden: Welches Restrisiko ist man gewillt oder genötigt einzugehen?