Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022

vom 8. Dezember 2017

Der Schweizerische Bundesrat
beschliesst:

Zusammenfassung

Als kritische Infrastrukturen (KI) werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind. Dazu zählen etwa die Energieversorgung, der Personen- und Güterverkehr oder die medizinische Versorgung. Die Schweiz verfügt in vielen Bereichen in Bezug auf alltägliche Risiken über ein hohes Sicherheitsniveau, sodass schwerwiegende Ausfälle von wichtigen Gütern und Dienstleistungen bisher selten und von kurzer Dauer waren. Ereignisse wie z. B. die kurzzeitigen Stromausfälle in Zürich, die durch einen Lastwagen beschädigte Brücke über die Autobahn A1 oder der SBB-Totalausfall von 2005 zeigen jedoch, wie anfällig die heutige Gesellschaft und die Wirtschaft auf Versorgungsstörungen sind. Ein länger andauernder, landesweiter Strom-Blackout oder ein Ausfall der Telekommunikation (u. a. der Internet-Verbindungen) würde beispielsweise zu einem unmittelbaren Stillstand von nahezu der gesamten Schweizer Wirtschaft führen, Ausfälle der übrigen KI (z. B. der Lebensmittelversorgung oder des Finanzwesens) verursachen und die Bevölkerung in schwerwiegendem Masse beeinträchtigen (Ausfall von Beleuchtungen, Wasserversorgung und Abwasserentsorgung, Heizungen usw.). Verschiedene Entwicklungen führen dazu, dass die Risiken für solche Ausfälle zunehmen, etwa durch häufigere Naturkatastrophen, ausgereiftere Cyber-Angriffe, Spardruck bei Unternehmen und der Verwaltung oder die Überalterung der baulichen Infrastruktur.

Im Juni 2012 hat der Bundesrat eine nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) verabschiedet, um die Resilienz (Widerstands-, Anpassungs- und Regenerationsfähigkeit) der Schweiz im Hinblick auf KI weiter zu verbessern. Die vorliegende aktualisierte Strategie hält grundsätzlich an der übergeordneten Zielsetzung und Stossrichtung der Strategie von 2012 fest. Mit der aktualisierten Strategie sollen die relevanten Arbeiten, wie z. B. die Führung eines periodisch aktualisierten SKI-Inventars, in einen kontinuierlichen Prozess überführt, rechtlich verankert und punktuell ergänzt werden.

Die nationale SKI-Strategie 2018–2022 bezeichnet 17 Massnahmen, mit denen die Resilienz sowohl sektorspezifisch als auch sektorübergreifend verbessert wird. Sektorspezifisch soll die jeweilige Resilienz der KI überprüft und bei Bedarf verbessert werden. Zum einen soll dies auf Ebene der KI-Betreiber erfolgen, die in der Regel über ein Risiko- und Kontinuitätsmanagement zur Aufrechterhaltung der Geschäftstätigkeit im Ereignisfall verfügen. Dies ist allerdings aus wirtschaftlichen Gründen nur bis zu einem gewissen Grad möglich. Die KI-Betreiber sollen deshalb, beispielsweise gestützt auf den bestehenden SKI-Leitfaden, in Eigenverantwortung die Resilienz überprüfen und nach Möglichkeit verbessern. Zum andern sind die Fach-, Aufsichts- und Regulierungsbehörden (gemäss Anhang 1) in den verschiedenen Sektoren der KI gefordert, gemeinsam zu prüfen, ob die Vorkehrungen ausreichen oder ob zusätzliche Massnahmen zur Verbesserung der Resilienz notwendig sind. Dazu sollen sie in den verschiedenen Sektoren analysieren, welche Verwundbarkeiten und Risiken jeweils bestehen. Zudem werden, falls notwendig, zusätzliche Massnahmen der Prävention und der Vorsorge erarbeitet und umgesetzt, um Ausfälle möglichst zu verhindern bzw. die Funktionsfähigkeit rasch wieder zu gewähr-

leisten. Die Beantwortung der Frage, wie sicher bzw. resilient die jeweiligen KI sein müssen, und die Klärung der finanziellen und rechtlichen Rahmenbedingungen im Hinblick auf allenfalls zusätzlich notwendige Schutzmassnahmen erfolgen wie bis anhin in den sektoriellen Politikbereichen (Energiepolitik, Verkehrspolitik, Gesundheitswesen usw.).

Sektorübergreifend wird die Resilienz verbessert, indem die Verwundbarkeit von Gesellschaft, Wirtschaft und Staat gegenüber schwerwiegenden Ausfällen verringert und Massnahmen zur Verbesserung der subsidiären Unterstützung der KI-Betreiber bei der Ereignisbewältigung im Falle von Katastrophen und Notlagen getroffen werden. U. a. wird dazu ein periodisch aktualisiertes Inventar der KI geführt. Um die KI-Betreiber in den Bereichen Notfall-, Krisen- und Kontinuitätsmanagement nach Möglichkeit zu unterstützen, werden beispielsweise vorsorgliche Einsatzplanungen der Partner im Bevölkerungsschutz (Polizei, Feuerwehr, Zivilschutz etc.) sowie der Armee zum Schutz von KI mit besonders wichtiger Bedeutung erstellt und periodisch aktualisiert.

Der Schutz kritischer Infrastrukturen ist eine Querschnittsaufgabe mit Nahtstellen zu verschiedenen Politik- und Aufgabenbereichen (Energiepolitik, Sicherheitspolitik, Schutz vor Naturgefahren usw.). Dementsprechend erfolgt auch die Umsetzung der nationalen SKI-Strategie massgeblich im Rahmen von dezentralen Strukturen und Zuständigkeiten. Die Kompetenzen der beteiligten Bundesstellen, der Kantone und Gemeinden sowie der KI-Betreiber bleiben vorbehalten. Im Rahmen der Umsetzung der SKI-Strategie soll jedoch u. a. die Erarbeitung einer Rechtsgrundlage mit sektorübergreifenden Vorgaben für die KI-Betreiber geprüft werden.

Die vorliegende Strategie wird per 2022 überprüft und bei Bedarf aktualisiert.

Inhaltsverzeichnis

Anhänge:

Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022

1 Einleitung

1.1 Ausgangslage

Die Schweiz ist angewiesen auf eine möglichst unterbruchsfreie Verfügbarkeit von essenziellen Gütern und Dienstleistungen wie Energie, Verkehr oder Telekommunikation. Erhebliche Störungen der Energieversorgung, der Verkehrssysteme, des Gesundheitswesens oder der öffentlichen Sicherheit verursachen schwerwiegende gesellschaftliche und volkswirtschaftliche Schäden. Der Schutz kritischer Infrastrukturen (SKI) ist deshalb von grosser Bedeutung. Der Schutz der kritischen Infrastrukturen (KI) umfasst dabei alle geeigneten Massnahmen, um die Resilienz der KI zu verbessern. Beispielsweise zählen dazu baulich-technische oder organisatorisch-administrative Massnahmen in der Prävention, der Vorsorge oder der Ereignisbewältigung. Bei SKI handelt es sich nicht um einen eigenständigen Politikbereich, sondern um eine Querschnittsaufgabe mit Bezugspunkten zu vielen anderen Aufgabenbereichen (etwa der Energiepolitik, der Verkehrspolitik, der Sicherheitspolitik oder der Raumplanung). Mit der nationalen SKI-Strategie sollen die Koordination sowie ein abgestimmtes Vorgehen zwischen den entsprechenden Aufgaben in den jeweiligen Politikbereichen verbessert werden.

Im Juni 2012 hat der Bundesrat die erste, nationale SKI-Strategie verabschiedet[1] und das Bundesamt für Bevölkerungsschutz (BABS) beauftragt, die Koordination bei der Umsetzung der darin definierten Massnahmen wahrzunehmen. Zudem hat er das BABS beauftragt, die SKI-Strategie periodisch zu überprüfen und bei Bedarf zu aktualisieren. Mit der SKI-Strategie von 2012 wurden wesentliche Massnahmen zur Verbesserung der Resilienz initiiert. Mit der vorliegenden aktualisierten SKI-Strategie sollen diese Arbeiten in einen etablierten Prozess überführt, rechtlich verankert und punktuell ergänzt werden. Die strategische Stossrichtung im SKI-Bereich bleibt jedoch weitgehend dieselbe.

1.2 Ziel, Zweck und Inhalt der SKI-Strategie

Die nationale SKI-Strategie 2018–2022 hat zum Ziel, die Resilienz (Widerstands-, Anpassungs- und Regenerationsfähigkeit) der Schweiz im Hinblick auf KI zu verbessern. Damit trägt die Strategie massgeblich zum Schutz der Bevölkerung, zur Erhaltung des wirtschaftlichen Wohlstands und zur Sicherheit des Landes bei.

Die Strategie hält fest, welche Ziele die Schweiz im SKI-Bereich verfolgt, und zeigt auf, welche Massnahmen getroffen werden, um die Resilienz der Schweiz in Bezug auf KI zu verbessern. Sie umschreibt den Geltungsbereich, bezeichnet die für die Schweiz kritischen Infrastrukturen und hält die übergeordneten Grundsätze beim

[1] BBl **2012** 7715

SKI fest. Sie gibt die übergeordneten Ziele im SKI-Bereich vor und nennt 17 Massnahmen, die im SKI-Bereich umzusetzen sind. In vielen Punkten knüpfen diese an diejenigen der Strategie von 2012 an. Zum Schluss zeigt sie auf, in welchen Strukturen und mit welchen Zuständigkeiten die Umsetzung erfolgt. Die vorliegende SKI-Strategie ersetzt diejenige von 2012.

1.3 Adressaten der SKI-Strategie

Als vom Bundesrat verabschiedete Strategie definiert die nationale SKI-Strategie Massnahmen, die primär von den Organisationseinheiten der Bundesverwaltung umzusetzen sind. Verschiedene Massnahmen betreffen auch die Kantone. Diese führen SKI-Arbeiten im Rahmen ihrer Kompetenzen und Aufgaben sowie entsprechend ihren Möglichkeiten und Bedürfnissen durch. Ebenfalls angesprochen von der Strategie sind die KI-Betreiber, deren Mitarbeit für die Erreichung der Ziele unerlässlich ist. Die meisten Betreiber unternehmen bereits heute grosse Anstrengungen, um Ausfälle und Störungen zu verhindern. Ihre Eigeninitiative, die bestehenden Vorkehrungen zu überprüfen und bei Bedarf zu verbessern, sowie ihre Bereitschaft zur Zusammenarbeit mit den staatlichen Stellen und den übrigen KI-Betreibern sind von zentraler Wichtigkeit.

2 Umfeld

2.1 Nationale SKI-Strategie 2012

Die nationale SKI-Strategie von 2012 bezeichnete insgesamt 15 Massnahmen. Der Bundesrat wurde per Ende 2016 mit einer Informationsnotiz und einem Bericht über den Stand der Umsetzung orientiert. Die Erfahrungen zeigten, dass sich die Strategie grundsätzlich bewährt hat und an der Stossrichtung der Strategie grundsätzlich festgehalten werden kann. Ein gewisser Handlungsbedarf zeigte sich in Bezug auf die Bezeichnung der kritischen Sektoren und Teilsektoren sowie auf die Massnahmen. Der entsprechende Anpassungsbedarf wird in einem Hintergrundbericht zur nationalen SKI-Strategie 2018–2022 vertieft dargelegt. Bei den Massnahmen in der vorliegenden Strategie werden die erreichten Ziele und der sich daraus ergebende Handlungsbedarf ebenfalls angesprochen.

2.2 Nahtstellen mit weiteren Arbeiten

SKI ist eine Querschnittsaufgabe mit Nahstellen zu vielen weiteren Aufgabenbereichen. Zahlreiche laufende und geplante Vorhaben, Projekte, Aufgaben usw. tragen dazu bei, die in der SKI-Strategie beschriebenen Ziele zu erreichen. In der Regel decken diese nur einen Teil des gesamten SKI-Spektrums ab – beispielsweise einzelne Sektoren oder einzelne Risiken (z. B. Cyber-Risiken oder Naturgefahren). Die Arbeiten im Rahmen der SKI-Strategie bauen auf den vorhandenen Grundlagen auf und ergänzen diese bei Bedarf in Zusammenarbeit mit den jeweils zuständigen

Stellen. Exemplarisch werden nachfolgend die Nahtstellen mit der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), der wirtschaftlichen Landesversorgung (WL) und der Risikopolitik des Bundes aufgeführt. Eine detaillierte Erfassung der relevanten Grundlagen und eine gemeinsame Analyse des verbleibenden Handlungsbedarfs erfolgen jeweils bei der Umsetzung der einzelnen Massnahmen.

2.2.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Zeitgleich mit der SKI-Strategie von 2012 hat der Bundesrat auch die erste NCS verabschiedet. Die NCS zeigt auf, wie sich die Schweiz vor Cyber-Risiken schützt und ihre Resilienz diesen gegenüber verbessert. Von 2012–2017 wurden insgesamt 16 Massnahmen in den Bereichen Prävention, Reaktion und Kontinuität umgesetzt. Ab 2018 soll die neue NCS gelten, welche in Zusammenarbeit mit allen Departementen, der Privatwirtschaft und den Kantonen erarbeitet wurde. Sie soll die bestehenden Arbeiten fortsetzen und weiterentwickeln.

Der Schutz der KI vor Cyber-Risiken ist ein wesentlicher Bestandteil der NCS. Sie deckt damit die Cyber-Aspekte der SKI-Strategie ab und setzt die entsprechenden Massnahmen in enger Koordination mit der SKI-Strategie um.

2.2.2 Wirtschaftliche Landesversorgung (WL)

Die WL hat zum Ziel, die Versorgung der Schweiz mit wichtigen Gütern und Dienstleistungen sicherzustellen. Im Falle von schwerwiegenden Versorgungsstörungen treten vorbereitete Massnahmen in Kraft (u. a. Freigabe von Pflichtlagern oder Bewirtschaftung von wichtigen Gütern wie Strom). Die WL deckt rund die Hälfte der kritischen Sektoren und Teilsektoren der nationalen SKI-Strategie ab und trägt damit massgeblich zur Erreichung der Ziele der SKI-Strategie bei. Die zusätzlichen Aktivitäten im Rahmen von SKI beschränken sich auf Teilsektoren, die nicht von der WL abgedeckt sind (z. B. Behörden oder Blaulichtorganisationen) sowie auf thematische Aspekte, die nicht von der WL behandelt werden. So fokussiert die WL vor allem auf längerfristige, nationale Versorgungsengpässe. Im Kontext der SKI-Strategie sind indessen auch kürzere Störungen sowie solche, die nicht die gesamte Schweiz betreffen (z. B. regionale Ausfälle und Störungen), relevant.

2.2.3 Risikopolitik des Bundes

Das Risikomanagement wurde beim Bund 2005 eingeführt. Es fokussiert auf Ereignisse, die wesentliche negative finanzielle und nichtfinanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben. Damit ist das Risikomanagement des Bundes vor allem im Hinblick auf den Sektor Behörden relevant. Bezugspunkte bestehen aber auch zu den Aufgaben der

Fach-, Aufsichts- und Regulierungsbehörden des Bundes in den übrigen Sektoren. Die wesentlichen Unterschiede bei SKI liegen darin, dass es nicht um die Risiken für den Bund geht, sondern um diejenigen für die Bevölkerung und die Wirtschaft. So gibt es Risiken, die für den Bund relevant sein können, die Gesellschaft und die Wirtschaft jedoch nicht besonders betreffen. Zudem befinden sich in vielen Fällen die KI nicht im ausschliesslichen Kompetenzbereich des Bundes, sondern auch oder nur in demjenigen der Kantone und Gemeinden (Wasserversorgung, Gesundheitswesen usw.). Im Rahmen der Umsetzung der verschiedenen Massnahmen der nationalen SKI-Strategie wird jeweils überprüft, welche Aspekte bereits im Rahmen des Risikomanagements Bund abgedeckt sind und welcher zusätzliche Handlungsbedarf noch besteht.

3 Geltungsbereich

Der Geltungsbereich der nationalen SKI-Strategie wird durch die Definition der Begriffe KI und SKI sowie durch die Bezeichnung der KI abgegrenzt.

3.1 Kritische Infrastrukturen

Der Begriff KI wird wie folgt definiert: *Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind*.

Für die Schweiz umfasst das Spektrum der KI folgende Bereiche:

Tabelle 1

Kritische Sektoren und Teilsektoren der Schweiz

Sektoren	Teilsektoren
Behörden	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Fern- und Prozesswärme
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	Finanzdienstleistungen
	Versicherungsdienstleistungen

Sektoren	Teilsektoren
Gesundheit	Chemie und Heilmittel
	Labordienstleistungen
	Medizinische Versorgung
Information und Kommunikation	IT-Dienstleistungen
	Medien
	Postdienste
	Telekommunikation
Nahrung	Lebensmittelversorgung
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisationen (Polizei, Feuerwehr, Sanität)
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr

In Anhang 1 wird präzisiert, welche Leistungen bzw. Funktionen der Teilsektoren aus SKI-Perspektive besonders relevant sind.

Es gelten grundsätzlich sämtliche Elemente (Betreiberfirmen, IT-Systeme, Anlagen, Bauten usw.) als Teil der KI, die Leistungen in einem der 27 Teilsektoren gemäss Tabelle 1 erbringen – unabhängig von ihrer Kritikalität. Die Kritikalität ist ein relatives Mass für die Bedeutung, die ein Ausfall der KI für die Bevölkerung und deren Lebensgrundlagen hat. Sie ist abhängig von der jeweiligen Betrachtungsebene: So gibt es KI, die auf lokaler oder kommunaler Ebene eine grosse Kritikalität haben (z. B. eine Trafo-Station im Strom-Verteilnetz), andere haben dagegen aus nationaler oder sogar internationaler Perspektive eine grosse Kritikalität (z. B. zentrale Steuerungssysteme im Übertragungsnetz).

3.2 Schutz kritischer Infrastrukturen

Der Schutz kritischer Infrastrukturen umfasst Massnahmen, welche die Eintrittswahrscheinlichkeit respektive das Schadensausmass einer Störung, eines Ausfalls oder einer Zerstörung von KI reduzieren bzw. die Ausfallzeit minimieren. Die Massnahmen sollen dabei verhältnismässig in Bezug auf die Bedeutung der jeweiligen KI sein. Demenentsprechend ist die Thematik SKI auch auf allen drei Staatsebenen relevant: Auf Ebene Bund, wo vor allem die KI mit gesamtnationaler oder gar internationaler Bedeutung im Fokus stehen, aber auch auf Kantons- oder Gemeindeebene mit Fokus auf die KI mit kantonal bzw. kommunal wichtiger Bedeutung.

4 Verwundbarkeiten, Risiken und Schutzmassnahmen

Ausfälle von KI können entstehen, wenn relevante Verwundbarkeiten vorliegen. Aus solchen Verwundbarkeiten resultieren Risiken, die mit geeigneten Schutzmassnahmen reduziert werden können.

4.1 Verwundbarkeiten

Die KI sind für ihr Funktionieren auf die Verfügbarkeit von Ressourcen wie Arbeitskräfte, Rohstoffe, Energie oder Informations- und Kommunikationstechnologien (IKT) angewiesen. Dort, wo ein Ausfall oder eine Störung einer Schlüsselressource das Funktionieren der KI beeinträchtigt, existieren relevante Verwundbarkeiten. Folgende Ressourcenbereiche können unterschieden werden:

- Arbeitskräfte: Darunter fallen Personen, die für die Funktionalität der kritischen Infrastruktur von grundlegender Bedeutung sind. Von besonderer Bedeutung sind Schlüsselpersonen und Spezialisten, die Wissensträger für den jeweiligen Prozess darstellen.
- Werkstoffe und Betriebsmittel: Dazu zählen Rohstoffe, Energieträger (Treib- und Brennstoff) sowie Halb- und Fertigfabrikate.
- Dienstleistungen: Dieser Bereich beinhaltet Logistik (Transporte, bauliche Infrastruktur) sowie Dienstleistungen in den Bereichen IKT (inkl. Daten) und Energieversorgung (z. B. Strom). Dabei ist zu berücksichtigen, dass relevante Leistungen sowohl im In- als auch im Ausland erbracht werden können. Viele KI sind beispielsweise auf weltraumbasierte Dienste angewiesen (z. B. GPS oder Galileo). Verwundbarkeiten können sich auch durch Konzentrationen auf wenige Anbieter (Monopolisten) ergeben.

4.2 Risiken

Relevante Verwundbarkeiten sind vertieft auf daraus resultierende Risiken zu untersuchen. Dabei können sowohl Naturgefahren als auch technische und gesellschaftliche Gefahren zu signifikanten Ausfällen führen:

- Naturgefahren: Gravierende Störungen können beispielsweise durch Hochwasser, Stürme, Lawinen oder Erdbeben verursacht werden.
- Technische Gefahren: Zu den technischen Gefahren zählen beispielsweise Systemversagen, ein Stromausfall oder eine mangelhafte Netztopologie.
- Gesellschaftliche Gefahren: Im Kontext von SKI sind beispielsweise Sabotageakte, Terrorismus oder eine Pandemie relevant. Durch den zunehmenden Einsatz von Automatisierungs- und Steuerungssystemen drohen zudem Ausfälle infolge von Cyber-Angriffen.

Für die Bestimmung der Risiken relevant sind jeweils die Wahrscheinlichkeit bzw. Plausibilität einer Gefährdung sowie die Schäden für die Bevölkerung und deren Lebensgrundlagen, die sich aus der Störung oder der Zerstörung der KI ergeben. Durch bereits implementierte Schutzmassnahmen resultieren dabei geringere Risiken.

4.3 Schutzmassnahmen

Bei den zu evaluierenden und umzusetzenden Schutzmassnahmen kann zwischen präventiven, vorsorglichen und einsatzbezogenen Massnahmen unterschieden werden. Damit sollen Ausfälle verhindert bzw. im Ereignisfall die Aufrechterhaltung der Funktionsfähigkeit (Kontinuität) gewährleistet oder das Schadensausmass reduziert werden (beispielsweise durch die Definition von Ersatz- oder Alternativprozessen). Von wichtiger Bedeutung sind auch Massnahmen im Hinblick auf die Verbesserung der Vorsorge bei der Bevölkerung und der Wirtschaft, welche vom Ausfall der KI betroffen sind.

Die Schutzmassnahmen können verschiedenen Kategorien zugeteilt werden:

- Baulich-technische Massnahmen: Härtung von Gebäuden, Beschaffung von Notstromanlagen, Segregation von IT-Systemen usw.
- Organisatorisch-administrative Massnahmen: Dazu zählen etwa die Einrichtung eines Krisenstabs, die Durchführung von Eingangskontrollen oder die Bestimmung von Ausweicharbeitsplätzen.
- Rechtlich-regulatorische Massnahmen: Darunter fällt beispielsweise die Anpassung einer fachgesetzlichen Grundlage (Gesetz, Verordnung, Weisung usw.).
- Personelle Massnahmen: Dazu zählt etwa die Festlegung von Stellvertreter-Regelungen oder die Schulung und Sensibilisierung von Mitarbeitenden.

Über alle Massnahmenbereiche hinweg wichtig ist auch der Informationsschutz.

5 Grundsätze für den Schutz kritischer Infrastrukturen

Ganzheitlicher, risikobasierter Ansatz: Der Schutz von KI folgt einem ganzheitlichen und risikobasierten Ansatz. Es sind sämtliche relevanten Verwundbarkeiten und Gefährdungen, die zu einer signifikanten Störung der KI führen können, zu berücksichtigen und miteinander in ein Verhältnis zu setzen. Auch bezüglich Erarbeitung und Umsetzung von Schutzmassnahmen ist ein umfassendes und risikobasiertes Vorgehen zu verfolgen.

Verhältnismässigkeit: Die Massnahmen zum Schutz von KI sollen ein optimales Verhältnis zwischen Massnahmenkosten und erzieltem Nutzen (Risikoreduktion) aufweisen. Explizit nicht angestrebt wird eine vollständige Elimination sämtlicher Risiken. Dies ist einerseits technisch nicht möglich und andererseits wirtschaftlich

mit unverhältnismässig grossem Aufwand verbunden. Die gewählten Massnahmen müssen überdies verfassungskonform und rechtlich legitimiert sein. Es darf zudem nicht zu Marktverzerrungen kommen.

Gemeinsame Verantwortung: Der SKI ist eine Querschnittsaufgabe mit Nahtstellen zu verschiedensten Politik- und Aufgabenbereichen. Sämtliche Verantwortungsträger sind gefordert, SKI-Aspekte im jeweiligen Bereich angemessen zu berücksichtigen. Von wichtiger Bedeutung ist die Eigeninitiative der KI-Betreiber bei der Überprüfung und Verbesserung ihrer Resilienz. Auch die Bevölkerung und die Wirtschaft, die auf das Funktionieren der KI angewiesen sind, sind gefordert, ihre Resilienz zu verbessern. Eine bessere Vorbereitung (z. B. mit Vorratshaltung von Lebensmitteln in Haushalten oder der Einrichtung einer Notstromversorgung in Unternehmen) trägt wesentlich dazu bei, dass das Schadensausmass im Falle von Störungen der KI reduziert wird.

Öffentlich-private Zusammenarbeit: SKI verlangt eine enge Zusammenarbeit zwischen allen involvierten Akteuren (Behörden auf den Ebenen Bund, Kantone und Gemeinden sowie KI-Betreibern). Wo möglich, sollen Schutzmassnahmen gemeinsam erarbeitet werden. Die öffentlich-private Zusammenarbeit ist insbesondere bei der Erarbeitung von Richtlinien und Normen oder bezüglich des Informationsaustauschs relevant.

Wahrung der Kompetenzen und Verantwortlichkeiten: Für die KI-Betreiber ergeben sich die Vorgaben und Auflagen insbesondere aus den sektoriellen Fachgesetzgebungen (in den Sektoren Energie, Verkehr, Finanzen usw.). Die Kantone sind mit Unterstützung des Bundes (z. B. Bundeskriminalpolizei, Grenzwachkorps oder Bundessicherheitsdienst) im Rahmen ihrer Möglichkeiten u. a. zuständig für die Gefahrenabwehr im Rahmen der inneren Sicherheit bzw. des Bevölkerungsschutzes. Im Rahmen von subsidiären Einsätzen kann die Armee nötigenfalls und abhängig von den zur Verfügung stehenden Mitteln die zivilen Behörden unterstützen.

6 Vision und Ziele der nationalen SKI-Strategie

6.1 Vision

Die nationale SKI-Strategie verfolgt folgende Vision:

Die Schweiz ist in Bezug auf kritische Infrastrukturen resilient, sodass grossflächige und schwerwiegende Ausfälle möglichst verhindert werden beziehungsweise im Ereignisfall das Schadensausmass möglichst gering gehalten wird.

Die Resilienz bezieht sich auf die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen (Widerstandsfähigkeit) und die Funktionsfähigkeit möglichst zu erhalten (Anpassungsfähigkeit) respektive möglichst schnell und vollständig wiederzuerlangen (Regenerationsfähigkeit).

6.2 Strategische Ziele

Übergeordnetes Ziel der nationalen SKI-Strategie ist es, die Resilienz der Schweiz betreffend KI zu verbessern. Dies soll durch folgende Teilziele erreicht werden:

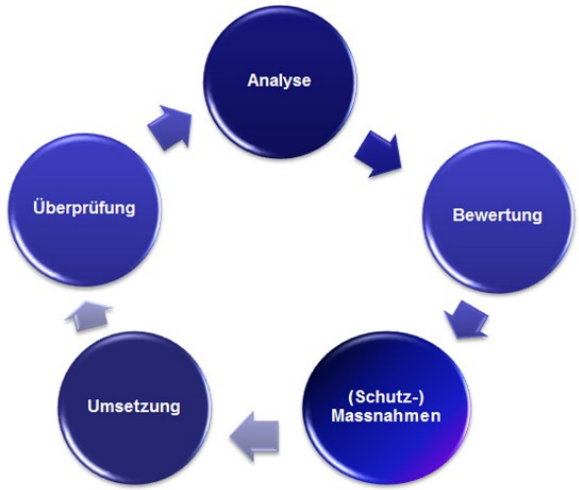
- Die KI sind resilient, sodass grossflächige und schwerwiegende Ausfälle möglichst verhindert und die Funktionsfähigkeit im Ereignisfall möglichst rasch wieder gewährleistet werden kann.
- Die Bevölkerung und die Wirtschaft sind resilient, sodass Ausfälle und Störungen der KI nicht zu schwerwiegenden Schäden führen.
- Die Behörden sind darauf vorbereitet, auf Ausfälle der KI angemessen reagieren zu können.
- Die KI-Betreiber werden bei der Ereignisbewältigung wirkungsvoll unterstützt.

6.3 Operationalisierung

Die Verbesserung der Resilienz basiert auf einem fünfstufigen Prozess, der sich aus folgenden Elementen zusammensetzt:

Abbildung 1:

Regelkreis zur Überprüfung und Verbesserung der Resilienz



Analyse

- Kritische Prozesse, Systeme, Objekte usw. sind identifiziert.
- Verwundbarkeiten und Risiken, die zu schwerwiegenden Ausfällen führen können, sind identifiziert und analysiert.
- Relevante Änderungen der Gefahren- und Bedrohungslage im Zusammenhang mit KI sind rechtzeitig erkannt und den relevanten Stellen kommuniziert.

Bewertung

- Abweichungen von geltenden Vorgaben sind erkannt.
- Das anzustrebende Sicherheitsniveau ist festgelegt.

(Schutz-)Massnahmen

- Es sind Massnahmen definiert und verabschiedet, mit denen
  - schwerwiegende Ausfälle möglichst verhindert,
  - Ereignisse bewältigt,
  - eine rasche Rückkehr zum Normalbetrieb ermöglicht oder
  - die Auswirkungen von Ausfällen reduziert werden können.

Die Massnahmen weisen dabei ein optimales Verhältnis zwischen Massnahmenkosten und verbleibenden Risiken auf.

Umsetzung

- Die definierten Massnahmen sind rechtzeitig umgesetzt.

Überprüfung

- Die Wirkung der getroffenen Massnahmen ist überprüft.
- Massnahmen sind mit Hilfe von Übungen und Ausbildungen gefestigt.

Um die Resilienz der Schweiz im Hinblick auf KI zu verbessern, sollen gemäss dem beschriebenen Prozess sowohl die Resilienz der KI in den einzelnen Sektoren als auch die Resilienz sektorübergreifend verbessert werden:

1. Verbesserung der Resilienz in den kritischen Sektoren: Die jeweilige Resilienz der KI soll überprüft und bei Bedarf verbessert werden. Dazu sollen gemäss dem oben beschriebenen Vorgehen spezifische Verwundbarkeiten und Risiken analysiert und bei Bedarf Massnahmen getroffen und umgesetzt werden, um die Resilienz der jeweiligen KI zu verbessern.
2. Sektorübergreifende Verbesserung der Resilienz: Dabei geht es u. a. darum, die Resilienz von Bevölkerung, Wirtschaft und Staat im Hinblick auf Ausfälle von KI zu verbessern oder Massnahmen zu treffen, um die KI-Betreiber subsidiär bei der Ereignisbewältigung zu unterstützen (in Ergänzung zu den sektorspezifischen Massnahmen zur subsidiären Unterstützung der KI-Betreiber).

7 Massnahmen der nationalen SKI-Strategie

Basierend auf den strategischen Zielen und der Operationalisierung (vgl. Ziff. 6) werden nachfolgend sektorspezifisch und sektorübergreifend Massnahmen definiert und eine Umsetzungsplanung abgeleitet. Diese wird nach Verabschiedung der nationalen SKI-Strategie mit einer separaten, detaillierten Umsetzungsplanung ergänzt. Im Kontext von SKI sind zahlreiche bereits etablierte oder geplante Projekte, Vorhaben, Massnahmen usw. relevant. Vielfach wird es bei der Umsetzung der nationalen SKI-Strategie darum gehen, bestehende Prozesse zu überprüfen und gegebenenfalls zu ergänzen. Wo immer möglich, baut die nationale SKI-Strategie auf Bestehendem auf. Im Detail wird der Abgleich mit laufenden Vorhaben im Rahmen der Umsetzungsplanung sichergestellt. In Anhang 2 wird ein Überblick über die Massnahmen und die wichtigsten Nahtstellen mit anderen Arbeiten gegeben; im Text wird auf eine explizite Nennung verzichtet.

7.1 Verbesserung der Resilienz in den kritischen Sektoren

Um die Resilienz des Gesamtsystems der KI zu verbessern, ist es wichtig, dass möglichst alle relevanten Einzelkomponenten (Stromversorgung, Telekommunikation, Strassenverkehr usw.) ihrer jeweiligen Bedeutung angemessen resilient sind. Sowohl seitens der KI-Betreiber als auch innerhalb der einzelnen Sektoren existieren in der Regel bereits zahlreiche Vorkehrungen zur Verbesserung der Resilienz (z. B. sektorspezifische Regulierungen oder vorbereitete Massnahmen beispielsweise im Rahmen der WL). Dementsprechend geht es im Bereich der sektorspezifischen Resilienz darum, zu überprüfen, ob die Vorkehrungen im Kontext der Ziele gemäss SKI-Strategie ausreichen oder Ergänzungen notwendig sind. Zu diesem Zweck sollen gemäss dem in Ziffer 6.3 beschriebenen Vorgehen die jeweils infrastrukturspezifischen Verwundbarkeiten und Risiken analysiert sowie, falls notwendig, präventive und vorsorgliche Massnahmen zur Reduktion der Risiken erarbeitet und umgesetzt werden.

Diese Arbeiten sollen insbesondere auf zwei Ebenen durchgeführt werden: Zum einen soll dies auf Ebene der einzelnen KI-Betreiber erfolgen. Diese verfügen in der Regel über ein Risikomanagement sowie über ein Notfall-, Krisen- und Kontinuitätsmanagement. Damit werden teils umfangreiche Vorkehrungen getroffen, um die Geschäftstätigkeit im Falle von Katastrophen und Notlagen aufrechtzuerhalten. Dabei ist jedoch nicht gewährleistet, dass diejenigen Prozesse, die für die Bevölkerung und die Wirtschaft essenziell sind, auch aus Sicht des Unternehmens als von höchster Priorität eingeschätzt werden (da der Fokus der Unternehmen vor allem auf dem wirtschaftlichen Wohlergehen liegt). Die Betreiber sollen deshalb in Zusammenarbeit mit den zuständigen Fach-, Aufsichts- und Regulierungsbehörden in den verschiedenen Sektoren in Eigenverantwortung überprüfen, ob die Vorkehrungen ausreichend sind oder die Resilienz verbessert werden muss. Das BABS hat zu diesem Zweck einen Leitfaden sowie eine Umsetzungshilfe publiziert, welche die Betreiber bei diesen Arbeiten unterstützen.

Die sektorspezifischen Fach-, Aufsichts- und Regulierungsbehörden (gemäss Anhang 1) sind gefordert, gemeinsam zu überprüfen, ob die Vorkehrungen ausreichend sind oder ob systemische Risiken im Hinblick auf grossflächige und schwerwiegende Ausfälle vorliegen. Deshalb soll die sektorspezifische Resilienz zum andern auf Ebene der verschiedenen kritischen Teilsektoren (Stromversorgung, Schienenverkehr, Telekommunikation usw.) überprüft werden. Dabei sind bereits bestehende Vorkehrungen (seitens der Betreiber, aber auch sektorielle Planungen beispielsweise der WL) einzubeziehen, und es ist zu prüfen, ob gravierende Risiken verbleiben, die reduziert werden müssen. Vielfach lassen sich solche Risiken mit branchenspezifischen Lösungen (z. B. einer Vereinbarung zur Zusammenarbeit im Ereignisfall) reduzieren. Unter Umständen kann es aber auch notwendig sein, zusätzliche Vorgaben oder Auflagen für die KI-Betreiber zu erlassen. Die Festlegung der entsprechenden Vorgaben sowie die Klärung der Finanzierung von allenfalls zusätzlich notwendigen Massnahmen erfolgen in den sektoriellen Politikbereichen (Energiepolitik, Verkehrspolitik, Gesundheitspolitik usw.). Im Rahmen der nationalen SKI-Strategie und der NCS von 2012 wurden für alle kritischen Teilsektoren entsprechende Analysen durchgeführt und erste Massnahmen in die Wege geleitet. In rund der Hälfte der Teilsektoren decken die Arbeiten vorerst nur IKT-Aspekte ab (für die anderen kritischen Teilsektoren wurden im Sinne der SKI-Strategie weitere relevante Verwundbarkeiten und Risiken berücksichtigt). Diese Arbeiten müssen demnach ergänzt werden. Weiter ist es notwendig, diese und die übrigen Analysen periodisch zu aktualisieren, da sich die Risiken im Laufe der Zeit verändern.

Aufgrund der Tatsache, dass die nationale SKI-Strategie weder für die Betreiber noch für die zuständigen Fach-, Aufsichts- und Regulierungsbehörden in den verschiedenen Sektoren rechtsverbindlich ist, ergibt sich die Herausforderung, dass die Überprüfung und Verbesserung der Resilienz der KI gemäss dem beschriebenen Vorgehen auf der Initiative und Eigenverantwortung der zuständigen Akteure basiert. Zudem gibt es einzelne Teilsektoren, bei denen es aufgrund fehlender Bundeskompetenzen (z. B. bei Spitälern) schwierig sein dürfte, allenfalls notwendige sektorielle Rechtsgrundlagen zu schaffen oder anzupassen. Dementsprechend könnte eine Rechtsgrundlage mit sektorübergreifenden Vorgaben zur Resilienz der KI-Betreiber die Erreichung der Zielsetzung massgeblich vereinfachen. Die Rechtsgrundlage sollte diejenigen Teilsektoren abdecken, bei denen die Abklärungen auf Ebene der kritischen Teilsektoren ergeben haben, dass dies notwendig ist, und wo die notwendigen Massnahmen nicht anderweitig getroffen werden können (z. B. durch eine Branchenlösung oder die Schaffung bzw. Anpassung einer sektoriellen Rechtsgrundlage).

Ziel:

– Die KI in allen kritischen Sektoren sind ihrer Bedeutung angemessen resilient. Alle relevanten Risiken sind erkannt, und Massnahmen zur Erreichung eines optimalen Masses an Sicherheit sind definiert und umgesetzt. Dabei wird ein umfassendes Gefahren- und Massnahmenspektrum berücksichtigt.

Massnahme 1:

– Für KI, bei denen noch keine entsprechenden Arbeiten vorliegen, sind gemäss dem in Ziffer 6.3 beschriebenen Vorgehen Risiko- und Verwundbarkeitsanalysen durchzuführen sowie Massnahmen zur Verbesserung der Resilienz zu erarbeiten und umzusetzen. Diese Arbeiten sind periodisch zu aktualisieren.

Umsetzung:

– Die KI-Betreiber überprüfen und verbessern ihre Resilienz, beispielsweise gestützt auf den SKI-Leitfaden, in Eigenverantwortung und in Zusammenarbeit mit den zuständigen Fach-, Aufsichts- und Regulierungsbehörden. Das BABS unterstützt diese Arbeiten so weit wie möglich methodisch.

– Die Verwundbarkeitsanalysen und Massnahmenplanungen für die kritischen Teilsektoren, die bis anhin nur IKT-Aspekte berücksichtigen, werden durch die zuständigen Fach-, Aufsichts- und Regulierungsbehörden (vgl. Anhang 1) in Zusammenarbeit mit den KI-Betreibern mit weiteren relevanten Gefährdungen ergänzt. Bestehende Arbeiten, die ein umfassendes Verwundbarkeits-, Risiko- und Massnahmenspektrum abdecken, werden alle vier Jahre aktualisiert. Die in Anhang 1 genannten Stellen vereinbaren, welches Amt federführend ist. Bei Bedarf kann das BABS die Arbeiten unterstützen.

Massnahme 2:

– Es ist die Erarbeitung einer rechtlichen Grundlage für den Erlass von sektorübergreifenden Vorgaben in Bezug auf die Resilienz der KI-Betreiber zu prüfen. Diese Rechtsgrundlage soll diejenigen Bereiche abdecken, wo die Abklärungen auf Ebene der kritischen Teilsektoren ergeben haben, dass dies zwingend notwendig ist.

Umsetzung:

– Das VBS (BABS) prüft zusammen mit den zuständigen Akteuren (insb. WBF, UVEK und EFD) die Erarbeitung eines Vorschlags für eine sektorübergreifende Rechtsgrundlage in Bezug auf Vorgaben zur Verbesserung der Resilienz von KI. Dabei ist insbesondere die Frage der Kompetenzüberschneidungen mit bestehenden Vorgaben und sektorspezifischen Regulierungen zu klären.

7.2 Sektorübergreifende Verbesserung der Resilienz

Die sektorübergreifende Verbesserung der Resilienz umfasst alle Tätigkeiten, die für die Gestaltung, Steuerung und Weiterentwicklung der SKI-relevanten Aktivitäten erforderlich sind. U. a. sollen die Resilienz von Gesellschaft, Wirtschaft und Staat erhöht und Massnahmen getroffen werden, um die KI-Betreiber bei der Ereignisbewältigung zu unterstützen. Die Ziele und Massnahmen orientieren sich dabei an dem in Ziffer 6.3 dargelegten Prozess.

7.2.1 Analyse

Handlungsfeld Analyse:
Kritische Infrastrukturen identifizieren und priorisieren

Bevor Schutzmassnahmen getroffen werden können, müssen die zuständigen Stellen wissen, welche Infrastrukturen besonders kritisch sind. Kenntnisse über die KI und ihre Bedeutung sind insbesondere notwendig, um im Falle von Katastrophen und Notlagen Lagebeurteilungen vornehmen und Schutzmassnahmen priorisieren zu können. Im Zuge der nationalen SKI-Strategie von 2012 wurde das Inventar der Objekte kritischer Infrastrukturen erarbeitet (SKI-Inventar). Das SKI-Inventar definiert Bauten und Anlagen, die entweder aus nationaler oder aus kantonaler Perspektive eine strategisch wichtige Bedeutung haben. Es ist in seiner Gesamtheit als GEHEIM klassifiziert. Auszüge, die nur einen Teil der Informationen enthalten (z. B. aus einem Kanton oder einem Sektor) sind in der Regel als VERTRAULICH klassifiziert. Das SKI-Inventar und die entsprechenden Angaben müssen periodisch aktualisiert werden. Neben den relevanten Bauten und Anlagen soll das SKI-Inventar zudem um Betreiber(firmen) von KI sowie kritische IT-Systeme erweitert werden. Nach Möglichkeit wird dazu auf Daten zurückgegriffen, die bereits im Rahmen von anderen Verzeichnissen erfasst wurden.

Ziel:

– Die KI der Schweiz sind identifiziert und unter Wahrung der Informations- und Datenschutzvorschriften mit aktuellen Angaben erfasst. Insbesondere sind Bauten und Anlagen sowie Systeme und Betreiber erkannt und priorisiert.

Massnahme 3:

– Das SKI-Inventar ist periodisch zu aktualisieren und mit Angaben zu kritischen IT-Systemen und Betreiberfirmen von KI zu ergänzen.

Umsetzung:

– Das BABS ist zuständig, in Zusammenarbeit mit den Fachämtern und den Betreibern die aus nationaler Perspektive kritischen Infrastrukturen zu identifizieren und die dazugehörenden Angaben periodisch zu aktualisieren. Um die Zusammenarbeit rechtlich abzustützen, prüft das BABS die Schaffung einer entsprechenden Rechtsgrundlage im BZG. Die Kantone identifizieren Objekte kritischer Infrastrukturen, die aus kantonaler Perspektive relevant sind, und aktualisieren diese Angaben periodisch.

Handlungsfeld Analyse:
Risiken, Verwundbarkeiten und Schutzmöglichkeiten kennen

Als Grundlage für die Verbesserung der Resilienz der KI müssen sektorübergreifende Aussagen über relevante Risiken gemacht werden können. Dazu müssen die Analysen aus den verschiedenen kritischen Teilsektoren konsolidiert und zu einer gesamthaften Risikoübersicht aggregiert werden.

Zudem sind zur methodischen Weiterentwicklung von SKI wissenschaftlich fundierte Erkenntnisse, etwa in den Bereichen der Interdependenz- oder Kritikalitätsanalysen, notwendig. Ebenfalls müssen Technologie-, Umwelt- und Umfeldentwicklungen verfolgt werden, die zu neuen Risiken führen können. Dies erfolgt im Rahmen der Ressortforschung der Bundesstellen und Kantone.

Ziele:

- Es liegt eine konsolidierte Übersicht über die Verwundbarkeiten und Risiken in Zusammenhang mit den KI vor, und der Handlungsbedarf ist aufgezeigt.
- Es sind wissenschaftlich fundierte Grundlagen vorhanden und den relevanten Akteuren bekannt, die zur methodischen Weiterentwicklung von SKI beitragen.

Massnahme 4:

- Die Erkenntnisse der Überprüfung und Verbesserung der Resilienz der kritischen Teilsektoren sind zu einer gesamtheitlichen Risikoübersicht zu konsolidieren.

Umsetzung:

- Das VBS (BABS) konsolidiert in Zusammenarbeit mit dem EFD (ISB und EFV) und dem WBF (BWL) die Erkenntnisse aus den teilsektorspezifischen Analysen.

Massnahme 5:

- Die Grundlagenforschung zu sektorübergreifenden Themen (z. B. Interdependenzen sowie Technologie-, Umwelt- und Umfeldentwicklungen) ist zu vertiefen.

Umsetzung:

- Die Bundesstellen, Kantone und Betreiber sind verantwortlich für die Ressortforschung in ihrem Zuständigkeitsgebiet. Das VBS (BABS) ist zuständig für die sektorübergreifende Grundlagenforschung im SKI-Bereich.

Handlungsfeld Analyse:
Zusammenarbeit und Informationsaustausch verbessern

KI sind hochgradig (inter-)dependent. Eine Zusammenarbeit und ein Dialog über Risiken und mögliche Schutzmassnahmen (Best Practices) zwischen den diversen Akteuren aus den KI-Sektoren sind deshalb von zentraler Bedeutung. Im Rahmen der nationalen SKI-Strategie von 2012 wurden drei relevante Plattformen geschaffen (Plattform der Betreiber national kritischer Infrastrukturen, Arbeitsgruppe SKI der Bundesstellen, kantonale Kontaktstellen SKI). Die Erfahrungen zeigen, dass die sektor- bzw. kantonsübergreifende Zusammenarbeit im SKI-Bereich auf grosses Interesse stösst. Die Plattformen bieten den Akteuren aus den verschiedenen Sektoren (Bundesstellen und KI-Betreiber) und Kantonen Gelegenheit, Erfahrungen auszutauschen und Lösungsansätze zu diskutieren. Da KI vielfach grenzüberschreitende Systeme darstellen, ist auch die internationale Zusammenarbeit von Bedeu-

tung. Der Austausch zu Cyber-Risiken erfolgt dabei über die Melde- und Analysestelle Informationssicherung (MELANI).

Ziel:

– Es sind sektorübergreifende Plattformen zur Verbesserung der Zusammenarbeit und zur Förderung des Informationsaustauschs über Risiken, Verwundbarkeiten und mögliche Schutzmassnahmen (Best Practices) etabliert.

Massnahme 6:

– Die bestehenden Plattformen werden weitergeführt, und die Zusammenarbeit in diesen wird bei Bedarf intensiviert. Die Zusammensetzungen der Plattformen sind periodisch zu überprüfen.

Umsetzung:

– Das VBS (BABS) koordiniert die Plattform der Betreiber national kritischer Infrastrukturen, die kantonalen Kontaktstellen SKI sowie die Arbeitsgruppe SKI der Behörden (Bund und Kantone). Auf internationaler Ebene stellt das VBS (BABS) den Point of Contact für SKI-Angelegenheiten dar. In Bezug auf Cyber-Risiken erfolgt die internationale Zusammenarbeit über MELANI.

Handlungsfeld Analyse:
Akute Gefährdungen und Bedrohungen frühzeitig erkennen und kommunizieren

Im Falle von akuten Gefährdungen und Bedrohungen ist es wichtig, dass einerseits die KI-Betreiber rechtzeitig orientiert werden, um ihr Sicherheitsdispositiv anzupassen. Andererseits ist es im Falle von Störungen der KI wichtig, dass die zuständigen Krisenorganisationen auf den Stufen Bund und Kantone sowie diejenigen bei anderen KI-Betreibern frühzeitig orientiert werden. Mit dem Nachrichtendienstgesetz (NDG) wurde eine wichtige Grundlage zur Erkennung von Bedrohungen u. a. für KI geschaffen. Für verschiedene andere Bedrohungen und Gefahren (z. B. hinsichtlich Cyber-Risiken oder Naturgefahren) existieren jeweils etablierte Formen der Zusammenarbeit, um die KI-Betreiber im Ereignisfall frühzeitig zu orientieren (z. B. geschlossene Kundenkreise von MELANI). Dabei gilt es, periodisch zu überprüfen, ob die jeweils relevanten KI-Betreiber in die entsprechenden Prozesse involviert sind. Für die Behörden ist es zudem wichtig, frühzeitig über Ausfälle und Sicherheitsvorfälle bei den KI orientiert zu sein, damit ein umfassendes Lagebild erstellt und rechtzeitig Massnahmen zur Ereignisbewältigung eingeleitet werden können. Diesbezüglich besteht im Rahmen des Bevölkerungsschutzes mit Netalert ein Meldesystem zur Meldung von solchen Ausfällen auf freiwilliger Basis. In einigen wenigen Teilsektoren sind die KI-Betreiber zudem verpflichtet, entsprechende Vorfälle der zuständigen Fachbehörde zu melden.

Ziel:

– Die relevanten KI-Betreiber werden gemäss ihrer Bedeutung frühzeitig und in ausreichender Qualität informiert. Die KI-Betreiber melden umgekehrt signifikante Störungen und Ausfälle den zuständigen Stellen auf den Ebenen Bund und Kantone. Dabei sind die Informationssicherheit und der Datenschutz zu gewährleisten.

Massnahme 7:

– Die gefährdungsspezifischen Prozesse zur frühzeitigen Orientierung im Ereignisfall werden periodisch hinsichtlich der Beteiligung der KI-Betreiber überprüft und falls notwendig ergänzt.

Umsetzung:

– Das VBS (BABS) überprüft gemeinsam mit den gefährdungsspezifisch verantwortlichen Stellen (u. a. MELANI), ob die relevanten KI-Betreiber involviert sind, und erarbeitet nötigenfalls Vorschläge zur Ergänzung der jeweiligen Prozesse.

Massnahme 8:

– Es ist die Erarbeitung eines Vorschlags für Rechtsgrundlagen zu prüfen, mit der die Betreiber verpflichtet werden, schwerwiegende Sicherheitsvorfälle bzw. Funktionsausfälle den zuständigen Behörden zu melden.

Umsetzung:

– Das VBS (BABS) prüft in Zusammenarbeit u. a. mit dem EFD (ISB) und dem UVEK die Schaffung von Rechtsgrundlagen für eine Pflicht, schwerwiegende Sicherheitsvorfälle und Ausfälle von KI zu melden. Diese soll jene Bereiche betreffen, wo dies nicht via sektorspezifische Rechtsgrundlagen geregelt werden kann. Dabei sind insbesondere Kriterien zu definieren, ab welchem Ausmass Meldungen erstattet werden müssen.

7.2.2 Bewertung

Im Rahmen der Bewertung gilt es einerseits zu überprüfen, ob allenfalls bestehende, sektorielle Vorgaben in Bezug auf die Resilienz erfüllt werden. Andererseits geht es im sektorübergreifenden Bereich darum, sicherzustellen, dass in jedem Sektor ein auf die anderen Sektoren abgestimmtes Sicherheitsniveau angestrebt wird. Die übergeordneten strategischen Ziele sind in Ziffer 6 festgehalten. Oberste Maxime beim Schutz von KI ist es, dass jede KI ihrer Bedeutung und der jeweiligen Lage angemessen resilient ist. Dementsprechend sollen in Bezug auf das Sicherheitsniveau für die KI keine fixen Schutzziele im Sinne von Grenzwerten (z. B. maximal tolerierte Ausfallzeit) zur Anwendung kommen. Stattdessen soll das für die jeweilige KI zu erreichende Mass an Sicherheit risikobasiert festgelegt werden. Entscheidend ist dabei jeweils, dass ein optimales Verhältnis zwischen Kosten für Schutzmassnahmen und verbleibenden, von Ausfällen der KI ausgehenden Risiken erreicht

wird. Ein entscheidender Faktor in Bezug auf das Sicherheitsniveau ist dabei die Bereitschaft der Gesellschaft, für die Erhöhung der Sicherheit zu bezahlen (z. B. um in einem Ereignisfall ein Todesopfer oder um wirtschaftlichen Schaden zu verhindern). Je höher dieser Betrag ist, desto mehr Mittel stehen für Sicherheitsmassnahmen zur Verfügung, woraus dementsprechend auch ein höheres Sicherheitsniveau resultiert. Somit ist es von zentraler Bedeutung, dass sektorübergreifend sichergestellt wird, dass in allen Sektoren die Zahlungsbereitschaft zur Verhinderung von Schäden infolge von Ausfällen der KI dieselbe ist. Entsprechende Vorschläge zur Zahlungsbereitschaft sind u. a. im SKI-Leitfaden aufgeführt. Sie können bei der Umsetzung auf Ebene der kritischen Teilsektoren oder der KI-Betreiber angewendet werden. Dabei ist zu berücksichtigen, dass das konkrete Mass an Sicherheit, das jeweils zu erreichen ist, erst im Rahmen der Massnahmenplanung festgelegt wird. Es soll jeweils dort liegen, wo ein optimales Verhältnis zwischen Massnahmenkosten und Kosten aus verbleibenden Risiken vorliegt. Ob die entsprechenden Massnahmen umgesetzt werden und dementsprechend das optimale Mass an Sicherheit erreicht wird oder nicht, ist dabei eine politisch-gesellschaftliche Entscheidung. Es ist jeweils eine Güterabwägung notwendig, bei der zusätzlich weitere Anliegen berücksichtigt werden müssen (z. B. Naturschutz, Nachhaltigkeit, Eingriffe in die Wirtschaftsfreiheit usw.).

Ziel:

– In jedem Sektor wird ein auf die anderen Sektoren abgestimmtes Sicherheitsniveau angestrebt, bei dem insbesondere die unterschiedliche Bedeutung (Kritikalität) der verschiedenen KI berücksichtigt wird.

Massnahme 9:

– Die vorhandenen Grundlagen in Bezug auf das Sicherheitsniveau sind bei Bedarf zu überprüfen.

Umsetzung:

– Das VBS (BABS) überprüft bei Bedarf in Zusammenarbeit mit dem UVEK (u. a. BAFU) und den zuständigen Fachämtern die Vorschläge für das Sicherheitsniveau. Eine allfällige sektorübergreifende rechtliche Vorgabe in Bezug auf die Resilienz der KI (Massnahme M2) würde sicherstellen, dass in allen kritischen Sektoren ein abgestimmtes Sicherheitsniveau angestrebt würde.

7.2.3 (Schutz-)Massnahmen

Handlungsfeld (Schutz-)Massnahmen:
Grundlagen zur Verhinderung von Ausfällen kritischer Infrastrukturen schaffen

Im sektorübergreifenden Bereich können verschiedene Massnahmen getroffen werden, um Risiken zu reduzieren, die für viele Sektoren relevant sind, und um schwerwiegende Ausfälle von KI zu verhindern. Solche generischen Risiken betref-

fen etwa das Personal, das für die Durchführung von zentralen Prozessen verantwortlich ist. Um den hohen Sicherheitsstandards zu genügen und einen Austausch mit klassifizierten Informationen zu ermöglichen, sollten diese Personen, abhängig von ihrer Funktion, einer Sicherheitsüberprüfung unterzogen werden können. Gemäss heutiger Rechtslage ist dies derzeit nur in Ausnahmefällen bzw. bei Anpassung der sektorspezifischen Rechtsgrundlagen möglich. Neben der Personensicherheitsprüfung spielen auch weitere personelle Massnahmen eine wichtige Rolle, um die Sicherheit zu gewährleisten. So ist es beispielsweise wichtig, die Personen im Bereich der integralen Sicherheit zu schulen bzw. zu sensibilisieren.

Um Ausfälle von KI zu verhindern, ist es wichtig, dass die relevanten Ressourcen zum Betrieb der KI möglichst unterbruchsfrei zur Verfügung stehen. Im Rahmen der nationalen SKI-Strategie von 2012 wurden diesbezüglich verschiedene Empfehlungen zur Priorisierung von KI bei Ausfällen von wichtigen Gütern und Dienstleistungen (z. B. bei einer Strommangellage) erarbeitet. Diese gilt es umzusetzen und periodisch zu aktualisieren.

Die bisher durchgeführten Arbeiten zur Überprüfung und Verbesserung der Resilienz der KI haben gezeigt, dass nahezu alle KI auf eine funktionierende Stromversorgung und funktionierende Telekommunikationsnetze angewiesen sind und die grössten Risiken durch grossflächige Strom- oder Telekommunikationsausfälle verursacht werden. Während es wirtschaftlich und technisch nicht möglich bzw. verhältnismässig ist, ein alternatives Stromnetz zu errichten, ist im Bereich der Telekommunikation geplant, ein eigenständiges, hochverfügbares und sicheres Datenkommunikationsnetz für die Führungsorgane von Bund und Kantonen sowie die KI-Betreiber zu erstellen. Die Realisierung eines solchen Datennetzes ist insbesondere auch aus SKI-Perspektive von übergeordnetem Interesse.

Ziele:

- Personen, die Zugang zu zentralen Prozessen im Bereich der KI haben, sollen entsprechend ihrer Funktion sicherheitsüberprüft werden können.
- KI werden bei Ausfällen oder Mangellagen von wichtigen Gütern und Dienstleistungen nach Möglichkeit prioritär behandelt.
- Es steht ein hochgradig ausfallsicheres Daten- und Kommunikationsnetz zur Verfügung, an das die KI-Betreiber angeschlossen werden können, um bei einem Ausfall der öffentlichen Telekommunikation relevante Prozesse zum Betrieb der KI aufrechtzuerhalten bzw. die Kommunikation zwischen den KI-Betreibern und den Organisationen für die Krisenbewältigung auf den Stufen Bund und Kantone sicherzustellen.

Massnahme 10:

- Es ist ein Vorschlag für eine zentrale gesetzliche Grundlage zur Sicherheitsprüfung von ausgewähltem Personal der KI-Betreiber und weiteren Zutrittsberechtigten zu schaffen.

Umsetzung:

– Das VBS (BABS in Zusammenarbeit mit IOS) prüft die Schaffung einer zentralen Rechtsgrundlage zur Personensicherheitsprüfung von ausgewähltem Schlüsselpersonal der KI-Betreiber und weiteren Zutrittsberechtigten.

Massnahme 11:

– Die Grundlagen in Bezug auf die Priorisierungen bei Ausfällen und Mangellagen werden gemäss den Empfehlungen überarbeitet.

Umsetzung:

– Die zuständigen Stellen (u. a. WBF (BWL)) setzen die Empfehlungen zur Priorisierung von KI bei Ausfällen und Mangellagen in Zusammenarbeit mit dem VBS (BABS) um.

Massnahme 12:

– Es soll ein alternatives, ausfallsicheres Datennetz realisiert werden, und es sollen die Grundlagen geschaffen werden, um KI-Betreiber an dieses Netz anzuschliessen. Um die Sprachkommunikation sicherzustellen, werden ausgewählte KI-Betreiber an das Sicherheitsfunknetz POLYCOM angeschlossen.

Umsetzung:

– Das VBS (BABS) realisiert auf Basis des Führungsnetzes Schweiz der Armee zusammen mit weiteren Bundesstellen und Kantonen das sichere Datenverbundnetz (SDVN) und klärt die Grundlagen zum Anschluss von KI-Betreibern. Dabei ist insbesondere zu klären, welche Betreiber an das Netz angeschlossen werden und welche technischen und finanziellen Bedingungen die Betreiber erfüllen müssen. Ausgewählte KI-Betreiber werden bei Bedarf im Rahmen der Notkommunikation der WL an das Sicherheitsfunknetz POLYCOM angeschlossen.

Handlungsfeld (Schutz-)Massnahmen:
Vorsorge von Bevölkerung, Wirtschaft und Staat verbessern

Schwerwiegende Ausfälle von KI können das Wohlergehen der Bevölkerung sowie das Funktionieren von Wirtschaft und Staat in schwerwiegendem Masse beeinträchtigen. Das Schadensausmass kann reduziert werden, wenn Bevölkerung, Wirtschaft und Staat angemessen vorbereitet sind. Aus diesem Grund kommt vorsorglichen Planungen zur Bewältigung der Ereignisse und einer vorgängigen Sensibilisierung der Bevölkerung und der Wirtschaft über mögliche Risiken und selbstvorsorglichen Massnahmen grosse Bedeutung zu. Aufgrund der enormen Bedeutung der Stromversorgung stehen vor allem Planungen im Hinblick auf die Bewältigung eines Stromausfalls bzw. einer Strommangellage im Vordergrund. Diesbezüglich sind sowohl auf Stufe Bund wie auch auf Stufe der Kantone zahlreiche Arbeiten initiiert worden. Diese gilt es periodisch zu aktualisieren. In Bezug auf die Sensibilisierung der Bevölkerung und der Wirtschaft sind im Rahmen der WL und von Alertswiss eben-

falls diverse Produkte (z. B. Stromratgeber für Wirtschaft und Bevölkerung, Vorlage für persönlichen Notfallplan usw.) erarbeitet worden.

Ziel:

– Bevölkerung, Wirtschaft und Staat sind im Hinblick auf schwerwiegende Ausfälle von KI vorbereitet, sodass die Auswirkungen reduziert und Ereignisse bewältigt werden können.

Massnahme 13:

– Bund und Kantone erstellen vorsorgliche Planungen zur Bewältigung von schwerwiegenden Ausfällen der KI – insbesondere der Stromversorgung – und aktualisieren diese periodisch.

Umsetzung:

– Die zuständigen Fachbehörden des Bundes erarbeiten im Rahmen der Vorsorgeplanungen des Bundes Planungen zur Bewältigung von Ausfällen der KI. Auf kantonaler Ebene erfolgen solche Planungen im Rahmen der kantonalen Gefährdungsanalysen und Vorsorge. Das VBS (BABS) erstellt eine Übersicht über vorhandene Vorsorgeplanungen und aktualisiert diese periodisch.

Massnahme 14:

– Die Bevölkerung und die Wirtschaft werden über selbstvorsorgliche Schutzmöglichkeiten für den Fall von Ausfällen der KI, insbesondere der Stromversorgung, informiert und sensibilisiert.

Umsetzung:

– Das WBF (BWL) aktualisiert und ergänzt bei Bedarf die Informations- und Sensibilisierungsprodukte in Zusammenhang mit Ausfällen der Stromversorgung und der Telekommunikation. Das VBS (BABS) erstellt im Rahmen von Alertswiss in Zusammenarbeit mit weiteren Stellen (u. a. BWL und Kantone) Sensibilisierungsprodukte zur Stärkung der Selbstvorsorge der Bevölkerung.

Handlungsfeld (Schutz-)Massnahmen:
KI-Betreiber bei der Ereignisbewältigung unterstützen

Im Falle von akuten Gefährdungen und Bedrohungen oder bei schwerwiegenden Ausfällen ist es wichtig, dass die Behörden die KI-Betreiber bei der Ereignisbewältigung möglichst wirkungsvoll subsidiär mit betriebsexternen Mitteln oder Fähigkeiten[2] unterstützen. Damit kann verhindert werden, dass – beispielsweise während eines Hochwassers – durch einen Ausfall von KI zusätzliche Schäden für die Bevölkerung und die Wirtschaft sowie weitere KI (Dominoeffekte) entstehen.

2 Dabei handelt es sich etwa um Einsatzkräfte (Polizei, Feuerwehr, Zivilschutz, Armee), Kommunikationsmittel oder Notstromaggregate.

Für konventionelle Risiken stehen – in teils beschränktem Ausmass – Mittel von Polizei, Feuerwehr, Sanität, Zivilschutz und Armee zu Verfügung. In Bezug auf chemische, biologische und radiologische Stoffe sind zudem subsidiär Mittel des BABS (Einsatzequipe VBS) zur Unterstützung der Einsatzkräfte vor Ort vorhanden. Da der Schutz von KI für diese Einsatzorganisationen jeweils einen Teilauftrag darstellt (neben zahlreichen weiteren Aufgaben), kann dieser nicht als alleinige Grundlage zur Ableitung von Bemessungsgrössen dienen. Weil je nach Ereignis unterschiedliche KI bedroht sein können, ist es ebenso wenig möglich, im Vornherein eine abschliessende Priorisierung oder eine Mindestanzahl an zwingend zu schützenden Objekten festzulegen. Vielmehr geht es darum, sicherzustellen, dass die vorhandenen Mittel im konkreten Ereignisfall möglichst optimal eingesetzt werden. In diesem Kontext kann das Ressourcenmanagement Bund (ResMaB) und dasjenige der Kantone (ResMaK) einen wichtigen Beitrag leisten. Die Prioritätensetzung bei der Mittelzuweisung im Rahmen der subsidiären Unterstützung muss dabei auf strategischer Ebene unter Berücksichtigung der Bedeutung (Kritikalität) der KI, der Bedrohungslage und der zur Verfügung stehenden Mittel erfolgen. Dabei ist davon auszugehen, dass nur wenige, dafür zentrale KI geschützt werden können. Wichtig ist deshalb, dass die Betreiber über eine möglichst gute Prävention bzw. ein ausgereiftes Krisen- und Kontinuitätsmanagement verfügen (wie dies etwa Massnahme 1 zum Ziel hat). Ebenfalls zentral ist die sektorielle und sektorübergreifende Zusammenarbeit der KI-Betreiber.

In Bezug auf die Prioritätensetzung seitens der staatlichen Einsatzorganisationen stellt sich die Herausforderung, dass im Bereich der polizeilichen Gefahrenabwehr bzw. im Bevölkerungsschutz sich die operativen Mittel in der Kompetenz der Kantone und Gemeinden befinden und die Prioritätensetzung in der Regel aus kantonaler bzw. kommunaler Perspektive erfolgt. Bei vielen KI handelt es sich aber um vernetzte Systeme, die auf nationaler oder gar internationaler Ebene betrieben werden (z. B. Übertragungsnetz in der Stromversorgung). Dementsprechend ist es wichtig, dass je nach Ereignis eine übergeordnete Beurteilung auf nationaler Ebene erfolgt. Neben den sektoriellen Krisenorganisationen (z. B. im Rahmen der WL) nimmt diesbezüglich auch der Bundesstab Bevölkerungsschutz (BST BevS) eine zentrale Rolle ein. Diese Zusammenarbeit mit den KI-Betreibern wird derzeit im Rahmen einer Verordnung geregelt und intensiviert. Auch auf lokaler, regionaler und kantonaler Ebene ist die Kooperation mit den zuständigen Führungsorganen von wichtiger Bedeutung, wobei die Zusammenarbeit auf diesen Stufen in vielen Fällen bereits etabliert ist.

Im Hinblick auf Cyber-Risiken sind im Gegensatz zu den konventionellen Risiken noch wenig zivile und militärische Mittel vorhanden, um die Betreiber subsidiär bei der Ereignisbewältigung zu unterstützen. Da der Schutz kritischer Infrastrukturen auch diesbezüglich nur eine Teilaufgabe darstellt, muss der Aufbau der entsprechenden Fähigkeiten in den jeweiligen Aufgabenbereichen sichergestellt werden (Sicherheitspolitik, NCS, Weiterentwicklung der Armee usw.). In der Folge geht es wie oben beschrieben ebenfalls darum, im Rahmen der vorhandenen Mittel sicherzustellen, dass bei der Prioritätensetzung die Bedeutung der KI berücksichtigt wird.

Um eine möglichst optimale Ereignisbewältigung zu gewährleisten, ist es schliesslich notwendig, über aktuelle vorsorgliche Einsatzplanungen zu verfügen. Für be-

sonders relevante Objekte des SKI-Inventars wurden entsprechende Planungen seitens der Armee und mehrerer Kantone bereits erstellt. Im Bereich der Unterstützung durch die Armee decken die Planungen jedoch nur den Schutz von Gebäuden und Anlagen vor Gewalteinwirkungen durch Dritte ab. Planungen sind auch in Bezug auf weitere Mittel (wie z. B. allenfalls aufgebaute Cyber-Mittel) notwendig.

Ziel:

– Die KI-Betreiber werden unter Berücksichtigung ihrer Bedeutung subsidiär mit externen Mitteln wirkungsvoll unterstützt, um Bedrohungen abzuwehren respektive einen Minimalbetrieb und eine rasche Rückkehr zum Normalbetrieb zu ermöglichen.

Massnahme 15:

– Die Prozesse betreffend die Zuteilung der externen Mittel zur Unterstützung der KI-Betreiber bei der Ereignisbewältigung werden mit den betroffenen Stellen analysiert und gegebenenfalls optimiert. Die Prozesse und Zuständigkeiten werden den beteiligten Stellen (insb. KI-Betreiber) kommuniziert.

Umsetzung:

– Das VBS (BABS) prüft zusammen mit weiteren Stellen des VBS (GS, Gruppe Verteidigung) sowie dem EJPD und dem EFD die bestehenden Prozesse und erarbeitet in Abstimmung mit den relevanten Fachämtern gegebenenfalls Vorschläge für eine Optimierung dieser Prozesse.

Massnahme 16:

– Es werden vorsorgliche Einsatzplanungen zum Schutz von KI erstellt und periodisch aktualisiert.

Umsetzung:

– Die Kantone erstellen z. B. im Rahmen der kantonalen Gefährdungsanalyse und Vorsorge zivile Planungen im Bereich des Bevölkerungsschutzes für ausgewählte KI. Das EFD (ISB) prüft zusammen mit dem VBS (GS) die Erarbeitung von zivilen und militärischen Einsatzplanungen in Bezug auf Cyber-Risiken. Die zivilen und militärischen Planungen werden periodisch aktualisiert.

7.2.4 Umsetzung und Überprüfung

Die Umsetzung der in der vorliegenden Strategie definierten Massnahmen muss kontrolliert und gesteuert werden. Weiter ist auch die Wirksamkeit der verschiedenen Massnahmen zu prüfen. Die entsprechenden Aufgaben werden nach Verabschiedung der vorliegenden Strategie in separaten Dokumenten konkretisiert. Weiter ist es wichtig, den Schutz von KI im Rahmen von Übungen zu testen.

Ziel:

– Massnahmen zum Schutz von KI werden im Rahmen von Übungen auf ihre Praxistauglichkeit getestet.

Massnahme 17:

– Im Rahmen von ohnehin geplanten Übungen (Sicherheitsverbundsübungen, strategische Führungsübungen des Bundes, kantonalen Übungen, Simulationsübungen usw.) sollen einzelne SKI-Aspekte gezielt geübt werden.

Umsetzung:

– Die für die Durchführung der Übungen verantwortlichen Stellen bei Bund, Kantonen und KI-Betreibern berücksichtigen SKI-Aspekte bei der Planung und Durchführung von Übungen. Die Erkenntnisse aus den Übungen fliessen wiederum in die übrigen SKI-Arbeiten ein. Das VBS (BABS) unterstützt diese Stellen bei Bedarf beratend.

8 Umsetzung der nationalen SKI-Strategie

8.1 Strukturen und Zuständigkeiten

Die Umsetzung der nationalen SKI-Strategie 2018–2022 erfolgt im Rahmen der bestehenden Strukturen und Zuständigkeiten. Die Koordination bei der Umsetzung der Strategie erfolgt durch die Geschäftsstelle SKI im BABS und wird durch den frühzeitigen Einbezug der relevanten Behörden (auf Stufen Bund und Kantone), der Wirtschaft (insbesondere KI-Betreiber) und der Wissenschaft sichergestellt.

Die Geschäftsstelle SKI unterstützt die zuständigen Stellen bei der Umsetzung der verschiedenen Massnahmen. Sie ist insbesondere für folgende Aufgaben verantwortlich:

– Koordination der Massnahmen zur Verbesserung der Resilienz im sektorübergreifenden Bereich (bspw. Führung des SKI-Inventars)
– Unterstützung der zuständigen Fach-, Aufsichts- und Regulierungsbehörden und der Betreiber bei der Überprüfung und Verbesserung der Resilienz der KI in den einzelnen Sektoren
– Beratung der Kantone bei SKI-relevanten Arbeiten
– Vorbereitung der Geschäfte für die Koordinationsplattformen
– Kontaktstelle für SKI-relevante Aspekte im nationalen und internationalen Umfeld
– Berichterstattung über den Stand der Umsetzung der nationalen SKI-Strategie

Die für die Umsetzung der Massnahmen verantwortlichen Stellen sind in der Strategie sowie in Anhang 2 bezeichnet. Die Überprüfung und Verbesserung der sektorspezifischen Resilienz erfolgt in Zusammenarbeit mit den jeweiligen Fach-, Aufsichts- und Regulierungsbehörden sowie den KI-Betreibern (vgl. Anhang 1).

Zur Steuerung der Arbeiten soll geprüft werden, den Bundesstab Bevölkerungsschutz (BST BevS) (aktuelle Bezeichnung Bundesstab ABCN), in dem die Direktoren aus nahezu allen SKI-relevanten Bereichen vertreten sind, als interdepartementalen Ausschuss (IDA) einzusetzen. Er soll insbesondere die Aufgabe haben, durch ein strategisches Controlling die ziel- und zeitgerechte Umsetzung der SKI-Strategie zu unterstützen.

Weiter soll geprüft werden, eine bestehende ausserparlamentarische Kommission mit SKI-Anliegen zu beauftragen. Sie soll auf strategischer Stufe den frühzeitigen Einbezug der oftmals privaten KI-Betreiber, der Kantone sowie der Wirtschaft und der Gesellschaft als Nutzer der KI sicherstellen. Die Kommission soll zudem gewährleisten, dass das notwendige Fachwissen aus den diversen Bereichen in die strategische Steuerung einfliesst.

8.2 Zeitplan und Controlling

Die Umsetzung der einzelnen Massnahmen wird mit Hilfe eines separaten Umsetzungs- und Controlling-Plans konkretisiert, der nach Verabschiedung der nationalen SKI-Strategie erarbeitet wird. In groben Zügen soll die Umsetzung der terminierbaren Massnahmen in folgendem Zeitplan erfolgen:[3]

Phase 1 (bis Ende 2018)

- Die Umsetzungsplanung ist erstellt.
- Das SKI-Inventar ist überarbeitet und mit Betreiberfirmen von KI ergänzt. (M3)
- Die Prozesse zur subsidiären Unterstützung der KI-Betreiber bei der Ereignisbewältigung sind überprüft, und falls notwendig liegen Vorschläge für deren Optimierung vor. (M15)

Phase 2 (bis Ende 2020)

- Die Prüfung einer Rechtsgrundlage betreffend eine Meldepflicht bei Ausfällen und Störungen ist abgeschlossen. (M2)
- Ein Vorschlag für eine Rechtsgrundlage zur Sicherheitsprüfung von ausgewähltem Personal der KI-Betreiber und weiteren Zutrittsberechtigten ist erstellt. (M10)
- Die Grundlagen zum Anschluss von KI-Betreibern an das SDVN sind geschaffen. (M12)

[3] Daueraufgaben wie das Betreiben von sektorübergreifenden Plattformen (M6) oder die Berücksichtigung von SKI-Aspekten in Übungen (M17) werden nicht gesondert aufgeführt, im Umsetzungsplan aber berücksichtigt.

Phase 3 (bis Ende 2022)

- Die Resilienz der kritischen Teilsektoren ist überprüft, und es sind Massnahmen zur Verbesserung der Resilienz erarbeitet. (M1)
- Die Prüfung einer Rechtsgrundlage mit sektorübergreifenden Vorgaben ist abgeschlossen. (M2)
- Die Erkenntnisse aus den Analysen auf Ebene der kritischen Teilsektoren sind konsolidiert. (M4)

Dem Bundesrat wird alle zwei Jahre über den Stand der Umsetzung Bericht erstattet.

8.3 Revision der SKI-Strategie

Die nationale SKI-Strategie trägt Veränderungen der Rahmenbedingungen und Umfeldentwicklungen Rechnung und wird bei Bedarf aktualisiert. Die vorliegende Strategie wird per 2022 umfassend überprüft und gegebenenfalls angepasst.

8. Dezember 2017

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Doris Leuthard
Der Bundeskanzler: Walter Thurnherr

Anhang 1

Beschreibung der Teilsektoren und Zuständigkeiten für die Verbesserung der Resilienz in den kritischen Sektoren (Massnahme 1)

Tabelle 2

Beschreibung der Teilsektoren und teilsektorspezifischen Zuständigkeiten Massnahme 1

Sektor	Teilsektor	Aus SKI-Perspektive besonders relevante Leistungen*	Zuständige Bundesstellen (nicht abschliessend)**
Behörden	Forschung und Lehre	Forschungsbasierte Dienstleistungen bei Katastrophen und Notlagen (z. B. Erdbebendienst)	SBFI
	Kulturgüter	Gewährleistung der Rechtssicherheit (insb. Staatsarchive), Identitätsstiftung	BABS, BAK
	Parlament, Regierung, Justiz, Verwaltung	Gesetzgebung, Lenkung und Vollzug der Staatsaufgaben, Rechtsprechung und -vollzug, allgemeine Verwaltungsaufgaben (u. a. Warnung und Alarmierung bei Gefahr, Wahrung der inneren Sicherheit)	PD, BK, EDA, MeteoSchweiz, fedpol, IOS, NDB, EFV, ISB und LE, BAFU
Energie	Erdgasversorgung	Handel, Transport, Speicherung und Verteilung von Erdgas	BFE, ERI, BWL
	Erdölversorgung	Handel, Transport, Speicherung und Verteilung von Brenn- und Treibstoffen (Benzin, Flugpetrol usw.)	BFE, ERI, BWL
	Stromversorgung	Erzeugung, Speicherung, Handel, Übertragung und Verteilung von elektrischer Energie (ohne Bahnstromversorgung)	BFE, ELCOM, ESTI, ENSI, BWL
	Fern- und Prozesswärme	Erzeugung und Verteilung von Fern- und Prozesswärme	BFE

Sektor	Teilsektor	Aus SKI-Perspektive besonders relevante Leistungen*	Zuständige Bundesstellen (nicht abschliessend)**
Entsorgung	Abfälle	Sammlung, Entsorgung und Verwertung von Sonder-, Siedlungs- und Industrieabfällen	BAFU
	Abwasser	Entsorgung von häuslichem sowie Gewerbe- und Industrieabwasser zum Schutz von Bevölkerung (Gesundheit) und Umwelt	BAFU
Finanzen	Finanzdienstleistungen	Abwicklung des Zahlungsverkehrs, Versorgung der Bevölkerung mit Bargeld, Kapitalisierung Dritter, Entgegennahme von Einlagen sowie Sicherstellung der Preisstabilität	FINMA, EFV, SIF, BWL, BAKOM
	Versicherungsdienstleistungen	Sicherstellung des Versicherungsschutzes, der finanziellen Unterstützung im Schadenfall sowie der Leistungen im Rahmen der Schadensverhütung (inkl. Kranken- und Sozialversicherungen)	FINMA, EFV, SIF, BSV
Gesundheit	Medizinische Versorgung	Haus-, fach- sowie spitalmedizinische Behandlung und Betreuung sowie tiermedizinische Grundversorgung	KSD, BAG
	Labordienstleistungen	Labordiagnostische Analysen für und zum Schutz von Mensch, Tier und Umwelt	BAG, BLV, BABS
	Chemie und Heilmittel	Versorgung mit Heilmitteln (Arzneimittel und Medizinprodukte), inkl. Impfstoffe	BWL, Swissmedic, Armeeapotheke
Information und Kommunikation	IT-Dienstleistungen	IT-Dienstleistungen für die Wirtschaft (insb. Datenbearbeitung und -speicherung)	BWL, ISB
	Telekommunikation	Notrufe, Internet, Verbreitung von Radio- und TV-Signalen	BAKOM, BWL
	Medien	Information der Bevölkerung bei Katastrophen und Notlagen, politische Meinungsbildung	BAKOM

Sektor	Teilsektor	Aus SKI-Perspektive besonders relevante Leistungen*	Zuständige Bundesstellen (nicht abschliessend)**
	Postdienste	Grundversorgung mit Postdiensten, insb. im Bereich der Amts- und Geschäftskorrespondenz	BAKOM, BWL
Nahrung	Lebensmittelversorgung	Versorgung der Bevölkerung mit Lebensmitteln	BWL, BLW
	Wasserversorgung	Versorgung der Bevölkerung und der Wirtschaft mit Trink- und Brauchwasser	BAFU, BWL
Öffentliche Sicherheit	Armee	Militärische Katastrophenhilfe, subsidiäre Sicherungseinsätze, Führungsunterstützung für Zivile, Landesverteidigung	Gruppe Verteidigung
	Blaulichtorganisationen (Polizei, Feuerwehr, Sanität)	Gewährleistung der öffentlichen Sicherheit, Hilfs- und Rettungseinsätze, Bewältigung von Katastrophen und Notlagen	fedpol, BABS
	Zivilschutz	Unterstützung der Partnerorganisationen zur Bewältigung von Katastrophen und Notlagen	BABS
Verkehr	Luftverkehr	Personen- und Gütertransport in der Luft	BAZL, BWL
	Schienenverkehr	Personen- und Gütertransport auf der Schiene	BAV, BWL
	Schiffsverkehr	Gütertransport auf dem Wasserweg (insb. Anbindung an Meereshäfen)	BAV, BWL
	Strassenverkehr	Personen- und Gütertransport auf der Strasse (motorisierter Individualverkehr und öffentlicher Verkehr)	ASTRA, BWL

* Nicht abschliessende Beschreibung; jeweilige Versorgungsziele werden durch die zuständigen Stellen (u. a. WL) definiert.

** Die genannten Stellen legen gemeinsam mit der Geschäftsstelle SKI fest, welche weitere(n) Stelle(n) (Bund, Kantone, Verbände usw.) bei der Überprüfung und Verbesserung der Resilienz federführend und einzubeziehen sind. Geltende Kompetenzen bleiben vorbehalten.

Anhang 2

Übersicht über Massnahmen, Zuständigkeiten und Nahtstellen

Tabelle 3

Massnahmen, Zuständigkeiten und Nahtstellen

Massnahme	Zuständige Stellen (nicht abschliessend)*	Nahtstellen mit anderen Vorhaben / Aufgaben / Stellen (nicht abschliessend)
M1: Überprüfung und Verbesserung Resilienz der KI	Gemäss Anhang 1	NCS, WL, div. Sektorspezifische Vorhaben und Aufgaben
M2: Prüfung Rechtsgrundlage mit Vorgaben für KI-Betreiber	BABS, Fach-, Aufsichts- und Regulierungsbehörden	NCS
M3: Führung periodisch aktualisiertes SKI-Inventar	BABS	KATAPLAN, Schutz vor Naturgefahren
M4: Erstellung Risikoübersicht über kritische Teilsektoren	BABS, ISB, EFV	NCS, Risikomanagement Bund, WL
M5: Vertiefung Grundlagenforschung im SKI-Bereich	BABS	Ressortforschung des Bundes
M6: Betreiben von Sektorübergreifenden Plattformen	BABS	MELANI, WL
M7: Periodische Überprüfung und Aktualisierung Prozesse zur Orientierung im Ereignisfall	BABS	MELANI
M8: Prüfung Meldepflicht bei Sicherheitsvorfällen und Ausfällen	BABS, ISB	NCS
M9: Periodische Überprüfung und Aktualisierung Angaben zum Sicherheitsniveau	BABS, Fach-, Aufsichts- und Regulierungsbehörden, BAFU	Schutz vor Naturgefahren
M10: Erarbeitung Vorschlag für Schaffung Rechtsgrundlage zur Sicherheitsprüfung von Personal der KI-Betreiber und weiteren Zutrittsberechtigten	BABS, IOS	ISG
M11: Umsetzung und periodische Aktualisierung Empfehlungen zur Priorisierung von KI bei Mangellagen und Ausfällen	BWL, BABS	WL
M12: Realisierung ausfallsicheres Datennetz und Schaffung Grundlagen zur Anbindung von KI-Betreibern	BABS, Gruppe Verteidigung, Kantone	SDVN
M13: Erarbeitung und Aktualisierung vorsorgliche Planungen zur Bewältigung von KI-Ausfällen	Kantone, Fachämter, BABS	KATAPLAN, Vorsorgeplanungen des Bundes, BST BevS
M14: Verbesserung Selbstvorsorge von Wirtschaft und Bevölkerung	BABS, BWL, BK	Alertswiss, WL
M15: Prüfung und Optimierung Prozesse zur subsidiären Unterstützung der KI-Betreiber	BABS, GS VBS, fedpol	ResMaB, FST P, BST BevS

Massnahme	Zuständige Stellen (nicht abschliessend)*	Nahtstellen mit anderen Vorhaben / Aufgaben / Stellen (nicht abschliessend)
M16: Erarbeitung und Aktualisierung vorsorgliche Einsatzplanungen	Kantone, ISB, GS VBS, BABS	NCS, KATAPLAN, PACD
M17: Berücksichtigung von SKI in Übungen	BABS, Kantone, BK, SVS	SFU, SVU

* Die Geschäftsstelle SKI übernimmt jeweils eine Koordinationsfunktion und stellt den Einbezug der zuständigen und relevanten Stellen sicher.

Anhang 3

Abkürzungsverzeichnis

ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAK	Bundesamt für Kultur
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BFE	Bundesamt für Energie
BK	Schweizerische Bundeskanzlei
BLW	Bundesamt für Landwirtschaft
BST ABCN	Bundesstab für atomare, biologische, chemische und Naturgefahren (neue Bezeichnung BST BevS)
BST BevS	Bundesstab Bevölkerungsschutz
BWL	Bundesamt für wirtschaftliche Landesversorgung
bspw.	beispielsweise
bzw.	beziehungsweise
BZG	Bevölkerungs- und Zivilschutzgesetz vom 4. Oktober 2002 (SR *520.1*)
EFD	Eidgenössisches Finanzdepartement
EFV	Eidgenössische Finanzverwaltung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ElCom	Eidgenössische Elektrizitätskommission
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
ERI	Eidgenössisches Rohrleitungsinspektorat
ESTI	Eidgenössisches Starkstrominspektorat ESTI
etc.	et cetera
fedpol	Bundesamt für Polizei
FINMA	Eidgenössische Finanzmarktaufsicht
GPS	Global Positioning System
GS	Generalsekretariat
IDA	Interdepartementaler Ausschuss
IKT	Informations- und Kommunikationstechnik
inkl.	inklusive
IOS	Informations- und Objektsicherheit
ISB	Informatiksteuerungsorgan des Bundes

ISG	Informationssicherheitsgesetz (Entwurf des Bundesrates vom 22. Febr. 2017, BBl *2017* 3097)
IT	Informationstechnik
KI	Kritische Infrastruktur(en)
KSD	Koordinierter Sanitätsdienst
LE	Leistungserbringer
MELANI	Melde- und Analysestelle Informationssicherung
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz vom 25. September 2015 (SR *121*)
PACD	Plan d'Action Cyber-Defence
PD	Parlamentsdienste
ResMaB	Ressourcenmanagement Bund
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SFU	Strategische Führungsübung
SIF	Staatssekretariat für internationale Finanzfragen
SKI	Schutz kritischer Infrastrukturen
SNB	Schweizerische Nationalbank
SVU	Sicherheitsverbundsübung
u.a.	unter anderem
usw.	und so weiter
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
V	Verteidigung
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
vgl.	vergleiche
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WL	Wirtschaftliche Landesversorgung
z. B.	zum Beispiel