RISK AND RESILIENCE
WORKSHOP REPORT

Vierter Trilateraler Workshop D-A-CH Schutz kritischer Infrastrukturen 4.-6. Juni 2018 in Bonn

Zürich, Dezember 2018

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich
im Auftrag des Bundesamt für Bevölkerungsschutz (BABS)

CSS ETH Zurich

ETH zürich

Dieser Bericht ist auf der Webseite www.css.ethz.ch verfügbar.

Center for Security Studies, ETH Zürich

Autoren: Linda Maduz & Florian Roth

Adresse:

Center for Security Studies (CSS)
ETH Zürich
Haldeneggsteig 4, IFW
8092 Zürich / Schweiz
Tel. +41 44 632 40 25
Fax +41 44 632 19 41
www.css.ethz.ch
css@sipo.gess.ethz.ch

Auftraggeber: Bundesamt für Bevölkerungsschutz (BABS)

Projektaufsicht: Stefan Brem, Chef Risikogrundlagen und Forschungskoordination

Auftragnehmer: Center for Security Studies (CSS) der ETH Zürich

Projektleitung ETH-CSS: Tim Prior, Leiter Risk and Resilience Research Team

Zitiervorschlag: *Maduz, Linda; Roth, Florian (2018): Vierter Trilateraler Workshop D-A-CH Schutz kritischer Infrastrukturen, 04.-06. Juni 2018 in Bonn, Risk and Resilience Report, 18-03, Center for Security Studies (CSS), ETH Zürich.*

1 Einleitung

Vom 4. bis zum 6. Juni 2018 trafen sich Behördenvertreterinnen und -vertreter aus den Bereichen Sicherheitspolitik und Bevölkerungsschutz zum vierten trilateralen Workshop *D-A-CH Schutz Kritischer Infrastrukturen (SKI/KRITIS)*.[1] Gemeinsam mit der Workshop-Reihe *D-A-CH Risiko-Analyse* stellt das Veranstaltungsformat zum Thema Kritische Infrastrukturen (KI) ein wertvolles und bewährtes Forum dar, sich grenzübergreifend über inhaltliche und methodische Entwicklungen, Projekte und Massnahmen auszutauschen. Der letzte Workshop zum Thema SKI/KRITIS hatte 2013 in Magglingen (CH) stattgefunden.[2]

Der diesjährige Workshop wurde durch das deutsche Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) an dessen Amtssitz in Bonn organisiert und gemeinsam mit dem österreichischen Bundeskanzleramt, dem österreichischen Bundesministerium für Inneres (BM.I), dem schweizerischen Bundesamt für Bevölkerungsschutz (BABS) und dem Center for Security Studies (CSS) der ETH Zürich durchgeführt. Am Workshop nahmen 18 Vertreterinnen und Vertreter von Bundesbehörden und aus der Wissenschaft teil.

1.1 Ziele des Workshops

Ziel des vierten trilateralen SKI/KRITIS-Workshops war es, die Diskussion zu aktuellen Ansätzen und Herausforderungen beim Schutz Kritischer Infrastrukturen zu fördern und von den unterschiedlichen Erfahrungen in den drei Ländern zu profitieren. Zudem diente der Workshop dazu, den Expertenaustausch hinsichtlich internationaler Entwicklungen und grenzüberschreitender Herausforderungen fortzuführen.

1.2 Struktur des Berichts

Der vorliegende Bericht stellt die Diskussionen entlang unterschiedlicher zentraler Themenfelder und Politikebenen dar. Dabei folgt die Darstellung nicht notwendigerweise der chronologischen Reihenfolge der Redebeiträge. Der Bericht ist wie folgt gegliedert: Nach dieser Einleitung gibt Kapitel 2 zunächst einen Überblick zum aktuellen Stand der Arbeiten im Bereich SKI/KRITIS in Deutschland, Österreich und in der Schweiz, wobei auch die Möglichkeiten einer Einbindung von KI-Betreibern in nationale Krisenstäbe diskutiert wird. Anschliessend werden in Kapitel 3 aktuelle Entwicklungen auf europäischer Ebene sowie im Rahmen weiterer interationaler Organisationen diskutiert. Kapitel 4 befasst sich mit methodischen Fragen im Zusammenhang mit der Analyse und Inventarisierung von kritischen Infrastrukturen. In Kapitel 5 werden ausgewählte Projekte zu den Themen Leitfäden für Unternehmen, Resilienzaufbau und Planungen zur Notstromversorgung vorgestellt. Darauf folgend widmet sich Kapitel 1 vertieft den mannigfaltigen Verbindungen zwischen dem Themenfeld SKI/KRITIS auf der einen Seite und des immer wichtiger werdenden Bereichs der Cybersicherheit auf der anderen Seite. Kapitel 1 behandelt unterschiedliche Aspekte im Themenkomplex Kommunikation, u.a. die Weiterentwicklung von Behördenfunk, Lageverbund und öffentliche Alarmierung. Kapitel 8 enthält einen kurzen Ausblick.

[1] In Deutschland wird für den Themenbereich Schutz Kritischer Infrastrukturen (so die Schreibweise in Deutschland) gemeinhin die Abkürzung KRITIS verwendet, in Österreich und der Schweiz wird die Abkürzung SKI gebraucht. Im vorliegenden Bericht werden beide Abkürzungen äquivalent genutzt.

[2] Der Bericht zum Workshop ist über die ETH Zürich verfügbar: http://www.css.ethz.ch/en/publications/risk-and-resilience-reports.html

2 Nationale SKI/KRITIS-Programme

Der erste Themenblock diente dazu, einen Überblick über den aktuellen Stand der Arbeiten im Bereich Kritische Infrastrukturen in allen am Workshop vertretenen Ländern zu vermitteln. Im Zentrum standen dabei die strategischen Entwicklungen auf bundesstaatlicher Ebene und die Fortschritte, die seit dem letzten D-A-CH-Workshop im Jahr 2013 erzielt wurden.

2.1 Deutschland

Der aktuelle Stand der Strategieentwicklung im Bereich Schutz Kritischer Infrastrukturen in Deutschland wurde von Susanne Krings (BBK) dargestellt. Derzeit bildet die bereits im Jahr 2009 verabschiedete *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS)*[3] den strategischen Rahmen für behördliche Massnahmen auf Bundesebene.

Bereits seit längerem wurde auf Bundesebene über eine Neufassung der Strategie diskutiert, um den politischen, konzeptionellen und regulatorischen Entwicklungen in unterschiedlichen Bereichen Rechnung zu tragen. Der kooperative Ansatz, den Deutschland ebenso wie Österreich und die Schweiz in der Zusammenarbeit zwischen Behörden und Unternehmen verfolgt, sollte darin beibehalten werden.

Die Strategie sollte strukturell erneuert werden, indem sie von vorausschauenden Umsetzungsprogrammen und zurückblickenden Fortschrittsberichten flankiert werden sollte. Auf diesem Weg sollte die Strategie selbst umfänglich „schlank“ gehalten und gleichzeitig der Darstellung aktueller Entwicklungen und konkreter Massnahmen Raum gegeben werden.

Im Zuge dieser Diskussion wurde auch überlegt, die Länder zu beteiligen und die KRITIS-Strategie so auf eine breitere Basis zu stellen, was auch länderseitig grundsätzlich auf positive Resonanz stiess. Später im Jahr, d.h. nach dem D-A-CH-Workshop, wurde allerdings letztlich die Neufassung der Strategie aufgrund anderer bundespolitischer Vorhaben vertagt, so dass die Strategie von 2009 weiterhin Bestand hat.

In der Diskussion erörterten die Teilnehmer des Workshops unter anderem, wie die zahlreichen thematischen Schnittstellen zwischen dem Bereich Schutz Kritischer Infrastrukturen auf der einen und dem stark dynamischen Bereich der Cybersicherheit auf der anderen Seite ausgebaut werden können. Ein weiterer Diskussionspunkt war, welche Auswirkungen die Entwicklungen auf dem Feld des Zivilschutzes, der mit der Konzeption Zivile Verteidigung[4] eine Aufwertung erfahren hat, auf die Weiterentwicklung im Bereich Schutz Kritischer Infrastrukturen in Deutschland künftig haben wird.

2.2 Österreich

In der zweiten Präsentation des Themenblocks gab Michael Kugler (Bundeskanzleramt) einen Überblick über die aktuellen Entwicklungen in Österreich im Bereich Schutz kritischer Infrastrukturen. Den strategischen Rahmen bildet hierbei das Konzept *Umfassende*

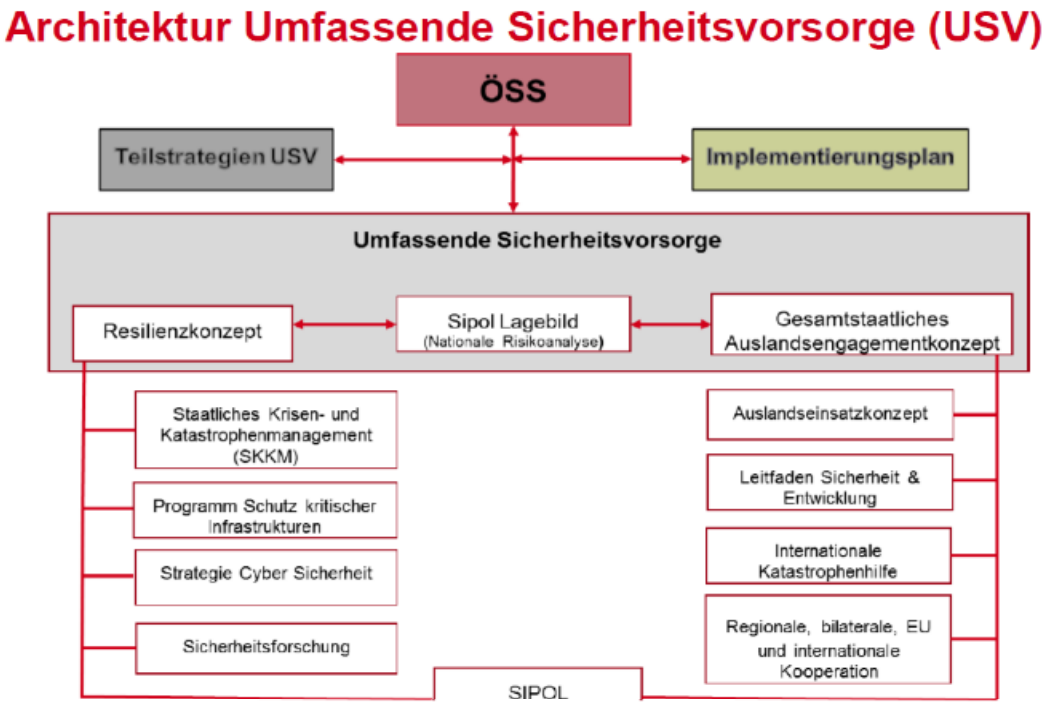

Abbildung 1: Struktur Umfassende Sicherheitsvorsorge. Quelle: BKA

[3] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html

[4] https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Sonstiges/Konzeption_Zivile_Verteidigung_KZV.pdf?__blob=publicationFile

Sicherheitsvorsorge (USV), in der das staatliche Programm zum Schutz Kritischer Infrastrukturen eingebunden ist (APCIP Bund, siehe Kapitel 4.1). Bereits seit gut zehn Jahren verfolgt dieses Programm das Ziel, die Resilienz bedeutender Infrastrukturen zu erhöhen. Zu diesem Zweck wurden zirka 400 strategische Unternehmen identifiziert, welche im Rahmen von sogenannten Sicherheitspartnerschaften bei unterschiedlichen Fragestellungen beraten werden. Hierzu gehören unter anderem regelmässige Sensibilisierungsgespräche zur aktuellen Bedrohungssituation, welche mit Betreibern besonders kritischer Infrastrukturen jährlich durchgeführt werden. Zudem können Unternehmen einzelne Mitarbeiter (mit deren Zustimmung) einer Sicherheitsüberprüfung unterziehen lassen.

Der Fokus der Behörden auf Bundesebene liegt hierbei auf den Betreibern von kritischen Infrastrukturen mit nationalstaatlicher Relevanz. Flankiert werden die Bemühungen der Bundesebene durch ein äquivalentes Programm auf Ebene der Bundesländer (APCIP Länder), das sich gegenwärtig im Abschluss befindet. Im Zentrum stehen hier Betreiber Kritischer Infrastrukturen mit regionaler Bedeutung. Auf diese Weise wird das Programm auf Bundesebene sinnvoll ergänzt. Seit 2014 existiert zudem ein Masterplan für den Bereich kritische Infrastrukturen, der die Grundlage für die jährliche Massnahmenplanung seitens Behörden und Betreiber bildet, Forschungsprojekte koordiniert und die internationale Zusammenarbeit steuert. Die Bereitschaft der Betreiber, sich zu engagieren entwickelt sich insgesamt sehr positiv. Dies ist einerseits darauf zurückzuführen, dass die Unternehmen einer möglichen gesetzlichen Regulierung vorweggreifen wollen. In Folge sicherheitsrelevanter Ereignisse (u.a. im Bereich Terrorismus) ist aber auch eine wachsende Zahl an Betreibern zunehmend sensibilisiert und erkennt gegenseitigen Nutzen und Mehrwert einer engen Zusammenarbeit mit den relevanten behördlichen Strukturen.

2.3 Schweiz

Die strategischen Entwicklungen in der Schweiz wurden durch Stefan Brem (BABS) vorgestellt. Der Schweizerische Bundesrat hat im Dezember 2017 die Aktualisierung der bisherigen *Strategie zum Schutz Kritischer Infrastrukturen (SKI)* von 2012 verabschiedet.[5] Die grundlegende Vision der Strategie für den Zeitraum 2018-2022 hat sich dabei nicht geändert. Vielmehr geht es um eine Institutionalisierung und Weiterführung der vorherigen Strategie. Zentraler Grundsatz ist weiterhin die gemeinsame Verantwortung von Behörden und Betreibern zur kontinuierlichen Verbesserung der Resilienz der Infrastrukturen in der Schweiz. Die Strategie bezeichnet insgesamt 17 Massnahmen, mit deren Hilfe grossflächige und schwerwiegende Ausfälle möglichst verhindert werden bzw. im Ereignisfall das Schadensmass möglichst geringgehalten werden soll. Hierzu zählen unter anderem die Führung eines periodisch aktualisierten SKI-Inventars, die Erarbeitung vorsorglicher Einsatzplanungen sowie die Prüfung einer Meldepflicht und Vorgaben in Bezug auf die Resilienz der KI-Betreiber.

Eine zentrale Funktion bei der Koordination der vielzähligen Aktivitäten zum Schutz Kritischer Infrastrukturen in der Schweiz erfüllen die sektorübergreifenden Plattformen. Eine wichtige Rolle spielt hierbei die Arbeitsgruppe SKI, in der sich neben den relevanten Bundesämtern auch zwei Kantone Genf und Basel Stadt stellvertretend engagieren. Ergänzt wird die Arbeitsgruppe durch die Plattform der kantonalen SKI-Kontaktstellen, die in erster Linie der horizontalen Abstimmung u.a. im Umgang mit der KI-Datenbank zwischen den Kantonen dient. Hinzu kommen die Plattform der nationalen KI-Betreiber für den Erfahrungsaustausch sowie die Plattformen für die einzelnen kritischen Teilsektoren für die Aktualisierung der KI-Datenbank.

Im föderal geprägten System der Schweiz liegt der Schwerpunkt der Verantwortung auf Bundesebene im Bereich der Identifikation der kritischen Infrastrukturen, der Sicherstellung von sicheren Datenverbindungen sowie der sektoriellen Überprüfung und Verbesserung der Resilienz in Zusammenarbeit mit den zuständigen Aufsichts- und Regulierungsbehörden. Hinzu kommen die Schutzaufgaben der Armee, die für national bedeutsame KI-Objekte Einsatzpläne erstellt. Diese Aktivitäten unterstützen die unterschiedlichen Arbeiten und Massnahmen auf Ebene der Kantone, bei denen die Hauptverantwortung bei der Koordination von zivilen Einsatzplanungen für die Kritischen Infrastrukturen liegt. Aktuell ist die Mehrheit der Kantone in diesem Bereich aktiv, wobei sich zum Teil deutliche Unterschiede in der Breite und Tiefe der Arbeiten auf Kantonsebene zeigen – von der Führung der kantonalen KI-Listen bis zu eigentlichen kantonalen SKI-Strategien.

2.4 Einbindung von KI-Betreibern in nationale Krisenstäbe

Ein interessanter Vergleich, der im Rahmen einer offenen Diskussion geführt wurde, betrifft die Organisation von nationalen Krisenstäben und die Einbindung von KI-Betreibern in diese Stäbe. Auch hier zeichnen sich stetige Entwicklungen in allen drei Ländern ab.

Den Schweizer Bundesstab für Bevölkerungsschutz (BSTB), der für die Koordination bei der Bewältigung aller bevölkerungsschutzrelevanter Ereignisse auf Bundesebene zuständig ist, gibt es in der aktuellen Form seit April 2018. Der Bundesrat beschloss dafür das Aufgabenspektrum des bisherigen Bundesstabs für atomare, biologische oder chemische Schadensereignisse sowie für Naturereignisse (BST ABCN) zu erweitern, der 2011 geschaffen worden ist. Der Einsatzbereich des BSTB umfasst Gefährdungen wie Erdbeben, Pandemien, Kernkraftwerks-Unfälle, aber auch grosse Stromausfälle oder Strommangellagen. Aufgewertet wurde die Zusammenarbeit der Kantone

[5] https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html

sowie die der KI-Betreiber: Neu werden neben den Regierungskonferenzen auch die Kantonalen Führungsorgane in den Stab integriert und bei Bedarf können KI-Betreiber und Fach-Sonderstäbe hinzugezogen werden. Der BSTB kann ebenfalls auf Ersuchen der KI-Betreiber aktiviert werden.

Die Strukturen in Deutschland sind vergleichbar mit denen in der Schweiz. Für bevölkerungsschutzrelevante und länderübergreifende/ nationale besondere Lagen stellt der Krisenstab des Innenministeriums (BMI) die zentralen Strukturen für das gesamtstaatliche Krisenmanagement. In die direkte fachliche Zuständigkeit des BMI fallen Krisen im Ernährungs-, Gesundheits- und Strombereich. Bei Naturgefahren hingegen wird das Krisenmanagement auf Bundesebene nur nach Ersuchen der betroffenen Länder aktiviert. Nach dem Modell des Krisenstabes BMI werden je nach Gefahren- und Schadenslage auch gemeinsame nationale Krisenstäbe mit anderen Ressorts gebildet. Eine entsprechende Verständigung gibt es zwischen dem BMI und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) im Falle von atomaren Gefahrenlagen und dem BMI und dem Bundesministerium für Gesundheit (BMG) im Falle einer Pandemie und des Bioterrorismus. Die KI-Betreiber werden nicht direkt in die Arbeit der Krisenstäbe einbezogen. Ihre Interessen fliessen über die einbezogenen Ämter oder Länder ein. Anders als der BST Bevölkerungsschutz in der Schweiz beschäftigt sich der Krisenstab BMI nicht mit der Vorsorgeplanung.

In Österreich wird die gesamtstaatliche Koordination bei Krisen und Katastrophen durch das Staatliche Krisen- und Katastrophenmanagement (SKKM) gewährleistet. Die Geschäftsstelle gehört dem Innenministerium an. Es gibt ein regelmässig tagendes Gremium von Vertretern des BM.I, des Verteidigungs- bzw. des Aussenministeriums und des Bundeskanzleramtes, welches auch im Krisenfall zusammenkommt. Für politische Koordinationsaufgaben kann der nach dem SKKM-Modell vorgesehene Krisenstab auch ausgebaut werden durch zuständige Ressorts und KI-Betreiber. In der Migrationskrise 2015/2016 übernahmen KI-Betreiber beispielsweise die Unterbringung und Versorgung.

3 Europäische und internationale Entwicklungen

Im zweiten Teil des Experten-Workshops standen Entwicklungen auf europäischer Ebene sowie im Rahmen weiterer internationaler Organisationen im Vordergrund.

3.1 Europäische Union

Der gegenwärtige Stand der Entwicklungen im Bereich Schutz Kritischer Infrastrukturen auf Ebene der Europäischen Union wurde von Michael Kugler (BKA) und Monika John-Koch (BBK) referiert. Zentrale Grundlage für die Zusammenarbeit der europäischen Partner bilden aktuell weiterhin das *Europäische Programm zum Schutz Kritischer Infrastrukturen (EPCIP)* mit der Richtlinie 2008/114/EC aus dem Jahr 2008[6] als einem wesentlichen Teilelement daraus. Hierbei stehen gegenwärtig die regelmässigen Berichtspflichten der Mitgliedsstaaten im Vordergrund. Viele EU-Staaten haben in den letzten Jahren die Richtlinie als Anstoss genutzt, um ihre nationalen Massnahmen im Bereich Schutz Kritischer Infrastrukturen voranzubringen.

Auf einen gegenseitigen Erfahrungsaustausch und auf die Unterstützung von assoziierten Drittstaaten und Beitrittskandidaten bei der Heranführung an EU-Programme zielt ein für Juli dieses Jahres in Wien geplanter Workshop im Rahmen von EPCIP ab. Veranstalter ist die Europäische Kommission, unterstützt durch das Mitgliedsland Österreich. Geografischer Fokus des Treffens sind insbesondere der Westbalkan und die östliche Nachbarschaft der EU. Der zweitägige Workshop soll dazu dienen, Erfahrungen und Best Practices auszutauschen und die Partnerländer an EU-Standards heranzuführen.

Für die kommenden Jahre ist eine Überarbeitung der strategischen Grundlagen geplant. Gegenwärtig finden Diskussionen statt, wie die EU-Richtlinie 2008/114/EC weiterentwickelt werden könnte, um einen neuen Impuls für den Themenbereich Kritische Infrastrukturen auf europäischer Ebene zu setzen. Ausgehend von den derzeitigen Planungen wird der Abschluss der Überarbeitung während der deutschen Ratspräsidentschaft 2020 erfolgen. Ziel einer möglichen neuen Richtlinie sollte sein, den Blick von rein bilateralen Konsultationen hin zu kritischen Infrastrukturen mit europäischer Bedeutung zu lenken und insbesondere bei grenzübergreifend relevanten Themen ein gemeinsames Vorgehen sicherzustellen. Als ein Beispiel hierfür wurde in der anschliessenden Diskussion das Thema Gasversorgung genannt (Bsp. Nord Stream 2), das eine gesamteuropäische Bedeutung hat, gegenwärtig aber vornehmlich auf nationaler Ebene behandelt wird. Auch das Thema hybride Bedrohungen könnte in Zukunft eine zunehmend wichtige Rolle auf EU-Ebene spielen. Gleichzeitig legen die Mitgliedsstaaten Wert darauf, dass ihr nationaler Handlungsspielraum nicht durch Vorgaben der EU eingeschränkt wird. Schliesslich diskutierten die Teilnehmer, inwiefern sich die Schweiz künftig stärker auf europäischer Ebene im Bereich Kritische Infrastrukturen engagieren könnte.

3.2 Weitere internationale Institutionen

Im zweiten Beitrag des Themenblocks stellte Linda Maduz (ETH Zürich) aktuelle Bestrebungen unterschiedlicher internationaler Institutionen im Bereich Schutz kritische Infrastrukturen dar. Wie auch nationale Behörden sind die internationalen Organisationen gezwungen, sich an sehr dynamische, häufig nicht-lineare technische Entwicklungen und die damit einhergehenden Herausforderungen anzupassen. Hinzukommen damit verknüpfte, aber auch parallel verlaufende sozio-organisatorische Trends, die ebenfalls tiefgreifende Auswirkungen auf den Schutz Kritischer Infrastrukturen haben können. Hierzu zählt unter anderem die wachsende Urbanisierung in vielen Weltregionen.

Im Zuge der zunehmenden grenzüberschreitenden Vernetzung im Bereich Kritische Infrastrukturen nimmt die Bedeutung internationaler Organisationen insgesamt zu. Zugleich lassen sich in Teilen auch Versuche der Re-Nationalisierung dieses Politikbereiches beobachten, was zu zusätzlichen Herausforderungen beim grenzüberschreitenden Schutz Kritischer Infrastrukturen führen kann. Relevant in diesem Zusammenhang sind insbesondere die Aktivitäten folgender Organisationen:

- NATO
- Weltbank
- Vereinten Nationen
- Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)
- Internationale Energieagentur (IEA)

In der anschliessenden Diskussion erörterten die Teilnehmer die Herausforderungen, die sich sowohl nationalen Behörden als auch internationalen Organisationen im Umgang mit zunehmend komplexen Technologiesystemen stellen. Insbesondere die Entwicklungen im Bereich künstliche Intelligenz werden zu tiefgreifenden Veränderungen führen. Als Beispiele wurden hier Smart Grids und Smart Meter genannt, die unter anderem in der Stromversorgung eine immer wichtigere Rolle spielen. Bereits heute haben Entscheidungsträger Probleme, die relevanten Systeme und deren Funktionsweisen ausreichend zu verstehen, um gegebenenfalls frühzeitig korrigierende Massnahmen ergreifen zu können. In Zukunft werden sich diese Herausforderungen aller Voraussicht nach weiter verschärfen.

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

4 Methodik

In diesem Abschnitt werden die methodischen Arbeiten zum Schutz Kritischer Infrastrukturen in Österreich, Deutschland und der Schweiz dargestellt.

4.1 Risikoanalysen SKI in Österreich

Die Risikoanalysen SKI in Österreich, d.h. der Stand der Arbeiten und aktuelle Entwicklungen, wurden von Isabella Palla (BM.I) und Sylvia Mayer vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) präsentiert. In Österreich erfolgen staatliche Risikoanalysen im Bereich SKI im Rahmen des *Österreichischen Programms zum Schutz Kritischer Infrastrukturen (APCIP*[7]*).* Das APCIP basiert auf einem auf KI-Betreiber ausgerichteten Arbeitsprogramm und verfolgt einen All-Gefahren-Ansatz. Ziel des Bundesprogrammes (Grundlage 2008, Masterplan APCIP 2014) und der Länderprogramme (Beschluss Landeshauptleutekonferenz 2016) ist die Identifikation, Analyse und Bewertung von Risiken für den SKI sowie die Unterstützung von strategisch wichtigen Unternehmen beim Aufbau einer umfassenden Sicherheitsarchitektur (ausschliesslich des betrieblichen Risikomanagements).

Die für die Risikoanalyse verwendeten Methoden und Verfahren wurden in Abstimmung mit den Arbeiten im österreichischen Sicherheitsforschungsprogramm *KIRAS* bestimmt und orientieren sich an internationalen Standards. Der Gefahrenkatalog wurde in Zusammenarbeit mit Unternehmen definiert; gefragt wurde nach branchenrelevanten Risiken. Unterschieden wird zwischen von der Natur verursachten, vom Mensch versursachten, d.h. terroristischen und sonstigen, sowie technischen Gefahren. Für diese vier Gefahrentypen werden in den Analysen, die allesamt nicht öffentlich zugänglich sind, separate, unterschiedlich skalierte Risikomatrizen erstellt.

Bei der Durchführung der staatlichen Risikoanalyse wird, anders als in der Schweiz, ein „top-down"-Ansatz verfolgt: Die Identifikation und Einschätzung von relevanten Risiken erfolgt in einem ersten Schritt auf einer gesamtstaatlichen, alle Sektoren umfassenden Ebene. In einem nächsten Schritt sollen die branchenspezifischen Risikoanalyse auf Ebene des Bundes erfolgen (separate Arbeitsgruppen, im ersten Schritt mit den Schwerpunktbranchen Gesundheit, Energie und Finanzen), bevor auf der Ebene der Länder die Risikoanalyse erst über alle Sektoren und dann sektorenspezifisch durchgeführt wird.

Im Plenum wurde unter anderem diskutiert, wie bei der Risikoidentifikation und -einschätzung die Zusammenarbeit und Konsensfindung zwischen den Teilnehmern aus Verwaltung und Wirtschaft optimal gestaltet werden kann und wie Divergenzen abgebildet werden können, um einen Informationsverlust zu vermeiden.

4.2 Risiko- und Verwundbarkeitsanalysen Schweiz

Ein wesentlicher Schwerpunkt sowohl der nationalen SKI-Strategie (siehe Kapitel 2.3). als auch der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken stellt die Überprüfung und Verbesserung der Resilienz der kritischen Teilsektoren dar. Giorgio Ravioli (BABS) stellt das methodische Vorgehen vor, das dabei zur Anwendung kommt. Es orientiert sich wesentlich am SKI-Leitfaden, der sich an die Betreiber der kritischen Infrastrukturen richtet.

Um mögliche systemische Schwachstellen zu identifizieren, wurden Risiko- und Verwundbarkeitsanalysen für alle 27 kritischen Teilsektoren durchgeführt. In einem weiteren Schritt konnten für die meisten dieser Teilsektoren auch schon mögliche Massnahmen gemeinsam erarbeitet und in einem Massnahmenbericht zusammengestellt werden.

Für die Erstellung der branchenspezifischen Risiko- und Verwundbarkeitsanalysen wurde eng mit Unternehmen und Dachverbänden in den jeweiligen Teilsektoren zusammengearbeitet. Das BABS identifizierte in Abstimmung mit den zuständigen Fachbehörden die relevanten Akteure. Betreiber und Verbände bildeten zusammen mit Fachbehörden und Regulatoren Expertengruppen, die sich in einer Reihe von Workshops trafen, um die relevanten kritischen Prozesse zu erheben und deren Abhängigkeit von Ressourcen zu bewerten. In einem weiteren Schritt identifizierten die Expertengruppen die für den jeweiligen Teilsektor relevanten Gefährdungen und bestimmen das entsprechende Schadensausmass und die Eintrittswahrscheinlichkeit. Dabei wurden insbesondere Cyber-Risiken, aber auch weitere relevante Gefährdungen betrachtet. Der in der nationalen Gefährdungsanalyse *Katastrophen und Notlagen 2015* enthaltene Gefahrenkatalog diente als Basis für das zu berücksichtigende Gefahrenspektrum.

Geplant ist, dass die Analysen in regelmässigen Zyklen weitergeführt werden. Der Mehrwert der Durchführung solcher Analysen wird in erster Linie auf der Ebene der Gesellschaft verortet - nicht auf Unternehmensebene. Allerdings waren die Unternehmen dem für sie nicht verpflichtenden Prozess gegenüber grundsätzlich sehr positiv eingestellt und entsprechend kooperativ. Durch den Prozess wurde eine Sensibilisierung der unterschiedlichen Branchen verbessert. Zudem wurde der Dialog zwischen den Branchen sowie mit anderen Akteuren wie dem NDB/ MELANI weiter etabliert. Dadurch wurde auch eine gute Basis für die Zusammenarbeit in der Massnahmenplanung geschaffen, welche in den branchenspezifischen Schlussberichten definiert wurde. Dass das BABS den Prozess primär methodisch begleitete und daher als Dienstleister und nicht als Regulator wahrgenommen wurde, war dem Prozess als Ganzes dienlich.

[7] Austrian Program for Critical Infrastructure Protection

4.3 Weiterentwicklung Methode SKI-Inventar (CH)

Die Methode zur Erstellung des SKI-Inventars in der Schweiz wurde von Nick Wenger (BABS) vorgestellt. Im Auftrag des Bundesrats erstellte das BABS Ende 2012 erstmals ein Verzeichnis der kritischen Infrastruktur-Objekte der Schweiz, welches zirka 1'000 Objekte umfasst. Ziel des Inventars ist es, einzelne Infrastruktur-Objekte zu identifizieren, die von strategisch wichtiger Bedeutung sind. Dabei handelt es sich um Objekte, die eine zentrale Bedeutung bei der Versorgung mit wichtigen Gütern und Dienstleistungen haben respektive um solche, die ein erhebliches Gefahrenpotenzial darstellen.

Die Identifikation und Beurteilung der Objekte basiert auf einem standardisierten Verfahren und einheitlichen Kriterien. Massgebend ist folgendes vierstufiges Verfahren, das in allen 27 Teilsektoren angewendet wurde: 1. Identifikation der relevanten Prozesse, 2. Bezeichnung der massgebenden Objektgruppen, 3. Festlegung Objektgruppen-spezifischer Kriterien, 4. Erfassung und Beurteilung der Bedeutung der Objekte.

Die Beurteilung der Bedeutung der KI-Objekte (Schritt 4) erfolgt entweder anhand der quantitativen Leistung des Objekts oder durch eine qualitative Beurteilung (Bestimmung des Funktionswerts: welchen Beitrag erbringt das einzelne Objekt zum Funktionieren des jeweiligen Teilsektors?).

Als *national* kritische Objekte werden Objekte gesehen mit hohem Leistungspotenzial (Leistungsklassen 4 und 5 von insgesamt fünf Klassen, wo bei einem Ausfall über 700'000 bzw. 2.5 Millionen Einwohner betroffen wären) und/oder Objekte mit „erheblichem" Gefahrenpotenzial. Das SKI-Inventar von 2012 wurde in rund 80% der Kantone mit kantonal relevanten Objekten ergänzt (im Schnitt zehn bis 20 zusätzliche Objekte).

Das SKI-Inventar wird heute als eine wichtige Planungs- und Priorisierungsgrundlage in der Vorsorge und Ereignisbewältigung für den Bundesstab Bevölkerungsschutz, die Armee, Kantone und KI-Betreiber verwendet. Es hat sich auch mehrfach im Ereignisfall (z.B. Priorisierung der Hochwasserschutzmassnahmen 2015) bewährt. Wichtig ist eine periodische Aktualisierung des SKI-Inventars, die alle zwei (Grunddaten) bzw. vier Jahre (vollständige Revision) geplant ist. Ausserdem sind weitere Ergänzungen vorgesehen: Das SKI-Inventar beschränkte sich bisher auf Bauten und Anlagen, weshalb Aussagen über national kritische Betreiber nur bedingt möglich waren. Vorgesehen ist die Definition von Kriterien zur Identifikation von versorgungsrelevanten Betreiberfirmen ähnlich wie in Deutschland oder Österreich. Demgegenüber werden in Deutschland seit den 70er Jahren keine Objekte mehr systematisch erfasst, in Österreich werden sowohl kritische Objekte als auch Betriebe identifiziert. Das Gesamtverzeichnis der KI-Objekte in der Schweiz ist als GEHEIM klassifiziert. Das BABS verfügt über die Grundinformationen und bestimmt, wer berechtigte Bedürfnisträger sind (z.B. Führungsorgane der Kantone), welche Zugriffe auf gewisse Informationen erhalten (z.B. betreffend einzelner Teilsektoren oder Kantone).
In der Diskussion im Plenum wurde die Schwierigkeit besprochen, Dependenzen und Redundanzen von KI-Objekten in einer Gesamtsicht zu bestimmen und abzubilden. Verschiedene relevante Forschungsprojekte wurden in diesem Zusammenhang genannt.

4.4 Integriertes Risiko- und Krisenmanagement Deutschland

Das in Deutschland verwendete *Integrierte Risiko- und Krisenmanagement im Bevölkerungsschutz* wurde von Eva Stock (BBK) erläutert. In Deutschland gibt es zum einen die die 2015 publizierte *Risikoanalyse im Bevölkerungsschutz: Ein Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz*.[8] Sie setzt sich mit der Perspektive des Staates, d.h. der Regionen und Städte, auseinander. Sie ist ein Leitfaden für Landkreise und kreisfreie Städte über die Rahmenbedingungen und die genaue Vorgehensweise bei der Einschätzung und Beurteilung von Gefährdungen sowie Stresstest für die Bewältigungskapazitäten der Gefahrenabwehr. Die Risikoanalyse im Bevölkerungsschutz richtet sich an die für die Analyse von Gefährdungsszenarien zuständigen Experten in den Städten und Regionen, welche u.a. die Betroffenheit der Bevölkerung von KI-Ausfällen abschätzen. Zum anderen gibt es die Publikation *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement (2011),* die die Perspektive der KI-Betreiber ins Zentrum rückt.[9] Sie versteht sich als Leitfaden für Unternehmen und Behörden und unterstützt bei der strukturierten Ermittlung von Risiken, der Abschätzung der betrieblichen Konsequenzen und der darauf basierenden Umsetzung von vorbeugenden Maßnahmen sowie dem effektiven und effizienten Umgang mit Krisen.

Das Integrierte Risikomanagement zielt auf eine Verzahnung zwischen dem Risikomanagement der KI-Betreiber und dem Risikomanagement der staatlichen Gefahrenabwehr und bildet somit das verbindende Element der bereits veröffentlichten Publikationen. Im Rahmen des durch das Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojektes *Kritische Infrastrukturen – Resilienz als Mindestversorgungskonzept (KIRMin)* der Förderlinie *Zivile Sicherheit* wird das *Integrierte Risikomanagement* in Pilotregionen umgesetzt und weiterentwickelt. Im Fokus stehen dabei Akteure der Kreisebene und KI-Betreiber, die z.B. in der Strom- und Wasserversorgung tätig sind. Damit unterscheidet sich der Ansatz von Risikoanalyse-Ansätzen in Österreich und der Schweiz, wo Analysen im SKI-Bereich in erster Linie auf der Ebene der Länder/ Kantone beziehungsweise des Bundes durchgeführt werden. Weiter

8 https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_16_Risikoanalyse_im_BS.pdf?__blob=publicationFile

9 https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf?__blob=publicationFile

zeichnet sich der Ansatz dadurch aus, dass er verfahrens- aber nicht sektoren- oder gefahrenspezifisch ist.

Der durch das Integrierte Risikomanagement angestrebte strukturierte Austausch von relevanten Informationen an den Schnittstellen zwischen den Unternehmen und Behörden soll die Grundlage für eine Vernetzung der Notfallplanung bilden. Vom BBK werden für diesen Austausch praktische Handreichungen in Form von Beispielszenarien und Checklisten mit einer Auswahl relevanter Fragen zur Verfügung gestellt. Die Checklisten enthalten Fragen, welche die Gefahrenabwehr an KI-Betreiber richten kann, wie z.B. zu den Kontaktstellen im Krisenfall, zu Einzelheiten bei Ausfällen infolge eines Ereignisses (Länge, Anzahl betroffener Personen etc.) und den Ressourcen der Unternehmen im Ereignisfall. Welche Szenarien für die Gefahrenabwehr relevant sind, ist umgekehrt eine Frage, welche von Seiten der KI-Betreiber an die Gefahrenabwehr gestellt werden kann. Die Publikation eines entsprechenden Leitfadens zum Integrierten Risikomanagement im Bevölkerungsschutz ist für 2019 geplant.

Die Risikoanalyse ist die dritte von sechs Phasen, die an der Schnittstelle des Risikomanagements von KI-Betreibern und Gefahrenabwehr identifiziert wurden. Sie sieht eine Verwundbarkeitsanalyse vor, welche die Resilienz der Anlagen prüft unter Annahme eines ausgewählten Szenarios, wie z.B. eines 24-stündigen Stromausfalls. Die KI-Betreiber müssen dafür eine Reihe von Ja/Nein-Fragen beantworten, u.a. zur Exposition, zur Funktionsanfälligkeit und der technischen und organisatorischen Ersetzbarkeit der Anlage. Die auf diese Weise systematisch erfassten Informationen, insbesondere Informationen zu Auswirkungen auf die Bevölkerung, die mit einem Ausfall der kritischen Dienstleistung verbunden sind, sollen dann der Gefahrenabwehr zur Verfügung gestellt werden. In der Praxis funktioniert der strukturierte Austausch zwischen Unternehmen und Behörden je nach Landkreis unterschiedlich gut. Im Umgang mit den Betreibern verfolgt Deutschland ähnlich wie Österreich und die Schweiz einen kooperativen Ansatz. Das heisst, die Zusammenarbeit mit den Unternehmen stützt sich weitestgehend auf deren freiwilliges Engagement. Hingegen sollen verpflichtende Vorgaben und Massnahmen weitestgehend vermieden werden.

Die Gründe für das (Nicht-) Funktionieren des strukturierten Austausches wurden in der nachfolgenden Diskussion besprochen. Ressourcenreiche, d.h. grosse oder reiche Unternehmen und Kommunen, engagierten sich eher im Rahmen des Integrierten Risikomanagements. Dasselbe gilt für „gebrannte Kinder“ wie z.B. hochwassererfahrene Kommunen. Jedoch ist vielerorts dieser strukturierte gemeinsame Austausch noch nicht selbstverständlich; vieles hängt auch vom Engagement einzelner Personen ab.

5 Ausgewählte Projekte

5.1 Leitfaden für die Sicherheit in Unternehmen in Österreich

Wie Michael Kugler (BKA) ausführte, nutzen bereits seit 2013 österreichische KI-Betreiber die Möglichkeit, anhand des *Leitfadens für die Sicherheit in Unternehmen in Österreich* ihre eigenen Massnahmen zu überprüfen und zu optimieren. Das mit Hilfe des EU-Innensicherheitsfonds (ISF) finanzierte Tool verfolgt den Ansatz, dass die Analyse von Verwundbarkeit durch die Unternehmen selbst geleistet werden sollte. Zudem sollen die Unternehmen dazu ermutigt werden, bereits bestehende Risikomanagement-, Business-Continuity-Management und Security-Management-Prozesse auszubauen.

Der Leitfaden gliedert sich in einen allgemeinen Informationsteil und einen detaillierten Bewertungsteil. Der zweite Teil des Leitfadens umfasst insgesamt rund 400 Fragen, die ein sehr breites Spektrum abdecken. Berücksichtigt werden neben organisatorischen und rechtlichen Fragen auch Herausforderungen, die durch Technikanwendungen bestimmt werden, Marktrisiken, Naturgefahren sowie intentionale Gefahren. Durch das detaillierte Self-Assessment können die Unternehmen ihr eigenes Schutzniveau sowie etwaige Lücken identifizieren. Voraussetzung hierfür ist die Mitwirkung des CEO sowie der relevanten Abteilungsleitungen als Risikoeigner. Um die Verwendung praktikabel zu halten, können die Unternehmen je nach Bedarf auch nur einzelne Elemente des Bewertungstools anwenden.

Die Selbstbewertung der Unternehmen erfolgt offline, um die Datensicherheit sicherzustellen. Eine Datenabfrage der Behörden findet bewusst nicht statt, um ein möglichst offenes Antwortverhalten der Unternehmen zu fördern. Auf Wunsch können die KI-Betreiber jedoch die Ergebnisse mit den Partnern bei den Behörden erörtern und gegebenenfalls Unterstützung bei der Planung eigener Massnahmen erhalten. Darüber hinaus kann der Leitfaden auch von Bundesländern genützt werden, um die von ihnen betreuten regionalen KI-Betreiber mit einem einheitlichen Ansatz zu unterstützen.

5.2 Massnahmen zur Verbesserung der Resilienz in der Schweiz

Nick Wenger (BABS) präsentierte den SKI-Leitfaden, den das BABS 2015 publiziert hat. Der Leitfaden richtet sich an die Betreiber kritischer Infrastrukturen und die jeweils zuständigen Fachbehörden und beschreibt, wie die Resilienz kritischer Infrastrukturen überprüft und verbessert werden kann. Er wurde in Kooperation mit Experten aus den Bereichen Risiko-, Krisen- und Kontinuitätsmanagement erarbeitet. Methodisch zeichnet er sich durch eine integrale und risikobasierte Herangehensweise aus. Das übergeordnete Ziel des Leitfadens ist es, schwerwiegende Ausfälle vermeiden respektive im Ereignisfall das Schadensausmass, d.h. die Ausfallzeit, reduzieren zu helfen. Hierbei steht für den SKI, in Abgrenzung zur Unternehmensperspektive, die Beeinträchtigung der Bevölkerung und ihrer (wirtschaftlichen) Lebensgrundlagen infolge von KI-Ausfällen bzw. -Störungen im Fokus.

Der Prozess zur Überprüfung und Verbesserung der Resilienz von Kritischen Infrastrukturen ist in fünf Teilschritte gegliedert: Nach der Analyse (inkl. Identifikation der kritischen Prozesse, der Verwundbarkeiten, der relevanten Gefährdungen und der Risikoeinschätzung) wird eine Bewertung vorgenommen, bei der u. a. das angestrebte Sicherheitsniveau festlegt wird. In einem dritten Schritt werden die optimalen (Schutz-)Massnahmen, d.h. präventive, vorsorgliche und ereignisbezogene Massnahmen, definiert. Diese werden in der Folge umgesetzt, bevor in einem letzten Schritt die Wirksamkeit der Massnahmen überprüft wird.

Der Schwerpunkt der Präsentation von Nick Wenger lag auf dem Vorgehen zur Ermittlung von geeigneten Massnahmen zur Verbesserung der Resilienz. Der SKI-Leitfaden verfolgt dazu einen risikobasierten Ansatz, der zum Ziel hat, ein optimales Verhältnis zwischen Kosten für zusätzliche Schutzmassnahmen und der damit erzielten Risikoreduktion zu erzielen. Zur Bestimmung der geeigneten Massnahmen wird für alle in Frage kommenden Massnahmen ermittelt, welche Kosten damit verbunden sind und wie stark sie das Risiko jeweils reduzieren. Die optimale Massnahmenauswahl liegt bei derjenigen Massnahmenkombination, bei der die Gesamtkosten (bestehend aus den Massnahmenkosten und den „Kosten“ aus verbleibenden Risiken) am tiefsten sind. Das entsprechende Vorgehen wird ausführlich in einer Umsetzungshilfe zum Leitfaden beschrieben, die das BABS 2018 publiziert hat.[10] Um die Umsetzung des SKI-Leitfadens zu fördern, hat das BABS zudem eine Informationsbroschüre veröffentlicht, die den Betreibern insbesondere den Nutzen des SKI-Leitfadens aufzeigt.[11] Erfolgreich umgesetzt wurde der SKI-Leitfaden u. a. in einem Pilotprojekt mit Swissgrid, der Betreiberin des Schweizer Strom-Übertragungsnetzes und den zuständigen Energiefachbehörden. Derzeit sind alle sechs Betreiber von Erdgashochdrucknetzen daran, den SKI-Leitfaden umzusetzen.

Für viel Diskussionsstoff sorgte der in der Umsetzung des SKI-Leitfadens verwendete risikobasierte Kosten-Nutzen-Ansatz beziehungsweise die Monetarisierung von Personenschäden. Positiv hervorgehoben wurden die Umsetzbarkeit des Ansatzes und seine Praxistauglichkeit über verschiedene Sektoren hinweg. Kritisch hinterfragt wurde der Ansatz aufgrund möglicher problematischer ethischer Fragestellungen sowie etwaiger Interessenskonflikte zwischen Unternehmen einerseits und Behörden beziehungsweise der Gesellschaft anderseits. Auch die Frage, ob absolute Schutzziele solchen relativen Schutzzielen nicht

[10] https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/leitfaden/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/141_1534504827295.download/20181217_Umsetzungshilfe_Leitfaden_SKI_de.pdf

[11] https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/leitfaden/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/15_1508244558576.download/20180910_RZ_Broschuere_SKI_de.pdf

vorzuziehen sind (u.a. wegen besserer Kommunizierbarkeit) wurde diskutiert.

5.3 Gesamtkonzept Notstrom Deutschland

Julia Mayer (BBK) präsentierte das für Deutschland entwickelte Gesamtkonzept für die Notfallplanung bei Stromausfall *Kritis Notstrom. Kritis Notstrom* ist weniger als Projekt denn als eine Kommunikationsplattform zu verstehen, die deutschlandweite Aktivitäten zusammenführt, die teilweise bereits seit Jahren im Bereich Notfallplanung bei Stromausfall liefen. Ziel der Plattform ist es, Informations- und Analyselücken in diesem Bereich zu schliessen. Der Fokus liegt dabei auf der Sicherstellung der übergeordneten Stromversorgung (und nicht auf der Identifizierung und Bekämpfung von Ursachen eines Stromausfalls). Über *Kritis Notstrom* werden Best Practice-Beispiele zur Verfügung gestellt, aber auch eine vertiefte inhaltliche Bearbeitung des Themas wird gefördert. Ein Beispiel dafür ist die Definition von Schwellenwerten und entsprechenden Formulierungen von Empfehlungen. Die Anfänge von *Kritis Notstrom* liegen im Bericht des Büros für Technikfolgen-Abschätzung des Deutschen Bundestages (2010), in dem die Folgen eines mehrwöchigen Stromausfalls dargestellt wurden. In der dazu veröffentlichten Stellungnahme der Bundesregierung, in welche die Analyse des BBK einfloss, wurde der Bedarf nach einem Gesamtkonzept definiert. Neun Themenfelder, die im Rahmen von *Kritis Notstrom* bearbeitet werden, wurden vorgestellt:

- Notstromkapazitäten: Übersicht über den Bestand und die Verfügbarkeit von Notstromaggregaten
- Best Practice zur Notstromversorgung in Bund, Ländern, Kommunen: Erfassung aller Aktivitäten im Bereich Notstrom zur Unterstützung der Länder
- Betriebliche Notstromversorgung: Publikation eines Leitfadens 2006 und in überarbeiteter Fassung 2014; gehört zu den meist nachgefragten BBK-Leitfäden.
- Treibstoffversorgung bei Stromausfall: Treibstoffversorgung als Knackpunkt bei Stromausfall. Neuster Leitfaden mit Empfehlungen wurde im Dezember 2017 vorgestellt.
- Schutzziele: Definition von Schutzzielen (z.B. Ersatzstromversorgung für 72 Stunden) und -niveaus Kritischer Infrastrukturen in Deutschland (siehe Forschungsprojekt DESKRIS der FU Berlin).
- Technische Lösungen: Scannen vorhandener und neuer technischer Lösungen
- Rechtslage Notstromversorgung: Redundanzen als wichtiges Thema
- Minimalversorgung: Erarbeitung eines Konzeptes zur Mindestversorgung (siehe dazu Forschungsprojekte KIRMin des BKK und der TH Köln[12] und Kat-Leuchttürme des Verbundes Kat-Leuchttürme: Katastrophenschutz-Leuchttürme als Anlaufstelle für die Bevölkerung in Krisensituationen[13])

Ein Thema, das in der Diskussion aufgegriffen wurde, ist die Priorisierung der Notstromabnehmer. In den Szenarien, die beispielsweise für die Treibstoffversorgung bei Stromausfall genutzt werden, wird die Bevölkerung als Abnehmer nicht priorisiert, eher die KI-Betreiber und Gefahrenabwehr. Da für die allgemeine nicht-polizeiliche Gefahrenabwehr die Länder zuständig sind, erfolgt die Priorisierung auf Landes- und regionaler Ebene. So würden die Länder gemäss Empfehlungen die Tanklager und die Kreise die wichtigen Tankstellen festlegen.

Übersicht Massnahmen

Art des Task / der Massnahme		Beschrieb	KTS
Informationsaustausch und Vernetzung	Verbesserung des Informationsaustauschs und der Zusammenarbeit in Bezug auf Cyber-Risiken	Intern in der Branche oder integration in MELANI	Medien, Abfälle, Kulturgüter, Versicherungen, Ärztliche Betreuung und Spitäler, Labors
Informationsaustausch und Vernetzung	Aufbau eines branchenweiten übergreifenden Krisenorgans		Banken
Ausbildung und Sensibilisierung	Sensibilisierung und Ausbildung der Mitarbeitenden		Forschung und Lehre, Labors, Abfälle, Kulturgüter, Versicherungen, Ärztliche Betreuung und Spitäler, Labors, PRJV
Ausbildung und Sensibilisierung	Durchführung von Übungen/Stresstests	Unternehmensintern, branchenweit, landesweit	Banken, Ärztliche Betreuung und Spitäler
Regulatorisch administrative	Ergänzung bestehender oder Erstellung neuer Richtlinien und Standards		Medien, Postverkehr, Versicherungen, Labors, Kulturgüter
Regulatorisch administrative	Erarbeitung einer Empfehlung zuhanden der Branche		Zivilschutz
Technische Massnahmen	Aufbau oder Ausbau der krisensicheren Kommunikation	Anbindung SDVN, POLYCOM oder eigene Mittel wie sat. Telefon usw.	Forschung und Lehre, Banken, Ärztliche Betreuung und Spitäler, PRJV (inkl. DVSiO)
Technische Massnahmen	Aufbau und/oder Ausbau krisensichere Alarmierungs- bzw. Aufgebotssysteme		Zivilschutz, Blaulichtorganisationen
Technische Massnahmen	Prüfung Aufbau und/oder Ausbau von Redundanzen bereits bestehender Standorte oder Systeme		Medien, Ärztliche Betreuung und Spitäler, Kulturgüter, PRJV (vorwiegend DVSiO)

Abbildung 2: Massnahmen der neuen Cyber-Strategie der Schweiz

[12] https://www.din.de/de/forschung-und-innovation/partner-in-forschungsprojekten/sicherheitsforschungsprojekte/kirmin-219678

[13] https://www.sifo.de/de/kat-leuchttuerme-katastrophenschutz-leuchttuerme-als-anlaufstelle-fuer-die-bevoelkerung-in-1965.html

6 SKI/KRITIS und Cyber

6.1 Schweizerische Nationale Cybersicherheitsstrategie

Im ersten Beitrag des Themenblocks stellte Giorgio Ravioli (BABS) die aktuellen Entwicklungen im Bereich Cybersicherheit in der Schweiz vor. Seit 2012 verfügt die Schweiz mit der *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiko (NCS)* über einen zentralen Referenzrahmen in diesem Bereich. Die Strategie verfolgt einen ganzheitlichen, risikobasierten Ansatz, um kritische Infrastrukturen vor Cyber-Ausfällen und -Angriffen zu schützen, wie auch deren Informationen zu sichern. Mit der Strategie werden drei Ziele verfolgt: Die Verbesserung der frühzeitigen Erkennung, die Stärkung der Cyber-Resilienz von kritischen Infrastrukturen (Hauptfokus der Strategie) sowie die generelle Minimierung von Cyberrisiken.

Parallel zur Strategie zum Schutz Kritischer Infrastrukturen wurde die Cyber-Strategie nun überarbeitet und im April 2018 durch den Bundesrat verabschiedet.[14] Die neue Strategie umfasst zahlreiche Massnahmen, die zum Grossteil direkt auf der Vorgängerstrategie aufbauen und diese in einigen Bereichen ergänzt. Ausgebaut werden soll künftig insbesondere die strategische Führung. Hierzu sollen einige Tätigkeiten zentralisiert werden. Zudem ist vorgesehen, dass die bestehenden Public-Private-Partnerships und Experten-Netzwerke gestärkt werden. Schliesslich wird die neue Strategie sowohl kleinere und mittlere Unternehmen (KMU) als auch die Kantone verstärkt einbeziehen. Zu berücksichtigen ist dabei auch, dass sich die Fähigkeiten und Kenntnisse von Branche zu Branche zum Teil erheblich unterscheiden. Während beispielsweise im Bankensektor das Thema Cybersicherheit bereits seit geraumer Zeit eine hohe Aufmerksamkeit geniesst, haben andere SKI-relevante Bereiche wie zum Beispiel die Abfallbranche in der Vergangenheit sich nicht im gleichen Masse mit Cybersicherheitsthemen beschäftigt.

Seitens der Unternehmen wurde die neue Strategie insgesamt positiv aufgenommen. Zahlreiche Unternehmen haben die Bedeutung des Themas erkannt und sehen den Mehrwert von eindeutigen regulatorischen Vorgaben, beispielsweise im Bereich der Meldepflichten für Cyber-Vorfälle, die sich gegenwärtig in der Prüfung befinden. Mit deren Hilfe soll nicht nur der Informationsaustausch zwischen Unternehmen und Behörden verbessert werden, sondern auch der Informationsfluss zwischen den unterschiedlichen Branchen. Das Interesse zahlreicher Unternehmen an einer engeren Zusammenarbeit mit den Behörden spiegelt sich auch darin wider, dass eine wachsende Zahl an KI-Betreibern an das sichere Datenverbundnetz sowie an das Sicherheitsfunknetz Polycom angeschlossen werden möchten. Inwiefern dies möglich ist, wird gegenwärtig abgeklärt, um im November 2018 dem Bundesrat eine Botschaft vorlegen zu können.

Wie in der Diskussion deutlich wurde, stellen die Verbindungen zwischen dem Thema Cybersicherheit und Schutz Kritischer Infrastrukturen – wie auch in Deutschland und Österreich – die Verantwortlichen vor zahlreiche Herausforderungen. Wie mehrere Teilnehmer anmerkten, droht durch die aktuell sehr grosse Aufmerksamkeit für das Thema Cyber, dass übrige Risiken im Bereich der kritischen Infrastrukturen eher nachrangig behandelt werden. Um dem entgegenzuwirken, sollen sowohl KI-Betreiber als auch die politischen Akteure verstärkt sensibilisiert werden, dass IT ein zunehmend wichtiges Element von SKI/KRITIS ist, die übrigen Risiken aber nicht vernachlässigt werden dürfen.

6.2 Auswirkung der NIS-Richtlinie auf nationale SKI-Programme

Über die Auswirkungen der 2016 verabschiedeten europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)[15] referierten Monika John-Koch (BBK) und Sylvia Mayer (BVT).

Deutschland hat die Umsetzung der Richtlinie und die Identifizierung der relevanten Unternehmen mittels Gesetz und zweier nach Sektoren getrennten Rechtsverordnungen abgeschlossen. Bei der Erstellung der Rechtsverordnungen waren neben den relevanten Bundesbehörden insbesondere Betreiber Kritischer Infrastrukturen der adressierten Sektoren beteiligt, in erster Linie Mitglieder aus dem UP KRITIS (Kapitel 7.3). Der Prozess zur Identifikation der unter das Gesetz fallenden Betreiber kritischer Infrastrukturen sieht vor, dass sich die Unternehmen anhand von definierten Anlagen und Schwellenwerten selbst identifizieren und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Nach Angaben des BSI in ihrem Bericht *Die Lage der IT-Sicherheit in Deutschland 2017* haben im Zuge der ersten Rechtsverordnung 205 Betriebe ca. 550 Anlagen registrieren lassen, für die zweite Rechtsverordnung wird mit 800 bis 1.000 weiteren Anlagen gerechnet. Unternehmen, die die in der Verordnung aufgeführten kritischen Anlagen oberhalb der Schwellenwerte betreiben innerhalb einer festgelegten Zeit jedoch keine Kontaktstelle benennen und sich damit nicht als Betreiber einer kritischen Infrastruktur identifiziert haben, begehen eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet wird. Fest steht zugleich, dass seitens der Behörden keine Erstellung umfassender Listen mit allen Unternehmen angestrebt wird, zum einen wegen Datenschutzbedenken und aus Sicherheitsgründen, zum anderen, weil dies nicht als notwendig erachtet wird. Im nächsten Schritt werden nun, zwei Jahre nach der Verabschiedung der Richtlinie und des deutschen Umsetzungsgesetzes, Mindeststandards festgelegt. Entgegen erster Überlegungen müssen diese Standards nicht auf Ebene der Unternehmen festgelegt, sondern können auch branchenspezifisch definiert werden. Als positives Zwischenfazit lässt sich festhalten, dass in Deutschland mit der Umsetzung der NIS-Richtlinie der

[14] https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

[15] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

Vorsorge-Gedanke stärker im Bewusstsein der Unternehmen verankert werden konnte.

In Österreich befindet sich das nationale NIS-Gesetz kurz vor der Verabschiedung seitens der Politik. Nach dessen Beschluss werden als strategische NIS-Behörde das Bundeskanzleramt und als operative NIS-Behörden das Cyber Security Center des Bundesministeriums für Inneres sowie des Bundesministeriums für Landesverteidigung (BMLV) an der Spitze der Koordinierungsstruktur stehen. Sie sind unter anderem für die Erörterung des Lagebildes nach Sicherheitsvorfällen und den Austausch klassifizierter Informationen zuständig. Im Rahmen der Regelungen in Deutschland sollen alle KI-Objekte jenseits eines Regelschwellenwerts von 500'000 betroffenen Personen erfasst werden. In Österreich sollen bis November dieses Jahres alle Betreiber wesentlicher Dienste ermittelt worden sein. Berücksichtigt werden dabei auch digitale Dienste, wie beispielsweise Suchmaschinendienste. Hingegen wird der Bankensektor aufgrund separater Berichtspflichten im Rahmen bestehender EU-Richtlinien voraussichtlich ausgenommen. Die Bereitschaft der Unternehmen, den Behörden relevante Ereignisse zu melden, soll unter anderem durch die Einrichtung von Computer-Notfallteams erhöht werden, welche auf Ebene der Branchen Unterstützung anbieten können. Geplant sind beispielsweise Notfallteams für die Bereiche Energie und Gesundheit sowie ein allgemeines Computer-Notfallteam (CERT.at). Die Betreiber werden verpflichtet, alle Sicherheitsvorfälle unverzüglich an das für sie zuständige Computer-Notfallteam zu melden. Zudem wird eine enge Einbindung der Bundesländer angestrebt, sowohl bei der Identifikation der Objekte als auch im gesamtstaatlichen Krisenmanagement bei möglichen künftigen Cyberkrisen.

In der anschliessenden Diskussion erörterten die Teilnehmer unter anderem, wie sich die im Rahmen der NIS-Richtlinie erforderliche Zertifizierung der Unternehmen gestaltet. In der Praxis zeichnet sich gegenwärtig ein Mangel an geeigneten Audit-Dienstleistern ab, die für eine fachgerechte und zügige Zertifizierung der Unternehmen notwendig wären. Es wird sich zeigen, ob diese Lücke von Seiten der Dienstleistungsbranche bald geschlossen werden kann. Ein weiterer Diskussionspunkt war, wie die Fehlwahrnehmung einiger Unternehmen korrigiert werden kann, die glauben mit der Erfüllung der NIS-Richtlinie bzw. von IT-Sicherheitsgesetzen bereits „ihr Soll“ getan zu haben, und darüber hinaus ihre Verantwortung im Bereich SKI/KRITIS sekundär behandeln.

Abbildung 3: Die Teilnehmer des D-A-CH Workshops SKI beim Besuch des Gemeinsamen Melde- und Lagezentrums (GMLZ) am Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn

6.3 Cybersicherheit und Bevölkerungsschutz in Deutschland

Wie Anja von Wulffen (BBK) ausführte, gewinnt mit dem steigenden Durchdringungsgrad von Informations- und Kommunikationstechnologien und der fortschreitenden Digitalisierung das Thema Cybersicherheit zunehmend an Bedeutung. Zugleich verfolgt das BBK generell einen All-Gefahren-Ansatz, das heisst, dass Cyberrisiken eine Gefahr unter vielen darstellen. Entsprechend ist die Behörde darum bemüht, Cyberaspekte in den Schutz Kritischer Infrastrukturen und den Bevölkerungsschutz im Allgemeinen zu integrieren. Dabei ist die bereits bei den vorigen Diskussionen angesprochene Herausforderung, dass die grosse Aufmerksamkeit für das Cyberthema droht,

die anderen Aspekte zu überlagern: Die *Cyber-Sicherheitsstrategie für Deutschland 2016*[16] auf der einen Seite befasst sich im Gegensatz zur *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiko* schwerpunktmäßig mit dem Thema Cybersicherheit und nicht mit dem Schutz Kritischer Infrastrukturen oder dem Bevölkerungsschutz. Auf der anderen Seite sind die UP KRITIS-Branchenkreise bislang sehr auf die Umsetzung des IT-Sicherheitsgesetzes fokussiert. Positiv hat sich jedoch der Befall von Krankenhäusern mit Ransomware 2016 auf die Sensibilität für die Notwendigkeit einer ganzheitlichen Betrachtungsweise von Cybersicherheit und Bevölkerungsschutz ausgewirkt.

Um Themen der IT-Sicherheit und der physischen Sicherheit stärker zu verbinden, verfolgt das BBK unterschiedliche Aktivitäten. Zunächst betätigt sich das Bundesamt als verknüpfende Instanz in verschiedenen Kooperationsnetzwerken, z.B. im UP KRITIS mit KI-Betreibern, im Nationalen Cyber-Abwehrzentrum mit anderen relevanten Bundesbehörden und in der AG KOST KRITIS mit den Bundesländern.

Um die Resilienz kritischer Dienstleistungen gegenüber Cybervorfällen zu stärken, setzt das BBK vor allem auf branchenspezifische Sicherheitsstandards (B3S), mit deren Hilfe Unternehmen ihre gesetzliche Verpflichtung zur Umsetzung angemessener IT-Sicherheitsvorkehrungen nach dem Stand der Technik umsetzen, die aber auch kleineren Unternehmen unterhalb der Schwelle zur gesetzlichen Verpflichtung als Richtschnur dienen können. Zudem ist das BBK an der Weiterentwicklung im Bereich Zivile Verteidigung beteiligt, wo Cyberangriffe zunehmend an Relevanz gewinnen. Darüber hinaus steht das Bundesamt mit mehreren vom BMBF geförderten Forschungsprojekten in Kontakt, die sich an der Schnittstelle von Cybersicherheit und Schutz Kritischer Infrastrukturen befinden. Hierzu zählen unter anderem Forschungsvorhaben zur IT-Sicherheit von Verkehrsleitstellen sowie zu sogenannten Schwachstellensuchmaschinen für industrielle Kontrollsysteme (u.a. Cyber-Safe, RiskViz, VeSiKi[17]). Nicht zuletzt sollen die an der Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) angebotenen Schulungen vermehrt dazu dienen, Verantwortliche im Bereich Bevölkerungsschutz/ Katastrophenschutz in ihrer Arbeit in Bezug auf Cyberrisiken zu sensibilisieren. Damit in Verbindung steht das Ziel, in allen relevanten fachlichen Arbeitsbereichen des BBK die Implikationen und Gefahren verbreiteter IT-Anwendung angemessen zu berücksichtigen. Beispielsweise wird der wachsenden Bedeutung der Cybersicherheit auch im Rahmen der Länderübergreifenden Krisenmanagementübung (LÜKEX) 2020 Rechnung getragen, in der IT-Themen eine zentrale Rolle spielen werden.

[16] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

7 Kommunikation

7.1 Einbindung der KI-Betreiber in den Behördenfunk in Österreich

Der BOS-Digitalfunk in Österreich stellt die Kommunikation zwischen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sicher und wird vom Innenministerium betrieben. Wie KI-Betreiber in den Behördenfunk eingebunden werden, wurde von Sylvia Mayer (BVT) vorgestellt. Der BOS-Digitalfunk entspricht hinsichtlich der Verschlüsselung dem NATO-Standard und erlaubt die Übertragung sensibler Daten sowie eine ausfall- und abhörsichere Kommunikation – auch bei Strom- oder IKT-Ausfall. Landesweit sind über 65‘000 Geräte bei Polizei, Rettung, Feuerwehr und sonstigen Hilfs- und Einsatzorganisationen im Einsatz. Für die KI-Betreiber wurden nach Sektoren Sprechgruppen eingerichtet, in denen gefunkt wird. Es sind Gruppenrufe möglich, bei denen alle Teilnehmer einer Sprechgruppe, d.h. innerhalb des jeweiligen Sektors, mithören, aber auch Einzelrufe. Der BOS-Digitalfunk kann auch für Telefonate oder zum Verschicken von Nachrichten genutzt werden. Die Erreichbarkeit der Unternehmen im Gruppenruf ist auf den jeweiligen Sektor beschränkt. Per Einzelruf kann darüber hinaus auch mit Unternehmen anderer Sektoren kommuniziert werden (z.B. Informationen bezüglich Energieversorgung für Krankenhäuser).

KI-Betreiber, welche BOS-Digitalfunkgeräte erhalten haben, gehören der Kategorie A (höchste Relevanzstufe) an. Es handelt sich österreichweit um zirka 120 Unternehmen und Organisationen. Pro Betreiber wird ein Funkgerät übergeben. Zuvor wird eine Kooperationsvereinbarung geschlossen und die als verantwortlich bezeichnete Person, wird einer Sicherheitsüberprüfung unterzogen. Die Bereithaltung auf Seiten der Betreiber wird durch 24/7-besetzte Bereiche (Leitstelle, Portier etc.) sichergestellt. Die Erreichbarkeit der Betreiber wird durch das zuständige Referat im Rahmen von sektorspezifischen Kommunikations-Checks überprüft. Die Aktivierung des Funkgerätes soll nur im wirklichen Bedarfsfall erfolgen, z.B. während eines IKT-Ausfalls oder für die Übertragung sensibler Daten. Bundesländer-Veranstaltungen zur Übergabe von BOS-Digitalfunkgeräten an KI-Betreiber begannen im Herbst 2017 (NÖ: 12.10.2017, Steiermark und Burgenland: 11.12.2017, Wien: 13.03.2018, Tirol und Salzburg: 27.06.2018). Zum Zeitpunkt des D-A-CH-Workshops Anfang Juni waren 80 Funkgeräte übergeben.

Fragen in der Diskussion betrafen die technische, aber vor allem auch die politische und praktische Umsetzung des Projektes. Die technischen Voraussetzungen waren bereits zu Beginn gegeben: Das Netz wird vom BM.I betrieben und von den Ländern mitfinanziert. Da es nicht weiterausgebaut werden musste und die Anzahl Betreiber (im Vergleich mit Deutschland) überschaubarer ist, hielten sich die Mehrkosten und der Aufwand in Grenzen. Anfragen von Betreibern aus anderen Kategorien wurden abgelehnt. Bis auf ein Unternehmen, das keinen Bedarf für ein Funkgerät sah, werten die Unternehmen die Einbindung in den Behördenfunk positiv.

7.2 Stand der Arbeiten Polycom, SDVN, Lageverbund und Alertswiss in der Schweiz

Stefan Brem (BABS) informierte über bestehende und geplante Alarmierungs- und Telekommunikationssysteme im Schweizer Bevölkerungsschutz:

Polycom: Das flächendeckende Sicherheitsfunknetz der Führungs- und Einsatzorganisationen im Schweizer Bevölkerungsschutz ermöglicht den Funkkontakt innerhalb wie zwischen den verschiedenen Organisationen der Gefahrenabwehr (zirka 55‘000 Nutzer). In Kooperation mit den Kantonen und anderen Bundesstellen stellt das BABS mit dem Vorhaben *Polycom 2030* den Werterhalt und somit die Verfügbarkeit von *Polycom* bis mindestens 2030 sicher. Die Migration der Teilnetze stellt dabei eine Herausforderung dar; wie auch bei anderen Projekten erschweren der schnelle technologische Wandel sowie die föderale politische Struktur (unterschiedliche Finanzierungs- und Modernisierungszyklen) die Umsetzung des Projektes.

Datenverbundsystem und Lageverbund: Der Bundesrat möchte ein nationales Sicheres Datenverbundsystem aufbauen, welches aus dem kabelgebundenen *Sicheren Datenverbundnetz* (SDVN), einem Datenzugangssystem und einem Datenkommunikationssystem besteht. Hierdurch soll das veraltete Meldevermittlungssystem VULPUS abgelöst werden. Weitere Vorhaben (Bundesratsbeschluss Dezember 2017) betreffen die konzeptionellen und technischen Abklärungen für ein nationales Lageverbundsystem, das Informationen aus bestehenden Führungssystemen der Kantone, KI-Betreiber und weiteren Stellen zusammenführt, sowie Abklärungen für eine *Drahtlose Breitbandkommunikation* (dBBK) im Rahmen eines Pilotprojekts. Bei einer allfälligen Einführung wären in allen Lagen – anders als beim heutigen Funksystem – auch ein Austausch von Bilddaten sowie der Zugriff auf Datenbanken möglich.

Alertswiss: Mit *Alertswiss* soll das bestehende Alarmierungskonzept von Sirenen und Radio mittels neuer mobiler Informations- und Kommunikationstechnologie ergänzt werden. Hierfür wurden in einer ersten Phase Informationskanäle initiiert, die in erster Linie der Vorsorgekommunikation dienen. Neben der Webseite und der App bedient das Redaktionsteam unterschiedliche Social-Media-Kanäle, um die Bevölkerung mit niederschwelligen Informationen zu versorgen und so für Bevölkerungsschutz-Themen zu sensibilisieren. Seitens der Bürger wird das Angebot bereits umfassend angenommen. Insbesondere bei den jährlichen Sirenentests suchen viele Nutzer nach Informationen bei *Alertswiss*. Für den Oktober dieses Jahres ist geplant, dass *Alertswiss* mit dynamischen und ereignisbezogenen Funktionen ergänzt werden soll. Damit kann über *Alertswiss* informiert, gewarnt und alarmiert werden. Diese Ausweitung zum *Alertswiss 2.0* genannten Serviceangebot soll im Rahmen

des Sirenentests 2019 umfangreich und öffentlichkeitswirksam beworben werden.

KI-Betreiber nutzen heute bereits die Kommunikationssysteme des Bevölkerungsschutzes und haben die Möglichkeit sich an zukünftigen Vorhaben zu beteiligen (SDVN, Lageverbund etc.). Der angestrebte Ansatz in der Zusammenarbeit zwischen Bund und KI-Betreibern besteht darin, dass der Bund für den Betrieb der zentralen Komponente der Systeme zuständig ist und die KI-Betreiber für ihre dezentralen Komponenten (einschliesslich deren Finanzierung).

7.3 Arbeiten des Umsetzungsplans KRITIS zur Krisenkommunikation in Deutschland

Monika John-Koch (BBK) präsentierte den in der Kooperation UP KRITIS besprochenen Ansatz zur Entwicklung eines technischen (Krisen-) Kommunikationssystems für den SKI-Bereich in Deutschland. Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen Behörden; die Zusammenarbeit erfolgt sowohl sektorspezifisch in Branchenarbeitskreisen als auch sektorübergreifend in Themenarbeitskreisen[18]. Kommunikation ist seit langem ein wichtiges Thema im UP KRITIS, so dass hierfür ein eigener Themenarbeitskreis gegründet wurde. Die KI-Betreiber haben einen Katalog mit Anforderungen erstellt, welche ein Kommunikationssystem erfüllen soll. Das zukünftige System soll nicht nur zu Kommunikationszwecken genutzt werden können, sondern auch für den Austausch sensibler Daten. In einem anschliessend durchgeführten Markterkundungsverfahren wurde eruiert, welche Systeme es auf dem Markt gibt, die die Anforderungen möglichst gut erfüllen. Das *Modulare Warnsystem* (*MoWaS)*, ein vom BBK insbesondere zur Warnung der Bevölkerung im Zivilschutzfall entwickeltes satellitengestütztes Kommunikationssystem der Lagezentren und Leitstellen von Bund und Ländern, wurde ebenfalls in die Prüfung einbezogen. Zurzeit werden die Ergebnisse ausgewertet und das weitere Vorgehen gemeinsam mit dem BMI besprochen.

7.4 Gesamtkonzept Kommunikation in Deutschland

Für eine effiziente Krisenbewältigung müssen verschiedene Behörden und Betreiber Kritischer Infrastrukturen zusammenarbeiten. Sind öffentliche Kommunikationsnetze gestört, ist dies kaum noch effizient möglich. Der Untersuchungsgegenstand eines geplanten BBK-Projektes, das von Stefan Mikus (BBK) vorgestellt wurde, sind die Entwicklung von Anforderungen an ein krisenfestes, redundantes Kommunikationssystem. Konkret soll im Rahmen des Projektes ein Musterkonzept erarbeiten werden, das technische und inhaltliche Anforderungen an redundante Kommunikationslösungen/ Notfall-Kommunikationssysteme im Bevölkerungsschutz definiert. Da es über alternative Kommunikationslösungen nur verstreute Erkenntnisse gibt, geht es in einem ersten Schritt darum, den Sachstand zu erheben. Dies umfasst eine Analyse der Stakeholder, des Rechtsrahmens, der bestehenden Kommunikationsmittel, Best Practices, Ausfallszenarien und des Forschungsstandes. Basierend auf dem Sachstand wird die Bedarfsanalyse durchgeführt. Bestimmt werden einerseits der Bedarf und die Anforderungen und anderseits die Leistungsfähigkeit eines Meldesystems.

8 Ausblick

In der Abschlussrunde betonten Vertreter aller Länderdelegationen, wie erneut gewinnbringend der Workshop für alle Seiten war. Wie mehrere Teilnehmer darstellten, bietet das etablierte D-A-CH-Format eine wertvolle Möglichkeit zu einem vertrauensvollen Fachaustausch. Auch wenn sich die rechtlichen und politischen Rahmenbedingungen in manchen Punkten unterscheiden, verbinden Deutschland, Österreich und die Schweiz viele sehr ähnliche Herausforderungen, die in Zeiten der Globalisierung immer weniger an Landesgrenzen haltmachen. Aus diesem Grund soll das Format auch in Zukunft weitergeführt werden.

Der nächste D-A-CH-Workshop SKI/KRITIS soll voraussichtlich im Jahr 2020 stattfinden. Österreich hat angeboten, die Veranstaltung turnusgemäss zu organisieren.

[18] Nähere Informationen unter www.kritis.bund.de

9 Teilnehmerliste

Name	Institution	Land
Brem, Stefan	Bundesamt für Bevölkerungsschutz	CH
Franz, Johannes	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
John-Koch Monika	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Krings, Susanne	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Kugler, Michael	Bundeskanzleramt	A
Lauwe, Peter	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Maduz, Linda	ETH Zürich	CH
Mayer, Julia	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Mayer, Sylvia	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung	A
Mikus, Stefan	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Palla, Isabella	Bundesministerium für Inneres	A
Ravioli, Giorgio	Bundesamt für Bevölkerungsschutz	CH
Roth, Florian	ETH Zürich	CH
Stock, Eva Maria	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Stolzenburg, Kathrin	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
von Wulffen, Anja	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D
Wenger, Nick	Bundesamt für Bevölkerungsschutz	CH
Wienand, Ina	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	D

CSS
ETH Zurich

Das Center for Security Studies (CSS) der ETH Zürich ist ein Kompetenzzentrum für schweizerische und internationle Sicherheitspolitik. Es bietet sicherheitspolitische Expertise in Forschung, Lehre und Beratung. Das CSS fördert das Verständnis für sicherheitspolitische Herausforderungen. Es arbeitet unabhängig, praxisrelevant und wissenschaftlich fundiert.