CSS TAGUNGSBERICHT

Dritter D-A-CH Workshop Schutz Kritischer Infrastrukturen

4.–6. Dezember 2013, Magglingen

Organisiert durch:
Bundesamt für Bevölkerungsschutz (BABS), Schweiz

Gemeinsam durchgeführt mit:
Bundeskanzleramt, Österreich
Bundesministerium für Inneres (BM.I) Österreich
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Deutschland
Center for Security Studies (CSS), ETH Zürich

BUNDESKANZLERAMT ÖSTERREICH

BM.I BUNDESMINISTERIUM FÜR INNERES

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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: Michel Herzog, 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: Dr. 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

In dieser Studie werden die Vorträge der Teilnehmer aus Deutschland, Österreich und der Schweiz und die Diskussionen zum Thema dargestellt.

Bitte zitieren als: Herzog, Michel; Roth, Florian (2014): Dritter Trilateraler Workshop D-A-CH – Schutz Kritischer Infrastrukturen, CSS Tagungsbericht, Januar 2014, Center for Security Studies (CSS), ETH Zürich.

Inhaltsverzeichnis

Einführung

Vom 4. bis zum 6. Dezember 2013 trafen sich Vertreterinnen und Vertreter aus dem Bereich Sicherheitspolitik und Bevölkerungsschutz zum dritten D-A-CH Workshop Schutz Kritischer Infrastrukturen (SKI/KRITIS). Gemeinsam mit der D-A-CH Workshop-Reihe *Risiko-Analyse* stellt das Veranstaltungsformat ein wertvolles und bewährtes Forum dar, sich grenzübergreifend über Entwicklungen der staatlichen Risikoanalyse, Zusammenarbeit mit der Wirtschaft sowie das immer wichtiger werdende Thema Cyber-Sicherheit auszutauschen. Der diesjährige Workshop wurde durch das schweizerische Bundesamt für Bevölkerungsschutz (BABS) im Swiss Olympic House in Magglingen organisiert und gemeinsam mit dem österreichischen Bundeskanzleramt, dem österreichischen Bundesministerium für Inneres (BM.I), dem deutschen Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Center for Security Studies (CSS) der ETH Zürich durchgeführt. Am Workshop nahmen 16 Vertreterinnen und Vertreter von Bundesbehörden und aus der Wissenschaft teil. Ziel des dritten trilateralen SKI-Workshops war es, den Austausch zu aktuellen Ansätzen und Herausforderungen beim Schutz Kritischer Infrastrukturen zu fördern und von den unterschiedlichen Erfahrungen zu profitieren.

Der vorliegende Bericht gliedert die Vorträge und Diskussionen des dreitägigen Austauschs in fünf Themenbereiche: Im ersten Teil wird der gegenwärtige Stand der nationalen Programme zum Schutz Kritischer Infrastrukturen in den drei beteiligten Ländern präsentiert. Zudem wird auf aktuelle Entwicklungen auf europäischer Ebene eingegangen. Der zweite Themenbereich widmet sich der Frage, wie kritische Infrastrukturen sowie Interdependenzen zwischen einzelnen Infrastrukturen identifiziert werden können. Zudem wird diskutiert, wie sich die Resilienz kritischer Infrastrukturen messen lässt. Im dritten Teil wird erörtert, inwiefern Leitfäden die Betreiber kritischer Infrastrukturen in ihren Schutzmassnahmen unterstützen können. Der vierte Teil widmet sich schwerpunktmässig dem Thema Cyber-Risiken und deren Relevanz für den Schutz Kritischer Infrastrukturen. Im letzten Teil des Berichts wird betrachtet, wie Informationsplattformen die Kommunikation zwischen den für den Schutz Kritischer Infrastrukturen relevanten Akteuren verbessern können. Die thematische Gliederung weicht in einigen Teilen von der chronologischen Reihenfolge der Beiträge ab.

1. Programme zum Schutz Kritischer Infrastrukturen: Stand der Arbeiten 2013

Im ersten Programmteil informierten Peter Lauwe vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Helmut Schnitzer vom österreichischen Bundeskanzleramt sowie Stefan Brem vom Bundesamt für Bevölkerungsschutz über den Stand der Programme zum Schutz Kritischer Infrastrukturen sowie über die Schwerpunkte für die kommenden Monate und Jahre. Im Anschluss wurde die Thematik anhand ausgewählter Projekte zum Schutz Kritischer Infrastrukturen aus allen drei Ländern vertieft. So berichtete Stefan Brem vom Bundesamt für Bevölkerungsschutz über Fortschritte bei der Gefährdungs- und Risikoanalyse in der Schweiz. Beate Wegscheider vom Bundesministerium für Inneres erörterte, wie in Österreich Risikomatrizen als Grundlage eines Risikomanagements eingesetzt werden, und Peter Lauwe berichtete von der länderübergreifenden Übung LÜKEX 2013 in Deutschland. In den anschliessenden Diskussionen wurden gemeinsame Herausforderungen diskutiert und Erfahrungen ausgetauscht.

1.1 Deutschland

Präsentation: Peter Lauwe, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

1.1.1 Ausgangslage

Das Programm zum Schutz Kritischer Infrastrukturen ist seit mehreren Jahren fest etabliert. Bereits seit 2009 verfügt Deutschland mit der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS) über ein einheitliches strategisches Rahmenkonzept. Im Zentrum der deutschen Strategie steht, die Auswirkungen eines potentiellen Ausfalls Kritischer Infrastrukturen auf die Bevölkerung zu minimieren.[1] Ergänzt wird die Strategie durch verschiedene Schutzkonzepte, u.a. durch einen Leitfaden zum Risiko- und Krisenmanagement, der sich an die Betreiber Kritischer Infrastrukturen richtet und diese sowohl bei der Risikoanalyse als auch bei vorbeugenden Massnahmen und im Krisenmanagement unterstützt.[2] Zudem liegt seit 2012 ein Metakonzept zur Erstellung von Schutzkonzepten für Kritische Infrastrukturen im Bevölkerungsschutz vor.[3]

1 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html?nn=3314962

2 http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf;jsessionid=AC0A9AF4462D2058BB7D2F57DF962A1E.1_cid356?__blob=publicationFile

3 www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/publikationen_node.html;jsessionid=80B80D941E0BA907EC3A8F630830BAF1.1_cid355

1.1.2 Stand der Arbeiten 2013

Gegenwärtig befinden sich die in der KRITIS-Strategie festgehaltenen Massnahmen in der Umsetzung. Der Leitfaden zum Risiko- und Krisenmanagement hat insgesamt zu positiven Rückmeldungen geführt, wenn auch die Komplexität der Thematik die Anwendung seitens der Behörden schwierig gestaltet. In den letzten Jahren ist der Schwerpunkt auf das Thema Strom gelegt worden. Dazu ist eine Publikation geplant, in welcher die Aktivitäten in diesem Bereich (einschliesslich Prävention, Vorbereitung und Reaktion) dargelegt werden sollen. Zudem ist die Entwicklung eines Notfallplans vorgesehen, in dem Mindestforderungen für eine Notversorgung in einem grossflächigen, langandauernden Stromausfall aufgestellt und mit den beteiligten Akteuren abgestimmt werden. Aktuelle und zukünftige Entwicklungen im deutschen Stromversorgungssystem werden im BBK mitverfolgt, um neue Kritikalitäten und Verwundbarkeiten rechtzeitig erkennen und auf ihre Reduzierung hinwirken zu können. Hierzu gehören eine Vielzahl unterschiedlicher Massnahmen, u.a. die Erstellung einer Prioritätenliste. So führt z.B. der Bau von Gleichstromtrassen zur Verbesserung der Versorgung. Gleichzeitig können durch die zunehmende Zentralisierung der Leitungsstrukturen auch neue Kritikalitäten entstehen.

Ein Schwerpunkt der gegenwärtigen Arbeiten besteht darin, den Schutz Kritischer Infrastrukturen in den jeweiligen Fachgesetzen zu berücksichtigen. Allerdings zeigen sich hier auch die Grenzen des Kooperationsansatzes im Umgang mit den Betreibern kritischer Infrastrukturen, da viele Unternehmen hohe Kosten durch die Umsetzung der Vorgaben fürchten. Es ist deshalb wichtig, die Schutzziele genau zu bestimmen und so eine präzise Defizitanalyse zu ermöglichen. Handlungsbedarf besteht ebenfalls hinsichtlich der Koordination von Strategien zum Schutz Kritischer Infrastruktur mit Strategien bezüglich Cyber-Risiken. Zudem wird der Resilienzbegriff in absehbarer Zukunft an Bedeutung zunehmen, was wiederum Handlungsbedarf notwendig machen könnte.

In der Diskussion wurden insbesondere Herausforderungen bei der Zusammenarbeit der verschiedenen Fachbereiche vertieft. Wie die Workshop-Teilnehmer berichteten, stellt es sich nach wie vor als Herausforderung dar, die SKI-Perspektive in die Fachdebatten einzubringen (bspw. bei der Diskussion zu Stromtrassen, die gegenwärtig von Effizienzüberlegungen bestimmt wird). Zudem werden die unterschiedlichen Teile der Bundesverwaltung von den Fachstellen zum Teil als unzureichend abgestimmt wahrgenommen. Einen weiteren Punkt in der Diskussion stellte die Frage dar, welche Auswirkungen energiepolitische Überlegungen auf den Schutz Kritischer Infrastrukturen haben könnten, bspw. die Bestrebung im Rahmen der Energiewende, überschüssigen Strom aus dem Norden Deutschlands in den Süden zu leiten.

1.2 Österreich

Präsentation: Helmut Schnitzer, Bundeskanzleramt (BKA)

1.2.1 Ausgangslage

Im Jahr 2013 wurden die Österreichische Sicherheitsstrategie und die Cyber-Strategie vom Ministerrat beschlossen.[4] Mit den Dokumenten werden die Resilienz und der Schutz Kritischer Infrastruktur zu zwei Kernthemen der Innen- und Verteidigungspolitik aufgewertet. Ergänzt werden diese beiden Dokumente durch das Austrian Program for Critical Infrastructure Protection (APCIP). Insgesamt verfolgt das APCIP fünf Teilziele: 1. eine Liste strategischer Unternehmen, 2. eine Reihung der Prioritäten, 3. die Definition und 4. Implementierung von Sicherungs- und Schutzstandards einschliesslich eines Leitfadens sowie 5. die Erstellung einer Informationsplattform. Der Schutz Kritischer Infrastrukturen wird hierbei als direkter Beitrag zur Daseinsvorsorge und für den Wirtschaftsstandort verstanden, da in Österreich die Analyse der Auswirkungen (loss of service) im Vordergrund steht. Darüber hinaus gewann der Schutz Kritischer Infrastrukturen zunehmend auch an gesamtgesellschaftlicher Bedeutung im Rahmen der Wehrpflichtdebatte.

1.2.2 Stand der Arbeiten 2013

Die Arbeiten in Österreich zielen auf ein umfassendes Risikomanagement, das über ein reaktives Krisenmanagement hinausgeht. Dabei setzt das APCIP soweit wie möglich auf Kooperation und Selbstverantwortung bei der Zusammenarbeit mit den privaten Betreibern. Gesetze sollen nur subsidiär ausgearbeitet werden.

Bis zum jetzigen Zeitpunkt konnte eine Liste 400 strategisch wichtiger Unternehmen und Organisationen (KI-Betreiber) erstellt werden, womit die Identifikationsphase abgeschlossen ist. Die betrachteten Unternehmen wurden in drei Kategorien eingeteilt. Derzeit laufen die Arbeiten zur Festlegung der Sicherungs- und Schutzstandards (Aufbau Risikomanagement). Das primäre Instrument hierzu ist ein Leitfaden zur Selbstevaluierung für alle strategischen Unternehmen, der an internationale und nationale Standards anknüpft. Die Rückmeldungen dazu sind überwiegend positiv. Der nächste Schritt beinhaltet eine Informationsplattform aufbauend auf der EU-Plattform CIWIN (Critical Infrastructure Warning Information Network)[5]. Sie steht einem begrenzten Nutzerkreis offen, um dessen Informationsaustausch zu intensivieren. In der anschliessenden Diskussion wurde von den Vertretern aller Länder übereinstimmend festgestellt, dass die Begriffe «strategische Unternehmen/ strategische Infrastruktur» von den privaten Betreibern wesentlich besser aufgenommen werden als der Begriff «Kritische Infrastruktur», da Letzterer teilweise negativ konnotiert ist.

4 *http://www.bka.gv.at/site/3503/default.aspx; http://www.bka.gv.at/DocView.axd?CobId=50748*

5 *https://ciwin.europa.eu/Pages/Home.aspx*

1.3 Schweiz

Präsentation: Stefan Brem, Bundesamt für Bevölkerungsschutz (BABS)

1.3.1 Ausgangslage

Die strategische Grundlage für das Programm zum Schutz Kritischer Infrastrukturen in der Schweiz bildet die gleichnamige Nationale Strategie, die vom Bundesrat im Juni 2012 zusammen mit der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) verabschiedet wurde.[6] Zentrales Ziel der Schweizer SKI-Strategie ist die Stärkung der Widerstandsfähigkeit (Resilienz) der Schweiz im Hinblick auf Risiken im Bereich der Kritischen Infrastrukturen. Hierfür wird ein risikobasierter Kosten-Nutzen-Ansatz verfolgt. Ebenso wie in Deutschland und Österreich sind die Betreiber Kritischer Infrastrukturen die zentralen Partner bei der Umsetzung der Strategie, denn der Schutz Kritischer Infrastrukturen stellt eine gemeinsame Aufgabe von Staat und KI-Betreibern dar. In jüngster Zeit ist es gelungen, SKI-Aspekte verstärkt bei der Überarbeitung von Fachgesetzen (bspw. Nachrichtendienstgesetz, Energieversorgungsgesetz, Weiterentwicklung der Armee usw.) einzubringen. Zudem berücksichtigen auch zahlreiche kantonale Gefährdungsanalysen und darauf aufbauende Vorsorgemassnahmen betreffende SKI-Aspekte.

1.3.2 Stand der Arbeiten 2013

Im Rahmen des Programms zum Schutz Kritischer Infrastrukturen wurden zehn Sektoren mit insgesamt 28 Teilsektoren identifiziert, in denen Kritische Infrastruktur-Objekte vorhanden sind. Das Ausmass der Kritikalität der einzelnen Teilsektoren ergibt sich aus den Auswirkungen auf die Bevölkerung, den ökonomischen Auswirkungen innerhalb des Teilsektors und in anderen Teilsektoren sowie aus den Interdependenzen zwischen den Teilsektoren. Bei der Umsetzung der Strategie werden u.a. kritische Prozesse innerhalb der Sektoren identifiziert sowie Abhängigkeiten zwischen unterschiedlichen Infrastrukturen aufgezeigt. Basierend auf umfassenden Risiko- und Auswirkungsanalysen werden schliesslich vorsorgliche Planungen zur Bewältigung von Ausfällen Kritischer Infrastruktur erstellt.

Das gegenwärtige Schutzniveau im Bereich Kritischer Infrastrukturen kann insgesamt als vergleichsweise hoch bezeichnet werden, da auch die strategischen Prozesse seit 2005 laufend weiterentwickelt wurden. Gegenwärtig bildet die Umsetzung der in der SKI-Strategie festgelegten 15 Massnahmen einen Schwerpunkt der Aktivitäten (s. Abbildung 1). Zu diesen Massnahmen gehört die Erarbeitung eines Konzepts zur Verbesserung des Informationsaustauschs ebenso wie die Unterstützung der SKI-Programme für Betreiber und Kantone. Eine erste Überprüfung der Umsetzung ist im Jahre 2016 vorgesehen.

6 http://www.infraprotection.ch.

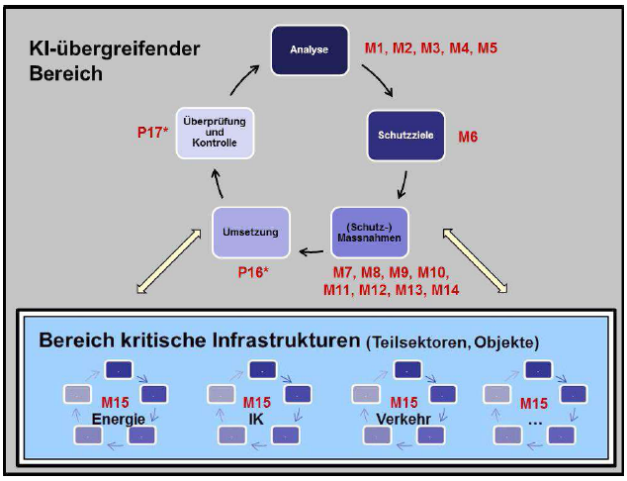

Abbildung 1: Prozessmodell Schutz Kritischer Infrastrukturen in der Schweiz

1.4 Ausgewählte Projekte zum Schutz Kritischer Infrastrukturen

1.4.1 Gefährdungs- und Risikoanalysen in der Schweiz

Präsentation: Stefan Brem, Bundesamt für Bevölkerungsschutz (BABS)

Aufgrund der föderalen Struktur liegt die Zuständigkeit für den Bevölkerungsschutz grundsätzlich bei den Kantonen. Die Kantone können auch selbständig entscheiden, ob und in welcher Form sie Risikoanalysen durchführen. Der Bund sorgt in Zusammenarbeit mit den Kantonen für die Forschung und Entwicklung im Bereich der Risikoanalyse. Insbesondere unterstützt das BABS die Kantone in der kantonalen Risikoanalyse durch die Bereitstellung des Leitfadens KATAPLAN, der einen integralen Risikomanagement-Ansatz verfolgt. Sowohl der Bund als auch die Mehrheit der Kantone führen Risikoanalysen im Bevölkerungsschutz durch. Das Bundesamt für Bevölkerungsschutz hat im Rahmen einer nationalen Gefährdungsanalyse einen umfassenden Gefährdungskatalog und ausführliche Gefährdungsdossiers (detaillierte Beschreibung und Dokumentation von Gefährdungen) erstellt, die sowohl für die nationale Gefährdungsanalyse als auch – in angepasster Form – als Grundlage für kantonale Gefährdungsanalysen dienen und bereits in verschiedene Arbeiten eingeflossen sind. Im Zentrum der Anstrengungen steht die Vorbereitung auf Katastrophen und Notlagen, welche die Schweiz als ‚Kollektiv' betreffen können. Ziel ist es, Gefährdungspotentiale von Katastrophen und Notlagen für die Schweiz vergleichbar zu machen und damit eine Grundlage für eine systematische, vorsorgliche Planung auf nationaler Stufe zu schaffen. Zudem bildet die nationale Gefährdungsanalyse eine wichtige Grundlage für die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen sowie für die Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken.

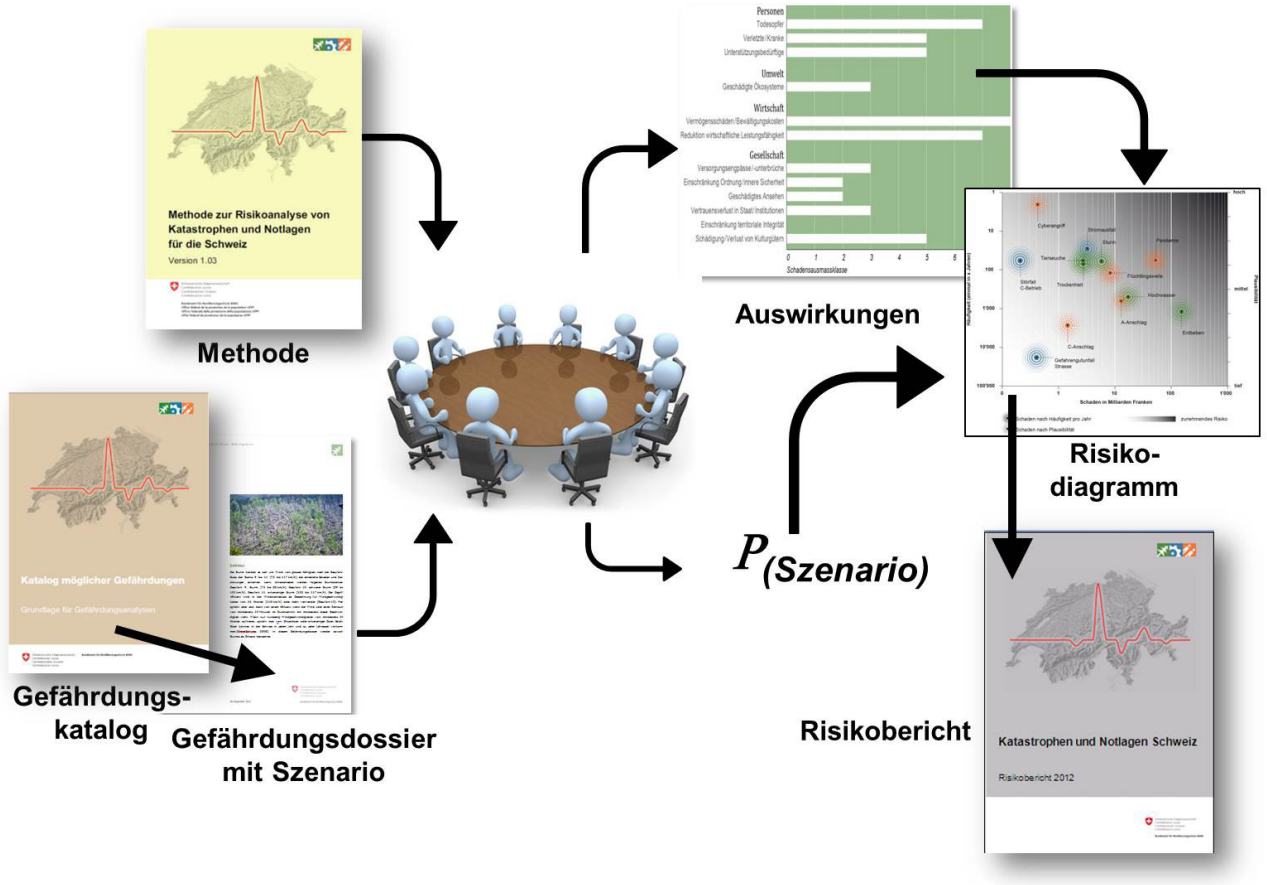

Abbildung 2: Methode der nationalen Gefährdungsanalyse Katastrophen und Notlagen Schweiz

Die Arbeiten an der nationalen Gefährdungsanalyse konnten in den letzten Jahren erfolgreich weitergeführt werden. Insbesondere konnte mit der Veröffentlichung des Risikoberichts 2012 ein bedeutender Fortschritt erreicht werden. Der Risikobericht basiert auf einer Reihe von Workshops, in denen die untersuchten Szenarien nach einer einheitlichen Methode analysiert wurden (s. Abbildung 2). Die Szenarien wurden mithilfe eines Grenzkosten-Ansatzes vergleichbar gemacht und in einem Risikodiagramm dargestellt.[7] An den Workshops nahmen je nach Gefährdung Expertinnen und Experten aus verschiedenen Bundes-, kantonalen und kommunalen Stellen, Wissenschaft, Verbänden sowie Betreiber von Kritischen Infrastrukturen teil.

Neben dem Risikobericht konnten in den letzten Jahren weitere Publikationen erstellt werden, welche die Grundlage für weiterführende Aktivitäten in der Gefährdungsanalyse und im Schutz Kritischer Infrastrukturen bilden. Insbesondere der Katalog möglicher Gefährdungen sowie die einzelnen Gefährdungsdossiers mit entsprechenden Szenario-Beschreibungen stellen eine wichtige Grundlage für den Bevölkerungsschutz auf Bundes- und Kantonsebene dar.[8] Für die nächsten Jahre besteht die Hauptaufgabe darin, das Projekt Gefährdungsanalyse in einen fortlaufenden Prozess zu überführen. Gegenwärtig ist ein Überprüfungszyklus von vier Jahren vorgesehen. Parallel dazu werden in den kommenden Jahren weitere Gefährdungsdossiers erarbeitet.

1.4.2 Risikomatrizen als Grundlage des Risikomanagements

Präsentation: Beate Wegscheider, Bundesministerium für Inneres BM.I

In Österreich werden Risikoanalysen im Bereich SKI zum einen im Rahmen der EU-Richtlinie EPCIP (Art. 7.) sowie unter dem Austrian Program for Critical Infrastrucure Protection (APCIP) durchgeführt. Ersterer analysiert aus Behördensicht Risiken, die strategisch wichtige Betriebe im Bereich der Energieversorgung betreffen. Das APCIP bezieht darüber hinaus die Unternehmenssicht mit ein. Die zentrale Herausforderung ist, die Unternehmenssicht (für welche kurzfristige Ausfälle kein grosses Problem darstellen) mit der gesellschaftlichen Perspektive (bei welcher auch kurze Unterbrüche gravierende Folgen haben können) in Einklang zu bringen. Die Risikomatrizen stellen dabei ein wichtiges Instrument dar, um die unterschiedliche Risikowahrnehmung

7 http://www.risk-ch.ch

8 http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/nat__gefaehrdungsanlayse/gefaehrdungsdossier.html

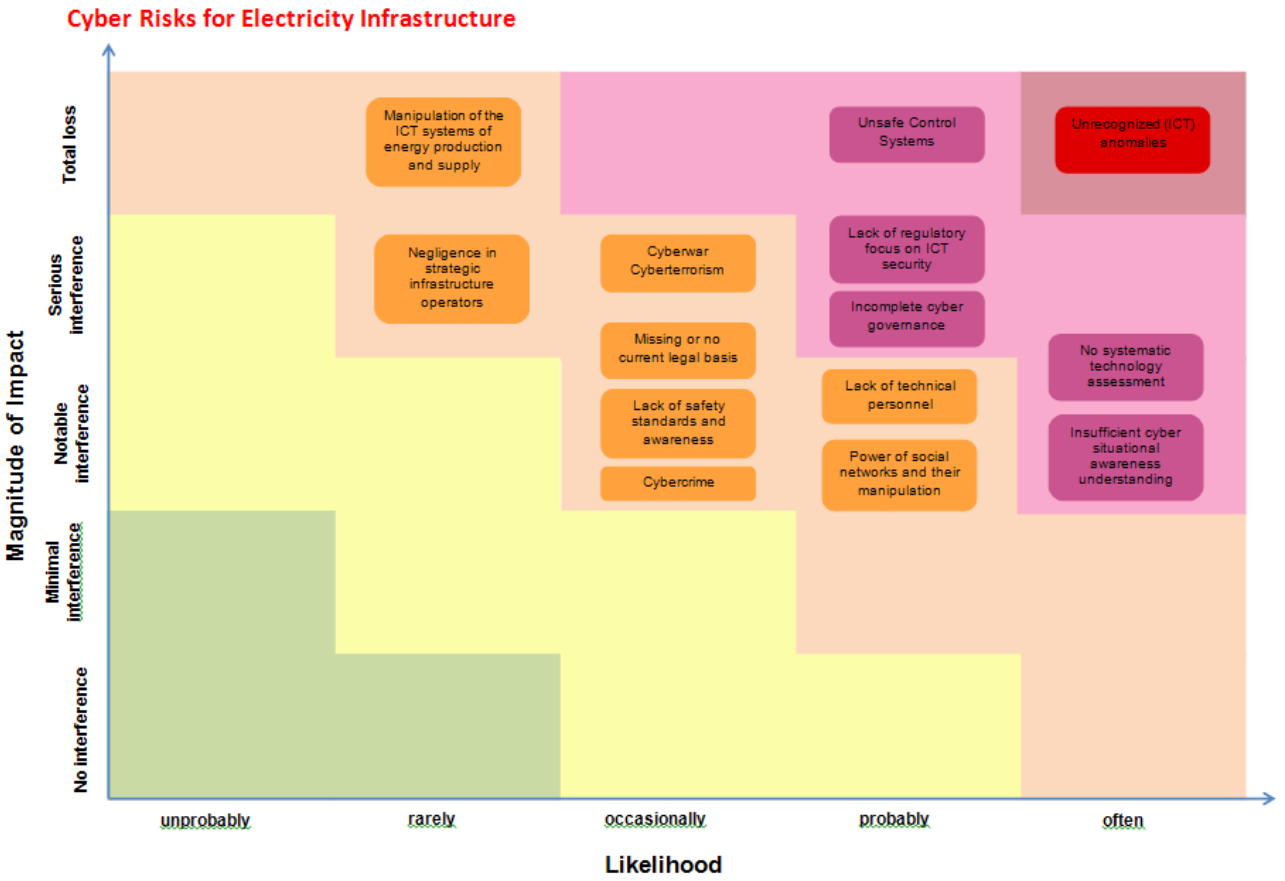

Abbildung 3: Risikomatrix für elektrische Infrastrukturen.

gegenüberzustellen sowie Massnahmen zu Risikoreduzierung zu erarbeiten. Die verwendeten Risikomatrizen bauen auf unterschiedlichen Studien zum Thema Stromversorgung auf (s. Abbildung 3). Wichtige Vorarbeiten wurden insbesondere mit der KIRAS-Studie 3S, der KSÖ Matrix «IKT» sowie dem EU-Projekt SESAME geleistet.[9] Mit den laufenden Arbeiten konnte das Bewusstsein der KI-Betreiber für diese Art Analysen gesteigert werden.

In einer nächsten Phase sollen durch eine verstärkte Integration bzw. verbesserte Koordination die bereits existierenden Risikoanalyseprozesse auf unterschiedlichen Ebenen (u.a. auf Gemeinde-, Länder- und Ministeriumsebene) in Einklang gebracht werden, da bis anhin eine gesamtstaatliche Analyse nur ansatzweise existiert. Bisher gibt es vor allem im Hochwassermanagement sowie bei der Bewertung von Cyber-Risiken ein hohes Mass an gesamtstaatlicher Analyse.

Gleichzeitig setzen unterschiedliche gesetzliche Bestimmungen einen rechtlichen Rahmen für die Risikoanalyse. So ist im österreichischen Aktiengesetz zwar ein Risikobericht vorgeschrieben, der Fokus liegt – im Gegensatz bspw. zur Gesetzgebung in Deutschland – jedoch auf dem Fortbestand des Unternehmens und nicht auf dessen gesellschaftlicher Verantwortung. Langfristig ist das Ziel, die Unternehmen weiter für die Thematik zu sensibilisieren und vom Nutzen freiwilliger Risikoanalysen zu überzeugen. Zugleich ist aber auch zu beachten, dass die Interessen der Unternehmen und der Gesellschaft bei grossen Risiken nicht immer konvergent sind, wenn ein umfassender Risikoschutz für die Unternehmen mit hohen Kosten verbunden ist.

1.4.3 Länderübergreifende Krisenmanagement-Übung LÜKEX 2013

Präsentation: Peter Lauwe, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Das Thema der Länderübergreifenden Krisenmanagement-Übung (LÜKEX 2013) vom 27. bis 28. November 2013 war eine aussergewöhnliche biologische Bedrohungslage. Als Übungsszenario wurde eine vorsätzliche Kontaminierung von Wurstwaren mit Toxinen sowie von Orchideen mit biologischen Erregern ausgewählt, wobei bewusst ein «überforderndes» Szenario generiert wurde. Eine besondere Herausforderung bestand darin, dass sich das Kontaminierungs-Szenario aus drei Strängen zusammensetzte, wobei es sich um zwei Kernszenarien sowie eine falsche Spur handelte.

9 https://www.sesame-project.eu; http://www.kiras.at/gefoerderte-projekte/detail/projekt/3s-vki-strategische-security-szenarien-fuer-die-vernetzung-kritischer-infrastruktur; http://www.kuratorium-sicheres-oesterreich.at/index.php?id=145&type=0&jumpurl=uploads%2Ftx_ksothema%2FKSO_Cyber_Risikomatrix.pdf&juHash=30b7a448ccc28250f893931f23dadc41323b2bf6d

Vorausgegangen war der Übung eine eineinhalbjährige Vorbereitungsphase.

An der Übung aktiv beteiligt waren die Bundesländer Nordrhein-Westfalen, Thüringen und Berlin, drei Bundesministerien (BMI, BMG, BMELV) sowie mehrere Bundesämter, u.a. das Robert-Koch-Institut, das Bundesamt für Risikobewertung sowie das BBK. Insgesamt waren ca. 2000 Personen an der Übung beteiligt. Im Zentrum der Übung standen die gemeinsame Lagebewältigung der beteiligten Akteure, die Organisation eines integrierten Ressourcenmanagement sowie die Implementierung eines einheitlichen Kommunikationsansatzes. Zudem wurden im Rahmen der Übung mehrere Hotlines simuliert sowie reale Pressekonferenzen abgehalten. Darüber hinaus fand jedoch nur eine beschränkte Öffentlichkeitsarbeit statt. Erstmals wurden in der Übung auch soziale Netzwerke simuliert. Es wurde erkannt, dass in Zukunft die Verwendung sozialer Medien verstärkt beachtet werden muss. Insgesamt verlief die Übung in weiten Teilen ruhig und gut organisiert. Eine fundierte wissenschaftliche Auswertung durch die Experten, die den gesamten Übungsverlauf beobachteten, wird noch folgen. Die nächste LÜKEX findet 2015 statt Das Übungsszenario wird eine Sturmflut sein.

Abbildung 4: Blick in das Lagezentrum während der LÜKEX 2013.

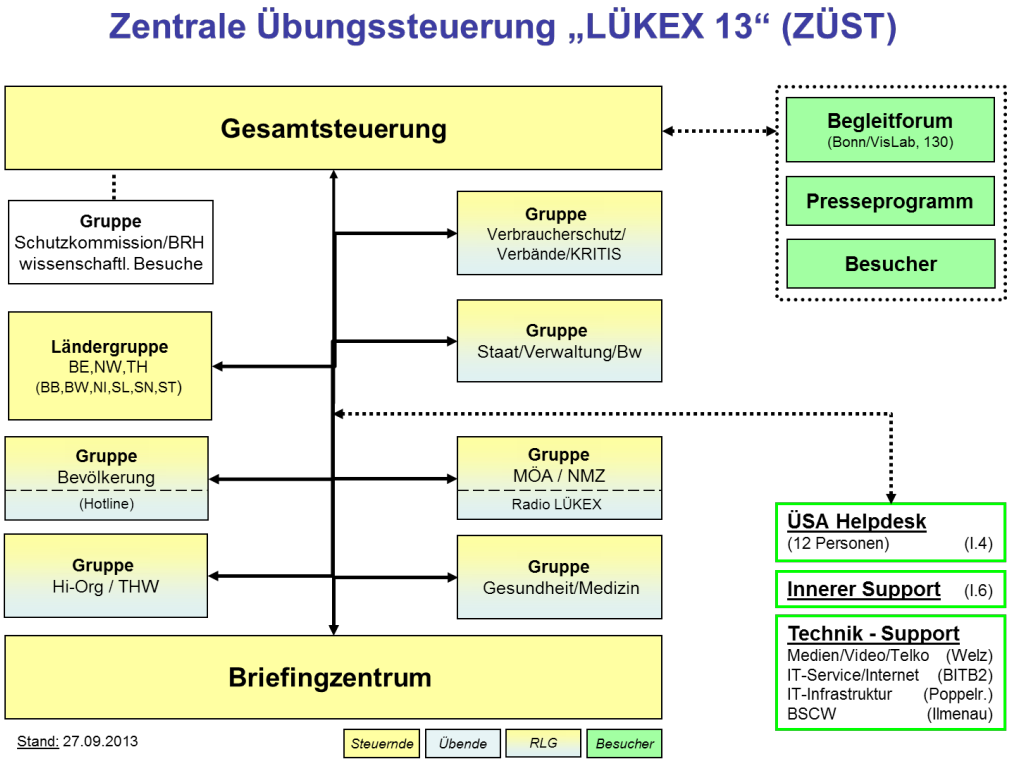

Abbildung 5: Organigramm LÜKEX 13

2. Identifizierung von Kritischen Infrastrukturen

Der zweite Teil des Workshops befasste sich mit der Identifizierung von Kritischen Infrastrukturen. Eine zentrale Rolle nimmt in diesem Zusammenhang die Erstellung von KI-Inventaren ein, wie sie bereits seit einigen Jahren in allen drei Ländern existiert – allerdings in sehr unterschiedlicher Ausprägung. In ihren Beiträgen präsentierten Peter Lauwe vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Alexander Pschikal vom österreichischen Bundeskanzleramt und Nick Wenger vom Bundesamt für Bevölkerungsschutz die Methoden, mit denen in Deutschland, Österreich und der Schweiz die KI-Inventare erstellt werden. Anschliessend wurde die Thematik durch zwei vertiefende Präsentationen ergänzt. Zuerst erörterte Peter Lauwe, wie sich Interdependenzen zwischen einzelnen Kritischen Infrastrukturen identifizieren lassen. Danach präsentierte Nick Wenger, wie in der Schweiz Schutz- und Leistungsziele ermittelt werden, um (Schutz-)Massnahmen zu priorisieren. Den Abschluss bildete der Vortrag von Florian Roth von der ETH Zürich zur Messung von Resilienz im Bereich Kritischer Infrastrukturen. Im Anschluss an die Präsentationen diskutierten die Teilnehmer, wie die bestehenden Methoden weiterentwickelt und verbessert werden können, um Kritikalitäten frühzeitig zu erkennen und Massnahmen einleiten zu können.

2.1 KRITIS-Inventar in Deutschland

Präsentation: Peter Lauwe, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Die Identifizierung der Kritischen Infrastrukturen stellt eine wichtige Vorstufe zum Risiko- und Krisenmanagement dar. Das Ziel ist dabei, einen Gesamtblick über alle Dienstleistungen, Produktionen und dazugehörige Einrichtungen zu erhalten, deren Ausfall zu dauerhaften Versorgungsengpässen für eine hohe Anzahl von Menschen führen könnte. Notwendig ist hierfür zunächst eine möglichst umfassende Erfassung aller relevanten Prozesse, Anlagen und Einrichtungen, was eine enge Zusammenarbeit zwischen Bundesbehörden, Bundesländern und Kommunen, KI-Betreibern sowie der Wissenschaft voraussetzt. Grundsätzlich sind bei der Identifikation Kritischer Infrastrukturen drei Kriterien ausschlaggebend: Erstens die qualitative Kritikalität (Welche Funktionen erfüllt ein Prozess oder eine Anlage?), zweitens die quantitative Kritikalität (Wie hoch ist der Versorgungsanteil?) und drittens die Zeit-Kritikalität (Für wie lange droht ein Ausfall?). Eine zentrale Aufgabe stellt in diesem Zusammenhang die Definition der entsprechenden Schwellenwerte dar.

In Deutschland wurde mit einem Grundlagenprojekt im Jahr 2009 der Ausgangspunkt für die Identifizierung Kritischer Infrastrukturen geschaffen. Im September 2013 wurde ein erster Länder-Workshop durchgeführt. 2014 wird die Arbeitsgruppe Länder-BBK einen praktikablen Umsetzungsvorschlag des Identifizierungsprozesses ausarbeiten. Die Testphase soll dann bis ca. 2015/2016 stattfinden.

Wie auch in Österreich und der Schweiz nimmt der Stromsektor in Deutschland eine zentrale Rolle bei der Erfassung Kritischer Infrastrukturen ein. In diesem spezifischen Umfeld wurde die nationale Kritikalitätsschwelle bei mindestens 500‘000 betroffenen Einwohnern (ab diesem Punkt werden die vorhandenen Ressourcen zur Bewältigung überfordert) und einer Zeitdauer von drei Tagen (in Anlehnung an die Vorsorgeleistung der anderen KI-Betreiber) angesetzt. Jedoch lässt sich diese Annahme nicht ohne weiteres auf andere Sektoren übertragen, da die Zeitkomponente stark vom jeweiligen Szenario abhängt. Es gestaltet sich daher schwierig, einen szenario-unabhängigen Identifikationsprozess von Kritischen Infrastrukturen zu entwickeln.

Die anschliessende Diskussion war von der Frage geprägt, wie bei der Identifizierung ein abgestuftes Verfahren etabliert werden kann, welches für alle administrativen Ebenen eingesetzt werden kann. Eine weitere Herausforderung, die in der Diskussion aufkam, ist die unvermeidliche Rest-Subjektivität bei der Bewertung von Kritischen Infrastrukturen. Es bedarf jedoch einer Gerichtsfestigkeit, wenn langfristige Anforderungen an KI-Betreiber gestellt werden sollen. Zum Beispiel könnte für das geplante IT-Sicherheitsgesetz das Inventar genutzt werden. Wichtig ist daher, dass die Kriterien und Prozesse der Auswahl nachvollziehbar sind.

2.2 Liste strategisch wichtiger Unternehmen und Organisationen in Österreich

Präsentation: Alexander Pschikal, Bundeskanzleramt BKA

In Österreich kommt der Identifikation Kritischer Infrastrukturen im Rahmen des bereits zuvor diskutierten APCIP eine wichtige Rolle zu. Die Liste speist sich aus einer Vielzahl öffentlicher und nicht-öffentlicher Quellen und wurde mit den Fachministerien sowie Interessenvertretungen akkordiert. Dabei werden die Unternehmen nach dem gängigen, internationalen NACE-System[10] in die jeweiligen Gruppen eingeteilt und nach ihrer Bedeutung für die Bundesebene gefiltert (Betriebe mit lediglich regionaler oder lokaler Bedeutung werden nicht erfasst und sind der Bearbeitung der Bundesländer und Gemeinden vorbehalten). Der Fokus liegt dabei auf den Auswirkungen eines Leistungsausfalls,die Daseinsvorsorge sowie den Wirtschaftsstandort Österreich, weshalb die Redundanz und die Marktanteile der jeweiligen Unternehmen im Vordergrund stehen. Die Liste umfasst

10 NACE: Nomenclature générale des Activités économiques dans les Communautés européennes.

gegenwärtig knapp 400 Unternehmen, ihre genaue Zusammensetzung steht unter Verschluss und wurde von Seiten der Wirtschaft weitgehend akzeptiert.

In der Diskussion wurde die Frage erörtert, ob das ganze Unternehmen auf seine Kritikalität hin bewertet wird. Der österreichische Ansatz besteht darin, Unternehmen und Organisationen zu identifizieren, diesen aber die Selektion zu überlassen, welche Prozesse, Anlagen oder Human Ressources schlussendlich die Kritikalität der Unternehmen im Sinne eines «all hazards approach» ausmachen (bspw. Raffinerien, aber nicht einzelne Tankstellen, das «Schlüsselpersonal»). Nur die Unternehmen selbst haben das Fachwissen dazu.

2.3 SKI-Inventar Schweiz

Präsentation: Nick Wenger, Bundesamt für Bevölkerungsschutz BABS

Das Ende 2012 erstellte nationale SKI-Inventar umfasst alle Objekte mit strategisch wichtiger Bedeutung für die Schweiz. Die zentralen Kriterien hierfür sind auf der einen Seite das Ausmass, in dem die Objekte essentielle Güter oder Dienstleistungen bereitstellen und auf der anderen Seite mit welchem Gefahrenpotential die Objekte verbunden sind. Das SKI-Inventar basiert dabei auf freiwilliger Teilnahme der privaten Betreiber und erlegt den Unternehmen keine zusätzlichen Leistungen oder Aufgaben auf. Es besteht auch keine Meldepflicht für Veränderungen; jedoch wird das erfasste Inventar alle zwei Jahre überprüft. Die verwendete Methode orientiert sich am entsprechenden Ansatz der EU. Die Erarbeitung und Aktualisierung des SKI-Inventars auf der nationalen Ebene erfolgt in 28 sektorenspezifischen Arbeitsgruppen, in denen u.a. KI-Betreiber, Verbände und Fachbehörden vertreten sind. Das Ziel ist primär die Erfassung von Objekten mit nationaler Bedeutung. Dabei wird die Bedeutung anhand eines Einwohnergleichwerts eruiert. Um nationale Bedeutung zu erlangen, muss die Versorgung von mindestens 150'000 Menschen betroffen sein. Zunächst wurden hierfür die relevanten Prozesse in allen Kritischen Teilsektoren (KTS) erfasst. Anschliessend wurden die Einzelobjekte zu Objektgruppen zusammengefasst, bevor spezifische Kriterien und Schwellenwerte für die einzelnen Objektgruppen definiert wurden. Abschliessend wurden die einzelnen Objekte in den Objektgruppen mithilfe eines Fragebogens hinsichtlich ihrer Kritikalität beurteilt und weitere objektspezifische Informationen erfasst.

Insgesamt wurden mit dieser Methode 100 nationale kritische Objekte identifiziert. Im Unterschied zu den existierenden EU-Richtlinien, welche sich auf Auswirkungsanalysen bei Ausfällen konzentrieren, fokussiert der Ansatz in der Schweiz auf die Leistung der Objekte (entweder quantitativ, soweit messbar, oder qualitativ im Sinne einer Funktionswertanalyse). Die Beurteilung der Gefährdung erfolgt

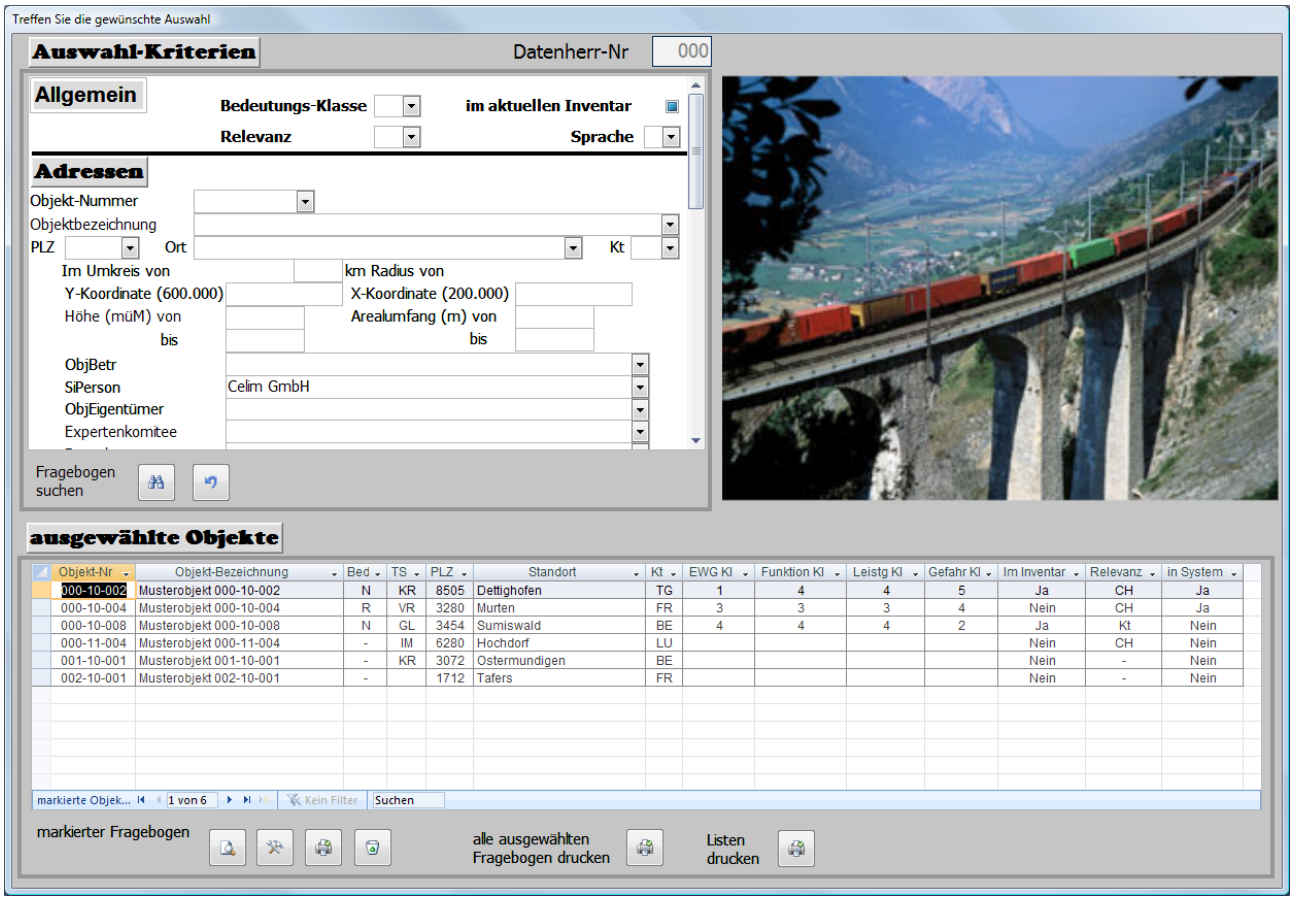

Abbildung 6: Screenshot Datenbank COBE-SKI (Musterauszug mit fiktivem Objektbeispiel)

nicht in Klassen, sondern wird dichotom beurteilt (relevant / nicht relevant). Das Inventar berücksichtigt Dependenzen, Redundanzen und Ausfallkonsequenzen. Das Gesamtinventar unterliegt der Geheimhaltung. Auszüge daraus (bspw. für die Kantone) sind vertraulich. Die Verwaltung des SKI-Inventars erfolgt deshalb auf einer vom Internet getrennten Datenbank COBE-SKI (s. Abbildung 6). Entsprechend klassifizierte Auszüge des Inventars sind beispielsweise für den Bundesstab ABCN, für das Ressourcenmanagement, die Nationale Alarmzentrale (NAZ), für Sicherheitseinsätze der Armee usw. sehr nützlich. Das Inventar wird auch in Übungen auf Bundesstufe verwendet und kann mit Gefahrenkarten zusammengeführt werden. Zurzeit werden die national erfassten kritischen Objekte von den kantonalen Stellen durch die für sie relevanten Objekte ergänzt.

2.4 Interdependenzen

Präsentation: Peter Lauwe, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Interdependenzen stellen einen der Hauptgründe dar, warum der Schutz Kritischer Infrastrukturen umfassend und systematisch erfolgen sollte. Zugleich ist die Entwicklung von praxisnahen Instrumenten zur Erkennung und Reduzierung von Interdependenzen bislang nur wenig entwickelt. In die richtige Richtung weisen die Schweizer Dependenzmatrix bzw. die Schwedische Kommunikationsmatrix. Weiter gehen die Ansätze des U.S.-amerikanischen National Infrastructure Simulation and Analysis Center, das eine Vielzahl von Modellen verknüpft, um Prognosen zu erstellen. Auch Projekte auf europäischer Ebene (u.a. DIESIS, CIPRNet) gelingt es, zunehmend komplexe Modelle zur Berechnung von Interdependenzen zu erstellen.

Gleichzeitig stellt sich bei der Interdependenzthematik die Frage, wie die existierenden wissenschaftlichen Ansätze zur Berechnung von Interdependenzen einen Mehrwert für die SKI-Anwendung bringen können. Einerseits sind die verwendeten Modelle extrem komplex und teilweise wenig praxisrelevant. Andererseits variieren die Ergebnisse bestehender Studien bislang häufig stark.

2.5 Schutz- und Leistungsziele

Präsentation: Nick Wenger, Bundesamt für Bevölkerungsschutz BABS

Die Definition von Schutz- und Leistungszielen ist ein zentraler Bestandteil in der Schweizer SKI-Strategie, da sie die Grundlage für die Massnahmenplanung bilden. Bei der Entwicklung von Schutzzielen existieren zwei gängige Ansätze: 1. die Festlegung von Grenzwerten akzeptabler Risiken; 2. der Grenzkosten-Ansatz, der auf die vollständige Monetarisierung der prioritär zu bearbeitenden Risiken abzielt, um das Kosten-Nutzen-Verhältnis für einzelne Massnahmen berechnen zu können. Um die Leistungs- bzw. Zahlungsbereitschaft sowie die Risiko-Aversion abzubilden, kommt dem Grenzkosten-Ansatz im schweizerischen SKI-Kontext eine wichtige Rolle zu. Die Grenze der Zahlungsbereitschaft ist schliesslich eine Abwägungsfrage im politisch-gesellschaftlichen Prozess gegenüber anderen Interessen und Prioritäten (bspw. Umweltschutz). In einem Praxistest wurden unterschiedliche Szenarien für ein Krankenhaus untersucht. Dabei standen nicht die Auswirkungen auf das Spital selbst im Fokus, sondern die gesellschaftlichen Auswirkungen, wenn das Spital ausfällt resp. Leistungseinbussen aufweist. Insgesamt hat sich der Grenzkosten-Ansatz bislang bewährt.

In der Diskussion wurde das Problem thematisiert, wie sich die gesellschaftliche Zahlungsbereitschaft erfassen lässt. In Deutschland gibt es dazu bislang keine Daten. In Österreich wurde im Rahmen des SESAME-Projekts versucht den «return on security investment» für bestimmte Massnahmen zu erfassen. In der Diskussion wurde auch erwähnt, dass ein sektorenübergreifender Vergleich wohl ein utopisches Fernziel darstellt, da die Priorisierung stark durch politische Prozesse und Rahmenbedingungen beeinflusst wird.

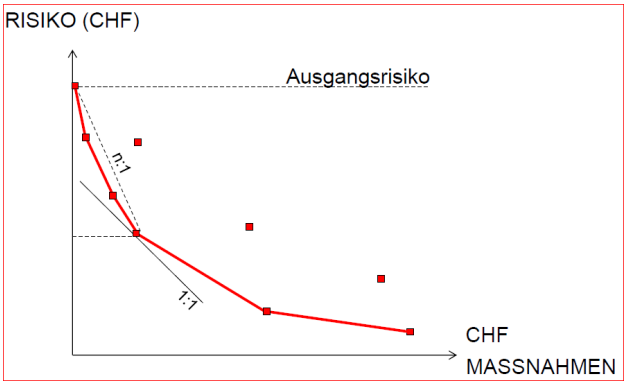

Abbildung 7: Beispiel-Diagramm Anwendung des Grenzkostenansatzes

2.6 Resilienz-Indikatoren

Präsentation: Florian Roth, Risk and Resilience Team, Center for Security Studies, ETH Zürich

Resilienz-Ansätze spielen eine zunehmend wichtige Rolle beim Schutz Kritischer Infrastrukturen. Sowohl in der akademischen Literatur als auch in Regierungsdokumenten und Unternehmensstrategien werden Widerstandsfähigkeit und Anpassungsfähigkeit immer mehr als Kernziele aller Massnahmen hervorgehoben. Gleichzeitig stehen dahinter häufig sehr unterschiedliche Vorstellungen, was das Konzept Resilienz im Zusammenhang mit Kritischen Infrastrukturen bedeutet, wer die Verantwortung für die Resilienz von Kritischen Infrastrukturen trägt und wie sich Resilienz produzieren bzw. fördern lässt. In diesem Zusammenhang kommt der Entwicklung von Indikatoren zur Operationalisierung und

Messung von Resilienz eine tragende Bedeutung zu. Eine wichtige Bedingung für die Erarbeitung von Resilienz-Indikatoren ist die Festlegung, welchem Ziel eine Resilienz-Messung dienen soll. Die Messung von Resilienz kann mindestens vier Zielen dienen:

1. um die Resilienz von KI-Objekten zu bewerten,
2. um die Ressourcen-Allokation bei der Resilienz-Förderung zu steuern,
3. um das Risikobewusstsein und die Verantwortung auf Seiten der KI-Betreiber zu fördern,
4. um Veränderungen zu messen, bspw. um die Performanz von Organisationen zu bewerten.

Aufgrund der Bandbreite der Ziele von Resilienz-Messungen, aber auch wegen der Spezifität von KI-Systemen erscheint es fraglich, ob die Entwicklung allgemeingültiger Resilienz-Indikatoren anzustreben ist. Zielführender erscheint hingegen die Entwicklung von Resilienz-Indikatoren, die an den jeweiligen Kontext und die Bedürfnisse angepasst sind. Zugleich gibt es einige Grundbestandteile oder Basisdimensionen von Resilienz, die den meisten gängigen Resilienz-Indikatoren zu Grunde liegen:

- Robustheit (u.a. Wahrscheinlichkeit eines KI-Ausfalls, Qualität/Alter/Instandhaltung der Infrastruktur)
- Redundanzen (u.a. Ersetzbarkeit einzelner Elemente, Backups)
- Ressourcen (u.a. in Hinblick auf Vorsorgeplanung und Krisenkommunikation)
- Effizienz (u.a. Reaktionszeit im Krisenfall, Wiederherstellungsdauer).

Bei der Operationalisierung der Basisdimensionen ist es stets entscheidend, auf das bestehende Risikomanagement so weit wie möglich aufzubauen, um der Duplizierung von Prozessen und Strukturen vorzubeugen. Wichtig ist zudem, alle relevanten Stakeholder in den Entwicklungsprozess einzubinden.

Bislang gibt es nur wenige empirische Beispiele für eine systematische Messung von Resilienz im Bereich Kritischer Infrastrukturen auf regionaler oder nationaler Ebene. Einer der umfassendsten Versuche in dieser Hinsicht stellt das Enhanced Critical Infrastructure Program (ECIP) des U.S.-amerikanischen Department of Homeland Security (DHS) dar.[11] Das Programm erfasst die Verwundbarkeit und Kritikalität von zahlreichen U.S.-amerikanischen KI-Objekten. Darüber hinaus nutzt es einen Benchmarking-Ansatz, um die Sicherheitsmassnahmen für einzelne Infrastrukturen zu vergleichen und den KI-Betreibern handlungsorientierte Informationen zur Verbesserung des Schutzniveaus bereitzustellen (s. Abbildung 8).

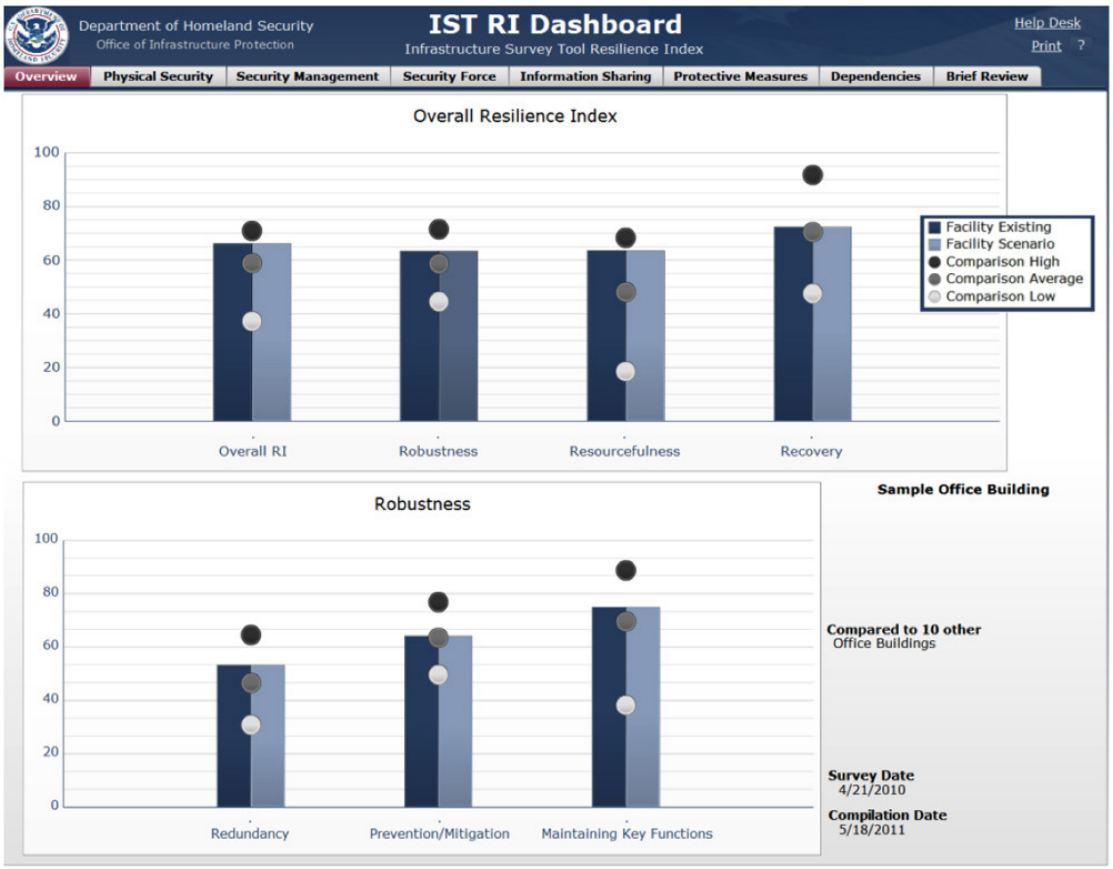

Abbildung 8: Fiktives Ergebnis ECIP-Benchmarking-Analyse

11 *http://www.lcrcip.org/Lists/Announcements%20Public/Attachments/25/Enhanced%20Critical%20Infrastructure%20Protection%20(ECIP)%20Fact%20Sheet%20-%20December%202011.pdf*

3. Leitfäden zum Schutz Kritischer Infrastrukturen

Leitfäden zum Schutz Kritischer Infrastrukturen bilden ein wichtiges Instrument der Behördenkommunikation mit den Betreibern von Kritischen Infrastrukturen. Die SKI-Leitfäden in allen drei Ländern verbindet das Ziel, eigenverantwortliches Handeln von Unternehmen im SKI-Bereich anzuregen und zu fördern. Hierzu werden den KI-Betreibern Leitlinien und Möglichkeiten zur Selbsteinschätzung angeboten, die darauf abzielen, die bestehenden Prozesse in den Unternehmen zu ergänzen bzw. bestehende Defizite zu identifizieren und Impulse für zusätzliche Anstrengungen auf Seiten der Unternehmen zu geben. Im dritten Teil des Workshops berichteten Christine Eismann vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Alexander Pschikal vom österreichischen Bundeskanzleramt und Ulrich Brandenberger vom Bundesamt für Bevölkerungsschutz, wie die unterschiedlichen nationalen SKI-Leitfäden erarbeitet wurden und wie sie angewendet werden. Den Abschluss bildete eine Präsentation von Günter Poßegger vom österreichischen Bundesministerium des Inneren, der erläuterte wie jenseits von Leitfäden das Risiko-Bewusstsein von KI-Betreibern gefördert werden kann. In der Diskussion wurden insbesondere Möglichkeiten und Grenzen kooperativer Ansätze zur Einbindung von Unternehmen in den Schutz Kritischer Infrastrukturen diskutiert.

3.1 Leitfaden in Deutschland

Präsentation: Christine Eismann, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK

Mit dem Leitfaden «Schutz Kritischer Infrastrukturen – Basisschutzkonzept» wurde 2005 eine erste Empfehlung für Betreiber Kritischer Infrastrukturen vorgelegt, die Massnahmen zum physischen, organisatorischen und personellen Schutz umfasst.[12] Der Leitfaden «Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement» erschien erstmals 2008 und wurde 2011 überarbeitet und mit einer Umsetzungshilfe herausgegeben.[13] Er gibt Unternehmen und Behörden Hilfestellungen, um ein einrichtungsbezogenes Risiko- und Krisenmanagement durchzuführen. Dieses enthält die Schritte Vorplanung in der Einrichtung, Risikoanalyse (inkl. Kritikalitätsanalyse, Gefahrenanalyse, Verwundbarkeitsanalyse, Risikoermittlung, Risikobewertung anhand operativer Schutzziele), vorbeugende Massnahmen, Krisenmanagement und Evaluierung.

In einem Forschungsprojekt wurde in Bezug auf die Stromversorgung eine Bow-Tie-Analyse durchgeführt: Erstens werden die direkten Auswirkungen von Schadensereignissen auf Kritische Infrastrukturen erfasst. Zweitens wird analysiert, ob und falls ja inwieweit es zu nachfolgenden Ausfällen bei weiteren Kritischen Infrastrukturen kommen kann. Drittens werden die Auswirkungen auf die Bevölkerung betrachtet. Basierend auf dieser dreigliedrigen Analyse können Massnahmen initiiert werden, mit denen Störungsmechanismen unterbrochen und Kaskadeneffekte vermieden werden können.

Der Leitfaden zum Risiko- und Krisenmanagement selbst ist vergleichsweise allgemein gehalten und gilt für alle Gefährdungstypen. Gleichzeitig dient er als Ausgangspunkt für mehrere Weiterentwicklungen zu einzelnen Infrastrukturen, beispielsweise für eine Empfehlung zum Risikomanagement in Krankenhäusern oder verschiedenen Gefahren. So gibt z.B. das Krisenhandbuch zum Thema Stromausfall, das gemeinsam vom BBK, dem Karlsruher Institut für Technologie (KIT), dem Bundesland Baden-Württemberg und dem Stromversorger EnBW entwickelt wurde, konkrete Empfehlungen für die Bewältigung der Gefahr Stromausfall. Es beinhaltet Checklisten für die Vorsorge, Bewältigung und Nachbereitung. Das Krisenhandbuch dient wiederum als Anhaltspunkt für die Arbeiten in anderen Bundesländern, da es neben den Baden-Württemberg-spezifischen Angaben auch viele allgemeingültige Informationen enthält.[14] Ebenfalls kürzlich erschienen sind die Leitfäden zu den Themen Hochwasser, Hitzewellen und Starkregen.[15] Schliesslich wurde ein Leitfaden zum Schutz von Informatiksystemen in Krankenhäusern erstellt.[16] Ergänzt werden die Leitfäden durch unterschiedliche Studien: So wird momentan an einer Studie zu den Melde- und Informationswegen zwischen den Behörden und den KI-Betreibern gearbeitet. Ebenfalls in der Entwicklung ist eine Überblicksstudie zur Forschung im SKI-Bereich, Evaluierung des KRITIS-Leitfadens sowie KRITIS-Module für ein Software-Tool zur Risikoanalyse.

Insgesamt sind die Arbeiten für den Stromsektor in Deutschland am weitesten fortgeschritten. Bereits seit 2007 existiert der Leitfaden Notstromversorgung.[17] Daran anknüpfend befindet sich gegenwärtig ein flächendeckendes Gesamtkonzept zur Notstromversorgung auf Bundesebene in Vorbereitung. Aufgrund der föderalen Strukturen existieren bislang keine aussagekräftigen Informationen oder einheitlichen Verpflichtungen zur Notstromversorgung von Kritischen Infrastrukturen. Zudem wird gegenwärtig eine

12 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2005/Basisschutzkonzept_kritische_Infrastrukturen.html?nn=3314962

13 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.html?nn=3314962

14 http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Krisenhandbuch_Stromausfall_Kurzfassung_pdf.html;jsessionid=E6D15A04672749E50097D2345D8BE895.1_cid345

15 http://www.bbk.bund.de/SharedDocs/Kurzmeldungen/BBK/DE/2013/Schutz_vor_Hitzewelle_Starkregen_Kommunen.html; http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_4_Praxis_BS_Hochwasser-Kommuna-Ebene.html;

16 http://www.bbk.bund.de/SharedDocs/Kurzmeldungen/BBK/DE/2013/Lf_Risikoanalyse_Krh_IT.html

17 http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/Publikationen/Leitfaden_Notstromversorgung.html

Studie zur Bevorratung/Lagerung von Lebensmitteln für den Fall eines flächendeckenden, langanhaltenden Stromausfalls durchgeführt.

Bislang basieren alle Arbeiten in diesem Bereich auf einem kooperativen Ansatz. Gleichzeitig zeigen sich zunehmend die Grenzen des Freiwilligkeitsprinzips, insbesondere wenn aus den Verwundbarkeitsanalysen ein Handlungsbedarf abgeleitet wird, der für die Betreiber Kritischer Infrastrukturen mit Folgekosten verbunden ist. Da die Betreiber häufig nicht bereit sind, die entsprechenden Massnahmen zu ergreifen, erscheint hier die Schaffung gesetzlicher Regelungen notwendig. Zunächst sollten aber auch weiterhin auf Handlungsempfehlungen gesetzt werden, um Unternehmen zur Umsetzung von Schutzmassnahmen zu bewegen. Wichtiger Bestandteil solcher Handlungsempfehlungen sind best practice-Beispiele, an denen sich die Unternehmen orientieren können.

Die anschliessende Diskussion befasste sich hauptsächlich damit, wie mithilfe der Leitfäden ein Mehrwert für die Unternehmen generiert werden kann resp. wie Unternehmen von der Notwendigkeit weiterer Massnahmen überzeugt werden können.

3.2 Leitfaden in Österreich

Präsentation: Alexander Pschikal, Bundeskanzleramt BKA

In Österreich werden die kritischen Prozesse in rund 400 strategischen Unternehmen mit dem interaktiven Leitfaden «Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich» unterstützt.[18] Der Leitfaden folgt dem Ansatz, dass die Analyse von Verwundbarkeit durch die Unternehmen selbst geleistet werden sollte. Daher liegt das Self-Assessment auf Ebene der CEOs sowie der Abteilungsleiter (Risk Owner) in den Unternehmen klar im Fokus des Leitfadens. Neben der theoretischen Zusammenfassung und vielen Praxisbeispielen sind 500 Fragen zur Selbstevaluation zentraler Bestandteil des Leitfadens. Die Fragen gliedern sich in die sechs Aufgabenbereiche: organisatorische Herausforderungen, Recht, technische Gefahren, Marktsituation, Naturgefahren und intentionale Gefahren. Der Leitfaden präsentiert sich dabei nicht als Checkliste, sondern als Fragenkatalog. Auf Grundlage eines Punktesystems wird die Selbsteinschätzung unterstützt und Mindestziele vorgeschlagen (siehe Abbildung 9). Ursprünglich war auch ein Benchmarking eingeplant, was jedoch von den Interessenvertretungen abgelehnt wurde. Ziel des Leitfadens ist primär Bewusstseinsförderung auf der Leitungsebene der Unternehmen. Insbesondere sollen die Unternehmen dazu motiviert werden, bereits bestehende Risikomanagement-, Business-Continuity-Management und Security-Management-Prozesse auszubauen und zu einer umfassenden Sicherheitsarchitektur zu integrieren, was letztlich die Resilienz und Sicherheit der Gesamtheit der Kritischen Infrastrukturen in Österreich erhöht.

Die Diskussion befasste sich mit der Frage, inwiefern das «Scheitern am Markt» von KI-Unternehmen ebenfalls als Risiko in die Betrachtung mit einbezogen werden soll/kann. In Österreich wird dieser Aspekt in den Verwundbarkeitsanalysen berücksichtigt. In Deutschland kam dieser Punkt erst im Rahmen der Finanzkrise in die Diskussion. Ebenso wurde die bereits zuvor diskutierte Frage wieder aufgegriffen, inwiefern die Ergebnisse des Self-Assessments in konkrete Massnahmen überführt werden können, insbesondere wenn hohe Kosten damit verbunden sind.

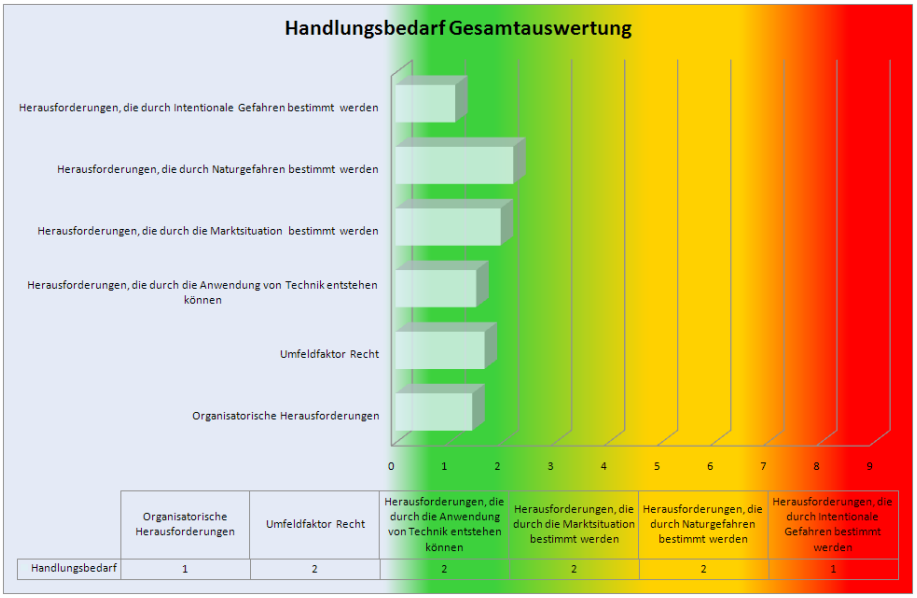

Abbildung 9: Beispiel-Ergebnis Handlungsbedarf nach Selbstevaluierung

18 *https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/schutz_strategischer_infrastrukturen/71359.html*

3.3 Leitfaden in der Schweiz

Präsentation: Ulrich Brandenberger, Bundesamt für Bevölkerungsschutz BABS

Seit 2011 erarbeitet das BABS einen SKI-Leitfaden für die Schweiz. Die Erarbeitung erfolgt in enger Zusammenarbeit mit der Arbeitsgruppe SKI, in der mehr als 20 Bundesstellen und zwei Kantone vertreten sind, sowie mit verschiedenen KI-Betreibern. Nach einer Pilotphase des Leitfadens mit Swissgrid in 2013 und der fachlichen Konsultation Anfang 2014 wird der Leitfaden voraussichtlich im Herbst 2014 veröffentlicht. Der Leitfaden wird vom Ziel geleitet, bestehende Einzelmassnahmen in einen umfassenden SKI-Ansatz zu überführen. Hierfür sollen vorhandene unternehmerische Managementsysteme mit einer SKI-Perspektive ergänzt werden, welche die Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen berücksichtigt. Damit soll ein Mehrwert gegenüber den betrieblichen Prozessen (u.a. Risikomanagement, BCM, Sicherheitsmanagement, s. Abbildung 10) erzielt werden. Neben den KI-Betreibern übernehmen die Branchenverbände (bspw. die Schweizerische Bankiervereinigung) eine wichtige Rolle, u.a. durch die Erarbeitung von Musterlösungen. Zudem baut der Leitfaden auf bestehende Instrumente der Gefährdungsanalyse auf. So können Unternehmen den durch das BABS erarbeiteten Gefährdungskatalog nutzen, um mithilfe von Szenarien die wichtigsten Gefährdungen zu identifizieren, die zum Ausfall der kritischen Prozesse und Ressourcen innerhalb des Unternehmens führen können.[19] Am Ende des Selbstevaluierungsprozesses erstellen die KI-Betreiber einen Analysebericht, der u.a. eine unternehmensspezifische Risikomatrix sowie eine Liste mit erkannten Lücken und erforderlichen Massnahmen umfasst.

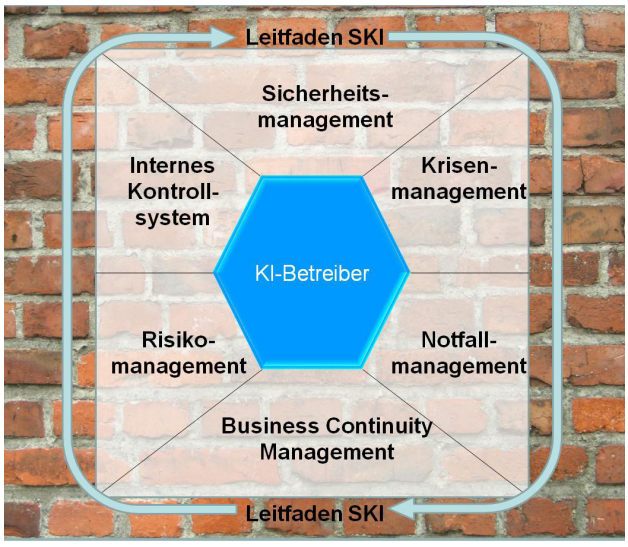

Abbildung 10: Verbindung des SKI-Leitfadens zu bestehenden Mechanismen der KI-Betreiber

Ebenso wie in Deutschland und Österreich setzt auch der schweizerische Ansatz Eigeninitiative der Unternehmen voraus, da es bislang keine spezifischen gesetzlichen Vorgaben gibt den Leitfaden anzuwenden. Der Leitfaden versteht sich deshalb als Hilfestellung resp. als Angebot zur Erweiterung des unternehmerischen Risikomanagements. Das BABS und die zuständigen Fachstellen unterstützen dabei die KI-Betreiber bei der Umsetzung des Leitfadens.

In der Diskussion wurde gefragt, ob es bereits zu Konflikten mit allenfalls vorhandenen Leitfäden der Fachbehörden gekommen sei. Dies war bis anhin weder in Deutschland noch in der Schweiz der Fall gewesen.

3.4 Bewusstseinsbildung bei KI-Betreibern

Präsentation: Günter Poßegger, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, Bundesministerium für Inneres

In Österreich wird den Bereichen Prävention und Bewusstseinsbildung eine wesentliche Bedeutung für die innere Sicherheit beigemessen. Im Rahmen der Bewusstseinsbildung bei Betreibern Kritischer Infrastrukturen sind folgende Ziele zentral:

- Nachhaltiges Konzept zur regelmässigen Bewusstseinsbildung bei Betreibern KI
- Information der Betreiber über Programme und Strategien
- Sensibilisierung der Betreiber hinsichtlich aktueller Gefahren und Risiken
- Verteilung des CD-Leitfadens und aktive Beratung
- Informationsmanagement über alle vorhandenen Handbücher/Produkte/Beratungen
- Sektorenspezifische/sektorenübergreifende Veranstaltungen

In diesem Rahmen ist das Referat Schutz Kritischer Infrastruktur in verschiedenen Bereichen bedeutend. Die Aufgaben umfassen die Erstellung eines Objektschutzkataloges, Kontaktgespräche sowie weitere Massnahmen zur Prävention und Bewusstseinsbildung.

19 http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/nat__gefaehrdungsanlayse/gefaehrdungskatalog.html

4. Cyber-Risiken und SKI

Der vierte Teil des Workshops widmete sich dem Thema Cyber-Sicherheit, das in den letzten Jahren zunehmend zentrale Bedeutung beim Schutz Kritischer Infrastrukturen gewonnen hat. Zum einen nimmt die gesellschaftliche Bedeutung von modernen Informations- und Kommunikationstechnologien immer weiter zu, zum anderen können Cyber-Risiken Auswirkungen auf viele andere SKI-Bereiche haben. Aus diesem Grund haben sowohl Deutschland, Österreich als auch die Schweiz bereits seit einigen Jahren ihre Aktivitäten im Bereich Cyber-Sicherheit stark ausgebaut. In der ersten Präsentation erläuterte Andreas Kullmann vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die deutsche Cyber-Sicherheitsstrategie und ihre Auswirkungen auf den Bereich Kritische Infrastrukturen. Im Anschluss informierte Uwe Jendricke vom Bundesamt für Sicherheit in der Informationstechnik über den aktuellen Stand des Umsetzungsplan Kritische Infrastrukturen (UP KRITIS), der in Deutschland zahlreiche Stellen aus dem Bereich IT-Sicherheit koordiniert. Danach stellte Helmut Schnitzer vom Bundeskanzleramt die kürzlich verabschiedete Österreichische Cybersecurity-Strategie (ÖSCS) vor. Schliesslich stellte Ka Schuppisser vom Informatiksteuerungsorgan des Bundes die zentralen Elemente der Nationalen Cyberstrategie (NCS) der Schweiz vor, die 2012 verabschiedet wurde. In der anschliessenden Diskussion erörterten die Workshop-Teilnehmern u.a. wie die Aktivitäten in den Themenbereichen Cyber-Sicherheit und Schutz Kritischer Infrastrukturen besser aufeinander abgestimmt werden können.

4.1 Deutschland

4.1.1 Cyber-Sicherheitsstrategie und KRITIS Deutschland

Präsentation: Andreas Kullmann, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK

Die 2011 beschlossene Cyber-Sicherheitsstrategie befindet sich an der Schnittstelle der Bereiche Terrorismus- und Kriminalitätsbekämpfung, IT-Schutz und Bevölkerungsschutz.[20] Die Führung im Strategieprozess liegt in der Fachabteilung des Bundesinnenministeriums und beim BSI als nachgeordnete Behörde. Ausgangspunkt des Strategiebildungsprozesses war die Erkenntnis, dass aus zunehmender Vernetzung grössere physische Verwundbarkeiten resultieren. Zudem wurde in jüngerer Zeit festgestellt, dass Kritische Infrastrukturen verstärkt Ziel von Cyberspionage werden, auch wenn das Ziel dieser Spionage nicht in allen Fällen geklärt werden konnte.

Gegenwärtig verteilt sich die Arbeit im Themenbereich Cybersicherheit und Kritische Infrastrukturen auf eine Vielzahl an Organisationen und Gremien; u.a. sind die staatlichen Akteure bereits seit 2007 in mehreren Public Private Partnerships (PPPs) engagiert. Dabei stehen vor allem die sogenannte Allianz für Cybersicherheit, eine Plattform allgemein für die Wirtschaft, und insbesondere der UP KRITIS, speziell für die KRITIS Unternehmen, im Fokus. Hinzu kommen verschiedene nicht-staatlichen Foren und Initiativen.

Um die unterschiedlichen Aktivitäten der deutschen Sicherheits- und Aufsichtsbehörden zu bündeln, soll das 2011 eingerichtete zentrale Cyber-Abwehrzentrum, das am BSI angesiedelt ist, eine zunehmend aktive Rolle in Analyse und Bewertung von Cyber-Sicherheitsvorfällen spielen.[21] Analog zur Melde- und Analysestelle Informationssicherung (MELANI) in der Schweiz dient das deutsche Abwehrzentrum in erster Linie als Drehscheibe zur Information und Koordination der beteiligten Akteure. Der Fokus liegt hierbei klar auf staatlicher Sicherheitsvorsorge, weshalb privatwirtschaftliche Vertreter nicht in das Abwehrzentrum eingebunden sind. Gleichzeitig berichtet das Abwehrzentrum an den Cyber-Sicherheitsrat, in dem neben hochrangigen staatlichen Vertretern auch die Wirtschaft eingebunden ist.

Für das BBK steht momentan die Frage im Raum, wie die Strategie spezifisch für den Bevölkerungsschutz und insbesondere den Zivilschutz verfeinert werden soll. Die Positionierung des BBK sieht dabei vor, die SKI-Perspektive in den Strategieprozess einzubringen ohne der primäre Kompetenzträger zu werden. Das heisst aus, Bevölkerungsschutzsicht besteht das primäre Ziel darin, Resilienz und Agilität als Ziele zu etablieren und auf diesem Wege Fragen des Versorgungsschutzes in die Diskussion einzubringen. Darüber hinaus soll im nächsten Schritt die Verbindung der Aktivitäten im Bereich der Risikoanalyse mit dem Themenfeld der Risikokommunikation besser verbunden werden.

4.1.2 Umsetzungsplan KRITIS – Sachstand

Präsentation: Uwe Jendricke, Bundesamt für Sicherheit in der Informationstechnik BSI

2007 wurde der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) veröffentlicht. Dieser baut auf dem Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) aus dem Jahr 2005 auf.[22] Als Ergebnis des Umsetzungsplans wurde die PPP «UP KRITIS» etabliert. Dieser hat das Ziel, den Informationsaustausch sowie branchenübergreifendes, lösungsorientiertes und gemeinsames Handeln zwischen den KRITIS-Betreibern untereinander sowie mit dem Staat zu fördern. Die Zahl der Teilnehmer ist in den letzten Jahren stark

20 *http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html*

21 *http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html*

22 *https://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.pdf?__blob=publicationFile*.

gewachsen. Derzeit sind es 50 Unternehmen und Behörden. Der UP KRITIS wurde in der Cyber-Sicherheitsstrategie 2011 bestätigt und durch weitere Elemente ergänzt.[23] In den letzten Jahren hat sich die Arbeit im UP KRITIS zunehmend institutionalisiert. So wurde neben dem Plenum ein Rat zur Anbindung an die Politik gebildet und ein Stab etabliert. Seit kurzem ist ein UP KRITIS-Vertreter auch im Cybersicherheitsrat repräsentiert. In den Bevölkerungsschutz ist der UP KRITIS auch über seine Beteiligung an Katastrophenschutzübungen integriert.

Ursprünglich war der UP KRITIS sehr IT-lastig. In jüngerer Zeit fokussiert er sich immer stärker auch auf Fragen des Business Continuity Managements (BCM). Um die Bandbreite der relevanten Fragestellungen abzudecken, wurden Arbeitskreise zu einzelnen Themen und Branchen gebildet. Gegenwärtig gibt es vier Branchenarbeitskreise (Strom, Medien, Lebensmittelhandel, Wasser/Abwasser) sowie vier Themenkreise (Operativer Informationsaustausch, Übungen, KRITIS-Regulierung, Fortschreibung UP KRITIS). Die Arbeitskreise werden durch die Betreiber und deren Verbände möglichst selbst verwaltet. Dabei ist festzustellen, dass der Stand der Arbeiten und das Bewusstsein je nach Branche unterschiedlich stark ausgeprägt sind. Eine der Hauptherausforderungen besteht momentan darin, dass nur ein Bruchteil der Vorfälle durch die betroffenen Unternehmen gemeldet wird. Das neue IT-Sicherheitsgesetz, das voraussichtlich im Verlauf des Jahres 2014 verabschiedet wird, soll hier einen verbindlichen Rahmen geben und damit die Informationslage verbessern. Ausserdem befindet sich ein Fortschreibungsdokument für den UP KRITIS in der Vorbereitungsphase.

In der Diskussion wurden die Beziehungen zwischen dem IT-Sicherheitsgesetz und dem Cyber-Sicherheitsgesetz erörtert. Zudem wurde diskutiert, wie die CIP-Perspektive im gegenwärtigen «Cyber-Hype» in die öffentliche Diskussion eingebracht werden kann. Schliesslich diskutierten die Workshop-Teilnehmer, ob sich die Aufmerksamkeit vor allem auf grosse Bedrohungen mit Auswirkungen für die KI fokussieren sollte oder ob auch schon bei «kleineren» Gefährdungen die SKI-Perspektive eingebracht werden sollte, um Vertrauen aufzubauen.

4.2 Österreich

4.2.1 ÖSCS

Präsentation: Helmut Schnitzer, Bundeskanzleramt BKA

Die Österreichische Cybersecurity-Strategie (ÖSCS) wurde 2013 beschlossen, momentan ist sie in der Umsetzung.[24] Die strategische Vision der Strategie ist ein sicherer, resilienter und verlässlicherer Cyber-Raum. Dabei sollen nicht nur die Risiken, sondern auch die Chancen des Cyberspace herausgearbeitet werden. Die Strategie basiert auf der entsprechenden EU-Strategie, der APCIP-Strategie sowie der österreichischen Sicherheitsstrategie. Massgeblich an der Strategiefindung beteiligt waren das Bundeskanzleramt, das BM.I., das BMLVS und das Bundesministerium für europäische und internationale Angelegenheiten. Die Steuerung erfolgt gemeinsam durch die Bundesministerien und einen Ländervertreter, die Einbindung der Betreiber ist gewährleistet. Als institutionelle Stützen sind ein gemeinsames Lagezentrum für Cybercrime, ein militärisches Zentrum (MilCert) und ein CERT-System (im Bundeskanzleramt) geplant. Die strategische Führung geht vom Bundeskanzleramt aus, die operative Führung liegt im BM.I. Grundsätzlich wird ein partnerschaftlicher Ansatz angestrebt, dennoch sind auch Meldepflichten und Sicherheitsstandards vorgesehen. Mittelfristig wird darüber hinaus ein nationales Cybersicherheitsgesetz angestrebt, durch das eine stärkere Regulierung ermöglicht würde. Wichtig in diesem Kontext ist das politische Momentum, das derzeit in der Cyber-Thematik vorhanden ist, auch für die Verbesserung des Risikomanagements im SKI-Bereich zu nutzen.

Ein weiteres wichtiges Element soll eine gemeinsame Plattform für IKT-Betreiber, Wissenschaft, Zivilgesellschaft und Behörden bilden, die neben dem Informationsaustausch auf strategischer Ebene insbesondere einen Rahmen für die strukturierte Bearbeitung von Cyber-Themen bietet. Sie befindet sich gegenwärtig in der Planung und soll bis Ende 2014 einsatzbereit sein.

In der Diskussion wurden die Erfahrungen der letzten Jahre in der Zusammenarbeit mit der Privatwirtschaft diskutiert. Als positives Beispiel wurde hier das Thema Online-Banking genannt, bei dem es bereits seit einiger Zeit eine erfolgreiche Partnerschaft zwischen Banken gibt, weil die Risiken von allen beteiligten Seiten anerkannt werden. Ausserdem wurde diskutiert, wie die Entwicklungen auf der europäischen Ebene in Zukunft berücksichtigt werden können. In Österreich sollen die NIS-Richtlinien abgewartet werden, die unter anderem eine nationale Zentrale vorsehen. In Deutschland hingegen gibt es Bemühungen, die europäische Entwicklung zur Verbesserung der Netz- und Informationssicherheit (NIS) aktiv zu beeinflussen.

4.3 Schweiz

4.3.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NSC)

Präsentation: Ka Schuppisser, Informatiksteuerungsorgan des Bundes ISB

Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (Nationale Cyberstrategie, NCS) wurde im Juni 2012

23 http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html

24 https://www.bka.gv.at/DocView.axd?CobId=50748

gleichzeitig mit der SKI-Strategie durch den Bundesrat verabschiedet.[25] Die Strategie verfolgt einen ganzheitlichen, risikobasierten Ansatz, um Kritische Infrastrukturen vor Cyber-Ausfällen und -Angriffen zu schützen, wie auch deren Informationen zu sichern. Insgesamt umfasst die Strategie 16 Massnahmen, die nun fortlaufend umgesetzt werden und deren erstmalige Überprüfung bis 2017 durchgeführt werden soll (siehe Abbildung 11). Mit der Strategie werden drei Ziele verfolgt: Die Verbesserung der frühzeitigen Erkennung, die Stärkung der Infrastruktur (Hauptfokus der Strategie) sowie die generelle Minimierung von Cyber-Risiken. Dafür werden neu 28 Personalstellen über sechs verschiedene Departemente hinweg geschaffen, welche die Strategie auf Stufe des Bundes umsetzen. Auf der Ebene der Kantone wurden vor kurzem vier Arbeitsgruppen gebildet. In der Wirtschaft gibt es auf fachlicher und politischer Ebene laufende Einbettungsmassnahmen. Nicht abgedeckt durch die Strategie werden hingegen die militärischen Aspekte der Cyberthematik. Als Informationsdrehscheibe zwischen den Behörden und einem geschlossenen Kundenkreis aus der Wirtschaft und Verwaltung fungiert die Melde- und Analysestelle Informationssicherung (MELANI).[26] Diese Plattform ist trotz, oder vielleicht auch dank der Freiwilligkeit, erfolgreich. Sie geniesst bei den KI-Betreibern ein grosses Vertrauen und soll künftig ausgebaut werden.

Die Umsetzung der Strategie in den verschiedenen Teilsektoren wird je nach Thematik durch das BABS und das Bundesamt für wirtschaftliche Landesversorgung (BWL) ausgeführt. Diese beiden Ämter werden in einem nächsten Schritt eine Methodik zur Risiko- und Verwundbarkeitsanalyse vorlegen, deren Umsetzung zwischen 2014 und 2016 vorgesehen ist.

In der Diskussion wurde besprochen, wie die Verbände in die Steuerung eingebunden werden können. Zudem wurde erörtert, dass IKT, wenn sie ausfällt, nicht nur ein Risiko darstellt, sondern auch eine Schlüsselressource für andere Bereiche darstellt. Ausserdem wurde der Frage nachgegangen, wie die Parallelität zwischen der IKT-Thematik und dem KI-Bereich überbrückt werden kann. Es wurde diskutiert, ob Cyber-Themen in das KRITIS-Framework (im Falle Deutschlands) integriert werden sollten anstatt einen eigenen IT-Framework zu erarbeiten. Des Weiteren wurde angemerkt, dass häufig die Fehlwahrnehmung vorherrscht, nur IKT-Betriebe seien von der Cyberproblemen betroffen. Tatsächlich sind IKT-Strukturen auch in vielen anderen Bereichen bereits kritisch.

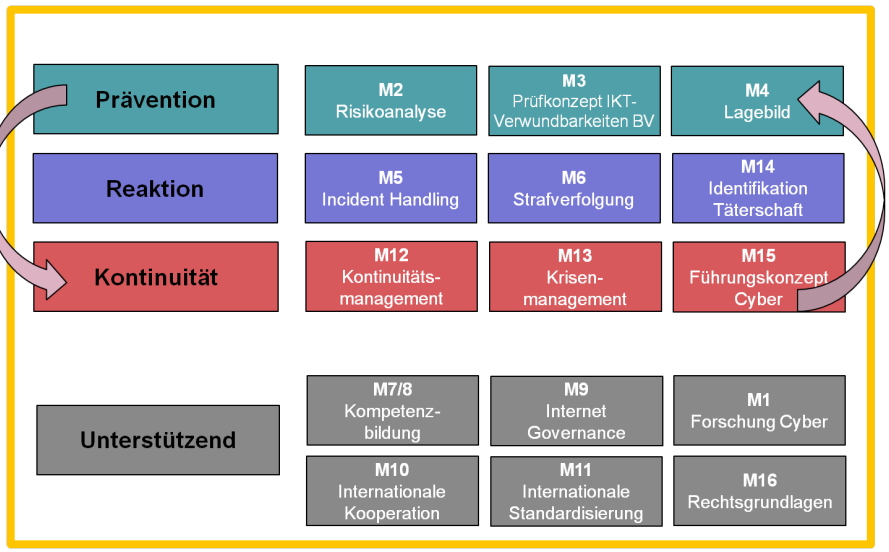

Abbildung 11: Übersicht Massnahmen der Nationalen Cyberstrategie

25 *http://www.isb.admin.ch/themen/01709/01710/index.html?lang=de*

26 *http://www.melani.admin.ch*

5. Informations-Plattformen im SKI-Bereich

SKI-Plattformen dienen dem Informationsaustausch zwischen den unterschiedlichen Akteuren im Bereich Kritischer Infrastrukturen. In ihren Präsentationen stellten Michel Herzog von der ETH Zürich und Alexander Pschikal vom österreichischen Bundeskanzleramt zwei unterschiedliche Beispiele solcher Plattformen vor.

5.1 Cybersecurity Framework des National Institute of Standards and Technology (NIST)

Präsentation: Michel Herzog, Risk and Resilience Team, Center for Security Studies, ETH Zürich

Das Hauptziel des Cybersecurity Frameworks des National Institute of Standards and Technology (NIST) ist die Verbesserung der Sicherheit national bedeutsamer Kritischer Infrastrukturen in den USA durch die Reduzierung von Cyber-Risiken. Dazu verfolgt das Programm einen flexiblen, leistungsbasierten und kosteneffizienten Ansatz, der Organisationen, die mit dem Schutz Kritischer Infrastrukturen betraut sind, im Umgang mit Cyber-Risiken unterstützt.[27] Dabei baut das NIST Framework auf folgende Prinzipien:

- Erarbeitung von technologieneutralen Lösungen, basierend auf dem Freiwilligkeitsprinzip
- Förderung methodischer Ansätze im Cyber-Sicherheitsbereich
- Berücksichtigung bestehender Regulierungen
- Verbesserung des Informationsaustausches zur Cyber-Bedrohungen sowohl im Hinblick auf die Quantität und Qualität als auch auf die Aktualität der Informationen
- Sicherung des Datenschutzes und individueller Freiheitsrechte beim Schutz Kritischer Infrastrukturen

Die Ausarbeitung des Frameworks wurde federführend durch das NIST geleitet. Zugleich wurde grossen Wert auf eine möglichst umfassende Einbindung der Vertreter aus der Industrie, Regierungsvertretern, aber auch interessierter Personen aus der Zivilgesellschaft gelegt. Abbildung 12 stellt den mehrstufigen Prozess dar, in dem das NIST Framework ausgearbeitet wurde.

5.2 CIWIN-AT

Präsentation: Alexander Pschikal, Bundeskanzleramt BKA

Das österreichische Critical Infrastructure Web Information Network (CIWIN-AT) soll die zentrale Informationsdrehscheibe im Bereich Kritischer Infrastrukturen in Österreich (siehe Abbildung 13) bilden. Die Plattform dient primär zum Austausch von Informationen zu sicherheitsrelevanten Themen (u.a. Publikationen, Links, Regulierungen) sowie als Schnittstelle zwischen Unternehmen und Behörden. Strategisch soll hierdurch auf der einen Seite das behördliche Informationsmanagement optimiert werden Auf der anderen Seite sollen Partnerschaften zwischen Privatwirtschaft und Behörden gefördert werden. Die Plattform ist nicht öffentlich, sondern richtet sich lediglich an die strategischen sowie involvierten Unternehmen. CIWIN-AT baut auf dem gleichnamigen EU-Projekt im Rahmen des Europäischen

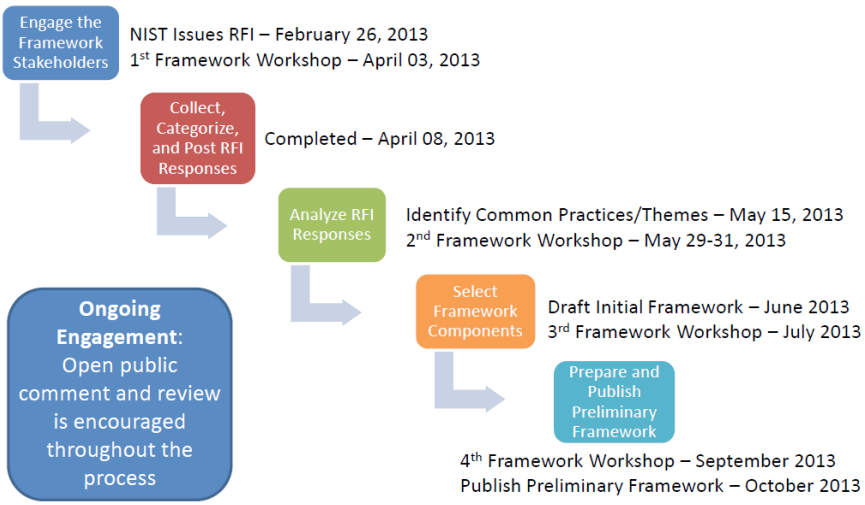

Abbildung 12: Arbeitsschritte NIST Cybersecurity Framework

27 Executive Order 13636 (2013): «Improving Critical Infrastructure Cybersecurity» *http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-12/cybersecurity-framework_nist.pdf.*

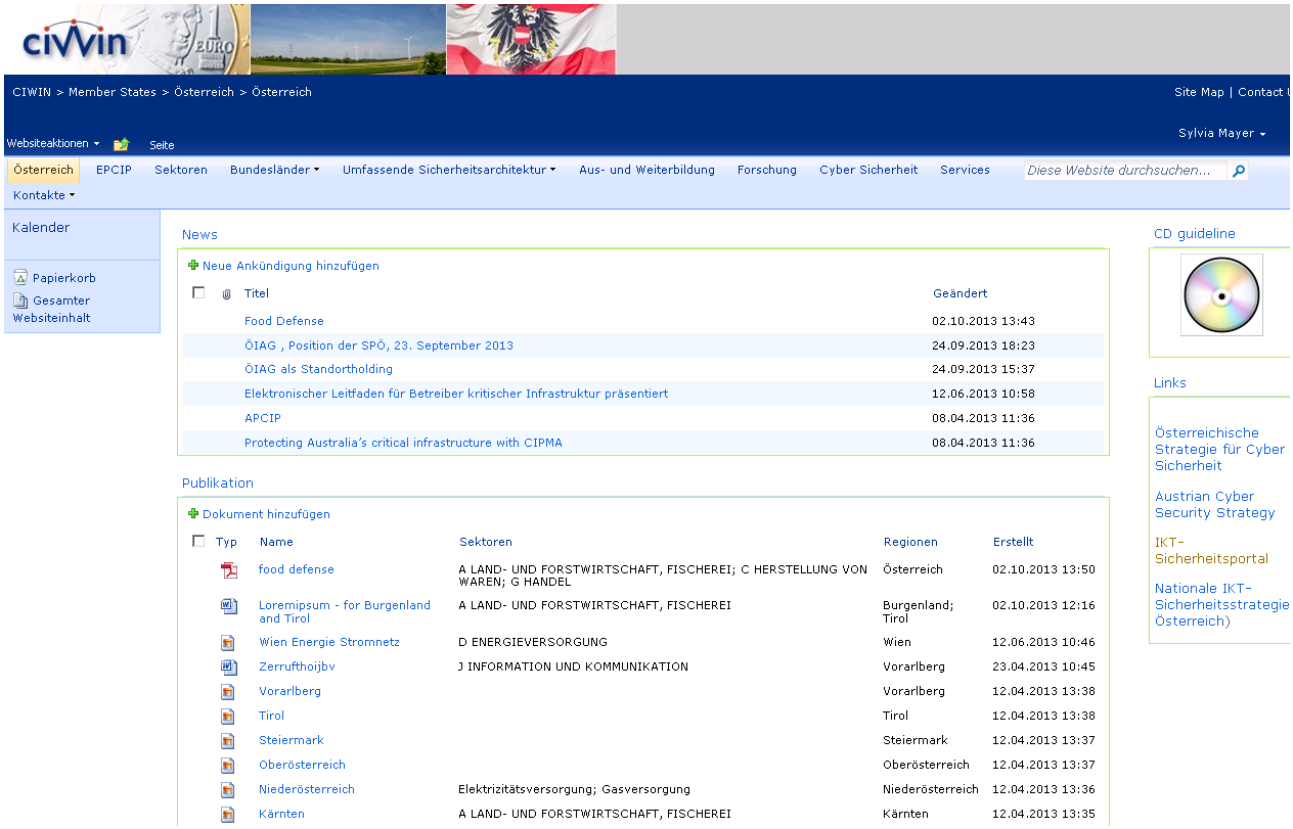

Abbildung 13: Startseite CIWIN-Plattform

Programms zum Schutz Kritischer Infrastrukturen (EPCIP) auf, an dem Österreich ebenfalls partizipiert.[28] Mithilfe einer Sharepoint-Lösung wurde die europäische Plattform für den österreichischen Kontext angepasst und nach den ÖNACE-Sektoren strukturiert. So verfügen auch die Bundesländer jeweils über eigene Unterseiten, die sie selbstständig verwalten können. Darüber hinaus besteht eine Verbindung zum IKT-Sicherheitsportal.[29] Im Jahr 2012 wurde CIWIN-AT initiiert, derzeit läuft der Pilotbetrieb. Der Roll-out für sämtliche Bundesländer wird voraussichtlich bis Ende 2014 abgeschlossen sein.

28 *https://ciwin.europa.eu/Pages/Home.aspx*

29 *https://www.onlinesicherheit.gv.at*

Schlussfolgerungen und Ausblick

In der Abschlussdiskussion betonten die Teilnehmer, wie gewinnbringend der dreitägige Austausch für alle Seiten war. Im Verlauf des Workshops konnten einige der wichtigsten aktuellen Fragen im Themenfeld Schutz Kritischer Infrastrukturen in einer sehr offenen Arbeitsatmosphäre kritisch und konstruktiv erörtert und Ansätze für die Weiterentwicklung der bestehenden Prozesse und Strukturen zum Schutz Kritischer Infrastrukturen diskutiert werden. Wie von mehreren Seiten hervorgehoben wurde, bestehen zwischen den drei teilnehmenden Staaten trotz zahlreicher Unterschiede in ihren Infrastruktur- und auch Bevölkerungsschutzsystemen viele Gemeinsamkeiten hinsichtlich gegenwärtiger und zukünftiger Herausforderungen im Bereich Kritische Infrastrukturen. Gerade weil die Arbeiten in einzelnen Aspekten zum Teil sehr unterschiedlich fortgeschritten waren und häufig auch verschiedene Wege eingeschlagen wurden, bietet das D-A-CH-Format eine wertvolle Möglichkeit für gegenseitiges Lernen. Aus diesem Grund begrüssten alle Teilnehmer, dass das erfolgreiche D-A-CH-Format bereits im April 2014 mit einem Workshop zu aktuellen Entwicklungen im Themengebiet Risikoanalyse im Bevölkerungsschutz in Bonn fortgesetzt wird. Darüber hinaus befürworteten die Teilnehmer, auch den trilateralen Austausch im Bereich Schutz Kritischer Infrastrukturen fortzusetzen. Der nächste D-A-CH-Workshop SKI soll im Jahr 2015 oder 2016 stattfinden.

Anhang I: Programm

1. Tag, Mittwoch, 4. Dezember 2013

Ab 12:30	*Eintreffen der Teilnehmer*
14:00 – 14:10	Begrüssung
	Stand der Arbeiten (Gegenseitiges und generelles Aufdatieren über den Stand der nationalen Programme)
14:10 – 14:40	Stand der Arbeiten in Österreich
14:40 – 15:10	Stand der Arbeiten in Deutschland
15:10 – 15:40	Stand der Arbeiten in der Schweiz
15:40 – 16:10	*Pause*
16:10 – 16:40	**Europäische und internationale Entwicklungen**
16:40 – 17:30	**Präsentation ausgewählter SKI-Projekte: Risikoanalysen, -matrizen und Übungen**
18:30	*Gemeinsames Nachtessen*

2. Tag, Donnerstag, 5. Dezember 2013

08:30 – 08:40	Begrüssung: Rückblick und Ausblick
	Identifizierung von kritischen Infrastrukturen
08:40 – 09:10	Methode und Umsetzung in der Schweiz
09:10 – 09:40	Methode und Umsetzung in Österreich
09:40 – 10:10	Methode und Umsetzung in Deutschland
10:10 – 10:40	*Pause*
10:40 – 11:00	**Erfassen von Interdependenzen und Berücksichtigung im Risiken- und Krisenmanagement (Diskussionsbeitrag D)**
11:00 – 11:20	**Ermittlung von Schutz- und Leistungszielen für kritische Infrastrukturen (Diskussionsbeitrag CH)**
11:20 – 12:00	**Diskussion und weiterer Erfahrungsaustausch**
12:00 – 13:30	*Mittagessen*
	Leitfäden und Vorgaben
13:30 – 13:55	Methode und Umsetzung in Deutschland
13:55 – 14:20	Methode und Umsetzung in Österreich
14:20 – 14:45	Methode und Umsetzung in der Schweiz
14:45 – 15:15	Diskussion und weiterer Erfahrungsaustausch
15:15 – 15:45	*Pause*
	Verhältnis SKI- zu Cyber-Risiko-Aktivitäten
15:45 – 16:15	Erfahrungen und Vorgehensweisen in der Schweiz
16:15 – 16:45	Erfahrungen und Vorgehensweisen in Deutschland
16:45 – 17:15	Erfahrungen und Vorgehensweisen in Österreich
17:15 – 17:45	Diskussion und weiterer Erfahrungsaustausch
19:00	*Gemeinsames Nachtessen*

3. Tag, Freitag, 6. Dezember 2013

08:30 – 08:35	Begrüssung: Rückblick und Ausblick
	SKI-Plattformen
08:35 – 09:00	SKI-Plattformen im Kontext öffentlich-privater Zusammenarbeit (Diskussionsbeitrag ETH Zürich)
09:00 – 09:25	CIWIN-AT als Infoplattform für APCIP
09:25 – 09:50	Diskussion und weiterer Erfahrungsaustausch
09:50 – 10:20	*Pause*
	Resilienz-Indikatoren
10:20 – 10:45	Resilienz-Indikatoren bei kritischen Infrastrukturen (Diskussionsbeitrag ETH Zürich)
10:45 – 11:10	Diskussion und Erfahrungsaustausch zu Resilienz-Indikatoren
11:10 – 11:30	**INNEN.SICHER.2013: Bewusstseinsbildung bei Betreibern KI (Diskussionsbeitrag A)**
11:30 – 12:00	**Fazit 3. D-A-CH SKI WS und weiteres Vorgehen**
12:00	Ende der Tagung
12:00 – 13:30	*Mittagessen und Abreise der Teilnehmer*

Anhang II: Teilnehmerinnen und Teilnehmer

Deutschland

Christine Eismann
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe BBK
Referentin Referat II.4 (Themen Stromversorgung)

Stefan von Holtey
Bundesministerium des Innern BMI
Leiter Referat KM4

Dr. Uwe Jendricke
Bundesamt für Sicherheit in der Informationstechnik BSI
Referent

Dr. Monika John-Koch
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe BBK
Leiterin Referat II.3 Grundsatzangelegenheiten Kritische Infrastrukturen

Andreas Kullmann
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe BBK
Referent Referat II.3 (Themen Cybersicherheit, Cyber-Abwehrzentrum)

Peter Lauwe
Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe BBK
Leiter Referat II.4 Gefährdungskataster, Schutzkonzepte Kritischer Infrastrukturen

Österreich

Günter Poßegger
Bundesministerium für Inneres BM.I
Leiter Abteilung II/BVT/3

Alexander Pschikal
Bundeskanzleramt BKA
Abt. IV/6

Helmut Schnitzer
Bundeskanzleramt BKA
Leiter Abt. IV/6

Beate Wegscheider
Bundesministerium für Inneres BM.I
Büro für Sicherheitspolitik

Schweiz

Ulrich Brandenberger
Bundesamt für Bevölkerungsschutz BABS
Wissenschaftlicher Mitarbeiter SKI

Stefan Brem
Bundesamt für Bevölkerungsschutz BABS
Chef Risikogrundlagen und Forschungskoordination

Ka Schuppisser
Informatiksteuerungsorgan des Bundes ISB
Koordinatorin Umsetzung Nationale Cyber-Risiken Strategie (NCS)

Nick Wenger
Bundesamt für Bevölkerungsschutz BABS
Programmleiter SKI

ETH Zürich – Center for Security Studies (CSS)

Michel Herzog
Center for Security Studies (CSS), ETH Zürich
Risk and Resilience Team

Tim Prior
Center for Security Studies (CSS), ETH Zürich
Leiter Risk and Resilience Team

Florian Roth
Center for Security Studies (CSS), ETH Zürich
Risk and Resilience Team

CSS
ETH Zurich

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