Bundesministerium
Finanzen

FFG
Forschung wirkt.

KIRAS
Sicherheitsforschung

# ISIDOR

## Folgen einer langandauernden und großflächigen Einschränkung der internetbasierten Dienste und Infrastrukturen


**Auftragnehmer**

Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik

Österreichische Akademie der Wissenschaften, Institut für Technikfolgen-Abschätzung

Infraprotect Gesellschaft für Risikoanalyse, Notfall- und Krisenmanagement GmbH

Mar Adentro e.U.

REPUCO Unternehmensberatung GmbH

**Bedarfsträger**

Bundesministerium für Inneres

Bundesministerium für Digitalisierung und Wirtschaftsstandort

**Autor:innen**

Larissa Schachenhofer

Manfred Gronalt

Jaro Krieger-Lamina

Helmut Pisecky

Gregor Konicar

Lars-Hendrik Hartwig

Wolfgang Czerni

Walter Peissl

Nico Schlauf

Hans Häuslmayer

Patrick Hirsch



Studie als Anhang zum Endbericht des Projekts im Programm KIRAS, FFG 879668

Wien, im November 2022

# Inhaltsverzeichnis

# Verzeichnisse

## Abbildungsverzeichnis



## Tabellenverzeichnis

# Executive Summary

Das Forschungsprojekt ISIDOR beschäftigte sich mit der Frage, was passiert, wenn das Internet in Österreich großflächig und für einen längeren Zeitraum ausfällt. Dabei wurden verschiedene Szenarien betrachtet, von Ausfällen bestimmter Internetdienste, bis hin zu einem Totalausfall. Dem „All Hazards"-Ansatz des Austrian Programme for Critical Infrastructure Protection (APCIP) folgend, standen nicht die Ursachen eines derartigen Ausfalls und deren Vermeidung im Fokus des Projekts, sondern das Augenmerk wurde auf den Bereich Cyber-Resilience gerichtet. Dabei galt es herauszufinden, wie sich die Lage nach einem Schadensfall entwickeln könnte, und wie die dadurch ausgelöste Krise bestmöglich gelöst werden könnte.

Anstoß für das Projekt war der entsprechende Arbeitsschwerpunkt im Staatlichen Krisen- und Katastrophenschutzmanagement. Es war klar, dass eine große Abhängigkeit von dieser Infrastruktur und Technik besteht. Es wurde aber bisher nicht im Detail untersucht, wie die Lage nach einem Ausfall in den verschiedenen Sektoren aussehen könnte, und welche sektorübergreifenden Fragestellungen sich daraus ergäben. Ziel des Projekts war es, einerseits Antworten auf diese Fragen zu finden und auszuloten, welche Maßnahmen in der Vorbereitung auf so eine Krise die Handlungsfähigkeit verbessern und den Impact im Ernstfall reduzieren würden. Andererseits wurde auch das generelle Verständnis für den Umgang mit vernetzten Krisen verbessert.

Das Projekt wurde im Rahmen des Sicherheitsforschungsförderprogramms KIRAS durch das Bundesministerium für Landwirtschaft, Regionen und Tourismus (später Bundesministerium für Finanzen) gefördert. Die Projektleitung lag beim Institut für Produktionswirtschaft und Logistik der Universität für Bodenkultur Wien. Weitere Projektpartner waren das Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften, das Bundesministerium für Inneres, das Bundesministerium für Digitalisierung und Wirtschaftsstandort, sowie die Firmen Infraprotect, Mar Adentro und Repuco.

## Ergebnisse

Wie sehr sind nun unterschiedliche Sektoren kritischer Infrastrukturen von einem Ausfall des Internets betroffen? Was voraussichtlich weiterhin funktioniert, ist die Versorgung mit Trinkwasser und die Entsorgung des Abwassers. Es ist auch zu erwarten, dass die Stromversorgung in Österreich zunächst nicht eingeschränkt wird, wiewohl es eine Ausnahmesituation für das Management der Netze darstellen würde, und eventuell weitere krisenhafte Ereignisse nicht ohne Weiteres ausgeglichen werden könnten.

Große Schwierigkeiten sind dort zu befürchten, wo IT-Prozesse und -Ressourcen im Normalbetrieb ausgelagert wurden. Das ist beispielsweise bei der Nutzung von Clouddiensten oder dem Outsourcing von IT-Personal der Fall. Ähnlich verhält es sich mit dezentralen, mobilen IT-Systemen, wie bspw. der Patientendokumentation im Rettungswesen. Stark betroffen wäre auch der Banken- und Finanzsektor, wo

viele Geschäftsprozesse ohne die Möglichkeit zur Datenkommunikation mittlerweile undenkbar sind.

Ein sektorübergreifendes Problem ergäbe sich aus der Betroffenheit des Transportwesens. Ohne Schnittstellen zur Datenkommunikation wäre der Transport von Gütern nur mit Einschränkungen möglich. Die Daten- und Dokumentationsverarbeitung, sowie das Transportmanagement (z.B. Sendungsverfolgung, Aviso, Einlagerung, Wiederauffinden, Zustellung etc.) sind in hohem Maße von miteinander vernetzten IT-Systemen abhängig. Gleichzeitig verlassen sich viele Organisationen darauf, dass z.T. mehrmals täglich – just in time – zugestellt wird, um kein großes Lager mit differenziertem Bestand betreiben zu müssen.

Durch die zu erwartenden Einschränkungen in der Mobilkommunikation, entweder durch Ausfall oder Überlastung des Mobilfunknetzes, ist davon auszugehen, dass oftmals Sicherheitstechnik nicht funktionieren wird: Alarmanlagen und Brandmelder, die direkt an Polizei oder Feuerwehr melden, wären ebenso wenig funktionsfähig wie Alarmierungen (z.B. von Krisenstäben) über Apps oder SMS.

Manches davon kann durch die Umstellung auf analoge Prozesse und erhöhten Personaleinsatz ausgeglichen werden, wenn das zuvor geübt wurde, und die notwendigen Ressourcen im Krisenfall zur Verfügung stehen.

## Vernetzte Krisen

Der Trend zu Konvergenz in der Infrastruktur und Effizienz in den Geschäftsprozessen führte in den vergangenen Jahrzehnten zu einer starken Reduktion von Puffern im Gesamtsystem. Dadurch steigt nicht nur allgemein die Abhängigkeit durch die voranschreitende Vernetzung, sondern es sinkt zugleich die Fehlertoleranz des Systems.

Durch die gegenseitigen Abhängigkeiten über sektorale Grenzen hinweg wird es kaum einen Bereich geben, der durch einen Ausfall internetbasierter Dienste nicht beeinträchtigt wäre. Ähnlich wie bei einem großflächigen Stromausfall spricht man auch hier von einer sogenannten ‚vernetzten Krise'. Letztendlich ist es auch mit viel Aufwand nicht möglich, genau vorherzusagen, wie die Lage nach so einem Schadensfall aussähe. Zielführender ist es, die Kräfte für das Krisenmanagement zu stärken und die First Responders in Trainings auf eine solche Situation vorzubereiten. Dadurch ließe sich die Handlungsfähigkeit im Ernstfall besser erhalten oder sogar erhöhen.

## Was ist zu tun?

Der Situation während eines großflächigen und lang andauernden Internetausfalls kann man auf verschiedenen Ebenen begegnen. Auszugsweise sind hier einige Handlungsempfehlungen aufgelistet; im Kapitel 9.1 findet sich eine umfangreichere Darstellung aller Empfehlungen:

- Der Ausfall des Internets oder wichtiger internetbasierter Dienste für einen langen Zeitraum ist in Österreich noch nicht vorgekommen. Dementsprechend fehlt es an Erfahrungswissen. Übungen für alle Organisationen, die in der Krisenbewältigung arbeiten, helfen dabei, die erforderlichen Kompetenzen für so einen Fall zu vermitteln und die Abläufe, die sich stark vom Regelbetrieb unterscheiden können, zu trainieren.
- Organisationsintern könnten KI-Betreiber strategische Überlegungen dazu anstellen, welche Prozesse im Ernstfall unabdingbar sind und sich auch offline erledigen ließen.
- In einigen Bereichen, z.B. Bargeld und Lebensmittellogistik, bedarf es weiterer Arbeit aller Stakeholder:innen, um einer robusten Lösung näher zu kommen.
- Speziell im Gesundheitswesen könnte es notwendig werden, krisenrelevante Versorgungsgüter in größerem Umfang dezentral zu bevorraten.
- Kommunikationswege, die von der fürs Internet genutzten Infrastruktur unabhängig sind, sollten bewahrt und ausgebaut werden, um in der Krise eine Kommunikation zwischen allen Beteiligten zu ermöglichen. Es gibt in Österreich schon einige Netze, die autark funktionieren können. Statt eines oft geforderten neu zu errichtenden Staatsgrundnetzes, wäre es leichter und günstiger, eine Ausfallslösung zu realisieren, die diese ‚Inseln' miteinander verbindet.
- Ebenso muss gewährleistet werden, dass der Kommunikationsaustausch auf internationaler Ebene und mit europäischen Institutionen auch während einer solchen Krise erhalten bleibt.
- Auf dem Gebiet der gemeinsamen Vorbereitung aller Akteure ist, nicht zuletzt im Rahmen des vorliegenden Projekts, in den vergangenen Jahren viel passiert. Eine weitere Vertiefung ist sinnvoll und wird von den Betreibern kritischer Infrastrukturen gewünscht. Auch weitere Forschung, aufbauend auf den Ergebnissen aus ISIDOR, ist erforderlich, um festzustellen, wo die Implementierung zukünftiger Technologien die Abhängigkeit vom Internet weiter erhöhen wird; bspw. im Feld autonomer Systeme.

# 1 Einleitung

Moderne Gesellschaften in den Industriestaaten sind durch die Digitalisierungsprozesse der vergangenen Jahrzehnte und eine fortschreitende Technologisierung des Alltags in eine immer stärker werdende Abhängigkeit von Technik im Allgemeinen und Informations- und Kommunikationstechnik (IKT) im Speziellen geraten. In spezifischen Bereichen ist eine moderne, digital vernetzte Gesellschaft besonders verwundbar. Auf Infrastrukturen bezogen spricht man hier von kritischen Infrastrukturen (KI), also von jenen Anlagen und Systemen, die eine große Bedeutung für die Aufrechterhaltung wesentlicher gesellschaftlicher Funktionen haben.

Durch Digitalisierungsprozesse sind auch diese kritischen Infrastrukturen heute im Wesentlichen von IKT abhängig und hochgradig vernetzt. Dies führt zu einer schon seit Jahren steigenden Anfälligkeit für Angriffe auf diese Infrastrukturen, die über Computernetze ausgeführt werden. Gleichzeitig sind die Betreiber kritischer Infrastrukturen Organisationen divergierender Größe und Ausstattung an Ressourcen zum Schutz dieser kritischen Infrastrukturen.

Cybervorfälle werden auch im aktuellen Jahr wieder als weltweites Top-Risiko vor Betriebsunterbrechungen und Naturkatastrophen bewertet (vgl. Allianz Global Corporate & Specialty SE 2022). Am 23. Juni 2021 gab etwa Salzburgmilch, die drittgrößte Molkerei Österreichs, bekannt, einem Cyberangriff zum Opfer gefallen zu sein, wodurch sämtliche IT-Systeme ausfielen. Alle Unternehmensbereiche der Molkerei, von der Produktion und Logistik bis zur Kommunikation, waren von dem Angriff betroffen, und die Produktion stand vorübergehend still (vgl. Lehmann 2021). Immer öfter sind auch Einrichtungen der öffentlichen Verwaltung von Cyberangriffen betroffen. Die Intensität solcher Angriffe steigt. Das zeigen unter anderem der am 24. Mai 2022 verübte Hackerangriff auf das Land Kärnten durch die Hackergruppe Black Cat mit Datendiebstahl und nachfolgender Lösegelderpressung (vgl. Der Standard 2022), sowie ein neuartiger Cyberangriff auf die Universität Salzburg Ende März 2022, der offenbar eine Rufschädigung der Universität zum Ziel hatte (vgl. Gruber 2022).

Gesellschaftliche Krisen können verschiedene Ursachen haben, von als ungleich empfundener Güterverteilung über politische Unruhen, Naturkatastrophen bis hin zum Ausfall eben jener Infrastrukturen, auf denen die Gesellschaft aufbaut. Nach dem Arbeitsschwerpunkt ‚Blackout' im österreichischen Staatlichen Krisen- und Katastrophenschutzmanagement (SKKM) wurde im Jahr 2019 beschlossen, als künftiges Referenzszenario den Fall einer langandauernden und großflächigen Einschränkung der internetbasierten Dienste und Infrastrukturen in Österreich auszuwählen. Da rasch klar war, dass es zu dem Thema deutlich weniger Forschung und daher auch veröffentlichtes Wissen gibt, als zum davor behandelten Thema Blackout, setzte sich das österreichische Staatliche Krisen- und Katastrophenschutzmanagement dafür ein, in einem Forschungsprojekt die Grundlagen für die weitere Bearbeitung des Themas zu schaffen. Als Ergebnisvorlage diente der sehr umfassende Bericht zu den Folgen eines Stromausfalls von Petermann et.al. (2011). In der Zusammensetzung des Projektkonsortiums wurde bereits die transdisziplinäre Ausrichtung

des Projekts festgeschrieben, die erforderlich ist, um die unterschiedlichen Wissensbestände zu erheben und nutzbar zu machen.

Ausgehend von einer massiven und großflächigen Einschränkung internetbasierter Dienste ist grundsätzlich zu befürchten, dass eine Kette von Versorgungsengpässen ausgelöst werden kann, die in weiterer Folge eine Gefahr für die öffentliche Ordnung darstellt. Aufgrund des hohen Vernetzungsgrades von Gesellschaft und Industrie spricht man daher im Zusammenhang mit einem möglichen Ausfall internetbasierter Dienste auch immer häufiger von vernetzten Krisen, die von einer hohen Komplexität aufgrund sektorübergreifender Wechselwirkungen sowie potenziell bislang unerkannter Wirkungszusammenhänge geprägt sein können. Diese gilt es zu analysieren, um ein besseres Verständnis vernetzter Krisen zu etablieren und damit eine Basis für adäquate Präventionsmaßnahmen im Vorfeld sowie effektive und effiziente Reaktionsmaßnahmen im Ereignisfall zu schaffen.

Die vorliegende Studie beschäftigt sich mit den Folgen einer langandauernden und großflächigen Einschränkung internetbasierter Dienste und Infrastrukturen. Für die Analyse wurde eine anwendungsorientierte Betrachtungsweise gewählt.

Ein Ausfall des Internets zeigt sich beispielsweise anhand einer merklichen Einschränkung bzw. dem gänzlichen Ausfall internetbasierter Dienste. Darunter werden im Folgenden sämtliche Dienste zusammengefasst, die sowohl Organisationen als auch Privatpersonen bei vorhandener LAN-, W-LAN Verbindung bzw. über mobile Daten, sowie einer ausreichend vorhandenen Bandbreite über das Internet zur Verfügung stehen. Beispiele sind etwa die Online-Suche über Suchmaschinen wie Google etc., digitale Finanzdienstleistungen (Online-Banking), die digitale Datenverwaltung und der Datenaustausch z.B. über Cloud-Dienste, sowie die gesamte digitale Kommunikation z.B. E-Mail, Messengerdienste (vgl. SBA Research GmbH 2017: 27-29).

Für österreichische Organisationen und die Bevölkerung in Österreich wurden die folgenden digitalen Dienstkategorien von der SBA Research GmbH identifiziert und zusammengefasst (siehe Tabelle 1: Kategorien internetbasierter Dienste (SBA Research GmbH 2017: S. 28-29)).

*Tabelle 1: Kategorien internetbasierter Dienste (SBA Research GmbH 2017: S. 28-29)*

| Privatpersonen | Unternehmen |
|---|---|
| Messaging und Kommunikation | Messaging und Kommunikation |
| Online-Dateiverwaltung & Dateiaustausch | Online-Dateiverwaltung & Dateiaustausch |
| Finanzdienstleistungen | Finanzdienstleistungen |
| Soziale Medien & Netzwerke | Soziale Medien & Webauftritt |
| Online-Suche | Internetgestütztes Enterprise-Resource-Planning |
| Mobilität & Reisen | Internetgestütztes Supply-Chain-Management |
| Video/Musik | Internetgestütztes Customer-Relationship-Management |
| Behördenwege | |
| Einkauf | |
| Informationsmedien | |
| Gaming Dienste | |
| Netzwerkdienste | |
| Internet der Dinge | |

Charakteristisch für ISIDOR ist, dass Prozesse erst ab dem Eintritt eines solchen Ereignisses untersucht werden, wobei sowohl die Auswirkungen einer partiellen Einschränkung (z.B. starker Abfall der Bandbreite), als auch ein vollständiger Ausfall internetbasierter Dienste analysiert wurden. Die Betrachtungsweise erfolgte dabei möglichst ursachenunabhängig unter Anwendung des „All Hazards“-Ansatzes des SKKM gemäß des Österreichischen Programmes zum Schutz kritischer Infrastrukturen (APCIP). Dabei wurde von einem Ausfallsereignis ausgegangen, welches zumindest weite Teile des Bundesgebietes betrifft (jedenfalls den Ballungsraum im Osten des Landes) und mindestens drei Tage andauert.

Daneben wurden bei verschiedenen Gelegenheiten auch andere Situationen betrachtet, die eine Einschränkung der Verfügbarkeit internetbasierter Dienste darstellen würden. So sind Bandbreitenreduktion, Erhöhung der Latenz, Vertrauensverluste (vermutete Kompromittierung einzelner Dienste oder Infrastrukturen, oder ein Ausfall im Bereich der Zertifikatsinfrastruktur), sowie der Ausfall einzelner, zentraler Dienste (bspw. DNS: Ausfall, DNS-Poisoning, Aufbrechen der Zonen-Synchronisierung usw.), auch für einen kürzeren Zeitraum, ebenfalls Themen der Betrachtungen gewesen.

Zentrale Aspekte bildeten im Rahmen dessen das Aufzeigen potenzieller Rückkopplungseffekte innerhalb unterschiedlicher Sektoren der kritischen Infrastruktur (KI),

sowie die Identifikation von Handlungsmöglichkeiten des SKKM auf Basis der erstellten Modelle und systemischen Abhängigkeiten.

Die Analyse von Gründen für den Eintritt eines großflächigen und langandauernden Ausfallsereignisses war nicht Teil der Aufgaben, die im Rahmen von ISIDOR definiert wurden. Dennoch hat sich während der Arbeit an den Themen herausgestellt, dass mögliche Gründe auch ohne nähere Betrachtung mitzudenken sind, wenn es um die Lageeinschätzung nach einem Schadensfall geht. Zu unterschiedlich sind die möglichen Ursachen, und damit auch die für die Krisenbewältigung verfügbaren Ressourcen, um diesen Aspekt gänzlich unbeachtet zu lassen. Auch die Erarbeitung von Maßnahmen aus dem Bereich Cyber-Security bzw. Netz- und Informationssicherheit, sowie die Ermittlung von Pflichten, die sich aus dem Netz- und Informationssicherheitsgesetz (NIS-Gesetz) ergeben, waren nicht Teil des Projektes.

In ISIDOR stand eine Verschränkung von interdisziplinärer, wissenschaftlicher Arbeit mit verschiedenen Perspektiven aus der Praxis im Fokus. Das Zusammenbringen wissenschaftlicher Erkenntnisse mit implizitem und explizitem Wissen von Expert:innen (auch aus dem Bereich der Bedarfsträger) spielte im Projekt eine entscheidende Rolle. Zu diesem Zweck wurden Vertreter:innen des staatlichen Krisen- und Katastrophenschutzmanagements, KI-Betreiber, Vertreter:innen der Länder und KI-Sektoren, sowie weitere relevante Stakeholder:innen regelmäßig eingebunden. Dies stärkte den gegenseitigen Austausch und setzte einen iterativen Prozess in Gang, in dem Forschung und Praxis kontinuierlich voneinander lernten. Wissenschaftliche Analysen wurden dabei um relevante, praktische Aspekte ergänzt und Einwände aus der Praxis wurden anhand von Erkenntnissen aus der Wissenschaft besprochen und kritisch hinterfragt. Der intensive Austausch im Rahmen zahlreicher Gespräche und Diskussionen, die während des Projektes ISIDOR zwischen Praktiker:innen und Wissenschafter:innen stattgefunden haben, gewährleistet somit relevante und aktuelle Forschungsergebnisse.

Aufgrund der Digitalisierungsprozesse auf verschiedenen Ebenen und der damit einhergehenden, zunehmenden Abhängigkeit von wesentlichen, internetbasierten Diensten sind die Forschungsergebnisse des Projektes sowohl für die Wirtschaft als auch die Gesellschaft und die öffentliche Verwaltung höchst relevant. Das Projekt förderte darüber hinaus die Vermittlung von Bewusstsein für die prinzipielle Kritikalität und Verletzbarkeit bestimmter Systeme. Über die Öffentlichkeitsarbeit in ISIDOR sowie die zielgruppenspezifische Aufbereitung relevanter Ergebnisse für Kommunikationszwecke wurde insbesondere die Sensibilität für vernetzte Krisen und deren potenzielle Auswirkungen auf Wirtschaft, Gesellschaft und Politik gestärkt. Durch den Austausch mit den Praxispartner:innen (im Rahmen der Stakeholder:innen-Workshops etc.) konnten auch die Vertreter der öffentlichen Verwaltung ihren Beitrag zur Schaffung einer umfassenden Strategie darstellen. Unter Einbindung des SKKM, der KI-Betreiber, der Länder usw. tragen die Ergebnisse des Projektes damit maßgeblich zur Weiterentwicklung des Resilienz-Managements im Jahr 2022 sowie den kommenden Jahren bei.

*Die vorliegende Studie gliedert sich wie folgt:*

Kapitel 1 erläutert den Problemhintergrund und die Zielsetzung des Projekts sowie die Relevanz für die einzelnen Zielgruppen. Kapitel 2 befasst sich mit Vorprojekten und parallel laufenden Arbeiten. In Kapitel 3 wird der Forschungsstand erläutert, der auf den Ergebnissen der Literaturanalyse beruht. In Kapitel 4 sind Überlegungen zu möglichen Ursachen und dem in ISIDOR gewählten „All Hazards“-Ansatz zu finden. In Kapitel 5 werden die verschiedenen Methoden, die während des Projektes zum Einsatz kamen, erklärt. Kapitel 6 stellt Modelle vor, deren Fokus auf Verlagerungsschleifen liegt, die bei einem Ausfall internetbasierter Dienste in Kraft gesetzt werden können, und potenziellen Abhängigkeiten, die sich anhand der Modelle gezeigt haben. Definierte Anwendungsfälle ergänzen dieses Kapitel mit verschiedenen Perspektiven aus der Praxis. Kapitel 7 betrachtet verschiedene sektorale Abhängigkeiten. In Kapitel 8 werden ergänzend offene Fragen und Themenkomplexe dargestellt, die Anknüpfungspunkte für weitere Forschung in diesem Bereich sein können. In Kapitel 9 folgen Handlungsempfehlungen, die sich aus der Projektarbeit ableiten ließen.

# 2 Vorprojekte und parallele Arbeiten

Die Literaturrecherche in der Antragsphase und vertiefend später, zu Beginn des Projekts, zeigte auf, dass das Thema eines großflächigen und langanhaltenden Ausfalls des Internets bisher kaum wissenschaftlich erforscht worden war. Umso wichtiger war es daher, einen größeren Überblick über parallele und bereits abgeschlossene Projekte zu erhalten, die sich mit relevanten Fragestellungen, jedoch anderen Schwerpunkten, auseinandersetzten. Insbesondere Studien zum Thema Blackout bildeten dabei einen wichtigen Ansatzpunkt, da hier ebenfalls systemische Auswirkungen von vernetzten Krisen erhoben wurden.

## 2.1 TAB-Studie zum Blackout in Deutschland als Schablone

Ausgangslage für die ISIDOR-Studie waren ähnliche Überlegungen zum langfristigen Ausfall bzw. einer Unterversorgung mit einem ähnlich relevanten Element der modernen Versorgung: einem Blackout oder einem langanhaltenden Stromausfall.

Eine zentrale Arbeit zu diesem Thema liegt in Form der Studie des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag von 2011 vor. Im Auftrag des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung befassten sind Petermann et. al. (2011) mit den Folgen eines langandauernden und großflächigen Stromausfalls und den Möglichkeiten und Grenzen des nationalen Systems des Katastrophenmanagements zur Bewältigung einer solchen Großschadenslage.

Die Studie befasst sich dabei nur am Rande mit den möglichen Auslösern eines Blackouts, und konzentriert sich stärker auf die Auswirkungen eines solchen Schadensfalls für verschiedene Bereiche der kritischen Infrastruktur (Informationstechnik und Telekommunikation, Transport und Verkehr, Wasserversorgung und Abwasserentsorgung Lebensmittelversorgung, Gesundheitswesen, Finanzdienstleistungen und Öffentliche Einrichtungen am Fallbeispiel »Gefängnis«). Für jeden dieser Bereiche werden die jeweiligen Vulnerabilitäten, Bewältigungsoptionen und der gegebene Handlungsbedarf ermittelt. Hinzu kommen themenübergreifende verhaltensbezogene Folgen eines Stromausfalls, die es für ein erfolgreiches Krisenmanagement und zu berücksichtigen gilt.

Während sich die konkreten Verletzbarkeiten und Bedrohungen, die durch einen Blackout entstehen, von denen im Rahmen eines Internetausfalls unterscheiden, sind es vor allem die konzeptionellen Überlegungen der Studie und die Erkenntnisse zur Komplexität der entstehenden Folgewirkungen mit dem Stromausfall als ein „Paradebeispiel für kaskadierende Schadenswirkungen“ (S.31) für die Teilbereiche der kritischen Infrastruktur und die Gesamtheit einer staatlichen Organisationseinheit, die wesentliche Grundlagen für die ISIDOR-Studie liefern konnten.

## 2.2 Digitaler Atlas Österreich

Der Digitale Atlas Österreich und sein Folgeprojekt, der Digitale Atlas Österreich 2.0, beschäftigten sich mit der Beschaffenheit der Internets in Österreich auf seinen drei relevanten Ebenen: der physischen Leitungen, des logischen Datenflussverlaufs und

der internetbasierten Anwendungen und Dienste. Forschungsziel der beiden Studien war es, jeweils die bestehenden Strukturen aufzuzeigen und relevante Erkenntnisse für Kritikalität oder Bedrohungspotenzial abzuleiten.

Im Digitalen Atlas Österreich wurde die Ebene der physischen Leitungen und des logischen Datenflussverlaufs in Österreich näher betrachtet. Dabei wurde mittels Tracerouting untersucht, wie der Datenverkehr in Österreich verteilt ist, und inwiefern Abhängigkeiten vom Ausland oder ausländischen Unternehmen (in Form der Internet-Service-Provider) bestehen. Die Studie gelangte zu mehreren relevanten Ergebnissen: Das Internet in Österreich ist insgesamt wenig störungsanfällig, sondern redundant aufgebaut. Nicht einmal der zentrale Knotenpunkt VIX (Vienna Internet Exchanges) ist essenziell; das Internet würde über die von TIER 3 zur Verfügung gestellten Netze funktionsfähig blieben, auch wenn einzelne Internet Service Provider ihre Dienste nicht mehr anbieten könnten. Das logische Tracerouting zeigte auf, dass die innerösterreichische Kommunikation nicht vom Ausland abhängig ist und nur ein verhältnismäßig kleiner Teil über das Ausland läuft. Auch wenn für Kommunikationsfunktionen das Ausland nicht benötigt wird, wird dennoch ein maßgeblicher Teil des abrufbaren Contents im Ausland liegen. Wäre Österreich vom ausländischen Internet abgeschnitten, würde das österreichische Internet demnach rein technisch noch funktionieren, aber es wäre nicht mehr das Internet in der derzeit gewohnten Form. Es ist nicht ersichtlich, wo physische Leitungen das österreichische Staatsgebiet tatsächlich verlassen und inwiefern daher auch die innerösterreichische Kommunikation von ausländischer Infrastruktur tatsächlich abhängig ist. Allerdings ist die Abhängigkeit vom Ausland schon in Bezug auf die Eigentumsverhältnisse der ISPs gegeben: Wirklich ‚österreichisch', also unter der Kontrolle österreichischer Staatsbürger:innen stehend, sind nur kleine Internet Service Providers (ISPs). Die wichtigsten ISPs sind maßgeblich vom Einfluss ausländischer natürlicher und juristischer Personen geprägt.

Die Folgestudie, der Digitale Atlas Österreich 2.0, beschäftigte sich mit internetbasierten Diensten und ihrer Bedeutung für die Bevölkerung und Unternehmen. Im Rahmen von repräsentativen Umfragen sowie Expert:innenbewertungen wurde die Kritikalität der Dienste (u.A. Häufigkeit der Nutzung, Möglichkeit zum Wechsel) abgefragt und evaluiert: Generell zeigt sich, dass die Privatbevölkerung in Österreich offen gegenüber der Nutzung von Online-Services ist, selbst für sensible Angelegenheiten wie Finanzgeschäfte und Behördenwege. Über Alternativen zu den genutzten Diensten ist die Bevölkerung gut informiert und kann im Falle eines Aus- oder Wegfalls eines Dienstes meist ohne Probleme ausweichen. Im Privatbereich ergeben sich damit keine strategischen Abhängigkeiten im Zusammenhang mit den untersuchten Diensten. Die Unternehmen in Österreich weisen in einigen Bereichen bzw. Dienstkategorien Abhängigkeiten auf. Dies betrifft vor allem die Zahlungsabwicklung und Banking, Kommunikationsdienste und Enterprise-Ressource-Management sowie die Bereiche Werbung, Öffentlichkeitsarbeit und Kundenkontakt. Die Abhängigkeiten dort beruhen darauf, dass ein Ausfall nicht schnell durch den Wechsel auf einen anderen Dienst kompensiert werden kann.

Die Ergebnisse der KIRAS Studien waren zum einen für eine Einordnung der Wahrscheinlichkeit eines Ausfall-Szenarios hilfreich, auch wenn dies nur ein Randbereich

der Studie war. Relevanter waren die Überlegungen zur Kritikalität der Dienste und der Auswirkungen des Ausfalls, vor allem im Finanz- und Payment-Bereich, der Datenspeicherungs- und Cloud-Systeme sowie staatlicher Register.

## 2.3 Digitaler Stillstand

Ob Energie, Wasser, Infrastruktur oder Kommunikation – Güter und Dienstleistungen werden durch IT-Systeme gesteuert. Dadurch wird ein Maß an Effizienz und Effektivität erreicht, das ohne Technik nicht vorstellbar wäre. Eine Begleiterscheinung dieser Technisierung sind jedoch eine zunehmende Komplexität und gesellschaftliche Abhängigkeit von diesen IT-Systemen.

Das Projekt „Digitaler Stillstand“ ging der Frage nach, was passiert, wenn alle oder ein Großteil dieser Systeme nicht mehr funktionieren. Verschiedene Szenarien sollten demonstrieren, welche Ursachen zu einem Ausfall der Versorgung und Kommunikation führen könnten. Für viele Katastrophenfälle gibt es Notfallpläne der einzelnen Infrastrukturbetriebe und der zuständigen staatlichen Stellen. Aber wie ist Österreich auf die konkreten Auswirkungen dieser Szenarien vorbereitet? In unterschiedlichen Bereichen des gesellschaftlichen Lebens sind verschiedene Rahmenbedingungen zu berücksichtigen. Nach der Analyse der Einschätzungen von Expert:innen zu diesen Fragen wurden in dem Projekt, unter Einbeziehung verschiedener Stakeholder:innen, Empfehlungen entwickelt. Die Arbeiten dazu fanden auf abstrakter, systemischer Ebene mit Beispielen aus der Praxis statt.

ISIDOR profitierte nicht nur von den in diesem Projekt erarbeiteten Erkenntnissen, sondern auch von der Vernetzung zwischen den Projektpartnern und den Betreibern kritischer Infrastrukturen, was insbesondere in der Phase der Interviews hilfreich war. Auf den Ergebnissen aus dem Projekt „Digitaler Stillstand“ aufbauend konnte in ISIDOR weiter in die Tiefe gearbeitet, und so der für das SKKM nötige Detailierungsgrad erreicht werden.

## 2.4 Nutrisafe

Das bilaterale (Deutschland und Österreich) KIRAS-Projekt NutriSafe erforschte den Einsatz von Distributed Ledger Technologie (DLT) in der Lebensmittelproduktion, sowie die Resilienz von Lebensmittelwertschöpfungsketten im Krisenfall. DLT ist gemäß Scherk und Pöchhacker-Tröscher (2017, 12) eine „öffentliche, dezentral geführte Datenbank (…), welche über ein Netzwerk von verschiedenen Teilnehmer:innen geteilt wird“. Das deutsche Projektteam fokussierte auf kleinere Sicherheitsvorfälle aus dem Bereich Lebensmittelsicherheit (Food Safety). Das österreichische Konsortium hingegen betrachtete Großereignisse, welche die Versorgung der Bevölkerung weitreichend beeinträchtigen können (Food Security).

Die Einsatzmöglichkeiten von DLT und Anforderungen an diese zur Erhöhung der Resilienz von Lebensmittelwertschöpfungsketten sowie Potentiale, Risiken und Auswirkungen dieser Technologie standen im Mittelpunkt der Forschung. Die DLT wird als Datenstruktur verstanden, die mehrere Computer und Standorte umfasst. Block-

chain stellt eine Unterkategorie der DLT dar (Steidl und Wenz 2022). Der Unterschied zwischen der DLT und Blockchain liegt in der Art der Datenspeicherung, weshalb nicht jede DLT synonym als Blockchain bezeichnet werden kann. Im Projekt Nutrisafe wurde die DLT herangezogen, um eine Blockchain aufzubauen. Blockchain kann, für die Rückverfolgung von Produkten, Bestandsüberwachungssysteme oder auch die allgemeine Sicherung von Daten sowie deren Sicherstellung von Integrität und Verfügbarkeit eingesetzt werden.

Im Rahmen des österreichischen Projektteams wurden anhand mehrerer Use Cases die Versorgungssicherheit in Krisenfällen analysiert und Handlungsempfehlungen abgeleitet. Krisenszenarien wie etwa Störungen in der Lieferkette, z.B. durch Tierseuchen, Pandemien, oder Ressourcenengpässe, wurden dabei aufgegriffen und untersucht.

Die identifizierten Krisenszenarien in den Wertschöpfungsketten der Use Cases Trinkmilch, Speisekartoffel und Schweinefleisch trugen maßgeblich dazu bei, kritische Infrastrukturelemente zu eruieren und relevante Zusammenhänge sichtbar zu machen.

Die konkreten Krisenszenarien wurden mit unterschiedlichen interdisziplinären Methoden (z.B. qualitative und quantitative Sozialforschung, System Dynamics, Optimierungsheuristiken oder computergestützte Simulation) analysiert. Aus den Simulationsmodellen konnten beispielsweise wesentliche Erkenntnisse zur zukünftigen Vorgehensweise in Krisenfällen und dem Handlungsbedarf abgeleitet und präzise Handlungsempfehlungen gegeben werden. Die aus dem Projekt hervorgegangenen Ergebnisse zu relevanten Abläufen in Krisen fanden Eingang in die ISIDOR-Studie und ergänzten diese entsprechend.

## 2.5 Resilienz Monitor Austria (Re.M)

Ziel des KIRAS-Projektes „Re.M“ war die Schaffung eines Resilienz-Monitors für ganz Österreich. Resilienz bezeichnet in diesem Zusammenhang die Kapazität eines Akteurs, mit Störungen und Krisen umzugehen und durch Adaption und soziales Lernen neue Funktionsleistungen zu kreieren, falls eine Rückkehr in den vorherigen Normalzustand nicht möglich ist.

Die Fähigkeit, rasch reagieren zu können, Schocks abzufangen und sich in Krisen weiterzuentwickeln, hängt unmittelbar mit der Struktur der Netzwerke jener Personen und Organisationen zusammen, die mit der Krise und deren mittelfristigen Folgen fertig werden müssen. Je mehr und je schneller getrennte Gruppen im Krisenfall miteinander interagieren und sich abstimmen können, desto höher ist die Fähigkeit eines Systems, sich auch unter Stress weiterzuentwickeln, zu improvisieren und zu lernen.

In dem vorliegenden Projekt ging es konkret um die softwaregestützte Messung und das Monitoring genau jener gesellschaftlichen Basisbedingungen, die für die Resilienz eines sozioökonomischen Systems von maßgeblicher Bedeutung sind. Das System, an dem dies dargestellt werden sollte, war das sozioökonomische und kulturelle System Österreichs.

Im Rahmen einer diesem Projekt vorangehenden Erhebung der bestehenden Ansätze der Resilienzforschung wurde eine relevante Forschungslücke erkannt und ein Beitrag zu deren Schließung geleistet: Die bisherigen Studien verfolgten in der Mehrheit einen Top-Down-Ansatz, in dem die Erfahrungen und das implizite Wissen von Key Stakeholder:innen nur ungenügend berücksichtigt wurden. Dies führt zu einer Reihe von Problemen, insbesondere bei der Anwendung der vorgeschlagenen Messmodelle für (gesellschaftliche) Resilienz. Aufgrund der mangelnden Unterstützung wichtiger Stakeholder:innen bleiben oft die Filterkriterien – welche Indikatoren nun in die Indexbildung ihren Eingang finden und welche nicht – in gewissem Sinne anfällig gegenüber politischer Interpretation.

Die konzeptionellen Arbeiten zum Bereich der Resilienz-Forschung sowie die Überlegungen zur (gesellschaftlichen) Resilienz und der Vernetzung der einzelnen Subsysteme einer gesamtheitlichen Organisationseinheit waren hilfreiche Grundlagen, die bei der Ausarbeitung der ISIDOR-Studie berücksichtigt werden konnten.

# 3 Forschungsstand

In diesem Kapitel werden die Ergebnisse der ausführlichen Literaturrecherche gegliedert nach Themenbereichen zusammengefasst.

## 3.1 Ausfallsursachen

In der Literatur finden sich, je nach Betrachtungsebene, zahlreiche verschiedene und teilweise überlappende Klassifikationen der Ursachen von Internetausfällen. Am erfolgsversprechenden erscheint ein multidimensionaler Ansatz, wie z.B. in Aceto et al. (2018) vorgeschlagen, der sich in Ursache und Ebene gliedert:

### 3.1.1 Ursache

*Natürlich vs. menschengemacht:* Zu den natürlichen Ursachen gehören beispielsweise Erdbeben oder Tsunamis, die Land- oder Unterseekabel beschädigen oder trennen, ebenso aber auch koronale Massenauswürfe der Sonne oder andere Störungen im Weltraumwetter. Bei den durch Menschen verursachten Störungen ist zusätzlich zwischen beabsichtigt und unbeabsichtigt zu unterscheiden – so kann es etwa im Zuge von Bauarbeiten oder bei der Instandhaltung zu unbeabsichtigten Störungen oder Beschädigungen kommen. Das Hauptaugenmerk der Forschung liegt aber auf intentionalen Angriffen und Bedrohungen, wie Wurminfektionen durch Stuxnet oder Slammer, wobei meist entweder die Kontroll- und Steuermechanismen angegriffen werden, oder die Kommunikation unmöglich gemacht wird, indem das System mit Anfragen überhäuft wird (DOS; DDOS) (Maglaras et al. 2018).

Im letzten Jahrzehnt haben Betreiber ursprünglich isolierte Systeme im Bereich der autonomen Steuerungsanlagen – Stichwort SCADA – zwecks einfacherer Kommunikation und schnellerer Reaktion vermehrt ans Internet angebunden. Dies eröffnet einerseits neue Angriffsvektoren auf Industrieanlagen und ermöglicht andererseits die Infiltration und den Einsatz der verwundbaren Anlagen für systemweite Angriffe. Eine besondere Rolle in diesem Kontext spielt auch das iIoT (industrial Internet of Things), das, ebenso wie das IoT selbst, in vielen Fällen nur extrem schlecht gegen Angriffe abgesichert ist (Simon 2017).

### 3.1.2 Ebene

*Primär physisch oder logisch:* Im Gegensatz zu Schäden durch Erdbeben oder getrennte Unterseekabel, die primär physischen Schaden verursachen, sind auch Internetausfälle durch Ursachen auf logischer Ebene möglich: einerseits wieder unbeabsichtigte Ursachen wie Softwarefehler, unerwartete Trafficspikes oder Fehlkonfigurationen von Routing-Elementen, andererseits auch intentional herbeigeführt wie DDOS-Attacken oder geplanten Abschaltungen durch meist autoritäre Regime (Aceto et al. 2018).

## 3.2 Ausfallserkennung

Ein wesentlicher Punkt in der Forschung ist die frühzeitige und möglichst umfassende Erkennung von Internetausfällen. Dies ist einerseits für eine Behebung der Ursache und eine Minimierung der verursachten Schäden von großer Bedeutung, andererseits ist die Erkennung und Dokumentation von Internetausfällen auch für die Forschung selbst essenziell. Es werden passive, aktive und hybride Ansätze unterschieden.

*Passiv:* Zahlreiche elektronische Geräte wie Smartphones oder SmartTVs senden regelmäßige, nicht von Benutzern getriggerte Abfragen an CDN-Server – ein Effekt, der als baseline Activity bezeichnet wird. Fallen diese Anfragen bei vielen Devices im selben oder in benachbarten Adressblöcken temporär weg, dann deutet dies zumindest auf eine Störung hin (Richter et al. 2018). Passive Ausfallserkennung kann sowohl auf Kontrollebene erfolgen, üblicherweise über BGP-Nachrichten, oder auf der Datenebene, wo zwischen kern- und kantenbasierten Ansätzen unterschieden wird. Massive Probleme bei passiver Ausfallserkennung gibt es mit der Reliabilität und der Interpretierbarkeit: Nur 20-25% der Störungen, die vermutlich mit Ausfällen verbunden sind, sind allein durch BGP-Nachrichten-Beobachtung sichtbar. Umgekehrt führen ca. 15% der Störungen zu BGP-Verdachtsmomenten, auch wenn sie nicht direkt mit Internetausfällen zu tun haben, sondern z.B. nur durch Neu-Zuteilung von IP-Adressen entstehen (Richter et al. 2018). Auch ist praktisch allen passiven Ansätzen ein Datenschutzproblem gemein, da in großem Maßstab Metadaten ohne Kenntnis oder Zustimmung von User:innen verwendet werden.

*Aktiv:* Aktive Internet-Ausfallserkennung wie Trinocular (Quan et al. 2013) basiert meistens auf ping und traceroute – ausgewählte Ziele werden in regelmäßigen Abständen kontaktiert und basierend auf deren Antwort (oder dem Ausbleiben einer solchen) wird die dazwischenliegende Strecke als funktional oder gestört klassifiziert. Um eine möglichst umfassende Übersicht über den aktuellen Zustand des Netzes zu bekommen, ist es allerdings nötig, eine Vielzahl von Geräten zu kontaktieren – ein Ansatz, der nur schwer skalierbar ist. Allein der Einsatz von Trinocular hat zu einer Erhöhung der „Hintergrundstrahlung des Internets“, der Summe aller nicht angeforderten Nachrichten von 0,7% geführt (Aceto et al. 2018).

*Hybrid:* Kombinierte Systeme wie Hubble oder Argus setzen auf passives Monitoring von BGP-Nachrichten und starten erst bei Entdeckung von Auffälligkeiten mit aktiver Ausfallserkennung (üblw. wieder Ping und Traceroute). Durch diesen Ansatz kann die Belastung des Netzes massiv reduziert werden (minus 94,5% Traffic bei Hubble), ohne die Erkennungsrate nennenswert zu reduzieren (Katz-Bassett et al. 2008).

## 3.3 Schweregrad des Ausfalls

Bei der Definition des Schwergrades eines Internetausfalles gibt es im Wesentlichen zwei Ansätze.

*Benutzer:innen-zentriert:* Der Schweregrad des Ausfalls soll durch Abschätzen der Bevölkerungszahl, die von den gestörten Routen betroffen ist einerseits und durch ein Hochrechnen der betroffenen Geräte, die durch aktive Ausfallserkennung nicht

mehr erreicht werden können andererseits ermittelt werden. Dieser Ansatz sieht den Fokus zwar bei dem einzelnen Anwender bzw. der einzelnen Anwenderin (oder dessen bzw. deren Geräten), lässt aber außer Acht, dass dessen bzw. deren Erwartung an die Internetverbindung kein binäres „funktioniert/funktioniert nicht“ darstellt, sondern dass auch andere Faktoren wie Latenz, Bandbreite, etc., eine wesentliche Rolle spielen.

*Netzwerk-zentriert:* Häufig wird zur Bestimmung des Schweregrades ein Vergleich des Netzwerkes vor dem Ausfall, währenddessen und danach herangezogen. Je nach Untersuchungsfokus kommen unterschiedliche Metriken zum Einsatz: Zahl der gestörten Verbindungen, Auslastung von alternativen Routen, Länge alternativer Routen, veränderte Lastverteilung an Knotenpunkten, Verhältnis verlorener Pakete zu verzögerten Paketen etc. Dieser Ansatz scheint durch den direkten Vergleich des Netzes vor dem Ausfall und danach gut geeignet, viele Aspekte abzubilden, die der User:innen-zentrierte Ansatz nicht berücksichtigt. Er setzt aber die Fähigkeiten zur detaillierten Erhebung und Modellierung des Netzzustandes voraus, was schon allein aufgrund kaum kartographierbarer Bereiche wie des Darknets in den meisten Szenarien äußerst schwerfällt (Aceto et al. 2018).

## 3.4 Risikobewertung

Es gibt zahlreiche Studien zur Risikobewertung kritischer Infrastruktur (z.B. im Energiesektor Giannopoulos et al. 2013), allerdings recht wenige mit Bezug zum Internet als System. Untersuchte Teilaspekte sind beispielsweise Datencenter, wo der Fokus oft auf einer optimalen geographischen Anbindung liegt (Engemann/Miller 2017) und Cloudcomputing (Miller/Engemann 2019). Risikoforschung von IP-Netzen beschäftigt sich mehr mit der Planung von Netzten und der Risikominimierung bei ihrer Konzeption (z.B. Minimierung des maximalen Schadens, Minimierung der maximalen Eintrittswahrscheinlichkeit) als mit der Analyse bestehender, heterogener Netze. Zusätzlich zu ihrer Komplexität und historisch gewachsenen Eigenheiten haben Risikobewertungsstudien von realen Netzen üblicherweise nur eine sehr begrenzte lokale und zeitliche Gültigkeit, da die Risiken meist situationsabhängig sind. Der Fokus liegt außerdem in der Regel auf klar definierten Ausfallsursachen, nicht auf dem Gesamtrisiko für ein Netzwerk (Aceto et al. 2018).

## 3.5 Gegenmaßnahmen

Als verbreitetste Gegenmaßnahme wird häufig Redundanz gesehen – sowohl auf der physischen Ebene, als auch auf der Ebene der Netzwerktopologie. Dieser Ansatz hat zwei Schwachstellen: Er ist einerseits kostenintensiv, da im Normalfall ungenutzte Infrastruktur angeschafft und betrieben werden muss, andererseits ist Redundanz üblicherweise nur bei Szenarien mit punktuellen Störungen erfolgsversprechend, nicht aber bei systemweiten Ausfällen/Angriffen.

Verbindungspriorisierung bezeichnet den Ansatz, den Fokus auf einige wichtige Verbindungen zu legen, die so weit als möglich verstärkt und abgesichert werden, um auch unter Krisenbedingungen operabel zu sein.

Wiederherstellungsmaßnahmen unterscheiden sich in proaktive und reaktive Maßnahmen: Bei reaktiver Wiederherstellung wird auf Netzwerkausfälle reagiert, indem z.B. die Routinginformationen angepasst werden und um beschädigte Netzbereiche herumgelotst wird. Dies kann, je nach Schwere des Ausfalls, einige Zeit dauern, zumal Protokolle wie BGP eher langsam sind, weshalb häufig proaktive Ansätze Anwendung finden: Bei diesen werden bereits im Vorfeld gewisse Störungen und Ausfälle angenommen und entsprechende Reaktionen vorbereitet, die im Eintrittsfall dann direkt zur Anwendung gelangen können. Ausfälle, auf die das System nicht vorbereitet ist, können durch proaktive Maßnahmen oft nicht abgefangen werden, was erneut die Wichtigkeit der erfolgreichen Ausfallserkennung und der Identifikation des Ausmaßes des Ausfalles und des betroffenen Netzes an sich unterstreicht. Andererseits kann es bei schweren Netzwerkschäden dazu kommen, dass reaktive Wiederherstellungsmaßnahmen das Problem vergrößern, indem sie zu kaskadierenden Ausfällen führen (Wang et al. 2011).

Progressive Wiederherstellungsmaßnahmen beschäftigen sich mit der Priorisierung bei der Wiederherstellung von Netzwerken. Zum Einsatz kommen meist heuristische Algorithmen, die als wesentlichste Metrik die Verbindungskapazität einzelner Elemente betrachten (Henry/Ramirez-Marquez 2012).

Abgesehen von der physischen Ebene zeigt die Literatur zahlreiche Ansätze auf höheren Ebenen auf – so auf der Sicherungsschicht (MPLS-FRR), der Vermittlungsschicht oder Anwendungsschicht (Resilient Routing Reconfiguration, LifeGuard, RiskRoute, GIRO) siehe z.B. (Eriksson et al. 2013).

Resilinets (Sterbenz/Hutchison 2006) bezeichnet eine umfassende Strategie um Netzwerkresilienz zu erhöhen und gliedert sich in zwei Phasen: eine unmittelbar reaktive Phase, in der es um die Verteidigung, Störungsidentifikation, Behebung und Wiederherstellung des Normalzustandes geht, sowie eine analytische Phase, in der es um Diagnose der Störung und um Verbesserung des Systems geht – mit dem Ziel, das Netz durch langfristige Evolution ausfallssicherer zu machen.

## 3.6 Resilienz

Der Begriff Resilienz ist in der Literatur je nach beteiligten Disziplinen und Fokus der Studien äußerst unterschiedlich definiert, da er beispielsweise in Soziologie, Physik oder Ökonomie ganz andere Bedeutungen hat. Interessant erscheint vor allem die duale Definition von Cholda et al. (2007), die einerseits von einer statischen Resilienz ausgeht, die die Fähigkeit des Systems bezeichnet, Störungen zu widerstehen. Andererseits gibt es die dynamische Resilienz, die angibt, wie schnell ein gestörtes System in der Lage ist, wieder in seinen ursprünglichen Zustand zurückzukehren.

Als wesentliche Aspekte der Resilienz können folgende Konzepte gesehen werden (Sterbenz et al. 2010):

- Fehlertoleranz: Fehlertolerante Netzwerke sind in der Lage, auch bei Auftreten von Störungen oder nicht-korrekten Betriebszuständen Serviceleistungen zur Verfügung zu stellen. Dies kann beispielsweise durch Redundanz erreicht werden.
- Reliabilität: Gibt die Wahrscheinlichkeit an, in einer definierten Zeitspanne keine Störung im Netzwerk zu finden. Sie ist von der Design- bis zur Wartungsphase von Systemen relevant und wird oft auch in Serviceverträge mit Kunden als relevante Kennzahl definiert.
- Verfügbarkeit: Fähigkeit eines Systems, zu einem definierten Zeitpunkt funktionsbereit zu sein. Eng mit Reliabilität verwandt, aber ein höherer Fokus liegt auf Zeitpunkt vs. Zeitspanne.
- Elastizität: Beschreibt die Fähigkeit eines Netzes, auf den Ausfall einzelner Knoten oder Verbindungen zu reagieren und Daten umzuleiten.

Die Resilienz des Internets ist ebenso aus ökonomischer Sicht relevant, wo es auch um die Resilienz einzelner Unternehmen in Abhängigkeit vom Internet als kommerziellen Ökosystem geht, wie in Cleary & Banasiewicz (2018) dargelegt. Selbst wenn sich Unternehmen nicht als Teil der kritischen Infrastruktur Internet verstehen, sondern nur als Nutznießer, so ist für sie doch die Resilienz des Internets per se wichtig, ebenso wie ihre eigene Resilienz gegenüber Internetausfällen.

## 3.7 Kaskadeneffekte

Die meisten Studien, die sich mit Kaskadeneffekten bei kritischer Infrastruktur beschäftigen, fokussieren auf den Energiesektor, obwohl Beltrán et al. (2005) bereits 2005 das Internet klar als kritische Infrastruktur identifizierten und u.a. Van Eeten schon 2011 festgestellt hat, dass ein hoher Prozentsatz der Kaskadeneffekte in kritischer Infrastruktur im Bereich der IKT liegen (von 830 untersuchten Vorfällen in den Niederlanden lagen 44% im Bereich IKT – nur knapp weniger als im Energiesektor – 47% und deutlich mehr als im Transportbereich – 3,2%) (Van Eeten et al. 2011). Entgegen der weit verbreiteten Annahme von seltenen, aber umso gravierenderen Dominoeffekten und langen Kausalketten kommt die Studie zum Schluss, dass Kaskadeneffekte eher häufig vorkommen, üblicherweise aber auch recht schnell wieder gestoppt werden können. Auch die Annahme, dass Kaskadeneffekte auf Ereignisse mit geringer Wahrscheinlichkeit, aber hohem Impact zurückzuführen sind, konnte nicht bestätigt werden – die meisten Kaskaden finden ihre Ursache in wohlbekannten systemischen Problemen wie Korruption, Gewinnmaximierung, Nachlässigkeit, Bürokratie und generellen Kommunikations- und Kollaborationsschwierigkeiten (Pescaroli/Alexander 2016).

## 3.8 Fallstudien

Da länger anhaltende Internetausfälle in demokratischen Staaten mit gut entwickelter Infrastruktur recht selten sind, beschäftigt sich die Mehrzahl von Fallstudien entweder mit länger zurückreichenden Vorfällen – insbesondere dem Erdbeben in Japan im Jahre 2011 (z.B. Cho et al. (2011)), mit großteils geplanten Abschaltungen in (semi)autoritären Regimen oder mit Ausfällen in Ländern mit schwächerer Internet-Infrastruktur. So untersucht z.B. Wagner (2018) die Lage in Pakistan, wo allein von 2012 bis 2017 insgesamt 41 Internetabschaltungen vorgenommen wurden. Auf technischer Ebene interessant scheint Dainotti et al. (2011), wo am Beispiel von Ägypten und Libyen die Methoden und Probleme bei der Identifikation und Analyse einer Internetabschaltung erörtert werden, ebenso die Erreichbarkeit einzelner Komponenten und die zur Abschaltung verwendeten Prozedere. Zu den analysierten Datensätzen zählt neben BGP-Data erstmals auch die ‚Hintergrundstrahlung' des Internets, also unangeforderte Daten aus dem Darknet, wie sie z.B. durch Malwareinfektionen entstehen. Einen guten Überblick über die Auswirkungen eines Ausfalls auf die unterschiedlichen wirtschaftlichen Sektoren in Indien liefert Kathuria (2018) wo auch der Effekt von kurzfristigen bzw. lange anhaltenden Ausfällen und die Unterschiede in der Verfügbarkeit von Landleitungen und mobilem Internet besprochen werden.

West (2016) analysiert die wirtschaftlichen Auswirkungen von Internetausfällen und kommt zu dem Schluss, dass Staaten alleine 2015 2,4 Milliarden Dollar durch absichtliche Internetabschaltungen entgangen sind – eine Zahl, die vermutlich deutlich hinter den wahren Kosten zurückbleibt, da sie nur den direkten Einfluss auf das BIP berücksichtigt, nicht aber entgangene Steuern, Auswirkungen der geringeren Produktivität von Arbeiter:innen und Angestellten, Expansionshindernisse oder gesunkenes Vertrauen von Konsument:innen und Investor:innen. Grundlegende ökonomische Aspekte des Internets werden aktuell auch in Greenstein (2020) besprochen, wo etwa unternehmensinterne Netzwerkstrukturen von Google, Microsoft, Apple oder Amazon thematisiert werden. Auch die Rolle von Monopolen und Konkurrenz für den Netzwerkausbau und das Spannungsverhältnis von kommerziellen Unternehmen, die als Anwender von Protokollen und Stacks fungieren, während diese fast ausschließlich von Non-profit Organisationen entwickelt und weiterentwickelt werden, kommen dabei zur Sprache.

Studien zu den sozialen Auswirkungen von Internetausfällen sind schwer zu finden und nur von bedingter Aussagekraft, da die Rolle, die das Internet spielt, von Land zu Land – und auch innerhalb eines Landes zwischen z.B. urbanen und ruralen Gebieten – sehr unterschiedlich ist (Kathuria 2018). Explorative Erhebungen zur erwarteten Wahrscheinlichkeit eines Internetausfalles und zu den persönlichen Folgen zeigen ein gewisses Bewusstsein, aber keine große Sorge vor Internetausfällen (Lupien et al. 2017). Als Problemfelder werden insbesondere Arbeit/Karriere, persönliche Beziehungen/soziale Medien und der Wegfall des Internets als Nachrichtenquelle genannt – grundlegendere Probleme wie Wasser/Stromversorgung oder Nahrung sind selten ein Thema. Grandhi et al. (2020) weisen darauf hin, dass viele Menschen, die mit der Frage nach einem Internetausfall und seinen Folgen konfrontiert werden, das Szenario primär aus einer persönlich-egozentrischen Perspektive sehen und die systemische und gesellschaftliche Ebene ausklammern. Dadurch rücken gravierende

Auswirkungen auf politischer, kommerzieller und infrastruktureller Ebene in der öffentlichen Wahrnehmung oftmals in den Hintergrund.

Aktuelle Ausfälle und Abschaltungen werden u.a. vom Shutdown Tracker Optimization Project (STOP) der NGO KeepItOn erfasst (#keepiton 2021), wo sowohl der Download der Daten zu Forschungszwecken möglich ist, als auch regelmäßige Berichte über das aktuelle Ausmaß von Internetabschaltungen und der Deaktivierung einzelner Dienste wie Facebook, Twitter oder Instagram veröffentlicht werden.

# 4 Ursachen

## 4.1 Ambivalenz in Bezug auf die Ursachen

Die österreichische Verwaltung verfolgt im Österreichischen Programm zum Schutz kritischer Infrastrukturen (APCIP) den sogenannten „All Hazards“-Ansatz, der den Fokus nicht auf bestimmte Ursachen richtet, sondern den Schutz kritischer Infrastrukturen vor allen möglichen Gefahren im Blick hat. Daher sollen als Ursache für Schadensfälle kriminelle oder terroristische Aktivitäten genauso in Betracht gezogen werden wie Naturkatastrophen und menschliches oder technisches Versagen. Das bedeutet, dass es auch in diesem Projekt darum ging, die Folgen eines langanhaltenden und großflächigen Internetausfalls möglichst ursachenunabhängig zu betrachten.

Das hat verschiedene Vorteile. Zunächst einmal verschiebt es den Betrachtungsschwerpunkt auf den Zeitpunkt nach Eintritt des Schadensfalls. Cybersecurity ist ein Thema, das in den letzten 20 Jahren zurecht immer mehr Aufmerksamkeit erhalten hat. Das Thema Internetausfall unter dem Blickwinkel von Cybersecurity zu betrachten, hieße jedoch, dass es mehr um die unterschiedlichen Cyberangriffe und deren Abwehr ginge. ursachenunabhängig heißt auch, dass der Ursache wenig Aufmerksamkeit geschenkt wird und man in unterschiedlichen Szenarien den Fokus auf die Bewältigung der Krise lenken kann. Oft werden Ausgangslagen in Übungen kritisiert, wenn den Teilnehmenden der Weg dorthin nicht plausibel erscheint. Eine vollständig unbekannte Ursache, auf die auch nicht näher eingegangen werden muss, hilft diesen Effekt zu vermeiden. Letztendlich muss man vielleicht auch davon ausgehen, dass gar nicht alle Ursachen für solche Ausfälle bekannt sind. Trotzdem wird es in so einer Situation wichtig sein, handlungsfähig zu bleiben und die Krise so rasch wie möglich unter Kontrolle zu bringen. Das heißt, man muss sich intensiv damit befassen, welche Vorgehensweisen und Ressourcen in allen Szenarien nötig bzw. hilfreich sind. Eine ursachenunabhängige Betrachtungsweise kann dabei helfen, die Gemeinsamkeiten zwischen allen möglichen Auslösern und Arten von Schadensfällen zu entdecken. Damit lassen sich in der Vorbereitung vor allem jene Felder stärken, die in der Bewältigung jeder vernetzten Krise sinnvoll sind und eine agile Krisenbewältigung unterstützen.

Die Nachteile sind z.T. auch dort zu bemerken, wo es Vorteile gibt. So kann im Gespräch mit Expert:innen aus der Praxis das Fehlen einer Begründung für den Ausfall wie oben beschrieben hilfreich sein. Es kann aber auch im Weg stehen, wenn die Situation als unmöglich oder zumindest unwahrscheinlich eingestuft wird, weil man damit Vertrauen einbüßt. Wenn man die Ursachen beschreiben könne, die zu dem unwahrscheinlichen Ergebnis geführt hätten, dann wäre es auch leicht, sich auf die Fragestellung einzulassen. Gleichzeitig würde ein sehr konkretes Szenario dabei helfen, die Gesprächspartner:innen dort abzuholen, wo sie in ihrem Alltag stehen. Im Gegenzug müsste man jedoch in Kauf nehmen, dass die Betrachtungen durch die vorgegebene Ursache stark eingeschränkt werden würden.

Trotz aller Vor- und Nachteile einer ursachenunabhängigen Betrachtungsweise ist allerdings auch klar, dass sich diese nicht zu 100% umsetzen lässt. Jede Ursache,

die zu einem großflächigen und langanhaltenden Ausfall internetbasierter Dienste führen kann, beeinflusst auch die Situation nach dem Schadenseintritt. Wie bereits erläutert wurde, sind die Ressourcen, die zur Krisenbekämpfung verfügbar sind, stark von der jeweiligen Ausfallsursache abhängig.

## 4.2 Mögliche Ursachen

Wichtig ist es zunächst festzuhalten, dass ein Ausfall in der während der ersten Phase des Projekts kommunizierten Form (mindestens drei Tage Totalausfall in ganz Österreich) noch nie vorgekommen ist. Ein derartiger Ausfall wird von den befragten Expert:innen auch einhellig als sehr unwahrscheinlich eingeschätzt, vor allem in Bezug auf die Gleichzeitigkeit aller betroffenen Provider. Dennoch erschien es den Autor:innen dieses Berichts wichtig, die gesammelten Einschätzungen hier darzustellen und zu analysieren, um sie für weiterführende Projekte nutzbar zu machen.

Aus den Antworten der Expert:innen in den Interviews, während der Workshops und den dahinter liegenden Einschätzungen lassen sich die folgenden, potenziellen Ursachen annehmen.

### 4.2.1 Blackout

Ein Blackout führt unweigerlich zu einem Internetausfall. Für eine großflächige Serviceunterbrechung würde vermutlich auch ein Blackout reichen, von dem nur der Großraum Wien betroffen ist. Ein Blackout als Ursache ist für viele Expert:innen das Naheliegendste. Vielleicht ist ein Blackout auch die einzige realistische Möglichkeit, dass wirklich alle Provider (gleichzeitig) von dem Ausfall betroffen sind.

### 4.2.2 Marktkonzentration

Eine abnehmende Vielfalt am Providermarkt wirkt sich negativ auf die Resilienz aus. Der Ausfall eines Mobilfunkbetreibers kann dramatische Folgen haben, weil es im Endkund:innenbereich nur drei gibt, die in Österreich ein eigenes Netz betreiben. Die Lage bei Internetanbindungen für den kommerziellen Bereich ist besser, weil es hier mehr Anbieter gibt, und außerdem die, die ihr Netz auf Infrastruktur von bspw. A1 aufbauen, dieses i.d.R. vom A1-Netz entkoppelt haben (Segmentierung und eigene aktive Netzkomponenten). Allerdings hat der Marktführer hier vermutlich einen sehr hohen Marktanteil[1].

### 4.2.3 Gemeinsame Ressourcennutzung

Das anvisierte Sharing von Infrastruktur im 5G-Netz könnte ein Problem werden, weil durch weitere Konvergenzmaßnahmen wie diese, die Zahl der Betroffenen bei einem Ausfall deutlich steigen kann. Die geforderte Unabhängigkeit von Hardware-Herstellern wird sich nach Expert:innenmeinung nicht umsetzen lassen.

[1] Detaillierte aktuelle Zahlen, die den Marktanteil im Businessbereich ausweisen, gibt es zurzeit weder von den Providern selbst, noch von der RTR.

### 4.2.4 Konvergierende Netze

Dadurch, dass heute die meisten Kommunikationsprozesse über Internet (IP)-Infrastruktur abgewickelt werden, sind mehr Dienste bei einem Ausfall der Infrastruktur betroffen (kein eigenes Telefonnetz mehr usw.) als früher. Letztendlich gab es auch Ende des 20. Jhdts. Knoten, an denen sich Telefon- und Datennetze überschnitten, die diesbezüglich als Single Points of Failure einzustufen waren. Jedoch hat sich das heute verschoben zu einer ‚Single Infrastructure'. Es laufen heute nahezu alle Kommunikationswege datenbasiert über dieselbe Breitbandinfrastruktur (eine Ausnahme wäre TETRA). Parallel betriebene analoge Infrastrukturen, wie von ORS für terrestrischen Rundfunk, sind wirtschaftlich kaum noch tragbar. Immer wieder enden daher Diskussionen über redundante Netze bei der Frage, wer für die Zusatzkosten aufkommen solle. Organisationseinheiten der staatlichen Verwaltung sind i.d.R. nicht mit den erforderlichen Ressourcen ausgestattet, auch wenn sie die Notwendigkeit dafür sähen. Private Firmen sind anderen Zielen verpflichtet und sehen sich nicht in der Zuständigkeit für dieses Problem, sodass letztlich nach Marktlogik entschieden wird.

### 4.2.5 Monokulturen bzw. Abhängigkeit von bestimmten Hardwareherstellern

Es gibt einige Netzwerkausrüster, deren Produkte im Businessbereich in Österreich verwendet werden, wie bspw. Cisco, Juniper, Nokia usw., die nicht alle über eine gleich starke Servicepräsenz in Österreich verfügen. Wenn es hier zu einem Problem mit den Netzwerkkomponenten eines bestimmten Herstellers käme, wäre das je nach Hersteller und dessen Kapazitäten vor Ort ein unterschiedlich gravierendes Problem.

Ein Wechsel des Ausrüsters mitten in einer Krise ist nicht denkbar. Dies würde schon im Normalbetrieb Monate bis Jahre an Vorbereitungsarbeiten brauchen, wenn es nicht deshalb zu Ausfällen kommen soll. Es ist jedenfalls kein standardisiertes Umfeld, in dem Netzwerkkomponenten beliebig getauscht werden könnten.

Ein großflächiger, zeitgleicher Ausfall auf Grund eines Softwarefehlers ist für viele Expert:innen nicht wahrscheinlich, selbst wenn es sich um eine Hersteller-Monokultur handelte, da jeder Provider andere Releasestände verwendet. Fehler würden sich also unmittelbar bei dem Provider bemerkbar machen, der am schnellsten die Softwareupdates eingespielt hat (eventuell nur in einer Testumgebung). Damit könnten andere gewarnt werden. Andere Interviewpartner:innen hatten dazu eine fast konträre Einschätzung und halten genau das, also die hohen Marktanteile bestimmter Hardware-Anbieter, für das größte Gefahrenpotential, bspw. in Form eines fehlerhaften Firmware-Updates für einen scheinbar unbedeutenden Mikrochip, der millionenfach verbaut wurde.

Abhängigkeiten von nicht-europäischen Herstellern (USA, Israel, China) werden als Problem gesehen, da befürchtet wird, dass dieses Abhängigkeitsverhältnis auf Grund politischer Motive missbraucht werden könnte.

### 4.2.6 Zusammenbruch des Peerings

Kunden könnten nur noch die Inhalte sehen, die im Netz des eigenen Providers gehostet werden und von keinen außerhalb liegenden Content-Lieferanten abhängig sind. Wer bzw. was unter diesen Umständen noch erreichbar ist, ist jedoch unvorhersehbar, da bei den einzelnen Organisationen i.d.R. nicht bekannt ist, welche anderen Organisationen sich im selben Providernetz befinden.

### 4.2.7 Absichtlich herbeigeführte Abschaltungen einzelner Dienste

Während es aus heutiger Sicht undenkbar erscheint, dass sich die Praxis autoritärer Regimes, einzelne Dienste oder den gesamten Internetzugang eines Staates zeitweise abzuschalten, auch in Österreich durchsetzt, kann allerdings beobachtet werden, dass große Plattformbetreiber ihr Angebot zeitweilig abschalten, um nicht (Rebiger 2018, Rudl 2018) oder erst recht (Jungehülsing 2021) mit nationalen Behörden in Konflikt zu geraten. Daher muss damit gerechnet werden, dass dies auch hinkünftig eine Methode des Protests oder zur Erzeugung politischen Drucks sein kann. Das wird auf den Betrieb kritischer Infrastrukturen eine geringere Auswirkung haben, wenn es sich um Dienste für Konsument:innen handelt (wiewohl der entstehende politische Druck gerade dadurch sehr groß werden könnte), als wenn es sich um bspw. Clouddienste handelt, die von KI-Betreibern oder Verwaltungseinheiten stark genutzt werden (siehe Mahn 2020, Windeck 2020).

### 4.2.8 Cyberangriffe

#### *4.2.8.1 Szenario Estland 2006*

Angriffe, wie auf Estland 2006, sind heute einerseits erfolgversprechender, weil konvergierende Netze dazu führen, dass immer mehr Kommunikationskanäle über Internetinfrastruktur abgewickelt werden, wofür es vor einigen Jahren noch eigene Netze gegeben hat; andererseits dürfte das Sicherheitsbewusstsein und die Kompetenz auf dem Gebiet höher sein als noch 2006.

#### *4.2.8.2 Angriffe à la SolarWinds*

Der Angriff auf die amerikanische Softwarefirma SolarWinds im Jahr 2019 war bis dahin beispiellos. Die Firma erzeugt Managementsoftware zur Überwachung, Datenanalyse, Performanzoptimierung etc. für große Netzwerke und Server (Orion Plattform). Durch den Schadcode, der über Updates für diese Managementsoftware in die Netze der SolarWinds-Kunden eingeschleust werden konnte, wurde weltweit (Schwerpunkt waren US-Behörden und US- und westeuropäische Privatfirmen) eine enorme Menge an Netzwerken kompromittiert. Auf diese Art die Netzwerksicherheitsmaßnahmen der Opfer zu umgehen, könnte als Vorbild für weitere Angriffe funktionieren. Die Ausführung des zuvor eingeschleusten Schadcodes könnte natürlich auch synchron zu einem bestimmten Zeitpunkt auf allen befallenen Systemen zugleich erfolgen, sodass zeitgleich eine große Anzahl an Angriffen automatisiert ausgeführt wird, und zwar nicht wie bei Bot-Netzen von außen, sondern aus dem Inneren der angegriffenen Netze. Expert:innen schätzen den Aufwand für solche Angriffe allerdings als sehr hoch ein. Der SolarWinds Angriff soll von mehr als 1.000 Personen koordiniert ausgeführt worden sein, was staatliche Akteure nahelegen würde,

und war nur ein Teil eines größeren, konzertierten Angriffsplans auf US-Einrichtungen im Jahr 2020 (Temple-Raston 2021, Kühl 2021, Moechel 2021, Tung 2021).

#### *4.2.8.3 (Cyber-)Angriffe auf zentrale Dienste oder Knoten*

Auch physische Angriffe auf kritische Kommunikationsinfrastrukturen sind denkbar (Mahn 2022). Der Aufwand wäre natürlich groß, aber die einhellige Meinung der Expert:innen ist in diesem Punkt klar: Ein Ausfall der großen Internet Exchange-Knoten im Osten, oder ein Angriff auf den größten Provider, sei es mit konventionellen oder Cyber-Mitteln, führten jedenfalls dazu, dass die verbliebenen Routen den sprunghaft ansteigenden Traffic nicht mehr bewältigen könnten und wegen Überlastung ausfielen.

Es besteht auch die Annahme, dass die Absicherung von Routing Tables mittels MD5-Hashes in naher Zukunft nicht mehr ausreichend sein könnte, was deren Manipulation wieder wahrscheinlicher mache. Zu großen Turbulenzen könnte auch der Ausfall zentraler Dienste führen, wie bspw. DNS, oder auch der zentraler Zertifikatsanbieter.

### 4.2.9 Indirekte Ursachen

Einige Ursachen, wie die zuvor beschriebenen wirken unmittelbar, wohingegen andere zu einem Zusammenbruch beitragen, oder ihn indirekt verursachen.

#### *4.2.9.1 Lieferengpässe*

Schwierigkeiten in den Logistikketten (z.B. bei Modems) könnten zu einer schleichenden Unterversorgung am Markt führen, aber nicht zu einem Totalausfall.

#### *4.2.9.2 Das „Window of Opportunity“ wird kleiner*

Solange Prozesse analog abgelaufen sind, war es bei Fehlern möglich, rasch korrigierend einzugreifen. Durch die gestiegene Geschwindigkeit in der Datenverarbeitung und bei der Abwicklung geschäftskritischer Prozesse, kann der Mensch i.d.R. nicht mehr steuernd eingreifen und verlässt sich auf Automatismen und Redundanzen. Funktionieren diese nicht, oder werden Redundanzen (z.B. aus wirtschaftlichen Gründen) abgebaut, entsteht hier das Potential für Kaskadeneffekte und Krisen. Das Security-by-Design-Prinzip werde diesbezüglich oft nicht ernst genug genommen.

#### *4.2.9.3 Ein Ausfall ist zunächst schwer zu erkennen*

Ein landesweit gleichzeitig eintretender Totalausfall wäre in der Bewältigung der Krise ein Vorteil, weil dann gleich klar sei, dass es sich um ein ernstes Problem handelte, so die Meinung einiger Expert:innen. Kommt der Ausfall schleichend, bspw. durch steigende Latenzen und abfallende Bandbreite in der Übertragung, oder iterierend, indem Services immer wieder ausfallen, dazwischen aber funktionieren, dann ist das Problem nicht nur schwerer zu erkennen, sondern auch die Integrität der Daten könnte mit jedem Wiederanlaufen weiter in Mitleidenschaft gezogen werden. Außerdem würde vielleicht anders und/oder langsamer reagiert, als wenn gleich klar wäre, wie die Dimension des Angriffs bzw. des Ausfalls ist. Dadurch ginge wertvolle Zeit verloren, und das Schadensausmaß könnte größer ausfallen, als es bei zeitgerechter, „richtiger“ Reaktion der Fall gewesen wäre.

### 4.2.10 Krieg

Wird bei Analysen i.d.R. nicht weiter betrachtet, weil es in solchen Situationen dann oft um elementare Aufgaben geht, die das Überleben sichern sollen. Durch die Entwicklungen seit Februar 2022, als Russland die Ukraine angegriffen hat, muss diese Einschätzung vielleicht überdacht werden. Zusätzlich verschwimmen auch die Grenzen zwischen Krieg und Frieden zunehmend, wenn hauptsächlich staatliche Akteure zu den großen Playern bei Cyber-Angriffen werden. Das Manipulieren oder Ausschalten der Kommunikationsmöglichkeiten gehört zu den ersten Maßnahmen in Kriegen (neben anderen Versorgungsunterbrechungen, wie Strom, Gas usw.). Bei Angriffen wie auf Estland 2006 wird aus politischen Gründen darauf verzichtet, diese als kriegerischen Akt zu deklarieren, aber gleichzeitig geht das Geschehene weit über das hinaus, was aus kriminellen oder sogar terroristischen Organisationen zu erwarten wäre. Lange wurden derartige Angriffe, ohne Mitwirken konventioneller Truppen, der Sphäre der Spionage zugeordnet. Allerdings werden auch Antworten auf Cyber-Angriffe unter Verwendung konventioneller Waffensysteme seit mehreren Jahren diskutiert. Die Frage bei der Suche nach möglichen Ursachen für einen großflächigen und lang anhaltenden Ausfall internetbasierter Dienste in Österreich ist also, ob mit kriegerischen Handlungen gleichzusetzende Aktionen aus dem Cyberspace, oder direkte Folgen kriegerischer Auseinandersetzungen (bspw. NEMP im Rahmen von Kampfhandlungen auch in Nachbarstaaten) eine Situation zur Folge haben können, die sich wesentlich von denen nach anders verursachten Ausfällen unterscheidet, und/oder ob die Folgen kriegerischer Auseinandersetzungen etwas sind, auf das das SKKM vorbereitet sein sollte. Vorstellbar wäre in diesem Zusammenhang auch die Situation, dass Österreich gar nicht direkt angegriffen werden soll, sondern dass, weil Österreich irgendwie passend ist, hier Methoden und Technik getestet werden, die für einen späteren Angriff auf ein anderes Land benötigt werden. Vergleichbar wäre dies mit den nach den Enthüllungen von Snowden aufgekommenen Vermutungen, dass amerikanische Nachrichtendienste, quasi als proof-of-concept, die gesamte Telekommunikation ausgewählter kleiner Staaten in Echtzeit abhören.

## 4.3 Motive hinter einem Angriff

Im Zusammenhang mit der Frage nach möglichen Ursachen müsste auch die Frage nach der Motivation der Angreifer gestellt werden. Die meisten Interviewpartner:innen nehmen an, dass ein großflächiger und lang anhaltender Internetausfall nicht zufällig, also durch die Verkettung unglücklicher Umstände, passieren kann, sondern jedenfalls mit Absicht herbeigeführt werden müsste. Falls das so ist, stellt sich die Frage nach der Motivation der Angreifer. Blackouts ließen sich leichter und billiger auf anderem Weg erreichen. Sind zivile Unruhen das Ziel? Oder geht es darum, Freund oder Feind die Stärke der eigenen Cybertruppe zu demonstrieren? Kann es ideologische Gründe haben? Oder handelt es sich – wie weiter oben schon angesprochen – um die Ouvertüre zu weiteren, auch physisch vor Ort ausgeführten Angriffen? Die Vorbereitung auf eine erfolgreiche Bewältigung einer derartigen Krise könnte vermutlich von der Antwort auf diese Frage profitieren.

# 5 Methodik

## 5.1 Inter- und transdisziplinärer Zugang des Projekts

Wie bei allen Forschungsprojekten aus dem Bereich der Technikfolgenabschätzung war es auch in diesem Fall wichtig, über einen interdisziplinären Zugang zu dem Thema verschiedene Sichtweisen zu integrieren. Entsprechend dieser Anforderung und den Vorgaben der Projektförderung hat ein sehr divers besetztes Projektteam an der Beantwortung der Forschungsfragen zwei Jahre lang gearbeitet. Das Wissen und die Methoden, die durch die Partner aus dem akademischen Bereich eingebracht wurden, wurden vom Praxiswissen und der Erfahrung der anderen Projektpartner ergänzt.

Zusätzlich war es dem Projektteam besonders wichtig, das wertvolle implizite und explizite Wissen derjenigen für das Projekt nutzbar zu machen, die täglich in dem Bereich der kritischen Infrastrukturen, oder dem Bereitstellen von internetbasierten Diensten arbeiten. Das war nicht zuletzt auch deshalb wichtig, weil das Fehlen aktueller wissenschaftlicher Arbeiten zu dem Thema gezeigt hat, dass dem von wissenschaftlicher Seite bisher anscheinend noch wenig Beachtung geschenkt wurde. Dieser transdisziplinäre Zugang im Projekt hat gemeinsam mit dem kontinuierlichen Austausch und den Evaluierungsmaßnahmen sehr zu den praxisrelevanten Ergebnissen beigetragen, mit denen das Projekt abgeschlossen werden konnte.

## 5.2 Expert:inneninterviews

Als eine der Grundlagen des Projekts wurden qualitative Expert:inneninterviews eingesetzt (vgl. Meuser/Nagel 2002 und Hopf 2003). Dadurch wurde in Verwirklichung eines transdisziplinären Forschungszuganges das Wissen aus der Praxis dem Projekt zugänglich gemacht. Ziel war es, bislang unbekannte Fakten zu der beforschten Themenstellung zu erlangen (bspw. die Betroffenheit der eigenen Organisation oder Branche), sowie eine Kontextualisierung des publizierten Wissens und eine Einschätzung zur Situation in Österreich zu bekommen. Damit hatten die Interviews, je nach Gesprächspartner:in und Situation, sowohl einen explorativen als auch einen systematisierenden Charakter (vgl. Bogner/Littig/Menz 2014: 72).

Auf Basis der Literaturrecherche und den Erfahrungen des Projektteams aus den Vorprojekten wurde ein Interviewleitfaden erstellt (siehe 10.2.2.1), der auch die beiden Rollen berücksichtigte, die befragte Organisationen einnehmen: Provider und deren Kunden. Die Interviews wurden als semi-strukturierte leitfadengestützte Expert:inneninterviews durchgeführt und danach transkribiert, sofern das nicht durch die Wünsche der Interviewten ausgeschlossen wurde. Den Interviewten wurde weiters zugesagt, dass sie nicht namentlich genannt (im öffentlich zugänglichen Bericht sind lediglich die Organisationen vermerkt) und nur nach Rückfrage wörtlich zitiert würden. Die (sektorspezifische) Darstellung der Ergebnisse in Kap. 7 speist sich daher nicht nur aus den Interviewdaten einzelner Organisationen aus diesem Bereich, sondern auch aus dem, was andere, Sektor-externe Organisationen dazu beigetra-

gen haben, sowie aus den Ergebnissen der Diskussionen in den zwei Workshopreihen (die unter der Chatham-House-Regel stattfanden), dem Evaluierungsworkshop und der Übung. Dadurch leidet zwar die Transparenz im veröffentlichten Bericht, aber nur unter diesen Bedingungen, die keine Rückführbarkeit bestimmter Aussagen auf einzelne Personen oder Organisationen zulassen, war es möglich, die sehr sensiblen Informationen zu erlangen und im Projekt zu verwenden. Dieser Trade-Off erscheint sinnvoll, um zu den Erkenntnissen aus dem Projekt zu gelangen und diese wieder der Community, der Forschung, sowie einer breiteren Öffentlichkeit zugänglich machen zu können.

Wie in der aktuellen wissenschaftlichen Literatur empfohlen (Bogner/Littig/Menz 2014: 72ff), wurden die Interviews qualitativ ausgewertet (nicht kodiert).

### 5.2.1 Überlegungen zur Auswahl der Interviewpartner:innen

Bei der Auswahl der Interviewpartner:innen galt es, verschiedene Aspekte zu berücksichtigen. In manchen Fällen gibt es für das hier betrachtete Szenario nur eine sinnvollerweise auswählbare Organisation. So wurde etwa der staatliche Rundfunk seit seinem Bestehen darauf ausgerichtet, in Krisenzeiten einen wichtigen Beitrag zur Kommunikation mit der Bevölkerung zu leisten. Privatsendern wurde diese Rolle hingegen nie auferlegt. Genauso ist in Österreich bspw. nur eine einzige Organisation für das Management des Strom-Übertragungsnetzes zuständig. In diesen und vergleichbaren Fällen war also gar keine Auswahl zu treffen.

In anderen Branchen war die Frage zu berücksichtigen, ob es einen für das Projekt relevanten Unterschied zwischen Konzernen und KMUs gibt, zwischen Versorgern im urbanen oder ländlichen Raum. In wieder anderen Fällen wurde ein Vertreter mit großem Leistungsportfolio stellvertretend für die gesamte Branche befragt.

In manchen Branchen ergaben sich die Interviewpartner:innen aus der Sachlage. So war bspw. im Telekommunikationsbereich aus den Vorprojekten (siehe Kap. 2.2) klar, dass der wichtigste Provider in Österreich (besonders im Businessbereich und allgemein bei der Infrastruktur) A1 ist (DAÖ: 345). Aus der ehemaligen Post und Telegraphenverwaltung hervorgegangen, verfügt A1 aus historischen Gründen und durch kontinuierlichen Ausbau über das größte Netz in Österreich. Leitungen innerhalb dieses Netzes werden auch anderen Betreibern vermietet, die diese Strecken zum Teil vollkommen autonom betreiben. Dadurch bildet die Infrastruktur von A1 auch die Grundlage für getrennt vom Internet verwaltete Netzbereiche wie die Vernetzung der österreichischen Behörden über den Government Internet Exchange (GovIX). Andere, für den Internetbetrieb in Österreich unerlässliche Knoten (Vienna Internet Exchange, VIX) werden durch eine Abteilung des Zentralen Informatikdienstes (ZID) der Universität Wien betrieben.

Im Gesundheitswesen war zu erwarten, dass kleinere Betreiber eventuell als Insel funktionieren würden, wohingegen größere über die Standorte verteilte Systeme betreiben, wodurch sie für eine Betrachtung interessanter wären. Ebenso ist bei einem größeren Betreiber anzunehmen, dass das Leistungsspektrum größer und die Anzahl an potenziellen Problemstellungen damit auch höher ist.

Generell wurde unter Berücksichtigung der zuvor beschriebenen Überlegungen versucht, ein einerseits möglichst vollständiges Bild der Betroffenheit kritischer Infrastrukturbetreiber von einem solchen Ausfall zu zeichnen, und andererseits möglichst viele unterschiedliche Probleme und Arten von Betroffenheit zu erfassen. Ein einschränkender Faktor waren dabei die begrenzten Projektressourcen. Im Projektantrag waren Einzelinterviews mit sieben Personen, sowie zumindest zwei Gruppeninterviews vorgesehen, z.B. mit verschiedenen Vertreter:innen einer Branche, wenn relevante Unterschiede zwischen den Betreibern kritischer Infrastrukturen innerhalb eines Sektors zu erwarten wären. Es galt also einerseits in wenigen Terminen einen Überblick zu erlangen und gleichzeitig konkret genug für die weiteren Arbeiten im Projekt darüber Bescheid zu wissen, in welchen Bereichen Schwierigkeiten im Fall eines Internetausfalls auftreten würden, und welcher Art diese Schwierigkeiten sein würden.

Das Projekt wurde um den Jahreswechsel 2019/20 geplant, als von der durch das Corona-Virus ausgelösten Pandemie in Europa medial noch keine Anzeichen wahrzunehmen waren. Der Startschuss war in den ersten Monaten der Pandemie, die Interviewphase begann mit der sog. zweiten Welle der Infektionen in Österreich im Herbst 2020. Im Verlauf der Vorarbeiten zu den Interviews wurde daher rasch klar, dass viele vom Projekt anzusprechende KI-Betreiber (genauso wie das BMI als Projektpartner) ihre Ressourcen anders einzusetzen hatten, Präsenztermine und Workshops auch aus Sicherheitsgründen nicht in der gewohnten Form durchzuführen waren, und es sehr schwierig würde, Gruppentermine zu organisieren. Es wurde daher entschieden, unter erhöhtem Ressourcenaufwand das Projekt mit einer wesentlich größeren Anzahl an Einzel- und Kleingruppeninterviews auf eine breitere Wissensbasis zu stellen. Deshalb wurden im Zeitraum Jänner bis Juni 2021 bei 22 Interviewterminen mit insgesamt 31 Personen Gespräche geführt (Interviewdetails siehe Kapitel 10.3 im Anhang).

## 5.3 Modellierung mit System Dynamics

Die Informationen, die im Zuge der Interviews erhoben wurden, stellten damit die wichtigste Datenbasis für die weitere Forschung dar. In einem zweiten Schritt galt es, valide Modelle zu erstellen, mit denen die empirischen Daten systematisch ausgewertet und strukturiert werden konnten, um daraus generalisierbare Aussagen abzuleiten. Um die dynamischen Prozesse zu analysieren, wurde daher auf das Konzept der System Dynamics zurückgegriffen.

Moderne Systeme unterliegen einem stetigen Wandel. System Dynamics ist eine Methode, die komplexe Systeme und ihr Verhalten im Zeitverlauf ins Zentrum stellt. Sie geht auf Jay Forrester und seine Arbeit Industrial Dynamics (Forrester 1961) zurück. In einem aktuelleren Werk beschreibt er den Hintergrund der Methode wie folgt:

> *„System dynamics combines the theory, methods, and philosophy needed to analyse the behaviour of systems not only in management, but also in environmental change, politics, economic behaviour, medicine, engineering, and other fields. System dynamics*

> *provides a common foundation that can be applied wherever we want to understand and influence how things change through time. The system dynamics process starts from a problem to be solved – a situation that needs to be better understood, or an undesirable behaviour that is to be corrected or avoided. The first step is to tap the wealth of information people possess in their heads. (…) System dynamics uses concepts drawn from the field of feedback control to organize available information into computer simulation models." (Forrester 1993: 5).*

Um komplexe, reale Probleme darzustellen, können mit Hilfe dieser Methodik nichtlineare, interdisziplinäre Zusammenhänge und Feedbackprozesse modelliert werden (vgl. Sterman 2000: 4f). Eine Möglichkeit, solche Wirkungszusammenhänge darzustellen, ist die Erstellung qualitativer Ursache-Wirkungsdiagramme (Anm.: Hier und im Folgenden auch Causal Loop-Diagramme oder kurz CLDs genannt). Causal Loop Diagramme beinhalten relevante Systemvariablen und kausale Zusammenhänge zwischen diesen Wirkungsgrößen, ausbalancierende und sich selbst verstärkende Prozesse sowie zeitliche Verzögerungen und Systemgrenzen (vgl. Mella 2012: 43). Sie visualisieren Ursache-Wirkungszusammenhänge und essenzielle Feedbackschleifen in Systemen. Durch die Visualisierung wichtiger Systemelemente tragen CLDs fundamental dazu bei, ein gemeinsames Verständnis für komplexe Systeme zu schaffen (vgl. Mella 2012: 90).

Wirkungsrichtungen werden in Causal Loop Diagrammen durch Pfeile angezeigt. Wenn der Wirkungszusammenhang zwischen zwei Variablen positiv ist, wird er mit einem ‚+' dargestellt. Wenn die Startvariable zunimmt, nimmt auch die Folgevariable zu (siehe Abbildung 1).

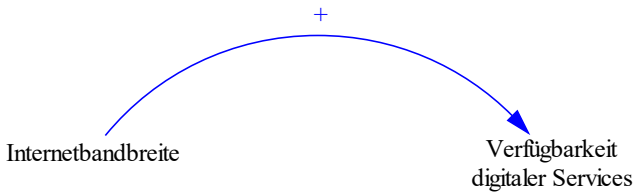



*Abbildung 1: Direkte Korrelation zwischen zwei Variablen (Universität für Bodenkultur Wien, 2021)*

Wenn der Wirkungszusammenhang zwischen zwei Variablen negativ ist, wird er mit einem ‚-' dargestellt (siehe Abbildung 2). Dies zeigt an, dass die Folgevariable abnimmt, wenn die Startvariable zunimmt und umgekehrt (vgl. Sterman 2000: 144f).

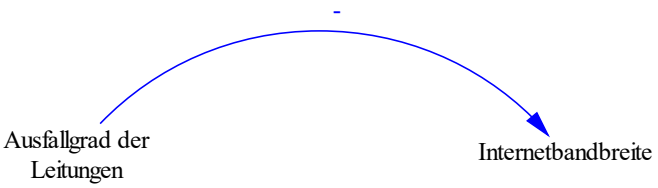



*Abbildung 2: Indirekte Korrelation zwischen zwei Variablen (Universität für Bodenkultur Wien, 2021)*

Aus mehreren Wirkungszusammenhängen können sich geschlossene Loops ergeben. Bei einer geraden Anzahl an negativen Verbindungen in einem Loop handelt es sich um sogenannte „Reinforcing Loops“. Diese führen zu einem Wachstum im System und werden wie folgt dargestellt:

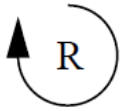



*Abbildung 3: Kennzeichnung von Reinforcing Loops in CLDs (vgl. Sterman 2000: 142)*

Wenn die Gesamtanzahl an negativen Verbindungen in einem geschlossenen Loop ungerade ist, handelt es sich um so genannte „Balancing Loops“, die zu einer Abnahme im System führen und wie folgt gekennzeichnet werden:

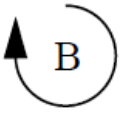



*Abbildung 4: Kennzeichnung von Balancing Loops in CLDs (vgl. Sterman 2000: 142)*

Wirkungszusammenhänge können außerdem verzögert auftreten, was in den Modellen mit einem so genannten „Delay Mark“ (zwei kurze Doppelstriche senkrecht zur Wirkungsrichtung) wie in Abbildung 5 ersichtlich gemacht wird (vgl. Sterman 2000: 150). Das Verzögerungszeichen zeigt, dass Problemlösungsmaßnahmen in Abhängigkeit vom jeweiligen Problem oft eine gewisse Zeit in Anspruch nehmen (vgl. Kapmeier 1999: 54). Verzögerungen können in komplexen Systemen auch Instabilitäten verursachen bzw. Potenziale aufzeigen, wo der Faktor Zeit eine besondere Relevanz besitzt und effizienter genutzt werden könnte (vgl. Kapmeier 1999: 79).

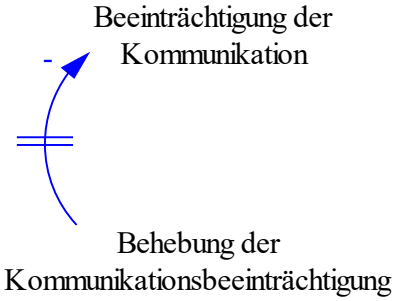



*Abbildung 5: Wirkungsverzögerung in CLDs (Universität für Bodenkultur Wien, 2021)*

Causal Loop-Diagramme dienen der Veranschaulichung von Wirkungsketten, die beispielsweise durch ein Ausfallsereignis, wie es im Rahmen von ISIDOR untersucht wird, in Gang gesetzt werden können. Die Modelle ermöglichen damit die Identifizierung potenzieller Folgeeffekte, die auf den ersten Blick nicht ersichtlich sind. Entscheidend dafür ist das zugrunde liegende Systemverhalten, das im Zeitverlauf beobachtbar ist und im Rahmen so genannter Archetypen dargestellt werden kann. Dabei handelt es sich um generische Strukturen, die weit verbreitet sind und in den unterschiedlichsten Systemen erkannt werden können. Sie werden in den Diagrammen ersichtlich und tragen wesentlich zum Verständnis komplexer Systeme bei.

Im Fall von ISIDOR spielen die Archetypen „Shifting the Burden“ und „Eroding Goals“ eine Schlüsselrolle bei der Abbildung des ursächlichen Systemverhaltens. Der Archetyp der Lastenverteilung bzw. „Shifting the Burden“ ist in Abbildung 6 dargestellt. Den Kern dieses Archetyps bildet ein zugrunde liegendes Problem, das ein Symptom hervorruft. Da dieses Problem jedoch oft schwer zu erkennen bzw. umständlich zu lösen ist, entscheidet man sich zugunsten der Lastenverteilung für einen so genannten ‚Quick-Fix‘, indem man sich stattdessen auf die Minderung des Symptoms konzentriert, woraus zwei stabilisierende Rückkopplungsprozesse und ein sich selbst verstärkender Nebeneffektsprozess resultieren. Die Lastenverteilung zugunsten der reinen Symptombekämpfung bewirkt, dass die eigentliche Problemlösung zunehmend in den Hintergrund rückt, was als so genannte Systemfalle verstanden werden kann, da es sich dabei um ein unerwünschtes Systemverhalten handelt (vgl. Meadows 2019: 197-202).

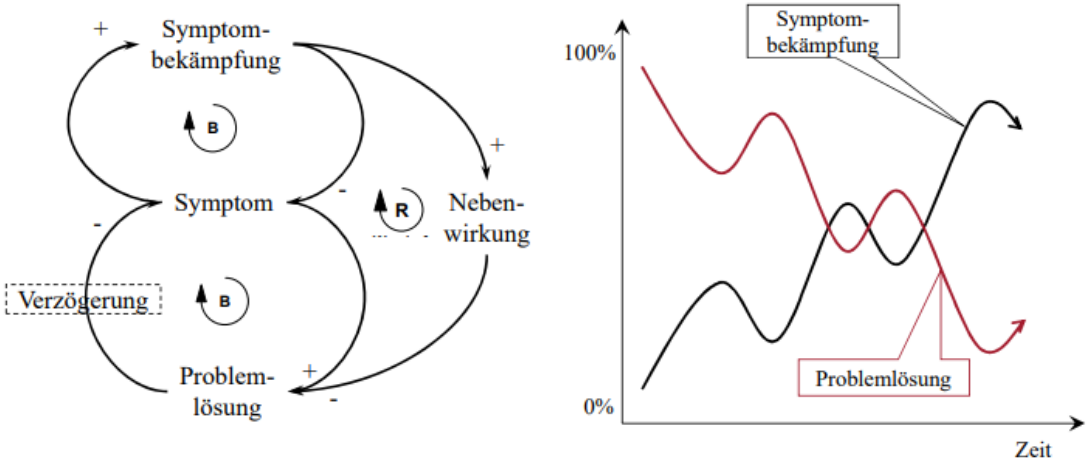



*Abbildung 6: Lastenverteilung (vgl. Mandl & Gronalt 2012: 33)*

Der zweite Archetyp, der für ISIDOR ebenfalls eine wichtige Rolle spielt, ist der Archetyp der abrutschenden Ziele bzw. „Eroding Goals“ in Abbildung 7. Dabei wird von einer Diskrepanz zwischen dem Soll- und Ist-Zustand ausgegangen, die einerseits durch eine Reduktion des Zieles und andererseits durch Korrekturmaßnahmen verringert werden kann. Aus beiden Optionen ergeben sich stabilisierende Rückkopplungsprozesse (B für Balancing). Während Korrekturmaßnahmen jedoch mit einer zeitlichen Verzögerung positiv auf den Status Quo wirken, bedingt eine Reduktion des Zieles eine Zielerosion, die sich im Zeitverlauf in Form eines kontinuierlichen Leistungsabfalles zeigt (vgl. Meadows 2019: 184-186).

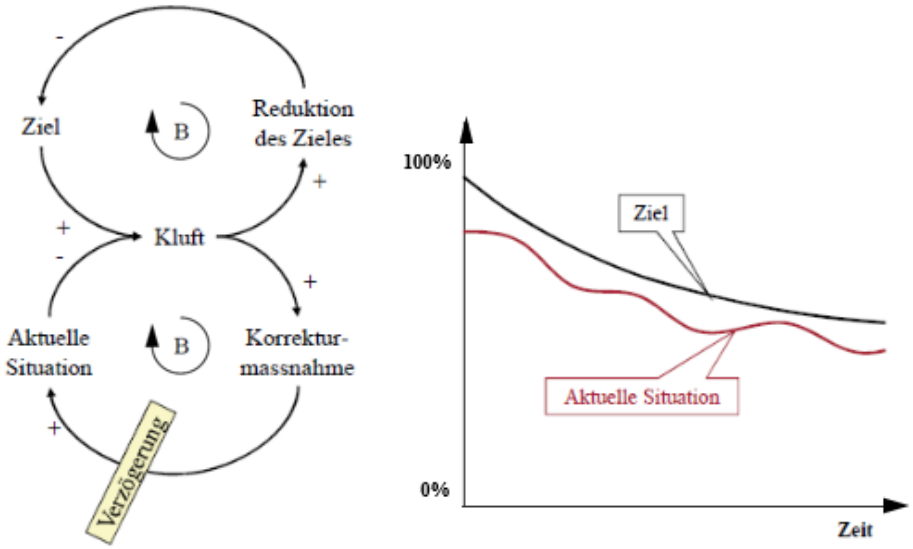



*Abbildung 7: Abrutschende Ziele (vgl. Mandl & Gronalt 2012: 39)*

Beide Archetypen sind exemplarisch an jeweils einem Beispiel aus ISIDOR in den Kapiteln 6.2 und 6.3 dargestellt. Es ist essenziell, Systemstrukturen wie diese zu identifizieren, um ein grundlegendes Systemverständnis zu schaffen. Basierend darauf können wirksame Maßnahmen entwickelt werden, wodurch den bereits zuvor erwähnten Systemfallen entgegengewirkt werden kann (vgl. Meadows 2019: 170f). Auch in ISIDOR können die entwickelten Modelle komplexe Systemstrukturen veranschaulichen und tragen somit zur Etablierung des notwendigen, tiefgreifenden Verständnisses bei, um in weiterer Folge wirksame Maßnahmen und Handlungsempfehlungen geben zu können.

Ein Vorteil von CLDs ist, dass diese anhand von Validierungsprozessen basierend auf neu gewonnenen Informationen stetig iterativ erweitert und adaptiert werden können (vgl. Sterman 2000: 87). Die Problematik hinter vernetzten Krisen ist derart komplex, dass auch im Projekt ISIDOR ein iterativer Lernprozess, wie er in Abbildung 8 dargestellt wurde, anzuwenden war.

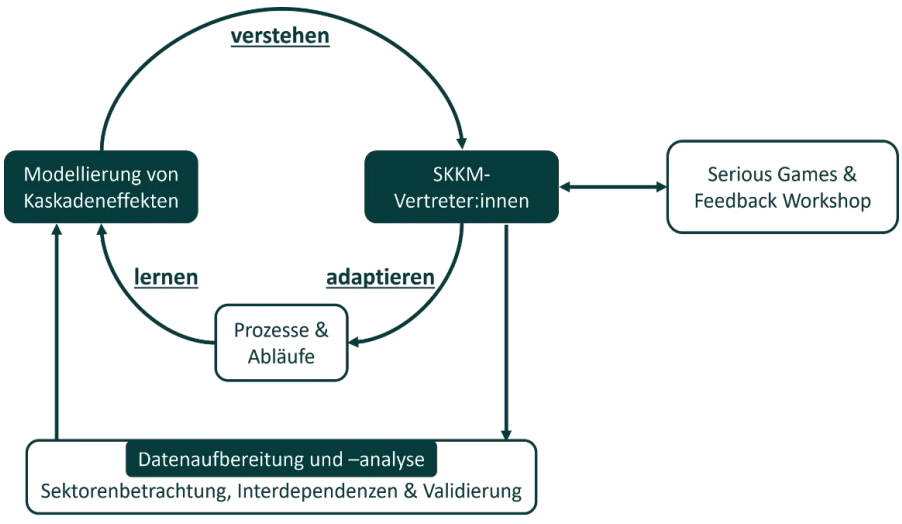



*Abbildung 8: Lernprozess in ISIDOR*

Den finalen Modellen ist eine Reihe verschiedener Entwicklungs- und Überarbeitungsschritte vorangegangen, die im Folgenden näher beschrieben werden.

Basierend auf den Expert:inneninterviews und einer umfassenden Literaturrecherche zu facheinschlägigen Vorprojekten und relevanten Quellen in verschiedenen Medien und wissenschaftlichen Literaturdatenbanken wurden die vorhandenen empirischen Ergebnisse, sowie jene aus der Primär- und Sekundärliteratur analysiert. Ein besonderer Schwerpunkt lag dabei auf potenziellen Systemvariablen und deren Wirkungszusammenhängen, die systematisch gesammelt und aufbereitet wurden. Dabei galt es, mögliche Systemvariablen nach ihrer Zugehörigkeit zum jeweiligen Sektor und ihrer Position im System zu analysieren. Der Systemaufbau ist in Abbildung 9 ersichtlich.

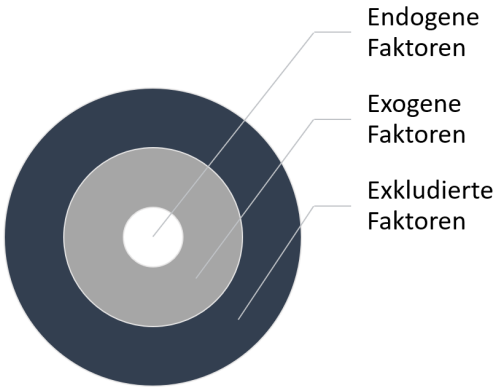



*Abbildung 9: Systemaufbau nach Ford (2010: 143)*

Beispiele für endogene Faktoren im Zusammenhang mit einem Internetausfall sind etwa die Kommunikation über digitale Kanäle, die innerhalb einer Organisation abläuft, sowie interne Hardware- und IT-Abhängigkeiten. Exogene Faktoren, die von außen auf das betrachtete System wirken, sind beispielsweise ein Abfall der Bandbreite, ein Blackout-Ereignis, sowie die Beeinträchtigung von Zulieferleitungen, aber auch behördliche Auflagen und Service Level Agreements (SLAs). SLAs sind Rahmenverträge zwischen Serviceanbietern und Kund:innen, die eine bestimmte Servicequalität garantieren (vgl. Girs et al. 2020: 134498). Exkludierte Faktoren sind Aspekte, die in der Systembetrachtung bewusst vernachlässigt werden. In ISIDOR waren das beispielsweise die Analyse der Gründe für den Eintritt eines Ausfallsereignisses.

Darüber hinaus wurden bei der Auswertung der Interviews die jeweiligen Textstellen, die auf eine Verbindung zwischen den analysierten Variablen hinweisen, dokumentiert. Die Variablen wurden in Start- bzw. Endvariablen der jeweiligen Verbindung gegliedert und positive bzw. negative Wirkungsbeziehungen wurden definiert.

Anhand der systematischen Aufbereitung konnten die Erstentwürfe der beiden sektorspezifischen Modelle aus dem Transport- und Gesundheitssektor entwickelt werden. Diese wurden mehrere Male innerhalb des Projektteams sowie bilateral mit verschiedenen Projektpartner:innen abgestimmt, durchdiskutiert und iterativ adaptiert bzw. erweitert.

Im Zuge des Feedbacks aus den Workshop-Reihen sowie und dem Evaluierungsworkshop erhielt das Projektteam weitere Informationen und neue Erkenntnisse von verschiedenen Expert:innen. Insgesamt wurden zwei Workshop-Reihen und eine Abschlussübung durchgeführt (für nähere Details diesbezüglich siehe Kapitel 5.4). Die neu gewonnen Erkenntnisse aus den Workshops und der Abschlussübung flossen nach systematischer Aufbereitung in die Modelle ein, die anhand neuer Informationen adaptiert bzw. ergänzt wurden. So wurden die Modelle iterativ validiert und Schwerpunktthemen, die sich bei der Modellierung herauskristallisierten, in den Workshops aufgegriffen und mit den anwesenden Expert:innen diskutiert. Auch der Aufbau der sektorspezifischen Modelle wurde im Rahmen projektinterner Diskussionen kritisch hinterfragt und überarbeitet. Anhand der zahlreichen Inputs aus der Praxis konnten systemische Muster und Archetypen abgeleitet werden, die in einem langandauernden und großflächigen Ausfall internetbasierter Dienste viele der ablaufenden Prozesse maßgeblich beeinflussen. Diese Muster wurden in die beiden sektorspezifischen Modelle eingearbeitet. Darüber hinaus wurde ein Baukasten für ein so genanntes Sektoren-Grundmodell erstellt. Dieses ist als Vormodell der beiden Sektorenmodelle aus dem Transport- und Gesundheitssektor zu verstehen und dient der sektorunabhängigen Darstellung von Feedbackschleifen bei einem Ausfall internetbasierter Dienste. Es setzt sich, wie der Name bereits verrät, aus flexibel anwendbaren ‚Baukästen' zusammen, die Organisationen dazu nutzen können, diese nach ihren Bedürfnissen anzupassen bzw. zu erweitern, um das Ausmaß der organisationsinternen Betroffenheit bei einem Ausfall internetbasierter Dienste visualisieren zu können. Die Darstellung in Form von Baukästen dient nicht zuletzt einer besseren Nachvollziehbarkeit der Auswirkungen, die eine vernetzte Krise, wie in ISIDOR beschrieben, auf die jeweilige Organisation haben könnte, sowie einer Ableitung von Entscheidungen und Handlungsoptionen, die jede:r Akteur:in im Rahmen von Vorkehrungen treffen kann, um sich rechtzeitig darauf vorzubereiten.

## 5.4 Workshops und Übung

Im Projekt war mindestens eine Übung mit Vertreter:innen der beteiligten Partner und Unternehmen geplant, um die vorhergehenden Ergebnisse zu validieren. In der Ausgangslage war vorgesehen, auf die bisherigen Erfahrungen im Bereich des SKKM aufzubauen und die bereits getesteten Formate weiterzuentwickeln. Maßgeblich war hierbei v.a. die SKKM-Übung Helios im Mai 2019, bei der unter Federführung des BMI etwa 100 Vertreter:innen von zwölf Ministerien, sechs Bundesländern, sechs verschiedenen Einsatzorganisationen sowie von drei Infrastruktureinrichtungen drei Tage lang einen Blackout bzw. eine Strommangellage simulierten. Auf Basis des Feedbacks der Teilnehmer:innen folgte ein weiterer Workshop im Jänner 2020, der v.a. die verschiedenen Akteur:innen zusammenführen sollte, die im Zuge einer vernetzten Krise, d.h. einer Disruption mit Folgen für Politik, Wirtschaft und Gesellschaft, bei der Bewältigung zusammenwirken würden.

Es wurden mehrere Übungstypen in Betracht gezogen, u.a. eine Kommunikations- und Alarmierungsübung (Überprüfung der Kommunikationsstrukturen durch einen Probealarm), ein Plan-Review, eine Planbesprechung (gemeinsame Durchsicht bestehender Planungen), eine Stabsübung oder Stabsrahmenübung (Simulation einer

Krisenbewältigung durch die eingesetzten Stäbe) sowie eine Vollübung (unter Einbeziehung aller betroffenen Strukturen und Organisationen). Aufgrund der Belastung durch die laufenden Ereignisse während der Projektlaufzeit und die damit verbundene eingeschränkte Verfügbarkeit der teilnehmenden Projektpartner wurde eine dreitägige Übung (analog zu Helios) verworfen und zwei Serien von Planbesprechungen per Videokonferenz sowie einem gemeinsamen Online-Workshop der Vorzug gegeben. Die Methode orientierte sich dabei an den Serious Games, die ursprünglich für Computerspiele mit interaktiven Lerninhalten entwickelt worden war (Motyka 2012). Die drei Übungsserien sollten dabei aufeinander aufbauen:

In der ersten Serie konfrontierte die Übungsleitung die Teilnehmer:innen mit dem Szenario einer Internetunterbrechung aufgrund eines Ausfalls von DNS-Severn. Die einzelnen Teams sollten auf dieser Basis eine erste Lagebeurteilung aus Sicht ihres Unternehmens durchführen. Die dabei erzielten Ergebnisse wurden von der Übungsleitung anschließend evaluiert und als Grundlage für die zweite Runde im Herbst 2021 herangezogen, bei der ein Erdbebenszenario zugrunde gelegt wurde. Die Teilnehmer:innen sollten dabei ihre Krisenreaktionspläne weiterentwickeln und auch die Auswirkungen des Szenarios auf andere Organisationen und Einrichtungen miteinbeziehen. Bei der dritten und letzten Runde stand die Vernetzung der Akteur:innen untereinander im Vordergrund, d.h. die teilnehmenden Personen sollten abschätzen, welchen Beitrag sie selbst zur Krisenbewältigung leisten könnten, und welche Leistungen sie von anderen Organisationen benötigen würden. Im Gesamtbild ermöglichten die drei Phasen damit einerseits eine effektive Validierung der vorhergehenden Ergebnisse, und andererseits neue Erkenntnisse für die Beurteilung der Situation nach einem Schadenseintritt.

### 5.4.1 Die einzelnen Übungsphasen im Detail:

Im Mai und Juni 2021 wurde die erste Phase der Serious Games in Form von Videokonferenzen durchgeführt. Es fanden acht Workshops mit insgesamt 253 Teilnehmer:innen statt. Die einzelnen Workshops waren nach Sektoren/Branchen gegliedert, wobei Entscheidungspunkte innerhalb der vertretenen Organisationen identifiziert werden konnten. Im Vordergrund standen dabei die Krisenvorbereitung und -vorsorge innerhalb der vertretenen Organisationen sowie Wechselwirkungen und Abhängigkeiten mit bzw. von anderen Akteur:innen der Produktionsketten. Die Teilnehmer:innen wurden zu Beginn der Workshops mit bis dahin erlangten Ergebnissen aus den Interviews und den Grundlagen der System Dynamics vertraut gemacht, sodass die einzelnen Beiträge für die weitere Projektarbeit möglichst gut zu verwerten waren.

Die Phase I der Workshops diente auch der ersten Validierung der Archetypen, die als relevant für ein Ausfallsereignis im Sinne von ISIDOR identifiziert worden waren. Die Ergebnisse der Phase I wurden in die System Dynamics Modelle zurückgespielt und bildeten die Grundlage für die Workshops der Phase II. In dieser wurden in einem ähnlichen Format sektorenübergreifende Teams gebildet und eine dynamische Lage simuliert, um die zugrunde gelegten Causal Loop Diagramme zu validieren.

*Tabelle 2: Daten zur ersten Workshopreihe*

| Datum | Sektor/Branche | Teilnehmende Personen |
|---|---|---|
| 17. Mai | Wasser, Lebensmittel | 55 |
| 20. Mai | Verfassungsmäßige Einrichtungen | 51 |
| 27. Mai | Energie | 25 |
| 31. Mai | Medien und Kommunikation | 18 |
| 1. Juni | Informations- und Kommunikationstechnologie | 36 |
| 14. Juni | Gesundheit und Soziales | 34 |
| 15. Juni | Verkehr, Transport, Chemie | 34 |

Im Zuge der Workshops wurden die Teilnehmer:innen mit einer fiktiven Ausgangslage konfrontiert, in der DNS-Services für einen unabsehbaren Zeitraum ausgefallen waren, wodurch die meisten internetbasierten Dienste nicht zur Verfügung standen. Die teilnehmenden Personen erarbeiteten auf dieser Basis eine erste Lagebeurteilung sowie Handlungsoptionen aus der Sicht ihres Unternehmens. Konkret wurden dabei folgende Aspekte erhoben:

- Status: Betroffenheit von Prozessen, Dienstleitungen, anderen Internetservices, Vertrauensdiensten
- Prognose: Darstellung des Worst Case bei Ausfall für kürzer/länger als 24 Stunden
- Implikationen: Zeitliche, fachliche und organisatorische Herausforderungen für die Organisation
- Nächste Schritte: Kommunikations- und Koordinationsbedarf, Unterstützung, Kommunikationsgeflecht

In weiteren Arbeitsschritten wurden Wechselwirkungen, Abhängigkeiten sowie (in Form eines online-Fragebogens) der Vorbereitungs- und Zielerreichungsgrad des Unternehmens bzw. der individuellen Teilnehmer:innen erhoben.

Bei der Zielerreichung zeigte sich, dass insgesamt die verfassungsmäßigen Einrichtungen (d.h. der öffentliche Sektor) in der Eigenwahrnehmung am besten auf das zugrunde liegende Szenario vorbereitet waren. Dies gilt insbesondere für die Vorbereitung der Mitarbeiter:innen auf die Bewältigung eines Internetausfalls. Die Sektoren Wasser und Lebensmittel betrachteten sich am wenigsten auf ein derartiges Szenario vorbereitet. Der Sektor Energie ist in der Eigenwahrnehmung ebenfalls gut für ein Ausfallszenario gerüstet, insbesondere in technischer Hinsicht.

Die Abhängigkeiten und Wechselwirkungen mit anderen Sektoren und Diensten wurden vorwiegend in Hinsicht auf die zuvor erarbeiteten Causal Loops erhoben. Hierbei ergaben sich sektorenübergreifend bzw. -spezifisch folgende Kernaussagen:

- Die Verfügbarkeit alternativer Kommunikationsmittel ist ein entscheidender Faktor zur Bewältigung eines Internetausfalls (BOS, Amateurfunk, Sprachkommunikation). Durch Umstellung auf (telefonische) Sprachübertragung kann ein großer Teil der Services auf Notfallniveau aufrechterhalten werden, allerdings um den Preis von Verzögerungen sowie eines vorübergehend stark erhöhten Personalbedarfs.
- Ein funktionierender Zahlungsverkehr ist oft die Voraussetzung für Warenlieferungen. Ein Ausfall von elektronischen Verrechnungssystemen kann also den Warenverkehr nachhaltig behindern.
- Die Energieversorgung ist kritisch für alle Sektoren.
- Bei einigen Services, insbesondere im Finanzsektor, ist die Dauer des Ausfalls ein kritischer Faktor. Hier können bereits innerhalb kurzer Zeit massive Schäden auftreten, die in weiterer Folge auch manifeste Haftungsrisiken darstellen.
- Schulen und Kindergärten sind i.d.R. kaum betroffen, da sie in direktem, persönlichen Kontakt mit Schüler:innen und Eltern stehen, und ein sinnvoller Betrieb auch ohne Internetverbindungen vorstellbar ist.
- Ein Ausfall des Internets könnte auch die politische Handlungsfähigkeit der Republik Österreich beeinträchtigen, da davon auch die Kommunikationslinien mit der EU und internationalen Organisationen sowie die Öffentlichkeitsarbeit betroffen wären.
- Zumindest das Österreichische Bundesheer, die Feuerwehr und das Rote Kreuz sind in Bezug auf Kommunikationsmittel redundant aufgestellt.
- Zeitpunkt und Wetterlage sind bei einem Ausfall insbesondere für die Sektoren Verkehr (Schneelage) und Energie (Jahreszeit) besonders wichtig.

Alle Sektoren beurteilten ein Zusammentreffen mit einer weiteren krisenhaften Entwicklung (Blackout, Bank Run, radiologisches Ereignis etc.) als kritisch. Weitgehende Übereinstimmung bestand auch darin, dass die Wiedererrichtung eines Staatsgrundnetzes wünschenswert wäre.

Zur Vertiefung der Ergebnisse der ersten Runde der Workshops wurde im Oktober 2021 eine zweite Runde durchgeführt, bei der grundsätzlich dieselben Unternehmen und Organisationen eingeladen wurden, diesmal jedoch zu sektorübergreifenden Workshops. Die Arbeitsgrundlagen bildeten vier Szenarien, die auf Basis der zuvor durchgeführten Interviews und der Ergebnisse der Workshops der ersten Runde für die Sektoren IKT, Gesundheit, Transport und Verfassungsmäßige Einrichtungen erstellt wurden.

Auf Basis des Eurocode 8[2] wurde eine Erdbebensituation angenommen: Aufgrund extrem tiefer Außentemperaturen und der Erderschütterungen wurden im Boden ver-

[2] Die Normen zum Eurocode 8 gelten für die Bemessung und Konstruktion von Bauwerken des Hoch- und Ingenieurbaus in Erdbebengebieten.

legte Kabel (primär das Glasfasernetz) unterbrochen. Parallel führten die Bodenbewegungen bei rotierenden Speichermedien (Festplatten) zu Datenintegritätsproblemen, wodurch wesentliche Services/Applikationen gestört wurden.

Das Szenario verstand sich dabei nur als Annahme, um Ausfälle im Internet flächendeckend zu simulieren. Die Betroffenheit wurde dabei auf Bezirksebene heruntergebrochen, um den Kontext zwischen Geografie und Internet-Topologie herstellen zu können. Daraus ergab sich eine komplexe, unbekannte Situation, die nur auf einer übergeordneten Koordinationsebene gemeinsam bewältigt werden konnte.

Die teilnehmenden Organisationen wurden aufgefordert:

- die eigene Betroffenheit darzustellen (logisch und geographisch)
- die Erwartungshaltung an die anderen teilnehmenden Organisationen zu formulieren; ebenso sollten sie Services identifizieren, die sie in diesem Szenario anderen Stakeholder:innen zur Verfügung stellen können.
- mögliche Gleichzeitigkeitseffekte darzustellen (welche Organisation greift eventuell auf idente Service-Provider bzw. Wartungs- und Instandhaltungskapazitäten zu)
- Kritikalitäten zu identifizieren
- die generischen Causal Loops für die ersten 24h bzw. in weitere Folge für 48h+ für die eigene Organisation zu ergänzen und zu kommentieren
- die eigenen Aufgaben für die nächsten sieben Tage nach Eintritt des Szenarios zu identifizieren

Insgesamt nahmen rund 200 Personen an den einzelnen Workshops am 1., 15. und 19. Oktober 2021 teil. Zur Auswertung wurden die Ergebnisse in folgenden Kategorien erhoben:

- Ausfall/Einschränkung eigener Prozesse (insges. 76 konkrete Prozesse identifiziert)
- Folgen für die eigene Organisation (76 Rückmeldungen)
- SKKM-Koordinationsbedarf (35 Rückmeldungen)
- Maßnahmen zur Prävention (26 Rückmeldungen)
- Maßnahmen zur Vorbereitung (16 Rückmeldungen)
- Maßnahmen zur Reaktion (59 Rückmeldungen)
- Maßnahmen zur Wiederherstellung (20 Rückmeldungen)

Bei den gemeldeten Reaktionsmaßnahmen stand vor allem die Verlagerung von Kommunikations- und Dokumentationsprozessen auf andere Medien im Vordergrund, etwa die verstärkte Nutzung von Sprach- statt Datenkommunikation. Bei den Wiederherstellungsmaßnahmen ging es vorwiegend um das Nacharbeiten bzw. elektronische Erfassen der inzwischen angefallenen Daten. Das SKKM sollte in diesem Szenario vor allem Lenkungsmaßnahmen ergreifen, d.h. Priorisierungen bei der Zuteilung von Ressourcen wie Brennstoffen (Gas, Heizöl, Biomasse), Betriebsmitteln (Gas, Benzin, Diesel), Maßnahmen zur Wiederherstellung von Notfalltelefonnummern, Telefondienste und Internetdienste für Betreiber Kritischer Infrastrukturen.

Weitere erwartete Leistungen des SKKM waren vor allem:

- der Einsatz von Einsatzkräften zur logistischen Unterstützung (Bundesheer),
- die Kommunikation mit der Bevölkerung,
- die Aufrechterhaltung der öffentlichen Ordnung und
- die Vereinfachung bzw. Sicherstellung von Verwaltungsprozessen.

Aufgrund aktueller Ereignisse konnte die für Mai 2022 geplante Abschlussübung nicht in der ursprünglich geplanten Form abgehalten werden, sodass am 25. Mai 2022 ein halbtägiger Workshop mit ca. 100 Vertreter:innen der Kritischen Infrastruktur durchgeführt wurde. Die Veranstaltung war in eine ganztätige Konferenz des Bundesministeriums für Inneres eingebunden und fand teilweise parallel zu anderen Inhalten statt.

Die teilnehmenden Organisationen erhielten dabei die Möglichkeit, die bereits in Phase II angesprochene Verlagerung von Kommunikationsprozessen weiter zu vertiefen und für den eigenen Gebrauch dazu Grundlagen zu erarbeiten. Dazu wurden zunächst die alternativen Kommunikationsmittel erhoben und nach Resilienz und Qualität beurteilt. Darüber hinaus analysierten die Teilnehmer:innen, mit welchen anderen Organisationen sie im Krisenfall bevorzugt kommunizieren müssten, und wie ein übergeordnetes (staatliches) Kommunikationsgeflecht die Kritische Infrastruktur unterstützen könnte. Dieser Workshop war vorwiegend dazu gedacht, die Teilnehmer:innen durch gezielte Fragen durch einen strukturierten Prozess zu führen, der eine Art ‚Krisentelefonbuch' ergab, in dem die wichtigsten Stakeholder:innen und deren Erreichbarkeit mit unterschiedlichen Mitteln zusammengeführt wurde.

Ein wichtiges Ergebnis der Debatte bestand in der Erkenntnis, dass die Infrastruktur der A1 eine entscheidende Rolle spielt. Sollte sich bei einem Ausfall des Internets die Kommunikation auf die mobile Sprachkommunikation verlagern, so hätte dies bei einem Ausfall des Mobilfunknetzes drastische Auswirkungen. Viele der aktuell diskutierten Notfallmaßnahmen drehten sich um die Frage, wie in einem solchen Fall Workarounds eingerichtet werden könnten. Zielführender wäre es laut einiger Teilnehmer:innen, das Mobilfunknetz grundsätzlich resilienter zu machen, was entsprechende Kosten mit sich bringen würde.

## 5.5 Qualitätssicherung

Die Sicherung der Qualität der Projektergebnisse fand auf unterschiedlichen Ebenen statt. Zum einen wurden die jeweils aktuellen Zwischenergebnisse projektintern vorgestellt und besprochen. Zum anderen wurden sie bei unterschiedlichen Gelegenheiten mit Projektexternen diskutiert. Dazu wurden einerseits bei den Workshops mit dem SKKM zu Beginn die für den Bereich relevanten Ergebnisse und die Methoden präsentiert (siehe voriger Abschnitt). Andererseits gab es in der letzten Phase des Projekts einen eigenen Workshop, der sich gezielt mit verschiedenen Aspekten der Handlungsempfehlungen des Projekts auseinandersetzte. In mehreren Diskussionsrunden besprachen die Teilnehmer:innen konkrete Fragestellungen, bei denen es um die Ausgestaltung bestimmter Empfehlungen ging. Die Ergebnisse flossen, ebenso wie das Feedback aus den Workshops mit dem SKKM in die finale Fassung der Empfehlungen ein. Eine detaillierte Darstellung findet sich im Anhang, Kap. 10.4.

# 6 Ergebnisse aus der Modellierung

Referenziert wird im vorliegenden Kapitel zu den Ergebnissen aus der Modellierung auf ein Working Paper von Schachenhofer et al. (2022). Die im Rahmen des Projektes erstellten CLDs bilden das Kernstück der Ergebnisse aus der Modellierung. Im Rahmen des Modellierungsprozesses wurden verschiedene Wirtschaftssektoren betrachtet und ein Baukasten im Sinne eines Sektoren-Grundmodelles erstellt, das den Ausgangspunkt für die sektorspezifischen Modelle darstellt. Für den Gesundheits- und Transportsektor wurden detaillierte kausale Schleifen-Diagramme erarbeitet, die die Darstellung von sektorspezifischen Ursache-Wirkungs-Zusammenhängen ermöglichen. Alle Modelle basieren auf einer umfassenden Literaturanalyse, sowie den Ergebnissen aus qualitativen Expert:inneninterviews und SKKM-Sektorenworkshops. Die Erkenntnisse aus den Workshops der ersten und zweiten Reihe sowie der Abschlussübung erlaubten die Validierung der bestehenden Modelle und eine iterative Anpassung bzw. Erweiterung der Modelle. Die anwendungsorientierte Darstellung zeigt sowohl im Sektoren-Grundmodell, als auch in den beiden sektorspezifischen Modellen Verlagerungen auf nicht digitale Arbeitsweisen und Kommunikationsmethoden, die mögliche Folgen einer wesentlichen Einschränkung internetbasierter Dienste jedoch nur teilweise kompensieren können. Verlagerungen gehen daher oft mit einer Beeinträchtigung der Kommunikations- und Datenqualität, einem Anstieg der Personalauslastung sowie einer Einschränkung der Verfügbarkeit abhängiger Leistungen einher. Die Modelle zeigen somit die große Bedeutung einer angemessenen Vorbereitung für Organisationen und Unternehmen auf, um die Resilienz in den einzelnen Sektoren sowie relevanten, sektorübergreifenden Schnittstellen zu erhöhen.

Die Modelle stellen dementsprechend eine wichtige Grundlage für die umfassende Bewusstseinsbildung und Wissensgenerierung im Umgang mit vernetzten Krisen dar, die im Zeitverlauf an Bedeutung gewinnen werden. Im Folgenden wird näher auf die einzelnen CLDs und ihre Systemvariablen eingegangen. Im Anschluss werden Anwendungsfälle, die mit Hilfe der empirischen Analysen aus den Modellen abgeleitet wurden, im Detail erläutert, um die Verlagerungseffekte und kausalen Wirkungszusammenhänge anhand realer Beispiele zu veranschaulichen.

## 6.1 Baukasten des Sektoren-Grundmodells

Im Rahmen der Erhebungen konnte festgestellt werden, dass bestimmte Abläufe bei einem Ausfall Internetbasierter Dienste sektorenunabhängig ähnlich ablaufen. Aus diesem Grund wurde ein Sektoren-Grundmodell entwickelt, das diese Sektor-übergreifenden Prozessmuster in übergeordnete Themenbereiche gliedert, die in einzelnen Bausteinen dargestellt werden (siehe Abbildung 14). Die Bausteine und deren relevante Zusammenhänge werden im Folgenden näher erläutert. Es wird an dieser Stelle nicht auf alle Systemvariablen im Detail eingegangen, da diese in Kapitel 6.2 und Kapitel 6.3 im Rahmen der beiden sektorspezifischen Modelle ausführlich beschrieben werden. Systemvariablen sind im vorliegenden Kapitel fortlaufend *kursiv* geschrieben, um auf die Verbindung zu den vorgestellten Modellen hinzuweisen.

### 6.1.1 Baustein: Ausgangsvariablen

Der erste Baustein (siehe Abbildung 10) umfasst die Ausgangsvariablen *Bandbreitenabfall bzw. Ausfall internetbasierter Dienste* und *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen*. Diese wirken sich auf die *Verfügbarkeit und Verwendbarkeit von internetbasierten Diensten* aus. Die negative Wirkungsbeziehung zwischen den beiden Ausgangsvariablen und der *Verfüg- und Verwendbarkeit internetbasierter Dienste* zeigt, dass je stärker die Beeinträchtigung der Ausgangsvariablen ist, desto weniger internetbasierte Dienste zu diesem Zeitpunkt genutzt werden können (Schachenhofer et al. 2022).

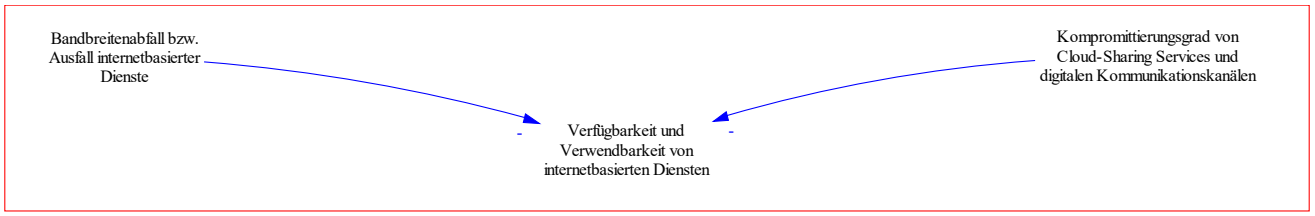



*Abbildung 10: Baustein Ausgangsvariablen eines Ausfalls internetbasierter Dienste (vgl. Schachenhofer et al. 2022)*

### 6.1.2 Baustein: Digitale Datenspeicherung und -zugriff

Der Baustein des Themas *Digitale Datenspeicherung und -zugriff* (siehe Abbildung 11) besteht aus den Sub-Themen *Organisationsinterne Daten, Organisationsexterne Daten* und *Digitale Abwicklung von Zahlungsprozessen.* In allen drei Bereichen treten Verlagerungseffekte auf. *Organisationsinterne Daten* wirkt positiv auf den *Verfügbarkeitsgrad Abspeicherung und Zugriff.* Dieser hat eine negative Wirkungsbeziehung zur *Verlagerung auf andere Dokumentationsmechanismen,* da bei einem geringeren *Verfügbarkeitsgrad Abspeicherung und Zugriff* mehr auf andere Dokumentationsmechanismen verlagert werden muss. Durch die vermehrte *Verlagerung auf andere Dokumentationsmechanismen* kann ein erhöhter *Verfügbarkeitsgrad Abspeicherung und Zugriff* erreicht werden, was anhand einer positiven Wirkungsbeziehung von der *Verlagerung auf andere Dokumentationsmechanismen* auf den *Verfügbarkeitsgrad Abspeicherung und Zugriff* zu erkennen ist. Der *Verfügbarkeitsgrad Abspeicherung und Zugriff* wirkt negativ auf die *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff,* die mit einer zeitlichen Verzögerung positiv auf den *Verfügbarkeitsgrad Abspeicherung und Zugriff* zurückwirkt. Im Rahmen der Verlagerung und der Wiederherstellung ergeben sich zwei ausbalancierte Rückkopplungskreise. Ausgehend von der *Verlagerung auf andere Dokumentationsmechanismen* entsteht darüber hinaus ein sich selbst verstärkender Rückkopplungskreis. Die *Verlagerung auf andere Dokumentationsmechanismen* wirkt positiv auf die *Bindung von Ressourcen,* was sich wiederum negativ auf die *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff auswirkt.*

*Organisationsexterne Daten* wirkt positiv auf den *Verfügbarkeitsgrad Echtzeitdaten*, der negativ auf die *Verlagerung auf analoge Daten* wirkt. Die *Verlagerung auf analoge Daten* wirkt wiederum positiv zurück auf den *Verfügbarkeitsgrad Echtzeitdaten,* wodurch ein ausbalancierter Rückkopplungskreis entsteht. *Verfügbarkeitsgrad Echtzeitdaten* wirkt außerdem negativ auf die *Wiederherstellung der Verfügbarkeit von*

*Echtzeitdaten.* Je weniger Echtzeitdaten verfügbar sind, umso mehr muss eine Wiederherstellung dieser erfolgen, die eine gewisse Zeit in Anspruch nimmt. Dementsprechend wirkt eine *Wiederherstellung der Verfügbarkeit von Echtzeitdaten* zeitlich verzögert positiv auf den *Verfügbarkeitsgrad Echtzeitdaten* zurück, wodurch ein weiterer ausbalancierter Rückkopplungskreis entsteht.

Analog dazu läuft die Verlagerung bei der *Digitalen Abwicklung von Zahlungsprozessen* ab, die in einem positiven Wirkungszusammenhang mit dem *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* steht. Dieser wirkt negativ auf die *Verlagerung auf andere Dokumentationsmechanismen*, die positiv zurück auf den *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* wirkt. Dieser steht außerdem in einem negativen Wirkungszusammenhang mit der *Wiederherstellung der Verfügbarkeit der digitalen Übermittlung*, die mit einer zeitlichen Verzögerung positiv zurück auf den *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* wirkt.

Die beschriebenen Verlagerungseffekte wirken sich in weiterer Folge auf die nachgelagerten Systemvariablen *Datenqualität, Abwicklung von rechnungs- und dokumentenabhängigen Prozessen* und die *Personalauslastung* aus. Dabei wirken der *Verfügbarkeitsgrad Abspeicherung und Zugriff* und der *Verfügbarkeitsgrad Echtzeitdaten* positiv auf die *Datenqualität,* während die *Verlagerung auf andere Dokumentationsmechanismen,* sowie die *Verlagerung auf analoge Daten* jeweils in einem negativen Wirkungszusammenhang mit der *Datenqualität stehen.*

Analog dazu wirkt der *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* positiv auf die *Abwicklung von rechnungs- und dokumentenabhängigen Prozessen*, während die *Verlagerung auf andere Dokumentationsmechanismen* in einem negativen Wirkungszusammenhang mit der *Abwicklung von rechnungs- und dokumentenabhängigen Prozessen* steht.

Die *Datenqualität* wirkt außerdem negativ auf die nachgelagerte *Personalauslastung,* da eine hohe *Datenqualität* mit einer geringeren *Personalauslastung* einhergeht und umgekehrt (Schachenhofer et al. 2022).

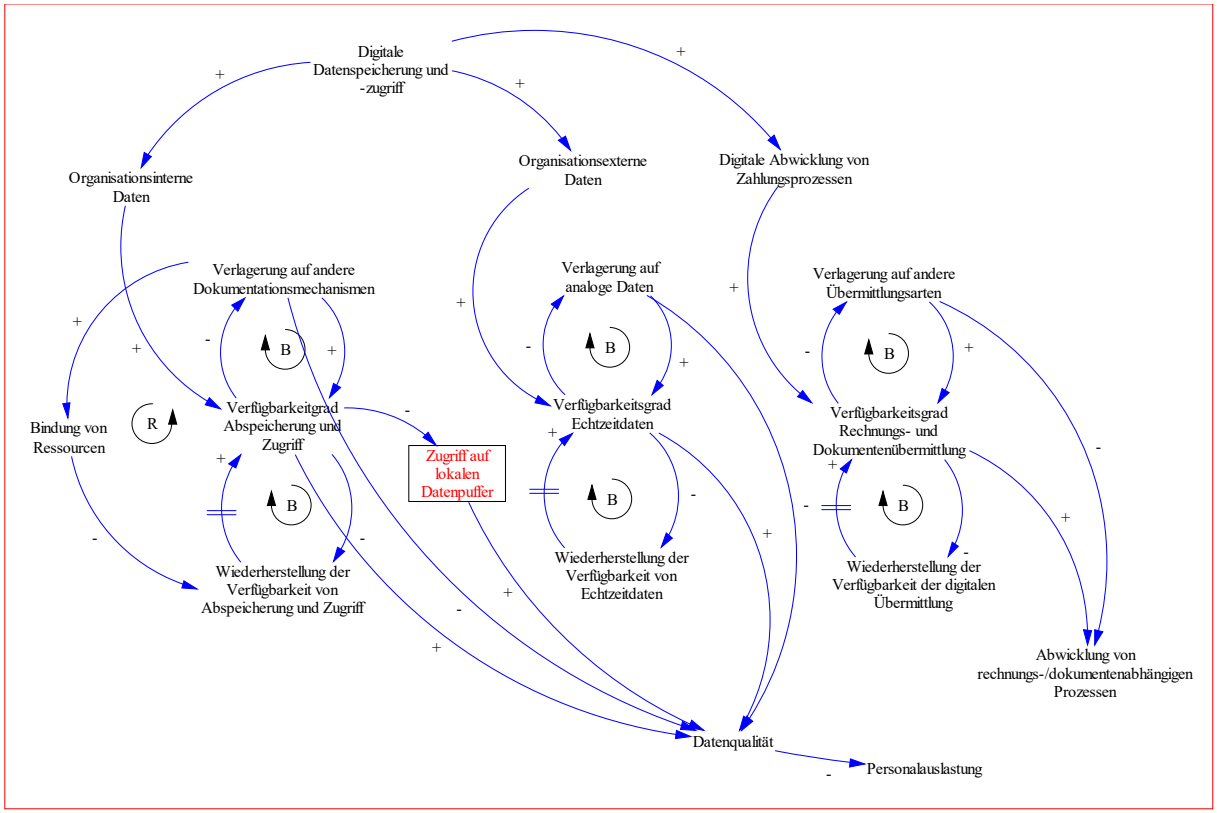



*Abbildung 11: Baustein Digitale Datenspeicherung und -zugriff (vgl. Schachenhofer et al. 2022)*

### 6.1.3 Baustein: Digitale Kommunikation in Prozessen der Organisation

Die *Digitale Kommunikation in Prozessen der Organisation* (siehe Abbildung 12) kann in die *Aktive Kommunikation* sowie die *Automatisierte Kommunikation* unterteilt werden. Im Falle des Ausfalls internetbasierter Dienste wurde sowohl in den Interviews, als auch im Rahmen der Workshops häufig von verschiedenen Akteuren erklärt, dass die Kommunikation in beiden Fällen nach Möglichkeit temporär auf den Mobilfunk verlagert wird. Je mehr verlagert werden muss, desto schlechter ist jedoch die *Kommunikationsqualität* und die *Qualität von Abstimmungs-/ Kontrolltätigkeiten*. Eine Verminderung dieser Qualitätsvariablen erhöht wiederum die *Personalauslastung*, da dadurch Kommunikations- und Monitoring-Prozesse maßgeblich erschwert werden und deutlich mehr Zeit im Vergleich zu den digitalen Abläufen beanspruchen. Im Falle der *Automatisierten Kommunikation*, die in Folge per Telefon durchgeführt werden würde, ist mit Genauigkeitseinbußen zu rechnen. Darüber hinaus veranschaulicht dieser Baustein einen Zusammenhang, der sektorübergreifend zu einem großen Problem werden kann: Wenn sämtliche Akteure aus den verschiedensten Sektoren ihre sonst digital ablaufenden Kommunikationsprozesse aufgrund eines Ausfallsereignis auf den Mobilfunk verlagern, kann es aufgrund einer deutlich erhöhten Menge zu übertragender Daten zu Überlastungserscheinungen im Mobilfunknetz in Form von Verzögerungen oder unter Umständen sogar Ausfällen kommen. Dies wiederum führt zu einer *Beeinträchtigung von Mobilfunk*, was während eines Aus-

fallsereignisses internetbasierter Dienste kritisch wäre, da die heutzutage konventionell am stärksten genutzten Kommunikationssysteme innerhalb kürzester Zeit zum Erliegen kommen könnten (Schachenhofer et al. 2022).

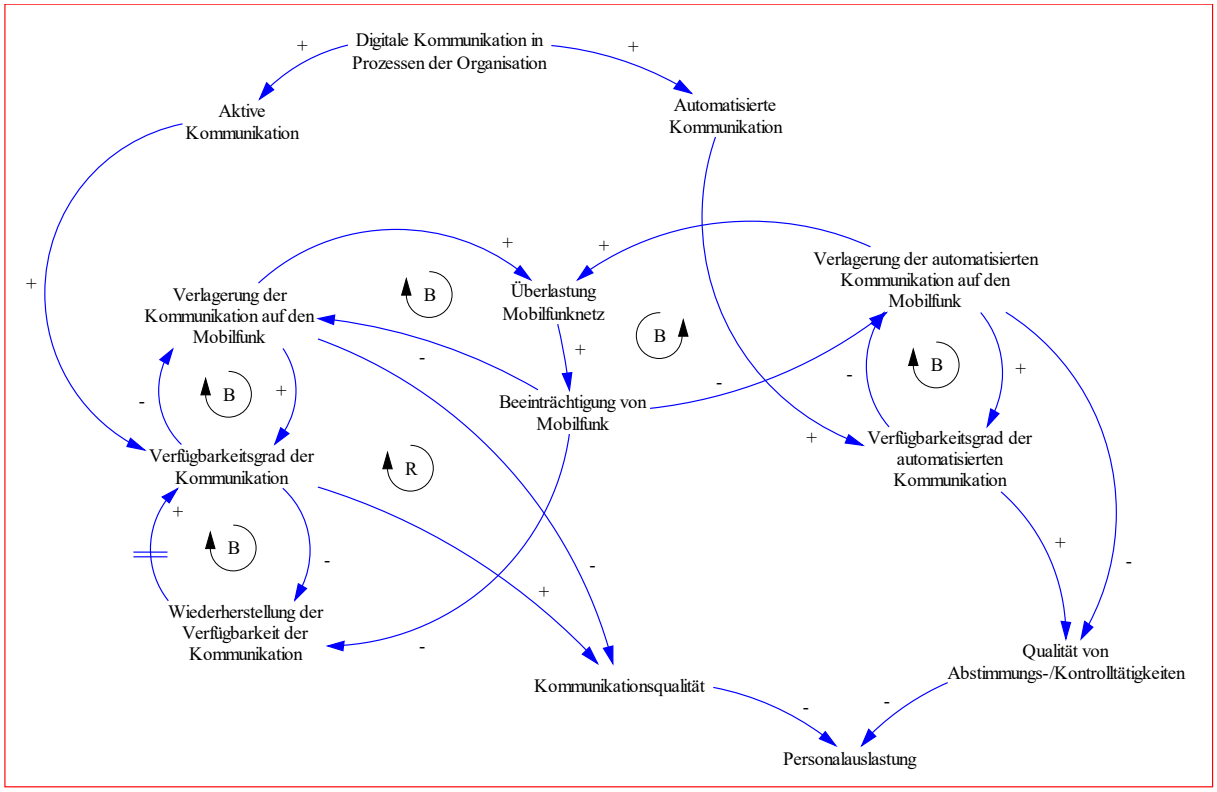



*Abbildung 12: Baustein Digitale Kommunikation in Prozessen der Organisation (vgl. Schachenhofer et al. 2022)*

### 6.1.4 Baustein: Verfügbarkeit abhängiger Leistungen

Die *Verfügbarkeit abhängiger Leistungen* (siehe Abbildung 13) zeigt, wie sich Verlagerungsprozesse auf die Leistungserbringung einer Organisation auswirken. Sie wirkt positiv auf die *Leistungserbringung Ist,* während mit einer geringeren *Verfügbarkeit abhängiger Leistungen* das *Ausmaß der umzusetzenden Business Continuity Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit* steigt. Mit der Zunahme dieser steigt wiederum ebenfalls die Variable *Korrekturmaßnahmen,* auf die in Kürze noch genauer eingegangen wird. Die Variable *Eingehende Anfragen* wirkt sich auf die *Leistungserbringung Soll* aus, da letztere mit der Anzahl eingehender Anfragen ebenfalls steigt. Umgekehrt ist es auch möglich, dass die Anzahl eingehender Anfragen sinkt, da keine Anfragen mehr an die zuständigen Akteure übermittelt werden können, wodurch auch die *Leistungserbringung Soll* vermindert wird. Wenn man davon ausgeht, dass *Eingehende Anfragen* zumindest noch innerhalb eines gewissen Zeitrahmens möglich sind, ist aufgrund der zuvor beschriebenen Verlagerungsprozesse und den damit verbundenen Beeinträchtigungen bzw. Verzögerungen in den organisationsinternen Abläufen mit einer *Diskrepanz zwischen Soll und Ist in der Leistungserbringung* zu rechnen. Entscheidet sich die betroffene Organisation nun für eine *Reduktion der Leistungserbringungsrate,* sinkt die *Leistungserbringung Soll*

temporär, wodurch sich die *Diskrepanz zwischen Soll und Ist bei der Leistungserbringung* erhöht. Entscheidet man sich in der betroffenen Organisation hingegen für *Korrekturmaßnahmen,* wirkt sich das mit einer gewissen, zeitlichen Verzögerung auf die *Leistungserbringung Ist* aus und die *Diskrepanz zwischen Soll und Ist* sinkt (Anmerkung: Wie in Kapitel 5.3 bereits erklärt wurde, zeigt das Verzögerungszeichen, dass eine Maßnahme mit einem gewissen Zeitaufwand verbunden ist). Darüber hinaus steht eine Erhöhung der Systemvariable *Leistungserbringung Ist* ebenfalls in einem positiven Wirkungszusammenhang mit der System-Outputvariable *Aufrechterhaltung der Betriebsfähigkeit.* Daraus ist die allgemein gültige Aussage ableitbar, dass je mehr bzw. wirksamere Korrekturmaßnahmen ergriffen werden, desto besser die tatsächliche Leistungserbringung einer Organisation aufrechterhalten werden kann, was sich wiederum ebenfalls positiv auf den Erhalt der Betriebsfähigkeit auswirkt (Schachenhofer et al. 2022).

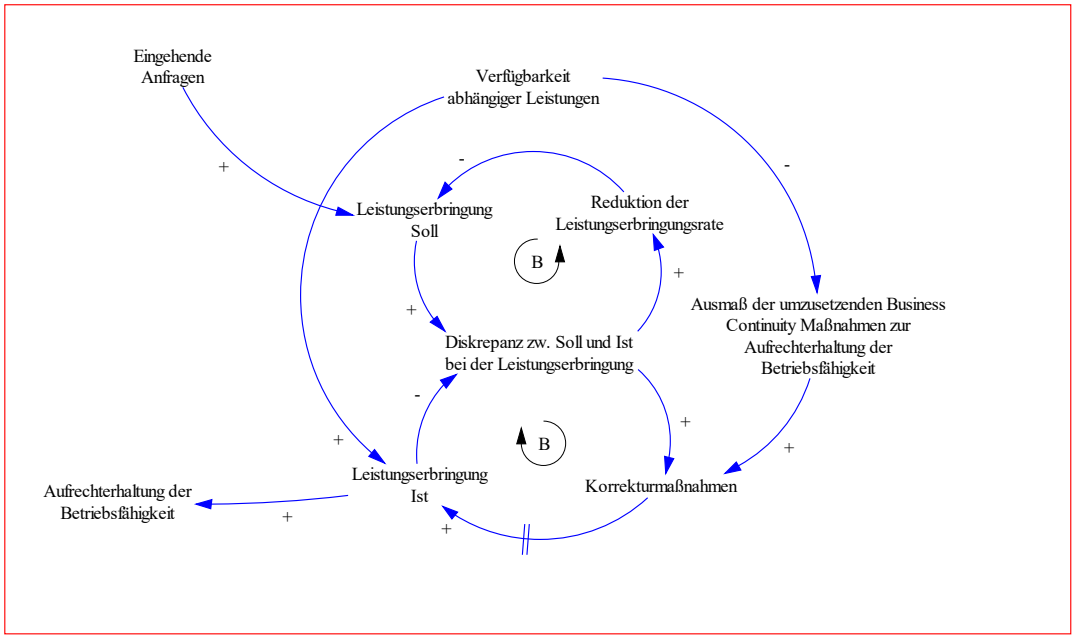
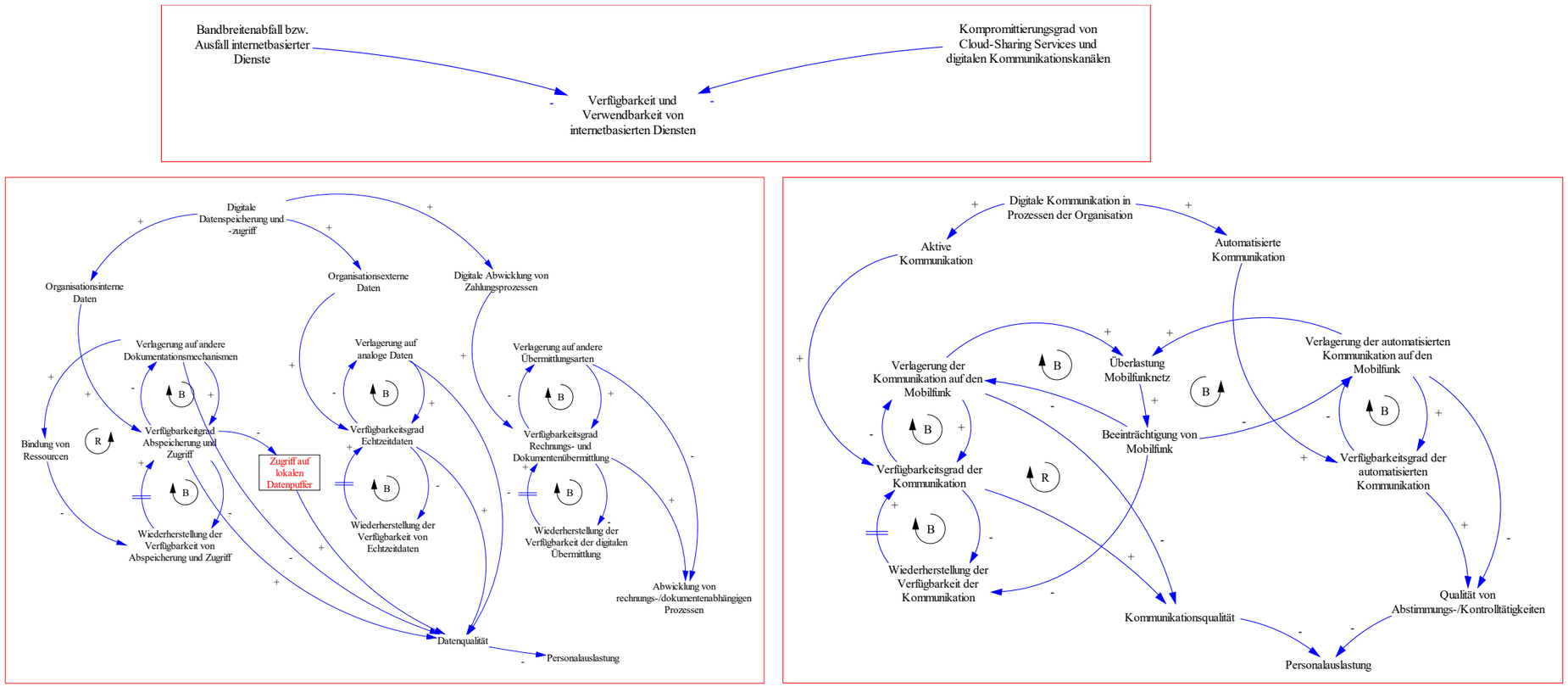



*Abbildung 13: Baustein Verfügbarkeit abhängiger Leistungen (vgl. Schachenhofer et al. 2022)*

Das Sektoren-Grundmodell kann aufgrund der Sektor-neutralen Darstellung betroffener Prozesse als Basis zur visuellen Darstellung von Rückkopplungseffekten bei einem Ausfall internetbasierter Dienste herangezogen werden und ermöglicht eine Anpassung und Erweiterung um organisationsspezifische Zusammenhänge. Reale Auswirkungen werden damit im Baukasten des Sektoren-Grundmodelles sektorübergreifend dargestellt, was eine Ableitung von Rückkopplungseffekten für verschiedenste Sektoren ermöglicht.

Die Aufteilung auf einzelne Bausteine ermöglicht es, die Verwendung des Modells individuell an einen Anwendungsfall anzupassen, um in einem Übungssetting die Auswirkungen bestimmter Feedbackschleifen zu betrachten. Eine Anordnung der verschiedenen Baukästen im Rahmen der Gesamtdarstellung ist in Abbildung 14 ersichtlich (Schachenhofer et al. 2022).



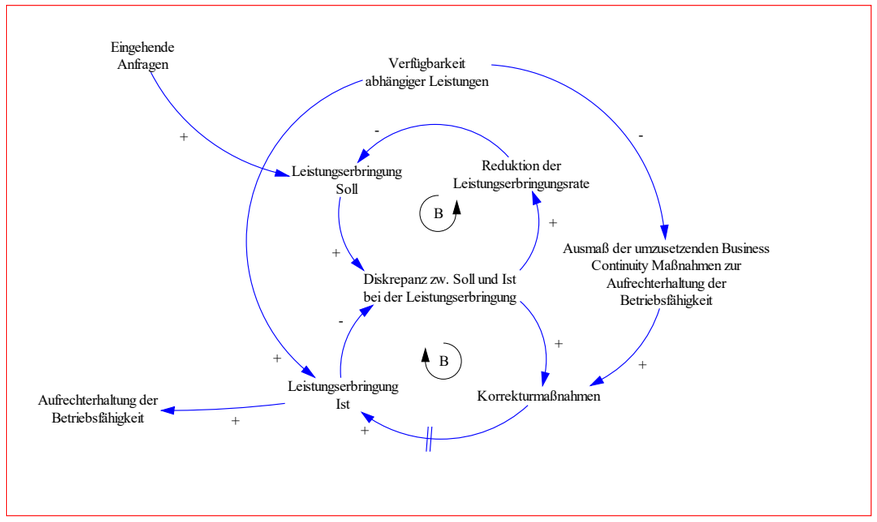




*Abbildung 14: Baukasten des Sektoren-Grundmodelles (vgl. Schachenhofer et al. 2022)*

Der Baukasten des Sektorengrundmodells umfasst alle bekannten Möglichkeiten einer Beeinträchtigung internetbasierter Dienste, von einer Einschränkung bis hin zu einem Totalausfall. Anhand des vorgestellten Ausgangsmodells können daher verschiedene Krisenszenarien bzw. Variationen mehrerer Faktoren in unterschiedlicher Ausprägung definiert werden, die in weiterer Folge als Basis für die Serious Games bzw. den Input aus der Praxis herangezogen werden können. Ausfallsszenarien können beispielsweise hinsichtlich

- ihrer Dauer, z.B. zwischen 0 bis 24 Stunden und darüber hinaus
- der Intensität der Einschränkung digitaler Dienste (in Prozent)
- der Anzahl betroffener Akteure
- sowie dem Zeitpunkt des Ereignisses (tagsüber oder nachts; besondere Stichtage, an welchen durch eine Beeinträchtigung digitaler Dienste eine Auszahlungsverzögerung eintritt etc.)

unterschieden werden. Als potenzielle Erweiterung des Krisenszenarios wäre im konkreten Fall etwa eine zusätzliche Überlastung des Mobilfunknetzes nach einer gewissen Zeit in Betracht zu ziehen (Schachenhofer et al. 2022). Das im Folgenden vorgestellte Szenario wurde gemeinsam im Team erarbeitet, um die Auswirkungen eines Ausfalls internetbasierter Dienste anhand eines konkreten Szenarios praktisch darzustellen. Es entspricht dem in ISIDOR gewählten Ausgangspunkt von einem „All Hazards"-Ansatz und unterscheidet klar zwischen organisationsexternen und organisationsinternen Netzen.

*„Aufgrund eines Ereignisses, dessen Ursache zum Zeitpunkt des Eintritts unbekannt ist (bspw. technisches Gebrechen oder eine menschliche Fehlleistung), kommt es im jeweiligen Organisationssektor zu einem Ausfall internetbasierter Dienste. Dabei sind sämtliche Kommunikationskanäle und Dienste, die über externe Service-Provider wie A1, Magenta oder Drei laufen, betroffen. Organisationsinterne Netze (LAN, interne VPNs) sind davon nicht betroffen, d.h. die organisationsinterne Kommunikation zwischen verschiedenen Standorten bleibt weiterhin aufrecht, sofern diese über interne Leitungen angebunden sind. Folglich ist sowohl die digitale Datenübertragung, als auch die digitale Kommunikation und die Nutzung einer Vielzahl digitaler Services, die durch externe Service-Provider zur Verfügung gestellt werden, vorübergehend nicht möglich."*

## 6.2 Modell mit Bezug zum Gesundheitssektor

### 6.2.1 Einleitung und Systemvariablen-Tabelle

Das im Rahmen dieses Kapitels beschriebene CLD, welches in Abbildung 16 ersichtlich ist, zeigt exemplarisch die Auswirkungen eines großflächigen und langanhaltenden Ausfalls internetbasierter Dienste auf Elemente mit Bezug zum Gesundheitssystem. Dabei werden Aspekte der digitalen Datenspeicherung und des digitalen Datenzugriffes im Rahmen organisationsinterner und -externer Daten, die aktive und standardisierte digitale Kommunikation, sowie die Telemedizin als Hybridaspekt zwischen digitalem Datenzugriff und digitaler Kommunikation dargestellt.

Bevor das Modell selbst beschrieben wird, sollen in Tabelle 3 zunächst jene Variablen des CLD-Modells erklärt werden, deren Bedeutung bzw. Wirkungsbereich nicht bereits eindeutig aus dem Variablennamen hervorgeht. Die Systemvariablen wurden anhand der Ergebnisse aus den Interviews und der systematischen Literaturrecherche definiert.

*Tabelle 3: Systemvariablentabelle mit Bezug zum Gesundheitssektor (vgl. Schachenhofer et al. 2022)*

| | |
|---|---|
| Bandbreitenabfall bzw. Ausfall internetbasierter Dienste | Von der Internetbandbreite (gemessen in Megabit pro Sekunde) hängt ab, wie viele Daten digital übertragen werden können. Ein Bandbreitenabfall wirkt sich z.B. auf die digitale Übermittlung von Dokumenten aus. Im Modell wird davon ausgegangen, dass sie teilweise oder gänzlich abfällt oder internetbasierte Dienste teilweise oder gänzlich ausfallen. |
| Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen | In der Cloud (Daten- bzw. Internetwolke) können beispielsweise Daten und Dokumente digital abgespeichert und gemeinschaftlich genutzt bzw. bearbeitet werden. Kommunikationskanäle dienen dazu, sich auszutauschen bzw. Informationen zu vermitteln. Digitale Kommunikationskanäle sind bspw. E-Mail und Messenger-Dienste. Im Modell wird davon ausgegangen, dass die Dienste kompromittiert sind. Nutzer:innen können nicht mehr auf die Sicherheit ihrer Daten vertrauen und werden nach und nach die Nutzung dieser Dienste einstellen. |
| Digitale Datenspeicherung und -zugriff | Sämtliche Abspeicherungsprozesse und der Zugriff auf Daten und Dokumente über Cloud-Dienste sind von der Beeinträchtigung betroffen und somit vorübergehend nicht möglich. |
| Digitale Kommunikation in Prozessen der Organisation | Das betrifft sämtliche Kommunikationsformen über digitale Kanäle (schriftlich und mündlich, sowie den Austausch von Daten und Dokumenten per Videotelefonie bzw. über Videokonferenzsysteme) zwischen Stakeholder:innen der Organisation. |
| Automatisierte Kommunikation (Auftrags- und Standortübermittlung) | Diese Systemvariable umfasst die digitale Übermittlung von Aufträgen und damit in Zusammenhang stehenden Daten z.B. durch Rettungswägen sowie von standortbezogenen Daten. |
| Echtzeitdaten aus der Umwelt | Echtzeitdaten werden regelmäßig und zeitnah erfasst und laufend digital aktualisiert. |

| | |
|---|---|
| | Der Zugriff auf Echtzeitdaten, die oft durch Drittparteien zur Verfügung gestellt werden, erfolgt ebenfalls digital. Echtzeitdaten sind z.B. Informationen zu Routenoptionen und zur aktuellen Verkehrslage. |
| Telemedizin | Medizinische Dienstleistungen, die mithilfe von Informations- und Kommunikationstechnologien erbracht werden, wobei Patient:in und Gesundheitsdienstanbieter an unterschiedlichen Orten sind, werden unter dem Begriff Telemedizin zusammengefasst. Gemeint sind damit z.B. die digitale Überwachung des Gesundheitszustandes von Patient:innen (Telemonitoring) und digitale Therapieformen über räumliche Distanzen (Teletherapie) (vgl. Laschkolnig 2021: 1). |
| Überlastung Mobilfunknetz | Aufgrund einer hohen Anzahl an Benutzer:innen bzw. einer großen Menge an zu übertragenden Daten kann es im Mobilfunknetz, wie in allen Netzen, zu Überlastungserscheinungen in Form von Verzögerungen bzw. Ausfällen kommen. Dies beeinflusst wiederum den Durchsatz (die Menge an übertragenen Daten in einem bestimmten Zeitraum) beispielsweise bei Netzüberlastung in einem bestimmten, geografisch abgegrenzten, Gebiet. |
| Datenqualität | Die Qualität der vorhandenen Daten, hinsichtlich Aktualität, Vollständigkeit, Korrektheit, etc. kann durch die Beeinträchtigung vorgelagerter Systemvariablen vermindert werden. |
| Kommunikationsqualität | Die Kommunikationsqualität zeigt sich in der Erreichbarkeit der gewünschten Personen, den verfügbaren Kommunikationskanälen und den damit zusammenhängenden Möglichkeiten (z.B. Bildschirmübertragung und Versenden von Dokumenten) und hat Auswirkungen auf Faktoren wie elektronische Beschaffung, digitale Bereitstellung von Services und Instandhaltung über digitale Kommunikationskanäle. |
| Qualität der Abstimmung | Das betrifft die Abstimmung zwischen verschiedenen Organisationen oder Organisationseinheiten, die digital und automatisiert passiert. Bei einer verminderten Verfügbarkeit internetbasierter Dienste ist diese nur |

| | |
|---|---|
| | eingeschränkt bzw. unter Umständen gar nicht möglich. |
| Verfügbarkeit abhängiger Leistungen | Das betrifft sämtliche, von einer Organisation zu erbringenden Leistungen, die von den vorgelagerten Qualitätsvariablen abhängig sind, z.B. Teletherapie. |
| Korrekturmaßnahmen | Unter diesem Begriff werden sämtliche Maßnahmen zusammengefasst, um die Leistungserbringung während eines Ausfallsereignisses zu steigern (z. B. zusätzlicher Personaleinsatz). |
| Gesellschaftliches medizinisches Versorgungsniveau | Das Versorgungsniveau der Gesellschaft und die damit zusammenhängende Bereitstellung benötigter Leistungen des Gesundheitssystems ist abhängig von der Verfügbarkeit vorgelagerter Variablen bzw. der Durchführbarkeit vorgelagerter Prozesse. |

Das Modell ist folgendermaßen strukturiert: Startpunkte sind jeweils die beiden Variablen in der obersten Zeile rechts und links: *Bandbreitenabfall bzw. Ausfall internetbasierter Dienste* und *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen*. Diese stellen die Beeinträchtigung internetbasierter Dienste bzw. einen Internetausfall als Ausgangssituation dar und wirken auf die nachfolgenden, zentralen Themenbereiche

- Digitale Datenspeicherung und -zugriff und
- Digitale Kommunikation in Prozessen der Organisation.

Der Themenbereich *Digitale Datenspeicherung und -zugriff* beinhaltet die Sub-Bereiche *Organisationsinterne Daten, Echtzeitdaten aus der Umwelt* und *Telemedizin.*

Der Themenbereich *Digitale Kommunikation in Prozessen der Organisation* umfasst zum einen die Sub-Bereiche *Aktive Kommunikation* und *Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)*, zum anderen hat er ebenfalls eine Verbindung zu dem Sub-Themenbereich *Telemedizin.*

In weiterer Folge werden in den jeweiligen Sub-Themenbereichen mögliche Verlagerungsschleifen in Form des Archetyps „Shifting the Burden“ ersichtlich. Zum besseren Verständnis werden die ablaufenden Prozesse im Rahmen dieses Archetyps anhand eines Praxisbeispiels aus den Erkenntnissen des Gesundheitssektors (Krankentransporte) erklärt. Abbildung 15 stellt die Abläufe beispielhaft dar.

Die Auftragsübermittlung an Gesundheitsorganisationen, die im Krankentransport tätig sind, erfolgt teilweise digital. Wenn bei *Leitstelle (1)* die Übertragung von Daten über das Internet gestört ist, ist folglich auch die digitale Auftragsübermittlung beeinträchtigt (ist das zu Grunde liegende Problem). Die Konsequenz daraus ist die erschwerte bzw. gänzlich unmögliche Auftragsbearbeitung durch *Leitstelle (1)* (ist das Symptom). Daher erfolgt eine Umleitung der Aufträge von *Leitstelle (1)* an *Leitstelle*

*(2)*. Somit wird das Symptom, aber nicht die eigentliche Ursache bekämpft. Daraus entsteht ein sich selbst verstärkender Nebeneffekt: Die Auslastung auf *Leitstelle (2)* steigt und hat möglicherweise Personal- oder anderweitige Ressourcenengpässe zur Folge. Je mehr man sich dementsprechend der reinen Symptombekämpfung widmet, desto mehr tritt die eigentliche Lösung des Problems in den Hintergrund, was die nachhaltige Problemlösung mittel- und langfristig beeinträchtigt (Schachenhofer et al. 2022).

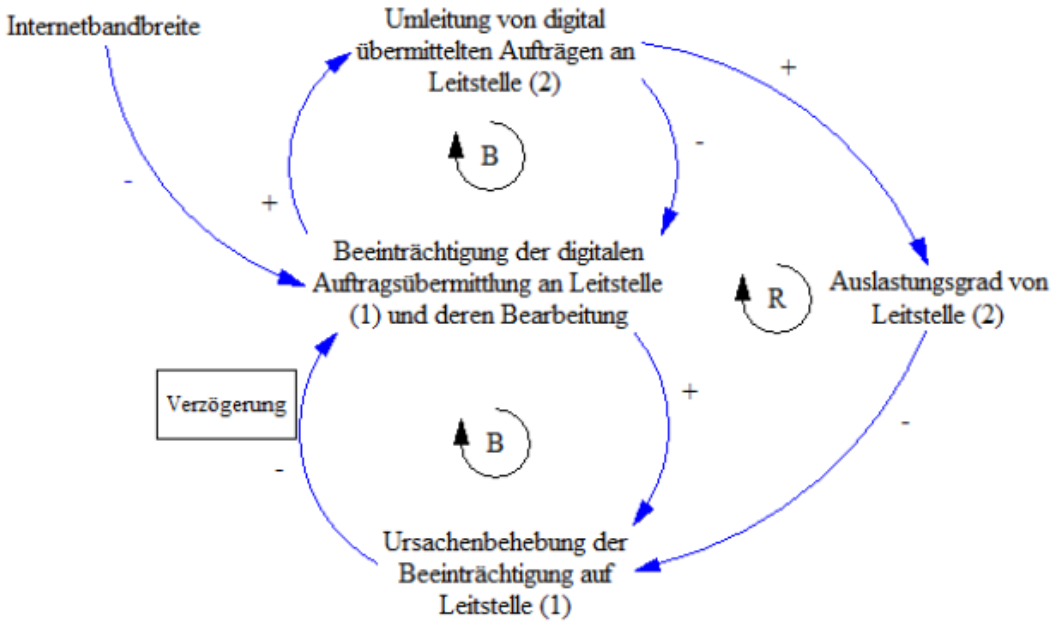



*Abbildung 15: Veranschaulichung des Archetyps „Shifting the Burden“ (vgl. Schachenhofer et al. 2022)*

Anhand dieses Beispiels wird ersichtlich, dass sich diese Verlagerungseffekte nachteilig auf nachgelagerte Prozesse bzw. das System auswirken können. In dem Modell, welches das System als Ganzes darstellt (siehe Abbildung 16) zeigen sich die Auswirkungen eines Ausfalls internetbasierter Dienste ebenso als Folge der verschiedenen Verlagerungsprozesse, die dadurch ausgelöst werden. Dies wird anhand der Beeinträchtigung der nachgelagerten Qualitätsvariablen *Datenqualität, Kommunikationsqualität* und *Qualität der Abstimmung* ersichtlich.

Die Qualitätsvariablen beeinflussen sowohl organisationsinterne als auch -externe Variablen. Diese wirken sich wiederum auf die erbrachten Leistungen aus, was den in Kapitel 5.3 beschriebenen Archetyp „Eroding Goals“ in Gang setzt. Dieser wirkt sich schlussendlich auf die Output-Variable *Gesellschaftliches medizinisches Versorgungsniveau* aus (Schachenhofer et al. 2022).

### 6.2.2 Beschreibung des Causal Loop Diagramms

In Abbildung 16 ist das CLD mit Bezug zu Elementen aus dem Gesundheitssektor dargestellt. Eine detailliertere Modellierung bzw. Analyse des Ausfalls kann in weiterer Folge von den verantwortlichen Sektorexpert:innen auf Basis dieses Grundmodelles entwickelt werden. Im Rahmen des vorliegenden Modelles werden die verschiedenen Bereiche von Organisationen im Gesundheitsbereich ersichtlich, auf die sich eine etwaige Bandbreiteneinschränkung bzw. ein Internetausfall auswirken kann. Die Wirkungsbeziehungen zwischen den Systemvariablen werden im Folgenden näher erläutert.[3]

[3] Anmerkung zum Modell: Systemvariablen, die im Modell definierte Notfallmaßnahmen darstellen, wurden mit einem * markiert.

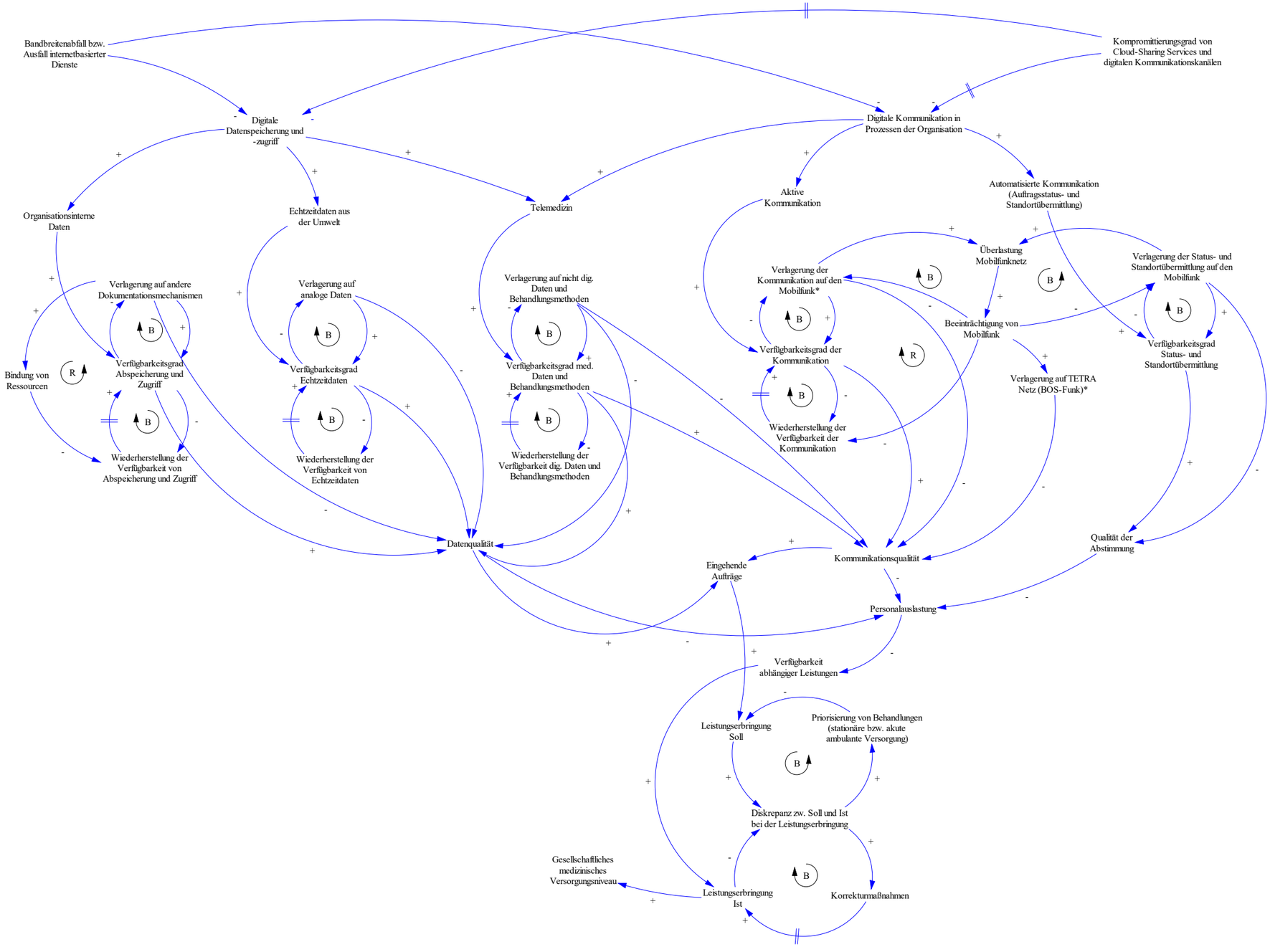



*Abbildung 16: Causal Loop Diagramm mit Bezug zum Gesundheitssektor (vgl. Schachenhofer et al. 2022)*

### 6.2.3 Auswirkungen und Verlagerungen in den verschiedenen Themenbereichen

Die Ausgangssituation wird durch einen *Bandbreitenabfall bzw. den Totalausfall internetbasierter Dienste*, sowie den *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen* bestimmt.

Diese Ausgangsvariablen wirken sich negativ auf die zentralen Themenbereiche

- Digitale Datenspeicherung und -zugriff und
- Digitale Kommunikation in Prozessen der Organisation, und deren Sub-Themenbereiche
- Organisationsinterne Daten,
- Echtzeitdaten aus der Umwelt,
- Telemedizin,
- Aktive Kommunikation
- und Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)

aus.

Nachfolgend werden die Betroffenheit der einzelnen Variablen, sowie etwaige Verlagerungsschleifen näher erläutert (Schachenhofer et al. 2022).

#### *6.2.3.1 Digitale Datenspeicherung und -zugriff – Organisationsinterne Daten*

*Digitale Datenspeicherung und -zugriff* wirkt sich positiv auf *Organisationsinterne Daten* aus, die wiederum eine positive Wirkung auf den *Verfügbarkeitsgrad Abspeicherung und Zugriff* haben. Hier beginnen nun Wechselwirkungen, die den Archetyp „Shifting the Burden“ widerspiegeln. Der *Verfügbarkeitsgrad Abspeicherung und Zugriff* wirkt negativ auf *Verlagerung auf andere Dokumentationsmechanismen* ein, diese Variable wiederum positiv auf *Verfügbarkeitsgrad Abspeicherung und Zugriff* (vgl. ISIDOR Expert:inneninterviews 2021). Es entsteht somit ein ausbalancierter geschlossener Rückkopplungskreis, da mehr auf andere Dokumentationsmechanismen verlagert wird, je weniger Abspeicherung und Zugriff digital verfügbar sind. Je mehr andere Dokumentationsmechanismen angewendet werden, desto mehr organisationsinterne Daten sind über andere Wege verfügbar.

*Verlagerung auf andere Dokumentationsmechanismen* wirkt positiv auf *Bindung von Ressourcen* ein, beispielsweise durch erhöhten Personalbedarf (vgl. Adams et al. 2019: 97). Diese Variable ist negativ verknüpft mit *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff*. Zusammen mit der verzögerten positiven Verbindung zum *Verfügbarkeitsgrad Abspeicherung und Zugriff* entsteht hier ein sich selbst verstärkender Rückkopplungskreis, da umso mehr Ressourcen gebunden werden, desto mehr auf andere Dokumentationsmechanismen verlagert wird und somit weniger Ressourcen für die Problemlösung vorhanden sind. Diese wären jedoch notwendig, um für die eigentliche Problemlösung durch die Wiederherstellung der Verfügbarkeit genutzt zu werden.

An dieser Stelle gibt es darüber hinaus noch einen weiteren ausbalancierten Rückkopplungskreis, der durch die negative Verbindung von *Verfügbarkeitsgrad Abspeicherung und Zugriff* zur *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff* und die positive Wirkungsbeziehung zurück entsteht. Das heißt: Je mehr organisationsinterne Daten verfügbar sind, desto weniger besteht die Notwendigkeit zur Wiederherstellung der Verfügbarkeit dieser über digitale Zugriffs- bzw. Abspeicherungsmethoden. Je mehr aber die Wiederherstellung betrieben wird, desto mehr ist auch nach einer Verzögerung die Verfügbarkeit dieser Daten über digitale Wege gegeben und diese Wechselwirkungen stehen miteinander im Gleichgewicht.

#### *6.2.3.2 Digitale Datenspeicherung und -zugriff – Echtzeitdaten aus der Umwelt*

*Digitale Datenspeicherung und -zugriff* steht in einem positiven Wirkungszusammenhang mit *Echtzeit-Daten aus der Umwelt.* Diese wirken positiv auf *Verfügbarkeitsgrad Echtzeitdaten* ein (vgl. Fauss 2018: 128). Der Verfügbarkeitsgrad wirkt wiederum negativ auf die *Verlagerung auf analoge Daten* und diese wirkt positiv zurück auf den Verfügbarkeitsgrad. Der ausbalancierte Rückkopplungskreis, der hier entsteht, bedeutet, dass je mehr Verfügbarkeit von Echtzeitdaten gegeben ist, desto weniger muss verlagert werden und je weniger verlagert werden muss, desto mehr Verfügbarkeit ist gegeben. *Verfügbarkeitsgrad Echtzeitdaten* wirkt wiederum negativ auf die *Wiederherstellung der Verfügbarkeit von Echtzeitdaten ein*, da je mehr Echtzeitdaten verfügbar sind, desto weniger eine Wiederherstellung dieser forciert wird. Sofern eine Wiederherstellung dieser unternommen wird, wirkt dies wiederum positiv auf *Verfügbarkeitsgrad Echtzeitdaten*. Durch diese Wirkungsbeziehungen entsteht ein weiterer, ausbalancierter Rückkopplungskreis.

#### *6.2.3.3 Digitale Datenspeicherung und -zugriff & Digitale Kommunikation in Prozessen der Organisation – Telemedizin*

Charakteristisch für den Sub-Themenbereich *Telemedizin* ist, dass dieser sowohl Teil des zentralen Themenbereiches *Digitale Datenspeicherung und -zugriff*, als auch *Digitale Kommunikation in Prozessen der Organisation* ist. Beide haben einen positiven Wirkungszusammenhang zur *Telemedizin,* die ebenfalls positiv auf den *Verfügbarkeitsgrad med. Daten und Behandlungsmethoden* wirkt. Der Verfügbarkeitsgrad wiederum wirkt negativ auf die *Verlagerung auf nicht digitale Daten und Behandlungsmethoden*, da umso mehr Verlagerung vorgenommen werden muss, desto weniger medizinische Daten und Behandlungsmethoden digital verfügbar sind. Die Verlagerung wiederum bedingt eine Erhöhung der Verfügbarkeit der benötigten Daten und Behandlungsmethoden, woraus ein ausbalancierter Rückkopplungskreis, der diesen Wirkungszusammenhang veranschaulicht, entsteht. Die Verlagerung kann jedoch nur eingeschränkt erfolgen, was sich negativ auf die *Datenqualität* und die *Kommunikationsqualität* auswirkt. Je mehr Daten und Behandlungsmethoden verfügbar sind, desto weniger wird eine *Wiederherstellung der Verfügbarkeit digitaler Daten und Behandlungsmethoden* forciert. Sofern dies jedoch getan wird, wirkt dies wiederum verzögert positiv auf den *Verfügbarkeitsgrad med. Daten und Behandlungsmethoden*, wodurch ein weiterer ausbalancierter Rückkopplungskreis entsteht (vgl. ISIDOR SKKM-Sektorenworkshops 2021).

#### 6.2.3.4 Digitale Kommunikation in Prozessen der Organisation – Aktive Kommunikation

*Digitale Kommunikation in Prozessen der Organisation* wirkt sich positiv auf die *Aktive Kommunikation* aus, die ebenfalls positiv auf den *Verfügbarkeitsgrad der Kommunikation* wirkt. Der Verfügbarkeitsgrad wiederum wirkt negativ auf die *Verlagerung der Kommunikation auf den Mobilfunk* und diese wiederum positiv auf den *Verfügbarkeitsgrad der Kommunikation*. Ein ausbalancierter Rückkopplungskreis entsteht durch die Möglichkeit der Verlagerung (vgl. Wurmb et al. 2020: 449f; ISIDOR Expert:inneninterviews 2021). Dasselbe ist bei der zu Grunde liegenden Problemlösung der Fall: Die negative Verbindung zwischen *Verfügbarkeitsgrad der Kommunikation* und *Wiederherstellung der Verfügbarkeit der Kommunikation* bedeutet eine erhöhte Notwendigkeit der Wiederherstellung, je weniger Kommunikation verfügbar ist. Diese ist mit Verzögerung mit dem *Verfügbarkeitsgrad der Kommunikation* positiv verknüpft, also je mehr diese Wiederherstellung erfolgt, desto höher ist in der Folge wiederum die Verfügbarkeit der (digitalen) Kommunikation. Diese Wirkungszusammenhänge bilden einen ausbalancierten Rückkopplungskreis.

Darüber hinaus entstehen an dieser Stelle einige Schleifen, die mit der Verlagerung der Kommunikationsprozesse in Verbindung stehen. Die *Verlagerung der Kommunikation auf den Mobilfunk* wirkt auf die *Überlastung Mobilfunknetz* positiv ein, das wiederum beeinflusst die *Beeinträchtigung von Mobilfunk* positiv, das wiederum wirkt auf die *Verlagerung der Kommunikation auf den Mobilfunk* negativ. Ein ausbalancierter Rückkopplungskreis entsteht, da je mehr der Mobilfunk als Ausweichmöglichkeit genutzt wird, desto mehr steigt die Wahrscheinlichkeit der Netzüberlastung und damit auch die Beeinträchtigung des Mobilfunks, der in Folge dessen weniger (bzw. im schlimmsten Fall gar nicht mehr) genutzt werden kann.

Es besteht auch eine negative Verbindung zwischen *Beeinträchtigung von Mobilfunk* und *Wiederherstellung der Verfügbarkeit der Kommunikation*, wodurch sich ein sich selbst verstärkender Rückkopplungskreis zwischen *Verlagerung der Kommunikation auf den Mobilfunk*, *Überlastung Mobilfunknetz*, *Beeinträchtigung von Mobilfunk*, *Wiederherstellung der Verfügbarkeit der Kommunikation* und *Verfügbarkeitsgrad der Kommunikation* ergibt. Denn je weniger digitale Kommunikation verfügbar ist, desto mehr wird auf den Mobilfunk verlagert, desto mehr ist dieser aber potenziell überlastet und beeinträchtigt, desto weniger kann die Wiederherstellung durchgeführt werden, was sich ebenso nachteilig auf die Verfügbarkeit der Kommunikation auswirkt.

Es besteht eine positive Verbindung zwischen *Beeinträchtigung von Mobilfunk* und *Verlagerung auf TETRA Netz (BOS-Funk)*, da es im Gesundheitssystem den BOS-Funk als weitere Sicherheitsebene bei Verbindungsausfällen gibt (vgl. ISIDOR Expert:inneninterviews 2021). Der BOS-Funk steht Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zur Verfügung. Dieses Funksystem entspricht den Grundsätzen der Einheitlichkeit und Hochverfügbarkeit, sowie den speziellen Anforderungen der Blaulichtorganisationen. Das umfasst neben einer zuverlässigen und effektiven Funktionsweise die optimale Unterstützung bei einer koordinierten Einsatzabwicklung. In Österreich wird das Digitalfunknetz BOS Austria durch die Feuerwehr, Polizei, Rettung (inklusive Berg- und Wasserrettung) und die Bezirkshaupt-

mannschaften, Landesregierungen, sowie das Bundesheer genutzt. Das Sicherheitsfunknetz dient dabei der Bewältigung von Krisen-, Katastrophen- und Großschadensereignissen, sowie für alltägliche Einsätze und Notfälle. Dabei kommt der internationale und explizit für den digitalen Bündelfunk definierte TETRA Standard (TErrestrial TRunked Radio) zum Einsatz (vgl. Oö. Landesfeuerwehr Verband 2020: 4, 27).

Im Zusammenhang mit dem TETRA Netz spricht man oft auch vom BOS-Digitalfunknetz. Nichtsdestotrotz handelt es sich dabei um Funkkommunikation. Das BOS-Digitalfunknetz besteht aus einzelnen Funkzellen und Informationen werden mittels Funkwellen von einem Endgerät zur Basisstation übermittelt. (vgl. Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben 2021: 20). Es gibt zwei verschiedene Betriebsarten. Im Netzmodus hat das Funkgerät über das Digitalfunknetz eine Verbindung zur Basisstation. Im TMO Modus (Trunked Mode Operation) besteht die Möglichkeit, alle Funkstellen im BOS Austria Netz zu erreichen, die sich auf derselben Sprechgruppe befinden (vgl. Oö. Landesfeuerwehr Verband 2020: 31). Die besondere Netzarchitektur ermöglicht den Einsatzkräften der BOS eine Netzverfügbarkeit, die über jene kommerzieller Mobilfunknetze hinausgeht und damit auch in Krisensituationen besteht (vgl. Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben 2021: 13).

#### *6.2.3.5 Digitale Kommunikation in Prozessen der Organisation – Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)*

Die *Automatisierte Kommunikation* (*Auftragsstatus- und Standortübermittlung)*, die in einem positiven Wirkungszusammenhang mit dem zentralen Themenbereich *Digitale Kommunikation in Prozessen der Organisation* steht, wirkt sich positiv auf den *Verfügbarkeitsgrad Status- und Standortübermittlung* aus. Dieser wiederum wirkt negativ auf die *Verlagerung der Status- und Standortübermittlung auf Mobilfunk*, die positiv zurück auf den *Verfügbarkeitsgrad Status- und Standortübermittlung* wirkt (vgl. ISIDOR Expert:inneninterviews 2021). Es entsteht ein ausbalancierter Rückkopplungskreis, da je weniger die Verfügbarkeit gegeben ist, desto mehr wird verlagert und desto mehr ist die Verfügbarkeit von Status- und Standortübermittlung danach wieder gegeben. Die *Verlagerung der Status- und Standortübermittlung auf Mobilfunk* wirkt sich positiv auf *Überlastung Mobilfunknetz* aus, diese wiederum positiv auf die *Beeinträchtigung von Mobilfunk.* Die letztgenannte Variable wirkt negativ zurück auf die Möglichkeit der Verlagerung, da sie diese durch die vorangegangene Überlastung des Mobilfunknetzes verschlechtert. Analog zur Kommunikation entsteht hier wieder ein ausbalancierter Rückkopplungskreis, wenn der Mobilfunk überlastet ist.

### 6.2.4 Auswirkungen der verschiedenen Themenbereiche auf die Qualitätsvariablen

Die zuvor beschriebenen Themenbereiche inklusive der Verlagerungsschleifen wirken sich auf die nachfolgenden Qualitätsvariablen *Datenqualität, Kommunikationsqualität,* und *Qualität der Abstimmung* aus.

Der *Verfügbarkeitsgrad Abspeicherung und Zugriff* wirkt sich positiv auf die *Datenqualität* aus, *Verlagerung auf andere Dokumentationsmechanismen* jedoch negativ, da es durch die Verlagerung zu Qualitätsverlusten kommt.

Auch der *Verfügbarkeitsgrad von Echtzeitdaten* wirkt sich positiv auf die *Datenqualität aus, die Verlagerung auf analoge Daten* wiederum negativ, da auch hier mit Qualitätseinbußen im Hinblick auf die verfügbare *Datenqualität* zu rechnen ist.

Ebenso wirkt sich der *Verfügbarkeitsgrad med. Daten und Behandlungsmethoden* positiv auf die *Datenqualität* aus, während eine *Verlagerung auf nicht dig. Daten und Behandlungsmethoden* eine negative Wirkungsbeziehung zur *Datenqualität* hat. Darüber hinaus wirkt sich der *Verfügbarkeitsgrad med. Daten und Behandlungsmethoden* positiv auf *die Kommunikationsqualität* aus, während die *Verlagerung auf nicht dig. Daten- und Behandlungsmethoden* sich auf die *Kommunikationsqualität* negativ auswirkt, da eine Verlagerung diese herabsetzt.

Der *Verfügbarkeitsgrad der Kommunikation* wirkt sich positiv auf die *Kommunikationsqualität* aus, die *Verlagerung der Kommunikation auf den Mobilfunk* und die *Verlagerung auf TETRA Netz (Sprachfunk)* jedoch negativ. Der Grund dafür ist, dass mit zunehmender Verfügbarkeit der Kommunikation auch die Qualität dieser steigt, während sie durch notwendige Verlagerungen aufgrund von Einschränkungen abnimmt.

Ähnliche Auswirkungen auf die nachfolgende Qualitätsvariable hat eine Verlagerung im Rahmen der *Automatisierten Kommunikation (Status- und Standortübermittlung)*: der *Verfügbarkeitsgrad Status- und Standortübermittlung* wirkt sich positiv auf die *Qualität der Abstimmung* aus, die *Verlagerung der Status- und Standortübermittlung auf den Mobilfunk* hingegen negativ (vgl. ISIDOR Expert:inneninterviews 2021; Schachenhofer et al. 2022).

### 6.2.5 Auswirkungen der Qualitätsvariablen organisationsintern und auf Drittparteien

Die zuvor beschriebenen Verlagerungen zeigen Auswirkungen auf die organisationsinternen Variablen *Eingehende Aufträge* und *Personalauslastung.* Diese wirken sich weiter auf externe Drittparteien bzw. Patient:innen in Form der Variable *Verfügbarkeit abhängiger Leistungen* aus (Schachenhofer et al. 2022).

#### *6.2.5.1 Organisationsinterne Auswirkungen*

*Datenqualität* und *Kommunikationsqualität* wirken sich positiv auf *Eingehende Aufträge* aus (vgl. ISIDOR Expert:inneninterviews 2021). Je besser die Datenlage ist und umso besser die Kommunikation funktioniert, desto mehr Aufträge können auch an die Organisation übermittelt werden. Auf die Variable *Personalauslastung* wirken alle drei Qualitätsvariablen *Datenqualität*, *Kommunikationsqualität*, und *Qualität der Abstimmung* negativ ein, da eine verringerte Qualität in allen drei Fällen mit einer erhöhten Auslastung einhergeht (vgl. Wurmb et al. 2020: 449; ISIDOR Expert:inneninterviews 2021). Über die beiden Qualitätsvariablen *Datenqualität* und *Kommunikationsqualität* veranschaulicht das vorliegende Modell außerdem einen wesentlichen Zusammenhang zwischen dem *Verfügbarkeitsgrad med. Daten und Behandlungsmethoden* und der *Personalauslastung*, da diese geringer ist, wenn der Verfügbarkeitsgrad telemedizinischer Prozesse höher ist (vgl. Wurmb et al. 2020: 449). Sofern

die Prozesse innerhalb einer Organisation nicht in der erforderlichen Qualität ablaufen, ist ein erhöhter Aufwand nötig, damit die Organisation dennoch entsprechende Leistungen erbringen kann.

#### *6.2.5.2 Auswirkungen auf Drittparteien*

Die *Personalauslastung* wirkt negativ auf die *Verfügbarkeit abhängiger Leistungen*, da eine erforderliche Verlagerung auf nicht digitale Daten und Behandlungsmethoden dazu führt, dass Arbeitsprozesse nicht so effizient wie gewohnt abgewickelt werden können (vgl. Wurmb et al. 2020: 449; Deutsche Krankenhausgesellschaft 2019: 35f; ISIDOR Expert:inneninterviews 2021). Die Variable *Verfügbarkeit abhängiger Leistungen* stellt die zentralen Auswirkungen auf Drittparteien dar, die den Archetyp „Eroding Goals“ in Gang setzt.

Die *Verfügbarkeit abhängiger Leistungen* wirkt positiv auf die *Leistungserbringung Ist* ein, diese wiederum wirkt negativ auf *Diskrepanz zw. Soll und Ist bei der Leistungserbringung*. *Eingehende Aufträge* wirken positiv auf *Leistungserbringung Soll* ein, diese wiederum wirkt auch positiv auf *Diskrepanz zw. Soll und Ist bei der Leistungserbringung* ein. Je weniger Leistungen verfügbar sind, desto geringer ist das Niveau der tatsächlichen Leistungserbringung, je mehr Aufträge allerdings eingehen, desto höher ist das Niveau der geforderten Leistungserbringung. Hier entsteht eine Diskrepanz zwischen Soll und Ist. Diese wirkt positiv auf die *Priorisierung von Behandlungen (stationäre bzw. akute ambulante Versorgung)* ein, die wiederum in einer negativen Wirkungsbeziehung mit der *Leistungserbringung Soll* steht (vgl. Adams et al. 2019: 97; Ghafur et al. 2019: 4f; ISIDOR Expert:inneninterviews 2021). Der ausbalancierte Rückkopplungskreis, der hier entsteht, zeigt, dass je größer die Lücke zwischen Soll und Ist der Leistungen ist, desto mehr müssen bestimmte Behandlungen vorgezogen und andere vernachlässigt werden (Stichwort: Triage), das verfolgte Niveau der Leistungserbringung wird also nach unten korrigiert und so verringert sich auch die Lücke zwischen Soll und Ist.

Die *Diskrepanz zw. Soll und Ist bei der Leistungserbringung* wirkt sich positiv auf etwaige *Korrekturmaßnahmen* aus, diese wirken mit einer Verzögerung positiv auf die *Leistungserbringung Ist* ein und diese wiederum beeinflusst die *Diskrepanz zw. Soll und Ist* negativ. Der ausbalancierte Rückkopplungskreis hier zeigt, dass je größer die Lücke zwischen Soll und Ist der Leistungserbringung ist, desto mehr Korrekturmaßnahmen müssen ergriffen werden, um mit einer zeitlichen Verzögerung trotzdem eine entsprechende Leistungserbringung zu ermöglichen. Eine Korrekturmaßnahme könnte zum Beispiel die Anforderung von zusätzlichem Personal sein.

Schlussendlich wirkt sich die *Leistungserbringung Ist* positiv auf das *Gesellschaftliche medizinische Versorgungniveau* aus, denn je mehr (weniger) medizinische Leistungen erbracht werden können, desto höher (geringer) ist auch das medizinische Versorgungsniveau der Bevölkerung mit erforderlichen Gesundheitsdienstleistungen.

## 6.3 Modell mit Bezug zum Transportsektor

### 6.3.1 Einleitung und Systemvariablen-Tabelle

Das im Rahmen dieses Kapitels beschriebene CLD in Abbildung 18 zeigt beispielhaft die Auswirkungen eines großflächigen und langanhaltenden Internetausfalls auf Unternehmen aus dem Transportsektor. Eine detailliertere Modellierung bzw. Analyse des Ausfalls kann in weiterer Folge von den verantwortlichen Sektorexpert:innen auf Basis dieses Grundmodelles entwickelt werden. Im Rahmen des vorliegenden Modelles werden Aspekte der digitalen Datenspeicherung und des digitalen Datenzugriffes im Rahmen betriebsinterner und -externer Daten, sowie die aktive und standardisierte digitale Kommunikation dargestellt.

Bevor näher auf das Modell mit Bezug zum Transportsektor eingegangen wird, werden in Tabelle 4 jene Variablen des CLD-Modells des Transportsektors erklärt, deren Bedeutung bzw. Wirkungsbereich nicht bereits eindeutig aus dem Variablennamen hervorgehen und daher näherer Erklärung bedürfen.

*Tabelle 4: Systemvariablentabelle mit Bezug zum Transportsektor (vgl. Schachenhofer et al. 2022)*

| | |
|---|---|
| Bandbreitenabfall bzw. Ausfall internetbasierter Dienste | Von der Internetbandbreite (gemessen in Megabit pro Sekunde) hängt ab, wie viele Daten digital übertragen werden können. Ein Bandbreitenabfall wirkt sich z.B. auf die digitale Übermittlung von Dokumenten aus. Im Modell wird davon ausgegangen, dass sie teilweise oder gänzlich abfällt oder internetbasierte Dienste teilweise oder gänzlich ausfallen. |
| Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen | In der Cloud (Daten- bzw. Internetwolke) können beispielsweise Daten und Dokumente digital abgespeichert und gemeinschaftlich genutzt bzw. bearbeitet werden. Kommunikationskanäle dienen dazu, sich auszutauschen bzw. Informationen zu vermitteln. Digitale Kommunikationskanäle sind bspw. E-Mail und Messenger-Dienste. Im Modell wird davon ausgegangen, dass die Dienste kompromittiert sind. Nutzer:innen können nicht mehr auf die Sicherheit ihrer Daten vertrauen und werden nach und nach die Nutzung dieser Dienste einstellen. |
| Digitale Datenspeicherung und -zugriff | Sämtliche Abspeicherungsprozesse und der Zugriff auf Daten und Dokumente über Cloud-Dienste sind von der Beeinträchtigung betroffen und somit vorübergehend nicht möglich. |
| Digitale Kommunikation in Prozessen des Betriebes | Das betrifft sämtliche Kommunikationsformen über digitale Kanäle (schriftlich und mündlich, sowie den Austausch von Daten |

| | |
|---|---|
| | und Dokumenten per Videotelefonie bzw. über Videokonferenzsysteme) zwischen Stakeholder:innen der Organisation. |
| Automatisierte Kommunikation (Auftrags- und Standortübermittlung) | Die automatisierte Kommunikation erfolgt digital. Gemeint sind in diesem Zusammenhang beispielsweise die digitale Übermittlung von Aufträgen und damit in Zusammenhang stehenden Daten, sowie von standortbezogenen Daten. |
| Echtzeitdaten aus der Umwelt | Echtzeitdaten werden regelmäßig und zeitnah erfasst und laufend digital aktualisiert. Der Zugriff auf Echtzeitdaten, die durch Drittparteien zur Verfügung gestellt werden, erfolgt ebenfalls digital. Echtzeitdaten sind z.B. Fahrplaninformationen mit laufender, digitaler Aktualisierung. |
| Digitale Abwicklung von Zahlungsprozessen | Die digitale Abwicklung von Zahlungsprozessen beinhaltet z.B. internetbasierte Zahlungsservices inklusive der digitalen Erstellung und Übermittlung von damit zusammenhängenden Dokumenten z.B. digitale Zahlungsnachweise, elektronische Rechnungen (evtl. mit digitaler Signatur) Lieferscheine etc.. Eine Beeinträchtigung dieser Systemvariable kann sich auf nachfolgende Variablen beispielsweise in Form von Lieferverzögerungen auswirken. |
| Überlastung Mobilfunknetz | Aufgrund einer hohen Anzahl an Benutzer:innen bzw. einer großen Menge an zu übertragenden Daten kann es im Mobilfunknetz, wie in allen Netzen, zu Überlastungserscheinungen in Form von Verzögerungen bzw. Ausfällen kommen. Dies beeinflusst wiederum den Durchsatz (die Menge an übertragenen Daten in einem bestimmten Zeitraum) beispielsweise bei Netzüberlastung in einem bestimmten, geografisch abgegrenzten, Gebiet. |
| Datenqualität | Die Qualität der vorhandenen Daten, hinsichtlich Aktualität, Vollständigkeit, Korrektheit etc. kann durch die Beeinträchtigung vorgelagerter Systemvariablen vermindert werden. |
| Kommunikationsqualität | Die Kommunikationsqualität zeigt sich in der Erreichbarkeit der gewünschten Personen, den verfügbaren Kommunikationskanälen |

| | |
|---|---|
| | und den damit zusammenhängenden Möglichkeiten (z.B. Bildschirmübertragung und Versenden von Dokumenten) und hat Auswirkungen auf Faktoren wie die elektronische Beschaffung, die digitale Bereitstellung von Services und die Instandhaltung über digitale Kommunikationskanäle. |
| Qualität des Monitorings inkl. allg. Kontrolltätigkeiten | Das betrifft Monitoring-Aktivitäten, die mithilfe digitaler Dienste ausgeführt werden (bspw. Zollinspektionen). Bei einer verminderten Verfügbarkeit internetbasierter Dienste ist diese nur eingeschränkt bzw. unter Umständen gar nicht möglich. |
| Verfügbarkeit abhängiger Leistungen | Das betrifft sämtliche, von einem Unternehmen zu erbringenden Leistungen, die von den vorgelagerten Qualitätsvariablen abhängig sind z.B. Güterbeförderung, digitale Temperaturüberwachung in Lebensmittel-Transporteinheiten etc.. |
| Korrekturmaßnahmen | Unter diesem Begriff werden sämtliche Maßnahmen zusammengefasst, um die Leistungserbringung während eines Ausfallsereignisses zu steigern (z. B. zusätzlicher Personaleinsatz). |
| Erfüllung von SLAs (Service Level Agreements) | Im Rahmen von SLAs werden Qualitätseigenschaften definiert, die maßgebend für die erbrachten Leistungen einer Organisation sind. Im Transportwesen werden SLAs z.B. zwischen Logistikservice-Anbietern und Kund:innen festgelegt, die garantieren, dass Transportservices in einer bestimmten Qualität durchgeführt werden (vgl. Marquezan et al. 2014: 564). Die Erfüllung von SLAs von Unternehmen im Transportbereich ist abhängig von der Verfügbarkeit vorgelagerter Variablen bzw. der Durchführbarkeit vorgelagerter Prozesse. |

Das Modell mit Bezug zum Transportsektor ist wie folgt aufgebaut: Startpunkte sind, analog zu dem zuvor beschriebenen CLD aus dem Bereich des Gesundheitssektors, jeweils die beiden Variablen in der obersten Zeile rechts und links: *Bandbreitenabfall bzw. Ausfall internetbasierter Dienste* und *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen.* Diese stellen die Beeinträchtigung internetbasierter Dienste als Ausgangssituation dar, die sich auf nachfolgende, zentrale Themenbereiche auswirkt. Solche Beeinträchtigungen und deren weitreichende Folgen, die sich aus einer erhöhten Interkonnektivität in den verschiedenen Geschäftsbereichen ergeben, wurde auch durch Pan et al. untersucht. Deren Studie

zeigte, dass Herausforderungen wie der kollektive Zugriff auf und die gemeinsame Nutzung von bestimmten Daten, Datenschutz und Kommunikation, die durch die erhöhte, digitale Interkonnektivität in Logistiknetzwerken noch stärker forciert wird, zu einem gewissen Grad mit dem Einsatz neuer Technologien wie beispielsweise der Digital Twin Technologie und dem Einsatz intelligenter Infrastrukturen begegnet werden kann. Zusätzlich dazu ist zu gewährleisten, dass Datenmanagement auch zwischen verschiedenen Organisationen nahtlos erfolgen kann, z.B. durch eine Unterscheidung in produktbezogene Daten und Daten betreffend Bestellungen. Aus den Ergebnissen geht hervor, dass solche Lösungsansätze durch interdisziplinäre Ansätze ergänzt werden müssen, um den Risiken der erhöhten Vernetzung in Logistik-Wertschöpfungsketten wirksam entgegenzusteuern (vgl. Pan et al. 2021: 2, 10-12).

Die Ausgangsvariablen *Bandbreitenabfall bzw. Ausfall internetbasierter Dienste* und *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen* wirken sich auf die nachfolgenden, zentralen Themenbereiche aus:

- Digitale Datenspeicherung und -zugriff und
- Digitale Kommunikation in Prozessen des Betriebes

Der Themenbereich *Digitale Datenspeicherung und -zugriff* beinhaltet die Sub-Bereiche *Betriebsinterne Daten, Echtzeitdaten aus der Umwelt* und *Digitale Abwicklung von Zahlungsprozessen.*

Der Themenbereich *Digitale Kommunikation in Prozessen des Betriebes* beinhaltet die Sub-Bereiche *Aktive Kommunikation* und *Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung).*

Das Ausmaß der Betroffenheit in den jeweiligen Themenbereichen zeigt sich in weiterer Folge, was darüber hinaus auch Verlagerungsschleifen im Rahmen des Archetyps „Shifting the Burden“ miteinbezieht. Die Betroffenheit manifestiert sich in der Beeinträchtigung der nachgelagerten Qualitätsvariablen *Datenqualität, Kommunikationsqualität* und *Qualität des Monitorings inkl. allgemeiner Kontrolltätigkeiten*. Zusätzlich dazu ist auch die Systemvariable *Einhaltung Liefertermine* als Teil der Qualitätsvariablen zu sehen.

Die Qualitätsvariablen wirken auf zwei zentrale Variablen des Systems ein. Sie nehmen sowohl auf unternehmensinterne, als auch unternehmensexterne Variablen Einfluss. Diese wirken sich wiederum auf die erbrachten Leistungen und schlussendlich auf die Output-Variable *Erfüllung von SLAs* aus.

Anhand des Modell-Ausschnittes aus dem Transportsektor in Abbildung 17 wird der zweite zum Tragen kommende Archetyp „Eroding Goals“ veranschaulicht. Dabei wird gezeigt, dass sich eine Einschränkung der Internetbandbreite auf die Diskrepanz zwischen dem Soll- und Ist-Zustand bei der Auftragserfüllung auswirkt. Während das Ergreifen von Korrekturmaßnahmen mit zeitlicher Verzögerung positiv auf die tatsächliche Auftragserfüllung wirkt, bedingt die Reduktion der Auftragserfüllungsrate eine Abnahme des Soll-Zustandes bei der Auftragserfüllung. Beides führt zu einer Angleichung von Soll- und Ist-Zustand, jedoch resultiert aus einer Reduktion der Auftragserfüllungsrate eine Zielerosion und damit eine Abnahme der Leistung des jeweiligen Unternehmens im Zeitverlauf (Schachenhofer et al. 2022).

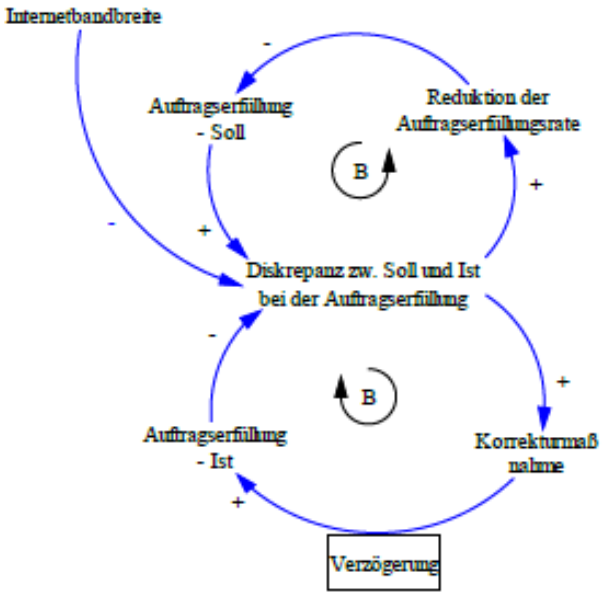



*Abbildung 17: Veranschaulichung des Archetyps „Eroding Goals“ (vgl. Schachenhofer et al. 2022)*

Wie bereits die Erläuterungen zum Archetyp „Shifting the Burden“ in Kapitel 6.2.1 zeigen, ist auch der Archetyp „Eroding Goals“ eine Art Systemfalle, die sich langfristig nachteilig auf nachgelagerte Prozesse und damit das gesamte System auswirken kann. Im Modell mit Bezug zum Transportsektor (siehe Abbildung 18) sind die Prozesse, die im Rahmen dieses Archetyps während eines Ausfalls internetbasierter Dienste in Gang gesetzt werden können, in das Gesamtbild eingebettet (Schachenhofer et al. 2022).

### 6.3.2 Beschreibung des Causal Loop Diagrammes

In Abbildung 18 ist das CLD mit Bezug zum Transportsektor dargestellt. Im Rahmen dessen werden die verschiedenen Bereiche ersichtlich, die im Fall einer etwaige Bandbreiteneinschränkung bzw. eines Internetausfall, oder einer Kompromittierung von Cloud-Sharing Services bzw. digitalen Kommunikationskanälen in Unternehmen des Transportbereiches beeinträchtigt wären. Die Wirkungsbeziehungen zwischen den Systemvariablen werden im Folgenden näher erläutert.[4]

[4] Anmerkung zum Modell: Systemvariablen, die im Modell definierte Notfallmaßnahmen darstellen, wurden mit einem * markiert.

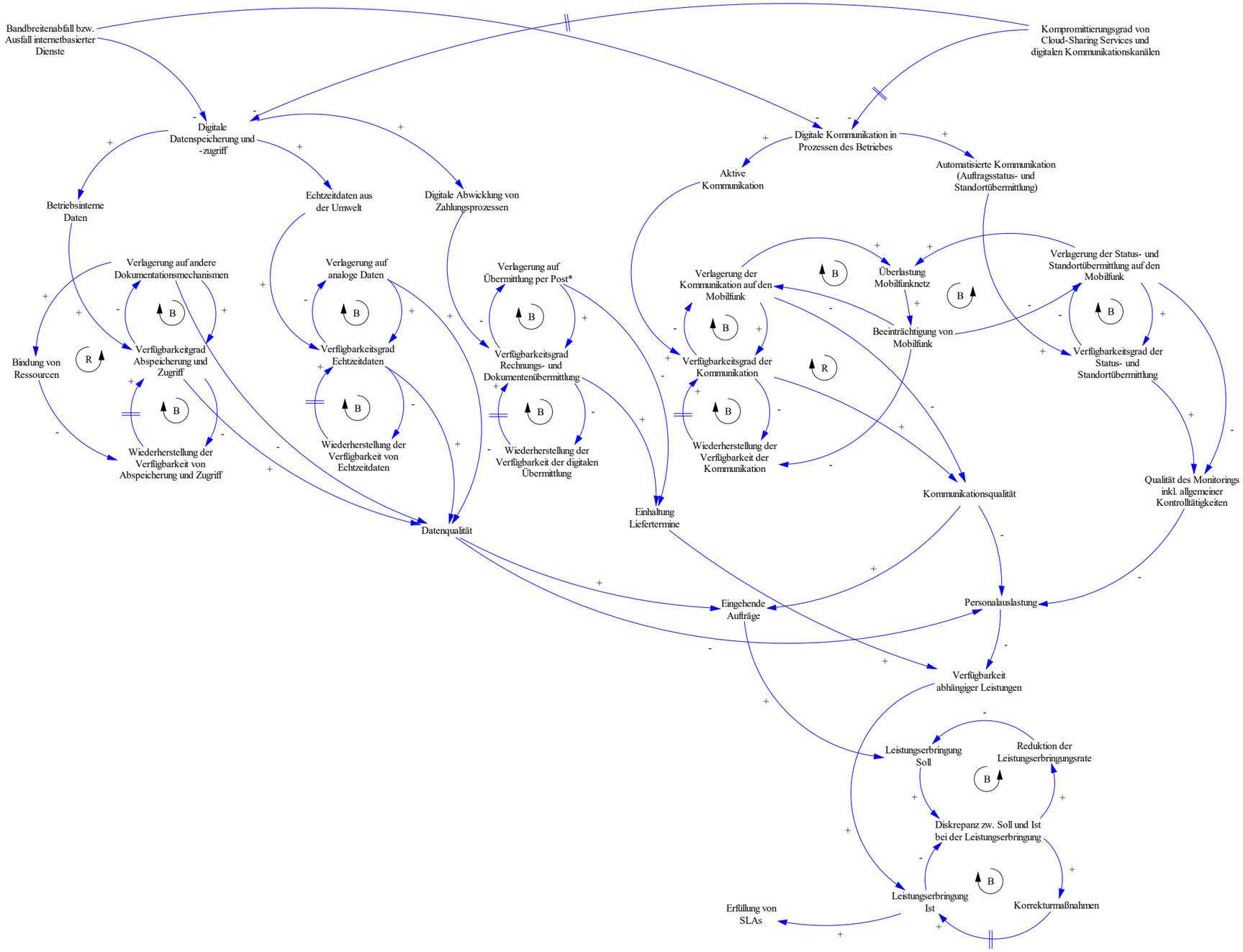



*Abbildung 18: Causal Loop Diagramm mit Bezug zum Transportsektor (vgl. Schachenhofer et al. 2022)*

Die Ausgangssituation wird durch einen *Bandbreitenabfall bzw. den Totalausfall internetbasierter Dienste*, sowie den *Kompromittierungsgrad von Cloud-Sharing Services und digitalen Kommunikationskanälen* bestimmt.

Diese Ausgangsvariablen wirken sich negativ auf die nachfolgenden, zentralen Themenbereiche aus:

- Digitale Datenspeicherung und -zugriff
- Digitale Kommunikation in Prozessen des Betriebes
    - Betriebsinterne Daten
    - Echtzeitdaten aus der Umwelt
    - Digitale Abwicklung von Zahlungsprozessen
    - Aktive Kommunikation
    - und Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)

Nachfolgend werden die Wirkungsbeziehungen zwischen den einzelnen Variablen, sowie etwaige Verlagerungsschleifen näher beschrieben (Schachenhofer et al. 2022).

#### *6.3.2.1 Digitale Datenspeicherung und -zugriff – Betriebsinterne Daten*

Die Systemvariable *Digitale Datenspeicherung und -zugriff* wirkt sich positiv auf *Betriebsinterne Daten* aus, die ebenfalls in positivem Wirkungszusammenhang mit dem *Verfügbarkeitsgrad Abspeicherung und Zugriff* digitaler Daten stehen. Hier beginnen Wechselwirkungen, die den Archetyp „Shifting the Burden“ widerspiegeln. Der Verfügbarkeitsgrad wirkt negativ auf die *Verlagerung auf andere Dokumentationsmechanismen* ein, diese Variable wiederum wirkt positiv auf den *Verfügbarkeitsgrad Abspeicherung und Zugriff* ausschließlich digital vorhandener, betriebsinterner Daten zurück (vgl. ISIDOR Expert:inneninterviews 2021). Es entsteht ein ausbalancierter geschlossener Rückkopplungskreis, da umso mehr auf andere Dokumentationsmechanismen verlagert wird, je weniger Abspeicherung und Zugriff digital verfügbar sind. Je mehr andere Dokumentationsmechanismen angewendet werden, desto mehr ist auch die Abspeicherung und der Zugriff auf Daten über andere Wege wieder möglich.

Die *Verlagerung auf andere Dokumentationsmechanismen* wirkt positiv auf die *Bindung von Ressourcen* ein. Diese Variable ist wiederum negativ verknüpft mit der *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff*, da diese beiden Variablen indirekt miteinander korrelieren. Das heißt, je größer das Ausmaß der *Bindung von Ressourcen* ist, umso weniger Ressourcen stehen für die *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff* zur Verfügung und umgekehrt, wodurch ein sich selbst verstärkender Rückkopplungskreis entsteht.

Darüber hinaus besteht eine negative Verbindung von *Verfügbarkeitsgrad Abspeicherung und Zugriff* zur *Wiederherstellung der Verfügbarkeit von Abspeicherung und Zugriff*. Je weniger (mehr) Möglichkeiten zwecks Datenspeicherung und -zugriff über nicht-digitale Wege vorhanden sind, desto mehr (weniger) besteht die Notwendigkeit zur Wiederherstellung der Verfügbarkeit ebendieser. Je mehr die Wiederherstellung der digitalen Abspeicherung und des Zugriffs auf digital vorhandene Daten betrieben

wird, desto mehr sind diese Komponenten nach einer gewissen zeitlichen Verzögerung wieder verfügbar, was sich wiederum anhand einer positiven Wirkungsbeziehung zwischen diesen beiden Variablen zeigt. Diese Wechselwirkungen halten sich in Balance, wodurch ein weiterer ausbalancierter Rückkopplungskreis entsteht.

#### *6.3.2.2 Digitale Datenspeicherung und -zugriff – Echtzeitdaten aus der Umwelt*

*Digitale Datenspeicherung und -zugriff* wirkt positiv auf *Echtzeitdaten aus der Umwelt*, die ebenfalls positiv mit dem *Verfügbarkeitsgrad von Echtzeitdaten* verknüpft sind (vgl. ISIDOR Expert:inneninterviews 2021). Der Verfügbarkeitsgrad wirkt wiederum negativ auf die *Verlagerung auf analoge Daten* und diese wirkt positiv zurück auf den Verfügbarkeitsgrad. Der ausbalancierte Rückkopplungskreis, der hier entsteht, bedeutet, dass je mehr Verfügbarkeit von Echtzeit-Informationen gegeben ist, desto weniger muss auf analoge Daten verlagert werden und je weniger verlagert wird, desto mehr kann von einem hohen Verfügbarkeitsgrad von Echtzeitdaten ausgegangen werden. *Verfügbarkeitsgrad Echtzeitdaten* wirkt darüber hinaus negativ auf die *Wiederherstellung der Verfügbarkeit von Echtzeitdaten ein*, da bei einer niedrigen (hohen) Verfügbarkeit von Echtzeitdaten die Wiederherstellung dieser umso mehr (weniger) forciert wird. Sofern eine Wiederherstellung dieser unternommen wird, wirkt dies wiederum mit einer Verzögerung positiv auf den *Verfügbarkeitsgrad Echtzeitdaten*, wodurch ein weiterer ausbalancierter Rückkopplungskreis entsteht.

#### *6.3.2.3 Digitale Datenspeicherung und -zugriff – Digitale Abwicklung von Zahlungsprozessen*

Die *digitale Datenspeicherung und -zugriff* ist positiv mit der *digitalen Abwicklung von Zahlungsprozessen* verknüpft und diese wirkt positiv auf den *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* ein. Je besser die digitale Abwicklung funktioniert, umso höher ist auch der Verfügbarkeitsgrad der damit in Verbindung stehenden Dokumente. Je weniger jedoch die Möglichkeit besteht, Rechnungen und andere Dokumente digital zu senden, desto mehr muss auf die Übermittlung per Post umgestiegen werden, was sich durch eine negative Wirkungsbeziehung zwischen dem *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* und der *Verlagerung auf Übermittlung per Post* zeigt. Diese wirkt wiederum positiv auf den *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* zurück, wodurch ein ausbalancierter Rückkoppelungskreis entsteht. Ausgehend von dem Verfügbarkeitsgrad besteht außerdem eine negative Wirkungsbeziehung zur *Wiederherstellung der Verfügbarkeit der digitalen Übermittlung,* da, je geringer dieser ist, eine Wiederherstellung der digitalen Übermittlung umso stärker forciert werden wird. Die Wiederherstellung ist wiederum positiv mit dem Verfügbarkeitsgrad verknüpft, da sie diesen nach einer gewissen Zeit, die die Wiederherstellungsmaßnahmen in Anspruch nehmen, erhöht. Durch diese Wirkungsbeziehungen entsteht der nächste, ausbalancierte Rückkopplungskreis.

Während der *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* in einem positiven Wirkungszusammenhang mit der Systemvariable *Einhaltung Liefertermine* steht, weist die *Verlagerung auf Übermittlung per Post* eine negative Kausalität zu dieser Variable auf, da im Fall vermehrter Verlagerungen auf den Postweg

durch viele Akteur:innen die Wahrscheinlichkeit steigt, dass Dokumente nicht zeitgerecht übermittelt werden können, wodurch ebenfalls mit Lieferverzögerungen zu rechnen ist (vgl. ISIDOR SKKM Sektorenworkshops 2021).

#### *6.3.2.4 Digitale Kommunikation in Prozessen des Betriebes – Aktive Kommunikation*

Die *Digitale Kommunikation in Prozessen des Betriebes* wirkt sich positiv auf *Aktive Kommunikation* aus, die wiederum ebenfalls positiv mit dem *Verfügbarkeitsgrad der Kommunikation* verknüpft ist (vgl. Pan et al. 2021: 4f). Der Verfügbarkeitsgrad hat wiederum eine negative Wirkung auf die *Verlagerung der Kommunikation auf den Mobilfunk* und diese wiederum eine positive auf den *Verfügbarkeitsgrad der Kommunikation*. Durch die Möglichkeit der Verlagerung auf den Mobilfunk entsteht ein ausbalancierter Rückkopplungskreis (vgl. ISIDOR Expert:inneninterviews 2021).

Ähnliche Wirkungsabläufe können im Hinblick auf die Problemlösung beobachtet werden. Die negative Verbindung zwischen dem *Verfügbarkeitsgrad der Kommunikation* und der *Wiederherstellung der Verfügbarkeit der Kommunikation* bedeutet eine erhöhte Notwendigkeit von Wiederherstellungsmaßnahmen, je weniger Kommunikation über digitale Kommunikationskanäle erfolgen kann. Die Wiederherstellung ist positiv, sowie zeitlich verzögert mit dem *Verfügbarkeitsgrad der Kommunikation* verknüpft. Je höher der Wiederherstellungsgrad der Kommunikation durch die ergriffenen Maßnahmen ist, desto höher ist in Folge dessen auch die Verfügbarkeit der Kommunikation. Der *Verfügbarkeitsgrad der Kommunikation* stellt in diesem Modellabschnitt somit die Symptomvariable dar, anhand welcher sich das zu Grunde liegende Problem der Bandbreiteneinschränkung bzw. des Ausfalls internetbasierter Dienste offenbart.

Hier entstehen nun einige Schleifen, die mit der Verlagerung im Rahmen des Archetyps „Shifting the Burden“ in Zusammenhang stehen. Die *Verlagerung der Kommunikation auf den Mobilfunk* wirkt auf die *Überlastung Mobilfunknetz* positiv ein. Dies beeinflusst die *Beeinträchtigung von Mobilfunk als Ausweichmöglichkeit* ebenfalls positiv verstärkend und das wirkt wiederum negativ auf die *Verlagerung der Kommunikation auf den Mobilfunk* zurück. Ein ausbalancierter Rückkopplungskreis entsteht, da mit der zunehmenden Nutzung des Mobilfunks auch eine höhere Gefahr der Netzüberlastung einhergeht. Und je höher die *Überlastung* ist, desto mehr *Beeinträchtigung von Mobilfunk als Ausweichmöglichkeit* ist gegeben, desto weniger besteht die Möglichkeit der *Verlagerung der Kommunikation auf den Mobilfunk*.

Darüber hinaus besteht eine negative Verbindung zwischen *Beeinträchtigung von Mobilfunk als Ausweichmöglichkeit* und *Wiederherstellung der Verfügbarkeit der Kommunikation*, wodurch ein sich selbst verstärkender Rückkopplungskreis zwischen *Verlagerung der Kommunikation auf den Mobilfunk*, *Überlastung Mobilfunknetz*, *Beeinträchtigung von Mobilfunk als Ausweichmöglichkeit*, *Wiederherstellung der Verfügbarkeit der Kommunikation* und *Verfügbarkeitsgrad der Kommunikation* entsteht. Denn je weniger digitale Kommunikation verfügbar ist, desto mehr wird auf den Mobilfunk verlagert. Dies geht mit einer erhöhten Überlastungsgefahr einher, was sich negativ auf etwaige Wiederherstellungsmaßnahmen auswirkt (da dafür unter Umständen auf den Mobilfunk zwecks Kommunikation zurückgegriffen werden müsste). Und je weniger erfolgreich die Wiederherstellung durchgeführt werden

kann, desto weniger kann auch der Verfügbarkeitsgrad der Kommunikation angehoben werden.

##### *6.3.2.5 Digitale Kommunikation in Prozessen des Betriebes – Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)*

Die *Digitale Kommunikation in Prozessen des Betriebes* wirkt sich positiv auf die *Automatisierte Kommunikation (Auftragsstatus- und Standortübermittlung)* aus, die wiederum ebenfalls positiv mit dem *Verfügbarkeitsgrad der Status- und Standortübermittlung* verknüpft ist (vgl. Pan et al. 2021: 2,4,8f). Dieser wirkt negativ auf die *Verlagerung der Status- und Standortübermittlung auf Mobilfunk*, die positiv zurück auf den Verfügbarkeitsgrad einwirkt (vgl. ISIDOR Expert:inneninterviews 2021). Je weniger die Verfügbarkeit gegeben ist, desto mehr Daten werden im Rahmen der Status- und Standortübermittlung verlagert. Die Verlagerung auf den Mobilfunk bewirkt wiederum eine erhöhte Verfügbarkeit von Status- und Standortübermittlung, wodurch sich ein ausbalancierter Rückkopplungskreis schließt. Die *Verlagerung der Status- und Standortübermittlung auf Mobilfunk* wirkt positiv verstärkend auf die *Überlastung Mobilfunknetz*, diese wiederum wirkt ebenfalls positiv auf die *Beeinträchtigung von Mobilfunk*. Die letztgenannte Variable wirkt negativ zurück auf die Möglichkeit der Verlagerung. Je stärker das Mobilfunknetz überlastet ist, desto weniger besteht die Möglichkeit, die Status- und Standortübermittlung auf den Mobilfunk zu verlagern. Analog zur Kommunikation entsteht an dieser Stelle ein weiterer ausbalancierter Rückkopplungskreis im Falle der Überlastung des Mobilfunknetzes.

### 6.3.3 Auswirkungen der verschiedenen Themenbereiche auf die Qualitätsvariablen

Die zuvor beschriebenen Themenbereiche inklusive ihrer jeweiligen Verlagerungsschleifen wirken sich auf die nachfolgenden Qualitätsvariablen *Datenqualität, Kommunikationsqualität, Qualität des Monitorings inkl. allgemeiner Kontrolltätigkeiten* und *Einhaltung Liefertermine* aus.

Der *Verfügbarkeitsgrad Abspeicherung und Zugriff* wirkt sich positiv auf die *Datenqualität* aus, die *Verlagerung auf andere Dokumentationsmechanismen* jedoch negativ, da es durch die Verlagerung zu Qualitätsverlusten kommt.

Auch der *Verfügbarkeitsgrad Echtzeitdaten* wirkt sich positiv auf die Datenqualität aus, während es durch eine *Verlagerung auf analoge Daten* zu einer negativen Wirkungsbeziehung mit der *Datenqualität* kommt. Je mehr auf analoge Daten zurückgegriffen werden muss, desto eher ist auch hier mit Einbußen in der Datenqualität zu rechnen.

Positiv auf die Systemvariable *Einhaltung Liefertermine* wirkt der *Verfügbarkeitsgrad Rechnungs- und Dokumentenübermittlung* ein, während sich eine *Verlagerung auf Übermittlung per Post* negativ auf *Einhaltung Liefertermine* negativ auswirkt. Die negative Auswirkung der Verlagerungsschleife auf die Einhaltung von Lieferterminen zeigt, dass je mehr Rechnungen und Dokumente per Post übermittelt werden müssen, desto weniger können Liefertermine eingehalten werden.

Der *Verfügbarkeitsgrad der Kommunikation* wirkt sich positiv auf die *Kommunikationsqualität* aus, die *Verlagerung der Kommunikation auf den Mobilfunk* jedoch negativ, da mit zunehmender Verfügbarkeit auch die Qualität steigt, während sie durch eine Verlagerung abfällt.

Derselbe Fall tritt bei der Status- und Standortübermittlung ein: Der *Verfügbarkeitsgrad Status- und Standortübermittlung* wirkt sich positiv auf die *Qualität des Monitorings inkl. allgemeiner Kontrolltätigkeiten* aus, die *Verlagerung der Status- und Standortübermittlung auf Mobilfunk* jedoch negativ (vgl. ISIDOR Expert:inneninterviews 2021; Schachenhofer et al. 2022).

### 6.3.4 Auswirkungen der Qualitätsmerkmale organisationsintern und auf Drittparteien

Im Folgenden werden organisationsinterne Auswirkungen im Rahmen der Variablen *Eingehende Aufträge, Personal-, Verwaltungs- und Zeitaufwand* und *Lieferverzögerungen* beschrieben. Diese wirken sich weiter auf externe Drittparteien bzw. nachgelagerte Kund:innen in Form der Variable *Verfügbarkeit abhängiger Leistungen* aus (Schachenhofer et al. 2022).

#### *6.3.4.1 Betriebsinterne Auswirkungen*

Wenn die Prozesse innerhalb einer Organisation nicht in der erforderlichen Qualität ablaufen, ist ein erhöhter Aufwand nötig, um das Leistungsniveau auf einem akzeptablen Level zu halten, was sich anhand einer erhöhten *Personalauslastung* zeigt (vgl. ISIDOR Expert:inneninterviews 2021). Auf die Variable *Personalauslastung* wirken daher die Qualitätsvariablen *Datenqualität*, *Kommunikationsqualität* und *Qualität des Monitorings inkl. allgemeiner Kontrolltätigkeiten* negativ ein, da eine verringerte Qualität in allen drei Fällen mit einem erhöhten Aufwand für das Personal eines Unternehmens einhergeht (vgl. ISIDOR Expert:inneninterviews 2021).

Weiters spiegeln sich die Auswirkungen einer Einschränkung internetbasierter Dienste betriebsintern in den *Eingehenden Aufträgen* wider. Daher wirken die *Datenqualität* und *Kommunikationsqualität* positiv auf *Eingehende Aufträge* ein. Je besser die Datenlage ist und je besser die Kommunikation funktioniert, desto mehr Aufträge erreichen beispielsweise ein Transportunternehmen (vgl. ISIDOR Expert:inneninterviews 2021).

#### *6.3.4.2 Auswirkungen auf Drittparteien*

Die *Personalauslastung* ist negativ mit der *Verfügbarkeit abhängiger Leistungen* verknüpft, während die *Einhaltung Liefertermine* positiv auf die Verfügbarkeit abhängiger Leistungen einwirkt (vgl. ISIDOR SKKM-Sektorenworkshops 2021). Dies zeigt, dass eine erhöhte Personalauslastung mit einer verminderten Verfügbarkeit abhängiger Leistungen einhergeht, während sich die Einhaltung von Lieferterminen positiv auf diese auswirkt. Mit der Variable *Verfügbarkeit abhängiger Leistungen* starten jene Prozesse, die in weiterer Folge die zentralen Auswirkungen auf Drittparteien im Rahmen des Archetyps „Eroding Goals“ bzw. der Zielerosion darstellen.

Die *Verfügbarkeit abhängiger Leistungen* wirkt positiv auf *Leistungserbringung Ist* ein, diese wiederum wirkt negativ auf die *Diskrepanz zw. Soll und Ist bei der Leis-*

*tungserbringung.* Die Variable *Eingehende Aufträge* wirkt positiv auf die *Leistungserbringung Soll* ein. Diese wirkt ebenfalls positiv auf die *Diskrepanz zw. Soll und Ist bei der Leistungserbringung* ein. Je weniger abhängige Leistungen verfügbar sind, desto geringer ist das Niveau der tatsächlichen Leistungserbringung. Im Gegensatz dazu bestimmt die Anzahl an eingehenden Aufträgen maßgeblich die Höhe des Niveaus der geforderten Leistungserbringung. Dadurch entsteht eine Diskrepanz zwischen dem Soll- und Ist-Zustand bei der Leistungserbringung. Die Variable *Diskrepanz zw. Soll- und Ist-Zustand bei der Leistungserbringung* wirkt positiv auf die *Reduktion der Leistungserbringungsrate* ein, welche wiederum negativ auf die *Leistungserbringung Soll* wirkt (vgl. ISIDOR Expert:inneninterviews 2021). Der ausbalancierte Rückkopplungskreis, der hier entsteht, zeigt an, dass je größer die Lücke zwischen dem leistungsbezogenen Soll und Ist-Zustand ist, desto mehr müssen bestimmte Aufträge priorisiert und andere im Sinne einer Reduktion der Leistungserbringung vernachlässigt werden. Das verfolgte Niveau der Leistungserbringung wird im Sinne einer Zielerosion nach unten korrigiert, wodurch sich die Lücke zwischen Soll und Ist verringert (vgl. Meadows 2019: 185).

Die *Diskrepanz zw. Soll und Ist bei der Leistungserbringung* wirkt sich positiv auf die *Korrekturmaßnahmen* aus, da diese beiden Variablen direkt miteinander korrelieren (je größer die Diskrepanz, desto mehr Korrekturmaßnahmen müssen ergriffen werden). Die *Korrekturmaßnahmen* wirken zeitlich verzögert positiv auf die *Leistungserbringung Ist* ein, welche wiederum die Diskrepanz negativ beeinflusst (je höher der Ist-Zustand der Leistungserbringung, umso geringer ist die Diskrepanz zwischen Soll und Ist bei der Leistungserbringung). Der ausbalancierte Rückkopplungskreis an dieser Stelle zeigt ebenfalls Folgendes: Je größer die Lücke zwischen dem Soll- und Ist-Zustand bei der Leistungserbringung ist, desto mehr bzw. effizientere Korrekturmaßnahmen müssen vorgenommen werden, um mit einer zeitlichen Verzögerung dennoch einen gewissen Leistungsstandard zu ermöglichen. Eine Korrekturmaßnahme könnte beispielsweise der erhöhte Einsatz von Personal sein, der positiv auf den Ist-Zustand der Leistungserbringung wirkt und damit die Lücke zwischen Soll und Ist verringert.

Schlussendlich wirkt sich die *Leistungserbringung Ist* positiv auf die *Erfüllung von SLAs* aus, denn je weniger Unternehmensleistungen erbracht werden können, desto geringer ist auch die Erfüllung von Service Level Agreements hinsichtlich erbrachter Transportleistungen (vgl. ISIDOR Expert:inneninterviews 2021).

## 6.4 Anwendungsfälle

Aus den sektorspezifischen Causal Loop Diagrammen (CLD) aus dem Transport- und Gesundheitssektor wurden in weiterer Folge konkrete Anwendungsfälle abgeleitet. Diese basieren auf den Erkenntnissen aus den im Rahmen des Projektes durchgeführten Interviews sowie den Ergebnissen aus den zwei Reihen der abgehaltenen SKKM Sektoren-Workshops. Referenziert wird in Kapitel 6.4 und Kapitel 6.5 auf ein Working Paper von Schachenhofer et al. (2022).

### 6.4.1 Anwendungsfälle aus dem Gesundheitssektor

In den nächsten Abschnitten werden die erhobenen Auswirkungen eines länger andauernden und großflächigen Internetausfalls anhand von zwei praktischen Anwendungsfällen aus dem Gesundheitssektor näher beschrieben. Die Anwendungsfälle wurden aus Expert:innengesprächen mit Vertreter:innen des Gesundheitssektors sowie den Informationen, die im Rahmen der abgehaltenen Workshops gewonnen wurden, abgeleitet und systematisch aufbereitet (Schachenhofer et al. 2022).

#### *6.4.1.1 Auswirkungen auf den Notfall- und Krankentransport*

Im Rahmen des Projektes ISIDOR wurde ein Expert:innengespräch mit einer Person einer Rettungsleitstelle geführt. Die Ausführungen zum Anwendungsfall in diesem Kapitel beziehen sich daher auf den Notfall- und Krankentransport.

##### Sofortige Auswirkungen eines Ausfalls internetbasierter Dienste

Eine Rettungsleitstelle kann nicht mehr auf internetbasierte Dienste zugreifen. Betroffen sind die digitale Daten-, Auftrags- und Statusübermittlung, die digitale Kommunikation, Dokumentation und Datensicherung, sowie der Datenzugriff. Konkret bedeutet dies für die Leitstelle, dass das Einsatzleitsystem nicht mehr zur Verfügung steht. Das betrifft das integrierte Geoinformationssystem mit hinterlegten Stammdaten, das Erfassen und Abrufen von Aufträgen bzw. die Übermittlung von Auftragsdaten der Leitstelle an die Einsatz-Fahrzeuge, das Disponieren von Einsatz-Fahrzeugen und die Übermittlung von Statusmeldungen der Einsatz-Fahrzeuge an die Leitstelle. Die Betroffenheit zeigt sich beispielsweise bei der Beeinträchtigung sämtlicher elektronischen Erfassungsvorgänge von Einsätzen durch die Leitstelle und Weitergabe an die Rettungsfahrzeuge, sowie der elektronischen Erfassung von Patient:innendaten und Einsatzprotokollen.

##### 1. Ausfallsebene: Umstellung von digitaler Kommunikation auf Mobilfunk

Grundsätzlich nehmen die Rettungsleitstellen neue Aufträge telefonisch entgegen. Die Auftragsinformationen werden in das Einsatzleitsystem eingegeben und im Rahmen eines digitalen Formulars erfasst, das per Mausklick an ein zuständiges Fahrzeug übermittelt wird. Dafür kommt als Dienst zur Datenübertragung GPRS zum Einsatz, das über das Mobilfunknetz läuft und eine Schnittstelle zwischen Mobilfunk und Internet ermöglicht, da die Aufträge über einen VPN-Tunnel verschlüsselt an die Fahrzeuge, die mit eigenen IP-Adressen ausgestattet sind, übermittelt werden.

Wenn die oben beschriebene digitale Übermittlung von Aufträgen aufgrund eines Ausfalls internetbasierter Dienste nicht möglich ist, sind einsatzbereite Handys in den Leitstellen vorhanden. In einem solchen Fall werden daher zwecks Notrufbearbeitung Anrufe auf Ansuchen beim zuständigen Netzbetreiber auf diese leitstelleninternen Mobiltelefone umgeleitet. Solange das Mobilfunknetz verfügbar ist, sind die Leitstellen dementsprechend weiterhin erreichbar. Wenn das nicht mehr der Fall sein sollte, ist nur noch die Erreichbarkeit per Funk gegeben.

Zusätzlich dazu verfügt jede Leitstelle über einen USB-Stick, über den alle zwei bis drei Minuten eine laufende Datensicherung über anstehende Transporte bzw. Statusmeldungen der Fahrzeuge erfolgt. Dementsprechend sind jene Informationen zu dem Zeitpunkt eines Ausfalles internetbasierter Dienste in der Regel erst wenige Minuten alt und können vorerst abgearbeitet werden.

Die digitale Dokumentation (z.B. über leitstellen-interne Tablets) wird auf eine analoge Dokumentation mittels vorgedruckter Notfallformulare umgestellt, was einen erheblichen, personellen Mehraufwand und eine erhöhte Fehleranfälligkeit aufgrund unbekannter Prozesse und hohem Zeitdruck zur Folge hat. Besonders bei jüngerem Personal muss damit gerechnet werden, dass mit einer kurzfristigen Umstellung auf eine analoge Arbeitsweise Schwierigkeiten einhergehen können, da diese unter Umständen noch gänzlich unvertraut mit analogen Ersatzabläufen sind. Auch die Erfassung von Statuszeiten muss händisch gemacht werden und die Wahrscheinlichkeit einer generellen Überlastung der Leitstelle ist erhöht.

Es ist außerdem möglich, dass die digitale Schnittstelle zur Warenanlieferung an einzelne Dienststellen durch internetbasierte Paketservices beeinträchtigt ist.

2. Ausfallsebene: Umstellung von Mobilfunk auf BOS-Funk (TETRA Netz)

Sofern die Notwendigkeit besteht, die Kommunikation auf den Sprach-Funk zu verlagern bspw. aufgrund einer Überlastung des Mobilfunknetzes, werden zu übermittelnde Statusmeldungen fortan per BOS-Funk getätigt und auf das Wesentliche reduziert. Die Dokumentation erfolgt weiterhin analog über vorgedruckte Notfallformulare.

Erwartbare Auswirkungen innerhalb 24-48 Stunden:

Mögliche Folgen eines längerfristigen Ausfalls internetbasierter Dienste sind die Schließungen von Ordinationen, sowie ein erhöhtes Unfallaufkommen. Unter Umständen ist daher mit einer verstärkten Anzahl von Notrufen zu rechnen. Das Rettungspersonal sollte dementsprechend in erhöhter Bereitschaft sein. Gegebenenfalls besteht zusätzlicher Personalbedarf. Die Umstellung auf den Krisenbetrieb in der Rettungsleitstelle ist notwendig. Das bedeutet, dass die Kommunikation zu den Einsatzfahrzeugen über das TETRA Netz hergestellt wird. Aufträge werden in dem Fall, dass keine anderen Übertragungsformen mehr zur Verfügung stehen, in bereits vorangefertigte Formulare überführt, die per PDF-Reader anhand von Vorselektionsfeldern schnell und unkompliziert ausgefüllt werden können. Diese Formulare werden ausgedruckt. Sollte kein Ausdruck (mehr) möglich sein, sind entsprechende Formulare ebenfalls bereits vorausgedruckt in den Leitstellen vorhanden, die manuell auszufüllen sind. Sofern diese Formulare ausgehen, wird dazu übergegangen, relevante Informationen per Zettel und Stift zu notieren. Es wurde jedoch angemerkt, dass die papierbasierte Erfassung bzw. Nacherfassung als Alternative zu den digitalen Dokumentationssystemen nur in einem Zeitrahmen von bis zu 48 Stunden annehmbar ist. Bei einem Ausfall internetbasierter Dienste, der über diesen Zeitrahmen hinausgeht, könnte der damit verbundene hohe, administrative Aufwand problematisch werden.

Ungeachtet dessen, in welcher Form die Informationen festgehalten werden, werden die wesentlichen Einsatzdaten fortan im Rahmen reduzierter Statusmeldungen per BOS-Funk an die Einsatzfahrzeuge übermittelt. Dabei ist zwischen dem Rettungsdienst und dem Krankentransport zu unterscheiden. Während die Statusmeldungen im (nicht-zeitkritischen) Krankentransport stark auf das Wesentliche reduziert werden können, werden im Rettungsdienst weiterhin alle Statusmeldungen übermittelt. Dies dient der Dokumentation des Zeitverlaufs. Einschränkungen im Betrieb sind von

außen nicht merkbar, da die Annahme von Notrufen und die Abarbeitung von Einsatzaufträgen weiterhin unbeeinträchtigt durchgeführt werden kann.

Wenn Einsatzdaten weder digital noch per Mobilfunk an Leitstellen übermittelt werden können, kann nur noch die Abarbeitung zuvor gespeicherter Aufträge, beispielsweise aufgrund von Voranmeldungen, erfolgen. Das ist in manchen Fällen sinnvoll, z.B. im Hinblick auf Dialyse-Patient:innen, jedoch im Hinblick auf ein Krisenszenario und die Erwartbarkeit einer erhöhten Anzahl an Unfällen, Ausschreitungen oder ähnlichen Umständen nicht in allen. So sind beispielsweise Aufträge, die über den leitstellen-internen USB-Stick gespeichert wurden, ab einem bestimmten Zeitpunkt entweder bereits abgearbeitet oder angesichts der länger andauernden Krisensituation und den möglichen, daraus resultierenden Umständen auf einen späteren Zeitpunkt zu verschieben, sofern dies möglich ist. Die Kommunikation zwischen den Einsatzorganisationen funktioniert weiterhin gesichert über das Digitalfunk- bzw. TETRA Netz aufgrund der Anbindung über Dark-Fiber-Leitungen, die die Verfügbarkeit der Kommunikation zwischen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sicherstellt. Einsatzfahrzeuge, zu welchen keine aufrechte Funkverbindung oder andere Möglichkeit der Kommunikation besteht und auch nicht hergestellt werden kann, kehren zu ihrer jeweiligen Dienststelle zurück, um dort neue Aufträge zu empfangen bzw. auf solche zu warten.

Zusammengefasst können beeinträchtigte Services bzw. Leistungen im Krankentransport

- die digitale Datenübermittlung
- die digitale Auftrags- und Standortübermittlung
- sowie die digitale Dokumentation und Datensicherung

betreffen (vgl. Schachenhofer et al. 2022).

#### *6.4.1.2 Auswirkungen auf ein Krankenhaus*

Die Aufrechterhaltung der Prozesse in einem Krankenhaus ist auch in einer Krisensituation maßgeblich, um die notwendige medizinische Versorgung der Bevölkerung zu gewährleisten bzw. aufrechtzuerhalten. Krankenanstalten können grundsätzlich anhand ihrer Zugehörigkeit zu einem Versorgungssektor (Akut-/ Kurzzeitversorgung bzw. Nicht-Akutversorgung), ihres Versorgungsbereiches (Allgemeinversorgung bzw. Spezialversorgung), des Krankenanstalts-Typs (Allgemeine Krankenanstalten bzw. Sonderkrankenanstalten sowie Sanatorien und Pflegeanstalten für chronisch Kranke), sowie ihrer Fondszugehörigkeit (landesgesundheitsfondsfinanziert bzw. nichtlandesgesundheitsfondsfinanziert) unterschieden werden (vgl. Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz 2021). Im Folgenden wird beschrieben, wie sich ein großflächiger, langandauernder Ausfall internetbasierter Dienste auf ein im Rahmen der Erhebungen nicht näher spezifiziertes Krankenhaus auswirkt und welche Folgen sich aus einer Beeinträchtigung der Prozesse ergeben können.

##### Sofortige Auswirkungen eines Ausfalls internetbasierter Dienste

Der Ausfall internetbasierter Dienste bedingt die Beeinträchtigung sämtlicher, digitaler Meldewege in einem Krankenhaus. Die papierlose Übergabe von Patient:innen

über Internet-Schnittstellen funktioniert nicht mehr, wodurch auch die Kommunikation mit anderen Krankenhäusern beeinträchtigt ist.

Web-basierte Applikationen zur Unterstützung medizinischer Kernprozesse, wie z.B. das Onkologie-Informationssystem, in dem sämtliche Patient:innendaten für das Tumorboard zusammengefasst werden, funktionieren nicht mehr. Auch der digitale Austausch mit Patient:innen, beispielsweise beim web-basierten Auslesen von Blutzuckermessgeräten und anderen, telemedizinischen Daten, ist nicht mehr möglich.

E-Card Anwendungen (e-Rezept etc.) und die elektronische Gesundheitsakte (ELGA) sind ebenfalls ausgefallen *(Anmerkung: ELGA dient als Informationssystem, um ELGA-Nutzer:innen und berechtigten ELGA-Gesundheitsanbietern wie z.B. Spitälern und Apotheken den digitalen Zugriff auf ELGA-Gesundheitsdaten zu ermöglichen und trägt damit maßgeblich zur digitalen Vernetzung zwischen Krankenhäusern, Ärzt:innen und anderen relevanten Gesundheitsanbietern bei (vgl. ELGA GmbH 2021))*. Ebenfalls von dem Ausfall betroffen sind Labor- und Krankenhausinformationssysteme. Da Ergebnisse nicht mehr elektronisch verarbeitet werden können, verringert sich der Labordurchsatz deutlich, was die Arbeitsprozesse in den Labors erschwert.

Patient:innendaten werden im Normalbetrieb elektronisch erfasst und in Verrechnungssysteme überspielt. Bei einem Ausfall internetbasierter Dienste ist ein erheblicher, personeller Mehraufwand notwendig, da Patient:innendaten manuell ein- bzw. übertragen werden müssen. Unter Umständen besteht zusätzlicher Personalbedarf. Wie auch im Notfall- und Krankentransport ist damit zu rechnen, dass insbesondere jüngeres Personal nur wenig bzw. u.U. sogar gar nicht mit analogen Ersatzprozessen vertraut ist.

Auch sämtliche elektronische Beschaffungsvorgänge sind bei einem Ausfall internetbasierter Dienste vorübergehend beeinträchtigt. Unter Umständen muss mit Lieferverzögerungen gerechnet werden. Im Hinblick auf Medikamente muss daher überprüft werden, wie lange die Versorgung von Patient:innen gewährleistet bzw. aufrechterhalten werden kann, falls Nachbestellungen vorübergehend auch telefonisch nicht möglich sein sollten bzw. es auf Grund der Situation zu generellen Lieferverzögerungen kommen sollte. Es wird außerdem angenommen, dass das Verbrauchsmaterial zum Zweck von Operationen und einer Akut-Versorgung etc. in einem solchen Krisenszenario relativ rasch (innerhalb weniger Stunden) zur Neige gehen könnte, während die Nahrungsmittelversorgung in den Kliniken unter Umständen auch ohne externe Zulieferungen für zumindest drei Tage gewährleistet ist.

Darüber hinaus sind in Spitälern oft Fernwartungen medizintechnischer Geräte, beispielsweise von Laborautomaten, notwendig. Auch Routinetätigkeiten wie die Kalibrierung von Geräten, die früher durch das Personal vor Ort durchgeführt werden konnten, werden zunehmend mittels Remote-Zugriff gemacht. Aufgrund der Abhängigkeit von einer verfügbaren, digitalen Datenverbindung ist bei einem Ausfall internetbasierter Dienste daher vorübergehend weder die Wiederherstellung noch die Fernwartung medizintechnischer Geräte durch qualifizierte Techniker:innen mittels Remote-Zugriff möglich.

Erwartbare Auswirkungen innerhalb 24-48 Stunden:
Definierte, nicht-elektronische Ersatzmeldewege werden in Anspruch genommen. Die Dokumentation erfolgt weiterhin analog über dafür vorgesehene Notfall- bzw. Einsatzprotokolle. Unter Umständen ist mit einem erhöhten Unfallaufkommen, sowie mit Schließungen von Ordinationen zu rechnen. Die Konsequenz sind überfüllte Ambulanzen. Um einer sinkenden Qualität der medizinischen Versorgung entgegenzuwirken, sollten verstärkt Ärzt:innen bzw. Pflegekräfte in den Ambulanzen eingesetzt werden. Sollte ein Versorgungsengpass eintreten, muss unter Umständen die Behandlung gewisser Patient:innen priorisiert werden. Im Falle von Unruhen bzw. Ausschreitungen müssen bei Krankenhäusern Einsatzkräfte stationiert werden. Auch die Umstellung auf den Krisenbetrieb ist notwendig.

Zusammengefasst können beeinträchtigte Services bzw. Leistungen in Krankenhäusern betreffen:

- Digitale Meldewege
- Die papierlose Übergabe von Patient:innen über Internetschnittstellen
- Die digitale Koordination von Rettungsanfahrtssperren
- web-basierte Applikationen zur Unterstützung med. Kernprozesse
- Labor- und Krankenhausinformationssysteme
- elektronische Beschaffung (ausreichende Medikamentenversorgung muss geprüft werden)
- Servicierung und Instandhaltung der Medizintechnik über Online-Zugriff (Fernwartung etc.)
- Sowie E-Card Anwendungen bspw. e-Rezept

(vgl. Schachenhofer et al. 2022).

#### *6.4.1.3 Relevante Schnittstellen zwischen Notfall- und Krankentransport und Krankenhäusern*

Ein Ausfall internetbasierter Dienste betrifft Krankenhäuser und den Notfall- und Krankentransport darüber hinaus in verschiedenen Schnittstellenbereichen. Darunter fällt beispielsweise die Kommunikation zwischen Krankenhäusern und Rettungsleitstellen über Internetschnittstellen, sowie die Online-Koordination der Krankenhausanfahrten, die daraufhin ausfällt. Auch die Koordination von Rettungsanfahrtssperren, die digital abläuft, ist vorübergehend nicht möglich. Somit müssen Einsatzfahrzeuge telefonisch koordiniert werden, was eine erhöhte Personalauslastung und die Gefahr von Missverständnissen zur Folge hat. Wenn die telefonische Anmeldung im aufnehmenden Krankenhaus beispielsweise aufgrund einer Überlastung des Mobilfunknetzes nicht möglich ist, muss diese über die Leitstelle per Funk erfolgen.

Darüber hinaus sind Rettungsprotokolle für Notfallambulanzen nicht mehr einsehbar. Ebenso können keine Abfragen über 1450 getätigt werden (Fastlane, die die Möglichkeit bietet, als Privatperson rasch von diplomiertem Krankenpersonal beraten zu werden und im Ernstfall wird der Rettungsdienst mit/ohne Notarzt entsendet (vgl. Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz o. D.)). Auch die Übermittlung von EKGs von Rettungswägen an die diensthabenden Kardiolog:innen in den Kliniken ist beeinträchtigt.

Automatische Schnittstellen zwischen Notruforganisationen und Klinikbetreibern sind unterbrochen. Auch Mobile Apps, die zur Kommunikation zwischen Rettungswägen, Leitstellen und Kliniken im Einsatz sind, stehen während der Zeit eines Ausfalls internetbasierter Dienste nicht zur Verfügung. Damit hängt auch der Akutversorgungsnachweis an den einzelnen Klinikstandorten zusammen, wodurch die Verfügbarkeit von Versorgungsleistungen überprüft wird.

Da auch der Flugplandatenaustausch in einem solchen Szenario eingeschränkt ist, findet vorübergehend nur noch der unbedingt notwendige Flugverkehr (bspw. Transport von Notfallgütern, sowie Militärtransporte und Sonderflüge) statt. Dementsprechend muss auch der Einsatz von Rettungshubschraubern vorerst soweit wie möglich ausgesetzt werden, weswegen Interhospitaltransporte auf die Straße verlegt werden. Dies führt zu verlängerten Transferzeiten, wodurch Patient:innenschäden (bspw. neonatologische Überstellung) nicht gänzlich ausgeschlossen werden können.

Bezogen auf den Heimtransport ergibt sich darüber hinaus ein Interessenskonflikt. Aus Krankenhaus-Sicht ist dieser aufgrund begrenzter Kapazitäten essenziell, während diesem aus Krankentransport-Sicht eine eher untergeordnete Rolle zukommt, da die Versorgung der Patient:innen bereits gewährleistet ist.

Dementsprechend können beeinträchtigte Services bzw. Leistungen an Schnittstellen zwischen Krankenhäusern und Organisationen aus dem Krankentransport wie folgt zusammengefasst werden:

- automatische Schnittstellen zwischen Notruforganisationen und Klinikbetreibern
- mobile Apps zur Kommunikation, insbesondere im Hinblick auf den Akutversorgungsnachweis an Klinikstandorten
- die Übermittlung von Rettungsprotokollen und EKGs an Notfallambulanzen bzw. Kliniken (vgl. Schachenhofer et al. 2022).

### 6.4.2 Anwendungsfälle aus dem Transportsektor

In den nächsten Abschnitten werden die erhobenen Auswirkungen eines länger andauernden und großflächigen Internetausfalls anhand von zwei praktischen Anwendungsfällen aus dem Transportsektor näher beschrieben. Die Anwendungsfälle wurden aus Expert:innengesprächen mit Vertreter:innen des Transportsektors sowie den Informationen, die im Rahmen der abgehaltenen Workshops gewonnen wurden, abgeleitet und systematisch aufbereitet (Schachenhofer et al. 2022).

#### *6.4.2.1 Auswirkungen auf ein Transportunternehmen*

Die Fahrzeugflotte des Transportunternehmens ist GPS- und internetbasiert mit der unternehmenseigenen Customer Relationship Management (CRM) Software verknüpft. Darüber wird ca. alle 30 Sekunden der Standort übermittelt. Die Standort-Dokumentation erfolgt internetbasiert über ein digitales System, in dem die Fahrzeuge erkennbar sind. Bei dem betrachteten Transportunternehmen handelt es sich um ein intermodales Transportunternehmen, dass die Verkehrsträger Straße und Schiene miteinander kombiniert (inkl. einem eigenen Containerterminal mit Bahnan-

schluss). Es umfasst mehrere Standorte und ein Team von Disponent:innen organisiert und disponiert die Transporte. Neben Straßentransporten und kombinierten Transporten bietet das Unternehmen auch die Lagerung verschiedener Güter (z.B. Lebensmittel, Sondergüter und Gefahrgut) an, wofür u.a. scannergeführte, computergestützte Hochregallager zum Einsatz kommen. Um eine leistungsfähige IT-Infrastruktur zu gewährleisten und die Server- und Storagearchitektur möglichst ausfallsicher zu gestalten, sind redundante Netzwerkanbindungen vorhanden. Das Unternehmen bietet als Application Service Provider außerdem verschiedene Softwarelösungen an, um komplexen logistischen Anforderungen zu begegnen. Diese dienen der Optimierung von Logistikkosten in der Produktionsstätte, sowie der Optimierung von Lagerbeständen und Durchlaufzeiten über eine mögliche Steuerung von Zulieferprozessen bis zur Anlieferung bei den Kund:innen.

#### Sofortige Auswirkungen eines Ausfalls internetbasierter Dienste

Wenn die Bandbreite abfällt, bekommen die Mitarbeiter:innen eine entsprechende Warnmeldung bzw. sieht man in der Zentrale, wenn keine Signale mehr von den Fahrzeugen empfangen werden. Die standortbezogenen Dienste und die Aktualisierung von Statusmeldungen sowie die digitale Dokumentation sind vorübergehend beeinträchtigt.

Aufträge werden laufend digital an die unternehmenseigene CRM-Software übermittelt, wo sie automatisch lokal abgespeichert werden. Dementsprechend sind in der Regel bis zum Zeitpunkt des Ausfalls Auftragsinformationen für die nächsten 1-2 Stunden unabhängig vom Internetzugriff vorhanden. Der Empfang und die Abspeicherung neuer Aufträge sind während eines Internetausfalls temporär nicht möglich.

Auch die digitale Kommunikation ist bei einem Ausfall internetbasierter Dienste beeinträchtigt. Die automatisierte Kommunikation als Teilbereich von digital ablaufenden Kommunikationsprozessen wird dementsprechend auf den Mobilfunk verlagert. Falls auch die Mobiltelefonie beeinträchtigt ist, melden sich Fahrer:innen beispielsweise über Telefonzellen an Tankstellen. Problematisch ist allerdings, dass die Anzahl von Telefonzellen kontinuierlich reduziert wird, da das vorhandene Telefonzellen-Netz durch die Mobiltelefonie stark an Bedeutung verloren hat. Viele Telefonzellen wurden dementsprechend bereits für andere Zwecke, z.B. als Bücherzellen, umfunktioniert. Das Beispiel des Transportunternehmens zeigt, dass ein gutes Telefonzellen-Netzwerk in einer Krisensituation jedoch entscheidend sein kann, um die betriebliche Kommunikation so gut wie möglich aufrechtzuerhalten. Durch die starke Reduktion einsatzfähiger Telefonzellen ist zu erwarten, dass sich einige Fahrer:innen in einer solchen Situation nicht im unmittelbaren Umkreis einer (funktionierenden) Telefonzelle befinden und daher erst nach einer suchen müssen, um die Kommunikation mit den Disponent:innen wiederherzustellen. Auch die Dokumentation muss vorübergehend analog erfolgen. Die Folgen sind ein höherer Zeit- und Arbeitsaufwand für Fahrer:innen und Disponent:innen und dementsprechend eine erhöhte Personalauslastung.

Statusmeldungen für Gefahren- und Kühlgüter, die in bestimmten Zeitabständen digital übermittelt werden, fehlen ab dem Zeitpunkt eines Ausfalls.

IT-Server sind am Unternehmensstandort vorhanden und es gibt eine redundante Anbindung. Wenn das System in der Zentrale ausfällt, ist ein Back-up von Daten

vorhanden. Die Ausfallursache und die Wahl des Speichermediums (bspw. in der Cloud oder lokal) können entscheidend dafür sein, ob der Zugriff auf Back-up Sicherungen weiterhin möglich ist.

Aufgrund der zunehmenden Modernisierung von Prozessen funktionieren viele Faxleitungen heute digital bzw. wurden teilweise direkt durch digitale Lösungen ersetzt (vgl. ISIDOR Expert:inneninterviews 2021; vgl. Burgstedt und Britze 2021). Auch Kund:innen-Schnittstellen sind oftmals internetbasiert. Darüber hinaus sind der E-Mail-Verkehr bzw. E-Mail-Zugänge zum System und andere Office 365 Anwendungen abhängig vom Internet. Insofern können neue Aufträge während eines Internetausfalls nur noch telefonisch entgegengenommen werden.

Maßnahmen und konkrete Abläufe für den Notbetrieb sind festgelegt. Es gibt zwei Ausfallsstufen: Daten und Telefonie. Wenn internetbasierte Dienste ausgefallen sind, sind interne und externe Meldewege per Telefon vorgesehen. Problematisch wird es, wenn die telefonische Kommunikation mit der Zentrale bzw. Kund:innen ebenfalls wegfällt.

Erwartbare Auswirkungen innerhalb 24-48 Stunden

Ein länger andauernder Ausfall internetbasierter Dienste hat schwere Folgen für ein Transportunternehmen. Es wird bereits ab einem halben Arbeitstag, schwierig, die Arbeitsprozesse aufgrund der Beeinträchtigung der automatisierten Kommunikation und Status- bzw. Standortübermittlung, sowie der digitalen Dokumentation aufrechtzuerhalten.

Im Überblick können beeinträchtigte Services bzw. Leistungen in Transportunternehmen gemäß den vorangegangenen Ausführungen daher beispielhaft

- standortbezogene Dienste
- den Empfang und Abspeicherung neuer Aufträge
- den Zugriff auf Back-Up Sicherungen
- E-Mail-Verkehr und die digitale Kommunikation
- die Aktualisierung von Statusmeldungen und digitale Dokumentation
- sowie die Statusmeldungen von Gefahren- und Kühlgut betreffen (vgl. Schachenhofer et al. 2022).

#### *6.4.2.2 Auswirkungen auf den Betreiber eines Verteilzentrums*

Der zweite Anwendungsfall aus dem Transportsektor bezieht sich auf den Betreiber eines Verteilzentrums. Dabei handelt es sich um ein trimodales Terminal, das durch die Verkehrsträger Wasser, Straße und Schiene angebunden ist. Das Angebot umfasst Stuffing/ Stripping, also die Be- und Entladung von Containern im Hafen, Lagerlogistik und Zolldienstleistungen. Zusätzlich dazu werden Kühlcontainer vor Ort gemäß gültiger Standards durch Reefer-Expert:innen, professionell auf Kühlgut spezialisiertes Personal, geprüft und repariert. Die Dokumentation der Vorgänge innerhalb des Verteilzentrums erfolgt im Normalbetrieb internetbasiert. Aufgrund des hohen Automatisierungsgrades hat ein großflächiger und längerfristiger Internetausfall daher schwerwiegende Folgen für den Betreiber eines Verteilzentrums. Diese werden im Folgenden näher erläutert.

### Sofortige Auswirkungen eines Ausfalls internetbasierter Dienste

Aus einem vergangenen Ereignis ist bekannt, dass sämtliche internetbasierte Schnittstellen mit Kund:innen, die über das interne Betriebssystem laufen, bei einem Internetausfall nicht mehr funktionieren. Das System enthält sämtliche, für den Betrieb erforderlichen Informationen wie beispielsweise Stockreports. Da nichts lokal bzw. in Papierform gespeichert ist, kann auch die Stellplatzdokumentation der Container im Terminal, das Abrufen von Bezugsdaten und vieles mehr vorübergehend nicht durchgeführt werden.

Auch die Abwicklung von Prozessen und Services, wie beispielsweise die Abfertigung von Güterzügen und LKWs inklusive der erforderlichen Containerausgaben und -entgegennahmen, ist temporär nicht möglich. Dementsprechend können Transportunternehmen ihre Zustellungen nicht durchführen.

Zusätzlich dazu ist auch die digitale Kommunikation mit den zuständigen Zollämtern, sowie die elektronische Zollabfertigung im Zeitraum des Ausfalls beeinträchtigt. Containermeldungen über das NTCS an die zuständige Zollstelle müssen daher vorübergehend analog gemacht werden.

Sämtliche Office 365 Anwendungen und Dienste (E-Mail Verkehr etc.), sowie digitale Kund:innen-Schnittstellen sind ebenfalls betroffen. Die Verständigung der Hauptkund:innen erfolgt daher vorübergehend per Telefon. Wie im Fall des zuvor beschriebenen Transportunternehmens hätte ein Ausfall der Telefonie auch für den Betreiber des Verteilzentrums nachteilige Folgen, da dadurch die Verständigung von Kund:innen vorübergehend zum Erliegen kommen würde.

### Erwartbare Auswirkungen innerhalb 24-48 Stunden

Eine Notlösung bei einem länger andauernden Ausfall ist die analoge Abwicklung per Papier und Stift. Dies bedingt jedoch eine erhöhte Personalauslastung während des Ausfalls, sowie danach zur Wiederherstellung des Stellplatzsystems, da die Dokumentation über das System grundsätzlich digital und automatisiert erfolgt. Die Abgabe von Voll-Containern ist beispielsweise nicht möglich, da dafür Bezugsdaten aus dem System benötigt werden, die nur digital vorhanden sind. Eine Ausgabe von Leercontainern wäre grundsätzlich möglich, allerdings wird auch dazu eine sogenannte Freistell-Nummer benötigt, auf die ebenfalls nur digital zugegriffen werden kann. Die Weiterarbeit ohne die Möglichkeit, digital auf das System und die darauf befindlichen Bezugsdaten zuzugreifen, bedingt einen hohen Mehraufwand.

Bei Bedarf wäre es darüber hinaus möglich, Zollkontrollen vor Ort durch einen Zollbeauftragten durchführen zu lassen, wenn dies notwendig ist.

Um nach dem Hochfahren der Systeme die Stellplatzdokumentation wieder auf den aktuellen Stand zu bringen, bräuchte das Unternehmen laut eigenen Angaben zwei bis drei Tage, bis die Weiterarbeit wieder wie gewohnt über das Betriebssystem aufgenommen werden kann.

Im Überblick können beeinträchtigte Services bzw. Leistungen in Verteilzentren gemäß den vorangegangenen Ausführungen daher beispielhaft betreffen:

- internetbasierte Schnittstellen mit Kund:innen, die über das Betriebssystem laufen
- den E-Mail-Verkehr
- die Dokumentation der Vorgänge und Stellplatzsystem im Terminal
- die Abfertigung von Zügen und LKWs sowie Containerausgaben und -entgegennahmen
- und die digitale Kommunikation mit Kund:innen, Zoll etc.

(vgl. Schachenhofer et al. 2022).

Sektorspezifische Auswirkungen eines langandauernden und großflächigen Ausfalls internetbasierter Dienste betreffen dementsprechend Organisationen aus beiden vorgestellten Sektoren in einem oder mehreren der folgenden Bereiche:

- internetbasierte Dienste
- Internetbandbreite
- Kompromittierung von Cloud-Sharing Services bzw. digitalen Kommunikationskanälen

Die durchgeführten Interviews und die Ergebnisse aus den Workshop-Reihen, die im kommenden Kapitel näher erläutert werden, bestätigten immer wieder Schwerpunktthemen, mit denen bei einem großflächigen Ausfall internetbasierter Dienste zu rechnen ist. Anhand der Modelle wurden relevante Verlagerungsschleifen visualisiert, die bei einem Ausfallsereignis in Kraft treten können. Diese Verlagerungen führen zu signifikanten Verzögerungen, beispielsweise bei der Übermittlung wichtiger Dokumente, Einschränkungen und Einbußen in der Qualität der Kommunikation und vorhandenen Datenlage, einer steigenden Personalauslastung und einer damit einhergehenden, erhöhten Fehleranfälligkeit aufgrund von steigendem Druck und unbekannten, analogen Prozessen. Darüber hinaus besteht bei einem Zusammentreffen mit einer weiteren Krise die erhöhte Gefahr des Zusammenbruchs des Systems, da Präventionsmaßnahmen selten mehr als eine Krise in Betracht ziehen.

Die beschriebenen Anwendungsfälle zeigen konkrete Auswirkungen auf Anwender:innen im System vor dem Hintergrund einzelner Modellausschnitte, wodurch wesentliche Verlagerungseffekte auch anhand realer Beispiele gezeigt wurden und die praktische Relevanz der Modelle nochmals verdeutlicht werden konnte.

In Kapitel 6.5 werden basierend auf den zuvor beschriebenen Erkenntnissen aus der Modellierung sowie den Anwendungsfällen Handlungsempfehlungen abgeleitet. Auf die Ausführungen zu Handlungsempfehlungen im Hinblick auf die vorgestellten Anwendungsfälle, sowie sektorübergreifende Handlungsempfehlungen im weiteren Sinne folgen Handlungsmöglichkeiten des SKKM im Ereignisfall.

## 6.5 Zwischenergebnisse aus den Modellen

Die Reaktion auf ein Ausfallsereignis, wie es in ISIDOR untersucht wird, ist davon abhängig, ob bereits zu Anfang bekannt ist, wie lange der Ausfall dauern wird. Je

nachdem, ob es sich dabei um eine abschätzbare bzw. bekannte Information handelt oder nicht, werden sich die Reaktionen und gesetzten Maßnahmen voneinander unterscheiden. Von der Dauer des Ausfalls ist auch abhängig, welche Handlungsempfehlungen ausgesprochen werden können. Es wurde beispielsweise festgestellt, dass es für manche Organisationen einfacher ist, während eines solchen Ereignisses den Betrieb einzustellen, sofern es sich nur um einen Ausfall von wenigen Stunden bis zu einem Tag handelt, da eine Weiterarbeit ohne digitale Dokumentation mehrere Tage Nachdokumentation erfordern würde. Es hängt dementsprechend stark von der individuellen Abhängigkeit eines Betriebes von digitalen Diensten im Rahmen betrieblicher Prozesse ab, wann es sinnvoll ist, auf analoge Prozesse zu verlagern. Im Folgenden werden Handlungsempfehlungen beschrieben, die bei einem langandauernden und großflächigen Ausfallsereignis entscheidend dazu beitragen können, dass Basisprozesse weiterhin aufrechterhalten werden können und kritische Daten nicht verloren gehen (Schachenhofer et al. 2022).

### 6.5.1 Zwischenergebnisse für die vorgestellten Anwendungsfälle

Im Krankentransport ist eine analoge Dokumentation sowie Datenübermittlung via USB eine Möglichkeit zur Verlagerung digitaler Dokumentations- und Datenübermittlungsprozesse, wobei allerdings mit einem erhöhten Arbeits- und Zeitaufwand zu rechnen ist. Die Auftragsentgegennahme funktioniert häufig ebenfalls über den Mobilfunk, bspw. über die Anrufumleitung auf ein leitstelleninternes Mobiltelefon. Bei Beeinträchtigung der Nutzung des Mobilfunks aufgrund einer möglichen Überlastung bleibt die Kommunikation über das BOS-Digitalfunknetz als weitere Ausfallebene aufrecht, auf die die Kommunikation zwischen Behörden und Organisationen mit Sicherheitsaufgaben verlagert werden kann. Die Kommunikation über den BOS-Funk ist jedenfalls nicht uneingeschränkt möglich, da zu beachten ist, dass nicht alle Betroffenen einen Zugang zum Digitalfunknetz Austria haben.

In Spitälern sollten bei einem Ausfall internetbasierter Dienste definierte (nicht elektronische) Ersatzmeldewege in Anspruch genommen werden. Die Dokumentation kann wie im Krankentransport analog über Einsatzprotokolle erfolgen. Sowohl in Spitälern als auch im Krankentransportbereich ist jedoch zu beachten, dass unter Umständen vor allem jüngeres Personal mit analogen Arbeitsweisen nicht vertraut ist und daher eventuell spezielle Einschulung benötigt. Auch die Koordination von Rettungsanfahrtssperren sollte vorübergehend telefonisch möglich sein. Wie im Krankentransport gibt es auch hier die Möglichkeit zur Kommunikation über den Mobil- oder BOS-Funk und auch hier muss bei Letztgenanntem bedacht werden, dass nicht jeder Zugang hat.

Sowohl bei Transportunternehmen als auch in Verteilzentren sollten In-House Lösungen als Alternative zu Cloud-Lösungen in Betracht gezogen werden. Auch im Transportbereich ist die Verlagerung auf die analoge Dokumentation im Ereignisfall in all jenen Unternehmensbereichen durchzuführen, wo dies möglich und sinnvoll ist. Der Arbeits- und Zeitaufwand im Fall des notwendigen Umstieges auf die analoge Dokumentation ist auch hier im Rahmen des Notbetriebes und Business Continuity Management Maßnahmen zu beachten. Die Kommunikationsverlagerung auf den Mobilfunk gilt auch im Transportbereich als Alternative, wenn digitale Kommunikati-

onskanäle kompromittiert bzw. anderweitig beeinträchtigt sind. Im Falle eines Transportunternehmens können beispielsweise auch Disponent:innen telefonisch über die Standorte der Fahrer:innen informiert werden. Auch im Fall von Verteilzentren wird insbesondere die Kommunikation mit den Hauptkund:innen vorübergehend auf den Mobilfunk verlagert werden, solange es zu keiner Beeinträchtigung des Mobilfunknetzes kommt. In Verteilzentren muss darüber hinaus auch die Containermeldung über NTCS an zuständige Zollstellen temporär analog durchgeführt werden. Darüber hinaus muss beachtet werden, dass die Wiederherstellung des Stellplatzsystems, sobald die internetbasierte Dokumentation wieder funktioniert, bis zu mehreren Tagen dauern kann (Schachenhofer et al. 2022).

### 6.5.2 Sektorübergreifende Zwischenergebnisse

Wie in den vorangegangenen Handlungsempfehlungen zu den Anwendungsfällen beschrieben, sind In-House Lösungen zur Abspeicherung von wichtigen Dokumenten auch sektorübergreifend als essenzielle Alternative zur Ablage in der Cloud bei der Vorbereitung auf einen Ausfall internetbasierter Dienste zu sehen. Dies ermöglicht auch im Anlassfall, weiterhin auf relevante Dokumente und damit verbundene Daten zugreifen zu können. Das ist auch insofern wichtig, da eine entsprechende In-House Lösung bzw. lokale Datensicherung gewährleistet, dass etwaige Daten nicht verloren gehen. Selbst wenn es sich um einen möglichen, durch einen Ausfall hervorgerufenen Fehler eines digital basierten Betriebs- oder Dokumentationssystems handelt, kann durch eine solche Maßnahme der Verlust relevanter Daten bzw. Dokumente vermieden werden. Anhand von Abbildung 19 wird ersichtlich, wie sich die Möglichkeit des Zugriffs auf einen lokalen Datenpuffer auf die nachgelagerte Datenqualität auswirkt. Je geringer der Verfügbarkeitsgrad der Abspeicherung und des Zugriffes auf digitale Daten ist, desto mehr wird der Zugriff auf den lokalen Datenpuffer genutzt, wodurch sich die nachgelagerte Datenqualität wiederum erhöht (Schachenhofer et al. 2022).

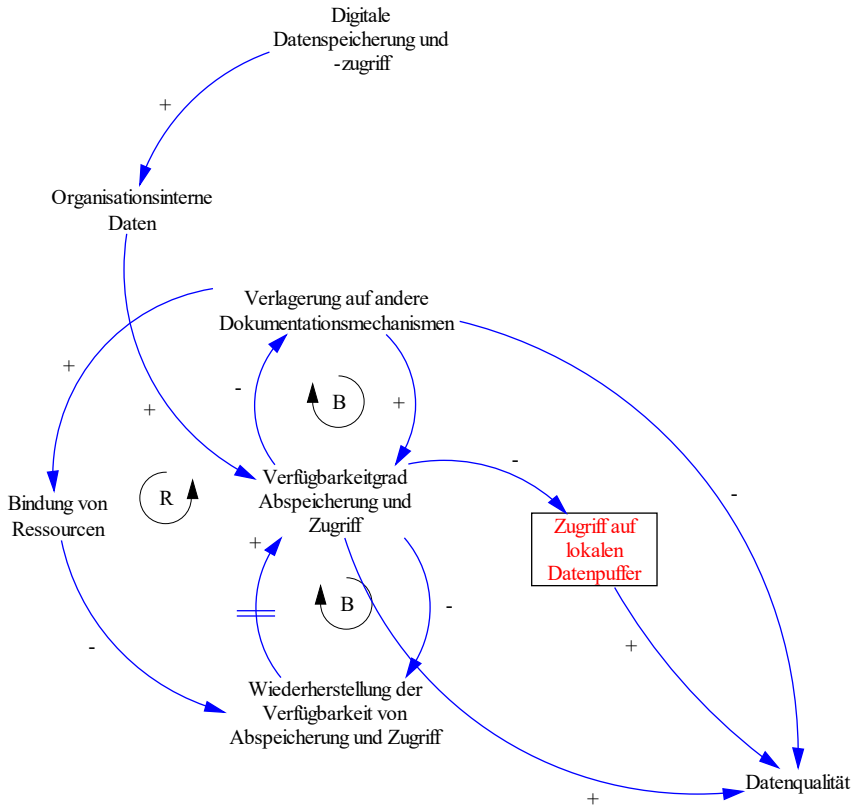



*Abbildung 19: Modell-Ausschnitt Digitale Datenspeicherung und Zugriff (vgl. Schachenhofer et al. 2022)*

Lokale Datenpuffer können zusätzlich zu Sicherungen (Back-Ups) in der Cloud genutzt werden. Ein Abgleich mit diesen Back-Ups kann täglich, stündlich oder minütlich erfolgen. Anhand definierter Parameter werden kritische Daten priorisiert, die in weiterer Folge in regelmäßigen, zeitlichen Abständen auf einen Network Attached Storage (Anmerkung: Ein NAS ist ein netzgebundener Speicher, der über Mechanismen wie Redundant Array of Independent Disks (RAID) redundant angebunden werden kann. Als Speichermedien können eine oder mehrere Festplatten oder SSDs (Solid State Drives) genutzt werden (vgl. Luber et al. 2021)) ausgeleitet werden und dementsprechend auch während eines Ausfalls internetbasierter Dienste zur Verfügung stehen (Schachenhofer et al. 2022).

Auch die analoge Dokumentation, wo diese möglich und sinnvoll erscheint, ist als Option in kritischen Betriebsprozessen zu erwägen. Da mit einer analogen Dokumentation ein erhöhter Arbeits- und Zeitaufwand einhergeht, kann eine gewisse Priorisierung bzw. Beschränkung auf die notwendigen Prozesse, die eine lückenlose Dokumentation erfordern, sinnvoll sein. Wie anhand der Anwendungsfälle aus dem Gesundheitssektor beschrieben wurde, sind in diesem Bereich vorausgedruckte Notfallformulare vorhanden, auf die bei Bedarf jederzeit zurückgegriffen werden kann. Notfallformulare, die speziell für Krisensituationen vorgesehen sind, und die bereits vor Ort in den Organisationsgebäuden vorgedruckt aufliegen, ergeben durchaus auch für Organisationen aus anderen Sektoren Sinn. Auch die Datenübermittlung

kann entsprechend analog bzw. über USB-Sticks und andere Speichermedien ausgeführt werden, wenn entsprechende Vorbereitungen dafür getroffen werden (Schachenhofer et al. 2022).

Es liegt im eigenen Verantwortungsbereich der Unternehmen, bzw. Organisationen, auch das eigene Personal so gut wie möglich auf einen langandauernden und großflächigen Ausfall internetbasierter Dienste vorzubereiten. Da aus den Gesprächen und Workshops hervorging, dass vor allem bei jüngerem Personal mit einem gewissen Grad an fehlendem Wissen im Hinblick auf eine analoge Arbeitsweise gerechnet werden sollte, könnten Schulungen und regelmäßige Trainings von Mitarbeiter:innen eine wirkungsvolle Maßnahme darstellen, um das gesamte Personal auf eine solche Ausnahmesituation vorzubereiten. Bevor Schulungen und Trainings stattfinden können, müssen manuelle Prozesse jedoch zuerst entwickelt bzw. dargestellt werden. Erst darauf aufbauend können Schulungen durchgeführt werden. Die Ablauforganisation, die Arbeits- und Informationsprozesse regelt, sollte den Bedingungen eines Ausfallsereignisses angepasst werden, wodurch sich auch Änderungen im Rahmen der Aufbauorganisation (z.B. Festlegung von Funktionen und Verantwortlichkeiten) ergeben können. Ein laufendes Angebot von Schulungen und insbesondere von Übungen, die unter Umständen auch verpflichtend vorgesehen sein könnten, rückt das Thema Internetausfall ins das Bewusstsein der Mitarbeiter:innen. Im Rahmen dessen sollten manuelle bzw. analoge Abläufe regelmäßig geübt werden, um eine Vertrautheit mit den Prozessen zu gewährleisten, wodurch voraussichtlich auch menschlichem Fehlverhalten in einer solchen Ausnahmesituation aufgrund unbekannter Prozesse entgegengewirkt werden könnte. Es ist essenziell, dass sich alle des Risikos eines solchen Ausfallsereignisses bewusst sind und Trainings und andere Aufklärungsangebote tragen dazu maßgeblich bei (Schachenhofer et al. 2022).

Risiken und deren Veränderungen im Wandel der Zeit müssen kontinuierlich beobachtet werden. Es ist wichtig, auch Business Continuity Management (BCM)-Maßnahmen laufend entsprechend aktueller Entwicklungen zu evaluieren und stellenweise oder gänzlich anzupassen, wenn diese nicht mehr zeitgemäß sind, um angemessen auf einen großflächigen Ausfall internetbasierter Dienste reagieren zu können. Angemessen bedeutet in diesem Zusammenhang, Kernbereiche und -aktivitäten zu priorisieren, welchen im Organisations- bzw. Unternehmensbereich bei der Aufrechterhaltung der Betriebstätigkeit mittel- und langfristig eine Schlüsselrolle zukommt, und die daher auch während eines Ausfalls internetbasierter Dienste vorübergehend in einer reduzierten Form weitergeführt werden müssen. Dafür müssen Verantwortungsbereiche klar definiert und von anderen abgegrenzt werden (Schachenhofer et al. 2022).

Die Inanspruchnahme definierter, nicht elektronischer, Ersatzmeldewege als eine weitere mögliche Gegenmaßnahme bei einem länger andauernden und großflächigen Internetausfall ist ebenfalls erforderlich. Diese sollten bereits im Zuge der Vorbereitung auf einen Krisenfall, wie er in ISIDOR untersucht wird, definiert werden. Ein Beispiel wäre die Abwicklung von Containermeldungen im Transportsektor an zuständige Zollstellen, die im Anlassfall vorübergehend eine analoge Durchführung ermöglichen sollte (Schachenhofer et al. 2022).

Die Verlagerung von digitalen Kommunikationskanälen auf den Mobilfunk war eine weitere Verlagerungsmöglichkeit von Kommunikationsprozessen, die von vielen verschiedenen Akteur:innen angeführt wurde. Allerdings geht dies mit einem erhöhten Zeit- und Arbeitsaufwand einher, was bereits in eine mögliche Planung von Notfallmaßnahmen bzw. den Krisenbetrieb und BCM-Maßnahmen miteinfließen sollte. Die temporäre Verlagerung auf den Mobilfunk sollte darüber hinaus durch redundant vorhandene Kontaktinformationen, wie beispielsweise lokal gespeicherte oder analoge Kontaktlisten und Telefonnummern, gewährleistet werden. Es ist außerdem empfehlenswert, in diesem Kontext auch eine mögliche Überlastung des Mobilfunknetzes in die Überlegungen zu etwaigen Vorbereitungen auf einen solchen Anlassfall miteinzubeziehen und vorausschauend miteinzuplanen. Da der Mobilfunk als prioritäre Verlagerungsmöglichkeit von nahezu allen Seiten angeführt wurde, ist zu erwarten, dass es auch im Zusammenhang mit dem Mobilfunknetz innerhalb kürzester Zeit zu Überlastungserscheinungen, also Verzögerungen bzw. unter Umständen sogar Netzausfällen kommen könnte. Während der BOS-Funk Behörden und Organisationen mit Sicherheitsaufgaben als weitere Verlagerungsoption von Kommunikationsprozessen zur Verfügung steht, gilt das für viele anderen Organisationen nicht. Aber auch wenn eine Verbindung über den BOS-Funk besteht, ist diese aus Sicht vieler Organisationen oft mit einer gewissen Unsicherheit verbunden, ob diese im Anlassfall tatsächlich funktionieren würde (Schachenhofer et al. 2022). Eine Möglichkeit, sich eine gewisse Unabhängigkeit von konventionellen Kommunikationsnetzen zu verschaffen, ist der Satellitenfunk. Große Fortschritte in diesem Bereich haben in den vergangenen Jahren dazu geführt, dass der Einsatz von Satellitenfunk zu Kommunikationszwecken in Krisenszenarien auch vermehrt in verschiedenen Europäischen Forschungsprojekten untersucht wurde. Ein Beispiel ist das Projekt MASSCRISCOM (Mass Crisis Communication with the Public), das insbesondere die Kommunikation zwischen der Öffentlichkeit und staatlichen Stellen während eines Krisenszenarios untersuchte (vgl. Pecorella et al. 2015: 171). Ein weiteres Projekt, das ebenfalls zu dem Schluss kam, dass öffentliche Netzwerke nicht genug Kapazität haben, um im Falle unerwarteter, großflächiger Krisenereignisse eine ausreichende Bandbreite für Widerherstellungsmaßnahmen bereitzustellen, ist das Projekt ABSOLUTE (Aerial Base Stations with Opportunistic Links for Unexpected & Temporary Events). Im Rahmen dessen wurden kooperative Netzwerk-Mechanismen untersucht, um öffentlichen Sicherheitskommunikationssystemen in Europa zu einer höheren Verfügbarkeit und dementsprechend einer starken Verlässlichkeit auch während Krisenszenarios zu verhelfen. Auch hier wurde Satellitenkommunikation als Ergänzung zu traditionellen Kommunikationsnetzwerken untersucht (vgl. Europäische Kommission 2019). Als weitere, relativ resiliente, Option hat sich Satelliteninternet in Krisensituationen herausgestellt, z.B. bei dem Erdbeben, dass sich am 12. Januar 2010 in Haiti ereignete. Obwohl das Erdbeben das Mobilnetz lahmlegte und Haitis einziges Untersee-Kabel durchtrennte, konnten NGOs dort über Satelliten weiterhin mit dem Internet verbunden bleiben (vgl. Goldstein 2010: 11f). Jedoch gibt es auch einige Bedenken: es ist nicht klar, wie damit umgegangen werden soll, dass unzählige neue Satelliten das bereits bestehende Weltraummüll-Problem weiter verstärken würden (vgl. Graydon 2020: 12). Zudem weist beispielsweise das Satelliteninternet Starlink, verglichen mit den derzeit hohen Anschaffungskosten und Monatszahlungen eine zu geringe Leistung auf, um in Europa eine breite Anwendung zu

finden. Aus Sicht potenzieller Anbieter ist die Instandhaltung der Satelliten-Infrastruktur gegenüber Funkstationen am Boden außerdem überaus teuer (vgl. Stepanek 2021). Darüber hinaus wäre zu prüfen, inwieweit eine Abhängigkeit der staatlichen Krisenkommunikation von privaten Anbietern, die in anderen Ländern angesiedelt sind, unerwünschte politische Abhängigkeiten erzeugt oder verstärkt.

Aus gesamtgesellschaftlicher Sicht ist es empfehlenswert, IT-Security bereits in der Schulbildung zu verankern, um bereits die jüngsten Mitglieder unserer Gesellschaft auf die Risiken aufmerksam zu machen, die es im World Wide Web gibt. Aktives Awareness Building und die Förderung eines verantwortungsvollen Umgangs mit digitalen Diensten ist aber auch grundsätzlich und altersunabhängig ein Kernthema, das verstärkt behandelt werden sollte. Grundzüge der IT-Sicherheit wie beispielsweise das Erkennen von Phishing Mails sind heutzutage für alle Personengruppen wichtig, da dies nicht nur im Organisationsumfeld, sondern auch im privaten Bereich vor Betrugsversuchen über digitale Kanäle schützt. Auch die Aufrechterhaltung der Vertrautheit mit analogen Prozessen, die bereits im professionellen Umfeld als Handlungsempfehlung angeführt wurde, ist für Privatpersonen im Ereignisfall entscheidend. Das Wissen um eine gewisse Unabhängigkeit von digitalen Diensten erlaubt es, auf den Ausfall internetbasierter Dienste mit einem klaren Kopf zu reagieren und verhindert Panikreaktionen, die bei einer größeren Menge von Personen zu weiteren Schwierigkeiten führen könnten. Aufklärungskampagnen über verschiedene Kanäle könnten dazu beitragen, Privatpersonen auf den Ausfall internetbasierter Dienste vorzubereiten. Zusätzlich dazu könnten Schulungen angeboten werden. Auch die Projektergebnisse aus ISIDOR könnten zielgruppenspezifisch aufbereitet und Teilnehmenden im Rahmen solcher Schulungen nähergebracht werden. Die Bewusstseinsbildung könnte auch dazu beitragen, die Gefahr von Panikreaktionen, die beispielsweise zu überfüllten Ambulanzen und Panikkäufen führen könnten, deutlich zu reduzieren. Im Ereignisfall spielt die Information der Bevölkerung über die Ursachen und Dauer des Ausfalls internetbasierter Dienste eine Schlüsselrolle bei der gemeinschaftlichen Krisenbewältigung. Alternative Kommunikationswege sind in diesem Fall beispielsweise die Übertragung über den öffentlich-rechtlichen Rundfunk (Fernsehen und Radiokanäle). Auch Lautsprecherwägen können im Krisenfall zwecks Information der Öffentlichkeit zum Einsatz kommen (Schachenhofer et al. 2022).

### 6.5.3 Zwischenergebnisse zu Handlungsmöglichkeiten des SKKM im Ereignisfall

Die Handlungsmöglichkeiten des SKKM im Ereignisfall sind – so wie auch die individuelle Reaktion jedes und jeder Einzelnen – abhängig von der Dauer des Ausfallsereignisses. Im Anlassfall ist essenziell, dass es eine wirksame Koordination zwischen Bund, Ländern und allen Betreibern kritischer Infrastrukturen gibt. Einsatzorganisationen und benötigte Einsatzkräfte müssen so rasch wie möglich mobilisiert werden. Sollte Bedarf an zusätzlichen Einsatzkräften bestehen, ist dieser ehebaldigst zu identifizieren und an die richtigen Schnittstellen und Personen zu kommunizieren. An dieser Stelle sollten insbesondere Fachkräfte aus dem IT-Bereich erwähnt werden, die in einem solchen Fall verstärkt an vielen verschiedenen Stellen gebraucht

werden. Das Fernsehen und der öffentlich-rechtliche Rundfunk sollten in Kommunikationsprozesse eingebunden werden, um einerseits einen solchen Bedarf an Helfer:innen und Fachkräften zu kommunizieren und um andererseits auch die Bevölkerung laufend und rasch zur aktuellen Situation und neuen Erkenntnissen zu informieren. Die Abstimmung mit Netzbetreibern funktioniert im Anlassfall über einen Krisenstab. Zusätzlich dazu kann der Amateurfunk als Unterstützung bei der Kommunikation mit der Bevölkerung dienen. Der Österreichische Versuchssenderverband (ÖVSV) übt laufend den Ausfall konventioneller Kommunikationsstrukturen und die Mitglieder des Verbandes sind mit den rechtlichen Grundlagen für den Amateurfunkdienst in Österreich vertraut. Die letzte Übung wurde beispielsweise am 1. Mai 2022 durchgeführt (vgl. ÖVSV 2022). Mitglieder könnten kleinräumig andere Personen innerhalb ihres eigenen, jeweiligen Wirkungskreises unterstützen. Inwieweit das technisch und rechtlich möglich ist (beispielsweise ist der Empfang von Informationen, die über den BOS-Funk übermittelt werden, nicht für die Öffentlichkeit bestimmt und daher verboten) muss im Rahmen der Vorbereitungen auf einen konkreten Anlassfall abgeklärt werden. Möglich wäre z.B. der Empfang wichtiger Informationen und die Weitergabe an die Nachbarschaft im engeren und weiteren Sinne, sowie das Absetzen von Notrufmeldungen bei medizinischen Notfällen wie Herzinfarkten oder Schlaganfällen. So könnten auch auf kleinräumiger Ebene Strukturen geschaffen werden, die in einer solchen Krisensituation im Sinne der Nachbarschaftshilfe durch Amateurfunker:innen unterstützend agieren könnten.

Kritische Versorgungseinrichtungen, die auch während des Ausfalls digitaler Dienste ihre Funktionsfähigkeit aufrechterhalten müssen, sollten priorisiert Unterstützung in Form von Helfer:innen und benötigten Fachkräften erhalten, wo dies erforderlich ist. An dieser Stelle sollte nochmals erwähnt werden, dass die Verlagerung auf den Satellitenfunk daher auch hier stellenweise als Kommunikationsmittel zum Einsatz kommen könnte, sofern dies möglich und sinnvoll erscheint und keine Verbindung über den BOS-Funk besteht bzw. auch als alternatives Kommunikationsmittel eingesetzt werden kann. Gegebenenfalls müssen Einsatzkräfte an manchen Stellen eingesetzt werden, wenn die Gefahr von Ausschreitungen bzw. Plünderungen besteht (Schachenhofer et al. 2022).

## 6.6 Wiederaufbau und zukünftige Entwicklungen

Der Wiederaufbau ist die Phase, in der das Problem, das zu dem großflächigen Ausfall internetbasierter Dienste geführt hat, identifiziert und soweit möglich behoben wird. Das erneute Hochfahren der Systeme sollte idealerweise in Schritten durchgeführt werden, sobald dies möglich ist. Dabei sollten systemkritische Einrichtungen und Dienste, die eine besondere Relevanz für die Bevölkerung aufweisen, priorisiert werden. In der Praxis wird sich so eine Vorgehensweise jedoch nicht umsetzen lassen. Auch in dieser Phase werden unter Umständen an vielen, verschiedenen Stellen IT-Notfallteams und Fachkräfte benötigt, was rechtzeitig an die zuständigen Stellen, sowie bei zusätzlichem Bedarf an die Bevölkerung kommuniziert werden sollte. Zudem sollten Zusatzbedarfe an Expert:innen und Fachkräften bereits während der Reaktionsphase miteingeplant werden, außerdem sind auch Gleichzeitigkeitseffekte d.h. Konsequenzen aufgrund des Ausfalls internetbasierter Dienste, die aufgrund der

Großflächigkeit an verschiedenen Stellen gleichzeitig auftreten und eventuell in Wechselwirkung miteinander stehen, in dieser Phase zu erwarten. Der Anwendungsfall des Verteilzentrums zeigt, dass unter Umständen längere Zeiträume erforderlich sind, um den Datenbestand wiederherzustellen bzw. zu aktualisieren. Bis zu dem Zeitpunkt der vollständigen Wiederherstellung bzw. Aktualisierung der Daten kann der operative Betrieb von Organisationen oftmals nur eingeschränkt erfolgen, was im Rahmen des Wiederaufbaus berücksichtigt werden muss und ausschlaggebend dafür ist, ob eine Organisation in einem gewissen Zeitrahmen eines Ausfalls internetbasierter Dienste eingeschränkt weiterarbeitet oder in dieser Zeit stillsteht.

Langfristig sollten Resilienz-Aspekte mitgedacht und auf allen Ebenen miteingeplant werden. Für die Maßnahmenumsetzung ist ausreichend Budget vorzusehen. Im Zusammenhang mit dem benötigten Budget wurde im Rahmen der Erhebungen angesprochen, dass der Ausbau eines Staatsgrundnetzes außerordentlicher Investitionen bedürfte. Brücken zwischen bestehenden Netzwerken wären eine weitere Möglichkeit, die Resilienz zu erhöhen und Kommunikationsstrukturen zu schaffen, die besser gegen Ausfälle geschützt wären. Aus Investitionssicht spricht einiges dafür, da vorhandene Strukturen bestmöglich genutzt werden, wodurch auch eine bessere ökonomische Effizienz erreicht werden könnte.

Nicht zuletzt zeigen die am Anfang der vorliegenden Studie bereits erwähnten Cyberangriffe auf Salzburg Milch, das Land Kärnten oder auch die Universität Salzburg, die allesamt während der Projektlaufzeit von ISIDOR stattfanden, dass Cyberattacken ein allgegenwärtiges Problem darstellen und deren Häufigkeit zunimmt. Grundsätzlich muss bei sämtlichen Überlegungen zu einem möglichen Ausfall internetbasierter Dienste, unabhängig von der konkreten Ursache, das Bewusstsein aller dahingehend vorhanden sein, dass Ressourcen in einer Krisensituation äußerst knapp sind und besonders KI-Betreiber zu einem gewissen Grad bereits im Vorfeld eigene Vorkehrungen treffen sollten, um im Anlassfall nicht unvorbereitet angetroffen zu werden. Anhand der vorangegangenen Ausführungen wird ersichtlich, dass bei einem langandauernden und großflächigen Ausfall internetbasierter Dienste keine alleinstehende Maßnahme zielführend sein wird. Vielmehr ist eine sinnvolle Kombination verschiedener Maßnahmen anzustreben, die die Nutzung vorhandener Kapazitäten und Ressourcen erlauben, und die möglichst effizient ineinandergreifen, um die optimale Bewältigung einer vernetzten Krise, wie sie in ISIDOR untersucht wurde, zu gewährleisten (Schachenhofer et al. 2022).

# 7 Sektorale und gesamtheitliche Betrachtung wahrscheinlicher Folgen eines Ausfalls

## 7.1 Vorbemerkung

Die im folgenden Kapitel beschriebenen Konsequenzen eines Internetausfalls in Österreich stammen aus der Zusammenführung und Analyse der Ergebnisse aus den Expert:inneninterviews, den Workshopreihen, der Übung und dem Evaluierungsworkshop am Ende des Projekts. Die Einteilung in bestimmte Sektoren kritischer Infrastrukturen folgt dabei lediglich den Bereichen, aus denen Expert:innen zu Wort gekommen sind. In der österreichischen Verwaltung gibt es zwar eine gemeinsame Vorstellung davon, was kritische Infrastrukturen sind, und selbstverständlich auch die Einstufung als KI-Betreiber für entsprechende Organisationen, aber keine einheitliche Kategorisierung. Diese folgt i.d.R. den Erfordernissen der jeweiligen Arbeitsprozesse.

### 7.1.1 Staatliches Krisen- und Katastrophenschutzmanagement (SKKM)

Unter Katastrophenmanagement wird in Österreich die „Gesamtheit aller aufeinander abgestimmten Maßnahmen in den Bereichen Katastrophenvermeidung, Katastrophenvorsorge, Katastrophenbewältigung und Wiederherstellung nach Katastrophen“ verstanden (BMI 2018). Die Elemente des Katastrophenmanagements decken dabei den kompletten Krisenzirkel (Katastrophenschutz = Vermeidung + Vorsorge; Katastrophenhilfe = Bewältigung + Wiederherstellung) basierend auf einer gemeinsamen Norm zum Integrierten Katastrophenmanagement ab (ÖNORM S 2304).

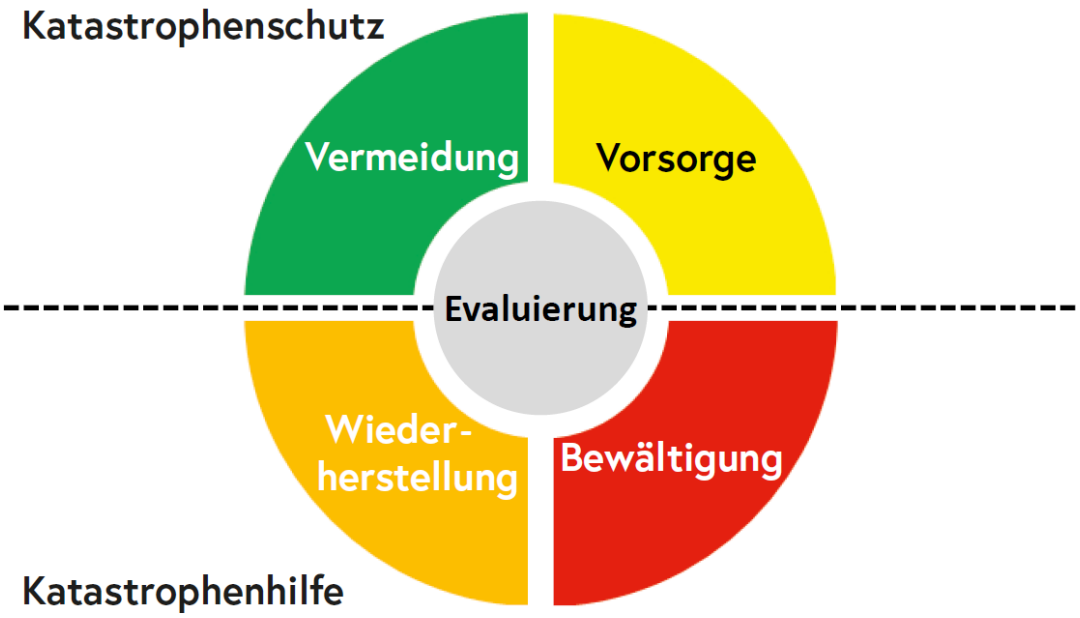



*Abbildung 20: Elemente des Katastrophenmanagements (BMI 2018 nach ÖNORM S2304)*

Die Aufgaben des Katastrophenmanagements liegen grundsätzlich bei den Gebietskörperschaften, das bedeutet operativ primär bei den Bundesländern. Diese nehmen außerhalb einer Katastrophen-Lage die Aufgaben der täglichen Gefahrenabwehr, der Vermeidung von Katastrophen und entsprechenden Vorsorge wahr. Die jeweiligen Katastrophenhilfegesetze regeln dabei die Feststellung einer Katastrophe sowie die behördliche Einsatzleitung in den Gemeinden, Bezirken und Ländern.

Die Kompetenzverteilung erfolgt basierend auf dem Subsidiaritätsprinzip von der lokalen Ebene zu den Bundesländern. Eine bundesweite Einsatzführung ist grundsätzlich nicht vorgesehen. Ausnahmen bilden hierbei Krisen und Katastrophen, die in den Kompetenzbestand des Bundes selbst fallen.

Krisen und Katastrophen machen allerdings einen erhöhten Koordinationsbedarf notwendig, vor allem wenn diese die regionalen Grenzen oder Ressourcen einzelner Länder überschreiten. Um die Koordination zu gewährleisten, wurde 2003 die Koordination des Staatlichen Krisen- und Katastrophenschutzmanagements und die internationale Katastrophenhilfe dem Bundesministerium für Inneres zugeteilt und ab 2004 als Staatliches Krisen- und Katastrophenschutzmanagement (SKKM) neu organisiert (BMI 2004).

Die Koordination des BMI erfolgt dabei vor allem durch den Koordinationsausschuss, in dem die Ministerien (jedenfalls das Bundeskanzleramt und die Ressorts für Außen, Finanzen, Gesundheit, Verteidigung und Soziales, sowie nach Bedarf die weiteren Bundesministerien), Bundeländer und Einsatzorganisationen, sowie ggf. Vertreter:innen der Presse (ORF, APA) und externe Expert:innen eingebunden werden. Der Vorsitz obliegt dem Generaldirektor für die öffentliche Sicherheit, unterstützt durch eine Fachabteilung im BMI. Dem Ausschuss obliegen bei großräumigen Gefährdungslagen die Koordination und Abstimmung der auf Bundes- und Landesebene erforderlichen Maßnahmen. Der Koordinationssauschuss tagt allerdings nicht nur im Katastrophenfall, sondern koordiniert auch die grundsätzliche Abstimmung der beteiligten Akteure. Zu diesem Zweck sind entsprechende Fachgruppen zu einzelnen Bereichen (u.A. Recht, Technik, etc.) eingerichtet.

Während der Laufzeit des Projekts Isidor wurde die SKKM-Architektur einer Neubewertung unterzogen und neu strukturiert, um vernetzte Krisen besser bewältigen zu können.

### 7.1.2 Nationale Rahmenbedingungen im Umgang mit vernetzten Krisen

Das Österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP) dient der Gewährleistung der Versorgungssicherheit im Hinblick auf Lebensmittel, Dienstleistungen aus den Bereichen Verkehr, Telekommunikation, Energie und Finanzen, sowie Sozial- und Gesundheitsdienstleistungen. Den strategischen Rahmen für das APCIP bildet die Österreichische Sicherheitsstrategie (Bundeskanzleramt Österreich 2015). Laut der Österreichischen Sicherheitsstrategie richtet Österreich seine Sicherheitspolitik am Konzept der „Umfassenden Sicherheitsvorsorge“ (USV) aus, dessen Ziel die systematische Zusammenarbeit verschiedener Politikfelder basierend auf einer Gesamt- sowie relevanten Teilstrategien ist. Als erforderliche Grundlagen für sicherheitspolitische Entscheidungen werden darin zum einen ein umfassendes Lagebild und zum anderen ein gemeinsames Lageverständnis aller Akteure

angeführt (Bundeskanzleramt Österreich 2013). Auch die neue Österreichische Strategie für Cybersicherheit (ÖSCS) 2021 stellt im Umgang mit vernetzten Krisen einen relevanten strategischen Rahmen zur Verfügung, der die nationale Cybersicherheitspolitik dabei unterstützt, einen sicheren Cyberraum zu schaffen und damit langfristig zur Erhöhung der gesamtstaatlichen Resilienz beizutragen (Bundeskanzleramt Österreich 2021). Die Richtlinie des Europäischen Parlaments und des Rates vom 06.07.2016 zu Vorgaben über Maßnahmen zwecks der Gewährleistung eines hohen gemeinsamen Netz- und Informationssicherheitsniveaus in der Union wurde national im Rahmen des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (kurz: Netz- und Informationssicherheitsgesetz bzw. NISG) sowie der zugeordneten Verordnung NISV umgesetzt. Das Netz- und Informationssystemsicherheitsgesetz legt Maßnahmen in den Sektoren Energie, Verkehr, Bank- und Finanzwesen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur sowie für Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung fest, die, wie der Name besagt, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen dienen (§ 2. Abs. 1 Z. 1 NISG). Inhalt der zugehörigen Verordnung sind Kriterien für die Parameter zu Sicherheitsvorfällen, Details zu den Regelungen im Rahmen der in § 2 NISG genannten Sektoren, Sicherheitsvorkehrungen und etwaigen Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste, jeweils mit Bezug zum NISG (§ 1. Abs. 1 Z. 1 NISV). Im Mai bzw. Juni 2020 wurde außerdem die Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020) in Kraft gesetzt. Inhalt der Verordnung ist zum einen die Festschreibung der in der Branchenpraxis zu dem Zeitpunkt bereits gängigen Mindestsicherheitsmaßnahmen aufgrund der technischen Leitlinien gemäß ENISA, die den Betrieb elektronischer Kommunikationsnetze und -dienste betreffen. Neben bestimmten Meldepflichten bei Sicherheitsvorfällen enthält die Verordnung ebenfalls die Möglichkeit freiwilliger Meldungen im Falle der Nichterreichung gewisser Schwellenwerte. Darüber hinaus werden im Rahmen der Verordnung spezifische Anforderungen an Betreiber von 5G-Netzen gestellt, die mehr als 100.000 Nutzer:innen in sämtlichen von ihnen betriebenen Netzen vorweisen können. Jene Betreiber sind außerdem dazu verpflichtet, im Hinblick auf potentielle Risikolieferanten halbjährlich eine Herstellerliste zu senden, die nach Funktionen kategorisierte Netzkomponenten enthält. Damit setzt die Verordnung bereits einige der Vorgaben aus der 5G EU Toolbox um, wie die Erfüllung gewisser Standards sowie die Umsetzung angeführter Sicherheitsmaßnahmen, wie z.B. die Verfolgung einer Multi-Vendor-Strategie (Czerni 2021).

## 7.2 Übersicht nach Sektoren

### 7.2.1 Energieversorgung

In vielen Konzernen bestehen i.d.R. vorab ausgearbeitete Pläne, die zwischen Störungen, Notfällen und Krisen unterscheiden. Je nach Schwere der Serviceunterbrechung werden andere Ressourcen aktiviert, und haben die handelnden Personen andere Spielräume, die bis zu sehr weitreichenden Befugnissen über Personal und Konzernbudget gehen können. Die Alarmierung erfolgt auch in dieser Branche meist

über SMS. Falls dieser Service ausfällt, gibt es noch die Möglichkeit, dass ein Betriebsfunk, integriert ins Kommunikationsnetz oder getrennt betrieben, zur Verfügung steht. Die notwendigen Endgeräte sind eventuell erst vom nächstgelegenen Betriebsgelände zu besorgen, womit sich eine zeitliche Verzögerung im Alarmierungsfall ergäbe. Alternativ, falls die Alarmierung außerhalb des Betriebs nicht gleich zu bemerken wäre (Internetausfall in der Nacht), wäre es denkbar die Funkgeräte über eine:n Fahrer:in zustellen zu lassen. Diese Verzögerung erscheint zunächst unbedenklich, da Leitstellen ohnedies 24/7 besetzt sind, und viele Betriebe davon ausgehen, dass die Versorgung auch über einige Stunden aufrechterhalten werden kann, ohne dass ein Eingreifen über das hinaus, was die Leitstelle leisten kann, notwendig ist.

In einigen Betrieben wurde ein Datennetz aufgebaut, das intern verwaltet wird, vom Internet unabhängig ist und alle (oder zumindest die wesentlichen) Standorte miteinander verbindet. Es besteht auch die Möglichkeit, intern ein Kommunikationsnetz aufzubauen, das z.B. durch die Nutzung unterschiedlicher Vorwahlen einen Übergang zwischen Festnetz, Mobilfunk und Funknetz ermöglicht. Damit müssten Mitarbeiter:innen bei einem Ausfall aller externen Netze und Verbindungen lediglich die nächste Niederlassung aufsuchen, um andere Personen im Konzern oder Organisationseinheiten erreichen zu können. Die Kommunikation und der konzerninterne Datenverkehr wären von einem Internetausfall zunächst nicht betroffen. Bei einer entsprechenden Betriebsgröße könnte ein solches Konzept einige der Auswirkungen eines Internetausfalls abmildern.

Die Prozesse zur Netzführung beim Übertragungsnetzbetreiber sind komplett abgekoppelt vom Internet und auf dessen Funktionieren nicht angewiesen. Eine Kommunikation nach Ausfall von Telefonie/SMS, ließe sich mit Einschränkungen auch hier über einen Betriebsfunk bzw. Satellitentelefone aufrechterhalten. Die Kommunikation zu Behörden (BMI, E-Control, etc.) wäre über BOS-Funk möglich.

Die Prozesse und die Planung bei EVUs berücksichtigen grundsätzlich in jedem Punkt die sog. n-1-Regel, die besagt, dass die Versorgung auch bei Ausfall einer beliebigen Komponente weiterlaufen muss.

Insgesamt betrachtet würde im Schadensfall als erstes voraussichtlich der Strommarkt zusammenbrechen. Langfristige Energie-Kontrakte wären vielleicht nicht betroffen, aber der sog. Spotmarkt, auf dem heute Angebote für die Versorgung morgen gehandelt werden, würde ausfallen. Es gäbe zum Teil Möglichkeiten, die Informationen auch über Fax oder Telefon einzumelden, solange dieser Kommunikationsweg noch funktioniert. Allerdings wird allgemein befürchtet, dass dies den zeitlichen Anforderungen nicht mehr entsprechen könnte: Es wären zu viele Daten, die im System der Strombörse wieder manuell eingegeben werden müssten. Damit wäre erforderlich, dass sich alle Kraftwerksbetreiber mit ihren Kunden und mit anderen Kraftwerks- bzw. Netzbetreibern koordinieren, um die Differenz zwischen Produktion und Verbrauch so gering zu halten, dass sie durch Ausgleichsenergie geschlossen werden kann. Ein wirtschaftlicher Betrieb ist so eigentlich nicht machbar, bzw. wäre reine Glückssache. Der noch kurzfristigere Intra-Day-Markt, auf dem Lieferungen mit z.T. nur 15 Minuten Vorlaufzeit gehandelt werden, wäre natürlich ebenfalls nicht mehr aufrechtzuerhalten. Der Ausgleichsenergiemarkt mit Primär-, Sekundär- und

Tertiärregelung, nebst den dahinterliegenden z.T. länderübergreifenden Automatismen, würde wahrscheinlich auch unter Datenlücken leiden oder ebenfalls ausfallen. Eine mögliche Konsequenz wäre ein österreichischer ‚Inselbetrieb'.

Auch aus Sicht der APG ist fragwürdig, ob sich die Marktmechanismen auf dem Strommarkt aufrechterhalten ließen, oder im Fall so einer Krise temporär ausgesetzt würden. Es käme dann zu einem Lastfolgebetrieb, in dem die APG den Zustand des Netzes monitort (über Messdaten, die über sog. Leittechniknetze hereinkommen und ebenfalls unabhängig vom Internet bereitgestellt werden können) und Anweisungen zur Einspeisung an die großen österreichischen Kraftwerksbetreiber gibt.

Das nicht mehr mögliche Bereithalten von Daten für Dritte wäre für die meisten kein großes Thema. Der Ausfall der Informationen über den Status anderer Kraftwerke in Europa, Wettervorhersagen, Daten des Aldis-Blitzortungssystems, Agenturdaten von bspw. Reuters oder Bloomberg usw. wären unangenehm, aber nicht bedrohlich.

Ein Austausch würde im Krisenfall mit dem eCERT und dem Cyber-Security-Center der DSN[5] angestrebt. Eine ständige Kommunikation zwischen APG und Kraftwerksbetreibern wäre auch erforderlich, da die Übermittlung der Fahrpläne der Kraftwerke derzeit automatisiert über Internet bzw. E-Mail erfolgt.

Die übereinstimmende Einschätzung der befragten Expert:innen ist, dass die Versorgung mit Strom weiterhin machbar wäre, allerdings nur mit deutlich erhöhtem Aufwand und eher im Grenzbereich ohne viel Spielraum für weitere Herausforderungen. Der Schwierigkeitsgrad in der Netzsteuerung wäre auch vom Wetter und anderen externen Faktoren abhängig. Ein Blackout als Folge eines Internetausfalls sollte vermeidbar sein.

Eine Schwierigkeit aus Sicht der APG ergibt sich aus dem Umstand, dass Internet und Stromnetz lange getrennt waren, aber immer weiter zusammenwachsen; insbesondere, wenn man Smart Meter mit dezentraler Produktion/Einspeisung, ev. Wegfall großer Kraftwerke zugunsten einer kleinteiligeren Struktur (die einen deutlich höheren Kommunikationsaufwand erfordert), Elektromobilität usw. ebenfalls als Teil des Stromnetzes betrachten möchte.

Der Dachverband Österreichs Energie arbeitet an einer internetunabhängigen Vernetzung aller EVUs in Österreich. Sobald diese Initiative erfolgreich abgeschlossen werden kann, oder das Ziel auf anderem Weg erreicht wird (vgl. Vorschläge zur Errichtung eines Staatsgrundnetzes), ergibt sich eine deutliche Verbesserung für die Versorgungsmöglichkeiten im Krisenfall.

### 7.2.2 Gesundheit

#### *7.2.2.1 Kliniken*

Besonders bei Blaulicht-Organisationen, dem Innenministerium und anderen Organisationen mit Aufgaben im Katastrophenfall wird insgesamt sehr umsichtig geplant. Allerdings kann sich immer unbemerkt eine Abhängigkeit von internetbasierten Diensten einstellen, insbesondere wenn Technologien gewechselt werden. Es wäre

[5] Direktion Staatsschutz und Nachrichtendienst, Nachfolger des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT)

daher wünschenswert, wenn nicht nur öfter Übungen/Simulationen durchgespielt würden, sondern wenn sich auch alle Personen, die in die Planung kritischer IT-Projekte involviert sind, dessen bewusst sind, dass die Abhängigkeit vom Internet ein großes Problem darstellen kann (mehr Fokus auf Security-by-Design).

Die Stadt Wien hat ein eigenes LWL-basiertes City-Netz, an das alle Betriebe der Wiener Stadtwerke angeschlossen sind, ebenso die Kliniken des Gesundheitsverbundes. Das Netz ist auf mehreren Ebenen redundant ausgeführt, sodass es allen Spitälern jederzeit möglich sein sollte, die zentralen Krankenhaus-Informationssysteme (KIS), die vom Rechenzentrum der Stadt Wien gehostet werden (MA01), zu erreichen. Telefonanlagen sind so konzipiert worden, dass die Standorte physisch direkt miteinander verbunden sind und keine Verstärker o.ä. Ausrüstung benötigen. Hier befände sich Wien jedoch in einer privilegierten Situation, die in anderen Städten und Gemeinden so vielleicht nicht mehr anzutreffen sei.

Häufig kommt es im Gesundheitssystem zu betriebsnotwendigen Fernwartungen (genannt wurden etwa Laborautomaten, aber auch Heizungssteuerungen). Oft lassen sich Probleme dadurch sehr rasch aus der Welt schaffen. Es sind aber zunehmend auch Routinetätigkeiten, die früher vom Personal vor Ort durchgeführt wurden, wie Gerätekalibrierungen, die heute über den Fernwartungszugang gemacht werden. Dadurch entsteht eine neue Abhängigkeit von dieser Datenverbindung (zusätzlich zu etwaigen Sicherheitsbedenken, die bei solchen Zugängen bestehen). Es wurde noch nicht systematisch analysiert, was passiert, wenn diese Systeme mehrere Tage nicht ans Netz können. Kommt es dann zu Sicherheitsabschaltungen, ist ein Offline-Betrieb ohne weiteres machbar, oder muss durch das Personal in der Klinik eingegriffen werden, um den Betrieb sicherstellen zu können? Sollte Letzteres zutreffen, stellt sich auch die Frage nach regelmäßigen Schulungen und Übungen.

Ein derzeit im Versuchsstadium befindliches Projekt, die papierlose Patient:innenübergabe von der Rettung an eine Klinik des Wiener Gesundheitsverbundes, soll den Weg in die Zukunft zeigen und wirft zugleich neue Fragen nach Abhängigkeiten auf Grund von Vernetzungen auf.

Ebenso wird schon jetzt die Kommunikation mit den Rettungsleitstellen zu einem großen Teil über Internetschnittstellen abgewickelt. So werden bspw. Anfahrtssperren in Fällen von überlasteten Notaufnahmen in dieser Art und Weise kommuniziert. Ein Ausweichen auf eine Telefonverbindung (solange diese funktioniert) ist denkbar, wäre aber mit enormen Effizienzeinbußen verbunden, d.h. es könnten nicht mehr so viele Patient:innen versorgt werden, und der Personalaufwand würde sich dramatisch erhöhen. Bei Ausfall des Telefonnetzes wäre in Wien noch ein Rückgriff auf das Landesgrundnetz möglich, als letzte verbleibende Lösung stünde noch der BOS-Funk zur Verfügung. Hierbei wird eingeräumt, dass Schwierigkeiten auftreten könnten, wenn das Personal den Umgang mit den Geräten nicht gewohnt ist, und andererseits nur drei Geräte pro Klinik verfügbar sind.

Ein Ausfall der Anbindung ans Rechenzentrum wäre für die Kliniken fatal. Auch eine Beschränkung auf reine Notfallmedizin wäre so nicht über drei Tage aufrecht zu erhalten.

Es wird auch angenommen, dass der Lagerbestand vor Ort an Verbrauchsmaterial für Akut-Versorgung, Operationen u.dgl. eher für Stunden als für Tage reichen würde, aber sicher nicht für drei oder mehr Tage. Wegen der erfolgten Umstellung auf elektronische Beschaffungsvorgänge, wäre die Versorgung mit diesen Gütern im Schadensfall stark beeinträchtigt.

Grundsätzlich wird die Situation so eingeschätzt, dass der Aufbau eines BCM im Bereich des Wiener Gesundheitsverbundes noch in den Kinderschuhen steckt. 2019 und in den Folgejahren war einiges dazu geplant, das dann durch die Pandemie weit nach hinten verschoben wurde. Ein Pilotprojekt gab es im Bereich Nahrungsmittelversorgung in den Kliniken. Hier scheint es möglich, die Versorgung ohne Lieferungen, Außenkommunikation usw. für zumindest drei Tage zu erbringen.

Auch im Gesundheitssektor wurde wiederholt von allen Befragten festgehalten, dass es sehr wünschenswert wäre, solche Schadensfälle auch üben zu können. Außerdem wäre es wichtig, in der Ausbildung des Personals für die notwendigen Prozesse Alternativen aufzuzeigen, die im Schadensfall funktionieren können.

#### *7.2.2.2 Rettung*

Bei den Rettungs- und Krankentransportdiensten werden die Informationen zum jeweiligen Einsatz über das Mobilfunknetz an die Einsatzfahrzeuge übertragen. In der gleichen Art und Weise funktioniert die Abwicklung der Statusmeldungen über das Mobilfunknetz. Sollte dieses nicht mehr zur Verfügung stehen, wäre das digitale Behördenfunknetz auf Basis des TETRA-Standards die nächste Rückfallebene, zusätzlich wird von Daten- auf Sprachkommunikation umgestellt. Statusmeldungen bei Krankentransporten werden deutlich reduziert, bei Rettungsfahrten werden alle Statusmeldungen aus dokumentarischen Gründen versendet. Formulare für Patiententransporte und Rettungseinsätze sind in jedem Wagen vorhanden.

Das Einsatzleitsystem ist über eigene Leitungen, die von verschiedenen Providern angemietet wurden, mit allen Leitstellen verbunden. Die Applikationsserver laufen redundant, auf mehrere regionale Standorte verteilt, mit Anbindungen zu entfernten Leitzentralen. Im Notfall sind Ausfälle mehrerer Leitstellen verkraftbar, ohne dass es Anrufende merken.

Dokumentationssysteme wie etwa die Tablets der Notärzt:innen würden durch Papier ersetzt, was den Betrieb verlangsamen würde, aber die Kapazitäten für Rettungsfahrten ließen sich auf jeden Fall aufrechterhalten.

Falls die Telefonverbindungen ausfallen, ist die Rettung mehr oder weniger lahmgelegt, weil niemand mehr anrufen kann, um einen Rettungs- oder Krankentransport zu bestellen. Das wäre ein Problem der Erreichbarkeit, aber nicht unbedingt der organisationsinternen Prozesse. Damit könnten über Sicherungen noch die letzten im System gespeicherten Aufträge ausgedruckt und verteilt werden (das kann für Dialyse-Patient:innen Sinn machen, dann trotzdem geholt und ins KH gebracht zu werden). Neue Aufträge könnten aber nur mehr persönlich angenommen und an die vor Ort verfügbaren Einsatzfahrzeuge vergeben werden.

Weitere Probleme können z.B. bei einem Blackout entstehen, wenn es schwierig wird, mit dem Personal zu kommunizieren. Dann müsste improvisiert werden, etwa

um mit dem eingerückten Personal Dienstpläne zu erstellen etc. Bei bestimmten Verbrauchsgütern, die schwer zu beschaffen und nicht in großen Mengen auf Lager sind, wie bspw. Sauerstoff, könnte es zu Engpässen kommen.

### 7.2.3 Informationstechnik und Telekommunikation

#### *7.2.3.1 Mobilfunk*

Internetprovider nehmen eine besondere Rolle unter den Betreibern kritischer Infrastrukturen ein, ebenso wie die weiter oben beschriebenen Energieversorger und Netzbetreiber. Elektrischer Strom und die Kommunikationsnetze gelten als ‚Hauptschlagadern' unserer modernen Gesellschaft, ohne die auch kein Betreiber kritischer Infrastrukturen für längere Zeit auskommen kann. Dementsprechend haben viele Kommunikationsinfrastrukturbetreiber einen für verschiedenste Krisen ausgearbeiteten Notfallplan.

Ein möglicher Ablauf im Fall eines Internetausfalls bei einem beliebigen großen Provider könnte so aussehen: Die Alarmierung des Krisenstabes erfolgt über ein NOC, entsprechend zuvor ausgearbeiteter Szenarien. Die Aufgabenprofile im Krisenstab sind nach der bekannten S1-S6 Kategorisierung der Sachgebiete vorab geregelt. Die Mitglieder des engeren und erweiterten Krisenstabes sind mit Mobiltelefonen ausgestattet, die SIM-Karten eines anderen Providers verwenden. Zusätzlich verfügen sie über Satellitentelefone und BOS-Funkgeräte. Wenn keine dieser Kommunikationsmöglichkeiten zur Verfügung steht, suchen die Krisenstabsmitglieder an verschiedenen Standorten eingerichtete Krisenzentren auf. Diese sind über direkte Standleitungen miteinander verbunden. An welchem Standort der Krisenstab zusammenkommt, ist vorab entschieden.

Bei A1 sind die Krisenzentren und das NOC über herkömmliche 2-Draht-Kupfer-Leitungen mit dem staatlichen Krisenmanagement und zentralen Medien verbunden. Dadurch kann sich der Krisenstab mit anderen Akteuren in der Krise abstimmen (BMI/SKKM, CERT, Medien etc.). Der Krisenstab kann sowohl selbstständig Entscheidungen treffen, als auch den Vorstand des Unternehmens beraten – abhängig davon, wer anwesend ist, und um welche Art von Krise es sich handelt. In manchen Unternehmen ist dafür vorab der Handlungsspielraum für den Krisenstab, auch in finanzieller Hinsicht, abgesteckt.

Im Fall eines Blackouts sind i.d.R. nur die wesentlichen Core-Elemente des Netzwerks dauerhaft notstromversorgt. Die Mobilfunkmasten, als letzte Komponenten Richtung Einzelkund:innen sind für 15-60 Minuten batteriegepuffert. Letztendlich wäre nicht damit zu rechnen, dass sich ein Kommunikationsbetrieb in den gesamten Datennetzen über Notstromaggregate aufrechterhalten ließe.

Ab einer Serviceunterbrechung für mehr als 100.000 Kund:innen für mehr als eine Stunde muss eine verpflichtende Meldung an die RTR erfolgen.

#### *7.2.3.2 Internet*

ACOnet und GovIX laufen auf A1 Glasfaser-Infrastruktur, getrennt vom A1 Produktionsnetz für andere Kund:innen. Das Management erfolgt durch den Zentralen Informatikdienst der Universität Wien. Solange keine physikalische Beschädigung vorliegt, sollten die beiden Netze unbeeinträchtigt von Fehlern im A1-Netz laufen.

WDM-Komponenten funktionieren zunehmend nach offenen Standards, sodass sich Netze mit Geräten unterschiedlicher Hersteller betreiben lassen, was wiederum die Resilienz gegenüber Hardware-Kompromittierung erhöht. Dies steckt allerdings noch in den Kinderschuhen. Selbst wenn die Hardware zusammenspielt, wäre es fraglich, ob die übergeordnete Managementsoftware mit einem so heterogenen Netz umgehen könnte.

Um eine zu starke Zentralisierung in Wien zu verhindern, bekommt das ACOnet auch einen Ausstiegspunkt in Salzburg, was die Resilienz weiter steigern wird.

Für die großen Provider besteht wahrscheinlich keine echte innerösterreichische Alternative zum VIX. Bei einem Ausfall würde der Verkehr vermutlich über Frankfurt, Mailand, Prag usw. laufen. Für mehr Resilienz wäre das auch ein Ansatzpunkt, ebenso wie der (neuerliche) Aufbau eines Staatsgrundnetzes.

Beim Aufbau eines Staatsgrundnetzes wäre jedenfalls zu berücksichtigen, wo sich die physikalischen Schnittpunkte der unterschiedlichen Netze befinden? Aus Kostengründen wäre es empfehlenswert, nicht ein komplett neues Netz aufzubauen, sondern bestehende Netze über Ausweichrouten miteinander zu verbinden.

Die innerbehördliche Kommunikation läuft primär über den GovIX (auf ACOnet-Architektur), hier könnten zukünftig auch KI-Betreiber angeschlossen werden. Eine eigene Namensauflösung wird schon angeboten, damit der Datenverkehr zwischen den Behörden auch ohne externes DNS funktioniert. In Zukunft soll auch die Firma A-Trust angeschlossen werden, um die Zertifikatsverfügbarkeit sicherzustellen. Dadurch ist nicht nur eine von Internetstörungen weitgehend unabhängige innerbehördliche Kommunikation möglich, sondern es kann auch sichergestellt werden, dass der Datenverkehr zwischen unterschiedlichen staatlichen Einrichtungen nicht über Peering Points im Ausland läuft.

Sehr problematisch sei laut Expert:innen in dem Zusammenhang der Trend zu vermehrtem Einsatz von Cloud-Lösungen. Das beträfe sowohl Cloud-Lösungen zur Datenspeicherung, als auch jene, die Rechenkapazität oder andere Services zur Verfügung stellen. Sobald bspw. dynamische Webseiten Inhalte aus einer Cloud nachladen, oder die Videokonferenzlösung über eine Cloud läuft, werden diese im Schadensfall nicht funktionieren, selbst wenn sonst alles über den GovIX läuft.

Probleme könnten sich daraus ergeben, dass immer mehr Organisationen über das Outsourcing von IT-Dienstleistungen firmeninternes Know-How auslagern oder ganz aufgeben. In einer Krise sei es jedoch erforderlich, dass ein kompetentes Team vor Ort ist. Es wäre auch unzureichend, wenn bei einer regionalen Krise in Tirol das Team mit dem nötigen Wissen in Wien zur Verfügung steht. Der Grad der Resilienz würde auch mit der Verteilung von kompetentem Personal steigen. Für den Regelbetrieb kann es zwar wirtschaftlich sinnvoll sein, sich (Personal)Ressourcen zu teilen, aber wenn im Krisenfall alle gleichzeitig auf die geteilte Ressource zugreifen wollen, gäbe es ein Skalierungsproblem. Letztendlich wäre das breit vorhandene geschulte Personal auch ein Standortvorteil für Österreich, wenn sich dieser Standard aufrechterhalten ließe. Deutlich mehr Übungen, sowohl organisationsintern als auch organisationsübergreifend bis hin zu gesamtstaatlichen Großübungen werden dringend empfohlen.

### 7.2.4 Transport und Verkehr

#### *7.2.4.1 Transport-Logistik*

Viele Unternehmen der Logistikbranche nutzen eine sehr engmaschige Kommunikation mit ihren Fahrzeugen, um Steuerungsprozesse zu optimieren. Es werden Statusnachrichten über Sendungen ausgetauscht, neue Aufträge an die Fahrer:innen übermittelt, Routen fürs Navigationssystem zur Verfügung gestellt, und die Positionen der Fahrzeuge erfasst. All das wäre bei einem Internetausfall nicht mehr möglich. Darunter würde vor allem die Effizienz leiden, weil nur noch ein Mal pro Tag, d.h. in der Früh beim Abfertigen der Fahrzeuge, die Route festgelegt werden würde. Informationen zur Sendungsverfolgung, Fahrzeugposition usw. könnten nur offline gesammelt und abends übertragen werden, wenn die Fahrzeuge wieder zurückgekehrt sind. Weiters würden die Schnittstellen zu externen Lieferanten und Kunden ausfallen, die für Berichte, Sendungsaviso, Rechnungsdruck, Statusmeldungen u.dgl.m. verwendet werden.

Im Bereich der Verwaltung von Lagerbeständen oder Containern ist die Abhängigkeit vom Internet oft hoch, wenn das Management-System internetbasiert ist. Beim Ausfall eines derartigen Systems Anfang 2022 in Wien wurde das offensichtlich. Solange die Anbindung ans Internet nicht funktioniert hat, war kein einziger Geschäftsprozess sinnvoll abzuwickeln. Eine Alternative zum Stillstand wäre das manuelle Heraussuchen der benötigten Container bei den Stellflächen. Dann könnte der Kran angewiesen werden, diesen Container zu verladen; er könnte abgefertigt und losgeschickt werden. Neben dem vergleichsweise hohen Zeitaufwand wäre das Hauptproblem, dass nach wenigen derartigen Eingriffen das Stellplatzsystem nicht mehr auf dem aktuellen Stand wäre, und daher auch bei einem Wiederanlaufen des Systems als Erstes das Lager neu sortiert bzw. dokumentiert werden müsste, bevor wieder ein regulärer Betrieb möglich ist. Dieser Wiederaufbau wäre eine herausfordernde Arbeit, die bis zu mehrere Tage in Anspruch nehmen kann. Dementsprechend werden solche Eingriffe nicht vorgenommen, wenn absehbar ist, dass das Problem innerhalb eines Tages behoben werden kann. In diesem Bereich wäre das rechtzeitige Erkennen der Größe eines Ausfalls von entscheidender Bedeutung. Einfacher wäre es, die Ausgabe von Leercontainern durchzuführen. Allerdings müsste hierbei wieder auf Papierdokumentation umgestellt werden.

Zollabfertigungen, die bei großen Frächtern hausintern erledigt wurden, werden derzeit auch über internetbasierte Kommunikation ‚remote' vorgenommen; jedenfalls solange es keinen Grund für eine Nachschau vor Ort gibt. Ohne die digitale Erreichbarkeit dieser Zollstellen würde sich auch diese Abfertigung deutlich verlangsamen.

#### *7.2.4.2 Fahrgastinformationssysteme*

Es werden für viele Transportunternehmen aus dem Bereich ÖV Dienstleistungen erbracht, die fast alle internetabhängig sind, sei es bei der Bereitstellung der Daten oder bei der Ausgabe über Webportale oder Apps, bspw. beim Kauf von Online-Tickets oder Fahrplanauskünften. Die Systeme sind hochverfügbar ausgelegt und auch von den Anbindungen her mehrfach redundant ausgeführt. Dennoch würde ein Anbieter solcher Dienstleistungen den Betrieb vermutlich einstellen, wenn die gesamte Internetanbindung ausfällt. Alternativen zur Fahrplanauskunft, wie früher gedruckte Kursbücher oder Fahrplanhefte, existieren nicht mehr.

Auch alle Angebote, die über zentrale Plattformen disponiert werden, wären von einem Internetausfall ebenfalls betroffen, konkret Anrufsammeltaxis (AST), weil von der Auftragsannahme, über die Übermittlung an die Lenker:innen, bis zur Fahrzeugpositionierung oder anderen Statusmeldungen nichts kommuniziert werden könnte. Funktaxiunternehmen, die noch über eigenen Funk verfügen, wären hier deutlich besser aufgestellt.

Zukünftig wären auch Systeme betroffen, bei denen Tickets nach tatsächlich gefahrener Strecke abgerechnet werden würden und Ähnliches.

#### *7.2.4.3 Bahn*

Durch einen Internetausfall wäre der Fahrbetrieb nicht betroffen, wohl aber die Schnittstellen zu den Kund:innen. Fahrplanauskünfte zu erteilen oder Tickets zu verkaufen, wäre online nicht mehr möglich. Vor Ort, d.h. auf den Bahnhöfen, ist beides auch ohne Internetverbindung durchführbar.

Der Rail Cargo-Bereich würde unter ähnlich drastischen Einschränkungen zu leiden haben, wie zuvor schon für andere Logistikfirmen beschrieben. Es wird mit einer Latenz von 6 bis 8 Stunden gerechnet, bevor es zu größeren Schwierigkeiten im Frachtgeschäft kommt. Laut Expert:innen gäbe es nach zwölf Stunden keinen internationalen Cargo-Verkehr mehr, nach ca. zwei Tagen würde auch der nationale Frachtverkehr vollständig zum Erliegen kommen. Neben der Frachtabwicklung wären vor allem Systeme für Statusupdates und das Tracking der Waggons betroffen.

Der Bereich der Bahn-Infrastruktur kommt aus heutiger Sicht einige Stunden bis Tage ohne Internetanbindung aus. Es gäbe natürlich Einschränkungen, v.a. was die Kommunikation mit Partnerfirmen betrifft, aber nicht in dem Ausmaß, dass ein Notfall oder eine Krise daraus entstehen würde. Hier wäre es zunächst die Konzernzentrale, die den Krisenstab einberufen würde, um die Betroffenheit vom Ausfall und weitere Schritte in den unterschiedlichen Teilbereichen auszuloten. Ein regelmäßiger Kontakt zum CERT ist ebenfalls vorhanden.

Die Netze, die für den Fahrbetrieb nötig sind, etwa zur Steuerung von Weichen, Signalen u.dgl., sind vollkommen getrennt von anderen Netzen und nicht mit dem Internet verbunden. Dies kann sich in den kommenden Jahren jedoch ändern. Bei einem Ausfall wäre es z.T. noch möglich auf andere Medien zurückzugreifen. Bis zu einer Woche im Voraus werden die Informationen für Triebfahrzeugführer:innen zusammengestellt, die Auskunft darüber geben, wo auf der Strecke Baustellen, Geschwindigkeitsbeschränkungen oder andere Beeinträchtigungen zu erwarten sind. Wäre das nicht mehr digital zu übermitteln, könnte es in ausgedruckter Form mitgegeben werden. Wenn diese Informationen jedoch nicht mehr in das System gelangten, wäre auch hier die Frage für den Krisenstab, wie mit diesem Sicherheitsproblem dann umzugehen wäre.

Die Strom-Eigenproduktion der Bahn würde nicht ausreichen, um den gesamten Betrieb zu versorgen. Ein sehr eingeschränkter Zugsverkehr (auch mit Diesellokomotiven) wäre möglich. Der Rest des im Normalbetriebs benötigten Stroms wird normalerweise am Strommarkt eingekauft. Wenn dieser, wie in Abschnitt 7.2.1 beschrieben, zusammenbräche, gäbe es Verträge mit großen EVUs, die hier einspringen

könnten. Allerdings ist unklar, ob es noch möglich ist, bei einem Kommunikationsausfall die Differenz zwischen Eigenproduktion und Verbrauch im Normalbetrieb zu erhalten.

### 7.2.5 Medien und Kultur

Der ORF fungiert als staatliche Rundfunkanstalt als wichtigstes Medium der Krisenkommunikation. Fast die gesamte Bevölkerung wird in einem derartigen Fall ihre Informationen über Kanäle des ORF beziehen. Sogar im Falle eines Blackouts ist anzunehmen, dass batteriebetriebene Radioempfänger (v.a. Autoradios) der primäre Kommunikationskanal zur Bevölkerung sein werden.

Das Service, das beim ORF durch einen Internetausfall unmittelbar betroffen wäre, sind die Online-Angebote über orf.at. Der Versorgungsauftrag umfasst nur die Distribution über terrestrische Kanäle, nicht aber die Online-Präsenz.

In weiterer Folge kann es zu Beeinträchtigungen der Produktionsprozesse kommen, weil viele Nachrichtenquellen nicht mehr verfügbar sind. Um dem zu begegnen, ist der ORF in vielen Bereichen redundant und/oder autark aufgestellt. So sind etwa alle Landesstudios redundant über LWL angebunden. Es gibt vorbereitetes Equipment (sog. Live-U-Rucksäcke), das alles für eine Übertragung über das Mobilfunknetz bereithält. Mit einer gewissen Vorlaufzeit können Sendewägen vor Ort bereitgestellt werden. An bestimmten Orten sind für die Krisenkommunikation vorbereitete Studioräume, die ebenfalls über Glasfaser mit dem ORF-Zentrum verbunden sind. Auch zur APA und zu A1 gibt es eine internetunabhängige Verbindung. Das terrestrische Fernsehprogramm (inkl. Teletext), sowie Ö3 über UKW sind bundesweit zu empfangen, zusätzlich sind regional lokale Radiostationen verfügbar.

### 7.2.6 Wasser

Die Wasserversorgung scheint bei einem Internetausfall nicht gefährdet zu sein. Das Management wäre eventuell schwieriger, weil es Zähler und Messstationen gibt, die über das Internet oder das Mobilfunknetz ihre Daten übermitteln. Die Erfassung dieser Daten ist jedoch nicht zeitkritisch. Ein:e Mitarbeiter:in des Unternehmens könnte auch in regelmäßigen Abständen vor Ort Nachschau halten, um Pegelstände zu kontrollieren oder andere Messwerte abzulesen.

Entweder sind im Regelbetrieb keine Daten verfügbar, die über eine Internetanbindung von extern angeliefert würden und für den Betrieb relevant wären; oder es sind nur Daten, die nicht unmittelbar benötigt werden. So werden bei manchen Anbietern bspw. Zählerstände über eine Cloudlösung abgeglichen, sie könnten aber auch telefonisch oder auf anderem Weg übermittelt werden. Ebenso wäre im Schadensfall kein tagesaktueller GIS-Plan der Leitungen, Hausanschlüsse etc. vorhanden, allerdings werden zumindest wöchentlich Offline-Backups erstellt.

Wartungsintervalle und Lieferverträge sind so konzipiert, dass ein Internetausfall von einigen Tagen kein Problem darstellen würde. Füllstandsüberprüfungen bei bspw. $CO_2$-Behältern erfolgen im Regelbetrieb automatisiert, begleitet von einer regelmäßigen Kontrolle durch Lieferanten. Im Schadensfall wäre die Ablesung der Mess-

werte, vergleichbar mit den Werten zu Wasserpegeln, nur vor Ort möglich. Die Überprüfungen sind jedoch so häufig, dass es durch den Schadensfall zu keiner Veränderung der eingespielten Prozesse kommen müsste. Bei kleineren Betreibern mit outgesourcter IT könnte es schwierig werden, wenn es keine Vereinbarung mit den externen Spezialisten über deren Support-Prioritäten gibt. (Und falls es diese gibt, ist die praktische Umsetzung im Krisenfalls dennoch fraglich.)

Alarmmeldungen würden bei einem Ausfall der Mobilfunkprovider nicht mehr über Mobiltelefone erfolgen. In dem Fall wären Zentralen oder Leitstellen 24/7 zu besetzen, um über das Konzernnetz eintreffende Meldungen bearbeiten zu können. Alternative Kommunikationswege gehen von Betriebsfunk bis zur Anbindung an BOS-Systeme, teilweise stehen für die Information der Bevölkerung Autos mit Sprechanlagen zur Verfügung.

Wirtschaftliche Probleme sind nicht zu erwarten, da Haushaltskunden einen geringeren Anteil am Umsatz ausmachen als Großkunden, die oft ohnedies nur quartalsweise abgerechnet werden. Eventuell gäbe es Zeitverzögerungen bei der Umsetzung der Abbuchungsaufträge durch die Banken oder der Datenübermittlung an externe Dienstleister zum Rechnungsdruck und -versand.

Wunsch nach internetunabhängiger Vernetzung: Es wird dringend ein unabhängiges Kommunikationsnetz gewünscht, auch aus einer Skepsis gegenüber dem digitalen Behördenfunk in Bezug auf dessen Krisenfestigkeit. Als beispielhafte Lösung wird etwa der Analogfunk vorgeschlagen. Zusätzlich sollte der Informationsaustausch im Krisenfall mit den Behörden auch geübt werden können.

### 7.2.7 Finanz- und Versicherungswesen

Die Zahlungsverkehrssysteme wären von einem Internetausfall deutlich stärker betroffen als andere Branchen. Die Expert:innen haben klar dargestellt, dass sich Bankomaten leeren würden und nicht wieder befüllt werden könnten. Die meisten Filialen blieben teils geschlossen – nicht nur wegen der Unmöglichkeit, die Zahlungsdaten im Schadensfall zu übermitteln, sondern vor allem deshalb, weil die Sicherheit der Angestellten nicht mehr zu gewährleisten wäre. Es gibt jedoch bei jeder Bank auch einzelne Filialen, die über ‚leased lines' angebunden sind und einen Kundenverkehr ermöglichen würden. Ähnliche Verbindungen gibt es auch zu manchen Börsen. Hier sind die Leitungsparameter allerdings von Fall zu Fall unterschiedlich und es ist unklar, welche Komponenten am Übertragungsweg noch nötig sind, wer diese wartet und wie sie bspw. mit Notstrom versorgt werden. Vor dem Eintritt so eines Schadensfalls erscheint es daher kaum abschätzbar, was dann letztendlich funktionieren wird, die Erwartungen sind aber gedämpft.

Demzufolge würde der internationale Zahlungsverkehr mit österreichischen Banken wahrscheinlich zusammenbrechen. Viele Systeme der heimischen Banken wurden in Cloud-Rechenzentren ausgelagert, zwar mit guten SLAs, aber diese würden im angedachten Schadensfall nicht weiterhelfen. Dadurch könnte es auch zu Problemen für die staatliche Verwaltung kommen, wenn etwa internationale Zahlungsverpflichtungen nicht mehr erfüllt werden könnten. Für einen Notbetrieb, um bspw. in

zentralen, städtischen Filialen Bargeld ausgeben zu können, wäre eine enge Zusammenarbeit mit der Nationalbank erforderlich. Hier gab es aber in der Vergangenheit noch keine Pläne für ein gemeinsames Vorgehen.

Bankomat- und Point-of-Sale-Kassen würden nicht mehr funktionieren, Bargeld wäre also wichtig für die Bevölkerung, um Alltagsgeschäfte weiter durchführen zu können. Diese Fragen müssten aber auch in Zusammenarbeit mit den Versorgungsdienstleistern wie Spar, REWE usw. geklärt werden, weil auch noch unklar ist, ob diese überhaupt gegen Bargeld verkaufen könnten/würden. So wurden bspw. nach einem Cyber-Angriff, der auch die Kassensysteme einer schwedischen Supermarktkette betraf, die Filialen dieser Kette geschlossen. (Wolff 2021)

### 7.2.8 Lebensmittellogistik

Organisationen in der Lebensmittellogistik sind Drehscheiben zwischen enorm vielen einzelnen Stellen. Auf der einen Seite sind alle Lieferanten, i.d.R. Produzenten oder deren Zwischenhändler. Wenn man sich kurz in Erinnerung ruft, wie groß das Sortiment einer Supermarktkette heute ist, in all den unterschiedlichen Produktsparten, wird schnell klar, dass schon auf der Seite der Lieferanten sehr viele Betriebe und ihre Ansprechpartner:innen zu organisieren sind, im allgemeinen weit über Tausend. Auf der anderen Seite sind die Supermarktketten und deren Filialen, die beliefert werden. Die Zahl geht oft ebenfalls in die Tausenden. Dazwischen ist die Firma selbst, der Lebensmittellogistikanbieter, der ab einer bestimmten Größe auch über einige Niederlassungen verfügt. Kommunikation und Datenaustausch, Verwaltung und Organisation sind in diesem Setting essentiell. Der Ausfall der Daten- und eventuell auch Sprachkommunikation wäre entsprechend schwierig.

Das Geschäft ist von einem sehr hohen Warendurchsatz (in etwa 20.000 Artikel pro Tag bei den großen Anbietern) bei geringen Margen geprägt. Dadurch sind wirtschaftlich keine großen Spielräume für Ausfälle oder Verzögerungen. Speziell problematisch wären Verzögerungen bei den Lebensmitteln aus dem Frischebereich, besonders jenen, die einer durchgängigen Kühlkette bedürfen. Die Lager arbeiten hier i.d.R. ohne Pufferung, um die Lebensmittel, die eingelagert werden, noch am selben Tag in die Supermarktfilialen und damit zum Kunden zu bringen. Im Bereich der Trockenprodukte ist der Lagerstand für mehr als 10 Tage ausreichend bei normalem Verbrauch. In Zeiten von Hamsterkäufen sicher kürzer.

Um in dieser Situation einen möglichst reibungslosen Betrieb zu gewährleisten, sind wichtige Datenverbindungen oft über alternative Kanäle wie Richtfunkstrecken o.ä. angebunden. Zusätzlich gibt es jedoch auch Infrastrukturen, die nicht in der Einflusssphäre der Logistikfirma liegen und für den täglichen Betrieb benötigt werden. Die Abwicklung mit den Lieferanten erfolgt bspw. über Plattformen, die Bestellungen u.dgl. über Nachrichten im Electronic-Data-Interchange (EDI)-Format erhalten. Selbst wenn es den Logistikfirmen gelänge, in einer Krise die Kommunikation mit so einer Plattform sicherzustellen, und diese ihren Betrieb aufrechterhalten kann, wäre immer noch die Frage, ob Lieferanten das ebenfalls könnten, da andernfalls keine strukturierte Kommunikation mit diesen erfolgen kann.

Durch diese Kommunikationsstruktur und die hohe Anzahl der zu verarbeitenden Artikel ist ein Ausweichen auf mündlich per Telefon durchgegebene Bestellungen o.ä.

nicht durchführbar. Was im Notfall noch zu schaffen wäre, ist die Auslieferung der im Lager verfügbaren Artikel an die Supermarktfilialen nach einem vorher festgelegten Schlüssel (nicht nach tatsächlichem Bedarf).

Als weitere Herausforderung wird auch gesehen, dass die meisten Menschen in den Supermärkten bargeldlos zahlen. In der Situation eines Internetausfalls ist das dann nicht mehr möglich. Zugleich ist es zu spät, um noch Bargeld abzuheben. Diese Situation könne zu einem Problem in den Filialen führen, wenn Lebensmittel zu Hause gebraucht werden, aber niemand mehr Bargeld hat, um diese zu bezahlen.

Eine andere Schwierigkeit besteht darin, dass die Lebensmittellogistik in Österreich von sehr großen Anbietern durchgeführt wird, die zu groß sind, um in der Krise von einem anderen Anbieter mitbetreut zu werden. Es könnte ein Konzept zur Ausfallssicherheit ja vorsehen, dass die Logistikfirmen unterschiedliche Provider nutzen und dadurch eine gewisse Fehlertoleranz erreichen. im Fall der Lebensmittellogistik in Österreich würde das jedoch nicht helfen, da keiner der Anbieter das Geschäft eines anderen – auch nur kurzfristig – übernehmen könnte.

### 7.2.9 Staat und Öffentliche Verwaltung

#### *7.2.9.1 BMLV*

Das BMLV betreibt die meisten benötigten IT-Services selbst, in vier verschiedenen Sparten (Luftraumüberwachung, Abwehramt, Nachrichtendienst und IT- und Cybersicherheitszentrum). Kritische Dienste werden zu 100% in-house erbracht, dadurch ergeben sich keine kurz- oder mittelfristigen Abhängigkeiten von externen Anbietern. Langfristig besteht durch die Beschaffung von Komponenten zwar eine Technologieabhängigkeit, diese würde aber bei einem Internetausfall keine unmittelbare Rolle spielen. Ein Ausfall internetbasierter Dienste würde das BMLV in seinem Betrieb nicht substanziell beeinträchtigen.

Schnittstellen, wie z.B. von der militärischen Luftraumüberwachung zur Austro-Control, gibt es, sie sind jedoch vom Internet unabhängig zu betreiben. Neben der Verbindung zur Austro-Control sind v.a. eine Schnittstelle zu EADS, die für den Betrieb der Eurofighter erforderlich ist, und eine Verbindung zum BRZ Portal Austria (PAT), für den Betrieb wichtig. Weiters gibt es Verbindungen zur Präsidentschaftskanzlei und zu den Auslandskontingenten. Diese sind redundant und über unterschiedliche Kanäle realisiert. Zum BMI und anderen Kontaktstellen gibt es Verbindungsoffiziere.

Enge Kontakte bestehen BMLV-intern zwischen den vier IT-Dienstleistern, aber auch zum CERT. Die Kommunikation erfolgt den Notwendigkeiten entsprechend offen und rasch, unabhängig von andernfalls erforderlichen Dienstwegen.

#### *7.2.9.2 Bundesrechenzentrum (BRZ)*

Das BRZ hat seinen Betrieb und damit die Dienstleistungen für die Kunden, die hauptsächlich aus der österreichischen Verwaltung kommen), je nach Kundenanforderungen bis zu hochverfügbar ausgelegt. Es wird hier den Anforderungen aus dem Standard ISO 22301 gefolgt.

Das BRZ ist mehrfach redundant über unterschiedliche Provider angebunden. Ein Ausfall der Konnektivität auf einer Leitung wäre daher noch kein substanzielles Problem, die wesentlichen Bereiche wären alle noch versorgt/erreichbar. Wie Kunden mit

der für sie notwendigen Sicherheit auf die Angebote des BRZ zugreifen, ist allerdings in deren Geschäftsprozessen geregelt. Das BRZ kann hier insofern unterstützen, als am Standort des BRZ Arbeitsplätze für Kunden verfügbar sind, um auf deren Datenverarbeitungen zuzugreifen.

Grundsätzlich ist auch das BRZ an den BOS-Funk angeschlossen. Durch die räumliche Nähe zu zentralen Verwaltungseinheiten, dem CERT oder dem SKKM im BMI, ist eine Kommunikation aber auch jederzeit persönlich möglich.

Das BRZ wurde bei der letzten Beurteilung nach NIS nicht als Betreiber wesentlicher Dienste eingestuft. Das wird sich mit NIS 2.0 vermutlich ändern.

## 7.3 Sektorübergreifende Ergebnisse

Neben den sektoral aufgeschlüsselten Ergebnissen aus den Interviews in Kapitel 7.2, finden sich im Folgenden Ergebnisse, die mehrere oder alle Sektoren betreffen.

Große Probleme würden sicherlich dort entstehen, wo die IT an Externe ausgelagert wurde. Das betrifft nicht nur Rechenzentrumskapazitäten, die in eine Cloud verschoben wurden, sondern auch die Fälle, wo Personal und/oder Know-How nicht mehr innerhalb der Organisation verfügbar sind. Die Zusammenarbeit wäre im Schadensfall schwierig bis unmöglich, und es ist ungewiss, ob man damit rechnen könnte, dass die Dienstleister vor Ort tätig werden (können). In einer Situation, die wahrscheinlich als ‚höhere Gewalt' eingestuft werden würde, in der SLAs unter Umständen nicht mehr gelten, könnte man sich nicht darauf verlassen, dass die erforderlichen Ressourcen zur Verfügung gestellt werden würden, womit es auch zum Ausfall interner IT-Leistungen und darauf basierender Geschäftsprozesse kommen könnte.

Grundsätzlich wäre ein Aufbau von Personalressourcen in Österreich wünschenswert, die über fundiertes technisches Wissen und Verständnis verfügen. Damit wäre jede Krise mit IT-Beteiligung (was auf viele vernetzte Krisen zutreffen würde), wodurch auch immer sie ausgelöst wird, leichter zu bewältigen. Neben den beim BMI und BMLV angesiedelten Gruppen, die in so einer Situation eingreifen könnten, bräuchte es vielleicht auch eine Eingreiftruppe auf Abruf, vergleichbar mit einer Miliz-Einheit oder der Freiwilligen Feuerwehr. Zum aktuellen Zeitpunkt ist aber noch unklar, wie sich diese zusammensetzen könnte und von welcher Stelle eine Koordination erfolgen könnte.

Schwierigkeiten im Bestellwesen und der Just-in-Time-Logistik wurden von praktisch allen Interviewpartner:innen vermutet und von den Expert:innen aus dem Logistiksektor konkret angesprochen. Dies würde in weiterer Folge Betriebe fast aller Sektoren betreffen.

Großflächige Ausfälle sind auch im Bereich der Sicherheitstechnik zu erwarten. Videoüberwachungssysteme, die die Bilder über gesicherte Internetverbindungen bereitstellen und die meisten Alarmübertragungssysteme (TUS-Anbindungen) zu Polizei und Feuerwehr (Brandmelder) hätten keine Verbindung mehr. Auch remote gesteuerte Gebäudetechnik könnte nur noch vor Ort konfiguriert werden.

Dringend gewünscht sind Übungen zum Thema Internetausfall. Das Durchspielen der Maßnahmen zur Krisenbewältigung mit allen relevanten Akteuren wird von allen Seiten befürwortet und z.T. vehement eingefordert.

Im Bereich der Ausbildung wurden Lücken identifiziert, die es nach Meinung der Interviewpartner:innen rasch zu schließen gilt. Dabei geht es oft um Fähigkeiten aus der Zeit vor der hochverfügbaren Vernetzung via Internet, die insbesondere jüngeren Mitarbeiter:innen fehlen. In den Interviews wurden Beispiele gebracht, in denen ältere Mitarbeiter:innen bei einem Computerausfall sofort auf Papier und Bleistift auswichen. Sie wüssten auch noch, wie die entsprechenden Formulare früher ausgesehen hätten und verfügten über ausreichende praktische Erfahrung, sodass etwa eine Nacherfassung der Daten problemlos möglich war. Ist das nur ein Rückgriff auf Altbewährtes, das Jüngere nicht kennen? Sind solche altbewährten Strategien auch als Workaround in einer derartigen Krise die beste Handlungsoption? Ist die geäußerte Kritik lediglich das Symptom eines Generationskonflikts? Jedenfalls war auffallend, dass jüngere Interviewpartner:innen solche Erfahrungen nicht erwähnten. Zur Frage, wie die jüngere Generation mit derartigen Vorfällen umgeht, dürfte also noch weiterer Forschungsbedarf bestehen.

Unmittelbar und massiv betroffen wäre der Bankensektor. Vermutlich wäre jede Art von Zahlungsverkehr unmöglich (jedenfalls ist nicht vorhersehbar, welche Prozesse dann noch funktionieren). Eine Zusammenarbeit zwischen den Banken und der Nationalbank (bzw. deren Tochtergesellschaft Geldservice Austria (GSA)) kam trotz diesbezüglicher Überlegungen im Zuge der Planungen für die Situation nach einem Blackout noch nicht zustande. Diese wäre wohl erforderlich, um die Frage zu klären, wie und unter welchen Bedingungen Bargeld ausgegeben werden könnte, um eine rudimentäre Warenwirtschaft aufrecht erhalten zu können.

Durch den Ausfall von Bankomat- und Point-of-Sale-Kassen, sowie vermutlich der meisten elektronischen Kassensysteme mit DWH-Anbindung, ist jedenfalls noch zu klären, wie Lebensmittelversorger mit so einer Situation umgehen würden.

Ebenfalls starke Einschränkungen, die die meisten anderen Branchen beträfen, wären im Transportsektor zu erwarten. Dort kämen diese vielleicht nicht einem Totalausfall gleich, aber die Abfertigungsgeschwindigkeit würde deutlich absinken, wodurch es letztendlich bei zahlreichen Waren zu Lieferengpässen kommen könnte.

In vielen Organisationen werden Alarmierungen über SMS und/oder App durchgeführt. Beim Ausfall der Mobilfunkprovider oder von deren Netzwerken, würde das nicht mehr funktionieren. Die Betriebe wären darauf angewiesen, dass schon im Vorfeld geklärt wurde, wer in so einem Fall an welchem Standort zum Dienst zu erscheinen hätte. Die Mitarbeiter:innen müssten im Vorfeld auf so einen Fall vorbereitet werden und im konkreten Anlassfall die Lage rechtzeitig und korrekt erfassen. Landesweite Stromausfälle sind relativ offensichtlich, aber es ist fraglich, ob Art und Ausmaß eines großen Internetausfalls ebenso schnell erfassbar wären. Zusätzlich ist davon auszugehen, dass sich viele Mitarbeiter:innen in erster Linie um die Sicherheit ihrer Familie kümmern und daher nicht zum Dienst erscheinen würden. Dieses Risiko wäre bereits bei der Planung der einzelnen Aufgabenbereiche bzw. beim Aufbau einer Notfallorganisation zu bedenken. Ein weiteres Problem dieser bislang unstrittigen Vorgehensweise wäre das zeitliche Zusammentreffen mit einer weiteren Krise,

z.B. mit der aktuellen Pandemielage. Ist es erstrebenswert, wenn sich alle für die Lösung eines Problems nötigen Mitarbeitenden eines Konzerns zentral an einem Ort, z.B. einem Krisenzentrum, einfinden? In den vergangenen Monaten, unter dem Eindruck hoher Ansteckungsgefahren wäre das kein wünschenswertes Szenario gewesen. Was müsste in der Vorbereitung auf solche Situationen geändert oder ergänzt werden – z.B. FFP2-Masken am Eingang verteilen, Abstand vorsehen, Lagezentren nur in gut zu belüftenden Räumen einrichten…?

Auch ein indirektes Zusammentreffen mehrerer krisenhafter Situationen sollte berücksichtigt werden. Ein Internetausfall wäre nicht nur ein technisches, organisatorisches oder psychologisches Problem, sondern könnte sich auch zu einem finanziellen Problem auswachsen. Dies kann in oder nach einer Krise, die – wie die aktuelle Pandemie oder die ebenfalls aktuellen Lieferkettenprobleme - ebenfalls große finanzielle Belastungen für viele Betriebe mit sich gebracht hat, zu langfristigen negativen Entwicklungen führen. Wenn alle finanziellen Puffer aufgebraucht sind, sei es auf staatlicher, privatwirtschaftlicher oder individueller Ebene, könnte eine weitere, auch finanziell belastende Situation das System zum Kippen bringen.

Eine andere Erfahrung aus der Pandemie ist der große Sprung in der Digitalisierung. Viele Arbeitsprozesse, von Besprechungen über Vorlesungen bis hin zum Unterricht, wurden auf Videokonferenzlösungen umgestellt. Homeoffice wurde in vielen Bereichen zur Regel statt zur Ausnahme. Was davon wird bleiben und eine Neuplanung bezüglich Verfügbarkeiten nötig machen?

Meldungen, die für bestimmte Sektoren vorgesehen sind, bspw. an die RTR, die FMA oder gemäß des NIS-Gesetzes, müssen z.T. zeitnah erfolgen, wobei noch unklar zu sein scheint, über welche Kommunikationswege das dann passieren soll. Was ist hier in einer Krise noch erforderlich und wie kann das geleistet werden?

Insgesamt lässt sich erkennen, dass die Arbeiten zur Vorbereitung auf einen Blackout und andere Krisen Früchte tragen und Synergiepotenziale bestehen, um auch die Vorbereitungen auf einen Internetausfall zu unterstützen. Generell ist die Ausfallsicherheit kritischer Systeme vermutlich deutlich höher als noch vor einigen Jahren. Gleichzeitig hat sich die Entwicklung fortgesetzt, Effizienz zu steigern und aus ökonomischen Gründen Puffer im Gesamtsystem zu reduzieren. Es werden einerseits Redundanzen abgebaut und gleichzeitig Infrastrukturen zusammengelegt, die früher in getrennten Netzen betrieben wurden, wodurch sich eine höhere Vulnerabilität ergibt.

Nach einem Internetausfall ist eine komplexe Situation mit hoher Dynamik und vielen Unbekannten zu erwarten. Jede Handlung in diesem aus dem Gleichgewicht geratenen System beeinflusst den weiteren Verlauf. Angesichts der möglichen Ursachen, abgesehen von einem Blackout, wird klar, dass sich vieles erst in der Krise herausstellen wird, was sich davor nicht letztgültig beantworten lässt. Aus diesen Gründen dürfte es vorteilhaft sein, sich auf die Krise vorzubereiten, indem die Kapazitäten zur Bewältigung erhöht werden. Durch bessere Ausbildungen, regelmäßig eingeübte Abläufe, notwendige technische Ausrüstung und eine große Anzahl an kompetentem Personal erhöht sich die Problemlösungskapazität und die Fähigkeit zur Improvisation. Es wird in einer Krise helfen, schon zuvor Netzwerke gebildet zu haben und Kommunikationswege offen zu halten. Zudem wird es notwendig sein, sich auf eine

Situation vorzubereiten, in der Entscheidungen unter unsicheren Bedingungen getroffen werden müssen. Auf Basis von Erfahrungen, Übungen, Plänen usw. können die einzelnen Akteure im Krisenfall flexibel und agil reagieren, um unvorhergesehene Herausforderungen zu bewältigen.

Bei sehr vielen Unbekannten ist es schwierig, mehr als einen Schritt vorauszudenken. Dennoch können vorbereitende Überlegungen, z.B. in Form sektorenübergreifender Workshops, zur Bewusstseinsbildung beitragen, neue Kontakte herstellen und Anstöße für zukünftige Planungen geben. In den ersten Stunden nach dem Eintritt eines solchen Schadensfalls ist ‚lediglich' der Internetausfall, im Zuge dessen allerdings eventuell auch ein kompletter Kommunikationsausfall zu meistern. Im weiteren Zeitverlauf müssten jedoch alle Sektoren auch mit den Problemen in den anderen Sektoren bzw. in der Gesellschaft allgemein zurechtkommen. So wäre etwa die Steuerung des Stromnetzes eine massive Herausforderung, die sich durch unvorhergesehene Verhaltensweisen der Bevölkerung noch weiter verschärfen könnte. Würde weniger Strom verbraucht, weil viele mit dem Internet verbundene Geräte nicht mehr benutzt werden würden? Oder würde mehr oder zu anderen Zeiten Strom verbraucht werden, weil viele Menschen daheim sind, im Winter bspw. durchgeheizt wird, oder Haushaltsgeräte zu anderen Zeiten laufen? Was ändert sich für KI-Betreiber, wenn ihr Personal keine Lebensmittel zahlen/bekommen kann? Welchen Stellenwert hat die Erfüllung beruflicher Aufgaben, wenn die Situation privat, für die eigene Familie, als existenzbedrohend empfunden wird?

Daneben gibt es natürlich auch technische Maßnahmen, die sich präventiv ergreifen lassen. Oft gewünscht wurde in diesem Zusammenhang der neuerliche Aufbau eines Staatsgrundnetzes. Von vielen Seiten wurde im Zuge der Gespräche darauf hingewiesen, dass die Überlegungen zur (Wieder)Errichtung eines Staatsgrundnetzes jedenfalls befürwortet werden würden. Ein anderer Vorschlag, der diesbezüglich nur einen Teilbereich abdeckte, aber leichter umzusetzen wäre, bestünde darin, an wichtigen Verkehrsknotenpunkten (Tankstellen, Rastplätze usw.) ausfallsichere Münztelefone zu betreiben.

Aber auch die Fragen, wie Systeme offline, d.h. im Inselbetrieb, notdürftig funktionieren könnten, oder wo man als Betreiber kritischer Infrastrukturen überhaupt Ressourcen auslagern sollte, müssten in diesem Zusammenhang beantwortet werden. Die Eingriffsmöglichkeiten des Staates sind hier natürlich beschränkt, aber in einer engen Abstimmung zwischen Verwaltung und KI-Betreibern ließen sich an manchen Stellen vielleicht bessere Lösungen finden als derzeit vorhanden sind.

Nicht vernachlässigt werden darf hier auch der Aspekt der Einbindung der Bevölkerung. Wie kann eine gute, positiv bestärkende, transparente Krisenkommunikation aussehen? In den Interviews wurde auch erwähnt, dass es hierzu hilfreich sein kann, sich schon im Vorfeld zu überlegen, welche Aufgaben in der Krise zu bewältigen sein werden, damit hilfsbereites Personal mit Aufgaben betraut werden kann, die mit den jeweiligen Fähigkeiten bewältigbar sind. Ein Schlüsselfaktor in der Krisenbewältigung ist daher, wie man die Menschen mit den entsprechenden Kompetenzen an den richtigen Stellen einsetzt, damit die Gesellschaft von deren Kompetenzen profitieren kann, und die Helfenden, indem sie fordernde, aber bewältigbare Aufgaben haben, einen positiven Beitrag zur Bewältigung der Krise leisten können.

# 8 Offene Fragen

Ein sehr breit aufgestelltes Forschungsprojekt wie das in diesem Bericht beschriebene, das erstmalig die Grundlagen für eine intensive Bearbeitung des Themas schafft, kann nicht in jedem Punkt in die Tiefe gehen. Während der Arbeit am vorliegenden Thema ergaben sich jedoch Fragen, die schon an potenzielle Folgeprojekte weitergegeben werden können, und die eine sinnvolle Ergänzung und Vertiefung der Arbeiten in ISIDOR darstellen würden. Das Projektteam hat sich daher dazu entschlossen, mit diesen offenen Punkten transparent umzugehen. Dieses Kapitel fasst die Fragen zusammen, um aufzuzeigen, wo es noch Forschungsbedarf gibt, damit den handelnden Akteur:innen nicht nur das Wissen, sondern auch das Nicht-Wissen auf dem Gebiet vermittelt werden kann.

## 8.1 Psychologische Aspekte eines Internetausfalls

- Wie funktionieren bspw. Trafiken und andere, weniger kritische Bereiche, die für einzelne Konsument:innen dennoch von großer Wichtigkeit sein können? Gibt es psychologische Effekte in der Krise, nicht nur auf individueller, sondern auch auf gesellschaftlicher Ebene, die bspw. durch die vorhersehbaren Unsicherheiten in der Bevölkerung hervorgerufen werden. Muss mit einem Bank Run, Plünderungen bei Mangel in einzelnen Produktbereichen (z.B. Hygieneartikel) gerechnet werden? Ist die Versorgung mit legalen oder illegalen Suchtmitteln von einem Internetausfall betroffen?
- Psychologische Folgen, ebenfalls individuell und gesellschaftlich: Wie verändert eine Krise Empfinden, Denken und Handeln? Wie verändern die beschriebenen Konsequenzen (Ausfall von Diensten, Kommunikationsmöglichkeiten, verlangsamte Logistik von erwünschten oder benötigten Gütern) das Sicherheitsgefühl? Was macht das mit einer Gesellschaft? Kann man das auch in Bezug auf die Dauer einer Krise beschreiben?

## 8.2 Digitale Souveränität

- Welche KI-Betreiber sind mehrheitlich in ausländischem Besitz? Wie ist die Risikostreuung in Bezug auf mögliche politische Einflussnahme? Müssten manche Infrastrukturen wieder in österreichische Hand, oder gar verstaatlicht werden?

## 8.3 Technik

- Inwiefern sind Systeme der Verkehrstelematik von Internetverbindungen abhängig?
- Wie zahlt der Staat Österreich, wenn alle österreichischen Banken keinen Internetzugang mehr haben? Wäre es noch möglich (oder überhaupt noch wichtig), internationalen Zahlungsverpflichtungen nachzukommen? Ab welchem Zeitraum wäre es ein Problem, wenn Österreich länger technisch zahlungsunfähig ist?

- Welche Technologien werden zukünftig auf der Verfügbarkeit einer Internetverbindung oder einer Vernetzung über Mobilfunk aufbauen? Wie sieht es mit Elektro-Mobilität aus, selbstfahrenden Autos, Lieferdrohnen, Gebäudesteuerungen, Smart Homes usw.? Wird man in den kommenden Jahrzehnten nicht mehr mit dem Auto oder Bus fahren können, wenn ein weitreichender Ausfall des Internets eine bestimmte Zeitspanne überschritten hat? Was ist alles im Bereich IoT mit 5G- oder 6G-Unterstützung geplant?

## 8.4 Juristische Fragestellungen

- Gibt es laut NIS-Gesetz o.a. Meldepflichten? Auf welchem Weg haben diese zu erfolgen? Hier fehlt eine Abklärung zur Differenz (und Relevanz) zwischen Regel- und Notbetrieb.
- Bei allen Befragten herrscht Einigkeit darüber, dass so ein Ausfall jedenfalls als höhere Gewalt zu beurteilen wäre, womit es vermeintlich konsequenzenlos bliebe, wenn etwaige SLAs (als Lieferant oder Leistungsempfänger) nicht eingehalten würden. Für eine Anerkennung als höhere Gewalt bestehen jedoch gewisse Voraussetzungen. Von der Beurteilung dieser Frage hängen auch etwaige Haftungsfragen und Schadensersatzansprüche ab. (Befreit ein Zustand höherer Gewalt grundsätzlich von der Leistungserbringung, oder müsste man liefern, so lange es ginge, und die höhere Gewalt entschuldigt nur die daraus resultierende Unmöglichkeit der Leistungserbringung?)
  Dabei ist auch die Frage offen, ob die Antwort darauf, ob es sich nun um höhere Gewalt handelte oder nicht, realiter überhaupt von Bedeutung sein wird. Ob eine Leistungserbringung zu Recht unterbleibt oder nicht, spielt erst in der juristischen Aufarbeitung der Ereignisse eine Rolle. In der Situation der Krise macht es vermutlich keinen Unterschied…

## 8.5 Kommunikationskanäle

- Funktionsweise Behördenfunk: Wie lange wäre er bei einem Blackout verfügbar? Gibt es Funklöcher bzw. Stellen, an denen keine Erreichbarkeit über den Behördenfunk gegeben ist?
- Wie erfolgt die Einberufung/Verständigung eines Krisenstabes durch das SKKM, bzw. des Nationalen Sicherheitsrates?
- Über die RTR ist in den vergangenen Jahren eine durch gegenseitiges Vertrauen geprägte Zusammenarbeit zwischen den KI-Betreibern und der RTR entstanden. Ist das ein Raum, den man nutzen könnte, um die Krisenvorbereitung zu verbessern?

## 8.6 Logistik im Pflege- und Gesundheitsbereich

- Versorgung der Krankenhäuser mit Verbrauchsmaterial
- Versorgung der Apotheken mit lebenswichtigen Medikamenten

## 8.7 Lebensmittellogistik und Supermärkte

- Lebensmittellogistik und Supermärkte: Was sind ihre Pläne in so einem Fall? Werden Waren ausgegeben, wenn das Warenmanagement über die Kassen nicht erreichbar ist? Ist ein Inselbetrieb einzelner Filialen möglich? Wird gegen Bargeld verkauft, wenn Kassen nicht mehr funktionieren? Werden Plünderungen in Kauf genommen oder knappe Güter rationiert?
- Wie sind die Bereiche der mobilen Pflege und „Essen auf Rädern“ betroffen?

## 8.8 Sicherheitslage

- Gibt es Sicherheitsvorkehrungen (neben den erwähnten TUS-Anbindungen), die bei einem Internetausfall versagen? Werden bestimmte Branchen, bestimmte Infrastrukturen oder deren Betreiber angreifbarer? Könnte ein Internetausfall dadurch zum Vorspiel für eine weitere Krise werden?

## 8.9 Aufbau eines Staatsgrundnetzes

- Das Healix-Netz (E-Health Internet Exchange) verbindet Einrichtungen aus dem Gesundheitsbereich und wurde über die Infrastruktur der EVUs realisiert. Damit sollte auch nach einem Stromausfall die Versorgung rasch wieder herstellbar sein (Netzknoten bspw. bei Umspannwerken). Welche vergleichbaren ‚Inseln‘ (neben dem GovIX) gibt es in Österreich, logisch und tatsächlich in autarker Hardware?
  Siehe dazu auch die Ergebnisse des KIRAS-Projekts „Hammond-Orgel“.[6]

## 8.10 Pandemiefolgen

- Welche Abhängigkeiten sind durch den Digitalisierungsschub in Ausbildung und Arbeit entstanden? Gibt es neue Abhängigkeiten durch ein geändertes Arbeitsverhalten während und nach der Pandemie?

[6] https://www.kiras.at/gefoerderte-projekte/detail/hammondorgel (zuletzt aufgerufen am 20.11.2022).

## 8.11 Kompetenzen

- Die Feststellung der Gefährdung der staatlichen Souveränität Österreichs würde die Zuständigkeit und Koordination zum Heer verlagern. Ab wann wäre das der Fall? Gibt es Eckpunkte (unterhalb einer offiziellen Kriegserklärung), bei denen man jedenfalls damit rechnen müsste? Wie wird diese Entscheidung getroffen? Wie wird mit einer Bedrohungslage umgegangen, in der die Grenzen zwischen Angriffen, Terrorismus und Cyber-Kriegsführung zunehmend verschwimmen?
- Was lässt sich aus der Corona-Krise diesbezüglich lernen?

# 9 Resümee

Wie sich durch die Arbeit im Projekt gezeigt hat, gibt es kaum Bereiche des gesellschaftlichen Lebens, die nicht vom Internet und dessen Funktionieren abhängig sind. Darüber hinaus gibt es große wechselseitige Abhängigkeiten zwischen den verschiedenen Sektoren kritischer Infrastrukturen. Als deutliches Beispiel kann hier die Logistik dienen. Zugleich sehen wir an diesem Beispiel, dass es Bereiche gibt, die auf den ersten Blick schlecht auf derartige Krisen vorbereitet scheinen. Möglicherweise ist das jedoch aktuell gar nicht so einfach besser zu lösen. Die Entscheidungen, die hier zu treffen sind, richten sich nach der Antwort auf die Frage, ob nach Lösungen für eine resilientere Logistik gesucht werden soll, oder ob nach Lösungen gesucht werden soll, die sich weniger auf eine gut funktionierende Logistik verlassen; oder ob ohnedies beides erforderlich sein wird.

Zeitgleich zur Arbeit an ISIDOR haben uns die aktuellen Entwicklungen in der Pandemie, im Bezug auf den Klimawandel und 2022 im Krieg gegen die Ukraine deutlich vor Augen geführt, dass schnell und unerwartet die grundsätzlich sichere Versorgungslage in Österreich gefährdet sein kann. Einem Ziel des Projekts folgend schließt dieser Bericht mit Handlungsempfehlungen, die dazu beitragen sollen, auf Internetausfälle im Speziellen und ganz allgemein auf vernetzte Krisen besser vorbereitet zu sein.

## 9.1 Lösungsansätze und Handlungsempfehlungen

### 9.1.1 Weitere Zusammenarbeit aller Akteure und mehr Übungen

Bei allen Interviews und Veranstaltungen im Rahmen dieses Projekts haben die Expert:innen aus der Praxis darauf verwiesen, dass sie sich mehr Übungen zu dem Thema wünschen würden. Dabei ist es natürlich nicht nur wichtig, bestimmte Situationen durchzuspielen, sondern es geht vor allem darum, dass alle Beteiligten ein Gefühl dafür bekommen, wie andere Akteure in der Krise aufgestellt sind, was an Leistungen noch erwartbar ist, wer helfen könnte, und wer Hilfe braucht.

Darüber hinaus ist es für die Handlungsfähigkeit in einer Krise wichtig, dass etablierte Kommunikationskanäle aus dem Regelbetrieb bestehen. Erst im Krisenfall eine Kommunikationsbeziehung herzustellen ist deutlich schwieriger, als wenn das kompetente und verantwortliche Gegenüber schon persönlich bekannt ist. Regelmäßige Übungen würden auch viel im Bereich des Problembewusstseins quer durch alle betroffenen Organisationen und Hierarchien bringen, und damit letztendlich auch für die notwendigen Ressourcen zur Krisenbewältigung sorgen.

### 9.1.2 Verstärkter Fokus bei KI-Betreibern auf offline-funktionstüchtige Prozesse

Speziell an die Betreiber kritischer Infrastrukturen werden hohe Erwartungen in Bezug auf die Ausfallsicherheit ihrer Geschäftsprozesse und Dienstleistungen gestellt. Unter diesem Gesichtspunkt sollten KI-Betreiber besonders darauf achten, ihre Prozesse nach Möglichkeit so zu gestalten, dass diese vom Internet oder auch anderen externen Ressourcen unabhängig funktionieren. Insbesondere erscheint es unter

diesen Überlegungen sinnvoll, sich mit der Frage nach ausgelagerten Ressourcen (Personal, Datenverarbeitung und -speicherung) und zeitkritischem Datenaustausch zu befassen.

Ähnlich wie die Empfehlung unter 9.1.1 würde es auch organisationsintern helfen, derartige Krisen durchzuspielen. Das wäre auch als Schulungsmaßnahme geeignet, um eventuell jüngere Mitarbeiter:innen auf den selben Wissensstand zu bringen wie Ältere, die analoge Prozesse noch aus dem Normalbetrieb der früheren Jahre kennen.

### 9.1.3 (Früh-)Warnsystem

Ungleich zu anderen Krisen würde ein großflächiger und langanhaltender Ausfall Internet-basierter Dienste eventuell nicht gleich als solcher zu erkennen sein. Für viele Betreiber kritischer Infrastrukturen wäre das Wissen um die Dimension und Dauer eines Ausfalls jedoch eine wertvolle Entscheidungsgrundlage für ihr organisationsinternes Vorgehen.

Es sollte daher erforscht werden, ob es basierend auf Netzsensoren oder anderen Lösungen Möglichkeiten gibt, ein Frühwarnsystem aufzubauen, das in der ersten Phase der Krisenbewältigung wertvolle Informationen für die handelnden Personen liefern könnte.

### 9.1.4 Bestehende autarke Komponenten weiter kombinieren

In der Interviewphase des Projekts wurde von vielen Interviewpartner:innen die Errichtung eines eigenen Staatsgrundnetzes vorgeschlagen, das alle in einer wie auch immer gearteten Krise relevanten Akteure miteinander verbindet, auch mit der Möglichkeit zu breitbandigem Datenaustausch. Im weiteren Projektfortgang stellte sich heraus, dass es in manchen Bereichen, privat und öffentlich, bereits autark funktionstüchtige Netzbereiche gibt, die man (wie im Projekt Hammond-Orgel[7] für die staatlichen Infrastrukturen bearbeitet) zu einem Netz zusammenschließen könnte, das in der Funktion einem Staatsgrundnetz nahe kommt, durch die Integration bestehender Elemente aber deutlich kostengünstiger umzusetzen wäre.

Daher empfehlen wir, die Erkenntnisse aus den Projekten ISIDOR und Hammond-Orgel zu kombinieren und auszuloten, wo es mit einem vernünftigen Kosten/Nutzen-Verhältnis möglich ist, die Funktion eines Staatsgrundnetzes für die Verwaltung, die Betreiber kritischer Infrastrukturen und weitere krisenrelevante Akteure zur Verfügung zu stellen.

### 9.1.5 Kommunikation in der Krise

Es ist wichtig, die Kommunikation zu den Betreibern kritischer Infrastrukturen aufrecht zu erhalten, ebenso wie zu anderen krisenrelevanten Akteuren. Dabei darf nicht außer Acht gelassen werden, dass es im gegenständlichen Anlassfall ebenso notwendig sein wird, nicht nur die nationalen Kommunikationswege abzusichern,

[7] https://www.kiras.at/gefoerderte-projekte/detail/hammondorgel (Zuletzt aufgerufen am 20.11.2022).

sondern auch die Verbindung zu europäischen und internationalen Institutionen sicherzustellen.

Aus Sicht dieses Forschungsprojektes böte es sich an, regelmäßig eine Evaluierung der bestehenden Kommunikationskanäle für den Krisenfall durchzuführen; sowohl im Hinblick auf deren Funktionstüchtigkeit, als auch auf die Vollständigkeit der damit versorgten Organisationen.

Darüber hinaus ist die Kommunikation auch in zwei andere Richtungen wichtig: Einerseits zur Einbindung von Unterstützungskräften, und andererseits zur transparenten Information der Bevölkerung, um Spekulationen und das Aufkommen von Verschwörungstheorien möglichst hintan zu halten. Gerade bei einem Internetausfall kann es sein, dass spezialisierte IT-Fachkräfte benötigt werden, die während dieser Kommunikationskrise schwer zu erreichen sind, und obendrein vielleicht gerade bei ihren Arbeitgebern versuchen die Auswirkungen der Krise abzufedern. Wie wären diese über das SKKM im Anlassfall zu koordinieren? Zusätzliche Hilfe könnte potenziell von allen Betreibern von Kommunikationseinrichtungen kommen. Die Art und Weise der Zusammenarbeit könnte beispielhaft mit dem ÖVSV geprobt werden, und als Vorlage für weitere Kooperationen dienen.

Andererseits mag es auch notwendig sein, ein Konzept für die Einbindung von hilfsbereiten Menschen parat zu haben, damit schon vorab klar ist, wo in so einer Situation geholfen werden kann, und wie diese Menschen im nächsten Spital, bei der Feuerwehr, in der Nachrichtenübermittlung, per Botendienst am Fahrrad o.ä. etwas Nützliches beitragen können. Dazu sollte vorab geklärt werden, wie ein solches Konzept in der Krise strukturiert werden kann, auch bezüglich der Frage, ob das SKKM es koordinieren kann bzw. soll, oder ob es nicht besser wäre, hier bestehende Plattformen, wie „Team Österreich“, „Österreich hilft Österreich“ o.Ä. zu nutzen.

### 9.1.6 Richtlinien zur Bevorratung krisenrelevanter Versorgungsgüter

Wie sich gezeigt hat, haben Kostendruck und gleichzeitig hoch qualitative Logistik dazu geführt, dass in vielen Bereichen die Lagerhaltung notwendiger Verbrauchsmaterialien dramatisch verringert wurde. Vor allem im Gesundheitsbereich, aber nicht nur dort, wird mit Lieferkonzepten gearbeitet, die eine Just-in-Time-Versorgung, mit mehreren Lieferungen pro Tag, auch für laufend dringend benötigte Versorgungsgüter vorsehen. Im Krisenfall würde diese Versorgung zunehmend schwieriger werden, eventuell nur noch mit starker Verzögerung möglich sein, oder ganz zusammenbrechen.

Um in so einem Fall nicht schon nach kurzer Zeit die Versorgung einstellen zu müssen, wäre es wichtig, dass betroffene Einrichtungen ihren Bedarf für so eine Situation erheben und sicherstellen, dass zumindest das Notwendigste für die schlechtesten Falls anzunehmende Ausfallsdauer vor Ort vorrätig ist. Das wäre sektorunabhängig eine wichtige Ergänzung zu Richtlinien für die Betreiber kritischer Infrastrukturen.

### 9.1.7 Weitere Arbeit am Problemfeld Bargeld/Lebensmittellogistik

Es gibt zwei im Normalbetrieb miteinander verschränkte Bereiche, die die Versorgung der Bevölkerung unmittelbar betreffen: Die Verfügbarkeit von Zahlungsmöglichkeiten und jene von Lebensmitteln. Bargeldlose Zahlungssysteme würden bei einem langanhaltenden Kommunikationsausfall nicht mehr funktionieren, ebenso wenig wie Bankomaten oder Bankfilialen. Das Problem scheint auch für den Fall eines Blackouts ungelöst zu sein.

Hier wäre es wichtig, alle Stakeholder:innen an einen Tisch zu bringen, um eine krisenfeste Lösung zu erarbeiten.

Die Lebensmittellogistik wird so wie die meisten anderen Logistikprozesse in der betrachteten Situation nach kurzer Zeit zusammenbrechen. Supermärkte und die übergeordneten Warenzwischenlager haben einen so großen täglichen Warenumsatz, dass die Lagerkapazitäten und natürlich auch die Frage der Frische bzw. der Lagerbedingungen es nicht zulassen, Vorräte für einen längeren Zeitraum anzulegen.

Gemeinsam mit den Partnern aus der Lebensmittellogistik und -produktion sollte ausgearbeitet werden, wie im Krisenfall die Versorgung der Bevölkerung mit den notwendigen Lebensmitteln sichergestellt werden kann. Eventuell wären ‚Leuchtturm-Supermärkte', von denen jeweils einer pro Versorgungsbezirk große Mengen haltbarer Lebensmittel bevorraten könnte, ein erster Schritt in diese Richtung.

### 9.1.8 Mehr Ressourcen und Kompetenzen bei krisenbewältigenden Organisationen

Einige Mobilfunkprovider sind mit schnell einsatzfähigen, mobilen Sendeanlagen ausgerüstet, um die Mobilfunkverbindung von Einsatzkräften in Katastrophengebieten zu ermöglichen. Die Organisationen, von denen in Österreich traditionell erwartet wird, dass sie in Krisensituationen helfen, sind neben anderen das Bundesheer und die freiwillige Feuerwehr. Natürlich können diese mobilen Anlagen nur von den Netzbetreibern selber in Betrieb genommen werden. Da die Möglichkeiten der Mobilfunkbetreiber aber begrenzt sind, und gerade in diesem Themenbereich der Wunsch nach einer Autarkie Österreichs vernehmbar ist, wäre es überlegenswert, die krisenbewältigenden Organisationen mit der nötigen Hardware und dem Know-How auszustatten, das nötig ist, um alternative Kommunikationskanäle zu betreiben.

Das österreichische Bundesheer baut die notwendigen Kompetenzen auf, um die eigenen Netze gegen Angriffe zu schützen. Darüber hinaus hat es die Aufgabe, Österreich zu verteidigen. Bei den bisher bereitgestellten Ressourcen kann es dieser Aufgabe zumindest im Cyberspace nicht nachkommen. Hier wäre es empfehlenswert, Teile des zuletzt deutlich aufgestockten Etats auch für einen Ausbau der Cyber-Defence zu verwenden.

Zusätzlich ist es wünschenswert, dass alle Organisationen, die in Krisen helfen und in der Bevölkerung auch als Anlaufstellen in krisenhaften Situationen erlebt werden, über ausreichendes Training verfügen, um zu wissen, was im Fall eines Internetausfalls zu tun ist.

### 9.1.9 Weitere Forschungsfragen für die Zukunft

Das Forschungsprojekt ISIDOR hat in vielen Bereichen Pionierarbeit geleistet, besonders in Bezug auf die Situation in Österreich. Einige Fragen, die im Zuge der Projektarbeit entstanden sind, blieben im Rahmen des Projekts unbeantwortet und könnten die Aufgaben für zukünftige Forschungsvorhaben stellen. Eine entsprechende Übersicht findet sich in Kap. 8.

Darüber hinaus gibt es ein Thema, das besonders wichtig erscheint, um zukünftige Abhängigkeiten zu vermeiden.

#### *9.1.9.1 Welche Technologien bauen zukünftig auf permanenter Vernetzung auf?*

Bei vielen emergenten Technologien bzw. deren Implementierungen bildet eine Kommunikationsfähigkeit über externe Netze die Grundlage ihrer Funktionsweise. So wird beispielsweise erwartet, dass autonome Fahrzeuge ständig mit ihrer Umgebung, der Verkehrsinfrastruktur, anderen Autos etc., in Kontakt sind, Verkehrsinformationen austauschen und Vieles mehr. Manches davon wird sich über ad hoc-Netzwerke realisieren lassen, für viele andere Funktionen ist jedoch eine Vernetzung über 5G oder 6G Mobilfunknetze angedacht. Hier wäre naheliegender Weise sicherzustellen, dass keine Funktionen auf dieser Vernetzung aufbauen, die essentiell für die Funktionstüchtigkeit der Fahrzeuge sind.

Aber auch in anderen Bereichen als der Mobilität spielt die zunehmende Vernetzung eine große Rolle. Beispielhaft seien hier die Bereiche Smart Home-Automatisierung bzw. Gebäudesteuerung und Fernwartung von lebenswichtigen Systemen, z.B. im Gesundheitsbereich, genannt. Es wäre wichtig, die Frage der Notwendigkeit bzw. Ausfallssicherheit der Vernetzung bei einer Beurteilung dieser technischen Konzepte mitzuberücksichtigen.

# 10 Anhang

## 10.1 Abkürzungsverzeichnis

| | |
|---|---|
| APA | Austria Presse Agentur |
| APCIP | Austrian Programme for Critical Infrastructure Protection |
| BCM | Business Continuity Management |
| BGP | Border Gateway Protocol |
| BOS | Behörden und Organisationen mit Sicherheitsaufgaben |
| CDN | Content Delivery Network |
| CERT | Computer Emergency Response Team |
| CLD | Causal Loop Diagramm |
| DLT | Distributed Ledger Technology |
| DNS | Domain Name Service |
| EVU | Energieversorgungsunternehmen |
| GovIX | Government Internet Exchange |
| GPRS | General Packet Radio Service |
| IKT | Informations- und Kommunikationstechnik |
| IP | hier: Internet Protocol (sonst auch: Intellectual Property) |
| ISP | Internet Service Provider |
| KI | hier: Kritische Infrastruktur(en) (sonst auch: Künstliche Intelligenz) |
| LWL | Lichtwellenleiter |
| MPLS-FRR | Multiprotocol Label Switching – Fast Reroute |
| NAS | Network Attached Storage |
| NEMP | Nuclear Electromagnetic Pulse (deutsch: nuklearer elektromagnetischer Impuls) |
| NOC | Network Operations Centre |
| NTCS | New Computerized Transit System |
| ÖPNV | Öffentlicher Personennahverkehr |
| ÖSCS | Österreichische Strategie für Cybersicherheit |
| ÖV | Öffentlicher Verkehr |
| ÖVSV | Österreichischer Versuchssenderverband |
| RAID | Redundant Array of Independent Disks |
| Re.M | Resilienz Monitor Austria |
| RTR | Rundfunk und Telekom Regulierungs-GmbH |
| SKKM | Staatliches Krisen- und Katastrophenschutzmanagement |
| SLA | Service Level Agreement |
| SSD | Solid State Drives |
| TAB | Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag |
| TETRA | Terrestrial Trunked Radio (früher: Trans European Trunked Radio) |
| VIX | Vienna Internet Exchange |
| VPN | Virtuelles Privates Netzwerk (auch englisch: Virtual Private Network) |
| WDM | Wavelength Division Multiplex (englisch; deutsche Bezeichnung: Wellenlängenmultiplexverfahren) |
| ZID | Zentraler Informatikdienst der Universität Wien |

## 10.2 Literatur

Aceto, G. et al. (2018). A comprehensive survey on internet outages. Journal of Network and Computer Applications 113, 36–63.

Adams, T., Connor, M. & Whittaker, R. (2019). Protecting our digital medicine infrastructure. npj Digital Medicine, 2(1), 97. https://doi.org/10.1038/s41746-019-0177-y.

Allianz Global Corporate & Specialty SE (2022). *Allianz Risk Barometer 2022: Cyber weltweites Top-Risiko für Unternehmen; Sorge vor Naturgefahren und Klimawandel in Deutschland*, 18. Januar, https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html, letzter Zugriff: 20. Juli 2022.

Beltrán, Fernando, Fontenay, Alain & Almeida, Marcio 2005. Internet as a critical infrastructure: lessons from the backbone experience in South America | Semantic Scholar. https://www.semanticscholar.org/paper/Internet-as-a-critical-infrastructure%3A-lessons-from-Beltr%C3%A1n-Fontenay/a2b90858f791ae23cc8733e5b221ab920dc61830 [Stand 2021-06-16].

Bogner, Alexander, Littig, Beate und Menz, Wolfgang (Hg.) (2002): Das Experteninterview – Theorie, Methode, Anwendung; Springer Fachmedien, Wiesbaden.

Bogner, Alexander, Littig, Beate und Menz, Wolfgang (2014): Interviews mit Experten – Eine praxisorientierte Einführung, Springer VS/Springer Fachmedien, Wiesbaden.

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (2021). *FAQ Digitalfunk BOS – Fragen und Antworten zum Digitalfunk der Behörden und Organisationen mit Sicherheitsausgaben* (Ausgabe 2021/ 2022). Berlin: BDBOS.

Bundeskanzleramt Österreich (2015): Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP), Masterplan 2014., https://www.bundeskanzleramt.gv.at/dam/jcr:bb6a1a41-eb1d-4552-96da-9b460bbc5c0b/%C3%96sterreichisches%20Programm%20zum%20Schutz%20kritischer%20Infrastrukturen%20(APCIP).pdf (zuletzt aufgerufen am 20.11.2022).

Bundeskanzleramt Österreich (2013): Österreichische Sicherheitsstrategie, Wien 2013. https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf (zuletzt aufgerufen am 25.11.2022).

Bundeskanzleramt Österreich (2021): Österreichische Strategie für Cybersicherheit, Wien 2021. https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsstrategien-und-Initiativen/2021-Oesterreichische-Strategie-Cybersicherheit.html (zuletzt aufgerufen am 25.11.2022).

Bundesministerium für Finanzen (o. D.). *Versandverfahren*, o.D., https://www.bmf.gv.at/themen/zoll/ueberfuehrung-in-ein-zollverfahren/versandverfahren, letzter Zugriff: 13. Juli 2022.

Bundesministerium für Inneres (2004) Ministerratsbeschluss vom 20. Jänner 2004: Neuorganisation des Staatlichen Krisen- und Katastrophenschutzmanagements sowie der internationalen Katastrophenhilfe (SKKM), https://www.bmi.gv.at/204/SKKM/files/001_Ministerratsbeschluss.pdf, letzter Zugriff 18.11.2022.

Bundesministerium für Inneres (2018). SKKM-Leitfaden für das Risikomanagement. https://www.bmi.gv.at/204/Download/files/SKKM-Leitfaden_fuer_das_Risikomanagement_Version_1_0.pdf, letzter Zugriff 18.11.2022.

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (o. D.). *Die Nummer zu Ihrer telefonischen Gesundheitsberatung*, o. D., https://www.1450.at, letzter Zugriff: 13. Juli 2022.

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (2021). *Krankenanstalten in Zahlen – Erläuterungen zu den Tabellen und Grafiken*, 6. April, http://www.kaz.bmg.gv.at/fileadmin/user_upload/Erlaeuterungen.pdf, letzter Zugriff: 13. Juli 2022.

Burgstedt, L. & Britze, N. (2021). *Tschüss Fax: Unternehmen digitalisieren ihre Kommunikation.* Berlin: Bitkom. [online] https://www.bitkom.org/Presse/Presseinformation/Tschuess-Fax-Unternehmen-digitalisieren-ihre-Kommunikation, letzter Zugriff: 23.07.2022.

Cho, Kenjiro u. a. (2011). The Japan Earthquake: the impact on traffic and routing observed by a local ISP. In *Proceedings of the Special Workshop on Internet and Disasters*. 1–8.

Cholda, Piotr u. a. (2007). A survey of resilience differentiation frameworks in communication networks. *IEEE Communications Surveys & Tutorials* 9, 4, 32–55.

Cleary, P. F. & Banasiewicz, A.D. (2018). Toward resilience of business ecosystems: The internet as a critical infrastructure. *Australian Academy of Accounting and Finance Review* 4, 1, 1–10.

Czerni, W. (2021). Bericht IKT Branchen Risikoanalyse. Version 3.0-2021 RTR WHITE-VERSION. Rundfunk & Telekom Regulierungs-GmbH. https://www.rtr.at/TKP/was_wir_tun/telekommunikation/anbieterservice/netzsicherheit/Bericht_v_3_0_WHITE_Version.pdf

Dainotti, A. u. a. (2011). Analysis of country-wide internet outages caused by censorship. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. 1–18.

DAÖ – Digitaler Atlas Österreich (2017): Digitaler Atlas Österreich – Wem gehört das Internet?, Projektbericht

Der Standard (2022). *Hackerangriff auf Kärnten: Weitere Daten im Darknet veröffentlicht*, in: Der Standard, 17.06.2022. [online] https://www.derstandard.at/story/2000136636627/hackerangriff-auf-kaernten-weitere-daten-im-darknet-veroeffentlicht, letzter Zugriff: 20.07.2022

Deutsche Krankenhausgesellschaft (2019). *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus* (Version 1.1), 22. Oktober, https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus, letzter Zugriff: 20. Juli 2022

DIN EN ISO 22301 (2020). Sicherheit und Resilienz - Business Continuity Management System - Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019.

ELGA GmbH (2021). *Wissenswertes zu ELGA*, 1. Februar, https://www.elga.gv.at/faq/wissenswertes-zu-elga, letzter Zugriff: 13. Juli 2022

Engemann, Kurt J. & Miller, Holmes E. (2017). Risk and Data Center Planning. In *Engineering and Management of Data Centers*. Springer, 73–89.

Eriksson, B., Durairajan, R. & Barford, P. (2013). RiskRoute: a framework for mitigating network outage threats. In *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*. CoNEXT '13: Conference on emerging Networking Experiments and Technologies. Santa Barbara California USA: ACM, 405–416. https://dl.acm.org/doi/10.1145/2535372.2535385 [Stand 2021-06-16].

Europäische Kommission (2019*). Aerial Base Stations with Opportunistic Links for Unexpected & Temporary Events*, 2. August, https://cordis.europa.eu/project/id/318632/de, letzter Zugriff: 20. Juli 2022

Fauss, E. (2018). *Case Study: Hospital Integrates Remote, Real-Time Monitoring Data from Isolation Unit*. Biomedical Instrumentation & Technology, 52(2), 125–129. https://doi.org/10.2345/0899-8205-52.2.125

Flick, Uwe, von Kardoff, Ernst und Steinke, Ines (2003): Qualitative Forschung – Ein Handbuch, Rowohlt Taschenbuch Verlag, Reinbek bei Hamburg, 2. Auflage: 2003

Ford, A. (2010). *Modeling the environment* (2nd ed.). Washington, DC: Island Press.

Forrester, J. W. (1993). *System Dynamics and the Lessons of 35 Years*. In K.B. De Greene (Hrsg.), A Systems-Based Approach to Policymaking (S. 199–240). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4615-3226-2_7

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. & Aylin, P. (2019). *A retrospective impact analysis of the WannaCry cyberattack on the NHS*. npj Digital Medicine, 2(1), 98. https://doi.org/10.1038/s41746-019-0161-6

Giannopoulos, G., Dorneanu, B. & Jonkeren, O. (2013). Risk assessment methodology for critical infrastructure protection. *JRC–Scientific and Policy Report* .

Girs, S., Sentilles,S., Abbaspour Asadollah, S., Ashjaei, M. & Mubeen, S. (2020): *A Systematic Literature Study on Definition and Modeling of Service-Level Agreements for Cloud Services in IoT*, in: IEEE Access, Bd. 8, S. 134498–134513, https://doi:10.1109/access.2020.3011483 , letzter Zugriff: 20.07.2022

Goldstein, H. (2010). *Satellite internet access withstands Haiti quake*. IEEE Spectrum, 47(3), 11–12. https://doi.org/10.1109/MSPEC.2010.5421883

Grandhi, Sukeshini A., Plotnick, Linda & Hiltz, Starr Roxanne (2020). An internet-less world? Expected impacts of a complete internet outage with implications for preparedness and design. *Proceedings of the ACM on human-computer interaction* 4, GROUP, 1–24.

Graydon, M. & Parks, L. (2020). 'Connecting the unconnected': a critical assessment of US satellite Internet services. Media, Culture & Society, 42(2), 260–276. https://doi.org/10.1177/0163443719861835

Greenstein, S. (2020). The basic economics of internet infrastructure. *Journal of Economic Perspectives* 34, 2, 192–214.

Gruber, A. (2022): *Neuartiger Cyberangriff legt Uni Salzburg lahm, i*n: Salzburg24, 05.04.2022, [online] https://www.salzburg24.at/news/salzburg/neuartiger-cyberangriff-legt-uni-salzburg-lahm-119485171, letzter Zugriff: 20.07.2022.

Henry, D. & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety* 99, 114–122. https://doi.org/10.1016/j.ress.2011.09.002

Hopf, C. (2003): Qualitative Interviews – ein Überblick, in: Flick, Uwe, von Kardoff, Ernst und Steinke, Ines (2003): Qualitative Forschung – Ein Handbuch, Rowohlt Taschenbuch Verlag, Reinbek bei Hamburg, 2. Auflage: 2003, S. 349-360

ISIDOR (2021). *Expert:inneninterviews mit Vertreter:innen aus dem Gesundheitssektor.* Geführt durch die Universität für Bodenkultur Wien und das Institut für Technikfolgenabschätzung im Rahmen des Projektes ISIDOR im Zeitraum Februar 2021 bis Juli 2021.

ISIDOR (2021). *Expert:inneninterviews mit Vertreter:innen aus dem Transportsektor.* Geführt durch die Universität für Bodenkultur Wien und das Institut für Technikfolgenabschätzung im Rahmen des Projektes ISIDOR im Zeitraum Februar bis Juli 2021.

ISIDOR (2021). *SKKM-Sektorenworkshops (1. Reihe) mit Vertreter:innen aus dem Transportsektor.* Geführt durch die Infraprotect GmbH und die Mar Adentro e.U. unter Anleitung des BMI und Mitwirkung des Institutes für Technikfolgenabschätzung und der Universität für Bodenkultur Wien im Rahmen des Projektes ISIDOR im Zeitraum Mai bis Juli 2021.

ISIDOR (2021). *SKKM-Sektorenworkshops (2. Reihe) mit Vertreter:innen aus verschiedenen Sektoren.* Geführt durch die Infraprotect GmbH und die Mar Adentro e.U. unter Anleitung des BMI und Mitwirkung des Institutes für Technikfolgenabschätzung und der Universität für Bodenkultur Wien im Rahmen des Projektes ISIDOR im Zeitraum Oktober 2021.

ISIDOR (2022). *Expert:inneninterview mit einem Vertreter aus dem Lebensmittelsektor.* Geführt durch die Universität für Bodenkultur Wien und das Institut für Technikfolgenabschätzung im Rahmen des Projektes ISIDOR im Jänner 2022.

Jungehülsing, J. (2021): Facebook blockiert journalistische Inhalte in Australien, https://www.zeit.de/digital/internet/2021-02/australien-facebook-medien-gesetz-blockade-google (zuletzt aufgerufen am 20.11.2022)

Kapmeier, F. (1999). *Vom systemischen Denken zur Methode System Dynamics*. Universität Stuttgart. https://doi.org/10.18419/OPUS-5449

Kathuria, Rajat 2018. *The anatomy of an internet blackout: measuring the economic impact of internet shutdowns in India*. New Delhi, India: Indian Council for Research on International Economic Relations.

Katz-Bassett, E. u. a. (2008). Studying Black Holes in the Internet with Hubble. In *NSDI*. 247–262.

#keepiton (2021). #KeepItOn update: who is shutting down the internet in 2021? Access Now. https://www.accessnow.org/who-is-shutting-down-the-internet-in-2021/ [Stand 2021-06-16].

Kühl, E. (2021): Ein Hackerangriff, der um die Welt geht, https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187 (zuletzt aufgerufen am 20.11.2022)

Laschkolnig, A. (2021): *Telemedizin in Österreich. Ergebnisbericht - Im Auftrag des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz.* Wien: Gesundheit Österreich GmbH.

Lehmann, N. (2021): Hackerangriff legt Molkerei in Österreich lahm, in: agrarheute, 24.06.2021, [online] https://www.agrarheute.com/management/agribusiness/hacker-legen-cyberangriff-molkerei-oesterreich-lahm-582644, letzter Zugriff: 22.07.2022.

Luber, S., Schadhauser; W., Ehneß, J. (2021). *Was ist ein NAS (Network Attached Storage)?*. 09.02.2021, https://www.storage-insider.de/was-ist-ein-nas-network-attached-storage-a-630418/ , letzter Zugriff 23.07.2022.

Lupien, N. u. a. 2017. Wait, Did You Say No Internet? An Exploratory Study of the Perceived Impact of Internet Outage. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 231–234.

Maglaras, Leandros A. u. a. 2018. Cyber security of critical infrastructures. *Ict Express* 4, 1, 42–45.

Mahn, J. (2022): Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich, https://www.heise.de/news/Sabotage-bei-der-Bahn-Viele-vertrauliche-Infos-sind-offen-zugaenglich-7307277.html (zuletzt aufgerufen am 20.11.2022)

MAHN, J., WÖLBERT C. (2020): Die riskante Abhängigkeit der Bundesrepublik von amerikanischen IT-Riesen, c't Magazin für Computertechnik, Ausgabe 19/2020, S. 64-69

Mandl, C. & Gronalt, M. (2012). *Systemarchetypen – Generische Modelle*. Wien: Universität für Bodenkultur Wien.

Marquezan Cassales, C., Metzger, A., Franklin, R., Pohl, K. (2014): *Runtime Management of Multi-level SLAs for Transport and Logistics Services*, in: Service-Oriented Computing, S. 560–574, [online] doi:10.1007/978-3-662-45391-9_49, letzter Zugriff: 22.07.2022.

Matthews, R. (2020). Was ist ein VPN-Tunnel?, 23. September, https://nordvpn.com/de/blog/was-ist-tunnel-vpn, letzter Zugriff: 13. Juli 2022

Meadows, D. H., Randers, J. & Bardi, U. (2019). *Die Grenzen des Denkens: wie wir sie mit System erkennen und überwinden können* (Bibliothek der Nachhaltigkeit). (K. Bossel, H. Bossel & S. Weis-Gerhardt, Übers.). München: oekom verlag.

Mella, P. (2012). *Systems Thinking – Intelligence in Action*. Italien: Springer Verlag.

Meuser, M., Nagel, U. (2002): ExpertInneninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion, in: Bogner, Alexander, Littig, Beate, Menz, Wolfgang (Hg.) (2002): Das Experteninterview – Theorie, Methode, Anwendung; Springer Fachmedien, Wiesbaden, S. 71-94

Miller, Holmes E. & Engemann, Kurt J. 2019. Business continuity management in data center environments. *International Journal of Information Technologies and Systems Approach (IJITSA)* 12, 1, 52–72.

Moechel, E. (2021): Cyberangriff auf die USA eskaliert immer weiter, https://fm4.orf.at/stories/3010878/ (zuletzt aufgerufen am 20.11.2022)

Motyka, M. (2012): Persuasion und Wissenserwerb durch Serious Games im Politikunterricht, Reihe Studium und Forschung der Universität Kassel, Heft 21

ÖNORM S2304 (2018): Integriertes Katastrophenmanagement. Benennungen und Definitionen.

ÖVSV (2022). *Notfunkübung „Mailüfterl" am 1. Mai 2022*, 28. April, https://www.oevsv.at/funkbetrieb/notfunk/, letzter Zugriff: 20. Juli 2022

Pan, S., Trentesaux, D., McFarlane, D., Montreuil, B., Ballot, E. & Huang, G. Q. (2021). Digital interoperability in logistics and supply chain management: state-of-the-art and research avenues towards Physical Internet. Computers in Industry, 128, 103435. https://doi.org/10.1016/j.compind.2021.103435

Pecorella, T., Ronga, L. S., Chiti, F., Jayousi, S. & Franck, L. (2015). *Emergency satellite communications: research and standardization activities*. IEEE Communications Magazine, 53(5), 170–177. https://doi.org/10.1109/MCOM.2015.7105657

Pescaroli, Gianluca & Alexander, David 2016. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Natural Hazards* 82, 1, 175–192.

PETERMANN, T., BRADKE, H., LÜLLMANN, A., PAETZSCH, M. und RIEHM, U. (2011): Was bei einem Blackout geschieht – Folgen eines langandauernden und großflächigen Stromausfalls, edition sigma, Berlin

Quan, L., Heidemann, J. & Pradkin, Y. (2013). Trinocular: Understanding internet reliability through adaptive probing. *ACM SIGCOMM Computer Communication Review* 43, 4, 255–266.

Rebiger, S. (2018): Kritik von allen Seiten für Googles chinesische „Zensurmaschine“, https://netzpolitik.org/2018/kritik-von-allen-seiten-fuer-googles-chinesische-zensurmaschine/ (zuletzt aufgerufen am 20.11.2022)

Richter, P. u. a. (2018). Advancing the Art of Internet Edge Outage Detection. In *Proceedings of the Internet Measurement Conference 2018*. IMC '18: Internet Measurement Conference. Boston MA USA: ACM, 350–363. https://dl.acm.org/doi/10.1145/3278532.3278563 [Stand 2021-06-16].

Rudl, T. (2018): Apple speichert private iCloud-Schlüssel ^künftig in China, https://netzpolitik.org/2018/apple-speichert-private-icloud-schluessel-kuenftig-in-china/ (zuletzt aufgerufen am 20.11.2022)

SBA Research GmbH, Repuco Unternehmensberatung GmbH & Institut für empirische Sozialforschung GmbH (2017). *Digitaler Atlas Österreich 2.0*. Wien: KIRAS Sicherheitsforschung

Schachenhofer, L., Hirsch, P. & Gronalt, M. (2022). *Analysing feedback processes of extensive and prolonged internet outages in the transport and health sector.* Wien: Universität für Bodenkultur Wien (Working Paper).

Scherk J. und Pöchhacker-Tröscher G. (2017). *Die Blockchain – Technologiefeld und wirtschaftliche Anwendungsbereiche.* Pöchhacker Innovation Consulting GmbH.

Simon, T. (2017). Chapter seven: Critical infrastructure and the internet of things. *Cyber Security in a Volatile World* 93.

Steidl, V. und Wenz D. (2022, 23. August). *Distributed-Ledger-Technologie (DLT): Definition und Anwendungen.* Bitcoin-2go. https://bitcoin-2go.de/distributed-ledger-technologie/#:~:text=W%C3%A4hrend%20die%20Blockchain%20eine%20Datenstruktur,eine%20Teilmenge%20der%20umfassenden%20DLT

Stepanek, M. (2021). *Satelliten-Internet Starlink: "Zu teuer, zu wenig Leistung".* 09. Februar, Futurezone.https://futurezone.at/produkte/satelliten-internet-starlink-zu-teuer-zu-wenig-leistung/401183263, letzter Zugriff: 18.07.2022.

Sterbenz, J. PG u. a. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks* 54, 8, 1245–1265.

Sterbenz, James PG & Hutchison, David 2006. *Resilinets: Multilevel resilient and survivable networking initiative wiki*.

Sterman, J. D. (2000). Business Dynamics – Systems Thinking and Modeling for a Complex World. USA: The McGraw-Hill Companies Inc.

Temple-Raston, D. (2021): A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (zuletzt aufgerufen am 20.11.2022)

Tung, L. (2021): Microsoft: SolarWinds attack took more than 1,000 engineers to create, https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/ (zuletzt aufgerufen am 20.11.2022)

Van Eeten, M. u. a. (2011). THE STATE AND THE THREAT OF CASCADING FAILURE ACROSS CRITICAL INFRASTRUCTURES: THE IMPLICATIONS OF EMPIRICAL EVIDENCE FROM MEDIA INCIDENT REPORTS. *Public Administration* 89, 2, 381–400.

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. *International Journal of Communication* 12, 1, 3917–3938.

Wang, J., Qiao, C. & Yu, H. (2011). On progressive network recovery after a major disruption. In *2011 Proceedings IEEE INFOCOM*. IEEE, 1925–1933. https://doi.org/10.1109/infcom.2011.5934996

West, Darrell M. (2016). Internet shutdowns cost countries $2.4 billion last year. *Center for Technological Innovation at Brookings, Washington, DC*

Windeck, Christof (2020): Kernaufgaben – Digitale Souveränität bei kritischen Infrastrukturen (KRITIS), c't Magazin für Computertechnik, Ausgabe 19/2020, S. 75

Wolff, Reinhard (2021): Cyberangriff legt Läden lahm, https://taz.de/Knapp-800-Supermaerkte-in-Schweden-zu/!5784023/ (zuletzt aufgerufen am 20.11.2022)

Wurmb, T., Kippnich, M., Schwarzmann, G., Mehlhase, J., Valotis, A., Firnkes, T. et al. (2020). *Vollausfall der Informationstechnologie im Krankenhaus: Entwicklung eines Konzepts zur Aufrechterhaltung der Patientenversorgung*. Der Unfallchirurg, 123(6), 443–452. https://doi.org/10.1007/s00113-020-00797-4

## 10.3 Interviews

### 10.3.1 Interviewpartner:innen

In vielen Organisationen haben unsere Interviewpartner*innen darum ersucht, nicht namentlich im Projektbericht genannt zu werden, daher werden im Folgenden nur die Organisationen und z.T. Organisationseinheiten genannt, mit denen wir gesprochen haben.

Insgesamt wurden in 22 Interviews 31 Personen befragt, aus den folgenden Organisationen:

- A1 Telekom Austria AG, Spezialisten aus dem Bereich Network
- Austrian Power Grid AG
- Bundesministerium für Inneres, Abt. IV/8 Design und Betrieb kritischer Kommunikationsinfrastrukturen
- Bundesministerium für Landesverteidigung, Sektion IV, Führungsunterstützung
- Bundesrechenzentrum GmbH, Information Security
- Cyber Security Austria – Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur
- Erste Bank der österreichischen Sparkassen AG
- EVN AG, Informationssicherheitsmanagement
- EVN Wasser GmbH
- Gartner KG
- ÖBB-Holding AG
- ÖBB-Infrastruktur AG
- Österreichischer Rundfunk
- REWE International AG
- Rotes Kreuz Oberösterreich
- Rundfunk- und Telekom Regulierungs-GmbH
- Universität Wien, Zentraler Informatikdienst, Abteilung ACOnet & Vienna Internet eXchange
- Verbund AG
- Verkehrsverbund Ost-Region GmbH, ITS Vienna Region
- Wasserleitungsverband der Triestingtal- und Südbahngemeinden
- WienCont – Container Terminal GmbH
- Wiener Gesundheitsverbund

### 10.3.2 Durchführung der Interviews

Durchgeführt wurden die Interviews im Zeitraum von Jänner bis Juni 2021 (eines wurde im Jänner 2022 nachgeholt) von folgenden Personen:

- Jaro Krieger-Lamina
- Larissa Schachenhofer
- Johanna Singer
- Patrick Hirsch

#### *10.3.2.1 Interviewleitfaden*

## Interviewleitfaden ISIDOR

Die Interviews sind als semistrukturierte Interviews geplant. Die unten gelisteten Fragen sind nicht wie ein Fragebogen zu verwenden, sondern abhängig von Ansprechpartner:in die jeweils relevanten auszusuchen. Grundsätzlich soll aber versucht werden, auf möglichst viele dieser Fragen Antworten zu bekommen.

Wichtig für die Auswertung sind in den Interviews chronologische Erzählungen, iSv „wenn das passiert, dann kommt als nächstes das, dann das…. usw." Daraus lassen sich auch Wirkungszusammenhänge erkennen, die sich modellieren lassen.

Ablauf:

- Begrüßung
- Danke für Zeit und Teilnahme
- Unabhängig von Vorgesprächen und Schriftverkehr nochmals darauf hinweisen, dass wir Vertraulichkeit garantieren:
  *Interviewinhalte werden nur projektintern verarbeitet. Niemand aus dem Projekt darf Material weitergeben.*
- Wir würden gern aufzeichnen für Transkription und projektinterne Weiterverarbeitung der Informationen in anderen Arbeitspaketen.
- Wörtliche Zitate sind nicht geplant. Falls es uns später doch sinnvoll erscheint, würden wir mit dem genauen Wortlaut nochmal eine explizite Erlaubnis einholen.
- Kommentare off-record sind möglich, diese würden ggfs. nicht transkribiert und nicht verwendet.
- Falls keine Aufzeichnung erwünscht ist, werden die wesentlichen Punkte per Hand mitgeschrieben.
- Im Anhang zum Projektbericht ist ein Verzeichnis aller Interviewpartner*innen geplant. Die Organisation erscheint jedenfalls. Dürfen wir auch Namen und/oder Org.-Einheit anführen?
- Kurze Projektvorstellung (Was ist das Ziel? All Hazards-Ansatz und Cyberresilience statt Cybersecurity erklären, Projektpartner/Koordinator, Fördergeber, wo stehen wir gerade, was kommt noch in dem Projekt…)

- Noch Fragen?
- Start des inhaltlichen Teils…
- Ende Befragung
- Nochmals bedanken, offene Fragen zu weiterem Verlauf? Möchte Interviewpartner*in noch irgendetwas anmerken?
- Verabschiedung

## Fragen (hauptsächlich für Provider)

- Was könnten Ursachen für einen Ausfall sein?
- Wie sehen die Vorbereitungen für Notfälle aus?
    - Wie tritt ein etwaiger Notfallplan in Kraft?
    - Wer ist immer erreichbar?
- Kontakte zu anderen? (CERTs, BMI, SKKM, Katastrophenschutz…)
    - Ab wann wird informiert? Und wie?
- Vorgaben durch bspw. RTR?
- Maßnahmen zur Redundanz und Maßnahmen zur Resilienz?
- Peering/Routing:
    - Welche Peerings existieren, zu welchen Peering-Points? Ausweichen über De-CIX/Frankfurt, oder Mailand, oder andere?
    - Ließe sich das Routing kurzfristig ändern, um kompromittierte Dienste/Peering-Points zu umgehen? Routing nur innerhalb Österreichs möglich?
- Abhängigkeiten von anderen (Hardware, Service, Software, Lizenzserver, Zertifikatsinfrastruktur, Diesel…)?
    - Bspw. Abhängigkeit Hardware: Lieferzeiten (auch unter Schadensfallbedingungen), Ersatzgeräte auf Lager, Geräte anderer Hersteller, remote/on-site-Wartung mit/ohne externem Personal…?
    - Analog andere Abhängigkeiten (siehe oben) ...
- Wer aller ist von Ihnen abhängig? Mit/ohne Service Level Agreements (SLAs)?
- Gibt es aktuelle Erfahrungen, wie etwa durch Solar Winds, den Vorfall im europ. Stromnetz am 8.1.2021?

## Fragen (hauptsächlich für Kunden)

Was passiert, wenn die *Internet-Bandbreite graduell schlechter wird*, bis zu einem völligen Ausfall?
Was passiert, wenn ein *Internet-Totalausfall* eintritt?

- Gab es schon einmal so eine Situation in Ihrem Unternehmen?
- Welche Bereiche des Unternehmens sind betroffen?
- Welche Services können nicht mehr erbracht werden? Ab wann?
- Ist das ein Grund für einen Notfall/K-Fall/Notbetrieb etc.?
- Ab welcher Dauer und/oder Informationslage wird auf Notbetrieb umgestellt?
    - Trifft jemand aktiv die Entscheidung, wenn ja, wer?
    - Oder ist es von vordefinierten Parametern abhängig? Wenn ja, welchen?

Was passiert im *Notbetrieb*?

- Gibt es ein Konzept dafür? Was sieht der Notfallplan vor? Berücksichtigt der Plan eine Situation, in der viel MitarbeiterInnen im Home Office sind?
- Gibt es eine Business Continuity Strategie? Pläne, wie der Übergang vom Notbetrieb zum Normalbetrieb erfolgt? Wer ist für das Business Continuity Management (BCM) zuständig?
- Welche Notfallmaßnahmen haben externe Abhängigkeiten (z.B. Notstromaggregat – Diesel)?
- Wie lange ist die Durchhaltefähigkeit im Notbetrieb?
    - Was kann knapp werden (Personal/Schichtbetrieb?, Ressourcen, Geld)?
- Was schafft das Unternehmen in der Zeit? (Erbringung aller Dienstleistungen, ev. unter erhöhtem Ressourceneinsatz, oder nur eingeschränktes Angebot, oder nur Überleben des Unternehmens, inkl. Abwenden von Schaden an der Infrastruktur…)

Wie hoch schätzen Sie die *Resilienz* gegenüber Internetausfall im Normalbetrieb ein?
Wie unterscheidet sich das von der *Resilienz im Notbetrieb* (gegenüber weiteren nachteiligen Entwicklungen)
Falls Notbetrieb: Was ist an weiteren Ausfällen verkraftbar? (Strom, andere Kommunikationswege, Ausfall Zulieferer etc.)

- Gibt es Workarounds? Wie funktionieren diese?

*Wirtschaftliche Durchhaltefähigkeit*: Wann muss aus wirtschaftlichen Gründen der Betrieb eingestellt werden?
Wie lautete die Antwort im Jänner 2020 und wie hat sich das in den vergangenen Monaten verändert? → Wirtschaftlicher/finanzieller Puffer für Notfälle…

Gibt es bekannte *Single Points of Failure*?

Gibt es bekannte *Abhängigkeiten*?

Wie würde man eine *unzuverlässige Verbindung* (Bandbreitenabfall oder Angriffe, bspw. Kompromittierung einzelner Dienste erkennen)?

Was muss in ausreichendem Maße vorhanden sein, um einen reibungslosen Betrieb zu garantieren?

- Was passiert bei *Personal*ausfällen im Zuge bspw. einer Pandemie?
    - Wie viel MitarbeiterInnen (wieviel Prozent der Belegschaft?) mit welchen Kompetenzen müssen immer vorhanden sein?
- Technisch:
    - Über wie viele *Leitungen* ist das Unternehmen angebunden?
    - Was passiert bei Leitungsausfall?
    - Wohin gehen die Leitungen physisch/logisch?
    - Bei redundanten Leitungen: Sind diese gleichwertig?
- Hardwareabhängigkeiten?
    - Welche *IT-Komponenten* müssen immer verfügbar sein?
    - Können alternative Produkte anderer Hersteller verwendet werden?

Gibt es *SLAs mit Zulieferern*? Was sehen diese vor?
Ist das Unternehmen *selbst Lieferant* mit/ohne vertragliche Verpflichtungen (SLA usw.)?
Wie sind die *Verpflichtungen* kalkuliert?
Bei Ausfall von wieviel Kapazität, können die SLAs nicht mehr bedient werden?

Gibt es *behördliche Auflagen* für den Betrieb?
Durch Regulierungsbehörden o.dgl.? (Gemeint sind nicht Betriebsstättengenehmigungen, sondern Auflagen in Bezug auf Einstufung als KI-Betreiber, oder sektorspezifische Auflagen zur Risikoabwehr…)

Wie funktionieren *Meldewege* außerhalb des Unternehmens?
Wer würde im Fall einer Serviceunterbrechung verständigt? Und wie?
Gibt es informelle Kontakte zu Mitbewerbern/anderen Anbietern innerhalb der Branche?
Bestehende Kontakte zu CERTs u.ä. Stellen (SKKM, BMI, BMLVS usw.)

Wo, in Ihrem Unternehmen oder woanders, funktioniert etwas *beispielhaft gut?*

Was würden Sie sich *wünschen*?

--- Ende---

## 10.4 Evaluierungsworkshop

### 10.4.1 Teilnehmende Organisationen

Es waren bei dem Workshop 15 Teilnehmer:innen aus den folgenden Organisationen anwesend:

- A1
- Bundeskanzleramt
- Bundesministerium für Inneres
- Infraprotect
- Mar Adentro
- Österreichische Akademie der Wissenschaften, Institut für Technikfolgen-Abschätzung
- ÖVSV
- Universität für Bodenkultur Wien, Institut für Produktionswirtschaft und Logistik
- Universität Wien, Zentraler Informatikdienst, AcoNet/VIX

### 10.4.2 Fragestellungen

Bei dem dreistündigen Workshop wurden nach einer Vorstellung des Projekts und einer Diskussion seiner vorläufigen Ergebnisse mit den Teilnehmenden vor allem die folgenden drei Themenkomplexe erörtert, mit dem Ziel einer Verbesserung und Konkretisierung der ausgearbeiteten Handlungsempfehlungen:

**1. Diskussionsrunde**

*Wenn das Internet ausfällt, hängt (extrem) viel am Mobilfunknetz (solange dieses noch funktioniert).*

Dazu gibt es zwei Lösungsansätze:

1. Neues Staatsgrundnetz – entweder komplett unabhängig oder als Zusammenschluss bestehender Netzsegmente
2. Ausfallsicheres Mobilfunknetz

Fragen:

- Was verstehen Sie unter den beiden Begriffen?
- Was ist technisch umsetzbar?
- Was sind Vor- und Nachteile der beiden Lösungen?
- Reicht eines oder brauchen wir ohnedies beide?
- Wer ist dafür zuständig oder könnte eine Umsetzung vorantreiben?

Jaro Krieger-Lamina

## 2. Diskussionsrunde

*Das Nutzen internetabhängiger Ressourcen für betriebskritische Prozesse wird in der Krise zu einem eventuell unlösbaren Problem, bspw. Cloud-Dienste.*

Fragen:

- Kann/soll/muss der Staat hier lenkend eingreifen, um die Funktionstüchtigkeit kritischer Infrastrukturen sicherzustellen? Wie weit kann der Staat in die Autonomie privatwirtschaftlicher Unternehmen eingreifen?
- Mögliche Auflagen und/oder Angebote?
- Gibt es Analogien, bspw. aus dem Cybersecurity-Bereich?
- Wer, wenn überhaupt, könnte dazu verpflichtet werden?
- Wer trägt die Kosten? Wie könnte so ein Mehraufwand abgegolten werden?

Jaro Krieger-Lamina

## 3. Diskussionsrunde

*Aus unterschiedlichen Gründen werden Ressourcen im Normalbetrieb geteilt bzw. sind im ausreichenden Maß vorhanden. Das kann sich in einer Krise ändern. Bsp: IT-Outsourcing, Verteilung von Betriebsmitteln…*

Fragen:

- Über welchen Mechanismus oder welche Regeln kann entschieden werden, wie knappe Ressourcen verteilt werden?
- Nach welchen Gesichtspunkten erfolgt eine Priorisierung bei der Zuteilung (auch von Reaktionskräften)? Wieviel Einfluss hat das staatliche Krisenmanagement darauf?
- Können Expert*innen von ihren Organisationen abgezogen werden, wenn sie auch zentral zur Krisenbewältigung gebraucht werden?

Jaro Krieger-Lamina

## 10.5 Glossar

| | |
|---|---|
| BCM | Business Continuity Management: „Im Kontext mit Business Continuity Management Systemen (…) werden Ziele zur Aufrechterhaltung der Betriebsfähigkeit von der Organisation (…) im Einklang mit ihrer Politik (…) zur Aufrechterhaltung der Betriebsfähigkeit gesetzt, um bestimmte Ergebnisse zur erreichen“ (vgl. DIN EN ISO 22301, 2020, 18). |
| DLT | Distributed Ledger Technology: „öffentliche, dezentral geführte Datenbank (…), welche über ein Netzwerk von verschiedenen Teilnehmer:innen geteilt wird (vgl. Scherk und Pöchhacker-Tröscher 2017, 12) |
| Domain Name Service (DNS) | Das DNS ist ein hierarchisch strukturiertes System zur Auskunft darüber, welche IP-Adressen in einem Netzwerk welchen Domain- Namen zugeordnet sind (Namensauflösung). |
| GPRS | Das General Packet Radio Service ist ein paketorientierter Dienst zur Datenübertragung in GSM-Netzen. Im Gegensatz zu leitungsvermittelten Datenübertragungen werden in diesem Fall die Daten in einzelne Pakete zerlegt, die nicht in der chronologischen Abfolge oder auf demselben Weg übermittelt werden müssen, und beim Empfang wieder zusammengesetzt werden. |
| Hash | Ein Hash kann eine Prüfsumme oder ein Streuwert sein. In beiden Fällen wird durch wiederholbare aber nicht umkehrbare Berechnung aus einer umfangreichen Eingabe ein vergleichsweise kurzer Wert errechnet. |
| Internet-Provider | Internet-Provider (deutsch auch Internetdiensteanbieter oder Internetzugangsanbieter, oder kurz Provider; englisch: Internet Service Provider oder Internet Access Provider) sind Firmen, die ihren Kund:innen den Zugang zum Internet technisch ermöglichen, bzw. die Ressourcen zur Verfügung stellen, um Inhalte oder Dienste im Internet anzubieten. |
| Lichtwellenleiter (LWL) | Lichtwellenleiter sind aus Lichtleitern bestehende Kabel zur Übertragung von Lichtimpulsen. Als Lichtleiter kommen oft Quarzglas oder Kunststoffe zum Einsatz. Mehrere gebündelte Lichtwellenleiter werden i.d.R. als Glasfaserkabel bezeichnet. |
| MD5 | Message Digest-Algorithm 5 ist eine kryptographische Hashfunktion, die aus jeder beliebigen Nachricht einen 128-Bit Hashwert erzeugen kann. Der Algorithmus wird oft dazu verwendet sicherzustellen, dass eine bestimmte Information |

| | |
|---|---|
| | nicht verändert/manipuliert wurde, gilt mittlerweile allerdings nicht mehr als sicher. |
| NAS | Network Attached Storage: Ein NAS ist ein netzgebundener Speicher, der über Mechanismen wie Redundant Array of Independent Disks (RAID) verfügen und redundant angebunden sein kann. Als Speichermedien können eine oder mehrere Festplatten oder SSDs genutzt werden (vgl. Luber et al. 2021). |
| NTCS | New Computerised Transit System: Dieses System wurde gemäß den Vorgaben der Europäischen Kommission eingeführt und dient als elektronisches Versandverfahren zur Verwaltung und dem Monitoring bei sämtlichen Zollstellen in Österreich |
| Nuclear Electro-Magnetic Pulse | Ein nuklearer elektromagnetischer Impuls ist die Folge einer Kernwaffenexplosion in mehreren hundert Kilometern Höhe über der Erdoberfläche. Dabei führt die rasch ansteigende starke Gammastrahlung indirekt zu einem starken elektromagnetischen Impuls, der elektronische Bauteile und elektrische Anlagen stark beeinträchtigen kann. |
| Peering (bei Internetprovidern) | Peering bezeichnet in diesem Zusammenhang den Zusammenschluss gleichrangiger Netzwerke einzelner Internet Provider zum Datenaustausch. |
| Peering Points | Peering Points sind Internet-Knoten, an denen verschiedene Provider angeschlossen sind. Routing Informationen werden an diesen Knoten über das Border Gateway Protocol (BGP) ausgetauscht. |
| Releasestände | Als Release wird in der Softwareentwicklung die Veröffentlichung einer Version bezeichnet. Der Releasestand bezeichnet auf den Systemen, die eine bestimmte Software verwenden, welche Version (mit welchen Patches usw.) eingesetzt wird. |
| Resilienz | Als Resilienz wird die Fähigkeit eines Systems bezeichnet, nach einem Systemschock wieder in den stabilen Ausgangszustand zurückzukehren. Im übertragenen Sinn wird damit auch oft die Fähigkeit bezeichnet mit Krisen umzugehen, diese zu bewältigen und rasch wieder in einen Normalbetrieb überzugehen. |
| Routing (Tables) | Routing bezeichnet der Ermittlung des Weges eines Nachrichtenstroms aus einzelnen Paketen durch das Internet. In Routing Tables werden die besten Wege zu oft genutzten |

| | |
|---|---|
| | Zielen eingetragen, um den Weg nicht jedes Mal neu ermitteln zu müssen. Was der beste Weg ist, ergeben die Routing-Parameter. Ein Beispiel dafür wäre das least cost routing. Dabei wird versucht, unter Berücksichtigung der Kosten einer Datenübermittlung zwischen zwei Knoten die billigste Route für die Übermittlung zu finden. |
| S1-S6 | Die Bezeichnungen S1 bis S6 bezeichnen Sachgebiete, die innerhalb eines Krisenstabes als Stabsstellen ausgebildet sein können. Hierarchisch betrachtet sind die Leiter:innen dieser Sachgebiete unterhalb der Leitung des Krisenstabs angesiedelt. Die Aufteilung der Sachgebiete wird i.d.R. wie folgt vorgenommen:<br>S1.....Personal<br>S2.....Lage<br>S3.....Einsatz<br>S4.....Versorgung<br>S5.....Presse und Medienarbeit<br>S6.....Informations- und Kommunikationswesen |
| Security by Design | Der Begriff “Security by Design” bedeutet, dass Sicherheitsanforderungen an Hard- oder Software, oder Systeme, bereits während der Entwicklungsphase berücksichtigt werden. Je früher in der Entwicklung solche Funktionalitäten mitgedacht werden, desto kostengünstiger sind sie umzusetzen und desto mehr Spielraum gibt es für Entwickler:innen eine solide Lösung zu erarbeiten. |
| SLAs | Service Level Agreements: Rahmenverträge zwischen Serviceanbietern und Kund:innen, die eine bestimmte Servicequalität garantieren (vgl. Girs et al. 2020: 134498) |
| TETRA | Standard für ein digitales Bündelfunksystem, das bspw. in Österreich und Deutschland die technische Basis für das jeweilige Funksystem der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) bildet. |
| VPN | Virtuelles Privates Netzwerk: *VPN-Tunnel dienen der Verschlüsselung des Datenverkehrs und der Verschleierung der Identität von Nutzer:innen. Die persönliche IP-Adresse wird durch jene des VPN-Anbieters ausgetauscht. Ein solcher Tunnel verbindet die räumlich getrennten Teilnehmer:innen des virtuellen, privaten Netzwerkes digital miteinander und ist von außen nicht einsehbar (vgl. Matthews 2020)* |